(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/30
H04L 9/08
H04L 9/32

(11) 공개번호 10-2005-0116821
(43) 공개일자 2005년12월13일

(21) 출원번호 10-2005-7017159
(22) 출원일자 2005년09월13일
번역문 제출일자 2005년09월13일
(86) 국제출원번호 PCT/US2004/007403
국제출원일자 2004년03월11일
(87) 국제공개번호 WO 2004/084458
국제공개일자 2004년09월30일

(30) 우선권주장 60/454,542 2003년03월14일 미국(US)

(71) 출원인 톰슨 라이센싱
프랑스 92648 블로뉴 세데 께 알퐁스 르 갈로 46

(72) 발명자 장, 준비아오
미국 08807 뉴저지주 브리지워터 제나 드라이브 20
마추어, 사우라브흐
미국 08536 인디애나주 플래인보로 콰일 리지 드라이브 4923
모디, 사친
미국 08648 뉴저지주 로렌스빌 화이트 파인 서클 708

(74) 대리인 주성민
백만기
전경석

심사청구 : 없음

(54) 보안 리키잉과 로그 오프를 이용한 WLAN 세션 관리기술

요약

본 발명은, 사용자 인증 단계 동안, 무선 사용자 머신과 WLAN 액세스 포인트 둘 다에, 초기 세션 키인 1개의 공유 비밀 대신 2개의 공유 비밀을 인스톨함으로써, WLAN 환경에 있는 이동 단말기의 보안성을 개선하기 위한 방법을 제공한다. 공유 비밀 중 하나는 초기 세션 키로서 사용하고, 다른 하나는 보안 시드로서 사용한다. 초기 인증이 안전하기 때문에, 이러한 2개의 키는 해커에게 알려지지 않는다. 초기 세션 키는 언젠가는 해커에 의해 크랙될 수도 있지만, 보안 시드는 임의의 불안전한 통신에 사용되지 않기 때문에 안전하게 유지된다.

대표도

도 2

색인어

사용자 인증, WLAN, 이동 단말기, 액세스 포인트, 세션 키

명세서

기술분야

관련 출원

본 출원은 2003년 3월 14일자로 출원한 미국 가특허 출원번호 60/454,542호의 우선권을 주장하며, 그 내용은 본 명세서에 참조로서 포함한다.

본 발명은 근거리 네트워크에 보안 통신 세션을 제공하기 위한 장치 및 방법에 관한 것으로서, 특히 주기적인 키(key) 업데이트 및 보안 로그 오프(logoff)를 이용하는 WLAN에 있는 이동 단말기에 보안 통신 세션을 제공하기 위한 장치 및 방법에 관한 것이다.

배경기술

본 발명의 배경은, 액세스 포인트(AP)를 구비한 IEEE 802.1x 아키텍처를 채용하는 무선 근거리 네트워크 또는 WLAN의 분야인데, 액세스 포인트는 이동 디바이스를 위한 액세스와, 인터넷과 같은 회로 접속(hard wired) 근거리 및 글로벌(global) 네트워크와 같은 다른 네트워크로의 액세스를 제공한다. WLAN 기술의 진보로 인하여, 휴게소, 카페, 도서관 및 유사한 공공 시설("핫 스폿"(hot spot))은 공개적으로 액세스 가능한 무선 통신이 된다. 현재, 공중 WLAN은 이동 통신 디바이스 사용자에게, 공동 인트라넷과 같은 사설 데이터 네트워크, 또는 인터넷, 피어 투 피어 통신 및 라이브 무선 VT 방송과 같은 공중 데이터 네트워크에 대한 액세스를 제공한다. 공중 WLAN을 실시 및 작동하는 상대적으로 낮은 비용뿐만 아니라 이용 가능한 높은 대역폭(통상적으로, 10Mb/s를 초과)으로 인하여, 공중 WLAN은 이상적인 액세스 메커니즘이 되고, 이를 통해 어떤 이동 무선 통신 디바이스 사용자는 외부 엔티티(entity)와 패킷을 교환할 수 있다. 그러나 이하에서 설명하는 바와 같이, 그러한 개방적인 배치는, 식별 및 인증을 위한 적절한 수단이 존재하지 않는 경우에는 보안성을 떨어뜨릴 수도 있다.

사용자가 공중 WLAN 커버리지(coverage) 영역 내의 서비스를 액세스하려는 경우, WLAN은 사용자 액세스를 인증 및 인정한 후에 네트워크 액세스를 허용한다. 인증 후, 공중 WLAN은 보안 데이터 채널을 이동 통신 디바이스에 개방하여, WLAN과 디바이스 간을 이동하는 데이터의 프라이버시(privacy)를 보호한다. 현재, 수많은 WLAN 장비 제조업체는, 배치되는 장비를 위해 IEEE 802.1x 프로토콜을 채택한다. 그러므로 WLAN을 위한 유력한 인증 메커니즘은 이 표준을 사용한다. 불행하게도, IEEE 802.1x 프로토콜은, 그 프로토콜의 활용 모델로서 사설 LAN 액세스를 사용하도록 설계되었다. 그러므로 IEEE 802.1x 프로토콜은 공중 WLAN 환경에서의 보안성을 개선하는 특징을 제공하지는 않는다.

웹 브라우저 기반의 인증 방법에서, 이동 단말기는, HTTPS(Hyper Text Transfer Protocol Secured Sockets) 프로토콜을 이용하여 작동하는 웹 브라우저를 사용하여 인증 서버와 통신하고, 이동 단말기와 인증 서버 간의 경로에 있는 임의의 사용자가 기밀 사용자 정보를 침해 또는 훔칠 수 없다는 점을 보증한다. 그러나 인증 서버가 이동 단말기와 관계하는 유일한 정보는, 자신의 IP 어드레스이다.

