



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0147402
(43) 공개일자 2021년12월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2020-0064585
(22) 출원일자 2020년05월28일
심사청구일자 2020년05월28일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
강다영
서울특별시 노원구 화랑로 564, 111동 503호(공릉동, 육사아파트)
최진영
서울특별시 노원구 동일로248길 16, 506동 1003호(상계동, 수락파크빌아파트)
(74) 대리인
이대호, 박진홍

전체 청구항 수 : 총 21 항

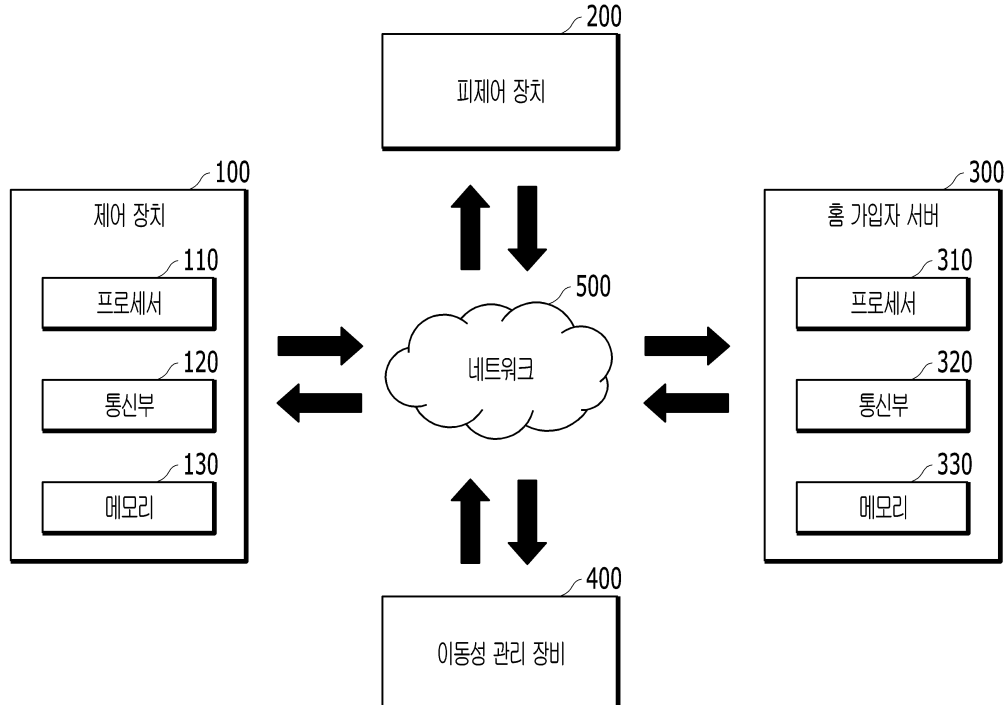
(54) 발명의 명칭 피제어 장치의 보안 인증 기법

(57) 요약

본 개시의 몇몇 실시예에 따라, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 제어 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은: 피제어 장치로부터 상기 피제어 장치의 SIM(Subscriber Identity Module)과 관련된 IMSI(International Mobile

(뒷면에 계속)

대표도 - 도1



Station Identity) 및 위치 정보를 획득하는 단계; 해시 함수(hash function)를 이용하여, 상기 IMSI를 해싱한 해시 값을 산출하는 단계; 비대칭 키 알고리즘(Asymmetric Key Algorithm)을 이용하여, 상기 제어 장치의 개인키로 상기 해시 값 및 상기 위치 정보를 암호화한 제 1 서명 데이터를 생성하는 단계; 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 홈 가입자 서버(Home Subscriber Server)의 공개키로 암호화한 제 1 암호 데이터를 생성하는 단계; 및 상기 제 1 암호 데이터를 포함하는 연결 요청 메시지를 홈 가입자 서버로 전송하는 단계;를 포함할 수 있다.

(52) CPC특허분류

H04L 9/0827 (2013.01)
H04L 9/0838 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/0877 (2013.01)
H04L 9/3213 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3271 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	20180005320031001
과제번호	2018-0-00532
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원 (IITP)
연구사업명	정보보호핵심원천기술개발
연구과제명	고등급(EAL6 이상) 보안 마이크로커널 개발
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명세서

청구범위

청구항 1

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 제어 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은:

피제어 장치로부터 상기 피제어 장치의 SIM(Subscriber Identity Module)과 관련된 IMSI(International Mobile Station Identity) 및 위치 정보를 획득하는 단계;

해시 함수(hash function)를 이용하여, 상기 IMSI를 해싱한 해시 값을 산출하는 단계;

비대칭 키 알고리즘(Asymmetric Key Algorithm)을 이용하여, 상기 제어 장치의 개인키로 상기 해시 값 및 상기 위치 정보를 암호화한 제 1 서명 데이터를 생성하는 단계;

상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 홈 가입자 서버(Home Subscriber Server)의 공개키로 암호화한 제 1 암호 데이터를 생성하는 단계; 및

상기 제 1 암호 데이터를 포함하는 연결 요청 메시지를 홈 가입자 서버로 전송하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 2

제 1 항에 있어서,

상기 피제어 장치로부터 상기 피제어 장치의 SIM(Subscriber Identity Module)과 관련된 IMSI(International Mobile Station Identity) 및 위치 정보를 획득하는 단계는,

유선 보안 채널(wired secure channel)을 이용하여, 상기 피제어 장치로부터 상기 IMSI 및 상기 위치 정보를 수신하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 3

제 1 항에 있어서,

상기 홈 가입자 서버에서 상기 연결 요청 메시지에 대한 연결 수락이 결정된 경우, 상기 홈 가입자 서버로부터 제 2 암호 데이터를 포함하는 연결 응답 메시지를 수신하는 단계;

상기 제 2 암호 데이터에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI(Temporary Mobile Subscriber Identity)를 추출하는 단계; 및

유선 보안 채널을 이용하여, 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 상기 피제어 장치로 전송하는 단계;

를 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 4

제 3 항에 있어서,

상기 제 2 암호 데이터는,

상기 홈 가입자 서버가 상기 비대칭 키 알고리즘을 이용하여, 상기 홈 가입자 서버의 개인키로 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 암호화한 제 2 서명 데이터를 생성하고, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 2 서명 데이터를 상기 제어 장치의 공개키로 암호화한 데이터인,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 5

제 4 항에 있어서,

상기 연결 응답 메시지에 포함된 상기 제 2 암호 데이터에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI(Temporary Mobile Subscriber Identity)를 추출하는 단계는,

상기 비대칭키 알고리즘을 이용하여, 상기 제 2 암호 데이터를 상기 제어 장치의 개인키로 복호화 하여, 상기 제 2 서명 데이터를 획득하는 단계; 및

상기 비대칭 키 알고리즘을 이용하여, 상기 제 2 서명 데이터를 상기 홈 가입자 서버의 공개키로 복호화 하여, 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 획득하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 6

제 3 항에 있어서,

상기 제 1 인증 토큰은,

EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm)에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 상기 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 상기 홈 가입자 서버가 획득하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 7

제 3 항에 있어서,

상기 제 1 인증 토큰은,

상기 홈 가입자 서버가 상기 제 1 인증 토큰을 전송한 것이 맞는지 여부를 상기 피제어 장치가 판단하는 검증 절차에 사용되는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 8

제 7 항에 있어서,

상기 검증 절차는 상기 피제어 장치에서 이하의 검증 단계들에 의해 수행되고, 상기 검증 단계들은:

상기 피제어 장치가 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 수신한 경우, EPS-AKA 알고리즘에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 상기 랜덤 값을 포함하는 제 2 입력 데이터를 입력하여 생성된 제 2 인증 토큰을 획득하는 단계; 및

상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일한지 여부에 따라 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞는지 여부를 판단하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 9

제 8 항에 있어서,

상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일한지 여부에 따라 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞는지 여부를 판단하는 단계는,

상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일하다고 인식한 경우, 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞다고 판단하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 10

제 8 항에 있어서,

상기 EPS-AKA 알고리즘은,

상기 제 2 입력 데이터가 입력됨에 따라, RES(response) 값 및 비밀키를 더 생성하고,

상기 제 1 TMSI, 상기 RES 값 및 상기 비밀키는,

상기 피제어 장치의 인증 절차에 사용되는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 11

제 10 항에 있어서,

상기 인증 절차는 상기 피제어 장치와 상기 피제어 장치의 통신을 관리하는 이동성 관리 장비(Mobility Management Entity)에서 이하의 인증 단계들에 의해 수행되고, 상기 인증 단계들은:

상기 피제어 장치가 상기 비밀키를 이용하여, 상기 RES 값 및 상기 제 1 TMSI를 암호화한 인증 요청 메시지를 생성하는 단계;

상기 피제어 장치가 상기 인증 요청 메시지를 상기 이동성 관리 장비로 전송하는 단계;

상기 이동성 관리 장비가 상기 인증 요청 메시지를 수신한 경우, 상기 인증 요청 메시지에서 상기 RES 값 및 상기 제 1 TMSI를 추출하기 위해 상기 이동성 관리 장비에 사전 저장된 비밀키를 이용하여, 상기 인증 요청 메시지를 복호화하는 단계; 및

상기 이동성 관리 장비가 상기 인증 요청 메시지에서 추출된 상기 RES 값 및 상기 제 1 TMSI와 상기 이동성 관

리 장비의 메모리에 사전 저장된 XRES(Expected Response) 값 및 제 2 TMSI를 비교한 결과에 기초하여, 상기 피 제어 장치를 인증하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 12

제 11 항에 있어서,

상기 이동성 관리 장비가 상기 인증 요청 메시지에서 추출된 상기 RES 값 및 상기 제 1 TMSI와 상기 이동성 관리 장비의 메모리에 사전 저장된 XRES(Expected Response) 값 및 제 2 TMSI를 비교한 결과에 기초하여, 상기 피 제어 장치를 인증하는 단계는,

상기 제 1 TMSI와 상기 제 2 TMSI가 동일하다고 인식하고, 상기 RES 값과 상기 XRES 값이 동일하다고 인식한 경우, 상기 피제어 장치에 대한 인증을 완료하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 13

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 홈 가입자 서버(Home Subscriber Server)의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은:

피제어 장치를 제어하는 제어 장치로부터 비대칭 키 알고리즘(Asymmetric Key Algorithm)에 기초하여 암호화된 제 1 암호 데이터를 포함하는 연결 요청 메시지를 수신하는 단계;

상기 제 1 암호 데이터에서 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 추출하는 단계;

상기 제 1 해시 값과 메모리에 사전 저장된 제 2 해시 값을 비교하여, 상기 피제어 장치의 통신망 가입 상태가 유효한지 여부를 판단하는 단계; 및

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치의 위치 정보에 기초하여, 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비(Mobility Management Entity)를 결정하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 14

제 13 항에 있어서,

상기 제 1 암호 데이터는,

상기 제어 장치가 상기 비대칭 키 알고리즘을 이용하여, 상기 제어 장치의 개인키로 상기 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 암호화한 제 1 서명 데이터를 생성하고, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 상기 홈 가입자 서버의 공개키로 암호화한 데이터인,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 15

제 14 항에 있어서,

상기 제 1 암호 데이터에서 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 추출하는 단계는,

상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 암호 데이터를 상기 홈 가입자 서버의 개인키로 복호화 하여, 상기 제 1 서명 데이터를 획득하는 단계; 및

상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 상기 제어 장치의 공개키로 복호화 하여, 상기 제 1 해시 값 및 상기 위치 정보를 획득하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 16

제 13 항에 있어서,

상기 제어 장치로부터 상기 연결 요청 메시지를 수신하기 전에, 상기 피제어 장치의 SIM(subscriber identity module)과 관련된 IMSI(International Mobile Station Identity) 및 인증키를 획득하는 단계; 및

