

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0127231 (43) 공개일자 2013년11월22일
(51) 국제특허분류(Int. Cl.) H04L 9/32 (2006.01) H04L 9/30 (2006.01)		(71) 출원인 서강대학교산학협력단 서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(21) 출원번호 10-2012-0051003		(72) 발명자 김주호 서울특별시 서초구 방배동 808-2
(22) 출원일자 2012년05월14일 심사청구일자 2012년05월14일		박근영 서울특별시 도봉구 창1동 661-13번지 원산아파트 603호 김용수 경기도 시흥시 정왕2동 계룡1차아파트 108동 202호
		(74) 대리인 특허법인충현

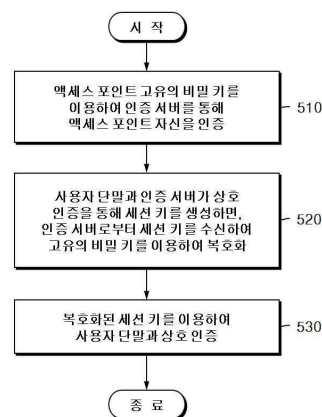
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 하드웨어 인증 모듈을 이용한 액세스 포인트 인증 장치 및 방법

(57) 요약

본 발명은 하드웨어 인증 모듈을 이용한 액세스 포인트 인증 장치 및 방법에 관한 것으로, 본 발명의 일 실시예에 따른 액세스 포인트의 인증 방법은, 사용자 단말로부터 접속을 요청받은 액세스 포인트가 액세스 포인트 고유의 비밀 키를 이용하여 인증 서버를 통해 자신을 인증하고, 액세스 포인트의 인증에 기반하여 사용자 단말과 인증 서버가 상호 인증을 통해 세션 키를 생성하면, 액세스 포인트가 인증 서버로부터 암호화된 세션 키를 수신하여 고유의 비밀 키를 이용하여 복호화하며, 복호화된 세션 키를 이용하여 사용자 단말과 상호 인증한다.

대표도 - 도5



특허청구의 범위

청구항 1

사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트(access point)의 인증 방법에 있어서,

상기 사용자 단말로부터 접속을 요청받은 액세스 포인트가 상기 액세스 포인트 고유의 비밀 키(secret key)를 이용하여 인증 서버를 통해 상기 액세스 포인트 자신을 인증하는 단계;

상기 액세스 포인트의 인증에 기반하여 상기 사용자 단말과 상기 인증 서버가 상호 인증을 통해 세션 키(session key)를 생성하면, 상기 액세스 포인트가 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화하는 단계; 및

상기 액세스 포인트가 상기 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증하는 단계;를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 고유의 비밀키는,

상기 액세스 포인트마다 유일한 값으로서, 변경이 불가능하도록 상기 액세스 포인트 내의 하드웨어 인증 모듈에 기록되고, 미리 정의된 제어 명령에 의해서만 접근 가능하며, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈로부터 독출되는 것을 특징으로 하는 방법.

청구항 3

제 1 항에 있어서,

상기 액세스 포인트 자신을 인증하는 단계는,

상기 액세스 포인트가 액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버(random number)와 함께 인증서 요청을 수신하는 단계;

상기 액세스 포인트가 암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하는 단계; 및

상기 액세스 포인트가 상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호화하도록 함으로써 상기 액세스 포인트 자신을 인증하는 단계;를 포함하는 방법.

청구항 4

제 3 항에 있어서,

상기 인증 서버는 상기 액세스 포인트 식별자 및 상기 고유의 비밀 키를 통해 상기 액세스 포인트를 유일하게 식별하는 것을 특징으로 하는 방법.

청구항 5

제 3 항에 있어서,

상기 인증 서버는 상기 액세스 포인트로부터 수신된 상기 인증서에 포함된 공개 키를 이용하여 상기 암호화된 랜덤 넘버를 복호화하고, 최초에 상기 인증 서버가 생성한 랜덤 넘버와 비교함으로써 유효성 검사를 수행하는 것을 특징으로 하는 방법.

청구항 6

제 1 항에 있어서,

상기 액세스 포인트가 상기 고유의 세션 키를 복호화하는 단계는,

상기 액세스 포인트가 상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하는 단계; 및

복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화하는 단계;를 포함하는 방법.

청구항 7

제 1 항에 있어서,

상기 액세스 포인트가 상기 사용자 단말과 상호 인증하는 단계는,

상기 액세스 포인트가 상기 복호화된 세션 키를 이용하여 페어와이즈 키(pairwise key)를 생성하는 단계; 및

상기 액세스 포인트가 상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹(handshaking)함으로써 상호 인증하는 단계;를 포함하는 방법.

청구항 8

제 1 항에 있어서,

상기 사용자 단말, 상기 액세스 포인트 및 상기 인증 서버는 WPA-Enterprise 보안 모드에 따른 인증 구조를 사용하여 동작하는 것을 특징으로 하는 방법.

청구항 9

제 1 항 내지 제 9 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 10

사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트의 인증 장치에 있어서,

사용자 단말 및 인증 서버와 통신하는 통신부; 및

상기 액세스 포인트와 상기 인증 서버 간의 인증 및 상기 액세스 포인트와 상기 사용자 단말 간의 상호 인증을 처리하는 인증 처리부;를 포함하며,

상기 인증 처리부는,

상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 인증 서버를 통해 상기 액세스 포인트 자신을 인증하고,

상기 액세스 포인트의 인증에 기반하여 상기 사용자 단말과 상기 인증 서버가 상호 인증을 통해 세션 키를 생성하면, 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화하며,

상기 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증하는 것을 특징으로 하는 장치.

청구항 11

제 10 항에 있어서,

상기 인증 처리부는,

상기 액세스 포인트마다 유일한 값으로서 변경이 불가능하도록 상기 고유의 비밀키를 기록하는 하드웨어 인증 모듈을 구비하며,

미리 정의된 제어 명령에 의해서만 상기 하드웨어 인증 모듈과 상호작용하여 상기 고유의 비밀키에 접근 가능하고, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈로부터 상기 고유의 비밀키를 독출할 수 있는 제어부;를 더 포함하는 것을 특징으로 하는 장치.

청구항 12

제 10 항에 있어서,

상기 인증 처리부는,

액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버와 함께 인증서 요청을 수신하고,

암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하며,

상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호화하도록 함으로써 상기 액세스 포인트 자신을 인증하는 것을 특징으로 하는 장치.

청구항 13

제 12 항에 있어서,

상기 인증 서버는 상기 액세스 포인트 식별자 및 상기 고유의 비밀 키를 통해 상기 액세스 포인트를 유일하게 식별하는 것을 특징으로 하는 장치.

청구항 14

제 12 항에 있어서,

상기 인증 서버는 상기 액세스 포인트로부터 수신된 상기 인증서에 포함된 공개 키를 이용하여 상기 암호화된 랜덤 넘버를 복호화하고, 최초에 상기 인증 서버가 생성한 랜덤 넘버와 비교함으로써 유효성 검사를 수행하는 것을 특징으로 하는 장치.

청구항 15

제 10 항에 있어서,

상기 인증 처리부는,

상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하고,

복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화하는 것을 특징으로 하는 장치.

청구항 16

제 10 항에 있어서,

상기 인증 처리부는,

상기 복호화된 세션 키를 이용하여 페어와이즈 키를 생성하고,

상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹함으로써 상호 인증하는 것을 특징으로 하는 장치.

청구항 17

제 10 항에 있어서,

상기 사용자 단말, 상기 액세스 포인트 및 상기 인증 서버는 WPA-Enterprise 보안 모드에 따른 인증 구조를 사용하여 동작하는 것을 특징으로 하는 장치.

