(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0132184
(43) 공개일자 2017년12월01일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
H04W 12/04 (2009.01) *H04W 12/06* (2009.01)
(52) CPC특허분류
H04L 63/067 (2013.01)
H04L 63/0428 (2013.01)
(21) 출원번호 10-2017-7027573
(22) 출원일자(국제) 2016년03월03일
심사청구일자 없음
(85) 번역문제출일자 2017년09월27일
(86) 국제출원번호 PCT/US2016/020545
(87) 국제공개번호 WO 2016/160256
국제공개일자 2016년10월06일
(30) 우선권주장
62/140,331 2015년03월30일 미국(US)
(뒷면에 계속)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
파라니군더, 아난드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

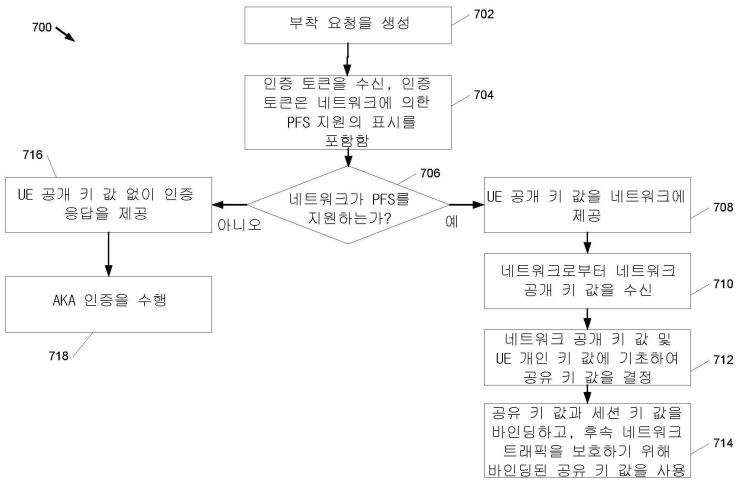
전체 청구항 수 : 총 30 항

(54) 발명의 명칭 **완전 순방향 비밀성을 통한 인증 및 키 합의**

(57) 요 약

PFS(perfect forward secrecy)를 갖는 AKA(authentication key agreement)를 제공하기 위한 시스템들 및 방법들이 개시된다. 일 실시예에서, 본 개시에 따른 네트워크는 UE로부터 부착 요청을 수신하고, 네트워크 지원 표시자를 포함하는 인증 요청을 네트워크 자원에 제공하고, 네트워크 자원으로부터 인증 토큰을 수신하고 – 인증 토큰이 네트워크가 PFS를 지원한다는 표시를 포함함 – , 인증 토큰을 UE에 제공하고, UE 공개 키 값을 포함하는 인증 응답을 수신하고, 네트워크 공개 키 값 및 네트워크 개인 키 값을 획득하고, 네트워크 개인 키 값 및 상기 UE 공개 키 값에 기초하여 공유 키 값을 결정하고, 바인딩된 공유 키 값을 생성하기 위해 공유 키 값과 세션 키 값을 바인딩하고, 그리고 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용할 수 있다.

대 표 도 - 도7



(52) CPC특허분류
H04L 63/0869 (2013.01)
H04L 9/0841 (2013.01)
H04L 9/085 (2013.01)
H04L 9/0891 (2013.01)
H04L 9/3066 (2013.01)
H04L 9/3242 (2013.01)
H04W 12/04 (2013.01)
H04W 12/06 (2013.01)

(30) 우선권주장
62/140,426 2015년03월30일 미국(US)
14/825,988 2015년08월13일 미국(US)

명 세 서

청구범위

청구항 1

사용자 장비와 네트워크 간에 PFS(perfect forward secrecy)를 갖는 인증 및 키 합의 프로토콜(authentication and key agreement protocol)을 제공하기 위한 방법으로서,

상기 사용자 장비를 통해, 부착 요청(attach request)을 생성하는 단계;

상기 사용자 장비를 통해, 상기 네트워크에 의한 PFS 지원의 표시를 포함하는 인증 토큰(authentication token)을 수신하는 단계;

상기 사용자 장비를 통해, 상기 네트워크가 PFS를 지원하는지를 결정하는 단계;

상기 사용자 장비를 통해, UE 공개 키 값(public key value)을 상기 네트워크에 제공하는 단계;

상기 사용자 장비를 통해, 상기 네트워크로부터 네트워크 공개 키 값을 수신하는 단계;

상기 사용자 장비를 통해, 상기 네트워크 공개 키 값 및 UE 개인 키 값(private key value)에 기초하여 공유 키 값을 결정하는 단계;

상기 사용자 장비를 통해, 바인딩된 공유 키 값을 생성하기 위해 상기 공유 키 값과 세션 키 값(session key value)을 바인딩하는 단계; 및

상기 사용자 장비를 통해, 후속 네트워크 트래픽을 보호하기 위해 상기 바인딩된 공유 키 값을 사용하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 부착 요청은 상기 사용자 장비가 PFS를 지원한다는 표시를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 사용자 장비를 통해, 부착 요청을 생성하는 단계는, 서비스 요청, 영역 추적 요청 또는 위치 업데이트 요청 중 하나를 생성하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 4

제 1 항에 있어서,

상기 사용자 장비를 통해, 상기 공유 키 값과 세션 키 값을 바인딩하는 단계는, 상기 공유 키 값 및/또는 상기 세션 키 값의 암호 해시(cryptographic hash)를 결정하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 5

제 1 항에 있어서,

상기 세션 키 값은 K_{ASME}인,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 6

제 1 항에 있어서,

상기 세션 키 값은 CK(Cipher Key) 또는 IK(Integrity Key) 중 적어도 하나인,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 7

제 1 항에 있어서,

상기 UE 공개 키 값을 상기 네트워크에 제공하는 단계는, 상기 사용자 장비를 통해, 타원-곡선 암호학(elliptic-curve cryptography)을 사용하여 임시적(ephemeral) Diffie-Hellman 쌍을 생성하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 8

제 1 항에 있어서,

상기 UE 공개 키 값을 상기 네트워크에 제공하는 단계는, 상기 사용자 장비를 통해, 유한 필드 연산(finite field arithmetic)을 사용하여 임시적 Diffie-Hellman 쌍을 생성하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 9

제 1 항에 있어서,

상기 네트워크가 PFS를 지원하지 않는다고 상기 UE가 결정하면, 상기 네트워크에 대한 연결을 거부하는 단계를 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 10

제 1 항에 있어서,

상기 인증 토큰은, 상기 네트워크가 PFS를 지원한다는 것을 표시하도록 구성된 AMF(authentication management field) 비트 값을 포함하는,

사용자 장비와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 방법.

청구항 11

사용자 장비(UE)와 네트워크 간에 PFS(perfect forward secrecy)를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치로서,

메모리; 상기 메모리에 동작 가능하게 커플링된 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는:

UE로부터 부착 요청을 수신하고; 네트워크 지원 표시자를 포함하는 인증 요청을 네트워크 자원에 제공하고;

상기 네트워크 자원으로부터 인증 토큰을 수신하고 – 상기 인증 토큰은 네트워크가 PFS를 지원한다는 표시를 포함함 – ;

상기 인증 토큰을 상기 UE에 제공하고; UE 공개 키 값을 포함하는 인증 응답을 수신하고;

상기 인증 응답이 예상된 응답이 아니면, 상기 부착 요청을 거부하고;

상기 인증 응답이 상기 예상된 응답이면,

네트워크 공개 키 값 및 네트워크 개인 키 값을 획득하고;

상기 네트워크 개인 키 값 및 상기 UE 공개 키 값에 기초하여 공유 키 값을 결정하고;

바인딩된 공유 키 값을 생성하기 위해 상기 공유 키 값과 세션 키 값을 바인딩하고; 그리고

후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용하도록 구성되는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 12

제 11 항에 있어서,

상기 인증 토큰은 상기 UE와 상기 네트워크 자원 간에 무결성 보호되는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 13

제 11 항에 있어서,

상기 적어도 하나의 프로세서는, 부착 요청 대신에, 서비스 요청, 영역 추적 요청 또는 위치 업데이트 요청 중 하나를 수신함으로써 상기 UE로부터 상기 부착 요청을 수신하도록 구성되는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 14

제 11 항에 있어서,

상기 적어도 하나의 프로세서는 상기 공유 키 값 및 상기 세션 키 값의 암호 해시를 결정하도록 구성되는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 15

제 11 항에 있어서,

상기 세션 키 값은 K_{ASME}, CK(Cipher Key) 또는 IK(Integrity Key) 중 적어도 하나인,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 16

제 11 항에 있어서,

상기 공유 키 값은 타원-곡선 암호학 또는 유한 필드 연산(finite field arithmetic) 중 하나에 의해 결정되는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 17

제 11 항에 있어서,

상기 부착 요청은, 상기 UE가 PFS를 지원한다는 표시를 포함하는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 18

제 11 항에 있어서,

상기 인증 토큰은, 상기 네트워크가 PFS를 지원한다는 것을 표시하기 위한 AMF(authentication management field) 비트 값을 포함하는,

UE와 네트워크 간에 PFS를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 장치.

청구항 19

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격(bid-down attack)을 방지하기 위한 방법으로서,

사용자 장비로부터 부착 요청을 수신하는 단계;

인증 요청을 홈 네트워크로 전송하는 단계 - 상기 인증 요청은, 네트워크가 상기 강한 보안 프로토콜을 지원한다는 표시를 포함함 - ;

상기 홈 네트워크로부터 무결성 보호 토큰을 수신하는 단계 - 상기 무결성 보호 토큰은, 상기 네트워크가 상기 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함함 - ; 및

상기 무결성 보호 토큰을 상기 사용자 장비로 전송하는 단계를 포함하는,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 20

제 19 항에 있어서,

상기 부착 요청은 상기 사용자 장비가 상기 강한 보안 프로토콜을 지원한다는 표시를 포함하는,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 21

제 19 항에 있어서,

상기 강한 보안 프로토콜은 완전 순방향 비밀성을 갖는 인증 및 키 합의 프로토콜인,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 22

제 19 항에 있어서,

상기 인증 요청은, 상기 네트워크가 상기 강한 보안 프로토콜을 지원한다는 것을 표시하기 위한 정보 엘리먼트들로서 AVP(Attribute Value Pairs)를 갖는 다이어미터 프로토콜 메시지(diameter protocol message)인,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 23

제 19 항에 있어서,

상기 무결성 보호 토큰은 상기 홈 네트워크로부터 수신된 인증 벡터에 포함되는,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 24

제 23 항에 있어서,

상기 적어도 하나의 비트는 AMF(Authentication Management Field)에 포함되는,

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 방법.

청구항 25

강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 명령들을 포함하는 비일시적인 프로세서-판독 가능 저장 매체로서, 상기 명령들은:

사용자 장비로부터 부착 요청을 수신하기 위한 코드;

인증 요청을 홈 네트워크로 전송하기 위한 코드 - 상기 인증 요청은, 네트워크가 상기 강한 보안 프로토콜을

지원한다는 표시를 포함함 - ;

상기 홈 네트워크로부터 무결성 보호 토큰을 수신하기 위한 코드 - 상기 무결성 보호 토큰은, 상기 네트워크가 상기 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함함 - ; 및

상기 무결성 보호 토큰을 상기 사용자 장비로 전송하기 위한 코드를 포함하는,

비일시적인 프로세서-판독 가능 저장 매체.

청구항 26

제 25 항에 있어서,

상기 부착 요청은 상기 사용자 장비가 상기 강한 보안 프로토콜을 지원한다는 표시를 포함하는,

비일시적인 프로세서-판독 가능 저장 매체.

청구항 27

제 25 항에 있어서,

상기 강한 보안 프로토콜은 완전 순방향 비밀성을 갖는 인증 및 키 합의 프로토콜인,

비일시적인 프로세서-판독 가능 저장 매체.

청구항 28

제 25 항에 있어서,

상기 인증 요청은, 상기 네트워크가 상기 강한 보안 프로토콜을 지원한다는 것을 표시하기 위한 정보 엘리먼트들로서 AVP(Attribute Value Pairs)를 갖는 다이어미터 프로토콜 메시지인,

비일시적인 프로세서-판독 가능 저장 매체.

청구항 29

제 25 항에 있어서,

상기 무결성 보호 토큰은 상기 홈 네트워크로부터 수신된 인증 벡터에 포함되는,

비일시적인 프로세서-판독 가능 저장 매체.

청구항 30

제 29 항에 있어서,

상기 적어도 하나의 비트는 AMF(Authentication Management Field)에 포함되는,

비일시적인 프로세서-판독 가능 저장 매체.

발명의 설명

기 술 분 야

[0001] [0001] 본 출원은 2015년 3월 30일에 출원되고 명칭이 "Authentication and Key Agreement with Perfect Forward Secrecy"인 미국 가출원 제 62/140,331 호, 2015년 3월 30일에 출원되고 명칭이 "Authentication and Key Agreement with Perfect Forward Secrecy"인 미국 가출원 제 62/140,426 호, 및 2015년 8월 13일에 출원되고 명칭이 "Authentication and Key Agreement with Perfect Forward Secrecy"인 미국 특허 출원 제 14/825,988 호를 우선권으로 주장하고, 상기 출원들 각각은 본 출원의 양수인에게 양도되고, 그들의 내용들이 전체적으로 본원에 인용에 의해 통합된다.

배 경 기 술

[0002] [0002] 일반적으로, 무선 통신 시스템은 네트워크와 네트워크를 액세스하려고 시도하는 디바이스 간의 인증 절

차들을 가능하게 할 수 있다. 상이한 네트워크들은 상이한 인증 절차들을 가질 수 있다. 디바이스는, 네트워크에 대한 액세스를 제공하기 전에, 디바이스를 인증하는데 사용되는 보안 크리덴셜들(security credentials)을 포함할 수 있다. 일부 시스템들에서, 기밀의 통신들은, 디바이스 상의 모듈에 저장되고 디바이스를 호스트 네트워크에 커플링하는 보안 크리덴셜들을 사용할 수 있다. 예를 들면, 널리 사용되는 AKA(Authentication and Key Agreement) 프로토콜은, 디바이스(예를 들면, 제거 가능한 USIM(Universal Subscriber Identity Module))와 네트워크(예를 들면, HSS(Home Subscriber Server)) 간에 안전하게 공유되는 대칭적인 루트 키(K)에 의존한다. 다른 네트워크들은 보안 교환들을 실현하기 위해 다른 타입들의 암호 보증들(cryptographic assurances)을 제공할 수 있다.

[0003] [0003] AKA를 사용하는 기존의 무선 네트워크들에서, 장기간 루트 키(예를 들면, K)가 훼손되면, 모든 과거의 통신들의 기밀성(confidentiality)이 훼손될 수 있다는 위험성이 존재한다. 즉, 공격자는 과거의 암호화된 통신들을 캡처하고, 일단 장기간 루트 키(K)가 훼손되면 이를 암호해독할 수 있다. (예를 들면, 약한 그리고 강한) 상이한 레벨들의 암호 보증들을 제공할 수 있는 네트워크들은, 강한 암호 보증이 더 약한 솔루션으로 비드-다운(bid-down)될 수 있어서, 중간자 공격(man-in-the-middle attack)에 취약할 수 있다는 위험성이 또한 존재한다.

발명의 내용

[0004] [0004] 다음은 논의되는 기술의 기본적인 이해를 제공하기 위해 본 개시의 일부 양상들을 요약한다. 이러한 요약은 본 개시의 모든 고려되는 특징들의 광범위한 개관이 아니며, 본 개시의 모든 양상들의 핵심적이거나 중요한 엘리먼트들을 식별하거나 본 개시의 임의의 또는 모든 양상의 범위를 설명하도록 의도되지 않는다. 그의 유일한 목적은 나중에 제공되는 더 상세한 설명에 대한 서두로서 본 개시의 하나 이상의 양상들의 일부 개념들을 요약 형태로 제공하는 것이다.

[0005] [0005] 본 개시에 따른 사용자 장비와 네트워크 간에 PFS(perfect forward secrecy)를 갖는 인증 및 키 합의 프로토콜(authentication and key agreement protocol)을 제공하기 위한 방법의 예는 사용자 장비를 통해, 부착 요청(attach request)을 생성하는 단계, 사용자 장비를 통해, 인증 토큰(authentication token)을 수신하는 단계 – 인증 토큰은 네트워크에 의한 PFS 지원의 표시를 포함함 – 사용자 장비를 통해, 네트워크가 PFS를 지원한다고 결정하는 단계, 사용자 장비를 통해, UE 공개 키 값(public key value)을 네트워크에 제공하는 단계, 사용자 장비를 통해, 네트워크로부터 네트워크 공개 키 값을 수신하는 단계, 사용자 장비를 통해, 네트워크 공개 키 값 및 UE 개인 키 값(private key value)에 기초하여 공유 키 값을 결정하는 단계, 사용자 장비를 통해, 바인딩된 공유 키 값을 생성하기 위해 공유 키 값과 세션 키 값(session key value)을 바인딩하는 단계, 및 사용자 장비를 통해, 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용하는 단계를 포함한다.

