(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월03일
(11) 등록번호 10-2118183
(24) 등록일자 2020년05월27일

(51) 국제특허분류(Int. Cl.)
*H04W 76/10* (2018.01) *H04L 9/30* (2006.01)
*H04W 12/06* (2009.01) *H04W 8/26* (2009.01)
*H04W 80/04* (2009.01)
(21) 출원번호 10-2014-7022284
(22) 출원일자(국제) 2013년01월10일
심사청구일자 2018년01월10일
(85) 번역문제출일자 2014년08월08일
(65) 공개번호 10-2014-0117518
(43) 공개일자 2014년10월07일
(86) 국제출원번호 PCT/US2013/020982
(87) 국제공개번호 WO 2013/106536
국제공개일자 2013년07월18일
(30) 우선권주장
61/585,420 2012년01월11일 미국(US)
61/719,663 2012년10월29일 미국(US)
(56) 선행기술조사문헌
KR1020090132650 A*
JP2006121576A
JP2007013649A
KR1020080077859A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**인터디지탈 패튼 홀딩스, 인크**
미국, 델라웨어주 19809, 윌밍턴, 벨뷰 파크웨이 200, 스위트 300
(72) 발명자
**왕 레이**
미국 캘리포니아주 92130 샌 디에고 진저 글렌 로드 13519
**타갈리 유시프**
미국 뉴저지주 07721 클리프우드 델라웨어 애비뉴 183
*(뒷면에 계속)*
(74) 대리인
**김진희, 김태홍**

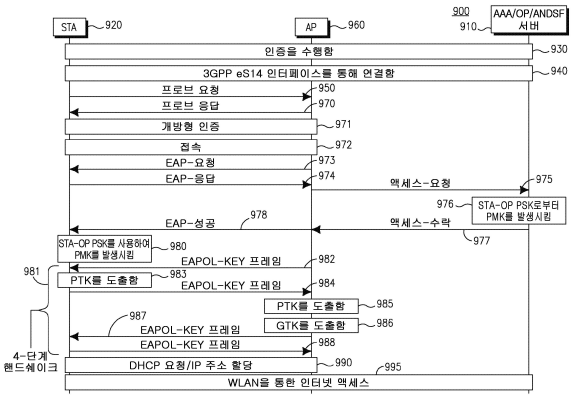
전체 청구항 수 : 총 16 항 심사관 : 윤병수

(54) 발명의 명칭 **ＩＥＥＥ 802.11 네트워크의 ＳＴＡ와 액세스 포인트 간의 가속화된 링크 설정 방법 및 장치**

## (57) 요 약

가속화된 링크 설정을 위한 방법 및 장치가 사용될 수 있다. 방법은 스테이션(STA)이 이전에 연결된 IEEE(Institute of Electrical and Electronics Engineers) 802.11 인터페이스 및/또는 IEEE 802.11 네트워크 이외의 인터페이스를 통해 사전에 IEEE 802.11 네트워크의 액세스 포인트에 관한 정보를 획득하는 단계를 포함할 수 있다. STA는, STA와 액세스 포인트 사이의 링크 설정 절차 동안, 획득된 정보를 사용할 수 있다. 정보는 STA와 액세스 포인트 사이의 링크 설정 절차를 완료하기 위한 특정의 절차에 대한 제안을 포함할 수 있다.

## 대 표 도



(72) 발명자

**그랜디 수드히어 에이**

미국 캘리포니아주 94588 플레젠튼 토노파 써클 3039

**왕 샤오페이**

미국 뉴저지주 07009 시더 그로브 체스넛 코트 30

**장 구오동**

미국 뉴욕주 11791 쇼셋 윌넛 드라이브 14

# 명 세 서

## 청구범위

### 청구항 1

액세스 포인트(access point, AP)에서 사용하는 방법에 있어서,

시스템 구성 식별자를 포함한 프로브 요청 프레임(probe request frame)을 수신하는 단계;

상기 수신된 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치하는지를 판정하는 단계;

상기 수신된 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치한다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 감소된 프로브 응답 프레임(reduced probe response frame)을 전송하는 단계; 및

상기 수신된 시스템 구성 식별자가 어떠한 저장된 시스템 구성 식별자와도 일치하지 않는다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 전체 프로브 응답 프레임(full probe response frame)을 전송하는 단계

를 포함하는, 액세스 포인트(AP)에서 사용하는 방법.

### 청구항 2

제 1 항에 있어서,

상기 수신된 시스템 구성 식별자는 구성 변경 횟수(configuration change count, CCC) 값인 것인, 액세스 포인트(AP)에서 사용하는 방법.

### 청구항 3

제 1 항에 있어서,

구성 변경이 검출될 때마다, 저장된 시스템 구성 식별자를 증가시키는 단계

를 더 포함하는, 액세스 포인트(AP)에서 사용하는 방법.

### 청구항 4

제 1 항에 있어서,

상기 프로브 요청 프레임은 상기 AP의 주소를 포함하는 것인, 액세스 포인트(AP)에서 사용하는 방법.

### 청구항 5

액세스 포인트(access point, AP)에 있어서,

시스템 구성 식별자를 포함한 프로브 요청 프레임(probe request frame)을 수신하도록 구성된 수신기;

상기 수신된 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치하는지를 판정하도록 구성된 프로세서; 및

상기 수신된 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치한다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 감소된 프로브 응답 프레임(reduced probe response frame)을 전송하도록 구성되고, 또한, 상기 수신된 시스템 구성 식별자가 어떠한 저장된 시스템 구성 식별자와도 일치하지 않는다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 전체 프로브 응답 프레임(full probe response frame)을 전송하도록 구성된 송신기

를 포함하는, 액세스 포인트(AP).

### 청구항 6

제 5 항에 있어서,

상기 수신된 시스템 구성 식별자는 구성 변경 횟수(configuration change count, CCC) 값인 것인, 액세스 포인트(AP).

**청구항 7**

제 5 항에 있어서,

구성 변경이 검출될 때마다, 저장된 시스템 구성 식별자를 증가시키는 것을 더 포함하는, 액세스 포인트(AP).

**청구항 8**

제 5 항에 있어서,

상기 프로브 요청 프레임은 상기 AP의 주소를 포함하는 것인, 액세스 포인트(AP).

**청구항 9**

비-액세스 포인트(non-access point, 비AP) 스테이션(station, STA)에서 사용하는 방법에 있어서,

액세스 포인트(access point, AP)로, 시스템 구성 식별자를 포함한 프로브 요청 프레임(probe request frame)을 전송하는 단계;

상기 전송된 시스템 구성 식별자가 상기 AP에 저장된 시스템 구성 식별자와 일치한다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 감소된 프로브 응답 프레임(reduced probe response frame)을 수신하는 단계; 및

상기 전송된 시스템 구성 식별자가 상기 AP에 저장된 어떠한 시스템 구성 식별자와도 일치하지 않는다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 전체 프로브 응답 프레임(full probe response frame)을 수신하는 단계

를 포함하는, 비-액세스 포인트 스테이션(비AP STA)에서 사용하는 방법.

**청구항 10**

제 9 항에 있어서,

상기 전송된 시스템 구성 식별자는 구성 변경 횟수(configuration change count, CCC) 값인 것인, 비-액세스 포인트 스테이션(비AP STA)에서 사용하는 방법.

**청구항 11**

비-액세스 포인트(non-access point, 비AP) 스테이션(station, STA)에 있어서,

액세스 포인트(access point, AP)로, 시스템 구성 식별자를 포함한 프로브 요청 프레임(probe request frame)을 전송하도록 구성된 송신기; 및

상기 전송된 시스템 구성 식별자가 상기 AP에 의해 저장된 시스템 구성 식별자와 일치한다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 감소된 프로브 응답 프레임(reduced probe response frame)을 수신하도록 구성되고, 또한, 상기 시스템 구성 식별자가 상기 AP에 의해 저장된 어떠한 시스템 구성 식별자와도 일치하지 않는다는 조건하에, 상기 프로브 요청 프레임에 응답하여, 전체 프로브 응답 프레임(full probe response frame)을 수신하도록 구성된 수신기

를 포함하는, 비-액세스 포인트 스테이션(비AP STA).

**청구항 12**

제 11 항에 있어서,

상기 전송된 시스템 구성 식별자는 구성 변경 횟수(configuration change count, CCC) 값인 것인, 비-액세스 포인트 스테이션(비AP STA).

**청구항 13**

제 1 항에 있어서,

상기 감소된 프로브 응답 프레임은 상기 전체 프로브 응답 프레임보다 적은 수의 정보 필드들을 포함하는 것인, 액세스 포인트(AP)에서 사용하는 방법.

**청구항 14**

제 5 항에 있어서,

상기 전체 프로브 응답 프레임은 현재의 시스템 구성 식별자를 포함하는 것인, 액세스 포인트(AP).

**청구항 15**

제 9 항에 있어서,

상기 감소된 프로브 응답 프레임은 상기 전체 프로브 응답 프레임보다 적은 수의 정보 필드들을 포함하는 것인, 비-액세스 포인트 스테이션(비AP STA)에서 사용하는 방법.

**청구항 16**

제 11 항에 있어서,

상기 전체 프로브 응답 프레임은 현재의 시스템 구성 식별자를 포함하는 것인, 비-액세스 포인트 스테이션(비AP STA).

**청구항 17**

삭제

**청구항 18**

삭제

**청구항 19**

삭제

**청구항 20**

삭제

## *발명의 설명*

### *기 술 분 야*

[0001] 관련 출원의 상호 참조

[0002] 본 출원은 2012년 1월 11일자로 출원된 미국 가특허 출원 제61/585,420호 및 2012년 10월 29일자로 출원된 미국 가특허 출원 제61/719,663호를 기초로 우선권을 주장하며, 이들 미국 출원의 내용은 참조 문헌으로서 본 명세서에 포함된다.

### *배 경 기 술*

[0003] IEEE(Institute of Electrical and Electronics Engineers) 802.11 통신 시스템에서 다수의 단계들(phases)을 포함하도록 링크 설정 절차(link setup procedure)가 구성될 수 있다. 한 예시적인 링크 설정 프로세스(link setup process)는 AP(access point, 액세스 포인트) 발견 단계, 네트워크 발견 단계, 부가의 TSF(time sync function, 시간 동기화 기능) 단계, 인증 및 접속(authentication and association) 단계, 그리고 상위 계층 IP(internet protocol, 인터넷 프로토콜) 설정 단계를 포함할 수 있다. 이러한 링크 설정 절차는 완료하는 데 최대 수 초 이상 걸릴 수 있다.

### *발명의 내용*

[0004] 방법 및 장치가 가속화된 링크 설정을 수행하도록 구성될 수 있다. 방법은 스테이션(station, STA)이 이전에 연결된 IEEE 802.11 인터페이스 및/또는 IEEE 802.11 네트워크 이외의 인터페이스를 통해 사전에 IEEE 802.11 네트워크의 AP에 관한 정보를 획득하는 단계를 포함할 수 있다. STA는, STA와 AP 사이의 링크 설정 절차 동안, 획득된 정보를 사용할 수 있다. 정보는 STA와 AP 사이의 링크 설정 절차를 완료하기 위한 특정의 절차에 대한

제안을 포함할 수 있다.

[0005] 방법 및 장치는, 다른 네트워크의 발견을 가능하게 하고 최적화하기 위해, STA와 네트워크 사이의 보안 접속(security association)을 사전 설정(pre-establish)하는 데 사용될 수 있다. 예를 들어, 고속 EAP(fast-EAP)가, 예를 들어, 인증 프레임(authentication frame) 또는 접속 프레임(association frame)과 같은 802.11 프레임 내에 캡슐화될 수 있다. 새로운 네트워크에 대해 수행되는 인증 절차는 비EAP(non-EAP) 기반일 수 있다.

[0006] 장치는 네트워크 엔터티에 대한 네트워크 발견 정보의 요청을 전송하고, 그에 응답하여, 네트워크 발견 정보를 수신할 수 있다. 네트워크 발견 정보는 셀룰러 네트워크(예를 들어, 3GPP 네트워크)를 거쳐 수신될 수 있다. 네트워크 발견 정보는 계층 2 프로토콜을 통해 수신될 수 있다.

[0007] 장치는 네트워크에 대한 IP 주소 구성(IP address configuration)을 획득하라는 요청을 전송할 수 있다. 예를 들어, 장치는 EAP 인증 프로세스 동안 또는 비EAP 인증 프로세스 동안 IP 주소 구성을 요청하고 수신할 수 있다. IP 주소 구성은 셀룰러 네트워크(예를 들어, 3GPP 네트워크)를 거쳐 수신될 수 있다.

## *도면의 간단한 설명*

[0008] 일례로서 첨부 도면과 관련하여 주어진 이하의 설명으로부터 보다 상세하게 이해할 수 있다.

도 1a는 하나 이상의 개시된 실시예들이 구현될 수 있는 예시적인 통신 시스템의 시스템도.

도 1b는 도 1a에 예시된 통신 시스템 내에서 사용될 수 있는 예시적인 WTRU(wireless transmit/receive unit, 무선 송수신 유닛)의 시스템도.

도 1c는 도 1a에 예시된 통신 시스템 내에서 사용될 수 있는 예시적인 무선 액세스 네트워크 및 예시적인 코어 네트워크의 시스템도.

도 2a는 한 예시적인 IEEE 802.11 설정 절차(IEEE 802.11 setup procedure)를 나타낸 도면.

도 2b는 도 2a에 도시된 예시적인 IEEE 802.11 설정 절차를 계속하여 나타낸 도면.

도 3은 사전 획득된 정보를 사용하는 ALS(accelerated link setup, 가속화된 링크 설정)를 위한 기준 절차(baseline procedure)의 플로우차트.

도 4는 ALS(accelerated link setup)를 지원하는 한 예시적인 짧은 비콘 프레임(short beacon frame)을 나타낸 도면.

도 5는 ALS를 지원하는 주 비콘 프레임(primary beacon frame)에 대한 한 예시적인 수정을 나타낸 도면.

도 6은 한 예시적인 FILS(fast initial link setup, 고속 초기 링크 설정) 관리 동작 프레임(management action frame)을 나타낸 도면.

도 7은 사전 획득된 지식에 기초하여 STA에 의해 개시되는 최적화된 AP(access point) 발견 절차의 한 예를 나타낸 도면.

도 8은 사전 획득된 정보에 기초하여 AP에 의해 개시되는 최적화된 AP 발견 절차의 한 예를 나타낸 도면.

도 9는 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA(authentication, authorization, and accounting, 인증, 권한 부여 및 계정 관리) 서버가 OP(Identity Provider, ID 제공자) 기능 및 eANDSF(enhanced access network discovery and selection function, 향상된 액세스 네트워크 발견 및 선택 기능) 기능을 통합시킬 수 있는 한 예시적인 방법을 나타낸 도면.

도 10은 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA(authentication, authorization, and accounting) 서버가 OP 기능 및 eANDSF(enhanced access network discovery and selection function) 기능을 통합시킬 수 있는 다른 예시적인 방법을 나타낸 도면.

도 11은 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA 서버가 OP 기능을 통합시킬 수 있는 한 예시적인 방법을 나타낸 도면.

도 12는 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA 서버가 OP 기능을 통합시킬 수 있는 다른 예시적인 방법을 나타낸 도면.

도 13은 매끄러운 인증 및 고속 초기 링크 설정을 가능하게 하기 위해 STA와 네트워크 사이의 사전 설정된 보안 접속을 위한 한 예시적인 방법을 나타낸 도면.

도 14는 매끄러운 인증 및 고속 초기 링크 설정을 가능하게 하기 위해 STA와 네트워크 사이의 사전 설정된 보안 접속을 위한 다른 예시적인 방법을 나타낸 도면.

도 15는 매끄러운 인증 및 고속 초기 링크 설정을 가능하게 하기 위해 STA와 네트워크 사이의 사전 설정된 보안 접속을 위한 다른 예시적인 방법을 나타낸 도면.

도 16은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 한 예시적인 방법을 나타낸 도면.

도 17은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 다른 예시적인 방법을 나타낸 도면.

도 18은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 다른 예시적인 방법을 나타낸 도면.

도 19는 STA가 전체 구성 인스턴스 정보(full configuration instance information) 없이 구성 인스턴스 식별자 정보(configuration instance identifier information)를 수신할 수 있는 한 예시적인 방법을 나타낸 도면.

도 20은 STA가 사전 획득된 시스템 구성에 대한 구성 인스턴스 식별자 정보를 포함시킬 수 있는 한 예시적인 방법을 나타낸 도면.

도 21은 위치 기반의 사전 획득된 지식에 의해 고속 링크 설정을 수행하는 한 예시적인 방법을 나타낸 도면.

도 22는 링크 설정 최적화를 위한 한 예시적인 방법을 나타낸 도면.

## *발명을 실시하기 위한 구체적인 내용*

[0009] 도 1a는 하나 이상의 개시된 실시예들이 구현될 수 있는 예시적인 통신 시스템(100)의 도면이다. 통신 시스템(100)은 음성, 데이터, 비디오, 메시징, 방송 등과 같은 콘텐츠를 다수의 무선 사용자에게 제공하는 다중 접속 시스템일 수 있다. 통신 시스템(100)은 다수의 무선 사용자가 시스템 자원(무선 대역폭을 포함함)의 공유를 통해 이러한 콘텐츠에 액세스할 수 있게 해줄 수 있다. 예를 들어, 통신 시스템(100)은 CDMA(code division multiple access, 코드 분할 다중 접속), TDMA(time division multiple access, 시분할 다중 접속), FDMA(frequency division multiple access, 주파수 분할 다중 접속), OFDMA(orthogonal FDMA, 직교 FDMA), SC-FDMA(single-carrier FDMA, 단일 반송파 FDMA) 등과 같은 하나 이상의 채널 접속 방법들을 이용할 수 있다.

[0010] 도 1a에 도시된 바와 같이, 통신 시스템(100)은 WTRU(wireless transmit/receive unit)(102a, 102b, 102c, 102d), RAN(radio access network, 무선 액세스 네트워크)(104), 코어 네트워크(106), PSTN(public switched telephone network, 공중 교환 전화망)(108), 인터넷(110), 및 기타 네트워크들(112)을 포함할 수 있지만, 개시된 실시예가 임의의 수의 WTRU, 기지국, 네트워크 및/또는 네트워크 요소를 생각하고 있다는 것을 잘 알 것이다. WTRU(102a, 102b, 102c, 102d) 각각은 무선 환경에서 동작하고 및/또는 통신하도록 구성되어 있는 임의의 유형의 디바이스일 수 있다. 일례로서, WTRU(102a, 102b, 102c, 102d)는 무선 신호를 전송 및/또는 수신하도록 구성될 수 있고, UE(user equipment, 사용자 장비), 이동국, 고정형 또는 이동형 가입자 유닛, 페이저, 휴대폰, PDA(personal digital assistant, 개인 휴대 단말기), 스마트폰, 랩톱, 넷북, 개인용 컴퓨터, 무선 센서, 가전 제품, IEEE 802.11 네트워크에서의 STA(station, 스테이션) 등을 포함할 수 있다.

[0011] 통신 시스템(100)은 또한 기지국(114a) 및 기지국(114b)을 포함할 수 있다. 기지국(114a, 114b) 각각은 하나 이상의 통신 네트워크들 - 코어 네트워크(106), 인터넷(110) 및/또는 네트워크들(112) 등 - 에 대한 액세스를 용이하게 해주기 위해 WTRU(102a, 102b, 102c, 102d) 중 적어도 하나와 무선으로 인터페이스하도록 구성되어 있는 임의의 유형의 디바이스일 수 있다. 예로서, 기지국들(114a, 114b)은 BTS(base transceiver station, 기지국 송수신기), 노드-B, eNode-B, 홈 노드 B, 사이트 제어기, AP(access point), 무선 라우터 등일 수 있다. 기지국들(114a, 114b) 각각이 단일 요소로서 나타내어져 있지만, 기지국들(114a, 114b)이 임의의 수의 상호연결된 기지국들 및/또는 네트워크 요소들을 포함할 수 있다는 것을 잘 알 것이다.

[0012] 기지국(114a)은 다른 기지국들 및/또는 네트워크 요소들(도시 생략) - BSC(base station controller, 기지국 제어기), RNC(radio network controller, 무선 네트워크 제어기), 중계 노드, 기타 등등 - 도 포함할 수 있는 RAN(104)의 일부일 수 있다. 기지국(114a) 및/또는 기지국(114b)은 특정의 지리적 지역 - 셀(도시 생략)이라고 할 수 있음 - 내에서 무선 신호를 전송 및/또는 수신하도록 구성될 수 있다. 셀은 여러 셀 섹터(cell sector)로 추가로 나누어질 수 있다. 예를 들어, 기지국(114a)과 연관된 셀이 3개의 섹터로 나누어질 수 있다. 따라

서, 일 실시예에서 기지국(114a)은 3개의 송수신기(즉, 셀의 각각의 섹터마다 하나씩)를 포함할 수 있다. 다른 실시예에서, 기지국(114a)은 MIMO(multiple-input multiple output, 다중 입력 다중 출력) 기술을 이용할 수 있고, 따라서, 셀의 각각의 섹터에 대해 다수의 송수신기를 이용할 수 있다.

[0013] 기지국(114a, 114b)은 임의의 적당한 무선 통신 링크[예컨대, RF(radio frequency, 무선 주파수), 마이크로파, IR(infrared, 적외선), UV(ultraviolet, 자외선), 가시광 등]일 수 있는 공중 인터페이스(116)를 통해 WTRU(102a, 102b, 102c, 102d) 중 하나 이상과 통신할 수 있다. 임의의 적당한 RAT(radio access technology, 무선 액세스 기술)를 사용하여 공중 인터페이스(116)가 설정될 수 있다.

[0014] 보다 구체적으로는, 앞서 살펴본 바와 같이, 통신 시스템(100)은 다중 접속 시스템일 수 있고, CDMA, TDMA, FDMA, OFDMA, SC-FDMA 등과 같은 하나 이상의 채널 접속 방식들을 이용할 수 있다. 예를 들어, RAN(104) 내의 기지국(114a) 및 WTRU(102a, 102b, 102c)는 WCDMA(wideband CDMA, 광대역 CDMA)를 사용하여 공중 인터페이스(116)를 설정할 수 있는 UTRA[UMTS(Universal Mobile Telecommunications System) Terrestrial Radio Access]와 같은 무선 기술을 구현할 수 있다. WCDMA는 HSPA(High-Speed Packet Access, 고속 패킷 액세스) 및/또는 HSPA+(Evolved HSPA)와 같은 통신 프로토콜을 포함할 수 있다. HSPA는 HSDPA(High-Speed Downlink Packet Access, 고속 하향링크 패킷 액세스) 및/또는 HSUPA(High-Speed Uplink Packet Access, 고속 상향링크 패킷 액세스)를 포함할 수 있다.

[0015] 다른 실시예에서, 기지국(114a) 및 WTRU(102a, 102b, 102c)는 LTE(Long Term Evolution) 및/또는 LTE-A(LTE-Advanced)를 사용하여 공중 인터페이스(116)를 설정할 수 있는 E-UTRA(Evolved UMTS Terrestrial Radio Access)와 같은 무선 기술을 구현할 수 있다.

[0016] 다른 실시예에서, 기지국(114a) 및 WTRU(102a, 102b, 102c)는 IEEE 802.16[즉, WiMAX(Worldwide Interoperability for Microwave Access)], CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, IS-2000(Interim Standard 2000), IS-95(Interim Standard 95), IS-856(Interim Standard 856), GSM(Global System for Mobile communications), EDGE(Enhanced Data rates for GSM Evolution), GSM EDGE(GERAN) 등과 같은 무선 기술을 구현할 수 있다.

[0017] 도 1a의 기지국(114b)은, 예를 들어, 무선 라우터, 홈 노드 B, 홈 eNode B, 또는 액세스 포인트(access point)일 수 있고, 사업장, 가정, 차량, 캠퍼스 등과 같은 국소화된 지역에서의 무선 연결을 용이하게 해주는 임의의 적당한 RAT를 이용할 수 있다. 일 실시예에서, 기지국(114b) 및 WTRU(102c, 102d)는 WLAN(wireless local area network, 무선 근거리 통신망)을 설정하기 위해 IEEE 802.11과 같은 무선 기술을 구현할 수 있다. 다른 실시예에서, 기지국(114b) 및 WTRU(102c, 102d)는 WPAN(wireless personal area network, 무선 개인 영역 네트워크)을 설정하기 위해 IEEE 802.15와 같은 무선 기술을 구현할 수 있다. 또 다른 실시예에서, 기지국(114b) 및 WTRU(102c, 102d)는 피코셀(picocell) 또는 펨토셀(femtocell)을 설정하기 위해 셀룰러-기반 RAT(예컨대, WCDMA, CDMA2000, GSM, LTE, LTE-A 등)를 이용할 수 있다. 도 1a에 도시된 바와 같이, 기지국(114b)은 인터넷(110)에의 직접 연결을 가질 수 있다. 따라서, 기지국(114b)은 코어 네트워크(106)를 통해 인터넷(110)에 액세스할 필요가 없을 수 있다.

[0018] RAN(104)은 음성, 데이터, 응용 프로그램, 및 VoIP(voice over internet protocol) 서비스를 WTRU들(102a, 102b, 102c, 102d) 중 하나 이상의 WTRU들에 제공하도록 구성되어 있는 임의의 유형의 네트워크일 수 있는 코어 네트워크(106)와 통신하고 있을 수 있다. 예를 들어, 코어 네트워크(106)는 호출 제어, 대금 청구 서비스, 모바일 위치-기반 서비스, 선불 전화(pre-paid calling), 인터넷 연결, 비디오 배포 등을 제공하고 및/또는 사용자 인증과 같은 고수준 보안 기능을 수행할 수 있다. 도 1a에 도시되어 있지는 않지만, RAN(104) 및/또는 코어 네트워크(106)가 RAN(104)과 동일한 RAT 또는 상이한 RAT를 이용하는 다른 RAN과 직접 또는 간접 통신을 하고 있을 수 있다는 것을 잘 알 것이다. 예를 들어, E-UTRA 무선 기술을 이용하고 있을 수 있는 RAN(104)에 연결되는 것에 부가하여, 코어 네트워크(106)는 또한 GSM 무선 기술을 이용하는 다른 RAN(도시 생략)과 통신하고 있을 수 있다.

[0019] 코어 네트워크(106)는 또한 WTRU(102a, 102b, 102c, 102d)가 PSTN(108), 인터넷(110) 및/또는 기타 네트워크들(112)에 액세스하기 위한 게이트웨이로서 역할할 수 있다. PSTN(108)은 POTS(plain old telephone service)를 제공하는 회선-교환 전화 네트워크를 포함할 수 있다. 인터넷(110)은 TCP/IP 인터넷 프로토콜군 내의 TCP(transmission control protocol, 전송 제어 프로토콜), UDP(user datagram protocol, 사용자 데이터그램 프로토콜) 및 IP(internet protocol, 인터넷 프로토콜)와 같은 공통의 통신 프로토콜을 사용하는 상호연결된 컴퓨터 네트워크들 및 디바이스들의 전세계 시스템(global system)을 포함할 수 있다. 네트워크들(112)은 다른

서비스 공급자가 소유하고 및/또는 운영하는 유선 또는 무선 통신 네트워크를 포함할 수 있다. 예를 들어, 네트워크들(112)은 RAN(104)과 동일한 RAT 또는 상이한 RAT를 이용할 수 있는 하나 이상의 RAN들에 연결된 다른 코어 네트워크를 포함할 수 있다.

[0020] 통신 시스템(100) 내의 WTRU(102a, 102b, 102c, 102d) 중 일부 또는 전부는 다중-모드 기능을 포함할 수 있다 - 즉, WTRU(102a, 102b, 102c, 102d)가 상이한 무선 링크를 통해 상이한 무선 네트워크와 통신하기 위한 다수의 송수신기를 포함할 수 있다 -. 예를 들어, 도 1a에 도시된 WTRU(102c)는 셀룰러-기반 무선 기술을 이용할 수 있는 기지국(114a)과 통신하도록, 그리고 IEEE 802 무선 기술을 이용할 수 있는 기지국(114b)과 통신하도록 구성될 수 있다. WTRU는 STA(station) 또는 비-액세스 포인트(non-access point, 비AP) STA라고 할 수 있다.

[0021] 도 1b는 예시적인 WTRU(102)의 시스템도이다. 도 1b에 도시된 바와 같이, WTRU(102)는 프로세서(118), 송수신기(120), 송신/수신 요소(122), 스피커/마이크(124), 키패드(126), 디스플레이/터치패드(128), 비이동식 메모리(106), 이동식 메모리(132), 전원 공급 장치(134), GPS(global positioning system, 위성 위치 확인 시스템) 칩셋(136), 및 기타 주변 장치들(138)을 포함할 수 있다. 실시예와 부합한 채로 있으면서 WTRU(102)가 상기한 요소들의 임의의 서브컴비네이션을 포함할 수 있다는 것을 잘 알 것이다.

[0022] 프로세서(118)가 범용 프로세서, 전용 프로세서, 종래의 프로세서, DSP(digital signal processor, 디지털 신호 처리기), 복수의 마이크로프로세서들, DSP 코어와 연관된 하나 이상의 마이크로프로세서들, 제어기, 마이크로제어기, ASIC(Application Specific Integrated Circuit, 주문형 반도체), FPGA(Field Programmable Gate Array, 현장 프로그램가능 게이트 어레이) 회로, 임의의 다른 유형의 IC(integrated circuit, 집적 회로), 상태 기계 등일 수 있다. 프로세서(118)는 WTRU(102)가 무선 환경에서 동작할 수 있게 해주는 신호 코딩, 데이터 처리, 전력 제어, 입력/출력 처리, 및/또는 임의의 다른 기능을 수행할 수 있다. 프로세서(118)는 송신/수신 요소(122)에 결합되어 있을 수 있는 송수신기(120)에 결합될 수 있다. 도 1b가 프로세서(118) 및 송수신기(120)를 개별 구성요소로서 나타내고 있지만, 프로세서(118) 및 송수신기(120)가 전자 패키지 또는 칩에 함께 통합되어 있을 수 있다는 것을 잘 알 것이다.

[0023] 송신/수신 요소(122)는 공중 인터페이스(116)를 통해 기지국[예컨대, 기지국(114a)]으로 신호를 전송하거나 기지국으로부터 신호를 수신하도록 구성될 수 있다. 예를 들어, 일 실시예에서, 송신/수신 요소(122)는 RF 신호를 전송 및/또는 수신하도록 구성된 안테나일 수 있다. 다른 실시예에서, 송신/수신 요소(122)는, 예를 들어, IR, UV 또는 가시광 신호를 전송 및/또는 수신하도록 구성되어 있는 방출기/검출기일 수 있다. 또 다른 실시예에서, 송신/수신 요소(122)는 RF 신호 및 광 신호 둘 다를 전송 및 수신하도록 구성될 수 있다. 송신/수신 요소(122)가 무선 신호의 임의의 조합을 전송 및/또는 수신하도록 구성될 수 있다는 것을 잘 알 것이다.

[0024] 그에 부가하여, 송신/수신 요소(122)가 도 1b에 단일 요소로서 나타내어져 있지만, WTRU(102)는 임의의 수의 송신/수신 요소(122)를 포함할 수 있다. 보다 구체적으로는, WTRU(102)는 MIMO 기술을 이용할 수 있다. 따라서, 일 실시예에서, WTRU(102)는 공중 인터페이스(116)를 통해 무선 신호를 전송 및 수신하기 위한 2개 이상의 송신/수신 요소(122)(예컨대, 다수의 안테나)를 포함할 수 있다.

[0025] 송수신기(120)는 송신/수신 요소(122)에 의해 전송되어야 하는 신호를 변조하고 송신/수신 요소(122)에 의해 수신되는 신호를 복조하도록 구성될 수 있다. 앞서 살펴본 바와 같이, WTRU(102)는 다중-모드 기능을 가질 수 있다. 따라서, 송수신기(120)는 WTRU(102)가, 예를 들어, UTRA 및 IEEE 802.11과 같은 다수의 RAT를 통해 통신할 수 있게 해주는 다수의 송수신기를 포함할 수 있다.

[0026] WTRU(102)의 프로세서(118)는 스피커/마이크(124), 키패드(126), 및/또는 디스플레이/터치패드(128)[예컨대, LCD(liquid crystal display, 액정 디스플레이) 디스플레이 유닛 또는 OLED(organic light-emitting diode, 유기 발광 다이오드) 디스플레이 유닛]에 결합될 수 있고 그로부터 사용자 입력 데이터를 수신할 수 있다. 프로세서(118)는 또한 사용자 데이터를 스피커/마이크(124), 키패드(126) 및/또는 디스플레이/터치패드(128)로 출력할 수 있다. 그에 부가하여, 프로세서(118)는 비이동식 메모리(106) 및/또는 이동식 메모리(132)와 같은 임의의 유형의 적당한 메모리로부터의 정보에 액세스하고 그 메모리에 데이터를 저장할 수 있다. 비이동식 메모리(106)는 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 하드 디스크, 임의의 다른 유형의 메모리 저장 디바이스를 포함할 수 있다. 이동식 메모리(132)는 SIM(subscriber identity module, 가입자 식별 모듈) 카드, 메모리 스틱, SD(secure digital) 메모리 카드 등을 포함할 수 있다. 다른 실시예에서, 프로세서(118)는 WTRU(102) 상에 물리적으로 위치하지 않은[예컨대, 서버 또는 가정용 컴퓨터(도시 생략) 상의] 메모리로부터의 정보에 액세스하고 그 메모리에 데이터를 저장할 수 있다.

[0027] 프로세서(118)는 전원 공급 장치(134)로부터 전력을 받을 수 있고, WTRU(102) 내의 다른 구성요소로 전력을 분배하고 및/또는 전력을 제어하도록 구성될 수 있다. 전원 공급 장치(134)는 WTRU(102)에 전원을 제공하는 임의의 적당한 디바이스일 수 있다. 예를 들어, 전원 공급 장치(134)는 하나 이상의 건전지들[예컨대, 니켈-카드뮴(NiCd), 니켈-아연(NiZn), 니켈 수소화금속(NiMH), 리튬-이온(Li--ion) 등], 태양 전지들, 연료 전지들 등을 포함할 수 있다.

[0028] 프로세서(118)는 또한 WTRU(102)의 현재 위치에 관한 위치 정보(예컨대, 경도 및 위도)를 제공하도록 구성될 수 있는 GPS 칩셋(136)에 결합될 수 있다. GPS 칩셋(136)으로부터의 정보에 부가하여 또는 그 대신에, WTRU(102)는 기지국[예컨대, 기지국(114a, 114b)] 공중 인터페이스(116)를 통해 위치 정보를 수신하고 및/또는 2개 이상의 근방의 기지국으로부터 수신되는 신호의 타이밍에 기초하여 그의 위치를 결정할 수 있다. 실시예와 부합한 채로 있으면서 WTRU(102)가 임의의 적당한 위치 결정 방법에 의해 위치 정보를 획득할 수 있다는 것을 잘 알 것이다.

[0029] 프로세서(118)는 또한 부가의 특징들, 기능 및/또는 유선 또는 무선 연결을 제공하는 하나 이상의 소프트웨어 및/또는 하드웨어 모듈들을 포함할 수 있는 기타 주변 장치들(138)에 결합될 수 있다. 예를 들어, 주변 장치들(138)은 가속도계, 전자 나침반, 위성 송수신기, 디지털 카메라(사진 또는 비디오용), USB(universal serial bus) 포트, 진동 디바이스, 텔레비전 송수신기, 핸즈프리 헤드셋, 블루투스® 모듈, FM(frequency modulated, 주파수 변조) 라디오 유닛, 디지털 음악 플레이어, 미디어 플레이어, 비디오 게임 플레이어 모듈, 인터넷 브라우저 등을 포함할 수 있다.

[0030] 도 1c는 RAN(104) 및 코어 네트워크(106)의 예시적인 시스템도이다. 앞서 살펴본 바와 같이, RAN(104)은 공중 인터페이스(116)를 통해 WTRU(102a, 102b, 102c)와 통신하기 위해 E-UTRA 무선 기술을 이용할 수 있다. RAN(104)은 또한 코어 네트워크(106)와 통신하고 있을 수 있다.

[0031] RAN(104)은 eNode B(140a, 140b, 140c)를 포함할 수 있지만, 실시예와 부합한 채로 있으면서 RAN(104)이 임의의 수의 eNode B를 포함할 수 있다는 것을 잘 알 것이다. eNode B(140a, 140b, 140c) 각각은 공중 인터페이스(116)를 통해 WTRU(102a, 102b, 102c)와 통신하기 위한 하나 이상의 송수신기들을 포함할 수 있다. 일 실시예에서, eNode B(140a, 140b, 140c)는 MIMO 기술을 구현할 수 있다. 따라서, 예를 들어, eNode B(140a)는 WTRU(102a)로 무선 신호를 전송하고 그로부터 무선 신호를 수신하기 위해 다수의 안테나를 사용할 수 있다.