사용자가 WLAN에 의해 인증되는 경우, 사용자와 WLAN은 보안 세션 키를 확립 및 공유한다. 후속하는 모든 통신은 이 세션 키를 사용하여 암호화된다. 보안성 공격, 예로서 IEEE 802.11 WEP 암호화 프로토콜에 있는 보안 홀(security hole)을 탐색하는 공격을 방지하고, 강력한 보안성을 보증하기 위하여, 세션 키는 주기적으로 업데이트할 필요가 있다. 실제로, 초기 세션 키가 WEP(Wired Equivalent Privacy) 키로서 사용되는 경우, 무선 사용자와 WLAN 액세스 포인트 간의 WEP 키를 사용하는 특정한 수의 통신 교환 이후에, 해커는 그 키를 크랙(crack)할 수도 있다. IEEE 802.1x에 있어서, 세션 키가 업데이트되는 WLAN에서의 보안 액세스 제어를 위해 사용된 프로토콜은 인증 서버에 의존한다. 본질적으로, 키가 업데이트되는 시간마다, 사용자는 초기 인증과 유사한 인증 단계를 통해 승인될 필요가 있다. 이 절차는 몇몇 애플리케이션에서 비효율적이고 불가능할 수 있다. WLAN 기술은, 사용자가 인증되고, 세션 키가 확립되면, 앞으로의 키 업데이트는 인증 서버의 참여를 더 이상 필요로 하지 않는 방법으로부터 이득을 얻을 수 있다.

추가로, 관리 정보를 처리하는 애플리케이션, 특히 로그 오프 요청은 통상적으로 해킹으로부터의 보안성을 필요로 한다. 그러나 IEEE 802.1x에 있어서, 그러한 정보는 암호화되지 않은 상태로 송신되므로, 이동 단말기는, 해커가 세션 키를 갖

고 있지 않더라도, 해커가 인증된 사용자를 로그 오프할 수 있는 공격에 쉽게 방치된다. 그렇기 때문에, WLAN 기술은, 세션 키를 이용하여 추가로 암호화되는 암호화 키 업데이트 또는 로그 오프 요청을 위해 제공되는 방법으로부터 이득을 얻을 수 있다.

<발명의 개요>

이동 단말기와 통신 네트워크 간에 보안 통신 세션을 제공하기 위한 방법은, 단말기와 통신 네트워크 간의 통신을 암호화하기 위해 세션 키를 사용하는 것이 바람직하고, 세션 키는, 단말기와, 통신 네트워크의 액세스 포인트에 저장되는 보안 키를 포함하는 키의 세트로부터 도출할 수도 있다. 또한, 보안 키는 보안 로그 오프 메커니즘을 제공하는데 사용할 수도 있다.

본 발명은, 사용자 인증 단계 동안, 무선 사용자 머신과 WLAN AP 둘 다에, 초기 세션 키로서 간주하는 1개의 공유 비밀을 인스톨하는 대신, 2개의 공유 키를 인스톨함으로써, WLAN 환경에 있는 이동 단말기의 보안성을 개선하기 위한 방법을 제공한다. 공유 키 중 하나는 초기 세션 키로서 사용하고, 다른 공유 키는 보안 시드로서 사용한다. 초기 인증된 통신이 안전하기 때문에, 그 2개의 보안 키가 확립되면, 해커가 이러한 형태의 보호를 크랙하는 것은 거의 불가능하다. 그리고 초기 세션 키는 언젠가는 해커에 의해 크랙될 수도 있지만, 보안 시드는 임의의 불안전한 통신에 사용되지 않기 때문에 항상 안전하게 유지된다.

본 발명의 실시예는, 키 업데이트 동안, 새로운 키가 WLAN 액세스 포인트와 이동 단말기 간에 생성되어 교환되는 프로세스를 포함한다. 이 새로운 키를 직접 사용하는 대신, 액세스 포인트와 이동 단말기는, 이 새로운 키를 보안 시드와 함께 사용하여 새로운 세션 키를 생성한다. 예로서, 보안 시드와 새로운 키를 연관시킨 다음, MD5(Message Digest 5) 해시 알고리즘과 같은 한 가지 방향의 해시 기능을 계산하여 고정된 스트링을 생성함으로써, 새로운 세션 키를 생성할 수도 있다. 해커는 보안 시드를 구비할 수 없기 때문에, 오래된 세션 키를 크랙할 수 있더라도, 새로운 세션 키를 얻지는 못한다.

본 발명의 실시예는, 세션 로그 오프 동안, 이동 단말기는, 해커가 인증된 이동 단말기를 로그 오프 못하게 하는 보안 상태를 유지하는 프로세스를 또한 포함한다. IEEE 802.1x 기반의 방식은 보안 로그 오프를 제공하지 않는데, 이는 로그 오프 요청이 암호화되지 않은 프레임에서 수행되기 때문이다. 그러나 본 발명의 실시예에서, 이동 단말기는 보안 시드에 의해 수행되는 암호화된 로그 오프 요청을 송신한다. 그래서, 해커가 세션 키를 크랙하는 경우이더라도, 인증된 사용자의 로그 오프는 불가능한데, 이는 보안 시드가 로그 오프 요청에 나타나기 때문이며, 더 이상 유효하지 않기 때문이며(사용자가 로그 인하는 시간마다 새로운 보안 시드가 교섭될 필요가 있음), 따라서 오래된 보안 시드가 해커에 의해 크랙되더라도, 해가 되는 결과는 없다.

또한, 본 발명의 실시예는, 이동 단말기와 무선 로컬 액세스 네트워크(WLAN) 간에 보안 통신 세션을 제공하기 위한 방법을 포함하는데, 상기 방법은, 제1 및 제2 보안 키를 생성하는 단계, 보안 통신 방법을 사용하여 상기 이동 단말기에 상기 제1 및 제2 보안 키-상기 제1 및 제2 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 이동 단말기에 저장함-를 전송하는 단계, 현재 세션 키를 사용하여 상기 이동 단말기에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 이동 단말기로부터 수신되는 데이터를 수신하여 암호해독 하는 단계-상기 제1 세션 키는 초기에는 상기 현재 세션 키로서 사용함-, 및 상기 제2 보안 키를 사용하여 후속 세션 키를 주기적으로 생성하고, 상기 WLAN과 상기 이동 단말기 간의 후속 통신 동안의 현재 세션 키로서 상기 후속 세션 키를 사용하는 단계를 포함한다.

