



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년05월24일
(11) 등록번호 10-1860440
(24) 등록일자 2018년05월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/14 (2006.01)
H04W 12/04 (2009.01) H04W 12/06 (2009.01)
(21) 출원번호 10-2011-0065387
(22) 출원일자 2011년07월01일
심사청구일자 2016년06월28일
(65) 공개번호 10-2013-0003806
(43) 공개일자 2013년01월09일
(56) 선행기술조사문헌
US20090196424 A1*
US20010023487 A1
US20090219850 A1
US20070280235 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
강현정
서울특별시 강남구 논현로 209 104동 602호 (도곡동, 경남아파트)
백영교
서울특별시 구로구 고척로3길 62, 동서빌라402호 (오류동)
라케쉬 타오리
경기도 수원시 영통구 효원로 363, 신아파트 111동 1101호 (매탄동, 매탄 위브 하늘채)
(74) 대리인
권혁록, 이정순

전체 청구항 수 : 총 34 항

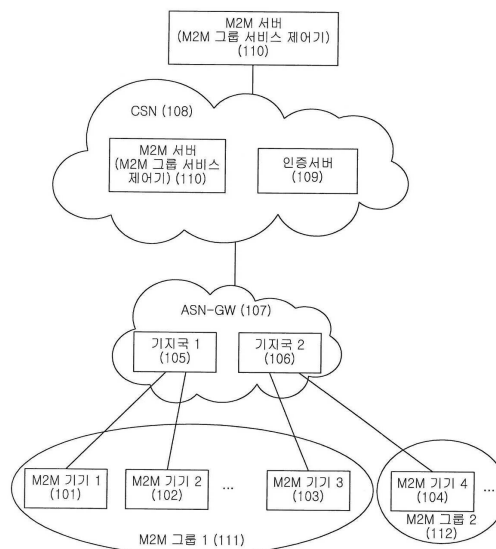
심사관 : 양종필

(54) 발명의 명칭 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키 관리 방법, 장치 그리고 시스템

(57) 요약

본 발명은 기기 간 통신 시스템에서 멀티캐스트 서비스를 송·수신하는 단말과 기지국 간 멀티캐스트 데이터의 암호화를 제공하기 위한 것으로, 상기 멀티캐스트 서비스를 관리하는 기기 통신 서비스 제어국이 상기 멀티캐스트 데이터를 암호화하기 위한 정보를 관리하고 상기 단말과 기지국에 제공하는 방안에 대한 것이다.

대표도 - 도1



명세서

청구범위

청구항 1

무선 통신 시스템에서 단말의 동작 방법에 있어서,
 기지국을 통해 네트워크 진입 절차를 수행하는 과정과,
 상기 네트워크 진입 절차 시, M2M(machine-to-machine) 서비스 그룹 보안 씨드(M2M service group security seed)를 상기 기지국으로부터 수신하는 과정과,
 M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, M2M 그룹 식별자, 멀티캐스트 데이터 암호화 키의 인덱스(index)를 나타내는 키 카운터 값(key counter value), 및 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열에 기반하여, 상기 멀티캐스트 데이터 암호화 키를 생성하는 과정과,
 상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 기지국과 데이터를 송수신하는 과정을 포함하는 방법.

청구항 2

제 1항에 있어서,
 상기 네트워크 진입 절차 시, 상기 M2M 그룹 식별자 및 상기 M2M 서비스 인증 키 중 적어도 하나를 상기 기지국으로부터 수신하는 과정을 더 포함하는 방법.

청구항 3

제 1항에 있어서,
 상기 멀티캐스트 데이터 암호화 키는, 하기 수학식에 의해 결정되는 방법.

$$MGTEK = \text{Dot16KDF}(MAK, MGSS \| \text{Key_counter} \| MGID \| \text{"MGTEK"}, 128)$$

여기서, MGTEK는 상기 멀티캐스트 데이터 암호화 키이고, MAK는 상기 M2M 서비스 인증 키, MGSS는 상기 M2M 서비스 그룹 보안 씨드, Key_counter는 상기 키 카운터 값이고, MGID는 상기 M2M 그룹 식별자, "MGTEK"는 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 상기 M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, 상기 키 카운터 값, 및 상기 M2M 그룹 식별자를 입력으로 하는 128비트의 상기 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘임.

청구항 4

제 1항에 있어서,
 상기 M2M 서비스 그룹 보안 씨드를 상기 기지국으로부터 수신하는 과정은,
 등록 요청 메시지를 상기 기지국으로 송신하는 과정과,
 상기 M2M 서비스 그룹 보안 씨드를 포함한 등록 응답 메시지를 상기 기지국으로부터 수신하는 과정을 포함하는 방법.

청구항 5

제 1항에 있어서,

상기 M2M 서비스 그룹 보안 씨드를 상기 기지국으로부터 수신하는 과정은,

상기 기지국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함하는 서비스 플로우 생성 요청 메시지를 수신하는 과정과,

상기 기지국에게 서비스 플로우 생성 응답 메시지를 송신하는 과정을 포함하거나,

상기 기지국에게 상기 서비스 플로우 생성 요청 메시지를 송신하는 과정과,

상기 기지국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 상기 서비스 플로우 생성 응답 메시지를 수신하는 과정을 포함하는 방법.

청구항 6

제 1항에 있어서,

유희모드 구간인지를 결정하는 과정과,

상기 유희모드 구간일 시, 위치등록 절차를 지시하는 페이징 메시지 수신 여부를 결정하는 과정과,

상기 위치등록 절차 시, 레인징 메시지를 통해 다른 M2M 서비스 그룹 보안 씨드가 수신되는지 여부를 결정하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하는 방법.

청구항 7

제 1항에 있어서,

유희모드 구간인지를 결정하는 과정과,

상기 유희모드 구간일 시, 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보를 포함하는 페이징 메시지를 수신하는 과정과,

상기 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보에 따라, 다른 M2M 서비스 그룹 보안 씨드를 수신하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하는 방법.

청구항 8

제 1항에 있어서,

서비스 변경 요청 메시지 혹은 인증 절차에서 교환되는 메시지를 통해, 다른 M2M 서비스 그룹 보안 씨드를 상기 기지국으로부터 수신하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하며,

상기 서비스 변경 요청 메시지는, 유니캐스팅 혹은 멀티캐스팅되는 방법.

청구항 9

무선 통신 시스템에서 기지국의 동작 방법에 있어서,

단말의 네트워크 진입 절차를 지원하는 과정과,

상기 네트워크 진입 절차 시, 시스템 제어국으로부터 M2M(machine-to-machine) 서비스 그룹 보안 씨드(M2M service group security seed)를 수신하여, 상기 M2M 서비스 그룹 보안 씨드를 상기 단말에게 송신하는 과정과,

M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, M2M 그룹 식별자, 멀티캐스트 데이터 암호화 키의 인덱스(index)를 나타내는 키 카운터 값(key counter value), 및 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열에 기반하여, 상기 멀티캐스트 데이터 암호화 키를 생성하는 과정과,

상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 단말과 데이터를 송수신하는 과정을 포함하는 방법.

청구항 10

제 9항에 있어서,

상기 M2M 그룹 식별자 및 상기 M2M 서비스 인증 키 중 적어도 하나를 상기 단말에게 송신하는 과정을 더 포함하는 방법.

청구항 11

제 9항에 있어서,

상기 멀티캐스트 데이터 암호화 키는, 하기 수학적식에 의해 결정되는 방법.

$$MGTEK = \text{Dot16KDF}(MAK, MGSS | \text{Key_counter} | MGID | \text{"MGTEK"}, 128)$$

여기서, MGTEK는 상기 멀티캐스트 데이터 암호화 키이고, MAK는 상기 M2M 서비스 인증 키, MGSS는 상기 M2M 서비스 그룹 보안 씨드, Key_counter는 상기 키 카운터 값이고, MGID는 상기 M2M 그룹 식별자, "MGTEK"는 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 상기 M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, 상기 키 카운터 값, 및 상기 M2M 그룹 식별자를 입력으로 하는 128비트의 상기 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘임.

청구항 12

제 9항에 있어서,

상기 네트워크 진입 절차 시, 시스템 제어국으로부터 M2M 서비스 그룹 보안 씨드를 수신하여, 상기 M2M 서비스 그룹 보안 씨드를 상기 단말에게 송신하는 과정은,

등록 요청 메시지를 상기 단말로부터 수신할 시, 상기 단말이 네트워크에 진입함을 알리는 단말 등록 요청 메시지를 상기 시스템 제어국으로 송신하는 과정과,

상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 등록 응답 메시지를 상기 시스템 제어국으로부터 수신하는 과정과,

상기 시스템 제어국으로부터 수신한 상기 M2M 서비스 그룹 보안 씨드를 상기 등록 응답 메시지를 통해 상기 단말로 송신하는 과정을 포함하는 방법.

청구항 13

제 9항에 있어서,

상기 네트워크 진입 절차 시, 시스템 제어국으로부터 M2M 서비스 그룹 보안 씨드를 수신하여, 상기 M2M 서비스

그룹 보안 씨드를 상기 단말로 송신하는 과정은,

상기 시스템 제어국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 서비스 플로우 생성 요청 메시지를 수신하는 과정과,

상기 시스템 제어국으로부터 수신한 상기 M2M 서비스 그룹 보안 씨드를 서비스 플로우 생성 요청 메시지를 통해 상기 단말로 송신하는 과정과,

상기 단말로부터 서비스 플로우 생성 응답 메시지를 수신하는 과정을 포함하는 방법.

청구항 14

제 9항에 있어서,

상기 네트워크 진입 절차 시, 시스템 제어국으로부터 M2M 서비스 그룹 보안 씨드를 수신하여, 상기 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하는 과정은,

상기 단말로부터 서비스 플로우 생성 요청 메시지를 수신 시, 상기 시스템 제어국에게 단말 서비스 플로우 생성 요청 메시지를 송신하는 과정과,

상기 시스템 제어국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 서비스 플로우 생성 응답 메시지를 수신하여, 서비스 플로우 생성 응답 메시지를 통해 상기 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하는 과정과,

상기 단말로부터 서비스 플로우 생성 확인 메시지를 수신한 후, 단말 서비스 플로우 생성 확인 메시지를 상기 시스템 제어국에 송신하는 과정을 포함하는 방법.

청구항 15

제 9항에 있어서,

상기 시스템 제어국으로부터, 다른 M2M 서비스 그룹 보안 씨드를 수신하는 과정과,

서비스 변경 요청 메시지 혹은 인증 절차에서 교환되는 메시지를 통해, 상기 다른 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하며,

상기 서비스 변경 요청 메시지는, 유니캐스팅 혹은 멀티캐스팅되는 방법.

청구항 16

제 9항에 있어서,

유희모드 구간인지를 결정하는 과정과,

상기 유희모드 구간일 시, 위치등록 절차를 지시하는 페이징 메시지를 상기 단말로 송신하는 과정과,

상기 위치등록 절차 시, 레인징 메시지를 통해 다른 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하는 방법.

청구항 17

제 9항에 있어서,

유희모드 구간인지를 결정하는 과정과,

상기 유희모드 구간일 시, 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보를 포함하는 페이지 메시지를 송신하는 과정과,

상기 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보에 따라, 다른 M2M 서비스 그룹 보안 씨드를 송신하는 과정과,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하는 과정을 더 포함하는 방법.

청구항 18

무선 통신 시스템에서 단말 장치에 있어서,

송수신부와,

상기 송수신부와 기능적으로 결합된 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

기지국을 통해 네트워크 진입 절차를 수행하고,

상기 네트워크 진입 절차 시, M2M(machine-to-machine) 서비스 그룹 보안 씨드(M2M service group security seed)를 상기 기지국으로부터 수신하고,

M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, M2M 그룹 식별자, 멀티캐스트 데이터 암호화 키의 인덱스(index)를 나타내는 키 카운터 값(key counter value), 및 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열에 기반하여, 상기 멀티캐스트 데이터 암호화 키를 생성하고,

상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 기지국과 데이터를 송수신하도록 제어하는 장치.

청구항 19

청구항 18에 있어서,

상기 적어도 하나의 프로세서는, 상기 네트워크 진입 절차 시, 상기 M2M 그룹 식별자 및 상기 M2M 서비스 인증 키 중 적어도 하나를 상기 기지국으로부터 수신하도록 제어하는 장치.

청구항 20

청구항 18에 있어서,

상기 멀티캐스트 데이터 암호화 키는, 하기 수학식에 의해 결정되는 장치.

$$MGTEK = \text{Dot16KDF}(MAK, MGSS \| Key_counter \| MGID \| "MGTEK", 128)$$

여기서, MGTEK는 상기 멀티캐스트 데이터 암호화 키이고, MAK는 상기 M2M 서비스 인증 키, MGSS는 상기 M2M 서비스 그룹 보안 씨드, Key_counter는 상기 키 카운터 값이고, MGID는 상기 M2M 그룹 식별자, "MGTEK"는 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 상기 M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, 상기 키 카운터 값, 및 상기 M2M 그룹 식별자를 입력으로 하는 128비트의 상기 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘임.

청구항 21

청구항 18에 있어서,
 상기 적어도 하나의 프로세서는,
 등록 요청 메시지를 상기 기지국으로 송신하고,
 상기 M2M 서비스 그룹 보안 씨드를 포함한 등록 응답 메시지를 상기 기지국으로부터 수신하도록 제어하는 장치.

청구항 22

청구항 18에 있어서,
 상기 적어도 하나의 프로세서는,
 상기 기지국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 서비스 플로우 생성 요청 메시지를 수신하고,
 상기 기지국에게 서비스 플로우 생성 응답 메시지를 송신하거나,
 상기 기지국에게 상기 서비스 플로우 생성 요청 메시지를 송신하고,
 상기 기지국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 상기 서비스 플로우 생성 응답 메시지를 수신하도록 제어하는 장치.

청구항 23

청구항 18에 있어서, 상기 적어도 하나의 프로세서는,
 유희모드 구간인지를 결정하고,
 상기 유희모드 구간일 시, 위치등록 절차를 지시하는 페이징 메시지 수신 여부를 결정하고,
 상기 위치등록 절차 시, 레인징 메시지를 통해 다른 M2M 서비스 그룹 보안 씨드가 수신되는지 여부를 결정하고,
 상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하는 장치.

청구항 24

청구항 18에 있어서,
 상기 적어도 하나의 프로세서는,
 유희모드 구간인지를 결정하고,
 상기 유희모드 구간일 시 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보를 포함하는 페이징 메시지를 수신하고,
 상기 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보에 따라, 다른 M2M 서비스 그룹 보안 씨드를 수신하고,
 상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하는 장치.

청구항 25

청구항 18에 있어서,
 상기 적어도 하나의 프로세서는,
 서비스 변경 요청 메시지 혹은 인증 절차에서 교환되는 메시지를 통해, 다른 M2M 서비스 그룹 보안 씨드를 상기

기지국으로부터 수신하고,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하고,

상기 서비스 변경 요청 메시지는, 유니캐스팅 혹은 멀티캐스팅되는 장치.

청구항 26

무선 통신 시스템에서 기지국 장치에 있어서,

송수신부와,

상기 송수신부와 기능적으로 결합된 적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

단말의 네트워크 진입 절차를 지원하고,

상기 네트워크 진입 절차 시, 시스템 제어국으로부터 M2M(machine-to-machine) 서비스 그룹 보안 씨드(M2M service group security seed)를 수신하여, 상기 M2M 서비스 그룹 보안 씨드를 상기 단말에게 송신하고,

M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, M2M 그룹 식별자, 멀티캐스트 데이터 암호화 키의 인덱스(index)를 나타내는 키 카운터 값(key counter value), 및 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열에 기반하여, 상기 멀티캐스트 데이터 암호화 키를 생성하고,

상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 단말과 데이터를 송신하도록 제어하는 장치.

청구항 27

청구항 26에 있어서,

상기 적어도 하나의 프로세서는,

상기 M2M 그룹 식별자 및 상기 M2M 서비스 인증 키 중 적어도 하나를 상기 단말에게 송신하도록 제어하는 장치.

청구항 28

청구항 26에 있어서,

상기 멀티캐스트 데이터 암호화 키는, 하기 수학식에 의해 결정되는 장치.

$$MGTEK = \text{Dot16KDF}(MAK, MGSS | \text{Key_counter} | MGID | "MGTEK", 128)$$

여기서, MGTEK는 상기 멀티캐스트 데이터 암호화 키이고, MAK는 상기 M2M 서비스 인증 키, MGSS는 상기 M2M 서비스 그룹 보안 씨드, Key_counter는 상기 키 카운터 값이고, MGID는 상기 M2M 그룹 식별자, "MGTEK"는 상기 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 상기 M2M 서비스 인증 키, 상기 M2M 서비스 그룹 보안 씨드, 상기 키 카운터 값, 및 상기 M2M 그룹 식별자를 입력으로 하는 128비트의 상기 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘임.