[0032] eNode B(140a, 140b, 140c) 각각은 특정의 셀(도시 생략)과 연관되어 있을 수 있고, 무선 자원 관리 결정, 핸드오버 결정, 상향링크 및/또는 하향링크에서의 사용자의 스케줄링 등을 처리하도록 구성되어 있을 수 있다. 도 1c에 도시된 바와 같이, eNode B(140a, 140b, 140c)는 X2 인터페이스를 통해 서로 통신할 수 있다.

[0033] 도 1c에 도시된 코어 네트워크(106)는 MME(mobility management gateway, 이동성 관리 게이트웨이)(142), SGW(serving gateway, 서비스 제공 게이트웨이)(144), 및 PDN(packet data network, 패킷 데이터 네트워크) 게이트웨이(146)를 포함할 수 있다. 상기 요소들 각각이 코어 네트워크(106)의 일부로서 나타내어져 있지만, 이들 요소 중 임의의 것이 코어 네트워크 운영자 이외의 엔터티에 의해 소유되고 및/또는 운영될 수 있다는 것을 잘 알 것이다.

[0034] MME(142)는 S1 인터페이스를 통해 RAN(104) 내의 eNode B(142a, 142b, 142c) 각각에 연결되어 있을 수 있고, 제어 노드로서 역할할 수 있다. 예를 들어, MME(142)는 WTRU(102a, 102b, 102c)의 사용자를 인증하는 것, 베어러 활성화/비활성화, WTRU(102a, 102b, 102c)의 초기 접속(initial attach) 동안 특정의 SGW(serving gateway)를 선택하는 것 등을 책임지고 있을 수 있다. MME(142)는 또한 RAN(104)과 GSM 또는 WCDMA와 같은 다른 무선 기술을 이용하는다른 RAN(도시 생략) 간에 전환하는 제어 평면 기능(control plane function)을 제공할 수 있다.

[0035] SGW(serving gateway)(144)는 S1 인터페이스를 통해 RAN(104) 내의 eNode B(140a, 140b, 140c) 각각에 연결될 수 있다. 서비스 제공 게이트웨이(144)는 일반적으로 WTRU(102a, 102b, 102c)로/로부터 사용자 데이터 패킷을 라우팅하고 전달할 수 있다. SGW(serving gateway)(144)는 eNode B간 핸드오버 동안 사용자 평면을 앵커링(anchoring)하는 것, WTRU(102a, 102b, 102c)에 대해 하향링크 데이터가 이용가능할 때 페이징(paging)을 트리거하는 것, WTRU(102a, 102b, 102c)의 컨텍스트를 관리하고 저장하는 것 등과 같은 다른 기능도 수행할 수 있다.

[0036] SGW(serving gateway)(144)는, WTRU(102a, 102b, 102c)와 IP-기반(IP-enabled) 디바이스 사이의 통신을 용이하게 해주기 위해, 인터넷(110)과 같은 패킷 교환 네트워크에 대한 액세스를 WTRU(102a, 102b, 102c)에 제공할 수

있는 PDN 게이트웨이(146)에도 연결될 수 있다. WLAN(wireless local area network)(155)의 AR(access router, 액세스 라우터)(150)은 인터넷(110)과 통신하고 있을 수 있다. AR(150)은 AP들(160a, 160b, 및 160c) 간의 통신을 용이하게 해줄 수 있다. AP(160a, 160b, 및 160c)는 STA(170a, 170b, 및 170c)와 통신하고 있을 수 있다.

[0037] 코어 네트워크(106)는 기타 네트워크들과의 통신을 용이하게 해줄 수 있다. 예를 들어, 코어 네트워크(106)는, WTRU(102a, 102b, 102c)와 종래의 지상선(land-line) 통신 디바이스 사이의 통신을 용이하게 해주기 위해, PSTN(108)과 같은 회선 교환 네트워크에의 액세스를 WTRU(102a, 102b, 102c)에 제공할 수 있다. 예를 들어, 코어 네트워크(106)는 코어 네트워크(106)와 PSTN(108) 사이의 인터페이스로서 역할하는 IP 게이트웨이[예컨대, IMS(IP multimedia subsystem, IP 멀티미디어 서브시스템) 서버]를 포함할 수 있거나 그와 통신할 수 있다. 그에 부가하여, 코어 네트워크(106)는 다른 서비스 공급자에 의해 소유되고 및/또는 운영되는 다른 유선 또는 무선 네트워크를 포함할 수 있는 네트워크들(112)에 대한 액세스를 WTRU(102a, 102b, 102c)에 제공할 수 있다.

[0038] 도 2a 및 도 2b는 802.11i/EAP(Extensible Authentication Protocol, 확장가능 인증 프로토콜)가 사용될 수 있는 한 예시적인 IEEE 802.11 링크 설정 절차를 나타낸 도면들이다. 이 예시적인 절차(200)는 AP 발견 단계(201), 네트워크 발견 단계(202), 부가의 TSF(time sync function) 단계(203), 인증 단계(204), 접속 단계(205), 보안 설정 단계(206), 및 IP 설정 단계(207)를 포함할 수 있다. 무선 통신 시스템은 하나 이상의 스테이션들(STA들)(208), 하나 이상의 AP들(209a, 209b, 209c), 및 하나 이상의 네트워크 요소들(209d)을 포함할 수 있다. STA(208)는 WTRU(wireless transmit/receive unit) 또는 비AP STA를 포함할 수 있고, 네트워크 요소(209d)는, 예를 들어, 라우터, HA(home agent, 홈 에이전트), AAA(authentication, authorization, and accounting) 서버, AS(authentication server, 인증 서버), 또는 RADIUS(remote authentication dial-in user service, 원격 인증 다이얼인 사용자 서비스)를 포함할 수 있다.

[0039] AP 발견 단계(201)에서, STA(208)는 도달 거리 내의 AP들을 찾아내기 위해 능동 스캔(active scanning) 또는 수동 스캔(passive scanning)을 사용할 수 있다. 능동 스캔 예에서, STA(208)는 각자의 프로브 요청 프레임들(probe request frames)(211a, 211b, 211c)을 AP1(209a), AP2(209b), 및 APn(209c)으로 전송할 수 있다. 그에 응답하여, 각각의 AP는 각자의 프로브 응답 프레임(probe response frame)(212a, 212b, 212c)을 STA(208)로 전송할 수 있다. 수동 스캔 예에서, STA(208)는, 프로브 요청/응답 프레임 교환을 수행하기 전에, AP1(209a), AP2(209b), 및 APn(209c)으로부터 각자의 비콘들(210a, 210b, 210c)을 수신하기 위해 기다릴 수 있다.

[0040] 네트워크 발견 단계(202)에서, STA(208)는 GAS(guarded action system) 초기 요청(initial request) 프레임(213a)을, 예를 들어, AP1(209a)로 전송함으로써 적당한 서비스 제공자 네트워크를 검색할 수 있다. 그에 응답하여, AP1(209a)은 질의 요청(query request)(213b)을 네트워크 요소(209d)로 전송하고, 질의 응답(query response)(213c)을 수신할 수 있다. 질의 응답(213c)을 수신한 것에 응답하여, AP1(209a)은 GAS 초기 응답(initial response) 프레임(213d)을 STA(208)로 전송할 수 있다. STA(208)는 GAS 컴백 요청(comeback request) 프레임(213e)을 AP1(209a)로 전송하고, 그에 응답하여, GAS 컴백 요청 프레임(213f)을 수신할 수 있다. 필요한 경우, 예를 들어, GAS 응답이 너무 커서 하나의 MMPDU(MAC management protocol data unit, MAC 관리 프로토콜 데이터 단위)에 들어가지 못하고 배달을 위해 GAS 단편화(GAS fragmentation)가 사용되는 경우, 하나 이상의 GAS 컴백 요청/응답 교환들(213g)이 수행될 수 있다.

[0041] 부가의 TSF 단계(203)가 수행될 수 있다. TSF 단계(203) 동안, STA(208)는 프로브 요청 프레임(214a)을, 예를 들어, AP1(209a)로 전송하고, 그에 응답하여, 프로브 응답 프레임(214b)을 수신할 수 있다. 부가의 TSF 단계는, 예를 들어, AP1(209a)과 STA(208) 사이에서 시간 동기화 타이머들을 추가적으로 동기화시키기 위해 사용될 수 있다. 동기화는 프로브 응답 프레임(214b) 내의 타임스탬프 필드를 사용하여 수행될 수 있다.

[0042] 인증 단계(204)가 수행될 수 있다. 인증 단계(204) 동안, STA(208)는 인증 요청(authentication request) 프레임(215a)을, 예를 들어, AP1(209a)로 전송하고, 그에 응답하여, 인증 응답(authentication response) 프레임(214b)을 수신할 수 있다.

[0043] 접속 단계(205)가 수행될 수 있다. 접속 단계(205) 동안, STA(208)는 접속 요청(association request) 프레임(216a)을, 예를 들어, AP1(209a)로 전송하고, 그에 응답하여, 접속 응답(association response) 프레임(214b)을 수신할 수 있다.

[0044] 보안 설정 단계(206)가 수행될 수 있다. STA(208)는 EAPOL[EAP(extensible authentication protocol) over LAN(local area network)] 시작 프레임(217a)을, 예를 들어, AP1(209a)로 전송하는 것에 의해 보안 설정 단계

(206)를 개시할 수 있다. AP1(209a)은 EAP 요청 프레임(217b)을 STA(208)로 전송할 수 있다. EAP 요청 프레임(217b)은 AP1(209a)의 ID(identity)를 나타내는 필드를 포함할 수 있다. STA(208)는, 그에 응답하여, EAP 응답 프레임(217c)을 AP1(209a)로 전송할 수 있다. EAP 응답 프레임(217c)은 STA(208)의 ID(identity)를 나타내는 필드를 포함할 수 있다. AP1(209a)은, 예를 들어, AAA 프로토콜을 사용하여 요청 프레임(217d)을 네트워크 요소(209d)로 전송할 수 있다. 요청 프레임(217d)은 STA(208)의 ID(identity)를 나타내는 필드를 포함할 수 있다.

[0045] 네트워크 요소(209d)는, 그에 응답하여, 신청(challenge)/TLS(transport layered security, 전송 계층 보안) 시작 프레임을 AP1(209a)로 전송할 수 있다. AP1(209a)은 EAP 요청/TLS 시작 프레임(217f)을 STA(208)로 전송할 수 있다. 그에 응답하여, STA(208)는 EAP 응답/TLS 클라이언트 헬로(client hello) 프레임(217g)을 AP1(209a)로 전송할 수 있다. AP1(209a)은 요청/통과(pass through) 프레임(217h)을 네트워크 요소(209d)로 전송하고, 그에 응답하여, 신청/서버 인증서 프레임(217i)을 수신할 수 있다. AP1(209a)은 EAP 요청/통과 프레임(217j)을 STA(208)로 전송하고, 그에 응답하여, EAP 응답/클라이언트 인증서 프레임(217k)을 수신할 수 있다.

[0046] AP1(209a)은 요청/통과 프레임(217l)을 네트워크 요소(209d)로 전송하고, 그에 응답하여, 신청/암호화 유형 프레임(217m)을 수신할 수 있다. AP1(209a)은 EAP 요청/통과 프레임(217n)을 STA(208)로 전송하고, 그에 응답하여, EAP 응답 프레임(217o)을 수신할 수 있다. AP1(209a)은 요청 프레임(217p)을 네트워크 요소(209d)로 전송하고, 그에 응답하여, 수락 프레임(217q)을 수신할 수 있다. AP1(209a)은 EAP 성공 프레임(217r)을 STA(208)로 전송할 수 있다. EAP 성공 프레임(217r)에 응답하여, STA(208) 및 AP1(209a)은 4-단계 핸드쉐이크(4-way handshake)(217s)를 수행할 수 있다.

[0047] IP 설정 단계(207)는 IP 주소 할당(IP address assignment)을 달성하기 위해 수행될 수 있다. 예를 들어, STA(208)는 DHCP(dynamic host configuration protocol, 동적 호스트 구성 프로토콜) 발견 프레임(218a)을, 예를 들어, AP1(209a)로 전송할 수 있다. AP1(209a)은 DHCP 발견 프레임(218b)을 네트워크 요소(209d)로 전송하고, 그에 응답하여, DHCP 제의(DHCP offer) 프레임(218c)을 수신할 수 있다. AP1(209a)은 DHCP 제의 프레임(218d)을 STA(208)로 전송할 수 있다. STA(208)는 DHCP 요청 프레임(218e)을 AP1(209a)로 전송할 수 있다. AP1(209a)은 DHCP 요청 프레임(218f)을 네트워크 요소(209d)로 전송하고, 그에 응답하여, DHCP ACK(acknowledgement, 확인 응답)(218g)를 수신할 수 있다. AP1(209a)은 DHCP ACK(218h)을 STA(208)로 전송할 수 있다.

[0048] 상호 인증을 제공하는 다른 EAP 방법들 - 예를 들어, EAP-SIM(EAP-Subscriber Identity Module, EAP-가입자 식별 모듈), EAP-AKA(Authentication and Key Agreement, 인증 및 키 합의) 및 EAP-TTLS(EAP-Tunneled Transport Layer Security, 터널 전송 계층 보안) - 이 또한 사용될 수 있다.

[0049] 도 2에 예시되어 있는 예와 같은 802.11 초기 링크 설정 절차들에서 몇몇 문제점들에 봉착되었다. 하나의 문제점은, 예를 들어, 802.11 네트워크가 STA와 초기 연결을 설정하는 데 필요한 최대 몇 초 이상의 시간 길이를 포함할 수 있다. 다른 문제점은 STA의 사용자가 대화형 세션(예를 들어, Skype 비디오)에 참여할 때, STA가 다른 네트워크로부터 802.11 네트워크로[예를 들어, 3GPP(Third Generation Partnership Project) 네트워크로부터 WLAN(wireless local area network)으로] 스위칭하는 경우, 연결이 유지될 수 없을 것이라는 것이다. 다른 문제점은 IEEE 802.11 네트워크들이 많은 수의 사용자들이 동시에 ESS(extended service set, 확장 서비스 세트)에 들어가는 것을 지원하고 그들에게 안전하게 인증을 제공해야만 할지도 모른다는 것이다.

[0050] 802.11 네트워크들에 대한 몇가지 목표들이 초기 링크 설정 시간, 최소 사용자 부하, 및 높은 배경 부하(background load)의 존재 하에서의 강건성과 관련하여 설정될 수 있다. 초기 링크 설정 시간과 관련하여, 하나의 예시적인 목표는, RSNA(Robust Security Network Association, 강건한 보안 네트워크 접속) 보안 레벨을 유지하면서, IEEE 802.11 네트워크들에 대한 초기 링크 설정 시간이 100 ms 미만이라는 것일 수 있고, 여기서 초기 링크 설정 시간은 유효한 IP(internet protocol) 주소를 갖는 IP 트래픽을 AP를 통해 송신할 수 있기 위해 필요한 시간의 양일 수 있다. 최소 사용자 부하와 관련하여, 한 예시적인 목표는 IEEE 802.11 네트워크들이 적어도 100개의 비AP STA들이 1초 이내에 ESS에 들어가는 것을 지원하고 링크 설정을 성공적으로 수행하는 것일 수 있다. 높은 배경 부하의 존재 하에서의 강건성과 관련하여, 한 예시적인 목표는 적어도 50%의 미디어 부하들에 대한 링크 설정을 제공하는 것일 수 있다.

[0051] 802.11 네트워크들에 대한 초기 링크 설정 시간을 감소시키는 예시적인 방법들이 표 1에 요약되어 있다. 그렇지만, 100 ms 링크 설정 시간 목표를 충족시키기 위해서는 이 예들로 충분하지 않을 수 있는데, 그 이유는 공격적인 예측을 사용하여도, 수동 스캔을 사용하는 링크 설정에 대한 가능한 달성 시간이, 네트워크 발견 단계를

고려하지 않더라도, 90 ms이기 때문이다. 많은 수의 AP들이 존재할 수 있는 실제의 네트워크들에서 현실적인 시간 소비는 상당히 더 길 수 있다. 게다가, 도 2에 예시되어 있는 IEEE 802.11 링크 설정 프로토콜은 아주 길고, 초기 링크 설정 시간 요구사항들을 충족시키지 않을 것이다.

표 1

[0052]

| 단계 | AP 발견 | | 네트워크 발견 | 부가의 TSF | 인증 및 접속 | 상위 계층 (DHCP/IP) |
|---|---|---|---|---|---|---|
| | 능동 스캔 | 수동 스캔 | | | | |
| 메시지 라운드의 수 | 1+, STA-AP<br>AP당 채널당 | 1.5, STA-AP<br>AP당 채널당 | 2+, STA-AP<br>1, AP-AS<br>AP당 | 1, STA-AP | 7~13, STA-AP<br>4+, AP-RADIUS | 2, STA-AP<br>2, AP-DHCP 서버 |
| 시간(오늘) | 평균:<br>2.4 GHz에 대해 102 ms:<br>5.8에 대해 해당 없음<br>최악의 경우:<br>680 ms | 평균:<br>2.4 GHz에 대해 1100 ms:;<br>5.8 GHz에 대해 2300 ms;<br>최악의 경우:<br>3400 ms | 5 ms 내지 30 ms<br>AP당<br>다수의 AP:<br>해당 없음 | 2 ms 내지 5 ms | 15 ms 내지 2 초 | ~ 100 ms |
| | | | | OFDM6에서의 EAP-GPSK(Extensible Authentication Protocol Generalized Pre-Shared Key, 확장가능 인증 프로토콜 일반화된 사전 공유 키): 6 ms + 71 ms 처리 시간, 여기서 OFDM6은 6 Mbps의 최소 데이터 레이트를 갖는 802.11PHY에서의 모드일 수 있다 | | |
| 가능한 달성(지식이 있는 경우) | 2 ms(5 GHz에서 가능함) | 50 ms | 많은 수의 사용자들이 동시에 네트워크에 들어가는 것에 대한 최적화들 | OFDM6에서의 피기백을 갖는 EAP-GPSK:<br>5 ms + 35 ms 처리 시간(감소된 수의 메시지들은 더 적은 처리 시간을 필요로 하고, 추가적인 최적화가 가능할 수 있다) | | |

[0053] 표 1을 참조하면, "가능한 달성" 행에 나타낸 시간 값들은, 예를 들어, 802.11ai에 기초하고 있을 수 있다.

[0054] 비록 RSNA가 사용될 때, 802.11 인증 단계가 제거될 수 있지만, 인증 단계는 그럼에도 불구하고 역호환에 도움을 주기 위해 수행될 수 있다. IP 주소 할당이 802.11ai에서의 링크 설정 프로세스의 이전의 단계들에 결합될 수 있다.

[0055] 예시적인 IETF(Internet Engineering Task Force) 절차들은 고속 IP 할당 방식인, IP 할당 단계를 최적화하기 위해 빠른 커밋(rapid commit)을 갖는 DHCP를 포함할 수 있다. GAS 구성 및/또는 AP 구성이 STA와 AP/네트워크 사이의 시스템 정보 통신을 최적화하기 위해 CCC들(configuration change counts, 구성 변경 횟수들) 또는 구성 시퀀스 번호들(configuration sequence numbers)이 사용될 수 있다.

[0056] 100 ms 미만의 초기 링크 설정 시간의 요구사항들을 달성하기 위해 802.11ai 절차들로 충분하지 않을 수 있다. 이러한 이유는, 수동 스캔을 사용하는 링크 설정에 대해, 네트워크 발견 단계를 고려하지 않더라도, 현재의 "가능한" 달성 시간이 90 ms이기 때문이다. 그에 부가하여, "가능한 달성" 행에 주어진 숫자들은 아주 공격적(예를 들어, 능동 스캔에 대해 2 ms)이다. 많은 수의 AP들이 존재할 수 있는 실제의 네트워크들에서 현실적인 시간 소비는 상당히 더 길 수 있다. 링크 설정 프로세스에서의 단계들 중 일부 또는 전부는 STA에 의해 개시될 수 있다. AP는 STA 요청에 응답할 수 있고, AP가 링크 설정 프로세스에서 최적화를 개시할 수 있게 하는 메커니즘을 갖지 않을 수 있다. 현재의 802.11 링크 설정 프로세스에서의 단계들의 대부분은, RSNA 보안 레벨을 유지하면서, 더 빠른 링크 설정 시간을 위해 추가로 최적화될 수 있다.

[0057] 현재의 초기 링크 설정 프로세스는 아주 길고, 초기 링크 설정 시간 요구사항들을 충족시키지 않을 수 있다. 많은 수의 사용자들이 동시에 ESS에 들어가는 것을 수용하는 것이 식별된 링크 설정 시간 프레임들 내에서 가능하지 않을 수 있다. 동적이고 유연하며 연동가능한 절차를 사용하여 링크 설정 프로세스를 최적화하는 방법 및 장치가 필요하다.

[0058] 802.11에서의 링크 설정 프로세스는 AP에서의 어떤 스텝들(steps) 또는 단계들(phases)의 제거를 포함하는 프로세스의 최적화를 가능하게 하지 않을 수 있다. 예를 들어, 802.11에서, 링크 설정 프로세스에서의 모든 단계들이, 도 2a에 도시된 바와 같이, STA에 의해 개시될 수 있다.

[0059] 시스템 구성이 정의될 수 있다. 예를 들어, 구성 변경 횟수 또는 구성 시퀀스 번호가 정의될 수 있다. 게다가, 도 2a 및 도 2b에 예시되어 있는 프로토콜과 같은 IEEE 802.11의 한 예시적인 초기 설정 절차에서, 링크 설정 프로세스에서의 모든 단계들이 STA에 의해 개시될 수 있다. AP는 STA 요청에 대해서만 응답하고, 링크

설정 프로세스에서 최적화를 개시하는 메커니즘을 갖지 않을 수 있다. 또한, 많은 수의 사용자들이 동시에 ESS에 들어가는 것을 수용하는 것이 식별된 링크 설정 시간 프레임들(예를 들어, 100 ms) 내에서 가능하지 않을 수 있다.

[0060] 상기한 바에 부가하여, 이동성에 대한 요구가 증가하고 다수의 무선 인터페이스들(예를 들어, 3GPP 및 IEEE 802.11)을 갖는 다중 모드 디바이스들의 이용가능성이 증가함에 따라, 이 네트워크들을 통한 매끄러운 핸드오버 및 서비스 연속성이 통신 사업자가 그의 사용자들에게 제공하는 차별화하는 서비스로 될 수 있다. 802.1x/EAP WLAN 네트워크들에의 보안 액세스 절차들은 자동화의 결여, 상당한 부가 대기시간, 매끄럽지 않은 핸드오프, 그리고 사용자 상호작용, 디바이스들을 사전 프로비저닝하는 것, 및 자격 증명들을 갖는 WLAN 네트워크들을 종종 필요로 하는 핸드오프의 결과로서 셀룰러 네트워크들을 통해 이전에 설정된 서비스들(예를 들어, VoIP(voice over internet protocol) 세션들)의 중단을 겪을 수 있다.

[0061] 본 명세서에 개시되어 있는 하나 이상의 실시예들은 AP 및/또는 STA가 사전 획득하는 정보를 사용함으로써 802.11 디바이스들에 대한 초기 링크 설정을 가속화시킬 수 있다. AP들 및/또는 STA들은 서로에 관한 특정의 정보를 사전 획득할 수 있다. 예를 들어, STA는 3G 네트워크와 같은 그의 이전의 연결로부터 WLAN 네트워크로, 또는 하나의 AP로부터 ESS 내의 다른 AP로 스위칭할 수 있다. 이 예에서, 적당한 또는 선호된 WLAN AP가 후보 STA에 관한 특정의 정보를 사전 획득하는 것이 가능할 수 있다. 또한, STA가, 예를 들어, 지리적 위치들 및 네트워크 액세스 이력(빈번히 방문한 곳, 일상 업무, 기타를 포함하지만 이들로 제한되지 않음)에 기초하여, 선호된 AP에 관한 지식을 사전 획득하는 것이 가능할 수 있다.

[0062] AP 및/또는 STA가 이러한 정보를 사전 획득하는 것에 의해, 링크 설정 절차에서의 특정의 단계들을 생략하고 그리고/또는 결합시키는 것이 가능할 수 있다. 그에 부가하여, AP 및/또는 STA가 어떤 정보를 얼마나 사전 획득했는지에 따라, 링크 설정 시간을 감소시키기 위해, 다양한 최적화들이 링크 설정 절차에 적용될 수 있다. 이러한 단축된 또는 최적화된 절차가 또한 AP에 의해 개시될 수 있다.

[0063] 도 3은 사전 획득된 정보를 사용하는 가속화된 링크 설정을 위한 기준 절차의 플로우차트이다. 무선 통신 시스템은 하나 이상의 스테이션들(STA들)(301), 하나 이상의 AP들(302a, 302b, 302c), 및 하나 이상의 네트워크 요소들(302d)을 포함할 수 있다. STA(301)는 WTRU(wireless transmit/receive unit)를 포함할 수 있고, 네트워크 요소(302d)는, 예를 들어, 라우터, HA(home agent), AAA 서버, AS, 또는 RADIUS를 포함할 수 있다.

[0064] 도 3에 도시되어 있는 예시적인 절차(300)에서, APn(302c)은 STA(301)에 관한 사전 획득된 정보를 사용함으로써 링크 설정 최적화들을 개시할 수 있다. 게다가, 도 3에 도시되어 있는 예시적인 절차는, 역호환을 유지하면서, 동적이고 유연하며 연동가능한 방식으로 가속화된 링크 설정 절차들의 다수의 변형례들에 대처할 수 있다.

[0065] 도 2에 예시되어 있는 링크 설정 절차와 관련하여, 도 3에 예시되어 있는 사전 획득된 정보를 사용하는 ALS(accelerated link setup)에 대한 기준 절차는 STA(301) 이외의 엔터티들에 의해 주도될 수 있다. STA 또는 AP에 관한 어떤 정보도 사전 획득되지 않은 경우, ALS는 AP 발견 단계(303), 네트워크 발견 단계(304), 부가의 TSF 단계(305), 인증 단계(306), 접속 단계(307), 보안 설정 단계(308), 및 IP 설정 단계(309)를 포함하는 802.11 링크 설정 절차로서 기능할 수 있다. 그렇지만, AP가 STA(301)에 관한 정보를 획득하기 위해 사전 획득된 정보 단계(310)를 수행하거나 그 반대인 경우, STA(301) 및 AP는 사전 획득된 정보를 사용하여 AP 발견 단계(303)를 최적화할 수 있다. 그에 부가하여, AP와 STA는, STA 및 AP가 서로에 대해 획득한 정보의 양에 따라, 사후 AP 발견(post-AP-discovery) 단계들, 예를 들어, 네트워크 발견 단계(304), 부가의 TSF 단계(305), 인증 단계(306), 접속 단계(307), 보안 설정 단계(308), 및 IP 설정 단계(309)를 생략하거나 단축시키기 위해 협상할 수 있다.

[0066] 예를 들어, STA가 3G 셀룰러 네트워크를 통해 대화형 Skype 통화를 수행하고 있는 경우, STA가 선호된 AP로부터의 강한 신호들이 있는 장소에 도착하면, STA는 WLAN 네트워크로 스위칭할 수 있다. STA 및 선호된 AP는, 3G 네트워크를 통한 링크 설정 이전에, 서로에 관한 정보(보안 관련 파라미터들, 이용가능한 네트워크 서비스들, 기타 등등)를 사전 획득할 수 있다. 사전 획득된 정보가 주어지면, STA는, 지역 내의 모든 이용가능한 AP들에 대해 스캔하는 것 대신에, 선호된 AP에 대해서만 능동적으로 스캔할 수 있고, 이는 AP 발견 프로세스를 상당히 단축시킬 수 있다. 게다가, STA 및 AP가 이미 사전 획득된 보안 관련 파라미터들 및 이용가능한 네트워크 서비스 정보를 가지고 있을 수 있기 때문에, 그들은, 요구된 RSNA 보안 레벨을 유지하면서, 네트워크 발견 단계(304), 부가의 TSF 단계(305)(TSF가 초기 프로브 요청/프로브 응답 교환 동안 수행될 수 있기 때문임) 및 보안 설정 단계(308)를 생략할 수 있어, 훨씬 더 빠른 링크 설정을 달성할 수 있다.

[0067] 도 3에 도시되어 있는 예시적인 기준 절차는 정보 사전 획득 단계(310), AP 발견 단계(303), 및 사후 AP 발견 단계(311)를 포함할 수 있다. 정보 사전 획득 단계(310)에서, AP들 및/또는 STA들은 바로 그들 사이에 있는 IEEE 802.11 공중 링크 이외의 인터페이스들을 통해 서로에 관한 지식을 획득할 수 있다. 정보 사전 획득 단계(310)는 링크 설정 시간의 일부로서 카운팅되지 않을 수 있고, AP와 STA 사이의 링크 설정 이전에 언제라도 수행될 수 있다. 정보 사전 획득 단계(310)가 꼭 링크 설정 이전에만 행해져야 하는 것은 아닐 수 있다. AP 발견 단계(303)에서, STA(301)는, 사전 획득된 정보를 사용하여 또는 사용하지 않으면서, 적당한 AP를 찾아낼 수 있다. 사전 획득된 정보가 이용가능한 경우, AP 발견이 그에 따라 최적화될 수 있고, 나머지 링크 설정 프로세스에 대한 특정의 절차가 AP와 STA 사이에서 전달되고 협상될 수 있다. 그렇지 않은 경우, AP 발견 절차(303) 및 나머지 링크 설정 단계들이 역호환을 유지하기 위해 사용될 수 있다. 사후 AP 발견 단계(311)는 STA와 AP 사이의 IP 연결의 설정을 위한 모든 남아 있는 단계들[네트워크 발견(304), 부가의 TSF(305), 인증(306), 접속(307), 보안 설정(308), 및 IP 설정(309) 등]을 포함할 수 있다. 사후 AP 발견 단계(311)는, 그의 단계들 중 어느 것도 필수적이지 않도록, 유연한 구조로 되어 있을 수 있다. 링크 설정 프로세스를 가속화시키기 위해, STA 및 AP에 관한 사전 획득된 정보의 이용가능성 및 양에 따라, 단계들 각각이 생략되거나 최적화될 수 있다. 그에 부가하여, 도 3에 예시되어 있는 ALS 절차는 결합된 단계들 또는 새로 정의된 절차에 대한 프레임워크를 제공한다. 링크 설정 경우에 대한 특정의 절차의 선택이, AP 발견 단계의 완료 시에, 제안된 시그널링 메커니즘들을 통해 AP와 STA 사이에서 전달될 수 있다.

[0068] 도 3을 참조하면, 정보 사전 획득 단계(310)에서, STA(301) 및 AP1(302a)은 정보를 사전 획득할 수 있다. 예를 들어, STA(301)가 WLAN에 연결되어 있는 경우, AP1은 APn(302c)으로부터 후보 STA 정보(312a)를 수신할 수 있고, STA(301)는 APn(302c)으로부터 후보 AP 정보(313a)를 수신할 수 있다. 다른 예에서, STA가 셀룰러 네트워크[예를 들어, 네트워크 요소(302d)]에 연결되어 있는 경우, AP1(302a)은 네트워크 요소(302d)로부터 후보 STA 정보(312b)를 수신할 수 있고, STA(301)는 네트워크 요소(302d)로부터 후보 AP 정보(313b)를 수신할 수 있다.

[0069] 후보 STA 정보(312a, 312b)는, 예를 들어, 장래의 어떤 시점에서 AP1(302a)과 통신할 수 있는 후보 STA에 관한 사전 획득된 지식일 수 있다. 후보 STA 정보(312a, 312b)는, 예를 들어, 후보 STA의 MAC(medium access control, 매체 접근 제어) 주소, 후보 STA의 능력, 보안 정보, 및/또는 서비스 패키지를 포함할 수 있다. 후보 AP 정보(313a, 313b)는 장래의 어떤 시점에서 STA(301)와 통신할 수 있는 후보 AP에 관한 사전 획득된 지식일 수 있다. 후보 AP 정보(313a, 313b)는, 예를 들어, SSID(service set identification, 서비스 세트 ID), BSSID(basic service set identifier, 기본 서비스 세트 식별자), AP 능력, 물리(PHY) 모드, 하나 이상의 레이트들, 보안 정보, 액세스 네트워크 서비스 정보, 및 비콘 또는 프로브 응답 프레임에 포함될 수 있는 임의의 다른 정보를 포함할 수 있다. 후보 STA 정보(312a, 312b) 및 후보 AP 정보(313a, 313b)는 또한 이하의 표 2에 나타낸 정보도 포함할 수 있다.

[0070] ALS(accelerated link setup) 능력 표시자는 ALS가 AP 및 비AP STA들을 비롯한 STA들에 의해 지원되는지 여부를 나타내는 데 사용될 수 있다. ALS 표시자는, 예를 들어, 예비 비트(reserved bit)를 사용함으로써 기존의 정보 필드에 인코딩될 수 있는 비트 플래그 정보를 포함할 수 있다. 예를 들어, 예비 비트는 비콘 프레임의 능력 정보(capability information) 필드일 수 있다. 예비 비트는 또한 하나 이상의 정보 필드들 또는 정보 요소들(IE들)에 인코딩될 수 있다.

[0071] AP 및 STA는, ALS 절차가 효과적으로 트리거될 수 있도록, 그들의 ALS 능력에 관해 서로에게 알려주기 위해 ALS 능력 표시자를 사용할 수 있다. 초기 링크 설정에서, AP 및 STA 둘 다는, 가능한 가장 빠른 기회에서, ALS 능력 표시자 정보를 송신할 수 있다. 예를 들어, AP는 ALS 능력 표시자를 비콘 프레임들 및/또는 프로브 응답 프레임들에서 송신할 수 있는 반면, STA는 ALS 능력 표시자를 프로브 요청 프레임들 및/또는 다른 관리/제어 프레임들에서 초기 프레임으로서 AP로 송신할 수 있다.

[0072] IE들은 ALS 절차들을 돕기 위해 사용될 수 있고, 예를 들어, I-know-you IE, I-know-you-response IE, Need-more-info IE, 및 Need-more-info-response IE를 포함할 수 있다. 이 IE들은 관리 프레임들에 포함될 수 있고, AP 및 비AP STA들을 비롯한 2개의 STA들 사이의 WLAN 공중 링크를 거쳐 전송될 수 있다.

[0073] I-know-you IE는 AP 및/또는 STA가 상대방에 관한 정보를 사전 획득했다는 것을 초기 링크 설정의 초반에 상대방에게 통지할 수 있게 할 것이다. I-know-you IE가 AP에 의해 사용될 때, 그 IE는, AP가 이미 어떤 정보를 사전 획득했는지를 STA에 통지하기 위해, AP로부터 STA로의 첫번째 유니캐스트 프레임(예를 들어, 프로브 응답 또는 인증 응답)에서 송신될 수 있다. 이 정보는, 예를 들어, AP가 48-비트 MAC 주소와 같은 STA ID(identity)를 알고 있을 수 있다는 것; AP가 STA의 서비스 요구 및 AP가 그 서비스들을 제공할 수 있다는 것을 알고 있을 수

있다는 것; AP 및 STA가 자격 증명/키 등을 공유한다는 것, 및/또는 어떤 정보가 필요한지(예를 들어, AP가 STA로부터의 확인 및/또는 공유 키 등에 관한 STA의 지식과 같은 STA에 관한 추가 정보를 필요로 할 수 있음)를 포함할 수 있다. I-know-you IE가 STA에 의해 사용될 때, 그 IE는 STA로부터 AP로의 첫번째 메시지에서 전송될 수 있고, STA가 AP에 관해 어떤 정보를 사전 획득했는지(예를 들어, AP가 STA의 선호된 AP라는 것); STA가 AP의 MAC/PHY 파라미터들을 사전 획득했다는 것; STA가 AP와 공유되는 자격 증명/키를 가진다는 것; STA가 STA에 관한 정보를 AP에 제공하고 있다는 것; 및/또는 STA가 AP로부터 어떤 정보를 여전히 필요로 하는지를 AP에 통지할 수 있다.

[0074] 그에 부가하여, I-know-you IE는 또한 나머지 링크 설정 프로세스를 어떻게 추적할지에 관한 그의 송신기로부터의 제안을 포함할 수 있다. 예를 들어, 제안은 링크 설정 프로세스를 완료하기 위한 특정의 절차를 포함할 수 있고, 사전 획득된 정보에 기초할 수 있다.

[0075] I-know-you-response IE는 추가의 정보를 필요로 할 수 있는 I-know-you IE에 대한 응답일 수 있다. 이러한 응답은 수신된 I-know-you IE에 열거되어 있는 정보 항목들에 대한 하나 이상의 확인들, 부가들, 및/또는 정정들을 포함할 수 있다.