해시 함수(hash function)를 이용하여, 상기 IMSI를 해싱한 상기 제 2 해시 값을 산출하고, 상기 제 2 해시 값 및 상기 인증키를 상기 메모리에 저장하는 단계;

를 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 17

제 16 항에 있어서,

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 연결 요청 메시지에 대응하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계; 및

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치와 상기 이동성 관리 장비 간 인증을 수행하도록 상기 이동성 관리 장비로 사전 접속 요청 메시지를 전송하는 단계;

를 더 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 18

제 17 항에 있어서,

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 연결 요청 메시지에 대응하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계는,

EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm)에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 제 1 인증 토큰을 획득하는 단계;

상기 IMSI에 대응하는 TMSI(Temporary Mobile Subscriber Identity)를 생성하는 단계; 및

상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 암호화한 제 2 암호 데이터를 포함하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 19

제 18 항에 있어서,

상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 암호화한 제 2 암호 데이터를 포함하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계는,

상기 비대칭 키 알고리즘을 이용하여, 상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 상기 홈 가입자 서버의 개인키로 암호화한 제 2 서명 데이터를 생성하는 단계; 및

상기 비대칭 키 알고리즘을 이용하여, 상기 제어 장치의 공개키로 암호화한 상기 제 2 암호 데이터를 생성하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 20

제 17 항에 있어서,

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치와 이동성 관리 장비 간 인증을 수행하도록 상기 이동성 관리 장비로 사전 접속 요청 메시지를 전송하는 단계는,

EPS-AKA 알고리즘에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 XRES 값 및 비밀키를 획득하는 단계;

상기 IMSI에 대응하는 TMSI를 생성하는 단계; 및

상기 피제어 장치와 상기 이동성 관리 장비 간 인증을 수행하는데 사용되는 상기 XRES 값, 상기 TMSI 및 상기 비밀키를 포함하는 상기 사전 접속 요청 메시지를 생성하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 21

제 13 항에 있어서,

상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치의 위치 정보에 기초하여, 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비(Mobility Management Entity)를 결정하는 단계는,

상기 피제어 장치의 위치 정보에 기초하여, 상기 피제어 장치의 위치에서 기 설정된 반경 이내에 위치하는 적어도 하나의 이동성 관리 장비를 인식하는 단계; 및

상기 기 설정된 반경 이내에 위치하는 상기 적어도 하나의 이동성 관리 장비를 상기 사전 접속 요청 메시지를 수신 받을 상기 이동성 관리 장비로 결정하는 단계;

를 포함하는,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술분야

[0001] 본 개시 내용은 피제어 장치의 보안 인증 기법에 관한 것으로서, 보다 구체적으로, 피제어 장치의 IMSI(International Mobile Station Identity)에 대한 보안성을 높인 보안 인증 기법에 관한 것이다.

배경기술

[0002] LTE는 Long-Term Evolution의 약어로 4세대 이동통신 기술이다. LTE는 고속 전송, 비트당 비용 절감, 낮은 전송 지연, 기존 주파수 대역 적용 가능 등을 목표로 설계되어, 현재 전 세계적으로 시장 도입 및 상용화 되어 있다.

[0003] 그러나, 상기 LTE 기술은 계속된 기술 업그레이드와 보안 취약점의 보완에도 불구하고 LTE 망 접속을 위한 Initial Attach 구간에서의 UE(User Equipment)의 식별 파라미터 값인 IMSI가 평문으로 노출되는 취약점은 개선되지 않고 있다. 또한, 해당 취약점은 LTE Standards Release 초기부터 존재한 취약점이다.

[0004] 해당 취약점이 개선되지 않은 상태에서 LTE 망에 접속할 경우, Initial Attach 구간에서의 식별 파라미터들의 유출 및 제 3자의 공격을 받을 수 있으며, 이로 인해 UE의 추적 및 Privacy 침해 등의 문제가 발생할 수 있다.

[0005] 한편, 국내외 통신 업계는 2016년부터 LTE 망을 이용한 LTE 통신 드론을 연구 및 개발하고 있다. 구체적으로, 통신 업계는 LTE 망을 이용하여 드론 운용 환경을 개선하고, 이를 토대로 기존 산업과 드론 융합을 시도하고 있다. LTE 망을 이용하여 드론을 운용하는 경우, 기존 드론의 단점(주파수 통신 방식으로 운용되는 주파수 통신 드론은 비행 거리가 전파 송수신 거리까지로 제한됨)을 극복하고 운용 범위를 넓힐 수 있다.

[0006] 전술한 LTE 통신 드론은 종래의 주파수 통신 드론의 한계점을 극복 가능하며, 다양한 분야에 이용될 수 있다. 하지만, LTE 망 사용시 LTE 통신 드론의 IMSI가 노출되는 취약점으로 인해 LTE 통신 드론의 사용 분야가 제한될 수도 있다.

[0007] 따라서, LTE 망에서의 보안 취약점을 극복하는 기술이 당업계에 요구될 수 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 공개특허공보 제10-2017-0112709호

발명의 내용

해결하려는 과제

[0009] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 피제어 장치의 식별 파라미터에 대한 보안성을 높인 보안 인증 기법을 제공하고자 하는 것이다.

[0010] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 제어 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은: 피제어 장치로부터 상기 피제어 장치의 SIM(Subscriber Identity Module)과 관련된 IMSI(International Mobile Station Identity) 및 위치 정보를 획득하는 단계; 해시 함수(hash function)를 이용하여, 상기 IMSI를 해싱한 해시 값을 산출하는 단계; 비대칭 키 알고리즘(Asymmetric Key Algorithm)을 이용하여, 상기 제어 장치의 개인키로 상기 해시 값 및 상기 위치 정보를 암호화한 제 1 서명 데이터를 생성하는 단계; 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 홈 가입자 서버(Home Subscriber Server)의 공개키로 암호화한 제 1 암호 데이터를 생성하는 단계; 및 상기 제 1 암호 데이터를 포함하는 연결 요청 메시지를 홈 가입자 서버로 전송하는 단계;를 포함할 수 있다.

[0012] 또한, 상기 피제어 장치로부터 상기 피제어 장치의 SIM(Subscriber Identity Module)과 관련된

IMSI(International Mobile Station Identity) 및 위치 정보를 획득하는 단계는, 유선 보안 채널(wired secure channel)을 이용하여, 상기 피제어 장치로부터 상기 IMSI 및 상기 위치 정보를 수신하는 단계;를 포함할 수 있다.

- [0013] 또한, 상기 단계들은, 상기 홈 가입자 서버에서 상기 연결 요청 메시지에 대한 연결 수락이 결정된 경우, 상기 홈 가입자 서버로부터 제 2 암호 데이터를 포함하는 연결 응답 메시지를 수신하는 단계; 상기 제 2 암호 데이터에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI(Temporary Mobile Subscriber Identity)를 추출하는 단계; 및 유선 보안 채널을 이용하여, 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 상기 피제어 장치로 전송하는 단계;를 더 포함할 수 있다.
- [0014] 또한, 상기 제 2 암호 데이터는, 상기 홈 가입자 서버가 상기 비대칭 키 알고리즘을 이용하여, 상기 홈 가입자 서버의 개인키로 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 암호화한 제 2 서명 데이터를 생성하고, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 2 서명 데이터를 상기 제어 장치의 공개키로 암호화한 데이터일 수 있다.
- [0015] 또한, 상기 연결 응답 메시지에 포함된 상기 제 2 암호 데이터에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI(Temporary Mobile Subscriber Identity)를 추출하는 단계는, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 2 암호 데이터를 상기 제어 장치의 개인키로 복호화 하여, 상기 제 2 서명 데이터를 획득하는 단계; 및 상기 비대칭 키 알고리즘을 이용하여, 상기 제 2 서명 데이터를 상기 홈 가입자 서버의 공개키로 복호화 하여, 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 획득하는 단계;를 포함할 수 있다.
- [0016] 또한, 상기 제 1 인증 토큰은, EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm)에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 상기 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 상기 홈 가입자 서버가 획득할 수 있다.
- [0017] 또한, 상기 제 1 인증 토큰은, 상기 홈 가입자 서버가 상기 제 1 인증 토큰을 전송한 것이 맞는지 여부를 상기 피제어 장치가 판단하는 검증 절차에 사용될 수 있다.
- [0018] 또한, 상기 검증 절차는 상기 피제어 장치에서 이하의 검증 단계들에 의해 수행되고, 상기 검증 단계들은: 상기 피제어 장치가 상기 랜덤 값, 상기 제 1 인증 토큰 및 상기 제 1 TMSI를 수신한 경우, EPS-AKA 알고리즘에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 상기 랜덤 값을 포함하는 제 2 입력 데이터를 입력하여 생성된 제 2 인증 토큰을 획득하는 단계; 및 상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일한지 여부에 따라 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞는지 여부를 판단하는 단계;를 포함할 수 있다.
- [0019] 또한, 상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일한지 여부에 따라 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞는지 여부를 판단하는 단계는, 상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일하다고 인식한 경우, 상기 제 1 인증 토큰이 상기 홈 가입자 서버가 전송한 것이 맞다고 판단하는 단계;를 포함할 수 있다.
- [0020] 또한, 상기 EPS-AKA 알고리즘은, 상기 제 2 입력 데이터가 입력됨에 따라, RES(response) 값 및 비밀키를 더 생성하고, 상기 제 1 TMSI, 상기 RES 값 및 상기 비밀키는, 상기 피제어 장치의 인증 절차에 사용될 수 있다.
- [0021] 또한, 상기 인증 절차는 상기 피제어 장치와 상기 피제어 장치의 통신을 관리하는 이동성 관리 장비(Mobility Management Entity)에서 이하의 인증 단계들에 의해 수행되고, 상기 인증 단계들은: 상기 피제어 장치가 상기 비밀키를 이용하여, 상기 RES 값 및 상기 제 1 TMSI를 암호화한 인증 요청 메시지를 생성하는 단계; 상기 피제어 장치가 상기 인증 요청 메시지를 상기 이동성 관리 장비로 전송하는 단계; 상기 이동성 관리 장비가 상기 인증 요청 메시지를 수신한 경우, 상기 인증 요청 메시지에서 상기 RES 값 및 상기 제 1 TMSI를 추출하기 위해 상기 이동성 관리 장비에 사전 저장된 비밀키를 이용하여, 상기 인증 요청 메시지를 복호화하는 단계; 및 상기 이동성 관리 장비가 상기 인증 요청 메시지에서 추출된 상기 RES 값 및 상기 제 1 TMSI와 상기 이동성 관리 장비의 메모리에 사전 저장된 XRES(Expected Response) 값 및 제 2 TMSI를 비교한 결과에 기초하여, 상기 피제어 장치를 인증하는 단계;를 포함할 수 있다.
- [0022] 또한, 상기 이동성 관리 장비가 상기 인증 요청 메시지에서 추출된 상기 RES 값 및 상기 제 1 TMSI와 상기 이동성 관리 장비의 메모리에 사전 저장된 XRES(Expected Response) 값 및 제 2 TMSI를 비교한 결과에 기초하여, 상기 피제어 장치를 인증하는 단계는, 상기 제 1 TMSI와 상기 제 2 TMSI가 동일하다고 인식하고, 상기 RES 값과 상기 XRES 값이 동일하다고 인식한 경우, 상기 피제어 장치에 대한 인증을 완료하는 단계;를 포함할 수 있다.