[0006] [0006] 그러한 방법의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 부착 요청은 사용자 장비가 PFS를 지원한다는 표시를 포함할 수 있다. 부착 요청을 생성하는 단계는 서비스 요청, 영역 추적 요청 또는 위치 업데이트 요청 중 하나를 포함할 수 있다. 공유 키 값과 세션 키 값을 바인딩하는 단계는 공유 키 값 및 세션 키 값의 암호 해시(cryptographic hash)를 결정하는 단계를 포함할 수 있다. 세션 키 값은 K_{ASME}, CK(Cipher Key) 또는 IK(Integrity Key)일 수 있다. UE 공개 키 값을 네트워크에 제공하는 단계는 타원-곡선 암호(elliptic-curve cryptography)를 사용하여 또는 유한 필드 연산(finite field arithmetic)을 사용하여 임시적(ephemeral) Diffie-Hellman 쌍을 생성하는 단계를 포함할 수 있다. 네트워크가 PFS를 지원하지 않는다고 결정하는 단계 및 네트워크에 대한 연결을 거부하는 단계. 인증 토큰은, 네트워크가 PFS를 지원한다는 것을 표시하기 위해 1로 설정된 AMF(authentication management field) 비트 값을 포함할 수 있다

[0007] [0007] 본 개시에 따른, 사용자 장비(UE)와 네트워크 간에 PFS(perfect forward secrecy)를 갖는 인증 및 키 합의 프로토콜을 제공하기 위한 예시적인 장치는 메모리, 메모리에 동작 가능하게 커플링된 적어도 하나의 프로세서를 포함하고, 적어도 하나의 프로세서는 UE로부터 부착 요청을 수신하고, 네트워크 지원 표시자를 포함하는 인증 요청을 네트워크 자원에 제공하고, 네트워크 자원으로부터 인증 토큰을 수신하고 – 인증 토큰은 네트워크가 PFS를 지원한다는 표시를 포함함 – , 인증 토큰을 UE에 제공하고, UE 공개 키 값을 포함하는 인증 응답을 수신하고, 인증 응답이 예상된 응답이 아니면, 부착 요청을 거부하고, 인증 응답이 예상된 응답이면, 네트워크 공개 키 값 및 네트워크 개인 키 값을 획득하고, 네트워크 개인 키 값 및 UE 공개 키 값에 기초하여 공개 키 값을 결정하고, 바인딩된 공유 키 값을 생성하기 위해 공유 키 값과 세션 키 값을 바인딩하고, 그리고 후속 네트

워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용하도록 구성된다.

[0008] [0008] 그러한 장치의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 인증 토큰은 UE와 네트워크 자원 간에 무결성 보호될 수 있다. UE로부터 수신된 부착 요청은, 부착 요청 대신에, 서비스 요청, 영역 추적 요청 또는 위치 업데이트 요청 중 하나를 수신하는 것을 포함할 수 있다. 공유 키 값 및 세션 키 값의 암호 해시가 결정될 수 있다. 세션 키 값은 K_{ASME}, CK(Cipher Key) 또는 IK(Integrity Key) 중 적어도 하나일 수 있다.

공유 키 값은 타원-곡선 암호학 또는 유한 필드 연산(finite field arithmetic) 중 하나에 의해 결정될 수 있다. 부착 요청은 UE가 PFS를 지원한다는 표시를 포함할 수 있다. 인증 토큰은, 네트워크가 PFS를 지원한다는 것을 표시하기 위해 1로 설정된 AMF(authentication management field) 비트 값을 포함할 수 있다.

[0009] [0009] 본 개시에 따른, 강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격(bid-down attack)을 방지하기 위한 방법의 예는, 사용자 장비로부터 부착 요청을 수신하는 단계, 인증 요청을 홈 네트워크로 전송하는 단계 - 인증 요청은, 네트워크가 강한 보안 프로토콜을 지원한다는 표시를 포함함 - , 홈 네트워크로부터 무결성 보호 토큰을 수신하는 단계 - 무결성 보호 토큰은, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함함 - , 및 무결성 보호 토큰을 사용자 장비로 전송하는 단계를 포함한다.

[0010] [0010] 그러한 방법의 구현들은 다음의 특징들 중 하나 이상을 포함할 수 있다. 부착 요청은, 사용자 장비가 강한 보안 프로토콜을 지원한다는 표시를 포함할 수 있다. 강한 보안 프로토콜은 완전 순방향 비밀성을 갖는 인증 및 키 합의 프로토콜일 수 있다. 인증 요청은, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하기 위한 정보 엘리먼트들로서 AVP(Attribute Value Pairs)를 갖는 다이어미터 프로토콜 메시지일 수 있다. 무결성 보호 토큰은 홈 네트워크로부터 수신된 인증 벡터에 포함될 수 있다. 적어도 하나의 비트는 AMF(Authentication Management Field)에 포함될 수 있다.

[0011] [0011] 본 개시에 따른, 강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 명령들을 포함하는 예시적인 비일시적인 프로세서-판독 가능 저장 매체는, 사용자 장비로부터 부착 요청을 수신하기 위한 코드, 인증 요청을 홈 네트워크로 전송하기 위한 코드 - 인증 요청은, 네트워크가 강한 보안 프로토콜을 지원한다는 표시를 포함함 - , 홈 네트워크로부터 무결성 보호 토큰을 수신하기 위한 코드 - 무결성 보호 토큰은, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함함 - , 및 무결성 보호 토큰을 사용자 장비로 전송하기 위한 코드를 포함한다.

[0012] [0012] 그러한 비일시적인 프로세서-판독 가능 저장 매체의 구현들은 다음의 제한들 중 하나 이상을 포함할 수 있다. 부착 요청은, 사용자 장비가 강한 보안 프로토콜을 지원한다는 표시를 포함할 수 있다. 강한 보안 프로토콜은 완전 순방향 비밀성을 갖는 인증 및 키 합의 프로토콜일 수 있다. 인증 요청은, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하기 위한 정보 엘리먼트들로서 AVP(Attribute Value Pairs)를 갖는 다이어미터 프로토콜 메시지일 수 있다. 무결성 보호 토큰은 홈 네트워크로부터 수신된 인증 벡터에 포함될 수 있다. 적어도 하나의 비트는 AMF(Authentication Management Field)에 포함될 수 있다.

[0013] [0013] 본원에 설명된 아이템들 및/또는 기술들은 다음의 능력들뿐만 아니라 언급되지 않은 다른 능력들 중 하나 이상을 제공할 수 있다. 모바일 디바이스는, 자신이 완전 순방향 비밀성을 지원한다는 것을 표시하는 표시를 네트워크에 제공할 수 있다. 네트워크는, 네트워크가 완전 순방향 비밀성을 지원한다는 것을 표시하기 위한 정보 엘리먼트를 홈 네트워크에 제공할 수 있다. 무결성 보호 토큰은 홈 네트워크에 의해 생성되고, 모바일 디바이스로 포워딩될 수 있다. 무결성 보호 토큰은, 네트워크가 완전 순방향 비밀성을 지원한다는 것을 표시하기 위한 정보 엘리먼트를 포함할 수 있다. 모바일 디바이스 및 네트워크는 공유 키를 생성하기 위해 Diffie-Hellman 교환에 참여할 수 있다. 공유 키는 세션 키에 바인딩되는데 사용될 수 있다. 바인딩된 세션 키는 후속 네트워크 트래픽을 보호하는데 사용될 수 있다. 완전 순방향 비밀성을 갖는 인증 및 키 합의 프로토콜이 실현될 수 있다. 비드-다운 공격에 대한 잠재성은 네트워크 완전 순방향 비밀성을 통합하는 무결성 보호 토큰의 사용에 의해 상당히 감소될 수 있다. 다른 능력들이 제공될 수 있고, 본 개시에 따른 모든 각각의 구현이 논의되는 능력들 전부를 제공하는 것이 아니라 이들 중 임의의 것을 제공하는 것이 틀림없다. 또한, 위에서 언급된 효과가 언급된 것 이외의 수단들에 의해 달성되는 것이 가능할 수 있고, 언급된 아이템/기술이 언급된 효과를 반드시 산출하지는 않을 수 있다.

[0014] [0014] 본 발명의 다른 양상들, 특징들 및 실시예들은 첨부 도면들과 함께 본 발명의 특정한 예시적인 실시예들의 다음 설명의 검토시, 해당 기술분야에서 통상의 지식을 가진 자들에게 명백해질 것이다. 본 발명의 특성들이 아래의 특정한 실시예들 및 도면들에 대해 논의될 수도 있지만, 본 발명의 모든 실시예들은, 본 명세서에 논

의되는 유리한 특성들 중 하나 이상을 포함할 수 있다. 즉, 하나 이상의 실시예들이 특정한 유리한 특성들을 갖는 것으로 논의될 수도 있지만, 그러한 특성들 중 하나 이상은 또한, 본 명세서에 논의되는 본 발명의 다양한 실시예들에 따라 사용될 수도 있다. 유사한 방식으로, 예시적인 실시예들이 디바이스, 시스템, 또는 방법 실시예들로서 아래에 논의될 수도 있지만, 그러한 예시적인 실시예들이 다양한 디바이스들, 시스템들, 및 방법들에서 구현될 수 있음이 이해되어야 한다.

도면의 간단한 설명

[0015] [0015] 도 1은 일부 양상들/실시예들에 따른 모바일 디바이스의 일 실시예의 컴포넌트들의 블록도이다.

[0016] 도 2는 일부 양상들/실시예들에 따른 예시적인 무선 통신 시스템의 블록도이다.

[0017] 도 3은 일부 양상들/실시예들에 따른, 도 2의 무선 통신 시스템에서 사용하기 위한 컴퓨터 시스템의 예의 블록도이다.

[0018] 도 4는 3GPP LTE(long term evolution) 인증 절차의 종래 기술의 호 흐름도이다.

[0019] 도 5는 일부 양상들/실시예들에 따른, PFS(perfect forward secrecy) 특성을 갖는 예시적인 인증 절차의 호 흐름도이다.

[0020] 도 6은 PFS(perfect forward secrecy) 특성을 갖는 다른 예시적인 인증 절차의 호 흐름도이다.

[0021] 도 7은 일부 양상들/실시예들에 따른, 모바일 디바이스와의 보안 통신들을 제공하는 프로세스의 블록 흐름도이다.

[0022] 도 8은 일부 양상들/실시예들에 따른, 네트워크 서버와의 보안 통신들을 제공하는 프로세스의 블록 흐름도이다.

[0023] 도 9는 일부 양상들/실시예들에 따른, 강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 프로세스의 블록 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] [0024] PFS(perfect forward secrecy)을 통해 AKA(authentication and key agreement)를 제공하기 위한 기술들이 논의된다. 본원에 사용된 바와 같이, 용어 완전 순방향 비밀성은, 장기간 키들 중 하나가 장래에 훼손되지 않는다면, 장기간 키들의 세트로부터 도출된 세션 키가 훼손되지 않는다는 것을 보장하는 것을 돕기 위해 키-합의 프로토콜들의 특성의 암호 정의(cryptography definition)를 지칭한다. 본원에 사용된 용어 완전(perfect)하다는 것은 결점들 또는 결함들에서 완전히 자유롭거나 가능한 그러한 조건에 가까운 어떤 것을 의미하지는 않는다. AKA는 현대 셀룰러 네트워크들(예를 들면, GSM, UMTS, LTE, eHRPD)에서 널리 사용되는 인증 및 키 합의 프로토콜이다. AKA는 3GPP TS 33.102에 지정된다. AKA의 보안은 일반적으로, UE(예를 들면, 통상적으로 USIM에 저장됨)와 홈 네트워크 내의 서버(예를 들면, HSS(Home Subscriber Server)) 사이에 안전하게 공유되는 대칭적인 루트 키(K)에 의존한다. AKA는 PFS(Perfect Forward Secrecy)를 제공하지 않는다. 즉, AKA는, 장기간 키(예를 들면, K)가 장래에 훼손되면, 훼손될 수 없는 세션 키를 제공하지 않는다. 논의될 바와 같이, 실시예에서, AKA의 잠재적인 보안 결함들은 PFS 특성들을 통해 완화될 수 있다. 예를 들면, DHE(Ephemeral Diffie-Hellman) 교환은, 모바일 디바이스와 네트워크 서버 사이에서 발생할 수 있다. 모바일 디바이스 및 네트워크 서버 각각은 개별적인 개인 키 값들 및 공개 키 값들을 결정할 수 있다. 공개 키들은 공유 키를 생성하기 위해 교환되어 개개의 개인 키들과 결합될 수 있다. 결과적인 공유 키는 인증 벡터 내의 베이스-키(예를 들면, K_{ASME})에 바인딩되고, 네트워크 내의 통신들을 보호하는데 사용될 수 있다. 보안 인증 정보 엘리먼트들은, 모바일 디바이스 및 네트워크 서버 둘 모두가 PFS를 지원하는 것을 보장하는데 사용될 수 있다. 보안 인증 비트들은 비드 다운 공격들(예를 들면, 중간자 공격들)을 방지할 수 있다.

[0017] [0025] 도 1을 참조하면, 본원의 다양한 기술들이 사용될 수 있는 모바일 디바이스(100)가 예시된다. 모바일 디바이스(100)는 UE(user equipment)이고, 다양한 모바일 통신 및/또는 컴퓨팅 디바이스들의 기능을 포함하거나 구현할 수 있고, 예들은, 현재 존재하거나 장래에 개발되든지 간에, PDA(personal digital assistant)들, 스마트폰들, 컴퓨팅 디바이스들, 가령, 랩톱들, 데스크톱들 또는 태블릿 컴퓨터들, 자동차 컴퓨팅 시스템 등을 포함하지만, 이에 제한되지 않는다.

[0018] [0026] 모바일 디바이스(100)는 프로세서(111)(또는 프로세서 코어) 및 메모리(140)를 포함한다. 모바일 디바

이스는 공개 버스(101) 또는 개인 버스(미도시)에 의해 메모리(140)에 동작 가능하게 연결된 신뢰하는 환경을 선택적으로 포함할 수 있다. 모바일 디바이스(100)는 또한 무선 네트워크를 통해 무선 안테나(122)를 경유하여 무선 신호들(123)을 전송 및 수신하도록 구성된 무선 트랜시버(121) 및 통신 인터페이스(120)를 포함할 수 있다. 무선 트랜시버(121)는 버스(101)에 연결된다. 여기서, 모바일 디바이스(100)는 단일 무선 트랜시버(121)를 갖는 것으로 예시된다. 그러나, 모바일 디바이스(100)는 대안적으로 Wi-Fi, CDMA, WCDMA(Wideband CDMA), LTE(Long Term Evolution), BLUETOOTH 단거리 무선 통신 기술 등과 같은 다수의 통신 표준들을 지원하기 위해 다수의 무선 트랜시버들(121) 및 무선 안테나들(122)을 가질 수 있다.

[0019] [0027] 통신 인터페이스(120) 및/또는 무선 트랜시버(121)는 다수의 캐리어들(상이한 주파수들의 파형 신호들) 상의 동작을 지원할 수 있다. 다중-캐리어 송신기들은 다수의 캐리어들 상에서 변조된 신호들을 동시에 송신할 수 있다. 각각의 변조된 신호는 CDMA(Code Division Multiple Access) 신호, TDMA(Time Division Multiple Access) 신호, OFDMA(Orthogonal Frequency Division Multiple Access) 신호, SC-FDMA(Single-Carrier Frequency Division Multiple Access) 신호 등일 수 있다. 각각의 변조된 신호는 상이한 캐리어 상에서 전송될 수 있고, 파일럿, 오버헤드 정보, 데이터 등을 반송할 수 있다.

[0020] [0028] 모바일 디바이스(100)는 또한 사용자 인터페이스(150)(예를 들면, 디스플레이, GUI), 및 SPS(satellite positioning system) 안테나(158)를 통해 (예를 들면, SPS 위성들로부터) SPS 신호들(159)을 수신하는 SPS 수신기(155)를 포함할 수 있다. SPS 수신기(155)는 단일 GNSS(global navigation satellite system) 또는 다수의 그러한 시스템들과 통신할 수 있다. GNSS는 GPS(Global Positioning System), Galileo, Glonass, Beidou(Compass) 등을 포함할 수 있지만, 이에 제한되지 않는다. SPS 위성은 또한 위성들, SV들(space vehicles) 등으로 지칭될 수 있다. SPS 수신기(155)는 SPS 신호들(159)을, 전체적으로 또는 부분적으로, 프로세싱하고, 모바일 디바이스(100)의 위치를 결정하기 위해 이들 SPS 신호들(159)을 사용한다. 프로세서(111), 메모리(140), DSP(112) 및/또는 특수 프로세서(들)(미도시)는 또한 SPS 신호들(159)을, 전체적으로 또는 부분적으로, 프로세싱하고 그리고/또는 SPS 수신기(155)와 공조하여 모바일 디바이스(100)의 위치를 계산하는데 사용될 수 있다. SPS 신호들(159) 또는 다른 위치 신호들로부터의 정보의 저장은 메모리(140) 또는 레지스터들(미도시)을 사용하여 수행된다. 단지 하나의 프로세서(111), 하나의 DSP(112) 및 하나의 메모리(140)가 도 1에 도시되지만, 이들 컴포넌트들 중 임의의 하나보다 더 많거나 한 쌍 또는 전부가 모바일 디바이스(100)에 의해 사용될 수 있다. 모바일 디바이스(100)와 연관된 프로세서(111) 및 DSP(112)는 버스(101)에 연결된다.

[0021] [0029] 메모리(140)는, 하나 이상의 명령들 또는 코드로서 기능들을 저장하는 비일시적인 컴퓨터-판독 가능 저장 매체(또는 매체들)를 포함할 수 있다. 메모리(140)를 구성할 수 있는 매체들은 RAM, ROM, FLASH, 디스크 드라이브들 등을 포함하지만, 이에 제한되지 않는다. 일반적으로, 메모리(140)에 의해 저장된 기능들은 범용 프로세서(들)(111), 특수 프로세서들 또는 DSP(들)(112)에 의해 실행된다. 따라서, 메모리(140)는, 프로세서(들)(111) 및/또는 DSP(들)(112)로 하여금 설명된 기능들을 수행하게 하도록 구성된 소프트웨어(프로그래밍 코드, 명령들 등)를 저장하는 프로세서-판독가능 메모리 및/또는 컴퓨터-판독가능 메모리이다. 대안적으로, 모바일 디바이스(100)의 하나 이상의 기능들은 하드웨어에서 전체적으로 또는 부분적으로 수행될 수 있다.