명세서

기술분야

본 발명은 사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트의 인증 기술에 관한 것으로, 특히 모바일 액세스 포인트를 이용한 통신 환경 하에서 사용자 단말이 접속하는 액세스 포인트의 신뢰성을 보장하기 위한 액세스 포인트 인증 장치, 방법 및 그 방법을 기록한 기록매체에 관한 것이다.

[0001]

배경 기술

- [0002] 무선 통신 기술의 발달과 더불어 과거 유선 네트워크를 통한 통신 환경이 점차 무선 네트워크 단일 또는 유무선 혼합 네트워크의 통신 환경으로 변화하고 있다. 과거의 WLAN(Wireless LAN) 환경에서는 액세스 포인트(Access Point, AP)가 유선 네트워크를 이용하였으며, 이러한 액세스 포인트로부터 사용자 단말까지 비로소 WLAN 핫스팟(HotSpot), 즉 무선 네트워크를 구성하였다. 이러한 과거의 WLAN 환경에서는 액세스 포인트 장치가 특정 유선 네트워크(LAN)에 지리적으로 종속되어 있었기 때문에 설치 환경에 많은 제약이 따를 뿐만 아니라, 전원 공급이 필요하므로 이동 중의 통신 서비스 제공이 불가능하였다.
- [0003] 최근 들어 3G/4G 이동 통신 네트워크를 이용하는 모바일 액세스 포인트의 보급이 증가하고 있다. 모바일 액세스 포인트는 종래의 유선 액세스 포인트와는 달리 특정 네트워크에 종속적이지 않기 때문에 설치 공간에 제약이 없고, 자체 배터리를 이용해 구동될 수 있어 통신 서비스 중에도 이동이 가능하다는 특징을 갖는다. 또한, 최근에는 전용 모바일 라우터(router) 단말뿐만 아니라, 대부분의 스마트폰도 WLAN 테더링(tethering) 기능을 제공하고 있기 때문에 스마트폰을 마치 모바일 액세스 포인트로서 활용할 수 있다.
- [0004] 향후, LTE/LTE-A와 같은 이동 통신 기술의 발달과 더불어 스마트폰과 같은 모바일 액세스 포인트를 이용한 WLAN 환경 구성이 보편화될 수 있으며, 장기적으로는 기존의 유선 네트워크 환경을 점진적으로 대체할 것으로 예상된다. 따라서, 종래의 유선 네트워크에 기반한 통신 환경과는 달리, 모바일 액세스 포인트를 이용한 무선 통신 환경에서의 보안 문제가 대두될 우려가 존재한다. 이하에서 인용되는 비특허문헌에는 이러한 무선 LAN 정보 보안에 관한 기술 동향이 소개되어 있다.

선행기술문헌

비특허문헌

- [0005] (비특허문헌 0001) IEEE 802.11 기반의 무선LAN 정보보호 기술 개발에 관한 연구, 정보통신부, 2005.

발명의 내용

해결하려는 과제

- [0006] 본 발명의 실시예들이 해결하고자 하는 기술적 과제는, 종래의 무선 통신 환경에서 사용자 단말이 접속하고자 하는 무선 액세스 포인트가 중간자 공격과 같은 불법적인 외부 공격에 취약하다는 문제점을 해결하고, 무선 액세스 포인트의 비밀 키의 유출이 용이하다는 취약점을 해소하며, 그 결과 무선 액세스 포인트의 신뢰도를 보장할 수 없다는 한계를 극복하고자 한다.

과제의 해결 수단

- [0007] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트(access point)의 인증 방법은, 상기 사용자 단말로부터 접속을 요청받은 액세스 포인트가 상기 액세스 포인트 고유의 비밀 키(secret key)를 이용하여 인증 서버를 통해 상기 액세스 포인트 자신을 인증하는 단계; 상기 액세스 포인트의 인증에 기반하여 상기 사용자 단말과 상기 인증 서버가 상호 인증을 통해 세션 키(session key)를 생성하면, 상기 액세스 포인트가 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화하는 단계; 및 상기 액세스 포인트가 상기 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증하는 단계;를 포함한다.
- [0008] 일 실시예에 따른 상기 액세스 포인트의 인증 방법에서, 상기 고유의 비밀키는, 상기 액세스 포인트마다 유일한 값으로서, 변경이 불가능하도록 상기 액세스 포인트 내의 하드웨어 인증 모듈에 기록되고, 미리 정의된 제어 명령에 의해서만 접근 가능하며, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈로부터 독출된다.
- [0009] 일 실시예에 따른 상기 액세스 포인트의 인증 방법에서, 상기 액세스 포인트 자신을 인증하는 단계는, 상기 액세스 포인트가 액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버(random number)와 함께 인증서 요청을 수신하는 단계; 상기 액세스 포인트가 암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하는 단계; 및 상기 액세스 포인트가 상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호

화하도록 함으로써 상기 액세스 포인트 자신을 인증하는 단계;를 포함한다.

- [0010] 일 실시예에 따른 상기 액세스 포인트의 인증 방법에서, 상기 액세스 포인트가 상기 고유의 세션 키를 복호화하는 단계는, 상기 액세스 포인트가 상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하는 단계; 및 복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화하는 단계;를 포함한다.
- [0011] 일 실시예에 따른 상기 액세스 포인트의 인증 방법에서, 상기 액세스 포인트가 상기 사용자 단말과 상호 인증하는 단계는, 상기 액세스 포인트가 상기 복호화된 세션 키를 이용하여 페어와이즈 키(pairwise key)를 생성하는 단계; 및 상기 액세스 포인트가 상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹(handshaking)함으로써 상호 인증하는 단계;를 포함한다.
- [0012] 한편, 이하에서는 상기 기재된 액세스 포인트의 인증 방법들을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- [0013] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트의 인증 장치는, 사용자 단말 및 인증 서버와 통신하는 통신부; 및 상기 액세스 포인트와 상기 인증 서버 간의 인증 및 상기 액세스 포인트와 상기 사용자 단말 간의 상호 인증을 처리하는 인증 처리부;를 포함하며, 상기 인증 처리부는, 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 인증 서버를 통해 상기 액세스 포인트 자신을 인증하고, 상기 액세스 포인트의 인증에 기반하여 상기 사용자 단말과 상기 인증 서버가 상호 인증을 통해 세션 키를 생성하면, 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화하며, 상기 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증한다.
- [0014] 일 실시예에 따른 상기 액세스 포인트의 인증 장치에서, 상기 인증 처리부는, 상기 액세스 포인트마다 유일한 값으로서 변경이 불가능하도록 상기 고유의 비밀키를 기록하는 하드웨어 인증 모듈을 구비하며, 미리 정의된 제어 명령에 의해서만 상기 하드웨어 인증 모듈과 상호작용하여 상기 고유의 비밀키에 접근 가능하고, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈로부터 상기 고유의 비밀키를 독출할 수 있는 제어부;를 더 포함한다.
- [0015] 일 실시예에 따른 상기 액세스 포인트의 인증 장치에서, 상기 인증 처리부는, 액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버와 함께 인증서 요청을 수신하고, 암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하며, 상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호화하도록 함으로써 상기 액세스 포인트 자신을 인증한다.
- [0016] 일 실시예에 따른 상기 액세스 포인트의 인증 장치에서, 상기 인증 처리부는, 상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하고, 복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화한다.
- [0017] 일 실시예에 따른 상기 액세스 포인트의 인증 장치에서, 상기 인증 처리부는, 상기 복호화된 세션 키를 이용하여 페어와이즈 키를 생성하고, 상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹함으로써 상호 인증한다.