[0076] Need-more-info IE는, I-Know-You IE 및 I-Know-You-Response IE를 갖는 메시지들이 필요한 정보 전달을 완료하지 않은 경우, AP 및 STA가 ALS를 돕기 위해 정보를 추가로 교환할 수 있게 할 것이다. 예를 들어, 링크 설정 프로세스를 어떻게 완료할지를 협상하기 위해, AP 및/또는 STA는 합의에 도달하기 위해 다른 메시지 교환 라운드를 필요로 할 수 있다. Need-more-info-response IE는 Need-more-info IE 또는 추가의 정보를 요청할 수 있는 I-know-you-response IE에 대한 응답일 수 있다.

[0077] 시스템 오버헤드를 감소시키고 고속 초기 링크 설정를 돕기 위해, 비콘 전송 프로토콜이 수행될 수 있다. 예를 들어, 정규의 비콘(regular beacon)에 부가하여, 짧은 비콘이 전송될 수 있다. 시스템 오버헤드를 감소시키고 고속 초기 링크 설정을 위한 필수 정보를 전달하기 위해, 짧은 비콘의 내용이 최소화될 수 있다. 이 예에서, 짧은 비콘은 링크 설정 지연 요구사항에 의해 요구되는 만큼 빈번히 전송될 수 있고, 그에 따라, 하나 이상의 연속적인 비콘 사이클들에서 정규의 주 비콘(regular primary beacon)을 대체할 수 있거나, 정규의 주 비콘을 주기적으로 대체할 수 있거나, 정규의 주 비콘보다 더 빈번히 전송될 수 있다. 그에 부가하여, 짧은 비콘 내용은 AP가 하나 이상의 STA들에 관한 사전 정보를 가질 수 있는 AP 인지 모드(AP aware mode)에 의해 영향을 받을 수 있다. 짧은 비콘은 다음과 같은 것들 중 하나 이상에 관련된 정보를 포함할 수 있다: AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE.

[0078] ALS를 지원하는 한 예시적인 짧은 비콘 프레임(400)이 도 4에 예시되어 있다. 예를 들어, 짧은 비콘 프레임(400)은 최적화된/최소화된 헤더(410), 주 비콘 관련 정보 필드(420), 주 비콘 내용 필드의 최적화된/최소화된 서브셋(430), AP 발견 정보 필드(440), 네트워크 발견 정보 필드(450), 보안 관련 정보 필드(460), 상위 계층 프로토콜 정보 필드(470), 및 하나 이상의 선택적인 요소들 필드(480)를 포함할 수 있다. AP 발견 정보 필드(440), 네트워크 발견 정보 필드(450), 보안 관련 정보 필드(460), 및/또는 상위 계층 프로토콜 정보 필드(470)는, 필요에 따라, 짧은 비콘 프레임(400)에 포함될 수 있다.

[0079] 다른 예에서, 비콘 프레임이 고속 초기 링크 설정을 돕도록 수정될 수 있다. 예를 들어, 주 비콘이 고속 초기 링크 설정을 위한 필수 정보를 포함할 수 있도록 수정될 수 있다. 이 예에서, 비콘 내용은 AP가 하나 이상의 STA들에 관한 사전 정보를 가질 수 있는 AP 인지 모드에 의해 영향을 받을 수 있다. 비콘은 다음과 같은 것들 중 하나 이상에 관련된 정보를 포함할 수 있다: AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE.

[0080] ALS를 지원하는 주 비콘 프레임(500)에 대한 예시적인 수정이 도 5에 예시되어 있다. 예를 들어, 주 비콘 프레임(500)은 헤더(510), 주 비콘 내용 필드(520), 짧은 비콘 관련 정보 필드(530), AP 발견 정보 필드(540), 네트워크 발견 정보 필드(550), 보안 관련 정보 필드(560), 상위 계층 프로토콜 정보 필드(570), 및 하나 이상의 선택적인 요소들 필드(580)를 포함할 수 있다. 짧은 비콘 관련 정보 필드(530), AP 발견 정보 필드(540), 네트워크 발견 정보 필드(550), 보안 관련 정보 필드(560), 및/또는 상위 계층 프로토콜 정보 필드(570)는, 필요에 따라, 주 비콘 프레임(500)에 포함될 수 있다.

[0081] 그에 부가하여, ALS 능력 표시자가 비콘 프레임들에, 짧은 비콘 및 수정된 주 비콘 둘 다에 포함될 수 있다.

ALS 능력 표시자가 예비 비트를 사용함으로써 비콘 프레임의 능력 정보 필드에 인코딩될 수 있거나, 비콘 프레임들에서의 다른 정보 필드들 또는 정보 요소들에 인코딩될 수 있다.

[0082] 링크 설정에서 전형적으로 사용되는 IEEE 802.11 관리 프레임들은 FILS(fast initial link setup)를 돕도록 수정될 수 있다. 예를 들어, AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE 중 하나 이상에 관련된 정보를 포함시킴으로써, 접속/재접속(association/re-association) 그리고 프로브 요청 및 응답 메시지들이 FILS를 돕도록 수정될 수 있다.

[0083] 스캔을 갖는 STA들을 지원하는 IEEE 802.11 측정 파일럿 프레임(measurement pilot frame)이 FILS를 돕도록 수정될 수 있다. 측정 파일럿 프레임은 주 비콘에 포함되어 있는 정보의 서브셋을 포함할 수 있고 주 비콘보다 더 자주 전송될 수 있는 공개 동작 프레임(public action frame)일 수 있다. 예를 들어, AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE 중 하나 이상에 관련된 정보를 포함시킴으로써, 측정 파일럿이 FILS를 돕도록 수정될 수 있다.

[0084] 그에 부가하여, AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE 중 하나 이상에 관련된 정보를 포함시킴으로써, GAS(generic advertisement service, 일반 광고 서비스) 초기 요청/응답 및 GAS 컴백 요청/응답 프레임들과 같은 다른 IEEE 802.11u 프레임들이 FILS를 돕도록 수정될 수 있다.

[0085] 다른 예에서, FILS를 돕는 관리 프레임(FILS 관리 프레임이라고 함)은 AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; 및/또는 Need-more-info IE 중 하나 이상에 관련된 정보를 포함할 수 있다. FILS 관리 프레임은 FILS 기능을 지원하는 것으로 정의된 동작을 갖는 FILS 관리 동작 프레임으로서 정의되고 구현될 수 있다. FILS 관리 동작 프레임은 다음과 같은 모드들 중 하나 이상을 포함할 수 있다: ACK(acknowledgement) 응답을 필요로 하는 정규 모드(regular mode) 및 수신기로부터의 ACK 응답을 필요로 하지 않을 비ACK 모드(No ACK mode).

[0086] FILS 관리 동작 프레임은 공개 동작 프레임일 수 있다. FILS 관리 동작 프레임은 인터-BSS(inter-Basic Service Set, 인터-기본 서비스 세트) 및 비접속 STA(unassociated-STA)와의 AP 정보 교환을 위해 사용될 수 있다. 이러한 정보 교환 시나리오들의 예들은 전송측 STA 또는 AP 및 수신측 STA 또는 AP가 상이한 BSS들과 접속되어 있고 전송측 및 수신측 STA들 중 하나 또는 둘 다가 BSS와 접속되어 있지 않은 것을 포함할 수 있다. FILS 관리 동작 프레임은 또한 STA-STA 통신(STA to STA communication)을 위해 사용될 수 있는 이중 보호 모드(dual protected mode)를 가질 수 있다.

[0087] 한 예시적인 FILS 관리 동작 프레임(600)이 도 6에 예시되어 있다. 예를 들어, FILS 관리 동작 프레임(600)은 카테고리 필드(610), 동작 필드(620), AP 발견 정보 필드(630), 네트워크 발견 정보 필드(640), 보안 관련 정보 필드(650), 상위 계층 프로토콜 정보 필드(660), 및 하나 이상의 선택적인 요소들 필드(670)를 포함할 수 있다. 카테고리 필드(610)는, 예를 들어, FILS 관리 동작 프레임이 공개 동작 프레임이라는 것을 나타낼 수 있다. 동작 필드(620)는 FILS 동작을 나타낼 수 있다. AP 발견 정보 필드(630), 네트워크 발견 정보 필드(640), 보안 관련 정보 필드(650), 및/또는 상위 계층 프로토콜 정보 필드(660)는, 필요에 따라, FILS 관리 동작 프레임에 포함될 수 있다.

[0088] FILS 관리 동작 프레임은 AP에 의해 전송될 수 있고, 유니캐스트 또는 브로드캐스트 모드로 전송될 수 있다. AP는, BSS/시스템에서의 FILS의 효율적인 동작을 지원하기 위해, FILS 관리 동작 프레임을 필요에 따라 빈번히 전송할 수 있다.

[0089] 다른 예에서, FILS 관리 동작 기능이 FILS 요청 프레임 및 FILS 응답/보고 프레임에 의해 지원될 수 있다. FILS 요청 프레임을 전송하는 디바이스는 다음과 같은 것들 중 하나 이상에 관련된 정보를 요청할 수 있다: AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로토콜; I-know-you IE; I-know-you-response IE; 및/또는 Need-more-info IE. FILS 응답/보고 프레임을 전송하는 디바이스는 다음과 같은 것들 중 하나 이상에 관련된 정보로 응답하거나 그 정보를 보고할 수 있다: AP 발견; 네트워크 발견; 보안, 예를 들어, 인증 및 접속; 링크 설정 프로세스를 가속시키기 위한 상위 계층 프로

토콜; I-know-you IE; I-know-you-response IE; Need-more-info IE; 및/또는 Need-more-info-response IE.

[0090] AP 및/또는 STA에 의해 사전 획득된 정보는 AP 발견을 효과적으로 최적화하기 위해 사용될 수 있다. 예를 들어, STA는 WLAN 네트워크로의 스위칭 이전의 네트워크에의 연결, 그리고 AP들 및 위치들과의 기억된 이력 데이터 등과 같은 다수의 메커니즘들을 통해 선호된 AP 정보를 획득할 수 있다. STA에서, 사전 획득된 정보는 다음과 같은 2가지 주된 유형들로 분류될 수 있다: 공중 인터페이스 MAC/PHY 파라미터들, 예를 들어, SSID(service set identification), BSSID(basic service set identification, 기본 서비스 세트 ID), 서비스 제의들, 능력, PHY 파라미터들, 지원되는 레이트들, QoS(quality of service, 서비스 품질) 능력 등과 같은 비콘 및/또는 프로브 응답 프레임들에서의 파라미터들, 그리고 보안 관련 정보, 예를 들어, RSN(robust security network, 강건한 보안 네트워크) 정보, 만료 시간을 갖는 공유 키/자격 증명 및/또는 만료 시간을 갖는 유효 인증 컨텍스트. STA에서의 최소의 사전 획득된 정보는 선호된 AP의 MAC 주소(예를 들어, BSSID)를 포함할 수 있다. 다른 정보 항목들이 이용가능하고 증분적 방식으로 사용될 수 있다.

[0091] AP의 BSSID가 STA가 AP의 커버리지 영역과 관련하여 사전 획득한 유일한 정보인 경우, AP 발견 프로세스는 적어도 2개의 측면들로부터 최적화될 수 있다. 첫째, STA는 유니캐스트 프로브 요청 프레임(와일드카드가 아님)을 전송할 수 있다. 둘째, 그 영역에 있는 모든 이용가능한 AP들을 스캔할 필요 없이, 그의 선호된 AP 선택을 확인해주는 프로브 응답 프레임이 수신되면, AP 발견 프로세스가 복귀될 수 있다. AP의 BSSID 및 임의의 다른 정보 항목들이 STA에 의해 사전 획득된 경우, 추가적인 최적화들이 AP 발견에 적용될 수 있다.

[0092] 도 7은 AP의 사전 획득된 지식을 사용하는 한 예시적인 AP 발견 방법(700)을 나타낸 도면이다. 이 예에서, AP(710) 및/또는 STA(720)는 네트워크(예를 들어, 3G, 다른 WLAN AP 등)에의 이전의 연결로부터 사전 획득된 정보를 가질 수 있다. 사전 획득된 정보는 또한 STA(720)의 메모리 및 그의 현재 위치로부터 온 것일 수 있다. 사전 획득된 정보는 각종의 방식들로 획득될 수 있다. 하나의 예에서, AP(710)는 네트워크 요소(725)로부터 후보 STA 정보(722)를 포함하는 메시지를 수신할 수 있다. 다른 예에서, STA(720)는 네트워크 요소(725)로부터 후보 AP 정보(726)를 포함하는 메시지를 수신할 수 있다.

[0093] 도 7을 참조하면, STA(720)는 AP(710)로부터 비콘(730)을 수신할 수 있다. 비콘(730)은 ALS 능력 표시자를 포함할 수 있다. STA는 유니캐스트 요청 프레임(740)을 AP(710)로 전송할 수 있다. 유니캐스트 요청 프레임(740)은 프로브 요청 프레임일 수 있고, I-Know-You IE를 포함할 수 있다. 유니캐스트 요청 프레임(740)은 새로운 MAC 관리 프레임 또는 수정된 802.11 MAC 관리 프레임일 수 있다. I-Know-You IE는 AP로부터 확인들 및/또는 정정들을 탐색하기 위해 AP에 관련된 STA의 지식에 관한 정보 항목들을 포함할 수 있고, 또한 AP에 추가 정보를 요구하기 위한 요청 표시자들을 포함할 수 있다.

[0094] AP(710)가 STA(720)로부터 I-Know-You IE를 갖는 이러한 요청 프레임을 수신할 때, AP(710)는 응답 프레임(750)을 다시 STA(720)로 전송할 수 있다. 응답 프레임(750)은 링크 설정 프로세스를 어떻게 완료할지에 관한 추가적인 상세를 포함하는 I-Know-You-Response IE를 포함할 수 있다. AP(710) 및 STA(720)가 서로에 관한 추가 정보를 획득하고 링크 설정 절차을 어떻게 완료할지에 관한 합의에 도달하기 위해, 다른 메시지 교환 라운드가 사용될 수 있다. 예를 들어, STA(720)는 추가 정보 필요(need-more information) 요청 프레임(760)을 전송하고, 그에 응답하여, AP(710)로부터 추가 정보 필요(need-more information) 응답 프레임(770)을 수신할 수 있다. AP 발견 단계(775)가 완료될 때, 나머지 링크 설정(780)이 수행될 수 있다.

[0095] 이 예에서, AP 발견 단계(775)는 STA와 AP 사이에서 1번 또는 2번의 메시지 라운드로 완료될 수 있고, 완료하는 데 약 4 ms 내지 10 ms 걸릴 수 있다. 그에 부가하여, 이러한 AP 발견 단계(775)에서, AP(710) 및 STA(720)에 의한 나머지 링크 설정 기능들을 완료하는 최적화된 방식을 도출하기 위해, 사전 획득된 지식이 적용될 수 있다.

[0096] AP는 네트워크에의 그의 연결들을 통해 후보 STA의 지식을 사전 획득할 수 있다. STA에 관한 사전 획득된 정보는 STA의 MAC 주소; 서비스 요구사항들; 보안 관련 정보, 예를 들어, 만료 시간을 갖는 공유 키/자격 증명; 및/또는 만료 시간을 갖는 유효 인증 컨텍스트 등을 포함할 수 있다. 이와 유사하게, AP가 STA에 관해 가질 수 있는 최소의 사전 획득된 지식은 STA의 MAC 주소를 포함할 수 있다. 다른 정보 항목들, 예를 들어, STA 능력, 하나 이상의 서비스 요구사항들, 보안 정보 등이 이용가능하고 증분적 방식으로 사용될 수 있다.

[0097] AP가 STA에 관한 사전 획득된 지식, 예를 들어, STA의 MAC 주소만 또는 부가의 정보 항목들과 함께 그의 MAC 주소를 가지는 경우, AP는 STA로부터 STA의 MAC 주소를 포함하는 첫번째 프레임을 수신한 후에 ALS 절차를 개시할 수 있다.

[0098] 도 8은 사전 획득된 정보에 기초하여 AP(810)에 의해 개시되는 최적화된 AP 발견 방법(800)의 한 예를 나타낸 도면이다. 사전 획득된 정보는 각종의 방식들로 획득될 수 있다. 예를 들어, 네트워크 요소(815)는 후보 STA 정보(817)를 포함하는 메시지를 AP(810)로 전송할 수 있다. 다른 예에서, 네트워크 요소(815)는 후보 STA 정보(819)를 포함하는 메시지를 STA(820)로 전송할 수 있다.

[0099] 도 8에 예시된 예에서, AP(810)가 STA(820)의 MAC 주소를 포함하는 첫번째 프레임(830), 예를 들어, 프로브 요청 프레임을 STA(820)로부터 수신할 때, AP(810)가 STA(820)에 관한 사전 획득된 정보를 가지고 있는 경우, AP(810)는 응답 프레임(840), 예를 들어, 프로브 응답 프레임을 전송할 수 있다. 응답 프레임(840)은 그가 STA(820)에 대한 올바른 AP일 수 있다는 것을 나타내는 I-Know-You IE를 포함할 수 있다. I-Know-You IE는 STA(820)에 추가 정보를 요청하기 위해 사용될 수 있다. 첫번째 프레임(830) 및 응답 프레임(840) 각각은 ALS 능력 표시자를 포함할 수 있다. 이러한 응답을 AP(810)로부터 수신할 때, STA(820)는, 스캔을 위해 사용되는 시간이 상당히 감소될 수 있도록, 스캔 프로세스를 종료할 수 있다. AP(810) 및 STA(820)는 추가 정보 교환들을 수행할 수 있다. 예를 들어, STA(820)는 STA에 관한 부가 정보를 포함하는 프레임(850)을 전송할 수 있다. 프레임(850)은 링크 설정 절차에 대한 제안을 포함할 수 있다. 그에 응답하여, AP(810)는 프레임(860)을 전송할 수 있다. 프레임(860)은 제안된 링크 설정 절차의 확인을 포함할 수 있다.

[0100] 그에 부가하여, AP(810)의 I-Know-You IE에 대한 STA(820)의 응답, 및 필요한 경우, AP(810)와 STA(820) 사이의 추가 정보 교환들을 통해, AP(810) 및 STA(820)는 링크 설정 프로세스를 어떻게 시간 효율적인 방식으로 완료할지에 관한 합의에 도달할 수 있다. 예를 들어, AP(810) 및 STA(820)는 특정의 링크 설정 단계들을 생략하거나, 최적화하거나 결합시키기로 합의할 수 있다. 이러한 방식으로, AP(810)는, 링크 설정 프로세스를 어떻게 최적화할지를 결정하는 데 능동적으로 참여하기 위해, 그의 사전 획득된 정보를 성공적으로 적용할 수 있다.

[0101] 사후 AP 발견 링크 설정 최적화들이 AP 및 STA가 AP 발견 이전에 그리고 AP 발견 단계 동안에 사전 획득했을 수 있는 이용가능한 정보에 따라 달라질 수 있다. 표 2는 사전 획득된 지식의 상이한 가정들에 기초한 예시적인 사후 AP 발견 링크 설정 최적화들을 제공한다.

*표 2*

[0102]

| 단계 | 기능 | 최적화 고려사항들 |
|---|---|---|
| 네트워크 발견 | 올바른 서비스 제공자 네트워크를 찾아냄 | • AP가 STA의 서비스 요구를 알고 있고 또한 연결된 네트워크가 서비스들을 제공할 수 있다는 것을 알고 있는 경우 생략될 수 있음 |
| 부가의 TSF | 선택된 AP와의 추가적인 시간 동기화 | • 공중 링크 상태에 따라 생략될 수 있음; AP는 또한 생략될 수 있는 경우 STA에 알려줄 수 있음 |
| 802.11 인증 | STA를 검증하지만, RSNA를 위해 유용하지 않음 | • RSNA가 사용되는 경우 생략될 수 있음 |
| 802.11 접속 | STA에 의해 제공되는 RSN 정보를 검사하고, 또한 AID(association identifier, 접속 식별자)를 할당함 | • AP 발견 단계에서의 마지막 메시지 라운드에 결합될 수 있음;<br>• 또한 다른 독립형 메시지 라운드일 수 있지만, 그 다음 링크 설정 단계들에 대한 어떤 정보 항목들(예컨대, EAP/802.1x 인증, 및/또는 IP 주소 할당)을 전달하는 데 사용될 수 있음 |

| | | |
|---|---|---|
| EAP/802.1x 인증 및 보안 | EAP 인증, 및 키들/파라미터들 설정 | 가능한 최적화들의 다수의 변형들, 예컨대:<br>• 상위 계층 세션 키들이 제공되는 경우, 생략되거나 단축됨<br>• 네트워크와의 STA 사전 설정된 보안 접속을 사용한 고속 EAP<br>• 네트워크와의 STA 사전 설정된 보안 접속을 사용한 고속 EAP 인증 및 고속 키 프로비저닝<br>• 네트워크와의 STA 사전 설정된 보안 접속을 사용한 고속 네트워크 발견 및 고속 EAP 인증<br>• 네트워크와의 STA 사전 설정된 보안 접속을 사용한 고속 네트워크 발견, 고속 EAP 인증 및 고속 키 프로비저닝<br>• AP와 STA 사이에서 교환되는 EAPOL-Key 프레임 메시지들의 수를 4개로부터 2개로 감소시키는 것에 의한 4-단계 핸드쉐이크 프로토콜에 대한 최적화. 이것은 PMK(pairwise master key, 짝 마스터 키) 키 및 GMK 키를 도출하기 위해 네트워크와 STA 사이에서 공유되는 사전 설정된 마스터 키를 이용함으로써 달성될 수 있다. |
| IP 주소 할당 | IP 주소를 STA에 할당함 | • IP 주소가 셀룰러 네트워크를 거쳐 eANDSF를 통해 할당될 수 있다<br>• AAA 서버가 EAP 메시지에서 IP 주소를 STA로 송신할 수 있다.<br>• 예컨대, 계층-2 정보 요소를 피기백하는 것을 통해, 이전의 단계들에 결합됨<br>• 어떤 고속 IP 주소 할당 방식들을 통해 최적화됨 |

[0103] 요구시에 매끄러운 방식으로 다른 네트워크(예를 들어, WLAN 네트워크) 상에서의 인증 및 보안 링크 설정을 가능하게 하기 위해 STA와 네트워크(예를 들어, 셀룰러 네트워크) 간의 설정된 보안 접속이 이용될 수 있다. 하나의 예에서, 네트워크 상에서의 응용 프로그램-계층 자격 증명들의 역 부트스트랩(reverse bootstrap)이 다른 네트워크에서의 후속하는 새로운 액세스 계층 인증 절차에서 사용되는 자격 증명들을 발생시키는 데 사용될 수 있다. 인증 메커니즘들을 개발하는 목적은 관여된 단계들 및 절차들을 최적화하고 모든 형태의 액세스 네트워크들에 걸쳐 로밍하는 동안 매끄러운 인증을 용이하게 하는 것일 수 있다.

[0104] SSO(Single Sign-On, 싱글 사인온) 프로토콜들(예를 들어, OpenID Connect) 및 역 부트스트랩핑(reverse bootstrapping)을 사용하는 한 예는 STA가 WLAN 네트워크들과 같은 이전에 몰랐던 네트워크들을 발견하고 그에 액세스할 수 있게 할 것이다. 새로운 네트워크에서 자격 증명들을 사전 프로비저닝할 필요가 없을 수 있는데, 그 이유는 이들이 이미 실행 중인 응용 프로그램 서비스 보안으로부터 부트스트랩될 수 있기 때문이다.

[0105] WLAN 네트워크들과의 SSO 통합을 위한 구현 옵션들은 OP(Identity Provider) 기능과 eANDSF(enhanced ANDSF, 향상된 ANDSF) 기능을 통합시키는 AAA 서버의 사용을 포함할 수 있고, AAA 서버는 OP 기능을 통합시킨다.

[0106] 도 9는 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA 서버(910)가 OP 기능과 eANDSF(enhanced ANDSF) 기능을 통합시킬 수 있는 한 예시적인 방법(900)의 도면이다. 이 예는 STA(920) 및 AAA 서버(910)의 OP 유닛이 WLAN 네트워크에 액세스하기 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(920)와 AAA 서버(910)의 OP 유닛 사이의 접속이 설정되지 않은 경우, OpenID Connect 인

증을 교환하고 양쪽 엔터티들 상에 마스터 키를 발생시키기 위해 STA(920)와 AAA 서버(910)의 OP 유닛 사이에서 능동 3GPP 연결이 사용될 수 있다.

[0107] 제1 예에서, STA(920)는 3GPP 액세스 네트워크를 거쳐 AAA 서버(910)의 OP 유닛에 대한 상호 인증(930)을 성공적으로 완료했을 수 있고, 공유 마스터 키들[예를 들어, PSK(pre-shared key, 사전 공유 키)]이 STA(920) 및 AAA 서버(910)의 OP 유닛 둘 다에 설정되어 있을 수 있다. 그에 부가하여, STA(920) 및 AAA(910)의 eANDSF는, 예를 들어, 3GPP eS14(enhanced S14, 향상된 S14) 인터페이스를 거쳐 상호 인증되고 설정된 보안 연결(940)을 가질 수 있다. STA(920)는 AAA 서버(910)의 eANDSF 유닛에 WLAN 네트워크 정보를 요청할 수 있고 그리고/또는 AAA 서버의 eANDSF 유닛은 WLAN 네트워크 정보를 보안 3GPP 연결을 거쳐 STA로 푸시할 수 있다. 네트워크 정보는 이용가능한 AP들, SSID들, 사용할 인증 방법, 및 다른 액세스 네트워크 파라미터들을 포함할 수 있다. 이용가능한 AP들 및 WLAN 네트워크들에 관한 정보를 사용하여, STA(920)는 비콘들에 대한 수동 스캔을 수행하거나 긴 네트워크 발견 절차를 수행할 필요가 없을 수 있다. STA(920)는 프로브 요청(950)을 AAA 서버(910)의 eANDSF 유닛에 의해 STA(920)에 제공되는 우선순위화된 목록으로부터 선택된 AP(960)로 즉각 전송할 수 있다.

[0108] STA(920)는, 선택된 AP(960)로부터 프로브 응답(970)을 수신한 후에, 개방형 인증(open authentication)(971)을 수행하고 선택된 AP(960)와 접속할 수 있다. 개방형 인증(971)은 어떤 보안 대책들도 제공하지 않을 수 있고, 802.1x/EAP 방법이 사용되는 경우, 생략될 수 있다.

[0109] AP(960)는, 이 예에서, 인증자(authenticator)라고 지칭될 수 있고, STA ID(identity)를 요청하는 EAP 요청(973)을 발행할 수 있다. STA(920)는 고유 ID(unique identity), 예를 들어, 그의 영역(realm)과 함께 IMSI(international mobile subscriber Identity, 국제 모바일 가입자 ID)를 포함할 수 있는 EAP 응답(974)을 반환할 수 있다. 이 영역은 SSO 인증을 사용하기 위한 힌트(예를 들어, IMSI@sso.MNO.com)를 포함할 수 있다. AP(960)는, 예를 들어, RADIUS 액세스 요청을 사용하여, 액세스 요청(975)을 AAA 서버로 전송할 수 있다. 액세스 요청(975)은 EAP ID를 포함할 수 있다. AAA 서버(910)의 OP 유닛은 STA ID(identity)를 인식하고, 이를 기존의 보안 접속과 상관시킬 수 있다. AAA 서버(910)의 OP 유닛은 STA(920)가 이미 인증된 것으로 결정하고, 고속 EAP 인증을 수행하며, STA와 공유되는 이전에 발생된 마스터 키에 기초하여 PMK(976)를 발생시킬 수 있다. AAA 서버(910)는 액세스 수락 메시지(977)를 AP(960)로 전송할 수 있다. 액세스 수락 메시지(977)는 EAP 성공 및 AP(960)에 대한 키 자료(key material)를 포함할 수 있다. AP(960)는 EAP 성공 메시지(978)를 STA(920)로 전달할 수 있다. STA(920)는 OP와의 그의 공유 마스터 키를 사용하여 PMK(980)를 발생시킬 수 있다.

[0110] AP(960)가 EAP 성공 메시지(978)를 전송하고 AP(960)가 유니캐스트 트래픽의 암호화를 위한 PTK(pairwise transient key, 짝 과도 키) 그리고 브로드캐스트 및 멀티캐스트 트래픽의 암호화를 위한 GTK(group temporal key, 그룹 임시 키)를 포함할 수 있는 임시 키들(983)을 도출하기 위해 4-단계 핸드쉐이크 프로토콜(981)을 개시할 수 있을 때, 802.1X/EAP 인증이 완료될 수 있다. 4-단계 핸드쉐이크 프로토콜(981)은 AP(960)와 STA(920) 사이에서 4개의 EAPOL-Key 프레임 메시지들을 사용할 수 있다.

[0111] 4-단계 핸드쉐이크는 다양한 입력들을 해싱하여 의사 난수 값들을 도출하기 위해 PRF들(pseudo-random functions, 의사 난수 함수들)을 사용할 수 있다. PMK는 STA(920) 및 AP(960) 상에서 PTK를 생성하기 위해 다른 입력들과 결합되는 입력들 중 하나일 수 있다. 의사 난수 함수에 의해 사용되는 다른 입력들 중 일부는 넌스(nonce)라고 지칭될 수 있다. 넌스는 한번만 발생되고, 암호 연산에서 사용되며, 주어진 암호 키와 연관되어 있는 난수 값(random numerical value)일 수 있다. 4-단계 핸드쉐이크의 경우, 넌스는 PMK와 연관되어 있을 수 있다. 넌스는 단지 한번만 사용될 수 있고, PMK에 대해 또다시 사용되지 않을 수 있다. 4-단계 핸드쉐이크에 의해 2개의 넌스들: AP 넌스(AP nonce)(ANonce) 및 요청자 넌스(supplicant nonce)(SNonce)가 생성될 수 있다. Snonce는 STA 넌스라고도 지칭될 수 있다.

[0112] PTK를 생성하기 위해, 4-단계 핸드쉐이크는 PMK, 수치 인증자 넌스, 요청자 넌스, 인증자의 MAC 주소(AA), 및 요청자의 MAC 주소(SPA)를 결합시키는 의사 난수 함수를 사용할 수 있다.

[0113] 4-단계 핸드쉐이크 절차에서, AP 및 STA 각각은 그들 각자의 넌스들을 랜덤하게 생성할 수 있다. 인증자[예를 들어, AP(960)]는 EAPOL-Key 프레임(982)을 요청자[예를 들어, STA(920)]로 전송할 수 있다. EAPOL-Key 프레임(982)은 ANonce를 포함할 수 있다. STA(920)는 이제 의사 난수 함수를 위한 모든 필요한 입력들을 가지고 있을 수 있다. STA(920)는 PMK, ANonce, SNonce, 및 MAC 주소들로부터 PTK(983)를 도출할 수 있다. STA(920)는 이제 유니캐스트 트래픽을 암호화하기 위해 사용될 수 있는 PTK를 소유하고 있을 수 있다.

[0114] STA(920)는 EAPOL-Key 프레임(984)을 AP(960)로 전송할 수 있다. EAPOL-Key 프레임은 SNonce를 포함할 수 있

다. AP(960)는 이제 의사 난수 함수를 위한 모든 필요한 입력들을 가지고 있을 수 있다. STA(920)는 또한 그의 RSN 정보 요소 능력 및 MIC(message integrity code, 메시지 무결성 코드)를 AP(960)로 전송할 수 있다. AP(960)는 PMK, ANonce, SNonce, 및 MAC 주소들로부터 PTK(985)를 도출할 수 있다. AP(960)는 또한 MIC를 유효성 확인할 수 있다. AP(960)는 이제 유니캐스트 트래픽을 암호화하기 위해 사용될 수 있는 PTK(pairwise transient key)를 소유하고 있을 수 있다.

[0115] AP(960)는 그가 소유하고 있는 GMK(group master key, 그룹 마스터 키)로부터 GTK(986)를 도출할 수 있다. AP(960)는 EAPOL-Key 프레임(987)을 STA(920)로 전송할 수 있다. EAPOL-Key 프레임(987)은 ANonce, AP의 RSN 정보 요소 능력, 및 MIC를 포함할 수 있다. EAPOL-Key 프레임(987)은 또한 임시 키들을 설치하기 위한 STA(920)로의 메시지를 포함할 수 있다. GTK(986)는 유니캐스트 EAPOL-Key 프레임(987) 내에서 STA(920)로 배달될 수 있다. GTK(986)가 PTK(985)로 암호화되어 있을 수 있기 때문에, 그의 기밀성이 보호될 수 있다. STA(920)는, 임시 키들이 설치되었다는 것을 확인하기 위해, EAPOL-Key 프레임(988)을 AP(960)로 전송할 수 있다.

[0116] 앞서 기술한 4-단계 핸드쉐이크 절차에 대한 최적화로서, AP와 STA 사이의 EAPOL-Key 프레임 메시지들의 수를 2개로 감소시키는 것이 가능할 수 있다. 이것은 이하의 예시적인 최적화들 중 임의의 것을 사용하여 달성될 수 있다. AAA 서버의 OP 유닛 및 STA는 PMK 키 및 GMK 키를 도출하기 위해 마스터 키를 이용할 수 있다. AAA 서버는 PMK 및 GMK 둘 다를 AP로 전송할 수 있다. 4-단계 핸드쉐이크의 첫번째 메시지는, ANonce,에 부가하여, AP에 의해 랜덤하게 발생된 GNonce(group nonce, 그룹 넌스)를 포함하도록 수정될 수 있다. STA는 PMK, ANonce, SNonce, 및 MAC 주소들로부터 PTK를 도출할 수 있다. STA는 또한 GMK, GNonce, 및 MAC 주소들로부터 GTK를 도출할 수 있다. STA는 이제 유니캐스트, 브로드캐스트, 및 멀티캐스트 트래픽을 암호화 및 복호화하는 데 사용될 수 있는 짝 과도 키들(PTK, GTK)을 소유하고 있을 수 있다. STA는 SNonce를 포함하는 EAPOL-Key 프레임을 AP로 전송할 수 있다. STA는 또한 그의 RSN 정보 요소 능력 및 MIC(message integrity code)를 AP로 전송할 수 있다. AP는 PMK, ANonce, SNonce, 및 MAC 주소들로부터 PTK를 도출할 수 있다. AP는 또한 GMK, GNonce, 및 MAC 주소들로부터 GTK를 도출할 수 있다. 그에 부가하여, AP는 MIC를 유효성 확인할 수 있다.

[0117] 4-단계 핸드쉐이크 절차 동안의 한 시점에서, STA 및 AP 둘 다는 유니캐스트, 브로드캐스트 및 멀티캐스트 트래픽을 암호화 및 복호화하는 데 사용될 수 있는 PTK 키 및 GTK 키를 가지고 있을 수 있다. 이와 같이, 나머지 4-단계 핸드쉐이크 절차가 필요하지 않을 수 있다.

[0118] 4-단계 핸드쉐이크 절차의 끝에서, STA(920)는 DHCP 프로토콜을 사용하여 IP 주소 및 필요한 구성들(990)[예를 들어, 사용할 하나 이상의 DNS들(domain name servers, 도메인 이름 서버들)]을 획득할 수 있고, STA는 이제 WLAN 네트워크(995)에 액세스할 수 있다.

[0119] STA가 그의 IP 주소 및 필요한 구성들을 획득하기 위한 최적화를 달성하는 한 변형예로서, eANDSF가 IP 주소 및 필요한 구성을 셀룰러 네트워크를 거쳐 STA에 제공하고 AAA 서버가, 예를 들어, EAP-Notify 메시지를 사용하여 EAP 메시지에 캡슐화된 IP 주소 및 필요한 구성들을 STA로 송신하는 경우, 이 단계가 생략될 수 있다.

[0120] 도 10은 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 AAA 서버(1005)가 OP 기능과 eANDSF 기능을 통합시키는 한 예시적인 방법(1000)의 도면이다. 이 예는 STA(1010) 및 AAA 서버(1005)의 OP 유닛이 WLAN 네트워크에 액세스하기 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(1010)는, 예를 들어, 3GPP 액세스 네트워크에 이전에 연결되어 있을 수 있는 네트워크를 거쳐 AAA 서버(1005)의 OP 유닛에 대한 상호 인증(1015)을 성공적으로 완료했을 수 있고, 공유 마스터 키들(PSK)이 STA(1010) 및 AAA 서버(1005)의 OP 유닛에 설정되어 있을 수 있다. 그에 부가하여, STA(1010) 및 AAA 서버의 eANDSF 유닛은 상호 인증될 수 있고, 예를 들어, 3GPP STA-eS14 인터페이스를 거쳐 보안 연결이 설정(1020)될 수 있다. STA(1010)는 AAA 서버(1005)의 eANDSF 유닛에 WLAN 네트워크 정보를 요청할 수 있고 그리고/또는 AAA 서버(1005)의 eANDSF 유닛은 WLAN 네트워크 정보를 보안 3GPP 연결을 거쳐 STA(1010)로 푸시할 수 있다. 네트워크 정보는 이용가능한 AP들, SSID들, 사용할 인증 방법, 및 다른 액세스 네트워크 파라미터들을 포함할 수 있다. 이용가능한 AP들 및 WLAN 네트워크들에 관한 정보를 사용하여, STA(1010)는 비콘들에 대한 수동 스캔을 수행하거나 긴 네트워크 발견 절차를 수행할 필요가 없을 수 있다. STA(1010)는 프로브 요청(1025)을 AAA 서버(1005)의 eANDSF 유닛에 의해 STA(1010)에 제공되는 우선순위화된 목록으로부터 선택된 AP(1030)로 즉각 전송할 수 있다.