- [0023] 진술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 홈 가입자 서버(Home Subscriber Server)의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은: 피제어 장치를 제어하는 제어 장치로부터 비대칭 키 알고리즘(Asymmetric Key Algorithm)에 기초하여 암호화된 제 1 암호 데이터를 포함하는 연결 요청 메시지를 수신하는 단계; 상기 제 1 암호 데이터에서 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 추출하는 단계; 상기 제 1 해시 값과 메모리에 사전 저장된 제 2 해시 값을 비교하여, 상기 피제어 장치의 통신망 가입 상태가 유효한지 여부를 판단하는 단계; 및 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치의 위치 정보에 기초하여, 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비(Mobility Management Entity)를 결정하는 단계;를 포함할 수 있다.
- [0024] 또한, 상기 제 1 암호 데이터는, 상기 제어 장치가 상기 비대칭 키 알고리즘을 이용하여, 상기 제어 장치의 개인키로 상기 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 암호화한 제 1 서명 데이터를 생성하고, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 상기 홈 가입자 서버의 공개키로 암호화한 데이터일 수 있다.
- [0025] 또한, 상기 제 1 암호 데이터에서 제 1 해시 값 및 상기 피제어 장치의 위치 정보를 추출하는 단계는, 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 암호 데이터를 상기 홈 가입자 서버의 개인키로 복호화 하여, 상기 제 1 서명 데이터를 획득하는 단계; 및 상기 비대칭 키 알고리즘을 이용하여, 상기 제 1 서명 데이터를 상기 제어 장치의 공개키로 복호화 하여, 상기 제 1 해시 값 및 상기 위치 정보를 획득하는 단계;를 포함할 수 있다.
- [0026] 또한, 상기 단계들은, 상기 제어 장치로부터 상기 연결 요청 메시지를 수신하기 전에, 상기 피제어 장치의 SIM(subscriber identity module)과 관련된 IMSI(International Mobile Station Identity) 및 인증키를 획득하는 단계; 및 해시 함수(hash function)를 이용하여, 상기 IMSI를 해싱한 상기 제 2 해시 값을 산출하고, 상기 제 2 해시 값 및 상기 인증키를 상기 메모리에 저장하는 단계;를 더 포함할 수 있다.
- [0027] 또한, 상기 단계들은, 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 연결 요청 메시지에 대응하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계; 및 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치와 상기 이동성 관리 장비 간 인증을 수행하도록 상기 이동성 관리 장비로 사전 접속 요청 메시지를 전송하는 단계;를 더 포함할 수 있다.
- [0028] 또한, 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 연결 요청 메시지에 대응하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계는, EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm)에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 제 1 인증 토큰을 획득하는 단계; 상기 IMSI에 대응하는 TMSI(Temporary Mobile Subscriber Identity)를 생성하는 단계; 및 상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 암호화한 제 2 암호 데이터를 포함하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계;를 포함할 수 있다.
- [0029] 또한, 상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 암호화한 제 2 암호 데이터를 포함하는 연결 응답 메시지를 상기 제어 장치로 전송하는 단계는, 상기 비대칭 키 알고리즘을 이용하여, 상기 랜덤 값, 상기 TMSI 및 상기 제 1 인증 토큰을 상기 홈 가입자 서버의 개인키로 암호화한 제 2 서명 데이터를 생성하는 단계; 및 상기 비대칭 키 알고리즘을 이용하여, 상기 제어 장치의 공개키로 암호화한 상기 제 2 암호 데이터를 생성하는 단계;를 포함할 수 있다.
- [0030] 또한, 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치와 이동성 관리 장비 간 인증을 수행하도록 상기 이동성 관리 장비로 사전 접속 요청 메시지를 전송하는 단계는, EPS-AKA 알고리즘에 상기 피제어 장치의 상기 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 XRES 값 및 비밀키를 획득하는 단계; 상기 IMSI에 대응하는 TMSI를 생성하는 단계; 및 상기 피제어 장치와 상기 이동성 관리 장비 간 인증을 수행하는데 사용되는 상기 XRES 값, 상기 TMSI 및 상기 비밀키를 포함하는 상기 사전 접속 요청 메시지를 생성하는 단계;를 포함할 수 있다.
- [0031] 또한, 상기 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 피제어 장치의 위치 정보에 기초하여, 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비(Mobility Management Entity)를 결정하는 단계는, 상기 피제어 장치의 위치 정보에 기초하여, 상기 피제어 장치의 위치에서 기 설정된 반경 이내에 위치하는 적어도 하나의 이동성 관리 장비를 인식하는 단계; 및 상기 기 설정된 반경 이내에 위치하는 상기 적어도 하나의 이동성 관리 장비를 상기 사전 접속 요청 메시지를 수신 받을 상기 이동성 관리 장비로 결정하는 단계;를 포함할

수 있다.

[0032] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0033] 본 개시는 피제어 장치의 IMSI에 대한 보안성을 높인 보안 인증 기법을 통해 피제어 장치의 추적 및 정보 유출 등의 문제를 해결할 수 있다.

[0034] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0035] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시될 수 있음은 명백할 것이다.

도 1은 본 개시의 다양한 양태가 구현될 수 있는 제어 장치, 피제어 장치, 홈 가입자 서버 및 이동성 관리 장비를 포함하는 보안 인증 시스템의 일례를 설명하기 위한 도면이다.

도 2는 본 개시의 몇몇 실시예에 따른 보안 인증 기법의 일례를 설명하기 위한 흐름도이다.

도 3은 본 개시의 몇몇 실시예에 따른 제어 장치가 보안 인증을 수행하는 방법의 일례를 설명하기 위한 흐름도이다.

도 4는 본 개시의 몇몇 실시예에 따른 제어 장치가 보안 인증을 수행하는 방법의 구체적인 일례를 설명하기 위한 흐름도이다.

도 5는 본 개시의 몇몇 실시예에 따른 검증 절차를 설명하기 위한 흐름도이다.

도 6은 본 개시의 몇몇 실시예에 따른 인증 절차를 설명하기 위한 흐름도이다.

도 7은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 일례를 설명하기 위한 흐름도이다.

도 8은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 구체적인 일례를 설명하기 위한 흐름도이다.

도 9는 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 다른 구체적인 일례를 설명하기 위한 흐름도이다.

도 10은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 추가적인 일례를 설명하기 위한 흐름도이다.

도 11은 본 개시 내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0036] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는

설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

- [0037] 또한, 다양한 양상들 및 특징들이 하나 이상의 장치들, 단말들, 서버들, 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있는 시스템에 의하여 제시될 것이다. 다양한 시스템들이, 추가적인 장치들, 단말들, 서버들, 디바이스들, 컴포넌트들 및/또는 모듈들 등을 포함할 수 있다는 점 그리고/또는 도면들과 관련하여 논의된 장치들, 단말들, 서버들, 디바이스들, 컴포넌트들, 모듈들 등의 전부를 포함하지 않을 수도 있다는 점 또한 이해되고 인식되어야 한다.
- [0038] 본 명세서에서 사용되는 용어 "컴퓨터 프로그램", "컴포넌트", "모듈", "시스템" 등은 서로 호환가능하게 사용될 수 있으며, 그리고 컴퓨터-관련 엔티티, 하드웨어, 펌웨어, 소프트웨어, 소프트웨어 및 하드웨어의 조합, 또는 소프트웨어의 실행을 지칭한다. 예를 들어, 컴포넌트는 프로세서상에서 실행되는 처리과정(procedure), 프로세서, 객체, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수 있지만, 이들로 제한되는 것은 아니다. 예를 들어, 컴퓨팅 장치에서 실행되는 애플리케이션 및 컴퓨팅 장치 모두 컴포넌트일 수 있다. 하나 이상의 컴포넌트는 프로세서 및/또는 실행 스레드 내에 상주할 수 있다. 일 컴포넌트는 하나의 컴퓨터 내에 로컬화 될 수 있다. 일 컴포넌트는 2개 이상의 컴퓨터들 사이에 분배될 수 있다.
- [0039] 또한, 이러한 컴포넌트들은 그 내부에 저장된 다양한 데이터 구조들을 갖는 다양한 컴퓨터 판독가능한 매체로부터 실행할 수 있다. 컴포넌트들은 예를 들어 하나 이상의 데이터 패킷들을 갖는 신호(예를 들면, 로컬 시스템, 분산 시스템에서 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터 및/또는 신호를 통해 다른 시스템과 인터넷과 같은 네트워크를 통해 전송되는 데이터)에 따라 로컬 및/또는 원격 처리들을 통해 통신할 수 있다.
- [0040] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.
- [0041] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 개시를 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.
- [0042] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 개시의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.
- [0043] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0044] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.
- [0045] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.
- [0046] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 “모듈” 및 “부”는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.
- [0047] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구

체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

- [0048] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0049] 본 개시내용의 청구범위에서의 단계들에 대한 권리범위는, 각 단계들에 기재된 기능 및 특징들에 의해 발생하는 것이지, 각각의 단계에서 그 순서의 선후관계를 명시하지 않는 이상, 청구범위에서의 각 단계들의 기재 순서에 영향을 받지 않는다. 예를 들어, A단계 및 B단계를 포함하는 단계로 기재된 청구범위에서, A단계가 B단계 보다 먼저 기재되었다고 하더라도, A단계가 B단계 이전에 선행되어야 한다는 것으로 권리범위가 제한되지는 않는다.
- [0051] 도 1은 본 개시의 다양한 양태가 구현될 수 있는 제어 장치, 피제어 장치, 홈 가입자 서버 및 이동성 관리 장비를 포함하는 보안 인증 시스템의 일례를 설명하기 위한 도면이다.
- [0052] 도 1을 참조하면, 보안 인증 시스템은 제어 장치(100), 피제어 장치(200), 홈 가입자 서버(300), 이동성 관리 장비(400) 및 네트워크(500)를 포함할 수 있다. 다만, 상술한 구성 요소들은 보안 인증 시스템을 구현하는데 있어서 필수적인 것은 아니어서, 신용평가 시스템은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.
- [0053] 본 개시의 몇몇 실시예에 따르면, 제어 장치(100)는 피제어 장치(200)를 제어하기 위한 장치일 수 있다. 예를 들어, 제어 장치(100)는 지상관제시스템(GCS, Ground Control System)을 의미할 수 있다. 다만, 이에 한정되는 것은 아니다. 한편, 피제어 장치(200)는 상술한 바와 같이, 제어 장치(100)에 의해 제어되는 장치를 의미할 수 있다. 예를 들어, 피제어 장치(200)는 드론 또는, 무인 비행체일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0054] 제어 장치(100)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 또한, 제어 장치(100)는 휴대폰, 스마트 폰(smart phone), 노트북 컴퓨터(laptop computer), PDA(personal digital assistants), 슬레이트 PC(slate PC), 태블릿 PC(tablet PC), 울트라북(ultrabook), 웨어러블 디바이스(wearable device, 예를 들어, 위치형 단말기 (smartwatch), 글래스형 단말기(smart glass), HMD(head mounted display)) 등이 포함될 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0055] 제어 장치(100)는 프로세서(110), 통신부(120) 및 메모리(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 제어 장치(100)를 구현하는데 있어서 필수적인 것은 아니어서, 제어 장치(100)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다. 여기서, 각각의 구성요소들은 별개의 칩이나 모듈이나 장치로 구성될 수 있고, 하나의 장치 내에 포함될 수도 있다.
- [0056] 제어 장치(100)의 프로세서(110)는 통상적으로 제어 장치(100)의 전반적인 동작을 제어한다. 프로세서(110)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(130)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.
- [0057] 또한, 프로세서(110)는 메모리(130)에 저장된 응용 프로그램을 구동하기 위하여, 제어 장치(100)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(110)는 상기 응용 프로그램의 구동을 위하여, 제어 장치(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.
- [0058] 제어 장치(100)의 통신부(120)는 제어 장치(100)와 피제어 장치(200) 사이, 제어 장치(100)와 홈 가입자 서버(300) 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 통신부(120)는 제어 장치(100)를 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.
- [0059] 본 개시의 몇몇 실시예에 따른 제어 장치(100)의 통신부(120)는 피제어 장치(200)와 유선 또는 무선으로 통신할 수 있다. 또한, 통신부(120)는 피제어 장치(200)를 제어하기 위한 제어 데이터를 상기 피제어 장치(200)와 상호 송수신할 수 있다. 또한, 통신부(120)는 피제어 장치(200)를 통신망(여기서, LTE 망)에 최초 등록하기 위한 식별 파라미터를 상기 피제어 장치(200)로부터 수신할 수 있다. 예를 들어, 통신부(120)는 피제어 장치(200)로부터 식별 파라미터인 IMSI(International Mobile Station Identity)를 수신할 수 있다. 여기서, 통신부(120)는

IMSI는 피제어 장치(200)의 보안을 위해 유선 보안 채널(wired secure channel)을 통해 수신할 수 있다. 다만, 이에 한정되는 것은 아니다.