[0022] [0030] 모바일 디바이스(100)는 뷰 내의 다른 통신 엔티티들 및/또는 모바일 디바이스(100)에 이용 가능한 정보에 기초하여 다양한 기술들을 사용하여 연관된 시스템 내의 자신의 현재 위치를 추정할 수 있다. 예를 들면, 모바일 디바이스(100)는 하나 이상의 무선 LAN(local area network)들, BLUETOOTH 또는 ZIGBEE® 등과 같은 단거리 무선 통신 기술을 사용하는 PAN(personal area network)들, SPS 위성들과 연관된 AP들(access points)로부터 획득되는 정보, 및/또는 맵 서버 또는 LCI 서버로부터 획득된 맵 제약 데이터를 사용하여 자신의 위치를 추정할 수 있다.

[0023] [0031] 다음에 도 2를 참조하면, 예시적인 통신 시스템(200)의 블록도가 도시된다. 통신 시스템(200)은, LTE(Long Term Evolution) 라디오 액세스 기술을 사용하여 UE(202)(즉, 모바일 디바이스(100))와 eNB(evolved NodeB)(204)(예를 들면, 기지국, 액세스 포인트 등) 간의 무선 라디오 통신들을 제공하는 LTE RAN(radio access network)을 포함할 수 있다. 다른 네트워크들이 사용될 수 있기 때문에, 도 2의 LTE 네트워크는 단지 예시적이다. 논의를 간단히 하기 위해, 도 2는 UE(202) 및 하나의 eNB(204)를 도시하지만, RAN은 임의의 수의 UE들 및/또는 eNB들을 포함할 수 있다. eNB(204)는 순방향 링크 또는 다운링크 채널을 통해 정보를 UE(202)로 송신하고, UE(202)는 역방향 링크 또는 업링크 채널을 통해 정보를 eNB(204)로 송신할 수 있다. 도시된 바와 같이, RAN들은, 이에 제한되지 않지만, LTE, LTE-A, HSPA, CDMA, HRPD(high rate packet data; eHRPD(evolved HRPD), CDMA2000, GSM, GPRS, EDGE(enhanced data rate for GSM evolution), UMTS 등과 같은 임의의 적절한 타

입의 라디오 액세스 기술을 사용할 수 있다.

[0024] [0032] eNB(204)는 과금(charging)(예를 들면, 서비스들에 대한 사용 과금들 등), 보안(예를 들면, 암호화 및 무결성 보호), 가입자 관리, 이동성 관리, 베어러 관리, QoS 핸들링, 데이터 흐름들의 정책 제어 및/또는 외부 네트워크와의 상호연결을 가능하게 하는 코어 네트워크와 통신할 수 있다. RAN 및 코어 네트워크는, 예를 들면, S1 인터페이스를 통해 통신할 수 있다. 코어 네트워크는, S-GW(serving gateway)(210)로부터의 시그널링을 제어하기 위한 엔드-포인트일 수 있는 MME(mobility management entity)(206)를 포함할 수 있다. MME(206)는 이동성 관리(예를 들면, 추적), 인증 및 보안과 같은 기능들을 제공할 수 있다. MME(206)는 S1 인터페이스를 통해 RAN과 통신할 수 있다. S-GW(serving gateway)(210)는, 코어 네트워크를 LTE RAN에 연결하는 사용자 평면 노드이다. MME(206)는 S11 인터페이스를 통해 S-GW(210)와 통신하도록 구성될 수 있다. MME(206) 및 S-GW(210)는, RAN으로부터 발신되고 그리고/또는 RAN에서 착신되는 사용자 및 제어 시그널링에 대한 단일 엔드-포인트를 제공하기 위해 단일 노드로서 구성될 수 있다. 네트워크는 또한 PCRF(policy and charging rules function)(212)를 포함할 수 있다.

[0025] [0033] 통신 시스템(200)은 또한, 코어 네트워크(및 RAN들)와 외부 네트워크들 간의 통신들을 가능하게 하는 PDN(packet data network) GW(gateway)(214)를 포함할 수 있다. PDN GW(214)는 패킷 필터링, QoS 폴리싱(policing), 과금, IP 어드레스 할당, 및 외부 네트워크들로의 트래픽의 라우팅을 제공할 수 있다. 예에서, S-GW(210) 및 PDN GW(214)는 S5 인터페이스를 통해 통신할 수 있다. 도 2에서 별개의 노드들로서 예시되지만, S-GW(210) 및 PDN GW(214)가, 예를 들면, 통신 시스템(200)에서 사용자 평면 노드들을 감소시키기 위해 단일 네트워크 노드로서 동작하도록 구성될 수 있다는 것이 인지된다. 통신 시스템(200)은 또한, MME(206)와 통신할 수 있는 HSS(home subscriber services) 엔티티(208)를 포함할 수 있다. 통신 시스템(200)은 또한 다른 네트워크 컴포넌트들, 가령, 3GPP AAA(authentication, authorization and accounting) 서버/프록시 및 서로 통신하고 PDN GW(214)와 HSS(208)와 추가로 통신하도록 구성된 3GPP2 AAA 서버/프록시(미도시)를 포함할 수 있다.

[0026] [0034] 통신 시스템(200)은 PDN GW(214)를 통해 외부 네트워크들과 통신하도록 구성될 수 있다. 외부 네트워크들(미도시)은 네트워크들, 가령, 이에 제한되지 않지만, PSTN(public switched telephone network), IMS(IP multimedia subsystem) 및/또는 IP 네트워크를 포함할 수 있다. IP 네트워크는 인터넷, 로컬 영역 네트워크, 광역 네트워크, 인트라넷 등일 수 있다. 도 2는 단지 하나의 가능한 구성의 예이고, 많은 다른 구성들 및 부가적인 컴포넌트들이 아래에 설명된 다양한 양상들 및 구현들에 따라 사용될 수 있다.

[0027] [0035] 도 3에 예시된 컴퓨터 시스템(300)은 도 2의 엘리먼트들의 기능을 적어도 부분적으로 구현하는데 사용될 수 있다. 도 3은, 본원에 설명된 다양한 다른 실시예들에 의해 제공된 방법들을 수행할 수 있고 그리고/또는 모바일 디바이스 또는 다른 컴퓨터 시스템으로 기능할 수 있는 컴퓨터 시스템(300)의 일 실시예의 개략적인 예시를 제공한다. 예를 들면, eNB(204), MME(206), HHS(208), S-GW(210), PCRF(212) 및 PDN GW(214)는 하나 이상의 컴퓨터 시스템들(300)로 구성될 수 있다. 도 3은 다양한 컴포넌트들의 일반화된 예시를 제공하고, 이들 중 임의의 것 또는 모두는 적절히 활용될 수 있다. 따라서, 도 3은 개별적인 시스템 엘리먼트들이 상대적으로 분리되거나 상대적으로 더 통합된 방식으로 구현될 수 있는 방법을 대략적으로 예시한다.

[0028] [0036] 버스(305)를 통해 전기적으로 커플링될 수 있는(또는 다른 방식으로 적절히 통신할 수 있는) 하드웨어 엘리먼트들을 포함하는 컴퓨터 시스템(300)이 도시된다. 하드웨어 엘리먼트들은, 비제한적으로 하나 이상의 범용 프로세서들 및/또는 하나 이상의 특수 목적 프로세서들(가령, 디지털 신호 프로세싱 칩들, 그래픽 가속 프로세서들 등)을 포함하는 하나 이상의 프로세서들(310); 비제한적으로 마우스, 키보드 등을 포함할 수 있는 하나 이상의 입력 디바이스들(315); 및 비제한적으로 디스플레이 디바이스, 프린터 등을 포함할 수 있는 하나 이상의 출력 디바이스들(320)을 포함할 수 있다. 프로세서(들)(310)는, 예를 들면, 지능형 하드웨어 디바이스들, 예를 들면, 가령 Intel® Corporation 또는 AMD®에 의해 제조된 CPU(central processing unit), 마이크로제어기, ASIC 등을 포함할 수 있다. 다른 프로세서 타입들이 또한 사용될 수 있다.

[0029] [0037] 컴퓨터 시스템(300)은 하나 이상의 비일시적인 저장 디바이스들(325)을 더 포함(및/또는 이들과 통신)할 수 있고, 비일시적인 저장 디바이스들(325)은, 비제한적으로, 로컬 및/또는 네트워크 액세스 가능 저장소를 포함할 수 있고, 그리고/또는 비제한적으로, 디스크 드라이브, 드라이브 어레이, 광학 저장 디바이스, 고체-상태 저장 디바이스, 가령, "RAM"(random access memory) 및/또는 "ROM"(read-only memory) – 이는 프로그래밍 가능하고, 플래시-업데이트 가능한 식일 수 있음 –을 포함할 수 있다. 그러한 저장 디바이스들은, 비제한적으로, 다양한 파일 시스템들, 데이터베이스 구조들 등을 포함하는 임의의 적절한 데이터 스토어들을 구현하도록 구성될 수 있다.

[0030] [0038] 컴퓨터 시스템(300)은 또한 통신 서브시스템(330)을 포함할 수 있고, 통신 서브시스템(330)은, 비제한적으로, 모뎀, 네트워크 카드(무선 또는 유선), 적외선 통신 디바이스, 무선 통신 디바이스 및/또는 칩셋(가령, BLUETOOTH 단거리 무선 통신 기술 트랜시버/디바이스, 802.11 디바이스, WiFi 디바이스, WiMax 디바이스, 셀룰러 통신 설비들 등) 등을 포함할 수 있다. 통신 서브시스템(330)은 데이터가 네트워크(가령, 하나의 예를 들자면 아래에 설명되는 네트워크), 다른 컴퓨터 시스템들 및/또는 본원에 설명된 임의의 다른 디바이스들과 교환되도록 허용할 수 있다. 많은 실시예들에서, 컴퓨터 시스템(300)은, 위에 설명된 RAM 또는 ROM 디바이스를 포함할 수 있는 작업 메모리(335)를 여기서와 같이 더 포함할 것이다.

[0031] [0039] 컴퓨터 시스템(300)은 또한, 다양한 실시예들에 의해 제공되는 컴퓨터 프로그램들을 포함할 수 있고 그리고/또는 본원에 설명된 바와 같이 다른 실시예들에 의해 제공되는 방법들을 구현하고 그리고/또는 시스템들을 구성하도록 설계될 수 있는 하나 이상의 애플리케이션 프로그램들(345)과 같은 운영 시스템(340), 디바이스 드라이버들, 실행 가능 라이브러리들 및/또는 다른 코드를 포함하여, 작업 메모리(335) 내에 현재 위치된 것으로 도시된 소프트웨어 엘리먼트들을 포함할 수 있다. 단지 예로서, 본원에 설명된 하나 이상의 프로세스들은 컴퓨터(및/또는 컴퓨터 내의 프로세서)에 의해 실행 가능한 코드 및/또는 명령들로서 구현될 수 있다. 그러한 코드 및/또는 명령들은 설명된 방법들에 따라 하나 이상의 동작들을 수행하기 위해 범용 컴퓨터(또는 다른 디바이스)를 구성 및/또는 적응시키는데 사용될 수 있다.

[0032] [0040] 이러한 명령들 및/또는 코드의 세트는 위에 설명된 저장 디바이스(들)(325)와 같은 컴퓨터-판독가능 저장 매체 상에 저장될 수 있다. 일부 경우들에서, 저장 매체는 컴퓨터 시스템(300)과 같은 컴퓨터 시스템 내에 통합될 수 있다. 다른 실시예들에서, 저장 매체(예를 들면, 제거 가능 매체, 가령, 콤팩트 디스크)는 컴퓨터 시스템과 별개이고 그리고/또는 설치 패키지에 제공될 수 있어서, 저장 매체는 그 안에 저장된 명령들/코드로 범용 컴퓨터를 프로그래밍, 구성 및/또는 적응시키는데 사용될 수 있다. 이들 명령들은 컴퓨터 시스템(300)에 의해 실행 가능한 실행 가능 코드의 형태를 취할 수 있고 그리고/또는 (예를 들면, 다양한 일반적으로 이용 가능한 컴파일러들, 설치 프로그램들, 압축/압축해제 유틸리티들 등 중 임의의 것을 사용하여) 컴퓨터 시스템(300) 상의 컴파일레이션 및/또는 설치 시에, 추후 실행 가능 코드 형태를 취하는 소스 및/또는 설치 가능 코드 형태를 취할 수 있다.

[0033] [0041] 도 4를 참조하면, 3GPP LTE(long term evolution) 인증 절차의 종래 기술의 호 흐름도(400)가 도시된다. 종래 기술의 호 흐름도(400)는 3GPP TS 33.401과 같은 공개된 표준들을 준수한다. 호 흐름에 표시된 메시지들은 컴퓨터 시스템들 간에 전기적으로 송신되는 정보(예를 들면, 데이터 필드들)를 나타낸다. 정보는 해당 분야에 알려진 데이터 타입들(예를 들면, 이진, 넘버, char, varchar, 데이트 등...)를 가질 수 있다. 도면(400)은 통신 시스템(200)에 의해 사용될 수 있는 보안 절차들을 나타내고, 따라서, 도면(400)은 UE(202)(예를 들면, 모바일 디바이스(100)), 네트워크(402) 및 홈 네트워크(404)를 포함한다. 네트워크(402)는 eNB(eNodeB)(204) 및 MME(206)를 포함할 수 있다. 홈 네트워크(404)는 적어도 HSS(208)를 포함한다. 호 흐름도(400)는 네트워크에 대한 크리덴셜들을 제공하기 위한 AKA(authentication and key agreement) 절차를 예시한다. UE(202)는 IMSI(International Mobile Station Equipment Identity)를 포함하는 NAS(Non Access Stratum) 요청 메시지(410)를 (예를 들면, eNB(204)를 통해) MME(206)로 전송한다. MME(206)는 사용자 인증을 수행하기 위해 HSS(208)로부터 인증 데이터를 리트리브(retrieve)하도록 구성된다. MME(206)는 IMSI(예를 들면, NAS 부착 요청 메시지(410)에 포함됨) 및 네트워크 아이덴티티 정보(SN_id)를 포함하는 인증 정보 요청 메시지(412)를 HSS(208)로 전송할 수 있다. SN_id는 모바일 국가 코드 및 모바일 네트워크 코드를 포함할 수 있다. 인증 정보 요청 메시지(412)는 또한 네트워크 타입(예를 들면, E-UTRAN) 및 요청된 인증 벡터(AV)들(미도시)의 수를 표시하는 데이터 필드들을 포함할 수 있다. HSS(208)는 인증 정보 요청 메시지(412)를 수신하고, 하나 이상의 AV들을 생성하도록 구성된다. 예에서, HSS(208)는 AuC(Authentication Center)(미도시)로부터 AV들을 요청할 수 있다. AV들은 AUTN(authentication token), XRES(expected response), RAND(random number) 및 K_{ASME}(Key Access Security Management Entity)를 포함한다. K_{ASME}는 NAS 시그널링 보호 및 사용자 평면 보호를 위한 AS(Access Stratum) 및 NAS 암호화 및 무결성 키들을 생성하기 위한 기반을 형성한다. AV들은 인증 정보 응답 메시지(414)로 MME(206)에 제공된다. AKA를 사용하는 다른 3GPP 네트워크들(예를 들면, UMTS, GSMA)에서, AV들은 AUTN(authentication token), XRES(expected response), RAND(random number), CK(Cipher Key) 및 IK(Integrity Key)를 포함한다. CK 및 IK는 메시지들의 암호화 및 무결성 보호를 위해 사용된다.

[0034] [0042] MME(206)는 EPS(Evolved Packet System) 프로토콜들을 통해 UE(202)의 인증을 개시하도록 구성될 수 있다. MME(206)는 홈 네트워크(404)로부터 수신된 AUTN 및 RAND 값들뿐만 아니라 수신된 K_{ASME} 값에 기초한 NAS

KSI_{ASME}(Key Set Identifier)를 포함하는 NAS 인증 요청 메시지(416)를 생성한다. KSI_{ASME}는 UE(202) 및 MME(206)에 저장된다. UE(202)는 (예를 들면, AUTN이 수용될 수 있는지를 체크함으로써) AV의 신선도(freshness)를 식별하도록 구성된다. 이어서, UE(202)는, 검증이 수용되면(예를 들면, AUTN이 수용됨), 응답(RES) 값을 컴퓨팅할 수 있고, 이어서 RES 값을 포함하는 NAS 인증 응답 메시지(418)를 전송한다. 검증이 실패하면, UE(202)는, 실패에 대한 이유를 표시하는 CAUSE 값을 갖는 인증 실패 메시지를 MME(206)로 전송한다. MME(206)는, RES 값 및 XRES 값이 동일한지를 결정하도록 구성된다. 그들이 동일하면, 인증은 성공적이다. 그들이 동일하지 않다면, MME(206)는 추가의 아이덴티티 요청들을 개시하거나 인증 거부 메시지를 UE(202)를 향해 전송하도록 구성될 수 있다.

