(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년09월02일
(11) 등록번호 10-2701924
(24) 등록일자 2024년08월29일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2021.01) *H04L 9/40* (2022.01)
H04W 12/08 (2021.01) *H04W 36/00* (2009.01)
(52) CPC특허분류
H04W 12/04 (2021.01)
H04L 63/061 (2013.01)
(21) 출원번호 10-2018-7025680
(22) 출원일자(국제) 2017년02월23일
심사청구일자 2022년02월07일
(85) 번역문제출일자 2018년09월05일
(65) 공개번호 10-2018-0120696
(43) 공개일자 2018년11월06일
(86) 국제출원번호 PCT/US2017/019203
(87) 국제공개번호 WO 2017/155704
국제공개일자 2017년09월14일
(30) 우선권주장
62/305,770 2016년03월09일 미국(US)
15/281,646 2016년09월30일 미국(US)
(56) 선행기술조사문헌
KR1020080067078 A*
KR1020150097608 A*
US20090054037 A1*
US20140050320 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
팔라니고운데르 아난드
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
말리넨 요우니
미국 92121-1714 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 66 항 심사관 : 이준석

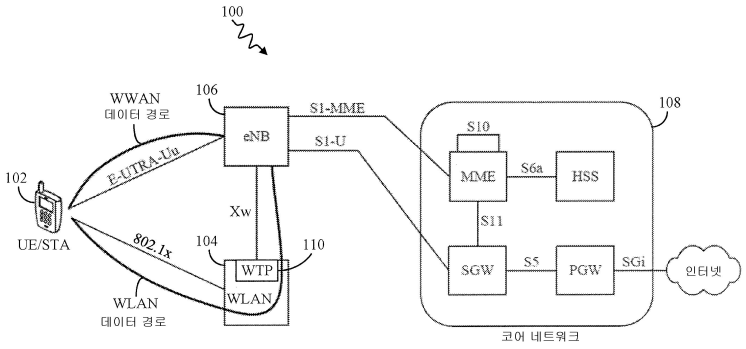
(54) 발명의 명칭 **WWAN-WLAN 집성 보안**

(57) 요 약

하나의 피처는 네트워크의 장치에서 보안 무선 통신을 위한 방법에 관련된다. 방법은 무선 광역 네트워크 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하는 단계, 및 쌍방식 마스터 키 (PMK) 로서 암호 키를 사용하는 단계를 포함한다. PMK 식별자 (PMKID) 는 PMK 에 기초하여 생성되고 이들 둘은 네

(뒷면에 계속)

대 표 도



트워크에 저장된다. PMK 보안 연관은 PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 초기화된다. 사용자 장비로부터 PMKID 를 포함하는 연관 요청이 수신되고, 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것이 결정된다. 사용자 장비와 무선 로컬 영역 네트워크 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환이 개시된다.

(52) CPC특허분류
H04L 63/0876 (2013.01)
H04W 12/08 (2021.01)
H04W 36/0038 (2013.01)
H04W 36/0069 (2023.05)

명 세 서

청구범위

청구항 1

네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법으로서,

상기 WLAN 장치에서, 무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하는 단계;

쌍방식 (pairwise) 마스터 키 (PMK) 로서 상기 암호 키를 사용하는 단계;

상기 WLAN 장치에서, 상기 PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하는 단계;

상기 PMK 및 상기 PMKID 를 저장하는 단계;

상기 PMK 를 적어도 상기 PMKID 및 상기 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 을 초기화하는 단계;

상기 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하는 단계;

상기 사용자 장비로부터 수신된 상기 PMKID 가, 저장된 상기 PMKID 와 매칭하는 것을 결정하는 단계; 및

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하는 단계를 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 2

제 1 항에 있어서,

상기 사용자 장비와의 성공적인 키 교환 후 상기 WLAN 장치와 상기 사용자 장비 사이에서 상기 WLAN 보안 연관이 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 상기 WLAN 장치로부터 상기 WWAN 노드에 송신하는 단계; 및

상기 WLAN 장치를 통해, 상기 WWAN 노드와 상기 사용자 장비 사이에서 송신된 데이터의 적어도 일부분을 송신하는 단계를 더 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 3

제 1 항에 있어서,

상기 사용자 장비 식별자는 상기 사용자 장비의 매체 액세스 제어 (MAC) 어드레스이고 상기 액세스 포인트 식별자는 상기 액세스 포인트의 MAC 어드레스인, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 4

제 1 항에 있어서,

상기 PMKSA 를 초기화하는 단계는, 상기 PMK 를 상기 PMK 의 수명 값 및 적응 키 관리 프로토콜과 연관시키는 단계를 더 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 5

제 1 항에 있어서,

상기 PMKID 는 다음 식에 기초하여 생성되며:

PMKID = 버림 (Truncate) - 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖사용자 장비 식별자)), 여기서 STRING_0 은 문자열인, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 6

제 1 항에 있어서,

상기 암호 키 및 상기 사용자 장비 식별자는 상기 장치의 무선 단말 포인트 (WTP) 에서 상기 WWAN 노드로부터 수신되는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 7

제 6 항에 있어서,

상기 PMKID 를 생성하는 단계, 상기 PMK 및 상기 PMKID 를 저장하는 단계, 상기 PMKSA 를 초기화하는 단계, 및 상기 사용자 장비로부터 수신된 상기 PMKID 가 상기 저장된 PMKID 와 매칭하는 것을 결정하는 단계는, 상기 장치의 상기 액세스 포인트에서 수행되는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 8

무선 로컬 영역 네트워크 (WLAN) 장치로서,

메모리 회로;

무선 광역 네트워크 (WWAN) 노드와 통신하도록 적응된 제 1 통신 인터페이스;

무선 로컬 영역 네트워크 (WLAN) 를 통해 사용자 장비와 통신하도록 적응된 제 2 통신 인터페이스; 및

상기 메모리 회로, 상기 제 1 통신 인터페이스, 및 상기 제 2 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 WWAN 노드로부터 암호 키 및 상기 사용자 장비를 식별하는 사용자 장비 식별자를 수신하고;

쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 사용하고;

상기 WLAN 장치에서, 상기 PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하고;

상기 PMK 및 상기 PMKID 를 상기 메모리 회로에 저장하고;

상기 PMK 를 적어도 상기 PMKID 및 상기 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 을 초기화하고;

상기 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하고;

상기 사용자 장비로부터 수신된 상기 PMKID 가, 상기 메모리 회로에 저장된 상기 PMKID 와 매칭하는 것을 결정하며; 그리고

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 초기화하도록 적응되는, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 9

제 8 항에 있어서,

상기 프로세싱 회로는 또한,

상기 사용자 장비와의 성공적인 키 교환 후 상기 WLAN 장치와 상기 사용자 장비 사이에서 상기 WLAN 보안 연관이 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 상기 WLAN 장치로부터 상기 WWAN 노드에 송신하고; 그리고

상기 WLAN 장치를 통해, 상기 WWAN 노드와 상기 사용자 장비 사이에서 송신된 데이터의 적어도 일부분을 송신하

도록 적응되는, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 10

제 8 항에 있어서,

상기 PMKID 는 다음 식에 기초하여 생성되며:

PMKID = 버림 - 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖사용자 장비 식별자)), 여기서 STRING_0 은 입력 문자열 값인, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 11

제 8 항에 있어서,

상기 암호 키 및 상기 사용자 장비 식별자는 상기 장치의 무선 단말 포인트 (WTP) 에서 상기 WWAN 노드로부터 수신되는, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 12

제 8 항에 있어서,

상기 PMKID 를 생성하고, 상기 PMK 및 상기 PMKID 를 저장하고, 상기 PMKSA 를 초기화하며, 그리고 상기 사용자 장비로부터 수신된 상기 PMKID 가 상기 메모리 회로에 저장된 PMKID 와 매칭하는 것을 결정하도록 적응된 상기 프로세싱 회로는, 상기 액세스 포인트의 프로세싱 회로에서 수행되는, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 13

무선 로컬 영역 네트워크 (WLAN) 장치로서,

상기 WLAN 장치에서, 무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하기 위한 수단;

쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 사용하기 위한 수단;

상기 WLAN 장치에서, 상기 PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하기 위한 수단;

상기 PMK 및 상기 PMKID 를 저장하기 위한 수단;

상기 PMK 를 적어도 상기 PMKID 및 상기 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 을 초기화하기 위한 수단;

상기 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하기 위한 수단;

상기 사용자 장비로부터 수신된 상기 PMKID 가, 저장된 상기 PMKID 와 매칭하는 것을 결정하기 위한 수단; 및

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하기 위한 수단을 포함하는, 무선 로컬 영역 네트워크 (WLAN) 장치.

청구항 14

네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하게 하고;

쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 사용하게 하고;

상기 WLAN 장치에서, 상기 PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하게 하고;

상기 PMK 및 상기 PMKID 를 저장하게 하고;

상기 PMK 를 적어도 상기 PMKID 및 상기 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는

것에 의해 PMK 보안 연관 (PMKSA) 을 초기화하게 하고;

상기 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하게 하고;

상기 사용자 장비로부터 수신된 상기 PMKID 가, 저장된 상기 PMKID 와 매칭하는 것을 결정하게 하며; 그리고

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 15

네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법으로서,

무선 로컬 영역 네트워크 (WLAN) 장치에서, 무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 단계로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하는 단계;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하는 단계;

상기 네트워크 생성 제 1 식별자를 상기 장치에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키는 단계;

상기 네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하는 단계로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하는 단계;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하는 단계;

마스터 세션 키 (MSK) 를 생성하는 단계; 및

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하는 단계를 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 16

제 15 항에 있어서,

상기 네트워크 생성 제 1 식별자 및 상기 사용자 장비 생성 제 1 식별자는 SHA-256 (암호 키, 사용자 장비 식별자, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 17

제 15 항에 있어서,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자를 수신하는 상기 장치를 식별하는 영역 (realm) 값을 포함하고, 상기 영역 값은 또한 상기 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 18

제 15 항에 있어서,

상기 사용자 장비와 WLAN 보안 연관이 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 상기 WWAN 노드에 송신하는 단계; 및

상기 WWAN 노드와 상기 사용자 장비 사이에서 데이터를 송신하는 단계를 더 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 19

제 15 항에 있어서,

상기 액세스 포인트에 EAP 도전 메시지를 송신하는 단계로서, 상기 EAP 도전 메시지는 목적지가 상기 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하는 단계;

상기 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하는 단계로서, 상기 EAP 도전 응답 메시지는 상기 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하는 단계;

상기 인증 값, 상기 제 1 랜덤 값, 및 상기 제 2 랜덤 값을 사용하여 상기 EAP 도전 응답 메시지를 검증하는 단계; 및

상기 EAP 도전 응답 메시지를 검증한 후 상기 MSK 를 생성하는 단계를 더 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 20

제 19 항에 있어서,

상기 제 1 랜덤 값 및 상기 제 2 랜덤 값은 128 비트 값들인, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 21

제 19 항에 있어서,

상기 EAP 도전 응답 메시지를 검증하는 단계는,

상기 장치에서 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_1) 과 동일한 AUTHRES 값을 생성하는 단계 (여기서, STRING_1 은 입력 문자열 값이다); 및

상기 AUTHRES 값이, 수신된 상기 인증 값과 매칭하는 것을 결정하는 단계를 포함하는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 22

제 19 항에 있어서,

상기 MSK 는 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_2) 과 동일하고, 여기서 STRING_2 은 입력 문자열 값인, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 23

제 19 항에 있어서,

상기 액세스 포인트에 송신된 상기 EAP 도전 메시지는 인증, 인가, 및 계정 (authentication, authorization, and accounting; AAA) 스킴에 따라 송신되고, 상기 EAP 도전 응답 메시지는 상기 인증, 인가, 및 계정 (AAA) 스킴에 따라 상기 액세스 포인트로부터 수신되는, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 장치에서 보안 무선 통신을 위한 방법.

청구항 24

장치로서,

네트워크와 연관된 장치를 포함하고,

메모리 회로:

무선 광역 네트워크 (WWAN) 노드와 통신하도록 적응된 제 1 통신 인터페이스;

액세스 포인트와 통신하도록 적응된 제 2 통신 인터페이스; 및

상기 메모리 회로, 상기 제 1 통신 인터페이스 및 상기 제 2 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 WWAN 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 것으로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하고;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하고;

상기 네트워크 생성 제 1 식별자를 상기 메모리 회로에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키고;

상기 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하는 것으로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하고;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하고;

마스터 세션 키 (MSK) 를 생성하며; 그리고

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하도록 적응되는, 장치.

청구항 25

제 24 항에 있어서,

상기 네트워크 생성 제 1 식별자 및 상기 사용자 장비 생성 제 1 식별자는 SHA-256 (암호 키, 사용자 장비 식별자, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 장치.

청구항 26

제 24 항에 있어서,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자를 수신하는 상기 장치를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한 상기 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 장치.

청구항 27

제 24 항에 있어서,

상기 프로세싱 회로는 또한,

상기 사용자 장비와 WLAN 보안 연관이 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 상기 WWAN 노드에 송신하고; 그리고

상기 WWAN 노드와 상기 사용자 장비 사이에서 데이터를 송신하도록 적응되는, 장치.

청구항 28

제 24 항에 있어서,

상기 프로세싱 회로는 또한,

상기 액세스 포인트에 EAP 도전 메시지를 송신하는 것으로서, 상기 EAP 도전 메시지는 목적지가 상기 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하고;

상기 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하는 것으로서, 상기 EAP 도전 응답 메시지는 상기 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하고;

상기 인증 값, 상기 제 1 랜덤 값, 및 상기 제 2 랜덤 값을 사용하여 상기 EAP 도전 응답 메시지를 검증하며; 그리고

상기 EAP 도전 응답 메시지를 검증한 후 상기 MSK 를 생성하도록 적응되는, 장치.

청구항 29

제 28 항에 있어서,

상기 EAP 도전 응답 메시지를 검증하도록 적응된 상기 프로세싱 회로는,

상기 장치에서 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_1) 과 동일한 AUTHRES 값을 생성하는 것으로서, STRING_1 은 입력 문자열 값이고, 상기 제 1 랜덤 값 및 상기 제 2 랜덤 값은 128 비트 값들인, 상기 AUTHRES 값을 생성하고; 그리고

상기 AUTHRES 값이, 수신된 상기 인증 값과 매칭하는 것을 결정하도록 적응된, 상기 프로세싱 회로를 포함하는, 장치.

청구항 30

제 28 항에 있어서,

상기 MSK 는 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_2) 와 동일하고, 여기서 STRING_2 은 입력 문자열 값인, 장치.

청구항 31

제 28 항에 있어서,

상기 액세스 포인트에 송신된 상기 EAP 도전 메시지는 인증, 인가, 및 계정 (AAA) 스킴에 따라 송신되고, 상기 EAP 도전 응답 메시지는 상기 인증, 인가, 및 계정 (AAA) 스킴에 따라 상기 액세스 포인트로부터 수신되는, 장치.

청구항 32

장치로서,

무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하기 위한 수단으로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하기 위한 수단;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하기 위한 수단;

상기 네트워크 생성 제 1 식별자를 상기 장치에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키기 위한 수단;

액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하기 위한 수단으로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하기 위한 수단;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하기 위한 수단;

마스터 세션 키 (MSK) 를 생성하기 위한 수단; 및

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하기 위한 수단을 포함하는, 장치.

청구항 33

제 32 항에 있어서,

상기 액세스 포인트에 EAP 도전 메시지를 송신하기 위한 수단으로서, 상기 EAP 도전 메시지는 목적지가 상기 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하기 위한 수단;

상기 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하기 위한 수단으로서, 상기 EAP 도전 응답 메시지는 상기 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하기 위한 수단;

상기 인증 값, 상기 제 1 랜덤 값, 및 상기 제 2 랜덤 값을 사용하여 상기 EAP 도전 응답 메시지를 검증하기 위한 수단; 및

상기 EAP 도전 응답 메시지를 검증한 후 상기 MSK 를 생성하기 위한 수단을 더 포함하는, 장치.

청구항 34

네트워크와 연관된 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하게 하는 것으로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하게 하고;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하게 하고;

상기 네트워크 생성 제 1 식별자를 상기 장치에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키게 하고;

상기 네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하게 하는 것으로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하게 하고;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하게 하고;

마스터 세션 키 (MSK) 를 생성하게 하며; 그리고

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 35

제 34 항에 있어서,

상기 명령들은, 상기 프로세서에 의해 실행될 때, 추가로 상기 프로세서로 하여금,

상기 액세스 포인트에 EAP 도전 메시지를 송신하게 하는 것으로서, 상기 EAP 도전 메시지는 목적지가 상기 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하게 하고;

상기 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하게 하는 것으로서, 상기 EAP 도전 응답 메시지는 상기 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하게 하고;

상기 인증 값, 상기 제 1 랜덤 값, 및 상기 제 2 랜덤 값을 사용하여 상기 EAP 도전 응답 메시지를 검증하게 하며; 그리고

상기 EAP 도전 응답 메시지를 검증한 후 상기 MSK 를 생성하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 36

네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법으로서,

쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하는 단계;

상기 PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 상기 장치에 저장되지 않는 것을 결정하는 단계;

상기 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하는 단계;

상기 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하는 단계;

상기 장치와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 상기 사용자 장비 생성 제 1 식별자를 송신하는 단계;

상기 WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하는 단계;

상기 MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하는 단계; 및

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하는 단계를 포함하고,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자가 송신되는 상기 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한 상기 WLAN 단말 포인트와 통신하는 무선 광역 네트워크 (WWAN) 노드의 서빙 네트워크 아이덴티티를 식별하는, 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법.

청구항 37

제 36 항에 있어서,

상기 사용자 장비 생성 제 1 식별자는 SHA-256 (암호 키, 사용자 장비 식별자, STRING_0) 과 동일하고, 여기서 SHA 는 보안 해시 알고리즘 (Secure Hash Algorithm) 을 의미하고, STRING_0 은 입력 문자열 값인, 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법.

청구항 38

삭제

청구항 39

제 36 항에 있어서,

상기 방법은,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 WLAN 단말 포인트로부터 수신하는 단계;

상기 사용자 장비에 상기 EAP 도전 메시지를 송신하는 단계;

제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 상기 사용자 장비로부터 수신하는 단계; 및

상기 WLAN 단말 포인트에 상기 EAP 도전 응답 메시지를 송신하는 단계를 더 포함하는, 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법.

청구항 40

제 39 항에 있어서,

상기 사용자 장비에 송신된 상기 EAP 도전 메시지는 인증, 인가 및 계정 (AAA) 스킴에 따라 송신되고, 상기 EAP 도전 응답 메시지는 상기 인증, 인가 및 계정 (AAA) 스킴에 따라 상기 사용자 장비로부터 수신되는, 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법.

청구항 41

장치로서,

메모리 회로;

사용자 장비 및 무선 로컬 영역 네트워크 (WLAN) 단말 포인트와 통신하도록 적응된 통신 인터페이스; 및

상기 메모리 회로 및 상기 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 상기 사용자 장비로부터 수신하고;

상기 PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 상기 메모리 회로에 저장되지 않는 것을 결정하고;

상기 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하고;

상기 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하고;

상기 장치와 연관된 상기 WLAN 단말 포인트에 상기 사용자 장비 생성 제 1 식별자를 송신하고;

상기 WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하고;

상기 MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하며; 그리고

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하도록 적응되고,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자가 송신되는 상기 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한 상기 WLAN 단말 포인트와 통신하는 무선 광역 네트워크 (WWAN) 노드의 서빙 네트워크 아이덴티티를 식별하는, 장치.

청구항 42

제 41 항에 있어서,

상기 사용자 장비 생성 제 1 식별자는 SHA-256 (암호 키, 사용자 장비 식별자, STRING_0) 과 동일하고, 여기서 SHA 는 보안 해시 알고리즘 (Secure Hash Algorithm) 을 의미하고, STRING_0 은 입력 문자열 값인, 장치.

청구항 43

삭제

청구항 44

제 41 항에 있어서,

상기 프로세싱 회로는 또한,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 WLAN 단말 포인트로부터 수신하고;

상기 사용자 장비에 상기 EAP 도전 메시지를 송신하고;

제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 상기 사용자 장비로부터 수신하고; 그리고

상기 WLAN 단말 포인트에 상기 EAP 도전 응답 메시지를 송신하도록 적응되는, 장치.

청구항 45

제 44 항에 있어서,

상기 사용자 장비에 송신된 상기 EAP 도전 메시지는 인증, 인가 및 계정 (AAA) 스킴에 따라 송신되고, 상기 EAP 도전 응답 메시지는 상기 인증, 인가 및 계정 (AAA) 스킴에 따라 상기 사용자 장비로부터 수신되는, 장치.

청구항 46

장치로서,

쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하기 위한 수단;

상기 PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 상기 장치에 저장되지 않는 것을 결정하기 위한 수단;

상기 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하기 위한 수단;

상기 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하기 위한 수단;

상기 장치와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 상기 사용자 장비 생성 제 1 식별자를 송신하기 위한 수단;

상기 WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하기 위한 수단;

상기 MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하기 위한 수단; 및

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개

시하기 위한 수단을 포함하고,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자가 송신되는 상기 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한 상기 WLAN 단말 포인트와 통신하는 무선 광역 네트워크 (WWAN) 노드의 서빙 네트워크 아이덴티티를 식별하는, 장치.

청구항 47

제 46 항에 있어서,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 WLAN 단말 포인트로부터 수신하기 위한 수단;

상기 사용자 장비에 상기 EAP 도전 메시지를 송신하기 위한 수단;

제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 상기 사용자 장비로부터 수신하기 위한 수단; 및

상기 WLAN 단말 포인트에 상기 EAP 도전 응답 메시지를 송신하기 위한 수단을 더 포함하는, 장치.

