(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04K 1/00

(11) 공개번호 특2002-0019581
(43) 공개일자 2002년03월12일

(21) 출원번호 10-2002-7001123
(22) 출원일자 2002년01월26일
번역문 제출일자 2002년01월26일
(86) 국제출원번호 PCT/US2000/40564
(86) 국제출원출원일자 2000년08월02일
(87) 국제공개번호 WO 2001/10071
(87) 국제공개일자 2001년02월08일

(81) 지정국 국내특허 : 일본, 대한민국, 미국,
EP 유럽특허: 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀랜드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴,

(30) 우선권주장 60/146,882 1999년08월03일 미국(US)

(71) 출원인 폴리콤 인코포레이티드
마이클 알. 쿠리
미합중국, 캘리포니아 95035, 밀피타스, 바버 레인 1565

(72) 발명자 로드만 제프리
미국 캘리포니아 94116 샌프란시스코 37 스트리트 2667
피어슨 길
미국 캘리포니아 94133 샌프란시스코 베이 스트리트 #100 35 0

(74) 대리인 정진상
박종혁

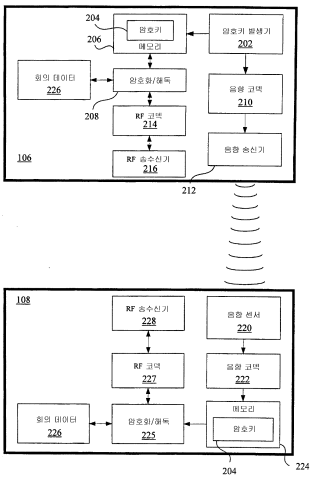
심사청구 : 없음

(54) 무선 통신 시스템내에서 안전하게 데이터를 전송하기 위한시스템 및 방법

요약

기지국 및 하나 이상의 원격장치를 포함하는 무선 네트워크 통신 시스템의 동작 동안에 데이터를 안전하게 전송하는 시스템 및 방법이 개시되어 있다. 기지국은 암호키(204)를 발생시키고(202), 이 암호키를 음향 신호로 인코딩하며, 이 음향 신호를 전송한다(212). 이 음향 신호는 통신 시스템내의 모든 함께 위치된 원격장치에 의해 수신되고, 암호키를 추출하기 위해 디코딩된다. 기지국 및 원격장치 사이의 연속적인 통신 전송은 전자 도청을 방지하기 위해 암호키를 사용하여 암호화된다.

대표도



색인어

기지국, 원격장치, 암호키, RF 송수신기, 음향 신호, 회의실, RF 코덱

명세서

기술분야

본 발명은 일반적으로 통신 시스템에 관한 것이고, 보다 상세하게는, 무선 네트워크 구성요소를 갖는 통신 시스템내에서 안전하게 데이터를 전송하기 위한 시스템 및 방법에 관한 것이다.

배경기술

음성 회의 또는 영상 회의 시스템과 같은 비지니스 통신 시스템에 마이크로폰, 스피커등과 같은 시스템 구성요소를 연결하기 위해 무선 네크워크를 사용하는 일이 증가하고 있다. 무선 네트워크를 사용하면 시스템 구성요소를 케이블로 함께 연결할 필요가 없게 되고, 그래서 시스템 세트업을 단순화하고 시스템 구성요소가 사용자의 필요를 채우도록 용이하게 재배열될 수 있게 한다. 시스템 구성요소를 연결하기 위해 무선 네트워크를 사용하면 보기 흉한 배선을 제거하거나 감소시켜서 상당한 미적 유익 또한 얻을 수 있다.

무선 통신 시스템과 관련된 단점은 기밀 정보 또는 민감한 정보를 유출할 가능성이 있다는 것이다. 비지니스 컨퍼런스 세팅에서, 회의 참석자에게만 논의되거나 보여지는 정보에 대한 접근을 제한하는 것이 많은 경우에 바람직하다. 이 때문에 회의 시스템은 전형적으로 완전히 밀폐된 공간, 즉, 회의실내에 위치된다. 그러나, 가장 상업적으로 유용한 무선 네트워크 통신 시스템은 다양한 시스템 구성요소 사이에서 정보를 전달하기 위해 무선 주파수(RF) 신호를 사용한다. 그러한 RF 신호는 용이하게 회의실의 벽, 천장등을 관통할 수 있고, 따라서 이 신호를 수신할 수 있는 다른 디바이스, 예를 들어, 제2 회의실내에 위치된 또 다른 무선 네트워크 시스템의 구성요소에 전송될 수도 있다. 또한 회의실 외부로 RF 신호가 송신되면 도청자 또는 산업 스파이가 도청할 수 있게 되고, 그래서 기밀성이 손상된다.

