(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/08

(11) 공개번호 10-2005-0048936
(43) 공개일자 2005년05월25일

(21) 출원번호 10-2003-0082684
(22) 출원일자 2003년11월20일

(71) 출원인 주식회사 팬택
서울특별시 영등포구 여의도동 25-12 신송센타빌딩

(72) 발명자 김현준
서울특별시강북구수유3동130-32호

(74) 대리인 특허법인 신성

심사청구 : 있음

(54) 무선통신단말기에서의 근거리 무선통신 보호 방법

요약

1. 청구범위에 기재된 발명이 속하는 기술분야

본 발명은, 무선통신단말기에서의 근거리 무선통신 보호 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 일반적인 무선통신 모드와 근거리 무선통신 모드의 이중모드를 지원하는 무선통신단말기 등에서 근거리 무선통신 모드로 통화시에, 송신측과 수신측 간에 미리 약속된 비밀키(Kc : Ciphering Key)를 이용하여 암호화된 통화 데이터(speech data)를 송수신함으로써 통화 내용을 보호하기 위한, 무선통신단말기에서의 근거리 무선통신 보호 방법을 제공하는데 그 목적이 있음.

3. 발명의 해결 방법의 요지

본 발명은, 무선통신단말기에서의 근거리 무선통신 보호 방법에 있어서, 서로 상응하는 각 무선통신단말기가 서로 상응하는 비밀키를 각각의 비밀키 테이블(Kc table)에 저장하여 공유하고 있는 제 1 단계; 서로 상응하는 적어도 둘 이상의 무선통신단말기가 근거리 무선통신 모드로 통화가 연결됨에 따라, 각 무선통신단말기가 자신의 비밀키 테이블(Kc table)을 검색하여 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함을 확인하는 제 2 단계; 상기 각 무선통신단말기는 상기 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함에 따라 상기 공유 비밀키(Kc)를 이용하여 통화 데이터(speech data)를 암호화하여 송신하는 제 3 단계; 및 상기 각 무선통신단말기는 상기 상대측 무선통신단말기로부터 암호화된 통화 데이터(speech data)를 수신하여 상기 공유 비밀키(Kc)를 이용하여 복호화하는 제 4 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 무선통신단말기 등에 이용됨.

대표도

도 7

색인어

무선통신단말기, 근거리 무선통신, 암호화 알고리즘(ciphering algorithm), 비밀키(Kc) 공유, 비밀키(Kc) 테이블

명세서

도면의 간단한 설명

도 1은 일반적인 이중모드 무선통신단말기의 일실시예 구성도.

도 2는 일반적인 이중모드 무선통신단말기에서의 근거리 무선통신 모드에 대한 일실시예 설명도.

도 3은 종래의 이중모드 무선통신단말기에서의 근거리 무선통신 방법에 대한 일실시예 신호 흐름도.

도 4는 본 발명에 이용되는 암호화 알고리즘(Ciphered Algorithm)에 대한 일실시예 설명도.

도 5는 본 발명에 따른 비밀키 테이블(Kc : ciphering key)에 대한 일실시예 설명도.

도 6은 본 발명에 따른 무선통신단말기에서의 근거리 무선통신 보호 방법에 대한 일실시예 신호 흐름도.

도 7은 본 발명에 따른 무선통신단말기에서의 근거리 무선통신 보호 방법에 대한 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호 설명

11 : 무선송수신장치 12 : 연산/제어장치

13 : 코덱(CODEC) 14 : 저장장치

15 : 입력장치(키패드) 16 : 표시장치(LCD)

17 : 음성입력장치(마이크) 18 : 음성출력장치(스피커)

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은, 무선통신단말기에서의 근거리 무선통신 보호 방법에 관한 것으로, 더욱 상세하게는 일반적인 무선통신 모드와 근거리 무선통신 모드의 이중모드를 지원하는 무선통신단말기 등에서 근거리 무선통신 모드로 통화시에, 송신측과 수신측 간에 미리 약속된 비밀키(Kc : Ciphering Key)를 이용하여 암호화된 통화 데이터(speech data)를 송수신함으로써 통화 내용을 보호하기 위한, 무선통신단말기에서의 근거리 무선통신 보호 방법에 관한 것이다.

