



**(19) 대한민국특허청(KR)**  
**(12) 등록특허공보(B1)**

(45) 공고일자 2008년08월13일  
 (11) 등록번호 10-0852146  
 (24) 등록일자 2008년08월07일

(51) Int. Cl.

H04L 12/26 (2006.01) H04L 9/00 (2006.01)

H04L 12/66 (2006.01)

(21) 출원번호 10-2007-0119164

(22) 출원일자 2007년11월21일

심사청구일자 2007년11월21일

(56) 선행기술조사문헌

EP1452000 A2

보안이 적용된 VOIP시스템의 합법적 감청을 위한 미디어 키 분배 기법(한국통신학회논문지, 2006.8)

(73) 특허권자

한국정보보호진흥원

서울특별시 송파구 가락동 78번지 IT벤처타워 서관

(72) 발명자

윤석용

경기도 성남시 중원구 성남동 2396번지 신동아파밀리에1003호

김중만

경기도 남양주시 화도읍 창현리 신명아파트 103동 1108호

(뒷면에 계속)

(74) 대리인

김 순 영, 김영철

전체 청구항 수 : 총 13 항

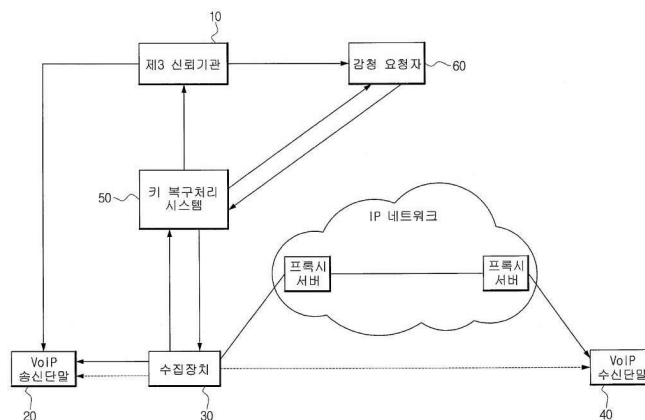
심사관 : 이희봉

**(54) 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청시스템 및 감청 방법**

**(57) 요약**

본 발명은 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템 및 감청 방법에 관한 것이다. 본 발명에 의하면, VoIP 송신단말은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 보안 패킷을 생성한 후 VoIP 수신단말과 통화한다. 키 복구처리 시스템으로부터 감청 명령을 받은 수집 장치는 상기 보안 패킷을 수집하여 키 복구처리 시스템으로 전송하고, 키 복구처리 시스템은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화한 후 감청 요청자에게 제공하거나 또는 제 3 신뢰기관으로부터 수신한 마스터키 및 상기 보안 패킷을 감청 요청자에게 제공해 준다. 이를 통해, VoIP 보안 통신 환경에서 완전한 감청을 제공할 수 있고, 제 3 신뢰기관에서 관리하는 마스터키가 매 통화시 변경되므로 완전 순방향 비밀성(Perfect Forward Secrecy)을 보장할 수 있다.

**대표도**



(72) 발명자

**원용근**

서울특별시 송파구 가락2동 154-9번지 B02호

**원유재**

경기도 용인시 수지구 신봉동 LG 빌리지5차 APT  
515동1401호

**정현철**

서울특별시 송파구 오금동 55-14 멀티파크 B동 20  
1호

## 특허청구의 범위

### 청구항 1

제 3 신뢰기관을 이용한 VoIP 송신단말 및 VoIP 수신단말 간의 보안 통신을 감청하기 위한 시스템으로서,

상기 VoIP 송신단말로부터 마스터키 요청을 수신하여 마스터키를 생성하고, 생성한 마스터키를 상기 VoIP 송신단말 및 키 복구처리 시스템으로 전송하는 제 3 신뢰기관;

감청 요청자로부터의 감청 요청을 받아 수집장치로 감청 명령을 하고, 상기 수집장치로부터 보안 패킷을 수신하고 상기 제 3 신뢰기관으로부터 상기 마스터키를 수신하며, 상기 마스터키를 이용하여 상기 보안 패킷을 복호화하여 상기 감청 요청자에게 복호화된 패킷을 제공하거나 상기 마스터키 및 상기 보안 패킷을 상기 감청 요청자에게 제공하는 키 복구처리 시스템; 및

상기 키 복구처리 시스템으로부터 수신한 감청 명령에 따라 상기 VoIP 송신단말과 상기 VoIP 수신단말간에 송수신되는 보안 패킷을 수집하고, 수집한 보안 패킷을 상기 키 복구처리 시스템으로 전송하는 수집장치를 포함하는 것을 특징으로 하는 감청 시스템.