기밀 정보의 유출을 방지하는 한 방법은 암호키를 사용하여 전송된 RF 신호를 인코딩하여, 본질적으로 잠재된 정보를 스크램블링하는 것이다. 신호는 동일하거나 보완적인 암호키를 사용하여 수신 구성요소에서 연속적으로 디코딩된다. 그러나, 이러한 방법에서는 통신 시스템내의 모든 구성요소가 RF 신호를 적절하게 인코딩 및/또는 디코딩하기 위해 동일한 암호키를 소유할 필요가 있다. 통신 시스템내의 모든 무선 네트워크 구성요소에 대해 동일한 암호키를 할당하는 한 기술은 각각의 구성요소에서 (스위치를 설정하거나 또는 키패드를 통해) 암호키를 수동으로 입력하는 방법을 포함한다. 그러나, 이러한 기술은 시간이 걸리고 사용자 에러가 나기 쉽다. 암호키를 할당하는 또 다른 기술은 암호화되지 않은 RF 신호를 사용하여 키를 초기에(즉, 시스템 동작이 개시할 때에) 배포하는 것이다. 불행하게도, RF 전송을 모니터링하는 도청자는 전송된 암호키를 가로챌 수 있고 그 암호키를 연속적인 전송 신호를 디코딩하는데 사용할 수 있다.

따라서, 무선 통신 시스템의 구성요소 사이에 정보를 안전하게 전송하기 위한 향상된 시스템 및 방법이 필요하게 되었다. 실질적인 조작원 개입을 필요로 하지 않고, 전송 주파수를 모니터링하는 도청자가 받아들일 수 없는 시스템 구성요소간의 암호키를 배포하는 시스템 및 방법이 더 구체적으로 필요하게 되었다.

발명의 상세한 설명

본 발명은 무선 네트워크 통신 시스템의 구성요소간에 정보를 안전하게 전송하는 시스템 및 방법을 제공한다. 바람직한 실시예에서, 통신 시스템의 구성요소는 주요 시스템 회로를 포함하는 기지국 및, RF 신호의 송신 및 수신에 의해 기지국과 그리고 서로 정상적으로 통신하는 실제로 함께 위치된 원격장치(마이크로폰, 스피커, 퍼스널 컴퓨터, LCD 프로젝터, 비디오 모니터등)의 세트를 포함한다.

그러나 암호키는 음향 신호를 사용하여 배포된다. 음향 신호에 의해 암호키를 배포하기 위해서, 기지국에 음향 송신기(즉, 스피커)가 제공되고, 각각의 원격장치에 음향 센서(즉, 마이크로폰)가 제공된다. 시스템 동작의 초기에, 기지국은 암호키를 발생시키고, 이 암호키를 음향 신호로 변환시키며, 이 신호를 송신한다. 예를 들어, 이 암호키는 무작위로 발생된 n-디짓 시퀀스의 수를 포함할 수 있는데, 이 시퀀스는 DTMF 톤의 상응하는 시퀀스로 변환된다.

각각의 원격장치에는 기지국에 의해 송신된 음향 신호를 감지하는 음향 센서가 제공된다. 이 음향 센서는 음향 코덱으로 통과되는 전기 신호를 반응적으로 발생시킨다. 이 음향 코덱은 메모리에 저장하기 위한 디지털로 표현된 암호키를 추출하도록 동작한다. 암호키는 RF 신호를 통하여 원격장치 및 기지국 사이에 통과되는 회의 데이터(conference data)를 암호화하고 해독하기 위해 기지국 및 원격장치에 의해 연속적으로 사용된다. 암호키를 배포하기 위해 음향 신호를 사용하면 함께 위치되지 않은 디바이스(즉, 회의실의 외부에 위치된 디바이스)가 암호키를 해독하는 것을 효과적으로 방지할 수 있다.