본 발명에서 무선통신단말기란 이동통신단말기, 개인휴대통신단말기(PCS), 개인용디지털단말기(PDA), 스마트폰, 차세대이동통신단말기(IMT-2000), 무선랜 단말기 등과 같이 개인이 휴대하면서 무선통신이 가능한 단말기를 말한다.

또한, 본 발명이 적용되는 무선통신단말기는 기지국 및 무선통신망을 거쳐서 통화하는 일반적인 무선통신 모드와 기지국을 거치지 않고 사용자 간에 소정의 주파수를 공동 사용함으로써 무전기와 같이 동작하는 근거리 무선통신 모드를 지원하는 이중모드 무선통신단말기이다.

이와 같은 이중모드 무선통신단말기는 도서지역이나 산악지역과 같이 전파 환경이 열악한 지역, 호가 폭주하는 지역, 또는 사용자가 서로 근접한 지역 등에서 기지국을 거치지 않고 직접 통화할 수 있으므로 매우 효율적이다. 일반적인 이중모드 무선통신단말기의 구성을 도 1을 참조하여 살펴보기로 한다.

도 1은 일반적인 이중모드 무선통신단말기의 일실시예 구성도이다.

도 1에 도시된 바와 같이, 일반적인 이중모드 무선통신단말기는, 안테나(19,20)를 통하여 무선으로 신호를 송수신하기 위한 이중모드의 무선송수신장치(11), 상기 무선통신단말기를 구동시키고 제어하기 위한 연산/제어장치(12), 상기 연산/제어장치(12)의 제어에 따라 상기 무선송수신장치(11)로부터 전달받은 신호를 음성으로 변환하여 음성출력장치(스피커)(18)로 출력하고, 음성입력장치(마이크)(17)로부터 입력받은 음성을 신호로 변환하여 상기 연산/제어장치(12)로 전달하여 상기 무선송수신장치(11)를 통하여 송출되도록 하기 위한 코덱(CODEC)(13), 상기 무선통신단말기를 구동시키기 위한 프로그램과 파일 시스템(이미지, 캐릭터, 아이콘) 등을 저장하고 있는 저장장치(14), 상기 코덱(CODEC)(13)으로부터 전달받은 음성을 출력하기 위한 음성출력장치(스피커)(18), 상기 연산/제어장치(12)의 제어에 의한 화면을 출력하기 위한 표시장치(LCD)(16), 버튼을 통해 전화번호, 메뉴선택정보 등을 입력받기 위한 입력장치(키패드)(15), 및 음성을 입력받아 상기 코덱(CODEC)(13)으로 전달하기 위한 음성입력장치(마이크)(17)를 포함한다.

이 때, 상기 무선송수신장치(11)는 연산/제어장치(12)의 제어에 따라 일반적인 무선통신 모드 또는 근거리 무선통신 모드로 동작하기 위하여 안테나 스위칭부를 공용으로 사용하고, 도 2에 도시된 바와 같이, 이중모드 무선통신단말기(21,22)의 근거리 무선통신 송신 주파수(f1)와 수신 주파수(f2)가 서로 다르고, 이중모드로 동작하므로 각각의 송신부(무선통신 송신부, 근거리 무선통신 송신부) 및 수신부(무선통신 수신부, 근거리 무선통신 수신부)를 포함한다.

또한, 일반적인 무선통신단말기는 이중모드로 동작하기 위하여 2개의 안테나(19,20)를 포함한다. 만약, 무선송수신장치(11)에 정합장치를 연결한다면 단일 안테나를 통하여 이중모드를 동작시킬 수도 있을 것이다.

한편, 이와 같은 이중모드 무선통신단말기가 근거리 무선통신을 수행하는 과정에 대하여 도 3을 참조하여 살펴보기로 한다.

도 3은 종래의 이중모드 무선통신단말기에서의 근거리 무선통신 방법에 대한 일실시예 신호 흐름도이다.

먼저, 송신측 무선통신단말기(31)가 수신측 무선통신단말기(32)와 근거리 무선통신 모드로 통화하기 위하여 호출 신호(paging signal)를 전송한다(301). 그에 따라 수신측 무선통신단말기(32)가 호출 신호에 대한 응답으로 수락 신호(accept signal)를 전송함으로써 통화 채널이 설정된다(302). 그러면, 송신측 무선통신단말기(31)와 수신측 무선통신단말기(32)는 설정된 통화 채널을 이용하여 통화 데이터(speech data)를 주고받음으로써(303) 근거리 무선통신 모드로 통화가 이루어진다.