[0121] STA(1010)는, 선택된 AP(1030)로부터 프로브 응답(1035)을 수신한 후에, 개방형 인증(1040)을 수행하고 선택된 AP(1030)와 접속(1042)할 수 있다. 개방형 인증(1040)은 어떤 보안 대책들도 제공하지 않을 수 있고,

802.1x/EAP 방법이 사용되는 경우, 생략될 수 있다.

[0122] AP(1030)는, 이 예에서, 인증자라고 지칭될 수 있고, STA ID(identity)를 요청하는 EAP 요청(1042)을 발행할 수 있다. STA(1010)는 고유 ID(unique identity), 예를 들어, 그의 영역과 함께 IMSI(international mobile subscriber Identity, 국제 모바일 가입자 ID)를 포함할 수 있는 EAP 응답(1043)을 반환할 수 있다. 이 영역은 SSO 인증을 사용하기 위한 힌트(예를 들어, IMSI@sso.MNO.com)를 포함할 수 있다. AP(1030)는, 예를 들어, RADIUS 액세스 요청을 사용하여, 액세스 요청(1044)을 AAA 서버(1005)로 전송할 수 있다. 액세스 요청(1044)은 EAP ID를 포함할 수 있다.

[0123] AAA 서버(1005)의 OP 유닛은, 액세스 수락 메시지를 AP로 송신하기 전에, STA(1010)가 재인증될 필요가 있는 것으로 결정할 수 있다. 따라서, EAP-성공 및 키잉 자료(keying material)를 AP로 송신하기 전에, 하나 이상의 EAP-신청/응답 메시지 라운드들이 교환될 수 있다. 예를 들어, AAA 서버(1005)는 STA-OP PSK(1045)에 기초하여 신청을 발생시키고 액세스 신청 메시지(1046)를 AP(1030)로 전송할 수 있다. 액세스 신청 메시지(1046)는 EAP ID 및/또는 EAP 신청을 포함할 수 있다. AP(1030)는, 액세스 신청 메시지(1046)에 응답하여, EAP-요청 메시지(1047)를 STA(1010)로 전송할 수 있다. EAP-요청 메시지(1047)는 ID(identity) 및/또는 신청을 포함할 수 있다. STA(1010)는 EAP-요청 메시지(1047)를 수신하고, MAC을 검증하며, SRES(1048)를 발생시키고, EAP-응답 메시지(1049)를 AP(1030)로 전송할 수 있다. EAP-응답 메시지(1049)는 ID(identity) 및/또는 신청에 대한 응답을 포함할 수 있다.

[0124] AP(1030)는 액세스 요청 메시지(1050)를 AAA 서버(1005)로 전송하고, 그에 응답하여 액세스 수락 메시지(1051)를 AAA 서버(1005)로부터 수신할 수 있다. 액세스 요청 메시지(1050)는 EAP ID 및/또는 신청에 대한 응답을 포함할 수 있다. 액세스 수락 메시지(1051)는 EAP ID, 성공의 표시, 및 AP에 대한 PMK 키를 포함할 수 있다. 액세스 수락 메시지(1051)를 수신한 것에 응답하여, AP(1030)는 EAP-성공 메시지(1052)를 STA(1010)로 전송할 수 있다. EAP-성공 메시지(1052)를 수신한 것에 응답하여, STA(1010)는 STA-OP PSK를 사용하여 PMK(1053)를 발생시킬 수 있고, AP(1030)와 4-단계 핸드쉐이크 프로토콜(1054)을 수행할 수 있으며, DHCP(1055)를 사용하여 IP 주소 할당을 요청할 수 있고, WLAN(1056)을 거쳐 인터넷에 액세스할 수 있으며, 이에 대해서는 앞서 도 9에 기술되어 있다.

[0125] 도 11은 매끄러운 인증 및 FILS를 가능하게 하기 위해 AAA 서버(1101)가 OP 기능을 통합시키는 한 예시적인 방법(1100)의 도면이다. 도 11의 예는 STA(1102) 및 AAA 서버(1101)의 OP 유닛이 WLAN 네트워크에 액세스하기 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(1102)는, 예를 들어, 3GPP 액세스 네트워크를 거쳐 OP에 대한 상호 인증을 성공적으로 완료했을 수 있고, 공유 마스터 키들(PSK)이 STA(1102) 및 AAA 서버(1101)의 OP 유닛에 설정되어 있을 수 있다. STA(1102)는 eANDSF에의 연결을 갖지 않을 수 있고, 따라서, 다른 메커니즘들을 통해(예를 들어, 802.11u를 사용하여) WLAN 네트워크 발견을 수행할 수 있다.

[0126] 도 11에 도시된 예에서, 고속 EAP 절차 동안, AAA 서버(1101)의 OP 유닛은 STA ID(identity)를 인식하고, 이를 기존의 보안 접속과 상관시킬 수 있다. AAA 서버(1101)의 OP 유닛은 STA(1102)가 이미 인증된 것으로 결정하고, 고속 EAP 인증을 수행하며, STA(1102)와 공유되는 이전에 발생된 마스터 키에 기초하여 PMK를 발생시킬 수 있다.

[0127] 예를 들어, STA(1102)는, 예를 들어, 3GPP 액세스 네트워크에 이전에 연결되어 있을 수 있는 네트워크를 거쳐 AAA 서버(1101)의 OP 유닛에 대한 상호 인증(1103)을 성공적으로 완료했을 수 있고, 공유 마스터 키들(PSK)이 STA(1102) 및 AAA 서버(1101)의 OP 유닛에 설정되어 있을 수 있다. STA(1102)는 수동 및/또는 능동 AP 발견(1104)을 수행할 수 있고, 이에 대해서는 도 9에 기술되어 있다. STA(1102)는 네트워크 발견(1105)을 수행하기 위해 하나 이상의 GAS 메시지 교환들을 수행할 수 있다. 예를 들어, STA(1102)는 GAS 메시지(1106)를 AP(1107)로 전송하고, 그에 응답하여, AP(1107)로부터 GAS 응답 메시지(1108)를 수신할 수 있다.

[0128] STA(1102)는 개방형 인증(1109)을 수행하고 선택된 AP(1107)와 접속(1110)할 수 있다. 개방형 인증(1109)은 어떤 보안 대책들도 제공하지 않을 수 있고, 802.1x/EAP 방법이 사용되는 경우, 생략될 수 있다.

[0129] AP(1107)는, 이 예에서, 인증자라고 지칭될 수 있고, STA ID(identity)를 요청하는 EAP 요청(1112)을 발행할 수 있다. STA(1102)는 고유 ID(unique identity), 예를 들어, 그의 영역과 함께 IMSI(international mobile subscriber Identity)를 포함할 수 있는 EAP 응답(1113)을 반환할 수 있다. 이 영역은 SSO 인증을 사용하기 위한 힌트(예를 들어, IMSI@sso.MNO.com)를 포함할 수 있다. AP(1107)는, 예를 들어, RADIUS 액세스 요청을

사용하여, 액세스 요청(1114)을 AAA 서버(1101)로 전송할 수 있다. 액세스 요청(1114)은 EAP ID를 포함할 수 있다.

[0130] AAA 서버(1101)는 STA-OP PSK(1115)로부터 PMK를 발생시키고 액세스 수락 메시지(1116)를 AP(1107)로 전송할 수 있다. 액세스 수락 메시지(1116)는 EAP ID, 성공의 표시, 및 AP에 대한 PMK 키를 포함할 수 있다. AP(1107)는 EAP 성공 메시지(1119)를 STA(1102)로 전송할 수 있다. 그에 응답하여, STA(1102)는 STA-OP PSK(1120)를 사용하여 PMK를 발생시킬 수 있고, AP(1107)와 4-단계 핸드쉐이크 프로토콜(1121)을 수행할 수 있으며, DHCP(1122)를 사용하여 IP 주소 할당을 요청할 수 있고, WLAN(1123)을 거쳐 인터넷에 액세스할 수 있으며, 이에 대해서는 앞서 도 9에 기술되어 있다.

[0131] 도 12는 매끄러운 인증 및 FILS를 가능하게 하기 위해 AAA 서버(1201)가 OP 기능을 통합시킬 수 있는 한 예시적인 방법(1200)의 도면이다. 이 예는 STA(1202) 및 AAA 서버(1201)의 OP 유닛이 WLAN 네트워크에 액세스하기 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(1202)는, 예를 들어, 3GPP 액세스 네트워크를 거쳐 AAA 서버(1201)의 OP 유닛에 대한 상호 인증(1203)을 성공적으로 완료했을 수 있고, 공유 마스터 키들(예를 들어, PSK)이 STA(1202) 및 AAA 서버(1201)의 OP 유닛에 설정되어 있을 수 있다. STA(1202)는 eANDSF에의 연결을 갖지 않을 수 있고, 따라서, 다른 메커니즘들을 통해(예를 들어, 802.11u를 사용하여) WLAN 네트워크 발견을 수행할 수 있다.

[0132] 도 12를 참조하면, STA(1204)는 수동 및/또는 능동 AP 발견(1205)을 수행할 수 있고, 이에 대해서는 도 9에 기술되어 있다. STA(1202)는 네트워크 발견(1206)을 수행하기 위해 하나 이상의 GAS 메시지 교환들을 수행할 수 있다. 예를 들어, STA(1202)는 GAS 메시지(1207)를 AP(1204)로 전송하고, 그에 응답하여, AP(1204)로부터 GAS 응답 메시지(1208)를 수신할 수 있다.

[0133] STA(1202)는 개방형 인증(1209)을 수행하고 선택된 AP(1204)와 접속(1210)할 수 있다. 개방형 인증(1209)은 어떤 보안 대책들도 제공하지 않을 수 있고, 802.1x/EAP 방법이 사용되는 경우 생략될 수 있다.

[0134] AP(1204)는, 이 예에서, 인증자라고 지칭될 수 있고, STA ID(identity)를 요청하는 EAP 요청(1211)을 발행할 수 있다. STA(1202)는 고유 ID(unique identity), 예를 들어, 그의 영역과 함께 IMSI(international mobile subscriber Identity)를 포함할 수 있는 EAP 응답(1212)을 반환할 수 있다. 이 영역은 SSO 인증을 사용하기 위한 힌트(예를 들어, IMSI@sso.MNO.com)를 포함할 수 있다. AP(1204)는, 예를 들어, RADIUS 액세스 요청을 사용하여, 액세스 요청(1213)을 AAA 서버(1201)로 전송할 수 있다. 액세스 요청(1213)은 EAP ID를 포함할 수 있다.

[0135] AAA 서버(1201)의 OP 유닛은, 액세스 수락 메시지를 AP(1204)로 전송하기 전에, STA(1202)가 재인증될 필요가 있는 것으로 결정할 수 있다. 그에 따라, EAP-성공 메시지 및 키잉 자료를 AP(1204)로 전송하기 전에, 하나 이상의 EAP-신청/응답 메시지 라운드들이 교환될 수 있다. 예를 들어, AAA 서버(1201)는 STA-OP PSK(1214)에 기초하여 신청을 발생시키고 액세스 신청 메시지(1215)를 AP(1204)로 전송할 수 있다. 액세스 신청 메시지(1215)는 EAP ID 및/또는 EAP 신청을 포함할 수 있다. AP(1204)는, 액세스 신청 메시지(1215)에 응답하여, EAP-요청 메시지(1215)를 STA(1202)로 전송할 수 있다. EAP-요청 메시지(1216)는 ID(identity) 및/또는 신청을 포함할 수 있다. STA(1202)는 EAP-요청 메시지(1216)를 수신하고, MAC를 검증하고 SRES(1217)를 발생시키며, EAP-응답 메시지(1218)를 AP(1204)로 전송할 수 있다. EAP-응답 메시지(1218)는 ID(identity) 및/또는 신청에 대한 응답을 포함할 수 있다.

[0136] AP(1204)는 액세스 요청 메시지(1219)를 AAA 서버(1201)로 전송하고, 그에 응답하여 AAA 서버(1201)로부터 액세스 수락 메시지(1220)를 수신할 수 있다. 액세스 요청 메시지(1219)는 EAP ID 및/또는 신청에 대한 응답을 포함할 수 있다. 액세스 수락 메시지(1220)는 EAP ID, 성공의 표시, 및 AP에 대한 PMK 키를 포함할 수 있다. 액세스 수락 메시지(1220)를 수신한 것에 응답하여, AP(1204)는 EAP-성공 메시지(1221)를 STA(1202)로 전송할 수 있다. EAP-성공 메시지(1221)를 수신한 것에 응답하여, STA(1202)는 STA-OP PSK를 사용하여 PMK(1222)를 발생시킬 수 있고, AP(1204)와 4-단계 핸드쉐이크 프로토콜(1223)을 수행할 수 있으며, DHCP(1224)를 사용하여 IP 주소 할당을 요청할 수 있고, WLAN(1225)을 거쳐 인터넷에 액세스할 수 있으며, 이에 대해서는 앞서 도 9에 기술되어 있다.

[0137] 도 13은 매끄러운 인증 및 고속 초기 링크 설정을 가능하게 하기 위해 STA(1301)와 네트워크 사이의 사전 설정된 보안 접속을 위한 한 예시적인 방법(1300)의 도면이다. 이 예에서, 고속 EAP가 802.11 인증 프레임들 내에 캡슐화될 수 있다. 이것은 STA(1301) 및 네트워크[예를 들어, 통합된 OP 기능을 갖는 AAA 서버(1302)]가 WLAN

네트워크에의 보안 액세스를 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA는 3GPP 액세스 네트워크를 거쳐 AAA/OP에 대한 상호 인증(1303)을 성공적으로 완료했을 수 있고, 공유 마스터 키들(PSK) 및 FILS ID(Identity)(1304)가 STA(1301) 및 AAA 서버(1302) 둘 다에 설정되어 있을 수 있다.

[0138] 이 예에서, 802.11 인증 프레임들은 STA(1301)와 AP(1305) 사이의 고속 EAP 메시지들을 캡슐화할 수 있다. 그에 부가하여, SNonce 및 ANonce가 인증 프레임들을 사용하여 교환될 수 있고, 이는 4-단계 핸드쉐이크 프로토콜이 동시에 수행될 수 있게 할 것이다. 예를 들어, STA(1301)는 SNonce(1306)를 발생시키고 인증 메시지(1307)를 AP(1305)로 전송할 수 있다. 인증 메시지(1307)는 EAP 응답 메시지를 포함하고, 순서 번호, FILS ID, SNonce, 및/또는 Auth-tag를 나타낼 수 있다. AP(1305)는 SNonce를 저장(1308)하고, 액세스 요청 메시지(1309)를 AAA 서버(1302)로 전송할 수 있다. 액세스 요청 메시지(1309)는 EAP 메시지일 수 있고, FILS ID, 시퀀스 번호(SEQ), 및/또는 Auth-tag를 포함할 수 있다.

[0139] AAA 서버(1302)는 STA(1301)와의 사전 설정된 보안 컨텍스트를 탐색하기 위해 FILS ID(identity)를 사용할 수 있다. AAA 서버(1302)는 시퀀스 번호를 검증할 수 있다. 이 서버는 이어서 계속하여 무결성 키를 사용하여 메시지의 무결성을 검증할 수 있고, 그로써 피어에 의한 그 키의 소유의 증명을 검증할 수 있다. 모든 검증들이 성공적인 경우, AAA 서버(1302)는 STA-OP PSK로부터 PMK를 발생(1310)시키고, 액세스 수락 메시지(1311)를 AP(1305)로 전송할 수 있다. 액세스 수락 메시지는 세션 키(예를 들어, PMK), EAP-성공 메시지, SEQ, FILS ID, CB-Info(Channel binding information, 채널 바인딩 정보) 필드, 및/또는 인증 태그(Auth-tag)를 포함할 수 있다. Auth-tag는 수신기(예를 들어, STA 또는 AAA 서버)가 수신된 메시지의 무결성을 검증하고 그의 유효성을 결정할 수 있게 할 것이다. AAA 서버(1302)는, STA가 EAP 메시지가 손상된 AP가 아니라 올바른 AP를 통해 수신되었다는 것을 검증할 수 있도록 CB-Info를 EAP 메시지(도시 생략)에서 전송할 수 있다.

[0140] STA(1301)가 선택적인 [IP_CFG_REQ] 필드를 인증 메시지(1307)에 포함시키는 경우, AAA 서버(1302)는 IP 구성들을 EAP-성공 메시지의 [IP_CFG_Reply] 필드에서 STA(1301)로 전송할 수 있다. 유의할 점은, 브라켓들이 선택적인 필드들을 나타낼 수 있다는 것이다.

[0141] 그에 부가하여, AAA 서버(1302)는, STA(1301)가 EAP 메시지가 손상된 AP가 아니라 올바른 AP를 통해 수신되었다는 것을 검증할 수 있도록 채널 바인딩 정보[CB-Info]를 EAP-성공 메시지에서 전송할 수 있다.

[0142] 액세스 수락 메시지(1311)를 수신한 것에 응답하여, AP(1305)는 PMK, ANonce, 및/또는 SNonce로부터 PTK를 도출(1312)하고, GTK를 발생시킬 수 있다. AP(1305)는 인증 메시지(1313)를 STA(1301)로 전송할 수 있다. 인증 메시지(1313)는, 예를 들어, SEQ, FILS ID, CB-Info, ANonce, 및/또는 Auth-tag를 나타낼 수 있는 EAP 성공 메시지를 포함할 수 있다.

[0143] 인증 메시지(1313)를 수신한 것에 응답하여, STA(1301)는 PTK(1314)를 도출하고 GTK를 설치할 수 있다. 성공적인 인증의 끝에서, STA(1301) 및 AP(1305)는 802.11 무선기(1315)를 거쳐 STA(1301)와 AP(1305) 사이에서 교환되는 데이터를 보호할 준비가 되어 있는 (PTG, GTK) 키들을 가질 수 있다.

[0144] STA(1301)가 필요한 IP 구성들을 가지고 있지 않을 수 있는 경우에, STA(1301)는, 응용 프로그램들(예를 들어, 인터넷 브라우징)을 기동시키거나 진행 중인 세션들을 하나의 네트워크(예를 들어, 3GPP)로부터 WLAN 네트워크로 안전하게 스위칭할 준비가 되어 있을 수 있도록, 예를 들어, FILS 인증된 STA에 대한 필요한 IP 주소 구성들을 제공하기 위해 802.11 접속 프레임 교환을 사용할 수 있다. 예를 들어, STA(1301)는 접속 메시지(1316)를 AP(1305)로 전송하고, 그에 응답하여 AP(1305)로부터 접속 메시지(1317)를 수신할 수 있다. 접속 메시지(1316)는 [IP-CFG-REQ] 필드를 포함할 수 있고, 접속 메시지(1317)는 [IP-CFG-Reply] 필드를 포함할 수 있다.

[0145] 도 14는 매끄러운 인증 및 고속 초기 링크 설정을 가능하게 하기 위해 STA(1401)와 네트워크[예를 들어, AAA 서버(1402)] 사이의 사전 설정된 보안 접속을 위한 한 예시적인 방법(1400)의 도면이다. 이 예에서, 고속 EAP가 802.11 접속 프레임들 내에 캡슐화될 수 있다. AAA 서버(1402)는 OP 기능들을 수행하도록 구성될 수 있다.

[0146] 이 예는 STA(1301) 및 AAA 서버(1402)가 WLAN 네트워크에의 보안 액세스를 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(1401)가 3GPP 액세스 네트워크를 거쳐 AAA 서버(1402)의 OP 유닛에 대한 상호 인증(1403)을 성공적으로 완료했고 공유 마스터 키들(PSK) 및 FILS ID(Identity)(1404)가 STA(1401) 및 AAA 서버(1402) 둘 다에 설정되어 있는 것으로 가정될 수 있다.

[0147] 이 예에서, STA(1401)는 SNonce(1405)를 발생시키고 접속 프레임(1406)을 AP(1407)로 전송할 수 있다. 접속 프레임(1406)은 EAP 메시지를 포함하고, SEQ, FILS ID, [IP-CFG- REQ], Snonce(1405), 및/또는 Auth-tag를 나

타낼 수 있다. AP(1407)는 접속 프레임(1406)을 수신하고 SNonce(1405)를 저장(1408)할 수 있다. AP(1407)는 액세스 요청 프레임(1409)을 AAA 서버(1402)로 전송할 수 있다. 액세스 요청 프레임(1409)은 EAP-응답 메시지를 포함하고, SEQ, FILS ID, [IP-CFG- REQ], 및/또는 Auth-tag를 나타낼 수 있다.

[0148] 액세스 요청 프레임(1409)을 수신한 것에 응답하여, AAA 서버(1402)는 STA-OP PSK로부터 PMK를 발생(1410)시킬 수 있다. AAA 서버(1402)는 액세스 수락 프레임(1411)을 AP(1407)로 전송할 수 있다. 액세스 수락 프레임(1411)은 PMK 및/또는 EAP-성공 메시지를 포함하고, SEQ, FILS ID, [IP-CFG-Reply], [CB-Info], 및/또는 Auth-tag를 나타낼 수 있다.

[0149] 액세스 수락 프레임(1411)을 수신한 것에 응답하여, AP(1407)는 PMK, ANonce, 및/또는 SNonce로부터 PTK를 도출(1412)하고, GTK를 발생시킬 수 있다. AP(1407)는 접속 프레임(1413)을 STA(1401)로 전송할 수 있다. 접속 프레임(1413)은 EAP-성공 메시지를 포함하고, SEQ, FILS ID, [CB-Info], Anonce, [IP-CFG-Reply], 및/또는 Auth-tag를 나타낼 수 있다. STA(1401)는 PTK를 도출(1414)하고 GTK를 설치하며 WLAN을 통해 인터넷에 액세스(1415)할 수 있다.

[0150] 이 예에서, 802.11 접속 프레임들은 적어도 다음과 같은 것들을 포함할 수 있다: (1) STA와 AP 사이의 고속 EAP 메시지들; (2) 4-단계 핸드쉐이크 프로토콜을 동시에 완료하는 데 필요한 SNonce 및 ANonce; (3) 동시적인 IP 주소 할당을 위한 STA로부터 AP로의 [IP-CFG-REQ] 및 AP로부터 STA로의 [IP-CFG-Reply]. 접속의 끝에서, FILS 인증된 STA는 WLAN 네트워크에 안전하게 액세스하기 위해 필요한 IP 주소 구성들을 가질 수 있다.

[0151] 도 15는 매끄러운 인증 및 고속 링크 설정을 가능하게 하기 위해 STA(1501)와 네트워크[예를 들어, AAA 서버(1502)] 사이의 사전 설정된 보안 접속을 위한 한 예시적인 방법(1500)의 도면이다. 이 예는 비EAP FILS 인증에 기초할 수 있다. AAA 서버(1502)는 OP 기능 및/또는 eANDSF 기능을 수행하도록 구성될 수 있다.

[0152] 이 예는 STA(1501) 및 AAA 서버(1502)가 WLAN 네트워크에의 보안 액세스를 위해 이용될 수 있는 보안 접속 및 마스터 키들을 이미 설정한 것으로 가정할 수 있다. STA(1501)가, 예를 들어, 3GPP 액세스 네트워크를 거쳐 AAA 서버(1502)의 OP 유닛에 대한 상호 인증(1503)을 성공적으로 완료했고 공유 마스터 키들(PSK) 및 FILS ID(Identity)가 STA(1501) 및 AAA 서버(1502) 둘 다에 설정(1504)되어 있는 것으로 가정될 수 있다.

[0153] 이 예에서, 802.11 인증 프레임들은 STA(1501)와 AP(1505) 사이에서 비EAP 인증 메시지들을 전달할 수 있다. 그에 부가하여, ANonce가 STA(1501)가 PTK를 도출할 수 있게 할 것인 인증 프레임들을 사용하여 AP(1505)로부터 STA(1501)로 전송될 수 있다.

[0154] 802.11 접속 프레임들은, AP(1505)가 자기 쪽에서 PTK를 도출할 수 있도록, SNonce를 STA(1501)로부터 AP(1505)로 전달할 수 있다. 그에 부가하여, 접속 프레임들은 선택적 IP 구성 요청 [IP-CFG-REQ]을 STA(1501)로부터 AP(1505)로 그리고 [IP-CFG-Reply]를 AP(1505)로부터 STA(1501)로 전달할 수 있다. 접속의 끝에서, FILS 인증된 STA는 WLAN 네트워크에 안전하게 액세스하기 위해 필요한 IP 주소 구성들을 가진다.

[0155] 예를 들어, STA(1501)는 인증 메시지(1506)를 AP(1505)로 전송할 수 있다. 인증 메시지(1506)는 SEQ, FILS ID, 및/또는 Auth-tag를 포함할 수 있다. 인증 메시지(1506)를 수신한 것에 응답하여, AP(1505)는 액세스 요청 메시지(1507)를 AAA 서버(1502)로 전송할 수 있다. 액세스 요청 메시지(1507)는 SEQ, FILS ID, 및/또는 Auth-tag를 포함할 수 있다. AAA 서버는 STA-OP PSK로부터 PMK를 발생(1508)시키고 액세스 수락 메시지(1509)를 AP(1505)로 전송할 수 있다. 액세스 수락 메시지는 PMK, SEQ, FILS ID, [CB-Info], 및/또는 Auth-tag를 포함할 수 있다.

[0156] 액세스 수락 메시지(1509)를 수신한 것에 응답하여, AP(1505)는 인증 메시지(1510)를 STA(1501)로 전송할 수 있다. 인증 메시지(1510)는 SEQ, [CB-Info], Anonce, 및/또는 Auth-tag를 포함할 수 있다. STA(1501)는 SNonce를 발생(1511)시키고, PTK를 도출하며, 접속 메시지(1512)를 AP(1505)로 전송할 수 있다. 접속 메시지(1512)는 Snonce, [IP-CFG-REQ], 및/또는 Auth-tag를 포함할 수 있다.

[0157] AP(1505)는 PMK, ANonce, 및/또는 SNonce로부터 PTK를 도출(1513)하고, GTK를 발생시킬 수 있다. AP(1505)는 접속 메시지(1514)를 STA(1501)로 전송할 수 있다. 접속 메시지(1514)는 GTK, [IP-CFG-Reply], 및/또는 Auth-tag를 포함할 수 있다. 접속 메시지(1514)를 수신한 것에 응답하여, STA(1501)는 GTK를 설치(1515)하고 WLAN을 통해 안전하게 인터넷에 액세스(1516)할 수 있다.

[0158] AP 발견 단계의 끝에서, ALS 가능 STA들 및 AP들은, STA들 및 AP들이 서로에 관해 사전 획득한 정보의 이용가능성 및 양에 기초하여, ALS 사후 AP 발견 절차들을 협상할 수 있다. 이 사전 획득된 정보는, 예를 들어, 네트워

크 서비스 정보, TSF 정보, 802.11 인증 및 접속 정보, EAP/802.1x 인증 및 보안 정보, 그리고 IP 주소 할당 정보 중 하나 이상을 포함할 수 있다. 이 이용가능한 사전 획득된 정보에 기초하여, STA 또는 AP는 커스터마이즈된 사후 AP 발견 절차들의 협상을 개시할 수 있다.

[0159] 사후 AP 발견 절차 협상들을 위해 사용되는 시그널링의 예들이 표 3에 나타내어져 있고, 사후 AP 발견 링크 설정 프로세스의 각각의 단계에서의 잠재적인 동작들이 열거되고 이진 시퀀스(binary sequence)로 표현되어 있다. 표 3에서 "0b"로 시작하는 숫자들의 시퀀스는 "0b" 이후의 숫자들이 이진 형식의 표현이라는 것을 나타낼 수 있다.

표 3

[0160]

| 단계 | 협상 시그널링의 예들 | |
|---|---|---|
| | 비트 수 | 상세 |
| 네트워크 발견 | 3 | 0b000: 802.11u<br>0b001: 802.11u-plus<br>0b010 - 0b110: 예비됨<br>0b111: 네트워크 발견 단계를 생략함 |
| 부가의 TSF | 1 | 0b0: 변하지 않음<br>0b1: 부가의 TSF를 생략함 |
| 802.11 인증 | 2 | 0b00: 변하지 않음<br>0b01 - 0b10: 예비됨<br>0b11: 802.11 인증 단계를 생략함 |
| 802.11 접속 | 2 | 0b00: 변하지 않음<br>0b01: 부가 정보 요소들을 전달하도록 갱신됨;<br>0b10: 예비됨<br>0b11: 802.11 접속 단계를 생략함 |
| EAP/802.1x 인증 및 보안 | 4 | 0b0000: 변하지 않음<br>0b0001: 고속 EAP 인증을 사용함<br>0b0010: 고속 EAP 인증 및 고속 키 프로비저닝을 사용함<br>0b0011: 고속 네트워크 발견 및 고속 EAP 인증;<br>0b0100: 고속 네트워크 발견, 고속 EAP 인증, 및 고속 키 프로비저닝<br>0b0101 - 0b1110: 예비됨<br>0b1111: EAP/802.1x 인증 및 보안 단계를 생략함 |
| IP 주소 할당 | 3 | 0b000: 변하지 않음<br>0b001: 계층-2 메시지들에서 그것을 행함,<br>0b010 - 0b110: 예비됨<br>0b111: IP 주소 할당 단계를 생략함 |

[0161] 사후 AP 발견 협상 시그널링의 구현이 다면적(multi-fold)일 수 있다. 예를 들어, 사후 AP 발견 협상이 앞서 기술한 FILS 관리 동작 프레임을 사용하여 구현될 수 있고, 사후 AP 발견의 각각의 단계에 대한 협상 시그널링 코드는 FILS 관리 동작 프레임에서의 대응하는 필드에 위치해 있을 수 있다. 다른 예에서, 협상 시그널링 코드들이 AP 발견 메시지들의 IE들에서, 예를 들어, I-Know-You IE 및/또는 I-know-you-response IE에서, 비트 맵으로서 구현될 수 있다. 다른 예에서, 협상 시그널링 코드들이 비콘, 프로브 요청들 및 프로브 응답들과 같은 다른 관리 및 제어 프레임들에 포함되어 있는 IE들에 구현될 수 있다.

[0162] 표 3에서의 예시적인 인코딩을 사용하여, 15-비트 ALS 정보 필드가 그의 가장 최적화된 사후 AP 발견 링크 설정 절차를 표현하기 위해 STA 또는 AP에 의해 포함될 수 있다. ALS 정보 필드는 상이한 크기의 세그먼트들로 세그먼트화될 수 있고, 각각의 세그먼트는 사후 AP 발견 링크 설정 단계에 대응한다. 식별자에서의 비트 순서는 표 3에 예시되어 있는 기능적 단계들의 동일한 순서일 수 있고, 예를 들어, 비트 14 및 비트 13은 네트워크 발견 단계에 대응한다.

[0163] 예를 들어, AP가 MAC 주소 및/또는 서비스 요구 정보와 같은 후보 STA의 ID(identity) 정보를 사전 획득한 경우, AP는 네트워크 발견, 부가의 TSF, 및 802.11 인증 단계들이 생략될 수 있고, AP가 STA로부터 프레임(예를

들어, 프로브 요청 프레임)을 수신할 때, 링크 설정 절차가 802.11 접속, EAP 인증, 및/또는 DHCP-기반 IP 주소 할당 단계들을 거쳐야만 하는 것으로 결정할 수 있다. 따라서, AP는 15-비트 사후 AP 발견 절차 코드 "0b111 1110 0000 0000"를 포함하는 I-know-you IE를 갖는 프로브 응답 프레임을 STA로 전송할 수 있다. STA가 이러한 사후 AP 발견 절차 코드를 수신하는 경우, STA는 사후 AP 발견 절차를 확인하거나 수정하기 위해 관리 프레임에서 동일하거나 수정된 코드를 갖는 I-know-you-response IE를 전송할 수 있거나, 코드에 의해 제안되는 그 다음 단계(예를 들어, 802.11 접속)로 곧바로 진행하는 것에 의해 그것을 암시적으로 수락할 수 있다. 이러한 방식으로, AP는 STA에 관한 그의 사전 획득된 지식을 사용함으로써 링크 설정 최적화들을 개시할 수 있다.

[0164] 다른 예에서, STA가 선호된 AP로의 그의 프로브 요청 프레임에 그의 ALS 사후 AP 발견 절차에 대한 ALS 정보 필드 "0b111 111 01 0010 001"를 포함시킬 때, STA는 다음과 같은 것들 중 하나 이상을 AP에 알려줄 수 있다: 이 특정의 AP에서의 가장 최적화된 ALS 사후 AP 발견 절차는 네트워크 발견 단계들을 포함할 수 있고, 부가의 TSF 및 802.11 인증은 생략될 수 있으며; 수정된 802.11 접속 단계가 사용될 수 있고; 고속 EAP 인증 및 고속 키 프로비저닝 방식이 사용될 수 있으며; 그리고/또는 최적화된 IP 주소 할당이, 예를 들어, 하나 이상의 계층-2 메시지들에서 하나 이상의 DHCP 메시지들을 전달하는 것에 의해 사용될 수 있다. STA가 사전 획득된 정보를 갖는 STA라는 것을 나타내는 프로브 요청을 수신하는 AP는, AP가 STA에 관해 사전 획득한 정보의 양에 따라, 유사한 시퀀스를 사용하여 프로브 응답 프레임을 전송할 수 있다. 프로브 요청을 수신하는 STA는 합의된 최적화되고 커스터마이즈된 ALS 사후 AP 발견 절차를 확인하기 위해 FILS 관리 동작 프레임을 전송하는 것으로 응답할 수 있다.

[0165] AP 및 STA가 사후 AP 발견 절차를 협상할 때, AP 및 STA의 링크 설정 프로세스들의 하나 이상의 단계들이 상이한 요구사항들을 가지는 경우, 더 엄격한 요구사항이 우선할 수 있다. 상이한 요구사항들의 한 예는 STA가 네트워크 발견 단계를 생략하도록 요청할 수 있는 반면 AP는 802.11u 네트워크 발견 단계를 요청할 수 있는 경우일 수 있다. 이 예에서, STA는 AP의 요청 시에 802.11u 네트워크 발견 단계에 합의할 수 있다. 그에 부가하여, 최종적인 합의된 최적화된 ALS 사후 AP 발견 절차는 ALS의 올바른 기능을 위해 긍정적으로 확인될 수 있다. 이러한 확인은 합의된 ALS 사후 AP 발견 절차를 포함하는 FILS 관리 동작 프레임 및 합의된 ALS 사후 AP 발견 절차를 나타내는 ALS 정보 필드를 유니캐스트 프레임(프로브 요청 프레임, 프로브 응답 프레임, 접속 요청 프레임, 기타 등등)에서 대응하는 STA 또는 AP로 전송함으로써 달성될 수 있다.

[0166] 다른 예시적인 방법은 사전 획득된 시스템 구성 지식을 사용하는 것을 포함할 수 있다. 이 예에 대한 시스템 구성은 특정의 시스템 설치(system deployment) 및 동작 모드에 대해 정적이거나 준정적인 시스템 파라미터들의 세트라고 지칭될 수 있다. 이러한 시스템 파라미터들은 또한 시스템 구성 파라미터들이라고도 할 수 있고, "시스템"은 이와 관련하여 IEEE 802.11 기반 무선 LAN 시스템을 말하는 것일 수 있다.

[0167] 시스템 구성은, BSS/AP와의 링크 설정 프로세스를 개시하기 전에, STA에 의해 사전 획득될 수 있고, 초기 링크 설정 프로세스를 가속화시키기 위해 사용될 수 있다.

[0168] 시스템 구성 파라미터 세트들이 정의될 수 있다. 예를 들어, 무선 LAN 시스템의 동작 모드를 명시하기 위해, 다음과 같은 3가지 상이한 구성들이 정의되고 사용될 수 있다: (1) BSS 구성 또는 AP 구성이라고도 하는 BSS/AP 구성; (2) 액세스 네트워크 구성; 및 (3) AP/네트워크 구성이라고도 하는 결합된 AP/네트워크 구성.