발명의 효과

- [0018] 본 발명의 실시예들은 무선 액세스 포인트의 고유의 비밀 키를 변경 및 복제가 불가능하도록 하드웨어 인증 모듈에 기록하고 이를 통해 액세스 포인트의 인증을 수행함으로써, 중간자 공격에 강인할 뿐만 아니라 무선 액세스 포인트의 비밀 키의 유출을 원천적으로 차단할 수 있고, 비밀 키의 고유성으로 인해 키 유출이 다른 액세스 포인트의 보안에 영향을 미치지 않으며, 그 결과 무선 액세스 포인트 보안의 신뢰도를 향상시킬 수 있다.

도면의 간단한 설명

- [0019] 도 1은 WLAN 표준 보안 방식 중, WPA-Personal Mode에서 발생할 수 있는 중간자 공격 등의 보안 문제를 설명하기 위한 도면이다.
- 도 2는 WLAN 표준 보안 방식 중, WPA-Enterprise Mode에서 발생할 수 있는 중간자 공격 등의 보안 문제를 설명하기 위한 도면이다.
- 도 3은 액세스 포인트 및 사용자 단말 간의 상호 인증을 보장하기 위하여 본 발명의 실시예들이 제안하는 액세스

스 포인트의 인증 장치를 예시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 액세스 포인트의 인증 장치를 도시한 블록도이다.

도 5는 본 발명의 일 실시예에 따른 액세스 포인트의 인증 방법을 도시한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 도 5의 액세스 포인트의 인증 방법을 상세하게 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 본 발명의 실시예들을 설명하기에 앞서, 종래의 보안 방식을 채택하고 있는 무선 네트워크 환경에서 발생하는 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 개괄적으로 소개하도록 한다. 이하에서, 액세스 포인트는 WLAN 서비스를 제공하는 무선 기지국 단말 장치를 나타내고, 특히 모바일 액세스 포인트는 백본(back-bone) 네트워크로서 유선 LAN을 사용하는 기존의 WLAN 액세스 포인트와는 달리 셀룰러(cellular) 네트워크를 백본 네트워크로서 사용하는 WLAN 모바일 라우터 장치를 나타낸다. 또한, 사용자 단말(User Equipment, UE)은 모바일 액세스 포인트로부터 WLAN 서비스를 제공받는 사용자 장치를 의미하는 것으로, 예를 들어 랩탑(Laptop) 컴퓨터, 스마트폰, 스마트패드 등이 이에 해당한다.
- [0021] WLAN 환경의 대표적인 보안 문제로는 중간자 공격(man in the middle Attack, MITM Attack)이 알려져 있다. 이 공격은 공격자가 해킹 툴(tool)이 탑재된 로그(Rogue) 액세스 포인트를 이용해 WLAN 사용자를 속이고, 사용자 단말과 액세스 포인트 사이의 통신 과정 중간에 개입한 뒤, 둘 사이의 통신을 릴레이(Relay)하며 통신 내용을 도청하거나 변경하는 공격을 말한다. 예를 들어, WLAN 사용자가 자신이 평소에 이용하던 SSID가 "office AP"인 액세스 포인트에 접속하고자 할 경우, 공격자는 로그 액세스 포인트에 동일한 SSID를 할당함으로써 WLAN 사용자로 하여금 로그 액세스 포인트에 접속하도록 유인한 다음, 통신 내용을 도청하면서 WLAN 사용자의 아이디 및 비밀번호 등의 개인 정보를 불법적으로 획득할 수 있다.
- [0022] 이러한 중간자 공격을 차단하기 위해서는 사용자 장치와 액세스 포인트 간의 완전한 상호 인증 구조가 보장되어야 한다. 즉, 사용자 역시 자신이 접속한 액세스 포인트 장치가 자신이 알고 있는 신뢰하는 장치가 맞는지 여부를 확인할 수 있어야 한다.
- [0023] 종래의 WLAN 표준 보안 방식으로는 WPA(Wi-Fi Protected Access) 방식이 존재한다. WPA는 IEEE 802.11i 보안 표준을 구현한 방식으로, 무선 링크 암호 방식에 따라 WPA1과 WPA2로 구분되고, 인증 방식에 따라 WPA-Personal(WPA-PSK) 모드(mode)와 WPA-Enterprise(WPA-802.1X) 모드로 구분된다. 이 중, 중간자 공격과 관련한 각각의 인증 방식의 특징과 그 문제점에 관해 도 1 및 도 2를 참조하여 설명하도록 한다.
- [0024] 도 1은 WLAN 표준 보안 방식 중, WPA-Personal 모드에서 발생할 수 있는 중간자 공격 등의 보안 문제를 설명하기 위한 도면이다. WPA-Personal 모드는 개인이 운영하는 소규모의 WLAN 환경을 위한 보안 모드로서, 사용자 단말(UE) 및 액세스 포인트(AP) 간의 인증 방식으로 사전 공유 키(Pre-shared Key)를 이용한 인증 방식을 사용한다. 즉 사용자 단말과 액세스 포인트는 도 1에서와 같이 사전에 동일한 키 값을 공유하고 있어야 한다. 그리고, 인증 과정에서는 각각 상대방이 자신과 동일한 키를 소유하고 있는지를 확인하여 상대를 인증한다. 이 방식은 사용자 단말 및 액세스 포인트 간의 상호 인증이 불가능하여, 로그 액세스 포인트(Rogue AP)를 이용한 중간자 공격에 취약하다. 이하에서 그 이유를 보다 구체적으로 설명한다.
- [0025] WPA-Personal 보안 모드에서 사용하는 공유 키 기반의 인증 절차에서, 사용자 단말(UE)과 액세스 포인트(AP)는 사전에 동일한 키 값을 공유하고 있다고 가정한다. 사용자 단말 및 액세스 포인트 간의 초기 접속 단계가 완료되면, 곧바로 사용자 단말 및 액세스 포인트 간의 인증 단계가 수행된다. 이 과정에서 사용자 단말과 액세스 포인트 각각은 자신이 알고 있는 공유 키를 이용해 페어와이즈 마스터 키(Pairwise Master Key, PMK)를 생성하고, 핸드셰이킹(4-way handshake) 절차를 수행하여 상대방이 자신과 동일한 PMK를 소유하고 있는지 여부를 확인함으로써 상대방을 인증한다.
- [0026] 그러나, 이러한 WPA-Personal 보안 모드에 따른 방식은 사용자 단말이 자신이 접속한 액세스 포인트가 과연 신뢰할만한 장치인지 아닌지를 구분할 수 있는 방법을 제공해주지 못한다. 또한, 모든 사용자가 동일한 비밀 키를 사용하기 때문에 비밀 키 유출의 경우 보안에 대한 위험이 매우 크기 때문에, 중간자 공격에 취약하다. 예를 들어, 도 1에서와 같이 하나의 액세스 포인트를 공유하고 있는 다수의 사용자들 중 한 명이 다른 사용자를 기만할 목적으로 자신이 소유한 해킹용 액세스 포인트(Rogue AP) 디바이스에 공유 액세스 포인트(AP)와 동일한 SSID 및 공유 키를 설정하여 다른 사용자를 유인한다면, 이 사실을 알 수 없는 다른 사용자는 공격에 쉽게 노출될 수 밖에 없다.