그런데, 이와 같은 종래의 근거리 무선통신 방법에서는 일반적인 무선통신과 달리, 송신측 무선통신단말기(31)와 수신측 무선통신단말기(32) 사이에 주고받는 통화 데이터(speech data)가 암호화되지 않기 때문에 통화 내용이 노출될 수 있는 위험성이 있었다.

즉, 이중모드 무선통신단말기가 일반적인 무선통신 모드로 동작할 때에는 도 4에 도시된 바와 같이, 자신이 가진 고유한 가입자 인증키(Ki)와 무선통신망 측에서 제공한 난수(RAND)를 이용하여 비밀키(Kc : ciphering key)를 생성하고, 이를 이용하여 통화 데이터(speech data)를 암호화하는 반면에, 근거리 무선통신 모드로 동작할 때에는 이러한 암호화 과정이 없기 때문에 통화 데이터(speech data)가 보호되지 않는 문제점이 있었다.

왜냐하면, 상기 이중모드 무선통신단말기가 통화 데이터를 암호화하기 위해서는, 도 4에 도시된 바와 같이, 자신이 관리하는 가입자 인증키(ki)와 무선통신망 측으로부터 전달받은 난수(RAND)를 A8 알고리즘에 따라 처리하여 비밀키(Kc : ciphering key)를 생성하고, 이와 같이 생성된 비밀키(Kc)를 이용하여 통화 데이터(speech data)를 A5 알고리즘에 따라 처리하여 암호화(ciphering)하여야 하는데, 상기 이중모드 무선통신단말기가 근거리 무선통신 모드로 동작할 때에는 무선통신망을 거치지 않고 무선통신단말기 간에 직접 통화가 이루어지기 때문에 단말기 정보가 공유되지 않고, 그에 따라 비밀키(Kc) 생성이 불가능하기 때문에 암호화가 불가능하게 된다.

발명이 이루고자 하는 기술적 과제

본 발명은, 상기와 같은 문제점을 해결하기 위하여 제안된 것으로, 일반적인 무선통신 모드와 근거리 무선통신 모드의 이중모드를 지원하는 무선통신단말기 등에서 근거리 무선통신 모드로 통화시에, 송신측과 수신측 간에 미리 약속된 비밀키(Kc : Ciphering Key)를 이용하여 암호화된 통화 데이터(speech data)를 송수신함으로써 통화 내용을 보호하기 위한, 무선통신단말기에서의 근거리 무선통신 보호 방법을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기의 목적을 달성하기 위한 본 발명은, 무선통신단말기에서의 근거리 무선통신 보호 방법에 있어서, 서로 상응하는 각 무선통신단말기가 서로 상응하는 비밀키를 각각의 비밀키 테이블(Kc table)에 저장하여 공유하고 있는 제 1 단계; 서로 상응하는 적어도 둘 이상의 무선통신단말기가 근거리 무선통신 모드로 통화가 연결됨에 따라, 각 무선통신단말기가 자신의 비밀키 테이블(Kc table)을 검색하여 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함을 확인하는 제 2 단계; 상기 각 무선통신단말기는 상기 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함에 따라 상기 공유 비밀키(Kc)를 이용하여 통화 데이터(speech data)를 암호화하여 송신하는 제 3 단계; 및 상기 각 무선통신단말기는 상기 상대측 무선통신단말기로부터 암호화된 통화 데이터(speech data)를 수신하여 상기 공유 비밀키(Kc)를 이용하여 복호화하는 제 4 단계를 포함한다.

상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

도 6은 본 발명에 따른 무선통신단말기에서의 근거리 무선통신 보호 방법에 대한 일실시예 신호 흐름도이다.

먼저, 송신측 무선통신단말기(61)가 수신측 무선통신단말기(62)와 근거리 무선통신 모드로 통화하기 위하여 호출 신호(paging signal)를 전송한다(601). 이 때, 상기 호출 신호(pasing signal)는 송신측 무선통신단말기(61)에 대한 정보를 담고 있으므로, 수신측 무선통신단말기(62)는 송신측 무선통신단말기(61)를 인식할 수 있게 된다.

