(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년11월26일
(11) 등록번호 10-0996983
(24) 등록일자 2010년11월22일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2005-7005696
(22) 출원일자(국제출원일자) 2003년09월30일
심사청구일자 2008년07월18일
(85) 번역문제출일자 2005년04월01일
(65) 공개번호 10-2005-0062586
(43) 공개일자 2005년06월23일
(86) 국제출원번호 PCT/IB2003/004298
(87) 국제공개번호 WO 2004/032415
국제공개일자 2004년04월15일
(30) 우선권주장
10/659,774 2003년09월10일 미국(US)
60/416,481 2002년10월03일 미국(US)
(56) 선행기술조사문헌
J. Arkko et al., "EAP AKA Authentication", Internet Draft
draft-arkko-pppext-eap-aka-04.txt, 2002.06.*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
노키아 코포레이션
핀랜드핀-02150 에스푸 카일알라덴티에 4
(72) 발명자
하베리넨 헨리
핀랜드 핀-33720 탐페레 아르크키테흐딘카투 15 에이 3
아흐마바아라 칼레
핀랜드 핀-00530 헬싱키 하카니에멘란타 18 디 62
(74) 대리인
리앤목특허법인

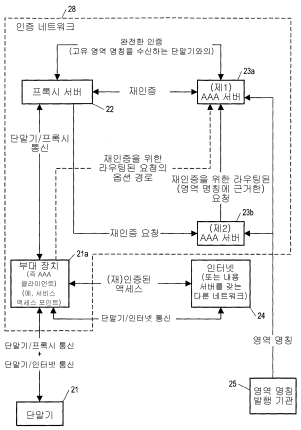
전체 청구항 수 : 총 23 항 심사관 : 정은선

(54) 셀룰러 통신 시스템에서의 재인증 허용 방법 및 장치

(57) 요 약

단말기(21) 및 서버(24)간의 정보 교환을 포함하는 통신 세션의 -- 제1 인증 서버(23a)에 의한 제1 완전한 인증 이후에 -- 재인증(reauthentication)에 사용하기 위한 방법(및 대응하는 장치)이 제공된다. 상기 방법은 상기 제1 인증 서버(23a) 및 다른 인증 서버들(23b) 각각에 각자의 고유 영역(realm) 명칭이 할당되는 단계(11); 및 상기 단말기 및 상기 제1 인증 서버(23a) 간의 인증 동안, 상기 제1 인증 서버(23a)가 상기 제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 상기 단말기(21)에 전송하는 단계(13)를 포함한다. 그 후에, 재전송 동안, 완전한 인증을 수행한 것과 동일한 인증 서버(23a)에 의해 -- 즉 제1 인증 서버(23a)에 의해 -- 재인증이 수행될 수 있도록, 재인증 아이덴티티가 재인증을 위한 요청에 포함된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

제1 인증 서버 및 다른 인증 서버들이 각각 대응하는 고유 영역 명칭들(unique realm names)을 수신하는 단계;

상기 제1 인증 서버가 단말기의 인증 요청을 수신하는 단계; 그리고

상기 단말기 및 상기 제1 인증 서버 간의 인증 동안, 상기 제1 인증 서버는 상기 제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 상기 단말기에 전송하는 단계를 포함하는, 셀룰러 통신 시스템에서의 재인증 허용 방법.

청구항 2

제1항에 있어서,

인증 장치가 상기 단말기에 의해 전송된 재인증 요청을 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 이용하여 수신하는 단계; 및

상기 인증 장치는 상기 고유 영역 명칭을 상기 요청에 포함된 재인증 아이덴티티로부터 결정하는 단계를 더 포함하는 것을 특징으로 하는, 셀룰러 통신 시스템에서의 재인증 허용 방법.

청구항 3

제2항에 있어서,

상기 인증 장치는 상기 재인증 아이덴티티의 부분으로서 포함된 고유 영역 명칭에 의해 표시된 상기 인증 서버에 상기 요청을 전송하는 단계; 및

상기 단말기 및 상기 고유 영역 명칭에 의해 표시된 상기 인증 서버는 재인증을 수행하는 단계를 더 포함하는 것을 특징으로 하는, 셀룰러 통신 시스템에서의 재인증 허용 방법.

청구항 4

인증을 수행하기 위한 수단; 및

인증을 요청하는 단말기에 인증 서버를 고유하게 식별하는 고유 영역 명칭을 포함하는 재인증 아이덴티티를 전송하는 수단을 포함하는 것을 특징으로 하는, 인증 서버.

청구항 5

제4항에 있어서,

재인증을 위해 단말기에 의한 상기 재인증 아이덴티티를 포함하는 요청을 수신하고, 상기 요청에 포함된 고유 영역 명칭을 상기 재인증 아이덴티티로부터 결정하는 수단을 더 포함하는 것을 특징으로 하는, 인증 서버.

청구항 6

제5항에 있어서,

만일 상기 고유 영역 명칭이 다른 인증 서버를 표시하면 상기 다른 인증 서버에 상기 요청을 전송하는 수단을 더 포함하는 것을 특징으로 하는, 인증 서버.

청구항 7

인증 서버의 컴퓨터 프로세서에 의해 실행하기 위한 컴퓨터 프로그램 코드가 수록된 컴퓨터 독출가능 저장 매체에 있어서,

상기 컴퓨터 프로그램 코드는 인증을 요청하는 단말기에 상기 인증 서버를 고유하게 식별하는 고유 영역 명칭을 포함하는 재인증 아이덴티티를 전송하기 위한 명령어들을 포함하는, 컴퓨터 독출가능 저장 매체.

청구항 8

제7항에 있어서, 상기 컴퓨터 프로그램 코드는

재인증을 위해 단말기에 의한 상기 재인증 아이덴티티를 포함하는 요청을 수신하고 상기 요청에 포함된 고유 영역 명칭을 상기 재인증 아이덴티티로부터 결정하기 위한 명령어들을 더 포함하는 것을 특징으로 하는, 컴퓨터 독출가능 저장 매체.

