(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년07월30일
(11) 등록번호 10-0910139
(24) 등록일자 2009년07월24일

(51) Int. Cl.
H04L 9/18 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2006-7027485
(22) 출원일자 2005년04월08일
심사청구일자 2006년12월27일
(85) 번역문제출일자 2006년12월27일
(65) 공개번호 10-2007-0015466
(43) 공개일자 2007년02월02일
(86) 국제출원번호 PCT/US2005/012068
(87) 국제공개번호 WO 2005/119963
국제공개일자 2005년12월15일
(30) 우선권주장
10/856,928 2004년05월27일 미국(US)
(56) 선행기술조사문헌
US5412722 A
US5404403 A
US5404404 A
EP0898260 A
전체 청구항 수 : 총 64 항

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
브렛 브렌든
미국 92109 캘리포니아주 샌디에고 사파이어 스트리트 727넘버411
마샬 마리아
미국 92054 캘리포니아주 오션사이드 푸에르테 스트리트 2286
(74) 대리인
특허법인코리아나

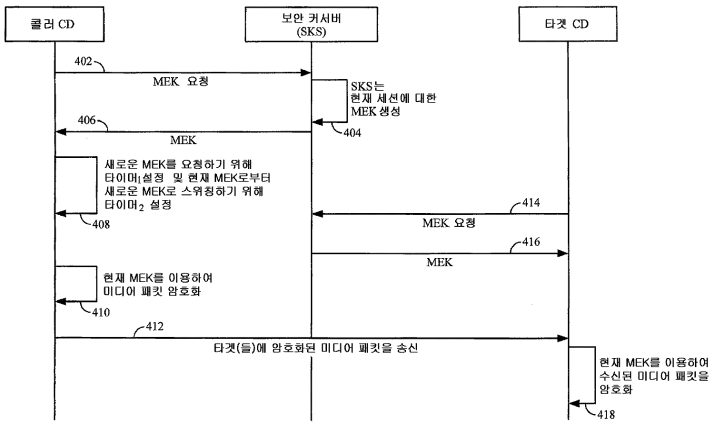
심사관 : 양종필

(54) 진행중인 미디어 통신 세션 동안 암호 키의 변환을 위한방법 및 장치

(57) 요 약

개시된 실시형태는 현재 미디어 암호 키 (MEK) 를 이용하여 미디어를 암호화하고, 새로운 MEK 를 요청하고, 새로운 MEK 를 수신하는 방법 및 장치를 제공한다. 본 방법은 현재 MEK 로부터 새로운 MEK 로 변환하여 새로운 MEK 를 이용하여 미디어를 암호화하기를 계속하는 단계를 더 포함한다. 또 다른 실시형태에서, 본 방법은 진행중인 미디어 통신 세션 동안 미디어를 해독하는 단계를 제공하고, 본 방법은 암호화된 미디어를 수신하여, 새로운 MEK 를 이용하여 암호화된 미디어를 해독하는 단계를 제공한다. 본 방법은 현재 MEK 의 관련 만료 타임에 기초하여 현재 MEK 가 만료하기 이전에 새로운 MEK 를 요청하고, 새로운 MEK 를 수신하여, 암호화된 미디어가 현재 MEK 또는 새로운 MEK 를 이용하여 암호화되었는지를 나타내는 수신된 MEK 지시 플래그 (MIF) 에 기초하여 암호화된 미디어를 해독하기를 계속하는 단계를 더 제공한다.

대 표 도



특허청구의 범위

청구항 1

콜러 통신 장치와 하나 이상의 타겟 통신 장치 사이에서 진행중인 미디어 통신 세션 동안 암호 키들을 변환하는 방법으로서,

상기 콜러 통신 장치가 현재 미디어 암호 키 (MEK; media encryption key) 를 이용하여 미디어 패킷들을 암호화하는 단계;

상기 콜러 통신 장치가 상기 현재 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 상기 하나 이상의 타겟 통신 장치로 송신하는 단계;

상기 콜러 통신 장치가 보안 키 서버 (SKS; secure key server) 로부터의 새로운 MEK 를 요청하는 단계;

상기 콜러 통신 장치가 상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 단계;

상기 콜러 통신 장치가 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 단계로서,

상기 콜러 통신 장치가 미디어 패킷들을 암호화하고, 각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하기 위해, 상기 각 미디어 패킷에 대해 MEK 지시 플래그 (MIF; MEK indicator flag) 를 설정하고,

상기 콜러 통신 장치가 암호화된 상기 미디어 패킷들과 각 미디어 패킷에 대한 상기 MIF 를 상기 하나 이상의 타겟 통신 장치로 송신하는,

상기 변환 단계;

상기 변환 후에, 상기 콜러 통신 장치가 상기 새로운 MEK 를 이용하여 미디어 패킷들을 암호화하는 단계; 및

상기 콜러 통신 장치가 상기 새로운 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 상기 하나 이상의 타겟 통신 장치로 송신하는 단계를 포함하는, 암호 키 변환 방법.

청구항 2

제 1 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 암호 키 변환 방법.

청구항 3

제 2 항에 있어서,

상기 요청하는 단계는 첫번째 타이머가 만료시 발생하는, 암호 키 변환 방법.

청구항 4

제 1 항에 있어서,

소정의 타임 주기 동안 상기 현재 MEK 또는 상기 새로운 MEK 중 하나를 이용하여 상기 미디어 패킷들을 암호화하는 단계를 더 포함하는, 암호 키 변환 방법.

청구항 5

제 4 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 방법.

청구항 6

제 4 항에 있어서,

상기 변환하는 단계는 세번째 타이머 만료시 발생하는, 암호 키 변환 방법.

청구항 7

제 4 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 방법.

청구항 8

삭제

청구항 9

콜러 통신 장치와 하나 이상의 타겟 통신 장치 사이에서 진행중인 미디어 통신 세션 동안 암호 키들을 변환하는 방법을 구현하는 코드를 수록한 컴퓨터 판독가능 매체로서,

상기 방법은:

상기 콜러 통신 장치가 현재 미디어 암호 키 (MEK) 를 이용하여 미디어 패킷들을 암호화하는 단계;

상기 콜러 통신 장치가 상기 현재 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 상기 하나 이상의 타겟 통신 장치로 송신하는 단계;

상기 콜러 통신 장치가 보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청하는 단계;

상기 콜러 통신 장치가 상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 단계;

상기 콜러 통신 장치가 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 단계로서,

상기 콜러 통신 장치가 미디어 패킷들을 암호화하고, 각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하기 위해, 상기 각 미디어 패킷에 대해 MEK 지시 플래그 (MIF; MEK indicator flag) 를 설정하고,

상기 콜러 통신 장치가 암호화된 상기 미디어 패킷들과 각 미디어 패킷에 대한 상기 MIF 를 상기 하나 이상의 타겟 통신 장치로 송신하는,

상기 변환 단계;

상기 변환 후에, 상기 콜러 통신 장치가 상기 새로운 MEK 를 이용하여 미디어 패킷들을 암호화하는 단계; 및

상기 콜러 통신 장치가 상기 새로운 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 상기 하나 이상의 타겟 통신 장치로 송신하는 단계를 포함하는, 컴퓨터 판독가능 매체.

청구항 10

제 9 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 컴퓨터 판독가능 매체.

청구항 11

제 10 항에 있어서,

상기 요청하는 단계는 첫번째 타이머 만료시 발생하는, 컴퓨터 판독가능 매체.

청구항 12

제 9 항에 있어서,

소정의 타임 주기 동안 상기 현재 MEK 또는 상기 새로운 MEK 중 하나를 이용하여 상기 미디어 패킷들을 암호화하는 단계를 더 포함하는, 컴퓨터 판독가능 매체.

청구항 13

제 12 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 컴퓨터 판독가능 매체.

청구항 14

제 9 항에 있어서,

상기 변환하는 단계는 세번째 타이머 만료시 발생하는, 컴퓨터 판독가능 매체.

청구항 15

제 12 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 컴퓨터 판독가능 매체.

청구항 16

삭제

청구항 17

하나 이상의 타겟 통신 장치와의 진행중인 무선 미디어 통신 세션 동안 암호 키들을 변환하는 장치로서,

현재 미디어 암호 키 (MEK) 를 이용하여 미디어 패킷들을 암호화하는 수단;

상기 현재 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 콜러 통신 장치로부터 상기 하나 이상의 타겟 통신 장치로 송신하는 수단;

보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청하는 수단;

상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 수단;

미디어 패킷들을 암호화하고, 각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하기 위해, 상기 각 미디어 패킷에 대해 MEK 지시 플래그 (MIF; MEK indicator flag) 를 설정하고, 암호화된 상기 미디어 패킷들과 각 미디어 패킷에 대한 상기 MIF 를 상기 하나 이상의 타겟 통신 장치로 송신함으로써, 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 수단;

상기 변환 후에, 상기 새로운 MEK 를 이용하여 미디어 패킷들을 암호화하는 수단; 및

상기 새로운 MEK 를 이용하여 암호화된, 상기 미디어 패킷들을 상기 하나 이상의 타겟 통신 장치로 송신하는 수단을 포함하는, 암호 키 변환 장치.

청구항 18

제 17 항에 있어서,

상기 새로운 MEK 가 수신시 하나 이상의 타이머가 설정되는, 암호 키 변환 장치.

청구항 19

제 18 항에 있어서,

상기 요청하는 것은 첫번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 20

제 17 항에 있어서,

소정의 타임 주기 동안 상기 현재 MEK 또는 상기 새로운 MEK 중 하나를 이용하여 상기 미디어 패킷들을 암호화하는 수단을 더 구비하는, 암호 키 변환 장치.

청구항 21

제 20 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 장치.