- [0060] 본 개시의 몇몇 실시예에 따른 제어 장치(100)의 프로세서(110)는 피제어 장치(200)로부터 통신망 최초 등록을 위한 식별 파라미터들을 수신한 경우, 상기 피제어 장치(200)를 통신망에 최초 등록시키기 위한 보안 인증 프로세스를 수행할 수 있다.
- [0061] 상술한 제어 장치(100)의 프로세서(110)가 보안 인증 프로세스를 수행하는 방법에 대한 설명은 도 2 내지 도 4를 참조하여 후술한다.
- [0062] 본 개시의 몇몇 실시예에 따르면, 홈 가입자 서버(300)는 통신망 가입자의 데이터베이스(database)의 역할을 수행하는 HSS(Home Subscribe Server)를 의미할 수 있다. 구체적으로, 홈 가입자 서버(300)는 통신망에 가입한 가입자들에 대한 정보를 가입 정보(subscription)의 형태로 저장할 수 있다. 또한, 홈 가입자 서버(300)는 가입자 등록/변경 관리, 인증, 권한 부여, 로케이션, 세션 라우팅, 과금 등의 호/세션 제어를 위한 모든 가입자 정보를 관리할 수 있다. 예를 들어, 홈 가입자 서버(300)는 IMS 망의 CSCF(Call Session Control Function)에 해당할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0063] 홈 가입자 서버(300)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0064] 홈 가입자 서버(300)는 프로세서(310), 통신부(320) 및 메모리(330)를 포함할 수 있다. 다만, 상술한 구성 요소들은 홈 가입자 서버(300)를 구현하는데 있어서 필수적인 것은 아니어서, 홈 가입자 서버(300)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다. 여기서, 각각의 구성요소들은 별개의 칩이나 모듈이나 장치로 구성될 수 있고, 하나의 장치 내에 포함될 수도 있다.
- [0065] 홈 가입자 서버(300)의 프로세서(310)는 통상적으로 홈 가입자 서버(300)의 전반적인 동작을 제어한다. 프로세서(310)는 위에서 살펴본 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(330)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.
- [0066] 또한, 프로세서(310)는 메모리(330)에 저장된 응용 프로그램을 구동하기 위하여, 홈 가입자 서버(300)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(310)는 상기 응용 프로그램의 구동을 위하여, 홈 가입자 서버(300)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.
- [0067] 홈 가입자 서버(300)의 통신부(320)는 홈 가입자 서버(300)와 제어 장치(100) 사이, 홈 가입자 서버(300)와 이동성 관리 장비(400) 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 통신부(320)는 홈 가입자 서버(300)를 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.
- [0068] 홈 가입자 서버(300)의 메모리(330)는 프로세서(310)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리(330)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 이러한 메모리(330)는 프로세서(310)에 제어에 의하여 동작 될 수 있다.
- [0069] 본 개시의 몇몇 실시예에 따른 메모리(330)는 인증센터(AuC, Authentication Center)일 수 있다. 또한, 메모리(330)는 통신망 가입자 정보(즉, 가입 단말의 정보)를 저장하고 있을 수 있다.
- [0070] 본 개시의 몇몇 실시예에 따르면, 홈 가입자 서버(300)의 통신부(320)는 제어 장치(100)로부터 피제어 장치(200)를 통신망에 최초 등록하기 위한 연결 요청 메시지를 수신할 수 있다. 이 경우, 프로세서(310)는 메모리(330)에 저장된 가입자 정보를 이용하여, 피제어 장치(200)의 통신망 가입 상태가 유효한지 여부를 판단할 수 있다. 또한, 프로세서(310)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우, 제어 장치(100)로 연결 응답 메시지를 전송하고, 이동성 관리 장비(400)로 사전 접속 요청 메시지를 전송하도록 통신부(320)를 제어할 수 있다.
- [0071] 예를 들어, 홈 가입자 서버(300)의 프로세서(310)는 통신부(320)를 통해 암호화된 피제어 장치(200)의 IMSI가

포함된 연결 요청 메시지를 제어 장치(100)로부터 수신할 수 있다. 그리고, 프로세서(310)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우, 상기 IMSI에 대응하는 TMSI(Temporary Mobile Subscriber Identity)를 암호화한 데이터를 포함하는 연결 응답 메시지를 제어 장치(100)로 전송할 수 있다.

[0072] 따라서, 홈 가입자 서버(300)와 제어 장치(100)는 피제어 장치(200)의 통신망 최초 등록 과정에서 메시지를 송수신할 때, 암호화된 데이터를 이용하여, 피제어 장치(200)의 식별 파라미터에 대한 보안성을 높일 수 있다. 다만, 이에 한정되는 것은 아니다.

[0073] 여기서, 홈 가입자 서버(300)의 프로세서(310)가 통신부(320)를 통해 제어 장치(100)로부터 연결 요청 메시지를 수신함에 따라 피제어 장치(200)의 통신망 가입 상태가 유효한지 여부를 판단하는 과정 및 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단함에 따라 연결 응답 메시지 및 사전 접속 요청을 전송하는 과정은 본 개시의 몇몇 실시예에 따른 보안 인증 프로세스에 포함될 수 있다.

[0074] 상술한 홈 가입자 서버(300)의 프로세서(310)가 보안 인증 프로세스를 수행하는 방법에 대한 설명은 도 2 및 도 7 내지 도 10을 참조하여 후술한다.

[0075] 본 개시의 몇몇 실시예에 따르면 이동성 관리 장비(400)는 통신망 가입자의 교환 장치 역할을 수행하는 MME(Mobility Management Entity)를 의미할 수 있다. 구체적으로, 이동성 관리 장비(400)는 통신망에 가입한 단말(여기서, 피제어 장치(200))을 인증(Authentication)하고, 핵심망에 접속하기 위한 NAS(Non Access Stratum) 신호를 처리하고, 단말과 패킷 데이터 망(PDN: Packet Data Network) 간 연결성(Connectivity)을 제공할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0076] 본 개시의 몇몇 실시예에 따르면, 이동성 관리 장비(400)와 피제어 장치(200)는 데이터를 상호 송수신 하여, 인증 절차를 수행할 수 있다.

[0077] 구체적으로, 이동성 관리 장비(400)는 홈 가입자 서버(300)로부터 인증 절차에 사용되는 사전 접속 요청 메시지를 수신할 수 있다. 한편, 피제어 장치(200)는 제어 장치(100)로부터 검증 절차 및 인증 절차에 사용되는 데이터를 수신할 수 있다. 그리고, 피제어 장치(200)는 제어 장치(100)로부터 수신된 데이터를 이용하여 검증 절차를 완료한 후에 인증 요청 메시지를 이동성 관리 장비(400)로 전송하여 인증 절차를 수행할 수 있다.

[0078] 상술한 피제어 장치(200)가 검증 절차를 수행하는 방법에 대한 설명은 도 5를 참조하여 후술한다. 그리고, 이동성 관리 장비(400)와 피제어 장치(200)가 인증 절차를 수행하는 방법에 대한 설명은 도 6을 참조하여 후술한다.

[0079] 본 개시의 몇몇 실시예들에 따른 네트워크(500)는 공중전화 교환망(PSTN: Public Switched Telephone Network), xDSL(x Digital Subscriber Line), RADSL(Rate Adaptive DSL), MDSL(Multi Rate DSL), VDSL(Very High Speed DSL), UADSL(Universal Asymmetric DSL), HDSL(High Bit Rate DSL) 및 근거리 통신망(LAN) 등과 같은 다양한 유선 통신 시스템들을 사용할 수 있다.

[0080] 또한, 여기서 제시되는 네트워크(500)는 CDMA(Code Division Multi Access), TDMA(Time Division Multi Access), FDMA(Frequency Division Multi Access), OFDMA(Orthogonal Frequency Division Multi Access), SC-FDMA(Single Carrier-FDMA) 및 다른 시스템들과 같은 다양한 무선 통신 시스템들을 사용할 수 있다.

[0081] 본 개시의 실시예들에 따른 네트워크(500)는 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있으며, 단거리 통신망(PAN: Personal Area Network), 근거리 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다. 또한, 상기 네트워크는 공지의 월드와이드웹(WWW: World Wide Web)일 수 있으며, 적외선(IrDA: Infrared Data Association) 또는 블루투스(Bluetooth)와 같이 단거리 통신에 이용되는 무선 전송 기술을 이용할 수도 있다.

[0082] 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.

[0083] 여기에 설명되는 다양한 실시예는 예를 들어, 소프트웨어, 하드웨어 또는 이들의 조합된 것을 이용하여 컴퓨터 또는 이와 유사한 장치로 읽을 수 있는 기록매체 및 저장매체 내에서 구현될 수 있다.

[0084] 하드웨어적인 구현에 의하면, 여기에 설명되는 실시예는 ASICs (application specific integrated circuits), DSPs (digital signal processors), DSPDs (digital signal processing devices), PLDs (programmable logic devices), FPGAs (field programmable gate arrays, 프로세서(processors), 제어기(controllers), 마이크로 컨트롤러(micro-controllers), 마이크로 프로세서(microprocessors), 기타 기능 수행을 위한 전기적인 유닛 중 적어도 하나를 이용하여 구현될 수 있다. 일부의 경우에 본 명세서에서 설명되는 실시예들이 제어 장치(100),