청구항 9

제7항에 있어서, 상기 컴퓨터 프로그램 코드는

만일 상기 고유 영역 명칭이 다른 인증 서버를 표시하면 상기 다른 인증 서버에 상기 요청을 전송하기 위한 명령어들을 더 포함하는 것을 특징으로 하는, 컴퓨터 독출가능 저장 매체.

청구항 10

복수의 단말기들, 복수의 인증 서버들, 및 적어도 하나의 내용 서버를 포함하는, 재인증을 허용하는 셀룰러 통신 시스템으로서, 상기 단말기들은 하나 또는 다른 하나의 인증 서버를 통한 인증 및 임시적인 재인증 후에 상기 내용 서버로부터 내용을 요청하도록 동작하며, 적어도 2개의 상기 인증 서버들은 제4항에 기재된 인증 서버들인 것을 특징으로 하는, 재인증을 허용하는 셀룰러 통신 시스템.

청구항 11

복수의 단말기들, 복수의 인증 서버들, 및 적어도 하나의 내용 서버를 포함하는, 재인증을 허용하는 셀룰러 통신 시스템으로서, 상기 단말기들은 하나 또는 다른 하나의 인증 서버를 통한 인증 및 임시적인 재인증 후에 상기 내용 서버로부터 내용을 요청하도록 동작하며, 적어도 2개의 상기 인증 서버들은 제5항에 기재된 인증 서버들인 것을 특징으로 하는, 재인증을 허용하는 셀룰러 통신 시스템.

청구항 12

복수의 단말기들, 복수의 인증 서버들, 및 적어도 하나의 내용 서버를 포함하는, 재인증을 허용하는 셀룰러 통신 시스템으로서, 상기 단말기들은 하나 또는 다른 하나의 인증 서버를 통한 인증 및 임시적인 재인증 후에 상기 내용 서버로부터 내용을 요청하도록 동작하며, 적어도 2개의 상기 인증 서버들은 제6항에 기재된 인증 서버들인 것을 특징으로 하는, 재인증을 허용하는 셀룰러 통신 시스템.

청구항 13

단말기 및 내용 서버 간의 통신 세션의 재인증을 요청하는 수단;

제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 상기 제1 인증 서버로부터 수신하는 수단; 및

상기 고유 영역 명칭을 포함하는 상기 재인증 아이덴티티를 이용하여 재인증 요청을 인증 장치에 전송하는 수단을 포함하는, 단말기.

청구항 14

제13항에 있어서,

상기 고유 영역 명칭을 포함하는 상기 재인증 아이덴티티를 이용하여 재인증 요청을 인증 장치에 전송하는 수단은 확장성 인증 프로토콜(Extensible Authentication Protocol)에 따라 아이덴티티 응답 패킷에 상기 재인증 아이덴티티를 포함시키는 것을 특징으로 하는, 단말기.

청구항 15

인증 서버에 있어서,

인증을 수행하도록; 그리고

인증을 요청하는 단말기에, 인증 서버를 고유하게 식별하는 고유 영역 명칭을 포함하는 재인증 아이덴티티를 전송하도록 구성된 인증 프로토콜 구성요소들을 포함하는, 인증 서버.

청구항 16

제15항에 있어서, 상기 인증 서버는,

재인증을 위해 단말기에 의한 상기 재인증 아이덴티티를 포함하는 요청에 포함된 고유 영역 명칭을 상기 재인증 아이덴티티로부터 결정하도록 추가로 구성된 인증 프로토콜 구성요소들을 포함하는 것을 특징으로 하는, 인증 서버.

청구항 17

제16항에 있어서, 상기 인증 서버는,

만일 상기 고유 영역 명칭이 다른 인증 서버를 표시하면 상기 다른 인증 서버에 상기 요청을 전송하도록 추가로 구성된 인증 프로토콜 구성요소들을 포함하는 것을 특징으로 하는, 인증 서버.

청구항 18

단말기에 의해 전송된 재인증 요청에 포함된 재인증 아이덴티티로부터 상기 요청에 포함되고 인증 서버를 고유하게 표시하는 고유 영역 명칭을 결정하는 수단; 및

상기 요청을 상기 고유 영역 명칭에 의해 표시된 인증 서버에 전송하기 위한 메시지를 준비하는 수단을 포함하는, 인증 장치.

청구항 19

인증 장치에 있어서,

단말기에 의해 전송된 재인증 요청에 포함된 재인증 아이덴티티로부터 상기 요청에 포함된 고유 영역 명칭을 결정하도록; 그리고

상기 요청을 싱기 고유 영역 명칭에 의해 표시된 인증 서버에 전송하기 위한 메시지를 준비하도록 구성된 인증 프로토콜 구성요소들을 포함하는, 인증 장치.

청구항 20

단말기와 내용 서버 간의 통신 세션의 재인증을 요청하는 수단;

제1 인증 서버로부터 상기 제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 수신하는 수단; 및

인증 장치에 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 사용하여 재인증 요청을 전송하는 수단을 포함하는, 단말기.

청구항 21

제20항에 있어서, 인증 장치에 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 사용하여 재인증 요청을 전송하는 수단은 확장성 인증 프로토콜에 따라 아이덴티티 응답 패킷 내에 상기 재인증 아이덴티티를 포함시키도록 구성되는 것을 특징으로 하는, 단말기.

청구항 22

단말기에 있어서,

상기 단말기와 내용 서버 간의 통신 세션의 재인증을 요청하도록;

제1 인증 서버로부터 상기 제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 얻도록; 그리고

인증 장치에 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 사용하여 재인증 요청을 전송하도록 구성된 인증 프로토콜 구성요소들을 포함하는, 단말기.

청구항 23

제22항에 있어서, 상기 단말기는,

확장성 인증 프로토콜에 따라 아이덴티티 응답 패킷 내에 상기 재인증 아이덴티티를 포함시키도록 추가로 구성된 인증 프로토콜 구성요소들을 포함하는 것을 특징으로 하는, 단말기.