또한, 본 발명은 이동 단말기와 WLAN 간에 보안 통신 세션을 제공하기 위한 장치를 포함하는데, 상기 장치는, 제1 및 제2 보안 키를 생성하기 위한 수단과, 상기 이동 단말기에 상기 제1 및 제2 보안 키를 전송하기 위한 수단을 포함한다. 이동 단말기는 후속하여 수신되는 데이터의 암호해독을 위해 제1 및 제2 보안 키를 저장한다. WLAN에서, 이동 단말기에 데이터를 암호화하여 전송하는 수단은 현재 세션 키를 사용한다. WLAN에서, 후속 세션 키를 주기적으로 생성하는 수단은, 제2 보안 키를 사용하고, WLAN과 이동 단말기 간의 통신 동안의 현재 세션 키로서 후속 세션 키를 사용한다.

도면의 간단한 설명

본 발명은 첨부한 도면을 참조하여 설명하는 다음의 상세한 설명을 통해 가장 잘 이해된다. 도면의 다양한 특징이 모두 도시되지는 않는다. 대조적으로, 명확하게 하기 위하여 다양한 특징이 임의로 확장 또는 축소될 수도 있다. 도면에 포함된 것은 다음과 같다.

도 1은 이동 무선 통신 디바이스를 인증하기 위한 본 원리의 방법을 실행하기 위한 통신 시스템의 블록 다이어그램이다.

도 2는 본 발명에 따른 2개의 보안 키를 확립하는 방법의 흐름도이다.

도 3은 본 발명에 따른 보안 로그 오프 절차를 확립하는 방법의 흐름도이다.

도 4는 본 발명을 실시하기 위한 장치의 블록 다이어그램이다.

실시예

논의될 도면에 있어서, 회로 및 관련 블록과 화살표는, 전기 회로와, 전기 신호를 전송하는 관련 배선 또는 데이터 버스로서 실시될 수도 있는 본 발명에 따른 프로세스의 기능을 표현한다. 대안으로, 하나 이상의 관련 화살표는, 특히 본 발명의 방법 또는 장치가 디지털 프로세스로서 실시되는 경우, 소프트웨어 루틴 간의 통신(예컨대, 데이터 흐름)을 표현할 수도 있다.

도 1에 따르면, 140_1～140_n으로 표현한 하나 이상의 이동 단말기는, 액세스 포인트(130_n), 방화벽(122)과 관련된 로컬 컴퓨터(120), 및 인증 서버(150_n)와 같은 하나 이상의 가상 오퍼레이터(operator)(150_{1-n})를 통해 통신한다. 단말기(140_{1-n})로부터의 통신은, 인터넷(110)과, 통상적으로 해커와 같이 승인되지 않은 엔티티로부터 높은 보안성을 요구하는 관련 통신 경로(152,154)를 사용하여 보안 데이터베이스 또는 다른 소스에 액세스하는 것을 필요로 한다.

도 1에 도시하는 바와 같이, IEEE 802.1x 아키텍처는, 네트워크 스택의 더 높은 계층에 투명한 국(station) 이동성을 제공하도록 상호작용하는 몇몇 컴포넌트 및 서비스를 포함한다. IEEE 802.1x 네트워크는 액세스 포인트(130_{1-n}) 및 이동 단말기(140_{1-n})와 같은 국을, 무선 매체(124)와 통신하고, IEEE 802.1x 프로토콜의 기능성을 포함하는 컴포넌트로서 정의하는데, 그 컴포넌트는 MAC(Medium Access Control)(138_{1-n}), 대응 PHY(Physical Layer)(도시하지 않음), 및 무선 매체로의 커넥션(127)이다. 통상적으로, IEEE 802.1x 기능은 무선 모뎀 또는 네트워크 액세스 또는 인터페이스 카드의 하드웨어 및 소프트웨어에서 실시한다. 본 발명은 식별 수단을 통신 스트림에 실시하기 위한 방법을 제안하여, 다운링크 트래픽(즉, 인증 서버로부터, 랩톱(laptop)과 같은 이동 단말기로)을 위한 IEEE 802.1x WLAN MAC 계층과 호환가능한 액세스 포인트(130_{1-n})는, 하나 이상의 무선 이동 디바이스(140_{1-n}), 로컬 또는 백 엔드(back end) 서버(120), 및 인증 서버(150)의 인증에 참여할 수도 있다.

본 원리에 따르면, 이동 단말기 자체뿐만 아니라 IEEE 802.1x 프로토콜에 따른 통신 스트림을 인증함으로써, 액세스(160)는 각각의 이동 단말기(140_{1-n})를 WLAN(115)에 안전하게 액세스 가능하게 한다. 액세스(160)가 그러한 보안 액세스를 가능하게 하는 방식은 도 1과 도 2를 참조하여 가장 잘 이해할 수 있다.

이동 무선 통신 디바이스, 즉 이동 단말기(140_n), 공중 WLAN(115), 로컬 웹 서버(120) 및 인증 서버(150) 간의 시간에 따라 발생하는 상호작용의 시퀀스가, IEEE 802.1x 프로토콜의 환경하에서 설명되는데, 도 1의 액세스 포인트(130_n)는 제어 포트 및 미제어 포트를 유지하고, 이를 통해 액세스 포인트는 이동 단말기(140_{1-n})와 정보를 교환한다. 액세스 포인트(130_n)에 의해 유지되는 제어 포트는, 액세스 포인트(130_n)를 통과하는 데이터 트래픽과 같은 미인증 정보를 위한 통로(entryway)로서의 기능을 하는데, 이는 액세스 포인트가 로컬 서버(120)와 이동 단말기(140_{1-n}) 간을 이동하기 때문이다. 통상적으로, 액세스 포인트(130_{1-n})는, 적절한 이동 단말기(140_{1-n})의 인증이 전달될 때까지, IEEE 802.1x 프로토콜에 따라 각각의 제어 포트를 폐쇄 상태로 유지한다. 액세스 포인트(130_{1-n})는 각각의 미제어 포트를 항상 개방 상태로 유지하여, 이동 단말기(140_{1-n})가 인증 서버(150)와 인증 데이터를 교환하게 한다.