청구항 22

제 17 항에 있어서,

상기 변환하는 것은 세번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 23

제 20 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 장치.

청구항 24

삭제

청구항 25

하나 이상의 타겟 통신 장치와의 진행중인 미디어 통신 세션 동안 암호 키들을 변환하는 장치로서,

메모리 유닛;

수신기;

송신기; 및

상기 메모리 유닛, 상기 수신기, 및 상기 송신기에 결합된 프로세서를 구비하고,

상기 프로세서는,

현재 미디어 암호 키 (MEK) 를 이용하여 미디어 패킷들을 암호화;

보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청;

상기 보안 키 서버로부터 상기 새로운 MEK 를 수신;

미디어 패킷들을 암호화하고, 각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하기 위해, 상기 각 미디어 패킷에 대해 MEK 지시 플래그 (MIF; MEK indicator flag) 를 설정함으로써, 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환; 및

상기 변환 후에, 상기 새로운 MEK 를 이용하여 미디어 패킷들을 암호화할 수 있는, 암호 키 변환 장치.

청구항 26

제 25 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 암호 키 변환 장치.

청구항 27

제 26 항에 있어서,

상기 요청하는 것은 첫번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 28

제 25 항에 있어서,

상기 프로세서는 또한, 소정의 타임 주기 동안 상기 현재 MEK 또는 상기 새로운 MEK 중 하나를 이용하여 상기 미디어 패킷들을 암호화할 수 있는, 암호 키 변환 장치.

청구항 29

제 28 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 장치.

청구항 30

제 25 항에 있어서,

상기 변환하는 것은 세번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 31

제 28 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 장치.

청구항 32

삭제

청구항 33

콜러 통신 장치와 하나 이상의 타겟 통신 장치 사이에서 진행중인 미디어 통신 세션 동안 암호 키를 변환하는 방법으로서,

상기 타겟 통신 장치가 현재 미디어 암호 키 (MEK; media encryption key) 를 이용하여 암호화된, 미디어 패킷들을 수신하는 단계;

상기 타겟 통신 장치가 상기 현재 미디어 암호 키를 이용하여 상기 암호화된 미디어 패킷들을 해독하는 단계;

상기 타겟 통신 장치가 보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청하는 단계;

상기 타겟 통신 장치가 상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 단계;

상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 단계로서,

상기 타겟 통신 장치는,

각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하는, 상기 각 미디어 패킷에 대한 MEK 지시 플래그 (MIF; MEK indicator flag) 와 암호화된 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하고,

상기 각 미디어 패킷에 대한 상기 MIF 에 기초하여 선택된 상기 현재 MEK 또는 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는, 상기 변환 단계;

상기 변환 후에, 상기 타겟 통신 장치가 상기 새로운 MEK 를 이용하여 암호화된, 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하는 단계; 및

상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는 단계를 포함하는, 암호 키 변환 방법.

청구항 34

제 33 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 암호 키 변환 방법.

청구항 35

제 34 항에 있어서,

상기 요청하는 단계는 첫번째 타이머 만료시 발생하는, 암호 키 변환 방법.

청구항 36

삭제

청구항 37

제 33 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 단계는 소정의 타임 주기의 시작시에 시작하는, 암호 키 변환 방법.

청구항 38

제 37 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 방법.

청구항 39

제 34 항에 있어서,

상기 변환하는 단계는 세번째 타이머 만료시 발생하는, 암호 키 변환 방법.

청구항 40

제 37 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 단계는 상기 소정의 타임 주기의 종료시에 종료하는, 암호 키 변환 방법.

청구항 41

제 40 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 방법.

청구항 42

제 40 항에 있어서,

상기 소정의 타임 주기의 종료 이후에, 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독하는 단계를 더 포함하는, 암호 키 변환 방법.

청구항 43

콜러 통신 장치와 하나 이상의 타겟 통신 장치 사이에서 진행중인 미디어 통신 세션 동안 암호 키들을 변환하는 방법을 구현하는 코드를 수록한 컴퓨터 판독 가능 매체로서,

상기 방법은:

상기 타겟 통신 장치가 현재 미디어 암호 키 (MEK) 를 이용하여 암호화된, 미디어 패킷들을 수신하는 단계;

상기 타겟 통신 장치가 상기 현재 미디어 암호 키를 이용하여 상기 암호화된 미디어 패킷들을 해독하는 단계;

상기 타겟 통신 장치가 보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청하는 단계;

상기 타겟 통신 장치가 상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 단계;

상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 단계로서,

상기 타겟 통신 장치는,

각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하는, 상기 각 미디어 패킷에 대한 MEK 지시 플래그 (MIF; MEK indicator flag) 와 암호화된 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하고,

상기 각 미디어 패킷에 대한 MIF 에 기초하여 선택된 상기 현재 MEK 또는 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는, 상기 변환 단계;

상기 변환 후에, 상기 타겟 통신 장치가 상기 새로운 MEK 를 이용하여 암호화된, 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하는 단계; 및

상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는 단계를 포함하는, 컴퓨터 판독 가능

매체.

청구항 44

제 43 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 컴퓨터 판독 가능 매체.

청구항 45

제 44 항에 있어서,

상기 요청하는 단계는 첫번째 타이머 만료시 발생하는, 컴퓨터 판독 가능 매체.

청구항 46

삭제

청구항 47

제 43 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 단계는 소정의 타임 주기의 시작시에 시작하는, 컴퓨터 판독 가능 매체.

청구항 48

제 47 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 컴퓨터 판독 가능 매체.

청구항 49

제 44 항에 있어서,

상기 변환하는 단계는 세번째 타이머 만료시 발생하는, 컴퓨터 판독 가능 매체.

청구항 50

제 47 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 단계는 상기 소정의 타임 주기의 종료시에 종료하는, 컴퓨터 판독 가능 매체.

청구항 51

제 50 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 컴퓨터 판독 가능 매체.

청구항 52

제 50 항에 있어서,

상기 방법은, 상기 소정의 타임 주기의 종료 이후에, 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독하는 단계를 더 포함하는, 컴퓨터 판독 가능 매체.

청구항 53

콜러 통신 장치와의 진행중인 미디어 통신 세션 동안 암호 키를 변환하는 장치로서,

현재 미디어 암호 키 (MEK) 를 이용하여 암호화된, 미디어 패킷들을 수신하는 수단;

상기 현재 미디어 암호 키를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는 수단;

보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청하는 수단;

상기 보안 키 서버로부터 상기 새로운 MEK 를 수신하는 수단;

각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하는 상기 각 미디어 패킷에 대한 MEK 지시 플래그 (MIF) 와 암호화된 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하고,

각 미디어 패킷에 대한 상기 MIF 에 기초하여 선택된 상기 현재 MEK 또는 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화함으로써, 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환하는 수단;

상기 새로운 MEK 를 이용하여 암호화된, 미디어 패킷들을 상기 콜러 통신 장치로부터 수신하는 수단; 및

상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화하는 수단을 포함하는, 암호 키 변환 장치.

청구항 54

제 53 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 암호 키 변환 장치.

청구항 55

제 54 항에 있어서,

상기 요청하는 것은 첫번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 56

삭제

청구항 57

제 53 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 것은 소정의 타임 주기의 시작시에 시작하는, 암호 키 변환 장치.

청구항 58

제 57 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 장치.

청구항 59

제 54 항에 있어서,

상기 변환하는 것은 세번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 60

제 57 항에 있어서,

상기 수신된 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 것은 상기 소정의 타임 주기의 종료시에 종료하는, 암호 키 변환 장치.

청구항 61

제 60 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 장치.

청구항 62

제 60 항에 있어서,

상기 소정의 타임 주기의 종료 이후에, 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독하는 수단을 더 구비하는, 암호 키 변환 장치.

청구항 63

콜러 통신 장치와의 진행중인 무선 미디어 통신 세션 동안 암호 키를 변환하는 장치로서,

메모리 유닛;

수신기;

송신기; 및

상기 메모리 유닛, 상기 수신기, 및 상기 송신기에 결합된 프로세서를 구비하고,

상기 프로세서는,

현재 미디어 암호 키 (MEK) 를 이용하여 암호화된 미디어 패킷들을 해독;

보안 키 서버 (SKS) 로부터의 새로운 MEK 를 요청;

상기 보안 키 서버로부터 상기 새로운 MEK 를 수신;

각 미디어 패킷이 상기 현재 MEK 를 이용하여 암호화되는지, 아니면 상기 새로운 MEK 를 이용하여 암호화되는지를 지시하는 상기 각 미디어 패킷에 대한 MEK 지시 플래그 (MIF) 에 기초하여 선택된 상기 현재 MEK 또는 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독화함으로써, 상기 현재 MEK 로부터 상기 새로운 MEK 로 변환;

상기 변환 후에, 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독할 수 있는, 암호 키 변환 장치.

청구항 64

제 63 항에 있어서,

상기 새로운 MEK 가 수신시, 하나 이상의 타이머가 설정되는, 암호 키 변환 장치.

청구항 65

제 64 항에 있어서,

상기 요청하는 것은 첫번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 66

삭제

청구항 67

제 63 항에 있어서,

상기 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 것은 소정의 타임 주기의 시작시에 시작하는, 암호 키 변환 장치.

청구항 68

제 67 항에 있어서,

상기 소정의 타임 주기는 두번째 타이머 만료시 시작하는, 암호 키 변환 장치.

청구항 69

제 64 항에 있어서,

상기 변환하는 것은 세번째 타이머 만료시 발생하는, 암호 키 변환 장치.

청구항 70

제 67 항에 있어서,

상기 MIF 에 기초하여 상기 암호화된 미디어 패킷들을 해독하는 것은 상기 소정의 타임 주기의 종료시에 종료하는, 암호 키 변환 장치.