청구항 48

네트워크와 연관된 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하게 하고;

상기 PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 상기 네트워크에 저장되지 않는 것을 결정하게 하고;

상기 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하게 하고;

상기 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하게 하고;

상기 장치와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 상기 사용자 장비 생성 제 1 식별자를 송신하게 하고;

상기 WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하게 하고;

상기 MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하게 하며; 그리고

상기 사용자 장비와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 사용자 장비와의 키 교환을 개시하게 하고,

상기 EAP 아이덴티티 응답은 상기 사용자 장비 생성 제 1 식별자가 송신되는 상기 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한 상기 WLAN 단말 포인트와 통신하는 무선 광역 네트워크 (WWAN) 노드의 서빙 네트워크 아이덴티티를 식별하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 49

제 48 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 추가로 상기 프로세서로 하여금,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 WLAN 단말 포인트로부터 수신하게 하고;

상기 사용자 장비에 상기 EAP 도전 메시지를 송신하게 하고;

제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 상기 사용자 장비로부터 수신하게 하며; 그리고

상기 WLAN 단말 포인트에 상기 EAP 도전 응답 메시지를 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 50

디바이스에 의한 보안 무선 통신을 위한 방법으로서,

무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하는 단계;

무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 활용하는 단계;

상기 PMK, 상기 디바이스를 식별하는 디바이스 식별자, 및 상기 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하는 단계;

상기 액세스 포인트에 상기 PMKID 를 포함하는 연관 요청을 송신하는 단계;

상기 PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 상기 AP 로부터 수신하는 단계;

상기 AP 로부터 EAP 아이덴티티 요청을 수신하는 단계;

상기 EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하는 단계로서, 상기 EAP 아이덴티티 응답은 상기 암호 키 및 상기 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하는 단계; 및

상기 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 액세스 포인트와의 키 교환을 개시하는 단계를 포함하고,

상기 EAP 아이덴티티 응답은 상기 디바이스 생성 제 1 식별자가 라우팅되는 상기 WLAN 의 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한, 상기 WLAN 단말 포인트와 연관된 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 51

제 50 항에 있어서,

상기 디바이스 식별자는 상기 디바이스의 매체 액세스 제어 (MAC) 어드레스이고 상기 액세스 포인트 식별자는 상기 액세스 포인트의 MAC 어드레스인, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 52

제 50 항에 있어서,

상기 PMKID 는 다음 식에 기초하여 생성되며:

PMKID = 버림 - 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖디바이스 식별자)), 여기서 STRING_0 은 입력 문자열인, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 53

제 50 항에 있어서,

상기 방법은,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 AP 로부터 수신하는 단계;

제 2 랜덤 값 및 인증 값을 생성하는 단계로서, 상기 인증 값은 상기 암호 키, 상기 제 1 랜덤 값 및 상기 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하는 단계; 및

상기 인증 값 및 상기 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 상기 AP 에 송신하는 단계를 더 포함하는, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 54

제 53 항에 있어서,

상기 디바이스 생성 제 1 식별자는 SHA-256 (암호 키, 디바이스 식별자, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 55

제 53 항에 있어서,

상기 제 1 랜덤 값 및 상기 제 2 랜덤 값은 128 비트 값들인, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 56

제 53 항에 있어서,

상기 인증 값은 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 57

삭제

청구항 58

제 53 항에 있어서,

상기 EAP 도전 메시지는 인증, 인가, 및 계정 (AAA) 스킴에 따라 수신되고, 상기 EAP 도전 응답 메시지는 상기 AAA 스킴에 따라 송신되는, 디바이스에 의한 보안 무선 통신을 위한 방법.

청구항 59

보안 무선 통신을 위한 디바이스로서,

무선 통신 인터페이스;

상기 무선 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하고;

무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 활용하고;

상기 PMK, 상기 디바이스를 식별하는 디바이스 식별자, 및 상기 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하고;

상기 액세스 포인트에 상기 PMKID 를 포함하는 연관 요청을 송신하며;

상기 PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 상기 AP 로부터 수신하고;

상기 AP 로부터 EAP 아이덴티티 요청을 수신하고;

상기 EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하는 것으로서, 상기 EAP 아이덴티티 응답은 상기 암호 키 및 상기 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하고; 그리고

상기 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 액세스 포인트와의 키 교환을 개시하도록 적응되고,

상기 EAP 아이덴티티 응답은 상기 디바이스 생성 제 1 식별자가 라우팅되는 상기 WLAN 의 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한, 상기 WLAN 단말 포인트와 연관된 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 보안 무선 통신을 위한 디바이스.

청구항 60

제 59 항에 있어서,

상기 디바이스 식별자는 상기 디바이스의 매체 액세스 제어 (MAC) 어드레스이고 상기 액세스 포인트 식별자는

상기 액세스 포인트의 MAC 어드레스인, 보안 무선 통신을 위한 디바이스.

청구항 61

제 59 항에 있어서,

상기 PMKID 는 다음 식에 기초하여 생성되며:

PMKID = 버림 - 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖디바이스 식별자)), 여기서 STRING_0 은 입력 문자열인, 보안 무선 통신을 위한 디바이스.

청구항 62

제 59 항에 있어서,

상기 프로세싱 회로는 또한,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 AP 로부터 수신하고;

제 2 랜덤 값 및 인증 값을 생성하는 것으로서, 상기 인증 값은 상기 암호 키, 상기 제 1 랜덤 값 및 상기 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하며; 그리고

상기 인증 값 및 상기 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 상기 AP 에 송신하도록 적응되는, 보안 무선 통신을 위한 디바이스.

청구항 63

제 62 항에 있어서,

상기 디바이스 생성 제 1 식별자는 SHA-256 (암호 키, 디바이스 식별자, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 보안 무선 통신을 위한 디바이스.

청구항 64

제 62 항에 있어서,

상기 인증 값은 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_0) 과 동일하고, 여기서 STRING_0 은 입력 문자열 값인, 보안 무선 통신을 위한 디바이스.

청구항 65

삭제

청구항 66

제 62 항에 있어서,

상기 EAP 도전 메시지는 인증, 인가, 및 계정 (AAA) 스킴에 따라 수신되고, 상기 EAP 도전 응답 메시지는 상기 AAA 스킴에 따라 송신되는, 보안 무선 통신을 위한 디바이스.

청구항 67

보안 무선 통신을 위한 디바이스로서,

무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하기 위한 수단;

무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 활용하기 위한 수단;

상기 PMK, 상기 디바이스를 식별하는 디바이스 식별자, 및 상기 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하기 위한 수단;

상기 액세스 포인트에 상기 PMKID 를 포함하는 연관 요청을 송신하기 위한 수단;

상기 PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 상기 AP 로부터 수신

하기 위한 수단;

상기 AP 로부터 EAP 아이덴티티 요청을 수신하기 위한 수단;

상기 EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하기 위한 수단으로서, 상기 EAP 아이덴티티 응답은 상기 암호 키 및 상기 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하기 위한 수단; 및

상기 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 액세스 포인트와의 키 교환을 개시하기 위한 수단을 포함하고,

상기 EAP 아이덴티티 응답은 상기 디바이스 생성 제 1 식별자가 라우팅되는 상기 WLAN 의 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한, 상기 WLAN 단말 포인트와 연관된 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 보안 무선 통신을 위한 디바이스.

청구항 68

제 67 항에 있어서,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 AP 로부터 수신하기 위한 수단;

제 2 랜덤 값 및 인증 값을 생성하기 위한 수단으로서, 상기 인증 값은 상기 암호 키, 상기 제 1 랜덤 값 및 상기 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하기 위한 수단; 및

상기 인증 값 및 상기 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 상기 AP 에 송신하기 위한 수단을 더 포함하는, 보안 무선 통신을 위한 디바이스.

청구항 69

디바이스에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하게 하고;

무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 상기 암호 키를 활용하게 하고;

상기 PMK, 상기 디바이스를 식별하는 디바이스 식별자, 및 상기 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하게 하고;

상기 액세스 포인트에 상기 PMKID 를 포함하는 연관 요청을 송신하게 하며;

상기 PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 상기 AP 로부터 수신하게 하고;

상기 AP 로부터 EAP 아이덴티티 요청을 수신하게 하고;

상기 EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하게 하는 것으로서, 상기 EAP 아이덴티티 응답은 상기 암호 키 및 상기 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하게 하고; 그리고

상기 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 상기 PMK 에 기초하여 상기 액세스 포인트와의 키 교환을 개시하게 하고,

상기 EAP 아이덴티티 응답은 상기 디바이스 생성 제 1 식별자가 라우팅되는 상기 WLAN 의 WLAN 단말 포인트를 식별하는 영역 값을 포함하고, 상기 영역 값은 또한, 상기 WLAN 단말 포인트와 연관된 WWAN 노드의 서빙 네트워크 아이덴티티를 식별하는, 비일시적 컴퓨터 판독가능 저장 매체.

청구항 70

제 69 항에 있어서,

상기 명령들은 상기 프로세서에 의해 실행될 때, 추가로 상기 프로세서로 하여금,

제 1 랜덤 값을 포함하는 EAP 도전 메시지를 상기 AP 로부터 수신하게 하고;

제 2 랜덤 값 및 인증 값을 생성하게 하는 것으로서, 상기 인증 값은 상기 암호 키, 상기 제 1 랜덤 값 및 상기 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하게 하며; 그리고

상기 인증 값 및 상기 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 상기 AP 에 송신하게 하는, 비일시적 컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] **관련 출원들에 대한 상호 참조**

[0002] 이 출원은 2016 년 3 월 9 일에 미국특허청 (USPTO) 에 출원된 가출원 제 62/305,770 호 및 2016 년 9 월 30 일에 미국특허청 (USPTO) 에 출원된 정규출원 제 15/281,646 호의 우선권 및 이익을 주장하며, 이들 전체 내용은 본 명세서에 참조로 통합된다.

[0003] **분야**

[0004] 본 개시물의 다양한 양태들은 무선 통신에 관한 것이며, 특히 무선 광역 네트워크 (WWAN) 무선 로컬 영역 네트워크 (WLAN) 집성을 채용하는 통신 컴포넌트들에 보안을 제공하기 위한 방법들, 장치들, 및 시스템들에 관한 것이다.

배 경 기 술

[0005] 최근, 모바일 디바이스의 사용량은 매년 거의 두 배씩 기하급수적으로 증가하고 있다. 셀룰러 기술에서의 진보가 셀룰러 네트워크의 성능 및 용량을 증가시키고 있지만, 이것이 단독으로 모바일 데이터에 대한 수요를 충족시키기에 충분하지 않을 것임이 예측된다. 비인가 (unlicensed) 스펙트럼을 사용하면 셀룰러 오퍼레이터들이 네트워크 데이터 용량을 증가시킴으로써 가입자들을 도울 수 있는 탁월한 기회를 제공한다.

[0006] 셀룰러 오퍼레이터들에 의해 비허가 스펙트럼으로 데이터를 오프로딩하기 위한 전형적인 방법은 802.1x 기반 WLAN 네트워크들을 사용하는 것이었다. 이들 네트워크들은 셀룰러 오퍼레이터들 자신 또는 다른 것들에 의해 배치될 수도 있다. WLAN 오프로딩에 대해 아키텍처 프레임워크 (architectural framework) 및 표준화를 제공하기 위해, 표준화 기구는 WLAN 과의 상호연동 (interworking) 을 가능하게 하고 WLAN 에 데이터 베어러들의 스위칭을 통해 데이터 오프로딩을 제공하는 몇몇 솔루션들을 개발하고 있다.

[0007] WWAN (예를 들어, 롱텀 에볼루션 (long term evolution; LTE) 네트워크) 및 WLAN 상호연동에 대한 하나의 옵션은 무선 액세스 네트워크 (RAN) 에서의 데이터 집성이다. 본 명세서에서 LTE-WLAN 집성 또는 LWA 로 지칭될 수도 있는 이러한 데이터 집성은 LTE 및 WLAN (예를 들어, Wi-Fi®) 무선 링크들 상에 서빙될 진화된 노드B (Evolved NodeB; eNB) 스케줄링 패킷들을 수반한다.

[0008] 이러한 방법의 하나의 이점은 LTE 및 WLAN 링크들 양자 모두 상에서 리소스들의 우수한 활용/제어를 제공할 수도 있다는 것이다. 이것은 모든 디바이스들/사용자들에 대한 집성 스루풋을 증가시키고 디바이스들/사용자들 사이에서 무선 리소스들을 더 잘 관리함으로써 총 시스템 용량을 개선할 수 있다. 각각의 링크에 대한 스케줄링 판정들은 실시간 채널 조건들 및 시스템 리소스 가용성에 기초하여 패킷 레벨에서 이루어질 수 있다.
또한, WLAN 무선 링크가 E-UTRAN (Enhanced Universal Terrestrial Radio Access Network) 의 부분이 되기 때문에, RAN 에서의 데이터 집성은 코어 네트워크에 대한 어떠한 변경없이 구현될 수 있다.

[0009] 앞서 언급한 LWA 의 이점들과 함께 데이터 보안에 대한 새로운 우려가 있다. 이제 WWAN 및 WLAN 링크들을 통해 전송되는 데이터를 보호하려는 주의가 취해져야 한다. 이러한 LWA 시스템들에서 사용자 디바이스들과 WWAN 및 WLAN 네트워크 컴포넌트들 사이의 통신들을 보안하는 방법들, 장치들 및 시스템들에 대한 필요가 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0010] 하나의 피처는 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법을 제공하며, 방법은, 무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하는 단계, 쌍방식 마스터 키 (pairwise master key; PMK) 로서 암호 키를 사용하는 단계, PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하는 단계, PMK 및 PMKID 를 저장하는 단계, PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 를 초기화하는 단계, 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하는 단계, 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하는 단계, 및 사용자 장비와 무선 로컬 영역 네트워크 (WLAN) 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하는 단계를 포함한다. 일 양태에 따라, 방법은 사용자 장비와의 성공적인 키 교환 후 WLAN 보안 연관이 사용자 장비와 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 WWAN 노드에 송신하는 단계를 더 포함한다. 다른 양태에 따라, 사용자 장비 식별자는 사용자 장비의 매체 액세스 제어 (MAC) 어드레스이고 액세스 포인트 식별자는 액세스 포인트의 MAC 어드레스이다.

[0011] 일 양태에 따라, PMKSA 를 초기화하는 단계는, PMK 를 PMK 의 수명 값 및 적응 키 관리 프로토콜과 연관시키는 단계를 더 포함한다. 다른 양태에 따라, PMKID 는 다음 식에 기초하여 생성되며: PMKID = 버림 (Truncate) - 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖사용자 장비 식별자)), 여기서 STRING_0 은 문자열이다. 또 다른 양태에 따라, 암호 키 및 사용자 장비 식별자는 장치의 무선 단말 포인트 (WTP) 에서 WWAN 노드로부터 수신된다. 또 다른 양태에 따라, PMKID 를 생성하는 단계, PMK 및 PMKID 를 저장하는 단계, PMKSA 를 초기화하는 단계, 및 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하는 단계는 장치의 액세스 포인트에서 수행된다.

[0012] 다른 피처는 장치를 제공하며, 장치는 메모리 회로, 무선 광역 네트워크 (WWAN) 노드 및 사용자 장비와 통신하도록 적응된 통신 인터페이스, 및 메모리 회로 및 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고, 프로세싱 회로는, WWAN 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하고, 쌍방식 마스터 키 (PMK) 로서 암호 키를 사용하고, PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하고, PMK 및 PMKID 를 메모리 회로에 저장하고, PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 를 초기화하고, 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하고, 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하며, 그리고 사용자 장비와 무선 로컬 영역 네트워크 (WLAN) 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 초기화하도록 적응된다. 일 양태에 따라, 프로세싱 회로는 또한, 사용자 장비와의 성공적인 키 교환 후 WLAN 보안 연관이 사용자 장비와 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 WWAN 노드에 송신하도록 적응된다. 일 양태에 따라, 프로세싱 회로는, PMKID 를 생성하는 것, PMK 및 PMKID 를 저장하는 것, PMKSA 를 초기화하는 것, 및 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하는 것이, 액세스 포인트의 프로세싱 회로에서 수행되도록 적응된다.

[0013] 다른 피처는 장치를 제공하며, 장치는, 무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하기 위한 수단, 쌍방식 마스터 키 (PMK) 로서 암호 키를 사용하기 위한 수단, PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하기 위한 수단, PMK 및 PMKID 를 저장하기 위한 수단, PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 를 초기화하기 위한 수단, 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하기 위한 수단, 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하기 위한 수단, 및 사용자 장비와 무선 로컬 영역 네트워크 (WLAN) 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하기 위한 수단을 포함한다.

[0014] 다른 피처는 네트워크와 연관된 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신하게 하고, 쌍방식 마스터 키 (PMK) 로서 암호 키를 사용하게 하고, PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하게 하고, PMK 및 PMKID 를 저장하게 하고, PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 를 초기화하게 하고, 사용자 장비로부터 PMKID 를 포함하는 연관 요청을 수신하게 하고, 사용자 장비로부터 수신된 PMKID 가, 저장된 PMKID 와 매칭하는 것을 결정하게 하며, 그리고 사용자 장비와 무선 로컬 영역 네트워크 (WLAN) 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와

의 키 교환을 개시하게 한다.

[0015] 다른 피처는 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법을 제공하며, 방법은, 무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 단계로서, WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하는 단계, WWAN 노드로부터 수신된 암호 키 및 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하는 단계, 네트워크 생성 제 1 식별자를 장치에 저장하고 네트워크 생성 제 1 식별자를 암호 키와 연관시키는 단계, 네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 ((Extensible Authentication Protocol; EAP) 아이덴티티 응답을 수신하는 단계로서, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하는 단계, 사용자 장비 생성 제 1 식별자가, 저장된 네트워크 생성 제 1 식별자에 대응하는 것을 결정하는 단계, 마스터 세션 키 (MSK) 를 생성하는 단계, 및 EAP 성공 메시지 및 MSK 를 액세스 포인트에 송신하는 단계를 포함한다. 일 양태에 따라, 네트워크 생성 제 1 식별자 및 사용자 장비 생성 제 1 식별자는 SHA-256 (암호 키, 사용자 장비 식별자, STRING_0) 와 동일하고, 여기서 STRING_0 은 입력 문자열 값이다. 다른 양태에 따라, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 수신하는 장치를 식별하는 영역 값을 포함하고, 영역 값은 또한 WWAN 노드의 서빙 네트워크 아이덴티티를 식별한다.

[0016] 일 양태에 따라, 방법은 사용자 장비와 WLAN 보안 연관이 확립되었다는 것을 표시하는 보안 연관 확인 메시지를 WWAN 노드에 송신하는 단계를 더 포함한다. 다른 양태에 따라, 방법은 액세스 포인트에 EAP 도전 메시지를 송신하는 단계로서, EAP 도전 메시지는 목적지가 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하는 단계, 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하는 단계로서, EAP 도전 응답 메시지는 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하는 단계, 인증 값, 제 1 랜덤 값, 및 제 2 랜덤 값을 사용하여 EAP 도전 응답 메시지를 검증하는 단계, 및 EAP 도전 응답 메시지를 검증한 후 MSK 를 생성하는 단계를 더 포함한다. 또 다른 양태에 따라, EAP 도전 응답 메시지를 검증하는 단계는, 장치에서 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_1) 과 동일한 AUTHRES 값을 생성하는 단계 (여기서, STRING_1 은 입력 문자열 값이다), 및 AUTHRES 값이, 수신된 인증 값과 매칭하는 것을 결정하는 단계를 포함한다.

[0017] 일 양태에 따라, MSK 는 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_2) 과 동일하고, 여기서 STRING_2 은 입력 문자열 값이다. 다른 양태에 따라, 액세스 포인트에 송신된 EAP 도전 메시지는 인증, 인가, 및 계정 (authentication, authorization, and accounting; AAA) 스킴에 따라 송신되고, EAP 도전 응답 메시지는 인증, 인가, 및 계정 (AAA) 스킴에 따라 액세스 포인트로부터 수신된다.

[0018] 다른 피처는 장치를 제공하며, 장치는 메모리 회로, 무선 광역 네트워크 (WWAN) 노드 및 액세스 포인트와 통신하도록 적응된 통신 인터페이스, 및 메모리 회로 및 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고, 프로세싱 회로는, WWAN 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 것으로서, WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하고, WWAN 노드로부터 수신된 암호 키 및 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하고, 네트워크 생성 제 1 식별자를 장치에 저장하고 네트워크 생성 제 1 식별자를 암호 키와 연관시키고, 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하는 것으로서, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하고, 사용자 장비 생성 제 1 식별자가, 저장된 네트워크 생성 제 1 식별자에 대응하는 것을 결정하고, 마스터 세션 키 (MSK) 를 생성하며, 그리고 EAP 성공 메시지 및 MSK 를 액세스 포인트에 송신하도록 구성된다. 일 양태에 따라, 프로세싱 회로는 또한, 액세스 포인트에 EAP 도전 메시지를 송신하는 것으로서, EAP 도전 메시지는 목적지가 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하고, 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하는 것으로서, EAP 도전 응답 메시지는 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하고, 인증 값, 제 1 랜덤 값, 및 제 2 랜덤 값을 사용하여 EAP 도전 응답 메시지를 검증하며, 그리고 EAP 도전 응답 메시지를 검증한 후 MSK 를 생성하도록 적응된다.

[0019] 일 양태에 따라, EAP 도전 응답 메시지를 검증하도록 적응된 프로세싱 회로는, 장치에서 SHA-256 (암호 키, 제 1 랜덤 값, 제 2 랜덤 값, STRING_1) 과 동일한 AUTHRES 값을 생성하고 (여기서, STRING_1 은 입력 문자열 값이고, 제 1 랜덤 값 및 제 2 랜덤 값은 128 비트 값이다), 그리고 AUTHRES 값이, 수신된 인증 값과 매칭하는 것

을 결정하도록 적응된 프로세싱 회로를 포함한다.

[0020] 다른 피처는 장치를 제공하며, 장치는, 무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하기 위한 수단으로서, WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하기 위한 수단, WWAN 노드로부터 수신된 암호 키 및 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하기 위한 수단, 네트워크 생성 제 1 식별자를 장치에 저장하고 네트워크 생성 제 1 식별자를 암호 키와 연관시키기 위한 수단, 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하기 위한 수단으로서, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하기 위한 수단, 사용자 장비 생성 제 1 식별자가, 저장된 네트워크 생성 제 1 식별자에 대응하는 것을 결정하기 위한 수단, 마스터 세션 키 (MSK) 를 생성하기 위한 수단, 및 EAP 성공 메시지 및 MSK 를 액세스 포인트에 송신하기 위한 수단을 포함한다. 일 양태에 따라, 장치는 액세스 포인트에 EAP 도전 메시지를 송신하기 위한 수단으로서, EAP 도전 메시지는 목적지가 사용자 장비이며 제 1 랜덤 값을 포함하는, EAP 도전 메시지를 송신하기 위한 수단, 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하기 위한 수단으로서, EAP 도전 응답 메시지는 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하기 위한 수단, 인증 값, 제 1 랜덤 값, 및 제 2 랜덤 값을 사용하여 EAP 도전 응답 메시지를 검증하기 위한 수단, 및 EAP 도전 응답 메시지를 검증한 후 MSK 를 생성하기 위한 수단을 더 포함한다.

[0021] 다른 피처는 네트워크와 연관된 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하게 하는 것으로서, WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하게 하고, WWAN 노드로부터 수신된 암호 키 및 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하게 하고, 네트워크 생성 제 1 식별자를 장치에 저장하고 네트워크 생성 제 1 식별자를 암호 키와 연관시키게 하고, 네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하게 하는 것으로서, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하게 하고, 사용자 장비 생성 제 1 식별자가, 저장된 네트워크 생성 제 1 식별자에 대응하는 것을 결정하게 하고, 마스터 세션 키 (MSK) 를 생성하게 하며, 그리고 EAP 성공 메시지 및 MSK 를 액세스 포인트에 송신하게 한다. 일 양태에 따라, 명령들은, 프로세서에 의해 실행될 때, 추가로 프로세서로 하여금, 액세스 포인트에 EAP 도전 메시지를 송신하게 하는 것으로서, EAP 도전 메시지는 목적지가 사용자 장비이며 제 1 랜덤 값을 포함하는, 상기 EAP 도전 메시지를 송신하게 하고, 액세스 포인트로부터 EAP 도전 응답 메시지를 수신하게 하는 것으로서, EAP 도전 응답 메시지는 사용자 장비에서 발신하고 제 2 랜덤 값 및 인증 값을 포함하는, 상기 EAP 도전 응답 메시지를 수신하게 하고, 인증 값, 제 1 랜덤 값, 및 제 2 랜덤 값을 사용하여 EAP 도전 응답 메시지를 검증하게 하며, 그리고 EAP 도전 응답 메시지를 검증한 후 MSK 를 생성하게 한다.

