(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0037907
(43) 공개일자 2016년04월06일

(51) 국제특허분류(Int. Cl.)
H04W 12/04 (2009.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01) *H04W 4/00* (2009.01)
H04W 8/20 (2009.01) *H04W 88/16* (2009.01)
(52) CPC특허분류
H04W 12/04 (2013.01)
H04L 63/062 (2013.01)
(21) 출원번호 10-2016-7002010
(22) 출원일자(국제) 2014년07월07일
심사청구일자 없음
(85) 번역문제출일자 2016년01월22일
(86) 국제출원번호 PCT/JP2014/003579
(87) 국제공개번호 WO 2015/015714
국제공개일자 2015년02월05일
(30) 우선권주장
JP-P-2013-158881 2013년07월31일 일본(JP)

(71) 출원인
닛본 덴끼 가부시끼가이샤
일본국 도꾜도 미나도꾸 시바 5쪼메 7방 1고
(72) 발명자
장 샤오웨이
일본국 도꾜도 미나도꾸 시바 5쪼메 7방 1고 닛본 덴끼 가부시끼가이샤 나이
프라사드 아난드 라가와
일본국 도꾜도 미나도꾸 시바 5쪼메 7방 1고 닛본 덴끼 가부시끼가이샤 나이
(74) 대리인
특허법인코리아나

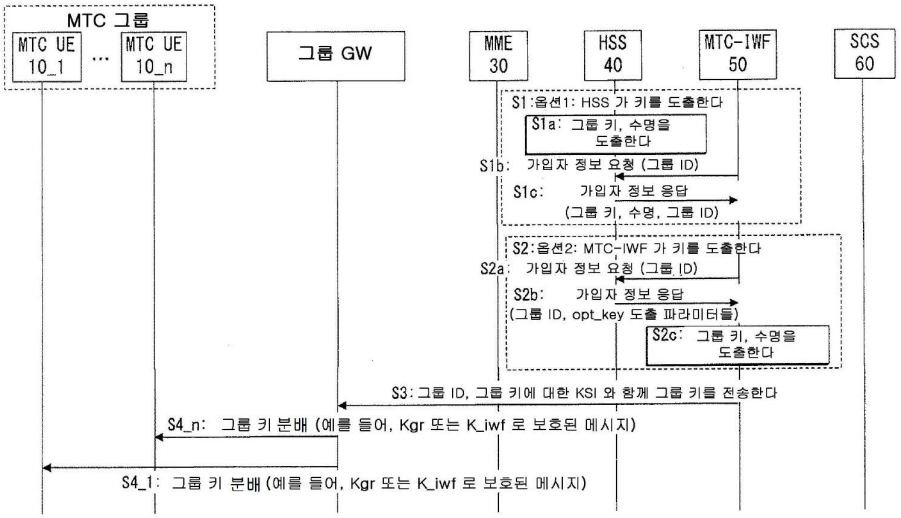
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 **MTC 그룹 키 관리를 위한 디바이스들 및 방법**

(57) 요 약

그룹 키를 분배할 시에 보안성을 향상시키기 위해, 코어 네트워크와 통신하는 MTC 디바이스들 (10_1-10_n) 의 그룹에 대한 코어 네트워크로의 게이트웨이 (20) 가 제공된다. 게이트웨이 (20) 는 그룹 키의 비밀성 및 무결성을 보호하고, MTC 디바이스들 (10_1-10_n) 의 각각의 디바이스에 보호된 그룹 키를 분배한다. 보호는 게이트웨이 (20) 와 MTC 디바이스들 (10_1-10_n) 의 각각의 디바이스 사이에서 사전에 공유되고, 게이트웨이 (20) 가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용되는 키 (Kgr); 또는 MTC-IWF (50) 와 MTC 디바이스들 (10_1-10_n) 의 각각의 디바이스 사이에서 공유되고, MTC-IWF (50) 와 MTC 디바이스들 (10_1-10_n) 의 각각의 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 키 (K_iwf) 를 이용함으로써 수행된다.

대 표 도



(52) CPC특허분류
H04L 63/065 (2013.01)
H04W 12/06 (2013.01)
H04W 4/005 (2013.01)
H04W 8/20 (2013.01)
H04W 88/16 (2013.01)
H04L 2463/062 (2013.01)

명 세 서

청구범위

청구항 1

통신 시스템으로서,

코어 네트워크와 통신하는 MTC (Machine-Type-Communication) 디바이스들의 그룹; 및

상기 그룹에 대한 상기 코어 네트워크로의 게이트웨이로서, 상기 게이트웨이는 그룹 통신을 안전하게 행하기 위해 제 1 키를 상기 MTC 디바이스들의 각각의 MTC 디바이스에 분배하는, 상기 게이트웨이를 포함하고,

상기 제 1 키를 분배할 시에, 상기 게이트웨이는,

상기 게이트웨이와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 사전에 공유되고, 상기 게이트웨이가 상기 MTC 디바이스들의 각각의 MTC 디바이스를 상기 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는

MTC-IWF (MTC Inter-Working Function) 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 공유되고, 상기 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키로서, 상기 MTC-IWF 는 상기 코어 네트워크를 통해 상기 그룹과 통신하는 SCS (Service Capability Server) 에 대한 상기 코어 네트워크로의 진입 지점의 역할을 하는, 상기 제 3 키를 이용함으로써 상기 제 1 키의 비밀성 및 무결성을 보호하는, 통신 시스템.

청구항 2

제 1 항에 있어서,

상기 MTC 디바이스들의 각각의 MTC 디바이스에 관한 가입 정보를 관리하고, 상기 게이트웨이로부터 상기 MTC 디바이스들의 각각의 MTC 디바이스로 분배될 상기 제 1 키를 도출하는 HSS (Home Subscriber Server) 를 더 포함하고,

상기 제 1 키를 도출하기 위한 파라미터로서, 상기 HSS 는,

상기 제 2 키;

상기 제 3 키;

Kasme (Key Access Security Management Entity); 또는

난수를 이용하는, 통신 시스템.

청구항 3

제 2 항에 있어서,

상기 HSS 는 상기 제 1 키를 상기 MTC-IWF 로 전송하는, 통신 시스템.

청구항 4

제 2 항 또는 제 3 항에 있어서,

상기 HSS 는,

상기 제 1 키의 수명이 만료되는 경우, 상기 그룹의 멤버가 상기 그룹으로부터 삭제되는 경우, 상기 파라미터가 변화되는 경우, 또는 상기 그룹 통신이 비활성 상태로 이전되는 경우, 상기 제 1 키를 업데이트하고;

상기 게이트웨이로 하여금 업데이트된 상기 제 1 키를 재분배하게 하도록 구성되는, 통신 시스템.

청구항 5

제 4 항에 있어서,

상기 HSS 는 상기 게이트웨이로 하여금 상기 업데이트된 제 1 키를 재분배하게 할 시에 삽입 가입자 데이터 메시지를 이용하는, 통신 시스템.

청구항 6

제 1 항에 있어서,

상기 MTC-IWF 는 상기 게이트웨이로부터 상기 MTC 디바이스들의 각각의 MTC 디바이스로 분배될 상기 제 1 키를 도출하고,

상기 제 1 키를 도출하기 위한 파라미터로서, 상기 MTC-IWF 는,

상기 제 2 키;

상기 제 3 키;

Kasme; 또는

난수를 이용하는, 통신 시스템.