청구항 71

제 70 항에 있어서,

상기 소정의 타임 주기는 네번째 타이머 만료시 종료하는, 암호 키 변환 장치.

청구항 72

제 70 항에 있어서,

상기 프로세서는 또한, 상기 소정의 타임 주기의 종료 이후에, 상기 새로운 MEK 를 이용하여 상기 암호화된 미디어 패킷들을 해독할 수 있는, 암호 키 변환 장치.

명 세 서

<1> **분야**

<2> 본 발명은 포인트 투 포인트, 포인트 투 멀티 포인트, 및 브로드캐스트 통신 시스템에 관한 것이다. 더욱 구체적으로, 본 발명은 통신 네트워크에서 보안 미디어 통신 세션 동안 보안 키를 할당하는 방법 및 장치에 관한 것이다.

<3> **배경**

<4> 빠르고, 효율적인, 원 투 원, 및 원 투 다수의 (그룹) 통신을 위해 의도된 무선 서비스의 클래스는 수년 동안 다양한 형태로 존재해 왔다. 일반적으로, 이들 서비스는 사용자가 그룹 통신을 개시하기 위해 폰/라디오상의 "푸시 투 토크" (PTT) 버튼을 누르는 하프-듀플렉스였다. 이들 서비스는 일반적으로 그룹 통신 서비스로 알려진 택시 운전자들 또는 필드 서비스 퍼스널과 같은 사람들 그룹과 한명의 사람이 통신하기를 원하는 애플리케이션에서 통상적으로 이용되어 왔다.

<5> 안전한 미디어 통신을 위해, 미디어는 타겟에 통신되기 이전에 미디어 암호 키 (MEK) 를 이용하여 암호화되고, 동일한 MEK 를 이용하여 타겟에서 수신된 이후 해독된다. 각각의 MEK 는, 만료시에 MEK 가 만료되고 더 이상 유효하지 않을 수도 있는 유지 시간 값 (time-to-live value) 을 포함한다. 진행중인 미디어 통신 세션 동안 현재 MEK 가 만료시에, 새로운 MEK 가 획득되고 사용되어 후속 미디어를 암호화한다. 그러나, 진행중인 통신 세션의 참가자는 동시에 정확히 모든 새로운 MEK 를 수신할 수 없을 수도 있기 때문에, 새로운 MEK 로의 변환은 잘못된 MEK 로 해독된 일부 패킷을 유발할 수도 있어, 그 결과 미디어 스트림의 암호화 및/또는 해독에 부정적인 영향을 미친다.

<6> 따라서, 미디어 패킷의 손실 또는 미디어 스트림의 암호화 및/또는 해독에 부정적인 영향을 미치지 않고 진행중인 미디어 통신 세션 동안 현재 MEK 로부터 새로운 MEK 로 동적으로 변환하는 메카니즘에 대한 필요가 있다.

<7> **요약**

<8> 개시된 실시형태는 진행중인 통신 세션 동안 암호 키를 변환하는 신규하고 개선된 방법 및 장치를 제공한다. 일 양태에서, 방법은 현재 미디어 암호 키 (MEK) 를 이용하여 미디어를 암호화하는 단계, 현재 MEK 가 만료되기 전에 새로운 MEK 를 요청하는 단계, 및 새로운 MEK 를 수신하는 단계를 제공한다. 본 방법은 현재 MEK 로부터 새로운 MEK 로 변환하여, 새로운 MEK 를 이용하여 미디어를 암호화하기를 계속하는 단계를 더 제공한다.

<9> 또 다른 양태에서, 방법은 진행중인 무선 미디어 통신 세션 동안 미디어를 해독하는 단계를 제공하고, 방법은 암호화된 미디어를 수신하는 단계, 및 현재 미디어 암호 키 (MEK) 를 이용하여 암호화된 미디어를 해독하는 단계를 포함한다. 방법은 현재 MEK 가 만료하기 이전에 새로운 MEK 를 요청하는 단계, 새로운 MEK 를 수신하는 단계, 및 암호화된 미디어가 현재 MEK 또는 새로운 MEK 를 이용하여 암호화 되었는지를 나타내는 수신된 MEK 지시 플래그 (MIF) 에 기초하여, 암호화된 미디어를 해독하기를 계속하는 단계를 더 포함한다.

<10> 일 양태에서, 진행중인 무선 통신 세션 동안 미디어 통신 키를 변환하는 장치는 메모리 유닛, 수신기, 송신기, 및 이 메모리 유닛, 수신기, 및 송신기에 통신적으로 결합된 프로세서를 구비한다. 프로세서는 상술한 방법을 수행할 수 있다.

<11> **도면의 간단한 설명**

<12> 본 발명의 특징 및 전술한 이하의 실시형태 상세한 설명으로부터 더욱 명백할 것이다.

<13> 도 1 은 그룹 통신 시스템을 도시한다.

<14> 도 2 는 몇몇의 통신 디바이스가 그룹 통신 서버와 어떻게 상호 작용하는 지를 도시한다.

<15> 도 3 은 다양한 개시된 실시형태에 대한 인프라구조의 실시형태를 도시한다.

<16> 도 4a, 도 4b, 및 도 5 는 미디어 통신 세션 동안 암호 키를 할당하는 프로세스를 도시한다.

<17> **상세한 설명**

<18> 몇몇 실시형태가 상세히 설명되기 이전에, 본 발명의 범위가 다음 설명에 개시되고, 도면에서 도시된 구성의 배열 및 구성의 세부사항에 한정되지 않는다는 것이 이해된다. 또한, 여기서 사용된 어구 및 용어는 설명의 목적을 위한 것이고 한정으로서 간주되어서는 안된다는 것이 이해된다.

<19> 도 1 은 일 실시형태를 구현하는 그룹 통신 시스템 (100) 기능 블록도이다. 또한, 그룹 통신 시스템 (100) 은 푸시 투 토크 (PTT) 시스템, 네트 브로드캐스트 서비스 (NBS), 디스패치 시스템, 또는 포인트 투 멀티 포인트 통신 시스템으로 알려졌다. 일 실시형태에서, 그룹 통신 시스템 (100) 은 집중된 배치 또는 분할된 배치 중 하나로 배치될 수도 있는 그룹 통신 서버 (GCS; 102) 를 포함한다. 그룹 통신 서버 (102) 는 이 분야에 알려진 바와 같이, 하나 이상의 프로세서, 하나 이상의 메모리 유닛, 및 입력/출력 하드웨어 및 다양한 미디어 통신 예를 들어, IP 미디어 통신에 대한 소프트웨어 모듈을 포함하여 구현될 수도 있다.

<20> CDMA (예를 들어, cdma2000) 핸드셋과 같은 그룹 통신 디바이스 (CD; 104, 106) 는, 예를 들어, 데이터 서비스 옵션을 이용하여 패킷 데이터 세션을 요청할 수도 있다. 각각의 CD 는 세션을 이용하여 CD 의 인터넷 프로토콜 (IP) 어드레스를 그룹 통신 서버로 등록하여 그룹 통신 초기화를 수행한다. 일 실시형태에서, 그룹 통신 서버 (102) 는 서비스 제공자의 네트워크 (116) 를 통해 서비스 제공자의 패킷 데이터 서비스 노드 (PDSN) 에 접속된다. 무선 인프라구조로부터 패킷 데이터 세션을 요청시, CD (104 및 106) 는 PDSN (114) 을 통해 그룹 통신 서버 (102) 로의 IP 접속을 가진다. 각각의 PDSN 은 패킷 제어 기능 (PCF; 108) 및 네트워크 (112) 를 통해 기지국 제어기 (BSC) 에 인터페이스할 수도 있다. PCF 는 기지국 (BS; 110) 내에 BSC 와 함께 위치할 수도 있다.

<21> 패킷 데이터 서비스는 몇 단계 중의 하나, 예를 들어, 활성 또는 접속된 상태, 휴면 상태, 및 널 (null) 또는 비활성 상태 중 하나에 속할 수도 있다. 활성 또는 접속된 상태에서, 활성 트래픽 채널은 참가 CD 와 BS 또는 BSC 사이에 존재하고 양측 중 하나가 데이터를 전송한다. 휴면 상태에서, 참가 CD 와 BSC 사이에 활성 트래픽 채널이 존재하지 않지만, 포인트 투 포인트 프로토콜 (PPP) 링크가 참가 CD 와 PDSN 사이에 유지된다. 널 또는 비활성 상태에서, 참가 CD 와 BSC 사이에 활성 트래픽 채널이 존재하지 않고, 참가 CD 와 PDSN 사이에 어떠한 PPP 링크도 유지되지 않는다.

<22> CD (104 및 106) 중 각 하나는 패킷 데이터 세션을 요청할 수도 있다. 패킷 데이터 세션을 확립하는 단계의 부분으로서, 각각의 CD 는 IP 어드레스를 할당받을 수도 있다. 각각의 CD 는 등록 프로세스를 수행하여 그룹 통신 서버 (102) 에 CD 의 IP 어드레스를 통지할 수도 있다. 등록은 사용자 데이터그램 프로토콜 (UDP) 을 통해 세션 초기화 프로토콜 (SIP) 과 같은 IP 프로토콜을 이용하여 수행될 수도 있다. 대응하는 사용자가 그룹 통신에 초대되거나 그룹 통신을 통지받은 경우 CD 의 IP 어드레스는 CD 에 콘택트하도록 사용될 수도 있다.