[0022] 다른 피처는 네트워크와 연관된 장치에서 보안 무선 통신을 위한 방법을 제공하며, 방법은, 쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하는 단계, PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되지 않는 것을 결정하는 단계, 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하는 단계, 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하는 단계, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신하는 단계, WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하는 단계, MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하는 단계, 및 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하는 단계를 포함한다. 일 양태에 따라, WLAN 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신한 후, 방법은, 제 1 랜덤 값을 포함하는 EAP 도전 메시지를 WLAN 단말 포인트로부터 수신하는 단계, 사용자 장비에 EAP 도전 메시지를 송신하는 단계, 제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 사용자 장비로부터 수신하는 단계, 및 WLAN 단말 포인트로 EAP 도전 응답 메시지를 송신하는 단계를 더 포함한다.

[0023] 다른 피처는 장치를 제공하며, 장치는 메모리 회로, 사용자 장비 및 무선 광역 네트워크 (WWAN) 단말 포인트와 통신하도록 적응된 통신 인터페이스, 및 메모리 회로 및 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고, 프로세싱 회로는, 쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하고, PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되지 않는 것을 결정하고, 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하고, 사용자 장비로부터 사용자

장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하고, WLAN 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신하고, WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하고, MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하며, 그리고 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하도록 적응된다. 일 양태에 따라, 프로세싱 회로가 WLAN 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신한 후, 프로세싱 회로는 또한, 제 1 랜덤 값을 포함하는 WLAN 단말 포인트로부터 EAP 도전 메시지를 수신하고, 사용자 장비에 EAP 도전 메시지를 송신하고, 제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 사용자 장비로부터 수신하고, 그리고 WLAN 단말 포인트로 EAP 도전 응답 메시지를 송신하도록 적응된다.

[0024] 다른 피처는 장치를 제공하며, 장치는, 쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하기 위한 수단, PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되지 않는 것을 결정하기 위한 수단, 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하기 위한 수단, 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하기 위한 수단, 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신하기 위한 수단, WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하기 위한 수단, MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하기 위한 수단, 및 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하기 위한 수단을 포함한다. 일 양태에 따라, 장치는, WLAN 단말 포인트에 사용자 장비 생성 제 1 식별자가 송신된 후 제 1 랜덤 값을 포함하는 WLAN 단말 포인트로부터 EAP 도전 메시지를 수신하기 위한 수단, 사용자 장비에 EAP 도전 메시지를 송신하기 위한 수단, 제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 사용자 장비로부터 수신하기 위한 수단, 및 WLAN 단말 포인트로 EAP 도전 응답 메시지를 송신하기 위한 수단을 더 포함한다.

[0025] 다른 피처는 네트워크와 연관된 장치에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신하게 하고, PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되지 않는 것을 결정하게 하고, 사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신하게 하고, 사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신하게 하고, 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신하게 하고, WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신하게 하고, MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출하게 하며, 그리고 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시하게 한다. 일 양태에 따라, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금 추가로, WLAN 단말 포인트에 사용자 장비 생성 제 1 식별자가 송신된 후 제 1 랜덤 값을 포함하는 WLAN 단말 포인트로부터 EAP 도전 메시지를 수신하게 하고, 사용자 장비에 EAP 도전 메시지를 송신하게 하고, 제 2 랜덤 값 및 인증 값을 포함하는 사용자 장비로부터 EAP 도전 응답 메시지를 수신하게 하며, 그리고 WLAN 단말 포인트로 EAP 도전 응답 메시지를 송신하게 한다.

[0026] 다른 피처는 디바이스에 의한 보안 무선 통신을 위한 방법을 제공하며, 방법은, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하는 단계, 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키로서 암호 키를 활용하는 단계, PMK, 디바이스를 식별하는 디바이스 식별자, 및 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하는 단계, 액세스 포인트에 PMKID 를 포함하는 연관 요청을 송신하는 단계, 및 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 액세스 포인트와의 키 교환을 개시하는 단계를 포함한다. 일 양태에 따라, 디바이스 식별자는 디바이스의 매체 액세스 제어 (MAC) 어드레스이고 액세스 포인트 식별자는 액세스 포인트의 MAC 어드레스이다. 다른 양태에 따라, PMKID 는 다음 식에 기초하여 생성되며: PMKID = 버림- 128(HMAC-SHA-256(PMK, STRING_0 ‖ 액세스 포인트 식별자‖디바이스 식별자)), 여기서 STRING_0 은 입력 문자열이다.

[0027] 일 양태에 따라, 액세스 포인트와의 키 교환을 개시하기 전에, 방법은, PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 AP 로부터 수신하는 단계, AP 로부터 EAP 아이덴티티 요청을 수신하는 단계, EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하는 단계로서, EAP 아이덴티티 응답은 암호 키 및 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하는 단계, 제 1 랜덤 값을 포함하는 EAP 도전 메시지를 AP 로부터 수신하는 단계, 제 2 랜덤 값 및 인증 값을 생성하는 단계로서, 인증 값은 암호 키, 제 1 랜덤 값 및 제 2 랜덤 값에 기초하는, 제 2 랜덤 값 및 인증 값을 생성하는 단계, 및 인증 값 및 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 AP 에 송신하는 단계를

더 포함한다.

[0028] 다른 피처는 보안 무선 통신을 위한 디바이스를 제공하며, 디바이스는 무선 통신 인터페이스, 무선 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고, 프로세싱 회로는, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하고, 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키로서 암호 키를 활용하고, PMK, 디바이스를 식별하는 디바이스 식별자, 및 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하고, 액세스 포인트에 PMKID 를 포함하는 연관 요청을 송신하며, 그리고 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 액세스 포인트와의 키 교환을 개시하도록 적응된다. 일 양태에 따라, 액세스 포인트와의 키 교환을 개시하기 전에, 프로세싱 회로는 또한, PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 AP 로부터 수신하고, AP 로부터 EAP 아이덴티티 요청을 수신하고, EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하는 것으로서, EAP 아이덴티티 응답은 암호 키 및 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하고, 제 1 랜덤 값을 포함하는 EAP 도전 메시지를 AP 로부터 수신하고, 제 2 랜덤 값 및 인증 값을 생성하는 것으로서, 인증 값은 암호 키, 제 1 랜덤 값 및 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하며, 그리고 인증 값 및 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 AP 에 송신하도록 적응된다.

[0029] 다른 피처는 보안 무선 통신을 위한 디바이스를 제공하며, 디바이스는, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하기 위한 수단, 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키로서 암호 키를 활용하기 위한 수단, PMK, 디바이스를 식별하는 디바이스 식별자, 및 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하기 위한 수단, 액세스 포인트에 PMKID 를 포함하는 연관 요청을 송신하기 위한 수단, 및 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 액세스 포인트와의 키 교환을 개시하기 위한 수단을 포함한다. 일 양태에 따라, 디바이스는, PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 AP 로부터 수신하기 위한 수단, AP 로부터 EAP 아이덴티티 요청을 수신하기 위한 수단, EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하기 위한 수단으로서, EAP 아이덴티티 응답은 암호 키 및 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하기 위한 수단, 제 1 랜덤 값을 포함하는 EAP 도전 메시지를 AP 로부터 수신하기 위한 수단, 제 2 랜덤 값 및 인증 값을 생성하기 위한 수단으로서, 인증 값은 암호 키, 제 1 랜덤 값 및 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하기 위한 수단, 및 인증 값 및 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 AP 에 송신하기 위한 수단을 더 포함한다.

[0030] 다른 피처는 디바이스에 의한 보안 무선 통신을 위한 명령들이 저장된 비일시적 컴퓨터 판독가능 저장 매체를 제공하며, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키를 획득하게 하고, 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트 (AP) 와의 보안 연관에 대한 쌍방식 마스터 키로서 암호 키를 활용하게 하고, PMK, 디바이스를 식별하는 디바이스 식별자, 및 액세스 포인트를 식별하는 액세스 포인트 식별자에 기초하여 PMK 식별자 (PMKID) 를 생성하게 하고, 액세스 포인트에 PMKID 를 포함하는 연관 요청을 송신하게 하며, 그리고 액세스 포인트와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 액세스 포인트와의 키 교환을 개시하게 한다. 일 양태에 따라, 명령들은 프로세서에 의해 실행될 때, 프로세서로 하여금 또한, PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답을 AP 로부터 수신하게 하고, AP 로부터 EAP 아이덴티티 요청을 수신하게 하고, EAP 아이덴티티 요청에 응답하여 EAP 아이덴티티 응답을 송신하게 하는 것으로서, EAP 아이덴티티 응답은 암호 키 및 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 송신하게 하고, 제 1 랜덤 값을 포함하는 EAP 도전 메시지를 AP 로부터 수신하게 하고, 제 2 랜덤 값 및 인증 값을 생성하게 하는 것으로서, 인증 값은 암호 키, 제 1 랜덤 값 및 제 2 랜덤 값에 기초하는, 상기 제 2 랜덤 값 및 인증 값을 생성하게 하며, 그리고 인증 값 및 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지를 AP 에 송신하게 한다.

도면의 간단한 설명

[0031] 도 1 은 본 명세서에 기재된 WWAN-WLAN 집성 보안 피처들 및 방법들을 피처링하는 LWA 를 활용한 통신 시스템의 예시적인 비병치 (non-collocated) 배열의 개략적인 블록 다이어그램이다.

도 2 는 예시적인 WLAN 의 개략적인 블록 다이어그램이다.

도 3 은 LAW 가능 통신 시스템의 개념적 프로토콜 스택을 도시한다.

도 4 는 UE/STA, WLAN, 및 eNB 를 수반하는 WLAN 보안 연관의 프로세스 플로우 다이어그램을 도시한다.

도 5a 및 도 5b 는 UE/STA, WLAN, 및 eNB 를 수반하는 WLAN 보안 연관의 제 1 예시적인 프로세스 플로우 다이어그램을 도시한다.

도 6a 및 도 6b 는 UE/STA, WLAN, 및 eNB 를 수반하는 WLAN 보안 연관의 제 2 예시적인 프로세스 플로우 다이어그램을 도시한다.

도 7a, 도 7b 및 도 7c 는 UE/STA, WLAN, 및 eNB 를 수반하는 WLAN 보안 연관의 제 3 예시적인 프로세스 플로우 다이어그램을 도시한다.

도 8 은 네트워크 장치에 의한 보안 무선 통신을 위한 제 1 예시적인 방법 플로우 다이어그램을 도시한다.

도 9a 및 도 9b 는 WLAN 단말 포인트와 같은 네트워크 장치에 의한 보안 무선 통신을 위한 제 2 예시적인 방법 플로우 다이어그램을 도시한다.

도 10a 및 도 10b 는 액세스 포인트와 같은 네트워크 장치에 의한 보안 무선 통신을 위한 제 3 예시적인 방법 플로우 다이어그램을 도시한다.

도 11 은 무선 네트워크 장치의 개략적인 블록 다이어그램을 도시한다.

도 12 는 디바이스 (예를 들어, UE/STA) 에 의한 보안 무선 통신을 위한 제 1 예시적인 방법 플로우 다이어그램을 도시한다.

도 13a 및 도 13b 는 디바이스 (예를 들어, UE/STA) 에 의한 보안 무선 통신을 위한 제 2 예시적인 방법 플로우 다이어그램을 도시한다.

도 14 는 디바이스 (UE/STA) 의 개략적인 블록 다이어그램을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0032] 다음의 기재에서 개시물의 다양한 양태들의 철저한 이해를 제공하기 위해 특정 상세들이 주어진다. 하지만, 양태들은 특정 상세들 없이 실시될 수도 있음은 당업자에 의해 이해될 것이다. 예를 들어, 회로들은 불필요한 상세들로 양태들을 모호하게 하는 것을 회피하기 위해 블록 다이어그램들로 나타낼 수도 있다. 다른 경우들에서, 잘 알려진 회로들, 구조들 및 기법들은 개시물의 양태들을 모호하게 하지 않도록 상세하게 나타내지 않을 수도 있다.

[0033] 단어 "예시적인" 은 본 명세서에서 "예, 예증, 또는 예시로서 작용하는 것" 을 의미하도록 사용된다. "예시적인" 으로서 본 명세서에 기재된 임의의 구현 또는 양태가 반드시 개시물의 다른 양태들보다 바람직하거나 이로운 것으로 해석되지 않아야 한다. 마찬가지로, 양태는 구현 또는 예이다. "양태", "일 양태", "일부 양태들", "다양한 양태들", 또는 "다른 양태들" 에 대한 명세서에서의 언급은, 양태들과 관련하여 기재된 피처, 구조, 또는 특징이 적어도 일부 실시형태들에 포함되지만, 반드시 본 기법의 모든 양태들에 포함되는 것은 아님을 의미한다. "양태", "일 양태", 또는 "일부 양태들" 의 다양한 형태들이 반드시 모두 동일한 양태들을 지칭하지 않는다. 양태로부터의 엘리먼트들 또는 양태들은 다른 양태의 엘리먼트들 또는 양태들과 결합될 수 있다.

[0034] 다음의 설명 및 청구항들에서, 용어 "커플링된" 은 2 이상의 엘리먼트들이 직접 물리적 또는 전기적 접촉에 있는 것을 의미할 수도 있다. 하지만, "커플링된" 은 또한 2 이상의 엘리먼트들이 서로 직접 접촉하지 않지만, 여전히 서로 협력하거나 상호작용하는 것을 의미할 수도 있다.

[0035] 본 명세서에 기재되고 예시된 모든 컴포넌트들, 피처들, 구조들, 특징들이 특정 양태 또는 양태들에 포함되어야 하는 것은 아니다. 명세서가 컴포넌트, 피처, 구조, 또는 특징이 포함 "될 수도", "되었을 수도", "될 수", 또는 "되었을 수" 있음을 언급하는 경우, 그 특정 컴포넌트, 피처, 구조, 또는 특징이 포함될 필요는 없다. 명세서 또는 청구항이 "a" 또는 "an" 엘리먼트를 지칭하는 경우, 그 것은 엘리먼트 중 단 하나만 있는 것을 의미하지 않는다. 명세서 또는 청구항이 "부가" 엘리먼트를 지칭하는 경우, 그것은 하나보다 많은 부가 엘리먼트가 있는 것을 배제하지 않는다.

[0036] 일부 양태들이 특정 구현들을 참조하여 기재되었지만, 다른 구현들이 몇몇 양태들에 따라 가능하다는 것을 유의

해야 한다. 또한, 도면들에 도시되고 및/또는 본 명세서에 기재된 회로 엘리먼트들 또는 다른 피처들의 배열 및/또는 순서가 도시되고 기재된 특정 방식으로 배열될 필요는 없다. 많은 다른 배열들이 일부 양태들에 따라 가능하다.

[0037] 각각의 도면에서, 엘리먼트들은 일부 경우들에서 각각 나타낸 엘리먼트들이 상이하고 및/또는 유사할 수 있음을 제시하기 위해 동일한 참조 번호 또는 상이한 참조 번호를 가질 수도 있다. 하지만, 엘리먼트는 상이한 구현들을 가지는데 충분히 유연성이 있으며 본 명세서에 나타내거나 기재된 시스템들의 일부 또는 모두와 작동할 수도 있다. 도면들에 나타낸 다양한 엘리먼트들은 동일하거나 상이할 수도 있다. 어느 것이 제 1 엘리먼트로 지칭되고 어느 것이 제 2 엘리먼트로 불리는 지는 임의적이다.

[0038] 도 1 은 일 양태에 따라 본 명세서에 기재된 WWAN-WLAN 집성 보안 피처들 및 방법들을 피처링하는 LWA 를 활용한 통신 시스템 (100) 의 예시적인 비병치 배치의 개략적인 블록 다이어그램을 도시한다. 시스템 (100) 은 셀룰러 코어 네트워크 (108) 에 커플링된 사용자 장비 (UE)(102), WLAN (104) 및 eNB (eNB)(106) 를 포함한다. UE (102) 는 WLAN 에서 종래의 스테이션 (STA) 에 의해 수행되는 것과 같은 동작들을 UE (102) 가 수행하도록 할 수도 있는 스테이션 성능을 포함한다. 결과적으로, 다음의 논의에서, 이 기능성은 "UE 내의 STA" 로서 지칭될 수도 있고, 용어들 "STA" 및 "UE" 는 동일한 디바이스를 지칭하는데 사용될 수도 있다.

[0039] 도 1 에 나타낸 바와 같이, UE (102) 는 WWAN 의 eNB (106) 에 접속되고 이로부터 WWAN 데이터 경로를 따라 데이터를 송신 및 수신할 수도 있다. 게다가, UE (102) 는 WWAN (104) 의 하나 이상의 액세스 포인트 (AP) 들에 접속되고 이로부터 WLAN 데이터 경로로부터 데이터를 송신 및 수신할 수도 있다.

[0040] eNB (106) 는 데이터 및 제어 평면들 양자 모두에 대한 앵커 (anchor) 노드이며 WWAN 및 WLAN 링크들 양자 모두에 대해 패킷 스케줄링을 제어한다. eNB (106) 는 Xw 통신 인터페이스 (예를 들어, Xw-C 제어 및 Xw-U 사용자) 를 통해 WLAN (104) 의 WLAN 단말 포인트 (WTP)(110) 와 통신한다. eNB (106) 는 또한 정규 S1 인터페이스들 (S1-C 및 S1-U) 을 통해 코어 네트워크 (CN) 에 접속하고 제어 및 사용자 데이터를 송신 및 수신한다.

[0041] 도 2 는 일 양태에 따른 예시적인 WLAN (104) 의 개략적인 블록 다이어그램을 도시한다. 상술한 바와 같이, STA (102) 는 WLAN (104) 과 연관된 하나 이상의 AP들 (202, 202a, 202b) 과 통신하고, eNB (106) 는 WLAN (104) 의 WTP (110) 와 통신한다. 나타낸 비제한적인 예에서, WLAN (104) 은 WLAN 제어기 (WLC)(204) 에 통신 가능하게 커플링될 수도 있는 복수의 AP들 (202, 202a, 202b) 을 포함하며, 결국 WTP (110) 에 통신 가능하게 커플링된다. 도 2 에 나타낸 예는 단지 예시적인 것이다. 다른 양태들에서, WLAN (104) 은 WTP (110) 에 통신가능하게 커플링되거나 그 자체로 액세스 포인트 및 WLAN 단말 포인트 양자 모두인 단일 AP (202) 를 포함할 수도 있다. 또한, 도 2 에 나타내고 본 명세서에 논의된 AP들 (202, 202a, 202b) 은 LWA 인식 AP들 (예를 들어, 쌍방식 마스터 키 (pairwise master key; PMK) 캐싱이 가능한 AP들) 또는 802.1x AP들 (예를 들어, "레거시 AP들") 중 어느 것일 수도 있다. 단순화를 위해 그리고 하기에서 참조되는 바와 같이, 하나의 AP (202a) 는 PMK 캐싱이 가능한 LWA 인식 AP 로 간주될 수도 있고 다른 AP (202b) 는 레거시 AP 로 간주될 수도 있다.

[0042] 도 3 은 일 양태에 따른 LWA 가능 통신 시스템의 개념적 프로토콜 스택을 도시한다. 도 3 에 나타낸 바와 같이, LTE 무선 리소스 제어 채널 (RRC 채널)(302) 및 LTE 비액세스 스트라텀 (Non-Access Stratum; NAS) 제어 채널 (304) 은 MME (306) 와 UE (102) 및 eNB (106)(예를 들어, MeNB) 사이에서 유지된다. UE (102) 로부터의 WWAN (예를 들어, LTE) 사용자 데이터 (308) 및 WLAN 사용자 데이터 (310) 는 패킷 데이터 수렴 프로토콜 (PDCP) 계층에서 집성된다.

[0043] 도 1 내지 도 3 을 참조하면, 초기 WLAN 연관은 현재 WWAN 보안 콘텍스트 (예를 들어, LTE 보안 콘텍스트) 로부터 생성된 키 S-K_{WT} (예를 들어, 이하 "암호 키" 일 수도 있음) 를 사용할 수도 있다. 일 양태에서, 키 S-K_{WT} 는 LTE 보안 콘텍스트의 eNB 키로부터 도출되는 256 비트 키일 수도 있다. STA (102) 는 UE (102) 의 WWAN 스택 (예를 들어, LTE 스택) 으로부터 키 S-K_{WT} 를 획득할 수도 있다. eNB (106) 는 Xw 통신 인터페이스를 통해 WLAN 의 WTP (110) 에 키 S-K_{WT} 를 제공할 수도 있다. 키 S-K_{WT} 는 그 후 UE/STA (102) 와 WLAN (104) 사이의 보안 접속을 확립하기 위해 4 방향 키 교환 핸드셰이크의 일부로서 WLAN (104) 및 UE/STA (102) 에 의해 쌍방식 마스터 키 (PMK) 로서 사용될 수도 있다.

[0044] 도 4 는 개시물의 일 양태에 따라 UE/STA (102), WLAN (104) 및 eNB (106) 를 수반하는 WLAN 보안 연관의 프로세스 플로우 다이어그램을 도시한다. 도시된 예에서, WLAN 의 AP (202a) 는 대역 외 소스로부터 키 (예를

들어, $S\text{-}K_{WT}$) 를 수신할 수 있고 이것을 보안 연관을 위한 쌍방식 마스터 키 (PMK) 로서 사용할 수 있다는 점에서 LWA 인식 액세스 포인트이다. 이는 성공적인 EAP 인증의 결과로 서 PMK 및 연관된 PMK 보안 연관 (PMKSA) 이 생성되는 전형적인 AP들 및 STA 들과는 상이하다. 즉, PMK 및 PMKSA 는 802.1x 특정 인증 절차를 수행할 필요 없이 생성될 수도 있다. 일 양태에서, 도 4 에 나타낸 AP (202a) 및 WTP (110) 는 액세스 포인트 및 무선 단말 포인트의 양자 모두의 기능들을 포함하는 하나의 단일 디바이스일 수도 있다.

[0045] 더욱이, eNB (106) 는 UE (102) 로부터 수신된 WLAN 측정들에 기초하여 데이터 무선 베어러 오프로드를 위한 후보 WLAN 서비스 세트를 선택할 수도 있다. eNB (106) 로부터 하나 이상의 데이터 무선 베어러들 (예를 들어, LTE 데이터 무선 베어러들) 을 오프로딩하라는 커맨드를 수신하면, UE (102) 는 eNB (106) 로부터 수신된 WLAN 서비스 세트로부터의 AP들 중 하나를 선택할 수도 있다. 선택은 AP (202a) 의 수신 신호 강도 표시자 (RSSI) 또는 일부 다른 UE 구현 특정 기준에 기초할 수도 있다. UE (102) 는 또한 프로브 요청을 전송하는 것에 의해 또는 AP (202a) 에 의해 브로드캐스팅된 메시지로부터 PMKSA 를 초기화하기 위해 AP의 MAC 어드레스를 획득할 수도 있다.