### 청구항 2

제 1 항에 있어서,

상기 제 3 신뢰기관은,

상기 마스터키를 이용하여 세션키를 생성하고, 상기 세션키를 키복구처리 시스템으로 전송하는 기능을 추가적으로 수행하고,

상기 키 복구처리 시스템은,

감청 요청자로부터의 감청 요청을 받아 수집장치로 감청 명령을 하고, 상기 수집장치로부터 보안 패킷을 수신하고 상기 제 3 신뢰기관으로부터 상기 세션키를 수신하며, 상기 세션키를 이용하여 상기 보안 패킷을 복호화하여 상기 감청 요청자에게 복호화된 패킷을 제공하거나 상기 세션키 및 상기 보안 패킷을 상기 감청 요청자에게 제공하는 것을 특징으로 하는 감청 시스템.

### 청구항 3

제 2 항에 있어서,

상기 제 3 신뢰기관은,

상기 VoIP 송신단말로부터의 마스터키 요청에 따라 마스터키를 생성하고, 상기 마스터키를 이용하여 세션키를 생성하는 암호키 생성부;

상기 암호키 생성부에 의해 생성된 상기 마스터키 및 상기 세션키를 저장하는 저장부;

상기 마스터키를 상기 VoIP 송신단말로 전송하고, 상기 세션키를 상기 키 복구처리 시스템으로 전송하는 전송부; 및

상기 제 3 신뢰기관을 구성하는 각 구성요소들의 제어를 담당하는 제어부를 포함하는 것을 특징으로 하는 감청 시스템.

### 청구항 4

제 3 항에 있어서,

상기 제어부는 키 복구 요청 기록 관리 및 감사 관리 기능을 추가적으로 수행하는 것을 특징으로 하는 감청 시스템.

### 청구항 5

제 1 항 또는 제 2 항에 있어서,

상기 키 복구처리 시스템은,

상기 제 3 신뢰기관으로부터 수신한 마스터키 또는 세션키를 이용하여 상기 수집장치로부터 수신한 보안 패킷을 복호화하는 복호부;

상기 복호부에 의해 복호화된 패킷으로부터 추출된 상기 VoIP 송신단말과 상기 VoIP 수신단말간의 통화 정보를 저장하는 저장부;

상기 수집장치로부터 보안 패킷을 수신하고, 상기 제 3 신뢰기관으로부터 마스터키 또는 세션키를 수신하며, 감청 요청자에게 상기 복호화된 패킷을 전송하는 전송부; 및

상기 키 복구처리 시스템을 구성하는 각 구성요소들의 제어를 담당하는 제어부를 포함하는 것을 특징으로 하는 감청 시스템.

#### 청구항 6

제 5 항에 있어서,

상기 통화 정보는 VoIP 송신단말 및 수신단말의 ID, VoIP 송신단말 및 수신단말의 IP/Port, 통화개시시간 및 통화종료시간 정보를 포함하는 것을 특징으로 하는 감청 시스템.

#### 청구항 7

제 5 항에 있어서,

상기 제어부는 키 복구 요청 기록 관리 및 감사 관리 기능을 추가적으로 수행하는 것을 특징으로 하는 감청 시스템.

#### 청구항 8

제 3 신뢰기관을 이용한 VoIP 송신단말 및 VoIP 수신단말 간의 보안 통신을 감청하기 위한 방법으로서,

키 복구처리 시스템이 감청 요청자로부터의 감청 요청에 따라 수집장치에 감청 명령을 하는 단계(a);

상기 제 3 신뢰기관이 상기 VoIP 송신단말로부터의 마스터키 요청을 수신하여 마스터키를 생성하고 생성한 마스터키를 상기 VoIP 송신단말로 전송하는 단계(b);

상기 VoIP 송신단말 및 VoIP 수신단말간에 상기 마스터키를 교환하고 보안 통신을 수행하는 단계(c);

상기 수집장치가 상기 VoIP 송신단말 및 VoIP 수신단말간에 송수신되는 보안 패킷을 수집하여 상기 키 복구처리 시스템으로 전송하는 단계(d); 및

상기 키 복구처리 시스템이 상기 제 3 신뢰기관으로부터 마스터키를 수신하고 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화하여 상기 감청 요청자에게 복호화된 패킷을 제공하는 단계(e)를 포함하는 것을 특징으로 하는 감청 방법.

#### 청구항 9

제 8 항에 있어서,

상기 단계(c)는,

상기 VoIP 송신단말 및 VoIP 수신단말간에 상기 마스터키를 교환하는 단계(c1); 및

상기 제 3 신뢰기관, 상기 VoIP 송신단말 및 상기 VoIP 수신단말 각각에서 상기 마스터키를 이용하여 세션키를 생성한 후 보안 통신을 수행하는 단계(c2)를 포함하며,

상기 단계(e)는,

상기 키 복구처리 시스템이 상기 제 3 신뢰기관으로부터 상기 세션키를 수신하고 상기 세션키를 이용하여 상기 보안 패킷을 복호화하여 상기 감청 요청자에게 복호화된 패킷을 제공하는 것을 특징으로 하는 감청 방법.

#### 청구항 10

제 8 항 또는 제 9 항에 있어서,

상기 단계(c)에서 상기 VoIP 송신단말 및 상기 VoIP 수신단말간의 마스터키의 교환은,

상기 VoIP 송신단말이 상기 VoIP 수신단말로 상기 마스터키를 포함하는 INVITE 메시지를 전송하는 단계; 및

상기 VoIP 수신단말이 상기 VoIP 송신단말로 상기 INVITE 메시지에 대한응답 메시지를 전송하는 단계를 포함하는 것을 특징으로 하는 감청 방법.