<23> 그룹 미디어 통신 세션이 확립된 경우, 컨퍼런스 ID 는 확립된 세션에 할당될 수도 있고 CD (104 및 106) 및 통신 서버 (GSC; 102) 는 할당된 컨퍼런스 ID 를 이용하여 미디어 및 시그널링 메시지를 교환할 수도 있다. 일 실시형태에서, 미디어는 UDP 를 통해 실시간 프로토콜 (RTP; real-time protocol) 을 이용함으로써 참가 CD 와 그룹 통신 서버 사이에 교환된다. 시그널링 메시지는 UDP 를 통해 시그널링 프로토콜을 이용함으로써 교환될 수도 있다.

<24> 그룹 통신 시스템 (100) 은 그룹 통신 서버를 동작시키기 위해 몇몇 상이한 기능들을 수행한다. 사용자 측

에 관한 기능들은 사용자 등록, 그룹 통신 초기화, 그룹 통신 종료, 그룹 참가자에게 메시지 전달, 그룹 통신에의 늦은 참가, 토커 조정, 그룹에 멤버 추가, 그룹으로부터 멤버 제거, 멤버 비등록, 사용자 인증을 포함한다. 시스템 사전 준비 및 동작에 관한 기능들은 관리 및 권한 설정, 범위성, 및 신뢰성을 포함한다.

<25> 도 2 는 CD (202, 204, 및 206) 가 그룹 통신 서버 (208) 와 어떻게 상호작용하는지를 도시하는 그룹 통신 구성 (200) 이다. 복수의 그룹 통시 서버는 큰 스케일 그룹에 바람직하게 배치될 수도 있다. 사용자는 통신 미디어, 예를 들어, 이미지, 및/또는 미디어를 하나 이상의 CD 와 교환하기 위해 통신 세션을 초기화하는 그 요구를 CD (202, 204, 206) 에 입력한다. 일 실시형태에서, 사용자는 CD 상의 PTT 버튼 또는 "초대" 를 누름으로써 미디어를 통신하기 시작하기 이전에 타겟 사용자 (들) 을 우선 초대할 수도 있다.

<26> 도 2 는, CD (202) 가 미디어를 그룹의 다른 멤버에게 송신하기 위한 사용권한을 가지는 경우, CD (202) 는 발신자로 알려지고 확립된 채널을 통해 미디어를 송신할 수도 있다. CD (202) 가 발신자로 지정된 경우, 나머지 참가자들인 CD (204) 및 CD (206) 은 그룹에 미디어를 송신하도록 허용되지 않을 수도 있다. 따라서, CD (204) 및 CD (206) 는 타겟으로 지정된다. 상술한 바와 같이, CD (202, 204, 및 206) 는 하나 이상의 채널을 이용하여 그룹 통신 서버 (208) 에 접속된다. 일 실시형태에서, 채널 (210, 212, 및 214) 은 세션 초기화 프로토콜 (SIP) 채널, 미디어 시그널링 채널, 및 미디어 트래픽 채널을 포함할 수도 있다.

<27> 도 3 은 다양한 개시된 실시형태를 구현할 수 있는 기지국/기지국 제어기 (BS/BSC; 304) 및 통신 디바이스 (306) 를 포함하는 인프라구조의 일 실시형태의 간단화된 블록도이다. 특정 미디어 통신을 위해, 음성, 데이터, 패킷 데이터, 및/또는 경고 메시지는 공중 인터페이스 (308) 를 통해 BS/BSC (304) 와 통신 디바이스 (306) 사이에 교환될 수도 있다. 다양한 유형의 메시지, 예를 들어, 기지국과 통신 디바이스 사이에 통신 세션을 확립하도록 사용된 메시지, 등록 및 페이징 메시지, 및 데이터 송신을 제어하도록 사용된 메시지 (예를 들어, 전원 제어, 데이터 레이트 정보, 확인 응답 등) 가 송신될 수도 있다. 이들 메시지 유형의 일부가 이하 더욱 상세히 설명된다.

<28> 역방향 링크에 대해, 통신 디바이스 (306) 에서, (예를 들어, 데이터 소스 (310) 로부터의) 음성 및/또는 패킷 데이터 및 (예를 들어, 제어기 (330) 으로부터의) 메시지가 송신 (TX) 데이터 프로세서 (312) 에 제공되어, 이 송신 (TX) 데이터 프로세서 (312) 는 하나 이상의 코딩 방식으로 메시지 및 데이터를 포맷하고 인코딩하여 코딩된 데이터를 생성한다. 각각의 코딩 방식은 사이클릭 리던던시 체크 (CRC), 컨벌루셔널 (convolutional), 터보, 블록, 및 다른 코딩의 임의의 조합을 가질 수도 있거나, 코딩을 전혀 가지지 않을 수도 있다. 음성, 패킷 데이터, 및 메시지는 상이한 방식을 이용하여 코딩될 수도 있고, 상이한 유형의 메시지는 상이하게 코딩될 수도 있다.

<29> 그 후, 코딩된 데이터는 변조기 (MOD; 314) 로 제공되고 더 프로세싱된다 (예를 들어, 변환, 짧은 PN 시퀀스로 확산, 및 통신 디바이스에 할당된 긴 PN 시퀀스로 스크램블됨). 그 후, 변조된 데이터는 송신기 유닛 (TMTR; 316) 으로 제공되고 컨디셔닝되어 (예를 들어, 하나 이상의 아날로그 신호로 변환, 증폭, 필터링, 및 쿼드러처 변조) 역방향 링크 신호를 생성한다. 역방향 링크 신호는 듀플렉서 (D; 318) 를 통해 라우팅되어 안테나 (320) 를 통해 BS/BSC (304) 로 송신된다.

<30> BS/BSC (304) 에서, 역방향 링크 신호는 안테나 (350) 에 의해 수신되고, 듀플렉서 (352) 를 통해 라우팅되어 수신기 유닛 (RCVR; 354) 으로 제공된다. 다른 방법으로, 안테나는 무선 오퍼레이터 네트워크의 일부일 수도 있고, 안테나와 BS/BSC 사이의 접속은 인터넷을 통해 라우팅될 수도 있다. BS/BSC (304) 는 통신 디바이스 (306) 로부터 경고 메시지 및 미디어 정보를 수신할 수도 있다. 수신기 유닛 (354) 은 수신 신호를 컨디셔닝하여 (예를 들어, 필터링, 증폭, 다운 변환, 및 디지털화) 샘플을 제공한다. 복조기 (DEMOD; 356) 는 샘플을 수신하고 프로세싱하여 (예를 들어, 역확산, 디커버 (decover), 및 파일롯 복조) 복구된 심볼을 제공한다. 복조기 (356) 는 수신 신호의 복수의 인스턴스들을 프로세싱하고 결합된 심볼을 생성하는 레이크 수신기를 구현할 수도 있다. 그 후, 수신기 (RX) 데이터 프로세서 (358) 는 심볼을 디코딩하여 역방향 링크상에서 송신된 메시지 및 데이터를 복구한다. 복구된 음성/패킷 데이터는 데이터 싱크 (360) 에 제공되고 이 복구된 메시지는 제어기 (370) 에 제공될 수도 있다. 제어기 (370) 는 정보를 송수신하고, 메시지에 대한 응답을 송수신하고, 미디어 암호 키 (MEK; media encryption key) 를 요청하고, 현재 MEK 로부터 새로운 MEK 로 변환하고, 새로운 MEK 를 요청하고 새로운 MEK 로 변환하는 타이머를 설정하고, 타겟을 식별하고, 이 타겟을 로케이팅하고, 발신자 및 타겟에 부과된 제한을 결정하고, 발신자 및/또는 타겟이 그룹 통신 시스템에 등록되었는지 여부 및/또는 하나 이상의 타겟이 미디어를 수신하기를 받아들이는지 결정하고, 미디어를 버퍼링하는 명령을 포함할 수도 있다. 복조기 (356) 및 RX 데이터 프로세서 (358) 에 의한 프로세싱은 원격 액세스 디바이스

(306) 에서 수행된 것에 상보적이다. 복조기 (356) 및 RX 데이터 프로세서 (358) 는 더 동작되어 복수의 채널, 예를 들어, 역방향 기본 채널 (R-FCH; reverse fundamental channel) 및 역방향 부가 채널 (R-SCH; reverse supplemental channel) 을 통해 수신된 복수의 전송을 프로세싱한다. 또한, 전송은 각각이 역방향 기본 채널, 역방향 부가 채널, 또는 양 채널에서 송신될 수도 있는 복수의 통신 디바이스로부터 동시의 것일 수도 있다.

<31> 순방향 링크상의 BS/BSC (304) 에서, (예를 들어, 데이터 소스 (362) 로부터의) 음성 및/또는 패킷 데이터 및 (예를 들어, 제어기 (370) 로부터의) 메시지는 송신 (TX) 데이터 프로세서 (364) 에 의해 프로세싱되고 (예를 들어, 포맷되고 인코딩됨) 변조기 (MOD; 366) 에 의해 더 프로세싱되고 (예를 들어, 커버되고 확산됨) 송신기 유닛 (TMTR; 368) 에 의해 컨디셔닝되어 (예를 들어, 아날로그 신호로컨버팅하고, 증폭되고, 필터링되고, 쿼드러처 변조됨) 순방향 링크 신호를 생성한다. 순방향 링크 신호는 듀플렉서 (352) 에 의해 라우팅되고 안테나 (350) 를 통해 원격 액세스 디바이스 (306) 에 송신된다. 순방향 링크 신호는 페이징 신호를 포함한다.