한편, 수신측 무선통신단말기(62)는 호출 신호(paging signal)에 대한 응답으로 수락 신호(accept signal)를 전송하고(602), 이를 전달받은 송신측 무선통신단말기(61)는 암호화 요청(ciphering request)을 수신측 무선통신단말기(62)로 전송하여(603), 그에 따른 암호화 응답(ciphering response)을 반환받는다(604).

이후, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)는 설정된 통화 채널을 이용하여 암호화된 통화 데이터(speech data)를 주고받게 된다(605). 이 때, 송신측 무선통신단말기(61) 및 수신측 무선통신단말기(62)는 자신의 메모리에 저장되어 있는 비밀키 테이블(Kc table)(도 5에 도시되어 있음)을 참조하여 미리 약속된 공유 비밀키를 적용하여 암호화한 통화 데이터(speech data)를 송신하고, 수신한 통화 데이터(speech data)를 복호화한다.

본 발명에 이용되는 비밀키 테이블(Kc table)은 도 5에 도시된 바와 같이, 상대측 무선통신단말기(예를 들어, 주소록에 등록되어 있는 무선통신단말기, 또는 통화 이력이 있는 무선통신단말기)에 상응하는 비밀키(Kc)가 미리 설정되어 있으며, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)에 공유되어 있어야 한다.

한편, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)가 비밀키 테이블(Kc table)을 이용하는 방법은 여러 가지가 있을 수 있다.

먼저, 상기에서 설명한 방법과 같이, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)가 서로 공유하는 비밀키(Kc)가 설정된 비밀키 테이블(Kc table)을 각각 저장하고 있는 상태에서, 근거리 무선통신 모드로 통화를 하게 되면, 양측의 무선통신단말기 각각은 상기 비밀키 테이블(Kc table)로부터 상대측 무선통신단말기(전화번호 등으로 식별)에 상응하는 비밀키(Kc)를 추출하여 이용한다.

또한, 다른 방법으로서, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)가 다수의 비밀키가 인덱스에 따라 저장되어 있는 비밀키 테이블을 공유(동일한 비밀키 테이블을 저장)하고 있는 상태에서, 근거리 무선통신 모드로 통화를 하게 되면, 송신측 무선통신단말기(61)가 통화 요청시(또는 암호화 요청(ciphering request) 시)에 특정 인덱스를 전달함으로써 수신측 무선통신단말기(62)가 해당 인덱스에 상응하는 비밀키를 공유할 수 있도록 한다.

도 7은 본 발명에 따른 무선통신단말기에서의 근거리 무선통신 보호 방법에 대한 일실시예 흐름도이다.

먼저, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62)의 저장장치에는 서로 공유하는 비밀키가 비밀키 테이블(Kc table)에 저장되어 있어야 한다.

이후, 송신측 무선통신단말기(61)와 수신측 무선통신단말기(62) 간에 근거리 무선통신 모드로 통화가 연결되면(701), 상기 송신측 무선통신단말기(61)와 상기 수신측 무선통신단말기(62) 각각은 자신의 비밀키 테이블(Kc table)에 상대측 무선통신단말기에 상응하는 공유 비밀키(Kc)가 존재하는지를 확인한다(702).

즉, 상기 송신측 무선통신단말기(61)가 자신의 비밀키 테이블(Kc table)을 검색하여 상기 수신측 무선통신단말기(62)에 상응하는 공유 비밀키(Kc)가 존재하는지 확인하고, 상응하는 공유 비밀키(Kc)가 존재하면 암호화 요청(ciphering request)을 상기 수신측 무선통신단말기(62)에 전송한다. 그러면, 상기 수신측 무선통신단말기(62)가 상기 송신측 무선통신단말기(61)로부터의 암호화 요청(ciphering request)에 따라 자신의 비밀키 테이블(Kc table)을 검색하여 상기 송신측 무선통신단말기(61)에 상응하는 공유 비밀키(Kc)가 존재하는지 확인하여, 상응하는 공유 비밀키(Kc)가 존재하면 암호화 응답(ciphering response)을 전송한다.