#### 청구항 11

제 8 항에 있어서,

상기 단계(e)는,

상기 키 복구처리 시스템이 상기 제 3 신뢰기관으로부터 마스터키를 수신하고 수신한 마스터키 및 상기 수집장치로부터 수신한 보안 패킷을 상기 감청 요청자에게 제공하는 것을 특징으로 하는 감청 방법.

#### 청구항 12

제 9 항에 있어서,

상기 단계(e)는,

상기 키 복구처리 시스템이 상기 제 3 신뢰기관으로부터 세션키를 수신하고 수신한 세션키 및 상기 수집장치로부터 수신한 보안 패킷을 상기 감청 요청자에게 제공하는 것을 특징으로 하는 감청 방법.

#### 청구항 13

제 11 항 또는 제 12 항에 있어서,

상기 단계(c)에서 상기 VoIP 송신단말 및 상기 VoIP 수신단말간의 마스터키의 교환은,

상기 VoIP 송신단말이 상기 VoIP 수신단말로 상기 마스터키를 포함하는 INVITE 메시지를 전송하는 단계; 및

상기 VoIP 수신단말이 상기 VoIP 송신단말로 상기 INVITE 메시지에 대한응답 메시지를 전송하는 단계를 포함하는 것을 특징으로 하는 감청 방법.

### 명세서

#### 발명의 상세한 설명

##### 기술분야

- <1> 본 발명은 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템 및 감청 방법에 관한 것이다. 본 발명에 의하면, VoIP 송신단말은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 보안 패킷을 생성한 후 VoIP 수신단말과 통화한다. 키 복구처리 시스템으로부터 감청 명령을 받은 수집 장치는 상기 보안 패킷을 수집하여 키 복구처리 시스템으로 전송하고, 키 복구처리 시스템은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화한 후 감청 요청자에게 제공하거나 또는 제 3 신뢰기관으로부터 수신한 마스터키 및 상기 보안 패킷을 감청 요청자에게 제공해 준다.. 이를 통해, VoIP 보안 통신 환경에서 완전한 감청을 제공할 수 있고, 제 3 신뢰기관에서 관리하는 마스터키가 매 통화시 변경되므로 완전 순방향 비밀성(Perfect Forward Secrecy)을 보장할 수 있다.

##### 배경기술

- <2> 현재, 공중 전화망(Public Switched Telephone Network; PSTN)에서 가입자들간의 통화 내용을 감청하는 방법은 널리 사용되고 있다. 또한, IP(Internet Protocol)를 사용하여 음성 정보를 전달하기 위한 VoIP(Voice over Internet Protocol)가 널리 사용됨에 따라, VoIP 망에서의 감청 방법도 제안되고 있다.
- <3> 한편, 제 3 신뢰기관(Trusted Third Party; TTP)은 사용자 인증 및 키 관리 등에서 사용자들로부터 신뢰를 얻고 중재, 인증, 증명, 관리 등을 수행하는 기관을 일컫는 것으로, VoIP 망에서의 보안 통신을 위해 암호

키의 관리를 수행하는 제 3 신뢰기관이 사용되기도 한다.

- <4> 종래의 VoIP 망에서의 감청 방법은 VoIP에서의 일반 통화에 대한 감청 방법에 관한 것으로, 상기와 같이 제 3 신뢰기관을 이용한 보안 통화에서 제 3 신뢰기관을 이용하여 감청을 수행하기 위한 기술은 개시되어 있지 않다.

**발명의 내용**

**해결 하고자하는 과제**

- <5> 본 발명은 전술한 바와 같은 문제점을 해결하기 위하여 안출된 것으로, 본 발명에서는, VoIP 송신단말이 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 보안 패킷을 생성한 후 VoIP 수신단말과 통화하는 동안, 키 복구처리 시스템으로부터 감청 명령을 받은 수집 장치가 상기 보안 패킷을 수집하여 키 복구처리 시스템으로 전송하고, 키 복구처리 시스템이 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화한 후 감청 요청자에게 제공하거나 또는 제 3 신뢰기관으로부터 수신한 마스터키 및 상기 보안 패킷을 감청 요청자에게 제공하는 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템 및 감청 방법을 제공하는 것을 목적으로 한다.