- [0027] 도 2는 WLAN 표준 보안 방식 중, WPA-Enterprise 보안 모드에서 발생할 수 있는 중간자 공격 등의 보안 문제를 설명하기 위한 도면이다. WPA-Enterprise 보안 모드는 중대형 규모의 WLAN 환경을 위한 보안 모드로서, 사용자 단말(UE) 및 액세스 포인트(AP) 간의 상호 인증을 위해 IEEE 802.1x 인증 구조를 사용한다. 이 방식은 WPA-Personal Mode와는 달리 사용자 단말 및 액세스 포인트 간의 인증에 사전 공유 키를 사용하지 않고, 사용자 단말(UE) 및 인증 서버(RADIUS 서버) 간의 인증 결과로 생성된 세션 키(session key)를 이용한다. 이 방식은 사용자 단말에게 자신이 접속한 액세스 포인트를 인증할 수 있는 수단을 제공하기 때문에, 종래의 WLAN 환경에서는 일정 수준으로 로그 액세스 포인트(Rogue AP)를 이용한 중간자 공격의 차단을 기대할 수 있었으나, 여전히 보안상의 한계점을 가진다. 이하에서 그 이유를 보다 구체적으로 설명한다.
- [0028] 앞서 소개한 바와 같이 WPA-Enterprise 보안 모드는 사용자 수준의 인증과 사용자 단말(UE) 및 액세스 포인트(AP) 간의 상호 인증을 제공하기 위해 IEEE 801.x 인증구조를 사용한다. 이 방식은 별도의 인증 서버(RADIUS server)를 통해 사용자와 서버가 상호 인증을 하고, 그 결과로 인해 생성되는 세션 키(Master Session Key, MSK)를 이용해 사용자 단말 및 액세스 포인트 간의 인증 절차를 수행한다. 도 2의 [A]를 참고하여 단계별 인증 절차를 소개하면 다음과 같다.
- [0029] 우선, 사용자 단말과 인증 서버는 TLS 프로토콜을 이용해 상호 인증을 수행한다. 그리고 상호 인증 과정에서 교환한 비밀 키(Master Secret)를 이용해 각각 세션 키(MSK)를 생성한다. 그런 다음, 인증 서버는 생성된 세션 키(MSK)를 액세스 포인트와의 공유 비밀 키(Shared Secret)(또는 공유 비밀번호 등이 될 수 있다.)로 암호화하여 액세스 포인트에 전달한다. 그러면, 액세스 포인트는 공유 비밀 키(Shared Secret)를 이용하여 수신된 암호문을 복호하여 사용자 단말과 인증 서버가 공유하고 있는 세션 키(MSK)를 확보한다. 이제, 사용자 단말과 액세스 포인트는 각각 소유한 세션 키(MSK)를 이용해 페어와이즈 키(PMK)를 생성하고, 핸드셰이킹(4-way handshake) 절차를 수행함으로써 상대를 인증한다. 이상의 과정은 앞서 소개한 WPA-Personal 보안 모드에서의 절차와 동일하다.
- [0030] 종래의 WPA 보안 방식에서 중간자 공격을 차단하기 위해서는 WPA-Enterprise 모드 보안 방식을 적용해야 했다. 그러나 이러한 WPA-Enterprise 모드 보안 방식 역시 다음과 같은 보안 한계점이 존재한다.
- [0031] (1) 첫 번째 보안 위험 : 종래의 WPA-Enterprise 모드 보안 방식에서 사용자 단말이 액세스 포인트를 인증하는 과정은 자신이 접속한 액세스 포인트가 자신과 TLS 기반의 상호 인증을 수행한 인증 서버와 공유 비밀 키(Shared Secret)를 공유하고 있는지 여부를 확인하는 절차이다. 즉, 인증 서버는 세션 키(MSK)를 액세스 포인트에 전달하는 과정에서 자신과 액세스 포인트가 공유하고 있는 공유 비밀 키를 이용해 암호화하여 전달한다. 따라서, 공유 비밀 키를 알고 있는 액세스 포인트만이 암호문으로부터 세션 키(MSK)를 복호화할 수 있기 때문에 사용자 단말 및 액세스 포인트 간의 세션 키(MSK) 기반의 인증 절차는 사용자 단말의 입장에서 액세스 포인트가 서버의 공유 비밀 키를 알고 있는지 여부를 확인하는 과정이라고 볼 수 있다. 결론적으로, WPA-Enterprise 모드 보안 방식에서는 공유 비밀 키를 알 경우 누구나 로그 액세스 포인트(Rogue AP)를 구성할 수 있다는 문제점이 존재한다.
- [0032] (2) 두 번째 보안 위험 : 종래 WPA-Enterprise 모드 보안 방식은 공유 비밀 키(Shared Secret)의 유출 위험이 매우 높다. 액세스 포인트 디바이스의 공유 비밀 키는 소유자(관리자)에 의해 배포되고 입력될 뿐만 아니라, 디바이스 내부에서 평문으로 저장된다. 보안 분야에서 널리 알려진 바와 같이, 사람에 의한 키 배포 및 관리는 안전을 보장하기 어렵다. 만약 관리자 혹은 디바이스 소유자에 의해 액세스 포인트 디바이스에 설정된 공유 비밀 키가 유출된다면, 동일한 공유 비밀 키를 사용하는 WLAN 네트워크에 속하는 디바이스들은 더 이상의 보안을 기대하기 힘들다.
- [0033] 나아가, 모바일 액세스 포인트를 사용하는 WLAN 환경은 종래의 유선 네트워크 기반의 WLAN 환경과는 달리 다음과 같은 추가적인 보안 위험이 두 가지 더 존재한다.
- [0034] (3) 세 번째 보안 위험 : 종래의 유선 네트워크 기반의 WLAN 환경에서 액세스 포인트는 특정 네트워크에 종속적이고 이동이 불가능하였다. 따라서, LAN 스위치를 이용한 액세스 포인트 디바이스의 MAC 주소 인증과 같이 네트워크 환경이 제공하는 추가적인 보안 수단 또는 설치 환경이 제공하는 환경적/물리적인 보안 수단을 기대할 수 있었다. 따라서, 액세스 포인트 디바이스에 대한 최소한의 신뢰성이 보장되기 때문에, 기존의 WPA-Enterprise 보안 방식만으로도 중간자 공격에 대한 안전성을 기대할 수 있었다. 그러나, 모바일 액세스 포인트는 휴대가 가능한 소형 디바이스이기 때문에 그러한 환경적인 보안 요소를 기대할 수 없을 뿐만 아니라, 디바이스 해킹에 항상 노출되어 있기 때문에 디바이스를 신뢰할 수 없다.
- [0035] (4) 네 번째 보안 위험 : 모바일 액세스 포인트는 종래의 유선 네트워크에 기반한 액세스 포인트와는 달리 개인

소유의 휴대 디바이스이다. 따라서, 종래와 같이 모바일 액세스 포인트 인증 서버와의 공유 비밀 키를 사용자가 직접 입력해야 하고, 또한 디바이스 내부에 평문으로 저장해야 한다면, 공유 비밀 키는 디바이스에 대한 모든 권한을 갖는 소유자에게 노출될 수 밖에 없다. 따라서, 공유 비밀 키의 안전한 배포, 저장 및 회수가 보장되지 않는 종래의 WPA-Enterprise 보안 방식으로는 모바일 액세스 포인트 환경에서 중간자 공격을 차단하기 어렵다.

[0036] 도 2의 [B]를 참고하여 이러한 공격에 대한 가상 시나리오를 검토해보자. 예를 들어, 어느 기업이 외부 출장이 잦은 영업사원들의 업무지원을 위해 모바일 액세스 포인트를 배포해주고 보안을 위해 WPA-Enterprise 보안 방식을 적용한 WLAN 환경을 사용하고 있다고 가정하자. 이 경우, 회사로부터 모바일 액세스 포인트를 배급받은 직원이 제공된 디바이스를 해킹하여 회사 내 인증 서버의 공유 비밀 키(Shared Secret)를 분석한 다음, 자신이 소유한 해킹용 액세스 포인트(Rogue AP)에 동일한 공유 비밀 키를 설정하여 네트워크를 구성하고, 다른 사원의 접속을 유도함으로써 통신 내용을 도청할 수 있다. 이 때, 피해자인 다른 사원은 자신이 접속한 모바일 액세스 포인트가 회사의 서버로부터 인증된 액세스 포인트이기 때문에 해당 모바일 액세스 포인트가 해킹용 액세스 포인트(Rogue AP)인지 여부를 전혀 인지할 수 없다. 왜냐하면, 도 2의 [B]에서 해킹용 액세스 포인트는 사용자 단말과 인증 서버 간의 인증 과정에서 생성된 세션 키(MSK)를 알고 있기 때문이다.