청구항 29

청구항 26에 있어서, 상기 적어도 하나의 프로세서는,

등록 요청 메시지를 상기 단말로부터 수신할 시, 상기 단말이 네트워크에 진입함을 알리는 단말 등록 요청 메시지를 상기 시스템 제어국으로 송신하고,

상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 등록 응답 메시지를 상기 시스템 제어국으로부터 수신하고,
상기 시스템 제어국으로부터 수신한 상기 M2M 서비스 그룹 보안 씨드를 등록 응답 메시지를 통해 상기 단말로 송신하도록 제어하는 장치.

청구항 30

청구항 26에 있어서, 상기 적어도 하나의 프로세서는,
상기 시스템 제어국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 서비스 플로우 생성 요청 메시지를 수신하고,
상기 시스템 제어국으로부터 수신한 상기 M2M 서비스 그룹 보안 씨드를 서비스 플로우 생성 요청 메시지를 통해 상기 단말로 송신하며,
상기 단말로부터 서비스 플로우 생성 응답 메시지를 수신하도록 제어하는 장치.

청구항 31

청구항 26에 있어서, 상기 적어도 하나의 프로세서는,
상기 단말로부터 서비스 플로우 생성 요청 메시지를 수신 시, 상기 시스템 제어국에게 단말 서비스 플로우 생성 요청 메시지를 송신하고,
상기 시스템 제어국으로부터 상기 M2M 서비스 그룹 보안 씨드를 포함한 단말 서비스 플로우 생성 응답 메시지를 수신하여, 서비스 플로우 생성 응답 메시지를 통해 상기 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하며,
상기 단말로부터 서비스 플로우 생성 확인 메시지를 수신한 후, 단말 서비스 플로우 생성 확인 메시지를 상기 시스템 제어국에 송신하도록 제어하는 장치.

청구항 32

청구항 26에 있어서,
상기 적어도 하나의 프로세서는,
상기 시스템 제어국으로부터, 다른 M2M 서비스 그룹 보안 씨드를 수신하고,
서비스 변경 요청 메시지 혹은 인증 절차에서 교환되는 메시지를 통해, 상기 다른 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하고,
상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하고,
상기 서비스 변경 요청 메시지는, 유니캐스팅 혹은 멀티캐스팅되는 장치.

청구항 33

청구항 26에 있어서,
상기 적어도 하나의 프로세서는,
유휴모드 구간인지 결정하고,
상기 송수신부는, 상기 유휴모드 구간일 시 위치등록 절차를 지시하는 페이징 메시지를 상기 단말로 송신하고,
상기 위치등록 절차 시 레인징 메시지를 통해 다른 M2M 서비스 그룹 보안 씨드를 상기 단말로 송신하고,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하는 장치.

청구항 34

청구항 26에 있어서,

상기 적어도 하나의 프로세서는,

유희모드 구간인지를 결정하고,

상기 유희모드 구간일 시 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보를 포함하는 페이징 메시지를 송신하고,

상기 멀티캐스트 데이터 암호화 키 갱신을 지시하는 정보에 따라 다른 M2M 서비스 그룹 보안 씨드를 송신하고,

상기 다른 M2M 서비스 그룹 보안 씨드를 이용하여, 상기 멀티캐스트 데이터 암호화 키를 재생성하여 저장하도록 제어하는 장치.

발명의 설명

기술 분야

[0001] 본 발명은 기기 간 통신 시스템(machine to machine communication system)에 관한 것으로서, 특히, 기기 무선 통신 시스템에서 멀티캐스트 서비스 데이터의 암호화를 지원하기 위한 장치 및 방법에 관한 것이다.

배경 기술

[0002] 사람의 직접 제어(human interaction)가 없거나 또는 사람의 제어가 아주 제한적인 경우에 기기(device) 간 데이터 통신을 지원하는 기기 간 통신(machine to machine communication) 서비스에 대한 연구가 진행 중에 있다. 상기 기기 간 통신 서비스는 자동 제어 및 통신을 통해 기기를 관리하는 비용을 절감하고자 하는 목적에서 주목을 받고 있다. 구체적으로, 차량 및 차량에 탑재된 물품의 자동화 관리(fleet management), 자동 계량(smart metering), 홈 오토메이션(home automation), 헬스 케어 등에서 적용할 수 있는 기술로서 그 활용 가능성이 예상되고 있다.

[0003] 상기 기기 간 통신 시스템의 경우, 시스템 설계자는 일반적인 통신 시스템의 단말과 달리 특정 데이터를 제한된 기기(device)만 수신하는 경우를 고려해야 한다. 예를 들어, 특정 유틸리티 회사에서 제공하는 정보는 해당 유틸리티 회사의 서비스에 가입된 스마트 미터링(smart metering)을 수행하는 기기만 수신해야 한다. 다른 예로서, 헬스 케어 기기의 경우, 상기 헬스 케어 기기는 헬스 케어 서버(health care server)로부터 헬스 케어 정보를 수신함으로써, 최신의 헬스 케어 정보를 유지할 수 있다. 이때 상기 헬스 케어 정보는 해당 서비스에 가입한 기기에게만 전송되어야 한다.

[0004] 상술한 바와 같이, 기기 간 통신 시스템에서 단말의 목적 및 용도에 따라 제한된 데이터를 송신하거나 수신하는 상황이 발생한다. 이때, 동일한 종류의 단말들이 다수 존재하는 경우, 상기 단말들 모두 동일한 데이터를 해당 M2M 서버로부터 수신하게 된다. 이 경우, 다수의 단말이 동일한 데이터를 전송하는 효율성을 제공하기 위해 멀티캐스트(multicast) 방식의 데이터 전송이 예상되므로, 해당 데이터를 안전하게 제한된 다수의 단말들에게만 전송하기 위한 방안이 필요하다.

[0005] 따라서, 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키 관리 방안이 필요하다.

발명의 내용

해결하려는 과제

- [0006] 본 발명의 목적은 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키 관리 방법 및 장치를 제공함에 있다.
- [0007] 본 발명의 다른 목적은 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키 관리 방법 및 시스템을 제공함에 있다.
- [0008] 본 발명의 또 다른 목적은 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 방법 및 장치를 제공함에 있다.

과제의 해결 수단

- [0009] 상기한 목적들을 달성하기 위한 본 발명의 제 1 견지에 따르면, 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 단말 동작 방법에 있어서, 기지국을 통해 네트워크 진입 절차를 수행하는 과정과, 상기 네트워크 진입 절차 시, 멀티캐스트 서비스 인증 정보를 상기 기지국으로부터 수신하는 과정과, 상기 멀티캐스트 서비스 인증 정보를 이용하여, 멀티캐스트 데이터 암호화 키를 생성하여 저장하는 과정과, 상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 기지국과 데이터를 송·수신하는 과정을 포함하는 것을 특징으로 한다.
- [0010] 상기한 목적들을 달성하기 위한 본 발명의 제 2 견지에 따르면, 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 기지국 동작 방법에 있어서, 단말의 네트워크 진입 절차를 지원하는 과정과, 상기 네트워크 진입 절차 시, 시스템 제어국으로부터 멀티캐스트 서비스 인증 정보를 수신하여, 상기 멀티캐스트 서비스 인증 정보를 상기 단말에 전달하는 과정과, 상기 멀티캐스트 서비스 인증 정보를 이용하여, 멀티캐스트 데이터 암호화 키를 생성하여 저장하는 과정과, 상기 멀티캐스트 데이터 암호화 키를 이용하여, 상기 단말과 데이터를 송·수신하는 과정을 포함하는 것을 특징으로 한다.
- [0011] 상기한 목적들을 달성하기 위한 본 발명의 제 3 견지에 따르면, 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 시스템 제어국 동작 방법에 있어서, 단말과 인증서버 사이의 인증 절차를 지원하는 과정과, 상기 인증 서버와 단말의 인증 정보를 교환하는 과정과, 상기 단말의 인증 정보 교환 시, 상기 인증 서버로부터 멀티캐스트 서비스 인증 정보가 포함되어 있는지를 판단하는 과정과, 상기 인증 서버로부터 수신한 멀티캐스트 서비스 인증 정보를 기지국으로 전달하는 과정을 포함하는 것을 특징으로 한다.
- [0012] 상기한 목적들을 달성하기 위한 본 발명의 제 4 견지에 따르면, 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 시스템 제어국 동작 방법에 있어서, 단말과 인증서버 사이의 인증 절차를 지원하는 과정과, 상기 인증 서버와 단말의 인증 정보를 교환하는 과정과, 그룹서비스 제어국에 단말 기기 서비스 인증을 요청하여, 멀티캐스트 서비스 인증 정보를 수신하는 과정과, 상기 그룹서비스 제어국으로부터 수신한 멀티캐스트 서비스 인증 정보를 기지국으로 전달하는 과정을 포함하는 것을 특징으로 한다.
- [0013] 상기한 목적들을 달성하기 위한 본 발명의 제 5 견지에 따르면, 기기 간 통신 시스템에서 멀티캐스트 데이터 서비스를 위한 그룹서비스 제어국 동작 방법에 있어서, 멀티캐스트 서비스 인증 정보를 결정하는 과정과, 인증 서버 혹은 시스템 제어국으로부터 단말 기기 서비스 인증 요청을 수신할 시, 상기 결정된 멀티캐스트 서비스 인증 정보를 상기 인증서버 혹은 상기 시스템 제어국으로 전송하는 과정과, 멀티캐스트 서비스 인증 정보에 대한 변경이 필요한지를 판단하는 과정과, 멀티캐스트 서비스 인증 정보에 대한 변경이 필요할 시, 새로운 멀티캐스트 서비스 인증 정보를 결정하여 상기 인증서버 혹은 상기 시스템 제어국으로 전송하는 과정을 포함하는 것을 특징으로 한다.

발명의 효과

- [0014] 상술한 바와 같이, 기기 간 통신 시스템에서 그룹에 속한 기기(device)들로 동일한 데이터를 멀티캐스트 방식으로 전송하는 경우를 고려하여 상기 데이터에 대한 멀티캐스트 용도의 암호화 키 관리 방안을 적용함으로써, 제한된 데이터가 불특정 기기에 의해 노출되는 것을 방지하고 효과적으로 데이터를 전송할 수 있는 이점이 있다.

도면의 간단한 설명

[0015]

도 1은 본 발명의 실시 예에 따른 기기 간 통신 시스템(machine to machine communication system)의 개략적인 구성을 도시하는 도면,

도 2는 본 발명의 제1실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하는 도면,

도 3은 본 발명의 제2실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하는 도면,

도 4는 본 발명의 제3실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하는 도면,

도 5는 본 발명의 제4실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하는 도면,

도 6은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 최초로 생성하는 단말의 동작 절차를 도시하는 도면,

도 7은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 최초로 생성하는 기지국의 동작 절차를 도시하는 도면,

도 8은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 시스템 제어국의 동작 절차를 도시하는 도면,

도 9는 본 발명의 다른 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 시스템 제어국의 동작 절차를 도시하는 도면,

도 10은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 인증서버의 동작 절차를 도시하는 도면,

도 11은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 그룹 서비스 제어국의 동작 절차를 도시하는 도면,

도 12는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 갱신하는 단말의 동작 절차를 도시하는 도면,

도 13은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 갱신하는 기지국의 동작 절차를 도시하는 도면,

도 14는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키의 변경을 처리하는 시스템 제어국의 동작 절차를 도시하는 도면,

도 15는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 키 카운터에 기반하여 멀티캐스트 데이터 암호화 키를 갱신하는 기지국의 동작 절차를 도시하는 도면,

도 16은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 키 카운터에 기반하여 멀티캐스트 데이터 암호화 키를 갱신하는 단말의 동작 절차를 도시하는 도면,

도 17은 본 발명의 실시 예에 따른 단말 장치도 및,

도 18은 본 발명의 실시 예에 따른 기지국, 시스템 제어국, 인증 서버, 그리고 그룹 서비스 제어국 장치도.

발명을 실시하기 위한 구체적인 내용

[0016]

이하 본 발명의 바람직한 실시 예를 첨부된 도면의 참조와 함께 상세히 설명한다. 그리고, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

- [0017] 이하 본 발명은 기기 간 통신 시스템에서 다수의 단말로 멀티캐스트 데이터를 전송하는 경우에 멀티캐스트 데이터를 암호화하는 키를 관리하는 기술에 대해 설명한다.
- [0018] 도 1은 본 발명의 실시 예에 따른 기기 간 통신 시스템(machine to machine communication system)의 개략적인 구성을 도시하고 있다.
- [0019] 상기 도 1을 참조하면, 상기 기기 간 통신 시스템은 기기 통신을 지원하는 M2M 단말(Machine to Machine Subscriber Station)(101, 102, 103, 104), 기기 통신을 지원하는 M2M 기지국(Machine to Machine Base Station)(105, 106), 액세스 서비스 네트워크 게이트웨이(ASN-GW: Access Service Network GateWay)(107)(이하, 시스템 제어국이라 칭함), 연결 서비스 네트워크(CSN: Connected Service Network)(108), 인증서버(AAA: authentication, authorization and accounting)(109), M2M 서버/그룹 서비스 제어국(M2M server/M2M group service controller)(110)를 포함한다.
- [0020] 상기 M2M 단말(101~104)은 사용자의 개입 없이 통신을 수행하는 기기로서, 기기 통신에 필요한 응용 프로그램이 탑재된 단말이다. 상기 M2M 단말(101~104)은 상기 M2M 서버(110)가 관리하는 멀티캐스트 서비스에 가입되어 있으며 상기 M2M 단말(101~103)은 멀티캐스트 그룹 1(111)에 가입되어 있고, 상기 M2M 단말(104)은 멀티캐스트 그룹 2(112)에 가입되어 있다. 상기 M2M 기지국(105, 106) 및 상기 ASN-GW(107)는 상기 M2M 단말(101~104) 및 상기 M2M 서버(110) 간의 통신에 필요한 무선 접속점을 제공하며, 특히, 상기 M2M 기지국(105, 106)은 M2M 단말(101~104)과 상기 M2M 서버(110) 간의 통신에 필요한 무선 자원을 제어한다. 상기 ASN-GW(107)은 상기 M2M 단말(101~104)의 유희 모드 동작을 관리하는 페이지 제어국의 기능도 수행한다. 상기 CSN(108)은 상기 M2M 단말(101~104)로 사용자 측 연결 서비스를 제공한다. 상기 CSN(108)에 위치한 인증서버(109)는 상기 M2M 단말(101~104)의 액세스 네트워크 인증 서비스를 제공한다. 상기 M2M 서버(110)는 상기 하나 혹은 다수의 M2M 단말(101~104)과 통신을 수행하며, 기기 통신에 필요한 응용 프로그램을 탑재하고 있고, 사용자가 접속할 수 있는 인터페이스를 갖추고 있다. 상기 도 1에서, 시스템 운용에 따라 상기 M2M 서버(110)는 상기 CSN(108)과는 별도의 객체이거나, 상기 M2M 서버(110)는 상기 CSN(108)에 포함될 수 있다. 또한 상기 M2M 서버/그룹 서비스 제어국(110)은 본 발명의 실시 예에 따라 상기 멀티캐스트 그룹 1(111)의 서비스에 가입한 M2M 단말(101~103)과 상기 멀티캐스트 그룹 2(112)의 서비스에 가입한 M2M 단말(104)의 멀티캐스트 서비스 데이터에 대한 인증 및 암호화 키를 관리한다. 즉, 상기 멀티캐스트 그룹 1(111) 혹은 멀티캐스트 그룹 2(112)에 속한 M2M 단말에 전송하는 멀티캐스트 데이터를 암호화하기 위해 필요한 기기 서비스 단말 인증 키(MAK: M2M service Authorization Key) 및 그룹 서비스 인증 키(MGSS: M2M service Group Security Seed)를 생성하고 갱신하는 동작을 수행한다.
- [0021] 상기 기기 간 통신 시스템에서 상기 M2M 단말(101~104) 및 상기 M2M 기지국(105, 106) 간 무선 인터페이스는 기존의 통신 규격에 따르거나, 또는, 기기 간 통신 시스템을 위해 고안된 통신 규격에 따를 수 있다. 예를 들어, IEEE(Institute of Electrical and Electronic Engineers) 802.16 통신 시스템 규격이 적용될 수 있으며, 이 경우, 상기 M2M 단말(101~104)은 상기 IEEE 802.16 통신 시스템에 정의된 단말(mobile station)과 같이 동작할 수 있다. 이하 본 발명은 OFDM(Orthogonal Frequency Division Multiplexing)/OFDMA(Orthogonal Frequency Division Multiple Access) 방식의 무선 인터페이스를 예로 들어 설명한다.
- [0022] 도 2는 본 발명의 제1실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하고 있다.
- [0023] 상기 도 2를 참조하면, M2M 단말(200)과 M2M 기지국(240)은 201단계에서 동기절차에 따라 하향링크 채널 획득, MAC 동기 그리고 상향링크 채널 파라미터를 획득한다. 이후, 상기 M2M 단말(200)은 203단계에서 레인징 요청 메시지(RNG-REQ)를 전송하고 상기 M2M 기지국(240)은 205단계에서 상기 레인징 요청 메시지에 대한 응답으로서 레인징 응답 메시지(RNG-RSP)를 전송하여, 레인징 절차를 수행한다.
- [0024] 상기 M2M 단말(200)은 207단계에서 상기 M2M 기지국(240)에 기본 제공 능력을 제공하기 위해, 기본 능력 협상 요청 메시지(SBC-REQ)를 전송하고, 상기 M2M 기지국(240)은 209단계에서 새로운 단말이 네트워크에 진입하는 것을 알리기 위해서, 시스템 제어국(250)에 상기 M2M 단말(200)에 대한 사전 등록 요청 메시지를 전송한다. 상기 시스템 제어국(250)은 211단계에서 상기 M2M 단말(200)에 대한 사전 등록 응답 메시지를 상기 M2M 기지국(240)에 전송한다. 또한, 상기 시스템 제어국(250)은 상기 M2M 단말(200)에 대한 액세스 네트워크 인증을 처리하기 위해 인증서버(260)에 상기 M2M 단말(200)의 정보를 제공한다(도시하지 않음). 상기 M2M 기지국(240)은 213단계

에서 상기 M2M 단말(200)에 상기 207단계의 응답으로서 기본 능력 협상 응답 메시지(SBC-RSP)를 전송한다.