[0046] 도 4 를 참조하면, eNB (106) 는 WTP 부가 요청 메시지를 WLAN 의 단말 포인트 (110) 에 송신할 수도 있다 (402). WTP 부가 요청 메시지는 UE 식별자 (예를 들어, UE MAC 어드레스) 및 키 $S\text{-}K_{WT}$ 를 포함할 수도 있다. 다음으로, WTP (110) 는 WTP 부가 요청 메시지의 성공적인 수신을 확인응답하는 WTP 부가 확인응답 메시지로 응답한다 (404). 키 $S\text{-}K_{WT}$ 는 그 후 WLAN 보안 연관을 위해 PMK 로서 AP (202a) 에 의해 사용될 수도 있다. AP (202a) 는 PMKID = 버림 - 128(HMAC-SHA-256(PMK, STRING_0 | AA | SPA)) 에 따라 PMK 에 기초하여 PMK 식별자 (PMKID) 를 생성하며, 여기서 "AA" 는 AP MAC 어드레스이고, "SPA"는 UE MAC 어드레스이며, "STRING_0" 은 임의의 입력 문자열이다. 또한, AP (202a) 는 저장된 PMK 를 AP 의 MAC 어드레스, PMK 의 수명, 적응 키 관리 프로토콜 (AKMP), PMKID 및/또는 다른 인증 정보 (예를 들어, SSID) 와 연관시킴으로써 PMK 보안 연관 (PMKSA) 을 파퓰레이트 (populate)(예를 들어, 초기화) 한다.

[0047] eNB (106) 로부터 접속 재구성 커맨드 (예를 들어, RRC_Connection_Reconfiguration 커맨드) 를 수신하면, UE (102) 는 WWAN 스택 (예를 들어, LTE 스택) 으로부터 PMK 를 획득 (예를 들어, UE 가 $S\text{-}K_{WT}$ 및 PMK : = $S\text{-}K_{WT}$ 를 획득) 하고 PMK 에 기초하여 PMKID 및 PMKSA 를 도출한다 (410). 접속 재구성 커맨드는 eNB (106) 로부터 BSSID/HESSID/ESSID 의 하나 이상을 갖는 WLAN 식별 정보를 포함하여 소정의 데이터 무선 베어러들을 식별된 WLAN으로 오프 로딩할 수도 있다. UE (102) 에서의 이들 액션들 (408, 410) 은 WLAN (104) 및 eNB (106) 에서 발생하는 액션들 (402, 404, 406) 에 독립적으로 수행될 수도 있다.

[0048] 후속하여, UE (102) 는 PMKID 를 포함하는 연관 요청 (412) 을 AP (202a) 에 송신할 수도 있다. AP (202a) 는 PMKID 를 사용하여 UE (102) 와 연관된 PMKSA 및 PMK 를 발견하고 (413), 연관 응답을 역 전송한다 (414). 그 후, UE (102) 및 AP (202a) 는 PMK 를 사용하여 4 방향 키 교환 핸드셰이크에 관여할 수도 있다 (416). 성공적인 연관 후에, UE 연관 메시지는 WTP (110) 에 송신될 수도 있고 (420), 결국 WTP 관련 메시지를 eNB (106) 에 송신한다 (420). UE 연관 메시지 및 대응 WTP 연관 메시지는 UE (102) 가 WLAN (104) 에 성공적으로 접속되었다는 것을 eNB (106) 가 알도록 하고, 이제 WLAN (104) 상으로 트래픽 (예를 들어, 데이터 무선 베어러들 (DRB)) 을 오프로딩하기 시작할 수도 있다. AP (202a) 및 UE (102) 는 또한 802.1x 에 기초하여 보안 통신을 송신 및 수신하기 시작 할 수도 있다 (422).

[0049] 또한, 도 5a 및 도 5b 는 개시물의 다른 양태에 따른 UE/STA (102), WLAN (104) 및 eNB (106) 를 수반하는 WLAN 보안 연관의 프로세스 플로우 다이어그램을 도시한다. 도시된 예에서, AP (202b) 는 대역 외 수신된 PMK 로부터 PMKSA 생성을 지원하지 않는 레거시 액세스 포인트 (즉, 802.1x 액세스 포인트) 이다. 먼저, eNB (106) 는 WLAN (104) 의 WLAN 단말 포인트 (110) 에 WTP 부가 요청 메시지를 송신한다 (502). WTP 부가 요청 메시지는 UE MAC 어드레스 및 키 $S\text{-}K_{WT}$ 를 포함할 수도 있다. 다음으로, WTP (110) 는 WTP 부가 요청 메시지의 성공적인 수신을 확인응답하는 WTP 부가 확인 응답 메시지로 응답한다 (504). 키 $S\text{-}K_{WT}$ 및 UE MAC 어드레스는 제 1 식별자 LWA-ID (예를 들어, "네트워크 생성 제 1 식별자") 를 생성하기 위해 WTP (110) 에 의해 사용될 수도 있다 (506). 일 예에 따라, LWA-ID 는 키 $S\text{-}K_{WT}$ 및 UE MAC 어드레스의 함수일 수도 있다.

예를 들어, LWA-ID = KDF($S\text{-}K_{WT}$, UE MAC 어드레스, STRING_0), 식 중 KDF 는 키 도출 함수 (예를 들어, SHA256 등과 같은 일 방향 함수) 이고, STRING_0 은 임의의 입력 문자열 값일 수도 있다.

[0050] eNB (106) 로부터 RRCConnectionReconfiguration 커맨드를 수신하면, UE (102) 는 WWAN 스택 (예를 들어, LTE

스택) 으로부터 PMK 를 획득 (예를 들어, UE 가 S-K_{WT} 및 PMK : = S-K_{WT} 를 획득) 하고 (508) 이 PMK 에 기초하여 PMKID 를 도출한다. UE (102) 에서의 이러한 액션 (508) 은 WLAN (104) 및 eNB (106) 에서 발생하는 액션들 (502, 504, 506) 에 독립적으로 수행될 수도 있다. 후속하여, UE (102) 는 PMKID 를 포함하는 연관 요청 (510) 을 AP (202b) 에 송신할 수도 있다. AP (202b) 는 레거시 액세스 포인트이기 때문에 UE (102) 의 연관된 PMKSA 를 갖지 않는다. 따라서, AP (202b) 는 PMKSA 가 발견되지 않았다는 것을 결정하고 (512), 대응 응답 (예를 들어, 발견된 PMKSA 없음) 을 UE (102) 에 회신한다 (514).

[0051] 또한, PMKSA 를 발견하지 않으면 UE (102) 에 EAP 아이덴티티 요청 메시지를 전송함으로써 (516), UE (102) 와 확장가능 인증 프로토콜 (EAP) 을 시작하도록 AP (202b) 를 프롬프트한다. UE (102) 는 그 후, 단지 하나의 예에 따라 KDF (S-K_{WT}, UE MAC 어드레스, STRING_0) 와 동일할 수도 있는 LWA-ID (예를 들면, "사용자 장비 생성 제 1 식별자") 를 생성한다 (518). UE (102) 는 AP (202b) 에 EAP 피어 아이덴티티로서 LWA-ID@realm (예를 들어, "제 1 값") 를 갖는 EAP 아이덴티티 응답으로서 생성된 LWA-ID 를 전송한다 (520). 또 다른 양태에서, LWA-ID 는 EAP 아이덴티티 요청 메시지의 수신 전에 (예를 들어, PMKID 가 생성될 때 (508)) UE (102) 에 의해 생성될 수도 있다.

[0052] 여기서, "realm (영역)" 은 eNB (106) 의 서빙 네트워크 아이덴티티를 나타낸다. 이는 eNB (106) (예를 들어, eNB (106) 의 물리적 셀 ID) 및/또는 eNB (106) 와 연관된 공중 육상 모바일 네트워크 (PLMN) 아이덴티티 또는 양자 모두를 식별할 수도 있다. 즉, "영역" 은 AP (202b) 가 인증 요청을 라우팅하기를 UE (102) 가 원하는 WTP (110) 를 식별한다. 예를 들어, 영역 값은 realm = lwa.wtid<WTID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org 로서 정의될 수도 있고, 여기서 모바일 네트워크 코드 (MNC), 및 모바일 국가 코드 (MCC) 는 eNB/MME 의 서빙 네트워크 PLMN 아이덴티티로부터 획득될 수도 있다. WTID 는 eNB (106)(예를 들어, eNB 의 E-UTRAN 셀 아이덴티티 (ECI)) 를 식별하는 식별자이다. WWAN 스택 (예를 들어, LTE 스택) 은 UE (102) 에 WTID, MNC, 및 MCC 를 제공한다. "영역" 을 사용하면 상이한 WTP들을 갖는 WLAN 네트워크가 다수의 서빙 네트워크들을 서빙하는 것을 가능하게 한다는 것을 알아야 한다. 예를 들어, WLAN 네트워크는 상이한 PLMN 오퍼레이터들에 속하는 상이한 eNB들 또는 동일한 PLMN 오퍼레이터들에 속하는 상이한 eNB들에 의한 트래픽 오프로드를 지원할 수도 있다.

[0053] 아이덴티티 LWA-ID@realm 을 갖는 EAP 아이덴티티 응답 메시지는 그 후 인증, 인가 및 계정 (AAA) 스킴하에서 아이덴티티의 "realm" 부분에 의해 식별된 WTP (110) 에 AP (202b) 에 의해 포워딩된다 (522). WTP (110) 는 EAP 인증 서버 (AS) 의 역할을 하며 수신된 값 (LWA-ID) 을 사용하여 UE (102) 와 연관된 키 S-K_{WT} 를 발견할 수도 있다 (524). 발견한 경우, WTP (110) 는 마스터 세션 키 (MSK) 를 생성하고 (525), 그 후 AP (202b) 에 MSK 와 함께 EAP 성공 메시지를 송신한다 (526). 다른 한편으로, 수신된 LWA-ID 가 저장된 LWA-ID 와 연관되지 않으면, EAP 실패 메시지가 대신 송신될 수도 있다.

[0054] 일 양태에 따라, WTP (110) 는 S-K_{WT} 를 자신과 결부시키는 것에 의해 MSK 를 생성하고 (즉, MSK = S-K_{WT} | S-K_{WT}) 그 후 AP (202b) 에 EAP 성공 메시지와 함께 MSK 를 송신할 수도 있다. AP (202b) 는 이제 MSK 를 가지기 때문에 PMK (예를 들어, PMK : = MSK 의 비트의 제 1 절반) 를 생성하고 (527) EAP 성공 메시지를 UE (102) 에 송신하며 (528), 이로써 UE (102) 를 성공적으로 인증할 수도 있다. 그 후, UE (102) 및 AP (202b) 는 PMK 를 사용하여 4 방향 키 교환 핸드셰이크에 관여할 수도 있다 (530). 성공적인 연관 후에, UE 연관 메시지가 WTP (110) 에 송신될 수도 있으며 (532), 이는 결국 WTP 연관 메시지를 eNB (106) 에 송신한다. AP (202b) 및 UE (102) 는 또한 802.1x 에 기초하여 보안 통신을 송신 및 수신하기 시작할 수도 있다 (536).

[0055] 또한, 도 6a 및 도 6b 는 개시물의 다른 양태에 따른 UE/STA (102), WLAN (104) 및 eNB (106) 를 수반하는 WLAN 보안 연관의 프로세스 플로우 다이어그램을 도시한다. 도시된 예에서, AP (202b) 는 대역 외 수신된 PMK 로부터 PMKSA 생성을 지원하지 않는 레거시 액세스 포인트 (즉, 802.1x 액세스 포인트) 이다. 먼저, eNB (106) 는 WLAN (104) 의 WLAN 단말 지점 (110) 에 WTP 부가 요청 메시지를 송신한다 (602). WTP 부가 요청 메시지는 UE MAC 어드레스 및 키 (S-K_{WT}) 를 포함할 수도 있다. 다음으로, WTP (110) 는 WTP 부가 요청 메시지의 성공적인 수신을 확인응답하는 WTP 부가 확인응답 메시지로 응답한다 (604). 그 후, 키 (S-K_{WT}) 및 UE MAC 어드레스는 값 LWA-ID (예를 들어, "네트워크 생성 제 1 식별자") 를 생성하기 위해 WTP (110) 에 의해 이용될 수도 있다 (606). 일 예에 따라, LWA-ID 는 키 (S-K_{WT}) 및 UE MAC 어드레스의 함수일 수도 있다.

예를 들어, LWA-ID = KDF(S-K_{WT}, UE MAC 어드레스, STRING_0), 여기서 KDF 는 키 도출 함수 (예를 들어, SHA256 등과 같은 일 방향 함수) 이고, STRING0 은 임의의 입력 문자열 값일 수도 있다.

[0056] RRCConnectionReconfiguration 커맨드의 수신 시, UE (102) 는 WWAN 스택으로부터 PMK 를 획득 (예를 들어, UE 가 S-K_{WT} 및 PMK : = S-K_{WT} 를 획득) 하고 (608) PMK에 기초하여 PMKID 자체를 도출한다 (608). UE (102) 에서의 이러한 액션 (608) 은 WLAN (104) 및 eNB (106) 에서 발생하는 액션들 (602, 604, 606) 에 독립적으로 수행될 수도 있다. 이어서, UE (102) 는 PMKID 를 포함하는 연관 요청 (610) 을 AP (202b) 에 송신할 수도 있다. AP (202b) 는 레거시 액세스 포인트이기 때문에 UE (102) 의 연관된 PMKSA 를 갖지 않는다. 따라서, PMKSA 가 발견되지 않았다는 것을 결정하고 (612), 대응 응답 (예를 들어, 발견된 PMKSA 가 없음) 을 UE (102) 에 회신한다 (614).

[0057] PMKSA 를 발견하지 않으면 EAP 아이덴티티 요청 메시지를 전송함으로써 (616), UE (102) 와의 확장가능 인증 프로토콜 (EAP) 을 시작하도록 AP (202b) 를 프롬프트한다. UE (102) 는 그 후 일 예에 따라 KDF (S-K_{WT}, UE MAC 어드레스, STRING_0) 와 동일할 수도 있는 값 LWA-ID (예를 들면, "사용자 장비 생성 제 1 식별자") 을 생성하고 (618) EAP 아이덴티티 응답 LWA-ID@realm 을 AP (202b) 에 전송한다. 또 다른 양태에서, LWA-ID 는 EAP 아이덴티티 요청 메시지의 수신 전에 (예를 들어, PMKID 가 생성될 때) UE (102) 에 의해 생성될 수도 있다.

[0058] 위에 논의된 바와 같이, "realm (영역)" 은 eNB (106) 의 서빙 네트워크 아이덴티티를 의미하며, eNB (106) 또는 eNB (106) 와 연관된 PLMN 아이덴티티를 식별할 수도 있다. "영역" 을 사용하면, WLAN 네트워크가 상이한 PLMN 오퍼레이터들에 속한 상이한 eNB들 또는 동일한 PLMN 오퍼레이터들에 속한 상이한 eNB들에 의한 트래픽 오프로드를 지원하는 WLAN 네트워크와 같은 다수의 서빙 네트워크를 서빙하는 것을 가능하게 한다.

[0059] 그 후, EAP 아이덴티티 응답 메시지 (LWA-ID@realm) 는 AAA 스킴 하에서 WTP (110) 로 포워딩된다 (622). WTP (110) 는 AP (202b) 로부터 수신된 것과 매칭하는 LWA-ID 가 저장되어 있는지 여부를 결정한다. 만약 그렇다면, LWA-특정 EAP 인증 프로토콜 (이하, "EAP-LWA" 인증 프로토콜이라 칭함) 을 개시하고 (624), 그렇지 않으면 AP (202b) 및 UE (102) 에 EAP 실패 통지를 회신한다. EAP-LWA 와 같은 LWA-특정 EAP 인증 프로토콜을 개시하는 이점은 기존 EAP 상태 머신의 준수를 유지하는 것이며, 여기서 EAP 피어 (즉, UE (102)) 는 EAP 성공이 피어에 의해 허용될 수도 있기 전에 EAP 인증 방법 특정 메시지 교환의 수신을 기대할 수도 있다. 일 양상에 따라, 일단 EAP-LWA 가 개시되면, WTP (110) 는 EAP-LWA 요청 () 메시지를 AP (202b) 에 전송하며 (626), 이것을 결국 UE (102) 에 포워딩한다 (628). UE (102) 는 AP (202b) 에 EAP-LWA 응답 () 메시지로 응답하고 (630), 결국 이것을 WAP (110) 로 다시 포워딩한다 (632).

[0060] 이 시점에서, WTP (110) 는 예를 들어 S-K_{WT} 를 그 자체와 결부시킴으로써 S-K_{WT} 로부터 MSK 를 도출한다 (즉, MSK = S-K_{WT} | S-K_{WT}). WTP (110) 는 그 후 MSK 와 함께 EAP-LWA 성공 메시지를 AP (202b) 에 전송한다 (636) (이들 메시지 (626, 628, 630, 632, 636) 는 인증 서버로서 작용하는 WTP (110) 와 AAA 스킴하에서 교환될 수도 있다). AP (202b) 는 이제 MSK 를 가지기 때문에, PMK (예를 들어, PMK : = MSK 의 비트의 제 1 절반) 를 생성할 수도 있고 (637), EAP 성공 메시지를 UE (102) 에 송신한다 (638). 그 후, UE (102) 및 AP (202b) 는 PMK 를 사용하여 4 방향 키 교환 핸드셰이크에 관여할 수도 있다 (640). 성공적인 연관 후, UE 연관 메시지는 WTP (110) 에 송신될 수도 있고 (644), 결국 WTP 연관 메시지를 eNB (106) 에 송신한다 (644). AP (202b) 및 UE (102) 는 또한 802.1x 에 기초하여 보안 통신들을 송신 및 수신하기 시작할 수도 있다 (646).

[0061] 또한, 도 7a, 도 7b 및 도 7c 는 개시물의 또 다른 양태에 따른 UE/STA (102), WLAN (104) 및 eNB (106) 를 수반하는 WLAN 보안 연관의 프로세스 플로우 다이어그램을 도시한다. 도시된 예에서, AP (202b) 는 대역 외 수신된 PMK 로부터 PMKSA 생성을 지원하지 않는 레거시 액세스 포인트 (즉, 802.1x 액세스 포인트) 이다. 먼저, eNB (106) 는 WLAN (104) 의 WLAN 단말 포인트 (110) 에 WTP 부가 요청 메시지를 송신한다 (702). WTP 부가 요청 메시지는 UE MAC 어드레스 및 키 (S-K_{WT}) 를 포함할 수도 있다. 다음으로, WTP (110) 는 WTP 부가 요청 메시지의 성공적인 수신을 확인응답하는 WTP 부가 확인응답 메시지로 응답한다 (704). 그 후, 키 (S-K_{WT}) 및 UE MAC 어드레스는 값 LWA-ID (예를 들어, "네트워크 생성 제 1 식별자") 를 생성하기 위해 WTP (110) 에 의해 이용될 수도 있다 (706). 일 예에 따라, LWA-ID 는 키 (S-K_{WT}) 및 UE MAC 어드레스의 함수일 수도 있다. 예를 들어, LWA-ID = KDF (S-K_{WT}, UE MAC 어드레스, STRING_0), 여기서 KDF 는 키 도출 함수

(예를 들어, SHA256 등과 같은 일 방향 함수) 이고, STRING_0 은 임의의 입력 문자열 값이다. WTP (110) 는 또한 값 LWA-ID 를 수신된 암호 키 S-K_{WT} 와 연관시킨다.

[0062] RRCConnectionReconfiguration 커맨드의 수신 시, UE (102) 는 WWAN 스택으로부터 PMK 를 획득 (예를 들어, UE 가 S-K_{WT} 및 PMK : = S-K_{WT} 를 획득) 하고 (708) PMK 에 기초하여 PMKID 자체를 도출한다 (708). UE (102) 에서의 이러한 액션 (708) 은 WLAN (104) 및 eNB (106) 에서 발생하는 액션들 (702, 704, 706) 에 독립적으로 수행될 수도 있다. 이어서, UE (102) 는 PMKID 를 포함하는 연관 요청 (710) 을 AP (202b) 에 송신할 수도 있다. AP (202b) 는 레거시 액세스 포인트이기 때문에, PMKID 또는 UE (102) 와 연관된 PMKSA 를 갖지 않는다. 따라서, 수신된 PMKID 와 연관된 PMKSA 가 발견되지 않았다는 것을 결정하고 (712), PMKID 를 생략하는 대응 응답 (예를 들어, 발견된 PMKSA 가 없음) 을 UE (102) 에 회신한다 (714).

[0063] PMKSA 를 발견하지 않으면 또한, EAP 아이덴티티 요청 메시지를 전송함으로써 (716), UE (102) 와 확장가능 인증 프로토콜 (EAP0 를 시작하도록 AP (202b) 를 프롬프트한다. UE (102) 는 그 일 예에 따라 KDF (S-K_{WT}, UE MAC 어드레스, STRING_0) 와 동일할 수도 있는 값 LWA-ID (예를 들면, "사용자 장비 생성 제 1 식별자") 를 생성하고 (718) EAP 아이덴티티 응답 LWA-ID@realm 을 AP (202b) 에 전송한다. 또 다른 양태에서, LWA-ID 는 EAP 아이덴티티 요청 메시지의 수신 전에 (예를 들어, PMKID 가 생성될 때) UE (102) 에 의해 생성될 수도 있다.

[0064] 위에 논의된 바와 같이, "realm (영역)" 은 eNB (106) 의 서빙 네트워크 아이덴티티를 의미하며, eNB (106) 또는 eNB (106) 와 연관된 PLMN 아이덴티티를 식별할 수도 있다. "영역" 을 사용하면 WLAN 네트워크가 상이한 PLMN 오퍼레이터들에 속하는 여러 eNB들 또는 동일한 PLMN 오퍼레이터들에 속하는 상이한 eNB들에 의한 트래픽 오프로드를 지원하는 WLAN 네트워크와 같은 다수의 서빙 네트워크를 서빙하는 것을 가능하게 한다.

[0065] 그 후 EAP 아이덴티티 응답 메시지 (LWA-ID@realm) 는 AAA 스킴 하에서 WTP (110) 로 포워딩된다 (722). WTP (110) 는 다음으로 AP (202b) 로부터 수신된 것과 매칭하는 LWA-ID 가 저장되어 있는지 여부를 결정한다. 만약 그렇다면, EAP-LWA 인증 프로토콜을 개시하고 (724), 그렇지 않으면 EAP 실패 통지를 AP (202b) 및 UE (102) 에 회신한다. EAP-LWA 와 같은 LWA-특정 EAP 인증 프로토콜을 개시하는 이점은 기존 EAP 상태의 준수를 유지하는 것이며, 여기서 EAP 피어 (즉, UE (102)) 는 EAP 성공이 피어에 의해 허용될 수도 있기 전에 EAP 인증 방법 특정 메시지 교환의 수신을 기대할 수도 있다. 일 양태에 따라, 일단 EAP-LWA 가 개시되면, WTP (110) 는 랜덤 값 AS_nonce (한번 사용된 번호) 를 포함하는 EAP-LWA 요청 (AS_nonce) 메시지를 AP (202b) 에 송신하고 (726), 결국 이것을 UE (102) 에 포워딩한다 (728). UE (102) 는 그 후 자신의 랜덤 값 (UE_nonce) 을 생성하고 값 AUTHRES = KDF (S-K_{WT}, AS_nonce, UE_nonce, STRING_1) 을 도출하며 (730), 여기서 KDF 는 키 도출 함수이고, STRING_1 은 임의의 입력 문자열일 수도 있다. 그 후 UE (102)는 UE_nonce 및 AUTHRES 를 포함하는 EAP-LWA 응답 (AUTHRES, UE_nonce) 메시지로 AP (202b) 에 UE_nonce 를 응답하며 (732), 결국 이것을 WTP (110) 에 포워딩한다 (734).