명 세 서

기 술 분 야

[0001] 본 발명은 범용 이동 통신 시스템(UMTS; Universal Mobile Telecommunications System)의 인증 및 (세션) 키 (분배) 협정(AKA; Authentication and (session) Key (distribution) Agreement)을 위한 확장성 인증 프로토콜(EAP; Extensible Authentication Protocol) 메커니즘과 같은, 및 또한 이동 통신 글로벌 시스템(GSM; Global System for Mobile communications)에서 사용되는 가입자 아이덴티티 모듈(SIM; Subscriber Identity Module)에서 구현되는 AKA를 위한 EAP 메커니즘과 같은, 통신 시스템에서의 인증 및 세션 키 분배를 위한 확장성 인증 프로토콜(EAP) 메커니즘에 관한 것이다. 보다 상세하게는, 본 발명은 GSM SIM 또는 UMTS AKA 인증을 위한 EAP 메커니즘을 이용하는 통신 시스템에서의 재인증에 관한 것이다.

[0002] 관련 출원의 상호 참조

[0003] EAP AKA 및 SIM 인증(EAP AKA AND SIM AUTHENTICATION)이라는 명칭의 2002년 10월 3일에 출원된 미국 가출원 번호 제60/416,481호를 참조하고 우선권을 주장한다.

배 경 기 술

[0004] 인증 및 (세션) 키 (분배) 협정(AKA; Authentication and (session) Key (distribution) Agreement)은 시도-응답(challenge-response) 메커니즘 및 대칭 암호화에 근거하고 UMTS에서의 AKA는 제3 세대 협력 프로그램(3GPP; Third Generation Partnership Program) 기술 사양(TS; Technical Specification) 33.102 V3.6.0: "기술 사양 그룹 서비스 및 시스템 양상; 3G 보안; 보안 구조 (릴리스 1999)(Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999))," 제3 세대 협력 프로젝트, 2000년 11월에 설명된다. AKA는 전형적으로 UMTS 가입자 아이덴티티 모듈(USIM; UMTS Subscriber Identity Module), 스마트 카드와 같은 장치에서 구동된다. 하지만, AKA의 응용성은 스마트 카드를 갖는 클라이언트 장치에 제한되지 않는다. 예를 들어, AKA 메커니즘은 또한 호스트 소프트웨어에서 구현될 수 있다. 또한 AKA는 GSM 03.20 (ETS 300 534): "디지털 셀룰러 통신 시스템(단계 2); 보안 관련 네트워크 기능(Digital cellular telecommunication system(phase 2); Security related network functions)" 유럽 통신 표준화 기구, 1997년 8월에 설명된 GSM 인증 메커니즘에 역방향 호환성을 제공한다. GSM 메커니즘에 비해, AKA는 실질적으로 더 긴 키 길이를 제공하고 또한 (클라이언트 측뿐 아니라) 서버측의 인증을 제공한다.

[0005] 무선 단말기와 같은 (보다 상세하게는 이동국과 같은) 클라이언트 장치가 운용자(operator)에 의해 제공되고 관리되는 통신 시스템의 서버와 같은 서버에 의해 제공되는 서비스(또는 실제로 예를 들어 인터넷을 포함하는 어떤 종류의 네트워크의 서버의 서비스)를 이용하기 위하여, 단말기 또는 사용자는 어떤 경우에 (어떤 네트워크에서 및 상기 네트워크의 어떤 서비스에서) 서버에 자신을 인증하거나 그 반대를 수행해야 한다(후자는 적어도 어떤 네트워크에서, 특히 UMTS에서). 즉 각자는 상대방에게 누가 요청하고 있는지를 증명해야 한다. 다이얼-업(dial-up) 네트워크, 무선 LAN, 유선 LAN 네트워크, 및 다양한 디지털 가입자 라인(xDSL; Digital Subscriber Line) 네트워크에서, 네트워크의 운용자는 전형적으로 소위 AAA(인증, 인가 및 어카운팅(Authentication, Authorization and Accounting)) 서버를 이용하여 클라이언트를 인증하고, 클라이언트가 서비스의 요청을 전송한 운용자 네트워크의 서버를 인증한다(또는 어떤 특정 서버와 무관하게 운용자 네트워크를 인증한다). AAA 서버는 사용자들(특정 사용자에 특정하여 사용자를 식별하는 구성요소를 갖는 단말기들)의 인증에 필요한 다른 자격 정보(credential information) 및 공유된 비밀의 저장을 책임질 수 있다. AAA 서버는 상기 자격 정보를 저장하기 위해 별개의 사용자 데이터베이스 서버를 이용할 수 있다. 확장성 인증 프로토콜(EAP)은 종종 AAA 서버 및 단말기간의 인증을 위해 AAA 서버를 이용하는 네트워크에서 사용된다. 네트워크의 운용자가 UMTS 또는 GSM 네트워크의 셀룰러 운용자인 경우, EAP 방법은 EAP AKA에서와 같은 향상된 UMTS 인증 및 키 협정 또는 EAP SIM에서와 같은 향상된 GSM 인증 및 키 협정을 캡슐화할 수 있다. 단말기는 인증 패킷들을 로컬 네트워크의 부대 장치(attendant device)와 교환한다. 상기 부대 장치는 네트워크의 상이한 유형에 따라 상이하지만, 예를 들어 무선 LAN 액세스 포인트, 이더넷 스위치(Ethernet switch) 또는 다이얼-업 네트워크 액세스 서버(NAS; Network Access Server)일 수 있다. 상기 부대 장치는 일반적으로 소위 AAA 클라이언트로서 동작하고, AAA 클라이언트

및 AAA 서버는 소위 AAA 프로토콜을 이용하여 인증을 수행한다.

[0006] EAP SIM 또는 EAP AKA를 가지고 설정되는 통신 세션의 시작시에, 단말기 및 AAA 서버는 본 명세서에서 소위 완전한 인증(full authentication), 즉 단말기 또는 AAA 서버 어느 것도 상대방을 인증하기 위한 어떤 기초를 갖지 않는 상태에서 시작하는 인증을 수행한다.