<32> 통신 디바이스 (306) 에서, 순방향 링크 신호는 안테나 (320) 에 의해 수신되고, 듀플렉서 (318) 에 의해 라우팅되어 수신기 유닛 (322) 에 제공된다. 수신기 유닛 (322) 은 수신 신호를 컨디셔닝하여 (예를 들어, 다운컨버팅하고, 필터링하고, 증폭하고, 쿼드러처 변조하고, 디지털화함) 샘플을 제공한다. 샘플은 복조기 (324) 에 의해 프로세싱되어 (예를 들어, 역확산되고, 디커버링되고, 파일럿 복조됨) 심볼을 제공하고, 이 심볼은 수신 데이터 프로세서 (326) 에 의해 더 프로세싱되어 (예를 들어, 디코딩되고 체크됨) 순방향 링크상에서 송신된 메시지 및 데이터를 복구한다. 복구된 데이터는 데이터 싱크 (328) 에 제공되고, 복구된 메시지는 제어기 (330) 에 제공될 수도 있다. 제어기 (330) 는 정보를 송수신하고, 메시지에 대한 응답을 송수신하고, 미디어 암호 키 (MEK) 를 요청하고, 현재 MEK 로부터 새로운 MEK 로 변환하고, 새로운 MEK 를 요청하고 그 새로운 MEK 로 변환하는 타이머를 설정하고, 미디어를 버퍼링하고, 그룹 통신 서버에 미디어를 송신하고, 발신자가 미디어를 전달하게 하는 허용을 승인하는 명령을 포함한다.

<33> 미디어 통신의 비밀성은 각각 미디어 패킷으로 번들링된 보코더를 암호화함으로써 유지될 수도 있다. 일 실시형태에서, 암호화는 128-비트 블록의 라인달 (Rijndael) (AES) 알고리즘을 통해 수행될 수도 있다. 미디어 암호화는 일반적으로 3 개의 콤포넌트 : 미디어 암호 키 (MEK), 암호 카운터 값 (또는 상태-벡터), 및 암호화되는 보코더 프레임을 요청한다.

<34> MEK 는 특정 미디어 통신 세션에 참가하는 클라이언트에게만 알려질 수도 있는 128-비트 값일 수도 있다. 이 값은 보안 방법으로 공중 경유 (over-the-air) 메시지를 통해 보안 키 서버 (SKS) 로부터 획득될 수도 있다. 클라이언트가 미디어 통신 세션에 인게이징하기를 시도하는 때마다 새로운 MEK 가 SKS 로부터 요청될 수도 있다. 보안을 위해, 보안 저장이 클라이언트의 통신 디바이스상에서 이용가능한 경우, MEK 는 클라이언트의 통신 디바이스상에서 지속적으로 저장될 수도 있다.

<35> 카운터 값은 128-비트 암호 마스크를 생성하기 위해 라인달 알고리즘을 통해 MEK 로 암호화될 수도 있다. 보코더 프레임은 128-비트 블록의 암호 마스크로 보코더 데이터를 XOR 함으로써 암호화될 수도 있다. 마찬가지로, 보코더 프레임은 발신자 암호에서 사용된 동일한 마스크 값으로 보코더 데이터를 XOR 함으로써 해독될 수도 있다. 암호화 카운터는 특정 MEK 로 암호화된 각각의 블록에 대해 유일할 수도 있다.

<36> 각각의 유일한 MEK 는 유지 시간 (TTL; time-to-live) 값과 관련된다. TTL 은 현재 MEK 가 만료하고 더 이상 유효하지 않는 타임을 특정한다. 현재 MEK 의 TTL 이 만료하는 경우, 현재 MEK 는 새로운 TTL 값을 갖는 새로운 MEK 를 위해 리타이어 (retire) 된다. 이것은 미디어 스트림의 암호화 및/또는 해독에 부정적인 영향을 미치지 않고 하나의 MEK 로부터 또 다른 MEK 로의 변환을 취급하는 메카니즘을 요구한다.

<37> TTL 값은 밀리초로 특정되고 미디어 패킷 입도 (granularity) 로 변환될 수도 있다. MEK 의 TTL 값이 미디어 패킷의 첫번째 프레임이 아닌 보코더 프레임에 대해 만료시, MEK 는 모든 보코더 프레임이 현재 패킷에서 암호화 및/또는 해독되기까지 만료되지 않을 수도 있다. 이것은 각각의 클라인언트가 2 개의 MEK, 즉, 현재 MEK 및 새로운 MEK 를 프로세싱할 수도 있음을 의미한다.

<38> 현재 MEK 는 진행중인 미디어 통신 세션 동안 보코더 프레임을 암호화 및/또는 해독하도록 사용되고 현재 유효한 키이다. 새로운 MEK 는 현재 MEK 의 TTL 이 만료한 이후에, 보코더 프레임을 암호화 및/또는 해독하도록 사용될 MEK 이다.

<39> 네트워크 지연 및 다른 이슈로 인해, 진행중인 통신 세션에 인게이징된 모든 클라이언트들에서의 MEK 가 동일한

타임에 정확히 만료됨에 대한 보장이 없다. 미디어 패킷의 전송기는 현재 MEK 가 만료하기 직전에 현재 MEK 로 보코더 프레임을 암호화할 수도 있다. 타겟이 암호화된 미디어 패킷을 수신하기까지, 현재 MEK 는 이미 새로운 MEK 로 변환되어 미디어 패킷이 잘못된 MEK 로 해독됨을 유발할 수도 있다. 따라서, 어느 클라이언트가 어느 MEK 를 사용하는지에 따라 불확실성의 짧은 주기가 존재한다. 이 주기를 키 변환 주기 (KTP; key transition period) 로 칭한다. KTP 의 만료시, 현재 MEK 는 폐기될 수도 있고, 새로운 MEK 는 현재 MEK 가 될 수도 있다. 이 프로세스는 MEK 변환으로 칭한다.

<40> KTP 는 클라이언트에 의해 초기화되는, 클라이언트가 수신된 미디어 패킷이 현재 MEK 또는 새로운 MEK 중 하나로 암호화 되었을 수도 있음을 가정하는, 소정의 타임 주기이다. 따라서, KTP 동안 수신된 미디어 패킷을 적당히 해독하기 위해 현재 MEK 및 새로운 MEK 모두 이용가능하도록 보장하기 위해 KTP 의 시작에 앞서 클라이언트는 새로운 MEK 를 요구할 수도 있다. 암호화하는 동안, 전송기는, 각각의 미디어 프레임에서 전송기가 미디어 프레임을 암호화하도록 어느 MEK 를 사용했는지를 지정하는, MEK 지시자 플래그 (MIF; MEK indicator key) 로서 칭하는 플래그를 설정할 수도 있다. 각각의 수신기는 수신된 MIF 를 사용하여 관련된 수신 미디어 프레임을 해독하기 위해 현재 또는 새로운 MEK 중 어느 것이 사용되어야 하는지를 결정한다. KTP 는, 모든 클라이언트, 전송기 및 수신기들이 그 KTP 내에서 현재 MEK 로부터 새로운 MEK 로 변환함을 보장하도록 설정된다. KTP 만료시, 수신기들은 새로운 MEK 를 이용하여 모든 장래의 미디어 프레임을 해독하기 시작한다.

<41> 도 4a, 도 4b, 및 도 5 는 일 실시형태에 따라 진행중인 미디어 통신 세션 동안 동적 미디어 암호 키를 변환하는 프로세스를 도시한다. 발신자가 멤버 리스트를 선택하고 그 또는 그녀의 CD 상의 PTT 버튼을 누른 후에, 그룹 콜 서버 (GCS) 는 미디어 통신 세션을 확립한다. 현재 통신 세션에 참가중인 모든 사용자에게 현재 진행중인 세션에 대한 유일한 컨퍼런스 ID 가 주어질 수도 있다.

<42> 미디어 패킷을 암호화하기 위해, 발신자의 CD 는 서비스 제공자 (캐리어) 측이거나 고객 후원 보안 미디어 통신, 예를 들어, 정부에 의해 제어되는 개별적인 엔터티 또는 GCS 의 일부일 수도 있는 (402) 에 의해 도시된 바와 같은 보안 키 서버 (SKS) 로부터 미디어 통신 키 (MEK) 를 요청한다. MEK 에 대한 요청은 현재 컨퍼런스 ID 로 칭할 수도 있고 현재 컨퍼런스 ID 를 포함할 수도 있다.

<43> SKS 는 (404) 에 의해 도시된 바와 같이 컨퍼런스 ID 에 참조되거나 수신된 컨퍼런스 ID 에 대응하는 현재 미디어 통신 세션에 대한 MEK 를 생성한다. MEK 는 MEK 만료시 TTL (life-to-live time) 값을 포함하고 MEK 는 만료하며 더 이상 유효하지 않는다. 그 후, SKS 는 (406) 에 도시된 바와 같이, 발신자의 CD 에 MEK 를 전송한다.

<44> MEK 를 수신시에, 발시자의 CD 및 타겟의 CD 는 (408) 에 도시된 바와 같이 4 개의 타이머를 설정한다. 첫번째 타이머는 현재 MEK 만료 이전에 새로운 MEK 를 요청하기 위한 것이다. 새로운 MEK 를 요청시에 CD 는 그들 각각의 MIF 를 "0" 으로 재설정할 수도 있다. 두번째 타이머는 KTP 를 초기화하기 위한 것이고, 세번째 타이머는 현재 MEK 로부터 새로운 MEK 로 변환하기 위한 것이고, 네번째 타이머는 KTP 의 만료를 시그널링하기 위해 사용된다. 발신자의 CD 는 (412) 에 의해 도시된 바와 같이 타겟(들) 에 전송하기 위해 (410) 에 의해 도시된 바와 같이 미디어 패킷을 암호화하기 위해 현재 MEK 를 사용한다.