도면의 간단한 설명

도 1은 회의실내에 위치된 무선 네트워크 통신 시스템의 구성요소를 도시하는 블록도,

도 2는 본 발명의 기지국 및 전형적인 원격장치의 블록도,

도 3은 본 발명에 따라, 음향 신호의 송신 및 수신에 의해 암호 키를 배포하는 방법의 단계를 도시하는 순서도.

실시예

도 1은 벽으로 둘러싸인 제1 회의실(100)내에 위치된 전형적인 무선 네트워크 통신 시스템(114)의 구성요소를 도시하고 있다. 캘리포니아주 산호세의 폴리콤 인코포레이티드에 의해 판매되고 있는 영상 회의 시스템 또는 음성 회의 시스템을 포함할 수 있지만, 그에 제한되는 것은 아니다. 통신 시스템(114)은 주요 시스템 회로를 포함하는 기지국(106)

및 전자기 신호, 전형적으로 무선 주파수(RF) 신호의 송신 및 수신에 의해 기지국과 그리고 서로 통신하는 원격장치(108, 110)와 같은 복수의 원격장치를 포함한다. 원격장치의 몇가지 예로서 마이크로폰, 스피커, 퍼스널 컴퓨터, LCD 프로젝터, 및 비디오 모니터가 있다. 기지국(106)은 공중 교환 전화망 또는 인터넷과 같은 패킷 교환망 또는 종래 회로상의 다른 통신 시스템(예를 들어, 다른 사이트에 위치된 영상 회의 시스템)과의 통신을 처리하도록 추가로 구성될 수 있다. 2개의 원격장치(108, 110)가 도면에 도시되어 있지만, 원격장치의 많고 적은 수의 원격장치가 사용될 수 있다는 것에 주목해야 한다.

도 1은 또한 제1 회의실(100)에 인접하고 벽(104)에 의해 제1 회의실로부터 분리된 제2 회의실(102)을 도시하고 있다. 통신 시스템(114)의 일부가 아닌 원격장치(112)가 제2 회의실(102)내에 위치되어 있다. 기지국(106) 및 원격장치(108, 110)에 의해 송신된 RF 신호가 용이하게 벽(104)을 관통하고 원격장치(112)에 도달할 수 있기 때문에, 송신된 RF 신호에 기초한 정보가 원격장치(112)에 접근한 사람에게도 흘러갈 수 있다. 그러한 정보가 민감하거나 독점적인 것이라면, 그 정보의 기밀성은 손상될 수 있다.

본 시스템 및 방법의 목적은 기지국(106) 및 원격장치(108, 110) 사이의 전송된 회의 데이터를 암호화함으로써 기밀 정보의 누출을 방지하는 것이다. 여기에서 사용되는 용어 " 회의 데이터" 는 음성, 영상등을 포함하는, 통신 시스템(114)의 동작 동안에 통신 시스템(114)의 사용자에게 제시될 수 있는 임의의 정보를 나타내는 데이터를 가리킨다. 회의 데이터를 성공적으로 암호화하고 해독하기 위해, 기지국(106) 및 원격장치(108, 110)는 공유 암호키를 가져야 한다. 본 시스템 및 방법에 따라, 암호키는 음향 신호를 송신 및 수신함으로써 배포된다. 음향 신호는 상대적으로 빠르게 감쇠되고 벽(104)과 같은 벽을 용이하게 관통하지 않기 때문에, 제1 회의실(100)의 외부에 위치된 디바이스는 음향적으로 암호화된 암호키의 전송 신호를 감지할 수 없고, 그래서 통신 시스템(104)로부터 퍼진 연속적으로 (기밀 정보를 나타내는 신호를 포함하는) 수신되는 RF 신호를 해독할 수 없다.

음향에 기초한 수단을 통한 암호키의 배포는 도 2의 블록도 및 도 3의 순서도를 참조함으로써 가장 잘 이해될 수 있다. 먼저 도 2에서, 기지국(106)의 구성요소 및 전형적인 원격장치(108)가 대략적으로 도시되어 있다. 기지국(106)에 주지된 랜덤 키 발생 알고리즘에 따라 암호키(204)를 무작위로 발생시키도록 구성된 암호키 발생기(202)가 제공된다. 암호키(204)는 예를 들어 무작위로 발생된 n-디짓 스트링을 포함할 수 있다. 암호키(204)는 암호화/해독 모듈(208)에 의해 연속적으로 사용되기 위해 메모리(206)내에 저장된다.