[0007] 완전한 인증이 설정된 이후에, 어떤 소정 시간 이후에 또는 어떤 다른 조건이 충족되는 경우에, "나쁜 사람(bad guy)"이 어떤 다른 장치(서버 장치 또는 클라이언트 장치)를 이용하여 원래의 인증된 실체로 가장하거나, 어떻게 해서 원래 인증된 장치의 물리적인 제어권을 얻어 (예를 들어 사용자가 인증된 단말기를 떠나 다른 곳에 간 경우) 요청을 전송하기 시작할 가능성을 감소시키기 위해 재인증이 요구될 수 있다. 로컬 네트워크에 의해 전송된 메시지를 이용하여 요구되는 경우 단말기가 여전히 네트워크 자원을 이용하고 있다는 것을 확인하기 위하여 재인증이 또한 요구될 수 있다. 또한, 키의 수명이 보안상 이유로 제한되는 경우 신규 보안 키를 협상하기 위하여 재인증이 이용될 수 있다. 재인증은 (GSM을 위한) EAP SIM 및 (UMTS를 위한) EAP AKA에서 동일하다.

[0008] EAP SIM 및 EAP AKA 프로토콜의 종래 기술은 AAA 서버로부터 재인증되는 단말기에 전송되는 별개의 재인증 사용자 아이덴티티를 이용하는 재인증을 제공한다. 재인증은 완전한 인증 동안 설정된 다른 콘텍스트 정보 및 세션 키에 근거한다.

[0009] 운용자는 부하 균형(load balancing)을 위해 그리고 다른 이유로 네트워크에서 몇몇 AAA 서버들을 이용할 수 있다. AAA 서버가 단말기를 인증하기 위해 임의로 선택되거나 라운드-로빈(round-robin) 메커니즘과 같은 어떤 소정의 메커니즘에 의해 선택될 수 있기 때문에, 단말기(사용자)가 항상 동일한 AAA 서버를 이용하여 인증되지 않을 수 있다. 이러한 네트워크에 있어서, 콘텍스트 정보가 완전한 인증을 수행한 AAA 서버에만 저장되어 있다는 점에서 재인증은 문제가 된다. 재인증은 완전한 인증 동안 제공된 몇몇 정보의 이용가능성을 가정하기 때문에, 단말기의 재인증을 위한 AAA 요청이 완전한 인증을 수행한 AAA 서버와는 다른 AAA 서버에 릴레이(relay)되는 경우 재인증이 동작하지 않을 것이다(즉, 재인증이 수행될 수 없다).

[0010] 따라서, 재인증을 위한 요청이 완전한 인증을 수행한 AAA 서버 이외의 다른 AAA 서버에 릴레이될 수 있는 네트워크에서 재인증이 동작하는 방법이 필요하다.

발명의 상세한 설명

[0011] 따라서, 본 발명의 제1 태양에 있어서, 인증 네트워크를 통한 단말기 및 서버간의 정보 교환을 포함하는 통신 세션의 재인증(reauthentication)에 사용하기 위한 방법으로서, 상기 통신 세션은 상기 인증 네트워크의 제1 인증 서버 및 상기 단말기에 의해 이미 인증된 방법에 있어서, 상기 제1 인증 서버 및 다른 인증 서버들 각각에 각자의 고유 영역 명칭(unique realm name)이 할당되는 단계; 및 상기 단말기 및 상기 제1 인증 서버 간의 인증 동안, 상기 제1 인증 서버는 상기 제1 인증 서버에 할당된 고유 영역 명칭을 포함하는 재인증 아이덴티티를 상기 단말기에 전송하는 단계를 포함하는 것을 특징으로 하는 방법이 제공된다.

[0012] 본 발명의 제1 태양에 따라, 상기 방법은 재인증을 수행하기 위하여 상기 단말기가 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 이용하여 재인증 요청을 전송하는 단계; 및 상기 재인증 요청을 수신하는 인증 네트워크 요소가 완전한 인증을 수행한 인증 서버를 나타내는 고유 영역 명칭을 상기 요청에 포함된 재인증 아이덴티티로부터 결정하는 단계를 더 포함할 수 있다. 상기 방법은 또한 인증 네트워크 요소가 상기 재인증 아이덴티티의 부분으로서 포함된 고유 영역 명칭에 의해 표시된 상기 인증 서버에 상기 요청을 전송하는 단계; 및 상기 단말기 및 상기 제1 인증 서버가 재인증을 수행하는 단계를 더 포함할 수 있다.

[0013] 본 발명의 제2 태양에 있어서, 단말기 및 내용 서버간의 통신 세션의 재인증을 위한 수단을 포함하는 셀룰러 통신 시스템의 인증 서버에 있어서, 할당된 고유 영역 명칭을 수신하는 수단; 및 상기 고유 영역 명칭을 포함하는 재인증 아이덴티티를 상기 단말기에 전송하는 수단을 포함하는 것을 특징으로 하는 인증 서버가 제공된다.

[0014] 본 발명의 제2 태양에 따라, 상기 인증 서버는 상기 재인증 아이덴티티를 이용하여 재인증 요청을 수신하고 상기 재인증 아이덴티티로부터 상기 고유 영역 명칭을 결정하는 수단을 더 포함할 수 있다. 상기 인증 서버는 또한 상기 재인증 아이덴티티의 부분으로서 포함된 고유 영역 명칭에 의해 표시되는 상기 인증 서버에 상기 요청을 전송하는 수단을 더 포함할 수 있다.

[0015] 본 발명의 제3 태양에 있어서, 인증 서버의 컴퓨터 프로세서에 의해 실행하기 위한 컴퓨터 프로그램 코드를 포함하는 컴퓨터 독출가능 저장 구조를 포함하는 컴퓨터 프로그램 생성물에 있어서, 상기 컴퓨터 프로그램 코드는 본 발명의 제2 태양에 따른 장치의 수단을 인에이블하는 명령어를 포함하는 것을 특징으로 하는 컴퓨터 프로그

램 생성물이 제공된다.