**과제 해결수단**

- <6> 본 발명은 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템에 관한 것이다. 상기 시스템은 제 3 신뢰기관을 이용한 VoIP 송신단말 및 VoIP 수신단말 간의 보안 통신을 감청하기 위한 시스템으로서, 상기 VoIP 송신단말로부터 수신한 마스터키 요청에 따라 마스터키를 생성하여 상기 VoIP 송신단말로 전송하고, 상기 마스터키를 이용하여 생성한 세션키를 키 복구처리 시스템으로 전송하는 제 3 신뢰기관; 감청 요청자로부터의 감청 요청을 받아 수집장치로 감청 명령을 하고, 상기 수집장치로부터 보안 패킷을 수신하고 상기 제 3 신뢰기관으로부터 상기 세션키를 수신하며, 상기 세션키를 이용하여 상기 보안 패킷을 복호화하여 상기 감청 요청자에게 복호화된 패킷을 제공하는 키 복구처리 시스템; 및 상기 키 복구처리 시스템으로부터 수신한 감청 명령에 따라 상기 VoIP 송신단말과 상기 VoIP 수신단말간에 송수신되는 보안 패킷을 수집하고, 수집한 보안 패킷을 상기 키 복구처리 시스템으로 전송하는 수집장치를 포함한다.

- <7> 또한, 본 발명은 제 3 신뢰기관을 이용하여 VoIP 보안 통신에서 감청하는 방법에 관한 것이다. 상기 방법은 제 3 신뢰기관을 이용한 VoIP 송신단말 및 VoIP 수신단말 간의 보안 통신을 감청하기 위한 방법으로서, 키 복구처리 시스템이 감청 요청자로부터의 감청 요청에 따라 수집장치에 감청 명령을 하는 단계(a); 상기 제 3 신뢰기관이 상기 VoIP 송신단말로부터의 마스터키 요청에 따라 마스터키를 생성하여 상기 VoIP 송신단말로 전송하는 단계(b); 상기 VoIP 송신단말 및 VoIP 수신단말간에 상기 마스터키를 교환하는 단계(c); 상기 제 3 신뢰기관, 상기 VoIP 송신단말 및 상기 VoIP 수신단말 각각에서 상기 마스터키를 이용하여 세션키를 생성한 후 보안 통신을 수행하는 단계(d); 상기 수집장치가 상기 VoIP 송신단말 및 VoIP 수신단말간에 송수신되는 보안 패킷을 수집하여 상기 키 복구처리 시스템으로 전송하는 단계(e); 상기 키 복구처리 시스템이 상기 제 3 신뢰기관으로부터 수신한 세션키를 이용하여 상기 보안 패킷을 복호화하는 단계(f); 및 상기 키 복구처리 시스템이 복호화된 패킷을 상기 감청 요청자에게 제공하는 단계(g)를 포함한다.

**효과**

- <8> 본 발명에 의하면, VoIP 송신단말은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 보안 패킷을 생성한 후 VoIP 수신단말과 통화한다. 키 복구처리 시스템으로부터 감청 명령을 받은 수집 장치는 상기 보안 패킷을 수집하여 키 복구처리 시스템으로 전송하고, 키 복구처리 시스템은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화한 후 감청 요청자에게 제공하거나 또는 제 3 신뢰기관으로부터 수신한 마스터키 및 상기 보안 패킷을 감청 요청자에게 제공해 준다. 이를 통해, VoIP 보안 통신 환경에서 완전한 감청을 제공할 수 있고, 제 3 신뢰기관에서 관리하는 마스터키가 매 통화시 변경되므로 완전 순방향 비밀성(Perfect Forward Secrecy)을 보장할 수 있다.

**발명의 실시를 위한 구체적인 내용**

- <9> 이하에서는, 도면을 참조하여 본 발명의 실시예를 구체적으로 설명한다. 그러나, 본 발명이 하기의 실시예에 의하여 제한되는 것은 아니다.

