(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월19일
(11) 등록번호 10-1009686
(24) 등록일자 2011년01월13일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04M 3/16 (2006.01)
(21) 출원번호 10-2005-7002312
(22) 출원일자(국제출원일자) 2003년08월13일
심사청구일자 2008년08월11일
(85) 번역문제출일자 2005년02월07일
(65) 공개번호 10-2005-0071473
(43) 공개일자 2005년07월07일
(86) 국제출원번호 PCT/US2003/025254
(87) 국제공개번호 WO 2004/017617
국제공개일자 2004년02월26일
(30) 우선권주장
60/403,495 2002년08월14일 미국(US)
(56) 선행기술조사문헌
US20020037708 A1
US20020094777 A1
전체 청구항 수 : 총 15 항

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
장, 준비아오
미국, 뉴저지 08807, 브리지워터, 제나 드라이브 20
(74) 대리인
김학수, 문경진

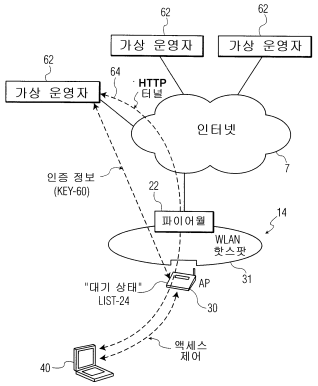
심사관 : 김대성

(54) 다수의 가상 운영자를 지원하는 공용 무선 LAN을 위한 세션 키 관리

(57) 요 약

본 발명은 모바일 단말기로 하여금 무선 근거리 네트워크(WLAN)에 액세스하도록 하기 위해 세션 키를 관리하는 방법 및 장치에 관한 것이다. 본 발명은 액세스 포인트와 가상 운영자 사이에 제 1 보안 채널을 확립하는 것과, 세션 키를 액세스 포인트로부터 가상 운영자로 제안하는 것을 제공한다. 제 2 보안 채널은 가상 운영자와 사용자 사이에 확립되고, 세션 키는 성공적인 사용자 인증시 제 2 보안 채널을 통해 사용자로 송신된다. 모바일 단말기는 세션 키를 이용하여 WLAN에 액세스한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

무선 근거리 네트워크("WLAN")에서의 액세스 포인트와 모바일 단말기 사이의 통신을 가능하게 하는데 사용된 세션 키 관리 방법으로서,

상기 모바일 단말기로부터 WLAN으로의 액세스에 대한 요청을 수신하는 단계와;

상기 액세스 요청과 연관된 가상 운영자(virtual operator)를 결정하는 단계와;

상기 액세스 포인트와 상기 가상 운영자 사이에 제 1 보안 채널을 확립하는 단계와;

상기 제 1 보안 채널을 통해 상기 가상 운영자로부터 사용자 인증을 요청하는 단계로서, 여기서 상기 가상 운영자는 상기 모바일 단말기를 인증하기 위해 제 2 보안 채널을 통해 상기 모바일 단말기와 통신하는, 사용자 인증 요청 단계와;

상기 액세스 포인트가 세션 키를 선택하고 상기 제 1 보안 채널을 통해 상기 세션 키를 상기 가상 운영자로 송신하는 단계로서, 여기서 상기 가상 운영자는 상기 제 2 보안 채널을 통해 상기 세션 키를 상기 모바일 단말기로 송신하는, 세션 키의 선택 및 송신 단계와;

상기 세션 키를 이용하여 상기 모바일 단말기와 통신하는 단계를

포함하되,

상기 사용자 인증 요청 단계는 상기 세션 키를 선택 및 송신하는 단계와 동시에 수행되는, 세션 키 관리 방법.

청구항 2

삭제

청구항 3

제 1항에 있어서, 상기 통신 단계는 사용자 인증이 성공하였다는 상기 가상 운영자로부터의 통보를 수신하자마자 상기 세션 키를 이용하여 모바일 단말기와 통신하는 단계를 포함하는, 세션 키 관리 방법.

청구항 4

제 1항에 있어서, 상기 세션 키 선택 단계는 사용자 인증이 성공하였다는 상기 가상 운영자로부터의 통보 때까지 상기 세션 키를 대기 상태(on hold)에 놓이게 하는 단계와, 통보받을시 대기 상태로부터 세션 키를 제거하고 상기 세션 키를 상기 가상 운영자로 송신하는 단계를 포함하는, 세션 키 관리 방법.

청구항 5

제 4항에 있어서, 상기 사용자 인증이 실패하였다면, 상기 세션 키를 대기 상태로 유지하는 단계를 더 포함하는, 세션 키 관리 방법.