[0016] 본 발명의 제4 태양에 있어서, 복수의 단말기들, 복수의 인증 서버들, 및 적어도 하나의 내용 서버를 포함하는 시스템으로서, 상기 단말기들은 하나 또는 다른 하나의 인증 서버에 대한 인증 및 간헐적인 재인증 이후에 상기 내용 서버로부터 내용을 요청하도록 동작하는 시스템에 있어서, 적어도 2개의 상기 인증 서버들 각각은 본 발명의 제2 태양에 따른 장치인 것을 특징으로 하는 시스템이 제공된다.

[0017] 본 발명의 상기 및 다른 목적들, 특징들 및 장점들은 첨부한 도면들과 관련하여 제시된 다음의 상세한 설명을 고려하는 경우 명백하게 될 것이다.

실 시 예

[0020] 본 발명은 완전한 인증을 수행한 AAA 서버 이외의 다른 AAA 서버에 재인증 요청이 릴레이될 수 있는 네트워크에서 재인증이 동작하는 것을 어떻게 보장하는지에 대한 문제의 해결책을 제공한다. 상기 문제를 해결하기 위하여, 본 발명은 재인증에 대한 AAA 서버로서 완전한 인증을 수행한 AAA 서버를 선택하는 것을 가능하게 한다.

[0021] 본 발명은 3GPP TS 33.102 V3.6.0: "기술 사양 그룹 서비스 및 시스템 양상; 3G 보안; 보안 구조 (릴리스 1999)(Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999))," 제3 세대 협력 프로젝트, 2000년 11월에서, 및 인터넷 엔지니어링 태스크 포스(IETF; Internet Engineering Task Force) 초안 문서, J. Arkko 및 H. Haverinen에 의한, "EAP AKA 인증(EAP AKA Authentication)" draft-arkko-pppext-eap-aka-04.txt, 2002년 6월에서 설명된 바와 같이, 범용 이동 통신 시스템(UMTS) 인증 및 키 협정(AKA; Authentication and Key Agreement)에서의 인증 및 세션 키 분배를 위한 확장성 인증 프로토콜(EAP; Extensible Authentication Protocol) 메커니즘과 관련하여 후술된다. UMTS는 제3 세대 글로벌 이동 네트워크 표준이다. 본 발명은 또한 명백하게 GSM 기술 사양 GSM 03.20 (ETS 300 534): "디지털 셀룰러 통신 시스템(단계 2); 보안 관련 네트워크 기능(Digital cellular telecommunication system(phase 2); Security related network functions)" 유럽 통신 표준화 기구, 1997년 8월에서, 및 IETF 초안 문서, H. Haverinen에 의한 "EAP SIM 인증(EAP SIM Authentication)", draft-haverinen-pppext-eap-sim-05.txt, 2002년 7월 2일에서 설명된 바와 같이, 이동 통신 글로벌 시스템(GSM) 가입자 아이덴티티 모듈(SIM)을 이용한 인증 및 세션 키 분배를 위한 EAP 메커니즘과 관련하여 이용된다. 비록 본 발명이 특히 확장성 인증 프로토콜 및 UMTS 및 GSM에 대한 방법을 이용하여 기술되지만, 본 발명에 대한 어떠한 것도 확장성 인증 프로토콜 또는 UMTS 또는 GSM 표준에 따른 셀룰러 통신 시스템에서의 이용에 제한되지 않는다. 본 발명은 실제로 AAA 프로토콜과 관련된 확장성 인증 프로토콜과 유사한 인증을 제공하는 어떤 통신 시스템에서 사용된다. 기술된 실시예의 경우에 있어서, 본 발명은 IETF의 네트워크 워킹 그룹에 의해 발행된 "PPP 확장성 인증 프로토콜(EAP)(PPP Extensible Authentication Protocol(EAP))"라는 명칭의 RFC 2284에서 설명된 바와 같이, 소위 확장성 인증 프로토콜(EAP)을 이용한다. (PPP) EAP는 인증을 위한 일반적인 프로토콜이고, 다중 인증 메커니즘을 지원한다.

[0022] 이제 도 1 및 도 2를 참조하면, 재인증이 항상 가능하도록 보장하기 위하여, 본 발명은 각 AAA 서버(23a, 23b)(동일하거나 상이한 운용자 네트워크에서의)에 고유 영역 명칭(unique realm name)이 할당되는 제1 단계(11)를 포함하는 방법을 제공한다. IP 서비스를 위한 인증 및 UMTS 또는 GSM의 경우에 있어서, 상기 명칭은 네트워크 액세스를 위한 인증과 관련하여 AAA 프로토콜에서 사용되는 (단말기의) 식별자인 (일부로서, 예를 들어 user@realm에서 "realm"은 고유 영역(realm) 명칭으로서) 네트워크 액세스 식별자(NAI; Network Access Identifier)에서 사용될 수 있는 유형의 명칭이다. 설정된 EAP 및 AAA 프로토콜들에 있어서, 인증 요청은 사용자의 네트워크 액세스 식별자를 포함한다. 완전한 인증(full authentication)의 경우에 있어서, EAP SIM 및 EAP AKA는 완전한 인증을 요청하기 위하여 단말기가 사용하는 아이덴티티 포맷을 명시한다. 설정된 사양에 따라, NAI의 사용자명 부분은 국제 이동 가입자 식별자(IMSI; International Mobile Subscriber Identifier) 또는 EAP SIM 및 EAP AKA 사양에서 가명(pseudonym)으로 지칭되는 임시 식별자를 포함한다. NAI에 사용되는 영역 명칭은 전형적으로 홈 운영자의 공통 식별자이다. 몇몇 AAA 서버들은 상기 영역 명칭에 전송되는 요청을 서비스하도록 채용될 수 있다. 따라서, 종래 기술에 따라, 일반적으로 NAI에서의 영역 명칭은 몇몇 AAA 서버들에 의해 공유될 수 있다. 예를 들어, 내 운영자(MyOperator)의 가입자들은 영역 명칭인 myoperator.com을 이용할 수 있고, AAA 메시지들은 myoperator.com의 AAA 서버들 중의 하나에 라우팅(routing)될 것이다. 상기 영역이 가능하게는 AAA 서버들의 그룹을 나타내는 것은 EAP SIM 및 EAP AKA 완전한 인증에서의 경우이다. 하지만, 본 발명에 따라, 각 AAA 서버에는 또한 예를 들어 serverX.myoperator.com과 같은 고유 영역 명칭이 할당될 것이고, 상기 고유 영역 명칭은 재인증 아이덴티티에서 사용되는 고유 영역 명칭이다. 여기서, 제3-레벨 명칭인 serverX는 상