- <10> 도 1은 본 발명에 따른 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템의 구성을 도시한 도면이다.
- <11> 본 발명에 따른 감청 시스템은 제 3 신뢰기관(10), VoIP 송신단말(20), 수집장치(30), VoIP 수신단말(40) 및 키 복구처리 시스템(50)을 포함한다.
- <12> 제 3 신뢰기관(10)은 VoIP 단말간의 보안 통신을 위해 암호키의 관리를 수행하는 기관이다.
- <13> 일 실시예에 따르면, 제 3 신뢰기관(10)이 VoIP 송신단말(20)로부터 VoIP 수신단말(40)과의 보안 통신을 위해 필요한 암호키의 일종인 마스터키(Traffic Generation Key; TGK)를 요청 받으면, 마스터키를 생성하여 VoIP 송신단말(20)로 전송한다. 또한, 제 3 신뢰기관(10)은 키 복구처리 시스템(50)으로도 상기 마스터키를 전송하여, 키 복구처리 시스템(50)이 후술하는 바와 같이 보안 패킷을 복호화할 수 있도록 한다.
- <14> 다른 방법으로는, 제 3 신뢰기관(10)이 VoIP 송신단말(20)로부터 VoIP 수신단말(40)과의 보안 통신을 위해 필요한 암호키의 일종인 마스터키를 요청 받으면, 마스터키를 생성하여 VoIP 송신단말(20)로 전송한다. 그 후, 제 3 신뢰기관(10)은 상기 마스터키로부터 세션키를 생성하고, 상기 세션키를 키 복구처리 시스템(50)으로 전송할 수도 있다. 이 때, 세션키는 VoIP 송신단말(20)과 수신단말(40)간의 음성 패킷을 실제로 암호화하는데 사용되는 암호키이다.
- <15> 도 2는 본 발명의 일 실시예에 따른 제 3 신뢰기관의 상세 구성을 도시한 도면으로, 구체적으로는, 제 3 신뢰기관(10)은 제어부(11), 암호키 생성부(12), 저장부(13) 및 전송부(14)를 포함한다.
- <16> 암호키 생성부(12)는 VoIP 송신단말(20)로부터의 암호키 요청이 있으면, 제어부(11)의 제어에 따라 마스터키를 생성하고, 상기 마스터키로부터 세션키를 생성한다.
- <17> 저장부(13)는 제어부(11)의 제어에 따라 암호키 생성부(12)에 의해 생성된 마스터키 및 세션키를 저장한다.
- <18> 전송부(14)는 제어부(11)의 제어에 따라 마스터키 및 세션키를 각각 VoIP 송신단말(20) 및 키 복구처리 시스템(50)으로 전송한다.
- <19> 제어부(11)는 제 3 신뢰기관(10)을 구성하는 각 구성요소들의 제어를 담당하며, 필요에 따라 키 복구 요청 기록 관리 및 감사 관리 등의 부가적인 기능을 수행할 수도 있다.
- <20> 수집장치(30)는 키 복구처리 시스템(50)으로부터 수신한 감청 명령에 따라 감청의 대상이 되는 VoIP 송신단말(20)과 VoIP 수신단말(40)간에 송수신되는 보안 패킷을 수집하고, 수집한 보안 패킷을 키 복구처리 시스템(50)으로 전송한다.
- <21> 키 복구처리 시스템(50)은 감청 요청자(60)로부터 감청 요청을 받아 수집장치(30)로 감청 명령을 한다. 또한, 키 복구처리 시스템(50)은 수집장치(30)로부터 보안 패킷을 수신하고 제 3 신뢰기관(10)으로부터 마스터키 또는 세션키를 수신한 후, 상기 마스터키 또는 세션키를 이용하여 상기 보안 패킷을 복호화하여 감청 요청자(60)에게 제공한다. 다른 방법으로는, 키 복구처리 시스템(50)은 제 3 신뢰기관(10)으로부터 수신한 마스터키 또는 세션키 및 상기 보안 패킷을 함께 감청 요청자(60)에게 제공하여, 감청 요청자(60)가 보안 패킷을 복호화하도록 할 수도 있다.
- <22> 도 3은 본 발명의 일 실시예에 따른 키 복구처리 시스템의 상세 구성을 도시한 도면으로, 구체적으로는, 키 복구처리 시스템(50)은 제어부(51), 복호부(52), 저장부(53) 및 전송부(54)를 포함한다.
- <23> 복호부(52)는 제 3 신뢰기관(10)으로부터 수신한 마스터키 또는 세션키를 이용하여 수집장치(30)로부터 수신한 보안 패킷을 복호화한다.
- <24> 저장부(53)는 제어부(51)의 제어에 따라 VoIP 송신단말(20)과 VoIP 수신단말(40)간의 통화 정보, 예를 들어 송수신단말의 ID, 송수신단말의 IP/Port, 통화개시시간, 통화종료시간 등과 같은 정보를 저장한다. 이 때, 통화 정보는 복호부(52)에서 복호화된 패킷으로부터 추출된다.
- <25> 전송부(54)는 수집장치(30)로부터 보안 패킷을 수신하고 제 3 신뢰기관(10)으로부터 마스터키 또는 세션키를 수신하며 감청 요청자(60)에게 복호화된 패킷을 전송한다.
- <26> 제어부(51)는 키 복구처리 시스템(50)을 구성하는 각 구성요소들의 제어를 담당하며, 필요에 따라 키 복구 요청 기록 관리 및 감사 관리 등의 부가적인 기능을 수행할 수도 있다.