도 2를 참조하여 더욱 구체적으로 설명하면, WLAN 환경에 있는 이동 단말기(140_n)의 보안성을 개선하기 위한 본 발명에 따른 방법은, 사용자 인증 단계 동안, 이동 단말기(140_n)와 WLAN 액세스 포인트(130_n) 둘 다에, 1개의 공유 비밀 대신 2개의 공유 비밀을 인스톨(install) 한다. 공유 비밀 중 하나는 초기 세션 키로서 사용하고, 다른 하나는 보안 시드(seed)로서 사용한다. 초기 인증이 안전하기 때문에, 이러한 2개의 키는 해커에게 알려지지 않는다. 그 키는, 알려진 방법, 예로서 그러한 키를 생성하여 분배하기 위한 인증 서버를 사용하여, 이동 단말기와 WLAN 액세스 포인트에 생성 및 분배할 수도

있다. 초기 세션 키는 언젠가는 해커에 의해 크랙될 수도 있지만, 보안 시드는 임의의 불안전한 통신에 사용되지 않기 때문에 안전하게 유지된다. 특히, 본 발명에 따른 방법은 이동 단말기(140_n)로부터의 웹 요청을 액세스 포인트(130_n)를 통해 처리하여 세션 ID(215)를 임베드(embed)한다.

도 2를 참조하면, 본 발명에 따른 방법은, 사용자 인증 단계 동안, 이동 단말기(140_n)와 WLAN 액세스 포인트(130_n) 둘 다에 적어도 2개의 공유 비밀을 인스톨하는 단계를 포함함으로써, WLAN 환경에 있는 이동 단말기(140_n)의 보안성을 개선하는데, 제1 비밀은 초기 세션 키이고, 후속 키는 보안 시드로서 사용한다.

본 발명의 원리에 따르면, 각 디바이스(140_1-140_n)와 같은 각 이동 통신 디바이스를, 디바이스 자체뿐만 아니라, 디바이스로부터 나오는 트래픽을 인증할 수 있는 WLAN(115)에 안전하게 액세스 가능하게 하는 기술을 제공한다. 도 2에서 사용되는 인증 기술은, 이동 단말기(140_n), 액세스 포인트(130_n) 및 인증 서버(150) 간의 시간에 따라 발생하는 통신의 시퀀스를 도시한다. 보안 액세스를 개시하기 위하여, 이동 단말기(140_n)는, 도 2의 단계 200에서, 액세스 포인트(130_n)에 액세스를 위한 요청을 전송한다. 실제로, 이동 단말기(140_n)는, 이동 단말기(140_n)에 의해 실행되는 브라우저 소프트웨어 프로그램(도시하지 않음)에 의해 시작된 HTTPS 액세스 요구(demand)에 의한 액세스 요청을 개시한다. 액세스 요청에 응답하여, 액세스 포인트(130_n)는, 단계 202에서, 이동 단말기(140_n)에 있는 브라우저 소프트웨어를 액세스 포인트(130_n)상의 로컬 웰컴 페이지에 리디렉트(redirect) 한다.

단계 202에 후속하여, 이동 단말기(140_n)는, 단계 204에서, 적당한 인증 서버의 아이덴티티(identity)를 위한 액세스 포인트(130_n)를 질의함으로써 인증 시퀀스를 개시한다. 이에 응답하여, 액세스 포인트(130_n)는, 단계 206에서, 적당한 인증 서버(예컨대, 서버 150)의 아이덴티티를 결정한 다음, 단계 208에서, 이동 단말기(140_n)에 있는 브라우저 소프트웨어를 HTTP 명령을 통해 그 서버에 송신한다. 단계 208에서, 인증 서버(150)의 아이덴티티가 새롭게 수신되고, 도 2의 단계 210에서, 이동 단말기(140_n)는 자신의 사용자 자격 증명(credential)을 그 서버에 송신한다.

이동 단말기(140_n)로부터 사용자 자격 증명을 수신하면, 인증 서버(150)는, 단계 212에서, 이동 단말기(140_n)가 유효 사용자를 구성하고 있는지를 판정한다. 이동 단말기가 유효 사용자를 구성하고 있다면, 인증 서버(150)는, WEP(Wired Equivalent Privacy) 암호화 키를 사용하는 단계 214에서 이동 단말기(140_n)에 응답하는데, 디바이스는, 디바이스의 브라우저 소프트웨어에 의한 ActiveX 컨트롤의 ActiveX 명령을 통해 WEP 암호화 키를 시동한다. ActiveX 컨트롤은 본질적으로는 웹 페이지 내에 임베드될 수 있는 실행가능한 프로그램이다. Microsoft Internet Explorer와 같은 수많은 소프트웨어 브라우저 프로그램은, 그러한 웹 페이지를 표시할 수 있고, 원격 서버(예컨대, 인증 서버 150)로부터 다운로드할 수 있는 임베드된 ActiveX 컨트롤을 시동할 수 있다. ActiveX 컨트롤의 실행은 브라우저 소프트웨어에 구성된 보안성 메커니즘에 의해 제한된다. 실제로, 대부분의 브라우저 소프트웨어는 선택가능한 몇몇 상이한 보안성 레벨을 구비한다. 가장 낮은 레벨에서, 웹으로부터의 임의의 ActiveX 컨트롤은 제한 없이 시동할 수 있다. 가장 높은 레벨에서, 브라우저 소프트웨어로부터 시동할 수 있는 ActiveX 컨트롤은 없다.