[0066] 그 후 WTP (110) 는 동일한 KDF, STRING_1, 수신된 UE_nonce 및 그 자신의 국부적으로 저장된 AS_nonce 및 S-K_{WT} 를 사용하여 그 자신의 AUTHRES 값을 생성한다. WTP (110) 가 생성하였던 AUTHRES 값이 AP/UE 로부터 그것이 수신했던 AUTHRES 값과 매칭하는 것을 결정하는 것에 의해, EAP-LWA 응답이 검증되고 (736) UE/STA (102) 가 인증된다. 이들 메시지 (726, 728, 730, 732, 736) 는 인증 서버로서 작동하는 WTP (110) 와 AAA 스킴 하에서 교환될 수도 있다.

[0067] 이 시점에서, WTP (110) 는 예를 들어 S-K_{WT} 를 그 자체와 결부시키는 것에 의해 S-K_{WT} 로부터 MSK 를 도출한다 (즉, MSK = S-K_{WT} | S-K_{WT}). 그 후, WTP (110) 는 MSK 와 함께 EAP-LWA 성공 메시지를 AP (202b) 에 전송한다 (740). AP (202b) 는 이제 MSK 를 가지기 때문에 PMK (예를 들어, PMK := MSK 의 비트의 제 1 절반) 를 생성할 수도 있고 (742), EAP 성공 메시지를 UE (102) 에 송신할 수도 있다 (744). 그 후, UE (102) 및 AP (202b) 는 PMK 를 사용하여 4 방향 키 교환 핸드셰이크로 (746) 에 관여할 수도 있다 (746). 성공적인 연관 후에, UE 연관 메시지는 WTP (110) 에 송신될 수도 있으며 (750), 결국 WTP 연관 메시지를 eNB (106) 에 송신한다 (750). AP (202b) 및 UE (102) 는 또한, 802.1x 에 기초하여 보안 통신을 송신 및 수신하기 시작할 수도 있다 (752). 다른 양태에서, MSK 는 MSK = PMK | PMK 대신에 MSK = KDF (S-K_{WT}, AS_nonce, UE_nonce, STRING_2) 와 같은 KDF 를 사용하여 도출될 수도 있으며, 여기서 STRING_2 는 임의의 입력 문자열이다.

[0068] 도 8 은 네트워크 및/또는 네트워크 장치 (예를 들어, WLAN, AP 및/또는 WTP) 에 의한 보안 무선 통신을 위한

방법 플로우 다이어그램을 도시한다. 먼저, 암호 키 (예컨대, $S\text{-}K_{WT}$) 및 사용자 장비를 식별하는 사용자 장비 식별자가 무선 광역 네트워크 (WWAN) 노드로부터 수신된다 (802). 다음으로, 암호 키는 쌍방식 마스터 키 (PMK) 로서 사용된다 (804). 그 후, PMK 식별자 (PKMID) 가 PMK 에 기초하여 생성된다 (806). 다음으로, PMK 및 PMKID 가 장치에 저장된다 (808). 그 다음, PMK 보안 연관 (PMKSA) 은 PMK 를 적어도 PMKID 및 장치의 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시킴으로써 초기화된다 (810). 다음으로, PMKID 를 포함하는 사용자 장비로부터 연관 요청이 수신된다 (812). 그 후, 사용자 장비로부터 수신된 PMKID 가 장치에 저장된 PMKID 와 매칭하는 것이 결정된다 (814). 다음으로, 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환이 개시된다 (816).

[0069] 도 9a 및 9b 는 네트워크 장치 (예를 들어, WTP) 에 의한 보안 무선 통신을 위한 방법 플로우 다이어그램을 도시한다. 먼저, 무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청이 수신되며 (902), 이 WLAN 단말 포인트 부가 요청은 암호 키 (예컨대, $S\text{-}K_{WT}$) 및 사용자 장비를 식별하는 사용자 장비 식별자 (예컨대, UE MAC 어드레스) 를 포함한다. 다음으로, WWAN 노드로부터 수신된 사용자 장비 식별자 및 암호 키에 기초하여 네트워크 생성 제 1 식별자 (예컨대, LWA-ID) 가 생성된다 (904). 그 후, 네트워크 생성 제 1 식별자는 장치에 저장되고 (906) 네트워크 생성 제 1 식별자를 암호 키와 연관시킨다. 다음으로, 네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답이 수신되며 (908), 이 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자 (예를 들어, LWA-ID@realm 의 부분으로서의 LWA-ID) 를 포함한다. 그 후, 사용자 장비 생성 제 1 식별자가, 저장된 네트워크 생성 제 1 식별자에 대응하는 것이 결정된다 (910). 다음으로, EAP 도전 메시지가 액세스 포인트에 송신되며 (912), EAP 도전 메시지는 목적지가 사용자 장비이고 제 1 랜덤 값 (예를 들어, AS_nonce) 을 포함한다. 그 후, 액세스 포인트로부터 EAP 챌린지 응답 메시지가 수신되며 (914), EAP 도전 응답 메시지는 사용자 장비에서 발신하고 제 2 랜덤 값 (예를 들어, STA_nonce) 및 인증 값 (예를 들어, AUTHRES) 을 포함한다. 다음으로, EAP 도전 응답 메시지는 인증 값, 제 1 랜덤 값 및 제 2 랜덤 값을 사용하여 검증된다 (916). 그 후, 마스터 세션 키 (MSK) 가 EAP 도전 응답 메시지를 검증한 후에 생성된다 (918). 다음으로, EAP 성공 메시지 및 MSK 가 액세스 포인트에 송신된다 (920).

[0070] 또한, 도 10a 및 도 10b 는 네트워크 장치 (예를 들어, 액세스 포인트) 에 의한 보안 무선 통신을 위한 방법 플로우 다이어그램을 도시한다. 먼저, 쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 사용자 장비로부터 연관 요청이 수신된다 (1002). 다음으로, PMKID 와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되어 있지 않은 것이 결정된다 (1004). 그 후, 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청이 사용자 장비에 송신된다 (1006). 다음으로, 사용자 장비로부터 사용자 장비 생성 제 1 식별자 (예를 들어, LWA-ID @realm 의 일부로서 LWA-ID) 를 포함하는 EAP 아이덴티티 응답이 수신된다 (1008). 그 후, 사용자 장비 생성 제 1 식별자가 네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트로 송신된다 (1010). 다음으로, 제 1 랜덤 값 (예를 들어, AS_nonce) 을 포함하는 EAP 도전 메시지가 WLAN 단말 포인트로부터 수신된다 (1012). 그 후, EAP 도전 메시지가 사용자 장비에 송신된다 (1014). 다음으로, 제 2 랜덤 값 (예를 들어, STA_nonce) 및 인증 값 (예를 들어, AUTHRES) 을 포함하는 EAP 도전 응답 메시지가 사용자 장비로부터 수신된다 (1016). 그 후, EAP 도전 응답 메시지가 WLAN 단말 포인트로 송신된다 (1018). 다음으로, 마스터 세션 키 (MSK) 가 WLAN 단말 포인트로부터 수신된다 (1020). 그 후, MSK 로부터 쌍방식 마스터 키 (PMK) 가 도출되고 (1022), 사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환이 개시된다 (1024).

[0071] 도 11 은 개시물의 일 양태에 따른 무선 통신 네트워크 장치 (예컨대, WLAN 장치)(1100) 의 개략적인 블록 다이어그램을 도시한다. 네트워크 (1100) 는 서로 통신하는 적어도 하나의 액세스 포인트 (1110) 및 적어도 하나의 무선 단말 포인트 (1120) 를 포함한다. 네트워크 (1100) 는 무선 단말 포인트 (1120) 에 통신가능하게 커플링되고 및/또는 도 11 에 나타내지 않은 부가 무선 단말 포인트에 통신 가능하게 커플링된 더 많은 액세스 포인트를 포함할 수도 있다. 도 11 에 나타낸 AP (1110) 및 WTP (1120) 는 단일 장치 (1100) 의 일부일 수도 있거나 각각 (1110, 1120) 이 무선 로컬 영역 네트워크 내에서 서로 독립적으로 하우징된 별도의 장치일 수도 있다.

[0072] 네트워크 (1100) 의 예시적인 액세스 포인트 (1110) 는 적어도 하나 이상의 통신 인터페이스 (1112), 하나 이상의 메모리 회로 (1114), 하나 이상의 프로세싱 회로 (1116) 및/또는 하나 이상의 입력 및/또는 출력 (I / O) 디바이스들/회로들 (1118) 을 포함할 수도 있으며 이들은 서로 통신가능하게 커플링된다. 통신 인터페이스 (1112) 는 액세스 포인트 (1110) 가 하나 이상의 UE/STA 와 무선으로 통신하도록 한다. 따라서, 인터페이스

(1112) 는 액세스 포인트 (1110) 가 802.1x 와 같은 WLAN 프로토콜 또는 다른 프로토콜 (Zigbee®, Bluetooth® 등) 을 통해 무선으로 통신하도록 한다.

[0073] 액세스 포인트의 메모리 회로 (1114) 는 하나 이상의 휘발성 메모리 회로 및/또는 비휘발성 메모리 회로를 포함할 수도 있다. 따라서, 메모리 회로 (1114) 는 DRAM, SRAM, MRAM, EEPROM, 플래시 메모리 등을 포함할 수도 있다. 메모리 회로 (1114) 는 하나 이상의 암호 키, 변수, 넌스 (nonce), 값 등을 저장할 수도 있다. 메모리 회로 (1114) 는 또한 프로세싱 회로 (1116) 에 의해 실행될 수도 있는 명령들을 저장할 수도 있다. I/O 디바이스들/회로들 (1118) 은 하나 이상의 키보드, 마우스, 디스플레이, 터치 스크린 디스플레이, 프린터, 지문 스캐너, 및 임의의 다른 입력 및/또는 출력 디바이스를 포함할 수도 있다.

[0074] 액세스 포인트의 프로세싱 회로 (1116)(예를 들어, 프로세서, 중앙 프로세싱 유닛 (CPU), 어플리케이션 프로세싱 유닛 (APU) 등) 는 메모리 회로 (1114) 에 저장된 명령들 및/또는 액세스 포인트 (110) 에 통신가능하게 커플링된 다른 컴퓨터 판독가능 저장 매체 (예를 들어, 하드 디스크 드라이브, 광 디스크 드라이브, 고체 상태 드라이브 등) 에 저장된 명령들을 실행할 수도 있다. 프로세싱 회로 (1116) 는 도 1, 도 2, 도 3, 도 4, 도 5a, 도 5b, 도 6a, 도 6b, 도 7a, 도 7b, 도 7c, 도 8, 도 10a 및/또는 도 10b 를 참조하여 논의된 것들을 포함하여 본 명세서에 기재된 액세스 포인트들의 단계들 및/또는 프로세스들 중 어느 하나를 수행할 수도 있다.

[0075] 네트워크 (1100) 의 예시적인 무선 단말 포인트 (1120) 는 적어도 하나 이상의 통신 인터페이스 (1122), 하나 이상의 메모리 회로 (1124), 하나 이상의 프로세싱 회로 (1126), 및/또는 하나 이상의 입력 및/또는 출력 (I/O) 디바이스/회로 (1128) 를 포함할 수도 있으며, 이들은 각각 서로 통신가능하게 커플링된다. 통신 인터페이스 (1122) 는 무선 단말 포인트 (1120) 가 eNB 와 같은 하나 이상의 WWAN 노드와 무선으로 통신하도록 한다.

[0076] 무선 단말 포인트의 메모리 회로 (1124) 는 하나 이상의 휘발성 메모리 회로 및/또는 비휘발성 메모리 회로를 포함할 수도 있다. 따라서, 메모리 회로 (1124) 는 DRAM, SRAM, MRAM, EEPROM, 플래시 메모리 등을 포함할 수도 있다. 메모리 회로 (1124) 는 하나 이상의 암호 키, 변수, 넌스, 값 등을 저장할 수도 있다. 메모리 회로 (1124) 는 프로세싱 회로에 의해 실행될 수도 있는 명령들을 저장할 수도 있다. I/O 디바이스들/회로들 (1128) 은 하나 이상의 키보드, 마우스, 디스플레이, 터치스크린 디스플레이, 프린터, 지문 스캐너 및 임의의 다른 입력 및/또는 출력 디바이스를 포함할 수도 있다.

[0077] 무선 단말 포인트의 프로세싱 회로 (1126)(예를 들어, 프로세서, 중앙 프로세싱 유닛 (CPU), 어플리케이션 프로세싱 유닛 (APU) 등) 는 메모리 회로 (1124) 에 저장된 명령들 및/또는 무선 단말 포인트 (1120) 에 통신가능하게 커플링된 다른 컴퓨터 판독가능 저장 매체 (예를 들어, 하드 디스크 드라이브, 광 디스크 드라이브, 고체 상태 드라이브 등) 에 저장된 명령들을 실행할 수도 있다. 프로세싱 회로 (1126) 는 도 1, 도 2, 도 3, 도 4, 도 5a, 도 5b, 도 6a, 도 6b, 도 7a, 도 7b, 도 7c, 도 8, 도 9a 및/또는 도 9b 를 참조하여 논의된 것들을 포함하여 본 명세서에 기재된 무선 단말 포인트들의 단계들 및/또는 프로세스들 중 어느 하나를 수행할 수도 있다.

[0078] 네트워크 (1100) 는 액세스 포인트 (1110) 및 무선 단말 포인트 (1120) 의 통신 인터페이스 (1112, 1122) 를 부분적으로 포함하는 통신 인터페이스 (1102) 를 포함할 수도 있다. 유사하게, 네트워크는 액세스 포인트 (1110) 및 무선 단말 포인트 (112) 의 메모리 회로 (1114, 1124) 를 부분적으로 포함하는 메모리 회로 (1104) 를 포함할 수도 있다. 네트워크는 또한 액세스 포인트 (1110) 및 무선 단말 포인트 (1120) 의 프로세싱 회로 (1116, 1128) 를 부분적으로 포함하는 프로세싱 회로 (1106) 를 포함할 수도 있다. 네트워크 (1100) 의 프로세싱 회로 (1106) 는 도 8, 도 9a, 도 9b, 도 10a 및/또는 도 10b 에 기재되고 나타낸 단계들을 수행하도록 구성된다. 네트워크 (1100) 의 메모리 회로 (1104) 는 프로세싱 회로 (1106) 에 의해 실행될 때 네트워크 (1100) 의 프로세싱 회로 (1106) 로 하여금 도 8, 도 9a, 도 9b, 도 10a 및/또는 도 10b 에 기재되고 나타낸 단계들을 수행하게 하는 명령들을 저장하도록 적응된다.

[0079] 도 12 는 디바이스 (예를 들어, UE/STA) 에 의한 보안 무선 통신을 위한 방법 플로우 다이어그램을 도시한다. 먼저, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키 (예를 들어, $S\text{-}K_{WT}$) 가 획득된다 (1202). 다음으로, 암호 키는 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 활용된다 (1204). 그 다음, PMK, 디바이스를 식별하는 디바이스 식별자 (예를 들어, UE MAC 어드레스) 및 AP를 식별하는 액세스 포인트 식별자 (예를 들어, AP MAC 어드레스)에 기초하여, PMK 식별자 (PMKID)가 생성된다 (1206). 다음으로, PMKID 를 포함하는 연관 요청이 AP 에 송신된다 (1208). 그 후, AP 와의 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 AP 와의 키 교환 (예를 들어, 4 방향 키 교환 핸

드셰이크) 이 개시된다 (1210).

[0080] 도 13 은 디바이스 (예컨대, UE/STA) 에 의한 보안 무선 통신을 위한 방법 플로우 다이어그램을 도시한다. 먼저, 무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키 (예를 들어, $S\text{-}K_{WT}$) 가 획득된다 (1302). 다음으로, 암호 키는 무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 활용된다 (1304). 그 후, PMK 식별자 (PMKID) 가 PMK, 디바이스를 식별하는 디바이스 식별자 (예를 들어, UE MAC 어드레스), 및 AP 를 식별하는 액세스 포인트 식별자 (예를 들어, AP MAC 어드레스) 에 기초하여 생성된다 (1306). 다음으로, AP 에 PMKID 를 포함하는 연관 요청이 전송된다 (1308). 그 후, PMKID 와 관련된 PMK 보안 연관 (PMKSA) 이 발견될 수 없음을 표시하는 연관 응답이 AP 로부터 수신된다 (1310). 다음으로, EAP 아이덴티티 요청이 AP로부터 수신된다 (1312). 그 후, EAP 아이덴티티 응답이 EAP 아이덴티티 요청에 응답하여 송신되며 (1314), EAP 아이덴티티 응답은 암호 키 및 디바이스 식별자에 기초한 디바이스 생성 제 1 식별자를 포함한다. 다음으로, 제 1 랜덤 값을 포함하는 EAP 도전 메시지가 AP 로부터 수신된다 (1316). 그 후, 제 2 랜덤 값 및 인증 값이 생성되며 (1318), 인증 값은 암호 키, 제 1 랜덤 값 및 제 2 랜덤 값에 기초한다. 다음으로, 인증 값 및 제 2 랜덤 값을 포함하는 EAP 도전 응답 메시지가 AP 에 송신된다 (1320). 그 후, 키 교환 (예를 들어, 4 방향 키 교환 핸드셰이크) 이 AP 와의 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 AP 와 개시된다 (1322).

[0081] 도 14 는 개시물의 일 양태에 따른 디바이스 (예를 들어, 사용자 장비 (UE) 및 스테이션 (STA))(1400) 의 개략적인 블록 다이어그램을 도시한다. 디바이스 (1400) 는 복수의 무선 통신 인터페이스들 (1402), 하나 이상의 메모리 회로들 (1404), 하나 이상의 입력 및/또는 출력 (I/O) 디바이스들/회로들 (1406) 및/또는 하나 이상의 프로세싱 회로들을 포함할 수도 있으며, 이들은 서로 통신가능하게 커플링된다. 예를 들어, 인터페이스 (1402), 메모리 회로 (1404), I/O 디바이스 (1406) 및 프로세싱 회로 (1408) 는 버스 (1410) 를 통해 서로 통신가능하게 커플링될 수도 있다. 무선 통신 인터페이스 (1402) 는 디바이스 (1400) 가 eNB (106) 와 무선으로 통신하도록 한다. 따라서, 인터페이스 (1402) 는 또한 디바이스 (1400) 가 802.1x 와 같은 WLAN 프로토콜 및/또는 Zigbee®, Bluetooth® 등과 같은 다른 프로토콜을 통해 WLAN (예를 들어, AP (202)) 에 무선으로 통신하도록 한다.

[0082] 메모리 회로 (1404) 는 하나 이상의 휘발성 메모리 회로 및/또는 비휘발성 메모리 회로를 포함할 수도 있다. 따라서, 메모리 회로 (1404) 는 DRAM, SRAM, MRAM, EEPROM, 플래시 메모리 등을 포함할 수도 있다. 메모리 회로 (1404) 는 하나 이상의 암호 키를 저장할 수도 있다. 또한, 메모리 회로 (1404) 는 프로세싱 회로 (1408) 에 의해 실행될 수도 있는 명령들을 저장할 수도 있다. I/O 디바이스들/회로들 (1406) 은 하나 이상의 키보드, 마우스, 디스플레이, 터치스크린 디스플레이, 프린터, 지문 스캐너, 및 임의의 다른 입력 및/또는 출력 디바이스를 포함할 수도 있다.

[0083] 프로세싱 회로 (1408)(예를 들어, 프로세서, 중앙 프로세싱 유닛 (CPU), 어플리케이션 프로세싱 유닛 (APU) 등) 은 메모리 회로 (1406) 에 저장된 명령들 및/또는 디바이스 (1400) 에 통신가능하게 커플링된 다른 컴퓨터 판독가능 저장 매체 (예를 들어, 하드 디스크 드라이브, 광학 디스크 드라이브, 고체 상태 드라이브 등) 에 저장된 명령들을 실행할 수도 있다. 프로세싱 회로 (1408) 는 도 1 내지 도 7c, 도 12, 도 13a, 및/또는 도 13b 를 참조하여 논의된 것들을 포함하여 본 명세서에 기재된 UE/STA (102들) 의 단계들 및/또는 프로세스들 중 어느 하나를 수행할 수도 있다.

[0084] 도 1, 도 2, 도 3, 도 4, 도 5a, 도 5b, 도 6a, 도 6b, 도 7a, 도 7b, 도 7c, 도 8, 도 9a, 도 9b, 도 10a, 도 10b, 도 11, 도 12, 도 13a, 도 13b, 및/또는 도 14 에 도시된 컴포넌트들, 단계들, 피처들, 및/또는 기능들 중 하나 이상은 단일 컴포넌트, 단계, 피처 또는 기능으로 재배열 및/또는 결합될 수도 있거나 몇몇 컴포넌트들, 단계들, 또는 기능들로 구현될 수도 있다. 부가 엘리먼트들, 컴포넌트들, 단계들, 및/또는 기능들은 또한 발명으로부터 벗어나지 않으면서 부가될 수도 있다. 도 1, 도 2, 도 3, 도 11, 및/또는 도 14 에 도시된 장치, 디바이스들, 및/또는 컴포넌트들은 도 3, 도 4, 도 5a, 도 5b, 도 6a, 도 6b, 도 7a, 도 7b, 도 7c, 도 8, 도 9a, 도 9b, 도 10a, 도 10b, 도 12, 도 13a, 및/또는 도 13b 에 기재된 방법들, 피처들, 또는 단계들 중 하나 이상을 수행하도록 구성될 수도 있다. 본 명세서에 기재된 알고리즘은 또한 효율적으로 소프트웨어로 구현되고 및/또는 하드웨어에 임베딩될 수도 있다.

[0085] 또한, 본 개시물의 양태들은 플로우챠트, 플로우 다이어그램, 구조 다이어그램, 또는 블록 다이어그램으로서 도시되는 프로세스로서 기술될 수도 있음을 유의해야 한다. 플로우챠트가 순차적 프로세스로서 동작들을 기술할 수도 있지만, 많은 동작들은 병렬로 또는 동시에 수행될 수도 있다. 또한, 동작들의 순서는 재배열될 수

도 있다. 프로세스는 그 동작들이 완료될 때 종료된다. 프로세스는 방법, 함수, 절차, 서브루틴, 서브프로그램 등에 대응할 수도 있다. 프로세스가 함수에 대응할 때, 그 종료는 호출 함수 또는 메인 함수로의 함수의 회신에 대응한다.