- <27> 이하, 도 4 및 도 5를 참조하여 본 발명에 따른 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 방법을 설명한다.
- <28> 도 4는 본 발명의 일 실시예에 따라 제 3 신뢰기관을 이용하여 VoIP 보안 통신에서 감청하는 과정을 도시한 흐름도이다.
- <29> 우선, 감청 요청자(60)가 키 복구처리 시스템(50)으로 감청 대상 단말 정보, 예를 들어 송수신단말의 ID, 송수신단말의 IP/Port 정보를 제공하며 감청 요청을 하면(S10), 키 복구처리 시스템(50)은 수집장치(30)로 상기 감청 대상 단말 정보를 전송하며 감청 명령을 한다(S11).
- <30> 한편, VoIP 송신단말(20)이 VoIP 수신단말(40)과의 보안 통신을 위해 제 3 신뢰기관(10)으로 마스터키를 요청하면(S12), 제 3 신뢰기관(10)은 마스터키를 생성하여 VoIP 송신단말(20)로 전송한다(S13).
- <31> 이 후, VoIP 송신단말(20)이 VoIP 수신단말(40)과의 보안 통신 개시를 위해 VoIP 수신단말(40)로 상기 마스터키를 포함하는 INVITE 메시지를 전송하면(S14), VoIP 수신단말(40)이 VoIP 송신단말(20)로 응답 메시지를 전송한 후(S15), VoIP 송신단말(20)과 VoIP 수신단말(40)간의 보안 통신이 이루어진다(S16).
- <32> 이처럼, VoIP 송신단말(20)과 VoIP 수신단말(40)간의 보안 통화가 이루어지는 동안, 수집장치(30)는 감청 대상인 VoIP 송신단말(20)과 VoIP 수신단말(40)간에 송수신되는 보안 패킷을 수집하고(S17), 수집한 보안 패킷을 키 복구처리 시스템(50)으로 전송한다(S18).
- <33> 이 후, 키 복구처리 시스템(50)은 제 3 신뢰기관(10)으로부터 마스터키를 수신하고(S19), 상기 마스터키를 이용하여 수집장치(30)로부터 수신한 보안 패킷을 실시간으로 복호화한 후(S20), 복호화된 패킷을 감청 요청자(60)에게 제공한다(S21).
- <34> 다른 방법으로는, 상기 단계 S19 이후에, 키 복구처리 시스템(50)이 제 3 신뢰기관(10)으로부터 수신한 마스터키 및 수집장치(30)로부터 수신한 보안 패킷을 함께 감청 요청자(60)에게 제공함으로써(미도시), 감청 요청자(60)가 직접 보안 패킷을 복호화하도록 할 수도 있다.
- <35> 도 5는 본 발명의 다른 실시예에 따라 제 3 신뢰기관을 이용하여 VoIP 보안 통신에서 감청하는 과정을 도시한 흐름도이다.
- <36> 우선, 감청 요청자(60)가 키 복구처리 시스템(50)으로 감청 대상 단말 정보, 예를 들어 송수신단말의 ID, 송수신단말의 IP/Port 정보를 제공하며 감청 요청을 하면(S30), 키 복구처리 시스템(50)은 수집장치(30)로 상기 감청 대상 단말 정보를 전송하며 감청 명령을 한다(S31).
- <37> 한편, VoIP 송신단말(20)이 VoIP 수신단말(40)과의 보안 통신을 위해 제 3 신뢰기관(10)으로 마스터키를 요청하면(S32), 제 3 신뢰기관(10)은 마스터키를 생성하여 VoIP 송신단말(20)로 전송한다(S33).
- <38> 이 후, VoIP 송신단말(20)이 VoIP 수신단말(40)과의 보안 통신 개시를 위해 VoIP 수신단말(40)로 상기 마스터키를 포함하는 INVITE 메시지를 전송하면(S34), VoIP 수신단말(40)이 VoIP 송신단말(20)로 응답 메시지를 전송한다(S35).
- <39> 이 후, 제 3 신뢰기관(10), VoIP 송신단말(20) 및 VoIP 수신단말(40) 각각에서는 상기 마스터키로부터 세션키를 생성한 후(S36), VoIP 송신단말(20)과 VoIP 수신단말(40)간의 보안 통신이 이루어진다(S37).
- <40> 이처럼, VoIP 송신단말(20)과 VoIP 수신단말(40)간의 보안 통화가 이루어지는 동안, 수집장치(30)는 감청 대상인 VoIP 송신단말(20)과 VoIP 수신단말(40)간에 송수신되는 보안 패킷을 수집하고(S38), 수집한 보안 패킷을 키 복구처리 시스템(50)으로 전송한다(S39).
- <41> 이 후, 키 복구처리 시스템(50)은 제 3 신뢰기관(10)으로부터 세션키를 수신하고(S40), 상기 세션키를 이용하여 수집장치(30)로부터 수신한 보안 패킷을 실시간으로 복호화한 후(S41), 복호화된 패킷을 감청 요청자(60)에게 제공한다(S42).
- <42> 다른 방법으로는, 상기 단계 S40 이후에, 키 복구처리 시스템(50)이 제 3 신뢰기관(10)으로부터 수신한 세션키 및 수집장치(30)로부터 수신한 보안 패킷을 함께 감청 요청자(60)에게 제공함으로써(미도시), 감청 요청자(60)가 직접 보안 패킷을 복호화하도록 할 수도 있다.
- <43> 본 발명에 따른 실시예는 상술한 것으로 한정되지 않고, 본 발명과 관련하여 통상의 지식을 가진 자에게 자명한 범위 내에서 여러 가지의 대안, 수정 및 변경하여 실시할 수 있다.