청구항 6

무선 근거리 네트워크("WLAN")에서의 액세스 포인트와 모바일 단말기 사이의 통신을 가능하게 하는데 사용된 세션 키 관리 방법으로서,

상기 모바일 단말기로부터 WLAN으로의 액세스에 대한 요청을 수신하는 단계와;

상기 액세스 요청과 연관된 가상 운영자(virtual operator)를 결정하는 단계와;

상기 액세스 포인트와 상기 가상 운영자 사이에 제 1 보안 채널을 확립하는 단계와;

상기 제 1 보안 채널을 통해 상기 가상 운영자로부터 사용자 인증을 요청하는 단계로서, 여기서 상기 가상 운영자는 상기 모바일 단말기를 인증하기 위해 제 2 보안 채널을 통해 상기 모바일 단말기와 통신하는, 사용자 인증 요청 단계와;

상기 액세스 포인트가 세션 키를 선택하고 상기 제 1 보안 채널을 통해 상기 세션 키를 상기 가상 운영자로 송

신하는 단계로서, 여기서 상기 가상 운영자는 상기 제 2 보안 채널을 통해 상기 세션 키를 상기 모바일 단말기로 송신하는, 세션 키의 선택 및 송신 단계와;

상기 세션 키를 이용하여 상기 모바일 단말기와 통신하는 단계를

포함하되,

상기 세션 키를 선택하고 상기 세션 키를 제 1 보안 채널을 통해 상기 가상 운영자로 송신하는 단계는 사용자 인증이 성공하였다는 상기 가상 운영자로부터의 통보를 수신한 후에만 수행되는, 세션 키 관리 방법.

청구항 7

제 1항에 있어서, 상기 가상 운영자는 인터넷 서비스 제공자, 셀룰러 제공자 및 신용 카드 제공자 중 하나를 포함하는, 세션 키 관리 방법.

청구항 8

모바일 단말기와 무선 근거리 네트워크("WLAN") 사이의 통신을 가능하게 하는데 사용된 세션 키 관리 장치로서,

상기 모바일 단말기로부터 상기 WLAN으로의 액세스에 대한 요청을 수신하는 수단과;

상기 액세스 요청과 연관된 가상 운영자를 결정하는 수단과;

제 1 보안 채널을 통해 상기 가상 운영자와 통신하는 제 1 수단으로서, 상기 제 1 통신 수단은 제 1 보안 채널을 통해 가상 운영자로부터 사용자 인증을 요청하고, 상기 가상 운영자는 상기 모바일 단말기를 인증하기 위해 제 2 보안 채널을 통해 모바일 단말기와 통신하는, 제 1 통신 수단과;

세션 키를 선택하고 상기 제 1 보안 채널을 통해 세션 키를 가상 운영자로 송신하기 위한, 상기 제 1 통신 수단에 결합된 수단으로서, 상기 가상 운영자는 제 2 보안 채널을 통해 상기 세션 키를 모바일 단말기로 송신하는, 세션 키의 선택 및 송신 수단과;

상기 세션 키를 이용하여 상기 모바일 단말기와 통신하는 제 2 수단을

포함하되,

상기 제 1 통신 수단은 상기 세션 키를 선택하고 송신하는 선택 수단과 동시에 사용자 인증을 요청하는, 세션 키 관리 장치.

청구항 9

삭제

청구항 10

제 8항에 있어서, 상기 제 2 통신 수단은 사용자 인증이 성공하였다는 상기 가상 운영자로부터의 통보를 수신하자마자 상기 세션 키를 이용하여 모바일 단말기와 통신하는, 세션 키 관리 장치.

청구항 11

제 8항에 있어서, 상기 선택 수단은, 사용자 인증이 성공하였다는 가상 운영자로부터의 통보 때까지 세션 키를 대기 상태에 놓고, 그러한 통보시, 대기 상태로부터 세션 키를 제거하고 상기 세션 키를 가상 운영자로 송신하는, 세션 키 관리 장치.

청구항 12

제 11항에 있어서, 상기 선택 수단은, 상기 사용자 인증이 실패하였다면, 세션 키를 대기 상태로 유지하는, 세션 키 관리 장치.

청구항 13

모바일 단말기와 무선 근거리 네트워크("WLAN") 사이의 통신을 가능하게 하는데 사용된 세션 키 관리 장치로서,

상기 모바일 단말기로부터 상기 WLAN으로의 액세스에 대한 요청을 수신하는 수단과;

상기 액세스 요청과 연관된 가상 운영자를 결정하는 수단과;

제 1 보안 채널을 통해 상기 가상 운영자와 통신하는 제 1 수단으로서, 상기 제 1 통신 수단은 제 1 보안 채널을 통해 가상 운영자로부터 사용자 인증을 요청하고, 상기 가상 운영자는 상기 모바일 단말기를 인증하기 위해 제 2 보안 채널을 통해 상기 모바일 단말기와 통신하는, 제 1 통신 수단과;