청구항 7

제 6 항에 있어서,

상기 MTC 디바이스들의 각각의 MTC 디바이스에 대한 가입 정보를 관리하는 HSS 를 더 포함하고,

상기 MTC-IWF 는 상기 HSS 로부터 상기 파라미터를 획득하는, 통신 시스템.

청구항 8

제 6 항 또는 제 7 항에 있어서,

상기 MTC-IWF 는,

상기 제 1 키의 수명이 만료되는 경우, 상기 그룹의 멤버가 상기 그룹으로부터 삭제되는 경우, 상기 파라미터가 변화되는 경우, 또는 상기 그룹 통신이 비활성 상태로 이전되는 경우, 상기 제 1 키를 업데이트하고;

상기 게이트웨이로 하여금 업데이트된 상기 제 1 키를 재분배하게 하도록 구성되는, 통신 시스템.

청구항 9

제 1 항에 있어서,

상기 게이트웨이는, 파라미터로서,

상기 제 2 키;

상기 제 3 키;

Kasme; 또는

난수를 이용함으로써 상기 제 1 키를 도출하는, 통신 시스템.

청구항 10

제 9 항에 있어서,

상기 게이트웨이는,

상기 제 1 키의 수명이 만료되는 경우, 상기 그룹의 멤버가 상기 그룹으로부터 삭제되는 경우, 상기 파라미터가 변화되는 경우, 또는 상기 그룹 통신이 비활성 상태로 이전되는 경우, 상기 제 1 키를 업데이트하고;

상기 제 2 키 또는 상기 제 3 키를 이용함으로써 업데이트된 상기 제 1 키를 보호하며;

보호되고 업데이트된 상기 제 1 키를 재분배하도록 구성되는, 통신 시스템.

청구항 11

코어 네트워크와 통신하는 MTC 디바이스들의 그룹에 대한 상기 코어 네트워크로의 게이트웨이로서,

그룹 통신을 안전하게 행하기 위해 제 1 키의 비밀성 및 무결성을 보호하는 보호 수단; 및

상기 MTC 디바이스들의 각각의 MTC 디바이스에 보호된 상기 제 1 키를 분배하는 분배 수단을 포함하고,

상기 보호 수단은,

상기 게이트웨이와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 사전에 공유되고, 상기 게이트웨이가 상기 MTC 디바이스들의 각각의 MTC 디바이스를 상기 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는

MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 공유되고, 상기 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키로서, 상기 MTC-IWF 는 상기 코어 네트워크를 통해 상기 그룹과 통신하는 SCS 에 대한 상기 코어 네트워크로의 진입 지점의 역할을 하는, 상기 제 3 키를 이용함으로써 보호를 수행하도록 구성되는, 게이트웨이.

청구항 12

제 11 항에 있어서,

상기 MTC 디바이스들의 각각의 MTC 디바이스에 대한 가입 정보를 관리하는 HSS 로부터, 또는 상기 MTC-IWF 로부터 상기 제 1 키를 수신하는 수신 수단을 더 포함하는, 게이트웨이.

청구항 13

제 12 항에 있어서,

상기 제 1 키가 상기 HSS 또는 상기 MTC-IWF 에 의해 업데이트되는 경우, 상기 수신 수단은 업데이트된 상기 제 1 키를 수신하도록 구성되고,

상기 보호 수단은 상기 제 2 키 또는 상기 제 3 키를 이용함으로써 상기 업데이트된 제 1 키를 보호하도록 구성되며,

상기 분배 수단은 보호되고 업데이트된 상기 제 1 키를 재분배하도록 구성되는, 게이트웨이.

청구항 14

제 11 항에 있어서,

파라미터로서,

상기 제 2 키;

상기 제 3 키;

Kasme; 또는

난수를 이용함으로써 상기 제 1 키를 도출하는 도출 수단을 더 포함하는, 게이트웨이.

청구항 15

제 14 항에 있어서,

상기 도출 수단은, 상기 제 1 키의 수명이 만료되는 경우, 상기 그룹의 멤버가 상기 그룹으로부터 삭제되는 경우, 상기 파라미터가 변화되는 경우, 또는 상기 그룹 통신이 비활성 상태로 이전되는 경우, 상기 제 1 키를 업데이트하도록 구성되고,

상기 보호 수단은 상기 제 2 키 또는 상기 제 3 키를 이용함으로써 업데이트된 상기 제 1 키를 보호하도록 구성되며,

상기 분배 수단은 보호되고 업데이트된 상기 제 1 키를 재분배하도록 구성되는, 게이트웨이.

청구항 16

코어 네트워크와 통신하도록 그룹화된 MTC 디바이스로서,

상기 MTC 디바이스는,

MTC 디바이스들의 그룹에 대한 상기 코어 네트워크로의 게이트웨이로부터, 그룹 통신을 안전하게 행하기 위해 제 1 키를 수신하는 수신 수단으로서, 상기 제 1 키의 비밀성 및 무결성은 제 2 키 또는 제 3 키로 보호되는, 상기 수신 수단을 포함하고,

상기 제 2 키는 상기 게이트웨이와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 사전에 공유되고, 상기 게이트웨이가 상기 MTC 디바이스들의 각각의 MTC 디바이스를 상기 그룹의 멤버로서 인증하는데 이용되며,

상기 제 3 키는 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 공유되고, 상기 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되며, 상기 MTC-IWF 는 상기 코어 네트워크를 통해 상기 그룹과 통신하는 SCS 에 대한 상기 코어 네트워크로의 진입 지점의 역할을 하는, 코어 네트워크와 통신하도록 그룹화된 MTC 디바이스.

청구항 17

코어 네트워크와 통신하는 MTC 디바이스들의 그룹에 대한 상기 코어 네트워크로의 게이트웨이에서의 동작들을 제어하는 방법으로서,

그룹 통신을 안전하게 행하기 위해 제 1 키의 비밀성 및 무결성을 보호하는 단계; 및

상기 MTC 디바이스들의 각각의 MTC 디바이스에 보호된 상기 제 1 키를 분배하는 단계를 포함하고,

상기 보호는,

상기 게이트웨이와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 사전에 공유되고, 상기 게이트웨이가 상기 MTC 디바이스들의 각각의 MTC 디바이스를 상기 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는

MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 공유되고, 상기 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키로서, 상기 MTC-IWF 는 상기 코어 네트워크를 통해 상기 그룹과 통신하는 SCS 에 대한 상기 코어 네트워크로의 진입 지점의 역할을 하는, 상기 제 3 키를 이용함으로써 수행되는, 게이트웨이에서의 동작들을 제어하는 방법.