[0086] 더욱이, 저장 매체는 판독 전용 메모리 (ROM), 랜덤 액세스 메모리 (RAM), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들을 포함한, 데이터를 저장하기 위한 하나 이상의 디바이스들, 및/또는 정보를 저장하기 위한 다른 머신 판독가능 매체들, 및 프로세서 판독가능 매체들 및/또는 컴퓨터 판독가능 매체들을 나타낼 수도 있다. 용어들 "머신 판독가능 매체", "컴퓨터 판독가능 매체", 및/또는 "프로세서 판독가능 매체" 는, 비일시적 매체들, 예컨대 휴대용 또는 고정 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 포함하거나 저장할 수 있는 다양한 다른 매체들을 포함할 수도 있다. 따라서, 본 명세서에 기재된 다양한 방법들은 전부 또는 부분적으로, 하나 이상의 프로세서들, 머신들 및/또는 디바이스들에 의해 실행되고 "머신 판독가능 매체", "컴퓨터 판독가능 매체", 및/또는 "프로세서 판독가능 매체" 에 저장될 수도 있는 명령들 및/또는 데이터에 의해 구현될 수도 있다.

[0087] 또한, 개시물의 양태들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로 코드, 또는 이들의 임의의 조합에 의해 구현될 수도 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로 코드로 구현될 때, 필요한 태스크들을 수행하는 프로그램 코드 또는 코드 세그먼트들은 저장 매체 또는 다른 스토리지(들) 과 같은 머신 판독가능 매체에 저장될 수도 있다. 프로세서는 필요한 태스크들을 수행할 수도 있다. 코드 세그먼트는 절차, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스 또는 명령들, 데이터 구조들 또는 프로그램 세그먼트들의 임의의 조합을 나타낼 수도 있다. 코드 세그먼트는 정보, 데이터, 인수 (argument) 들, 파라미터들 또는 메모리 컨텐츠를 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수도 있다. 정보, 인수, 파라미터들, 데이터 등은 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 송신 등을 포함한 임의의 적절한 수단을 통해 전달, 포워딩 또는 송신될 수도 있다.

[0088] 본 명세서에 개시된 예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 엘리먼트들 및/또는 컴포넌트들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적 회로 (ASIC), 필드 프로그램가능 게이트 어레이 (FPGA) 또는 다른 프로그램가능 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트, 또는 본 명세서에 기재된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현되거나 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안적으로, 프로세서는 임의의 종래 프로세서, 제어기, 마이크로제어기 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 컴포넌트들의 조합, 예를 들어 DSP 및 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로 구현될 수도 있다. 단지 하나의 예로서, 도 11 의 프로세싱 회로들 (1106, 1116, 1126) 은 특히 도 8, 도 9a, 도 9b, 도 10a, 및/또는 도 10b 에 도시된 단계들의 하나 이상을 수행하도록 하드 와이어링되는 ASIC들일 수도 있다. 유사하게, 도 14 의 프로세싱 회로 (1408) 는 특히 도 12, 도 13a, 및/또는 도 13b 에 도시된 단계들의 하나 이상을 수행하도록 하드 와이어링되는 ASIC 일 수도 있다.

[0089] 본 명세서에 개시된 예들과 관련하여 설명된 방법들 또는 알고리즘은 프로세싱 유닛, 프로그래밍 명령들 또는 다른 디렉션들의 형태로 하드웨어에서, 프로세서에 의해 실행가능한 소프트웨어 모듈에서, 또는 양자의 조합에서 직접 구현될 수도 있고, 단일 디바이스에 포함되거나 다수의 디바이스들에 걸쳐 분산될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 이동식 디스크, CD-ROM 또는 당업계에 알려진 저장 매체의 임의의 다른 형태에 상주할 수도 있다. 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기입할 수 있도록 프로세서에 커플링될 수도 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수도 있다.

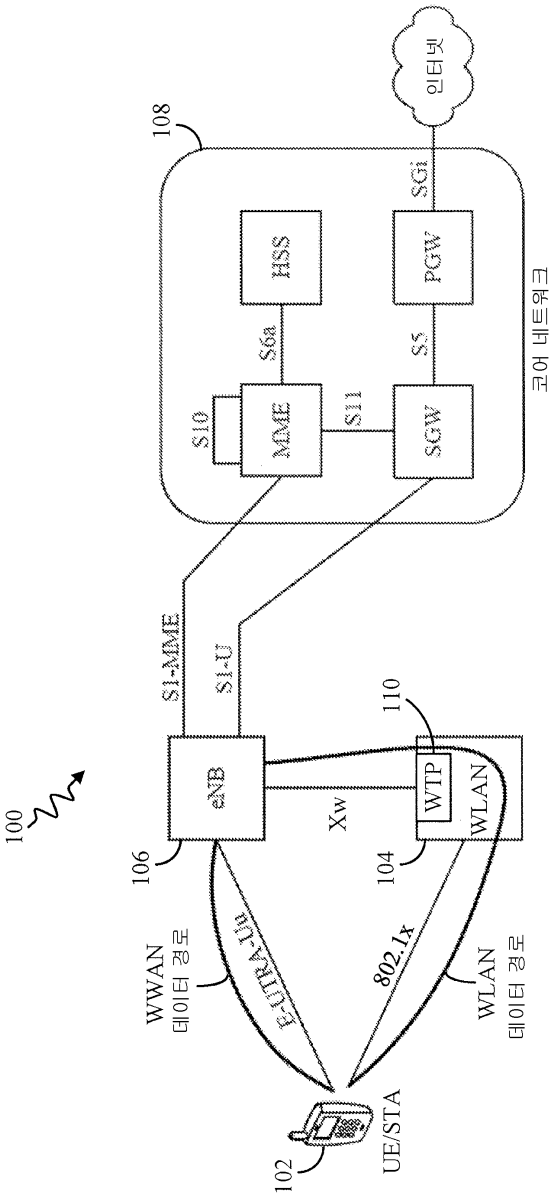
[0090] 당업자는 본 명세서에 개시된 양태들과 관련하여 기재된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 조합으로서 구현될 수도 있다는 것을 더 인식할 것이다. 이러한 하드웨어 및 소프트웨어의 상호 교환가능성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 기능성의 관점에서 일반적으로 설명되었다. 그러한 기능성이 하드웨어 또는 소프트웨어로 구현되는지 여부는 전체 시스템에 부과된 설계 제약들 및 특정 어플리케이션에 의존한다.

[0091] 본 명세서에 기재된 발명의 다양한 피처들은 발명으로부터 벗어나지 않으면서 상이한 시스템들로 구현될 수도 있다. 개시물의 상술한 양태들은 단지 예들일 뿐이며, 발명을 제한하는 것으로 해석되지 않아야 함을 유의

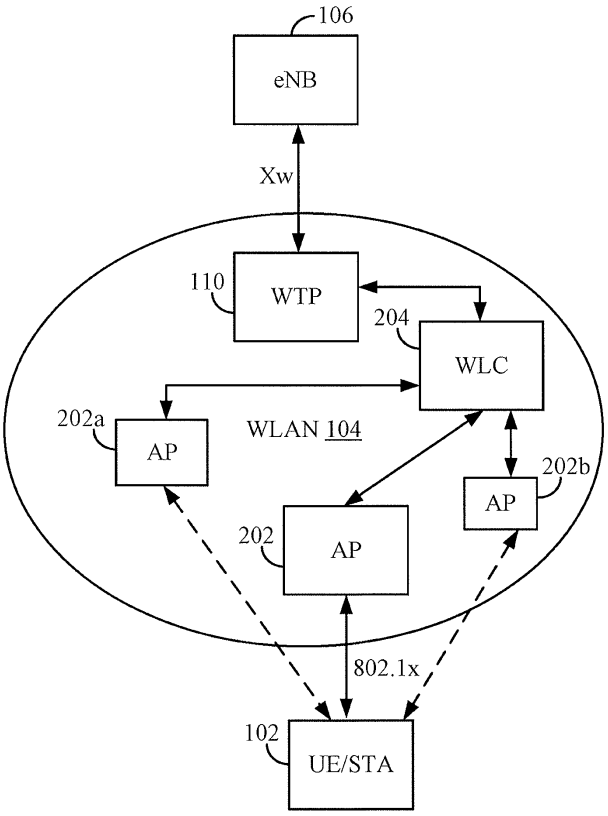
해야 한다. 본 개시물의 양태들의 설명은 예시적인 것으로 의도되며, 청구항들을 제한하려는 것으로 의도되지 않는다. 이와 같이, 본 교시들은 다른 유형의 장치들에 쉽게 적용될 수 있고, 많은 대안들, 수정들 및 변형들이 당업자에게 명백할 것이다.

도면

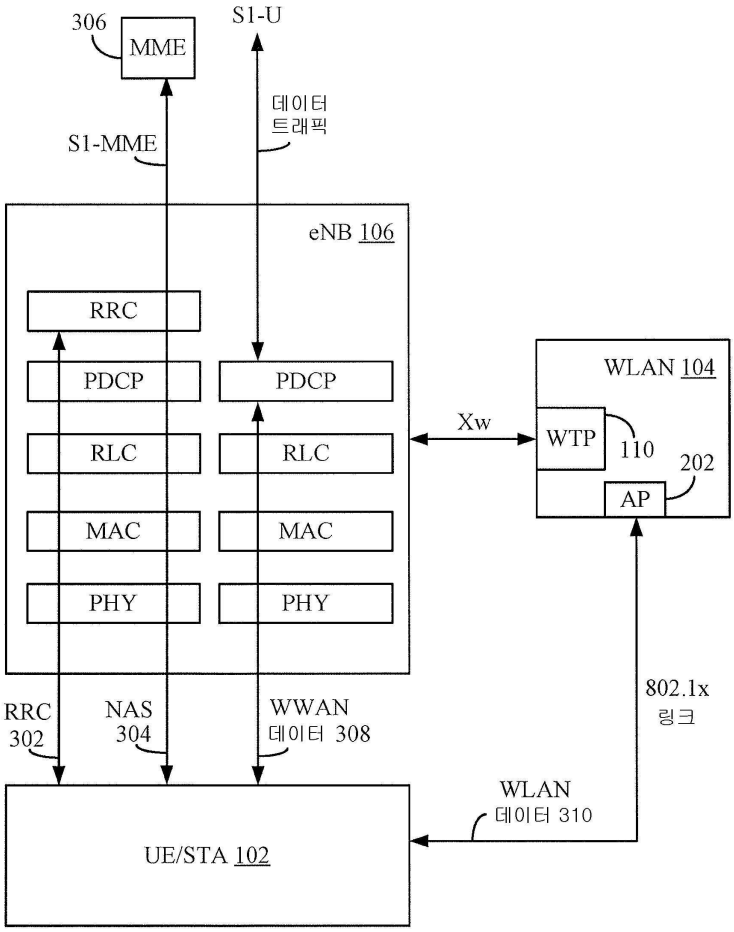
도면1



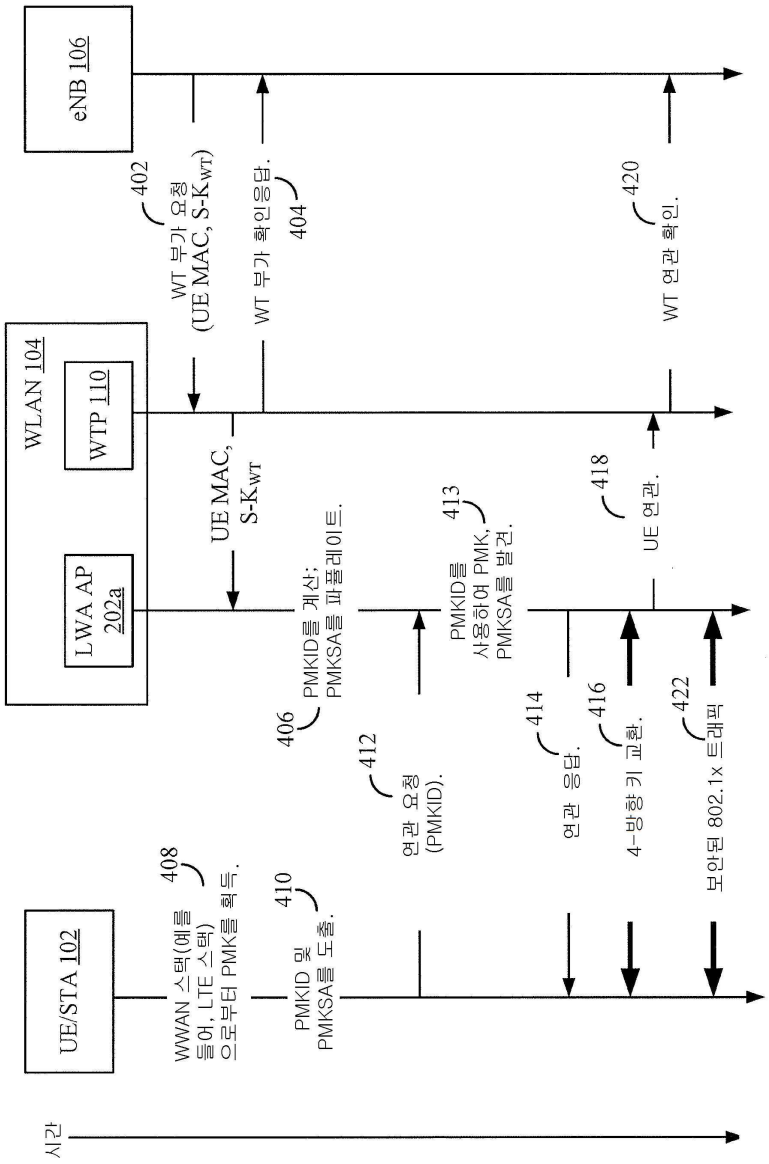
도면2


106
eNB
Xw
110
WTP
204
WLC
202a
AP
WLAN 104
202b
AP
202
AP
802.1x
102
UE/STA

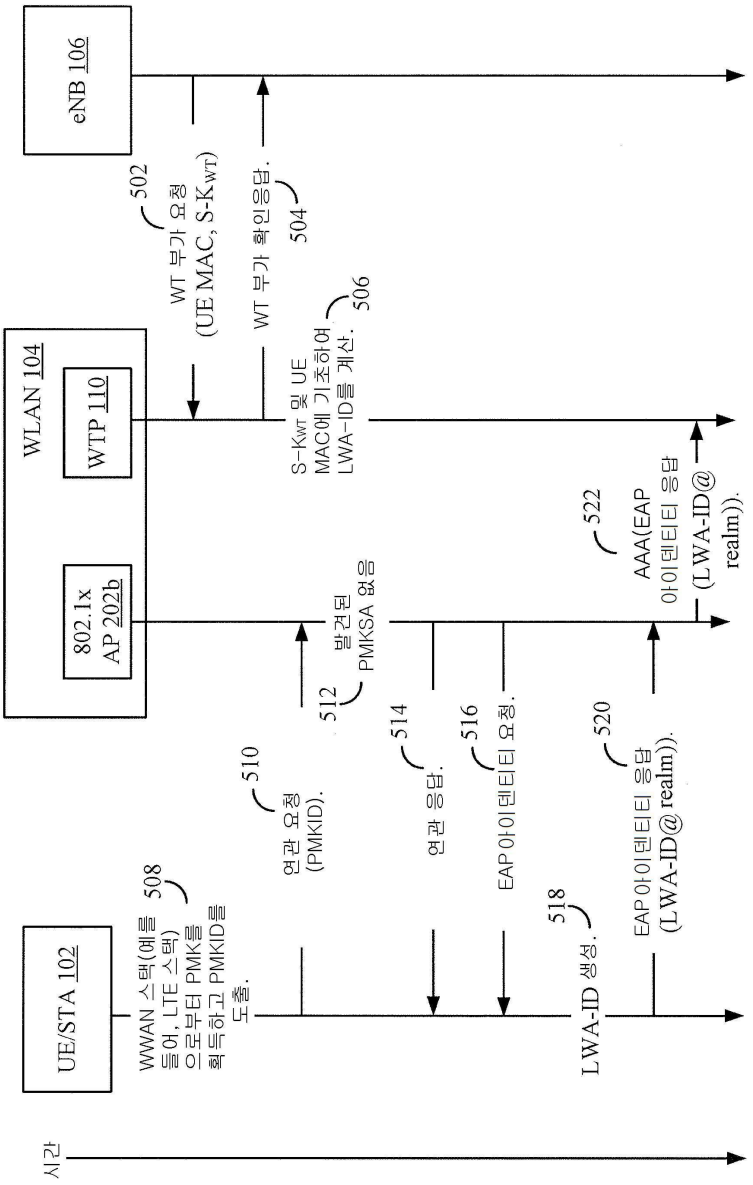
도면3


306
MME
S1-U
데이터
트래픽
S1-MME
eNB 106
RRC
PDCP
PDCP
RLC
RLC
MAC
MAC
PHY
PHY
WLAN 104
Xw
WTP
110
202
AP
802.1x
링크
RRC
302
NAS
304
WWAN
데이터 308
WLAN
데이터 310
UE/STA 102

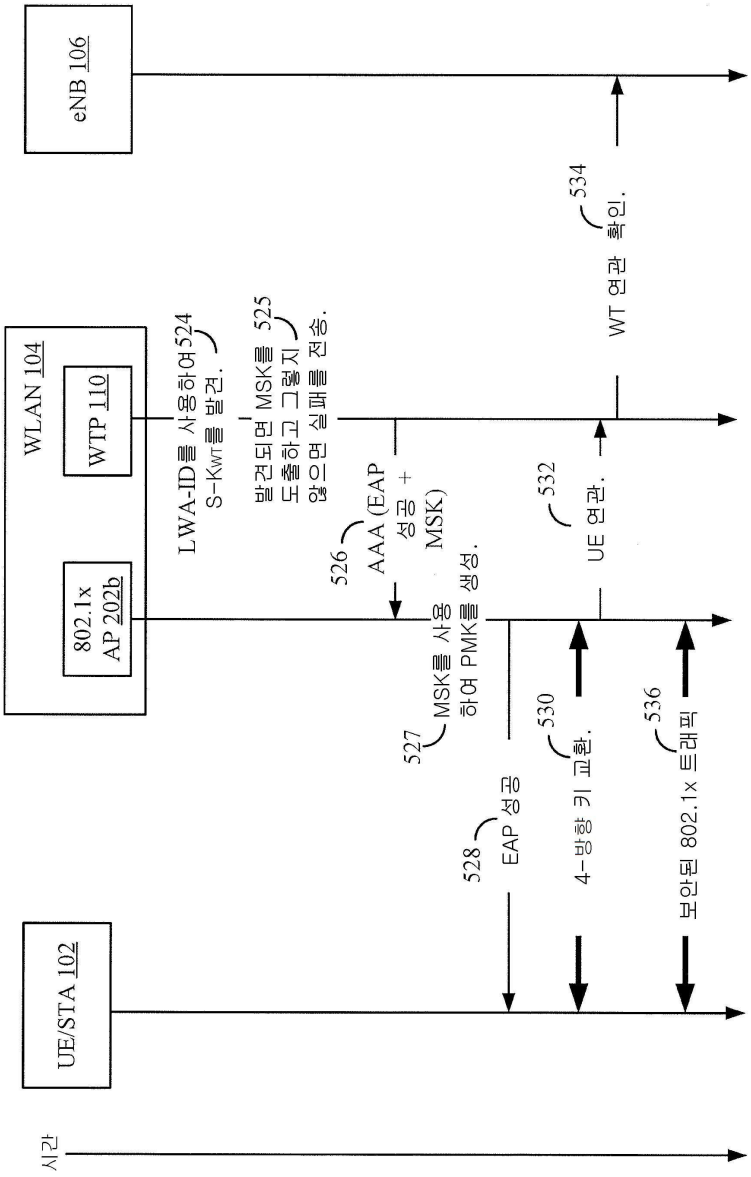
도면4


eNB 106
WLAN 104
WTP 110
LWA AP 202a
UE/STA 102
시간
402
WT 부가 요청 (UE MAC, S-KWT)
404
WT 부가 확인응답.
420
WT 연관 확인.
UE MAC, S-KWT
406
PMKID를 계산; PMKSA를 파플레이트.
408
WWAN 스택(예를 들어, LTE 스택)으로부터 PMK를 획득.
410
PMKID 및 PMKSA를 도출.
412
연관 요청 (PMKID).
413
PMKID를 사용하여 PMK, PMKSA를 발견.
414
연관 응답.
416
4-방향 키 교환.
418
UE 연관.
422
보안된 802.1x 트래픽

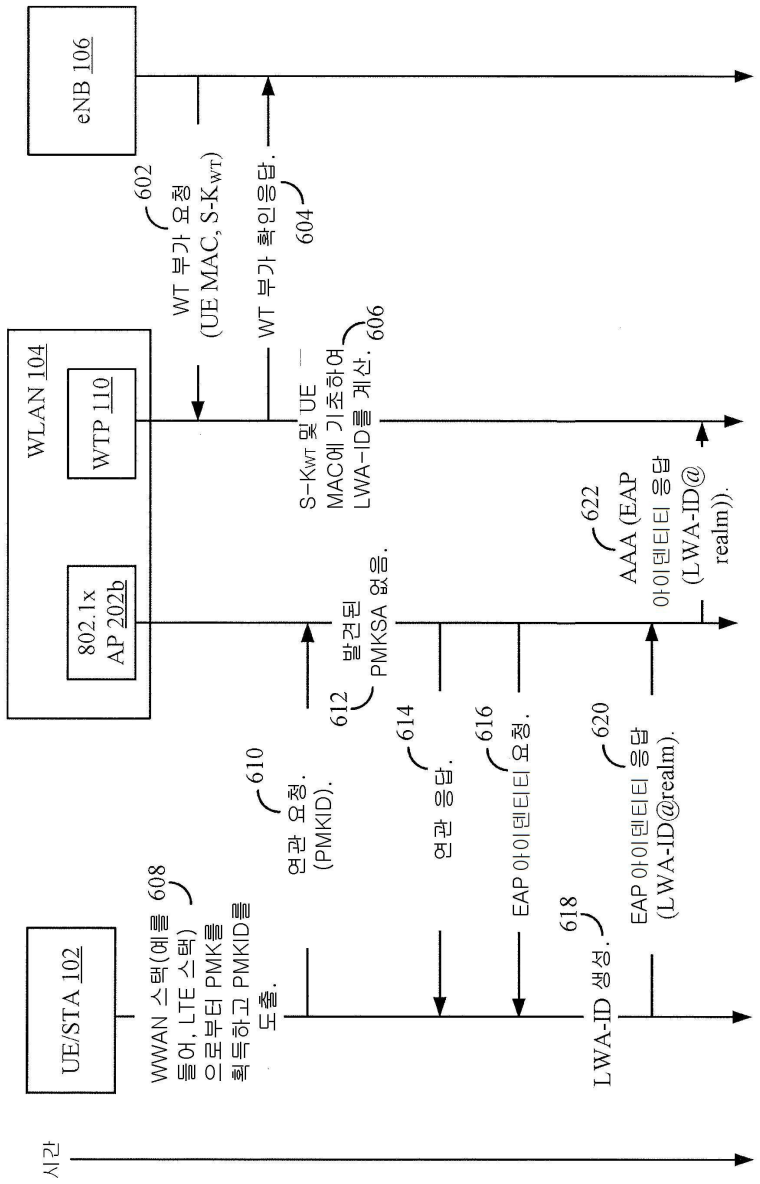
도면5a


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
502
WT 부가 요청 (UE MAC, S-K$_{WT}$)
504
WT 부가 확인응답.
506
S-K$_{WT}$ 및 UE MAC에 기초하여 LWA-ID를 계산.
508
WWAN 스택(예를 들어, LTE 스택)으로부터 PMK를 획득하고 PMKID를 도출.
510
연관 요청 (PMKID).
512
발견된 PMKSA 없음
514
연관 응답.
516
EAP 아이덴티티 요청.
518
LWA-ID 생성.
520
EAP 아이덴티티 응답 (LWA-ID@realm)).
522
AAA(EAP 아이덴티티 응답 (LWA-ID@realm)).