세션 키를 선택하고 상기 제 1 보안 채널을 통해 세션 키를 상기 가상 운영자로 송신하기 위한, 상기 제 1 통신 수단에 결합된 수단으로서, 상기 가상 운영자는 제 2 보안 채널을 통해 상기 세션 키를 상기 모바일 단말기로 송신하는, 세션 키의 선택 및 송신 수단과;

상기 세션 키를 이용하여 상기 모바일 단말기와 통신하는 제 2 수단을

포함하되,

상기 선택 수단은, 상기 모바일 단말기의 인증이 성공하였다는 상기 가상 운영자로부터의 통보를 수신 후에만, 상기 세션 키를 선택하고 상기 세션 키를 제 1 보안 채널을 통해 상기 가상 운영자로 송신하는, 세션 키 관리 장치.

청구항 14

제 8항에 있어서, 상기 가상 운영자는 인터넷 서비스 제공자, 셀룰러 제공자 및 신용 카드 제공자 중 하나를 포함하는, 세션 키 관리 장치.

청구항 15

삭제

청구항 16

모바일 단말기로서,

WLAN으로의 액세스에 대한 요청을 송신하는 수단과;

상기 모바일 단말기를 인증하기 위해 보안 채널을 통해 가상 운영자와 통신하는 수단으로서, 선택된 세션 키는 상기 보안 채널을 통해 상기 모바일 단말기에 전달되고, 추가로, 상기 선택된 세션 키를 수신한 후에, 상기 모바일 단말기는 상기 세션 키를 이용하여 통신하는, 통신 수단을

포함하는, 모바일 단말기.

청구항 17

제 16항에 있어서, 상기 모바일 단말기는 상기 모바일 단말기의 인증이 성공하였다는 상기 가상 운영자로부터의 통보를 수신하자마자 상기 세션 키를 이용하여 통신하는, 모바일 단말기.

청구항 18

제 16항에 있어서, 상기 가상 운영자는 인터넷 서비스 제공자, 셀룰러 제공자 및 신용 카드 제공자 중 하나를 포함하는, 모바일 단말기.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 네트워크에 관한 것으로, 더 구체적으로, 제 3자인 가상 운영자를 지원하는 공용 무선 근거리 네트워크(WLAN) 환경에서 세션 키로의 액세스를 관리하는 메커니즘에 관한 것이다.

배 경 기 술

[0002] 현재 무선 근거리 네트워크(WLAN) 인증, 인가, 어카운팅(AAA: Authentication, Authorization, Accounting) 솔루션은, 특히 WLAN 액세스에 사용된 세션 키의 관리에 대해 다중 가상 운영자와의 비즈니스 관계를 유지시키기 위해 WLAN 운영자를 위한 적절한 지원을 제공하지 않는다. 세션 키의 적절한 제어 및 관리가 실패하면, 잠재적

인 보안 및 관리 문제가 발생할 수 있다.

[0003] WLAN은 호텔, 공항 및 카페와 같은 핫스팟(hot spot)에 점점 더 배치되고 있다. 건전하고 효과적인 AAA(인증, 인가, 어카운팅) 솔루션은 보안 공용 무선 LAN 액세스를 인에이블링하는데 매우 중요하다. 특히, 그러한 AAA 솔루션은, ISP, 셀룰러 운영자 및 선불 카드 제공자와 같은 제 3자인 제공자가 AAA 서비스를 공용 WLAN 및 무선 사용자에게 제공하는 가상 운영자 개념을 지원할 수 있어야 한다. 이러한 방식으로, 무선 사용자는, 서로 다른 핫스팟으로 갈 때마다 계정을 열거나 신용 카드로 지불할 필요가 없으며; 그 대신, 무선 사용자는 공용 WLAN으로의 액세스를 달성하기 위해 기존의 ISP 계정, 셀룰러 계정 또는 어디선가 구매한 선불 카드를 이용할 수 있다. 이것은 WLAN 운영자뿐 아니라 제 3자인 가상 운영자를 위한 비즈니스 기회를 크게 증가시킬 수 있다. 그러나, 현재 무선 LAN 액세스 솔루션은, 단일 인증 서버가 사용되는 공동 환경(corporate environment)과 같은 로컬 설정(local set-up)에 대해 모두 설계된다. 예를 들어, IEEE 802.11 표준 바디는 WLAN 액세스 제어를 위한 솔루션으로서 IEEE 802.1x를 선택하고, 현재 사용 모델은 세션 키 할당을 제어하기 위해 인증 서버를 이용한다. 이것이 공동 환경 등에 충분하지만, 상이한 비즈니스 개체(entity)에 속하는 다중 인증 서버가 공존할 수 있는 공용 핫스팟에서 특히 문제가 발생한다. 이왕 가능하다면, 이러한 인증 서버가 액세스 포인트를 위한 키 할당을 조정하는 것이 매우 어렵다.