본 발명에 따른 방법은, 인증 및 승인 이후의 단계 217에서, 제1 키를 생성하고, 액세스 포인트(130_n)와 이동 단말기(140_n)에 그 새로운 키를 분배하는 단계를 포함한다. 단계 221에서, 보안 시드(123)로서 참조되는 제2 키는, 이동 단말기(140_n)와 액세스 포인트(130_n)에 분배한다. 그 이후, 이동 단말기와 액세스 포인트는, 데이터를 암호화하는 세션으로서 제1 키를 사용하여 통신한다. 그 이후, 액세스 포인트(130_n)와 이동 단말기(140_n)는 키(119)와 보안 시드(123)를 채택하여 새로운 세션 키(121)를 주기적으로 생성하는데, 이에 의해, 새로운 세션 키는 이동 단말기와 액세스 포인트 간의 후속 통신을 위해 사용한다. 제2 키는, 통신 세션 동안, 이동 단말기와 액세스 포인트에 비밀로서 항상 저장 및 유지되어, 해커는 제2 키를 판정할 수 없다. 새로운 세션 키를 생성하고, 보안을 위해 그 새로운 키를 사용하기에 앞서, 그 새로운 세션 키를 보안 시드에 연관시키는 것과 같은 결합한 키의 관리를 더 용이하게 하는 몇몇 기술이 채택될 수도 있다. 결합한 세션 키와 보안 시드를 연관시키면, 그 프로세스는, 연관된 새로운 세션 키와 보안 시드에 대해 해시(hash) 알고리즘을 계산할 수도 있고, 전송을 위한 고정 스트링(string)을 생성할 수도 있다.

WLAN 환경에 있는 이동 단말기의 보안성을 개선하기 위한 방법은, 이동 단말기(140_n)가, 세션 로그 오프 동안, 보안 시드에 의해 수행되는 암호화된 로그 오프 요청을 송신하여, 보안 시드가 로그 오프 요청에 나타나게 하는 단계를 더 포함한다. 세션 로그 오프 동안, 이동 단말기(140_n)는, 해커가 인증된 이동 단말기(140_n)를 로그 오프 못하게 하는 보안 상태를 유지

한다. IEEE 802.1x 기반의 방식은 보안 로그 오프를 제공할 수 없는데, 이는 로그 오프 요청이 암호화되지 않은 프레임에서 수행되기 때문이다. 그러나 본 발명의 실시예에서, 이동 단말기(140_n)는 보안 시드(123)에 의해 수행되는 암호화된 로그 오프 요청(228)을 송신한다. 그래서, 해커가 세션 키를 크랙하는 경우이더라도, 이동 단말기(140_n)에 대한 인증된 사용자의 로그 오프는 불가능한데, 이는 보안 시드(123)가 로그 오프 요청(228)에 나타나기 때문이며, 사용자가 로그 인하는 시간마다 새로운 보안 시드가 교섭될 필요가 있는 이후에는 더 이상 사용되지 않기 때문이다.

도 4는 이동 단말기(140_n)와 WLAN 간의 보안 통신 세션을 위한 장치를 도시한다. 액세스 포인트(130_n)는, 제1 및 제2 보안 키를 생성하기 위한 수단(410)과, 이동 단말기(140_n)에 제1 보안 키(119)와 제2 보안 키(123)를 전송하기 위한 수단(420)을 포함한다. 이동 단말기(140_n)는 제1 보안 키(119)와 제2 보안 키(123)를 수신하고, 그 키를 보안 통신 동안에 사용하기 위하여 레지스터(430)에 저장한다. 액세스 포인트(130_n)는, 데이터를 암호화하는 수단(415)과, 현재의 세션 키를 사용하여 WLAN(115)을 통해 이동 단말기(140_n)에 데이터를 전송하는 수단(420)을 포함한다. 이동 단말기(140_n)는, 수신하는 수단(450)과, 현재의 세션 키를 사용하여 액세스 포인트(130_n)로부터 수신되는 데이터를 암호해독 하는 수단(435)을 포함하는데, 제1 보안 키는 초기에는 현재 세션 키(119)로서 사용한다. 액세스 포인트(130_n)는 제2 세션 키를 사용하여 후속 세션 키를 주기적으로 생성하는 수단(425)을 포함하고, WLAN(115)과 이동 단말기(140_n) 간의 후속 통신 동안, 그 후속 세션 키를 현재 세션 키로서 사용한다.

도시한 바와 같은 본 발명의 형태는 단순히 바람직한 실시예로서 이해하게 된다. 부품의 기능 및 배열에서 다양한 변경이 이루어질 수도 있는데, 동등한 수단이 예시 및 설명된 수단으로 대체될 수도 있으며, 어떤 특징은 다음의 청구항에서 정의되는 본 발명의 사상 및 범위로부터 벗어나지 않으면서 다른 특징과 무관하게 사용할 수도 있다.

(57) 청구의 범위

청구항 1.

통신 네트워크에서 사용자 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

보안 통신 방법을 사용하여 상기 사용자 단말기에 제1 및 제2 보안 키-상기 제1 및 제2 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 사용자 단말기에 저장하기 적합함-를 전송하는 단계,

현재 세션 키를 사용하여 상기 사용자 단말기에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 사용자 단말기로부터 수신되는 데이터를 수신하여 암호해독 하는 단계-상기 제1 보안 키는 초기에는 상기 현재 세션 키로서 사용함-, 및

상기 제2 보안 키를 사용하여 후속 세션 키를 주기적으로 생성하고, 상기 통신 네트워크와 상기 사용자 단말기 간의 후속 통신 동안의 현재 세션 키로서 상기 후속 세션 키를 사용하는 단계

를 포함하는 통신 세션 제공 방법.

청구항 2.

제1항에 있어서,

상기 제2 보안 키에 의해 수행되는 상기 사용자 단말기로부터의 암호화된 로그 오프 요청에 응답하여 상기 사용자 단말기를 로그 오프하는 단계를 더 포함하는 통신 세션 제공 방법.

청구항 3.

제1항에 있어서,

상기 주기적인 생성 단계는 상기 현재 세션 키와 상기 제2 보안 키를 연관시키고, 해시 알고리즘을 적용함으로써 상기 후속 세션 키를 생성하는 단계를 포함하는 통신 세션 제공 방법.