[0025] 이후, 215단계에서 상기 M2M 단말(200), M2M 기지국(240), 시스템 제어국(250) 및 인증서버(260)는 상기 M2M 단말(200)에 대한 액세스 네트워크 인증 및 암호화 절차를 수행한다. 여기서, EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA 같은 EAP 인증 방법이 사용될 수 있다.

[0026] 상기 215단계의 액세스 네트워크 인증 및 암호화 절차의 일례로서, 상기 M2M 단말(200)은 상기 M2M 기지국(240)에 인증/암호화 요청 메시지를 송신하고 상기 M2M 기지국(240)으로부터 인증/암호화 응답 메시지를 수신한다 (215-1단계 및 215-6단계). 상기 215-1단계 및 215-6단계에서는 2회 이상의 메시지 교환이 상기 M2M 단말(200)과 상기 M2M 기지국(240) 간에 발생하게 된다. 또한 상기 M2M 기지국(240)은 상기 M2M 단말(200)에 대한 인증 및 암호화 정보를 포함하는 인증 요청 메시지/인증 응답 메시지를 상기 시스템 제어국(250)과 송·수신한다 (215-2단계 및 215-5단계). 상기 215-2단계 및 215-5단계에서는 2회 이상의 메시지 교환이 상기 M2M 기지국(240)과 상기 시스템 제어국 간에 발생하게 된다. 상기 시스템 제어국(250)은 상기 M2M 단말(200)에 대한 액세스 네트워크 인증 및 암호화를 관리하는 인증서버(260)과 단말 인증 요청 메시지 및 단말 인증 응답 메시지를 송수신하며(215-3단계 및 215-4단계), 이 경우에도 상기 시스템 제어국(250)과 상기 인증서버(260) 간에 2회 이상의 메시지 교환이 발생한다.

[0027] 상기 인증서버(260)는 상기 M2M 단말(200)의 기기 통신 서비스를 제어하는 그룹 서비스 제어국(270) 즉, M2M 서버에게 217단계에서 상기 M2M 단말(200)에 대한 단말 기기 서비스 인증 요청 메시지를 전송한다. 상기 그룹 서비스 제어국(270)은 상기 M2M 단말(200)에 대한 기기 서비스 인증을 수행하고, 상기 M2M 단말(200)이 멀티캐스트 서비스에 가입되어 있는 경우에는 상기 M2M 단말(200)의 멀티캐스트 서비스 정보 및 상기 멀티캐스트 서비스 데이터 암호화에 필요한 기기 서비스 단말 인증 키 및 그룹 서비스 인증 키를 포함하는 단말 기기 서비스 인증 응답 메시지를 219단계에서 상기 인증서버(260)에 전송한다. 상기 멀티캐스트 서비스 정보는 상기 M2M 단말(200)이 가입한 멀티캐스트 그룹의 식별자 등을 포함한다.

[0028] 예를 들어, 상기 멀티캐스트 서비스 정보 및 멀티캐스트 서비스 인증 정보는 하기 <표 1>과 같이 구성될 수 있다.

표 1

Name	Description/Notes
Multicast group ID	Identifier of M2M multicast group
M2M service authorization key (기기 서비스 단말 인증 키)	M2M service authorization key that is provided to all authorized M2M devices
M2M service group security seed (그룹 서비스 인증 키)	M2M service group security seed that is common for all M2M devices in the same multicast group

[0030] 여기서, Multicast group ID 및 그룹 서비스 인증 키(M2M service group security seed)는 상기 그룹 서비스 제어국(270)에서 결정되는 파라미터이다. 상기 기기 서비스 단말 인증 키(M2M service authorization key)는 215단계에서의 액세스 네트워크 인증 및 암호화 절차 과정에서 기 M2M 단말(200), M2M 기지국(240), 시스템 제어국(250) 및 인증서버(260)에 공유되는 키(예: 마스터 세션 키(MSK: Master Session Key) 혹은 인증 키(AK: Authorization Key))이다. 구현에 따라, 상기 멀티캐스트 서비스 정보 중 기기 서비스 단말 인증 키 정보는 생략될 수 있다.

[0031] 상기 멀티캐스트 서비스 정보 및 멀티캐스트 서비스 인증 정보는 상기 기기 통신을 위한 멀티캐스트 서비스에 가입한 M2M단말을 인증하고 상기 M2M 단말의 서비스를 인증하는 용도로 사용된다. 상기 기기 서비스 단말 인증 키(MAK)은 상기 <표1>과 같이 전달되지 않고 상기 M2M 기지국과 상기 M2M 단말에게 오프라인으로 직접 전달하거나 상위 계층의 안전한 키 공유 방법을 통하여 생성 혹은 전달될 수도 있다.

[0032] 상기 219단계의 단말 기기 서비스 인증 응답 메시지를 수신한 상기 인증서버(260)은 상기 215-4단계의 단말 인증 응답 메시지를 이용하여 상기 <표 1>의 멀티캐스트 서비스 인증 정보를 상기 시스템 제어국(250)에 전송한다.

[0033] 한편 상기 M2M 단말(200)은 221단계에서 상기 M2M 기지국(240)에 등록 요청 메시지(REG-REQ)를 전송하고 상기 M2M 기지국(240)은 223단계에서 상기 M2M 단말(200)에 대한 단말 등록 요청 메시지를 상기 시스템 제어국(250)에 전송한다. 상기 시스템 제어국(250)은 225단계에서 상기 인증서버(260)로부터 수신한 그룹 서비스 인증 키를

포함하는 멀티캐스트 서비스 인증 정보를 단말 등록 응답 메시지를 이용하여 상기 M2M 기지국(240)에 전송한다. 상기 M2M 기지국(240)은 227단계에서 상기 M2M 단말(200)에 상기 그룹 서비스 인증 키를 포함하는 상기 멀티캐스트 서비스 인증 정보를 등록 응답 메시지(REG-RSP)를 이용하여 전송한다. 상기 M2M 단말(200)과 상기 M2M 기지국(240)은 각각 상기 그룹 서비스 인증 키를 포함하는 상기 멀티캐스트 서비스 인증 정보를 이용하여 멀티캐스트 데이터 암호화 키를 생성한다(229단계, 231단계). 여기서 상기 멀티캐스트 데이터 암호화 키는 하기 <수학식 1>에 의해 생성된다.

수학식 1

$$MGTEK = Dot16KDF(MAK, MGSS || MGID || "MGTEK", 128)$$

[0034]

[0035]

여기서, MGTEK는 멀티캐스트 데이터 암호화 키이고, MAK는 기기 서비스 단말 인증 키, MGSS는 그룹 서비스 인증 키, MGID는 그룹 식별자, "MGTEK"는 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 기기 서비스 단말 인증 키, 그룹 서비스 인증 키, 그룹 식별자를 입력으로 하는 128비트의 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘이다.

[0036]

다른 예로서, 상기 도 2에서 217단계 내지 219단계와 같이 상기 M2M 단말(200)이 가입한 멀티캐스트 서비스에 대한 정보 및 상기 멀티캐스트 서비스에 대한 인증 정보를 획득하기 위한 절차는 상기 시스템 제어국(250)이 요청하고 상기 그룹 서비스 제어국(270)이 응답하는 메시지 트랜잭션을 이용할 수도 있다.

[0037]

도 3은 본 발명의 제2실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하고 있다.

[0038]

상기 도 3을 참조하면, M2M 단말(300)은 301단계에서 M2M 기지국(350)에 대한 동기를 획득하고, 303단계에서 레인징 요청 메시지를 상기 M2M 기지국(350)으로 전송한다. 상기 M2M 기지국(350)은 305단계에서 상기 레인징 요청 메시지에 대한 응답으로서 레인징 응답 메시지를 상기 M2M 단말(300)으로 전송한다. 상기 M2M 단말(300)은 307단계에서 상기 M2M 기지국(350)으로 기본 능력 협상 요청 메시지를 전송하고, 상기 M2M 기지국(350)은 309단계에서 상기 M2M 단말(300)에 대한 사전 등록 요청 메시지를 시스템 제어국(360)으로 전송한다. 상기 시스템 제어국(360)은 311단계에서 상기 M2M 단말(300)에 대한 사전 등록 응답 메시지를 상기 M2M 기지국(350)으로 전송한다. 또한, 상기 시스템 제어국(360)은 상기 M2M 단말(300)에 대한 액세스 네트워크 인증을 처리하기 위해 인증서버(370)으로 상기 M2M 단말(300)의 정보를 제공한다(도시하지 않음). 상기 M2M 기지국(350)은 313단계에서 상기 307단계의 응답으로서 기본 능력 협상 응답 메시지를 상기 M2M 단말(300)로 전송한다. 이후, 315단계에서 상기 M2M 단말(300), M2M 기지국(350), 시스템 제어국(360) 및 인증서버(370)은 상기 M2M 단말(300)에 대한 액세스 네트워크 인증 및 암호화 절차를 수행한다. 상기 315단계의 액세스 네트워크 인증 및 암호화 절차는 상기 도 2의 215단계, 215-1단계 내지 215-6단계와 동일하다.

[0039]

이후, 상기 M2M 단말(300)은 317단계에서 상기 M2M 기지국(350)에 등록 요청 메시지를 전송하고 상기 M2M 기지국(350)은 319단계에서 상기 M2M 단말(300)에 대한 단말 등록 요청 메시지를 상기 시스템 제어국(360)으로 전송한다. 상기 시스템 제어국(360)은 321단계에서 상기 M2M 단말(300)에 대한 단말 기기 서비스 인증 요청 메시지를 상기 M2M 단말(300)의 기기 통신 서비스를 제어하는 그룹 서비스 제어국(380)으로 전송한다. 상기 그룹 서비스 제어국(380)은 323단계에서 상기 M2M 단말(300)에 대한 기기 서비스 인증을 수행하고, 상기 M2M 단말(300)이 멀티캐스트 서비스에 가입되어 있는 경우에는 상기 <표 1>의 M2M 단말(300)의 멀티캐스트 서비스 정보 및 상기 멀티캐스트 서비스 데이터 암호화에 필요한 기기 서비스 단말 인증 키 및 그룹 서비스 인증 키를 포함하는 단말 기기 서비스 인증 응답 메시지를 상기 시스템 제어국(360)으로 전송한다. 구현에 따라, 상기 기기 서비스 단말 인증 키가 315단계에서 액세스 네트워크 인증 및 암호화 절차 시, 단말(300), 기지국(350), 시스템 제어국(360), 인증서버(370)에 의해 공유될 경우, 단말 기기 서비스 인증 응답 메시지에 포함되지 않을 수 있다.

[0040]

상기 시스템 제어국(360)은 325단계에서 상기 그룹 서비스 제어국(380)로부터 수신한 그룹 서비스 인증 키를 포함하는 멀티캐스트 서비스 인증 정보를 단말 등록 응답 메시지를 이용하여 상기 M2M 기지국(350)으로 전송한다. 상기 M2M 기지국(350)은 327단계에서 상기 그룹 서비스 인증 키를 포함하는 상기 멀티캐스트 서비스 인증 정보를 등록 응답 메시지를 이용하여 상기 M2M 단말(300)으로 전송한다. 상기 M2M 단말(300)과 상기 M2M 기지국

(350)은 각각 상기 그룹 서비스 인증 키를 포함하는 상기 멀티캐스트 서비스 인증 정보를 이용하여 상기 <수학식 1>을 이용하여 멀티캐스트 데이터 암호화 키를 생성한다(329단계, 331단계).

[0041] 다른 일 예로서, 상기 도 3에서 321단계 내지 323단계와 같이 상기 M2M 단말(300)이 가입한 멀티캐스트 서비스에 대한 정보 및 상기 멀티캐스트 서비스에 대한 인증 정보를 획득하기 위한 절차는 상기 인증서버(370)이 요청하고 상기 그룹 서비스 제어국(380)이 응답하는 메시지 트랜잭션을 이용할 수도 있다. 이때 상기 시스템 제어국(360)은 상기 인증서버(370)로부터 상기 멀티캐스트 서비스 인증 정보를 전달받은 후에 상기 325단계의 절차를 수행하게 된다.

[0042] 도 4는 본 발명의 제3실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하고 있다.

[0043] 상기 도 4를 참조하면, M2M 단말(400)은 401단계에서 M2M 기지국(450)에 대한 동기를 획득하고, 403단계에서 레인징 요청 메시지를 M2M 기지국(450)으로 전송한다. 상기 M2M 기지국(450)은 405단계에서 레인징 요청 메시지에 대한 응답으로서 레인징 응답 메시지를 전송한다. 상기 M2M 단말(400)은 407단계에서 상기 M2M 기지국(450)으로 기본 능력 협상 요청 메시지를 전송하고, 상기 M2M 기지국(450)은 시스템 제어국(460)으로 409단계에서 상기 M2M 단말(400)에 대한 사전 등록 요청 메시지를 전송한다. 상기 시스템 제어국(460)은 411단계에서 상기 M2M 단말(400)에 대한 사전 등록 응답 메시지를 상기 M2M 기지국(450)으로 전송한다. 또한, 상기 시스템 제어국(460)은 상기 M2M 단말(400)에 대한 액세스 네트워크 인증을 처리하기 위해 인증서버(470)로 상기 M2M 단말(400)의 정보를 제공한다(도시하지 않음). 상기 M2M 기지국(450)은 413단계에서 상기 407단계의 응답으로서 기본 능력 협상 응답 메시지를 상기 M2M 단말(400)로 전송한다. 이후 415단계에서 상기 M2M 단말(400), M2M 기지국(450), 시스템 제어국(460) 및 인증서버(470)는 상기 M2M 단말(400)에 대한 액세스 네트워크 인증 및 암호화 절차를 수행한다. 상기 415단계의 액세스 네트워크 인증 및 암호화 절차는 상기 도 2의 215단계, 215-1단계 내지 215-6단계와 동일하다.

[0044] 상기 M2M 단말(400)은 417단계에서 상기 M2M 기지국(450)으로 등록 요청 메시지를 전송하고 상기 M2M 기지국(450)은 419단계에서 상기 M2M 단말(400)에 대한 단말 등록 요청 메시지를 상기 시스템 제어국(460)으로 전송한다. 상기 시스템 제어국(460)은 421단계에서 상기 M2M 단말(400)에 대한 등록 요청을 처리하고 상기 M2M 기지국(450)으로 단말 등록 응답 메시지를 전송한다. 상기 M2M 기지국(450)은 423단계에서 상기 M2M 단말(400)에 등록 응답 메시지를 전송한다. 한편 상기 시스템 제어국(460)은 425단계에서 상기 M2M 단말(400)의 기기 통신 서비스를 제어하는 그룹 서비스 제어국(480)에 상기 M2M 단말(400)에 대한 단말 기기 서비스 인증 요청 메시지를 전송한다. 상기 그룹 서비스 제어국(480)은 427단계에서 상기 M2M 단말(400)에 대한 기기 서비스 인증을 수행하고, 상기 M2M 단말(400)이 멀티캐스트 서비스에 가입되어 있는 경우에는 상기 <표 1>의 M2M 단말(400)의 멀티캐스트 서비스 정보 및 상기 멀티캐스트 서비스 데이터 암호화에 필요한 기기 서비스 단말 인증 키 및 그룹 서비스 인증 키를 포함하는 단말 기기 서비스 인증 응답 메시지를 상기 시스템 제어국(460)에 전송한다. 구현에 따라, 상기 기기 서비스 단말 인증 키가 415단계에서 액세스 네트워크 인증 및 암호화 절차 시, 단말(400), 기지국(450), 시스템 제어국(460), 인증서버(470)에 의해 공유될 경우, 단말 기기 서비스 인증 응답 메시지에 포함되지 않을 수 있다.