따라서, 상기 송신측 무선통신단말기(61)가 상기 수신측 무선통신단말기(62)로부터 암호화 응답(ciphering response)을 받았다는 것은 양측에 공유 비밀키(Kc)가 존재한다는 것을 의미한다.

상기 확인 결과(702), 양측(송신측 무선통신단말기(61), 수신측 무선통신단말기(62))에 공유 비밀키(Kc)가 존재하면, 상기 공유 비밀키(Kc)를 이용하여 암호화된 통화 데이터(speech data)를 송수신하여 통화 중에 통화 데이터(speech data)가 보호되도록 한다(703). 즉, 양측의 무선통신단말기가 통화 데이터(speech data)를 송신할 때에는 공유 비밀키(Kc)를 이용하여 암호화한(ciphering) 후 송신하고, 암호화된 통화 데이터(speech data)를 수신한 때에는 공유 비밀키(Kc)를 이용하여 복호화한 후 처리하게 된다.

한편, 상기 확인 결과(702), 양측(송신측 무선통신단말기, 수신측 무선통신단말기) 중 어느 한측이라도 미리 약속된 공유 비밀키(Kc)가 존재하지 않으면, 암호화되지 않은 통화 데이터를 송수신하여 기존의 방식대로 통화하도록 한다(704).

즉, 상기 송신측 무선통신단말기(61)가 자신의 비밀키 테이블(Kc table)을 검색한 결과, 상기 수신측 무선통신단말기(62)에 상응하는 공유 비밀키(Kc)가 존재하지 않으면 암호화 요청(ciphering request)을 전송하지 않고, 기존의 방식대로 통화가 이루어지게 된다.

또한, 상기 수신측 무선통신단말기(62)가 상기 송신측 무선통신단말기(61)로부터의 암호화 요청(ciphering request)에 따라 자신의 비밀키 테이블(Kc table)을 검색한 결과, 상기 송신측 무선통신단말기(61)에 상응하는 공유 비밀키(Kc)가 존재하지 않으면 암호화 응답(ciphering response)을 전송하지 않게 되고, 상기 송신측 무선통신단말기(61)는 암호화 요청(ciphering request) 전송 후 소정 시간 내에 암호화 응답(ciphering response)이 수신되지 않으면 기존의 방식대로 통화가 이루어지게 된다.

이상의 일예에서는 1 대 1 의 근거리 무선통신을 일예로 들어 설명하였으나, 무선통신단말기가 1 대 다의 근거리 무선통신을 수행할 때에도 같은 방법으로 용이하게 적용할 수 있을 것이다.

이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

발명의 효과

상기와 같이 본 발명은, 무선통신 모드와 근거리 무선통신 모드의 이중모드를 지원하는 무선통신단말기 등에서 근거리 무선통신 모드로 통화시에, 송신측과 수신측 간에 미리 약속된 비밀키(Kc : Ciphering Key)를 이용하여 통화 데이터(speech data)를 암호화한 후 송수신함으로써, 도청에 의한 통화 내용 누설을 방지하여 통화 내용을 보호할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

무선통신단말기에서의 근거리 무선통신 보호 방법에 있어서,

서로 상응하는 각 무선통신단말기가 서로 상응하는 비밀키를 각각의 비밀키 테이블(Kc table)에 저장하여 공유하고 있는 제 1 단계;

서로 상응하는 적어도 둘 이상의 무선통신단말기가 근거리 무선통신 모드로 통화가 연결됨에 따라, 각 무선통신단말기가 자신의 비밀키 테이블(Kc table)을 검색하여 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함을 확인하는 제 2 단계;

상기 각 무선통신단말기는 상기 상대측 무선통신단말기와 서로 상응하여 공유하는 비밀키가 존재함에 따라 상기 공유 비밀키(Kc)를 이용하여 통화 데이터(speech data)를 암호화하여 송신하는 제 3 단계; 및

상기 각 무선통신단말기는 상기 상대측 무선통신단말기로부터 암호화된 통화 데이터(speech data)를 수신하여 상기 공유 비밀키(Kc)를 이용하여 복호화하는 제 4 단계

를 포함하는 무선통신단말기에서의 근거리 무선통신 보호 방법.

청구항 2.