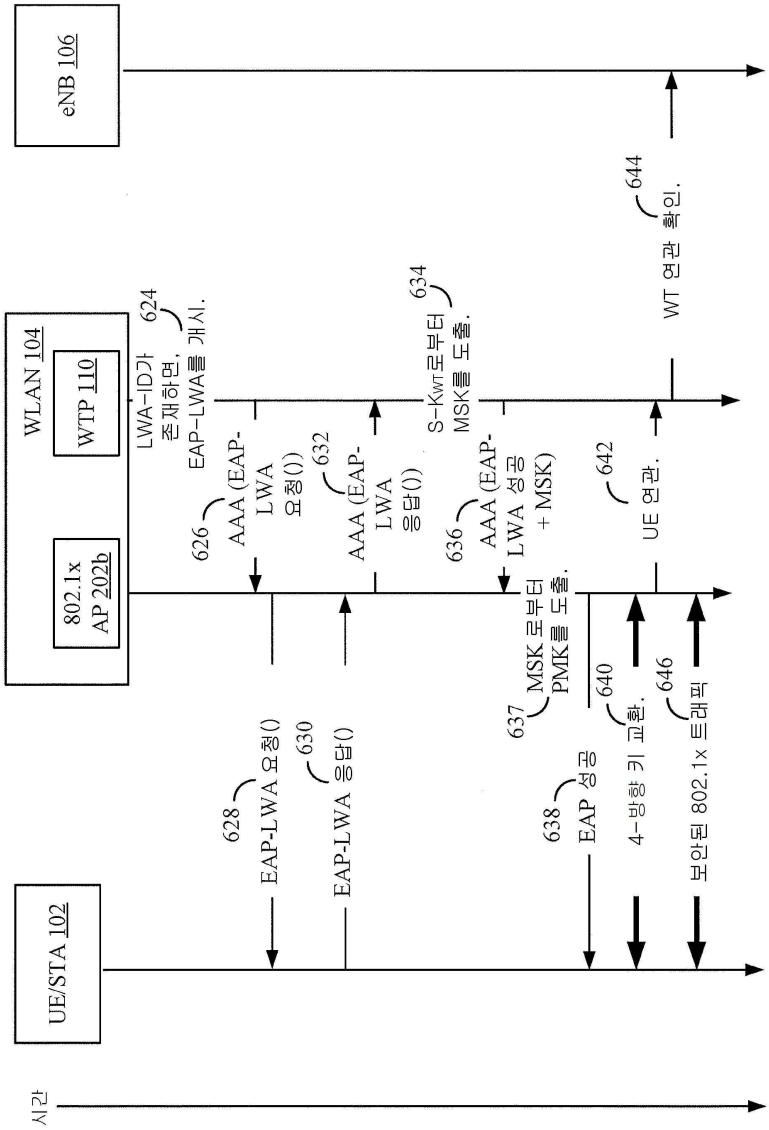
도면5b


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
LWA-ID를 사용하여 S-Kwt를 발견. 524
발견되면 MSK를 도출하고 그렇지 않으면 실패를 전송. 525
AAA (EAP 성공 + MSK) 526
MSK를 사용하여 PMK를 생성. 527
EAP 성공 528
4-방향 키 교환. 530
UE 연관. 532
WT 연관 확인. 534
보안된 802.1x 트래픽 536

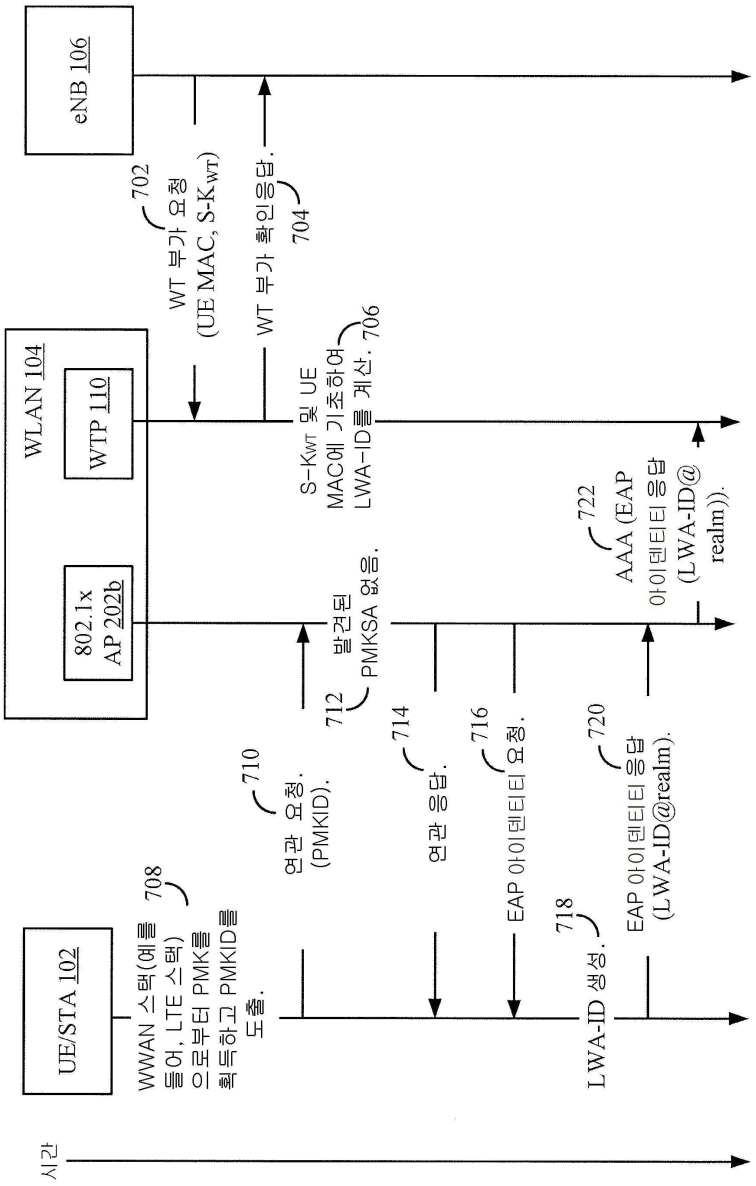
도면6a


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
602
WT 부가 요청 (UE MAC, S-K$_{WT}$)
604
WT 부가 확인응답.
606
S-K$_{WT}$ 및 UE MAC에 기초하여 LWA-ID를 계산.
608
WWAN 스택(예를 들어, LTE 스택)으로부터 PMK를 획득하고 PMKID를 도출.
610
연관 요청. (PMKID).
612
발견된 PMKSA 없음.
614
연관 응답.
616
EAP 아이덴티티 요청.
618
LWA-ID 생성.
620
EAP 아이덴티티 응답 (LWA-ID@realm).
622
AAA (EAP 아이덴티티 응답 (LWA-ID@realm)).

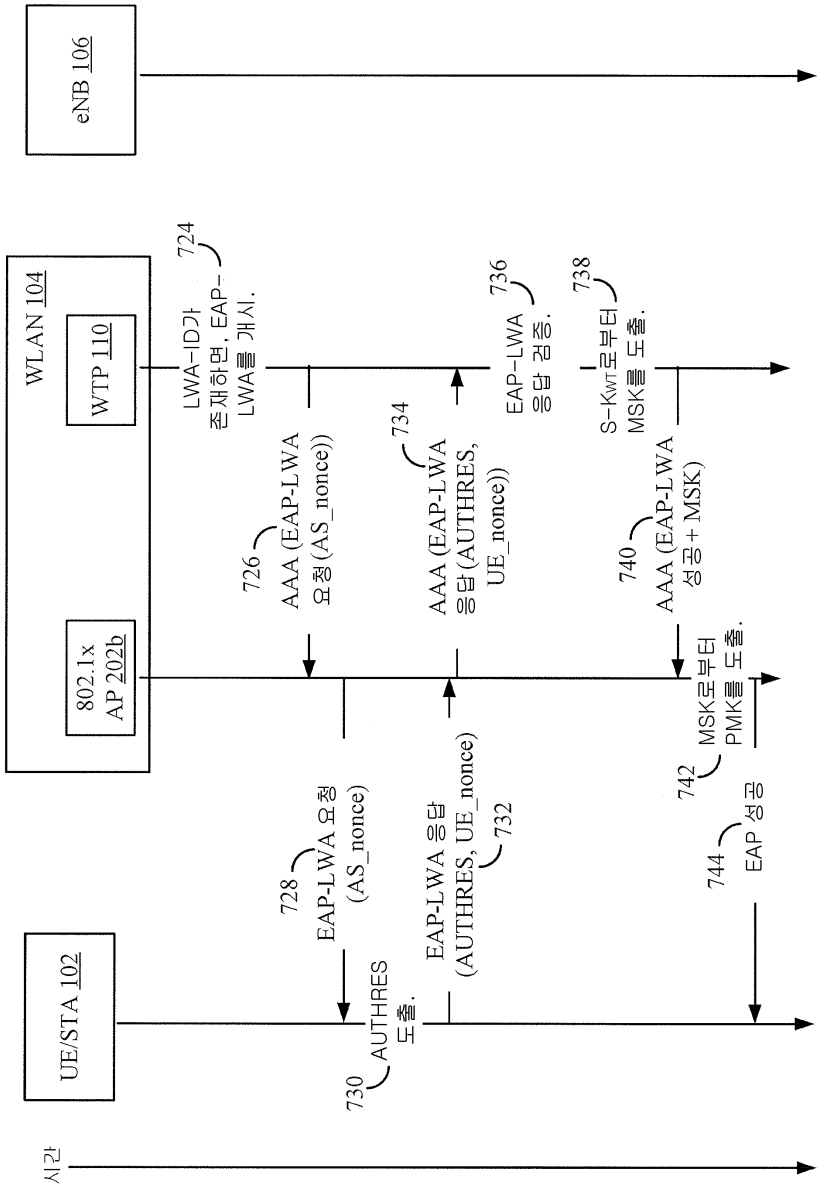
도면6b


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
624 LWA-ID가 존재하면, EAP-LWA를 개시.
626 AAA (EAP-LWA 요청())
628 EAP-LWA 요청()
630 EAP-LWA 응답()
632 AAA (EAP-LWA 응답())
634 S-KWT로부터 MSK를 도출.
636 AAA (EAP-LWA 성공 + MSK)
637 MSK 로부터 PMK를 도출.
638 EAP 성공
640 4-방향 키 교환.
642 UE 연관.
644 WT 연관 확인.
646 보안된 802.1x 트래픽

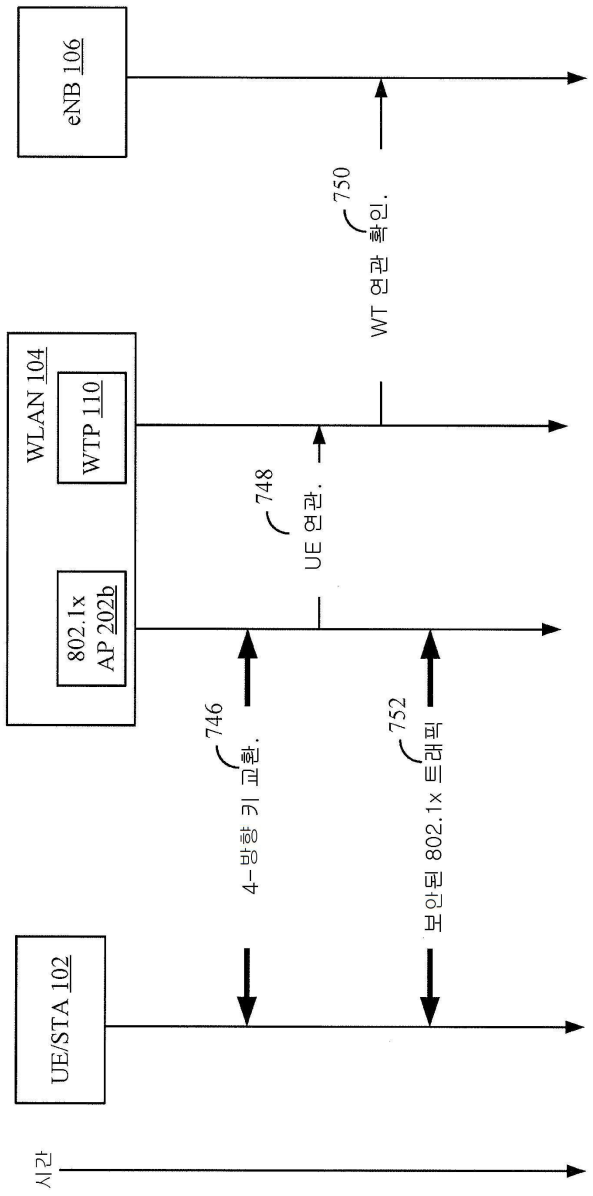
도면7a


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
WT 부가 요청 (UE MAC, S-K_WT) 702
WT 부가 확인응답. 704
S-K_WT 및 UE MAC에 기초하여 LWA-ID를 계산. 706
WWAN 스택(예를 들어, LTE 스택)으로부터 PMK를 획득하고 PMKID를 도출. 708
연관 요청. (PMKID). 710
발견된 PMKSA 없음. 712
연관 응답. 714
EAP 아이덴티티 요청. 716
LWA-ID 생성. 718
EAP 아이덴티티 응답 (LWA-ID@realm). 720
AAA (EAP 아이덴티티 응답 (LWA-ID@realm)). 722

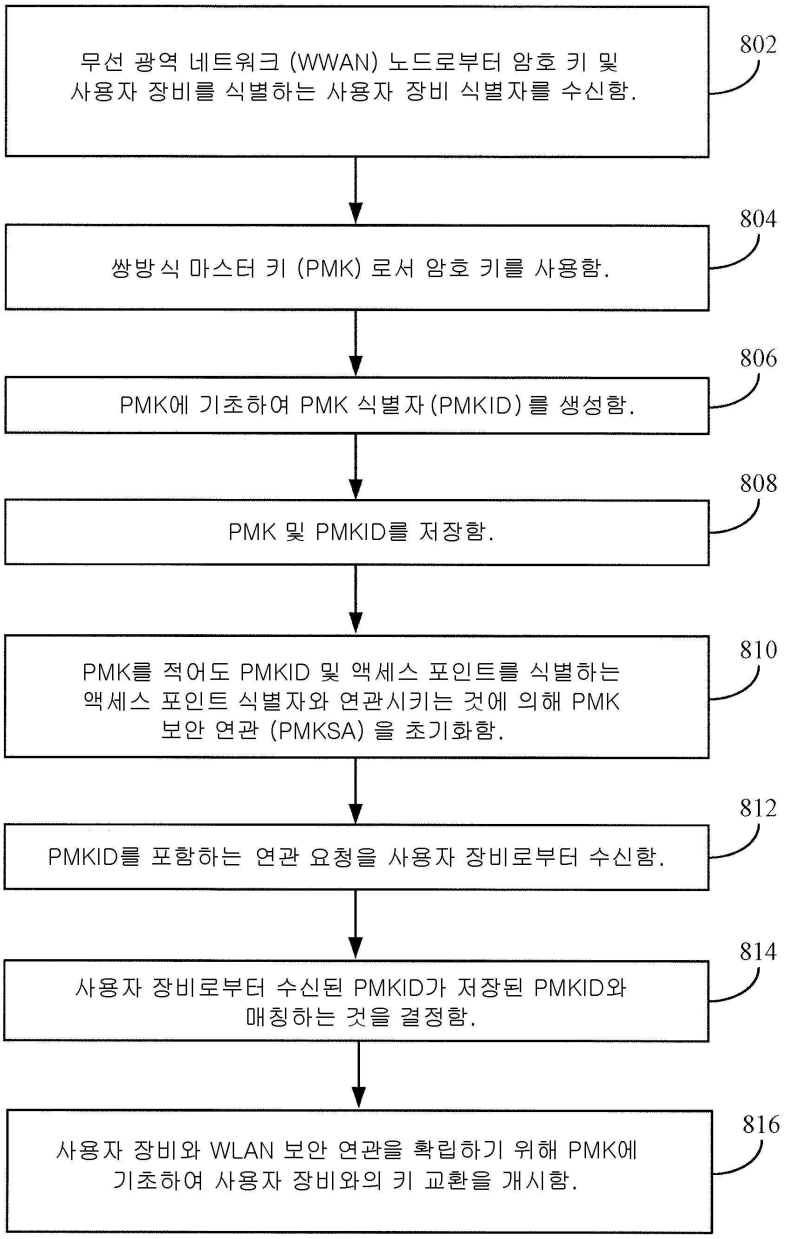
도면7b


eNB 106
WLAN 104
WTP 110
802.1x AP 202b
UE/STA 102
시간
724
LWA-ID가 존재하면, EAP-LWA를 개시.
726
AAA (EAP-LWA 요청 (AS_nonce))
728
EAP-LWA 요청 (AS_nonce)
730
AUTHRES 도출.
732
EAP-LWA 응답 (AUTHRES, UE_nonce)
734
AAA (EAP-LWA 응답 (AUTHRES, UE_nonce))
736
EAP-LWA 응답 검증.
738
S-KWT로부터 MSK를 도출.
740
AAA (EAP-LWA 성공 + MSK)
742
MSK로부터 PMK를 도출.
744
EAP 성공

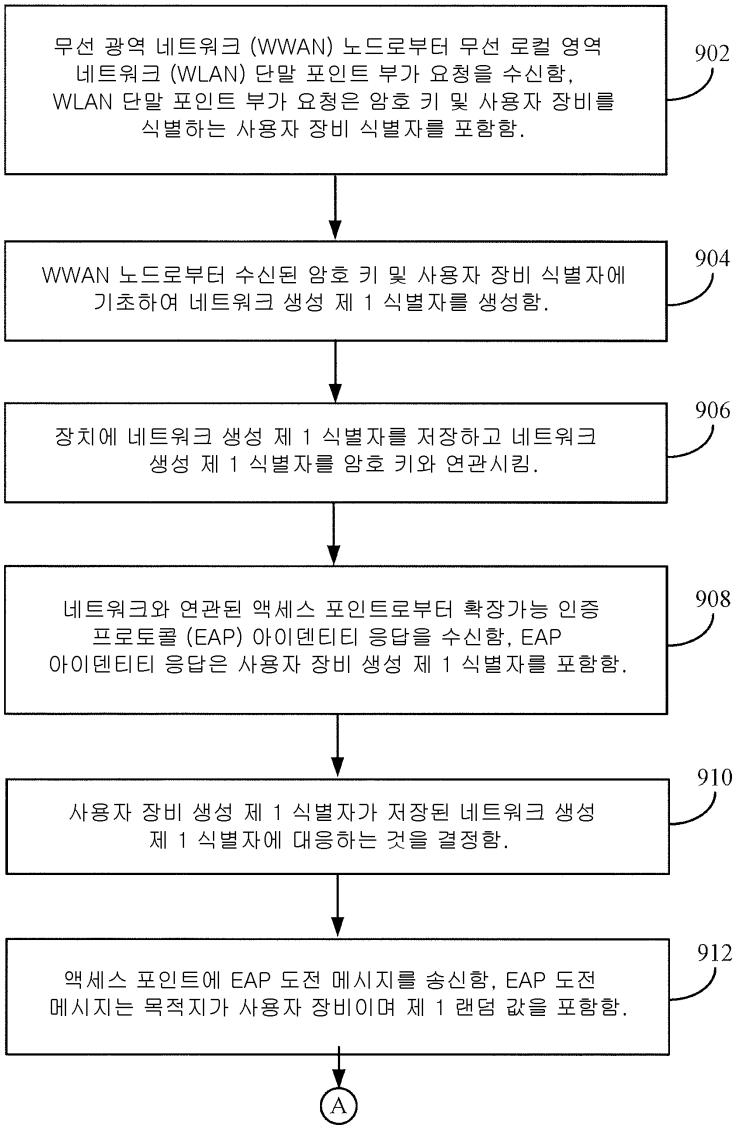
도면7c


eNB 106
750
WT 연관 확인.
WLAN 104
WTP 110
748
UE 연관.
802.1x
AP 202b
746
4-방향 키 교환.
752
보안된 802.1x 트래픽
UE/STA 102
시간

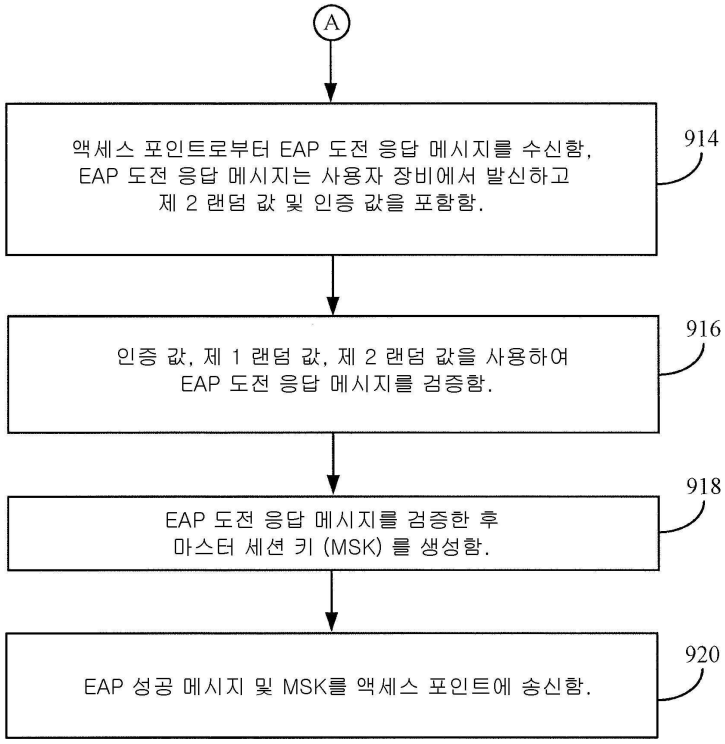
도면8


무선 광역 네트워크 (WWAN) 노드로부터 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 수신함.
802
쌍방식 마스터 키 (PMK) 로서 암호 키를 사용함.
804
PMK에 기초하여 PMK 식별자(PMKID)를 생성함.
806
PMK 및 PMKID를 저장함.
808
PMK를 적어도 PMKID 및 액세스 포인트를 식별하는 액세스 포인트 식별자와 연관시키는 것에 의해 PMK 보안 연관 (PMKSA) 을 초기화함.
810
PMKID를 포함하는 연관 요청을 사용자 장비로부터 수신함.
812
사용자 장비로부터 수신된 PMKID가 저장된 PMKID와 매칭하는 것을 결정함.
814
사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK에 기초하여 사용자 장비와의 키 교환을 개시함.
816