[0037] 따라서, 상기된 보안 위험을 해소하기 위해 다음과 같이 모바일 액세스 포인트를 이용하는 WLAN 환경에서의 보안 요구 사항을 고려할 필요가 있다.

[0038] (1) 첫 번째 보안 요구 사항 : WPA-Enterprise 보안 모드에서 인증 서버는 모바일 액세스 포인트를 유일하게 식별할 수 있어야 하며, 식별에 사용되는 값은 변경 및 복제가 불가능하고 모바일 액세스 포인트 디바이스의 운영체제(OS) 해킹으로부터 영향을 받지 않아야 한다.

[0039] (2) 두 번째 보안 요구 사항 : WPA-Enterprise 보안 모드에서 서버의 모바일 액세스 포인트 인증에 사용되는 키(key)는 디바이스마다 유일해야 하며, 디바이스 소유자라도 변경 및 복제할 수 없어야 한다.

[0040] (3) 세 번째 보안 요구 사항 : WPA-Enterprise 보안 모드에서 사용자는 서버의 액세스 포인트 인증 및 세션 키(MSK) 전달 과정에 전혀 개입할 수 없어야 하며, 이는 액세스 포인트의 소유자라도 불가능해야 한다.

[0041] (4) 네 번째 보안 요구 사항 : WPA-Enterprise 보안 모드에서 인증 서버는 WLAN 서비스를 제공하는 디바이스가 해킹된 디바이스(해킹을 위해 변조되거나 해킹코드가 탑재된 디바이스를 포함한다.)인지 아닌지 여부를 검증할 수 있어야 한다. 이후에 보다 구체적으로 설명한 것이나, 이러한 검증을 위해 인증 서버는 최초에 모바일 액세스 포인트의 디바이스 인증 과정에서 사용되는 해쉬(hash) 값을 가지고 있는 것이 바람직하다.

[0042] 상기된 보안 요구 사항을 종합적으로 고려하여 이하에서 기술되는 본 발명의 실시예들은 사용자, 운영체제 및 소프트웨어 기반의 어플리케이션의 실행 환경과 독립된 하드웨어 기반의 인증 체계를 제안한다. 이하에서, 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0043] 도 3은 액세스 포인트 및 사용자 단말 간의 상호 인증을 보장하기 위하여 본 발명의 실시예들이 제안하는 액세스 포인트의 인증 장치를 예시한 도면으로서, 하드웨어 인증 모듈(27)을 이용하여 모바일 액세스 포인트의 인증을 처리하는 기술을 제안하고 있다.

[0044] 모바일 액세스 포인트(20)와 사용자 단말(10) 간의 안전한 상호 인증을 보장하기 위하여 도 3의 제안 방식에서는 하드웨어 인증 모듈(27)을 이용한 IEEE 802.1x 인증 방식을 사용한다. 종래의 보안 방식에서 발생하는 문제점들은 근본적으로 인증 서버가 액세스 포인트 디바이스를 인증하는데 사용되는 공유 비밀 키가 모바일 액세스 포인트에 안전하게 배포, 회수 내지 저장되지 않는다는 점에 있다. 따라서, 도 3의 제안 방식에서는 인증 서버(30)가 모바일 액세스 포인트(20)에 구비된 하드웨어 인증 모듈(27)을 통해 인증 절차를 수행하도록 함으로써 모바일 액세스 포인트(20)의 사용자(소유자)가 인증 과정과 인증에 사용되는 키 값에 원천적으로 접근할 수 없도록 구성하였다.

[0045] 인증 서버(30)와 모바일 액세스 포인트(20)의 인증 과정에서 하드웨어 인증 모듈(27)의 역할은 크게 ① 디바이스 인증과 ② MSK의 안전한 전달이다. 즉, 인증 서버(30)는 접속을 요청하는 모바일 액세스 포인트(20)를 하드웨어 인증 모듈(27)을 통해 유일하게 식별 및 인증하고, 오직 인증된 모바일 액세스 포인트(20)에게만 사용자 단말 및 인증 서버 간의 상호 인증을 허용한다.

[0046] 이를 위해, 인증 서버(30)는 액세스 포인트(20)에 구비된 하드웨어 인증 모듈(27)이 제공하는 고유 식별자

(Universal Identifier, SN)에 대해 자신이 가지고 있는 고유 식별자 리스트에 그 값이 포함되어 있는지 여부를 검사하고, 검사된 고유 식별자가 하드웨어 인증 모듈(27)에 의해 프로그램된 것이 맞는지 여부를 확인하기 위해 하드웨어 인증 모듈(27)의 공개키 인증서에 포함된 고유 식별자를 확인한다. 또한, 공개 키에 대응되는 비밀 키를 하드웨어 인증 모듈(27)이 소유하고 있는지 여부를 확인하기 위해 이를 검증하는 과정(이후 도 6을 통해 구체적으로 소개하는 challenge-response를 주고 받는 과정에 해당한다.)을 수행하게 된다. 이상의 과정은 결국 (고유 식별자)-(공개 키 인증서)-(하드웨어 인증 모듈) 간의 상관 관계를 규명하기 위한 일련의 절차에 해당하는 것이다.

[0047] 한편, 디바이스의 무결성 검증과 관련하여, 모바일 액세스 포인트(20)는 인증 과정에서 하드웨어 인증 모듈(27)을 이용해 모바일 액세스 포인트(20)에서 실행되는 소프트웨어 이미지의 해쉬(hash) 값을 검사하여 디바이스의 무결성을 확인할 수 있을 것이다. 특히, 하드웨어 인증 모듈(27)이 인증 서버(30)의 요청에 의해 산출된 해쉬(hash) 값을 응답(response)에 포함하여 인증 서버(30)에 전송하면, 인증 서버(30)는 수신된 해쉬 값을 검사함으로써 원격으로 액세스 포인트(20)의 무결성을 판단하는 것이 가능하다.

[0048] 나아가, 상호 인증의 결과로 생성된 세션 키(MSK)를 액세스 포인트(20)에 전달하는 과정에서도 해당 세션 키를 암호화하여 전송함으로써, 오직 디바이스 인증 과정에 사용된 하드웨어 인증 모듈(27)만이 세션 키를 복호할 수 있도록 한다.

[0049] 이러한 하드웨어 인증 모듈(27)은 앞서 소개한 보안 요구 사항을 만족하는 것으로서, 모바일 액세스 포인트(20)마다 유일한 값으로서 변경이 불가능하도록 설정된 고유의 비밀 키를 기록한다. 또한, 디바이스 인증 과정과 세션 키의 전달 과정에서, 모바일 액세스 포인트(20)는 미리 정의된 제어 명령에 의해서만 하드웨어 인증 모듈(27)과 상호작용하여 고유의 비밀 키에 접근 가능하고, 암호화 과정을 통해서만 하드웨어 인증 모듈(27)로부터 고유의 비밀 키를 독출할 수 있다.

[0050] 이러한 하드웨어 인증 모듈(27)은 다양한 형태로 구현될 수 있으나, 도 3을 통해 예시된 구성을 소개하면 다음의 표 1과 같다.