[0035] [0043] 성공적인 인증 시에, MME(206)는, MME(206)와 UE(202) 사이의 라운드트립 메시지로 구성된 NAS SMC(security mode command) 절차를 개시하도록 구성될 수 있다. MME(206)는 기밀성 및 무결성 알고리즘들을 포함하는 NAS SMC(Security Mode Command) 메시지(420)를 전송한다. 예를 들면, NAS SMC 메시지(420)는 재생되는 UE 보안 능력들, 선택된 NAS 알고리즘들, K_{ASME}를 식별하기 위한 KSI_{ASME} 값 및 유휴 이동성에서 맵핑된 컨텍스트를 생성하는 경우에 $NONCE_{UE}$ 및 $NONCE_{MME}$ 값들 둘 모두를 포함할 수 있다. NAS SMC 메시지(420)는 메시지 내의 KSI_{ASME} 값에 의해 표시된 K_{ASME}에 기초한 NAS 무결성 키로 무결성 보호될 수 있다(그러나, 암호화되지 않음). UE(202)는 NAS SMC 메시지(420)의 무결성을 검증하도록 구성된다. 이는, MME(206)에 의해 전송된 UE 보안 능력들이, 이들이 공격자에 의해 수정되지 않았다는 것을 보장하기 위해 UE(202)에 저장된 것들과 매칭하도록 보장하는 것 및 표시된 NAS 무결성 알고리즘 및 KSI_{ASME} 값에 의해 표시된 K_{ASME}에 기초한 NAS 무결성 키를 사용하여 무결성 보호를 체크하는 것을 포함할 수 있다. NAS 보안 모드 커맨드의 체크들이 통과되면, UE(202)는 NAS 보안 모드 완료 메시지(422)로 응답하도록 구성된다. UE(202)는 NAS 무결성 보호 및 암호/암호해독을 실행하고, NAS 보안 모드 완료 메시지(422)를 암호화하여 무결성 보호하여 MME(206)로 전송하도록 구성된다. MME(206)는 NAS 보안 모드 커맨드에 표시된 키들 및 알고리즘들을 사용하여 NAS 보안 모드 완료 메시지(422)를 암호해독하고 그에 대한 무결성 보호를 체크하도록 구성된다. 이러한 보안 컨텍스트의 경우에, MME에서의 NAS 다운링크 암호화는 NAS 보안 모드 완료 메시지(422)를 수신한 후에 시작될 수 있다. MME(206)에서의 NAS 업링크 암호해독은 NAS SMC 메시지(420)를 전송한 후에 시작될 수 있다.

[0036] [0044] NAS 보안 모드 완료 메시지(422)를 수신한 다음에, MME(206)는 S1AP 초기 컨텍스트 설정 메시지(424)를 전송함으로써 eNB(204)와 MME(206) 간에 S1 인터페이스를 개시하도록 구성될 수 있다. 일반적으로, 초기 컨텍스트 설정 절차의 목적은 E-RAB(E-UTRAN Radio Access Bearer) 컨텍스트, 보안 키, 핸드오버 제약 리스트, UE 라디오 능력 및 UE 보안 능력들 등을 포함하는 필요한 전체 초기 UE 컨텍스트를 설정하는 것이다. 절차는 UE-연관 시그널링을 사용한다. S1AP 초기 컨텍스트 설정 메시지(424)는, MME에서 이용가능한 경우, 트레이스 활성화 정보 엘리먼트(IE), 핸드오버 제약 리스트 IE(로밍, 영역 또는 액세스 제약들을 포함할 수 있음), UE 라디오 능력 IE, RAT/주파수 우선순위에 대한 가입자 프로파일 ID IE, CS 폴백 표시자 IE, SRVCC 동작 가능 IE, CSG 멤버쉽 상태 IE, 등록된 LAI IE, UE를 서빙하는 MME를 표시하는 GUMMEI ID IE, MME에 의해 할당된 MME UE S1AP ID를 표시하는 MME UE S1AP ID 2 IE, 관리 기반 MDT 허용 IE, 및 RAT/주파수 우선순위에 대한 가입자 프로파일 ID IE를 포함할 수 있다. eNB는, 가령, 3GPP TS 25.331 프로토콜 규격에 설명된 RRC(Radio Resource Control) 프로토콜들을 통해 UE(202)와의 보안 통신들을 개시하도록 구성될 수 있다. eNB는 RRC SMC 메시지(426)를 UE(202)로 전송할 수 있고, UE(202)는 그 규격에 설명된 바와 같이 RRC 보안 모드 완료 메시지(428)를 생성하도록 구성될 수 있다.

[0037] [0045] 도 5를 참조하고, 도 2를 추가로 참조하면, PFS(perfect forward secrecy)을 갖는 예시적인 인증 절차의 호 흐름도(500)가 도시된다. 도면(500)은 통신 시스템(200)에 의해 사용될 수 있는 보안 절차들을 나타내고, 따라서, 도면(500)은 UE(202)(예를 들면, 모바일 디바이스(100)), 네트워크(502) 및 홈 네트워크(504)를 포함한다. 네트워크(502)는 eNB(eNodeB)(204) 및 MME(206)를 포함할 수 있다. 홈 네트워크(504)는 PFS 특성을 갖는 AKA를 지원하는 것으로 가정되는 적어도 HSS(208)를 포함한다. 호 흐름도(500)는, PFS(perfect forward secrecy) 특성을 부가함으로써 도 4에 설명된 AKA(authentication and key agreement) 절차를 개선한다. (예를 들면, 도 4의 호 흐름과 비교하여) 도면(500)에서 새로운 또는 개선된 필드들은 'PFS' 접두사로 라벨링되고, 도면(500)에서 밑줄로 강조된다. 선택적인 엘리먼트들은 이탤릭체로 표시된다. 도면(500)에서 새로운 계산 절차들(예를 들면, 단계들)은 개개의 프로세스 박스들에 표시된다.

[0038] [0046] UE(202)는 PFS NAS 부착 요청(510)을 MME(206)로 전송하도록 구성될 수 있다. PFS NAS 부착 요청(510)은 정보(예를 들면, IMSI)를 식별하는 것을 포함하고, 선택적으로 또한 UE PFS IE(Information Element)를

포함할 수 있다. UE PFS IE는 불(boolean) 데이터 비트, 또는 UE(202)가 PFS 특성을 갖는 AKA를 프로세싱할 수 있다는 것을 표시하기 위한 임의의 데이터 타입일 수 있다. 그러나, UE PFS IE는, PFS 특성을 갖는 AKA를 프로세싱하는 UE의 능력이 다른 방식들로 (예를 들면, 다른 메시지 교환들에서 존재하는 정보 엘리먼트들을 통해) 설정될 수 있기 때문에, 선택적이다. 요청의 수신 시에, MME(206)는 홈 네트워크(504)(예를 들면, HSS(208))로부터 인증 벡터들을 요청하도록 구성된다. MME(206)는 UE 보안 정보(예를 들면, IMSI), 네트워크 타입(예를 들면, E-UTRAN)을 표시하는 데이터 필드들, 및 네트워크(502)가 PFS 특성을 지원한다는 표시(예를 들면, MME (SN) PFS 정보 엘리먼트)를 포함하는 PFS 인증 정보 요청 메시지(512)를 생성한다. PFS 인증 정보 요청 메시지(512)는 통상적으로 정보 엘리먼트들로서 AVP(Attribute Value Pairs)을 갖는 다이어미터(diameter) 프로토콜 메시지이다. MME (SN) PFS 정보 엘리먼트는 불(Boolean) 값 또는 다른 데이터 값일 수 있고, 네트워크(502)가 PFS 특성을 지원한다는 것을 표시하는데 사용된다. 이러한 표시는 MiM(man-in-the-middle) 공격들을 방지하는 것을 돕는데 사용될 수 있다. 즉, PFS NAS 부착 요청(510)을 인터셉트하는 악의적인 스테이션은, MME (SN) PFS 정보 엘리먼트 없이 단지 PFS NAS 부착 요청 메시지를 홈 네트워크(504)로 포워딩할 수 없고, PFS 특성 없이 AKA 프로토콜을 사용하도록 UE에 강제하려는 것을 시도할 수 없다.

[0039] [0047] HSS(208)는 PFS 인증 정보 요청 메시지(512)를 수신하고, 네트워크(502)가 PFS 특성을 지원하는지를 결정하도록 구성된다. PFS가 지원되면, 단계(526)에서, HSS(208)는 AUTN(authentication token)을 생성하도록 구성된다. 이러한 경우에, AUTN(authentication token) 내의 AMF(Authentication Management Field) 내의 필드는, 네트워크(502)가 PFS 특성을 지원한다는 것을 표시하도록 설정된다(예를 들면, 불 비트가 1로 설정됨). 이것은 PFS 비트로 지칭될 수 있다. 네트워크(502)가 PFS 특성을 지원하지 않는다면, PFS 비트는, PFS가 지원되지 않고 표준 AKA 프로토콜이 사용될 것이라는 것을 표시하기 위한 값으로 설정된다(예를 들면, 불 비트가 제로로 설정됨). HSS(208)는 AV(Authentication Vector)를 포함하는 PFS 인증 정보 응답 메시지(514)를 생성한다. PFS 인증 정보 응답 메시지(514) 내의 AV는 위에 설명된 PFS 비트를 갖는 AUTN(authentication token), XRES(expected response) 값, RAND(random number) 값, 및 K_{ASME}(Key Access Security Management Entity) 값을 포함한다.

[0040] [0048] UE(202) 및 MME(206)는 단계들(521 및 524)에서 각각 공개 및 개인 DHE(Ephemeral Diffie-Hellman) 키들의 개개의 쌍들을 생성하도록 구성된다. Diffie-Hellman 쌍들은, 예를 들면, 타원 곡선 암호(elliptical curve cryptography) 또는 유한 필드 연산(finite field arithmetic)을 사용하여 생성될 수 있다. 비제한적인 예로서, DHE 쌍들은 1977년 9월 6일에 출원되고 명칭이 "Cryptographic Apparatus and Method"인 미국 특허 제4,200,770 호에 설명된 바와 같을 수 있다. UE(202)는 UE 개인 키 값($DHEpriKey_{UE}$) 및 UE 공개 키 값($DHEpubKey_{UE}$)을 생성하도록 구성된다. MME(206)는 MME 개인 키 값($DHEpriKey_{MME}$) 및 MME 공개 키 값($DHEpubKey_{MME}$)을 생성하도록 구성된다. 개인 키들($DHEpriKey_{UE}$, $DHEpriKey_{MME}$)은 통상적으로 CSPRNG(cryptographically secure pseudo-random number generator)를 사용하여 생성되지만, 개개의 시스템들에서 이용 가능한 다른 기밀의(및 바람직하게는 비-결정론적(deterministic)) 정보가 사용될 수 있다. 대응하는 공개 키들은 또한 개개의 시스템들에 의해 생성된다. DHE 키 쌍들은 잠재적인 네트워크 공격의 영향(예를 들면, DHE 키들을 생성하는 것으로 인한 프로세싱 지연들)을 감소시키기 위해 UE(202) 및 MME(206)에 의해 사전에 선택되어 생성(예를 들면, 미리 계산)될 수 있다. UE가 단계(521) 전에 언제라도 자신의 DHE 쌍들을 생성할 수 있고, MME가 단계(530) 전에 언제라도 또는 단계(530)에서 자신의 DHE 쌍들을 생성할 수 있다는 것이 주목되어야 한다.

[0041] [0049] UE(202) 및 MME(206)는 AKA 인증 절차들 동안에 자신들의 공개 키들을 교환하고, 각각 공유 키(예를 들면, sharedDHkey)를 도출하도록 구성된다. 예를 들면, MME(206)는 HSS(208)로부터 수신된 AUTN 및 RAND 값들뿐만 아니라 수신된 K_{ASME} 값에 기초한 NAS 키 세트 식별자(KSI_{ASME})를 포함하는 PFS NAS 인증 요청 메시지(516)를 생성한다. 단계(528)에서, UE(202)가 PFS 특성을 프로세싱할 수 있다면, UE(202)는, PFS 특성이 지원된다는 것을 AUTN 값 내의 PFS 비트가 표시하는지를 결정하도록 구성된다. UE(202)가 PFS 특성을 지원하도록 구성되지 않는다면, 메시지 교환은 표준 AKA 절차들 하에서 계속될 수 있다(예를 들면, UE는 도 4에 설명된 NAS 인증 응답 메시지(418)를 전송함). UE(202)는 또한, 이전에 설명된 바와 같이, AUTN 값이 새로운 것인지를 결정하도록 구성된다. AUTN 값이 수용되고, PFS 비트가 설정되면, UE(202)는 RES 값을 컴퓨팅하고, RES 값 및 UE 공개 키 값(즉, $DHEpubKey_{UE}$)을 포함하는 PFS NAS 인증 응답 메시지(518)를 MME(206)에 제공한다. AUTN 값이 수용되지만, PFS 비트가 설정되지 않는다면(예를 들면, 제로 값), UE(202)는 PFS 특성을 지원하지 않는 네트워크와의 연결 절차들을 중단할 것을 결정할 수 있거나, 표준 AKA 절차들에 따라 RES를 컴퓨팅하여 전송할 수 있다(예를 들

면, UE는 도 4에 설명된 NAS 인증 응답 메시지(418)를 전송함). AUTN 검증이 실패하면, UE(202)는, 실패에 대한 이유를 표시하는 CAUSE 값을 갖는 인증 실패 메시지를 MME(206)로 전송한다.

[0042] [0050] PFS NAS 인증 응답 메시지(518)의 수신 시에, 단계(530)에서, MME(206)는, RES 값이 XRES 값과 동일한지를 결정하고, 이어서 수신된 UE 공개 키(즉, $DHEpubKey_{UE}$)에 기초하여 Diffie-Hellman 공유 키(즉,sharedDHEkey)를 도출하도록 구성된다. UE의 인증이 실패하면(즉, RES 값이 XRES와 동일하지 않음), 네트워크가 부착 요청을 거부할 수 있고, 어떠한 컴퓨팅 자원도 비싼 비대칭적인 암호 동작들을 수행하는데 낭비되지 않는다는 것이 인지되어야 한다. 이는 악의적인 UE들에 의한 임의의 서비스 거부 공격들을 완화하는 것을 돕는다. 이어서, 공유 키는 HSS(208)로부터 수신된 K_{ASME} 값(예를 들면, 세션 키)에 바인딩되고, 바인딩된 키는 모든 후속 NAS 트래픽을 보호하는데 사용된다. 예를 들면, 바인딩된 키는 K'_{ASME}(K_{ASME}-프라임)로 지정될 수 있고, K_{ASME} 및 공유 키의 KDF(key derivation function)에 기초하여 생성될 수 있다. 즉, $K`_{ASME} = KDF(K_{ASME}, sharedDHEkey)$이다. KDF는 암호 해싱 함수(예를 들면, SHA256, SHA512, SHA3 등...)일 수 있다. 결과적인 K'_{ASME} 값은 후속 LTE 보안 절차들에서 K_{ASME} 값으로서 사용될 수 있다.

[0043] [0051] MME(206)는 또한 MME 공개 키(즉, $DHEpubKey_{MME}$)뿐만 아니라 기밀성 및 무결성 알고리즘들을 포함하는 PFS NAS SMC 메시지(520)를 전송한다. 예를 들면, PFS NAS SMC 메시지(520)는 재생되는 UE 보안 능력들, 선택된 NAS 알고리즘들, K_{ASME}를 식별하기 위한 KSI_{ASME} 값 및 유휴 이동성에서 맵핑된 컨텍스트를 생성하는 경우에 $NONCE_{UE}$ 및 $NONCE_{MME}$ 값들 둘 모두를 포함할 수 있다. PFS NAS SMC 메시지(520)는, 메시지 내의 KSI_{ASME} 값에 의해 표시된 K_{ASME}에 기초하여 NAS 무결성 키로 무결성 보호될 수 있다(그러나, 암호화되지 않음). UE(202)는 PFS NAS SMC 메시지(520)의 무결성을 검증하도록 구성된다. 이는, MME에 의해 전송된 UE 보안 능력들이, 이들이 공격자에 의해 수정되지 않았다는 것을 보장하기 위해 UE에 저장된 것들과 매칭하도록 보장하는 것 및 표시된 NAS 무결성 알고리즘 및 KSI_{ASME} 값에 의해 표시된 K_{ASME} 값에 기초한 NAS 무결성 키를 사용하여 무결성 보호를 체크하는 것을 포함할 수 있다. 단계(532)에서, UE(202)는 MME 공개 키(예를 들면, $DHEpubKey_{MME}$)에 기초하여 Diffie-Hellman 공유 키(예를 들면, sharedDHEkey)를 도출하도록 구성된다. 이어서, sharedDHEkey는 위에서 설명된 바와 같이 K'_{ASME} 를 생성하기 위해 K_{ASME} 값(예를 들면, KSI_{ASME} 값에 의해 식별됨)에 바인딩된다. 결과적인 K'_{ASME} 값은 모든 후속 LTE 보안 절차들에서 K_{ASME} 값으로서 사용될 수 있다.

[0044] [0052] PFS NAS SMC 메시지(520)에 기초한 체크들이 통과되면(즉, MME에 의해 전송된 UE 보안 능력들이 UE에 저장된 것들과 매칭하고, 무결성 보호가 표시된 NAS 무결성 알고리즘 및 KSI_{ASME} 값에 의해 표시된 K_{ASME} 에 기초한 NAS 무결성 키를 사용하면), UE(202)는 PFS NAS 보안 모드 완료 메시지(522)로 응답하도록 구성된다. UE(202)는 K'_{ASME} 에 기초한 NAS 무결성 보호 및 암호화/암호해독을 실행하고, (예를 들면, K'_{ASME} 에 기초하여) 암호화되고 무결성 보호되는 PFS NAS 보안 모드 완료 메시지(522)를 MME(206)로 전송하도록 구성된다. MME(206)는 PFS NAS SMC 메시지(520)에 표시된 K'_{ASME} 및 다른 알고리즘들에 기초한 키들을 사용하여 PFS NAS 보안 모드 완료 메시지(522)를 암호해독하고 그에 대한 무결성 보호를 체크하도록 구성된다.