[0169] 이상의 구성들 각각은 대응하는 시스템 동작 설정을 명시하는 시스템 파라미터들의 세트를 포함할 수 있다. AP 구성 파라미터 세트는 값 변화와 관련하여 시간의 경과에 따라 정적이거나 준정적인 BSS/AP 동작 파라미터들/기술자들(descriptors)을 포함할 수 있다.

[0170] 링크 설정 프로세스를 가속화시키기 위해 시스템 구성 정보를 사전 획득된 지식으로서 사용하기 위해, AP 구성 파라미터들을 선택하기 위해 다음과 같은 기본적인 기준들이 적용될 수 있다: (a) BSS/AP 동작을 시작하기 위해 사용될 수 있는 파라미터들, 예를 들어, 802.11에서 MLME_START.request 프리미티브들에서 사용되는 파라미터들; (b) AP와 STA들 사이에서, 예를 들어, 비콘 프레임 또는 프로브 응답 프레임 등에서 전달될 수 있는 BSS/AP 동작 설정들을 명시하기 위해 사용될 수 있는 파라미터들; (c) 시간의 경과에 따라 값들을 동적으로 변화시키지 않을 수 있는, 예를 들어, 몇 시간, 며칠, 심지어 몇 달 동안 동일한 값들을 유지하는 파라미터들; 및/또는 (d) 링크 설정에 관련이 있을 수 있는 파라미터들.

[0171] 기본적인 선택 기준들에 기초하여, 이하의 표 4는 인프라 BSS/AP 구성 파라미터 세트의 한 예를 제공한다.

*표 4*

[0172] 인프라 BSS/AP 구성 파라미터 세트의 한 예

| 파라미터 이름 | 값 | | 설명 | 부가 유의점 |
|---|---|---|---|---|
| | 존재 표시자 | 유효 값 범위 | | |
| BSSID | 존재해야만 함 | AP STA의 6-바이트 MAC 주소 | AP STA의 6-바이트 MAC 주소 | AP STA에 의해 송신되는 MAC 프레임 헤더에 있음 |
| SSID | 존재해야만 함 | 옥테트 문자열, 0 내지 32 옥테트 | BSS의 SSID | 비콘/프로브 응답/FD 프레임에 있음 |
| SSIDEncoding | 존재함/존재하지 않음 | 열거: UNSPECIFIED, UCS(Universal Character Set, 범용 문자 세트) UTF8(Transformation Format 8, 변환 형식 8). 이 값은 8-비트 값일 수 있다. | SSID에 대해 사용되는 인코딩 | 비콘/프로브 응답에서의 확장 능력(exended capability) IE에 있음 |
| BSSType | 존재함/존재하지 않음 | 열거: INFRASTRUCTURE, INDEPENDENT, MESH | BSS의 유형 | 비콘/프로브 응답에서의 능력(capability) IE에 있음; |
| BeaconPeriod | 존재함/존재하지 않음 | 정수: >=1 | BSS의 비콘 기간[단위: TU(Time Unit)] | 비콘/프로브 응답에서의 비콘 구간 |
| Contention Free (CF) parameter set | 존재함/존재하지 않음 | CF 파라미터 세트 요소는 PCF(point coordination function, 점 조정 함수)를 지원하는 데 필요한 파라미터들의 세트를 포함한다. 정보(Information) 필드는 CFPCount, CFPPeriod, CFPMaxDuration, 및 CFPDurRemaining 필드들을 포함한다. 정보 필드의 총 길이는 6 옥테트이다. | BSS가 CF 모드를 지원하는 경우, CF 기간들에 대한 파라미터 세트. | 비콘/프로브 응답에 있음 |
| PHY parameter set | 존재함/존재하지 않음 | 정보 필드는 Dwell Time(체류 시간), Hop Set(홉 세트), Hop Pattern(홉 패턴), 및 Hop Index(홉 인덱스) 파라미터들을 포함할 수 있다. 정보 필드의 총 길이는 5 옥테트일 수 있다. 다른 대안으로서, 정보 필드는 dot11CurrentChannel을 포함하는 단일의 파라미터를 포함할 수 있고, 길이가 1 옥테트일 수 있다. | PHY에 관련되어 있는 파라미터 세트들 | 비콘/프로브 응답에 있음 |
| CapabilityInformation | 존재함/존재하지 않음 | 능력 정보(Capability Information) 필드의 총 길이는 2 옥테트일 수 있다. | BSS에 대해 광고될 능력 | 비콘/프로브 응답에 있음 |

| | | | | |
|---|---|---|---|---|
| BSSBasicRateSet | 존재함/존재하지 않음 | 정수들의 세트: (세트 내의 각각의 정수에 대해) 1 내지 127(경계 포함) | 이 BSS에 가입하기 위해 모든 STA들에 의해 지원되어야 하는 데이터 레이트들의 세트 BSS를 생성하고 있는 STA는 세트에 열거되어 있는 데이터 레이트들 각각에서 수신하고 전송할 수 있어야 한다. | 비콘/프로브 응답에서의 Supported Rates IE에 있음 |
| OperationalRateSet | 존재함/존재하지 않음 | 정수들의 세트: (세트 내의 각각의 정수에 대해) 1 내지 127(경계 포함) | BSS 내에서의 통신을 위해 STA가 사용하고자 하는 데이터 레이트들의 세트 STA는 세트에 열거되어 있는 데이터 레이트들 각각에서 수신할 수 있어야 한다. 이 세트는 BSSBasicRateSet 파라미터에 포함되어 있는 레이트들의 수퍼셋이다. | 비콘/프로브 응답에서의 Supported Rates IE, extended supported Rates IE, 및/또는 ERP IE에 있음 |
| Country | 존재함/존재하지 않음 | 길이가 6 내지 7 옥테트일 수 있다. | STA가 위치해 있는 규제 영역(regulatory domain)을 식별하는 데 그리고 그 규제 영역에서의 동작을 위해 그의 PHY를 구성하는 데 필요한 정보 | 비콘/프로브 응답에 있음 |
| EDCAParameterSet | 존재함/존재하지 않음 | 길이가 20 옥테트일 수 있다. | BSS에서 사용될 초기 EDCA(enhanced distributed channel access, 향상된 분산 채널 액세스) 파라미터 세트 값들 | 비콘/프로브 응답에 있음 |
| DSERegisteredLocation | 존재함/존재하지 않음 | 길이가 22 옥테트일 수 있다. | DSE(data service element, 데이터 서비스 요소) 등록 위치(Registered Location) 요소에 대한 정보 | 비콘/프로브 응답에 있음 |
| High Throughput(HT) Capabilities | 존재함/존재하지 않음 | 길이가 28 옥테트일 수 있다. | BSS에 대해 광고될 HT 능력 | 비콘/프로브 응답에 있음 |
| HT Operation | 존재함/존재하지 않음 | 길이가 24 옥테트일 수 있다. | BSS에 대해 광고될 부가의 HT 능력 | 비콘/프로브 응답에 있음 |
| BSSMembershipSelectorSet | 존재함/존재하지 않음 | 정수들의 세트: 세트의 각각의 구성원에 대해 표 8 내지 표 55로부터의 값 | 이 BSS에 가입하기 위해 모든 STA들에 의해 지원되어야 하는 특징들의 세트를 나타내는 BSS 멤버쉽 선택자들 BSS를 생성하고 있는 STA는 세트에 의해 표현되는 특징들 각각을 지원할 수 있어야 한다. | 비콘/프로브 응답에서 Supported rate IE에 하나의 값 설정으로서 포함됨 |

| | | | | |
|---|---|---|---|---|
| BSSBasicMCSSet | 존재함/존재하지 않음 | 정수들의 세트: 각각이 0부터 76까지의 범위에 있는 MAC 인덱스 값을 나타냄 | 이 BSS에 가입하기 위해 모든 HT STA들에 의해 지원되어야 하는 MCS(modulation and coding scheme, 변조 및 코딩 방식) 값들의 세트 BSS를 생성하고 있는 STA는 세트에 열거되어 있는 MCS 값들 각각에서 수신하고 전송할 수 있어야 한다. | 비콘/프로브 응답에서 HT operation IE에 하나의 서브필드로서 포함됨 |
| HTOperational MCSSet | 존재함/존재하지 않음 | 정수들의 세트: 각각이 0부터 76까지의 범위에 있는 MAC 인덱스 값을 나타냄 | BSS 내에서의 통신을 위해 STA가 사용하고자 하는 MCS 값들의 세트 STA는 세트에 열거되어 있는 데이터 레이트들 각각에서 수신할 수 있어야 한다. 이 세트는 BSSBasicMCSSet 파라미터에 포함되어 있는 MCS 값들의 수퍼셋이다. | 비콘/프로브 응답에서 HT capability IE에 하나의 서브필드로서 포함됨 |
| Extended Capabilities | 존재함/존재하지 않음 | 길이가 가변적일 수 있다. | MAC 엔터티에 의해 지원되는 Extended Capabilities 요소 내에 파라미터들을 명시한다. | 비콘/프로브 응답에 있음 |
| 20/40 BSS Coexistence | 존재함/존재하지 않음 | 길이가 3 옥테트일 수 있다. | MAC 엔터티에 의해 나타내어지는 20/40 BSS Coexistence 요소 내에 파라미터들을 명시한다. | 비콘/프로브 응답에 있음 |
| Overlapping BSS Scan Parameters | 존재함/존재하지 않음 | 길이가 16 옥테트일 수 있다. | MAC 엔터티에 의해 나타내어지는 Overlapping BSS Scan Parameters 요소 내에 파라미터들을 명시한다. | 비콘/프로브 응답에 있음 |
| MultipleBSSID | 존재함/존재하지 않음 | 길이가 가변적일 수 있다. | AP가 2개 이상의 구성원들을 갖는 Multiple BSSID Set의 구성원일 때 다수의 BSSID 정보를 명시한다. | 비콘/프로브 응답에 있음 |
| InterworkingInfo | 존재함/존재하지 않음 | 길이가 3, 5, 9 또는 11 옥테트일 수 있다. | STA의 연동 능력을 명시한다. | 비콘/프로브 응답에 있음 |
| AdvertismentProtocolInfo | 존재함/존재하지 않음 | 0 내지 255 | BSS들에서 사용될 0개 이상의 광고 프로토콜들 및 광고 제어를 식별해준다. | 비콘/프로브 응답에 있음 |
| RoamingConsortium Info | 존재함/존재하지 않음 | 길이가 가변적일 수 있다. | AP에 대해 인증하는데 사용될 수 있는 보안 자격 증명들을 갖는 SSP들(subscription service providers, 가입 서비스 제공자들)에 대한 식별 정보를 명시한다. | 비콘/프로브 응답에 있음 |

| | | | | |
|---|---|---|---|---|
| Power Constraint | 존재함/존재하지 않음 | 길이가 3 옥테트일 수 있다. | STA가 현재의 채널에서의 로컬 최대 전송 전력을 결정할 수 있게 하는 데 필요한 정보를 포함한다. | 비콘/프로브 응답에 있음 |
| RSN | 존재함/존재하지 않음 | 길이가 최대 255 옥테트일 수 있다. | 인증 및 짝 암호 스위트 선택자들(pairwise cipher suite selectors), 단일의 그룹 데이터 암호 스위트 선택자, RSN Capabilities 필드, PMKID(PMK identifier, PMK 식별자) 카운트, PMKID 목록, 및 단일의 그룹 관리 암호 스위트 선택자를 포함한다. | 비콘/프로브 응답에 있음 |
| AP Channel Report | 존재함/존재하지 않음 | 길이가 가변적일 수 있다. | STA가 AP를 찾아낼 가능성이 있는 채널들의 목록을 포함한다. | 비콘/프로브 응답에 있음 |
| Supported Regulatory Classes | 존재함/존재하지 않음 | 길이가 2 내지 253 옥테트일 수 있다. | 국가 내에서 동작할 수 있는 동작 클래스들을 광고한다. | 비콘/프로브 응답에 있음 |
| VendorSpecificInfo | 존재함/존재하지 않음 | 길이가 가변적일 수 있다. | 벤더 관련 정보를 포함한다. | 비콘/프로브 응답에 있음 |

[0173] 상기한 예시적인 BSS/AP 구성 파라미터 세트는 BSSID(예를 들어, AP의 6-바이트 MAC 주소)에 의해 식별되는 BSS/AP에 따른 것이다.

[0174] 표 4에 나타낸 바와 같이, AP 구성 파라미터 세트에서의 각각의 파라미터는 파라미터의 값이 특정의 구성 인스턴스(configuration instance)에 존재하는지 여부를 나타내기 위해 존재-표시자(present-indicator)를 가진다. 구성 인스턴스는 구성 표시자라고 지칭될 수 있다. 이것은 구성 세트 내의 파라미터들의 서브셋이 특정의 PHY 모드의 사용 및/또는 어떤 선택적인 시스템 특징들 및 기능들(예를 들어, QoS 지원, 연동 서비스 등)의 선택에 의해 특정의 BSS/AP 동작 모드를 명시할 수 있게 할 것이다.

[0175] 액세스 네트워크 구성 파라미터 세트는 STA들의 링크 설정에 관련되어 있을 수 있는 BSS/AP의 배후에 있는 액세스 네트워크의 정적 또는 준정적 동작 파라미터들 또는 기술자들을 포함할 수 있다. 이와 유사하게, 링크 설정 프로세스를 가속화시키기 위해 액세스 네트워크 구성 정보를 사전 획득된 지식으로서 사용하기 위해, 액세스 네트워크 구성 파라미터들을 선택하기 위해 다음과 같은 기본적인 기준들이 적용될 수 있다: (a) 액세스 네트워크 서비스들, 능력들, 속성들, 및/또는 기능들을 명시하기 위해 사용될 수 있는 파라미터들, 예를 들어, 액세스 네트워크 질의 프로토콜(ANQP/GAS)과 같은 액세스 네트워크 발견 메시지들에서 사용되는 그 파라미터들; (b) 시간의 경과에 따라 값들을 동적으로 변화시키지 않을 수 있는, 예를 들어, 몇 시간, 며칠, 심지어 몇 달 동안 동일한 값들을 유지하는 파라미터들; 및/또는 (c) 링크 설정에 관련이 있을 수 있는 파라미터들.

[0176] 이상의 선택 기준들에 기초하여, 이하의 표 5는 액세스 네트워크 구성 파라미터 세트의 한 예를 제공한다.

*표 5*

[0177] 액세스 네트워크 구성 파라미터 세트의 한 예

| 파라미터 이름 | 존재 표시자 | 설명 |
|---|---|---|
| Venue Name information | 존재함/존재하지 않음 | BSS와 연관되어 있는 0개 이상의 장소 이름들(venue names)을 제공한다. |

| | | |
|---|---|---|
| Emergency Call Number information | 존재함/존재하지 않음 | STA의 지리적 위치에서 사용되는, PSAP(public safety answering point, 공공 안전 대응 센터)에 의해 보내지는 것과 같은, 긴급 전화 번호들의 목록을 비상 응답기(emergency responder)에 제공한다. |
| Network Authentication Type | 존재함/존재하지 않음 | 인증 유형들의 목록을 제공한다. |
| Roaming Consortium | 존재함/존재하지 않음 | 이 AP를 통해 액세스할 수 있는 네트워크들을 갖는 로밍 컨소시엄(Roaming Consortium) 및/또는 SSP들에 관한 정보의 목록을 제공한다. |
| IP Address Type Availability | 존재함/존재하지 않음 | 성공적인 접속 후에 STA에 할당될 수 있을 IP 주소 버전 및 유형의 이용가능성에 관한 정보를 STA에 제공한다. |
| NAI Realm | 존재함/존재하지 않음 | 이 AP를 통해 액세스할 수 있는 네트워크들 또는 서비스들을 갖는 SSP들 또는 다른 엔터티들에 대응하는 NAI(network access identifier, 네트워크 액세스 식별자) 영역들의 목록을 제공하고; 선택적으로 각각의 NAI 영역에 대해, 그 NAI 영역이 인증을 위해 사용하는 하나 이상의 EAP 방법 서브필드들의 목록이 포함되어 있다. |
| 3GPP Cellular Network | 존재함/존재하지 않음 | 3GPP 비AP STA가 3GPP 네트워크들에 액세스하기 위해 AP를 선택하는 것을 돕기 위해 네트워크 광고 정보(예컨대, 네트워크 코드들 및 국가 코드들)와 같은 셀룰러 정보를 포함한다. |
| AP Geospatial Location | 존재함/존재하지 않음 | AP의 위치를 위도, 경도, 고도, 및 선택적인 방위각 정보를 포함하는 LCI(Location Configuration Information, 위치 구성 정보) 형식으로 제공한다. |
| AP Civic Location | 존재함/존재하지 않음 | 주소(Civic) 형식으로 AP의 위치를 제공한다. |
| AP Location Public Identifier URI | 존재함/존재하지 않음 | AP의 위치 정보에 대한 간접 참조(indirect reference)를 제공한다. |
| Domain Name | 존재함/존재하지 않음 | IEEE 802.11 액세스 네트워크를 운영하는 엔터티의 하나 이상의 도메인 이름들의 목록을 제공한다. |
| Emergency Alert Identifier URI | 존재함/존재하지 않음 | EAS 메시지 검색을 위한 URI(Uniform Resource Identifier, 통합 자원 식별자)를 제공한다. |
| Tunneled Direct Link Setup (TDLS) capability | 존재함/존재하지 않음 | 피어 STA의 TDLS 능력을 발견하기 위해 STA에 의해 사용될 정보를 포함한다. |
| Emergency NAI | 존재함/존재하지 않음 | 긴급 액세스 요청을 나타내기 위해 그의 ID(identity)로서 STA에 의해 사용될 수 있는 긴급 문자열(emergency string)을 포함한다. |
| Neighbor Report | 존재함/존재하지 않음 | 이웃하는 AP들에 관한 0개 이상의 이웃 보고들을 제공한다. |
| vendor-specific | 존재함/존재하지 않음 | 액세스 네트워크에 관한 벤더 관련 정보를 포함한다. |

[0178] 이와 유사하게, 이상의 액세스 네트워크 구성 파라미터 세트는 BSS/AP에 따른 것일 수 있고, 액세스 네트워크는 STA가 BSS/AP의 무선 LAN을 통해 연결할 수 있는 네트워크일 수 있다. 또한, 표 5에 나타낸 바와 같이, 액세스 네트워크 구성 파라미터 세트 내의 각각의 파라미터에 대해, 존재-표시자는 파라미터의 값이 특정의 구성 인스턴스에 존재하는지 여부를 나타내기 위해 사용될 수 있고, 따라서 구성 파라미터들의 서브셋이 선택된 선택적인 특징들 및 기능들(예를 들어, 긴급 경보 서비스 등)을 갖는 특정의 네트워크 동작을 명시할 수 있다.

[0179] 개별적인 AP 및 네트워크 구성 파라미터 세트들을 정의하는 것에 대한 대안으로서, AP 및 액세스 네트워크 둘 다의 동작 설정들 및 서비스들을 명시하기 위해 결합된 단일의 AP/네트워크 구성 파라미터 세트가 정의될 수 있다. 결합된 단일의 AP/네트워크 구성 파라미터는 BSS/AP 및 액세스 네트워크 둘 다에 대한 동작 파라미터들/기술자들을 포함할 수 있다.

[0180] 결합된 AP/네트워크 구성 파라미터 세트의 선택 기준들은 AP 구성 파라미터 세트 선택 기준들 및 액세스 네트워크 구성 선택 기준들의 조합일 수 있다. 그에 부가하여, 표 4 및 표 5에 있는 2개의 파라미터 세트들은 결합된 AP/네트워크 구성 파라미터 세트의 한 예를 제공하기 위해 결합될 수 있다.

[0181] 구성 변경 횟수를 갖는 시스템 구성 인스턴스가 식별될 수 있다. 시스템 구성 인스턴스는 구성 파라미터 세트들 각각에 할당된 특정의 값들을 갖는 구성 파라미터 세트를 참조할 수 있다. 구성 파라미터들은 대응하는 시스템 동작 모드를 명시하는 데 사용될 수 있다. 구성 파라미터 세트가 선택적인 특징들 또는 기능들을 갖는 시스템에 대해 정의될 수 있고 구성 인스턴스가 유효한 값들을 갖는 구성 파라미터들의 서브셋을 포함할 수 있는 경우, 나머지 파라미터들은 "존재하지 않음"으로서 표시될 수 있다.

[0182] 구성 인스턴스에 대한 임의의 변경들의 결과, 새로운 구성 인스턴스, 예를 들어, 파라미터 값 변경, 할당된 유효한 값으로 "존재하지 않음" 파라미터가 "존재함"으로 변경됨, 또는 "존재함" 파라미터가 "존재하지 않음"으로 변경됨 등이 얻어질 수 있다. 구성 인스턴스가 CCC(Configuration Change Count, 구성 변경 횟수), 또는 CSN(Configuration Sequence Number, 구성 시퀀스 번호)라고도 하는 그의 버전 번호에 의해 식별될 수 있다. CCC는 구성 인스턴스가 변할 때마다 값이 변할 수 있는 정수 변수일 수 있다. CCC는 사전 정의된 기능에 기초하여 변화될 수 있다. 하나의 예는 구성 인스턴스가 변할 때마다 CCC가 1만큼 증가하고 그의 최대 값에 도달하면 0으로 랩어라운드되는 것일 수 있다.

[0183] BSS/AP 구성은 BSSID(예를 들어, AP의 MAC 주소)에 의해 식별될 수 있는 BSS/AP에 따라 정의될 수 있다. AP-CCC(AP Configuration Change Count, AP 구성 변경 횟수)는 AP 구성의 인스턴스를 식별하는 데 사용될 수 있다. 그리고/또는 BSSID, 구성 유형, 및/또는 AP-CCC의 조합은, 예를 들어, 주어진 AP의 구성 인스턴스를 식별하는 데 사용될 수 있고, 구성 유형은 정의되고 사용될 수 있는 다수의 구성들(예를 들어, BSS/AP 구성, 액세스 네트워크 구성 등) 중에서 특정의 구성을 나타낼 수 있다.

[0184] 이와 유사하게, AN-CCC(Access Network Configuration Change Count, 액세스 네트워크 구성 변경 횟수)와 같은 정수 변수가 액세스 네트워크 구성 인스턴스의 버전 번호를 식별하는 데 사용될 수 있다. BSSID, 구성 유형, 및/또는 AN-CCC의 조합은 AP를 통해 액세스 네트워크의 구성 인스턴스를 식별하는 데 사용될 수 있다.

[0185] 결합된 AP/네트워크 구성이 사용되는 경우, AP/AN-CCC(AP/Access Network Configuration Change Count, AP/액세스 네트워크 구성 변경 횟수)와 같은 정수 변수가 결합된 구성 인스턴스의 버전 번호를 식별하는 데 사용될 수 있다. 예를 들어, BSSID, 구성 유형, 및/또는 AP/AN-CCC의 조합은 AP를 통해 AP 및 액세스 네트워크의 구성 인스턴스를 식별하는 데 사용될 수 있다.

[0186] 시스템 정보 전달이 사전 정의된 시스템 구성 파라미터 세트들에 의해 수행될 수 있다. 무선 LAN 시스템들에서, 시스템 정보, 예를 들어, BSS/AP 동작 파라미터들, 액세스 네트워크 기능들, 및/또는 속성들 등이 초기 링크 설정을 위해 그리고 전력 절감 모드로부터 복귀할 때 링크 재시작(link resumption)을 위해 STA들로 전달될 수 있다. AP/네트워크와 STA들 사이의 시스템 정보 전달의 효율을 향상시키기 위해 시스템 구성 파라미터 세트들이 정의될 수 있다.

[0187] 시스템 구성들이 효율적인 시스템 통신들을 용이하게 하기 위해 사용될 때, AP/네트워크 및 STA들이 시스템 구성 파라미터 세트들의 정의들을 알고 있을 수 있다. 이러한 요구사항을 충족시키는 하나의 방법은 구성 파라미터 세트들의 정의들을 표준 단체들(예를 들어, IEEE 802)을 통해 표준화하는 것일 수 있다. 다른 대안으로서, 시스템 구성 파라미터 세트들의 정의들은, 구성이 사용될 수 있기 전에, 먼저 무선 링크 및/또는 유선 링크들을 통해 AP/네트워크와 STA들 사이에서 전달될 수 있다.

[0188] 사전 정의된 시스템 구성 파라미터 세트들은 AP/네트워크 및 STA들에서 사용될 수 있다. 이하의 예들은 AP/네트워크가 STA들과 시스템 정보를 주고 받기 위해 어떻게 사전 정의된 시스템 파라미터 세트들의 사용을 지원할 수 있는지를 요약한 것이다.

[0189] 제1 예에서, 각각의 정의된/사용된 시스템 구성 파라미터 세트에 대해, AP는 구성 인스턴스, 및 구성 인스턴스가 변할 때마다 구성 변경 횟수를 갱신하는 것을 비롯하여, 그의 대응하는 CCC(예를 들어, AP-CCC, AN-CCC, 및/또는 AP/AN-CCC)를 유지할 수 있다.

[0190] 제2 예에서, AP는, 사전 정의된 BSS/AP 구성 파라미터 세트에 기초하여, AP 시스템 정보를 제공할 수 있다. 이 예는 전체 BSS/AP 구성 인스턴스를 그의 대응하는 AP-CCC와 함께, 예를 들어, 비콘 프레임 및/또는 프로브 응답 프레임에서 제공하는 것을 포함할 수 있다. 다른 대안으로서, AP는 AP-CCC를 통해서만, 예를 들어, FILS 발견 프레임, 짧은 비콘 프레임 등에서 AP 시스템 정보를 제공할 수 있다.

[0191] 제3 예에서, AP는, 사전 정의된 액세스 네트워크 구성 파라미터 세트에 기초하여, 액세스 네트워크 시스템 정보를 제공할 수 있다. 예를 들어, AP는 전체 액세스 네트워크 구성 인스턴스를 그의 대응하는 AN-CCC와 함께, 예를 들어, GAS/ANQP 프레임들에서 제공할 수 있다. 다른 대안으로서, AP는 AN-CCC를 통해서만, 예를 들어, 비콘, 프로브 응답, FILS 발견, 및/또는 짧은 비콘 프레임들에서 액세스 네트워크 정보를 제공할 수 있다.

[0192] 제4 예에서, AP는, 사전 정의된 결합된 AP/네트워크 구성 파라미터 세트에 기초하여, AP/네트워크 시스템 정보를 제공할 수 있다. 예를 들어, AP는 전체 AP/네트워크 구성 인스턴스를 그의 대응하는 AP/AN-CCC와 함께, 예를 들어, 비콘 프레임, 프로브 응답 프레임, 및/또는 GAP/ANQP 프레임들에서 제공할 수 있다. 다른 대안으로서, AP는 AP/AN-CCC를 통해서만, 예를 들어, FILS 발견 프레임, 짧은 비콘 프레임 등에서 AP/네트워크 정보를 제공할 수 있다.

[0193] 도 16은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 한 예시적인 방법(1600)의 도면이다. 도 16을 참조하면, AP는 시스템 구성 식별자, 예를 들어, AP가 가지고 있는 것과 일치할 수 있는 BSSID, 구성 유형, 및/또는 CCC의 조합을 포함하는 프로브 요청을 수신(1610)할 수 있다. 수신된 시스템 구성 식별자가 AP의 시스템 구성 식별자와 일치하는 경우(1620), AP는 감소된 프로브 응답을 전송(1630)할 수 있다. 감소된 프로브 응답은 한 세트의 프로브 구성 파라미터들 각각이 응답 프레임에 개별적으로 제시되어 있지 않을 수 있는 응답 프레임을 말하는 것일 수 있다. 그 대신에, 프로브 요청 프레임에서와 동일한 CCC 값이 구성 파라미터 세트를 표현하는 데 사용되어, 프로브 요청 송신자 STA가 유효한 구성 인스턴스를 가진다는 것을 나타낼 수 있다. 수신된 시스템 구성 식별자가 AP의 시스템 구성 식별자와 일치하지 않는 경우(1620), AP는 갱신된 구성 파라미터 값들의 세트 및 대응하는 구성 인스턴스 식별자들을 갖는 전체 프로브 응답을 전송(1640)하거나, 부분적으로 감소된 프로브 응답을 전송할 수 있고, 부분적으로 감소된 프로브 응답은 전체 구성 인스턴스를 포함하지 않을 수 있는 프로브 응답 프레임을 말하는 것일 수 있다. 그 대신에, 부분적으로 감소된 프로브 응답은 새로운 구성 인스턴스 식별자 및 구성 파라미터들의 서브셋(예를 들어, 새로운 값들을 갖는 그 구성 파라미터들)을 포함할 수 있다. 환언하면, 이는 프로브 요청 프레임에서 제공된 구성 인스턴스 식별자에 의해 식별되는 구성 인스턴스와 상이한 값들을 포함할 수 있다.

[0194] 이 예는 AP가 그의 현재 구성 인스턴스와 프로브 요청 프레임에서 제공된 구성 인스턴스 식별자에 의해 식별되는 것 간의 차이를 식별할 수 있을 것 - 이는 이전의 구성 인스턴스들의 몇개의 사본들 및 현재의 구성 인스턴스들과 비교한 각자의 변화들을 저장하는 것, 및/또는 구성 인스턴스들을 파라미터들의 서브셋들(예를 들어, 서브셋 1, 서브셋 2, 서브셋 3 및 서브셋 4)로 나누는 것에 의해 달성될 수 있음 - 을 필요로 할 수 있다. CCC는 4개의 부분들로 나누어질 수 있고, 예를 들어, 처음 4 비트는 서브셋 1과 연관되어 있고; 그리고/또는 마지막 4 비트는 서브셋 4와 연관되어 있다. 프로브 요청에 있는 STA로부터의 CCC를 검사함으로써, AP는 변경된 파라미터 서브셋들을 발견할 수 있다.

[0195] STA는, 시스템 정보를 획득하기 위해, 사전 정의된 시스템 구성 파라미터 세트들의 형태로 되어 있는 BSS 및/또는 네트워크에 관한 사전 획득된 지식을 추적하고 사용할 수 있다. 예를 들어, STA는, 구성 지식 데이터베이스를 사용함으로써, BSS/AP 및/또는 액세스 네트워크 시스템 정보에 관한 그의 획득된 지식을 추적할 수 있다. STA가 그에 관한 정보를 획득한 각각의 BSS/AP에 대해, BSSID, SSID, 위치, 마지막으로 갱신된 시각, 구성 파라미터 세트들 및/또는 대응하는 구성 변경 횟수들, 예를 들어, BSS/AP 구성, 액세스 네트워크 구성, 및/또는 결합된 AP/네트워크 구성 등, 및 그의 존재-표시자에 의해 나타내어지는 바와 같이 존재할 수 있는 각각의 구성 파라미터에 대한 값들을 포함할 수 있는 항목이 데이터베이스에서 있을 수 있다. 구성 데이터베이스에서의 항목들은 내용에 대한 고속 액세스를 용이하게 하기 위해 조직화될 수 있다(예를 들어, BSS/AP의 STA 사용에 기초

하여 정렬되거나, BSS/AP들의 위치들에 기초하여 정렬되거나, STA의 물리적 이동 경로에 기초하여 정렬되거나 기타 등등임). 구성 데이터베이스에서의 항목은, STA가 새로운 BSS/AP에 관한 지식을 획득할 때, 초기화될 수 있고, STA가 BSS/AP에 관한 갱신, 예를 들어, 새로운 CCC 값을 갖는 구성 인스턴스를 수신할 수 있을 때마다 항목이 유지될 수 있다. STA는 BSS/AP와의 무선 링크 또는 다른 BSS/AP와의 무선 링크, 또는 셀룰러 네트워크에서의 무선 링크, 또는 유선 링크 등을 통해 BSS/AP 구성 및/또는 액세스 네트워크 구성의 지식을 획득할 수 있다.

[0196] 도 17은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 다른 예시적인 방법(1700)의 도면이다. 예를 들어, STA가 전체 구성 인스턴스 및 그의 대응하는 CCC를, 예를 들어, 비콘 프레임들, 프로브 응답 프레임들, 및/또는 GAS/ANQP 프레임들에서 수신(1710)할 때, STA는 그의 획득된 구성 지식 데이터베이스에 항목이 있는지를 검사(1720)할 수 있다. 그의 획득된 구성 지식 데이터베이스에 항목이 없는 경우, STA는 새로운 항목을 생성(1730)할 수 있다. 그의 획득된 구성 지식 데이터베이스에 항목이 있는 경우, STA는 새로 수신된 구성 변경 횟수가 구성 데이터베이스에 있는 것과 일치하는지를 검사(1740)할 수 있다. 일치하는 경우, 구성 데이터베이스에 어떤 갱신도 필요하지 않다(1750). 일치하지 않는 경우, STA는 새로 수신된 구성 인스턴스및 그의 대응하는 CCC 값으로 데이터베이스를 갱신(1760)할 수 있다.

[0197] 도 18은 사전 정의된 시스템 파라미터 세트들의 사용을 지원하는 다른 예시적인 방법(1800)의 도면이다. 예를 들어, STA는 전체 구성 인스턴스 정보 없이 구성 인스턴스 식별자를, 예를 들어, FILS 발견 프레임들, 짧은 비콘 프레임들에서, 또는 감소된 프로브 응답 프레임들에서 수신(1810)할 수 있다. STA는 수신된 구성 인스턴스 식별자에서의 CCC 값이 저장된 값과 일치하는지를 판정(1820)할 수 있다. 새로 수신된 구성 인스턴스 식별자에서의 CCC 값이 구성 데이터베이스에 저장된 값과 일치하지 않는 경우, STA는 대응하는 구성 인스턴스에 데이터베이스에서 "폐기됨"으로서 표시(1830)할 수 있다. 새로 수신된 구성 인스턴스 식별자에서의 CCC 값이 구성 데이터베이스에 저장된 값과 일치하는 경우, STA는 구성 데이터베이스에 대해 어떤 변경도 행하지 않을 수 있다(1840).

[0198] 도 19는 STA가, AP 및/또는 네트워크의 최신의 시스템 정보를 획득했는지를 판정하기 위해, 전체 구성 인스턴스 정보 없이 수신된 구성 인스턴스 식별자 정보를 사용할 수 있는 한 예시적인 방법(1900)의 도면이다. 이 예는 시스템 정보 전달 효율을 향상시키는 데 사용될 수 있다. 예를 들어, STA는 스캔을 시작(1910)할 수 있다. STA는 능동 또는 수동 스캔을 수행할 수 있다. STA는 전체 구성 인스턴스 정보 없이 BSS/AP 구성 변경 횟수 값을, 예를 들어, FILS 발견 프레임들, 짧은 비콘 프레임들에서, 또는 감소된 프로브 응답 프레임들에서 수신(1920)할 수 있다. STA는 구성 데이터베이스에 BSS/AP의 유효한 항목이 있는지를 판정(1930)할 수 있다. 구성 데이터베이스에 BSS/AP의 유효한 항목이 있는 경우, STA는 수신된 구성 변경 횟수 값이 구성 데이터베이스에 있는 것과 일치하는지를 판정(1940)할 수 있다. 수신된 AP-CCC가 데이터베이스에 있는 AP-CCC와 일치하는 경우, STA는 유효한 최신의 BSS/AP 시스템 정보를 가지고 있는 것으로 결론지을 수 있다. STA는 이어서, 비콘 프레임 또는 프로브 응답 프레임을 기다리지 않고, BSS/AP의 스캔 프로세스를 완료(1950)할 수 있다. 이 경우에, 데이터베이스에 있는 BSS/AP 구성 정보는 STA의 MLME가 MLME-SCAN.confirm 프리미티브에 스캔 보고를 작성하는 데 사용될 수 있고(1960), 또한 STA가 초기 링크 설정 프로세스에서의 다음 단계 동작(예를 들어, 접속)을 개시하는 데 사용될 수 있다. 구성 데이터베이스에 유효한 BSS/AP 항목이 없거나, 수신된 구성 변경 횟수 값이 데이터베이스에 있는 것과 일치하지 않는 경우, STA는 스캔을 계속(1970)할 수 있다.

[0199] 도 20은 STA가 사전 획득된 시스템 구성에 대한 구성 인스턴스 식별자 정보를 포함시킬 수 있는 한 예시적인 방법(2000)의 도면이다. 능동 스캔(2010) 동안, STA는 그의 사전 획득된 시스템 구성들에 대한 구성 인스턴스 식별자 정보를 포함하는 프로브 요청 프레임을 전송(2020)할 수 있고, 구성 인스턴스 식별자는 BSSID, 구성 유형, 및/또는 CCC의 조합일 수 있다. 프로브 요청 프레임에서 사용될 때, 구성 인스턴스 식별자(예를 들어, AP-구성 식별자)는 구성에서의 파라미터들을 나타낸다. 그러면, 그 구성 파라미터들은 각각의 프로브 요청 프레임 또는 감소된 프로브 요청 프레임에 더 이상 개별적으로 포함될 필요가 없다. 환언하면, 구성 인스턴스 식별자 정보의 사용은 STA가 감소된 프로브 요청 프레임을 사용할 수 있게 하고, 따라서 프로브 요청의 에어타임 점유율(airtime occupancy)이 감소될 수 있다.