암호키(204)는 전기적으로 음향 송신기(212)에 연결된 음향 코덱(210)에 추가적으로 전송된다. 음향 코덱(210)은 음향 송신기(212)가 암호키를 인코딩하는 음향 신호(즉, 사운드)를 방출하게 하는 음향 송신기(212)에 전기 신호를 인가하도록 구성된다. 일 예에서, n-디짓 암호키는 이중 톤 다중 주파수(DTMF)톤의 스트링으로서 인코딩된다. 당업자는 음향 코덱(210)이 무제한의 모뎀 톤, 음악 현, 및 스펙트럼 확산 모듈레이션을 포함하는, 음향 신호와 같이 암호키(204)를 인코딩하는 다양한 대안적인 방법을 사용할 수 있다는 것을 인식할 것이다.

임의의 경우에, 종래의 확성기를 포함할 수 있는 음향 송신기(212)는 음향 신호 인코딩된 암호키(204)를 방출한다. 음향 신호 파워는 함께 위치된 원격장치가 신호를 감지할 수 있게 할 만큼 충분히 커야 하지만 그 파워는 회의실(100)내에 참석한 사람들이 불쾌한 사운드를 듣지 못하게 하는 것은 물론 회의실(100; 도 1)의 외부에서 신호를 감지하는 것을 방지하도록 최소화되어야 한다는 것을 이해해야 한다.

음향 신호는 회의실(100; 도 1)을 통해 전파되고 원격장치(108)에서 수신된다. 도 2에 도시된 바와 같이, 원격장치(

108)에 종래 마이크로폰을 포함하는 음향 센서가 제공된다. 음향 센서(220)는 음향 신호 인코딩된 암호키(204; 예를 들어, DTMF 톤의 스트링)를 감지하고 그에 반응하여 상응하는 전기 신호를 발생시키도록 동작한다. 이 전기 신호는 메모리(224)내에 저장되기 위한 디지털로 표현된 암호키(204)를 끌어내도록 구성된 음향 코덱(222)으로 이동된다. 암호키(204)는 암호화/해독 모듈(225)에 의해 연속적으로 접근될 수 있어서, 기지국(106) 또는 다른 함께 위치된 디바이스에 송신된 회의 데이터(226)를 암호화하고 통신 시스템(114; 도 1)의 기지국(106) 또는 다른 함께 위치된 디바이스로부터 수신된 회의 데이터(226)를 해독할 수 있다.

일단 암호키(204)가 (도 1의 통신 시스템(114)의 다른 원격장치는 물론) 원격장치(108)에 배포되면, 암호키(204)는 통신 시스템(114)의 다양한 구성요소 사이의 RF 신호에 의해 송신된 회의 데이터(226)를 인코딩하고 해독하도록 사용된다. 기지국(106)에 암호화/해독 모듈(208), RF 코덱(214), 및 RF 송수신기(216)가 제공된다. 당업자는 암호화/해독 모듈(208, 225) 및 RF 코덱(214, 227)이 하드에어, 소프트웨어, 또는 그 조합으로 구성될 수 있다는 것을 인식할 것이다.

중계 모드에서, (상술된 바와 같이, 음성, 영상등을 포함할 수 있는) 회의 데이터(226)는 암호키(204)를 사용하여 암호화/해독 모듈(208 또는 225)에 의해 암호화된다. 암호화/해독 모듈(208 또는 225)은 당업분야에서 잘 알려진 많은 암호 기술중 임의의 하나를 사용할 수 있다. 암호화된 회의 데이터는 그후에 RF 송수신기(216 또는 228)에 의해 RF 신호로서 송신되기 위하여 코덱(214 또는 227)에 의해 인코딩된다. RF 신호가 암호화된(이해할 수 없는) 정보를 포함하기 때문에, RF 신호를 가로채는 사람들이 잠재된 회의 데이터(226)에 접근하지 않을 것이다.