청구항 18

코어 네트워크와 통신하도록 그룹화된 MTC 디바이스에서의 동작들을 제어하는 방법으로서,

MTC 디바이스들의 그룹에 대한 상기 코어 네트워크로의 게이트웨이로부터, 그룹 통신을 안전하게 행하기 위해 제 1 키를 수신하는 단계로서, 상기 제 1 키의 비밀성 및 무결성은 제 2 키 또는 제 3 키로 보호되는, 상기 제 1 키를 수신하는 단계를 포함하고,

상기 제 2 키는 상기 게이트웨이와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 사전에 공유되고, 상기 게이트웨이가 상기 MTC 디바이스들의 각각의 MTC 디바이스를 상기 그룹의 멤버로서 인증하는데 이용되며,

상기 제 3 키는 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 공유되고, 상기 MTC-IWF 와 상기 MTC 디바이스들의 각각의 MTC 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되며, 상기 MTC-IWF 는 상기 코어 네트워크를 통해 상기 그룹과 통신하는 SCS 에 대한 상기 코어 네트워크로의 진입 지점의 역할을 하는, MTC 디바이스에서의 동작들을 제어하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 MTC (Machine-Type-Communication) 에 기초한 그룹에 대한 보안 솔루션에 관한 것이다. 특히, 본 발명은 코어 네트워크 내에서 MTC 디바이스들에게 그룹 키를 분배하며, 그룹 키를 도출하고/하거나, 그룹 키를 관리하는 기법들에 관한 것이다.

배 경 기 술

[0002] MTC 의 3GPP (3rd Generation Partnership Project) 아키텍처가 비특허문헌 1 에서 연구되었다. MTC 에 기

초한 그룹의 연구가 또한 비특허문헌 2 에서 착수되었다.

[0003] 또한, 특허문헌 1 은 MTC 디바이스들의 그룹에 대한 코어 네트워크로의 게이트웨이의 역할을 하고, 그룹 멤버들과 통신을 안전하게 행하기 위해 그룹 키를 이용하는 GW (Gateway) 를 개시한다.

[0004] MTC 디바이스는 MTC 를 위한 장비를 갖춘 UE (User Equipment) 이며, MTC 는 다음의 설명에서 종종 "MTC UE" 또는 "UE" 로 지칭될 것이다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 특허문헌 1: 국제 특허 공개 제 WO 2012/018130 호

비특허문헌

[0006] (비특허문헌 0001) 비특허문헌 1: 3GPP TS 23.682, "Architecture enhancements to facilitate communications with packet data networks and applications (Release 11)", V11.2.0, 2012-09

(비특허문헌 0002) 비특허문헌 2: 3GPP TR 23.887, "Machine-Type and other Mobile Data Applications Communications Enhancements (Release 12)", V0.5.0, 2012-11, 조항 8, pp.78-94

(비특허문헌 0003) 비특허문헌 3: 3GPP TR 33.868, "Security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements; (Release 12)", V0.13.0, 2013-04, 조항 A.6.4.2, pp.87-88

발명의 내용

해결하려는 과제

[0007] 그러나, 본 출원의 발명자들은 그룹 키가 임의의 보호 없이 그룹 멤버들에게 분배되는 특허문헌 1 에 문제가 있음을 발견하였다.

[0008] 비특허문헌 3 은 MME (Mobility Management Entity) 가 NAS (Non Access Stratum) 보안 컨텍스트를 이용함으로써 그룹 키를 보호하는 것을 개시한다. 그러나, NAS 보안 컨텍스트는 단지 그룹 키의 비밀성만을 보장한다는 문제가 비특허문헌 3 에 있다.

[0009] 이에 따라, 본 개시물의 일 모범적인 목적은 그룹 키를 분배할 시에 보안성을 향상시키는 것이다.

과제의 해결 수단

[0010] 위에서 언급된 목적을 달성하기 위해, 본 발명의 제 1 예시적인 양상에 따른 통신 시스템은 코어 네트워크와 통신하는 MTC 디바이스들의 그룹, 및 그룹에 대한 코어 네트워크로의 게이트웨이를 포함한다. 게이트웨이는, MTC 디바이스들의 각각의 디바이스에, 그룹 통신을 안전하게 행하기 위해 제 1 키를 분배한다. 제 1 키를 분배할 시에, 게이트웨이는, 게이트웨이와 MTC 디바이스들의 각각의 디바이스의 사이에서 사전에 공유되고, 게이트웨이가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는 MTC-IWF (MTC Inter-Working Function) 와 MTC 디바이스들의 각각의 디바이스의 사이에서 사전에 공유되고, MTC-IWF 와 MTC 디바이스들의 각각의 디바이스의 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키를 이용함으로써 제 1 키의 비밀성 및 무결성을 보호한다. MTC-IWF 는 코어 네트워크를 통해 그룹과 통신하는 SCS (Service Capability Server) 에 대한 코어 네트워크의 진입 지점의 역할을 한다.

[0011] 또한, 본 발명의 제 2 예시적인 양상에 따른 게이트웨이는 코어 네트워크와 통신하는 MTC 디바이스들의 그룹에 대한 코어 네트워크로의 게이트웨이로서의 역할을 한다. 게이트웨이는 그룹 통신을 안전하게 행하기 위해 제 1 키의 비밀성 및 무결성을 보호하는 보호 수단; 및 MTC 디바이스들의 각각의 디바이스에 보호된 제 1 키를 분배하는 분배 수단을 포함한다. 보호 수단은 게이트웨이와 MTC 디바이스들의 각각의 디바이스 사이에서 사전에 공유되고, 게이트웨이가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는 MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 공유되고, MTC-IWF 와 MTC 디바이스들의 각각

의 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키를 이용함으로써 보호를 수행하도록 구성된다. MTC-IWF 는 코어 네트워크를 통해 그룹과 통신하는 SCS 에 대한 코어 네트워크로의 진입 지점의 역할을 한다.

[0012] 또한, 본 발명의 제 3 예시적인 양상에 따른 MTC 디바이스는 코어 네트워크와 통신하도록 그룹화된다. MTC 디바이스는: MTC 디바이스들의 그룹에 대한 코어 네트워크로의 게이트웨이로부터, 그룹 통신을 안전하게 행하기 위해 제 1 키를 수신하는 수신 수단을 포함한다. 제 1 키의 비밀성 및 무결성은 제 2 키 또는 제 3 키로 보호된다. 제 2 키는 게이트웨이와 MTC 디바이스들의 각각의 디바이스 사이에서 사전에 공유되고, 게이트웨이가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용된다. 제 3 키는 MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 공유되고, MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용된다. MTC-IWF 는 코어 네트워크를 통해 그룹과 통신하는 SCS 에 대한 코어 네트워크로의 진입 지점의 역할을 한다.

[0013] 또한, 본 발명의 제 4 예시적인 양상에 따른 방법은 코어 네트워크와 통신하는 MTC 디바이스들의 그룹에 대한 코어 네트워크로의 게이트웨이에서의 동작들을 제어하는 방법을 제공한다. 이러한 방법은: 게이트웨이는 그룹 통신을 안전하게 행하기 위해 제 1 키의 비밀성 및 무결성을 보호하는 단계; 및 MTC 디바이스들의 각각의 디바이스에 보호된 제 1 키를 분배하는 단계를 포함한다. 보호는 게이트웨이와 MTC 디바이스들의 각각의 디바이스 사이에서 사전에 공유되고, 게이트웨이가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용되는 제 2 키; 또는 MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 공유되고, MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용되는 제 3 키를 이용함으로써 수행된다. MTC-IWF 는 코어 네트워크를 통해 그룹과 통신하는 SCS 에 대한 코어 네트워크로의 진입 지점의 역할을 한다.