[0045] [0053] 도 6을 참조하고, 도 2, 4 및 5를 추가로 참조하면, PFS(perfect forward secrecy)을 갖는 다른 예시적인 인증 절차의 호 흐름도(600)가 도시된다. 도면(600)은 통신 시스템(200)에 의해 사용될 수 있는 대안적인 보안 절차들을 나타내고, 따라서 도면(600)은 UE(202)(예를 들면, 모바일 디바이스(100)), 네트워크(602) 및 홈 네트워크(604)를 포함한다. 네트워크(602)는 eNB(eNodeB)(204) 및 MME(206)를 포함할 수 있다. 홈 네트워크(604)는 PFS 특성을 갖는 AKA를 지원하는 것으로 가정되는 적어도 HSS(208)를 포함한다. 호 흐름도(600)는, PFS(perfect forward secrecy) 특성을 부가함으로써 도 4에 설명된 AKA(authentication and key agreement) 절차를 개선한다. 도면(600)은 또한 도 5에 이전에 설명된 메시지들 중 일부를 포함한다. 예를 들면, UE(202)는 PFS NAS 부착 요청(510)을 MME(206)로 전송하도록 구성될 수 있다. 요청의 수신 시에, MME(206)는 홈 네트워크(604)(예를 들면, HSS(208))로부터 인증 벡터들을 요청하도록 구성된다. MME(206)는 (예를 들면, MME (SN) PFS 정보 엘리먼트를 포함하는) PFS 인증 정보 요청 메시지(512)를 생성하고, 이를 홈 네트워크(604)에 제공한다. 홈 네트워크(604)(예를 들면, HSS(208))는 PFS 인증 정보 요청 메시지(512)를 수신하고, 네트워크(602)가 PFS 특성을 지원하는지를 결정하도록 구성된다. PFS가 지원되면, 단계(526)에서, HSS(208)는 도 5에서 논의된 PFS 비트를 포함하는 AUTN(authentication token)을 생성하도록 구성된다. 네트워크(602)가 PFS 특성을 지원

하지 않는다면, PFS 비트는, PFS가 지원되지 않고 표준 AKA 프로토콜이 사용될 것이라는 것을 표시하기 위한 값으로 설정된다(예를 들면, 불 비트가 제로로 설정됨). HSS(208)는 AV(Authentication Vector)를 포함하는 PFS 인증 정보 응답 메시지(514)를 생성한다. PFS 인증 정보 응답 메시지(514) 내의 AV는 위에 설명된 PFS 비트를 갖는 AUTN(authentication token), XRES(expected response) 값, RAND(random number) 값, 및 K_{ASME}(Key Access Security Management Entity) 값을 포함한다.

[0046] [0054] UE(202) 및 MME(206)는 단계(521 및 524)에서 공개 및 개인 DHE(Ephemeral Diffie-Hellman) 키들의 개개의 쌍들을 각각 생성하도록 구성된다. UE(202)는 UE 개인 키 값($DHEpriKey_{UE}$) 및 UE 공개 키 값($DHEpubKey_{UE}$)을 생성하도록 구성된다. MME(206)는 MME 개인 키 값($DHEpriKey_{MME}$) 및 MME 공개 키 값($DHEpubKey_{MME}$)을 생성하도록 구성된다. 개인 키들($DHEpriKey_{UE}$, $DHEpriKey_{MME}$)은 통상적으로 CSPRNG(cryptographically secure pseudo-random number generator)를 사용하여 생성되지만, 개개의 시스템들에서 이용 가능한 다른 기밀의 정보가 사용될 수 있다. 대응하는 공개 키들은 개개의 시스템들에 의해 유사한 비-결정론적 방식으로 생성될 수 있다. DHE 키 쌍들은 잠재적인 네트워크 공격의 영향(예를 들면, DHE 키들을 생성하는 것으로 인한 프로세싱 지연들)을 감소시키기 위해 UE(202) 및 MME(206)에 의해 사전에 선택되어 생성(예를 들면, 미리 컴퓨팅)될 수 있다. MME가 단계(524) 전에 언제라도 자신의 DHE 쌍들을 생성할 수 있고, UE가 단계(521) 전에 언제라도 자신의 DHE 쌍들을 생성할 수 있다는 것이 주목되어야 한다.

[0047] [0055] UE(202) 및 MME(206)는 AKA 인증 절차들 동안에 자신들의 공개 키들을 교환하고, 각각 공유 키(예를 들면, sharedDHkey)를 도출하도록 구성된다. 도 5의 PFS NAS 인증 요청 메시지(516)와 대조적으로, 도 6의 호 흐름에서, MME(206)는 HSS(208)로부터 수신된 AUTN 및 RAND 값들, 수신된 K_{ASME} 값에 기초한 NAS 키 세트 식별자(KSI_{ASME})뿐만 아니라 MME 공개 키(즉, $DHEpubKey_{MME}$)를 포함하는 PFS NAS 인증 요청 메시지(616)를 생성한다. 단계(628)에서, UE(202)는, PFS 특성이 지원된다는 것을 AUTN 값 내의 PFS 비트가 표시하는지를 결정하고, MME 공개 키(즉, $DHEpubKey_{MME}$)가 PFS NAS 인증 요청 메시지(616)에 존재하는지를 결정하도록 구성된다.

[0048] [0056] UE(202)는 또한, 이전에 설명된 바와 같이, AUTN 값이 새로운 것인지를 결정하도록 구성된다. AUTN 값이 수용되고, PFS 비트가 설정되고, 이어서 MME 공개 키(즉, $DHEpubKey_{MME}$)가 존재하면, UE(202)는 RES 값을 컴퓨팅하고, RES 값 및 UE 공개 키 값(즉, $DHEpubKey_{UE}$)을 포함하는 PFS NAS 인증 응답 메시지(518)를 MME(206)에 제공한다. AUTN 값이 수용되지만, PFS 비트가 설정되지 않고(예를 들면, 제로 값), MME 공개 키(즉, $DHEpubKey_{MME}$)가 존재하지 않는다면, UE(202)는 PFS 특성을 지원하지 않는 네트워크와의 연결 절차들을 중단할 것을 결정할 수 있거나, 표준 AKA 절차들에 따라 RES를 컴퓨팅하여 전송할 수 있다(예를 들면, UE는 도 4에 설명된 NAS 인증 응답 메시지(418)를 전송함). PFS 비트가 설정되지만 MME 공개 키(즉, $DHEpubKey_{MME}$)가 존재하지 않거나 AUTN 검증이 실패하면(예를 들면, PFS 값 및 MME 공개 키의 존재와 상관없이), UE(202)는 인증 실패 메시지를 MME(206)로 전송한다. 예에서, 실패 메시지는 실패에 대한 이유를 표시하는 CAUSE 값을 포함할 수 있다.

[0049] [0057] 단계(530)에서, MME(206)는, RES 값이 XRES 값과 동일한지를 결정하고, 이어서 수신된 UE 공개 키(즉, PFS NAS 인증 응답 메시지(518) 내의 $DHEpubKey_{UE}$)에 기초하여 Diffie-Hellman 공유 키(즉, sharedDHEkey)를 도출하도록 구성된다. 이어서, 공유 키는 HSS(208)로부터 수신된 K_{ASME} 값에 바인딩되고, 바인딩된 키는 모든 후속 NAS 트래픽을 보호하는데 사용된다. 예를 들면, 바인딩된 키는 K'_{ASME}(예를 들면, K_{ASME}-프라임)로 지정될 수 있고, K_{ASME} 및 공유 키의 KDF(key derivation function)에 기초하여 생성될 수 있다. 즉, $K'_{ASME} = KDF(K_{ASME}, sharedDHEkey)$이다. KDF는 암호 해싱 함수(예를 들면, SHA256, SHA512, SHA3 등...)일 수 있다. 결과적인 K'_{ASME} 값은 LTE 네트워크에서 K_{ASME} 값으로서 사용될 수 있다. 단계(632)에서, UE(202)는 MME 공개 키(예를 들면, $DHEpubKey_{MME}$)에 기초하여 Diffie-Hellman 공유 키(예를 들면, sharedDHEkey)를 도출하도록 구성된다. 이어서, sharedDHEkey는 위에서 설명된 바와 같이 K'_{ASME} 를 생성하기 위해 K_{ASME} 값(예를 들면, KSI_{ASME} 값에 의해 식별됨)에 바인딩된다. 결과적인 K'_{ASME} 값은 모든 후속 LTE 보안 절차들에서 K_{ASME} 값으로서 사용될 수 있다.

[0050] [0058] MME(206)는 기밀성 및 무결성 알고리즘들을 포함하는 PFS NAS SMC 메시지(620)를 전송한다. 예를 들면,

PFS NAS SMC 메시지(620)는 재생되는 UE 보안 능력들, 선택된 NAS 알고리즘들 및 유휴 이동성에서 맵핑된 컨텍스트를 생성하는 경우에 $NONCE_{UE}$ 및 $NONCE_{MME}$ 값들 둘 모두를 포함할 수 있다. 실시예에서, PFS NAS SMC 메시지(620)는, 단계(530)에서 결정된 K'_{ASME}에 기초하여 NAS 무결성 키로 무결성 보호될 수 있다(그러나, 암호화되지 않음). UE(202)는 PFS NAS SMC 메시지(620)의 무결성을 검증하도록 구성된다. 이는, 이들이 공격자에 의해 수정되지 않았다는 것을 보장하기 위해 MME에 의해 전송된 UE 보안 능력들이 UE에 저장된 것들과 매칭한다는 것을 보장하는 것 및 표시된 NAS 무결성 알고리즘 및 단계(632)에서 도출된 K'_{ASME} 값에 기초한 NAS 무결성 키를 사용하여 무결성 보호를 체크하는 것을 포함할 수 있다.

[0051] [0059] PFS NAS SMS 메시지(620)에 기초한 체크들이 통과되면(즉, MME에 의해 전송된 UE 보안 능력들이 UE에 저장된 것들과 매칭하고, 무결성 보호가 표시된 NAS 무결성 알고리즘 및 K'_{ASME} 에 기초한 NAS 무결성 키를 사용하면), UE(202)는 PFS NAS 보안 모드 완료 메시지(522)로 응답하도록 구성된다. UE(202)는 K'_{ASME} 에 기초한 NAS 무결성 보호 및 암호화/암호해독을 실행하고, 암호화되고 무결성 보호되는 PFS NAS 보안 모드 완료 메시지(522)를 MME(206)로 전송하도록 구성된다. MME(206)는 PFS NAS SMC 메시지(620)에 표시된 K'_{ASME} 및 다른 알고리즘들에 기초한 키들을 사용하여 PFS NAS 보안 모드 완료 메시지(522)를 암호해독하고 그에 대한 무결성 보호를 체크하도록 구성된다.

[0052] [0060] PFS 특성과 연관된 보안 양상들을 포함하는 것 이외에, 도 5 및 6에 제공된 호 흐름예들은 비드-다운 공격들(예를 들면, 중간자 공격들, 여기서 악의적인 엔티티는 메시지 교환을 수정함)에 대한 보호를 제공한다. 즉, 호 흐름들은 중간자가 "PFS를 갖는 AKA" 절차로부터 "PFS가 없는 AKA" 절차로 비드 다운하는 것을 방지한다. 가입자의 홈 네트워크(예를 들면, HSS(208))가 PFS를 지원할 때, HSS가 MME로부터 수신된 표시들(예를 들면, MME (SN) PFS 정보 엘리먼트)을 이해하고, AKA AV(authentication vector) 생성 동안에 AUTN(authentication token) 내의 AMF 필드 내의 PFS 비트를 설정할 수 있다는 것을 의미한다. 일반적으로, 네트워크(예를 들면, MME)가 PFS를 지원하면, 이는 자신의 PFS가 AV 요청의 부분으로서 홈 네트워크(예를 들면, HSS)를 지원한다는 것을 표시한다. 이러한 표시는, UE가 부착 요청에서 PFS 지원을 표시하지 않을지라도, HSS에 포함된다. HSS는 AUTN에서 AMF 비트(예를 들면, PFS 비트)를 설정한다. AUTN은 HSS와 UE 사이에서 무결성이 보호된다. PFS를 지원하는 UE는, PFS 비트가 AUTN에서 설정되는지를 체크하도록 구성된다. PFS 비트가 설정되지만, AKA가 PFS 없이 수행되면, UE는 인증을 거부할 것이다. PFS를 지원하지 않는 UE는 비트 체킹을 무시할 수 있다. 네트워크(예를 들면, MME)가 PFS를 지원하지 않는다면(즉, PFS 비트가 AV에서 제로로 설정됨), UE가 네트워크에서 PFS 없이 인증을 계속할지를 결정하기 위해 UE 정책이 인보크될 수 있다.

[0053] [0061] 도 7을 참조하고, 추가로 도 1-6을 참조하면, 모바일 디바이스와의 보안 통신들을 제공하기 위한 프로세스(700)는 도시된 단계들을 포함한다. 그러나, 프로세스(700)는 단지 예이고 비제한적이다. 프로세스(700)는, 예를 들면, 단계들이 부가, 제거, 재배열, 결합 및/또는 동시에 수행되게 함으로써 변경될 수 있다. 예를 들면, UE 공개 키 및 UE 개인 키는 이전에 컴퓨팅될 수 있다. 프로세스(700)는, 또한 통신 시스템(200) 내의 UE(202)의 예인 모바일 디바이스(100) 상에서 실행될 수 있다.

[0054] [0062] 단계(702)에서, 모바일 디바이스(100) 내의 프로세서(111) 및 무선 트랜시버(121)는 부착 요청을 생성하도록 구성된다. 실시예에서, 부착 요청은 PFS 지원 표시자를 포함할 수 있다. 프로세서(111) 및 무선 트랜시버(121)는 부착 요청을 생성하기 위한 수단이다. 부착 요청은 통신 네트워크, 이를테면, LTE, LTE-A, HSPA, CDMA, HRPD(high rate packet data), eHRPD(evolved HRPD), CDMA2000, GSM, GPRS, EDGE(enhanced data rate for GSM evolution), UMTS 등과 모바일 디바이스(100) 간의 무선 통신일 수 있다. 통신 시스템은 네트워크에서 메시지 흐름을 보안하기 위해 'PFS를 갖는 AKA' 프로토콜을 사용할 수 있다. 부착 요청을 생성하는 것은 PFS NAS 부착 요청(510)을 eNB(204)를 통해 모바일 디바이스로부터 MME(206)로 전송하는 것일 수 있다. PFS 지지 부착 요청은 선택적으로 불 비트 또는 임의의 데이터 타입, 가령, PFS NAS 부착 요청(510) 내의 선택적인 UE PFS 정보 엘리먼트를 포함할 수 있다.

[0055] [0063] 단계(704)에서, 모바일 디바이스(100) 내의 프로세서(111) 및 무선 트랜시버(121)는 인증 토큰을 갖는 인증 요청을 수신하도록 구성되어, 인증 토큰이 서빙 셀에 의한 PFS 지원의 표시를 포함한다. 인증 토큰의 값은 네트워크 지원 표시자(예를 들면, MME PFS)에 적어도 부분적으로 기초한다. 즉, 인증 토큰은, 네트워크가 PFS를 지원하는지 여부를 표시하도록 구성된다. 예를 들면, 네트워크에 의한 PFS 지원의 표시는 PFS 인증 정보 응답 메시지(514) 내의 AUTN 필드일 수 있다. 인증 토큰은, 네트워크가 PFS(예를 들면, AUTN 내의 PFS 비트)를 지원한다는 표시로서 데이터 필드(예를 들면, 비트, 바이트들)를 포함할 수 있다.

[0056] [0064] 단계(706)에서, 모바일 디바이스(100) 내의 프로세서(111)는, 네트워크가 PFS(perfect forward secrecy)를 지원하는지를 결정하도록 구성된다. 단계(704)에서 수신된 인증 토큰은, 네트워크가 PFS를 지원하는지 여부를 표시하기 위한 PFS 비트(예를 들면, AMF 비트)를 포함할 수 있다. 네트워크가 PFS를 지원하지 않는다면(즉, PFS 비트가 제로와 동일함), 단계(716)에서, 모바일 디바이스(100)는 UE 공개 키 값 없이 인증 응답을 제공하도록 구성된다. 예를 들면, 도 4를 참조하면, 인증 응답은 NAS 인증 응답 메시지(418)일 수 있다. 단계(718)에서, 모바일 디바이스(100)는 도 4에 도시된 것과 같은 표준 AKA 인증 절차를 수행하도록 구성된다.

[0057] [0065] 네트워크가 PFS를 지원한다고(예를 들면, AUTN 내의 PFS 비트가 1과 동일함) 모바일 디바이스(100)가 결정하면, 단계(708)에서, 모바일 디바이스(100) 내의 프로세서(111)는 UE 공개 키 값을 (예를 들면, 인증 응답으로) 네트워크에 제공하도록 구성된다. 프로세서(111) 및 무선 트랜시버(121)는 UE 공개 키 값을 네트워크에 제공하기 위한 수단이다. 예를 들면, 프로세서(111)는 UE 공개 키 값 및 UE 개인 키 값을 생성하도록 구성된다. 공개 및 개인 키들은 Diffie-Hellman 쌍들로서 생성된다. 프로세서(111)는 UE 개인 및 공개 키들을 생성하기 위한 수단이다. 프로세서(111)는 UE 개인 키 값으로서 CSPRNG(cryptographically secure pseudo-random number generator)를 생성하도록 구성될 수 있다. UE 공개 키 값은 또한 프로세서(111)에 의해 비-결정론적 방식으로 생성된다. UE 개인 및 공개 키 값들은 프로세스(700)의 실행 전에 생성되고, 모바일 디바이스 상의 메모리에 저장되고, 요구될 때 리트리브될 수 있다. 도 5의 LTE 예에서, 모바일 디바이스(100)는 RES 값 및 UE 공개 키 값(즉, $DHEpubKey_{UE}$)을 포함하는 PFS NAS 인증 응답 메시지(518)를 MME(206)에 제공할 수 있다.