청구항 4.

무선 로컬 액세스 네트워크(WLAN)에서 이동 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

보안 통신 방법을 사용하여 상기 이동 단말기에 제1 및 제2 보안 키-상기 제1 및 제2 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 이동 단말기에 저장하기 적합함-를 전송하는 단계,

현재 세션 키를 사용하여 상기 이동 단말기에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 이동 단말기로부터 수신되는 데이터를 수신하여 암호해독 하는 단계-상기 제1 보안 키는 초기에는 상기 현재 세션 키로서 사용함-, 및

상기 제2 보안 키를 사용하여 후속 세션 키를 주기적으로 생성하고, 상기 이동 단말기와의 후속 통신 동안의 현재 세션 키로서 상기 후속 세션 키를 사용하는 단계

를 포함하는 통신 세션 제공 방법.

청구항 5.

제4항에 있어서,

상기 주기적인 생성 단계는 상기 제1 보안 키를 사용하여 생성되는 새로운 키와 상기 제2 보안 키의 결합을 사용하여 후속 세션 키를 생성하는 단계를 포함하는 통신 세션 제공 방법.

청구항 6.

제5항에 있어서,

상기 주기적인 생성 단계는 상기 새로운 키와 상기 제2 보안 키를 연관시키고, 후속 세션 키를 생성하는 해시 알고리즘을 작동시킴으로써 후속 세션 키를 생성하는 단계를 포함하는 통신 세션 제공 방법.

청구항 7.

무선 로컬 액세스 네트워크(WLAN)에서 이동 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

보안 키를 생성하는 단계,

보안 통신 방법을 사용하여 상기 이동 단말기에 상기 보안 키-상기 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 이동 단말기에 저장함-를 전송하는 단계,

현재 세션 키를 사용하여 상기 이동 단말기에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 이동 단말기로부터 수신되는 데이터를 수신하여 암호해독 하는 단계, 및

상기 이동 단말기로부터의 로그 오프 메시지 수신-상기 로그 오프 메시지는 암호화된 형태이고, 상기 보안 키를 포함함-에 응답하여 상기 보안 통신 세션을 종료하는 단계

를 포함하는 통신 세션 제공 방법.

청구항 8.

무선 로컬 액세스 네트워크(WLAN)에서 이동 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

제1 및 제2 보안 키를 생성하는 단계,

보안 통신 방법을 사용하여 상기 WLAN에 상기 제1 및 제2 보안 키-상기 제1 및 제2 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 WLAN에 저장함-를 전송하는 단계,

현재 세션 키를 사용하여 상기 WLAN에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 WLAN으로부터 수신되는 데이터를 수신하여 암호해독 하는 단계-상기 제1 보안 키는 초기에는 상기 현재 세션 키로서 사용함-, 및

상기 제2 보안 키를 사용하여 후속 세션 키를 주기적으로 생성하고, 상기 이동 단말기와의 후속 통신 동안의 현재 세션 키로서 상기 후속 세션 키를 사용하는 단계

를 포함하는 통신 세션 제공 방법.

청구항 9.

제8항에 있어서,

상기 주기적인 생성 단계는 상기 제1 보안 키를 사용하여 생성되는 새로운 키와 상기 제2 보안 키의 결합을 사용하여 후속 세션 키를 생성하는 단계를 포함하는 통신 세션 제공 방법.

청구항 10.

제9항에 있어서,

상기 주기적인 생성 단계는 상기 새로운 키와 상기 제2 보안 키를 연관시키고, 후속 세션 키를 생성하는 해시 알고리즘을 작동시킴으로써 후속 세션 키를 생성하는 단계를 포함하는 통신 세션 제공 방법.

청구항 11.

무선 로컬 액세스 네트워크(WLAN)에서 이동 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

보안 키를 생성하는 단계,

보안 통신 방법을 사용하여 상기 WLAN에 상기 보안 키-상기 보안 키는 상기 보안 통신 세션 동안에 사용하기 위해 상기 WLAN에 저장함-를 전송하는 단계,

현재 세션 키를 사용하여 상기 WLAN에 데이터를 암호화하여 전송하고, 상기 현재 세션 키를 사용하여 상기 WLAN로부터 수신되는 데이터를 수신하여 암호해독 하는 단계, 및

상기 WLAN으로부터의 로그 오프 메시지 수신-상기 로그 오프 메시지는 암호화된 형태이고, 상기 보안 키를 포함함-에 응답하여 상기 보안 통신 세션을 종료하는 단계

를 포함하는 통신 세션 제공 방법.

청구항 12.

무선 로컬 액세스 네트워크(WLAN)에서 이동 단말기와의 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

사용자 인증 단계 동안 상기 이동 단말기와 WLAN 액세스 포인트 둘 다에 적어도 2개의 공유 비밀을 인스톨하는 단계를 포함하고, 이에 의해 제1 비밀은 초기 세션 키이고, 제2 비밀은 후속 세션 키를 생성하는 보안 시드로서 사용하는 통신 세션 제공 방법.

청구항 13.

제12항에 있어서,

새로운 키를 생성하고, 현재 키를 이용하여 상기 새로운 키를 암호화하며, 상기 WLAN과 상기 이동 단말기 간에 상기 새로운 키를 교환하는 단계를 더 포함하는 통신 세션 제공 방법.

청구항 14.

제12항에 있어서,

상기 WLAN과 상기 이동 단말기는 상기 새로운 세션 키와 상기 보안 시드를 채택하는 새로운 세션 키를 생성하는 단계를 더 포함하는 통신 세션 제공 방법.

청구항 15.

제14항에 있어서,

상기 새로운 세션 키 생성 단계는 상기 새로운 키와 상기 보안 시드를 연관시키는 단계를 포함하는 통신 세션 제공 방법.

청구항 16.

제15항에 있어서,

상기 연관된 결과에 해시 알고리즘을 적용함으로써 새로운 세션 키를 생성하는 단계를 더 포함하는 통신 세션 제공 방법.