[0200] STA가 응답을 수신(2030)할 때, STA는 수신된 응답이 전체, 부분, 또는 감소된 프로브 응답 프레임인지를 판정(2040)할 수 있다. STA가 구성 식별자 정보를 갖지만 전체 구성 인스턴스를 갖지 않는 감소된 프로브 응답 프레임(2045)을 수신할 때, STA는 앞서 기술된 방식으로 그의 사전 획득된 지식을 검색(2050)하기 위해 그의 구성 데이터베이스를 사용할 수 있다. STA가 부분 프로브 응답 프레임(2055)을 수신할 때, STA는 그에 따라 데이터베이스를 갱신(2060)할 수 있다. STA가 전체 프로브 응답 프레임(2065)을 수신할 때, STA는 수신된 응답에서의

CCC 값이 데이터베이스에 있는 것과 일치하는지를 판정(2070)할 수 있다. CCC 값이 일치하는 경우(2075), 데이터베이스에 어떤 갱신도 필요하지 않다(2080). CCC 값이 일치하지 않는 경우(2085), STA는 그에 따라 데이터베이스를 갱신(2060)할 수 있다.

[0201] 네트워크 발견 및 선택 동안, 예를 들어, GAS/ANQP를 사용하여, STA는 그의 사전 획득된 네트워크 구성 지식을 알려주기 위해 액세스 네트워크 구성 식별자 정보를 GAS 요청 프레임에 포함시킬 수 있다. 그에 부가하여, 구성 인스턴스 식별자 정보를 갖지만 전체 네트워크 구성 인스턴스를 갖지 않는 GAS 응답이 수신될 때, STA는 그의 사전 획득된 네트워크 구성 지식을 검색하기 위해 그의 구성 데이터베이스를 사용할 수 있다.

[0202] 또한 사전 획득된 구성 지식 데이터베이스가 어떻게 STA의 계층화된 프로토콜 아키텍처에서 관리될 수 있는지에 관한 다수의 대안들이 있을 수 있다. 예를 들어, 사전 획득된 구성 지식 데이터베이스는 MLME(MAC Layer Management Entity, MAC 계층 관리 엔터티), SME(Station Management Entity, 스테이션 관리 엔터티), 또는 무선 LAN 공중 인터페이스의 MAC/PHY보다 상위에 있는 연결 관리자 모듈 등에 의해 관리될 수 있다.

[0203] 사전 획득된 구성 지식 데이터베이스가 MLME에 의해 관리되지 않는 경우, 데이터베이스로부터의 어떤 정보(예를 들어, 구성 인스턴스 식별자)가 MLME와 데이터베이스를 관리하는 모듈(예를 들어, SME) 사이의 SAP들(service access points, 서비스 액세스 포인트들)에서 프리미티브들에 포함될 필요가 있을 수 있다.

[0204] 사전 획득된 구성 지식 데이터베이스가 MLME에 의해 관리되지 않는 경우(예를 들어, SME에 의해 관리되는 경우), 2개의 파라미터들이 프리미티브 MLME-Scan.request(예를 들어, ConfigurationType 및 APConfigurationChangeCount)에 포함될 수 있다. 한 예가 이하의 표 6에 나타내어져 있다.

*표 6*

[0205] MLME-Scan.request 프리미티브에 부가된 새로운 파라미터들의 한 예

| 이름 | 유형 | 유효 범위 | 설명 |
|---|---|---|---|
| APConfigurationType | 정수 | 0 ~ N-1 | STA가 마지막으로 획득한 AP/네트워크의 구성 유형 |
| APConfigurationChangeCount | 정수 | 0 ~ K-1 | STA가 마지막으로 획득한 AP/네트워크의 AP 구성 변경 횟수 |

[0206] 사전 획득된 구성 지식 데이터베이스가 MLME에 의해 관리되지 않는 경우(예를 들어, SME에 의해 관리되는 경우), FILS 발견 비콘, 짧은 비콘 또는 감소된 프로브 응답 프레임들로부터 구성 유형 및 AP-CCC만이 사용될 수 있는 경우를 가능하게 하기 위해, BSSDescriptionUsingConfigurationChangeCountSet 파라미터가 프리미티브 MLME-Scan.confirm에 포함될 수 있다. 한 예가 이하의 표 7에 나타내어져 있다.

*표 7*

[0207] MLME-Scan.confirm 프리미티브에 부가된 새로운 파라미터들의 한 예

| 이름 | 유형 | 유효 범위 | 설명 |
|---|---|---|---|
| BSSDescriptionUsingConfigurationChangeCountSet | BSSDescriptionUsingConfigurationChangeCount의 세트 | 해당 없음 | 구성 유형 및 AP-CCC로 표현된 스캔 요청의 결과를 알려주기 위해, BSSDescriptionUsingConfigurationChangeCountSet가 반환된다. 이는 BSSDescriptionUsingConfigurationChangeCount의 0개 이상의 인스턴스들을 포함하는 세트이다. AP-CCC가 사용되는 802.11 시스템들에 대해서만 존재한다. |

[0208] 각각의 BSSDescriptionUsingConfigurationChangeCount는 이하의 표 8에 나타내어져 있는 요소들 중 하나 이상

을 포함할 수 있다.

표 8

[0209] BSSDescriptionUsingConfigurationChangeCount의 한 예

| 이름 | 유형 | 유효 범위 | 설명 |
|---|---|---|---|
| SSID 또는 압축된 SSID | 옥테트 문자열 | SSID에 대해 0 내지 32 옥테트 또는 압축된 SSID에 대해 0 내지 4 옥테트 | 발견된 BSS의 SSID 또는 해싱된 SSID |
| 짧은 타임스탬프 | 정수 | 해당 없음 | 발견된 BSS로부터 수신된 프레임(프로브 응답/비콘)의 타임스탬프의 최하위 4 바이트 |
| 그 다음 전체 비콘까지의 시간 | 정수 | 해당 없음 | 수신된 짧은 비콘 프레임과 그 다음 전체 비콘 사이의 시간 |
| AP의 BSSID 또는 MAC 주소 | MAC 주소 | 6 바이트 | AP의 MAC 주소는 수신된 짧은 비콘 프레임에서의 SA(Source address, 소스 주소)로부터 획득된다. |
| 구성 유형 | 정수 | $Log_2$ N 비트 | 발견된 AP의 구성 유형 |
| AP-CCC | 정수 | $Log_2$ K 비트 | 발견된 AP의 AP 구성 변경 횟수 |

[0210] 또 다른 예에서, 위치 기반의 사전 획득된 지식을 사용한 고속 링크 설정이 사용될 수 있다. 위치 기반의 사전 획득된 지식은 STA가 일상에서의 집, 사무실, 회의실, 기차역, 지역 공항, 부모의 집, 또는 다른 가족 구성원의 집 등을 비롯한 빈번히 방문한 곳들과 같은 특정의 지리적 위치들에 대한 액세스가능한 및/또는 선호된 네트워크에 관해 알아낸 것을 말하는 것일 수 있다. 위치 기반의 액세스가능한/선호된 네트워크 지식은 네트워크 동작 모드에 관한 시스템 정보는 물론, STA와 네트워크 간의 보안 접속 정보를 포함할 수 있다. 빈번히 방문하는 곳에 들어갈 때, 이러한 위치 기반의 사전 획득된 액세스가능한/선호된 네트워크 지식은 링크 설정 프로세스를 가속화시키는 데 사용될 수 있다. 그에 부가하여, 이는 또한 액세스가능한 네트워크들 사이의 고속 전환들(예를 들어, 셀룰러로부터 WLAN으로의 오프로딩, 또는 WiFi로부터 셀룰러로의 전환)을 용이하게 하는 데 사용될 수 있다.

[0211] STA는 위치 기반의 선호된 네트워크 데이터베이스에서의 위치 기반의 사전 획득된 지식 - 위치 기반 네트워크 프로파일 또는 간단히 위치 프로파일이라고도 할 수 있음 - 을 추적할 수 있다. 데이터베이스에서의 위치는 지리적 위치 기술자들[예를 들어, 위도, 경도, 고도, 및 선택적인 방위각, 및/또는 주소(civic location) 설명들]에 의해 명시될 수 있다.

[0212] 데이터베이스에서의 각각의 위치에 대해, 하나 또는 다수의 액세스가능한 및/또는 선호된 네트워크들이 있을 수 있다. 액세스가능한/선호된 네트워크들 각각에 대해, 데이터베이스는 STA 사전 획득된 지식, 예를 들어, 네트워크 식별자, 네트워크 유형, 네트워크 구성 파라미터 세트들 및 값들, 및 STA와 네트워크 간의 보안 접속 정보 등을 기록할 수 있다.

[0213] 도 21은 위치 기반의 사전 획득된 지식에 의해 고속 링크 설정을 수행하는 한 예시적인 방법(2100)의 도면이다. 이 예에서, STA는 링크 설정을 시작(2110)하고 STA 위치가 이용가능한지를 판정(2120)할 수 있다. STA 위치가 이용가능하지 않은 경우(2130), STA는 정상 링크 설정 프로세스(2140)를 계속할 수 있다. STA 위치가 이용가능한 경우(2150), STA는 STA 위치 프로파일이 이용가능한지를 판정(2160)할 수 있다. STA 위치 프로파일이 이용가능한 경우(2170), STA는 최적화된 링크 설정(2180)을 계속할 수 있다. STA 위치 프로파일이 이용가능하지 않은 경우(2185), STA는 정상 링크 설정(2140)을 계속할 수 있다.

[0214] 위치 기반 네트워크 데이터베이스에서의 내용은 STA에 맞춰 구성되어 있을 수 있고 그리고/또는 STA에 의해 자체적으로 학습되고 유지될 수 있다. STA의 현재 위치의 정보가 이용가능한 경우, STA의 네트워크 관리 모듈(예를 들어, 네트워크 연결 관리자)은 그의 네트워크 동작들을 최적화(예를 들어, 고속 초기 링크 설정에 의한 셀룰러 네트워크로부터 WiFi 네트워크로의 오프로딩, 상이한 유형들의 트래픽을 배포하기 위해 제2 네트워크와의

부가의 연결을 설정하는 것, 및/또는 더 적합한 네트워크를 재선택하는 것 등)하기 위해 그의 위치 기반 네트워크 데이터베이스를 사용할 수 있다.

[0215] 이하의 예들은, 예를 들어, STA가, 예를 들어, 기존의 네트워크 연결 및/또는 내장된 위치 확인 유틸리티를 통해 그의 현재 위치를 알 때, WiFi 네트워크에서 링크 설정 프로세스를 가속화시키기 위해 위치 기반의 사전 획득된 지식을 사용할 수 있다.

[0216] 도 22는 그의 위치 기반 네트워크 데이터베이스에 액세스할 수 있는 STA가 주어진 위치에 대해 연결할 BSS를 정확하게 알고 있는 링크 설정 최적화를 위한 제1 예시적인 방법(2200)의 도면이다. 이 예에서, STA는 전형적인 802.11 링크 설정 절차에서 접속 단계 이전의 모든 단계들을 생략할 수 있다. STA는 정규의 접속 요청 프레임과 비슷한 어떤 부가 정보 항목들[예를 들어, AP/네트워크 동작 설정들에 관한 그의 지식(예를 들어, BSSID, 구성 유형, 및/또는 CCC의 조합을 갖는 구성 인스턴스 식별자를 사용함); 및/또는 AP/네트워크와의 보안 접속에 관한 그의 지식]을 갖는 접속 요청 프레임을 BSS/AP로 전송(2210)할 수 있다. STA는 BSS/AP로부터 응답이 수신되었는지를 판정(2220)할 수 있다.

[0217] STA가 사전 정의된 시간 구간 내에 응답을 수신하지 않는 경우(2225), BSS/AP는 이용가능하지 않을 수 있고, STA는 위치 기반 네트워크 데이터베이스를 사용하여 또는 보통의 스캔 프로세스를 통해 BSS/AP 재선택을 수행(2230)할 수 있다. 유의할 점은, 이 시나리오가 가능하지만, STA가 선호된 네트워크(홈 네트워크 또는 사무실 네트워크 등)가 액세스가능하다는 것을 알고 있다는 가정을 포함할 수 있기 때문에 더욱 드문 경우라는 것이다.

[0218] STA가 STA의 사전 획득된 지식이, 예를 들어, 일치하는 구성 변경 횟수의 포함과 관련하여 유효하다는 것을 확인해주는 응답을 AP로부터 수신(2235)하는 경우, STA는, 그의 사전 획득된 지식 데이터베이스에 대한 어떤 유지관리 동작도 없이, 링크 설정 절차에서의 그 다음 단계로 진행할 수 있다. 이 예는 수신된 응답이 또한 보통의 접속 응답 내용 항목들을 포함할 수 있는 것으로 가정할 수 있다.

[0219] STA가, 보통의 접속 응답 내용 항목들에 부가하여, 예를 들어, 상이한 구성 변경 횟수 및 대응하는 구성 인스턴스 정보의 포함과 관련하여 STA의 사전 획득된 지식이 하나 이상의 갱신을 필요로 한다(2240)는 것을 나타내는 응답을 AP로부터 수신하는 경우, 이 예에서, STA는 AP/네트워크에 관한 그의 사전 획득된 지식에 대해 갱신을 수행(2250)하고, 링크 설정 절차에서의 그 다음 단계로 진행(2260)하기 전에, 그의 데이터베이스에 대해 대응하는 갱신을 수행할 수 있다. STA가 STA의 사전 획득된 지식이 갱신을 필요로 하지 않는다는 것을 나타내는 응답을 AP로부터 수신하는 경우, STA는 링크 설정 절차를 계속(2260)할 수 있다.

[0220] STA는 보안 설정 프로세스를 최적화하기 위해 AP/네트워크와의 사전 획득된 보안 접속 정보를 사용할 수 있다. 유의할 점은, 이상의 최적화들에 의해, 위치 기반의 사전 획득된 지식을 사용함으로써, 링크 설정 절차가 하나의 시간이 걸리는 단계(예를 들어, AP/네트워크 발견)를 완전히 생략할 수 있고 또한 다른 시간이 걸리는 단계(예를 들어, 보안 설정)에 대한 시간을 상당히 감소시킬 수 있다는 것이다. 이 절차는, STA와 AP/네트워크 사이의 IP 연결 설정을 완료하기 위해, 단지 STA와 AP 사이에서의 약 5번의 메시지 라운드들(예를 들어, 1번은 접속을 위한 것이고, 2번은 보안을 위한 것이며, 2번은 IP 주소 할당을 위한 것임), 및 AP와 DHCP 서버 사이에서의 2번의 메시지 라운드들을 필요로 할 수 있다. 그에 따라, 이 절차가 앞서 주어진 링크 설정 단계들의 동일한 시간 값들을 사용하는 경우, 링크 설정 시간이 약 20 ms로 감소될 수 있다.

[0221] 그의 위치 기반 네트워크 데이터베이스에의 액세스를 갖는 제2 예에서, STA는 주어진 위치에 있는 선호된 BSS/AP(들)에 관한 지식을 가질 수 있지만, 연결을 설정하기 전에 추가적인 확인을 필요로 할 수 있다. 이 예에서, STA는 먼저 AP/네트워크에 관한 유효한 정보를 가지고 있는지를 검증할 수 있고, 이어서 링크 설정 프로세스를 완료하기 위해 이전의 예에서 주어진 단계들을 사용할 수 있다. 이하의 최적화들은 AP/네트워크 정보 검증을 가속화시키기 위해 고려될 수 있다.

[0222] STA는 감소된 프로브 요청/응답 프레임들 및/또는 감소된 GAS 요청/응답 프레임들을 사용할 수 있고, "감소된"은, 각각의 파라미터들을 개별적으로 포함하는 대신에, 그 프레임들에서의 파라미터들의 세트를 표현하는 구성 식별자 정보(예를 들어, BSSID, 구성 유형, 및/또는 CCC의 조합)를 말하는 것일 수 있다. STA가 데이터베이스에 있는 정보와 일치하는 구성 식별자 정보를 갖는 응답 프레임을 수신할 때, STA는 AP/네트워크에 관한 그의 데이터를 검증할 수 있고, 링크 설정 프로세스에서의 그 다음 단계로 진행할 수 있다.

[0223] 그에 부가하여, STA가 전체 구성 인스턴스 및 상이한 CCC 값을 갖는 응답 프레임을 수신하는 경우, STA는 대응하는 시스템 정보의 새로운 갱신을 실제로 획득했을 수 있고, 따라서 역시 그 다음 단계로 진행할 수 있다. 게다가, 감소된 프로브 요청/응답 프레임들을 전송하는 다수의 방식들이 있을 수 있고, 예를 들어, STA는 유니캐

스트 감소된 프로브 요청을 전송할 수 있고, 구성 인스턴스 식별자 정보가 MAC 프레임 헤더에서 BSSID에 의해 제공될 수 있고, 구성 유형 및 CCC 값의 하나 또는 다수의 조합들이 프레임 보디에서 제공된다. 유니캐스트 감소된 프로브 요청의 경우, STA는 하나 또는 다수의 사전 정의된 시스템 구성 파라미터 세트들로 하나의 BSS/AP에 관한 그의 사전 획득된 지식 및 그의 접속된 액세스 네트워크를 검증할 수 있고; STA는 브로드캐스트 감소된 프로브 요청을 전송할 수 있으며, 각각이 BSSID, 구성 유형, 및/또는 CCC의 조합을 갖는 다수의 구성 인스턴스 식별자들이 포함될 수 있다. 브로드캐스트 감소된 프로브 요청의 경우, STA는 동일한 커버리지 영역 내의 하나 또는 다수의 BSS들/AP들 및 그들의 접속된 네트워크들에 관한 그의 사전 획득된 지식을 검증할 수 있다. 브로드캐스트 감소된 프로브 요청을 수신한 후에, AP의 BSSID가 요청 프레임에서 제공되는 구성 인스턴스 식별자 정보에서의 BSSID들 중 하나인 경우, AP 및/또는 STA는 응답할 수 있고; AP 및/또는 STA는, 요청 프레임에서 제공된 식별자들 중 하나와 일치하는 적어도 하나의 구성 인스턴스 식별자를 가지는 경우, 수신된 감소된 프로브 요청에 대해 감소된 프로브 응답 프레임으로 응답할 수 있고; 그의 구성 인스턴스의 BSSID 및 구성 유형이 요청 프레임에서 제공된 식별자들 중 하나에서의 대응하는 값들과 일치하지만 구성 변경 횟수가 일치하지 않는 경우, AP 및/또는 STA는 수신된 감소된 프로브 요청에 대해 전체 구성 인스턴스 및 그의 식별자를 갖는 정규의 프로브 응답 프레임으로 응답할 수 있다.

[0224] STA는 구성 인스턴스 식별자 정보, 예를 들어, (정규의 비콘 프레임과 비교하여) 더 빈번히 전송되는 더 작은 시스템 정보 공지 프레임(예를 들어, 짧은 비콘 프레임, 고속 비콘 프레임, 또는 FILS 발견 프레임 등)에서 제공된 BSSID, 구성 유형, 및/또는 CCC 값의 조합을 사용할 수 있다. 구성 인스턴스 식별자가 데이터베이스에서의 대응하는 구성 인스턴스 식별자와 일치하는 경우, 검증이 완료되고, STA는 링크 설정 프로세스에서의 그 다음 단계로 진행할 수 있다.

[0225] 유의할 점은, 이 경우에서의 링크 설정 시간이 AP/네트워크 정보를 검증하는 데 사용된 시간과 이전의 예의 시간의 합일 수 있다는 것이다. 능동 스캔을 사용하는 경우, 예를 들어, 감소된 프로브 요청/응답 프레임들을 사용하는 경우, 링크 설정 시간은 약 25 ms일 수 있다. (정규의 비콘 프레임과 비교하여) 더 빈번히 전송되는 더 작은 시스템 정보 공지 프레임들(예를 들어, 짧은 비콘 프레임, 또는 고속 비콘 프레임, 또는 FILS 발견 프레임 등)을 사용하는 경우, 링크 설정 시간은 약 20 ms + 이러한 프레임들의 간격일 수 있다.

[0226] 실시예들

[0227] 1. 장치로서,

[0228] 메시지를 수신하도록 구성되어 있는 수신기;

[0229] PMK(pairwise master key, 짝 마스터 키)를 발생시키도록 구성되어 있는 프로세서; 및

[0230] WLAN(wireless local area network, 무선 근거리 통신망)을 통해 IP(internet protocol, 인터넷 프로토콜) 주소 할당을 설정하라는 요청을 AP(access point, 액세스 포인트)로 전송하도록 구성되어 있는 송신기를 포함하고;

[0231] 수신기 및 송신기는 또한 PMK를 사용하여 WLAN을 통해 서버와 통신하도록 구성되어 있는 것인 장치.

[0232] 2. 실시예 1에 있어서, 메시지는 EAP(Extensible Authentication Protocol, 확장가능 인증 프로토콜) 절차가 성공적이라는 것을 나타내는 것인 장치.

[0233] 3. 실시예 1 또는 실시예 2에 있어서, 요청은 DHCP(dynamic host configuration protocol, 동적 호스트 구성 프로토콜)에 대한 요청인 장치.

[0234] 4. 실시예 1 내지 실시예 3 중 어느 한 실시예에 있어서, 서버는 AAA(authentication, authorization, and accounting, 인증, 권한 부여 및 계정 관리) 서버인 장치.

[0235] 5. 실시예 1 내지 실시예 4 중 어느 한 실시예에 있어서, 수신기 및 송신기는 또한 eANDSF(enhanced access network discovery and selection function, 향상된 액세스 네트워크 발견 및 선택 기능)를 포함하는 서버와 통신하도록 구성되어 있는 것인 장치.

[0236] 6. 실시예 1 내지 실시예 5 중 어느 한 실시예에 있어서, 수신기 및 송신기는 또한 OP(identity provider, ID 제공자) 기능을 포함하는 서버와 통신하도록 구성되어 있는 것인 장치.

[0237] 7. 실시예 1 내지 실시예 6 중 어느 한 실시예에 있어서, 프로세서는 STA-OP(station Identity Provider, 스테이션 ID 제공자) PSK(pre-shared key, 사전 공유 키)를 사용하여 PMK를 발생시키도록 구성되어 있는 것인 장치.

[0238] 8. 실시예 1 내지 실시예 7 중 어느 한 실시예에 있어서, 송신기 및 수신기는 또한 4-단계 핸드쉐이크 프로토콜(4-way handshake protocol)을 수행하도록 구성되어 있는 것인 장치.

[0239] 9. 실시예 8에 있어서, 4-단계 핸드쉐이크 프로토콜은 의사 난수 값(pseudo-random value)을 도출하기 위해 의사 난수 함수(pseudo-random function)를 사용하는 것인 장치.

[0240] 10. 실시예 9에 있어서, 의사 난수 값은 넌스(nonce)인 장치.

[0241] 11. 실시예 10에 있어서, 넌스는 PSK(pre-shared key)와 연관되어 있는 것인 장치.

[0242] 12. 실시예 1 내지 실시예 11 중 어느 한 실시예에 있어서, 수신기는 또한 제1 EAPOL[EAP(extensible authentication protocol) over LAN(local area network, 근거리 통신망)]-Key 프레임을 수신하도록 구성되어 있는 것인 장치.

[0243] 13. 실시예 12에 있어서, 송신기는 또한, 제1 EAPOL-Key 프레임에 응답하여, 제2 EAPOL-Key 프레임을 전송하도록 구성되어 있는 것인 장치.

[0244] 14. 실시예 12에 있어서, 제1 EAPOL-Key 프레임은 AP와 연관되어 있는 넌스를 포함하는 것인 장치.

[0245] 15. 실시예 14에 있어서, 제2 EAPOL-Key 프레임은 장치와 연관되어 있는 넌스를 포함하는 것인 장치.

[0246] 16. 실시예 13 내지 실시예 15 중 어느 한 실시예에 있어서, 수신기는 또한 제3 EAPOL-Key 프레임을 수신하도록 구성되어 있는 것인 장치.

[0247] 17. 실시예 16에 있어서, 송신기는 또한, 제3 EAPOL-Key 프레임에 응답하여, 제4 EAPOL-Key 프레임을 전송하도록 구성되어 있는 것인 장치.

[0248] 18. 실시예 1 내지 실시예 17 중 어느 한 실시예에 있어서, 송신기는 또한 WLAN 정보에 대한 요청을 서버로 전송하도록 구성되어 있는 것인 장치.

[0249] 19. 실시예 18에 있어서, WLAN 정보는 이용가능한 AP, SSID(service set identification, 서비스 세트 ID), 인증 방법, 또는 액세스 네트워크 파라미터를 포함하는 것인 장치.

[0250] 20. 실시예 18 또는 실시예 19에 있어서, 송신기는 또한, 요청된 WLAN 정보에 기초하여 스캔을 수행하는 일 없이, 프로브 요청 프레임(probe request frame)을 AP(access point)로 전송하도록 구성되어 있는 것인 장치.

[0251] 21. 실시예 20에 있어서, 스캔은 능동 스캔(active scan)인 장치.

[0252] 22. 실시예 20에 있어서, 스캔은 수동 스캔(passive scan)인 장치.

[0253] 23. 실시예 1 내지 실시예 22 중 어느 한 실시예에 있어서, 수신기는 또한 프로브 응답 프레임(probe response frame)을 수신하도록 구성되어 있는 것인 장치.

[0254] 24. 실시예 1 내지 실시예 23 중 어느 한 실시예에 있어서, 프로세서는 또한 개방형 인증 프로토콜(open authentication protocol)을 수행하고 AP와 접속(associate)하도록 구성되어 있는 것인 장치.

[0255] 25. 실시예 1 내지 실시예 24 중 어느 한 실시예에 있어서, 수신기는 또한 AP로부터 EAP(Extensible Authentication Protocol) 요청을 수신하도록 구성되어 있는 것인 장치.

[0256] 26. 실시예 25에 있어서, 송신기는 또한 EAP 응답을 AP로 전송하도록 구성되어 있는 것인 장치.

[0257] 27. 실시예 26에 있어서, EAP 응답은 장치의 ID(identity)를 포함하는 것인 장치.

[0258] 28. 실시예 1 내지 실시예 27 중 어느 한 실시예에 있어서, 장치가 스테이션(station, STA)인 장치.

[0259] 29. 실시예 1 내지 실시예 27 중 어느 한 실시예에 있어서, 장치가 IC(integrated circuit, 집적 회로)인 장치.

[0260] 30. 장치로서,

[0261] 요청을 전송하도록 구성되어 있는 송신기; 및

[0262] 요청에 응답하여 응답을 수신하도록 구성된 수신기를 포함하는 장치.

[0263] 31. 실시예 30에 있어서, 요청은 액세스 요청 메시지(access request message)인 장치.

[0264] 32. 실시예 30 또는 실시예 31에 있어서, 응답은 액세스 수락 메시지(access accept message)인 장치.

[0265] 33. 실시예 30 내지 실시예 32 중 어느 한 실시예에 있어서, 송신기는 또한 제1 EAPOL[EAP(extensible authentication protocol) over LAN(local area network)]-Key 프레임을 스테이션(STA)으로 전송하도록 구성되어 있는 것인 장치.

[0266] 34. 실시예 33에 있어서, 수신기는, 제1 EAPOL-Key 프레임에 응답하여, 제2 EAPOL-Key 프레임을 수신하도록 구성되어 있는 것인 장치.

[0267] 35. 실시예 33 또는 실시예 34에 있어서, 제1 EAPOL-Key 프레임은 AP와 연관되어 있는 넌스를 포함하는 것인 장치.

[0268] 36. 실시예 35에 있어서, 제2 EAPOL-Key 프레임은 장치와 연관되어 있는 넌스를 포함하는 것인 장치.

[0269] 37. 실시예 30 내지 실시예 36 중 어느 한 실시예에 있어서,

[0270] PTK(pairwise transient key, 짝 과도 키)를 도출하도록 구성되어 있는 프로세서를 추가로 포함하는 장치.

[0271] 38. 실시예 37에 있어서, 프로세서는 또한 GTK(group temporal key, 그룹 임시 키)를 도출하도록 구성되어 있는 것인 장치.

[0272] 39. 실시예 34 내지 실시예 38 중 어느 한 실시예에 있어서, 송신기는 또한 제3 EAPOL-Key 프레임을 전송하도록 구성되어 있는 것인 장치.

[0273] 40. 실시예 39에 있어서, 수신기는 또한, 제3 EAPOL-Key 프레임에 응답하여, 제4 EAPOL-Key 프레임을 수신하도록 구성되어 있는 것인 장치.

[0274] 41. 실시예 30 내지 실시예 40 중 어느 한 실시예에 있어서, 응답은 액세스 신청 메시지(access challenge message)인 장치.

[0275] 42. 실시예 41에 있어서, 수신기는 또한 스테이션(STA)으로부터 EAP 응답을 수신하도록 구성되어 있는 것인 장치.

[0276] 43. 실시예 42에 있어서, 송신기는 또한, 수신된 EAP 응답에 응답하여, 액세스 요청을 서버로 전송하도록 구성되어 있는 것인 장치.

[0277] 44. 실시예 43에 있어서, 수신기는 또한 서버로부터 액세스 수락 메시지를 수신하도록 구성되어 있는 것인 장치.

[0278] 45. 실시예 30 내지 실시예 44 중 어느 한 실시예에 있어서, 장치가 AP(access point)인 장치.

[0279] 46. 실시예 30 내지 실시예 44 중 어느 한 실시예에 있어서, 장치가 IC(integrated circuit)인 장치.

[0280] 47. 실시예 1 내지 실시예 29 중 어느 한 실시예의 장치에 의해 수행될 수 있는 방법.

[0281] 48. 실시예 30 내지 실시예 46 중 어느 한 실시예의 장치에 의해 수행될 수 있는 방법.

[0282] 49. 방법으로서,

[0283] 프로브 요청 프레임을 수신하는 단계;

[0284] 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치하는지를 판정하는 단계; 및

[0285] 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치하는 경우, 프로브 요청 프레임에 응답하여, 감소된 프로브 응답 프레임(reduced probe response frame)을 전송하는 단계를 포함하는 방법.

[0286] 50. 실시예 49에 있어서, 프로브 요청 프레임은 시스템 구성 식별자를 포함하는 것인 방법.

[0287] 51. 실시예 49 또는 실시예 50에 있어서, 감소된 프로브 응답 프레임은 파라미터를 생략한 프로브 응답 프레임인 방법.

[0288] 52. 실시예 49 내지 실시예 51 중 어느 한 실시예에 있어서, 시스템 구성 식별자가 저장된 시스템 구성 식별자와 일치하지 않는 경우, 프로브 요청 프레임에 응답하여, 전체 프로브 응답 프레임(full probe response frame) 또는 부분적으로 감소된 프로브 응답 프레임(partially reduced probe response frame)을 전송하는 단계를 추

가로 포함하는 방법.

[0289] 53. 실시예 52에 있어서, 부분적으로 감소된 프로브 응답 프레임은 전체 구성 표시자(full configuration indicator)를 포함하지 않는 프로브 응답 프레임인 방법.

[0290] 54. 방법으로서,

[0291] 구성 표시자(configuration indicator) 및 대응하는 CCC(configuration change count, 구성 변경 횟수) 값을 수신하는 단계를 포함하는 방법.

[0292] 55. 실시예 54에 있어서,

[0293] 획득된 구성 지식 데이터베이스(configuration knowledge database)에 구성 표시자 항목(configuration indicator entry)이 있는지를 판정하는 단계를 추가로 포함하는 방법.

[0294] 56. 실시예 55에 있어서, 획득된 구성 지식 데이터베이스에 구성 표시자 항목이 없는 경우, 새로운 구성 표시자 항목을 생성하는 단계를 추가로 포함하는 방법.

[0295] 57. 실시예 56에 있어서, 새로운 구성 표시자 항목은 수신된 구성 표시자 및 수신된 대응하는 CCC 값에 기초하는 것인 방법.

[0296] 58. 실시예 57에 있어서,

[0297] 수신된 CCC 값이 획득된 구성 지식 데이터베이스에 있는 CCC 값과 일치하는지를 판정하는 단계를 추가로 포함하는 방법.

[0298] 59. 실시예 58에 있어서,

[0299] 수신된 CCC 값이 획득된 구성 지식 데이터베이스에 있는 CCC 값과 일치하지 않는 경우, 획득된 구성 지식 데이터베이스를 갱신하는 단계를 추가로 포함하는 방법.

[0300] 60. 실시예 59에 있어서, 획득된 구성 지식 데이터베이스는 수신된 CCC 값에 기초하여 갱신되는 것인 방법.

[0301] 61. 실시예 49 내지 실시예 53 중 어느 한 실시예의 방법을 수행하도록 구성되어 있는 AP(access point).

[0302] 62. 실시예 49 내지 실시예 53 중 어느 한 실시예의 방법을 수행하도록 구성되어 있는 IC(integrated circuit).

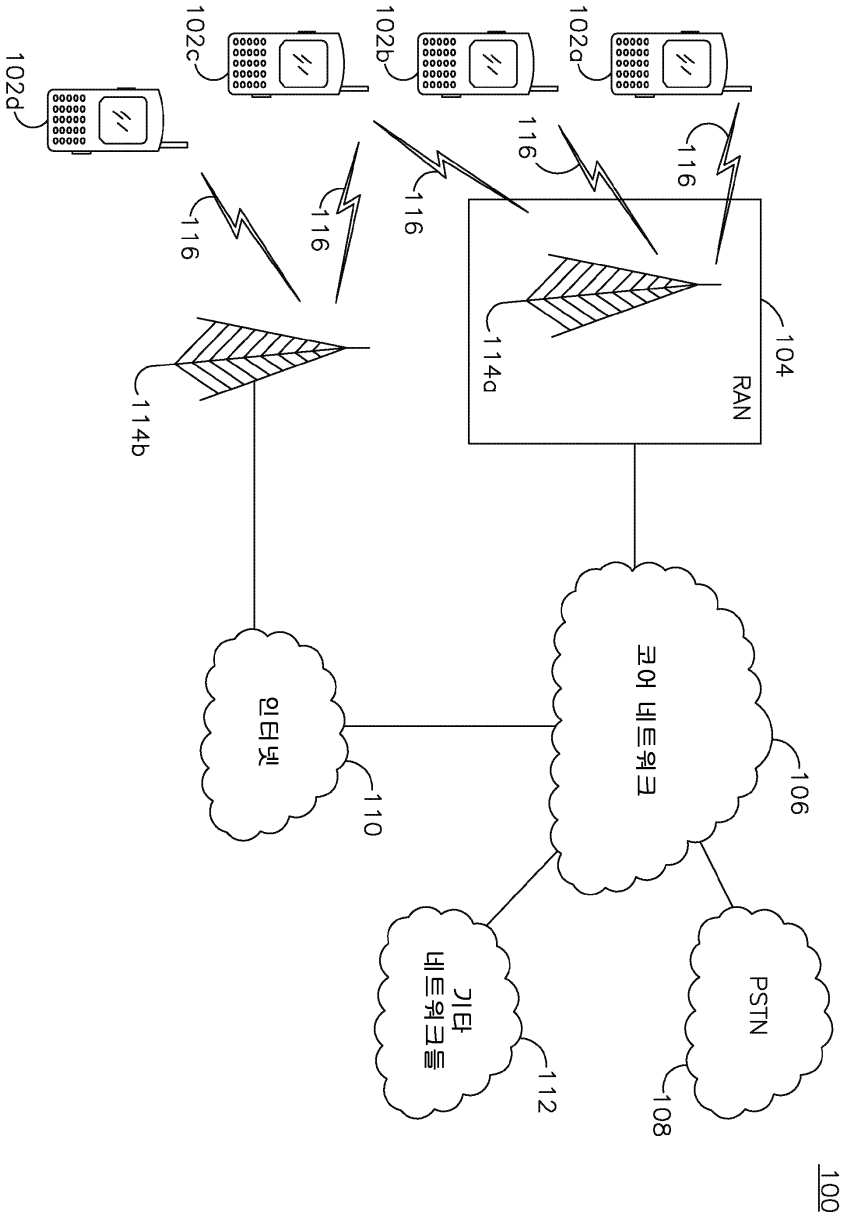
[0303] 63. 실시예 54 내지 실시예 60 중 어느 한 실시예의 방법을 수행하도록 구성되어 있는 비AP(non-access point).

[0304] 64. 실시예 54 내지 실시예 60 중 어느 한 실시예의 방법을 수행하도록 구성되어 있는 IC(integrated circuit).