[0004] 현재 키 분배가 이제 설명될 것이다. 하나의 시나리오에서, 공용 WLAN 핫스팟에 있는 모바일 사용자는 WLAN 액세스 포인트와의 이전의 신뢰성있는 관계를 갖지 않는다. 사용자는 신뢰성있는 브리징 개체로서 제 3자인 서비스 제공자{예를 들어, 인터넷 서비스 제공자(ISP)}를 이용하려고 의도한다. 서비스 제공자는 가상 운영자로서 언급될 수 있다. 사용자는 이러한 가상 운영자와의 계정을 유지하는데, 이것은 WLAN 운영자와의 비즈니스 관계를 갖는다. 사용자가 가상 운영자와의 신뢰성있는 관계를 확립하기 때문에, 사용자는 보안 방식으로 가상 운영자에 대해 자신을 인증할 수 있다. 그 다음에, 가상 운영자는 세션 키를 사용자 뿐 아니라 WLAN 액세스 포인트로 안전하게 송신한다(가상 운영자도 또한 WLAN과의 신뢰성있는 관계를 갖기 때문에). 이러한 공유 세션 키로 인해, 무선 LAN은, 사용자가 네트워크에 액세스하도록 인증받아, 사용자로의 액세스를 승인한다는 것을 인식한다. 이러한 구성에서, 가상 운영자가 사용자 및 WLAN 모두와 신뢰성있는 관계를 갖기 때문에 세션 키를 할당한다는 것을 주의하자.

[0005] 세션 키는 로컬 액세스에 사용되고, WLAN 액세스 포인트에 대해 국부적이어야 하는데, 예를 들어, 액세스 포인트에 의해 할당되고 유지되어야 한다. 다수의 가상 운영자가 존재할 때, 전술한 키 관리 구성은 적어도 2개의 영역에서 문제가 있다. 첫 번째로, 가상 운영자에 대해, 상이한 개체에 속하는 수 만개의 액세스 포인트에 액세스 키를 할당 및 관리하는 것, 즉 상이한 유형의 액세스 포인트에 대해 상이한 암호화 알고리즘 및 상이한 키 길이를 수용하는 것은 종종 문제가 발생한다. 두 번째로, 액세스 포인트에 대해, 일관된 방식으로 다수의 가상 운영자가 세션 키를 할당하는 것을 보장하는 것이 어려울 수 있는데, 예를 들어 2명의 사용자가 2개의 상이한 가상 운영자에 의해 할당된 동일한 키를 동시에 사용하지 않는다는 것을 보장해야 한다.

[0006] 키 어려움은, 액세스 포인트가 무선 사용자와 비밀을 공유하지 않아서, 액세스 포인트로부터의 세션 키를 사용자에게 직접 송신하는 것이 안전하지 않다는 것이다. 이러한 문제에 대한 한가지 해결책으로는, 가상 운영자가 사용자 인증이 성공적으로 이루어질 때 사용자의 공용 키에 대해 액세스 포인트(AP)에게 통보하는 것이다. 그 다음에, AP는 사용자의 공용 키를 이용하여 세션 키를 암호화하고, 그 다음에 그 결과를 사용자에게 송신한다. 특정 사용자만이 대응하는 개인 키를 이용하여 세션 키를 암호 해독할 수 있기 때문에, 세션 키는 AP와 무선 사용자 사이에 안전하게 확립될 수 있다. 그러나, 이러한 구성은 공용/개인 키의 이용을 필요로 하는데, 이것은 무선 사용자와 인증 서버 사이에서 실제 인증 방법과 호환되지 않을 수 있다. 사용자가 2개의 상이한 유형의 키(세션 키를 암호 해독하기 위한 개인 키, 및 인증 서버와의 인증을 위한 암호 유형의 키)를 유지해야 한다는 것 같다. 이것은 클라이언트 소프트웨어 복잡도를 증가시킬 뿐 아니라, 키를 안전하게 유지하는데 있어서의 어려움을 증가시킨다. 더욱이, 이러한 구성은 WLAN 보안에서의 표준이 되는 IEEE 802.1x로 작용하지 않는다.

[0007] 그러므로, 키가 국부적으로 할당되고 액세스 포인트에 의해 관리되고, 다른 무선 사용자는 액세스 포인트와의 이전의 신뢰성있는 관계없이 세션 키를 안전하게 얻을 수 있는 솔루션이 필요하다.