제 1 항에 있어서,

상기 제 2 단계는,

서로 상응하는 적어도 둘 이상의 무선통신단말기가 근거리 무선통신 모드로 통화가 연결됨에 따라 송신하고자 하는 특정 무선통신단말기가 자신의 비밀키 테이블(Kc table)을 검색하여 상기 상대측 무선통신단말기에 상응하는 공유 비밀키(Kc)가 존재하는지 확인하여, 상응하는 공유 비밀키(Kc)가 존재함에 따라 암호화 요청(ciphering request)을 상기 상대측 무선통신단말기로 전송하는 제 5 단계;

상기 상대측 무선통신단말기가 상기 특정 무선통신단말기로부터의 암호화 요청(ciphering request)에 따라 자신의 비밀키 테이블(Kc table)을 검색하여 상기 특정 무선통신단말기에 상응하는 공유 비밀키(Kc)가 존재하는지 확인하여, 상응하는 공유 비밀키(Kc)가 존재함에 따라 전송한 암호화 응답(ciphering response)을 상기 특정 무선통신단말기가 수신하는 제 6 단계; 및

상기 특정 무선통신단말기가 상기 상대측 무선통신단말기로부터 수신한 암호화 응답(ciphering response)으로부터 공유하는 비밀키가 존재함을 확인하는 제 7 단계

를 포함하는 무선통신단말기에서의 근거리 무선통신 보호 방법.

청구항 3.

제 1 항 또는 제 2 항에 있어서,

상기 각 무선통신단말기가 상기 상대측 무선통신단말기와 공유하는 비밀키의 존재를 확인하는 과정은,

상기 서로 상응하는 무선통신단말기 간에 미리 약속된 공유 비밀키(Kc)를 저장하고 있는 비밀키 테이블(Kc table)로부터 상기 상대측 무선통신단말기에 상응하는 비밀키를 검색하여 확인하는 것을 특징으로 하는 무선통신단말기에서의 근거리 무선통신 보호 방법.

청구항 4.