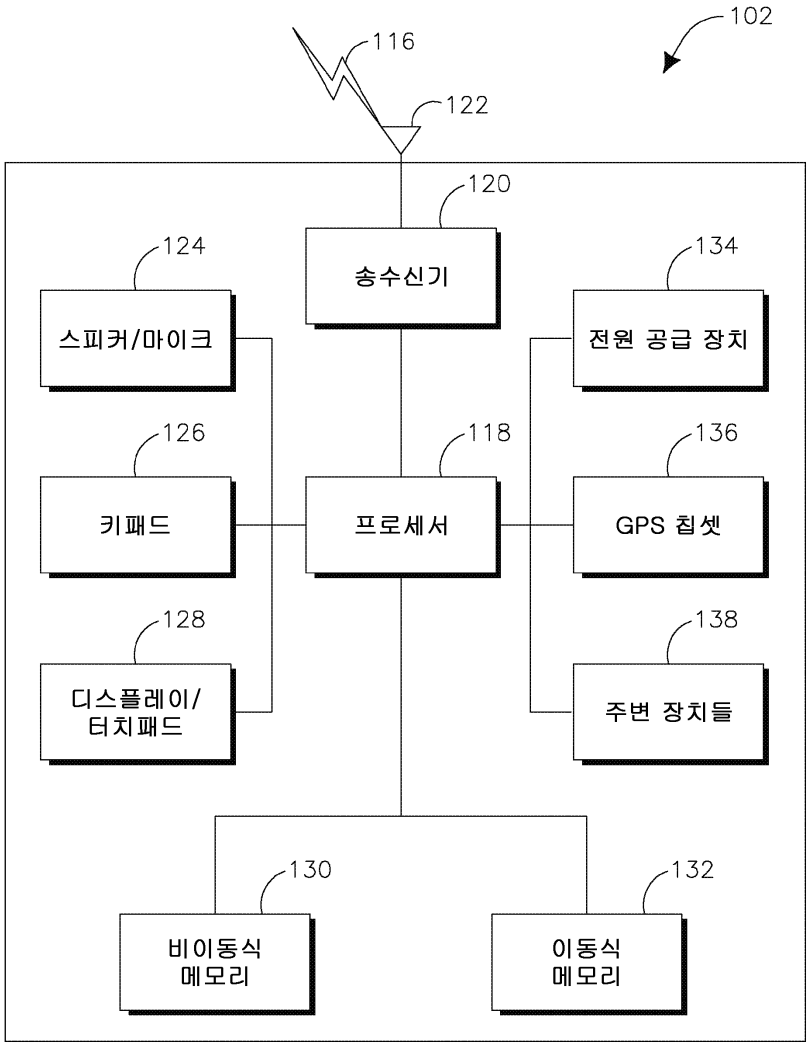
[0305] 특징 및 요소가 특정의 조합으로 앞서 기술되어 있지만, 당업자라면 각각의 특징 또는 요소가 단독으로 또는 다른 특징 및 요소와 임의의 조합으로 사용될 수 있다는 것을 잘 알 것이다. 그에 부가하여, 본 명세서에 기술된 방법이 컴퓨터 또는 프로세서에서 실행하기 위해 컴퓨터 판독가능 매체에 포함되어 있는 컴퓨터 프로그램, 소프트웨어, 또는 펌웨어로 구현될 수 있다. 컴퓨터 판독가능 매체의 일례는 전자 신호(유선 또는 무선 연결을 통해 전송됨) 및 컴퓨터 판독가능 저장 매체를 포함한다. 컴퓨터 판독가능 저장 매체의 일례로는 ROM(read only memory), RAM(random access memory), 레지스터, 캐시 메모리, 반도체 메모리 장치, 내장형 하드 디스크 및 이동식 디스크 등의 자기 매체, 광자기 매체, 그리고 CD-ROM 디스크 및 DVD(digital versatile disk) 등의 광 매체가 있지만, 이들로 제한되지 않는다. 소프트웨어와 연관된 프로세서는 WTRU, UE, 단말, 기지국, RNC, 또는 임의의 호스트 컴퓨터에서 사용하기 위한 무선 주파수 송수신기를 구현하는 데 사용될 수 있다.

도면

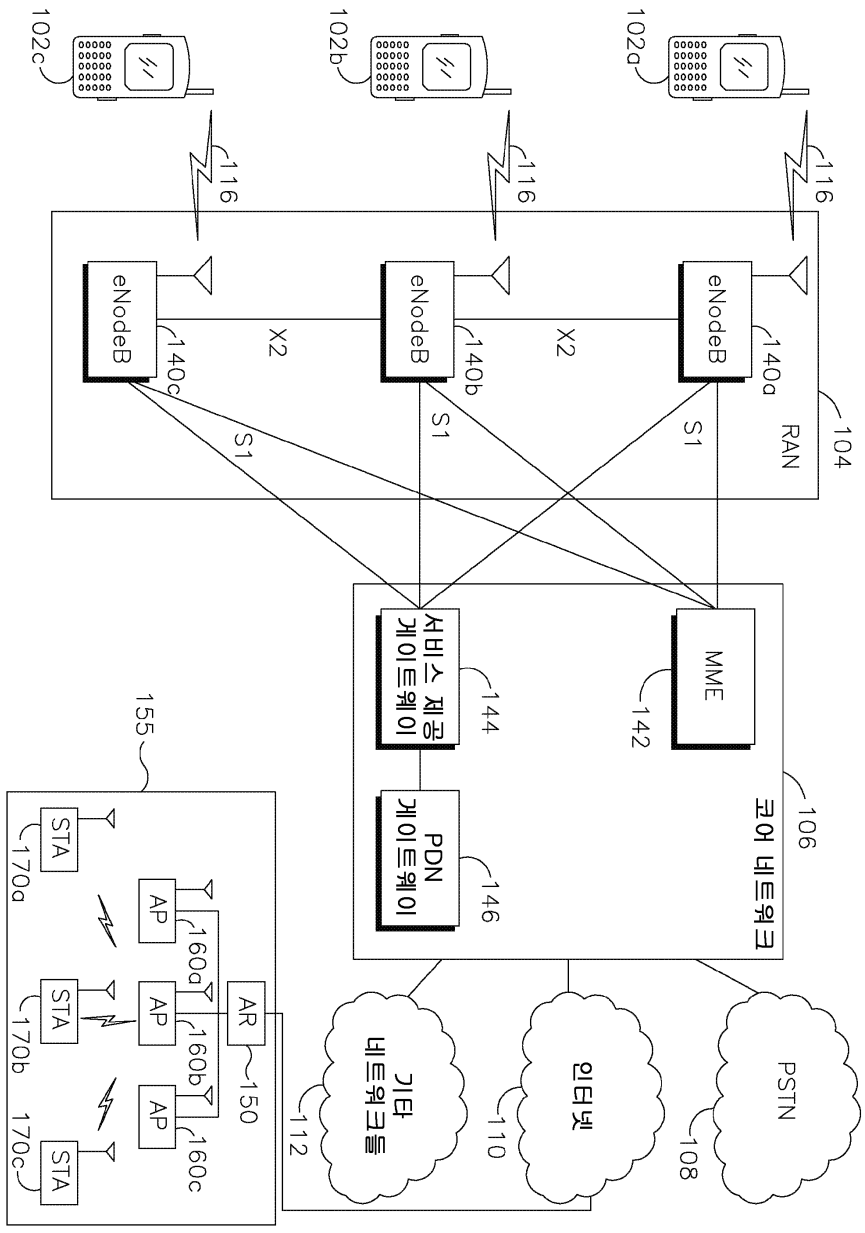
도면1a


102a
102b
102c
102d
116
116
116
116
114a
114b
RAN
104
코어 네트워크
106
인터넷
110
기타 네트워크들
112
PSTN
108
100

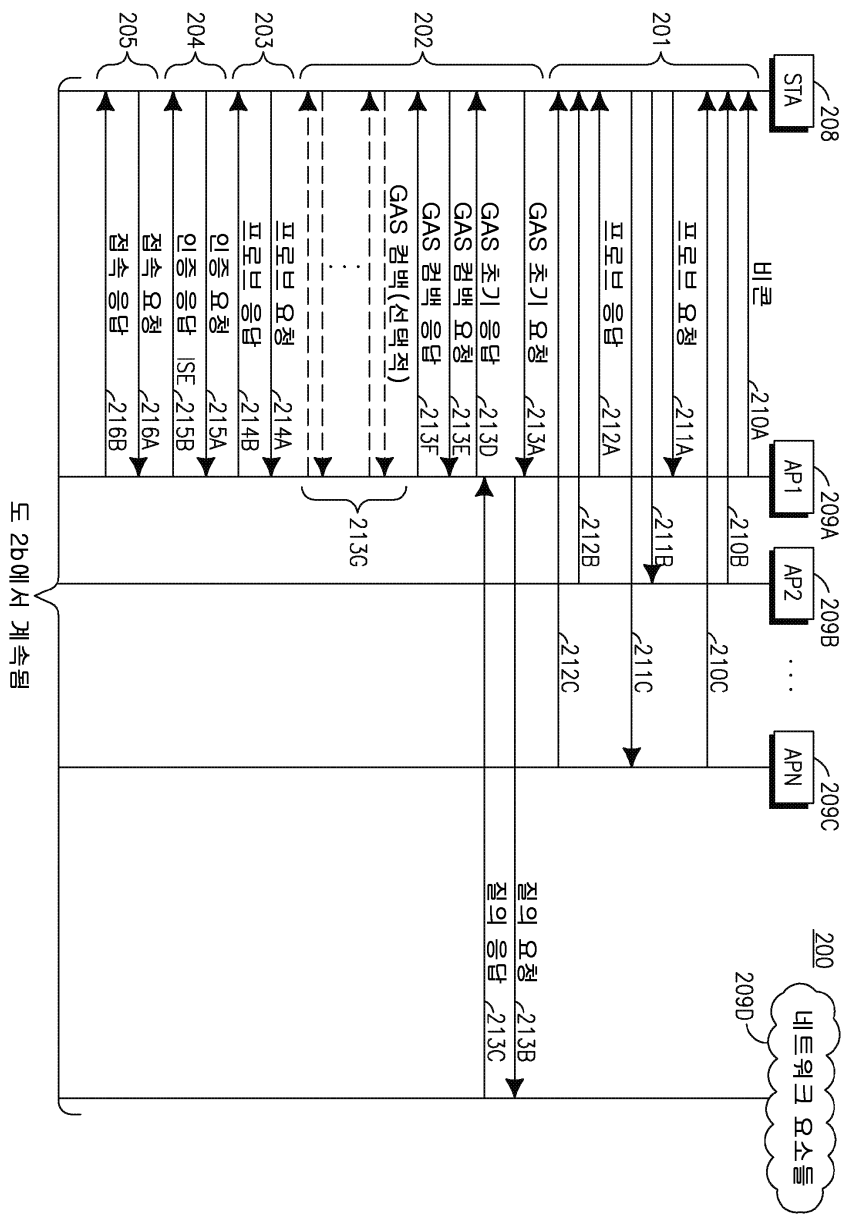
도면1b


102
116
122
120
송수신기
124
스피커/마이크
126
키패드
128
디스플레이/
터치패드
118
프로세서
130
비이동식
메모리
132
이동식
메모리
134
전원 공급 장치
136
GPS 칩셋
138
주변 장치들

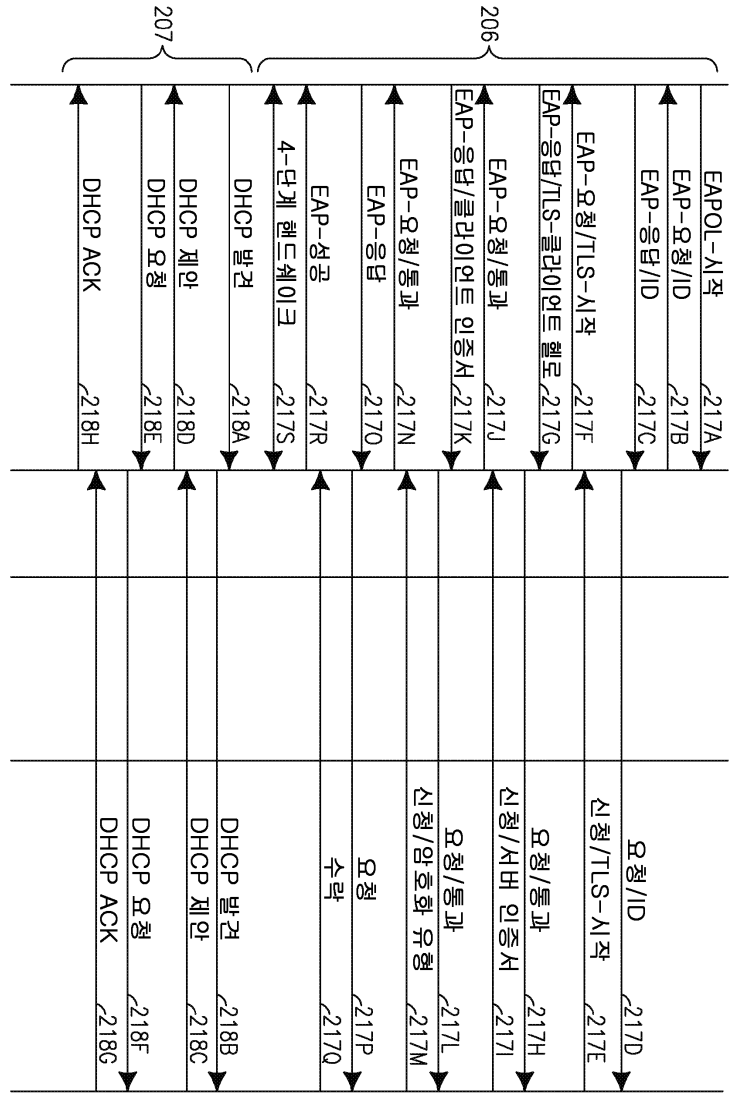
도면1c


102c
102b
102a
116
116
116
eNodeB
eNodeB
eNodeB
140c
140b
140a
X2
X2
S1
S1
S1
RAN
104
서비스 제공 게이트웨이
144
MME
142
PDN 게이트웨이
146
코어 네트워크
106
155
STA
170a
AP
160a
AR
150
STA
170b
AP
160b
AP
160c
STA
170c
기타 네트워크들
112
인터넷
110
PSTN
108

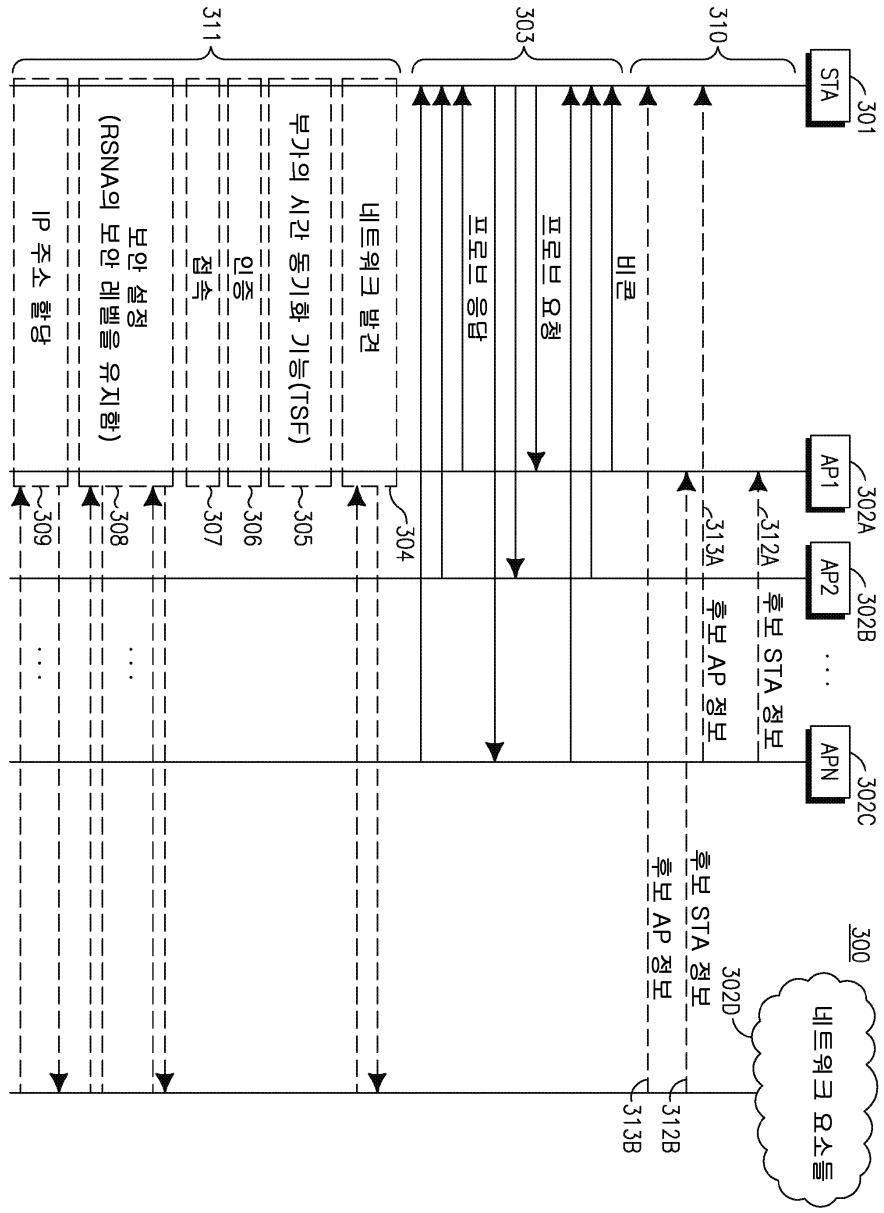
도면2a


STA
208
AP1
209A
AP2
209B
APN
209C
200
네트워크 요소들
209D
201
202
203
204
205
비콘
210A
프로브 요청
211A
210B
211B
프로브 응답
212A
212B
GAS 초기 요청
213A
210C
211C
212C
GAS 초기 응답
213D
GAS 컴백 요청
213E
GAS 컴백 응답
213F
GAS 컴백(선택적)
213G
프로브 요청
214A
프로브 응답
214B
인증 요청
215A
인증 응답
215B
ISE
결속 요청
216A
결속 응답
216B
질의 요청
213B
질의 응답
213C
도 2b에서 계속됨

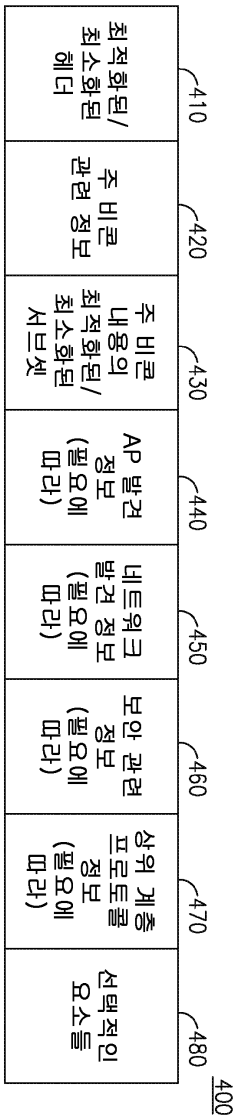
도면2b


206
207
EAPOL-시작 217A
EAP-요청/ID 217B
EAP-응답/ID 217C
EAP-요청/TLS-시작 217F
EAP-응답/TLS-클라이언트 헬로 217G
EAP-요청/통과 217J
EAP-응답/클라이언트 인증서 217K
EAP-요청/통과 217N
EAP-응답 217O
EAP-성공 217R
4-단계 핸드쉐이크 217S
DHCP 발견 218A
DHCP 제안 218D
DHCP 요청 218E
DHCP ACK 218H
요청/ID 217D
신청/TLS-시작 217E
요청/통과 217H
신청/서버 인증서 217I
요청/통과 217L
신청/암호화 유형 217M
요청 217P
수락 217Q
DHCP 발견 218B
DHCP 제안 218C
DHCP 요청 218F
DHCP ACK 218G

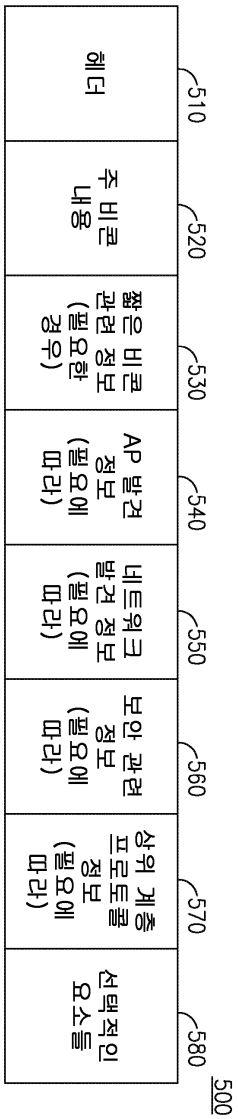
도면3


STA
301
AP1
302A
AP2
302B
APN
302C
네트워크 요소들
300
302D
310
303
311
비콘
프로브 요청
프로브 응답
312A
313A
후보 STA 정보
후보 AP 정보
312B
313B
후보 STA 정보
후보 AP 정보
네트워크 발견
304
부가의 시간 동기화 기능(TSF)
305
인증
306
접속
307
보안 설정
(RSNA의 보안 레벨을 유지함)
308
IP 주소 할당
309

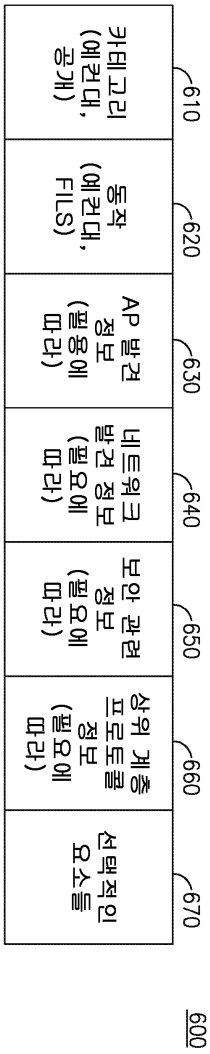
도면4


최적화된/최소화된 헤더
410
주 비콘 관련 정보
420
주 비콘 내용의 최적화된/최소화된 서브셋
430
AP 발견 정보 (필요에 따라)
440
네트워크 발견 정보 (필요에 따라)
450
보안 관련 정보 (필요에 따라)
460
상위 계층 프로토콜 정보 (필요에 따라)
470
선택적인 요소들
480
400

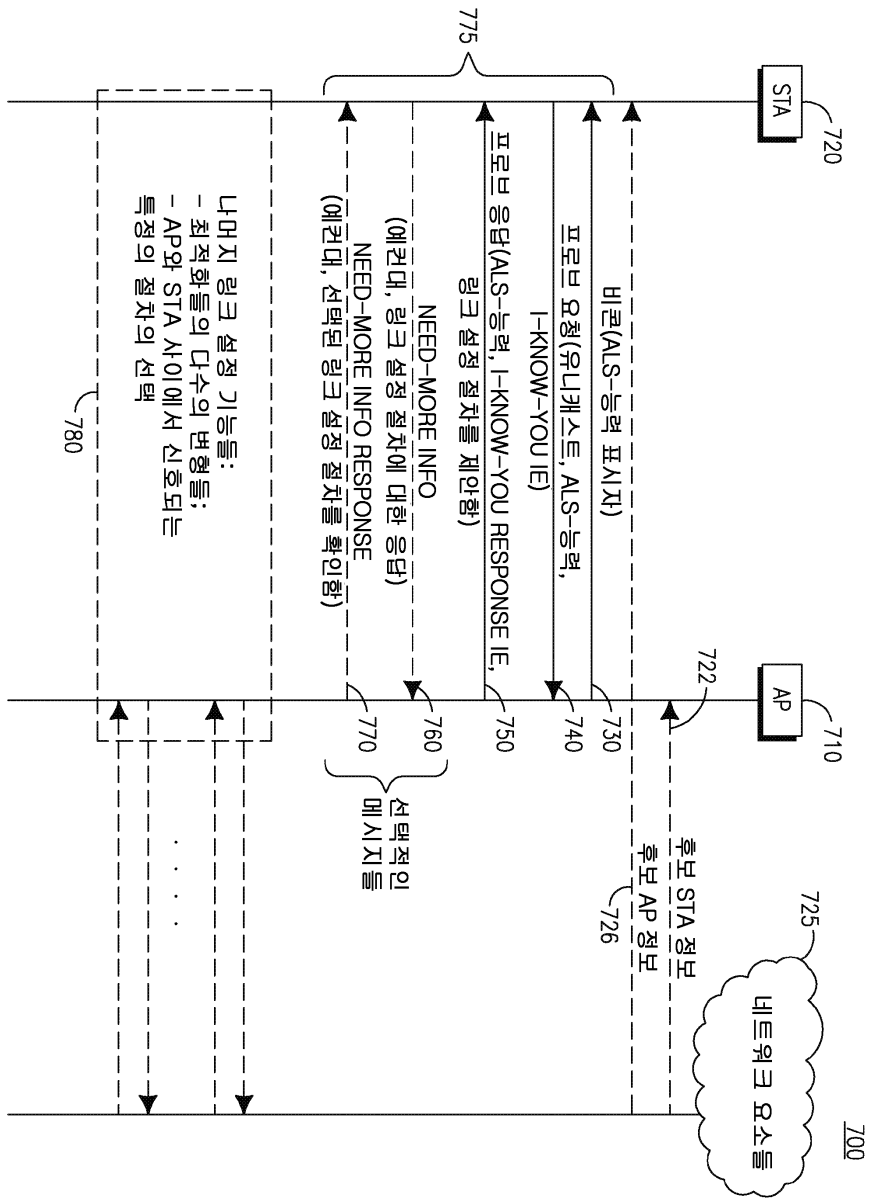
도면5


헤더
510
주 비콘 내용
520
짧은 비콘 관련 정보 (필요할 경우)
530
AP 발견 정보 (필요에 따라)
540
네트워크 발견 정보 (필요에 따라)
550
보안 관련 정보 (필요에 따라)
560
상위 계층 프로토콜 정보 (필요에 따라)
570
선택적인 요소들
580
500

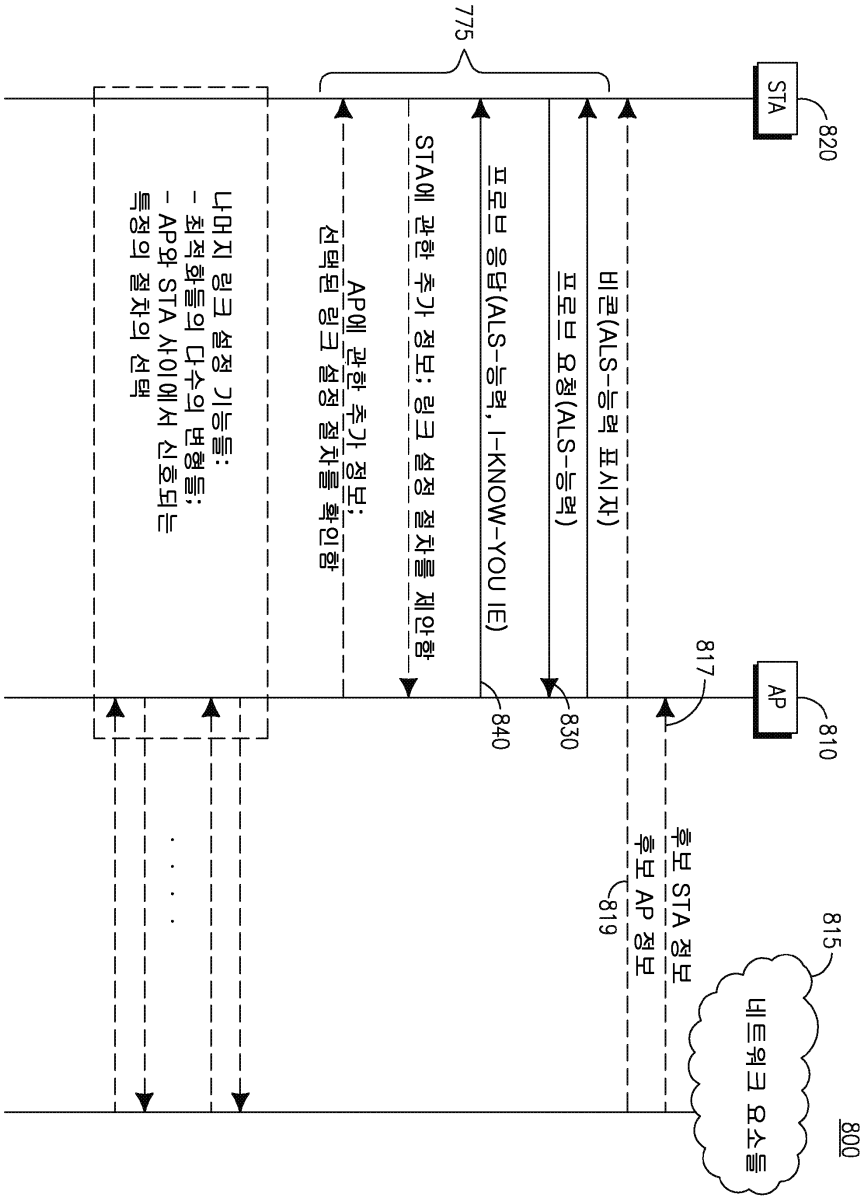
도면6


카테고리 (예컨대, 공개)
610
동작 (예컨대, FILS)
620
AP 발견 정보 (필요에 따라)
630
네트워크 발견 정보 (필요에 따라)
640
보안 관련 정보 (필요에 따라)
650
상위 계층 프로토콜 정보 (필요에 따라)
660
선택적인 요소들
670
600

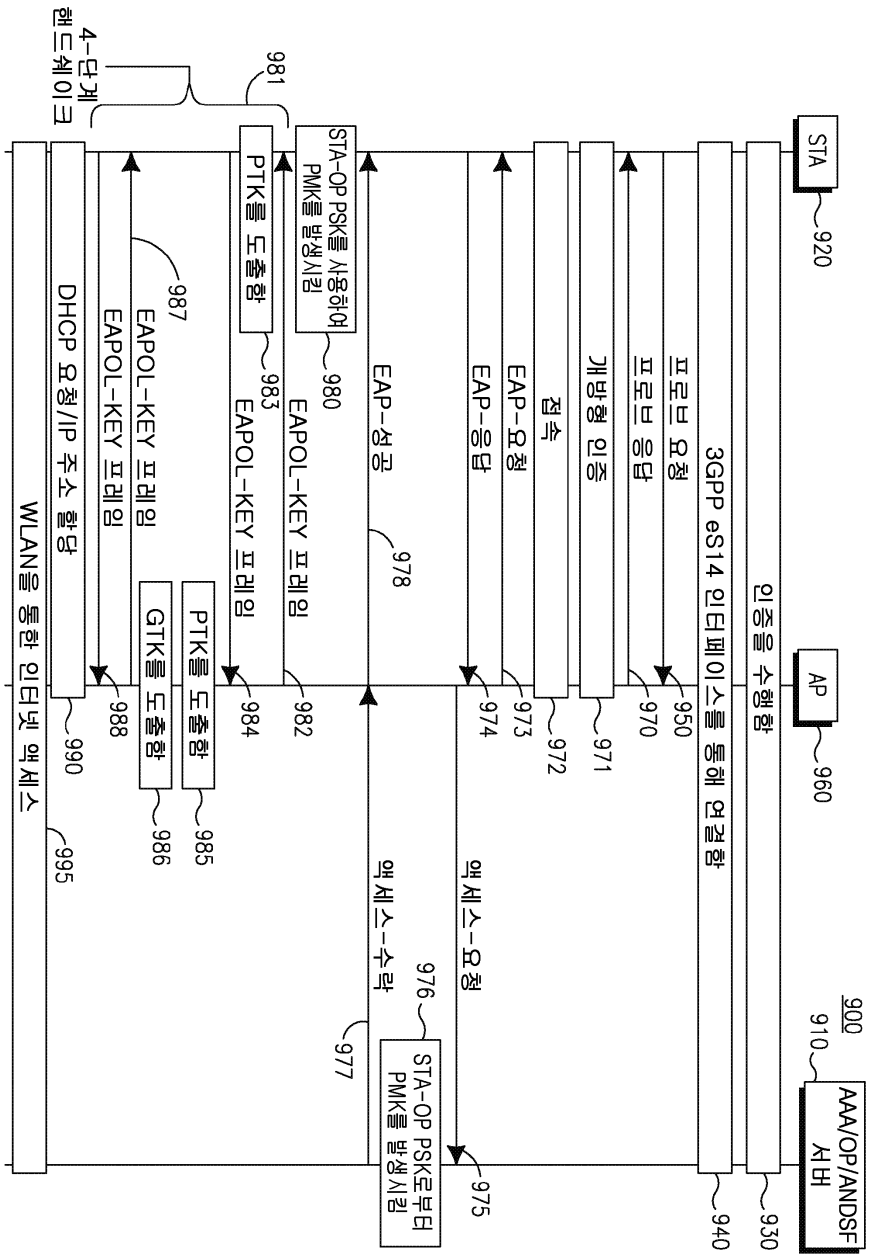
도면7


STA
720
AP
710
700
네트워크 요소들
725
775
780
722
730
740
750
760
770
726
비콘(ALS-능력 표시자)
프로브 요청(유니캐스트, ALS-능력, I-KNOW-YOU IE)
프로브 응답(ALS-능력, I-KNOW-YOU RESPONSE IE, 링크 설정 절차를 제안함)
NEED-MORE INFO (예컨대, 링크 설정 절차에 대한 응답)
NEED-MORE INFO RESPONSE (예컨대, 선택된 링크 설정 절차를 확인함)
선택적인 메시지들
후보 STA 정보
후보 AP 정보
나머지 링크 설정 기능들:
- 최적화들의 다수의 변형들;
- AP와 STA 사이에서 신호되는 특정의 절차의 선택
. . . .

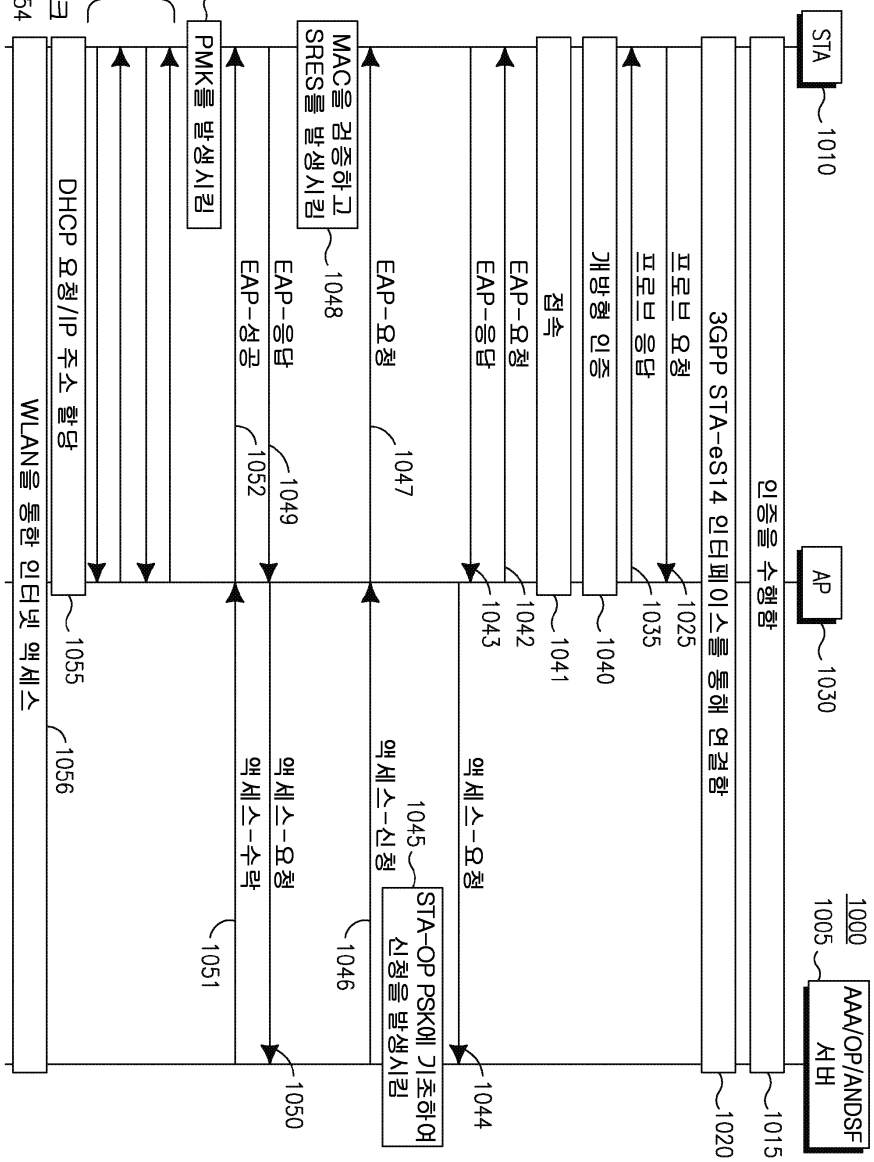
도면8


775
STA
820
AP
810
817
840
830
819
815
800
네트워크 요소들
비콘(ALS-능력 표시자)
프로브 요청(ALS-능력)
프로브 응답(ALS-능력, I-KNOW-YOU IE)
STA에 관한 추가 정보; 링크 설정 절차를 제안함
AP에 관한 추가 정보;
선택된 링크 설정 절차를 확인함
후보 STA 정보
후보 AP 정보
나머지 링크 설정 기능들:
- 최적화들의 다수의 변형들;
- AP와 STA 사이에서 신호되는
특정의 절차의 선택
. . . .