[0058] [0066] 단계(710)에서, 모바일 디바이스 내의 무선 트랜시버(121) 및 프로세서(111)는 네트워크로부터 네트워크 공개 키 값을 수신하도록 구성된다. 예를 들면, 모바일 디바이스(100)는 네트워크(502)(예를 들면, eNB(204)를 통해 MME(206))로부터 PFS NAS SMC 메시지(520)를 수신하도록 구성된다. PFS NAS SMC 메시지(520)는 네트워크 공개 키(예를 들면, $DHEpubKey_{MME}$)뿐만 아니라 기밀성 및 무결성 알고리즘들을 포함할 수 있다.

[0059] [0067] 단계(712)에서, 모바일 디바이스(100) 내의 프로세서(111)는 네트워크 공개 키 값 및 UE 개인 키 값에 기초하여 공유 키 값을 결정하도록 구성된다. 예를 들면, 프로세서(111)는 수신된 네트워크 공개 키 값(즉, DHEpubKeyMME) 및 이전에 생성된 UE 개인 키 값($DHEpriKey_{UE}$)에 기초하여 Diffie-Hellman 공유 키(즉, sharedDHEkey)를 도출하도록 구성된다.

[0060] [0068] 단계(714)에서, 모바일 디바이스(100) 내의 프로세서(111)는 공유 키 값과 세션 키 값을 바인딩하고, 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용하도록 구성된다. 공유 키 값과 세션 키 값을 바인딩하는 것은 공유 키 값과 세션 키 값의 연쇄(concatenation)(예를 들면, SHA256(공유 키, 루트 키))에 대해 암호 해시를 수행하는 것을 포함할 수 있다. 도 5를 참조하면, 공유 키 값(즉, sharedDHEkey)은 K_{ASME} 값에 바인딩된다. 결과적인 바인딩된 공유 키 값은 K'_{ASME}로 지정되고, K_{ASME} 및 공유 키의 KDF(key derivation function)에 기초하여 생성될 수 있다. 즉, $K'_{ASME} = KDF(K_{ASME}, sharedDHEkey)$이다. KDF는 암호 해싱 함수(예를 들면, SHA256, SHA512, SHA3 등...)일 수 있다. 결과적인 K'_{ASME} 값(즉, 바인딩된 공유 키 값)은 LTE 네트워크에서 K_{ASME} 값으로서 사용된다. 즉, 바인딩된 공유 키 값은 후속 네트워크 트래픽을 보호하는데 사용된다.

[0061] [0069] 도 8을 참조하고, 도 1-6을 추가로 참조하면, 네트워크 서버와의 보안 통신들을 제공하기 위한 프로세스(800)는 도시된 단계들을 포함한다. 그러나, 프로세스(800)는 단지 예이고 비제한적이다. 프로세스(800)는, 예를 들면, 단계들이 부가, 제거, 재배열, 결합 및/또는 동시에 수행되게 함으로써 변경될 수 있다. 예를 들면, 네트워크 공개 및 개인 키 값들은 미리 컴퓨팅되고, 메모리에 저장되고, 프로세스(800)에 의해 요구될 때 리트리브될 수 있다. 프로세스(800)는, 또한 통신 시스템(200) 내의 MME(206)의 예인 컴퓨터 시스템(300) 상에서 실행될 수 있다.

[0062] [0070] 단계(802)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 UE로부터 부착 요청을 수신하도록 구성된다. 예에서, 부착 요청은 선택적인 PFS 지원 표시자를 포함할 수 있다. 네트워크(502)는 부착 요청을 수신하기 위한 수단으로서 컴퓨터 시스템(300)을 포함할 수 있다. 도 5의 LTE 예에서, 네트워크(502)는 UE(202)로부터 PFS NAS 부착 요청(510)을 수신한다. PFS NAS 부착 요청은 식별 정보(예를 들면, IMSI)를 포함할 수 있고, 선택적으로 UE PFS IE(Information Element)를 포함할 수 있다. 선택적인 UE PFS IE는, UE(202)가 PFS 특성을 지원한다는 것을 표시하도록 구성된 데이터 필드(예를 들면, 불 비트 또는 다

른 캐릭터)이다. PFS NAS 부착 요청(510)은 UE(202)로부터 MME(206)로 전송된다.

[0063] [0071] 단계(804)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 네트워크 지원 표시자를 포함하는 인증 요청을 네트워크 자원에 제공하도록 구성된다. 표준 AKA 절차들은 홈 네트워크(예를 들면, HSS)로부터 인증 벡터를 요청하도록 네트워크(예를 들면, MME)에 요구한다. AKA 프로토콜로의 PFS의 부가는 통신 시스템(200) 상의 보안 강도를 개선한다. UE의 홈 네트워크가 PFS를 지원한다고 가정된다. 그러나, UE에 대해 이용 가능한 잠재적으로 많은 상이한 네트워크들이 존재하기 때문에, UE가 PFS를 지원하지 않는 네트워크에 부착될 수 있다는 것이 가능하다. 따라서, 중간자가 요청된 'PSF를 갖는 AKA' 프로토콜을 'PFS가 없는 AKA' 프로토콜로 비드 다운하려고 시도할 수 있다는 것이 또한 가능하다. 프로세스(800)는, PFS를 지원하는 자신 능력을 홈 네트워크에 표시하도록 네트워크에 요구함으로써 이러한 위험성을 제거할 수 있다. LTE 예에서, 이러한 표시는, 네트워크가 PFS 특성을 지원한다는 표시(예를 들면, MME (SN) PFS 정보 엘리먼트)로서 PFS 인증 정보 요청 메시지(512)에 포함된다. 인증 요청은 통상적으로 정보 엘리먼트들로서 AVP(Attribute Value Pairs)를 갖는 다이어미터 프로토콜 메시지이지만, 다른 네트워크들에서 다른 데이터 값 또는 타입들은 네트워크가 PFS 특성을 지원한다는 것을 표시하는데 사용될 수 있다.

[0064] [0072] 단계(808)에서, 통신 서브시스템(330) 및 프로세서(들)(310)는 네트워크 자원으로부터 인증 토큰을 수신하도록 구성되어, 인증 토큰은 네트워크가 PFS를 지원한다는 표시를 포함한다. 단계(804)에서 제공된 인증 요청을 수신한 것에 응답하여, 네트워크 자원은 하나 이상의 인증 벡터들로 응답하도록 구성된다. 인증 벡터들은, 네트워크 자원과 UE 사이에서 무결성 보호되는 인증 토큰을 포함한다. 인증 토큰의 값은 네트워크 지원 표시자에 적어도 부분적으로 기초한다. 즉, 인증 토큰은, 네트워크(예를 들면, 단계(804)에서 인증 요청을 제공한 네트워크)가 PFS를 지원할지 여부를 표시하도록 구성된다. 예를 들면, 인증 토큰은 PFS 인증 정보 응답 메시지(514) 내의 AUTN 필드일 수 있다. 인증 토큰은, 네트워크가 PFS를 지원한다는 표시(예를 들면, AUTN 내의 PFS 비트)로서 데이터 필드(예를 들면, 비트, 바이트들)를 포함할 수 있다.

[0065] [0073] 단계(810)에서, 통신 서브시스템(330) 및 프로세서(들)(310)는 인증 토큰을 UE에 제공하도록 구성된다. LTE 예에서, 인증 토큰은 RAT(예를 들면, eNB(204))를 통해 제공되고, PFS NAS 인증 요청 메시지들(516, 616)(즉, AUTN 값) 중 하나에 포함될 수 있다. 단계(812)에서, 네트워크는 UE 공개 키 값을 포함하는 인증 응답을 수신하도록 구성된다. 컴퓨터 시스템(300) 내의 통신 서브시스템(330)은 인증 응답을 수신하기 위한 수단이다. 예를 들면, 인증 응답은 RES 값 및 UE 공개 키 값(즉, $DHEpubKey_{UE}$)을 포함하는 PFS NAS 인증 응답 메시지(518)일 수 있다.

[0066] [0074] 단계(814)에서, 프로세서(들)(310)는, 단계(812)에서 수신된 인증 응답이 예상된 응답인지를 결정하도록 구성된다. 예상된 응답은, 예를 들면, 응답 값(예를 들면, RES)이 이전에 저장된 예상된 응답 값(예를 들면, XRES)과 동일한 것이다. LTE 예에서, RES 값은 PFS NAS 인증 응답 메시지(518)에 포함되고, XRES 값은 네트워크 자원으로부터 수신된 인증 벡터에 포함되었다. 프로세서(들)(310)는 2 개의 값들에 대해 논리 비교 연산을 수행하도록 구성된다. 그들이 매칭하지 않는다면, UE의 부착 요청이 단계(818)에서 거부된다.

[0067] [0075] 단계(806)에서, 컴퓨터 시스템(300) 내의 프로세서(들)(310)는 네트워크 공개 키 값 및 네트워크 개인 키 값을 생성하도록 구성된다. 네트워크 공개 및 개인 키 값들은 타원-곡선 암호를 사용하여 생성된 Diffie-Hellman 쌍들일 수 있다. 다른 비-결정론적 방법들(예를 들면, CSPRNG의 결과들)은 또한 키들을 생성하는데 사용될 수 있다. 키들의 콜렉션은 프로세스(800)의 실행 전에 미리 생성되고, 메모리에 저장될 수 있다. 한 쌍의 키들은 프로세스(800)에 의해 요구될 때 메모리로부터 리트리브될 수 있다.

[0068] [0076] 단계(816)에서, 프로세서(들)(310)는 네트워크 개인 키 값 및 UE 공개 키 값에 기초하여 공유 키 값을 결정하도록 구성된다. 공유 키 값은 단계(812)에서 수신되는 수신된 UE 공개 키(즉, $DHEpubKey_{UE}$) 및 단계(806)에서 생성된 네트워크 개인 키에 기초하여 Diffie-Hellman 공유 키(즉, sharedDHEkey)이다.

[0069] [0077] 단계(820)에서, 프로세서(들)(310)는 공유 키 값과 세션 키 값을 바인딩하고, 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용하도록 구성된다. 일반적으로, 세션 키 값은, UE와 네트워크 자원 사이에 공유되는 대칭적인 루트 키로부터 도출된다. AKA 절차들에서 세션 키의 예는 K_{ASME} 키 값이다. 공유 키 값은 KDF(key derivation function)를 통해 세션 키 값(예를 들면, K_{ASME})에 바인딩될 수 있다. KDF는 암호 해싱 함수(예를 들면, SHA256, SHA512, SHA3 등...)일 수 있다. 다른 바인딩 알고리즘들이 또한 사용될 수 있다. 도 5에 설명된 LTE 예에서, 바인딩된 공유 키는, KDF 함수(예를 들면, $K'_{ASME} = KDF(K_{ASME}, sharedDHEkey)$)로

생성된 K'_{ASME}이다. 결과적인 K'_{ASME}값은 LTE 네트워크에서 후속 트래픽을 보호하기 위해 K_{ASME} 값으로서 사용될 수 있다.

[0070] [0078] 도 9를 참조하고, 도 1-6을 추가로 참조하면, 강한 보안 프로토콜을 통해 시스템에 대한 비드-다운 공격을 방지하기 위한 프로세스(900)는 도시된 단계들을 포함한다. 그러나, 프로세스(900)는 단지 예이고 비제한적이다. 프로세스(900)는, 예를 들면, 단계들이 부가, 제거, 재배열, 결합 및/또는 동시에 수행되게 함으로써 변경될 수 있다. 프로세스(900)는, 네트워크(502)에 포함된 컴퓨터 시스템(300) 상에서 실행될 수 있다.

[0071] [0079] 단계(902)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 사용자 장비로부터 부착 요청을 수신하도록 구성된다. 예에서, 강한 보안 프로토콜은 PFS 특성을 지원한다. 따라서, 상대적인 비교에서, PFS를 지원하는 AKA 절차는, PFS를 지원하지 않는 AKA 절차보다 더 강하다. LTE 예에서, UE(202)는 PFS NAS 부착 요청(510)을 컴퓨터 시스템(300)으로 전송하도록 구성된다.

[0072] [0080] 단계(904)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 인증 요청을 홈 네트워크로 전송하도록 구성되어, 네트워크가 강한 보안 프로토콜을 지원한다는 표시를 인증 요청이 포함한다. 예에서, 컴퓨터 시스템(300)은 홈 네트워크로부터 인증 벡터들을 요청하고, 사용자 장비와 연관된 보안 정보(예를 들면, IMSI), 및 네트워크 타입(예를 들면, E-UTRAN)을 표시하는 데이터 필드들, 및 네트워크가 강한 보안 프로토콜을 지원한다는 표시를 포함하는 인증 요청을 생성하도록 구성된다. PFS 인증 정보 요청 메시지(512)는 단계(904)에서 전송된 인증 요청의 예이다. 대응하는 MME (SN) PFS 정보 엘리먼트는, 네트워크가 강한 보안 프로토콜(예를 들면, PFS를 갖는 AKA)을 지원한다는 표시의 예이다. 인증 요청은 MiM(man-in-the-middle)가 PFS를 갖는 AKA를 표준 AKA 프로토콜로 비드 다운하는 것을 방지하는 것을 돕는다. 예에서, 단계(902)에서 수신된 부착 요청을 인터셉트할 수 있는 MiM(예를 들면, 스테이션)은 단지 그 부착 요청을 홈 네트워크로 포워딩할 수 없는데, 왜냐하면 결과적인 포워딩된 메시지가, 네트워크가 강한 보안 프로토콜(예를 들면, PFS를 갖는 AKA)을 지원한다는 표시를 포함하지 않을 것이기 때문이다.

[0073] [0081] 단계(906)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 홈 네트워크로부터 무결성 보호 토큰을 수신하도록 구성되어, 무결성 보호 토큰은, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함한다. 무결성 보호 토큰은 사용자 장비와 홈 네트워크 사이의 무결성 보호를 제공한다. LTE 예에서, 인증 토큰 AUTN은 무결성 보호 토큰이다. AUTN에서, AMF(Authentication Management Field) 내의 필드는, 네트워크가 PFS 특성을 지원한다는 것을 표시하도록 설정될 수 있다(예를 들면, 불 비트는 1로 설정됨). AUTN 내의 PFS 비트는, 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트의 예이다. 예를 들면, 네트워크가 강한 보안 프로토콜을 지원하면, PFS 비트는, 강한 보안 프로토콜이 지원된다는 것을 표시하기 위한 값으로 설정될 수 있다(예를 들면, PFS 비트가 1로 설정됨). 반대로, 강한 보안 프로토콜이 네트워크에 의해 지원되지 않는다면, PFS 비트는 제로로 설정될 수 있다.

[0074] [0082] 단계(908)에서, 컴퓨터 시스템(300) 내의 통신 서브시스템(330) 및 프로세서(들)(310)는 무결성 보호 토큰을 사용자 장비로 전송하도록 구성된다. 사용자 장비는, 네트워크가 강한 보안 프로토콜을 지원하는지를 결정하기 위해, 무결성 보호 토큰으로부터의 적어도 하나의 비트를 파싱(parse)하도록 구성될 수 있다. 도 5에 설명된 LTE 예에서, 사용자 장비는, PFS 특성이 지원된다는 것을 AUTN 값 내의 PFS 비트가 표시하는지를 결정하도록 구성될 수 있다. PFS 비트가 설정되면(그리고 다른 인증 값들이 유효함), 사용자 장비는 Diffie-Hellman 공개 키를 네트워크에 제공한다. 공개 키는, 상대적으로 더 약한 보안 프로토콜(예를 들면, PFS가 없는 AKA)에서 요구되지 않은 강한 보안 프로토콜의 컴포넌트이다. 무결성 보호 토큰 내의 PFS 비트가 설정되지 않는다면(예를 들면, 제로의 값), 사용자 장비는 더 약한 보안 프로토콜에 따라 응답하도록 구성될 수 있다. 무결성 보호 토큰이 사용자 장비와 홈 네트워크 간에 보호를 제공하기 때문에, 강한 보안 프로토콜은 약한 보안 프로토콜로 비드-다운될 수 없는데, 왜냐하면 중간자가 무결성 보호 토큰의 값을 변경할 수 없기 때문이다.