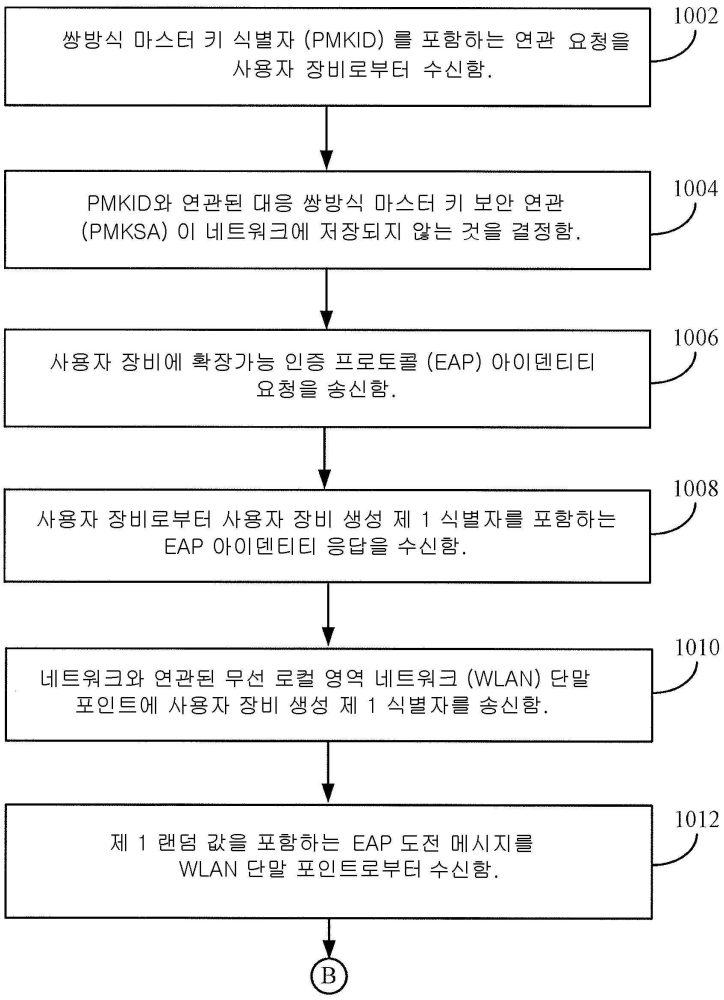
도면9a


무선 광역 네트워크 (WWAN) 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신함, WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함함.
902
WWAN 노드로부터 수신된 암호 키 및 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성함.
904
장치에 네트워크 생성 제 1 식별자를 저장하고 네트워크 생성 제 1 식별자를 암호 키와 연관시킴.
906
네트워크와 연관된 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신함, EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함함.
908
사용자 장비 생성 제 1 식별자가 저장된 네트워크 생성 제 1 식별자에 대응하는 것을 결정함.
910
액세스 포인트에 EAP 도전 메시지를 송신함, EAP 도전 메시지는 목적지가 사용자 장비이며 제 1 랜덤 값을 포함함.
912
A

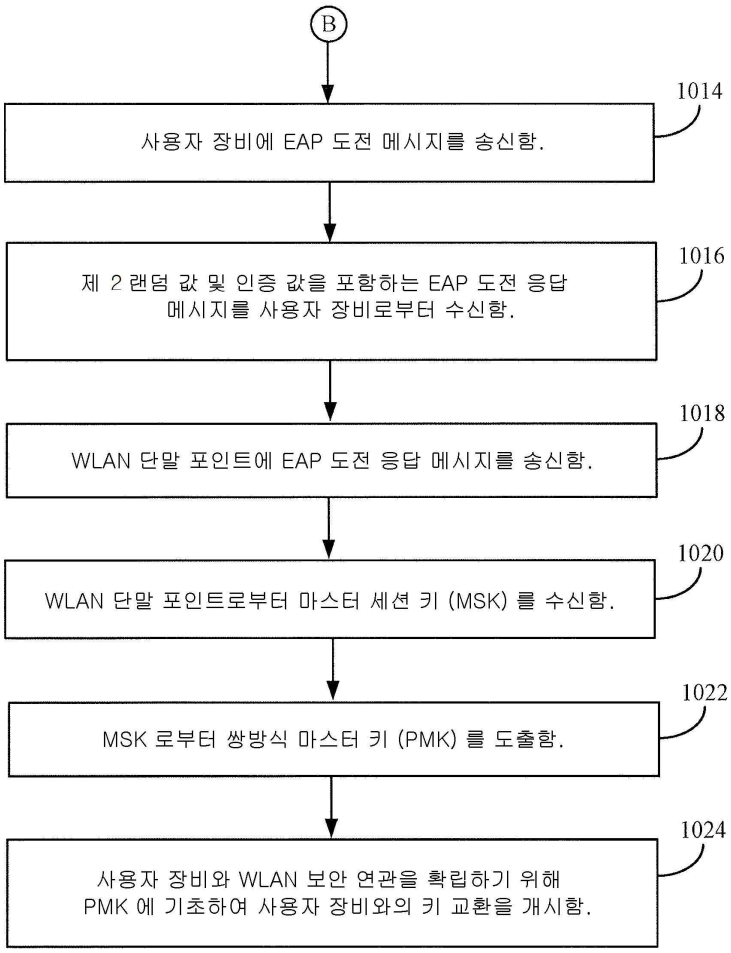
도면9b


A
액세스 포인트로부터 EAP 도전 응답 메시지를 수신함,
EAP 도전 응답 메시지는 사용자 장비에서 발신하고
제 2 랜덤 값 및 인증 값을 포함함.
914
인증 값, 제 1 랜덤 값, 제 2 랜덤 값을 사용하여
EAP 도전 응답 메시지를 검증함.
916
EAP 도전 응답 메시지를 검증한 후
마스터 세션 키 (MSK) 를 생성함.
918
EAP 성공 메시지 및 MSK를 액세스 포인트에 송신함.
920

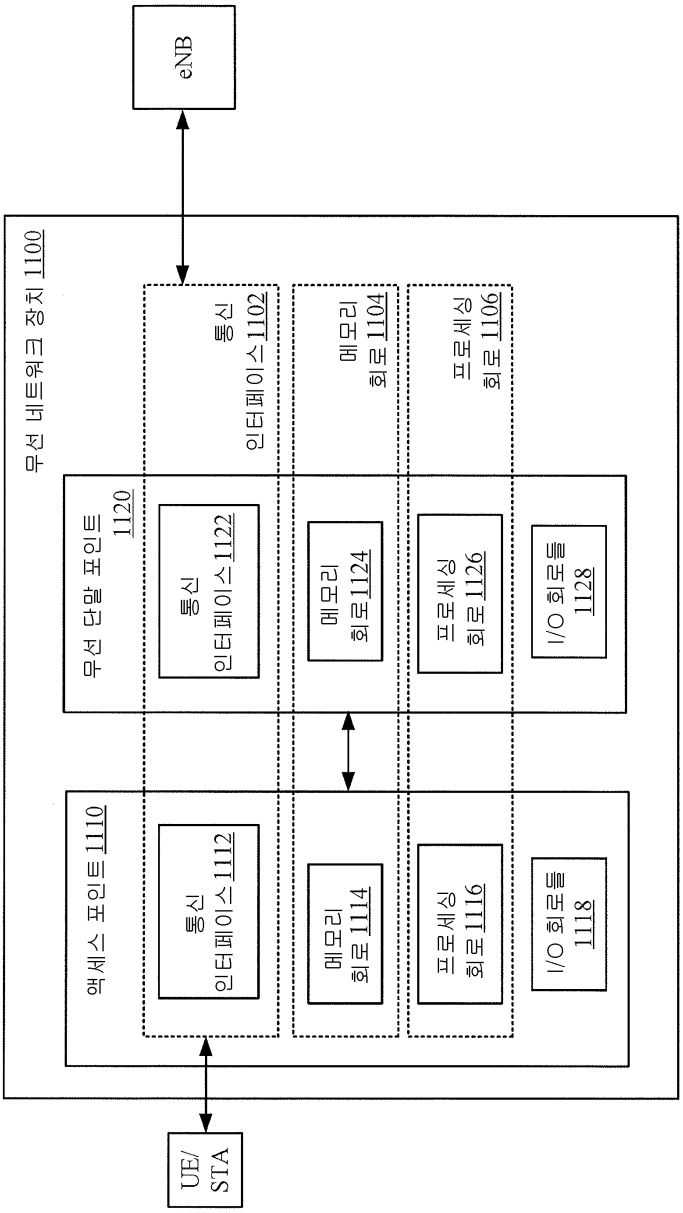
도면10a


쌍방식 마스터 키 식별자 (PMKID) 를 포함하는 연관 요청을 사용자 장비로부터 수신함.
1002
PMKID와 연관된 대응 쌍방식 마스터 키 보안 연관 (PMKSA) 이 네트워크에 저장되지 않는 것을 결정함.
1004
사용자 장비에 확장가능 인증 프로토콜 (EAP) 아이덴티티 요청을 송신함.
1006
사용자 장비로부터 사용자 장비 생성 제 1 식별자를 포함하는 EAP 아이덴티티 응답을 수신함.
1008
네트워크와 연관된 무선 로컬 영역 네트워크 (WLAN) 단말 포인트에 사용자 장비 생성 제 1 식별자를 송신함.
1010
제 1 랜덤 값을 포함하는 EAP 도전 메시지를 WLAN 단말 포인트로부터 수신함.
1012
B

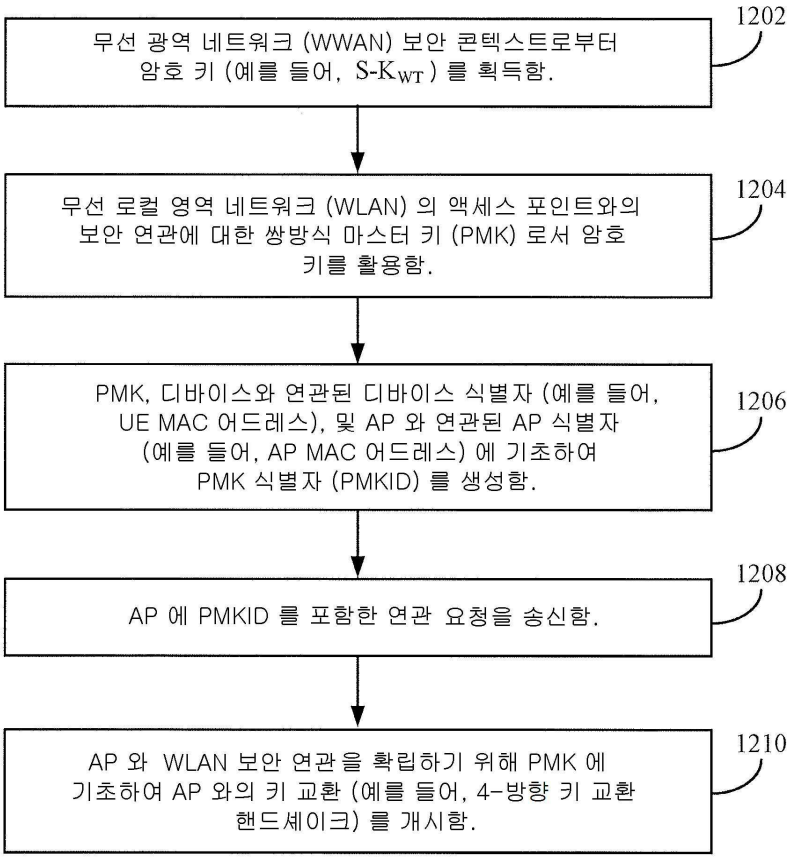
도면10b


B
1014
사용자 장비에 EAP 도전 메시지를 송신함.
1016
제 2 랜덤 값 및 인증 값을 포함하는 EAP 도전 응답 메시지를 사용자 장비로부터 수신함.
1018
WLAN 단말 포인트에 EAP 도전 응답 메시지를 송신함.
1020
WLAN 단말 포인트로부터 마스터 세션 키 (MSK) 를 수신함.
1022
MSK 로부터 쌍방식 마스터 키 (PMK) 를 도출함.
1024
사용자 장비와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 사용자 장비와의 키 교환을 개시함.

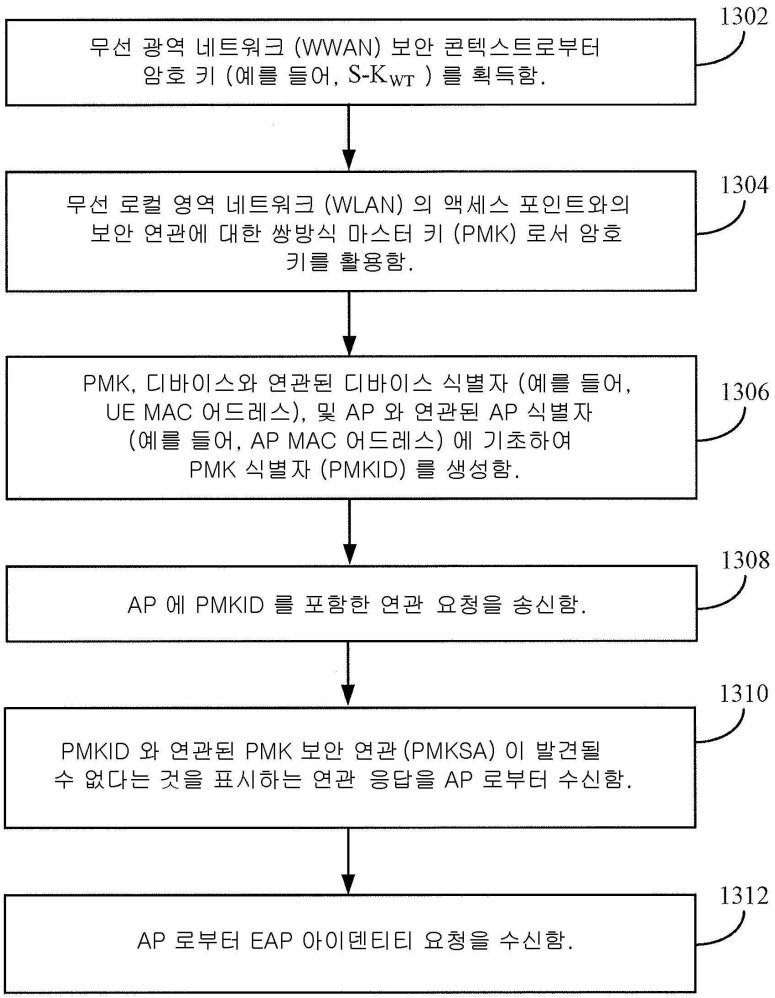
도면11


eNB
무선 네트워크 장치 1100
통신 인터페이스 1102
메모리 회로 1104
프로세싱 회로 1106
무선 단말 포인트 1120
통신 인터페이스 1122
메모리 회로 1124
프로세싱 회로 1126
I/O 회로들 1128
액세스 포인트 1110
통신 인터페이스 1112
메모리 회로 1114
프로세싱 회로 1116
I/O 회로들 1118
UE/ STA

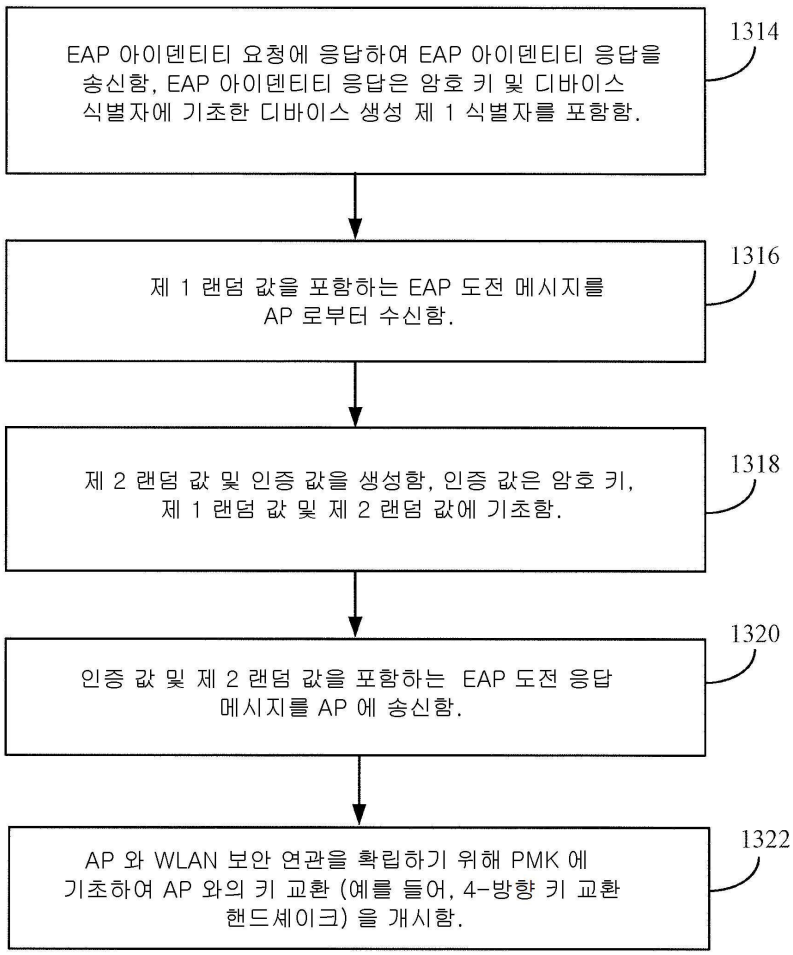
도면12


무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키 (예를 들어, S-K_{WT}) 를 획득함.
1202
무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 암호 키를 활용함.
1204
PMK, 디바이스와 연관된 디바이스 식별자 (예를 들어, UE MAC 어드레스), 및 AP 와 연관된 AP 식별자 (예를 들어, AP MAC 어드레스) 에 기초하여 PMK 식별자 (PMKID) 를 생성함.
1206
AP 에 PMKID 를 포함한 연관 요청을 송신함.
1208
AP 와 WLAN 보안 연관을 확립하기 위해 PMK 에 기초하여 AP 와의 키 교환 (예를 들어, 4-방향 키 교환 핸드셰이크) 를 개시함.
1210

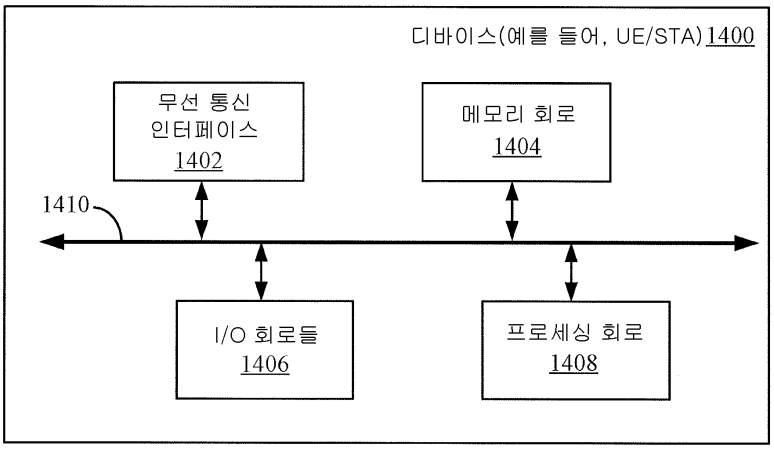
도면13a


무선 광역 네트워크 (WWAN) 보안 콘텍스트로부터 암호 키 (예를 들어, S-K_{WT}) 를 획득함.
1302
무선 로컬 영역 네트워크 (WLAN) 의 액세스 포인트와의 보안 연관에 대한 쌍방식 마스터 키 (PMK) 로서 암호 키를 활용함.
1304
PMK, 디바이스와 연관된 디바이스 식별자 (예를 들어, UE MAC 어드레스), 및 AP 와 연관된 AP 식별자 (예를 들어, AP MAC 어드레스) 에 기초하여 PMK 식별자 (PMKID) 를 생성함.
1306
AP 에 PMKID 를 포함한 연관 요청을 송신함.
1308
PMKID 와 연관된 PMK 보안 연관 (PMKSA) 이 발견될 수 없다는 것을 표시하는 연관 응답을 AP 로부터 수신함.
1310
AP 로부터 EAP 아이덴티티 요청을 수신함.
1312

도면13b



도면14



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 24

【변경전】

장치로서,

네트워크와 연관된 장치를 포함하고, 상기 방법은,

메모리 회로:

무선 광역 네트워크 (WWAN) 노드와 통신하도록 적응된 제 1 통신 인터페이스;

액세스 포인트와 통신하도록 적응된 제 2 통신 인터페이스; 및

상기 메모리 회로, 상기 제 1 통신 인터페이스 및 상기 제 2 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 WWAN 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 것으로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하고;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하고;

상기 네트워크 생성 제 1 식별자를 상기 메모리 회로에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키고;

상기 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하는 것으로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하고;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하고;

마스터 세션 키 (MSK) 를 생성하며; 그리고

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하도록 적응되는, 장치.

【변경후】

장치로서,

네트워크와 연관된 장치를 포함하고,

메모리 회로:

무선 광역 네트워크 (WWAN) 노드와 통신하도록 적응된 제 1 통신 인터페이스;

액세스 포인트와 통신하도록 적응된 제 2 통신 인터페이스; 및

상기 메모리 회로, 상기 제 1 통신 인터페이스 및 상기 제 2 통신 인터페이스에 통신가능하게 커플링된 프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 WWAN 노드로부터 무선 로컬 영역 네트워크 (WLAN) 단말 포인트 부가 요청을 수신하는 것으로서, 상기 WLAN 단말 포인트 부가 요청은 암호 키 및 사용자 장비를 식별하는 사용자 장비 식별자를 포함하는, 상기 WLAN 단말 포인트 부가 요청을 수신하고;

상기 WWAN 노드로부터 수신된 상기 암호 키 및 상기 사용자 장비 식별자에 기초하여 네트워크 생성 제 1 식별자를 생성하고;

상기 네트워크 생성 제 1 식별자를 상기 메모리 회로에 저장하고 상기 네트워크 생성 제 1 식별자를 상기 암호 키와 연관시키고;

상기 액세스 포인트로부터 확장가능 인증 프로토콜 (EAP) 아이덴티티 응답을 수신하는 것으로서, 상기 EAP 아이덴티티 응답은 사용자 장비 생성 제 1 식별자를 포함하는, 상기 EAP 아이덴티티 응답을 수신하고;

상기 사용자 장비 생성 제 1 식별자가, 저장된 상기 네트워크 생성 제 1 식별자에 대응하는 것을 결정하고;

마스터 세션 키 (MSK) 를 생성하며; 그리고

EAP 성공 메시지 및 상기 MSK 를 상기 액세스 포인트에 송신하도록 적응되는, 장치.