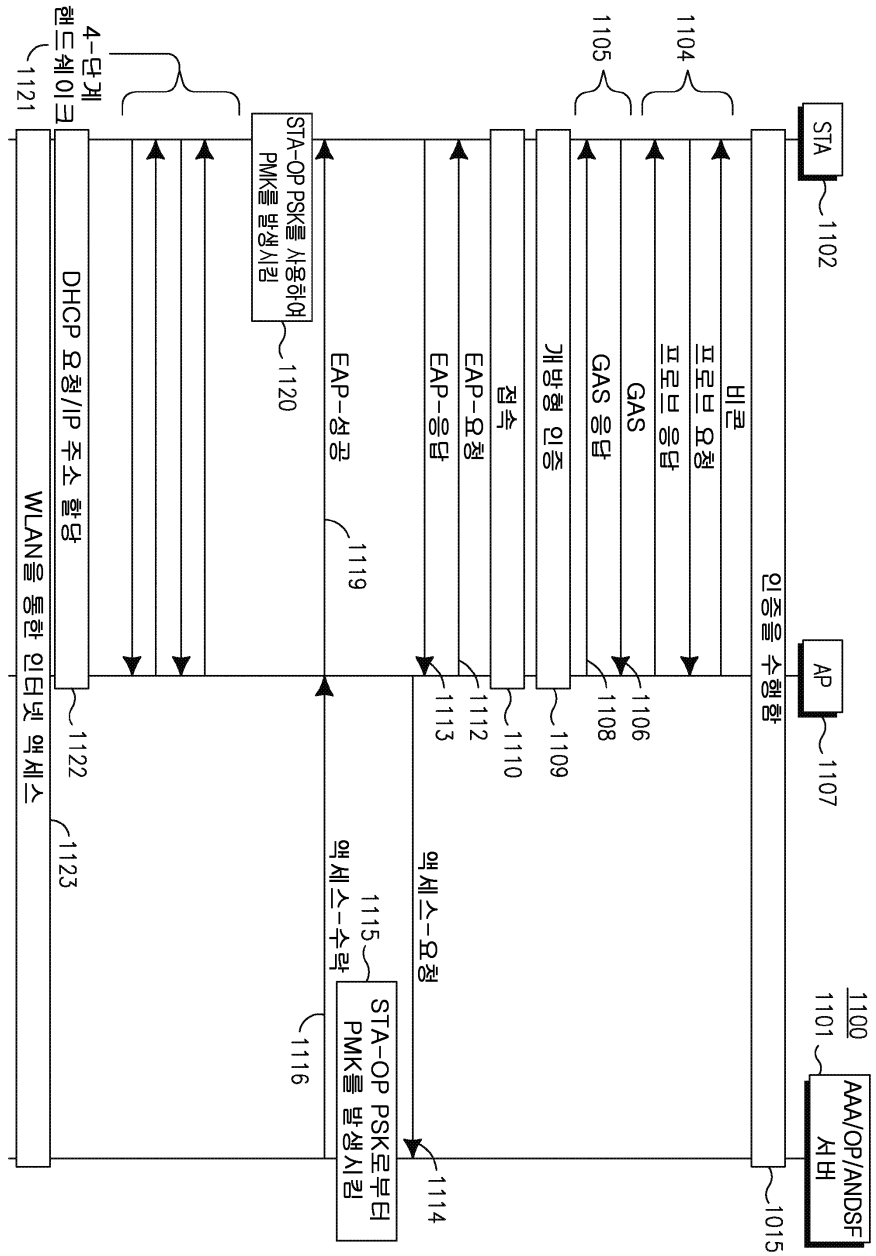
도면9


900
STA
920
AP
960
AAA/OP/ANDSF 서버
910
인증을 수행함
930
3GPP eS14 인터페이스를 통해 연결함
940
프로브 요청
950
프로브 응답
970
개방형 인증
971
접속
972
EAP-요청
973
EAP-응답
974
액세스-요청
975
STA-OP PSK로부터 PMK를 발생시킴
976
액세스-수락
977
EAP-성공
978
4-단계 핸드쉐이크
981
STA-OP PSK를 사용하여 PMK를 발생시킴
980
EAPOL-KEY 프레임
982
PTK를 도출함
983
EAPOL-KEY 프레임
984
PTK를 도출함
985
GTK를 도출함
986
EAPOL-KEY 프레임
987
EAPOL-KEY 프레임
988
DHCP 요청/IP 주소 할당
990
WLAN을 통한 인터넷 액세스
995

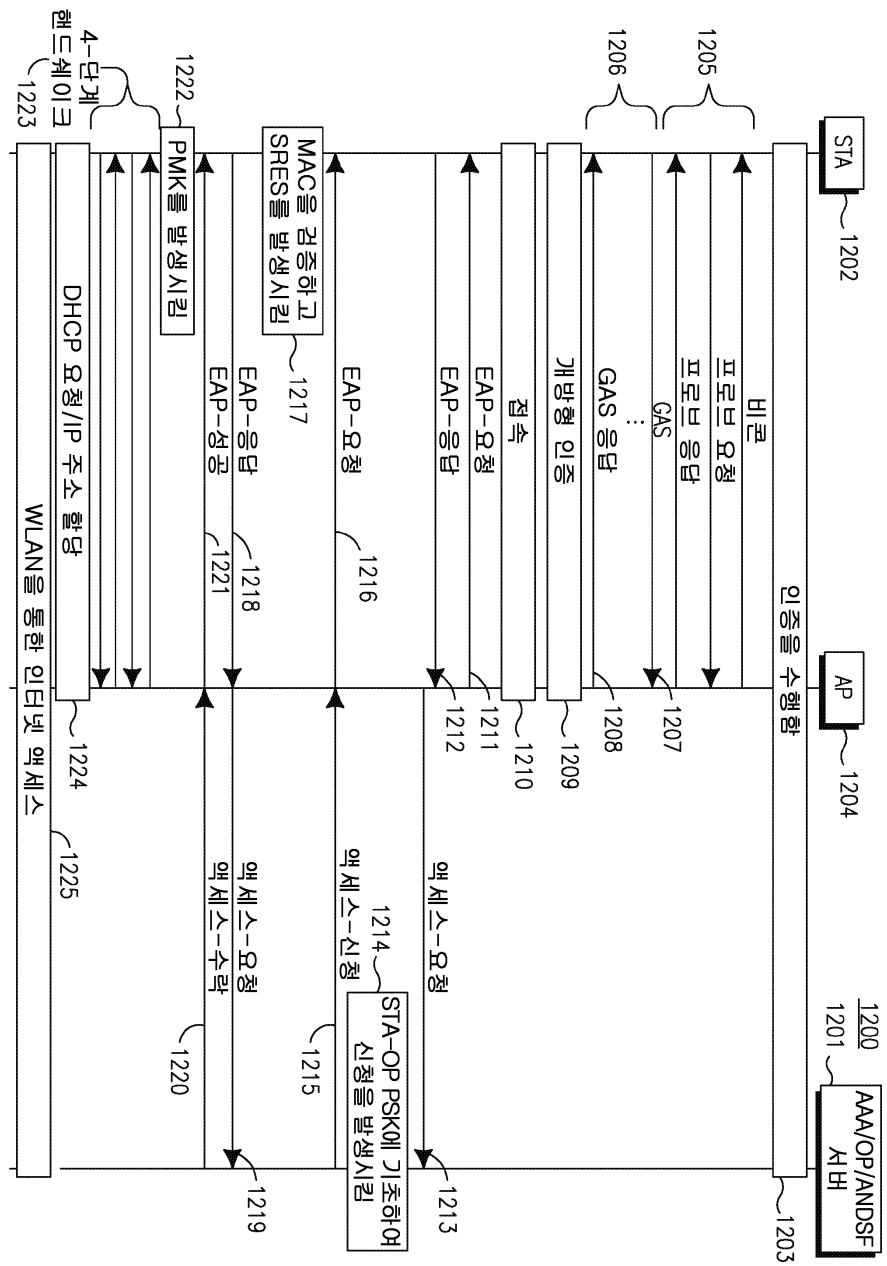
도면10


STA
1010
AP
1030
1000
1005
AAA/OP/ANDSF
서버
1015
인증을 수행함
1020
3GPP STA-eS14 인터페이스를 통해 연결함
프로브 요청
1025
프로브 응답
1035
개방형 인증
1040
접속
1041
EAP-요청
1042
EAP-응답
1043
액세스-요청
1044
STA-OP PSK에 기초하여
신청을 발생시킴
1045
액세스-신청
1046
MAC을 검증하고
SRES를 발생시킴
1048
EAP-요청
1047
EAP-응답
1049
EAP-성공
1052
액세스-요청
액세스-수락
1050
1051
PMK를 발생시킴
1053
4-단계
핸드쉐이크
1054
DHCP 요청/IP 주소 할당
1055
WLAN을 통한 인터넷 액세스
1056

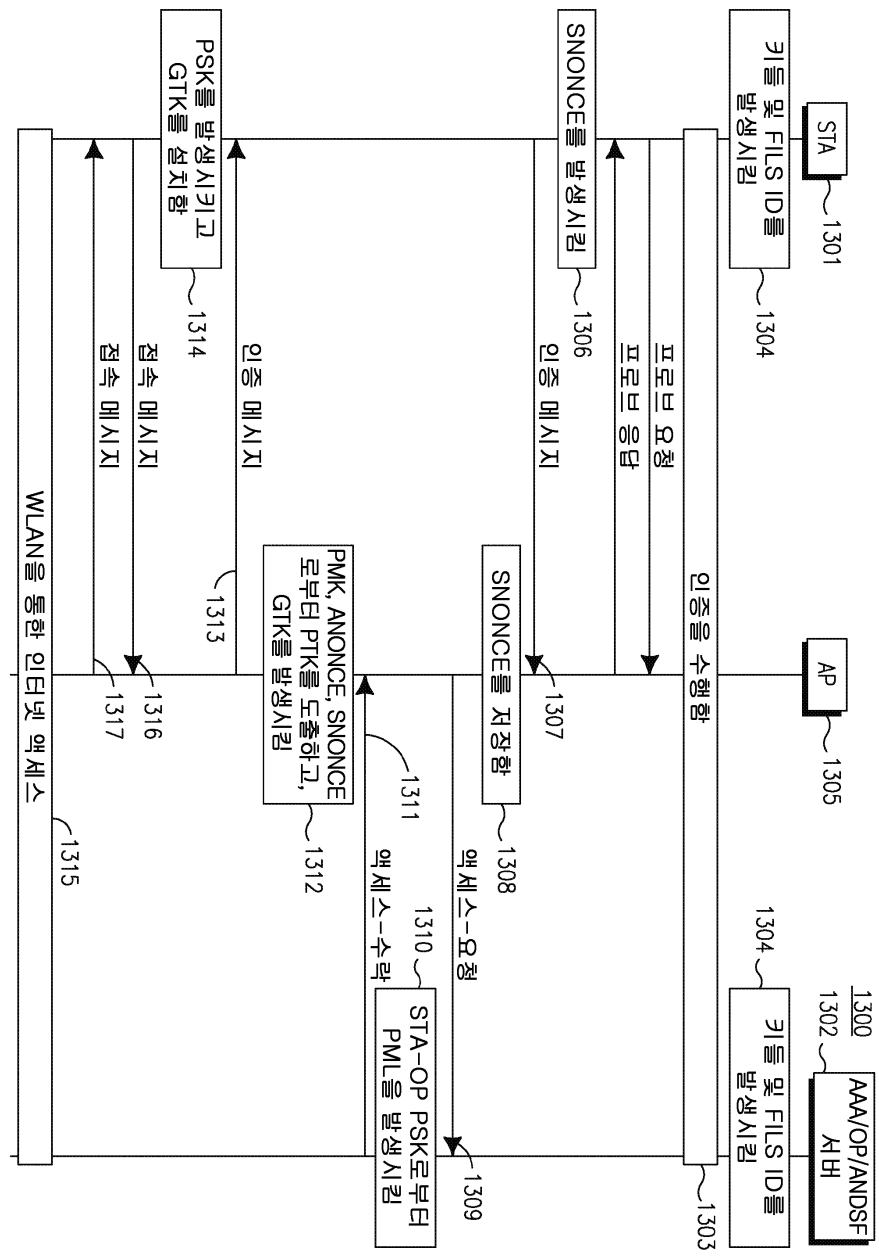
도면11


STA
1102
AP
1107
1100
1101
AAA/OP/ANDSF 서버
1015
인증을 수행함
1104
비콘
프로브 요청
프로브 응답
1105
GAS
GAS 응답
개방형 인증
1106
1108
1109
접속
EAP-요청
EAP-응답
1110
1112
1113
EAP-성공
1119
STA-OP PSK를 사용하여 PMK를 발생시킴
1120
4-단계 핸드쉐이크
1121
DHCP 요청/IP 주소 할당
1122
1123
WLAN을 통한 인터넷 액세스
액세스-요청
1114
1115
액세스-수락
STA-OP PSK로부터 PMK를 발생시킴
1116

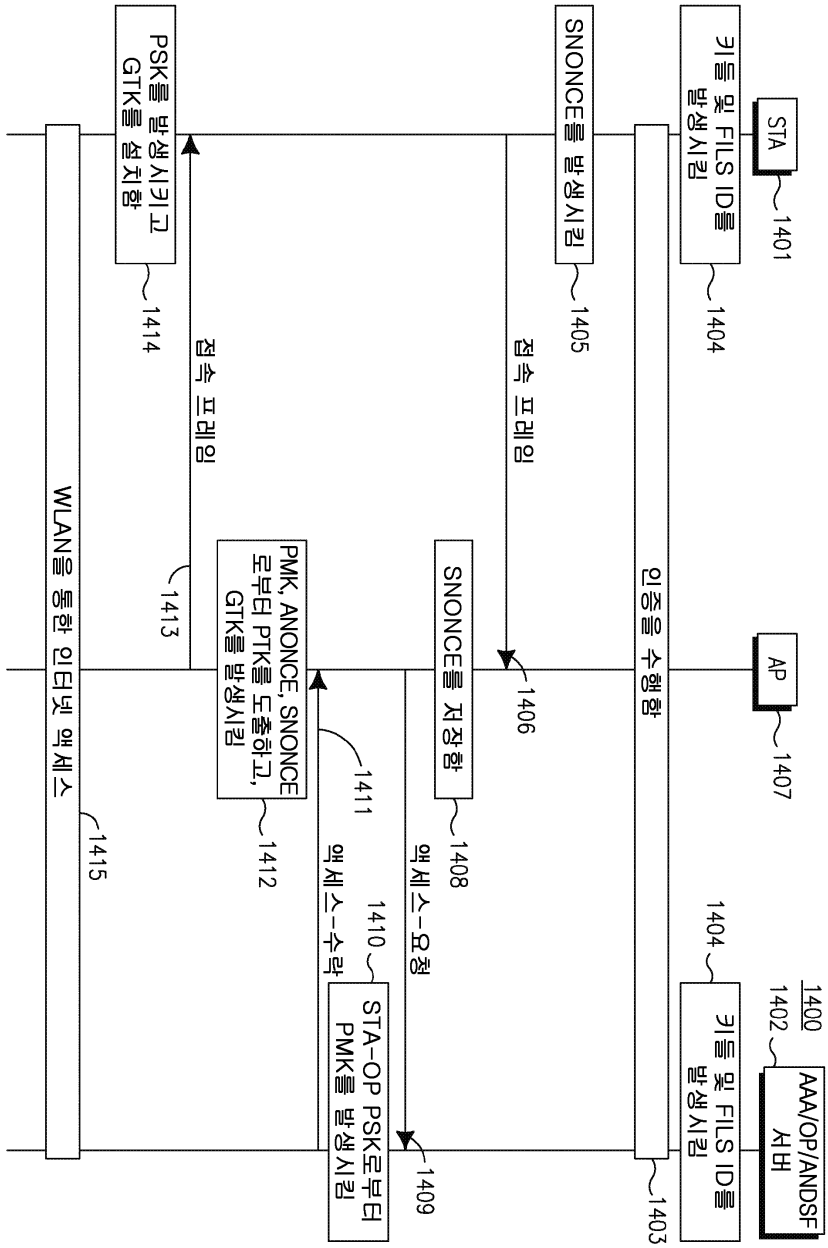
도면12


STA
1202
AP
1204
1200
1201
AAA/OP/ANDSF 서버
1203
1205
1206
비콘
프로브 요청
프로브 응답
GAS
GAS 응답
개방형 인증
접속
EAP-요청
EAP-응답
인증을 수행함
1207
1208
1209
1210
1211
1212
1213
MAC을 검증하고 SRES를 발생시킴
1217
EAP-요청
1216
EAP-응답
EAP-성공
1218
1221
PMK를 발생시킴
1222
4-단계 핸드쉐이크
1223
DHCP 요청/IP 주소 할당
1224
WLAN을 통한 인터넷 액세스
1225
액세스-요청
1214
STA-OP PSK에 기초하여 신청을 발생시킴
액세스-신청
1215
액세스-요청
액세스-수락
1220
1219

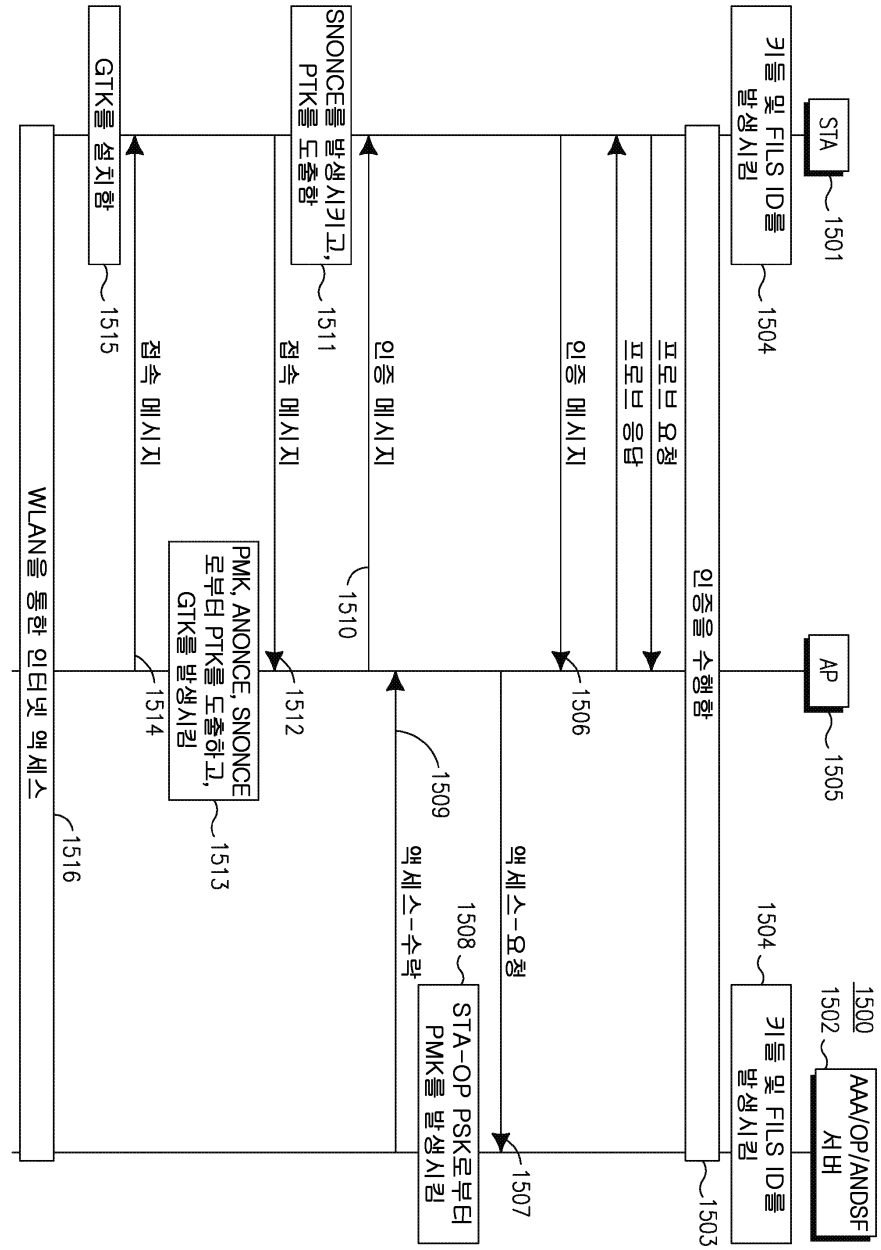
도면13


STA
AP
1300
1302
AAA/OP/ANDSF 서버
1301
1305
키들 및 FILS ID를 발생시킴
1304
1304
키들 및 FILS ID를 발생시킴
프로브 요청
프로브 응답
인증을 수행함
1303
SNONCE를 발생시킴
1306
인증 메시지
SNONCE를 저장함
1307
1308
액세스-요청
1309
PSK를 발생시키고 GTK를 설치함
1314
인증 메시지
1313
PMK, ANONCE, SNONCE로부터 PTK를 도출하고, GTK를 발생시킴
1312
1311
액세스-수락
1310
STA-OP PSK로부터 PML을 발생시킴
점속 메시지
1316
점속 메시지
1317
WLAN을 통한 인터넷 액세스
1315

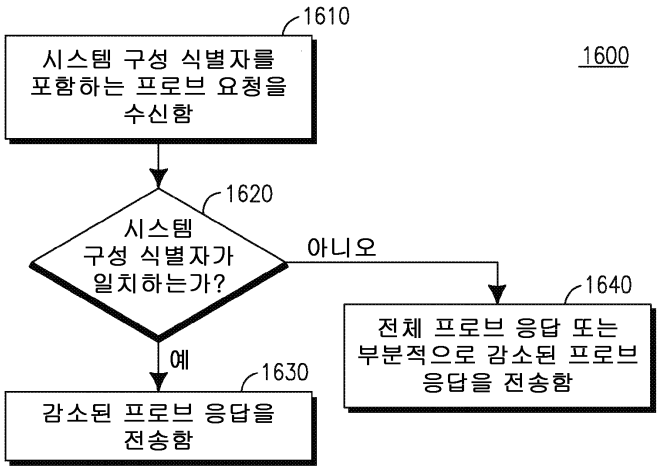
도면14


STA
1401
AP
1407
1400
1402
AAA/OP/ANDSF 서버
키들 및 FILS ID를 발생시킴
1404
SNONCE를 발생시킴
1405
인증을 수행함
1403
키들 및 FILS ID를 발생시킴
1404
접속 프레임
1406
SNONCE를 저장함
1408
액세스-요청
1409
STA-OP PSK로부터 PMK를 발생시킴
1410
액세스-수락
1411
PMK, ANONCE, SNONCE로부터 PTK를 도출하고, GTK를 발생시킴
1412
접속 프레임
1413
PSK를 발생시키고 GTK를 설치함
1414
WLAN을 통한 인터넷 액세스
1415

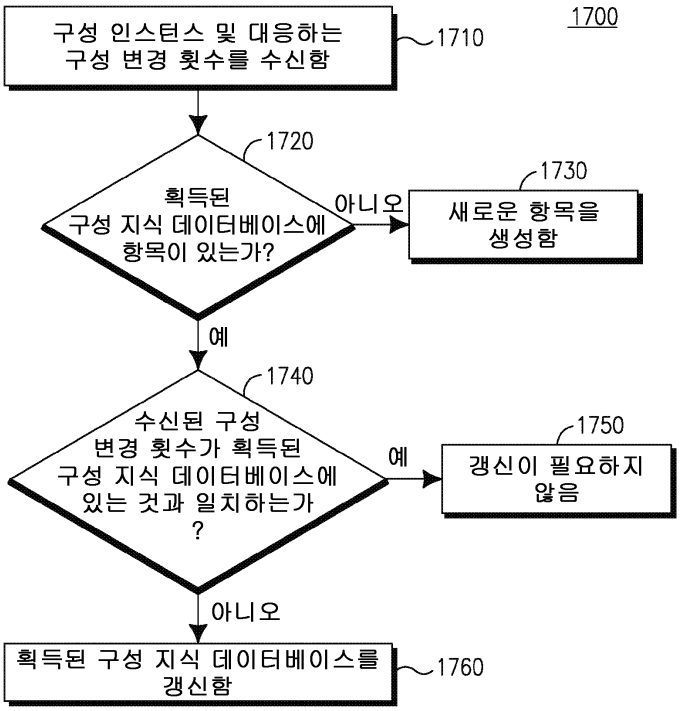
도면15


STA
AP
AAA/OP/ANDSF 서버
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
키들 및 FILS ID를 발생시킴
프로브 요청
프로브 응답
인증을 수행함
키들 및 FILS ID를 발생시킴
인증 메시지
액세스-요청
STA-OP PSK로부터 PMK를 발생시킴
액세스-수락
인증 메시지
SNONCE를 발생시키고, PTK를 도출함
접속 메시지
PMK, ANONCE, SNONCE로부터 PTK를 도출하고, GTK를 발생시킴
접속 메시지
GTK를 설치함
WLAN을 통한 인터넷 액세스

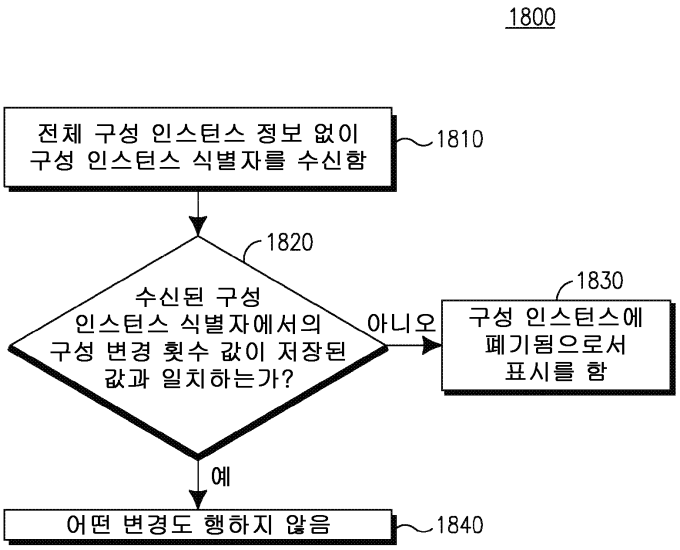
도면16


1600
1610
시스템 구성 식별자를 포함하는 프로브 요청을 수신함
1620
시스템 구성 식별자가 일치하는가?
아니오
예
1630
감소된 프로브 응답을 전송함
1640
전체 프로브 응답 또는 부분적으로 감소된 프로브 응답을 전송함

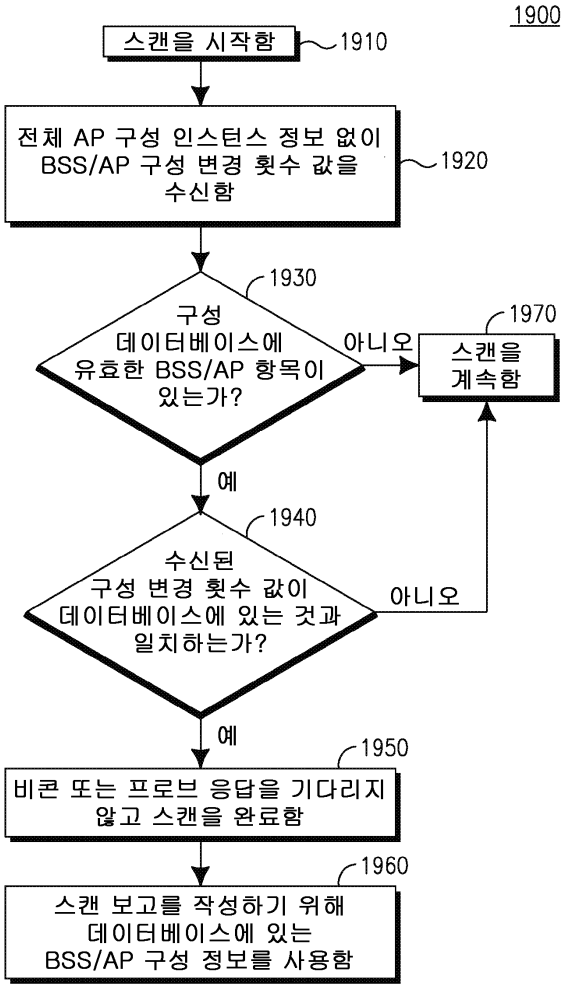
도면17


1700
구성 인스턴스 및 대응하는 구성 변경 횟수를 수신함
1710
1720
획득된 구성 지식 데이터베이스에 항목이 있는가?
아니오
1730
새로운 항목을 생성함
예
1740
수신된 구성 변경 횟수가 획득된 구성 지식 데이터베이스에 있는 것과 일치하는가 ?
예
1750
갱신이 필요하지 않음
아니오
획득된 구성 지식 데이터베이스를 갱신함
1760

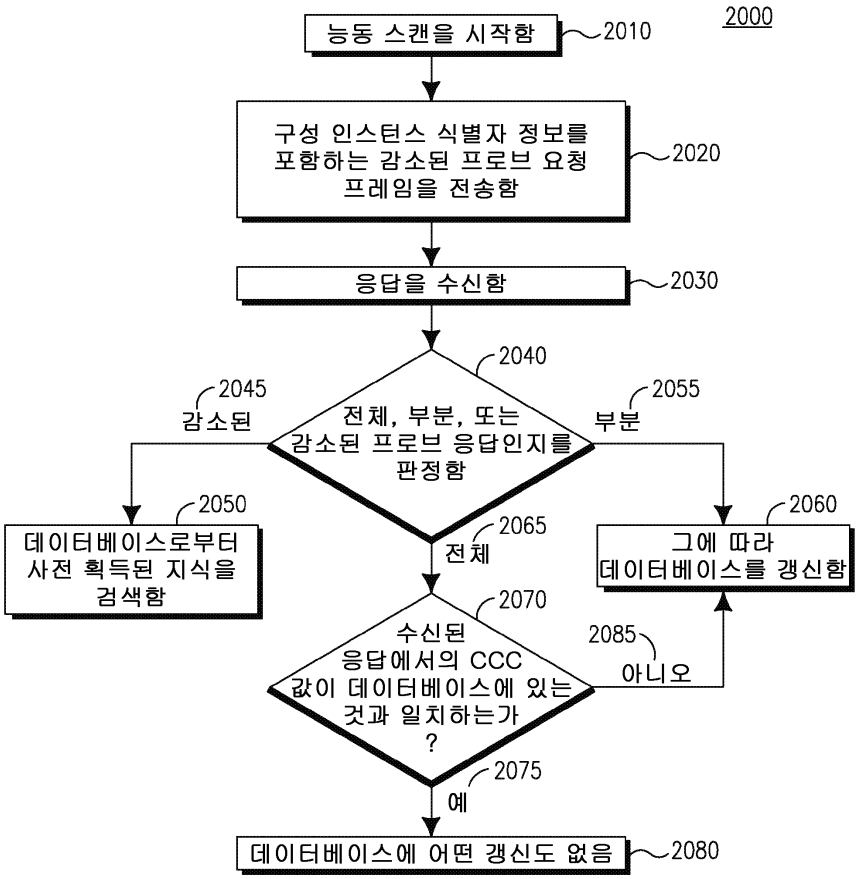
도면18


1800
전체 구성 인스턴스 정보 없이 구성 인스턴스 식별자를 수신함
1810
1820
수신된 구성 인스턴스 식별자에서의 구성 변경 횟수 값이 저장된 값과 일치하는가?
아니오
1830
구성 인스턴스에 폐기됨으로서 표시를 함
예
어떤 변경도 행하지 않음
1840

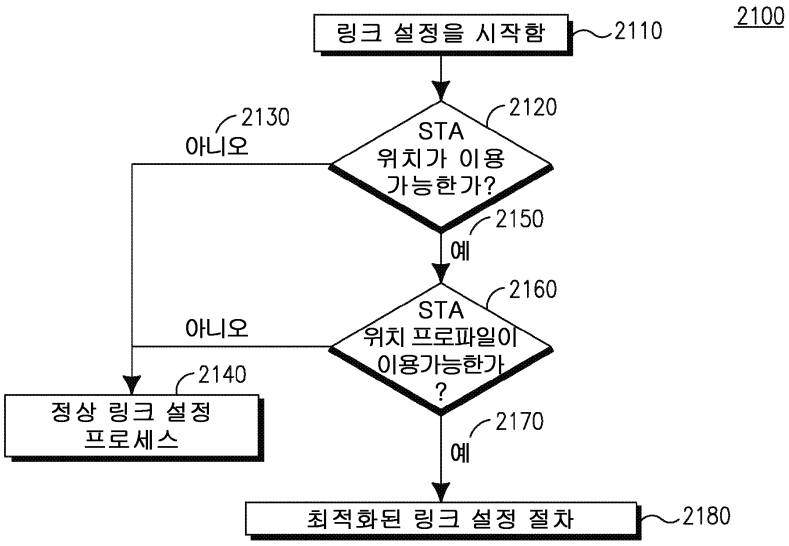
도면19


1900
스캔을 시작함
1910
전체 AP 구성 인스턴스 정보 없이 BSS/AP 구성 변경 횟수 값을 수신함
1920
1930
구성 데이터베이스에 유효한 BSS/AP 항목이 있는가?
아니오
1970
스캔을 계속함
예
1940
수신된 구성 변경 횟수 값이 데이터베이스에 있는 것과 일치하는가?
아니오
예
1950
비콘 또는 프로브 응답을 기다리지 않고 스캔을 완료함
1960
스캔 보고를 작성하기 위해 데이터베이스에 있는 BSS/AP 구성 정보를 사용함

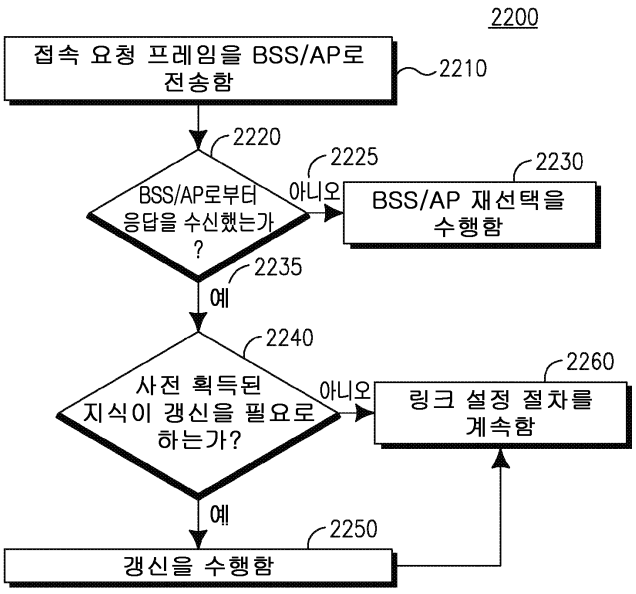
도면20


2000
능동 스캔을 시작함
2010
구성 인스턴스 식별자 정보를 포함하는 감소된 프로브 요청 프레임을 전송함
2020
응답을 수신함
2030
2040
전체, 부분, 또는 감소된 프로브 응답인지를 판정함
2045
감소된
2055
부분
2050
데이터베이스로부터 사전 획득된 지식을 검색함
2060
그에 따라 데이터베이스를 갱신함
2065
전체
2070
수신된 응답에서의 CCC 값이 데이터베이스에 있는 것과 일치하는가 ?
2085
아니오
2075
예
데이터베이스에 어떤 갱신도 없음
2080

도면21


2100
링크 설정을 시작함
2110
2120
STA 위치가 이용 가능한가?
2130
아니오
2150
예
2160
STA 위치 프로파일이 이용가능한가 ?
아니오
2140
정상 링크 설정 프로세스
2170
예
최적화된 링크 설정 절차
2180

도면22


2200
접속 요청 프레임을 BSS/AP로 전송함
2210
2220
BSS/AP로부터 응답을 수신했는가 ?
2225
아니오
2230
BSS/AP 재선택을 수행함
2235
예
2240
사전 획득된 지식이 갱신을 필요로 하는가?
아니오
2260
링크 설정 절차를 계속함
예
2250
갱신을 수행함