[0014] 또한, 본 발명의 제 5 예시적인 양상에 따른 방법은 코어 네트워크와 통신하도록 그룹화된 MTC 디바이스에서의 동작들을 제어하는 방법을 제공한다. 이러한 방법은: MTC 디바이스들의 그룹에 대한 코어 네트워크로의 게이트웨이로부터, 그룹 통신을 안전하게 행하기 위해 제 1 키를 수신하는 단계를 포함한다. 제 1 키의 비밀성 및 무결성은 제 2 키 또는 제 3 키로 보호된다. 제 2 키는 게이트웨이와 MTC 디바이스들의 각각의 디바이스 사이에서 사전에 공유되고, 게이트웨이가 MTC 디바이스들의 각각의 디바이스를 그룹의 멤버로서 인증하는데 이용된다. 제 3 키는 MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 공유되고, MTC-IWF 와 MTC 디바이스들의 각각의 디바이스 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용된다. MTC-IWF 는 코어 네트워크를 통해 그룹과 통신하는 SCS 에 대한 코어 네트워크로의 진입 지점의 역할을 한다.

발명의 효과

[0015] 본 발명에 따르면, 위에서 언급된 문제들을 해결하고, 따라서 그룹 키를 분배할 시에 보안성을 향상시키는 것이 가능하다.

도면의 간단한 설명

[0016] 도 1 은 본 발명의 일 예시적인 실시형태에 따른 통신 시스템의 구성 예를 도시하는 블록도이다.

도 2 는 예시적인 실시형태에 따른 통신 시스템의 제 1 동작 예를 도시하는 시퀀스 도면이다.

도 3 은 예시적인 실시형태에 따른 통신 시스템의 제 2 동작 예를 도시하는 시퀀스 도면이다.

도 4 는 예시적인 실시형태에 따른 통신 시스템의 제 3 동작 예를 도시하는 시퀀스 도면이다.

도 5 는 예시적인 실시형태에 따른 통신 시스템의 제 4 동작 예를 도시하는 시퀀스 도면이다.

도 6 은 예시적인 실시형태에 따른 통신 시스템의 제 5 동작 예를 도시하는 시퀀스 도면이다.

도 7 은 예시적인 실시형태에 따른 통신 시스템의 제 6 동작 예를 도시하는 시퀀스 도면이다.

도 8 은 예시적인 실시형태에 따른 MTC UE 의 구성 예를 도시하는 블록도이다.

도 9 는 예시적인 실시형태에 따른 그룹 GW 의 구성 예를 도시하는 블록도이다.

도 10 은 예시적인 실시형태에 따른 HSS 의 구성 예를 도시하는 블록도이다.

도 11 은 예시적인 실시형태에 따른 MTC-IWF 의 구성 예를 도시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하에서, 본 발명의 예시적인 실시형태가 첨부 도면들을 참조하여 설명될 것이다.

[0018] 이러한 실시형태에서, 코어 네트워크에서의 그룹 키들 도출, 적절한 네트워크 노드들 및 UE 들에 대한 키 분배, 키 관리, 및 그룹 키들이 통신을 안전하게 하기 위해 어떻게 이용되는지에 대한 세부사항들이 제안될 것이다. 키 도출 파라미터들은 HSS (Home Subscriber Server) 로부터 MTC-IWF 로, 또는 MTC-IWF 로부터 HSS 로 전송될 수 있다. 도출 알고리즘들은 네트워크 노드에서 이용가능하다.

[0019] 도 1 에 도시된 바와 같이, 이러한 실시형태에 따른 통신 시스템은 코어 네트워크 (3GPP 네트워크), MTC 를 위한 장비를 갖추고 있고 RAN (Radio Access Network) 을 통해 코어 네트워크에 접속하는 UE 들인 하나 이상의 MTC UE 들 (10) 을 포함한다. 이러한 예시적인 실시형태에서, MTC UE 들 (10) 은 코어 네트워크와 통신하기 위해 그룹화된다. 도시가 생략되었으나, RAN 은 복수의 기지국들 (즉, eNB (evolved Node B) 들) 에 의해 형성된다.

[0020] MTC UE 들 (10) 은 코어 네트워크에 연결된다. MTC UE 들 (10) 은 하나 또는 다수의 MTC 애플리케이션들을 호스팅할 수 있다. 외부 네트워크에서의 대응하는 MTC 애플리케이션들은 SCS (60) 상에서 호스팅된다. SCS (60) 는 MTC UE 들 (10) 과 통신하기 위해 코어 네트워크에 접속한다.

[0021] 또한, 코어 네트워크는 코어 네트워크의 네트워크 노드들의 일부분으로서 MME (30), HSS (40), 및 MTC-IWF (50) 를 포함한다. MME (30) 는 RAN 과 MTC-IWF (50) 사이의 트래픽을 중계한다. HSS (40) 는 MTC UE 들 (10) 등에 대한 가입 정보를 관리한다. MTC-IWF (50) 는 SCS (60) 에 대한 코어 네트워크로의 진입 지점의 역할을 하고, 필요한 경우, HSS (40) 로부터 가입 정보 등을 획득한다. 코어 네트워크는 또한, 다른 네트워크 노드들로서, SGSN (Serving GPRS (General Packet Radio Service) Support Node), MSC (Mobile Switching Centre) 등을 포함한다. SGSN 및 MSC 는 MME (30) 와 함께 기능한다.

[0022] 도 1 에서는 도시가 생략되었으나, 코어 네트워크는 MTC UE 들 (10) 의 그룹에 대한 코어 네트워크로의 게이트웨이를 포함한다. 이후부터, 이러한 게이트웨이는 "그룹 GW" 라고 지칭되고 심볼 20 으로 표기된다. 통상적으로, 그룹 GW (20) 는 그룹 GW (20) 와 MTC UE 들 (10) 의 그룹 사이에서 그룹 통신을 안전하게 행하기 위한 그룹 키를 MTC UE 들 (10) 의 각각의 MTC UE 에 분배한다. 그룹 GW (20) 는 네트워크 노드에 배치되거나 독립적인 노드일 수 있다.

[0023] 다음으로, 이러한 예시적인 실시형태의 동작 예들이 도 2 내지 도 7 을 참조하여 상세히 설명될 것이다. MTC UE (10), 그룹 GW (20), HSS (40), 및 MTC-IWF (50) 의 구성 예들이 도 8 내지 도 11 을 참조하여 추후에 설명될 것임에 유의한다.

[0024] 1. 키 분배

[0025] 그룹 통신은 그룹 GW (20) 및 MTC UE 들 (10) 의 그룹 멤버가 동일한 그룹 키를 공유할 것을 요구한다.

[0026] 그룹 GW (20) 가 그룹 키들을 얻을 수 있는 2 가지 옵션들이 있다. 옵션들 중 하나의 옵션은 그룹 GW (20) 그 자체가 그룹 키를 도출하는 경우이다. 그룹 키를 어떻게 도출하는지는 추후에 설명될 것이다. 옵션들 중 다른 옵션은 그룹 GW (20) 가 다른 네트워크 노드로부터 그룹 키를 수신하는 경우이다. 이러한 예시적인 실시형태는 그룹 GW (20) 가 MTC-IWF (50) 에서 구성되는지 여부를 더 고려한다.

[0027] (1) MTC-IWF (50) 가 그룹 GW (20) 는 아니지만 그룹 키를 공유하는 경우

[0028] 이러한 경우에, 도 2 에 도시된 바와 같이, HSS (40) 는 그룹 키를 도출하여 그것을 가입자 정보 응답 메시지에 그룹 ID 와 함께 MTC-IWF (50) 에 전송한다 (단계 S1a 내지 단계 S1c).