발명의 상세한 설명

[0008] 본 발명은 이러한 문제를 다루는데 효율적이고 효과적인 메커니즘을 설명한다. 세션 키는 WLAN에 의해 국부적으로 할당되고 관리되며(이러한 키가 국부 액세스 제어에 사용되기 때문에), 대응하는 가상 운영자와의 신뢰성있는 관계를 단지 유지하는 무선 사용자에게 안전하게 분배될 수 있다.

[0009] 무선 근거리 네트워크를 위한 세션 키 관리 방법은, 액세스 포인트와 가상 운영자 사이의 제 1 보안 채널을 확립하는 것과, 액세스 포인트로부터 가상 운영자로 세션 키를 제안하는 것을 포함한다. 제 2 보안 채널은 가상 운영자와 사용자 사이에 확립되고, 세션 키는 가상 운영자에 의해 송신되어, 액세스 포인트와 사용자 사이에 통신을 가능하게 한다.

[0010] 무선 근거리 네트워크에 대한 세션 키 관리를 위한 시스템은 액세스 포인트를 포함하는데, 이것은 액세스 포인트와 가상 운영자 사이에 제 1 보안 채널을 확립한다. 세션 키는 액세스 포인트로부터 가상 운영자에 제안된다. 가상 운영자는 사용자 인증시 가상 운영자와 사용자 사이에 제 2 보안 채널을 확립하고, 가상 운영자는 액세스 포인트와 사용자 사이의 통신을 가능하게 하도록 세션 키를 설정한다.

[0011] 본 발명의 장점, 특성 및 다양한 추가 특징은 첨부 도면과 연계하여 이제 더 구체적으로 설명될 예시적인 실시예를 고려하여 완전히 나타날 것이다.

실 시 예

[0015] 도면은 단지 본 발명의 개념을 예시하기 위한 것이고, 본 발명을 예시하기 위한 유일하게 가능한 구성이 아님이 이해되어야 한다.

[0016] 본 발명은 일반적으로 네트워크 통신에 관한 것으로, 더 구체적으로 제 3자인 가상 운영자를 지원하는 공용 무선 근거리 네트워크(WLAN) 환경에서 액세스 세션 키를 관리하기 위한 메커니즘에 관한 것이다. 그러한 가상 운영자는 인터넷 서비스 제공자(ISP), 셀룰러 운영자, 또는 선지불 카드 제공자를 포함할 수 있다. 수입 소스(revenue source)를 최대화하기 위해, 공용 무선 근거리 네트워크(WLAN)는 다수의 가상 운영자와의 비즈니스 관계를 유지할 수 있다.

[0017] 본 발명이 IEEE 802.11, HIPERLAN 2, 및/또는 초광대역(ultrawide band) 표준에 따른 시스템과 같은 WLAN 시스템에 관해 설명되는 것이 이해될 것이다; 그러나, 본 발명은 훨씬 더 넓을 수 있고, 다른 통신 시스템에 대한 다른 시스템 관리 구성에 적용가능할 수 있다. 더욱이, 본 발명은 전화, 케이블, 컴퓨터(인터넷), 위성 등을 포함하는 임의의 네트워크 시스템에 적용가능할 수 있다.

[0018] 이제 유사한 참조 번호가 수 개의 도면 전체에 유사하거나 동일한 요소를 나타내는 도면을 이제 언급하면, 처음에 도 1에서, 무선 근거리 네트워크(WLAN)(14)는 WLAN 핫스팟(31)을 위한 액세스 포인트(30)를 포함한다. WLAN(14)은 예를 들어 IEEE 802.11 및 HIPERLAN2 표준을 이용할 수 있다. WLAN(14)은 예를 들어 인터넷(7)과 같은 외부 네트워크 사이에 방화벽(firewall)(22)을 포함할 수 있다. 최종 사용자 또는 모바일 유닛(40)은 본 명세서에 설명된 바와 같이 예를 들어 HTTPS 터널(tunnel) 또는 다른 보안 채널(64)을 이용하여 인터넷(7)을 통해 WLAN(14)으로부터 가상 운영자(62)에 액세스할 수 있다.

[0019] 무선 근거리 네트워크(14)는 셀룰러 네트워크의 셀 사이 또는 셀 내에 산재되어 있다. 본 발명에 따라, 세션 키는 가상 운영자(62)로부터 사용자(40)로 송신된다. 가상 운영자(62)는, 통신 네트워크를 통해 서비스를 제공하는 인터넷 서비스 제공자(ISP), 셀룰러 운영자, 또는 선지불 카드 제공자 또는 다른 개체를 포함할 수 있다. 수입 소스를 최대화하기 위해, 공용 무선 근거리 네트워크(WLAN)는 다수의 가상 운영자와의 비즈니스 관계를 유지할 수 있다. 그러나, 적절한 시스템 보안을 유지하는 동안 복수의 가상 운영자를 유지하는 것은 어렵다.