피제어 장치(200), 홈 가입자 서버(300) 및 이동성 관리 장비(400) 각각의 프로세서 자체로 구현될 수 있다

- [0085] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 제어 장치(100), 피제어 장치(200), 홈 가입자 서버(300) 및 이동성 관리 장비(400) 각각의 메모리에 저장되고, 제어 장치(100), 피제어 장치(200), 홈 가입자 서버(300) 및 이동성 관리 장비(400) 각각의 프로세서에 의해 실행될 수 있다.
- [0087] 도 2는 본 개시의 몇몇 실시예에 따른 보안 인증 기법의 일례를 설명하기 위한 흐름도이다.
- [0088] 도 2의 설명에서는 본 개시의 몇몇 실시예에 따른 보안 인증 시스템에 포함될 수 있는 제어 장치(100), 피제어 장치(200), 홈 가입자 서버(300) 및 이동성 관리 장비(400) 각각이 수행하는 보안 인증 기법의 흐름을 간략하게 설명한다.
- [0089] 도 2를 참조하면, 피제어 장치(200)는 IMSI 및 위치 정보를 제어 장치(100)로 전송할 수 있다(S1).
- [0090] 구체적으로, 피제어 장치(200)는 통신망 서비스에 가입하는 경우, 식별 파라미터가 할당된 SIM(Subscriber Identity Module)을 제공받을 수 있다. 그리고, 피제어 장치(200)는 통신망 최초 등록을 위해 제어 장치(100)로 SIM과 관련된 IMSI(즉, SIM에 할당된 IMSI) 및 피제어 장치(200)의 현재 위치에 대한 위치 정보를 전송할 수 있다.
- [0091] 좀더 구체적으로, 피제어 장치(200)는 유선 보안 채널을 이용하여, 제어 장치(100)로 IMSI 및 위치 정보를 전송할 수 있다. 예를 들어, 피제어 장치(200)는 USB 연결을 통해 IMSI 및 위치 정보를 제어 장치(100)로 전송할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0092] 따라서, 피제어 장치(200)는 무선 채널을 통해 전송할 때, 발생될 수 있는 식별 파라미터의 노출을 방지할 수 있다.
- [0093] 제어 장치(100)는 피제어 장치(200)로부터 IMSI 및 위치 정보를 수신한 경우, IMSI 및 위치 정보를 암호화할 수 있다.
- [0094] 구체적으로, 제어 장치(100)는 해시 함수를 이용하여 피제어 장치(200)의 IMSI에 대한 해시 값을 획득할 수 있다. 제어 장치(100)는 해시 값과 위치 정보를 제어 장치(100)의 개인키로 서명(암호화)하여, 제 1 서명 데이터를 생성할 수 있다. 제어 장치(100)는 제 1 서명 데이터를 홈 가입자 서버(300)의 공개키로 암호화한 제 1 암호 데이터를 생성할 수 있다.
- [0095] 여기서, 제어 장치(100)가 제어 장치(100)의 개인키를 이용하여, 제 1 서명 데이터를 생성하거나, 홈 가입자 서버(300)의 공개키를 이용하여, 제 1 암호 데이터를 생성할 때, 비대칭 키 알고리즘(Asymmetric Key Algorithm)을 이용할 수 있다. 여기서, 비대칭 키 알고리즘은, 암호화 및 복호화 시 각기 다른 두 가지 키(예컨대, 공개키(public key)와 개인키(private key))가 필요한 암호화 알고리즘이다. 즉, 공개키로 암호화된 데이터는 개인키로 복호화 할 수 있고, 개인키로 암호화(서명)된 데이터는 공개키로 복호화 할 수 있다.
- [0096] 한편, 제 1 암호 데이터를 생성한 제어 장치(100)는 제 1 암호 데이터를 포함하는 연결 요청 메시지를 홈 가입자 서버(300)로 전송할 수 있다(S2).
- [0097] 즉, 제어 장치(100)는 암호화된 데이터가 포함된 메시지를 홈 가입자 서버(300)로 전송함에 따라 피제어 장치(200)의 IMSI 및 위치 정보에 대한 보안성을 높일 수 있다.
- [0098] 홈 가입자 서버(300)는 제어 장치(100)로부터 연결 요청 메시지를 수신하기 전에, 피제어 장치의 SIM과 관련된 IMSI 및 인증키를 획득할 수 있다. 이 경우, 홈 가입자 서버(300)는 해시 함수를 이용하여, 상기 IMSI를 해싱한 제 2 해시 값을 산출하고, 제 2 해시 값 및 인증키를 메모리에 저장할 수 있다. 여기서, 인증키는 IMSI와 같이, 피제어 장치(200)가 통신망 서비스에 가입할 때 제공된 SIM에 할당된 키 값이다.
- [0099] 즉, 홈 가입자 서버(300)는 통신망 서비스를 제공하는 것과 관련된 서버로서 특정 단말이 통신망에 가입하는 경우, 상기 특정 단말에 제공되는 SIM과 관련된 정보를 저장하고 있을 수 있다.
- [0100] 한편, 홈 가입자 서버(300)는 제어 장치(100)로부터 연결 요청 메시지를 수신한 경우, 연결 요청 메시지에 포함

된 제 1 암호 데이터에서 제 1 해시 값 및 위치 정보를 추출할 수 있다.

- [0101] 구체적으로, 홈 가입자 서버(300)는 상술한 비대칭 키 알고리즘을 통해 제 1 암호화 데이터를 복호화 하여, 제 1 해시 값 및 위치 정보를 획득할 수 있다.
- [0102] 상술한 홈 가입자 서버(300)가 제 1 해시 값 및 위치 정보를 획득하는 방법에 대한 설명은 도 8을 참조하여 후술한다.
- [0103] 제 1 해시 값을 획득한 홈 가입자 서버(300)는 메모리에 사전 저장된 제 2 해시 값과 제 1 해시 값을 비교하여, 피제어 장치(200)의 통신망 가입 상태가 유효한지 여부를 판단할 수 있다(S3).
- [0104] 홈 가입자 서버(300)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우, 사전 접속 요청 메시지를 이동성 관리 장비(400)로 전송할 수 있다(S4). 구체적으로, 홈 가입자 서버(300)는 연결 요청 메시지에 포함된 피제어 장치(200)의 위치 정보에 기초하여, 피제어 장치(200)와 가장 가까운 위치에 존재하는 적어도 하나의 이동성 관리 장비(400)로 사전 접속 요청 메시지를 전송할 수 있다.
- [0105] 따라서, 홈 가입자 서버(300)가 피제어 장치(200)와 인접한 적어도 하나의 이동성 관리 장비(400)에게만 사전 접속 요청 메시지를 전송하여, 메시지 전송에 사용되는 트래픽 사용량 및 자원 사용량을 줄일 수 있다. 뿐만 아니라, 홈 가입자 서버(300)는 최소한의 이동성 관리 장비(400)에게만 사전 접속 요청 메시지를 전송하기 때문에 사전 접속 요청 메시지에 포함된 데이터의 유출 위험을 최소화할 수 있다.
- [0106] 한편, 홈 가입자 서버(300)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우, 연결 요청 메시지에 대응하는 연결 응답 메시지를 제어 장치(100)로 전송할 수 있다(S5).
- [0107] 여기서, 사전 접속 요청 메시지 및 연결 응답 메시지 각각은 피제어 장치(200)와 이동성 관리 장비(400) 간 인증 절차에 이용되는 데이터를 포함할 수 있다. 추가로, 연결 응답 메시지는 피제어 장치(200)가 홈 가입자 서버(300)에 대한 검증 절차를 수행하는데 이용되는 데이터를 포함할 수 있다.
- [0108] 상술한 검증 절차 및 인증 절차에 대한 설명은 도 5 및 도 6을 참조하여 후술한다.
- [0109] 이동성 관리 장비(400)는 사전 접속 요청 메시지를 홈 가입자 서버(300)로부터 수신한 경우, 사전 접속 요청 메시지를 메모리에 저장할 수 있다(S6).
- [0110] 한편, 제어 장치(100)는 연결 응답 메시지를 홈 가입자 서버(300)로부터 수신한 경우, 연결 응답 메시지에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 추출하여, 피제어 장치(200)로 전송할 수 있다(S7). 여기서, 제 1 인증 토큰은 상호 인증 알고리즘(구체적으로, EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm))에서 출력되는 토큰(또는, 값)으로, 상호 인증을 위한 토큰이다. 구체적으로, 상호 인증 알고리즘은 제 1 입력 데이터를 입력받는 경우, 제 1 인증 토큰을 출력할 수 있다. 그리고, 상기 상호 인증 알고리즘은 제 1 입력 데이터와 동일한 제 2 입력 데이터를 입력 받는 경우, 제 1 인증 토큰과 동일한 제 2 인증 토큰을 출력할 수 있다.
- [0111] 이러한 상호 인증 알고리즘의 특징을 이용하여, 서로 다른 단말(또는, 장치) 간 상호 인증을 수행할 수 있다. 예를 들어, 제 1 단말은 제 2 단말과 입력 데이터의 일부를 공유하고, 제 2 인증 토큰(제 2 단말이 제 2 데이터를 상호 인증 알고리즘에 입력하여 출력된 토큰)을 수신할 수 있다. 그리고, 제 1 단말은 제 1 입력 데이터를 상호 인증 알고리즘에 입력하여 출력된 제 1 인증 토큰을 획득할 수 있다. 그리고, 제 1 단말은 제 1 인증 토큰과 제 2 인증 토큰을 비교하여, 상기 제 1 인증 토큰과 상기 제 2 인증 토큰이 동일하다고 인식된 경우, 제 2 단말에 대한 인증(또는, 검증)을 수행할 수 있다. 한편, 제 2 단말은 제 1 단말로부터 상기 제 1 인증 토큰을 수신하고, 제 2 단말이 획득한 제 2 인증 토큰과 비교하여, 제 1 단말에 대한 인증을 수행할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0112] 상술한 제어 장치(100)가 연결 응답 메시지에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 추출하는 방법에 대한 설명은 도 4를 참조하여 후술한다.
- [0113] 피제어 장치(200)는 랜덤 값 및 제 1 인증 토큰을 이용하여, 홈 가입자 서버(300)를 검증할 수 있다. 이하, 피제어 장치(200)가 랜덤 값 및 제 1 인증 토큰을 이용하여, 홈 가입자 서버(300)를 검증하는 방법에 대한 설명은 도 5를 참조하여 후술한다.
- [0114] 피제어 장치(200)는 홈 가입자 서버(300)에 대한 검증이 완료된 경우, 제 1 TMSI를 포함하는 인증 요청 메시지를 이동성 관리 장비(400)로 전송할 수 있다(S8).

- [0115] 이 경우, 이동성 관리 장비(400)는 메모리에 사전 저장된 사전 접속 요청 메시지와 인증 요청 메시지를 이용하여, 피제어 장치(200)를 인증할 수 있다(S9). 이하, 이동성 관리 장비(400)가 사전 접속 요청 메시지와 인증 요청 메시지를 이용하여, 피제어 장치(200)를 인증하는 방법에 대한 설명은 도 6을 참조하여 후술한다.
- [0117] 도 3은 본 개시의 몇몇 실시예에 따른 제어 장치가 보안 인증을 수행하는 방법의 일례를 설명하기 위한 흐름도이다. 도 4는 본 개시의 몇몇 실시예에 따른 제어 장치가 보안 인증을 수행하는 방법의 구체적인 일례를 설명하기 위한 흐름도이다.
- [0118] 도 3을 참조하면, 제어 장치(100)의 프로세서(110)는 피제어 장치(200)로부터 피제어 장치(200)의 IMSI와 관련된 IMSI 및 위치 정보를 획득할 수 있다(S110).
- [0119] 구체적으로, 프로세서(110)는 유선 보안 채널(wired secure channel)을 이용하여, 피제어 장치(200)로부터 IMSI 및 위치 정보를 수신할 수 있다. 예를 들어, 프로세서(110)는 통신부(120)를 통해 USB 채널을 이용하여, 피제어 장치(200)로부터 IMSI 및 위치 정보를 수신할 수 있다. 다만, 이에 한정되는 것은 아니다.
- [0120] 즉, 제어 장치(100) 및 피제어 장치(200) 각각은 유선 보안 채널을 이용하여 IMSI 및 위치 정보를 송수신하기 때문에, IMSI 및 위치 정보의 유출을 방지하여, IMSI 및 위치 정보의 보안성을 높일 수 있다.
- [0121] 제어 장치(100)의 프로세서(110)는 해시 함수를 이용하여, IMSI를 해싱한 해시 값을 산출할 수 있다(S120). 그리고, 제어 장치(100)의 프로세서(110)는 비대칭 키 알고리즘을 이용하여, 제어 장치(100)의 개인키로 해시 값 및 위치 정보를 암호화한 제 1 서명 데이터를 획득할 수 있다(S130). 또한, 프로세서(110)는 비대칭 키 알고리즘을 이용하여, 제 1 서명 데이터를 홈 가입자 서버(300)의 공개키로 암호화한 제 1 암호 데이터를 생성할 수 있다(S140).
- [0122] 제어 장치(100)의 프로세서(110)는 제 1 암호 데이터를 포함하는 연결 요청 메시지를 홈 가입자 서버(300)로 전송할 수 있다(S150).
- [0123] 즉, 제어 장치(100)는 홈 가입자 서버(300)로 전송해야 하는 피제어 장치(200)의 IMSI 및 위치 정보를 암호화한 후 암호화된 데이터(즉, 제 1 암호 데이터)를 포함하는 연결 요청 메시지를 전송하기 때문에, IMSI 및 위치 정보의 보안성을 향상시킬 수 있다.
- [0124] 추가로, 암호화된 데이터가 악의적인 사용자에게 의해 탈취(즉, 유출 및 복호화) 되더라도 피제어 장치(200)의 IMSI를 해싱한 해시 값만 유출되기 때문에, 피제어 장치(200)의 IMSI에 대한 유출을 방지할 수 있다.
- [0125] 한편, 제어 장치(100)의 프로세서(110)는 홈 가입자 서버(300)에서 연결 요청 메시지에 대한 연결 수락이 결정된 경우, 홈 가입자 서버(300)로부터 제 2 암호 데이터를 포함하는 연결 응답 메시지를 수신할 수 있다. 이 경우, 제어 장치(100)의 프로세서(110)는 제 2 암호 데이터에서 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 추출할 수 있다(S170). 여기서, 제 2 암호 데이터는 비대칭 키 알고리즘을 이용하여 암호화된 데이터일 수 있다. 즉, 제어 장치(100)의 프로세서(110)는 비대칭 키 알고리즘을 이용하여 제 2 암호 데이터를 복호화 할 수 있다.
- [0126] 구체적으로, 도 4를 참조하면, 제어 장치(100)의 프로세서(110)는 비대칭 키 알고리즘을 이용하여, 제 2 암호 데이터를 제어 장치(100)의 개인키로 복호화 하여, 제 2 서명 데이터를 획득할 수 있다(S171). 그리고, 프로세서(110)는 비대칭 키 알고리즘을 이용하여 제 2 서명 데이터를 홈 가입자 서버(300)의 공개키로 복호화 하여, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 획득할 수 있다(S172).
- [0127] 즉, 제 2 암호 데이터는 홈 가입자 서버(300)가 비대칭 키 알고리즘을 이용하여, 홈 가입자 서버(300)의 개인키로 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 암호화한 제 2 서명 데이터를 생성하고, 비대칭 키 알고리즘을 이용하여, 제 2 서명 데이터를 제어 장치(100)의 공개키로 암호화한 데이터일 수 있다.
- [0128] 따라서, 홈 가입자 서버(300)는 제어 장치(100)로 전송해야 하는 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 암호화한 후 암호화된 데이터(즉, 제 2 암호 데이터)를 포함하는 연결 응답 메시지를 전송하기 때문에, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI의 보안성을 향상시킬 수 있다.
- [0129] 한편, 상술한 제 1 인증 토큰은 홈 가입자 서버(300)가 EPS-AKA 알고리즘(Evolved Packet System-Authentication and Key Agreement algorithm)에 피제어 장치(200)의 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여, 상기 홈 가입자 서버(300)가 획득하는 토큰을 의미한다. 여기서, 제 1 입력 데이터는 상술한 인증키 및 랜덤 값 외에 다른 값을 더 포함할 수 있다. 예를 들어, 제 1 입력 데이터는 인증키