[0029] 그렇지 않으면, MTC-IWF (50) 가 가입자 정보 응답 메시지에서 HSS (40) 로부터 그룹 ID 및 선택적으로 키 도출 파라미터를 수신한 경우, MTC-IWF (50) 가 그룹 키를 도출한다 (단계 S2a 내지 단계 S2c).

[0030] 도출된 그룹 키는 그룹 키의 그룹 ID 및 KSI (Key Set Identifier) 와 함께, MME (30) 를 통해 그룹 GW (20) 로 전송된다.

[0031] 그 다음에, 그룹 GW (20) 는 MTC 그룹의 멤버들인 MTC UE 들 (10_1 내지 10_n (n?2)) 에 그룹 키를 분배한다

(단계 S4_1 내지 단계 S4_n).

[0032] MTC UE 들 (10_1 내지 10_n) 에 분배할 시에 그룹 키를 보호하는 2 가지 방식들이 있다.

[0033] 방식들 중 한 가지 방식은 이용된 그룹 키 Kgr 의 사전-구성된 인증을 이용하는 것이다. 키 Kgr 은 그룹 GW (20) 와 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 사이에서 사전에 공유되고, 그룹 GW (20) 가 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 를 MTC 그룹의 멤버로서 인증하는데 이용된다.

[0034] 인증 시에, MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 는 그룹 GW (20) 로부터 인증 요청 메시지를 수신하고, 그 다음에 키 Kgr 로 예를 들어, RES (인증 응답) 을 컴퓨팅한다. MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 는 컴퓨팅된 RES 를 포함하고 있는 인증 응답 메시지를 그룹 GW (20) 에 전송한다. 그룹 GW (20) 는 키 Kgr 로 수신된 RES 를 검사함으로써, MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 를 인증한다.

[0035] 분배 시에, 그룹 GW (20) 는 그룹 키의 비밀성을 보호하기 위해 키 Kgr 로 그룹 키를 암호화하고, 또한 키 Kgr 로 그룹 키의 무결성을 보장한다. MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 는 키 Kgr 로 수신된 그룹 키를 해독하고, 또한 키 Kgr 로 수신된 그룹 키의 무결성을 검사한다.

[0036] 방식들 중 다른 하나의 방식은 루트 키 K_iwf 를 이용하는 것이다. 루트 키 K_iwf 는 MTC-IWF (50) 와 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 사이에서 공유되고, MTC-IWF (50) 와 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 사이에서 개개의 통신을 안전하게 행하기 위해 임시 키들을 도출하는데 이용된다.

[0037] 임시 키들 중 하나의 임시 키는 MTC-IWF 와 MTC UE 사이에서 이송되는 메시지들을 암호화하고 해독하기 위한 비밀성 키이다. 임시 키들 중 다른 하나의 키는 MTC-IWF 와 MTC UE 사이에서 이송되는 메시지의 무결성을 검사하기 위한 무결성 키이다.

[0038] 분배 시에, 그룹 GW (20) 는 그룹 키의 비밀성을 보호하기 위해 키 K_iwf 로 그룹 키를 암호화하고, 또한 키 K_iwf 로 그룹 키의 무결성을 보장한다. MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 는 키 K_iwf 로 수신된 그룹 키를 해독하고, 또한 키 K_iwf 로 수신된 그룹 키의 무결성을 검사한다.

[0039] 이러한 실시형태에 따르면, 그룹 키의 비밀성 및 무결성 양자 모두가 그룹 멤버에게로의 분배 시에 보장되어, 위에서 언급된 특허문헌 1 및 비특허문헌 3 과 비교하여 보안성을 크게 향상시키는 것이 가능하다.

[0040] (2) MTC-IWF (50) 가 그룹 GW (20) 인 경우

[0041] 이러한 경우에, 도 3 에 도시된 바와 같이, HSS (40) 또는 (역시 그룹 GW 의 역할을 하는) MTC-IWF (50A) 는 도 2 와 유사한 방식으로 그룹 키를 도출한다 (단계 S11a 내지 단계 S12c).

[0042] 그 다음에, MTC-IWF (50A) 는 도 2 와 유사한 방식으로 MTC UE 들 (10_1 내지 10_n) 에 그룹 키를 분배한다 (단계 S14_1 내지 단계 S14_n).

[0043] (3) MTC-IWF (50) 가 그룹 GW (20) 가 아니고 그룹 키를 공유할 필요가 없는 경우

[0044] 이러한 경우에, 도 4 에 도시된 바와 같이, HSS (40) 는 그룹 키를 도출하여, 예를 들어, 인증 데이터 응답 메시지로 UE 인증 절차 중에 MME (30) 에 그룹 키를 전송한다 (단계 S21 및 단계 S22). 인증 데이터 응답 메시지에 그룹 키를 포함시키는 경우, 통신 프로토콜들에 대한 영향을 감소시키는 것이 가능하다. 이는 인증 데이터 응답 메시지가 통상적인 MME 와 HSS 사이에서 전송되는 기존의 메시지이기 때문이다.

[0045] MME (30) 는 새로운 메시지로 그룹 GW (20) 에 그룹 키를 전송하거나, 포워딩된 트리거에 그룹 키를 포함시킬 수 있다 (단계 S23).

[0046] 그룹 키는 오직 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 가 그룹 멤버로서 개별적으로 코어 네트워크에 대해 인증된 경우에만 활성화될 수 있다. 그 후에, MME (30) 는 또한 MTC UE 들 (10_1 내지 10_n) 의 각각의 MTC UE 가 그룹 멤버로서 개별적으로 인증되었음이 확인된 후에 그룹 GW (20) 에 그룹 키를 전송할 수 있다.

[0047] 그 다음에, 그룹 GW (20) 는 도 2 와 유사한 방식으로 MTC UE 들 (10_1 내지 10_n) 에 그룹 키를 분배한다 (단계 S24_1 내지 단계 S24_n).

[0048] 2. 키 도출

[0049] 그룹 키를 도출하기 위해, 3GPP TS 33.401 에 정의된 KDF (Key Derivation Function) 가 재-이용될 수 있다.

[0050] 입력 파라미터의 4 개의 옵션들이 있다:

[0051] (1) (MTC UE 및 그룹 GW 에서) 사전-구성된 키 Kgr;

[0052] (2) MTC-IWF 와 MTC UE 사이에서 공유되는 키 K_iwf;

[0053] (3) 3GPP TS 33.401 에서 정의된 Kasme; 및

[0054] (4) 난수.

[0055] 다른 파라미터들은: 내부 그룹 ID, 그룹 게이트웨이 ID, 키 도출 알고리즘 식별자, 카운터일 수 있다.

[0056] 새로운 그룹 키들이 도출되는 경우에 수명 값이 또한 생성될 수 있다.

[0057] 키 도출 파라미터들은 HSS (40) 로부터 MTC-IWF (50) (또는 50A) 로, 또는 MTC-IWF (50) (또는 50A) 로부터 HSS (40) 로 전송될 수 있다. 그룹 키를 도출하는 도출 알고리즘들은 네트워크 노드에서 구성된다.