청구항 17.

제16항에 있어서,

상기 WLAN과 상기 이동 단말기 간의 통신 시 상기 새로운 세션 키를 사용하는 단계를 더 포함하는 통신 세션 제공 방법.

청구항 18.

이동 단말기와 무선 로컬 액세스 네트워크(WLAN) 간에 보안 통신 세션을 제공하기 위한 방법으로서,

상기 방법은,

이동 단말기가, 세션 로그 오프 동안, 보안 시드를 수반하는 암호화된 로그 오프 요청을 송신하여, 상기 보안 시드가 상기 로그 오프 요청에 나타나게 하는 단계를 포함하는 통신 세션 제공 방법.

청구항 19.

이동 단말기와 무선 로컬 액세스 네트워크(WLAN) 간에 보안 통신 세션을 제공하기 위한 액세스 포인트로서,

보안 통신 방법을 사용하여 상기 이동 단말기에 제1 및 제2 보안 키를 전송하기 위한 수단, 및

상기 제1 보안 키를 사용하여 데이터를 암호화하는 수단과, 상기 제2 보안 키를 사용하여 후속 세션 키를 주기적으로 생성하는 수단

을 포함하는 액세스 포인트.

청구항 20.

통신 네트워크에 보안 통신 세션을 제공하기 위한 단말기 디바이스로서,

제1 보안 키와 제2 보안 키를 수신하는 수단과, 상기 보안 통신 세션 동안에 사용하기 위해 상기 제1 보안 키와 상기 제2 보안 키를 저장하는 수단과,

데이터를 수신하는 수단과, 상기 보안 통신 세션 동안에 현재 세션 키를 사용하여 데이터를 암호해독 하는 수단-상기 제1 보안 키는 초기에는 상기 현재 세션 키로서 사용함-, 및

상기 현재 세션 키와 상기 제2 보안 키를 사용하여 후속 세션 키-상기 후속 세션 키는 그 이후에 후속 통신을 위한 현재 세션 키로서 사용함-를 생성하는 수단

을 포함하는 단말기 디바이스.

청구항 21.

제20항에 있어서,

상기 단말기 디바이스는 이동 단말기를 포함하고, 상기 통신 네트워크는 무선 로컬 액세스 네트워크(WLAN)을 포함하는 단말기 디바이스.

청구항 22.

제20항에 있는 이동 단말기와 무선 로컬 액세스 네트워크(WLAN) 간에 보안 통신 세션을 제공하기 위한 액세스 포인트로서,

후속 세션 키를 주기적으로 생성하는 상기 수단은, 상기 제1 보안 키를 사용하는 수단에 의해 생성되는 새로운 키와 상기 제2 보안 키의 결합을 사용하여 후속 세션 키를 생성하는 수단을 포함하는 액세스 포인트.

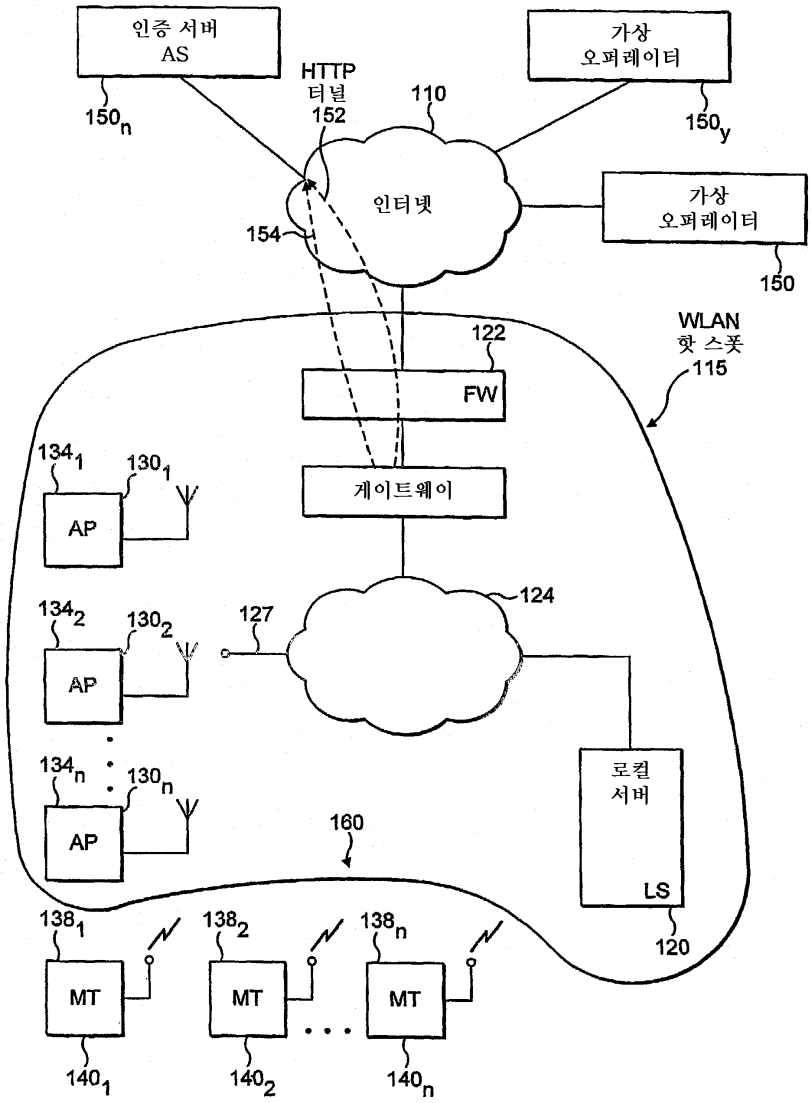
청구항 23.