및 랜덤 값 외에 홈 가입자 서버(300)가 생성하는 SQN(Sequence Number) 및 이동성 관리 장비(400)로부터 수신된 SN ID(Serving Network Identity)를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0130] 또한, 제 1 인증 토큰은 피제어 장치(200)에서 홈 가입자 서버(300)가 제 1 인증 토큰을 전송한 것이 맞는지 여부를 판단하는 검증 절차에 사용될 수 있다. 이하, 검증 절차에 대한 설명은 도 5를 참조하여 후술한다.

[0131] 다시 도 3을 참조하면, 제어 장치(100)는 유선 보안 채널을 이용하여, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 피제어 장치(200)로 전송할 수 있다(S180). 예를 들어, 프로세서(110)는 통신부(120)를 통해 USB 채널을 이용하여, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 피제어 장치(200)로 전송할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0132] 즉, 제어 장치(100) 및 피제어 장치(200) 각각은 유선 보안 채널을 이용하여 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 송수신하기 때문에, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI의 유출을 방지하여, 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI의 보안성을 높일 수 있다.

[0134] 도 5는 본 개시의 몇몇 실시예에 따른 검증 절차를 설명하기 위한 흐름도이다.

[0135] 도 5를 참조하면, 피제어 장치(200)는 제어 장치(100)로부터 랜덤 값, 제 1 인증 토큰 및 제 1 TMSI를 수신한 경우, EPS-AKA 알고리즘에 피제어 장치(200)의 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 2 입력 데이터를 입력하여 생성된 제 2 인증 토큰을 획득할 수 있다(S210). 여기서, 제 2 입력 데이터는 상술한 인증키 및 랜덤 값 외에 다른 값을 더 포함할 수 있다. 예를 들어, 제 2 입력 데이터는 인증키, 랜덤 값, SQN 및 SN ID를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0136] 추가로, EPS-AKA 알고리즘은 제 2 입력 데이터가 입력됨에 따라, RES(response) 값 및 비밀키를 더 생성할 수 있다. 즉, 피제어 장치(200)는 제 2 입력 데이터를 EPS-AKA 알고리즘에 입력하여, 제 2 인증 토큰, RES 값 및 비밀키를 획득할 수 있다.

[0137] 한편, 피제어 장치(200)는 제어 장치(100)로부터 수신된 제 1 TMSI와 제 2 입력 데이터를 EPS-AKA 알고리즘에 입력하여 획득된 RES 값 및 비밀키를 상기 피제어 장치(200)의 인증 절차에 사용할 수 있다. 여기서, RES 값은 제 2 입력 데이터를 EPS-AKA 알고리즘에 입력하였을 때 출력되는 출력 값(즉, 응답 값)을 의미할 수 있다. 그리고, 비밀키는 인증 절차에서 사용되는 메시지를 암호화 및 복호화 하는데 이용되는 키를 의미할 수 있다. 이하, 인증 절차에 대한 설명은 도 6을 참조하여 후술한다.

[0138] 피제어 장치(200)는 제 1 인증 토큰과 제 2 인증 토큰이 동일한지 여부에 따라 제 1 인증 토큰이 홈 가입자 서버(300)가 전송한 것이 맞는지 여부를 판단할 수 있다(S220).

[0139] 구체적으로, 피제어 장치(200)는 제 1 인증 토큰과 제 2 인증 토큰이 동일하다고 인식한 경우, 제 1 인증 토큰이 홈 가입자 서버(300)가 전송한 것이 맞다고 판단할 수 있다. 즉, 제 1 인증 토큰과 제 2 인증 토큰이 동일한 경우, 피제어 장치(200)가 홈 가입자 서버(300)에 대한 검증을 완료할 수 있다.

[0140] 그리고, 피제어 장치(200)는 홈 가입자 서버(300)에 대한 검증이 완료됨에 따라 이동성 관리 장비(400)와 인증 절차를 수행할 수 있다.

[0141] 한편, 피제어 장치(200)는 제 1 인증 토큰과 제 2 인증 토큰이 동일하지 않다고 인식한 경우, 제 1 인증 토큰이 홈 가입자 서버(300)가 전송한 것이 아니라고 판단할 수 있다. 이 경우, 피제어 장치(200)는 상기 피제어 장치(200)를 통신망에 최초 등록하기 위한 보안 인증 프로세스를 중단할 수 있다.

[0142] 따라서, 피제어 장치(200)는 홈 가입자 서버(300)에 대한 검증이 완료되었을 경우에만 다음 인증 프로세스를 수행하여, 본 개시의 보안 인증 프로세스의 신뢰성을 향상시킬 수 있다.

[0144] 도 6은 본 개시의 몇몇 실시예에 따른 인증 절차를 설명하기 위한 흐름도이다.

[0145] 본 개시의 몇몇 실시예에 따르면, 제어 장치(100)는 피제어 장치(200)를 통신망에 최초 등록하기 위한 연결 요청 메시지를 홈 가입자 서버(300)로 전송할 수 있다. 이 경우, 홈 가입자 서버(300)는 피제어 장치(200)의 통신망 가입 상태가 유효한지 판단할 수 있다.

[0146] 그리고, 홈 가입자 서버(300)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우, 이동성 관리

장비(400)로 사전 접속 요청 메시지를 전송할 수 있다. 여기서, 사전 접속 요청 메시지는 XRES(Expected Response) 값 및 제 2 TMSI를 포함할 수 있다. 상기 XRES 값은 제 2 입력 데이터를 EPS-AKA 알고리즘에 입력하였을 때 출력될 것으로 예상되는 예상 출력 값(즉, 예상 응답 값)을 의미할 수 있다.

[0147] 한편, 이동성 관리 장비(400)는 홈 가입자 서버(300)로부터 사전 접속 요청 메시지를 수신한 경우, 사전 접속 요청 메시지에 포함된 XRES 값 및 제 2 TMSI를 메모리에 저장할 수 있다. 여기서, 이동성 관리 장비(400)의 메모리에 저장된 XRES 값 및 제 2 TMSI는 이동성 관리 장비(400)가 피제어 장치(200)에 대한 인증을 수행할 때 이용될 수 있다.

[0148] 한편, 도 6을 참조하면, 피제어 장치(200)는 홈 가입자 서버(300)에 대한 검증이 완료됨에 따라, 비밀키를 이용하여 RES 값 및 제 1 TMSI를 암호화한 인증 요청 메시지를 생성할 수 있다(S310). 그리고, 피제어 장치(200)는 인증 요청 메시지를 이동성 관리 장비(400)로 전송할 수 있다(S320).

[0149] 한편, 이동성 관리 장비(400)는 인증 요청 메시지를 수신한 경우, 인증 요청 메시지에서 RES 값 및 제 1 TMSI를 추출하기 위해 이동성 관리 장비(400)에 사전 저장된 비밀키를 이용하여 인증 요청 메시지를 복호화할 수 있다(S330).

[0150] 그리고, 이동성 관리 장비(400)는 인증 요청 메시지에서 추출된 RES 값 및 제 1 TMSI와 이동성 관리 장비(400)의 메모리에 사전 저장된 XRES 값 및 제 2 TMSI를 비교한 결과에 기초하여, 피제어 장치(200)를 인증할 수 있다(S340).

[0151] 구체적으로, 이동성 관리 장비(400)는 제 1 TMSI와 제 2 TMSI가 동일하다고 인식하고, RES 값과 XRES 값이 동일하다고 인식한 경우, 피제어 장치(200)에 대한 인증을 완료할 수 있다.

[0152] 즉, 홈 가입자 서버(300)가 이동성 관리 장비(400)로 전송한 예상 응답 값(XRES)과 피제어 장치(200)가 생성한 실제 응답 값(RES)이 동일한 경우, 피제어 장치(200)에 대한 인증이 완료될 수 있다.

[0154] 도 7은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 일례를 설명하기 위한 흐름도이다. 도 8은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 구체적인 일례를 설명하기 위한 흐름도이다. 도 9는 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 다른 구체적인 일례를 설명하기 위한 흐름도이다.

[0155] 도 7을 참조하면, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)의 SIM과 관련된 IMSI 및 인증키를 획득할 수 있다(S410).

[0156] 구체적으로, 홈 가입자 서버(300)는 피제어 장치(200)를 통신망 서비스 가입시킬 때 피제어 장치(200)의 사용자(또는 관리자)로부터 입력 받은 정보를 획득할 수 있다. 또한, 홈 가입자 서버(300)는 통신망 서비스에 가입된 피제어 장치(200)로 제공한 SIM에 대한 정보를 획득할 수 있다. 여기서, SIM은 식별 파라미터(즉, IMSI 및 인증키)가 할당(또는, 저장)되어 있을 수 있다.

[0157] 홈 가입자 서버(300)의 프로세서(310)는 해시 함수를 이용하여, IMSI를 해싱한 제 2 해시 값을 산출할 수 있다. 그리고, 프로세서(310)는 제 2 해시 값 및 인증키를 메모리(330)에 저장할 수 있다(S420).

[0158] 한편, 홈 가입자 서버(300)의 프로세서(310)는 통신부(320)를 통해 피제어 장치(200)를 제어하는 제어 장치(100)로부터 비대칭 키 알고리즘에 기초하여 암호화된 제 1 암호 데이터를 포함하는 연결 요청 메시지를 수신할 수 있다(S430). 이 경우, 홈 가입자 서버(300)의 프로세서(310)는 제 1 암호 데이터에서 제 1 해시 값 및 피제어 장치(200)의 위치 정보를 추출할 수 있다(S440).