[0058] 3. 키 관리

[0059] 그룹 키는:

[0060] 그룹 키의 수명이 만료되는 경우;

[0061] 그룹 번호가 그룹으로부터 삭제되는 경우;

[0062] 도출 파라미터 (예를 들어, 루트 키 K_iwf) 가 업데이트된 경우; 또는

[0063] 비활성 상태로 이전되기 전에 새로운 그룹 키들을 도출하여 저장하는 경우 업데이트될 수 있다.

[0064] 키 업데이트 절차의 예들이 도 5 내지 도 7 에 도시된다.

[0065] (1) MTC-IWF (50) 가 그룹 GW (20) 는 아니지만 그룹 키를 공유하는 경우

[0066] 이러한 경우에, 도 5 에 도시된 바와 같이, HSS (40) 는 그룹 키를 업데이트하여 그것을 가입자 정보 응답 메시지로 그룹 ID 와 함께 MTC-IWF (50) 에 전송한다 (단계 S31a 내지 단계 S31b).

[0067] 그렇지 않으면, MTC-IWF (50) 는 그룹 키를 업데이트하고, HSS (40) 로부터 키 도출 파라미터들을 선택적으로 취출한다 (단계 S32a 및 단계 S32b).

[0068] 업데이트된 그룹 키는 그룹 ID 및 업데이트된 그룹 키의 KSI 와 함께, MME (30) 를 통해 그룹 GW (20) 에 전송된다 (단계 S33).

[0069] 그 다음에, 그룹 GW (20) 는 MTC UE 들 (10_1 내지 10_n) 에게 업데이트된 그룹 키를 재분배한다 (단계 S34_1 내지 단계 S34_n). 이 시점에서, 업데이트된 그룹 키는 키 Kgr 또는 K_iwf 를 이용함으로써 보호된다.

[0070] (2) MTC-IWF (50) 가 그룹 GW (20) 인 경우

[0071] 이러한 경우에, 도 6 에 도시된 바와 같이, HSS (40) 또는 MTC-IWF (50A) 는 도 5 와 유사한 방식으로 그룹 키를 업데이트한다 (단계 S41a 내지 단계 S42b).

[0072] 그 다음에, MTC-IWF (50A) 는 도 5 와 유사한 방식으로 MTC UE 들 (10_1 내지 10_n) 에 업데이트된 그룹 키를 재분배한다 (단계 S44_1 내지 단계 S44_n).

[0073] (3) MTC-IWF (50) 가 그룹 GW (20) 가 아니고 그룹 키를 공유할 필요가 없는 경우

[0074] 이러한 경우에, 도 7 에 도시된 바와 같이, HSS (40) 가 그룹 키를 업데이트하고, 예를 들어, 삽입 가입자 데이터 메시지로 MME (30) 에게 그룹 키를 전송한다 (단계 S51 및 단계 S52). 삽입 가입자 데이터 메시지에 업데이트된 그룹 키를 포함시키는 경우에, 통신 프로토콜들에 대한 영향을 감소시키는 것이 가능하다. 이는 삽입 가입자 데이터가 통상적인 MME 와 HSS 사이에서 이송되는 기존의 메시지이기 때문이다.

[0075] MME (30) 는 새로운 메시지로 그룹 GW (20) 에 업데이트된 그룹 키를 전송할 수 있다 (단계 S53).

[0076] 그 다음에, 그룹 GW (20) 는 도 5 와 유사한 방식으로 MTC UE 들 (10_1 내지 10_n) 에 업데이트된 그룹 키를 재분배한다 (단계 S54_1 내지 단계 S54_n).

[0077] 다음으로, 본 예시적인 실시형태에 따른 MTC UE (10), 그룹 GW (20), HSS (40), 및 MTC-IWF (50) (50A) 의 구성 예들은 도 8 내지 도 11 을 참조하여 설명될 것이다.

[0078] 도 8 에 도시된 바와 같이, MTC UE (10) 는 그룹 GW (20) 로부터 보호된 그룹 키를 수신하는 수신 유닛 (11) 을 포함한다. 수신 유닛 (11) 은, 예를 들어, RAN 을 통해 코어 네트워크와 무선으로 통신을 행하는 송수신기, 및 이러한 송수신기를 제어하는 CPU (Central Processing Unit) 와 같은 제어기에 의해 구성될 수도 있다.

[0079] 도 9 에 도시된 바와 같이, 그룹 GW (20) 는 적어도 보호 유닛 (21) 및 분배 유닛 (22) 을 포함한다. 보호 유닛 (21) 은 키 Kgr 및 K_iwf 를 이용함으로써 그룹 키를 보호한다. 분배 유닛 (22) 은 MTC UE (10) 에 보호된 그룹 키를 분배한다. HSS (40) 또는 (그룹 GW (20) 가 아닌) MTC-IWF (50) 가 그룹 키를 도출하는 경우, 그룹 GW (20) 는 HSS (40) 또는 MTC-IWF (50) 로부터 그룹 키를 수신하는 수신 유닛 (23) 을 더 포함한다. 수신 유닛 (23) 은 또한 업데이트된 그룹 키를 수신한다. 수신 유닛 (23) 에 대한 대체로서, 그룹 GW (20) 는, 도출 파라미터들로서, 키 Kgr, 키 K_iwf, Kasme, 또는 난수를 이용함으로써 그룹 키를 도출하는 도출 유닛 (24) 을 포함할 수도 있다. 도출 유닛 (24) 은 또한 그룹 키를 업데이트한다. 어느 경우에도, 보호 유닛 (21) 은 키 Kgr 또는 K_iwf 를 이용함으로써 업데이트된 그룹 키를 보호하고, 분배 유닛 (22) 은 보호되고 업데이트된 그룹 키를 재분배한다. 이러한 유닛들 (21 내지 24) 은 버스 등을 통해 서로 상호 접속된다는 것에 유의한다. 이러한 유닛들 (21 내지 24) 은, 예를 들어, 코어 네트워크 내의 다른 노드들과 통신을 행하는 송수신기들, 및 이러한 송수신기들을 제어하는 CPU 와 같은 제어기에 의해 구성될 수 있다.

[0080] 도 10 에 도시된 바와 같이, HSS (40) 는 통상적인 HSS 에 더해 도출 유닛 (41) 및 전송 유닛 (42) 을 포함할 수 있다. 도출 유닛 (41) 은, 키 도출 파라미터들로서, 키 Kgr, 키 K_iwf, Kasme, 또는 난수를 이용함으로써 그룹 키를 도출한다. 전송 유닛 (42) 은 그룹 GW (20) 및/또는 MTC-IWF (50) 에 그룹 키를 전송한다. 도출 유닛 (41) 은 그룹 키를 업데이트할 수도 있고, 전송 유닛 (42) 은 그룹 GW (20) 및 또는 MTC-IWF (50) 에 업데이트된 그룹 키를 전송할 수도 있다. 이러한 유닛들 (41 내지 42) 은 버스 등을 통해 서로 상호 접속된다는 것에 유의한다. 이러한 유닛들 (41 내지 42) 은, 예를 들어, 코어 네트워크 내의 다른 노드들과 통신을 행하는 송수신기들, 및 이러한 송수신기들을 제어하는 CPU 와 같은 제어기에 의해 구성될 수 있다.