기 영역 명칭 serverX.myoperator.com을 고유 영역 명칭으로 만든다. 영역 명칭의 구조화된 형식은 일부 AAA 요소들이 영역 명칭을 고유하게 하는데 추가되어야 하는 어떤 제3-레벨 명칭을 고려하지 않고 myoperator.com으로 끝나는 모든 영역들을 올바른 다음 홉(hop)으로 라우팅하도록 허용할 수 있다. 예를 들어, 부대 장치(attendant device)(21a)는 완전한 영역 명칭에 유념할 필요가 없고 대신에 간단한 규칙을 이용할 수 있다. "*.myoperator.com을 MyOperator AAA 프록시에 라우팅한다" (여기서 * 문자는 와일드카드(wildcard)로서 기능한다. 즉 명칭에서 허용되는 어떠한 세트의 문자들을 나타낸다).

[0023] 다음 단계(12)에 있어서, AAA 서버들(23a, 23b) 중 제1 서버(23a)는 부대 장치(21a)가 (인터넷과 같은) 네트워크(24)로의 단말기(21) 액세스를 허용할 수 있도록 단말기(21)에 관하여 (완전한) 인증을 위해 프록시 AAA 서버(22)를 통해 부대 장치(21a) (즉, AAA 클라이언트, 및 특히 예를 들어 서비스 액세스 포인트)로부터 요청을 수신한다. AAA 서버들(23a, 23b) 중 하나 또는 나머지 하나에 통신을 라우팅하는 다른 요소들뿐 아니라 단말기(21) 및 AAA 서버들(23a, 23b) 간의 무선 통신을 가능하게 하는 하나 이상의 운용자 네트워크들(즉, 특히 각 운용자 네트워크를 위한 무선 액세스 네트워크들)의 다양한 요소들이 (명료함을 위해) 도 2에는 도시되지 않는다.

[0024] 다음 단계(13)에 있어서, 제1 AAA 서버(23a)는 (이후 재인증시에 단말기에 의해 이용하기 위해) 재인증 아이덴티티를 (프록시 서버(22) 및 부대 장치(21a)를 통해) 단말기(21)에 전송하고, 재인증 아이덴티티에 고유 영역 명칭을 포함하며, 또한 사용자명 부분을 포함한다. 상기 재인증 아이덴티티는 완전한 인증에 사용되는 가명 아이덴티티 및 IMSI-기반 아이덴티티와는 상이하다. 단계 13은 도 1에서 명료함을 위해 생략된 다른 단계들을 포함하는 완전한 인증 절차의 일부로서 수행된다. 재인증 아이덴티티의 사용자명 부분은 서버에 의해 선택된 원-타임(one-time) 사용자명이다. 상기 사용자명은 임의로 선택된 식별자 또는 숫자일 수 있다. 따라서 재인증 아이덴티티는 예를 들어 다음과 같을 수 있다.

[0025] 1209834387@server15.myoperator.com

[0026] 다음 단계(14)에 있어서, (전형적으로 충족된 어떤 조건에 근거하여) 재인증을 수행하기 위하여, 단말기(21)는 고유 영역 명칭을 포함하는 재인증 아이덴티티를 이용하여 재인증 요청을 전송한다. 일반적으로, 재인증이 개시될 수 있는 몇가지 방법이 있다. 한가지 방법은 부대 장치(21a)가 재인증을 개시할 수 있는 것이다. 이 경우에 있어서, -- 고유 영역 명칭에 근거하여 전송되는 "재인증 요청(reauthentication request)"이 EAP 아이덴티티 응답 패킷을 포함하는 -- 무선 랜(LAN)에서 부대 장치(21a)는 EAP 아이덴티티 요청 패킷을 단말기(21)에 전송하고, 단말기는 재인증 아이덴티티를 포함하는 EAP 아이덴티티 응답을 가지고 응답한다. 상기 패킷은 AAA 프로토콜에 의하여 올바른 AAA 서버에 전송된다. 대안으로, 단말기(21) 자신이 재인증을 개시할 수 있다. 무선 랜에서, 단말기(21)는 EAPOL-시작(랜에 의한 EAP 시작(EAP over LAN start)) 패킷을 부대 장치(21a)에 전송한다. EAPOL-시작을 수신하는 경우, 부대 장치(21a)는 EAP 아이덴티티 요청 패킷을 단말기에 전송하고, 재인증 교환이 후술되는 바와 같이 진행된다.

[0027] 다음 단계(15)에 있어서, 요청을 수신한 어떤 AAA 네트워크 요소(부대 장치(21a), 프록시(22), 및 AAA 서버들(23a, 23b))는 요청에 포함된 재인증 아이덴티티를 검사하여 (영역 명칭을 통해 제1 AAA 서버(23a)를 나타내는 재인증 아이덴티티에 근거하여) 어디에 상기 요청을 라우팅할지를 결정한다. 상기 라우팅은 예를 들어, 라우팅 테이블(routing table)에 근거하거나 적합한 다른 보통의 AAA 라우팅 수단에 근거한다. 전형적으로, 프록시 서버(22)는 영역 명칭을 검사하고 요청을 직접 제1 AAA 서버(23a)에 라우팅한다. 따라서 상기 요청은 완전한 인증을 수행한 AAA 서버에 의해, 즉 제1 AAA 서버(23a)에 의해 조만간 수신된다.