[0020] 가상 운영자(62) 및 사용자(MS 40)가 보안 채널과 같은 비밀을 공유하거나 정보 또는 코드의 공유 부분을 이용하기 때문에, 키(60)는 그 사이에 보안 채널(64)을 통해 송신될 수 있다. 그러나, 세션 키(60)를 결정하고 유지하는 가상 운영자(62)를 갖는 것 대신에, 키는 WLAN 액세스 포인트(30)에 의해 선택되고, 그 다음에 가상 운영자에게 암시된다. 키는 예를 들어 난수 생성, 미리 저장된 수의 키로부터의 선택 등을 포함하는 복수의 방법에 의해 선택될 수 있다.

[0021] 도 2를 참조하면, 본 발명을 구현하는 일실시예는 다음과 같이 예시적으로 설명된다. 블록(102)에서, 사용자{모바일 단말기(MT)}는 액세스 포인트(AP)(30)에서 무선 LAN 액세스를 요청하고, 가상 운영자(VO)(62)를 지정한다. 블록(104)에서, AP(30)는 가상 운영자(62)와의 보안 채널(SC_1)을 확립한다. AP(30)와 가상 운영자(62) 사이의 모든 후속적인 통신은 SC_1을 통과할 것이다. 블록(106)에서, 사용자는 가상 운영자(62)와의 보안 채널(SC_2)을 확립하고, SC_2를 통해 가상 운영자에 대해 자신을 인증한다. 이것은 성공적인 사용자 인증까지 세션 키를 대기 상태(on hold)에 있도록 하는 것을 포함할 수 있다.

[0022] 블록(108)에서, 성공적인 사용자 인증시, 가상 운영자는 그 결과에 대해 AP(30)에게 통보하고, SC_1을 통해

AP(30)에게 세션 키(60)를 요청한다. 세션 키가 대기 상태에 있으면, 인증이 성공적이지 않은 경우 대기 상태로부터 제거될 수 있다. 블록(110)에서, AP(30)는 세션 키(60)를 선택하고, 이 세션 키(60)를 SC_1을 통해 가상 운영자(62)로 송신한다. 블록(112)에서, 가상 운영자는 이 세션 키를 SC_2를 통해 사용자로 송신한다. 블록(114)에서, 사용자 및 AP(30)는 이들 사이{보안 채널(SC_3)}의 후속적인 통신을 위한 세션 키를 이용하기 시작한다.

[0023] 도 3을 참조하면, 도 2에 도시된 방법은 예시된 바와 같이 속도 및 효율에 대해 더 개선될 수 있다. 성공적인 인증 이후에 가상 운영자가 세션 키를 요청하도록 하는 것 대신에, AP(30)는 SC_1이 확립된 직후에 제안된 세션 키를 제공하고, 액세스 포인트(30)에서 메모리(24)에 이 키를 "대기 상태"에 놓이게 한다. 성공적인 사용자 인증시, AP(30)는 가상 운영자에 의해 통보받고, SC_3을 위해 이 키를 이용하기 시작한다. 성공적이지 않은 인증의 경우에(예를 들어, 사용자에 의한 특정 횟수의 성공적이지 않은 시도 이후에), AP(30)는 또한 통보받고, "대기 상태" 목록(24)으로부터 키를 제거한다. 이것은, 침입자가 성공적이지 않은 인증 시도를 계속해서 하는 서비스 거부(denial-of-service) 공격을 방지한다. AP가 성공적이지 않은 인증에 관해 통보받지 않으면, 제안된 키는 AP의 메모리 저장부에 축적된다. 인증 단계는 다음 단계를 포함할 수 있다.

[0024] 단계(202)에서, 사용자 요청 무선 LAN은 AP(30)에 액세스하고, 가상 운영자(62)를 지정한다. 단계(204)에서, AP(30)는 가상 운영자(62)와의 보안 채널(SC_1)을 확립한다. AP와 가상 운영자 사이의 모든 후속적인 통신은 SC_1을 통과할 것이다. 단계(206)에서, AP(30)는 제안된 세션 키를 가상 운영자(62)로 송신하고, 이 키를 "대기 상태"가 되게 할 것이다. 단계(208)에서, 사용자는 가상 운영자(62)와의 보안 채널(SC_2)을 확립하고, 블록(209)에서 SC_2를 통해 가상 운영자(62)에 대해 자신을 인증한다. 단계(210)에서, 가상 운영자(62)는 인증 결과에 관해 AP(30)에게 통보하고, AP(30)는 제안된 키를 "대기 상태" 목록으로부터 제거한다. 블록(212)에서, 성공적인 인증의 경우에, 가상 운영자(62)는 세션 키를 사용자로 송신한다. 블록(214)에서, 사용자 및 AP(30)는 이들 사이{보안 채널(SC_3)}에 후속하는 통신을 위해 세션 키를 이용하기 시작한다.