<45> 현재 미디어 통신 세션에 참가하는 또 다른 사용자, 예를 들어, 타겟(들) 은 (414) 에 의해 도시된 바와 같이 MEK 를 요청하고, 이 요청은 현재 세션에 관련된 동일한 컨퍼런스 ID 로 칭하거나, 이를 포함하며, 이 또 다른 사용자는 (416) 에 의해 도시된 바와 같이 MEK 를 수신한다. 암호화된 미디어 패킷이 타겟(들) 에 도달시, 타겟의 CD 는 (418) 에 의해 도시된 바와 같이 현재 MEK 를 이용하여, 수신된 암호화된 미디어 패킷을 해독한다.

<46> 도 4b 및 도 5 를 참조하면, 현재 통신 세션 동안 발신자의 CD 에서 첫번째 타이머의 만료시, MEK 가 거의 만료됨을 나타내어, (420 및 502) 에 의해 도시된 바와 같이 발신자의 CD 는 SKS 로부터 새로운 MEK 를 요청한다. (422) 에 의해 도시된 바와 같이 SKS 는 새로운 TTL 값을 포함하는 새로운 MEK 를 생성하여, (424) 에 의해 도시된 바와 같이 발신자의 CD 에 새로운 MEK 를 전송한다. (504) 에 의해 도시된 바와 같이 발신자의 CD 는 현재 MEK 를 이용하여 미디어 패킷의 암호화를 계속한다. 발신자의 CD 는 예를 들어, 각각의 암호화된 미디어 프레임 및/또는 패킷에 대해 미디어 패킷의 암호화에서 현재 MEK 의 사용을 나타내기 위해 MEK 식별 플래그 (MIF) 를 "0" 으로 설정한다.

<47> 두번째 타이머의 만료시, (426 및 516) 에 의해 도시된 바와 같이, 수신된 MIF 비트에 기초하여 현재 MEK 또는

새로운 MEK 중 하나를 이용하여 타겟(들)은 그가 수신한 미디어를 해독하고 KTP 가 시작한다.

<48> 발신자의 CD 에서 세번째 타이머의 만료시, 현재 MEK 의 만료를 나타내어, (428) 에 의해 도시된 바와 같이, 발신자의 CD 는 현재 MEK 로부터 새로운 MEK 로 변환하고, (430 및 508) 에 의해 도시된 바와 같이 새로운 MEK 를 이용하여 미디어 패킷을 암호화한다. 발신자의 CD 는 예를 들어, 각각의 암호화된 미디어 패킷에 대해 그 미디어 패킷의 암호화에서의 새로운 MEK 의 사용을 나타내기 위해 MEK 식별 플래그 (MIF) 를 "1" 로 설정한다.
암호화된 미디어 패킷은 (432) 에 의해 도시된 바와 같이 타겟(들) 에 통신된다.

<49> 현재 미디어 통신 세션에 참가하는 또 다른 사용자, 예를 들어, 타겟(들) 은 (434 및 510) 에 의해 도시된 바와 같이 새로운 MEK 를 요청하고, 이 요청은 현재 세션에 관련된 컨퍼런스 ID 를 포함하고, 이 또 다른 사용자는 단계 436 에서 도시된 바와 같이 새로운 MEK 를 수신하고, (438 및 512) 에 도시된 바와 같이 MEK 의 대응하는 세번째 타이머가 만료시 현재 MEK 로부터 새로운 MEK 로 변환한다.

<50> 네트워크 지연 및 다른 팩터로 인해, 현재 MEK 가 현재 세션에 인게이징된 모든 CD 에서 동일한 타임에 정확히 만료된다는 보장이 없다. 미디어 패킷의 전송기는 현재 MEK 의 만료 직전에 현재 MEK 로 미디어 패킷 (보코더 프레임) 을 암호화할 수도 있다. 타겟이 미디어 패킷을 수신하는 타임까지, 새로운 MEK 로 이미 변환될 수도 있어, 일부 미디어 패킷이 잘못된 MEK 로 해독됨을 유발할 수도 있다. 따라서, 어느 사용자의 CD 가 어느 MEK 를 이용하는지에 따라 불확실성의 짧은 주기가 존재한다. 이것은 키 변환 주기 (KTP) 로 칭한다.

<51> KTP 는, CD 가 수신된 미디어 패킷이 현재 MEK 또는 새로운 MEK 중 하나를 이용하여 암호화되었을 수도 있음을 가정하는, 각각의 참가 CD 에 의해 초기화될 수도 있는 타임 주기이다. 따라서, CD 는 KTP 의 시작에 앞서 새로운 MEK 를 요청하여 현재 MEK 및 새로운 MEK 모두 KTP 동안 수신된 미디어 패킷을 해독하는데 이용가능함을 보장한다. 암호화하는 동안, 전송기는 각각의 미디어 프레임에 MEK 지시자 플래그 (MIF) 를 설정하여 미디어 프레임을 암호화하기 위해 사용자가 어느 MEK 를 이용하였는지를 나타낸다. 각각의 수신기는 수신된 MIF 를 이용하여 수신된 암호화된 미디어 패킷을 적당한 MEK 로 해독하기 위해 어느 MEK 가 사용되어야 하는지를 결정한다. KTP 는 프로그램되어 모든 CD 들, 전송기 및 수신기들이 KTP 내에서 현재 MEK 로부터 새로운 MEK 로 변환함을 보장한다. KTP 만료시, 수신기는 새로운 MEK 를 이용하여 미디어 패킷을 해독하기 시작한다.

<52> KTP 가 시작한 이후, (514) 에 의해 도시된 바와 같이 암호화된 미디어 패킷이 KTP 동안 타겟(들) 에 도달하고, 타겟의 CD 는 (426 및 516) 에 의해 도시된 바와 같이 MIF 가 "0" 또는 "1" 로 각각 설정되었는지에 기초하여 현재 MEK 또는 새로운 MEK 중 하나를 이용하여 대응하는 MIF 에 기초하여 수신된 암호화된 미디어 패킷을 해독한다. (518) 에 의해 도시된 바와 같이, KTP 의 만료시, 타겟의 CD 는 (440 및 520) 에 의해 도시된 바와 같이 새로운 MEK 를 이용하여 수신된 암호화된 미디어 패킷을 해독한다.

<53> 당업자는 다양한 서로 다른 기술 및 기법을 이용하여 정보 및 신호를 표현할 수도 있음을 알 수 있다. 예를 들어, 상기의 설명 전반에 걸쳐 참조될 수도 있는 데이터, 명령, 커맨드 (commands), 정보, 신호, 비트, 심볼, 및 칩은 전압, 전류, 전자기파, 자계 또는 자성 입자, 광계 또는 광자, 또는 이들의 임의의 결합으로 나타낼 수도 있다.

<54> 또한, 당업자는 여기에서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들을 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 결합으로 구현할 수도 있음을 알 수 있다. 하드웨어와 소프트웨어의 이러한 대체 가능성을 분명히 설명하기 위하여, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들을 주로 그들의 기능의 관점에서 상술하였다. 그러한 기능이 하드웨어로 구현될지 소프트웨어로 구현될지는 전체 시스템에 부과된 특정한 애플리케이션 및 설계 제약조건들에 의존한다.
당업자는 설명된 기능을 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 구현할 수도 있지만, 그러한 구현의 결정이 본 발명의 범주를 벗어나도록 하는 것으로 해석하지는 않아야 한다.

<55> 여기에서 개시된 실시형태들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들은 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적회로 (ASIC), 필드 프로그래머블 게이트 어레이 (FPGA), 또는 기타 프로그래머블 로직 디바이스, 별도의 게이트 또는 트랜지스터 로직, 별도의 하드웨어 컴포넌트들, 또는 여기서 설명된 기능을 수행하도록 설계되는 이들의 임의의 결합으로 구현 또는 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 다른 방법으로, 그 프로세서는 임의의 종래 프로세서, 제어기, 마이크로 제어기, 또는 상태 기계일 수도 있다. 또한, 프로세서는 컴퓨팅 디바이스들의 결합, 예를 들어, DSP 와 마이크로프로세서의 결합, 복수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들 또는 임의의 기타 다른 구성물로 구현될 수도 있다.

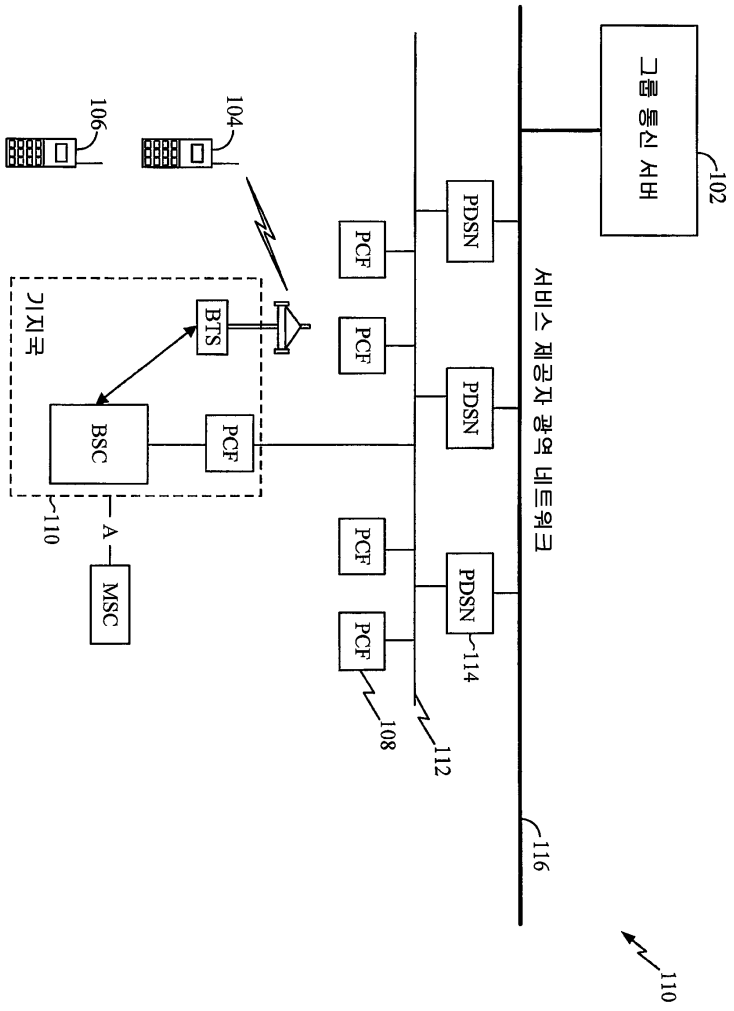
<56> 여기에 개시된 실시형태들과 관련하여 설명된 방법 또는 알고리즘의 단계는 프로세서에 의해 실행되는 하드웨어, 소프트웨어 모듈, 또는 그 2 개의 결합으로 직접 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드 디스크, 착탈형 디스크, CD-ROM, 또는 당업계에 알려진 임의의 다른 형태의 저장 매체에 상주할 수도 있다. 예시적인 저장 매체는 프로세서에 커플링되며, 그 프로세서는 저장 매체로부터 정보를 판독할 수 있고 저장 매체에 정보를 기입할 수 있다. 다른 방법으로, 저장 매체는 프로세서와 일체형일 수도 있다. 프로세서 및 저장 매체는 ASIC 내에 상주할 수도 있다. ASIC는 사용자 단말기 내에 상주할 수도 있다. 다른 방법으로, 프로세서 및 저장 매체는 사용자 단말기 내에 개별 컴포넌트로서 상주할 수도 있다.