제20항에 있는 이동 단말기와 무선 로컬 액세스 네트워크(WLAN) 간에 보안 통신 세션을 제공하기 위한 액세스 포인트로서,

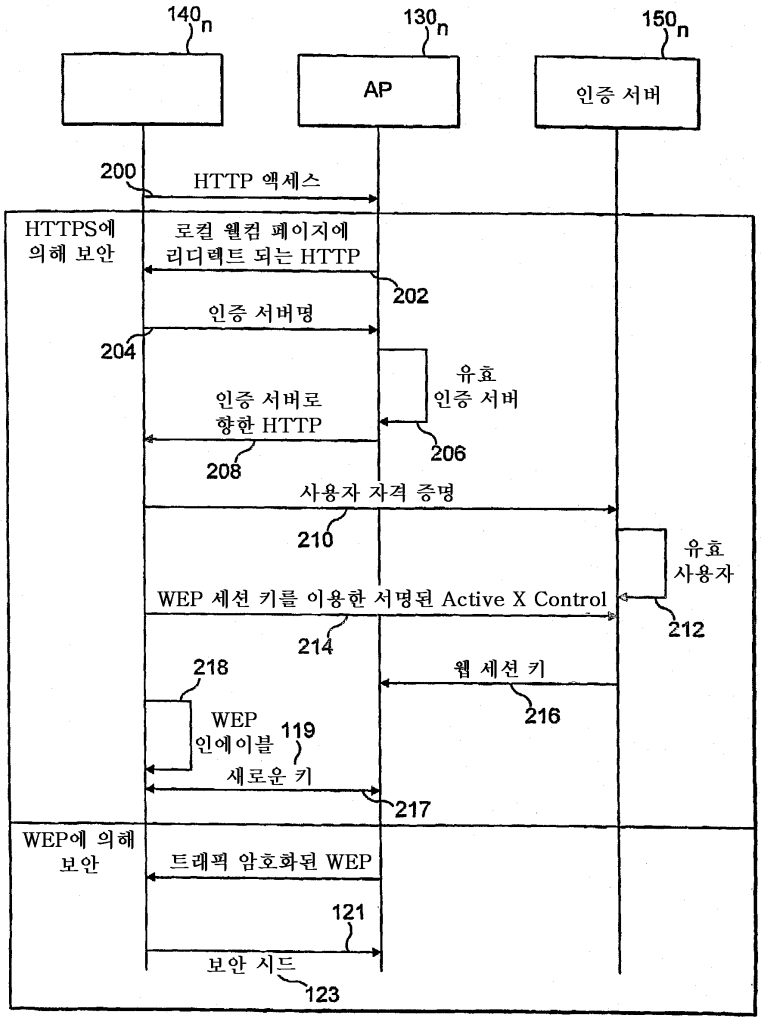
후속 세션 키를 주기적으로 생성하는 상기 수단은, 상기 새로운 키와 상기 제2 보안 키를 연관시킴으로써 후속 세션 키를 생성하는 수단과, 상기 후속 세션 키를 생성하는 해시 알고리즘을 작동하기 위한 수단을 포함하는 액세스 포인트.

도면

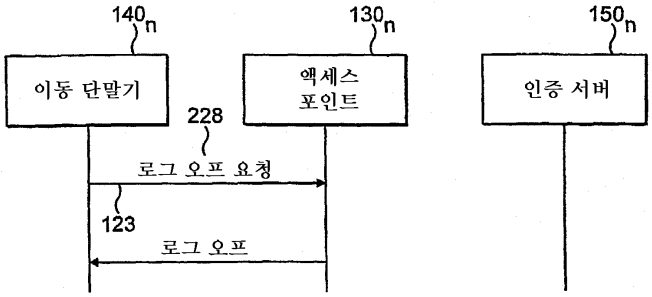
도면1


인증 서버
AS
150n
HTTP
터널
152
110
가상
오퍼레이터
150y
인터넷
154
가상
오퍼레이터
150
WLAN
핫 스폿
115
122
FW
게이트웨이
124
127
1341
1301
AP
1342
1302
AP
134n
130n
AP
160
로컬
서버
LS
120
1381
1382
138n
MT
MT
MT
1401
1402
140n

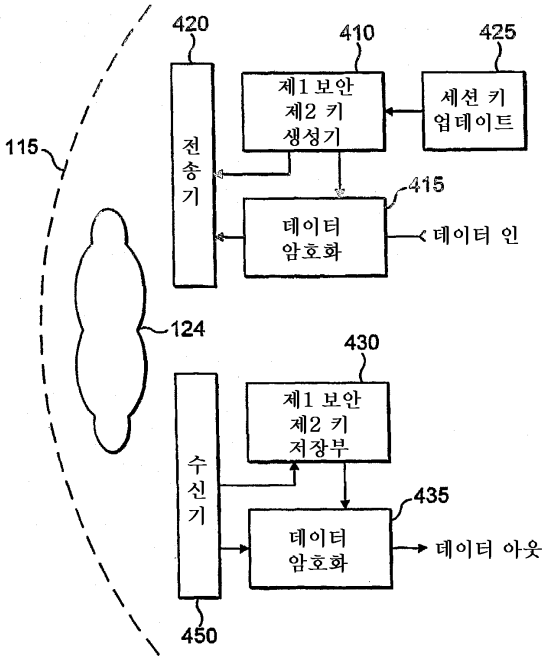
도면2


140n
130n
150n
AP
인증 서버
200
HTTP 액세스
HTTPS에 의해 보안
로컬 웰컴 페이지에 리디렉트 되는 HTTP
202
인증 서버명
204
유효 인증 서버
인증 서버로 향한 HTTP
206
208
사용자 자격 증명
210
유효 사용자
WEP 세션 키를 이용한 서명된 Active X Control
212
214
218
웹 세션 키
216
WEP 인에이블
119
새로운 키
217
WEP에 의해 보안
트래픽 암호화된 WEP
121
보안 시드
123

도면3


140n
130n
150n
이동 단말기
액세스 포인트
인증 서버
228
로그 오프 요청
123
로그 오프

도면4


420
410
425
115
전송기
제1 보안 제2 키 생성기
세션 키 업데이트
415
데이터 암호화
데이터 인
124
430
제1 보안 제2 키 저장부
수신기
435
데이터 암호화
데이터 아웃
450