표 1

구성 요소	내용
버스 인터페이스 (Bus Interface)	디바이스의 다른 모듈들과 버스를 통해 통신하기 위한 인터페이스를 나타낸다.
고유 식별자 (Universal Identifier, SN)	각각의 하드웨어 인증 모듈(즉, 모바일 액세스 포인트를 의미한다.)을 유일하게 식별하기 위한 식별자 혹은 일련번호 값을 의미한다.
비밀 키 (Secret Key)	모든 하드웨어 인증 모듈은 유일한 비대칭 키 쌍을 소유하고 있다. 이 중 비밀 키는 보안 모듈 내부에 안전하게 저장되어 외부의 접근 및 변경이 불가능하다.
비대칭 키 암호화/복호화 모듈 (Asymmetric Key Encryption/Decryption Module)	비대칭 키 암호화/복호화 연산을 수행하는 암호 장치로서, RSA 또는 ECC와 같은 비대칭 키 암호 함수가 구현된 하드웨어 모듈로 구현될 수 있다.
해쉬 엔진 (Hash Engine)	SHA-1 또는 SHA-256과 같이 암호학적인 메시지 다이제스트(Message Digest) 연산을 수행하는 장치로서, 모바일 액세스 포인트의 소프트웨어 구성 요소들의 해쉬 값을 연산하는데 사용된다.

[0052] 한편, 모바일 액세스 포인트(20)는 이에 구비된 하드웨어 인증 모듈(27)이 소유한 비밀 키(Secret Key)에 대응되는 공개 키에 대한 인증서(예를 들어, X.509 인증서가 될 수 있다.)를 소유한다. 이 인증서에는 하드웨어 인증 모듈(27)의 공개 키와 더불어 고유 식별자(Universal Identifier, SN)의 값이 CA(Certificate Authority)에 의해 서명(Sign)되어 있다. 따라서, 인증서를 수신한 인증 서버(30)는 CA와의 인증서 검증 절차를 수행함으로써, 인증서에 포함된 공개 키와 디바이스(20)의 고유 식별자에 대한 진위 여부를 확인할 수 있다.

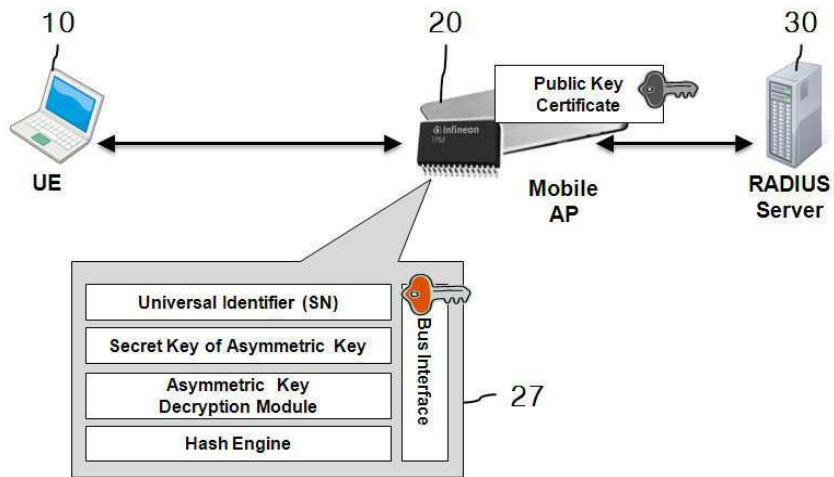
[0053] 도 4는 본 발명의 일 실시예에 따른 사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트의 인증 장치를 도시한 블록도로서, 앞서 소개한 도 3의 모바일 액세스 포인트(20)의 구성을 기능 단위로 표현한 도면이다. 여기서 사용자 단말(미도시), 액세스 포인트(20) 및 인증 서버(미도시)는 WPA-Enterprise 보안 모드에 따른 인증 구조를 사용하여 동작하는 것이 바람직하다.

- [0054] 통신부(21)는 사용자 단말 및 인증 서버와 통신하는 장치로서, 모바일 액세스 포인트 기술 분야에서 활용되고 있는 다양한 통신 수단이 활용될 수 있다.
- [0055] 인증 처리부(23)는 액세스 포인트(20)와 인증 서버(미도시) 간의 인증 및 액세스 포인트(20)와 사용자 단말(미도시) 간의 상호 인증을 처리한다. 이러한 인증 처리부(23)는, 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 인증 서버를 통해 상기 액세스 포인트 자신을 인증하고, 상기 액세스 포인트의 인증에 기반하여 상기 사용자 단말과 상기 인증 서버가 상호 인증을 통해 세션 키를 생성하면, 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화하며, 상기 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증하게 된다.
- [0056] 여기서, 인증 처리부(23)는, 액세스 포인트(20)마다 유일한 값으로서 변경이 불가능하도록 상기 고유의 비밀 키를 기록하는 하드웨어 인증 모듈(27)을 구비한다. 또한, 인증 처리부(23)는, 미리 정의된 제어 명령에 의해서만 상기 하드웨어 인증 모듈(27)과 상호작용하여 상기 고유의 비밀키에 접근 가능하고, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈(27)로부터 상기 고유의 비밀키를 독출할 수 있는 제어부(25)를 더 포함하는 것을 바람직하다. 이러한 하드웨어 인증 모듈(27) 및 제어부(25)는 액세스 포인트(20) 사용자에게 의한 임의적인 비밀 키 접근 및 변조를 방지하는 기술적 수단이 된다.
- [0057] 액세스 포인트 자신을 인증함에 있어서 인증 처리부(23)는, 액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버와 함께 인증서 요청을 수신하고, 암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하며, 상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호화하도록 함으로써 상기 액세스 포인트 자신을 인증한다. 여기서, 상기 인증 서버는 상기 액세스 포인트 식별자 및 상기 고유의 비밀 키를 통해 상기 액세스 포인트를 유일하게 식별할 수 있다. 또한, 상기 인증 서버는 상기 액세스 포인트로부터 수신된 상기 인증서에 포함된 공개 키를 이용하여 상기 암호화된 랜덤 넘버를 복호화하고, 최초로 상기 인증 서버가 생성한 랜덤 넘버와 비교함으로써 유효성 검사를 수행하는 것이 바람직하다.
- [0058] 세션 키를 복호화함에 있어서 인증 처리부(23)는, 상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하고, 복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화한다.
- [0059] 사용자 단말과 상호 인증을 위해 인증 처리부(23)는, 상기 복호화된 세션 키를 이용하여 페어와이즈 키를 생성하고, 상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹함으로써 상호 인증한다.
- [0060] 도 5는 본 발명의 일 실시예에 따른 사용자 단말에 무선 네트워크 서비스를 제공하는 액세스 포인트의 인증 방법을 도시한 흐름도로서, 앞서 소개한 도 4의 인증 장치들의 개별 구성 요소들의 수행 동작들에 대응하는 구성을 제안하고 있으므로, 여기서는 설명의 중복을 피하기 위해 그 개요만을 약술하도록 한다.
- [0061] 510 단계에서, 사용자 단말로부터 접속을 요청받은 액세스 포인트는 상기 액세스 포인트 고유의 비밀 키(secret key)를 이용하여 인증 서버를 통해 상기 액세스 포인트 자신을 인증한다. 여기서, 고유의 비밀키는, 액세스 포인트마다 유일한 값으로서, 변경이 불가능하도록 액세스 포인트 내의 하드웨어 인증 모듈에 기록되고, 미리 정의된 제어 명령에 의해서만 접근 가능하며, 암호화 과정을 통해서만 상기 하드웨어 인증 모듈로부터 독출된다.
- [0062] 보다 구체적으로, 액세스 포인트 자신을 인증하는 510 단계는, 상기 액세스 포인트가 액세스 포인트 식별자를 이용하여 상기 인증 서버에게 접근을 요청하고, 상기 인증 서버로부터 랜덤 넘버(random number)와 함께 인증서 요청을 수신하고, 상기 액세스 포인트가 암호화 명령에 따라 상기 고유의 비밀 키를 이용하여 상기 수신된 랜덤 넘버를 암호화하며, 상기 액세스 포인트가 상기 암호화된 랜덤 넘버와 상기 고유의 비밀 키에 대응하는 공개 키가 포함된 인증서를 상기 인증 서버에 전송하여 복호화하도록 함으로써 상기 액세스 포인트 자신을 인증함으로써 수행된다.
- [0063] 520 단계에서, 상기 510 단계를 통한 액세스 포인트의 인증에 기반하여 사용자 단말과 인증 서버가 상호 인증을 통해 세션 키(session key)를 생성하면, 액세스 포인트는 상기 인증 서버로부터 암호화된 세션 키를 수신하여 상기 고유의 비밀 키를 이용하여 복호화한다. 즉, 520 단계는, 상기 액세스 포인트가 상기 인증 서버로부터 수신한 세션 키를 상기 액세스 포인트 내의 하드웨어 인증 모듈에 전달하고, 복호화 명령에 따라 상기 하드웨어 인증 모듈에 기록된 상기 액세스 포인트 고유의 비밀 키를 이용하여 상기 암호화된 세션 키를 복호화함으로써 수행된다.