<57> 개시되어 있는 실시형태들에 대한 상기의 설명은 당업자로 하여금 본 발명을 제조 또는 이용할 수 있도록 제공된다. 당업자는 이들 실시형태에 대한 다양한 변형들을 명백히 알 수 있으며, 여기에서 정의된 일반적인 원리들은 본 발명의 사상 또는 범위를 벗어나지 않고도 다른 실시형태들에 적용될 수도 있다. 따라서, 본 발명은 여기에서 설명된 실시형태들에 제한되는 것이 아니라, 여기에서 개시된 원리 및 신규한 특징들과 부합하는 최광의 범위를 부여하려는 것이다.

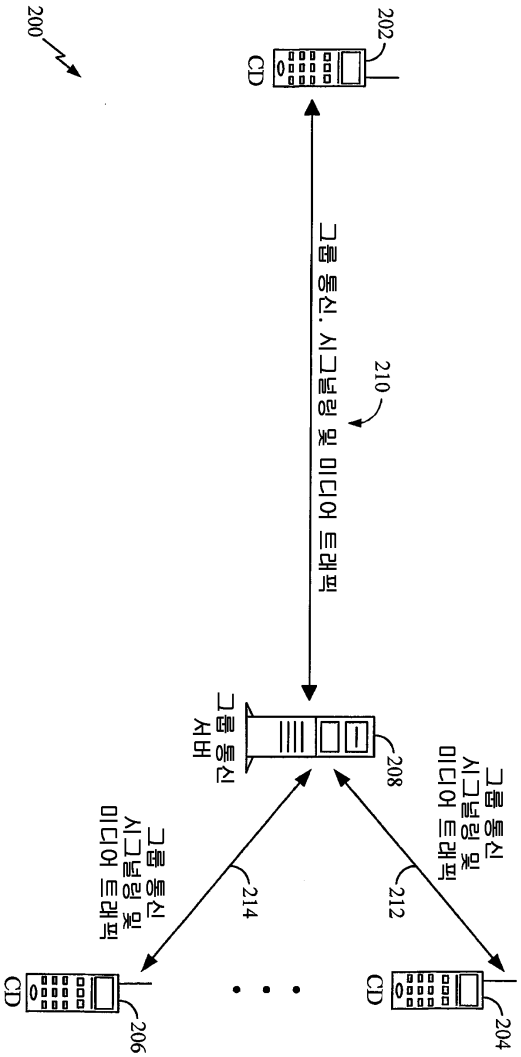
<58> "예시적인" 은 "예, 예증, 또는 실례" 를 의미하기 위해 전적으로 사용된다. 여기에 "예시적인" 으로 개시된 임의의 실시형태는 다른 실시형태보다 선호되거나 유리하게 해석될 필요가 없다.

도면

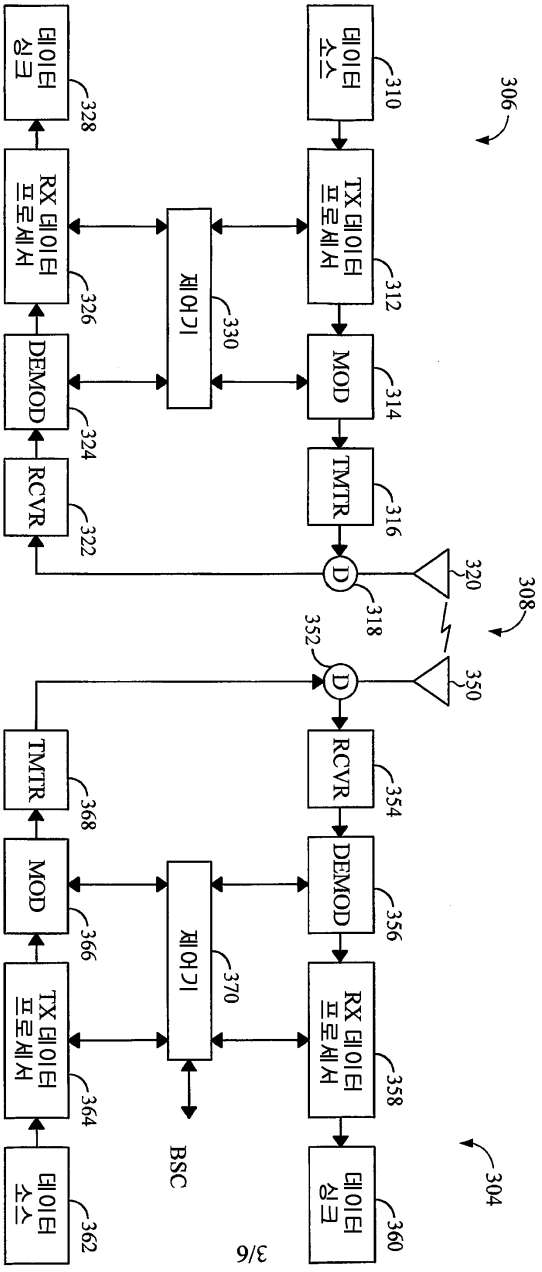
도면1



도면2

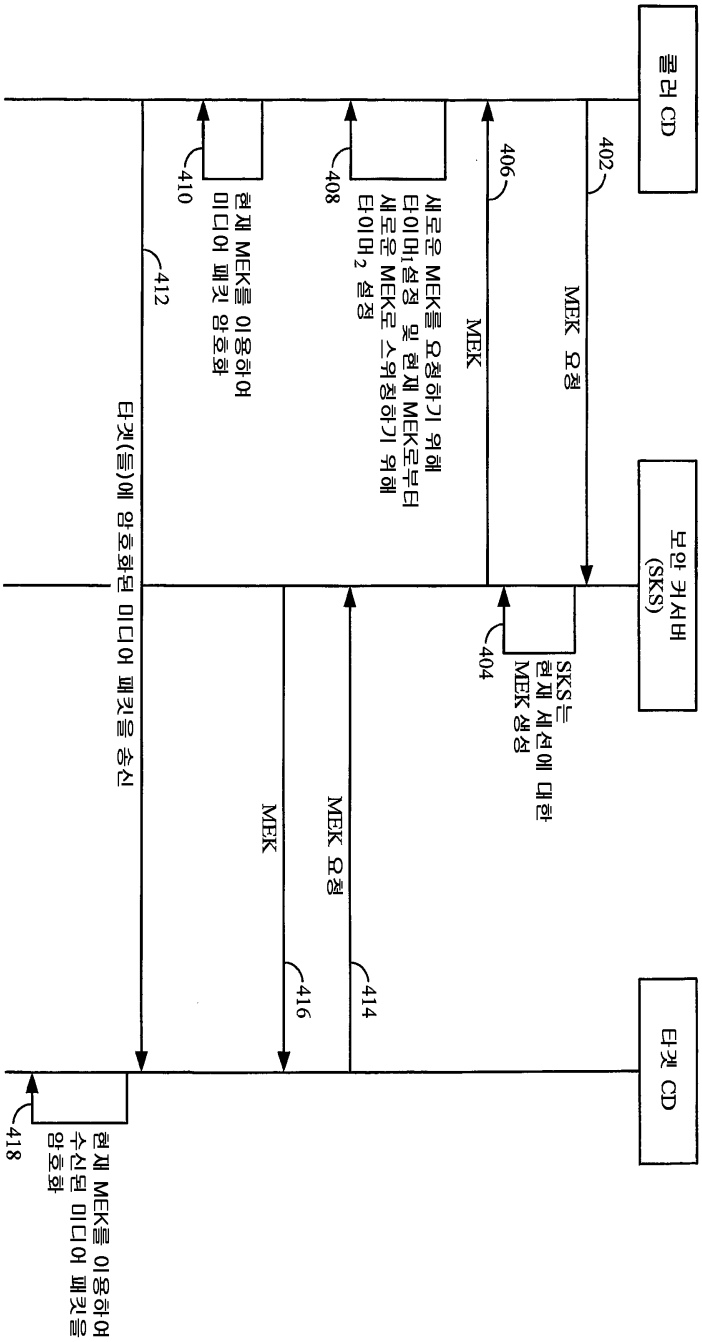

200
202
CD
그룹 통신, 시그널링 및 미디어 트래픽
210
그룹 통신 서버
208
그룹 통신 시그널링 및 미디어 트래픽
212
그룹 통신 시그널링 및 미디어 트래픽
214
CD
206
CD
204