[0025] 도 3의 방법이 더 효과적인 이유는, 도 2의 방법으로부터 1회 왕복 통신 시간을 절감하는데, 예를 들어 가상 운영자가 인증의 마지막까지 대기하는 것과, 세션 키에 대해 AP에게 요청하는 것과, 그 다음에 상기 키에 관해 사용자에게 통보하는 것을 필요로 하지 않기 때문이다. 단계(206)에서, AP가 제안된 키를 가상 운영자에게 송신할 필요가 없지만, 단계(208)와 동시에 이루어질 수 있다. 따라서, 전체적으로, 왕복 지연을 피하게 된다. 다른 실시예에서, 단계(206)는 단계(208)와 함께 순차적으로 수행될 수 있다.

[0026] 본 발명이 예를 들어 모바일 단말기, 액세스 포인트, 및/또는 셀룰러 네트워크 내에서 하드웨어, 소프트웨어, 펌웨어, 특수용 프로세서, 또는 이들의 조합의 다양한 형태로 구현될 수 있다는 것이 이해되어야 한다. 본 발명은 하드웨어와 소프트웨어의 조합으로서 구현되는 것이 바람직하다. 더욱이, 소프트웨어는 프로그램 저장 디바이스 상에 명백히 구현된 응용 프로그램으로서 구현되는 것이 바람직하다. 응용 프로그램은 임의의 적합한 구조를 포함하는 기계로 업로딩될 수 있고, 상기 기계에 의해 수행될 수 있다. 기계는 하나 이상의 중앙 처리 유닛(CPU), 랜덤 액세스 메모리(RAM), 입/출력(I/O) 인터페이스(들)와 같은 하드웨어를 갖는 컴퓨터 플랫폼 상에서 구현되는 것이 바람직하다. 컴퓨터 플랫폼은 또한 운영 체계 및 마이크로지령 코드를 포함한다. 본 명세서에 기재된 다양한 프로세스 및 기능은 운영 체계를 통해 수행되는 마이크로지령 코드의 부분 또는 응용 프로그램의 부분(또는 이들의 조합)일 수 있다. 더욱이, 추가 데이터 저장 디바이스 및 프린팅 디바이스와 같은 다양한 다른 주변 디바이스는 컴퓨터 플랫폼에 연결될 수 있다.

[0027] 첨부 도면에 도시된 구성 시스템의 구성요소 및 방법 단계 일부가 소프트웨어로 구현될 수 있기 때문에, 시스템 구성요소(또는 프로세스 단계) 사이의 실제 연결은 본 발명이 프로그래밍되는 방식에 따라 상이할 수 있다는 것이 더 이해될 것이다. 본 명세서의 가르침이 주어지면, 당업자는 본 발명의 이러한 및 유사한 구현 또는 구성을 구상할 수 있을 것이다.

[0028] 다수의 가상 운영자(한정하려는 것이 아니라 단지 예시적인 것으로 의도되는)를 지원하는 공용 무선 LAN에 대한 세션 키 관리를 위한 바람직한 실시예를 설명하였지만, 상기 가르침을 비추어 보아 당업자에 의해 변형 및 변경이 이루어질 수 있음이 주지된다. 그러므로, 첨부된 청구항에 의해 기술된 본 발명의 사상 및 범주 내에서 개시된 본 발명의 특정 실시예에 대한 변화가 이루어질 수 있음이 이해될 것이다. 이에 따라 특허법에 의해 요구된 세부사항 및 상세한 사항에 대해 본 발명을 설명하였지만, 특허 결정에 의해 보호받게 되기를 원하고 청구하는 것은 첨부된 청구항에 기재되어 있다.

산업상 이용 가능성

[0029] 상술한 바와 같이, 본 발명은 일반적으로 네트워크에 관한 것으로, 더 구체적으로, 제 3자인 가상 운영자를 지원하는 공용 무선 근거리 네트워크(WLAN)에서 세션 키로의 액세스를 관리하는 메커니즘 등에 이용된다.