수신 모드에서, 통신 시스템(114; 도 1)의 또 다른 구성요소에 의해 송신된 RF 신호는 RF 송수신기(216, 228)에 의해 수신되어, RF 코덱(214 또는 227)에 의해 디지털로 표현된 암호화된 회의 데이터로 변환된다. 그후에, 암호화/해독 모듈(208 또는 225)은 다양한 목적으로 연속적으로 사용될 수 있는 회의 데이터(226)를 해독하도록 동작한다. 일 예에서, 원격장치(108)는 회의 참석자의 음성을 나타내는 회의 데이터를 발생시키는 마이크로폰을 포함할 수 있다. 음성을 나타내는 회의 데이터는 암호화되어 RF 신호에 의해 기지국(106)에 송신된다. 기지국(106)은 RF 신호를 수신하고, 잠재된 회의 데이터를 암호화하며, 이러한 데이터를 전화망을 통해 도 다른 통신 시스템에 전달한다.

원격장치(108)가 RF 송수신기(228)를 갖는 것으로 도시되었지만, 다른 원격장치가 기지국(106)과의 단방향(즉, 기지국(106)으로부터 원격장치로, 또는 원격장치로부터 기지국(106)으로의) RF 통신을 위해 사용될 수 있다는 것을 주목해야 한다. 그러한 경우에, RF 송신기 또는 RF 수신기가 RF 송수신기(228)를 대신할 것이다.

도 3은 본 시스템 및 방법에 따라 음향 신호를 사용하여 암호키(204; 도 2)를 배포하는 전형적인 방법의 단계를 도시하는 순서도(300)이다. 단계(302)에서, 키 배포 시퀀스가 초기화된다. 단계(302)는 통신 시스템(114; 도 1)을 턴 온 시킴으로써 자동으로 트리거링될 수 있거나, " 리셋" 제어등을 사용하는 사용자에 의해 수동으로 트리거링될 수 있다. 다음으로, 암호 키 발생기(202; 도 2)는 단계(304)에서 암호키(204)를 무작위로 발생시켜서 메모리(206; 도 2)에 암호키(204)를 저장한다. 그후에 암호키(204)는 단계(306)에서 코덱(210; 도 2)에 의해 인코딩되어 음향 송신기(212)에 의해 음향 신호로서 송신된다.

다음으로, 암호키(204; 도 2)를 나타내는 음향 신호는 단계(308)에서 원격장치(108; 도 2)의 음향 센서(220; 도 2)에 의해 수신되어 음향 코덱(222)에 의해 디코딩되고, 그래서 디지털로 표현된 암호키(204)가 추출된다.

(특히 음향 신호의 송신 및 수신을 간섭할 수 있는 고레벨의 주변 노이즈를 갖는 환경에서) 암호키(204; 도2)가 정확하게 송신되고 디코딩되는 것을 보장하기 위해 음향 코덱(222; 도 2)내에 (체크 섬 또는 유사한 방법을 사용하는) 에러 감지 시스템을 제공하는 것이 바람직할 수 있다. 따라서, 선택 단계(310)에서, 음향 코덱(222)은 에러가 암호키(204)의 수신/디코딩과 관련하여 발생하였는지를 결정하기 위해 에러 감지 단계를 수행한다. 음향 코덱(222)이 에러 조건을 감지하면, RF 코덱(227; 도 2) 및 송수신기(228; 도 2)를 통하여 기지국(106; 도 2)에 요구를 보내고, 그래서 단계(312)에서 암호키(204)를 나타내는 음향 신호를 재송신한다. 아무 에러 조건도 감지되지 않았다면, 암호키(204)는 단계(314)에서 메모리(224; 도 2)내에 저장되고 사용되어 회의 데이터(226; 도 2)의 연속 RF 송신 신호를 암호화하고 해독하게 된다.

본 방법은 새로운 암호키가 필요한지를 결정하는 단계(316)를 추가적으로 포함할 수 있다. 새로은 암호키의 발생은 예를 들어 소정의 시간 주기의 종료에 의해서(보안은 주기적으로 암호키를 변경함으로써 향상될 수 있다) 또는 수동 사용자 요구에 의해 트리거링될 수 있다. 새로운 암호키가 필요하다면, 본 방법은 단계(304)로 돌아가고, 그렇지 않으면, 본 방법은 기존의 암호키(206; 도 2)를 사용하여 회의 데이터(226; 도 2)를 암호화하고 해독하는 단계로 돌아간다.

도 2에 도시되고 상술된 본 실시예가 암호키 발생기(202) 및 음향 송신기(212)를 기지국(106)내에 위치시켰지만, 하나 이상의 원격장치내에 이러한 요소를 위치시킬 수 있는 대안적인 실시예가 본 발명의 범위내에 있음을 이해해야한다.