[0028] 다음 단계(16)에 있어서, 제1 AAA 서버(23a)는 재인증을 위해 설정된 프로토콜에 의하여 재인증을 위한 요청에 응답한다. 다음 단계(17)에 있어서, 단말기(21)에서 제1 AAA 서버(23a)로의 다음 통신이 부대 장치(21a)를 통해 제1 AAA 서버(23a) 및 단말기(21)간에 설정된 AAA 프로토콜들에 의하여 통신된다. 다음 통신은 부대 장치(21a) 및 제1 AAA 서버(23a)간에 직접 라우팅되거나 중간 AAA 요소들을 통해 라우팅될 수 있다. 설정된 AAA 프로토콜들은 전형적으로 인증을 수행하는 AAA 서버(23a)가 인증 교환 동안 변하지 않도록 보장하는 수단을 포함한다.

[0029] 몇몇 경우에 있어서, 단말기(21)는 각 세션에 대해 완전한 인증 절차를 이용하여 동시에 몇몇 상이한 세션을 통해 통신할 수 있다. 상기 세션들은 동일한 AAA 서버에 의해 또는 상이한 AAA 서버들에 의해 인증될 수 있고, 인증을 수행하기 위해 동일하거나 상이한 애플리케이션 및 동일하거나 상이한 무선 기술을 이용할 수 있다. 본 발명에 따라, 상기 가변성을 수용하기 위하여, 단말기(21)는 각 세션에 대해 별개의 상태 정보를 유지하고, 단말기(21)는 도 1과 관련하여 설명된 바와 같이 각 세션에 대해 별개로 재인증을 수행할 수 있다. 대응하여, 하나 이상의 동시 발생하는 세션들에 대한 인증에서 사용되는 각 AAA 서버(23a, 23b)는 각 세션에 대한 별개의 상태 정보를 유지한다.

[0030] 비록 본 발명이 무선 랜 인증에 관련되지만, 본 발명은 또한 xDSL, 다이얼-업(dial-up), 이더넷(Ethernet), 및 다른 인증 콘텍스트들에 관련된다는 것을 유의한다. UMTS 및 GSM 인증을 위한 확장성 인증 프로토콜 방법은 WLAN 또는 다른 상보성(complementary) 액세스 네트워크들을 관리하기를 원하는 이동 운용자들을 대상으로 한다. 본 발명은 실제 UMTS 또는 GSM 네트워크에 전혀 사용되지 않을 수도 있다.

[0031] 상술된 구성은 단지 본 발명의 원리의 응용의 예시인 것을 이해해야 한다. 다수의 변형 및 대안적인 구성이 본 발명의 범위를 벗어나지 않으면서 당업자에 의해 고안될 수 있다. 첨부된 청구범위는 상기 변형 및 구성을 포함하도록 의도된다.

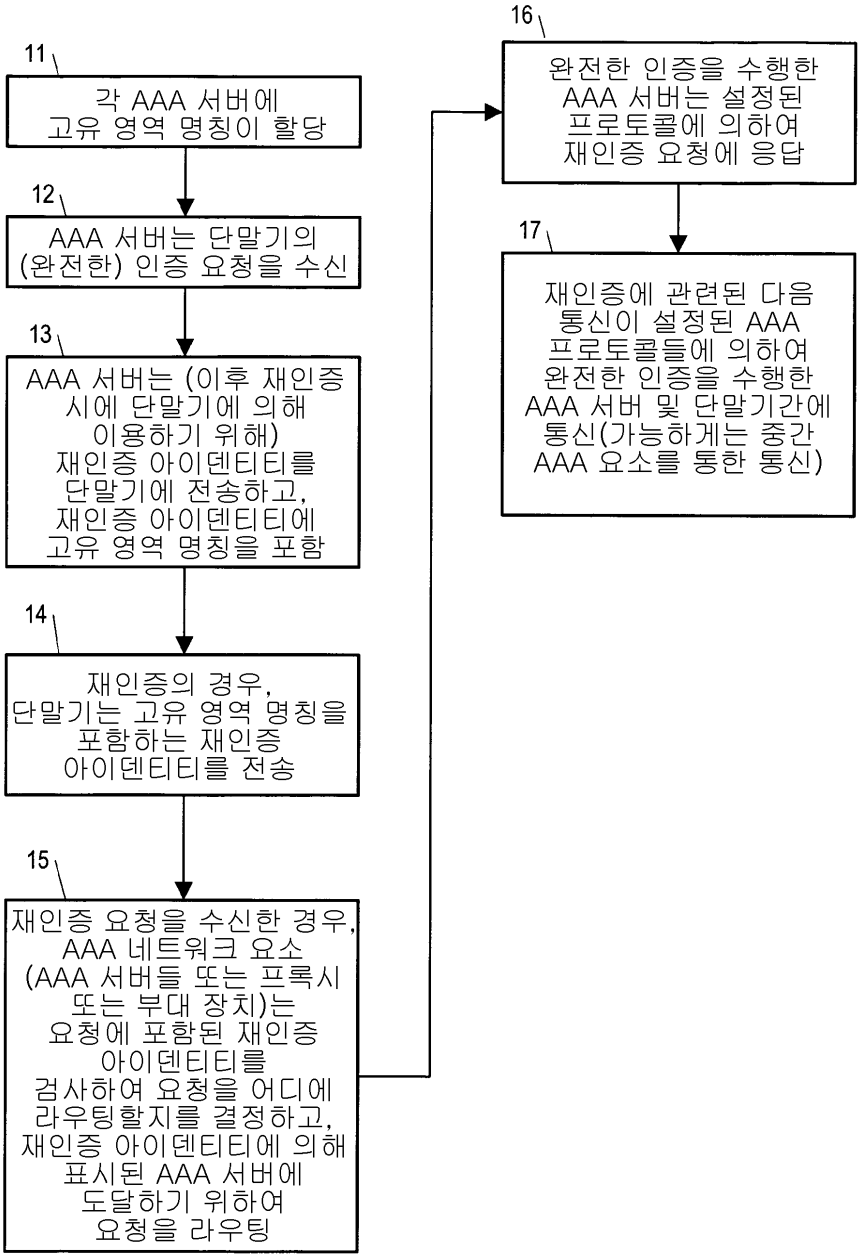
도면의 간단한 설명

[0018] 도 1은 본 발명에 따른 (인증 에이전트로서 동작하는 인증 서버를 가지고) 단말기를 재인증하는 방법의 흐름도이다.