[0045] 상기 시스템 제어국(460)은 429단계에서 상기 M2M 단말(400)에 대한 서비스 및 경로를 생성하기 위해 단말 서비스/경로 생성 요청 메시지를 상기 M2M 기지국(450)에 전송한다. 상기 단말 서비스/경로 생성 요청 메시지는 상기 427단계에서 상기 그룹 서비스 제어국(480)에 수신한 상기 <표 1>의 그룹 서비스 인증 키 정보를 포함한다. 상기 M2M 기지국(450)은 431단계에서 상기 M2M 단말(400)에 상기 <표 1>의 그룹 서비스 인증 키 정보를 포함하는 서비스 생성 요청 메시지를 전송한다. 상기 M2M 단말(400)은 433단계에서 상기 M2M 기지국(450)에 서비스 생성 응답 메시지를 전송하고, 상기 M2M 기지국(450)은 435단계에서 서비스 생성 확인 메시지를 상기 M2M 단말(400)에 전송한다. 또한 상기 M2M 기지국(450)은 437단계에서 상기 시스템 제어국(460)에 상기 M2M 단말(400)에 대한 서비스 및 경로가 생성되었음을 알리는 단말 서비스/경로 생성 응답 메시지를 전송한다. 상기 시스템 제어국(460)은 439단계에서 상기 M2M 기지국(450)에 단말 서비스/경로 생성 확인 메시지를 전송하며, 이로써 상기 M2M 단말(400)에 서비스 플로우가 생성되고 상기 서비스 플로우를 지원할 경로가 생성된다.

[0046] 또한 상기 M2M 단말(400)과 상기 M2M 기지국(450)은 상기 수신한 그룹 서비스 인증 키를 포함하는 상기 멀티캐

스트 서비스 인증 정보를 이용하여 상기 <수학적 식 1>에 의해서 멀티캐스트 데이터 암호화 키를 생성한다(441단계, 443단계).

[0047] 다른 예로서, 상기 도 4에서 425단계 내지 427단계와 같이 상기 M2M 단말(400)이 가입한 멀티캐스트 서비스에 대한 정보 및 상기 멀티캐스트 서비스에 대한 인증 정보를 획득하기 위한 절차는 상기 인증서버(470)가 요청하고 상기 그룹 서비스 제어국(480)이 응답하는 메시지 트랜잭션을 이용할 수도 있다. 이때, 상기 시스템 제어국(460)은 상기 인증서버(470)로부터 상기 멀티캐스트 서비스 인증 정보를 전달받은 후에 상기 429단계의 절차를 수행하게 된다.

[0048] 또한 상기 도 4의 예에서는 상기 시스템 제어국(460) 및 상기 M2M 기지국(450)이 상기 서비스 생성 요청 메시지를 전송함으로써 상기 M2M 단말(400)의 서비스 생성을 트리거링하는 경우에 대해 설명하였으나, 상기 M2M 단말(400)이 상기 서비스 생성 요청 메시지를 전송함으로써 서비스 생성을 트리거링하는 경우에는 상기 M2M 기지국(450)이 상기 M2M 단말(400)에 전송하는 서비스 생성 응답 메시지를 통해 상기 <표 1>의 그룹 서비스 인증 키 정보가 제공된다.

[0049] 도 5는 본 발명의 제4실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 송수신하는 단말, 기지국, 시스템 제어국, 인증서버 및 그룹서비스 제어국의 신호 교환을 도시하고 있다.

[0050] 상기 도 5를 참조하면, M2M 단말(500)은 501단계에서 M2M 기지국(550)에 대한 동기를 획득하고, 503단계에서 레인징 요청 메시지를 전송한다. 상기 M2M 기지국(550)은 505단계에서 레인징 요청 메시지에 대한 응답으로서 레인징 응답 메시지를 전송한다. 상기 M2M 단말(500)은 507단계에서 상기 M2M 기지국(550)에 기본 능력 협상 요청 메시지를 전송하고, 상기 M2M 기지국(550)은 509단계에서 시스템 제어국(560)에 상기 M2M 단말(500)에 대한 사전 등록 요청 메시지를 전송한다. 상기 시스템 제어국(560)은 511단계에서 상기 M2M 단말(500)에 대한 사전 등록 응답 메시지를 상기 M2M 기지국(550)에 전송한다. 또한, 상기 시스템 제어국(560)은 상기 M2M 단말(500)에 대한 액세스 네트워크 인증을 처리하기 위해 인증서버(570)에 상기 M2M 단말(500)의 정보를 제공한다(도시하지 않음). 상기 M2M 기지국(550)은 상기 M2M 단말(500)에 상기 507단계의 응답으로서 기본 능력 협상 응답 메시지를 513단계에서 전송한다. 이후 515단계에서 상기 M2M 단말(500), M2M 기지국(550), 시스템 제어국(560) 및 인증서버(570)는 상기 M2M 단말(500)에 대한 액세스 네트워크 인증 및 암호화 절차를 수행한다. 상기 515단계의 액세스 네트워크 인증 및 암호화 절차는 상기 도 2의 215단계, 215-1단계 내지 215-6단계와 동일하다.

[0051] 상기 M2M 단말(500)은 517단계에서 상기 M2M 기지국(550)에 등록 요청 메시지를 전송하고 상기 M2M 기지국(550)은 519단계에서 상기 M2M 단말(500)에 대한 단말 등록 요청 메시지를 상기 시스템 제어국(560)에 전송한다. 상기 시스템 제어국(560)은 521단계에서 상기 M2M 단말(500)에 대한 등록 요청을 처리하고 상기 M2M 기지국(550)에 단말 등록 응답 메시지를 전송한다. 상기 M2M 기지국(550)은 523단계에서 상기 M2M 단말(500)에 등록 응답 메시지를 전송한다. 상기 M2M 단말(500)은 상기 M2M 기지국(550)을 통해서 상기 시스템 제어국(560)과 상기 M2M 단말(500)의 액세스 서비스 및 경로 설정 절차를 수행한다. 상기 액세스 서비스 및 경로 설정 절차를 통해 상기 M2M 단말(500)의 일반적인 데이터 트래픽이 전송된다.

[0052] 이후 상기 M2M 단말(500)은 527단계에서 상기 그룹 서비스 제어국(580)이 제공하는 기기 통신 서비스 및 멀티캐스트 서비스를 수신하기 위한 서비스 생성 요청 메시지를 전송한다. 상기 M2M 기지국(550)은 상기 서비스 생성 요청 메시지에 따라 529단계에서 상기 시스템 제어국(560)으로 상기 M2M 단말(500)의 단말 서비스 생성 요청 메시지를 전송한다. 상기 시스템 제어국(560)은 531단계에서 상기 M2M 단말(500)의 기기 통신 서비스를 제어하는 그룹 서비스 제어국(580)에 상기 M2M 단말(500)에 대한 단말 기기 서비스 인증 요청 메시지를 전송한다. 상기 그룹 서비스 제어국(580)은 533단계에서 상기 M2M 단말(500)에 대한 기기 서비스 인증을 수행하고, 상기 M2M 단말(500)이 멀티캐스트 서비스에 가입되어 있는 경우에는 상기 <표 1>의 M2M 단말(500)의 멀티캐스트 서비스 정보 및 상기 멀티캐스트 서비스 데이터 암호화에 필요한 기기 서비스 단말 인증 키 및 그룹 서비스 인증 키를 포함하는 단말 기기 서비스 인증 응답 메시지를 상기 시스템 제어국(560)에 전송한다. 구현에 따라, 상기 기기 서비스 단말 인증 키가 515단계에서 액세스 네트워크 인증 및 암호화 절차 시, 단말(500), 기지국(550), 시스템 제어국(560), 인증서버(570)에 의해 공유될 경우, 단말 기기 서비스 인증 응답 메시지에 포함되지 않을 수 있다.

[0053] 상기 시스템 제어국(560)은 535단계에서 상기 M2M 기지국(550)에 단말 서비스 생성 응답 메시지를 전송한다. 상

기 단말 서비스 생성 응답 메시지는 상기 533단계에서 상기 그룹 서비스 제어국(580)에 수신한 상기 <표 1>의 그룹 서비스 인증 키 정보를 포함한다. 상기 M2M 기지국(550)은 537단계에서 상기 M2M 단말(500)에 상기 <표 1>의 그룹 서비스 인증 키 정보를 포함하는 서비스 생성 응답 메시지를 전송한다. 상기 M2M 단말(500)은 539단계에서 상기 M2M 기지국(550)에 서비스 생성 확인 메시지를 전송하고, 상기 M2M 기지국(550)은 541단계에서 단말 서비스 생성 확인 메시지를 상기 시스템 제어국(560)에 전송한다. 또한 상기 M2M 단말(500)과 상기 M2M 기지국(550)은 각각 상기 수신한 그룹 서비스 인증 키를 포함하는 상기 멀티캐스트 서비스 인증 정보를 이용하여 상기 <수학식 1>에 의해서 멀티캐스트 데이터 암호화 키를 생성한다(543단계, 545단계).

[0054] 도 6은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 최초로 생성하는 단말의 동작 절차를 도시하고 있다.

[0055] 상기 도 6을 참조하면, M2M 단말은 600단계에서 M2M 기지국과 동기를 획득하고, 602단계에서 상기 M2M 기지국과 레인징 절차를 수행한다. 상기 M2M 단말은 상기 M2M 기지국과 604단계에서 기본 능력 협상 절차를 수행하고, 606단계에서 인증 절차를 수행한다. 상기 M2M 단말은 608단계에서 상기 M2M 기지국과 등록 절차를 수행함으로써 네트워크 진입 절차를 완료한다. 상기 M2M 단말은 610단계에서 자신이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단한다. 상기 그룹 서비스 인증 키 정보는 상기 도 2 내지 도 5에서 기술한 바와 같이 상기 608단계의 등록 절차 중에 획득되거나(도 2 혹은 도 3 참조), 혹은 상기 608단계의 등록 절차 이후의 서비스 생성 절차(도 4 혹은 도 5 참조)를 통해 획득된다(도시하지 않음). 상기 610단계의 판단에 의해 상기 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였으면, 상기 M2M 단말은 612단계에서 상기 <수학식 1>에 의해 멀티캐스트 데이터 암호화 키를 만들고, 614단계에서 상기 M2M 기지국과의 데이터 송수신을 수행한다. 상기 614단계에서 상기 M2M 기지국을 통해 멀티캐스트 데이터를 수신한 경우에 상기 M2M 단말은 상기 612단계에서 생성한 멀티캐스트 데이터 암호화 키를 이용하여 상기 멀티캐스트 데이터를 해독한다.

[0056] 도 7은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 최초로 생성하는 기지국의 동작 절차를 도시하고 있다.

[0057] 상기 도 7을 참조하면, 상기 M2M 기지국은 700단계에서 상기 M2M 기지국을 통해 네트워크 서비스에 등록하려는 M2M 단말의 네트워크 진입 절차 처리를 수행한다. 상기 M2M 기지국은 702단계에서 상기 네트워크 진입 절차 중 상기 M2M 단말에 대한 인증 절차를 처리하고, 704단계에서 상기 M2M 단말의 등록 절차를 처리한다. 상기 M2M 기지국은 706단계에서 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 갖고 있는지 판단한다. 상기 그룹 서비스 인증 키 정보는 상기 M2M 단말의 등록 절차(도 2 혹은 도 3 참조) 혹은 상기 M2M 단말의 서비스 생성 절차(도 4 혹은 도 5 참조) 중에 상기 시스템 제어국을 통해 획득된다. 상기 M2M 기지국은 708단계에서 상기 그룹 서비스 인증 키 정보를 이용하여 상기 <수학식 1>에 의하여 멀티캐스트 데이터 암호화 키를 생성한다. 또한 상기 M2M 기지국은 710단계에서 상기 M2M 단말의 등록 절차 혹은 상기 M2M 단말의 서비스 생성 절차 중에 상기 그룹 서비스 인증 키 정보를 상기 M2M 단말에 전송한다. 712단계에서 상기 M2M 기지국은 상기 M2M 단말과의 데이터 송수신을 수행하며, 특히 상기 M2M 단말이 가입한 멀티캐스트 그룹의 멀티캐스트 데이터를 송신해야 하는 경우에는 상기 708단계에서 만든 멀티캐스트 데이터 암호화 키를 통해 상기 멀티캐스트 데이터를 암호화한다.

[0058] 상기 도 7에서는 상기 M2M 기지국이 멀티캐스트 그룹에 대해 최초로 그룹 서비스 인증 키를 수신하고 멀티캐스트 데이터 암호화 키를 생성하는 동작에 대해 설명하였다. 만약 상기 M2M 기지국이 상기 멀티캐스트 그룹에 대한 그룹 서비스 인증 키를 이미 갖고 있는 경우에는 M2M 단말의 네트워크 진입 절차 혹은 서비스 생성 절차를 통해 상기 그룹 서비스 인증 키를 수신하지 않고, 상기 M2M 단말이 가입한 멀티캐스트 그룹 식별자 정보를 상기 시스템 제어국에서 수신함으로써 상기 M2M 단말에 적용할 그룹 서비스 인증 키를 결정할 수 있다.

[0059] 도 8은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 시스템 제어국의 동작 절차를 도시하고 있다.

[0060] 상기 도 8을 참조하면, 상기 시스템 제어국은 800단계에서 상기 M2M 기지국을 통해 전달된 상기 M2M 단말의 인

증 절차를 진행한다. 상기 시스템 제어국은 802단계에서 상기 M2M 단말에 대한 인증 정보를 상기 인증 서버와 교환한다. 상기 시스템 제어국은 상기 인증 서버로부터 804단계에서 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단한다. 상기 그룹 서비스 인증 키 정보의 획득 절차는 상기 도 2 내지 도 5에서 기술한 바와 동일하다. 상기 시스템 제어국은 806단계에서 상기 <표 1>의 그룹 서비스 인증 키 정보를 상기 M2M 기지국에 전달하고, 808단계에서 상기 M2M 단말에 대한 인증 및 서비스 경로 설정 절차를 완료한다.

[0061] 도 9는 본 발명의 다른 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 시스템 제어국의 동작 절차를 도시하고 있다.

[0062] 상기 도 9를 참조하면, 상기 시스템 제어국은 900단계에서 상기 M2M 기지국을 통해 전달된 상기 M2M 단말의 인증 절차를 진행한다. 상기 시스템 제어국은 902단계에서 상기 M2M 단말에 대한 인증 정보를 상기 인증 서버와 교환한다. 상기 시스템 제어국은 904단계에서 상기 그룹 서비스 제어국에 상기 M2M 단말에 대한 기기 서비스 인증을 요청하고, 906단계에서 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단한다. 상기 그룹 서비스 인증 키 정보의 획득 절차는 상기 도 2 내지 도 5에서 기술한 바와 동일하다. 상기 시스템 제어국은 908단계에서 상기 <표 1>의 그룹 서비스 인증 키 정보를 상기 M2M 기지국으로 전달하고, 910단계에서 상기 M2M 단말에 대한 인증 및 서비스 경로 설정 절차를 완료한다.

[0063] 도 10은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 인증서버의 동작 절차를 도시하고 있다.

[0064] 상기 도 10을 참조하면, 상기 인증서버는 1000단계에서 상기 시스템 제어국으로부터 상기 M2M 단말에 대한 인증 요청을 처리하고, 1002단계에서 상기 M2M 단말에 대한 액세스 네트워크 인증 절차를 수행한다. 상기 인증서버는 1004단계에서 상기 그룹 서비스 제어국에 상기 M2M 단말에 대한 기기 서비스 인증 요청을 전송한다. 상기 1004단계는 상기 인증서버가 직접 기기 서비스 인증 요청을 트리거링하는 경우이거나 상기 시스템 제어국이 트리거링하는 기기 서비스 인증 요청을 전달하는 경우이다. 상기 인증서버는 1006단계에서 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단한다. 상기 1006단계의 판단결과, 상기 그룹 서비스 인증 키 정보를 획득하였으면 상기 <표 1>의 그룹 서비스 인증 키 정보를 1008단계에서 상기 시스템 제어국에 전송한다. 상기 인증서버는 1010단계에서 상기 M2M 단말에 대한 인증 절차를 완료한다.

[0065] 도 11은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키를 처리하는 그룹 서비스 제어국의 동작 절차를 도시하고 있다.