본 발명은 암호키의 음향 송신에 범위를 제한시키도록 의도된 것이 아니라는 것에 또한 주목해야 한다. 회의실 벽을 용이하게 관통하지 않고 그래서 회의실의 외부에서 감지할 수 없는 다른 종류의 신호가 암호키를 인코딩하고 배포하기 위해 사용될 수 있다. 예를 들어, 기지국에 암호키를 인코딩한 적외석(IR) 신호를 송신하는 적외선 전송기가 제공될 수 있다. 이에 상응하여 관련된 원격장치에 송신된 IR 신호를 감지하는 IR 센서 및 수신된 신호로부터 암호키를 구하는 IR 코덱이 제공된다. 회의실내에 위치된 물체 또는 사람이 IR 신호의 전송 통로를 차단하여서 원격장치가 IR 신호를 수신하는 것을 방지할 수 있기 때문에 IR 신호를 통한 암호키의 배포는 음향 신호를 사용하는 것에 비하여 덜 매력적일 수 있다.

본 발명이 특정 실시예에 관하여 위에서 설명되었다. 본 발명의 넓은 범위로부터 벗어남 없이 다양한 수정이 만들어지고 다른 실시예가 사용될 수 있다는 것이 당업자에게 명백할 것이다. 따라서, 본 특정 실시예에 대한 여러 변형은 본 발명내에 포함되고 첨부된 청구항에 의해서만 제한될 수 있다.

(57) 청구의 범위

청구항 1.

무선 네트워크 통신 시스템내에서 데이터를 안전하게 전송하는 방법에 있어서,

통신 시스템의 제1 디바이스내에 암호키를 발생시키는 단계;

인코딩된 신호를 형성하도록 암호키를 인코딩하는 단계;

제1 디바이스로부터 멀리 떨어진 통신 시스템의 제2 디바이스로 인코딩된 신호를 전송하는 단계;

암호키를 추출하기 위해 제2 디바이스에서 인코딩된 신호를 디코딩하는 단계; 및

제1 디바이스 및 제2 디바이스 사이의 연속적인 무선 전송에 대해 데이터를 암호화 및 해독하기 위해 암호키를 사용하는 단계;를 포함하는 것을 특징으로 하는 방법.

청구항 2.

제 1 항에 있어서, 상기 인코딩된 신호는 음향 신호인 것을 특징으로 하는 방법.

청구항 3.

제 2 항에 있어서, 상기 음향 신호는 DTMF 톤인 것을 특징으로 하는 방법.

청구항 4.

제 1 항에 있어서, 상기 인코딩된 신호는 적외선 신호인 것을 특징으로 하는 방법.

청구항 5.

제 1 항에 있어서, 상기 인코딩된 신호를 디코딩하는 단계는 메모리내에 디코딩된 암호키를 저장하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 6.

제 1 항에 있어서, 상기 인코딩된 신호를 디코딩하는 단계는 암호키의 수신 또는 디코딩과 관련하여 에러가 발생하였는지를 결정하기 위해 에러 감지를 실행하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 7.

제 6 항에 있어서, 에러가 감지되었다면 상기 인코딩된 신호의 재송신을 위한 요구를 보내는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 8.

제 1 항에 있어서, 연속적인 무선 전송 신호를 암호화하고 해독하기 위해 암호키를 사용하는 단계는 데이터를 무선 주파수 신호로 인코딩하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 9.

제 1 항에 있어서, 새로운 암호키가 필요한지를 결정하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 10.

무선 통신 시스템에서 데이터를 안전하게 전송하는 시스템에 있어서,

암호키를 발생시키는 암호키 발생기 및 암호키를 나타내는 인코딩된 신호를 송신하는 신호 송신기를 갖는 통신 시스템의 제1 디바이스; 및

제1 디바이스로부터 인코딩된 신호를 수신하는 신호 센서 및 인코딩된 신호로부터 암호키를 추출하는 디코더 디바이스를 갖는 통신 시스템의 제2 디바이스;를 포함하고, 상기 암호키는 제1 디바이스 및 제2 디바이스 사이에서 전송되는 데이터를 암호화하기 위해 사용되는 것을 특징으로 하는 시스템.

청구항 11.

제 10 항에 있어서, 제1 디바이스는 송신을 위해 암호키를 인코딩된 신호로 인코딩하는 인코더 디바이스를 더 포함하는 것을 특징으로 하는 시스템.