[0159] 구체적으로, 도 8을 참조하면, 홈 가입자 서버(300)의 프로세서(310)는 비대칭 키 알고리즘을 이용하여, 제 1 암호 데이터를 홈 가입자 서버(300)의 개인키로 복호화 하여, 제 1 서명 데이터를 획득할 수 있다(S441). 그리고, 프로세서(310)는 비대칭 키 알고리즘을 이용하여, 제 1 서명 데이터를 제어 장치(100)의 공개키로 복호화 하여, 제 1 해시 값 및 위치 정보를 획득할 수 있다(S442).

[0160] 즉, 제 1 암호 데이터는 제어 장치(100)가 비대칭 키 알고리즘을 이용하여, 제어 장치(100)의 개인키로 제 1 해시 값 및 피제어 장치(200)의 위치 정보를 암호화한 제 1 서명 데이터를 생성하고, 비대칭 키 알고리즘을 이용하여, 제 1 서명 데이터를 홈 가입자 서버(300)의 공개키로 암호화한 데이터일 수 있다.

- [0161] 따라서, 제어 장치(100)는 홈 가입자 서버(300)로 전송해야 하는 피제어 장치(200)의 IMSI 및 위치 정보를 암호화한 후 암호화된 데이터(즉, 제 1 암호 데이터)를 포함하는 연결 요청 메시지를 전송하기 때문에, IMSI 및 위치 정보의 보안성을 향상시킬 수 있다.
- [0162] 다시 도 7을 참조하면, 홈 가입자 서버(300)의 프로세서(310)는 제 1 해시 값과 메모리에 사전 저장된 제 2 해시 값을 비교하여, 피제어 장치(200)의 통신망 가입 상태가 유효한지 여부를 판단할 수 있다(S450).
- [0163] 구체적으로, 홈 가입자 서버(300)의 프로세서(310)는 제 1 해시 값과 제 2 해시 값이 동일하다고 인식한 경우, 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단할 수 있다.
- [0164] 한편, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치의 통신망 가입 상태가 유효하다고 판단한 경우, 피제어 장치(200)의 위치 정보에 기초하여, 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비(400)를 결정할 수 있다(S460).
- [0165] 구체적으로, 도 9를 참조하면, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)의 위치 정보에 기초하여, 피제어 장치(200)의 위치에서 기 설정된 반경 이내에 위치하는 적어도 하나의 이동성 관리 장비(400)를 인식할 수 있다(S461). 그리고, 프로세서(310)는 기 설정된 반경 이내에 위치하는 적어도 하나의 이동성 관리 장비(400)를 사전 접속 요청 메시지를 수신 받을 이동성 관리 장비로 결정할 수 있다(S462).
- [0166] 즉, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)와 인접한 적어도 하나의 이동성 관리 장비(400)에게만 사전 접속 요청 메시지를 전송할 수 있다. 이 경우, 프로세서(310)는 메시지 전송에 사용되는 트래픽 사용량 및 자원 사용량을 줄일 수 있다. 뿐만 아니라, 프로세서(310)는 최소한의 이동성 관리 장비(400)에게만 사전 접속 요청 메시지를 전송하기 때문에 사전 접속 요청 메시지에 포함된 데이터의 유출 위험을 최소화할 수 있다.
- [0168] 도 10은 본 개시의 몇몇 실시예에 따른 홈 가입자 서버가 보안 인증을 수행하는 방법의 추가적인 일례를 설명하기 위한 흐름도이다.
- [0169] 본 개시의 몇몇 실시예에 따르면, 홈 가입자 서버(300)의 프로세서(310)는 통신부(320)를 통해 제어 장치(100)로부터 연결 요청 신호를 수신할 수 있다. 이 경우, 프로세서(310)는 연결 요청 신호에 포함된 제 1 암호 데이터를 복호화 하여, 제 1 해시 값 및 피제어 장치(200)의 위치 정보를 획득할 수 있다.
- [0170] 그리고, 도 10을 참조하면, 홈 가입자 서버(300)의 프로세서(310)는 제 1 해시 값과 홈 가입자 서버(300)의 메모리(330)에 사전 저장된 제 2 해시 값을 비교하여, 피제어 장치(200)의 통신망 가입 상태가 유효한지 여부를 판단할 수 있다(S510).
- [0171] 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)의 통신망 가입 상태가 유효하지 않다고 판단한 경우(S510, No), 통신망 가입 상태가 유효한 피제어 장치(200)와 관련된 연결 요청 신호가 수신될 때까지 대기할 수 있다.
- [0172] 한편, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단한 경우(S510, Yes), 연결 요청 메시지에 대응하는 연결 응답 메시지를 제어 장치로 전송할 수 있다(S520).
- [0173] 구체적으로, 홈 가입자 서버(300)의 프로세서(310)는 EPS-AKA 알고리즘에 피제어 장치(200)의 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 제 1 인증 토큰을 획득할 수 있다. 또한, 프로세서(310)는 IMSI에 대응하는 TMSI를 생성할 수 있다.
- [0174] 홈 가입자 서버(300)의 프로세서(310)는 비대칭 키 알고리즘을 이용하여, 랜덤 값, TMSI 및 제 1 인증 토큰을 홈 가입자 서버(300)의 개인키로 암호화한 제 2 서명 데이터를 생성할 수 있다. 프로세서(310)는 비대칭 키 알고리즘을 이용하여, 제어 장치(100)의 공개키로 암호화한 제 2 암호 데이터를 생성할 수 있다. 그리고, 프로세서(310)는 랜덤 값, TMSI 및 제 1 인증 토큰을 암호화한 제 2 암호 데이터를 포함하는 연결 응답 메시지를 제어 장치(100)로 전송하도록 통신부(320)를 제어할 수 있다.
- [0175] 한편, 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)의 통신망 가입 상태가 유효하다고 판단함에 따라, 피제어 장치(200)와 이동성 관리 장비(400) 간 인증을 수행하도록 이동성 관리 장비(400)로 사전 접속 요청 메시지를 전송할 수 있다(S530).

- [0176] 구체적으로, 홈 가입자 서버(300)의 프로세서(310)는 EPS-AKA 알고리즘에 피제어 장치의 SIM과 관련된 인증키 및 랜덤 값을 포함하는 제 1 입력 데이터를 입력하여 XRES 값 및 비밀키를 획득할 수 있다. 또한, 프로세서(310)는 IMSI에 대응하는 TMSI를 생성할 수 있다. 상기 XRES 값은 제 2 입력 데이터를 EPS-AKA 알고리즘에 입력하였을 때 출력될 것으로 예상되는 예상 출력 값(즉, 예상 응답 값)을 의미할 수 있다.
- [0177] 홈 가입자 서버(300)의 프로세서(310)는 피제어 장치(200)와 이동성 관리 장비(400) 간 인증을 수행하는데 사용되는 XRES 값, TMSI 및 비밀키를 포함하는 사전 접속 요청 메시지를 생성할 수 있다. 그리고, 프로세서(310)는 XRES 값, TMSI 및 비밀키를 포함하는 사전 접속 요청 메시지를 이동성 관리 장비(400)로 전송하도록 통신부(320)를 제어할 수 있다.
- [0179] 도 11은 본 개시 내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도를 도시한다.
- [0180] 본 개시가 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 기술되었지만, 당업자라면 본 개시가 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있다는 것을 잘 알 것이다.
- [0181] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시저, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.
- [0182] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘 다에 위치할 수 있다.
- [0183] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.
- [0184] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.
- [0185] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.
- [0186] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.
- [0187] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리

(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0188] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 새시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘다를 포함한다.

[0189] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 zip 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0190] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부가 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0191] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0192] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0193] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원격 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0194] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(114

2)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0195] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순히 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0196] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0197] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

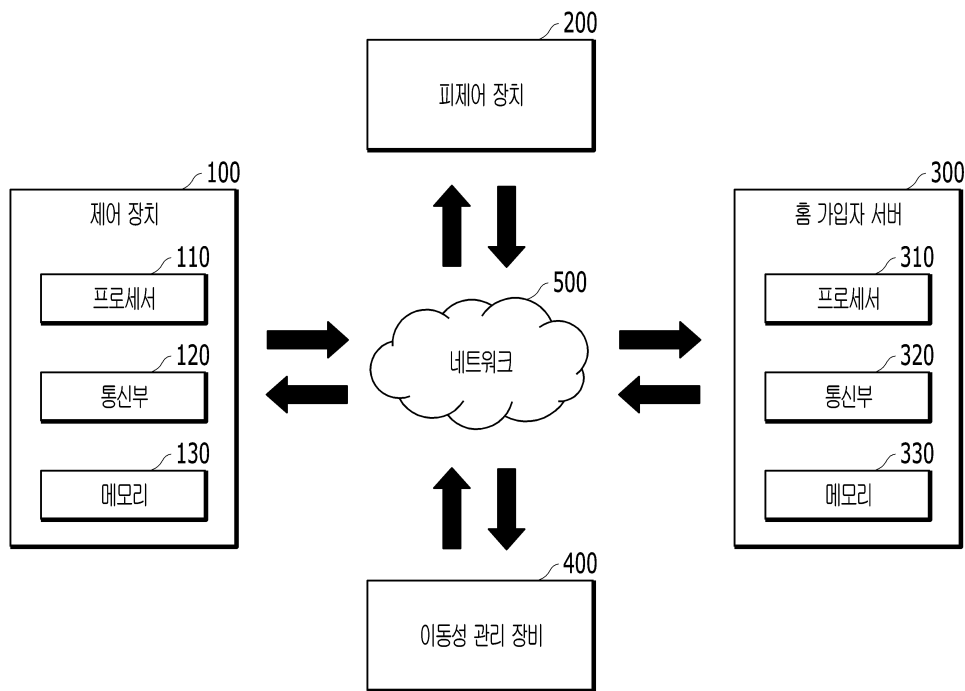
[0198] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조물품(article)으로 구현될 수 있다. 용어 "제조물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트림, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

[0199] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 설계 우선순위들에 기반하여, 본 개시의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.