[0066] 상기 도 11을 참조하면, 상기 그룹 서비스 제어국은 1100단계에서 기기 통신의 멀티캐스트 서비스, 멀티캐스트 그룹 및 상기 멀티캐스트 그룹 서비스 인증 키 정보를 관리한다. 상기 1102단계에서 상기 그룹 서비스 제어국은 M2M 단말에 대한 기기 서비스 인증 요청을 수신하면, 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 상기 <표 1>의 그룹 서비스 인증 키 정보를 1104단계에서 전달한다.

[0067] 이후 상기 그룹 서비스 제어국은 1106단계에서 상기 멀티캐스트 그룹에 대한 변경이 있는지 판단한다. 상기 멀티캐스트 그룹에 대한 변경은 그룹에 가입한 M2M 단말이 탈퇴하거나 새로운 M2M 단말이 가입하는 경우에 해당한다. 상기 멀티캐스트 그룹에 변경이 있으면 상기 그룹 서비스 제어국은 1108단계에서 상기 멀티캐스트 그룹에 대한 그룹 서비스 인증 키를 새로 생성한다. 상기 그룹 서비스 제어국은 1110단계에서 상기 새로 생성한 그룹 서비스 인증 키 정보를 상기 서비스 제어국 혹은 상기 인증 서버에 전달한다. 혹은 상기 멀티캐스트 그룹에 변경이 없으면, 상기 그룹 서비스 제어국은 1112단계에서 상기 그룹 서비스 인증 키에 대한 유효 시간이 완료되는지를 판단한다. 상기 1112단계에서 상기 그룹 서비스 인증 키의 유효 시간이 완료되는 경우에는 상기 1108단계로 진행하여 새로운 그룹 서비스 인증 키를 생성한다. 반면 상기 1112단계에서 상기 그룹 서비스 인증 키의 유효 시간이 완료되지 않은 경우 1100단계로 진행한다.

[0068] 상기 도 11에서, 멀티캐스트 그룹 변경 혹은 그룹 서비스 인증 키의 유효시간 만료로 인해 재생성된 그룹 서비스 인증키는 멀티캐스트 그룹 내 모든 M2M 단말에 유니캐스팅 혹은 멀티캐스팅으로 전송되어야 한다. 예를 들어, 그룹 변경시 그룹에서 탈퇴한 M2M 단말에 재생성된 그룹 서비스 인증키를 전송할 필요 없으므로, 이때는

멀티캐스트 그룹 내의 나머지 단말들 각각에 대해 재생성된 그룹 서비스 인증키를 유니캐스팅한다. 그룹 서비스 인증 키의 유효시간 만료로 인해(멀티캐스트 그룹 변경 없음) 재생성된 그룹 서비스 인증키는 제어메시지(예: DSC (Dynamic Service Change) 메시지)를 통해 멀티캐스팅되거나, 멀티캐스트 데이터를 통해 멀티캐스팅될 수 있다.

[0069] 도 12는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 갱신하는 단말의 동작 절차를 도시하고 있다.

[0070] 상기 도 12를 참조하면, 상기 M2M 단말은 1200단계에서 액티브 모드의 동작을 수행한다. 상기 액티브 모드의 동작은 상기 M2M 기지국과 유니캐스트 데이터 송·수신을 수행하는 것을 의미한다. 상기 M2M 단말은 1202단계에서 액티브 모드에서 유휴 모드(idle mode)로 진입하는지를 판단한다. 상기 1102단계에서 유휴 단계로 진입하지 않을 시, 상기 M2M 단말은 1204단계에서 새로운 그룹 서비스 인증 키 정보를 수신하였는지 판단한다. 상기 새로운 그룹 서비스 인증 키 정보는 상기 M2M 기지국이 전송하는 서비스 변경 요청 메시지 혹은 상기 606단계의 인증 절차에서 교환하는 메시지 혹은 멀티캐스트 데이터를 통해 전달된다. 상기 1204단계의 판단결과, 새로운 그룹 서비스 인증 키가 수신되면 상기 M2M 단말은 상기 <수학식 1>에 의해 1206단계에서 멀티캐스트 데이터 암호화 키를 다시 생성한다. 만약 상기 1202단계의 판단결과, 상기 M2M 단말이 유휴 모드로 진입하는 경우에는 1208단계로 진행하여 유휴 모드 동작을 수행한다. 상기 M2M 단말은 1210단계에서 위치 등록 절차 수행을 지시하는 페이지징 메시지를 수신하는지 판단한다. 상기 1210단계의 판단결과, 위치 등록 절차 수행이 지시되었으면 상기 M2M 단말은 1212단계에서 위치 등록 절차를 수행한다. 상기 M2M 단말은 1214단계에서 상기 위치 등록 절차를 수행하는 중에 새로운 그룹 서비스 인증 키 정보를 수신하였는지 판단한다. 상기 1214단계의 상기 새로운 그룹 서비스 인증 키는 레인징 응답 메시지를 통해 전달된다. 상기 새로운 그룹 서비스 인증 키가 수신된 경우에는 상기 M2M 단말은 1216단계에서 상기 <수학식 1>에 의해 멀티캐스트 데이터 암호화 키를 다시 생성한다.

[0071] 한편, 상기 1210단계에서 상기 유휴 모드 단말이 멀티캐스트 데이터 암호화 키를 갱신해야 함을 지시하기 위해 위치 등록 절차 수행 지시하는 대신, 상기 멀티캐스트 데이터 암호화 키 갱신 지시를 직접 페이지징 메시지에 포함할 수도 있다.

[0072] 도 13은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키를 갱신하는 기지국의 동작 절차를 도시하고 있다.

[0073] 상기 도 13을 참조하면, 상기 M2M 기지국은 1300단계에서 M2M 단말과의 데이터 송·수신 등 상기 M2M 단말의 통신 서비스를 지원하는 동작을 수행한다. 상기 M2M 기지국은 1302단계에서 상기 시스템 제어국으로부터 상기 <표 1>의 새로운 그룹 서비스 인증 키 정보를 수신한다. 상기 M2M 기지국은 1304단계에서 상기 새로운 그룹 서비스 인증 키를 이용하여 멀티캐스트 데이터 암호화 키를 다시 생성한다. 상기 M2M 기지국은 1306단계에서 유휴 모드 단말에 상기 새로운 그룹 서비스 인증 키 정보를 전송해야 하는지 판단한다. 상기 1306단계는 상기 시스템 제어국(페이징 제어국 포함)으로부터 유휴 모드 단말에 상기 그룹 서비스 인증 키 정보를 수신하여 멀티캐스트 데이터 암호화 키를 갱신하도록 지시하는 페이지징 요청 메시지를 수신하는 경우이다. 상기 1306단계의 판단에 의해 상기 유휴 모드 단말에게는 상기 멀티캐스트 데이터 암호화 키를 갱신하도록 지시하지 않아도 되는 경우에는 1308단계로 진행하여 액티브 모드에 있는 단말에 상기 1302단계에서 수신한 새로운 그룹 서비스 인증 키 정보를 전송한다. 상기 1308단계에서 상기 새로운 그룹 서비스 인증 키 정보는 서비스 변경 요청 메시지 혹은 상기 606단계의 인증 절차에서 교환하는 메시지 혹은 멀티캐스트 데이터를 통해 제공된다.

[0074] 혹은 상기 1306단계의 판단에 의해 상기 유휴 모드 단말에도 상기 멀티캐스트 데이터 암호화 키를 갱신하도록 지시해야 하는 경우에는 1310단계로 진행하여 상기 유휴 모드 단말에 위치 등록 절차 수행을 지시하는 정보를 포함하는 페이지징 메시지를 전송한다.

[0075] 이후 상기 M2M 기지국은 1312단계에서 상기 새로운 그룹 서비스 인증 키 정보를 수신해야 하는 멀티캐스트 그룹의 유휴 모드 단말이 위치 등록 절차를 수행하는지 판단한다. 상기 멀티캐스트 그룹의 유휴 모드 단말이 위치 등록 절차를 수행하는 것으로 판단되면, 상기 M2M 기지국은 1314단계에서 상기 유휴 모드 단말에 위치 등록 절차 중의 레인징 응답 메시지를 이용하여 새로운 그룹 서비스 인증 키 정보를 전송한다.

[0076] 한편 상기 1310단계에서 상기 유휴 모드 단말에 멀티캐스트 데이터 암호화 키를 갱신하도록 위치 등록 절차 수행을 지시하는 대신, 상기 멀티캐스트 데이터 암호화 키 갱신 지시 정보를 직접 상기 페이지징 메시지에 포함할

수도 있다.

- [0077] 상기 1308단계에서 상기 M2M 기지국이 상기 새로운 그룹 서비스 인증 키 정보를 M2M 단말에 멀티캐스트 방식으로 전달해야 하는지를 판단하기 위해서는, 시스템 제어국으로부터 그룹 변경에 의한 멀티캐스트 데이터 암호화 키 갱신을 지시하는지에 대한 지시자가 상기 1302단계에서 수신되어야 한다.
- [0078] 도 14는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 그룹 서비스 인증 키의 변경을 처리하는 시스템 제어국의 동작 절차를 도시하고 있다.
- [0079] 상기 도 14를 참조하면, 상기 시스템 제어국은 1400단계에서 상기 그룹 서비스 제어국 혹은 상기 인증 서버로부터 새로운 그룹 서비스 인증 키를 수신한다. 상기 시스템 제어국 중 유희 모드 단말을 관리하는 페이징 제어국은 1402단계에서 상기 새로운 그룹 서비스 인증 키를 상기 유희 모드 단말에도 전송해야 하는지 판단한다. 상기 1402단계의 판단에 의해, 상기 유희 모드 단말에도 상기 새로운 그룹 서비스 인증 키를 전송해야 하는 경우에는 상기 시스템 제어국은 M2M 기지국에게 1404단계에서 상기 새로운 그룹 서비스 인증 키와 상기 유희 모드 단말이 위치 등록 절차를 통해 상기 멀티캐스트 데이터 암호화 키를 갱신해야 함을 지시하는 페이징 요청 메시지를 전송한다.
- [0080] 혹은 상기 1402단계의 판단에 의해, 상기 유희 모드 단말에 상기 새로운 그룹 서비스 인증 키를 전송하지 않아도 되는 경우에는 상기 시스템 제어국은 1406단계에서 상기 M2M 기지국에 상기 새로운 그룹 서비스 인증 키를 전송한다.
- [0081] 상기 1404단계 혹은 상기 1406단계에서 상기 시스템 제어국은 그룹 변경에 의한 멀티캐스트 데이터 암호화 키 갱신을 지시하는지에 대한 지시자도 포함한다.
- [0082] 도 15는 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 키 카운터에 기반하여 멀티캐스트 데이터 암호화 키를 갱신하는 기지국의 동작 절차를 도시하고 있다.
- [0083] 상기 도 15를 참고하면, 상기 M2M 기지국은 1500단계에서 멀티캐스트 데이터 송신을 포함하여 상기 M2M 단말의 통신 서비스를 지원하는 동작을 수행한다. 상기 M2M 기지국은 1502단계에서 상기 M2M 단말에 전송하는 데이터에 대한 재전송 공격(replay attack)을 방지하기 위해 사용하는 재전송 공격 방지용 카운터가 만료되었는지 판단한다. 상기 1502단계의 판단에 의해, 상기 재전송 공격 방지용 카운터가 만료되지 않은 경우에는 상기 1500단계의 동작을 수행한다. 만약 상기 1502단계의 판단에 의해, 상기 재전송 공격 방지용 카운터가 만료된 경우에는 상기 M2M 기지국은 1504단계로 진행하여 키 카운터가 만료되었는지 판단한다. 상기 키 카운터는 멀티캐스트 데이터 암호화 키를 생성하는 데 사용하며, 상기 키 카운터가 만료되는 경우에는 상기 멀티캐스트 데이터 암호화 키를 갱신한다. 상기 키 카운터는 기기 서비스 단말 인증 키 혹은 그룹 서비스 인증 키에 의해 상기 멀티캐스트 데이터 암호화 키를 갱신하지 않아도 되는 경우, 상기 재전송 공격 방지를 위해 사용하는 재전송 공격 방지용 카운터의 만료로 인해 상기 멀티캐스트 데이터 암호화 키를 갱신해야 하는 오버헤드를 줄이기 위해 사용한다. 상기 재전송 공격 방지용 카운터 및 키 카운터는 상기 멀티캐스트 데이터 암호화 키가 갱신될 때마다 초기화된다.
- [0084] 여기서 상기 키 카운터를 입력 값으로 하는 상기 멀티캐스트 데이터 암호화 키는 하기 <수학식 2>에 의해 생성된다.

수학식 2

$$[0085] \quad MGTEK = \text{Dot16KDF}(MAK, MGSS \| \text{Key_counter} \| MGID \| "MGTEK", 128)$$

[0086] 여기서, MGTEK는 멀티캐스트 데이터 암호화 키이고, MAK는 기기 서비스 단말 인증 키, MGSS는 그룹 서비스 인증 키, Key_counter는 키 카운터 값이고, MGID는 그룹 식별자, "MGTEK"는 멀티캐스트 데이터 암호화 키임을 나타내는 문자열이고, Dot16KDF는 MAK, MGSS, Key_counter, MGID를 입력으로 하는 128비트의 멀티캐스트 데이터 암호화 키를 생성하는 알고리즘이다.

[0087] 상기 1504단계의 판단에 의해 상기 키 카운터가 만료된 경우에는 상기 M2M 기지국은 상기 멀티캐스트 데이터 암

호화 키를 갱신해야 함을 인지하고, 1506단계에서 상기 그룹 서비스 제어국에 상기 그룹 서비스 인증 키 정보를 요청한다. 상기 1506단계에서 상기 그룹 서비스 인증 키 정보 요청은 상기 시스템 제어국을 통해, 혹은 인증 서버를 통해 상기 그룹 서비스 제어국에 전송된다. 상기 M2M 기지국은 1508단계에서 상기 그룹 서비스 제어국이 전송한 상기 <표 1>의 새로운 그룹 서비스 인증 키 정보를 수신한다. 상기 M2M 기지국은 1510단계에서 상기 새로운 그룹 서비스 인증 키를 이용하여 멀티캐스트 데이터 암호화 키를 다시 생성한다. 상기 M2M 기지국은 1512단계에서 M2M 단말에 상기 새로운 그룹 서비스 인증 키 정보를 전송한다. 상기 1512단계에서 상기 M2M 기지국은 도 13의 절차를 따른다.

[0088] 만약 상기 1504단계의 판단에 의해 상기 키 카운터가 만료되지 않았으면 상기 M2M 기지국은 1500단계의 동작을 수행한다.

[0089] 도 16은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 키 카운터에 기반하여 멀티캐스트 데이터 암호화 키를 갱신하는 단말의 동작 절차를 도시하고 있다.

[0090] 상기 도 16을 참고하면, 상기 M2M 단말은 1600단계에서 상기 M2M 기지국을 통해 멀티캐스트 데이터 수신을 포함한 통신 서비스를 제공받는다. 상기 M2M 단말은 1602단계에서 상기 재전송 공격 방지용 카운터가 만료되었는지 판단한다. 상기 1602단계의 판단에 따라 상기 재전송 공격 방지용 카운터가 만료되지 않았으면 상기 M2M 단말은 1600단계의 동작을 수행한다. 만약 상기 1602단계의 판단에 따라 상기 재전송 공격 방지용 카운터가 만료되었으면 상기 M2M 단말은 1604단계에서 상기 키 카운터가 만료되었는지 판단한다. 상기 1604단계의 판단에 의해 상기 키 카운터가 만료되었으면 상기 M2M 단말은 1606단계에서 상기 M2M 기지국을 통해 전송되는 상기 <표 1>의 새로운 그룹 서비스 인증 키 정보를 수신한다. 여기서 상기 새로운 그룹 서비스 인증 키 정보를 수신하는 동작은 상기 도 12의 절차를 따른다. 상기 M2M 단말은 1608단계에서 상기 새로운 그룹 서비스 인증 키를 이용하여 멀티캐스트 데이터 암호화 키를 갱신한다.

[0091] 만약 상기 1604단계의 판단에 의해 상기 키 카운터가 만료되지 않았으면, 상기 M2M 단말은 1600단계의 동작을 수행한다.

[0092] 도 17은 본 발명의 실시 예에 따른 단말 장치도를 도시하고 있다.

[0093] 상기 도 17을 참조하면, 상기 단말은 제어부(1702), OFDM수신기(1700), 그리고 OFDM송신기(1704)를 포함하여 구성된다.

[0094] 상기 OFDM수신기(800)는 OFDM/OFDMA 통신방식에 기반하여, 상기 M2M 기지국으로부터 신호를 수신한다. 예를 들어, OFDM수신기(1700)는 네트워크 진입 절차 및 M2M 서비스 등록 절차시 상기 M2M 기지국과 교환되는 메시지를 수신하여 상기 제어부(1702)로 제공한다.