도면3

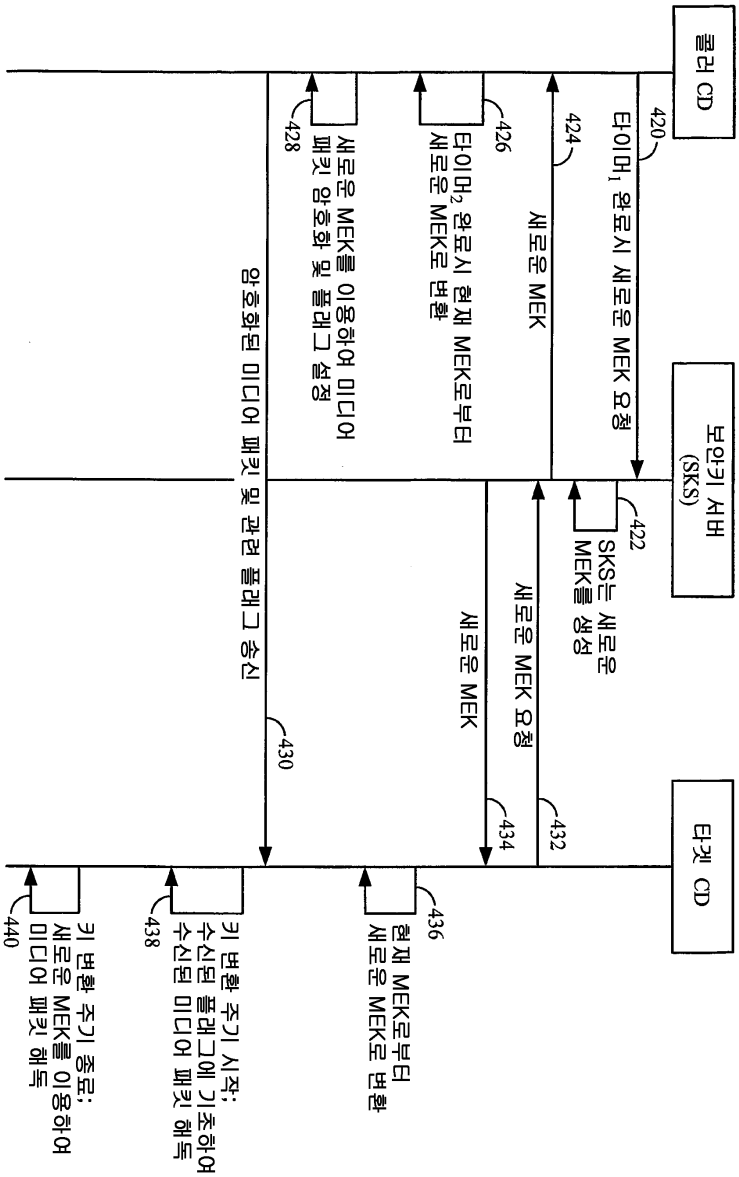

306
데이터 소스
310
TX 데이터 프로세서
312
MOD
314
TMTR
316
D
318
320
308
352
D
350
RCVR
354
DEMOD
356
RX 데이터 프로세서
358
데이터 싱크
360
304
TMTR
368
MOD
366
TX 데이터 프로세서
364
데이터 소스
362
제어기
370
BSC
제어기
330
RX 데이터 프로세서
326
DEMOD
324
RCVR
322
데이터 싱크
328

3/6

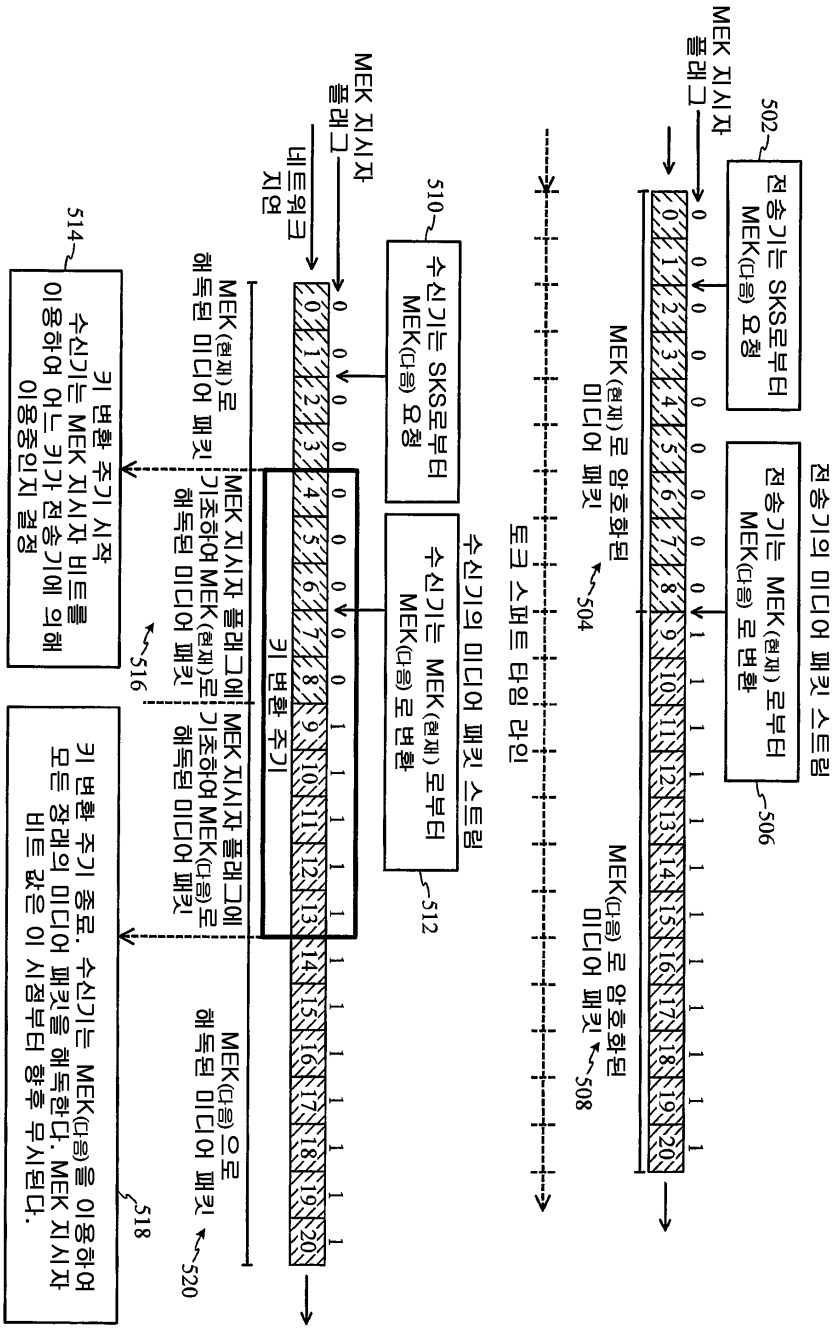
도면4a


콜러 CD
보안 커서버 (SKS)
타겟 CD
402
MEK 요청
406
MEK
404
SKS는 현재 세션에 대한 MEK 생성
408
새로운 MEK를 요청하기 위해 타이머1설정 및 현재 MEK로부터 새로운 MEK로 스위칭하기 위해 타이머2 설정
410
현재 MEK를 이용하여 미디어 패킷 암호화
412
타겟(들)에 암호화된 미디어 패킷을 송신
MEK
416
MEK 요청
414
418
현재 MEK를 이용하여 수신된 미디어 패킷을 암호화

도면4b


클라 CD
보안키 서버 (SKS)
타겟 CD
420
타이머1 완료시 새로운 MEK 요청
424
새로운 MEK
422
SKS는 새로운 MEK를 생성
426
타이머2 완료시 현재 MEK로부터 새로운 MEK로 변환
428
새로운 MEK를 이용하여 미디어 패킷 암호화 및 플래그 설정
암호화된 미디어 패킷 및 관련 플래그 송신
430
새로운 MEK
새로운 MEK 요청
434
432
436
현재 MEK로부터 새로운 MEK로 변환
키 변환 주기 시작; 수신된 플래그에 기초하여 수신된 미디어 패킷 해독
438
키 변환 주기 종료; 새로운 MEK를 이용하여 미디어 패킷 해독
440

도면5


전송기의 미디어 패킷 스트림
전송기는 SKS로부터 MEK(다음) 요청
502
전송기는 MEK(현재) 로부터 MEK(다음) 로 변환
506
MEK 지시자 플래그
MEK(현재)로 암호화된 미디어 패킷
504
MEK(다음) 로 암호화된 미디어 패킷
508
토크 스퍼트 타임 라인
수신기의 미디어 패킷 스트림
수신기는 SKS로부터 MEK(다음) 요청
510
수신기는 MEK(현재) 로부터 MEK(다음) 로 변환
512
MEK 지시자 플래그
네트워크 지연
키 변환 주기
MEK(현재)로 해독된 미디어 패킷
516
MEK 지시자 플래그에 기초하여 MEK(현재)로 해독된 미디어 패킷
MEK 지시자 플래그에 기초하여 MEK(다음)로 해독된 미디어 패킷
520
키 변환 주기 시작
수신기는 MEK 지시자 비트를 이용하여 어느 키가 전송기에 의해 이용중인지 결정
514
키 변환 주기 종료. 수신기는 MEK(다음)을 이용하여 모든 장래의 미디어 패킷을 해독한다. MEK 지시자 비트 값은 이 시점부터 향후 무시된다.
518