도면의 간단한 설명

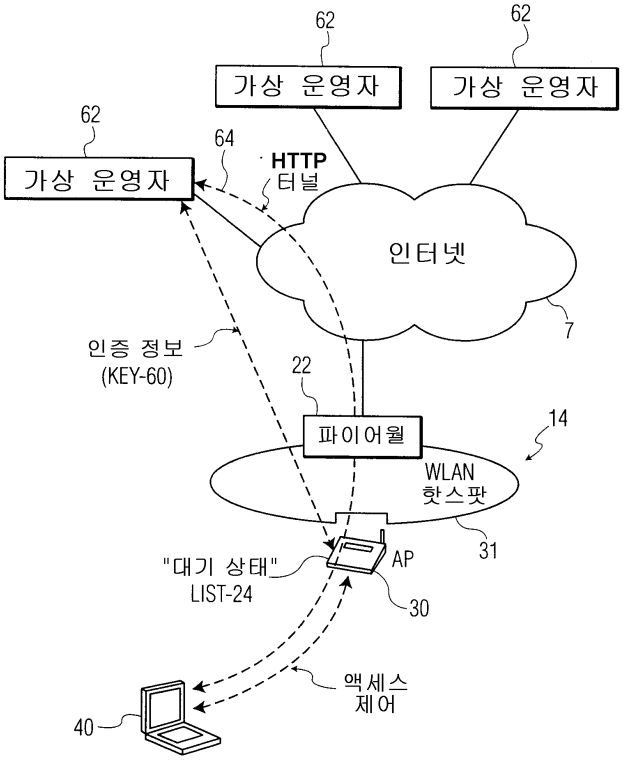
[0012] 도 1은 본 발명의 일실시예에 따른 예시적인 시스템을 도시한 도면.

[0013] 도 2는 본 발명의 일실시예에 따른 세션 키 관리 방법을 구현하는 예시적인 단계를 도시한 흐름도.

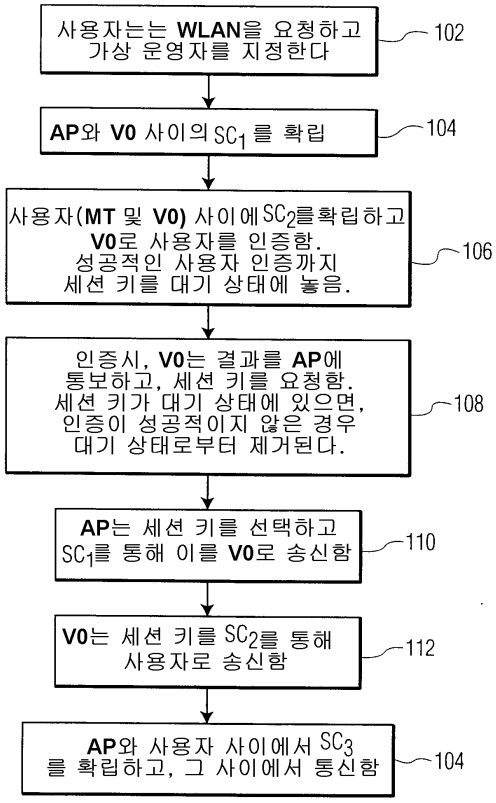
[0014] 도 3은 본 발명의 다른 실시예에 따라 무선 근거리 네트워크를 위한 또 다른 예시적인 세션 키 관리 방법을 도시한 도면.

도면

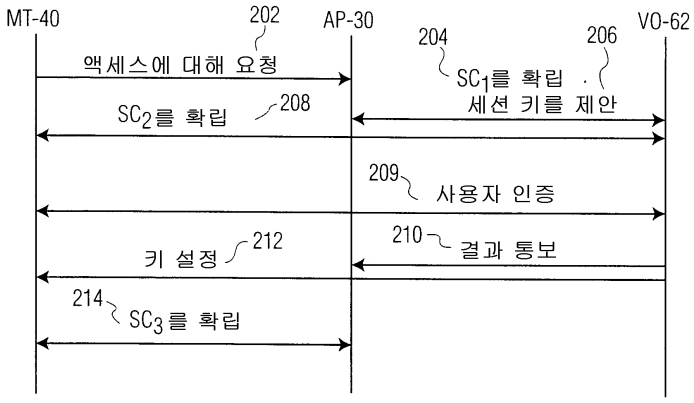
도면1



도면2


사용자는는 WLAN을 요청하고 가상 운영자를 지정한다
102
AP와 V0 사이의 SC_1 를 확립
104
사용자(MT 및 V0) 사이에 SC_2를확립하고 V0로 사용자를 인증함. 성공적인 사용자 인증까지 세션 키를 대기 상태에 놓음.
106
인증시, V0는 결과를 AP에 통보하고, 세션 키를 요청함. 세션 키가 대기 상태에 있으면, 인증이 성공적이지 않은 경우 대기 상태로부터 제거된다.
108
AP는 세션 키를 선택하고 SC_1를 통해 이를 V0로 송신함
110
V0는 세션 키를 SC_2를 통해 사용자로 송신함
112
AP와 사용자 사이에서 SC_3 를 확립하고, 그 사이에서 통신함
104

도면3


MT-40
AP-30
VO-62
202
액세스에 대해 요청
204
SC_1를 확립
206
세션 키를 제안
SC_2를 확립
208
209
사용자 인증
210
결과 통보
키 설정
212
214
SC_3를 확립