[0075] [0083] PFS 속성을 갖는 인증 절차들은 도 5 및 6에 도시된 호 흐름들에 제한되지 않는다. 예를 들면, 이동성 시나리오들에서, UE는 PFS NAS 부착 요청(510) 대신에 서비스 요청 또는 위치 영역 업데이트 또는 TAU(Tracking Area Update) 요청 메시지들을 시작할 수 있다. UE는 선택적으로 (예를 들면, UE PFS IE를 포함함으로써) 이들 메시지들로 자신의 PFS 지원을 표시할 수 있다. 따라서, MME가 변경되거나 MME가 새로운 AKA를 개시하도록 결정하면, PFS 특성을 갖는 새로운 AKA는 필요될 때 수행될 수 있다. 또한, PFS 특성은 AS(Access Stratum) 보안을 위해 구현될 수 있다. K_{ASME}(및 다른 NAS 보안 키들)와 마찬가지로, 위에서 설명된 임시적(Ephemeral) DHE

방법들은 eNB와 UE 간에 PFS 특성을 갖는 AS 보안 키들을 설정하는데 사용될 수 있다. K_{eNB} 및 다른 AS 보안 키들은 K_{eNB}와 UE 사이에 유도된 sharedDHEkey에 바인딩될 수 있다. 예를 들면, eNB(204) 및 UE(202)는, 개개의 Diffie-Hellman 공개 키들을 교환하고 PFS 특성을 갖는 AS 보안 키들을 설정하기 위해, RRC 메시지 교환(예를 들면, RRCConnectionSetupComplete 및 RRC 보안 모드 커맨드)을 사용하여 DHE 공개 키들을 교환할 수 있다. PFS 특성의 이러한 구현은, AS 보안 키들을 도출하는데 사용되는 NAS 레벨 키들(예를 들면, K_{ASME})이 장래에 훼손되면, UE와 eNB 간의 과거 OTA(over-the-air) 트래픽의 기밀성의 훼손을 방지한다. 이는, UE가 유휴 모드와 활성 모드 사이에서 전환할 때, 또는 UE가 유휴 모드 이동성 동안에 상이한 eNB로 이동할 때 발생할 수 있다.

[0076] [0084] 실질적인 변형들이 특정 요구들에 따라 이루어질 수 있다. 예컨대, 맞춤화된 하드웨어가 또한 사용될 수 있고, 그리고/또는 특정 엘리먼트들이 하드웨어, 소프트웨어(휴대용 소프트웨어, 예컨대 애플릿들 등을 포함함) 또는 둘 다로 구현될 수 있다. 추가로, 네트워크 입/출력 디바이스들과 같은 다른 컴퓨팅 디바이스들에 대한 접속이 사용될 수 있다.

[0077] [0085] 컴퓨터 시스템(이를테면, 컴퓨터 시스템(300))은 본 개시에 따른 방법들을 수행하는데 사용될 수 있다. 작업 메모리(335)에 포함된 하나 이상의 명령들(운영 시스템(340) 및/또는 다른 코드, 가령 애플리케이션 프로그램들(345)에 통합될 수 있음)의 하나 이상의 시퀀스들을 프로세서(310)가 실행하는 것에 응답하여, 그러한 방법들의 절차들 중 일부 또는 전부가 컴퓨터 시스템(300)에 의해 수행될 수 있다. 이러한 명령들은 다른 컴퓨터-판독가능 매체, 이를테면, 저장 디바이스(들)(325) 중 하나 이상으로부터 작업 메모리(335)에 판독될 수 있다. 단지 예로서, 작업 메모리(335)에 포함된 명령들의 시퀀스들의 실행은 프로세서(들)(310)로 하여금 본원에 설명된 방법들의 하나 이상의 절차들을 수행하게 할 수 있다.

[0078] [0086] 본원에 사용된 바와 같은 용어들 "머신-판독가능 매체" 및 "컴퓨터-판독가능 매체"는, 머신으로 하여금 특정 방식으로 동작하게 하는 데이터를 제공하는 것에 참여하는 임의의 매체를 지칭한다. 모바일 디바이스(100) 및/또는 컴퓨터 시스템(300)을 사용하여 구현되는 실시예에서, 다양한 컴퓨터-판독가능 미디어는 명령들/코드를 실행을 위해 프로세서(들)(111, 310)에 제공할 때 수반될 수 있고, 그리고/또는 이러한 명령들/코드를 (예컨대, 신호들로서) 저장 및/또는 반송하는데 사용될 수 있다. 많은 구현들에서, 컴퓨터-판독가능 매체는 물리적 및/또는 유형의 저장 매체이다. 그러한 매체는, 이에 제한되지 않지만, 비휘발성 매체, 휘발성 매체 및 송신 매체를 포함하는 많은 형태들을 취할 수 있다. 비-휘발성 매체는, 예를 들어, 광학 및/또는 자기 디스크들, 예를 들어 저장 디바이스(들)(140, 325)를 포함한다. 휘발성 매체는 동적 메모리, 이를테면, 작업 메모리(140, 335)를 포함(이것으로 제한되지 않음)한다. 송신 매체는, 버스(101, 305)를 포함하는 와이어들뿐만 아니라 통신 서브시스템(330)의 다양한 컴포넌트들(및/또는 통신 서브시스템(330)이 다른 디바이스들과 통신하게 제공되는 매체)을 비롯하여, 동축 케이블들, 구리 와이어 및 광섬유를 포함(이것으로 제한되지 않음)한다. 따라서, 송신 매체는 또한 (라디오, 어쿠스틱 및/또는 광파들(waves), 이를테면, 라디오-파 및 적외선 데이터 통신들 동안 생성된 것들을 포함하지만, 이것으로 제한되지 않는) 파들의 형태를 취할 수 있다.

[0079] [0087] 물리적 및/또는 유형의 컴퓨터-판독가능 미디어의 일반적인 형태들은, 예컨대, 플로피 디스크, 플렉서블 디스크, 하드 디스크, 자기 테이프, 또는 임의의 다른 자기 매체, CD-ROM, 블루-레이 디스크, 임의의 다른 광학 매체, 펀치 카드들, 페이퍼 테이프, 홀들의 패턴들을 갖는 임의의 다른 물리적 매체, RAM, PROM, EPROM, FLASH-EPROM, 임의의 다른 메모리 칩 또는 카트리지, 이후에 설명되는 바와 같은 캐리어 파, 또는 임의의 다른 매체(이 매체로부터, 컴퓨터가 명령들 및/또는 코드를 판독할 수 있음)를 포함한다.

[0080] [0088] 실행을 위해 하나 이상의 명령들의 하나 이상의 시퀀스들을 프로세서(들)(111, 310)로 반송할 때 다양한 형태들의 컴퓨터-판독가능 매체가 수반될 수 있다. 단지 예로서, 명령들은 원격 컴퓨터의 자기 디스크 및/또는 광학 디스크 상에서 초기에 반송될 수 있다. 원격 컴퓨터는 자신의 동적 메모리에 명령들을 로딩하고, 모바일 디바이스(100) 및/또는 컴퓨터 시스템(300)에 의해 수신 및/또는 실행되도록 송신 매체 상에서 신호들로서 명령들을 전송할 수 있다. 전자기 신호들, 어쿠스틱 신호들, 광학 신호들 등의 형태일 수 있는 이러한 신호들은 모두, 본 발명의 다양한 실시예들에 따라, 명령들이 인코딩될 수 있는 캐리어 파들의 예들이다.

[0081] [0089] 위에서 논의된 방법들, 시스템들, 및 디바이스들은 예들이다. 다양한 대안적인 구성들은 적절히 다양한 절차들 또는 컴포넌트들을 생략하거나, 대체하거나, 또는 부가할 수 있다. 예를 들면, 대안적인 방법들에서, 단계들은 위의 논의와 상이한 순서들로 수행될 수 있고, 다양한 단계들이 부가, 생략 또는 결합될 수 있다. 또한, 특정 구성들에 대하여 설명된 특징들이 다양한 다른 구성들로 결합될 수 있다. 구성들의 상이한 양상들 및

엘리먼트들이 유사한 방식으로 결합될 수 있다. 또한, 기술이 진보하고, 따라서 엘리먼트들 중 다수는 예들이고 본 개시 또는 청구항들의 범위를 제한하지 않는다.

[0082] [0090] 예시적인 구성들(구현들을 포함함)의 철저한 이해를 제공하기 위해 특정 세부사항들이 설명에 제공된다. 그러나, 이러한 특정한 세부사항들 없이도 구성들이 실시될 수 있다. 예를 들어, 구성들을 모호하게 하는 것을 방지하기 위하여, 불필요한 세부사항 없이, 잘 알려진 회로들, 프로세스들, 알고리즘들, 구조들, 및 기술들이 도시되었다. 이러한 설명은 단지 예시적인 구성들을 제공하고, 청구항들의 범위, 적용 가능성 또는 구성들을 제한하지 않는다. 오히려, 구성들의 이전 설명은 설명된 기술들을 구현하기 위한 가능한 설명을 당업자들에게 제공할 것이다. 본 발명의 사상 또는 범위로부터 벗어남 없이, 다양한 변경들이 엘리먼트들의 어레인지먼트 및 기능에서 이루어질 수 있다.

[0083] [0091] 구성들은 흐름도 또는 블록도로서 도시된 프로세스로서 설명될 수 있다. 각각이 순차적 프로세스로서 동작들을 설명할 수 있지만, 동작들 중 많은 동작들은 병렬로 또는 동시에 수행될 수 있다. 부가하여, 동작들의 순서는 재배열될 수 있다. 프로세스는 도면에 포함되지 않은 부가적인 단계들을 가질 수 있다. 또한, 방법들의 예들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 설명 언어들, 또는 이들의 임의의 결합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어, 또는 마이크로코드로 구현될 때, 필요한 작업들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 저장 매체와 같은 비일시적인 컴퓨터-판독가능 매체에 저장될 수 있다. 프로세서들은 설명된 작업들을 수행할 수 있다.

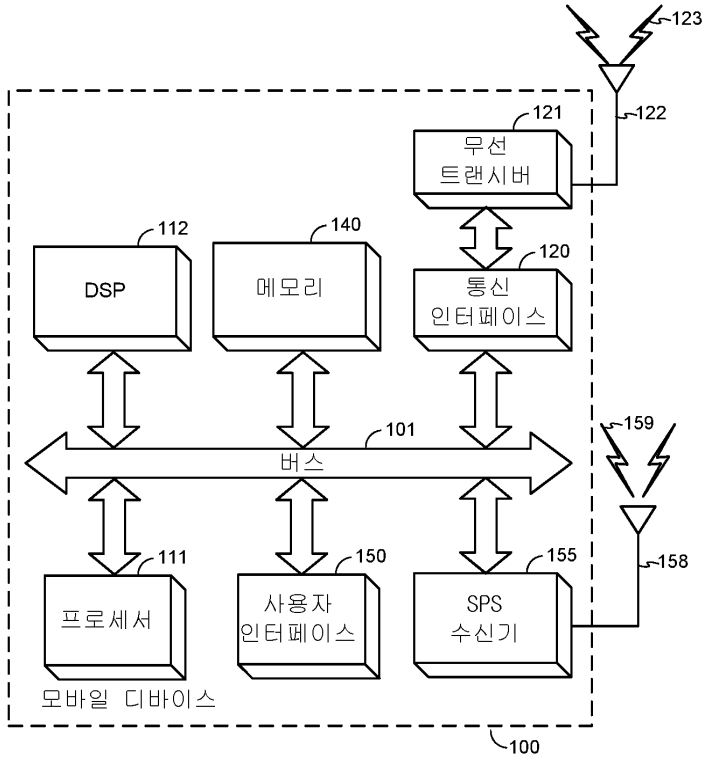
[0084] [0092] 청구항들을 포함하여 본 명세서에서 사용된 바와 같이, "~ 중 적어도 하나"가 말미에 쓰여진 항목들의 리스트에 사용된 "또는"은 예를 들어, "A, B 또는 C 중 적어도 하나"의 리스트가 A 또는 B 또는 C 또는 AB 또는 AC 또는 BC 또는 ABC(즉, A와 B와 C) 또는 하나보다 더 많은 특징과의 조합(예를 들면, AA, AAB, ABBC 등)를 의미하도록 택일적인 리스트를 나타낸다.

[0085] [0093] 청구항들을 포함하여 본원에 사용된 바와 같이, 달리 언급되지 않는다면, 기능 또는 동작이 아이템 또는 조건에 "기초"한다는 서술은, 기능 또는 동작이 서술된 아이템 또는 조건에 기초하고 서술된 아이템 또는 조건 이외에 하나 이상의 아이템들 및/또는 조건들에 기초할 수 있다는 것을 의미한다.

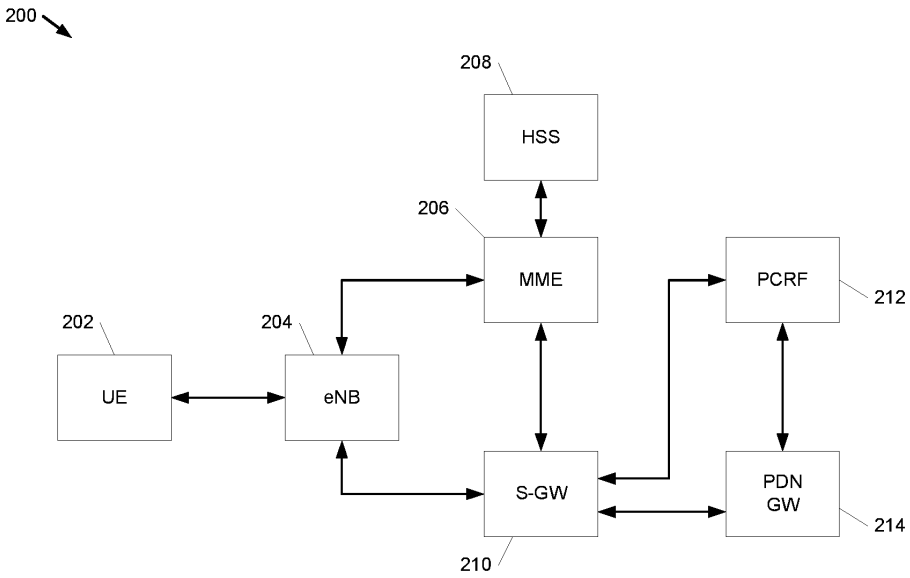
[0086] [0094] 여러 예시적인 구성들을 설명했지만, 본 개시물의 사상으로부터 벗어남 없이, 다양한 수정들, 대안적 구성들, 및 대등물들이 사용될 수 있다. 예를 들어, 위의 엘리먼트들은 더 큰 시스템의 컴포넌트들일 수 있으며, 다른 규칙들이 본 발명의 애플리케이션보다 우선할 수 있거나 또는 그렇지 않으면 본 발명의 애플리케이션을 수정할 수 있다. 또한, 위의 엘리먼트들이 고려되기 이전에, 그 동안에, 또는 그 이후에, 다수의 단계들이 착수될 수 있다. 따라서, 위의 설명은 청구항들의 범위를 제한하지 않는다.

도면

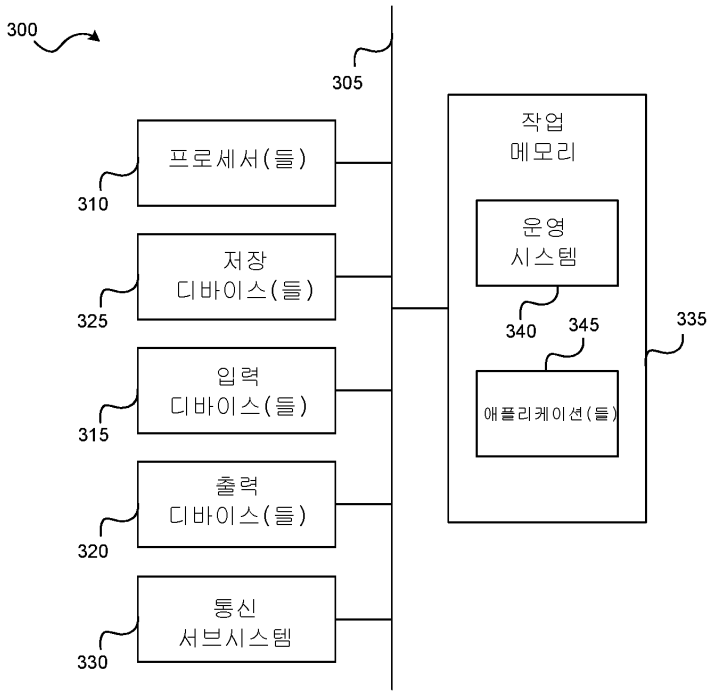
도면1


123
122
121
무선
트랜시버
112
DSP
140
메모리
120
통신
인터페이스
101
버스
159
158
111
프로세서
150
사용자
인터페이스
155
SPS
수신기
모바일 디바이스
100