청구항 12.

제 11 항에 있어서, 상기 인코더 디바이스는 음향 코덱인 것을 특징으로 하는 시스템.

청구항 13.

제 10 항에 있어서, 상기 인코딩된 신호는 음향 신호인 것을 특징으로 하는 시스템.

청구항 14.

제 10 항에 있어서, 신호 송신기는 음향 송신기이고 신호 센서는 음향 센서인 것을 특징으로 하는 시스템.

청구항 15.

제 10 항에 있어서, 디코더 디바이스는 음향 코덱인 것을 특징으로 하는 시스템.

청구항 16.

제 10 항에 있어서, 암호키의 저장을 위해 제1 디바이스 및 제2 디바이스내에 메모리를 더 포함하는 것을 특징으로 하는 시스템.

청구항 17.

제 10 항에 있어서, 송신을 위해 데이터를 암호화하고 다른 디바이스로부터 수신된 데이터를 해독하기 위해 제1 디바이스 및 제2 디바이스내에 암호화/해독 모듈을 더 포함하는 것을 특징으로 하는 시스템.

청구항 18.

제 10 항에 있어서, 데이터를 무선 주파수 신호로 인코딩하기 위해 제1 디바이스 및 제2 디바이스내에 무선 주파수 코덱을 더 포함하는 것을 특징으로 하는 시스템.

청구항 19.

제 18 항에 있어서, 통신 시스템내에서 무선 주파수 신호를 송신 및 수신하기 위해 제1 디바이스 및 제2 디바이스내에 무선 주파수 송수신기를 더 포함하는 것을 특징으로 하는 시스템.

청구항 20.

무선 통신 시스템내에서 데이터를 안전하게 전송하는 시스템에 있어서,

통신 시스템의 제1 디바이스내에서 암호키를 발생시키는 수단;

인코딩된 신호를 형성하기 위해 암호키를 인코딩하는 수단;

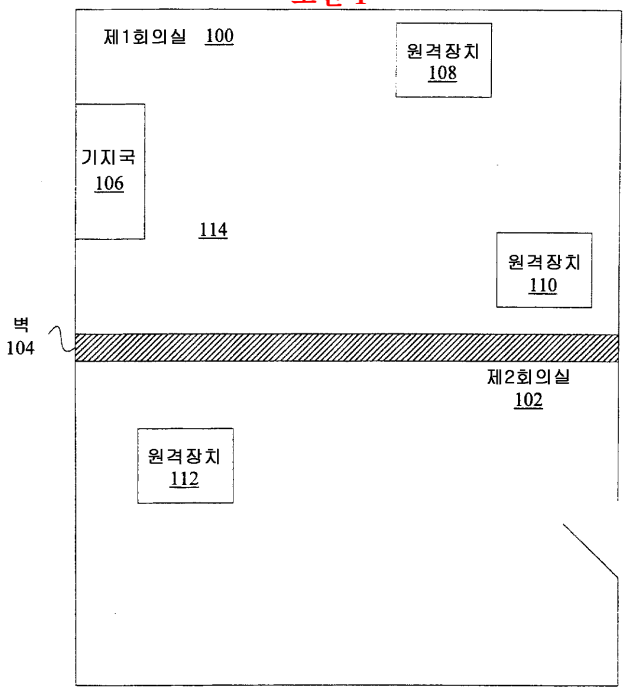
제1 디바이스로부터 멀리 떨어진 통신 시스템의 제2 디바이스로 인코딩된 신호를 송신하는 수단;