**산업이용 가능성**

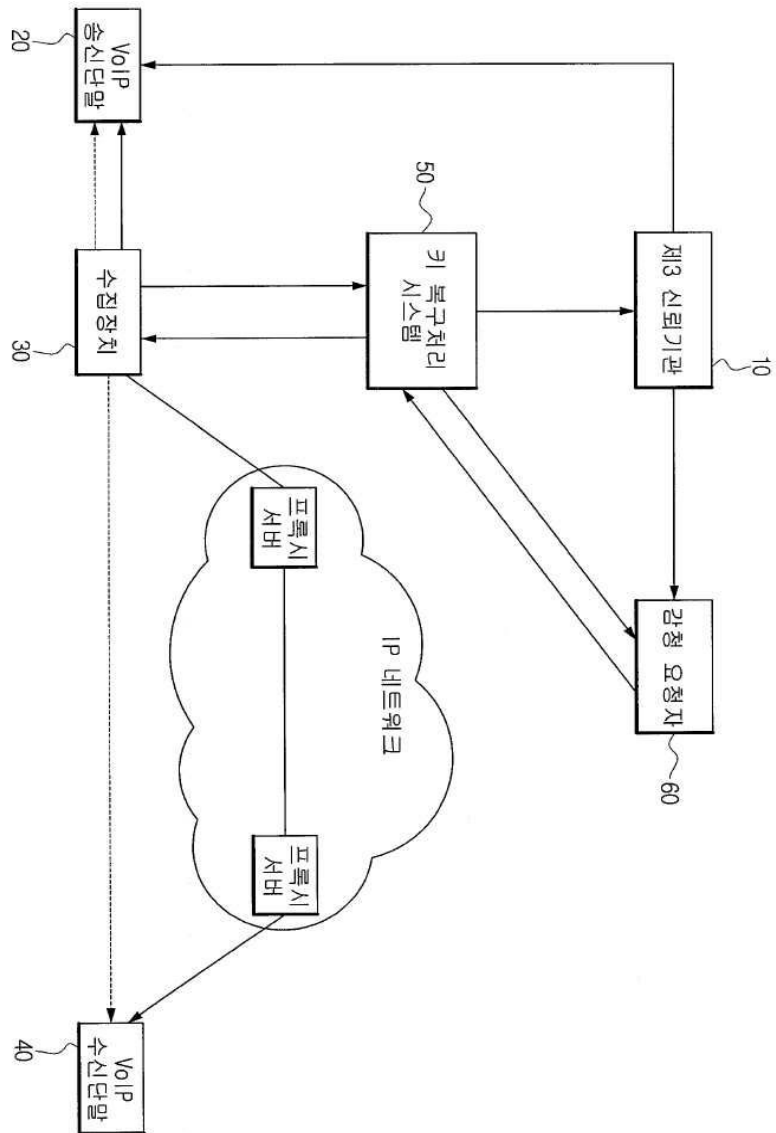
<44> 본 발명에 의하면, VoIP 송신단말은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 보안 패킷을 생성한 후 VoIP 수신단말과 통화한다. 키 복구처리 시스템으로부터 감청 명령을 받은 수집 장치는 상기 보안 패킷을 수집하여 키 복구처리 시스템으로 전송하고, 키 복구처리 시스템은 제 3 신뢰기관으로부터 수신한 마스터키를 이용하여 상기 보안 패킷을 복호화한 후 감청 요청자에게 제공하거나 또는 제 3 신뢰기관으로부터 수신한 마스터키 및 상기 보안 패킷을 감청 요청자에게 제공해 준다.. 이를 통해, VoIP 보안 통신 환경에서 완전한 감청을 제공할 수 있고, 제 3 신뢰기관에서 관리하는 마스터키가 매 통화시 변경되므로 완전 순방향 비밀성(Perfect Forward Secrecy)을 보장할 수 있다.

**도면의 간단한 설명**

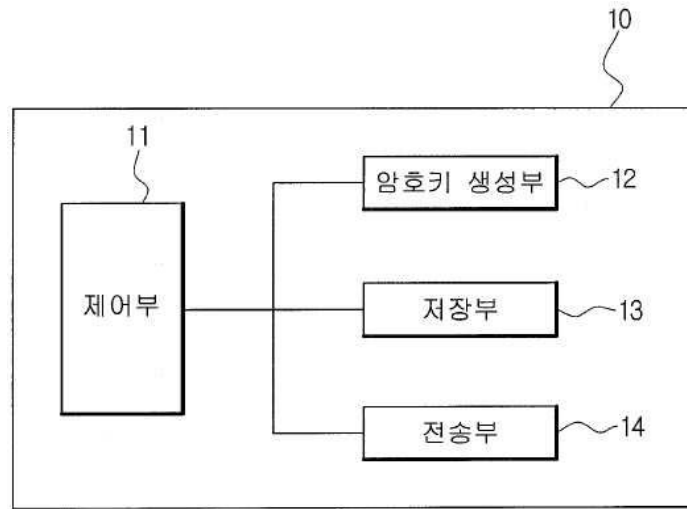
- <45> 도 1은 본 발명에 따른 제 3 신뢰기관을 이용한 VoIP 보안 통신에서의 감청 시스템의 구성을 도시한 도면.
- <46> 도 2는 본 발명의 일 실시예에 따른 제 3 신뢰기관의 상세 구성을 도시한 도면.
- <47> 도 3은 본 발명의 일 실시예에 따른 키 복구처리 시스템의 상세 구성을 도시한 도면.
- <48> 도 4는 본 발명의 일 실시예에 따라 제 3 신뢰기관을 이용하여 VoIP 보안 통신에서 감청하는 과정을 도시한 흐름도.
- <49> 도 5는 본 발명의 다른 실시예에 따라 제 3 신뢰기관을 이용하여 VoIP 보안 통신에서 감청하는 과정을 도시한 흐름도.