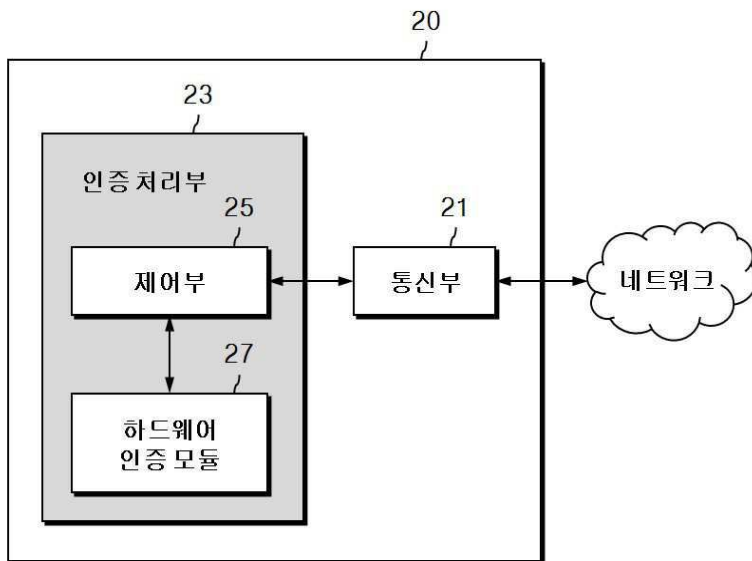
- [0064] 530 단계에서, 액세스 포인트는 상기 520 단계를 통해 복호화된 세션 키를 이용하여 상기 사용자 단말과 상호 인증한다. 즉, 530 단계는, 상기 액세스 포인트가 상기 복호화된 세션 키를 이용하여 페어와이즈 키(pairwise key)를 생성하고, 상기 액세스 포인트가 상기 생성된 페어와이즈 키를 이용하여 상기 사용자 단말과 핸드셰이킹(handshaking)함으로써 상호 인증함으로써 수행된다.
- [0065] 도 6은 본 발명의 일 실시예에 따른 도 5의 액세스 포인트의 인증 방법을 상세하게 도시한 도면으로서, 여기서는 ① 디바이스 인증 과정 및 ② 세션 키 전달 과정에 집중하여 그 차별적 특징을 설명하도록 한다.
- [0066] **(1) 모바일 액세스 포인트 디바이스의 인증 과정**
- [0067] 사용자 단말(10) 및 모바일 액세스 포인트(20) 간의 초기 접속 절차가 완료되면, 모바일 액세스 포인트(20)는 인증 서버(30)에 인증하기 위해 하드웨어 인증 모듈을 이용한 디바이스 인증 절차(도 6의 610 단계 내지 660 단계)를 시작하는데, 그 구체적인 과정은 다음과 같다.
- [0068] 610 단계에서, 모바일 액세스 포인트(20)는 인증 서버(30)에 접속 요청을 보낸다. 이 때, 디바이스의 고유 식별 번호인 SN를 함께 전송한다.
- [0069] 620 단계에서, 인증 서버(30)는 수신된 SN를 이용하여 접속을 요청한 모바일 액세스 포인트(20) 디바이스가 자신이 알고 있는 장치인지 여부를 확인한다. 이를 위해 인증 서버(30)는 미리 유효한 SN에 대한 리스트를 보유하고 있는 것이 바람직하다. 그런 다음, 인증 서버(30)는 모바일 액세스 포인트 인증을 위한 일종의 랜덤 넘버(Challenge, Random Number)를 생성한다.
- [0070] 630 단계에서, 인증 서버(30)는 620 단계를 통해 생성된 랜덤 넘버를 모바일 액세스 포인트(20)에 전송하고 하드웨어 인증 모듈의 공개 키 인증서를 요청한다. 이 때, 이러한 인증 서버의 요청을 받은 모바일 액세스 포인트(20)는 수신된 랜덤 넘버를 하드웨어 인증 모듈에 전달하고, 응답(Response) 생성을 요청한다.
- [0071] 640 단계에서, 모바일 액세스 포인트(20)에 구비된 하드웨어 인증 모듈은 응용 프로그램의 부트 이미지(boot image)를 포함하여 모바일 액세스 포인트(20)에서 실행되고 있는 소프트웨어의 해쉬 값을 산출한다. 그리고, 이 값을 인증 서버(30)가 생성한 랜덤 넘버와 자신이 소유한 비밀 키를 사용해 서명(Sign)함으로써 응답(Response) 메시지를 생성한다. 즉, 자신의 비밀 키로 랜덤 넘버를 암호화한다.
- [0072] 650 단계에서, 모바일 액세스 포인트(20)는 하드웨어 인증 모듈이 생성한 응답과 자신의 공개 키 인증서를 인증 서버(30)에 전송한다.
- [0073] 660 단계에서, 인증 서버(30)는 모바일 액세스 포인트(20)로부터 수신한 공개 키 인증서를 검증한다. 이 때, 인증서에 포함된 모바일 액세스 포인트(20)의 SN가 앞서 610 단계에서 전송된 것과 같은 값인지 여부를 검사한다. 그리고, 인증서에 포함된 하드웨어 인증 모듈의 공개 키를 이용하여 응답 메시지를 복호화함으로써 검증한다. 이 과정에서 모바일 액세스 포인트(20)가 생성한 응답 메시지가 자신이 630 단계에서 생성한 랜덤 넘버를 사용하였는지를 확인함으로써 모바일 액세스 포인트(20)를 검증할 수 있다. 즉, 모바일 액세스 포인트(20)가 SN의 소유자가 맞고 그에 대응되는 비밀 키를 소유한 하드웨어 인증 모듈이 장착된 장치가 맞는지 여부를 확인하게 된다. 이제, 오직 검증이 완료된 경우에만 사용자 단말(10) 및 인증 서버(30) 간의 상호 인증 절차를 시작하게 된다.
- [0074] **(2) 세션 키(MSK) 전달 과정**
- [0075] 이상에서 설명한 사용자 단말(10) 및 모바일 액세스 포인트(20) 간의 디바이스 인증 과정이 완료되면, 사용자 단말(10) 및 인증 서버(30)는 TLS 기반의 상호 인증 절차를 수행한다. 그리고, 상호 인증이 완료되면 인증 서버(30)는 상호 인증 과정에서 생성된 세션 키(MSK)를 모바일 액세스 포인트(20)에 암호화하여 전달한다. 이 과정은 다음과 같다.
- [0076] 670 단계에서, 인증 서버(30)는 사용자 단말(10)과의 TLS 기반 상호 인증 절차에서 생성된 세션 키(MSK)를 모바일 액세스 포인트(20)의 공개 키 인증서에 포함된 공개 키를 이용해 암호화한다.
- [0077] 680 단계에서, 인증 서버(30)는 암호화된 세션 키를 모바일 액세스 포인트(20)에 전달한다. 이 때, 모바일 액세스 포인트(20)는 수신받은 암호화된 세션 키를 하드웨어 인증 모듈에 전달한다.