[0095] 상기 OFDM송신기(1704)는 상기 제어부(1702)로부터 네트워크 진입 절차 및 M2M 서비스 등록 절차를 위한 메시지를 제공받아, 상기 메시지를 OFDM/OFDMA 통신방식에 기반하여, 상기 M2M 기지국으로 전송한다.

[0096] 상기 제어부(1702)는 네트워크 진입 절차 및 M2M 서비스 등록 절차를 수행하기 위해서, 상기 OFDM수신기(1700)로부터 제공받은 해당 제어 메시지를 분석하고, 해당 제어 메시지를 생성하여 상기 OFDM송신기(1704)로 출력한다. 본 발명에 더하여, 상기 제어부(1702)는 상기 도 2 내지 상기 도 5 그리고 상기 도 6, 도 12를 참조하여 설명한 본 발명의 실시 예와 관련된 동작을 수행하기 위하여 디지털 신호 처리 과정을 수행하고 다양한 처리 모듈들의 동작을 제어한다.

[0097] 예를 들면, 상기 제어부(802)는 등록절차 시, 기지국으로부터의 해당 제어메시지 내에 단말이 속한 관리영역 정보가 포함되어 있는지를 확인하고, 상기 해당 제어메시지 내에 단말이 속한 관리영역 정보가 포함되어 있을 시, 상기 단말이 속한 관리영역 정보를 기반으로, 통신을 수행한다.

[0098] 구체적으로, 상기 제어부(1702)는 M2M 기지국과 동기절차, 레인징 절차, 기본 능력 협상 절차, 인증 절차 그리고 등록 절차를 수행함으로써 네트워크 진입 절차를 완료한다. 이후, 상기 제어부(1702)는 서비스 플로우 생성을 M2M 기지국에 요청하거나 상기 M2M 기지국으로부터 서비스 플로우 생성을 요청받을 수 있다. 또한, 상기 제어부(1702)는 상기 도 2 내지 도 5에서 기술한 바와 같이 상기 608단계의 등록 절차 중에 획득되거나(도 2 혹은 도 3 참조), 혹은 서비스 플로우 생성 절차(도 4 혹은 도 5 참조)를 통해 멀티캐스트 그룹에 대한 그룹 서비스

인증 키 정보를 획득하였는지 판단한다. 그리고, 상기 제어부(1702)는 상기 그룹 서비스 인증 키 정보를 이용하여 상기 <수학식 1>에 의해 멀티캐스트 데이터 암호화 키를 생성하여, M2M 기지국과의 데이터 송·수신을 수행한다.

[0099] 한편, 상기 제어부(1702)는 액티브 모드에서 유휴 모드(idle mode)로 진입하는지를 판단하여, 유휴 단계로 진입하지 않을 시, 새로운 그룹 서비스 인증 키 정보를 수신하였는지 판단한다. 상기 새로운 그룹 서비스 인증 키 정보는 상기 M2M 기지국이 전송하는 서비스 변경 요청 메시지 혹은 상기 인증 절차에서 교환하는 메시지를 통해 전달된다. 그리고, 상기 제어부(1702)는 상기 새로운 그룹 서비스 인증 키가 수신되면 상기 <수학식 1>를 이용하여 멀티캐스트 데이터 암호화 키를 다시 생성한다. 만약 상기 M2M 단말이 유휴 모드로 진입하는 경우, 유휴 모드 동안에 위치 등록 절차 수행을 지시하는 페이징 메시지를 수신하는지 판단하고, 위치 등록 절차 수행이 지시되었으면 위치 등록 절차를 수행한다. 상기 제어부(1702)는 상기 위치 등록 절차를 수행하는 중에 새로운 그룹 서비스 인증 키 정보를 수신하였는지 판단한다. 여기서, 상기 새로운 그룹 서비스 인증 키는 레인징 응답 메시지를 통해 전달된다. 상기 새로운 그룹 서비스 인증 키가 수신된 경우에는 상기 <수학식 1>에 의해 멀티캐스트 데이터 암호화 키를 다시 생성한다.

[0100] 또한, 상기 제어부(1702)는 재전송 공격 방지용 카운터 및 키 카운터가 만료되었는지 판단하여, 상기 재전송 공격 방지용 카운터 및 키 카운터 만료 여부에 따라 상기 M2M 기지국을 통해 전송되는 상기 <표 1>의 새로운 그룹 서비스 인증 키 정보를 수신한다. 여기서 상기 새로운 그룹 서비스 인증 키 정보를 수신하는 동작은 상기 도 12의 절차를 따른다. 그리고 상기 새로운 그룹 서비스 인증 키를 이용하여 멀티캐스트 데이터 암호화 키를 갱신한다.

[0101] 도 18은 본 발명의 실시 예에 따른 기기 간 통신 시스템에서 멀티캐스트 데이터 암호화 키 관리를 위한 장치도를 도시하고 있다. 상기 장치는 기지국, 시스템 제어국, 인증 서버, 그리고 그룹 서비스 제어국 중 하나일 수 있다.

[0102] 상기 도 18을 참조하면, 제어부(1802), 인터페이스부(1802) 그리고 데이터베이스(1802)를 포함하여 구성된다.

[0103] 상기 제어부(1802)는 해당 네트워크 엔티티(예: 기지국, 시스템 제어국, 인증 서버, 그리고 그룹 서비스 제어국 중 하나임)의 전반적인 동작하고, 인터페이스부(1802)는 네트워크 엔티티간 해당 프로토콜을 기반으로 신호전송을 담당한다. 그리고 데이터베이스(1802)는 해당 네트워크 엔티티 동작 중에 발생하는 데이터를 저장한다. 예를 들어, 상위 네트워크 엔티티로부터 제공받은 그룹 서비스 인증 키 정보를 저장한다.

[0104] 구체적으로, 기지국의 상기 제어부(1802)는 네트워크 서비스에 등록하려는 M2M 단말의 네트워크 진입 절차(동기 절차, 레인징 절차, 기본 능력협상 절차, 인증절차, 등록 절차 등등을 포함) 처리를 수행한다. 그리고, 상기 제어부(1802)는 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 갖고 있는지 판단한다. 상기 그룹 서비스 인증 키 정보는 상기 M2M 단말의 등록 절차(도 2 혹은 도 3 참조) 혹은 상기 M2M 단말의 서비스 생성 절차(도 4 혹은 도 5 참조) 중에 시스템 제어국을 통해 획득된다. 그리고 상기 제어부(1802)는 상기 그룹 서비스 인증 키 정보를 이용하여 상기 <수학식 1>에 의하여 멀티캐스트 데이터 암호화 키를 생성한다.

[0105] 시스템 제어국의 제어부(1802)는 M2M 기지국을 통해 전달된 M2M 단말의 인증 절차를 진행하고, 상기 M2M 단말에 대한 인증 정보를 인증 서버와 교환한다. 그리고, 상기 제어부(1802)는 상기 인증 서버로부터 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단한다. 상기 그룹 서비스 인증 키 정보의 획득 절차는 상기 도 2 내지 도 5에서 기술한 바와 동일하다.

[0106] 인증서버의 제어부(1802)는 상기 시스템 제어국으로부터 M2M 단말에 대한 인증 요청을 처리하고, 상기 M2M 단말에 대한 액세스 네트워크 인증 절차를 수행한다. 제어부(1802)는 상기 그룹 서비스 제어국에 상기 M2M 단말에 대한 기기 서비스 인증 요청을 전송한다. 이는, 상기 인증서버가 직접 기기 서비스 인증 요청을 트리거링하는 경우이거나 상기 시스템 제어국이 트리거링하는 기기 서비스 인증 요청을 전달하는 경우이다. 상기 제어부(1802)는 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 그룹 서비스 인증 키 정보를 획득하였는지 판단하고, 상기 그룹 서비스 인증 키 정보를 획득하였으면 상기 <표 1>의 그룹 서비스 인증 키 정보를 상기 시스템 제어국으로 전송한다.

[0107] 그룹 서비스 제어국의 제어부(1802)는 기기 통신의 멀티캐스트 서비스, 멀티캐스트 그룹 및 상기 멀티캐스트 그룹 서비스 인증 키 정보를 관리한다. 즉, M2M 단말에 대한 기기 서비스 인증 요청을 수신하면, 상기 M2M 단말이 가입한 멀티캐스트 그룹에 대한 상기 <표 1>의 그룹 서비스 인증 키 정보를 전달한다. 그리고, 상기 멀티캐스트

그룹에 대한 변경이 있는지 판단한다. 상기 멀티캐스트 그룹에 대한 변경은 그룹에 가입한 M2M 단말이 탈퇴하거나 새로운 M2M 단말이 가입하는 경우에 해당한다. 상기 멀티캐스트 그룹에 변경이 있으면 상기 멀티캐스트 그룹에 대한 그룹 서비스 인증 키를 새로 생성하여 서비스 제어국 혹은 상기 인증 서버로 전달한다. 혹은 상기 멀티캐스트 그룹에 변경이 없으면, 제어부(1802)는 상기 그룹 서비스 인증 키에 대한 유효 시간이 완료되는지를 판단하여, 상기 그룹 서비스 인증 키의 유효 시간이 완료되는 경우에는 새로운 그룹 서비스 인증 키를 생성한다.

[0108] 상기 기지국의 제어부(1802)는 유희 모드에서 새로운 그룹 서비스 인증 키 정보를 전송해야 하는지 판단한다. 즉, 상기 시스템 제어국(페이징 제어국 포함)으로부터 유희 모드 단말에 상기 그룹 서비스 인증 키 정보를 수신하여 멀티캐스트 데이터 암호화 키를 갱신하도록 지시하는 페이징 요청 메시지를 수신할 수 있다. 상기 유희 모드 단말에게는 상기 멀티캐스트 데이터 암호화 키를 갱신하도록 지시하지 않아도 되는 경우에는 액티브 모드에 있는 단말에 수신한 새로운 그룹 서비스 인증 키 정보를 전송한다. 혹은 상기 유희 모드 단말에도 상기 멀티캐스트 데이터 암호화 키를 갱신하도록 지시해야 하는 경우에는 상기 유희 모드 단말에 위치 등록 절차 수행을 지시하는 정보를 포함하는 페이징 메시지를 전송한다. 이후 제어부(1802)는 상기 새로운 그룹 서비스 인증 키 정보를 수신해야 하는 멀티캐스트 그룹의 유희 모드 단말이 위치 등록 절차를 수행하는지 판단한다. 상기 멀티캐스트 그룹의 유희 모드 단말이 위치 등록 절차를 수행하는 것으로 판단되면, 상기 유희 모드 단말에 위치 등록 절차 중의 레인징 응답 메시지를 이용하여 새로운 그룹 서비스 인증 키 정보를 전송한다. 구현에 따라, 상기 유희 모드 단말에 멀티캐스트 데이터 암호화 키를 갱신하도록 위치 등록 절차 수행을 지시하는 대신, 상기 멀티캐스트 데이터 암호화 키 갱신 지시 정보를 직접 상기 페이징 메시지에 포함할 수도 있다.

[0109] 시스템 제어국의 제어부(1802)는 그룹 서비스 제어국 혹은 상기 인증 서버로부터 새로운 그룹 서비스 인증 키를 수신하고, 상기 새로운 그룹 서비스 인증 키를 상기 유희 모드 단말에도 전송해야 하는지 판단한다. 그리고 판단에 따라 상기 유희 모드 단말에도 상기 새로운 그룹 서비스 인증 키를 전송해야 하는 경우에는 M2M 기지국에 상기 새로운 그룹 서비스 인증 키와 상기 유희 모드 단말이 위치 등록 절차를 통해 상기 멀티캐스트 데이터 암호화 키를 갱신해야 함을 지시하는 페이징 요청 메시지를 전송한다.

[0110] 한편, 상기 기지국의 제어부(1802)는 M2M 단말에 전송하는 데이터에 대한 재전송 공격을 방지하기 위해 사용하는 재전송 공격 방지용 카운터 및 키 카운터가 만료되었는지 판단하여, 상기 멀티캐스트 데이터 암호화 키를 갱신한다. 상기 키 카운터는 멀티캐스트 데이터 암호화 키를 생성하는 데 사용한다. 그리고, 상기 키 카운터가 만료된 경우에는 상기 M2M 기지국은 상기 멀티캐스트 데이터 암호화 키를 갱신해야 함을 인지하고, 상기 그룹 서비스 제어국에 상기 그룹 서비스 인증 키 정보를 요청하여, 상기 그룹 서비스 제어국이 전송한 상기 <표 1>의 새로운 그룹 서비스 인증 키 정보를 수신하고, 상기 새로운 그룹 서비스 인증 키를 이용하여 멀티캐스트 데이터 암호화 키를 다시 생성하여, M2M 단말에 상기 새로운 그룹 서비스 인증 키 정보를 전송한다.

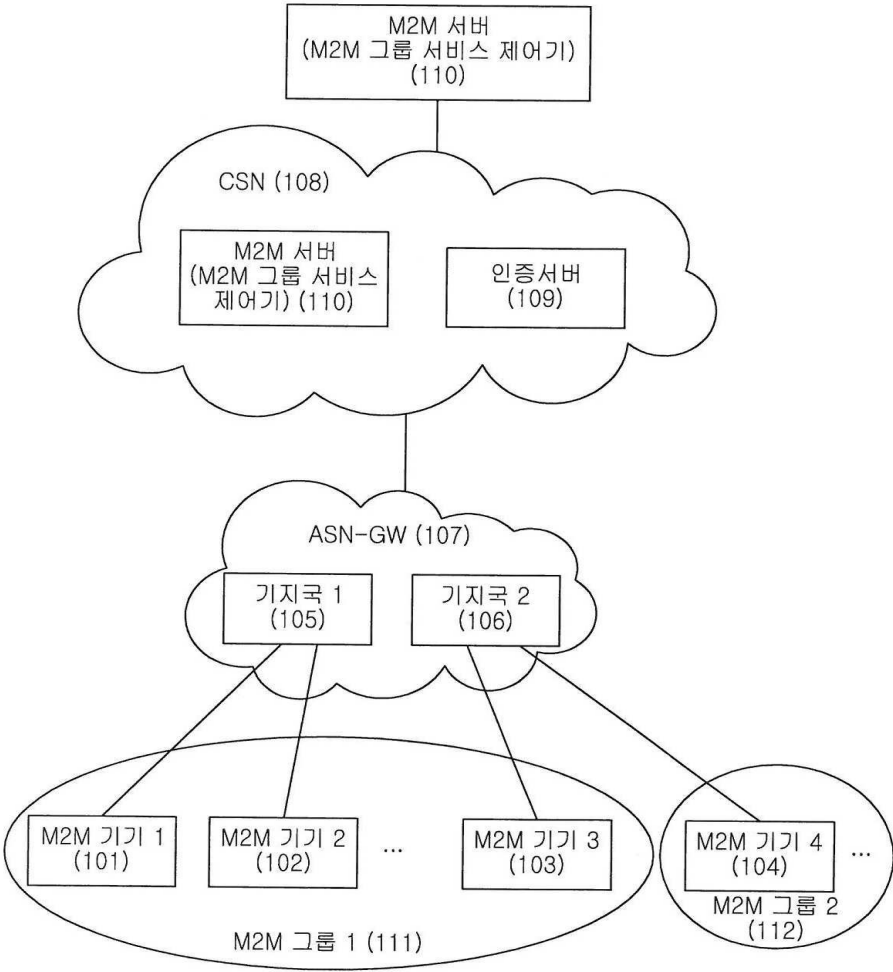
[0111] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 아니 되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

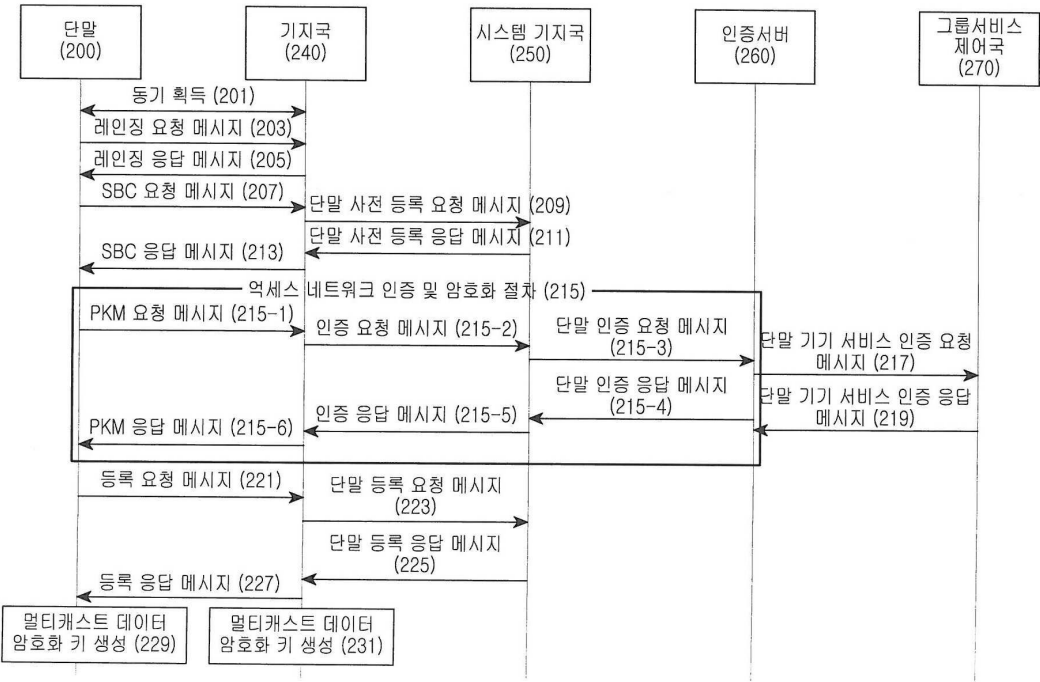
[0112] 111, 112: M2M 그룹, 110: 그룹 서비스 제어기, 109: 인증 서버.