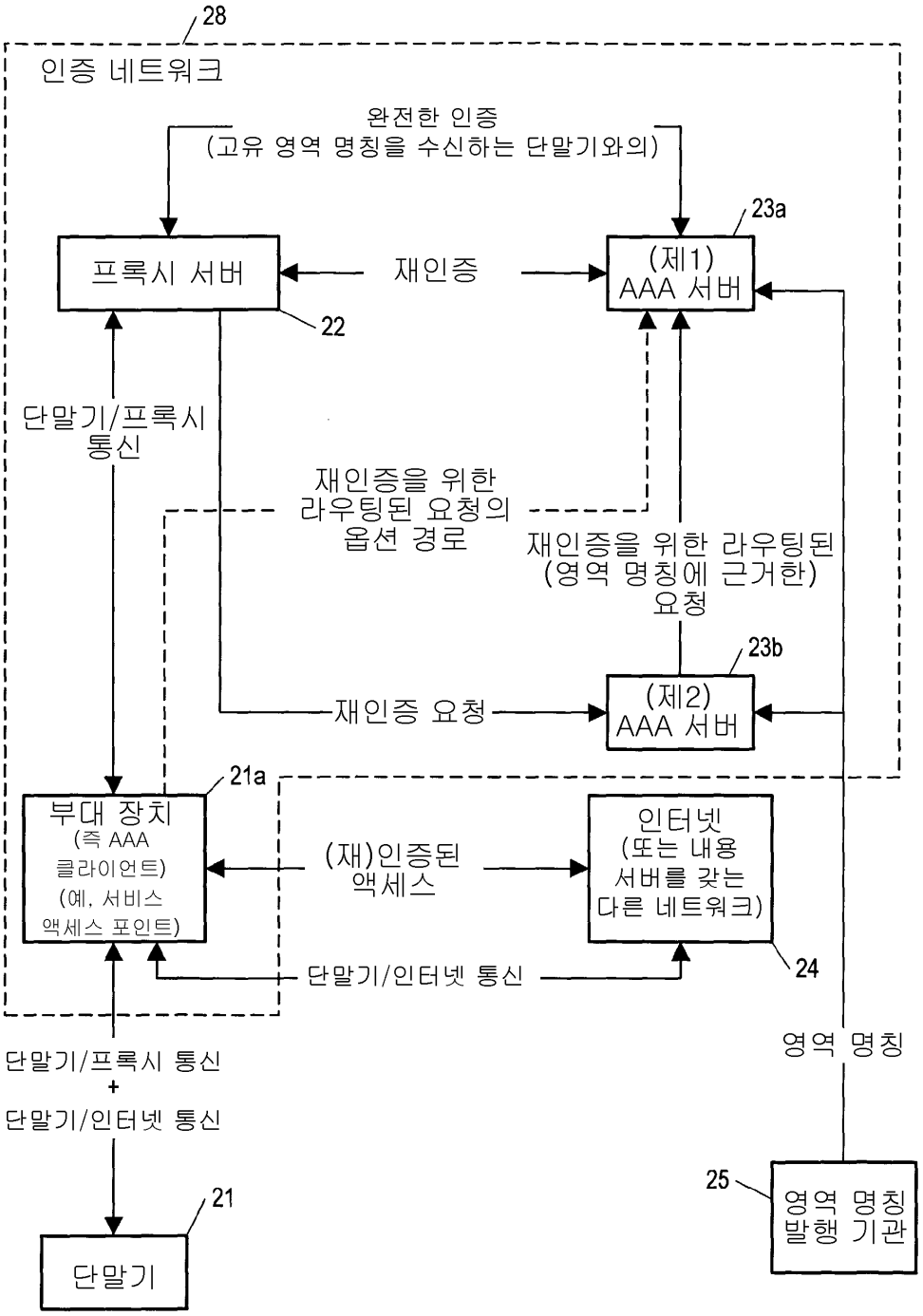
[0019] 도 2는 본 발명에 따른 인증 서버를 가지고 인증하고 재인증하는 단말기의 블록도/흐름도이다.

도면

도면1


11
각 AAA 서버에 고유 영역 명칭이 할당
12
AAA 서버는 단말기의 (완전한) 인증 요청을 수신
13
AAA 서버는 (이후 재인증 시에 단말기에 의해 이용하기 위해) 재인증 아이덴티티를 단말기에 전송하고, 재인증 아이덴티티에 고유 영역 명칭을 포함
14
재인증의 경우, 단말기는 고유 영역 명칭을 포함하는 재인증 아이덴티티를 전송
15
재인증 요청을 수신한 경우, AAA 네트워크 요소 (AAA 서버들 또는 프록시 또는 부대 장치)는 요청에 포함된 재인증 아이덴티티를 검사하여 요청을 어디에 라우팅할지를 결정하고, 재인증 아이덴티티에 의해 표시된 AAA 서버에 도달하기 위하여 요청을 라우팅
16
완전한 인증을 수행한 AAA 서버는 설정된 프로토콜에 의하여 재인증 요청에 응답
17
재인증에 관련된 다음 통신이 설정된 AAA 프로토콜들에 의하여 완전한 인증을 수행한 AAA 서버 및 단말기간에 통신(가능하게는 중간 AAA 요소를 통한 통신)

도면2


28
인증 네트워크
완전한 인증
(고유 영역 명칭을 수신하는 단말기와의)
23a
프록시 서버
재인증
(제1)
AAA 서버
22
단말기/프록시
통신
재인증을 위한
라우팅된 요청의
옵션 경로
재인증을 위한 라우팅된
(영역 명칭에 근거한)
요청
23b
재인증 요청
(제2)
AAA 서버
21a
부대 장치
(즉 AAA
클라이언트)
(예, 서비스
액세스 포인트)
(재)인증된
액세스
인터넷
(또는 내용
서버를 갖는
다른 네트워크)
24
단말기/인터넷 통신
영역 명칭
단말기/프록시 통신
+
단말기/인터넷 통신
25
영역 명칭
발행 기관
21
단말기