도면

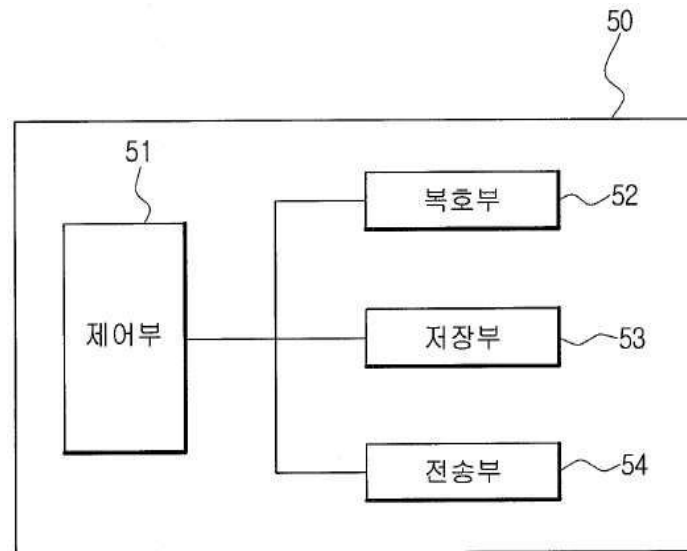
도면1



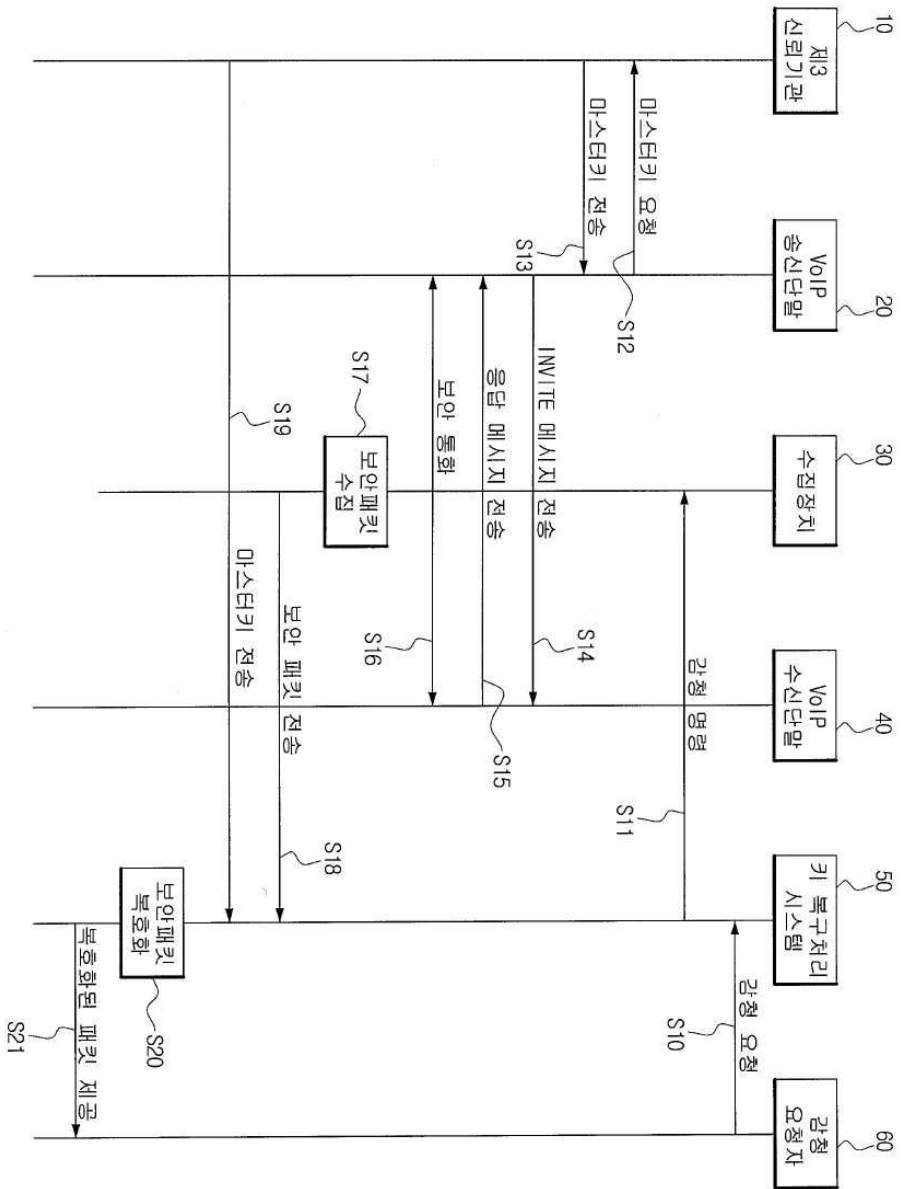
도면2



도면3



도면4



도면5