도면

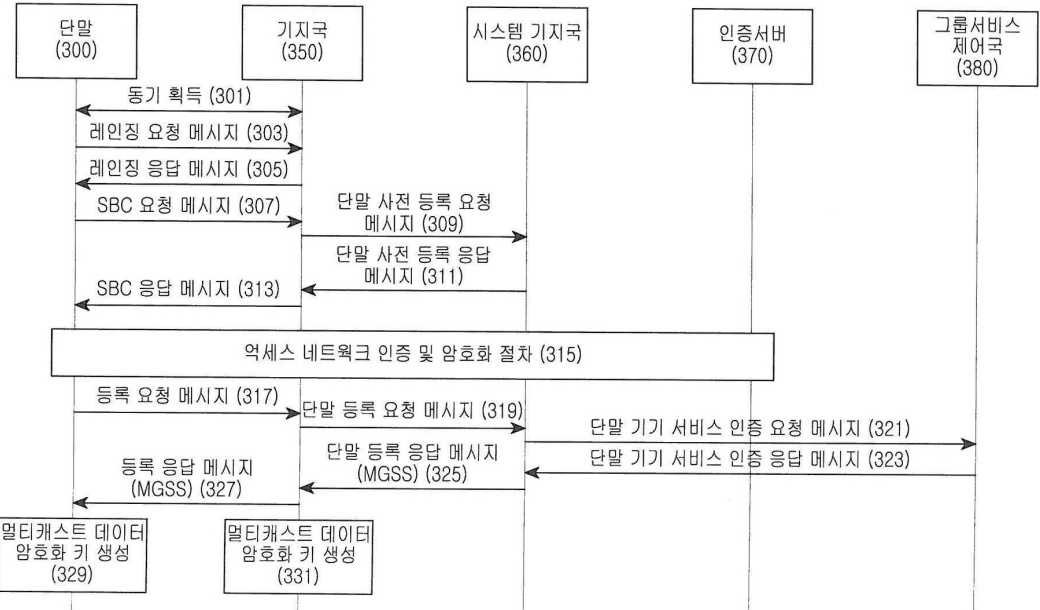
도면1



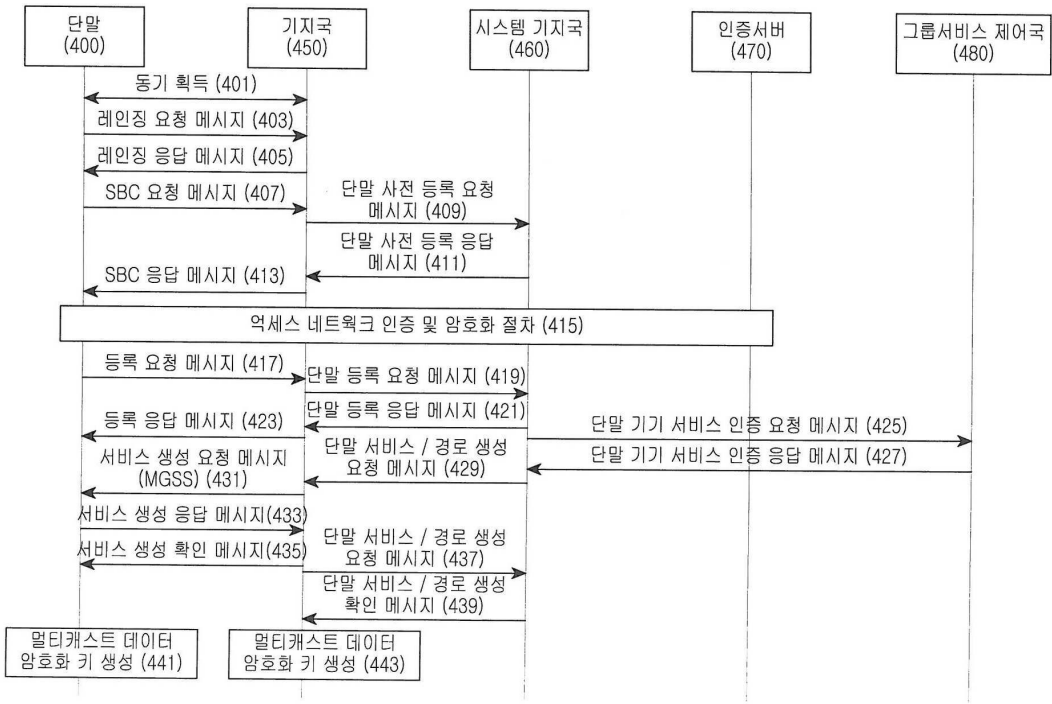
도면2



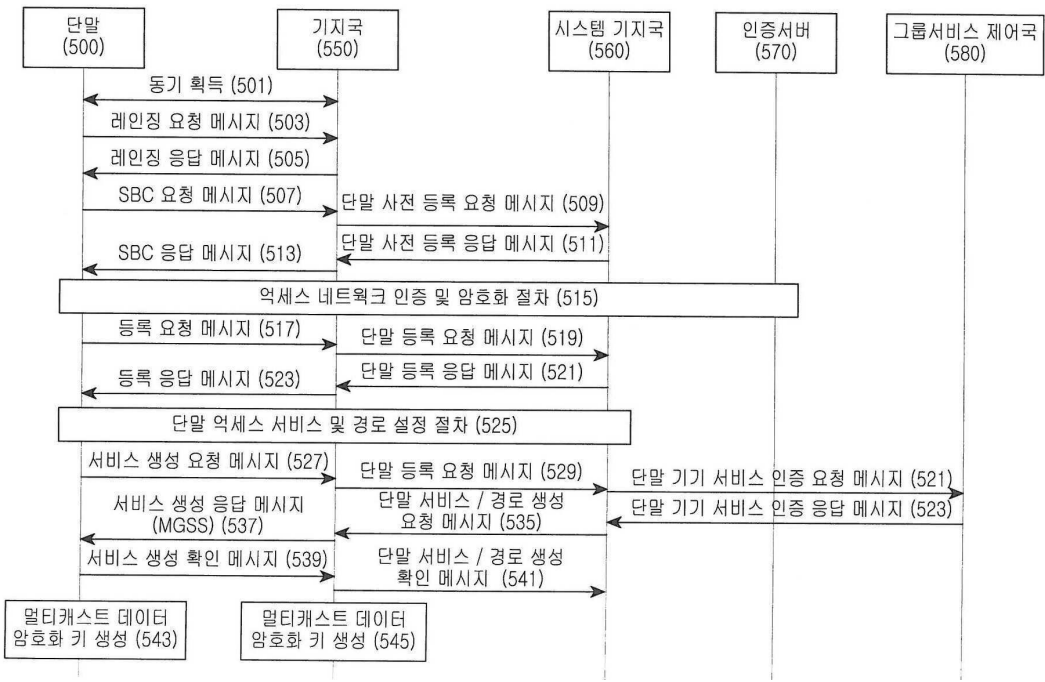
도면3



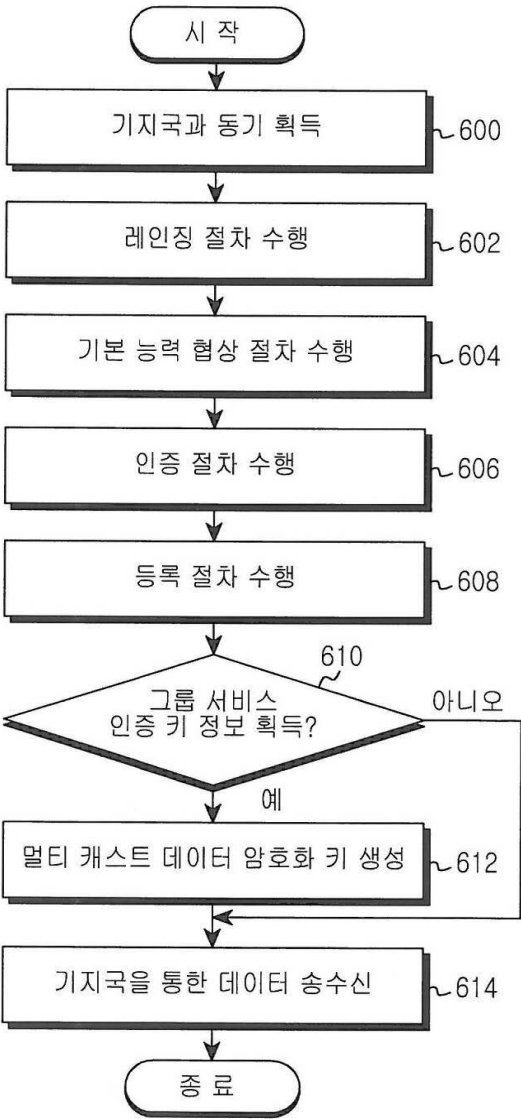
도면4



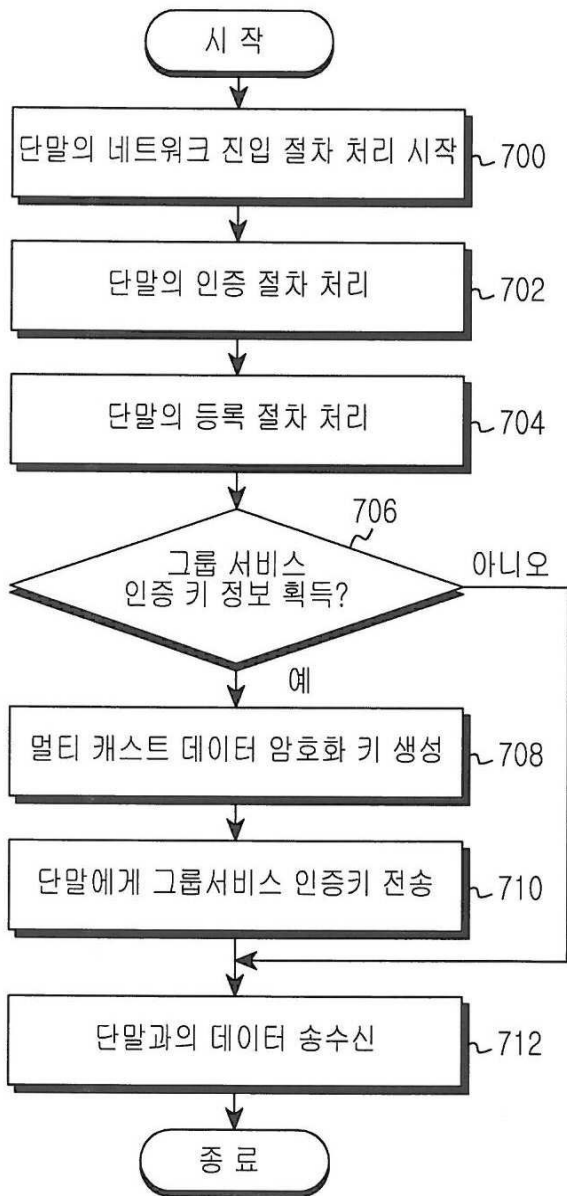
도면5



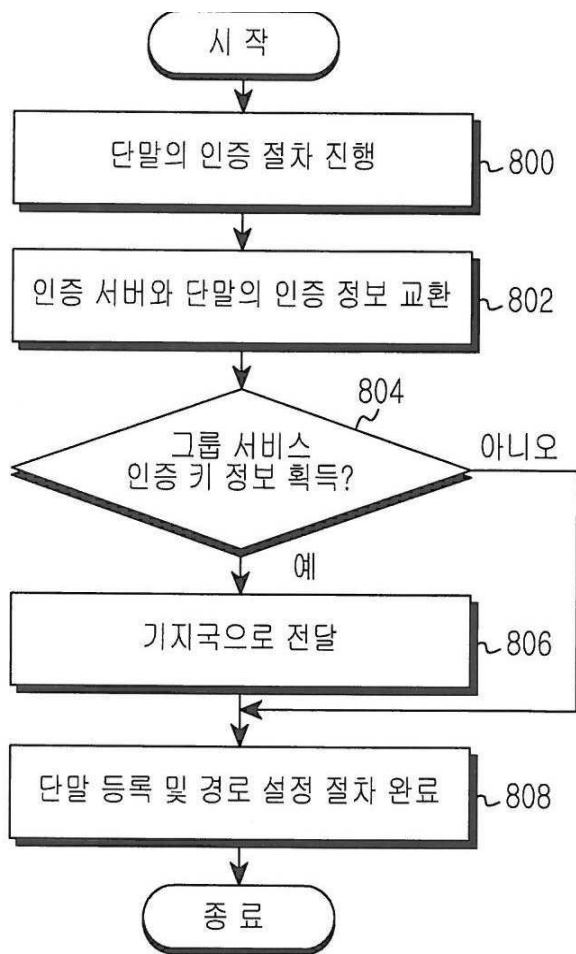
도면6



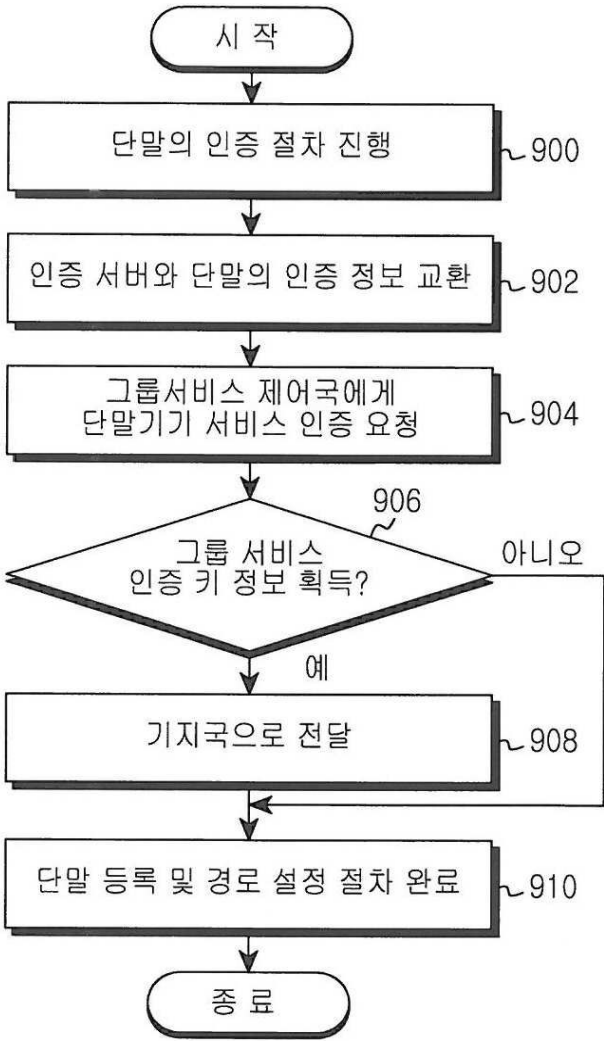
도면7



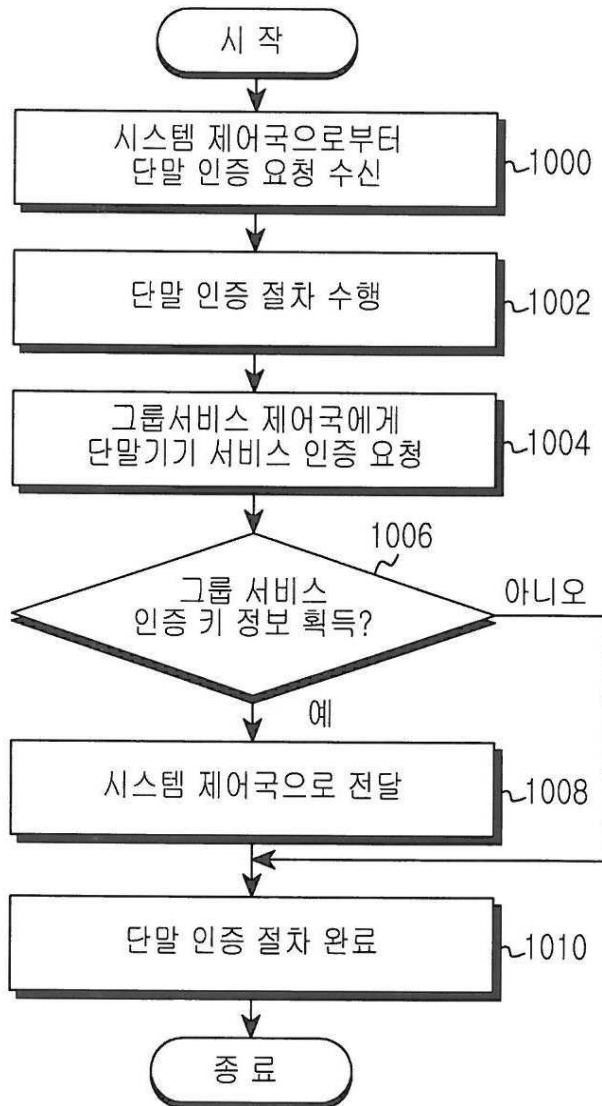