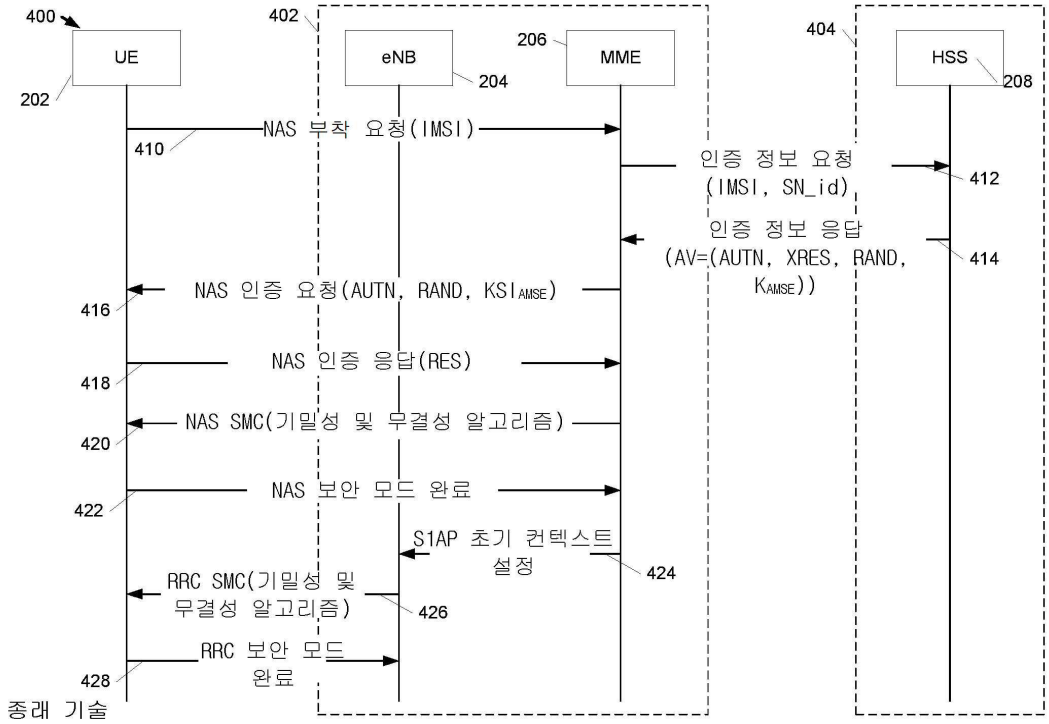
도면2


200
208
HSS
206
MME
PCRF
212
202
UE
204
eNB
S-GW
PDN
GW
214
210

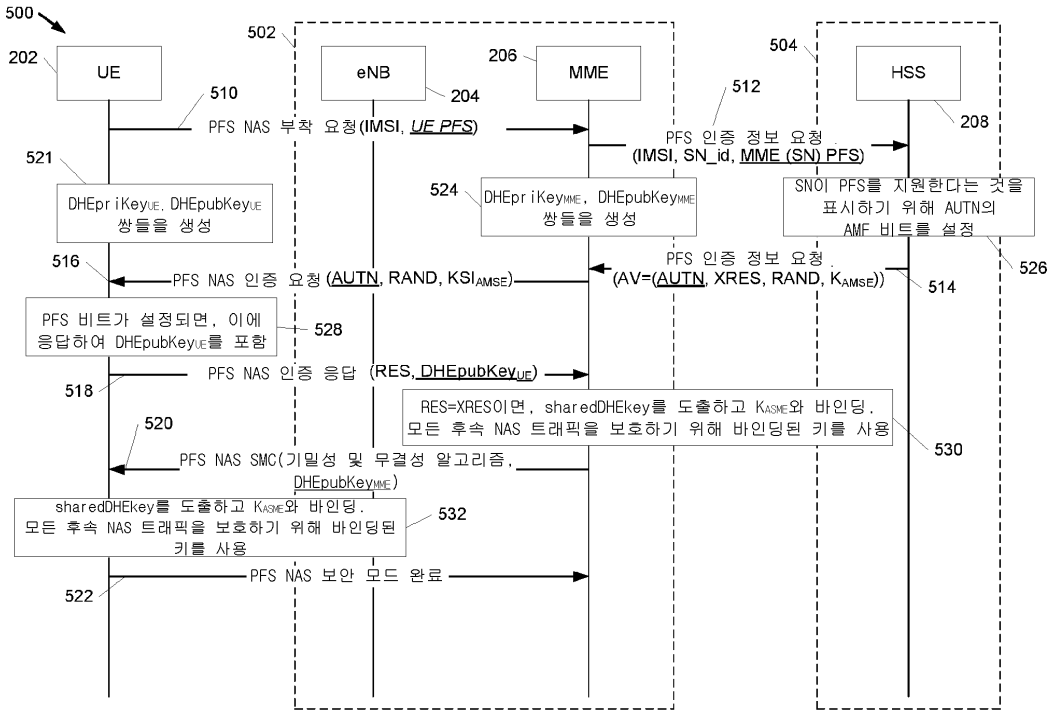
도면3


300
305
프로세서(들)
310
저장 디바이스(들)
325
입력 디바이스(들)
315
출력 디바이스(들)
320
통신 서브시스템
330
작업 메모리
운영 시스템
340
345
335
애플리케이션(들)

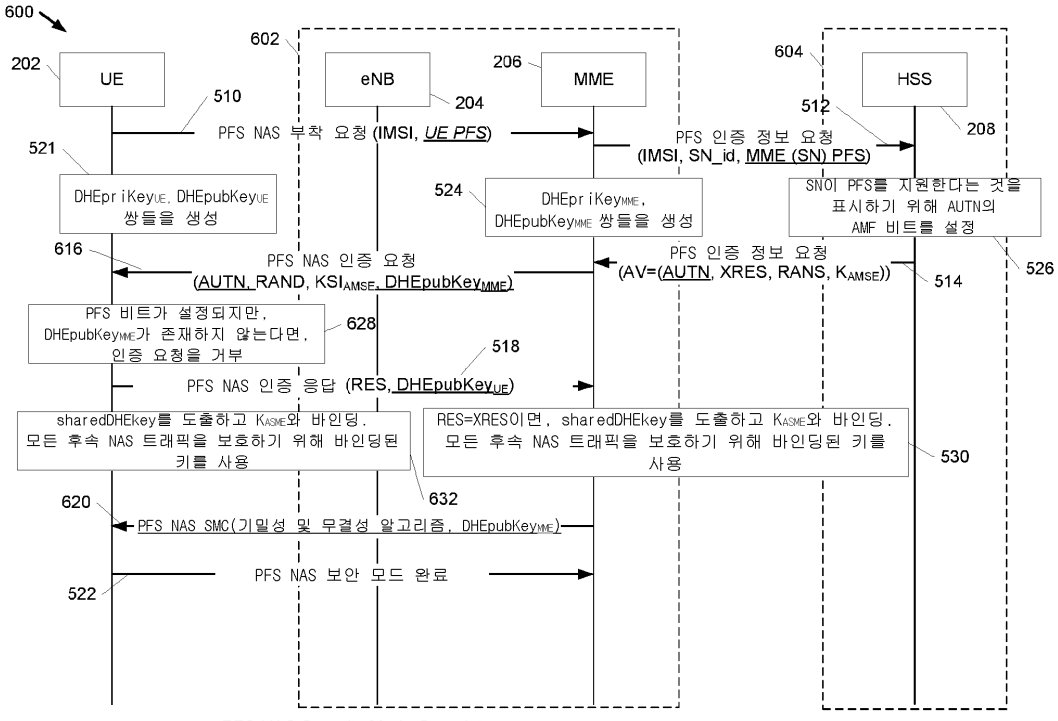
도면4


400
UE
202
402
eNB
204
206
MME
404
HSS
208
NAS 부착 요청(IMSI)
410
인증 정보 요청 (IMSI, SN_id)
412
인증 정보 응답 (AV=(AUTN, XRES, RAND, KAMSE))
414
NAS 인증 요청(AUTN, RAND, KSIAMSE)
416
NAS 인증 응답(RES)
418
NAS SMC(기밀성 및 무결성 알고리즘)
420
NAS 보안 모드 완료
422
S1AP 초기 컨텍스트 설정
424
RRC SMC(기밀성 및 무결성 알고리즘)
426
RRC 보안 모드 완료
428
종래 기술

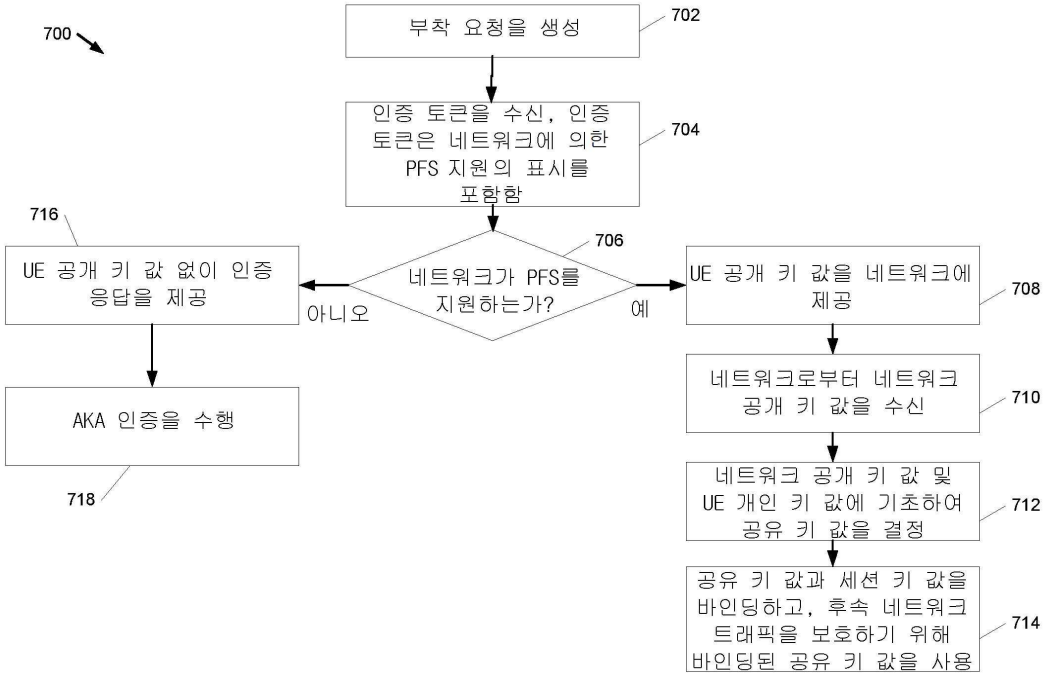
도면5


500
502
202
UE
eNB
206
MME
504
HSS
204
208
510
PFS NAS 부착 요청(IMSI, UE PFS)
512
PFS 인증 정보 요청
(IMSI, SN_id, MME (SN) PFS)
521
DHEpriKeyUE, DHEpubKeyUE
쌍들을 생성
524
DHEpriKeyMME, DHEpubKeyMME
쌍들을 생성
SN이 PFS를 지원한다는 것을
표시하기 위해 AUTN의
AMF 비트를 설정
526
516
PFS NAS 인증 요청 (AUTN, RAND, KSIAMSE)
PFS 인증 정보 요청
(AV=(AUTN, XRES, RAND, KAMSE))
514
PFS 비트가 설정되면, 이에
응답하여 DHEpubKeyUE를 포함
528
PFS NAS 인증 응답 (RES, DHEpubKeyUE)
518
RES=XRES이면, sharedDHEkey를 도출하고 KASME와 바인딩,
모든 후속 NAS 트래픽을 보호하기 위해 바인딩된 키를 사용
530
520
PFS NAS SMC(기밀성 및 무결성 알고리즘,
DHEpubKeyMME)
sharedDHEkey를 도출하고 KASME와 바인딩,
모든 후속 NAS 트래픽을 보호하기 위해 바인딩된
키를 사용
532
PFS NAS 보안 모드 완료
522

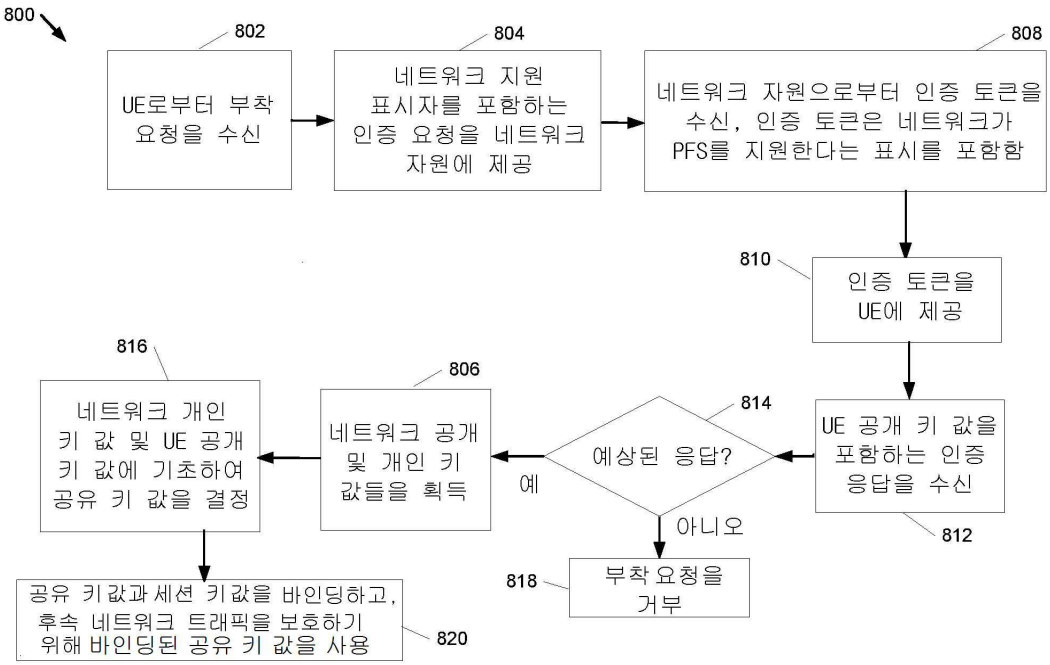
도면6


600
602
202
UE
eNB
206
MME
604
HSS
204
208
510
PFS NAS 부착 요청(IMSI, UE PFS)
512
PFS 인증 정보 요청
(IMSI, SN_id, MME (SN) PFS)
521
DHEpriKeyUE, DHEpubKeyUE
쌍들을 생성
524
DHEpriKeyMME,
DHEpubKeyMME 쌍들을 생성
SN이 PFS를 지원한다는 것을
표시하기 위해 AUTN의
AMF 비트를 설정
526
616
PFS NAS 인증 요청
(AUTN, RAND, KSIAMSE, DHEpubKeyMME)
PFS 인증 정보 요청
(AV=(AUTN, XRES, RANS, KAMSE))
514
PFS 비트가 설정되지만,
DHEpubKeyMME가 존재하지 않는다면,
인증 요청을 거부
628
518
PFS NAS 인증 응답 (RES, DHEpubKeyUE)
sharedDHEkey를 도출하고 KASME와 바인딩,
모든 후속 NAS 트래픽을 보호하기 위해 바인딩된
키를 사용
RES=XRES이면, sharedDHEkey를 도출하고 KASME와 바인딩,
모든 후속 NAS 트래픽을 보호하기 위해 바인딩된 키를
사용
530
632
620
PFS NAS SMC(기밀성 및 무결성 알고리즘, DHEpubKeyMME)
PFS NAS 보안 모드 완료
522

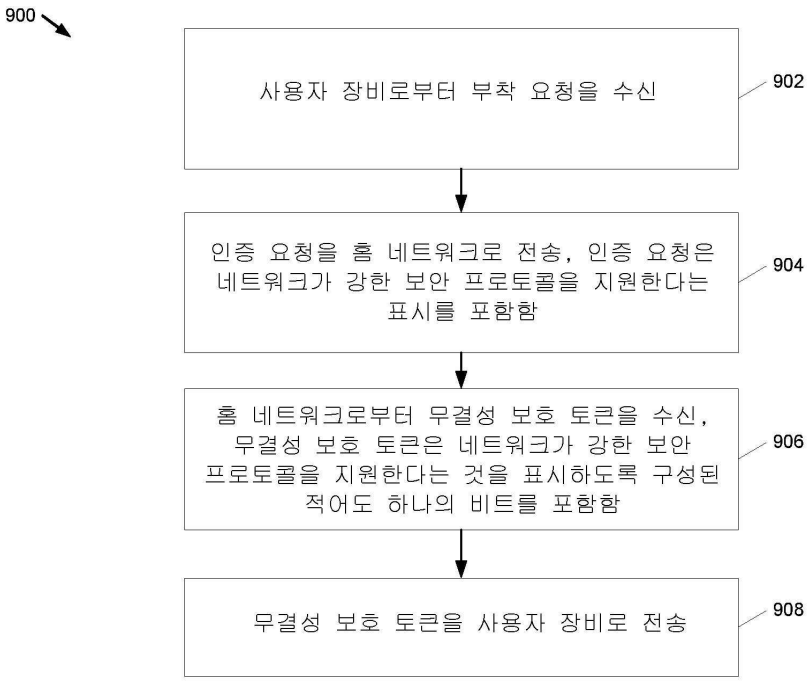
도면7


700
부착 요청을 생성
702
인증 토큰을 수신, 인증 토큰은 네트워크에 의한 PFS 지원의 표시를 포함함
704
네트워크가 PFS를 지원하는가?
706
예
아니오
UE 공개 키 값을 네트워크에 제공
708
네트워크로부터 네트워크 공개 키 값을 수신
710
네트워크 공개 키 값 및 UE 개인 키 값에 기초하여 공유 키 값을 결정
712
공유 키 값과 세션 키 값을 바인딩하고, 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용
714
716
UE 공개 키 값 없이 인증 응답을 제공
AKA 인증을 수행
718

도면8


800
802
UE로부터 부착 요청을 수신
804
네트워크 지원 표시자를 포함하는 인증 요청을 네트워크 자원에 제공
808
네트워크 자원으로부터 인증 토큰을 수신, 인증 토큰은 네트워크가 PFS를 지원한다는 표시를 포함함
810
인증 토큰을 UE에 제공
UE 공개 키 값을 포함하는 인증 응답을 수신
812
814
예상된 응답?
예
아니오
806
네트워크 공개 및 개인 키 값들을 획득
816
네트워크 개인 키 값 및 UE 공개 키 값에 기초하여 공유 키 값을 결정
818
부착 요청을 거부
공유 키 값과 세션 키 값을 바인딩하고, 후속 네트워크 트래픽을 보호하기 위해 바인딩된 공유 키 값을 사용
820

도면9


900
사용자 장비로부터 부착 요청을 수신
902
인증 요청을 홈 네트워크로 전송, 인증 요청은 네트워크가 강한 보안 프로토콜을 지원한다는 표시를 포함함
904
홈 네트워크로부터 무결성 보호 토큰을 수신, 무결성 보호 토큰은 네트워크가 강한 보안 프로토콜을 지원한다는 것을 표시하도록 구성된 적어도 하나의 비트를 포함함
906
무결성 보호 토큰을 사용자 장비로 전송
908