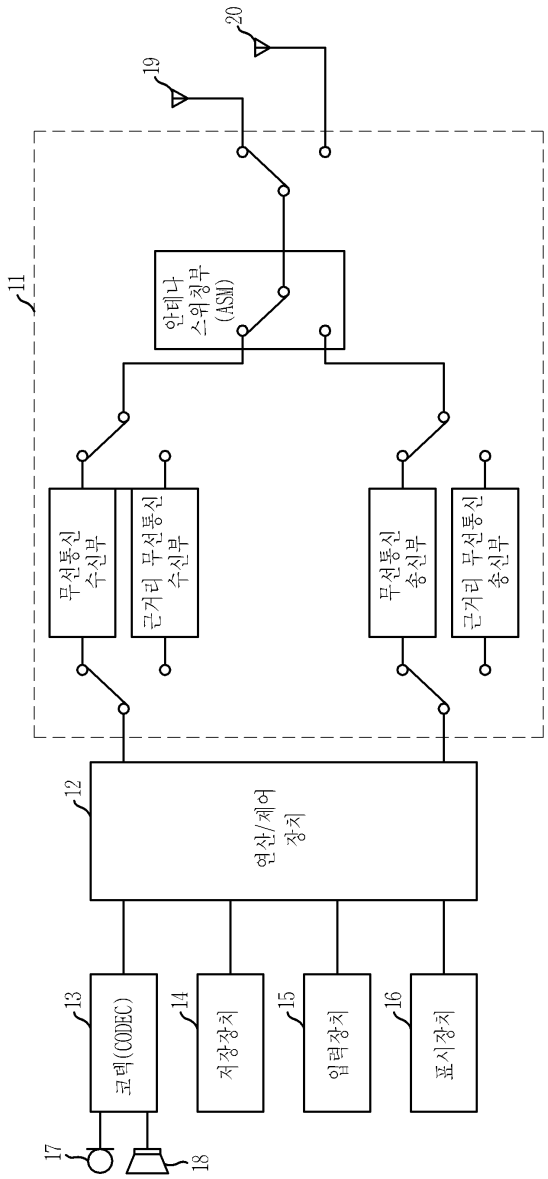
제 1 항 또는 제 2 항에 있어서,

상기 각 무선통신단말기가 상기 상대측 무선통신단말기와 공유하는 비밀키의 존재를 확인하는 과정은,

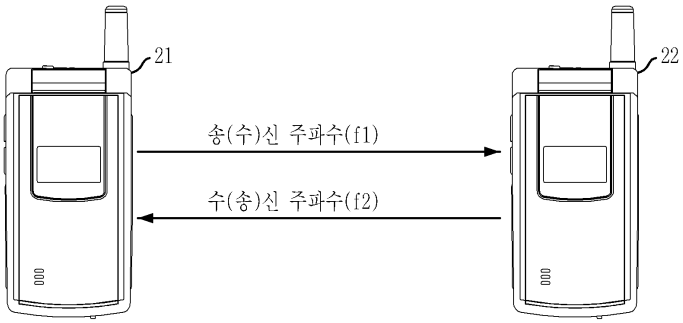
인덱스에 상응하여 비밀키가 설정된 비밀키 테이블(Kc table)을 상기 각 무선통신단말기가 각각 저장하고 있는 상태에서, 어느 하나의 특정 무선통신단말기가 특정 인덱스를 상기 상대측 무선통신단말기로 전달하고, 상기 상대측 무선통신단말기가 자신의 비밀키 테이블(Kc table)로부터 상기 특정 인덱스에 상응하는 비밀키를 검색하여 확인하는 것을 특징으로 하는 무선통신단말기에서의 근거리 무선통신 보호 방법.

도면

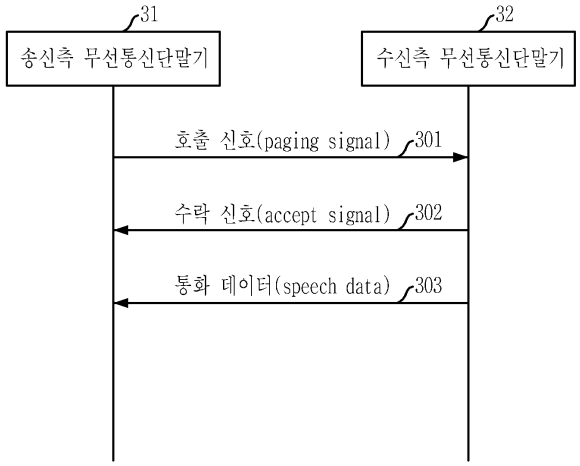
도면1



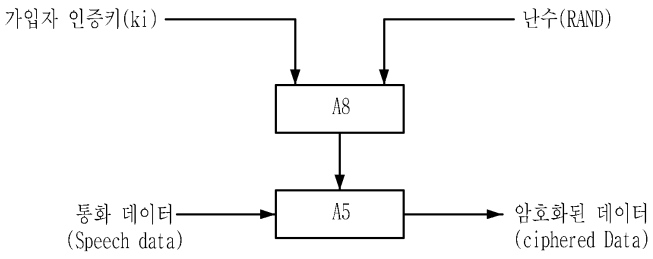
도면2


21
22
송(수)신 주파수(f1)
수(송)신 주파수(f2)

도면3


31
송신측 무선통신단말기
32
수신측 무선통신단말기
호출 신호(paging signal)
301
수락 신호(accept signal)
302
통화 데이터(speech data)
303

도면4

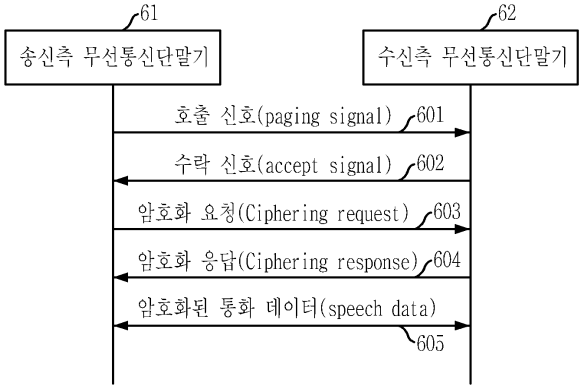

가입자 인증키(ki)
난수(RAND)
A8
A5
통화 데이터
(Speech data)
암호화된 데이터
(ciphered Data)

도면5

비밀키 테이블

상대측 무선통신단말기	Ciphering key(kc)
A	0xFF
B	0x12
C	0xA0
D	0x76

도면6



도면7