[0081] 도 11 에 도시된 바와 같이, MTC-IWF (50) (50A) 는 통상적인 MTC-IWF 의 엘리먼트들에 더해 도출 유닛 (51) 및 전송 유닛 (52) 을 포함할 수 있다. 도출 유닛 (51) 은, 키 도출 파라미터들로서, 키 Kgr, 키 K_iwf, Kasme, 또는 난수를 이용함으로써 그룹 키를 도출한다. 전송 유닛 (52) 은 그룹 GW (20) 및/또는 MTC UE (10) 에 그룹 키를 전송한다. 도출 유닛 (51) 은 그룹 키를 업데이트할 수도 있고, 전송 유닛 (52) 은 그룹 GW (20) 및 또는 MTC UE (10) 에 업데이트된 그룹 키를 전송할 수도 있다. 이러한 유닛들 (51 내지 52) 은 버스 등을 통해 서로 상호 접속된다는 것에 유의한다. 이러한 유닛들 (51 내지 52) 은, 예를 들어, 코어 네트워크 내의 다른 노드들과 통신을 행하는 송수신기들, 및 이러한 송수신기들을 제어하는 CPU 와 같은 제어기에 의해 구성될 수 있다.

[0082] 본 발명은 위에서 언급된 예시적인 실시형태로 제한되지 않고, 청구항들의 기재에 기초하여 당업자들에 의해 다양한 수정들이 이루어질 수 있음이 자명하다는 것에 유의한다.

[0083] 본 출원은 2013 년 7 월 31 일에 출원된 일본 특허 출원 제 2013-158881 호에 기초하고 그 우선권을 주장하며, 그 개시물은 참조로서 그 전체가 본원에 포함된다.