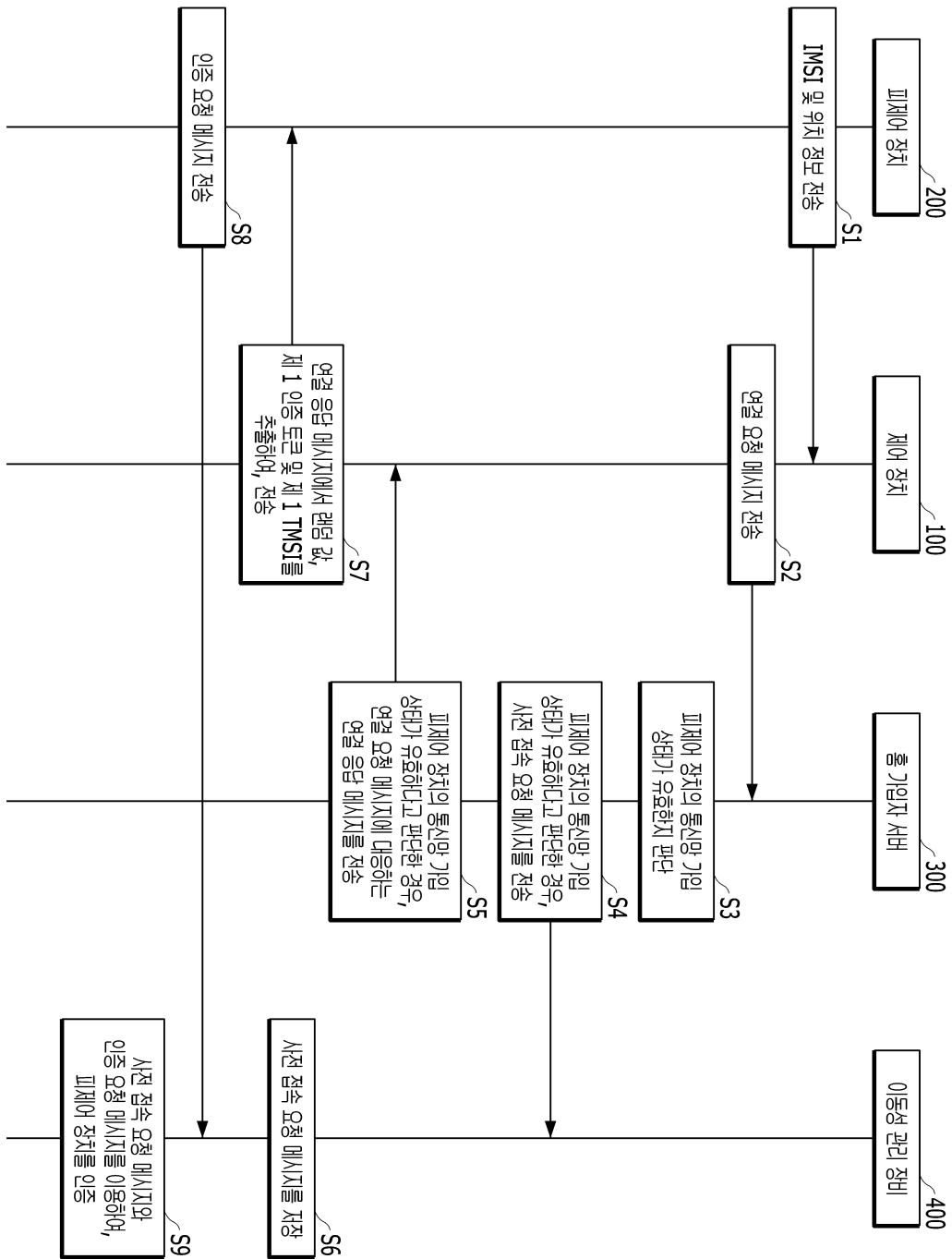
[0200] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의 범위에서 해석되어야 할 것이다.

도면

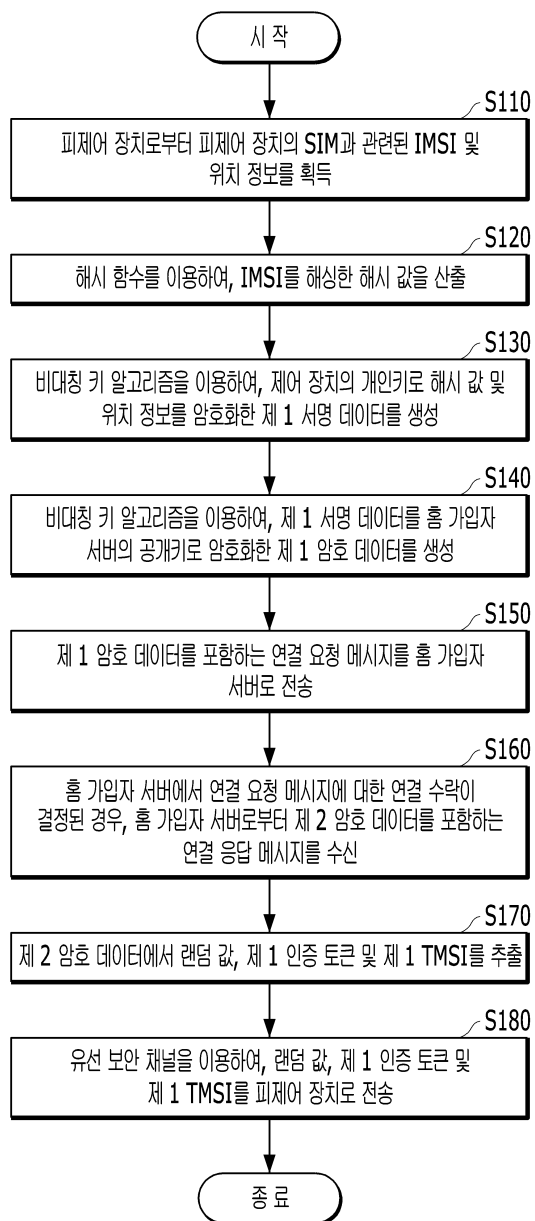
도면1



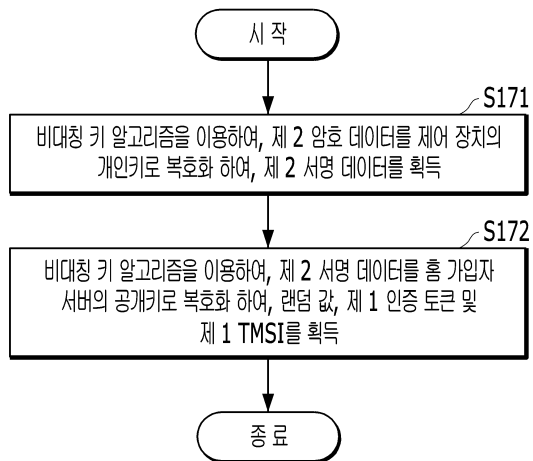
도면2



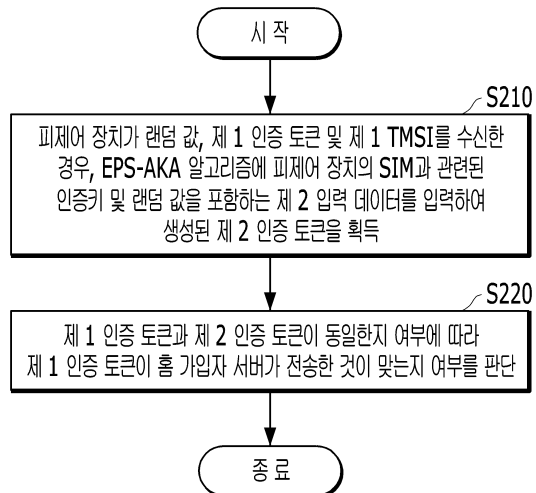
도면3



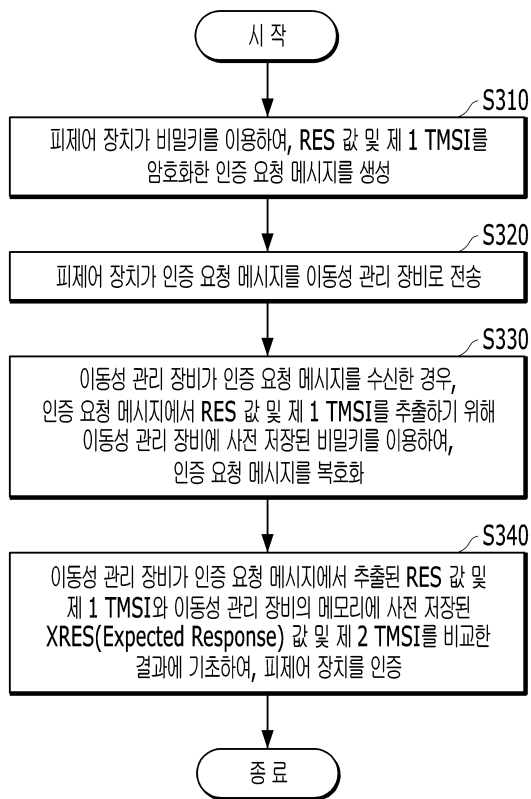
도면4



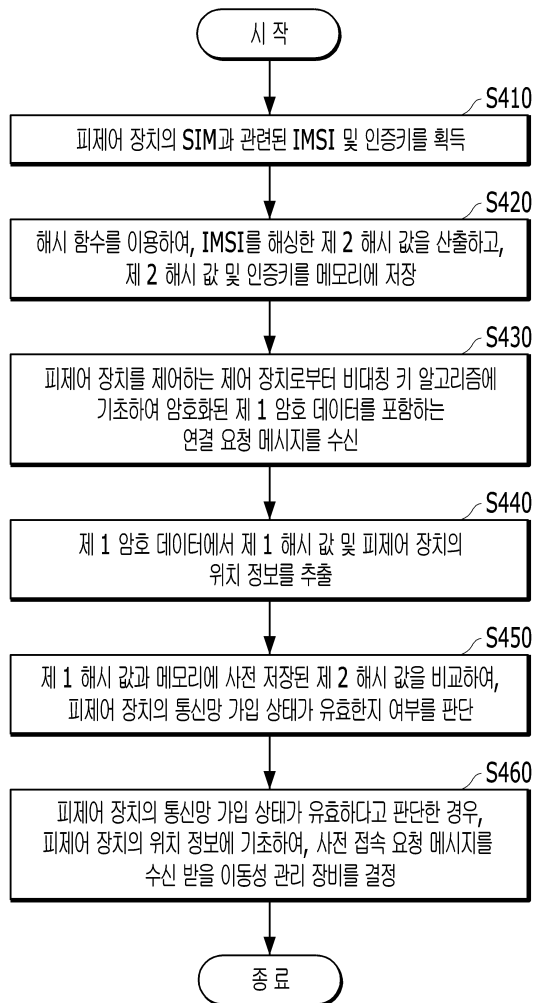
도면5



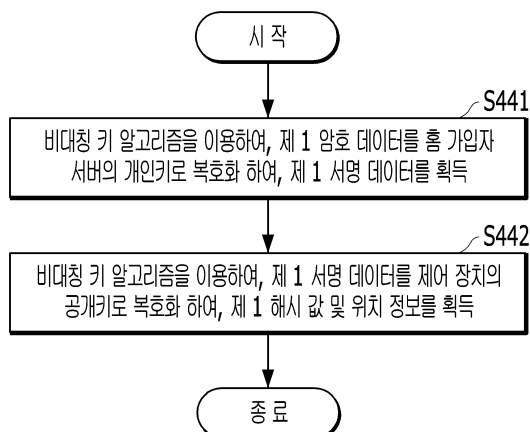
도면6



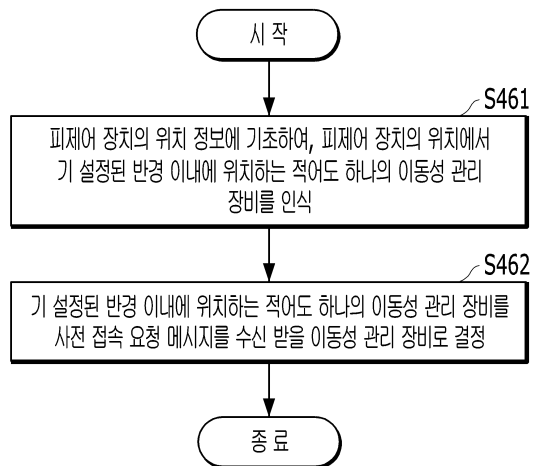
도면7



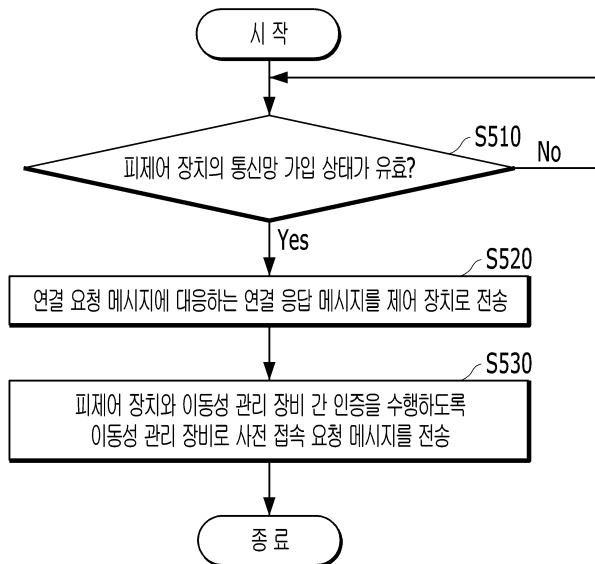
도면8



도면9



도면10



도면11