도면8



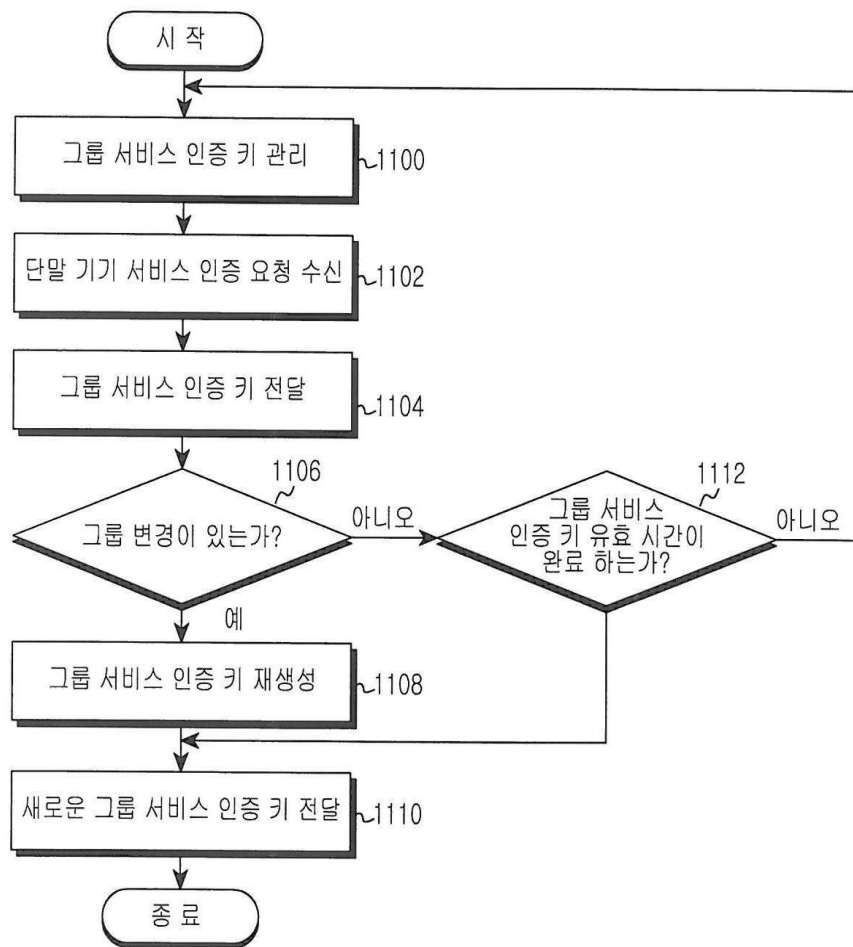
도면9



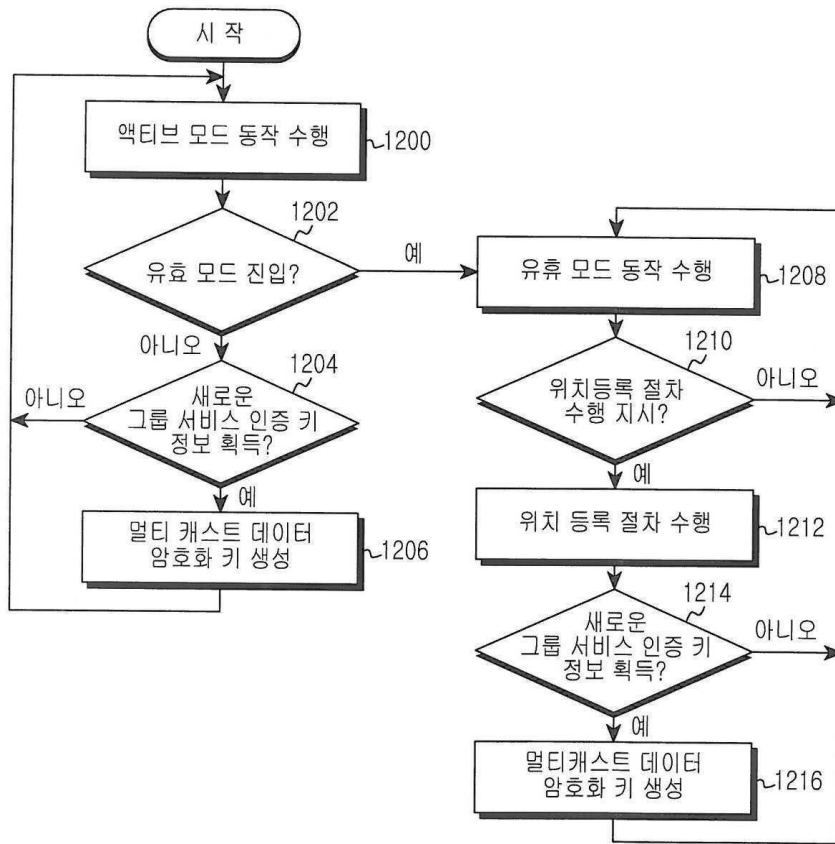
도면10



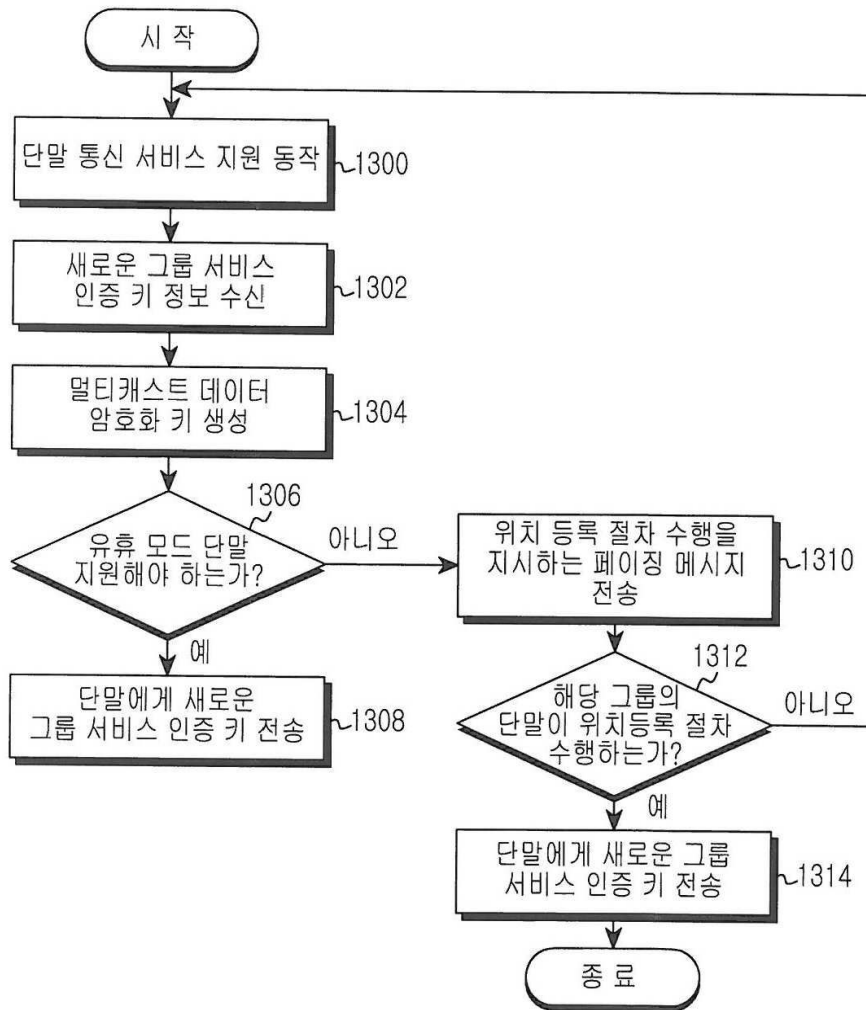
도면11



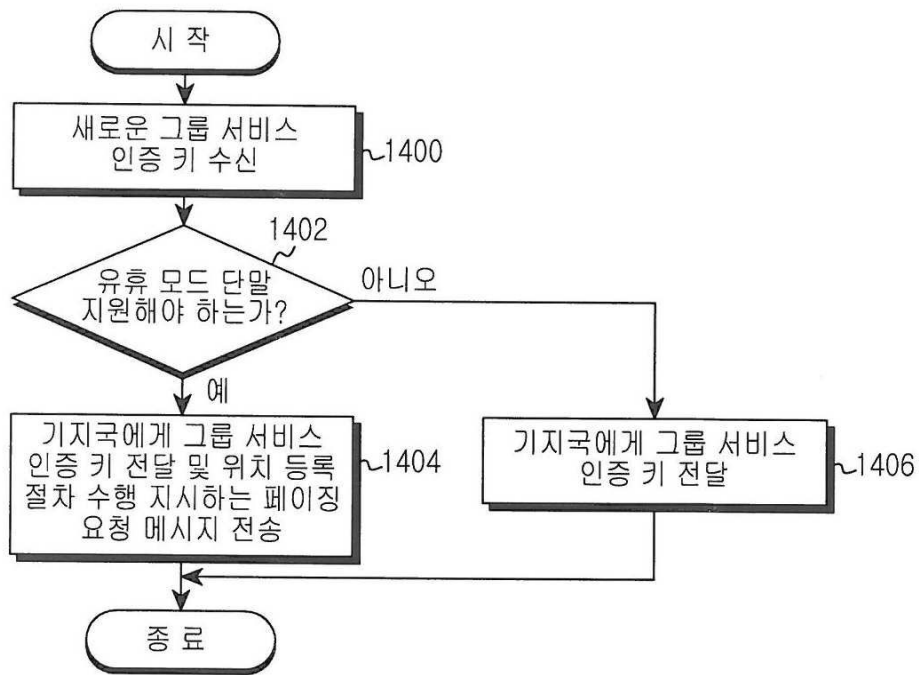
도면12



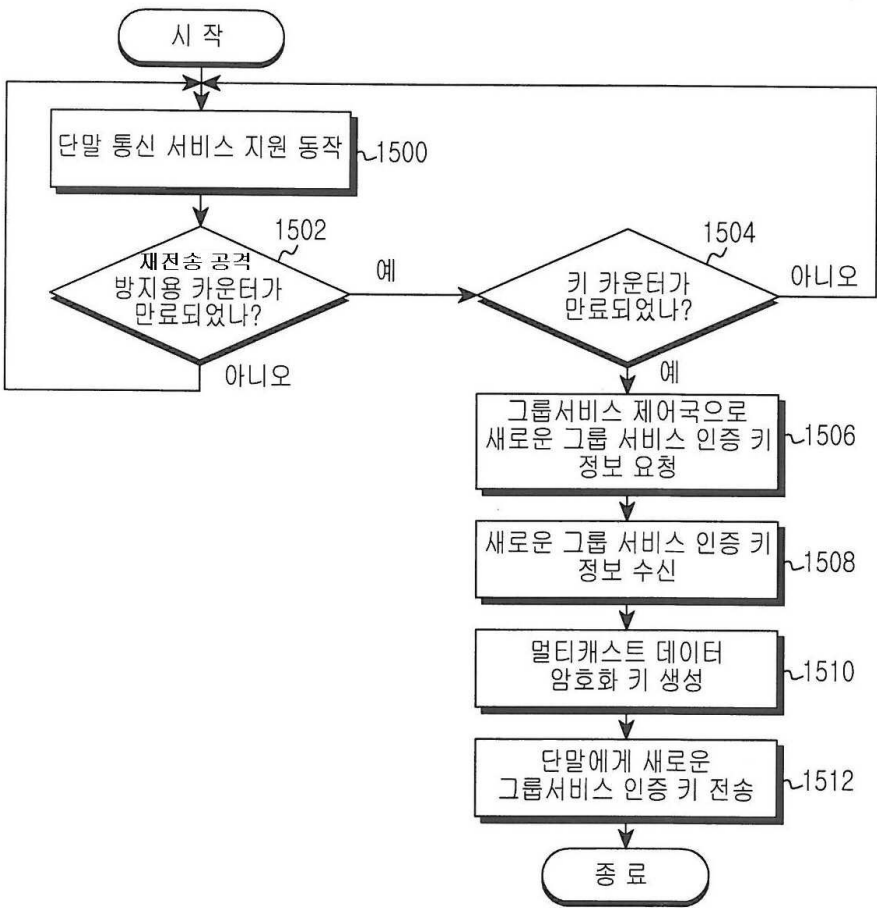
도면13



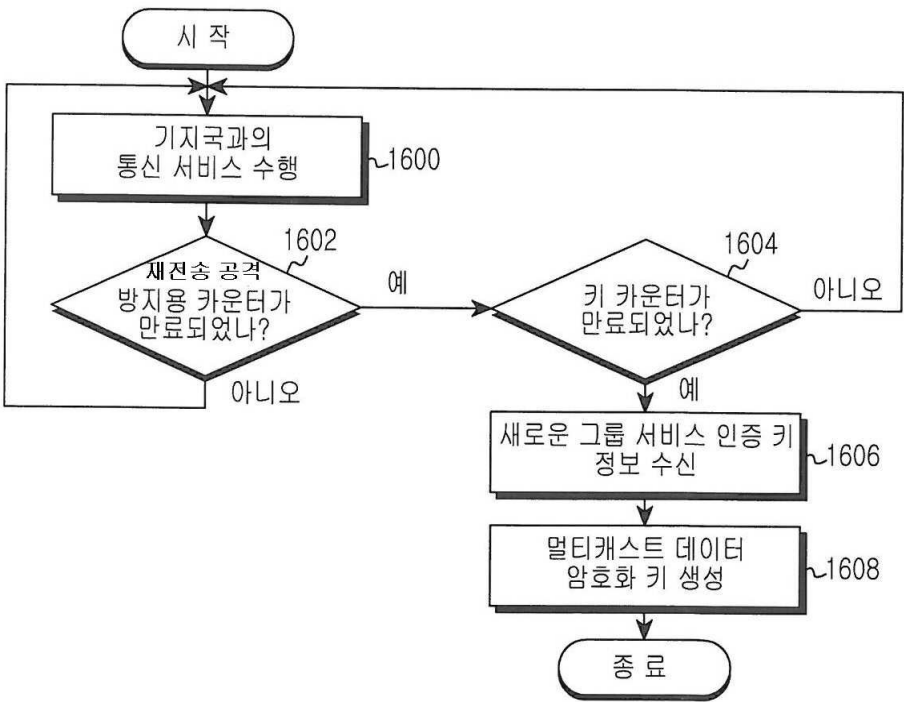
도면14



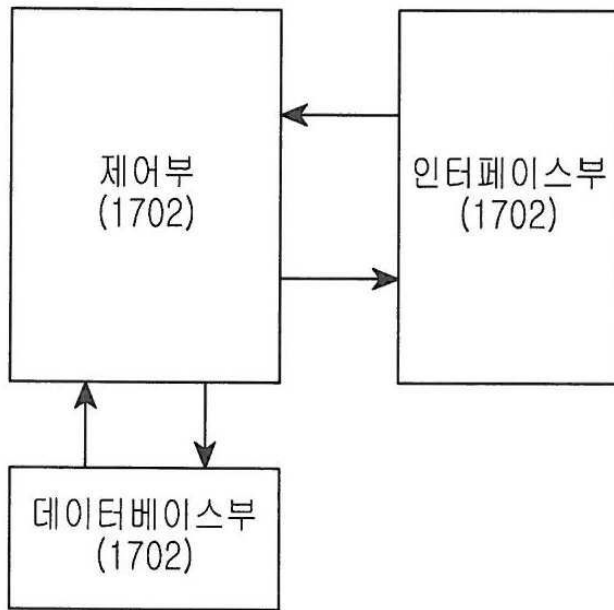
도면15



도면16



도면17



도면18