암호키를 추출하기 위해 제2 디바이스에서 상기 인코딩된 신호를 디코딩하는 수단; 및

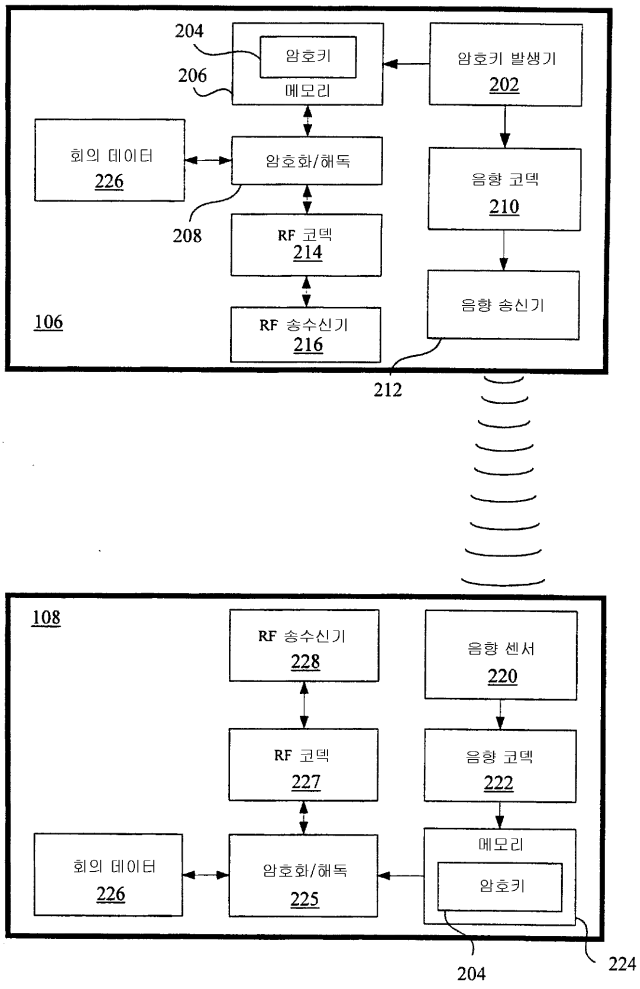
제1 디바이스 및 제2 디바이스 사이의 연속적인 무선 전송에 대해 데이터를 암호화하고 해독하기 위해 암호키를 사용하는 수단;을 포함하는 것을 특징으로 하는 시스템.

도면

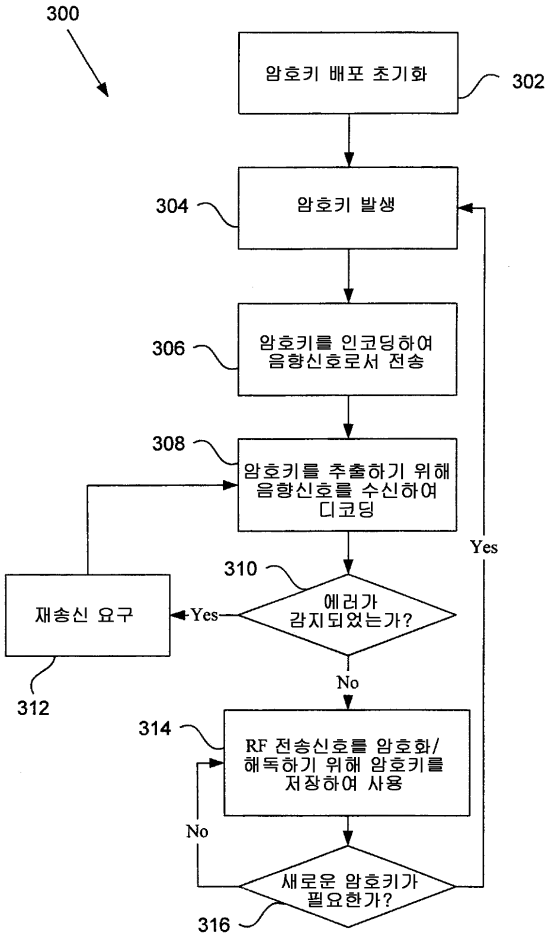
도면 1


제1회의실 100
원격장치 108
기지국 106
114
원격장치 110
벽 104
제2회의실 102
원격장치 112

도면 2


204
암호키
206
메모리
암호키 발생기
202
회의 데이터
226
암호화/해독
음향 코덱
210
208
RF 코덱
214
음향 송신기
106
RF 송수신기
216
212
108
RF 송수신기
228
음향 센서
220
RF 코덱
227
음향 코덱
222
메모리
회의 데이터
226
암호화/해독
225
암호키
204
224

도면 3


300
암호키 배포 초기화
302
304
암호키 발생
306
암호키를 인코딩하여 음향신호로서 전송
308
암호키를 추출하기 위해 음향신호를 수신하여 디코딩
310
에러가 감지되었는가?
Yes
재송신 요구
312
No
314
RF 전송신호를 암호화/해독하기 위해 암호키를 저장하여 사용
No
새로운 암호키가 필요한가?
316
Yes