- [0078] 690 단계에서, 하드웨어 인증 모듈은 자신이 소유한 비밀 키를 사용하여 암호화된 세션 키를 복호화한다.
- [0079] 700 단계에서, 모바일 액세스 포인트(20)는 하드웨어 인증 모듈을 이용해 복호화한 세션 키를 사용해 페어와이즈 키(PMK)를 생성한 다음, 사용자 단말(10) 및 모바일 액세스 포인트(20) 간의 상호 인증을 절차를 수행한다.
- [0080] 이상에서 본 발명의 다양한 실시예들에 따른 모바일 액세스 포인트의 보안 장치 및 방법에 대해 설명하였다. 종래의 WPA-Enterprise 보안 방식에서는 WLAN 핫스팟 구성을 위해 설치되는 모든 액세스 포인트 디바이스에 공유 비밀 키(Shared Secret)를 할당해야만 했다. 그 결과 공유 비밀 키를 할당 또는 배포하는 과정에서 키 값이 유출될 가능성이 매우 컸고, 공유 비밀 키는 디바이스에 평문 형태로 저장되기 때문에 액세스 포인트 디바이스에 대한 모든 권한을 갖는 소유자에게 노출될 수 밖에 없는 위험을 안고 있었으며, 일단 할당된 키는 회수가 불가능하기 때문에 키가 유출되면 동일한 키를 사용하는 네트워크의 모든 액세스 포인트에 영향을 미치는 한계를 가지고 있었다.
- [0081] 이에 반해, 본 발명의 실시예들을 통해 제안된 보안 방식에서는 인증 서버의 액세스 포인트 인증에 공유 비밀 키를 사용하지 않고, 모바일 액세스 포인트에 구비된 하드웨어 인증 모듈에 기록된 비대칭 키를 이용하는 공개 키 기반 인증 방식을 적용하였다. 따라서, 모바일 액세스 포인트 디바이스에 공유 비밀 키를 관리자가 수작업으로 할당할 필요가 없어 키 유출의 위험이 없고, 비대칭 키 쌍 중 비밀키는 하드웨어 보안 칩셋 내부에 존재하여 외부 접근이 불가능하며, 디바이스 소유자라도 키 값을 알 필요가 없다는 장점을 갖는다. 또한, 공개 키 기반 구조의 특성상 CA에 의한 인증서 폐기가 가능하고, 각각의 하드웨어 인증 모듈은 고유의 식별 번호 및 고유의 비대칭 키 쌍을 갖고 있기 때문에, 비록 하나의 디바이스의 키 값이 유출된다고 할지라도 다른 모바일 액세스 포인트의 안전성에 전혀 영향을 미치지 않는다.
- [0082] 최근 LTE 기반의 4세대 통신 서비스가 시작된 이후로 모바일 라우터의 종류와 판매 대수가 급격히 증가하고 있다. 또한, 향후 무선 백본 네트워크 구축을 목표로 하고 있는 LTE-A 통신 서비스가 시작된다면, 그 수는 더욱 증가할 것으로 예상된다. 이러한 전망 속에서 만일 기업, 공공단체, 학교 등 일정 규모 이상의 단체가 모바일 라우터를 이용해 WLAN 핫스팟을 구성하기 위해서는 앞서 논의된 바와 같은 보안 관련 요구사항을 충족할 수 있는 기술적 수단이 필수적이며, 이상에서 제안된 본 발명의 실시예들을 통해 이러한 기술 수요를 충족시킬 수 있다.
- [0083] 또한, KT, SK와 같은 국내 사업자들은 물론 Verizon과 같은 국외 무선 통신 사업자들은 새로운 사업 모델로 전용 회선으로 구성된 가내 네트워킹 환경을 모바일 라우터로 이용하는 무선 네트워크 환경으로 대체하는 방안을 계획하고 있다. 이러한 사업이 현실화되기 위해서는 모바일 액세스 포인트 디바이스의 인증이 필수적이므로 본 발명의 실시예들의 채택이 기대되는 바이다.
- [0084] 나아가, 본 발명의 실시예들이 채택하고 있는 보안 방식은 모바일 액세스 포인트를 활용한 무선 네트워크 환경 뿐만 아니라, 종래의 유선 네트워크 기반의 WLAN 환경에도 적용 가능하다. 앞서 언급한 바와 같이 종래의 WLAN 보안 방식은 환경적/물리적 보안 요소의 도움이 요구되는 불완전한 방식이다. 만약 기존 WLAN 환경에서도 이상에서 제안된 본 발명의 실시예들을 적용할 경우 이러한 환경적/물리적 보안 요소에 의지하지 않더라도 그 자체로 중간자 공격으로부터 안전하며 신뢰도 높은 보안 수단을 제공할 수 있다.
- [0085] 요약하건대, 상기된 본 발명의 실시예들에 따르면, 무선 액세스 포인트의 고유의 비밀 키를 변경 및 복제가 불가능하도록 하드웨어 인증 모듈에 기록하고 이를 통해 액세스 포인트의 인증을 수행함으로써, 중간자 공격에 강인할 뿐만 아니라 무선 액세스 포인트의 비밀 키의 유출을 원천적으로 차단할 수 있고, 비밀 키의 고유성으로 인해 키 유출이 다른 액세스 포인트의 보안에 영향을 미치지 않으며, 그 결과 무선 액세스 포인트 보안의 신뢰도를 향상시킬 수 있다.
- [0086] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- [0087] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

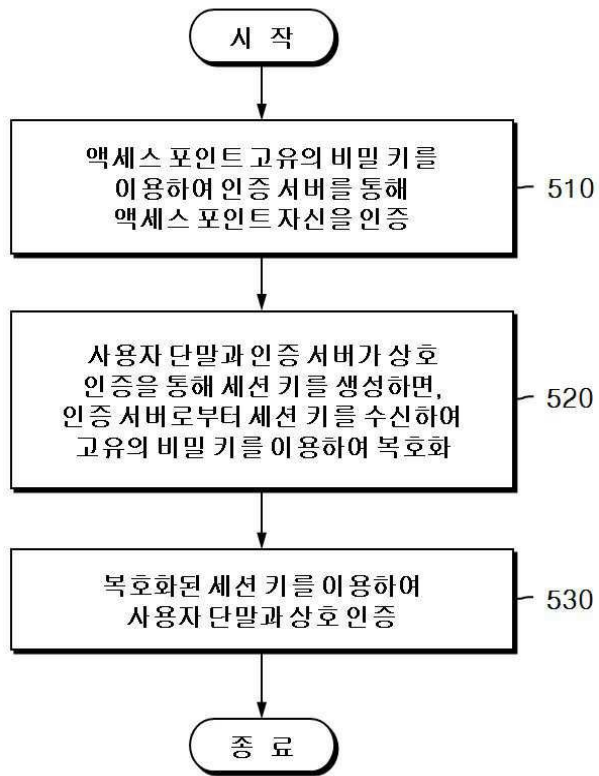
도면3



도면4



도면5



도면6