부호의 설명

[0084] 10, 10_1-10_n MTC UE

11, 23 수신 유닛

20 그룹 GW

21 보호 유닛

22 분배 유닛

24, 41, 51 도출 유닛

30 MME

40 HSS

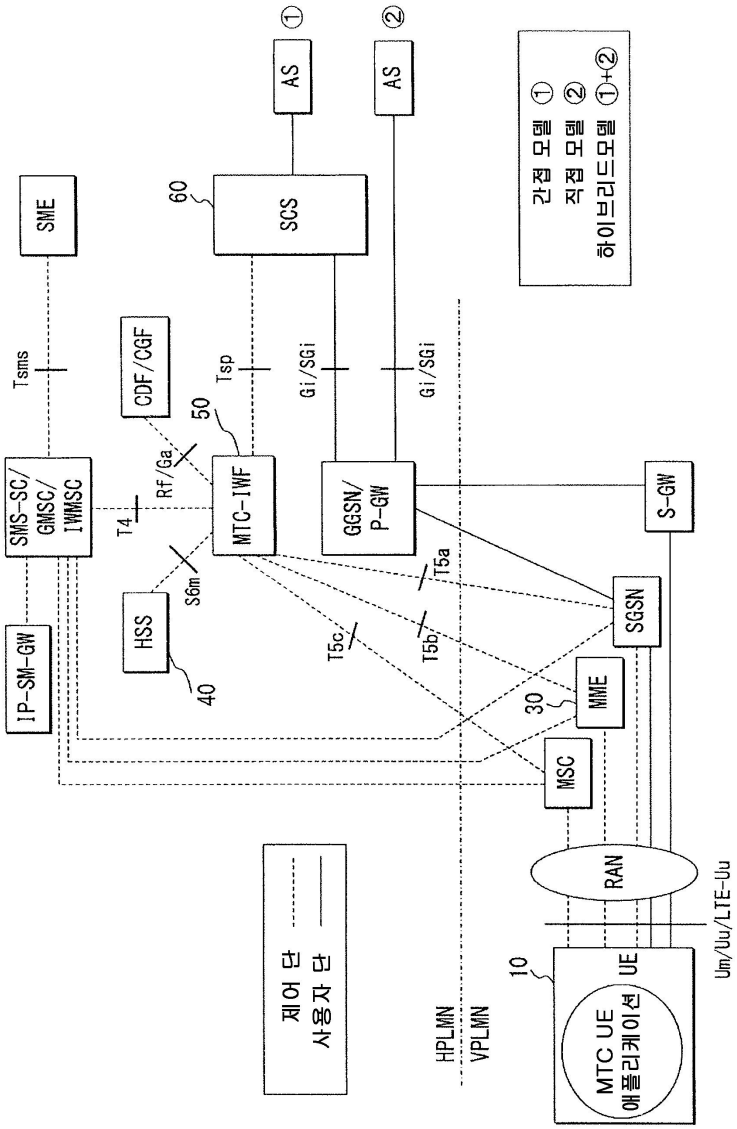
42, 52 전송 유닛

50, 50A MTC-IWF

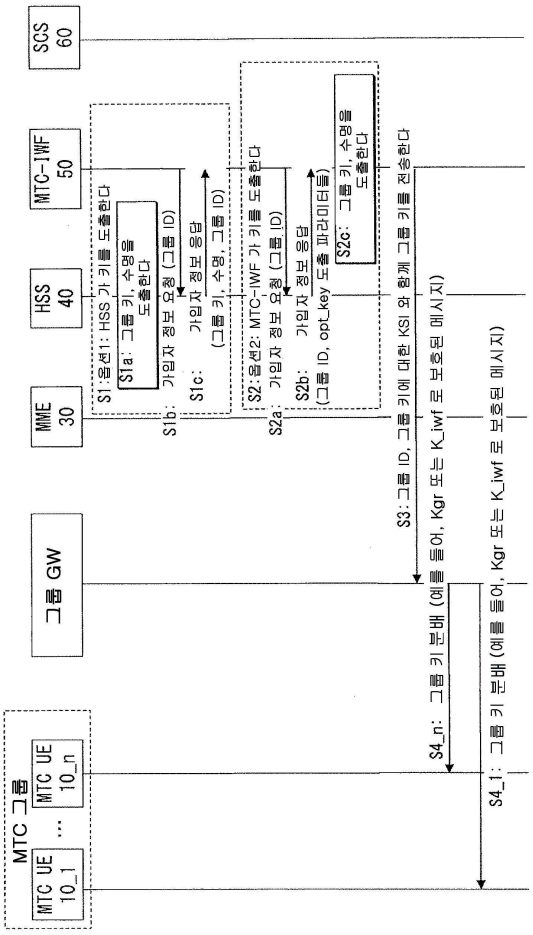
60 SCS

도면

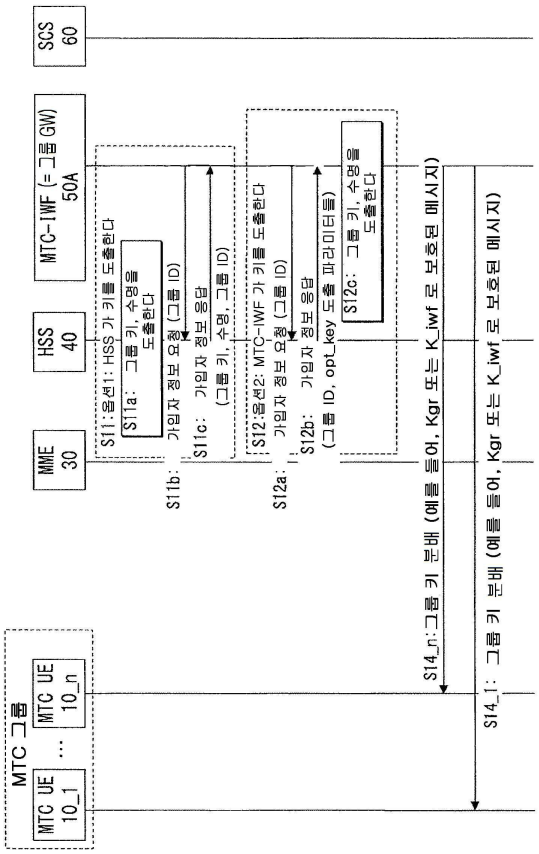
도면1



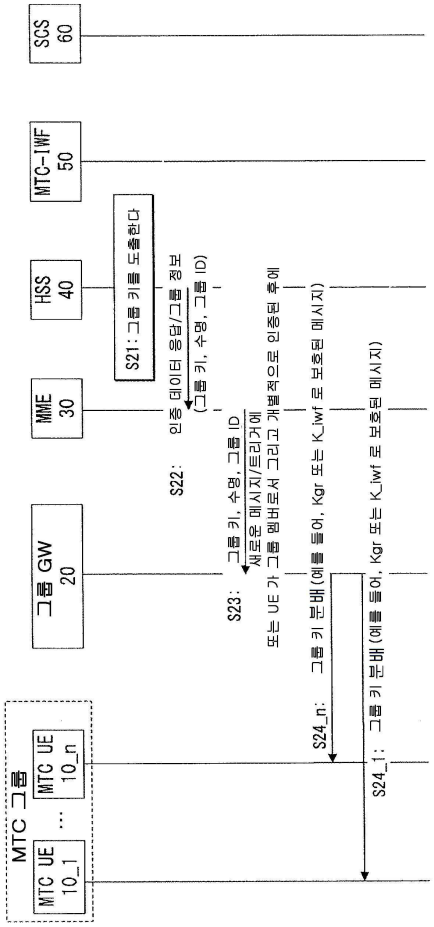
도면2


SCS 60
MTC-IWF 50
HSS 40
MME 30
그룹 GW
MTC 그룹
MTC UE 10_1
MTC UE 10_n
S1: 옵션1: HSS가 키를 도출한다
S1a: 그룹 키, 수명을 도출한다
S1b: 가입자 정보 요청 (그룹 ID)
S1c: 가입자 정보 응답 (그룹 키, 수명, 그룹 ID)
S2: 옵션2: MTC-IWF가 키를 도출한다
S2a: 가입자 정보 요청 (그룹 ID)
S2b: 가입자 정보 응답 (그룹 ID, opt_key 도출 파라미터들)
S2c: 그룹 키, 수명을 도출한다
S3: 그룹 ID, 그룹 키에 대한 KSI 와 함께 그룹 키를 전송한다
S4_n: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S4_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

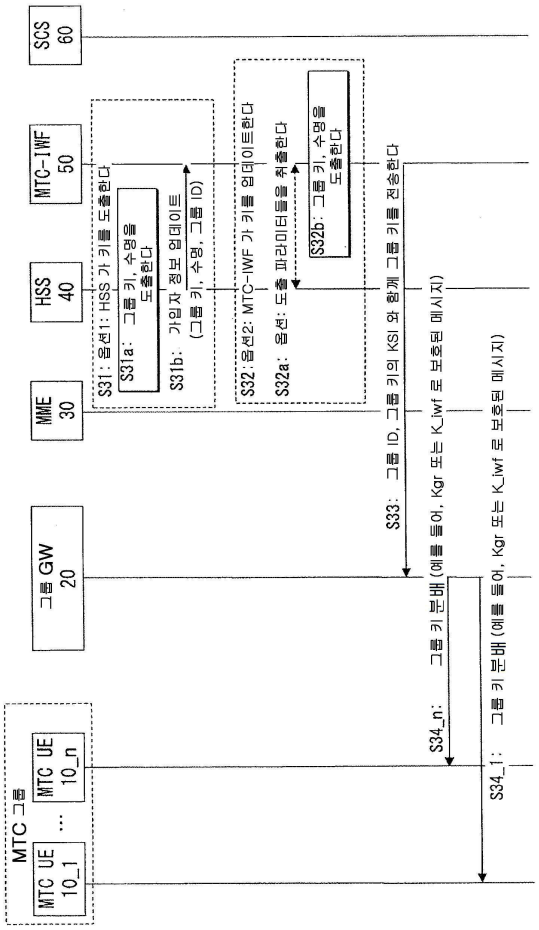
도면3


MTC 그룹
MTC UE 10_1
MTC UE 10_n
MME 30
HSS 40
MTC-IWF (= 그룹 GW) 50A
SCS 60
S11: 옵션1: HSS가 키를 도출한다
S11a: 그룹 키, 수명을 도출한다
S11b: 가입자 정보 요청 (그룹 ID)
S11c: 가입자 정보 응답 (그룹 키, 수명, 그룹 ID)
S12: 옵션2: MTC-IWF가 키를 도출한다
S12a: 가입자 정보 요청 (그룹 ID)
S12b: 가입자 정보 응답 (그룹 ID, opt_key 도출 파라미터들)
S12c: 그룹 키, 수명을 도출한다
S14_n: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S14_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

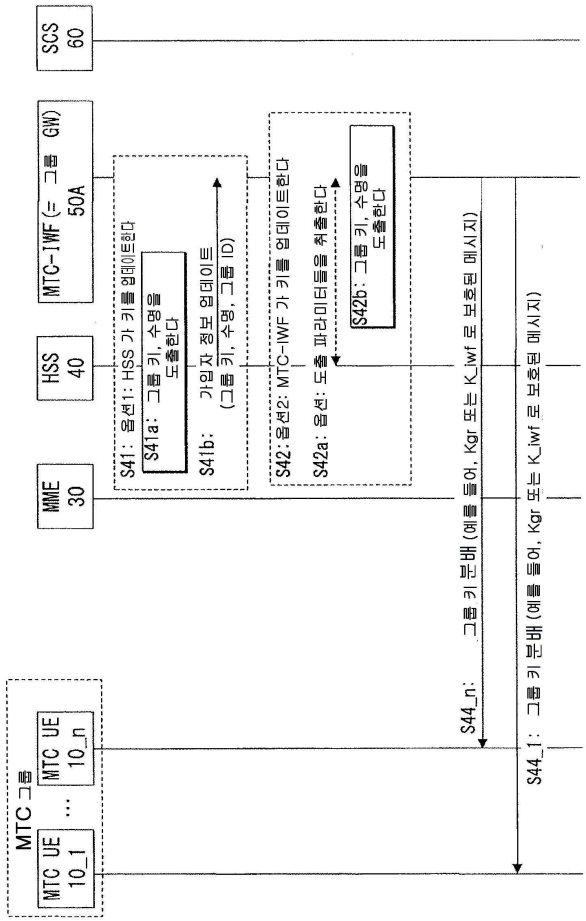
도면4


SGS 60
MTC-IWF 50
HSS 40
MME 30
그룹 GW 20
MTC 그룹
MTC UE 10_1
MTC UE 10_n
S21: 그룹 키를 도출한다
S22: 인증 데이터 응답/그룹 정보 (그룹 키, 수명, 그룹 ID)
S23: 그룹 키, 수명, 그룹 ID 새로운 메시지/트리거에 또는 UE 가 그룹 멤버로서 그리고 개별적으로 인증된 후에
S24_n: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S24_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

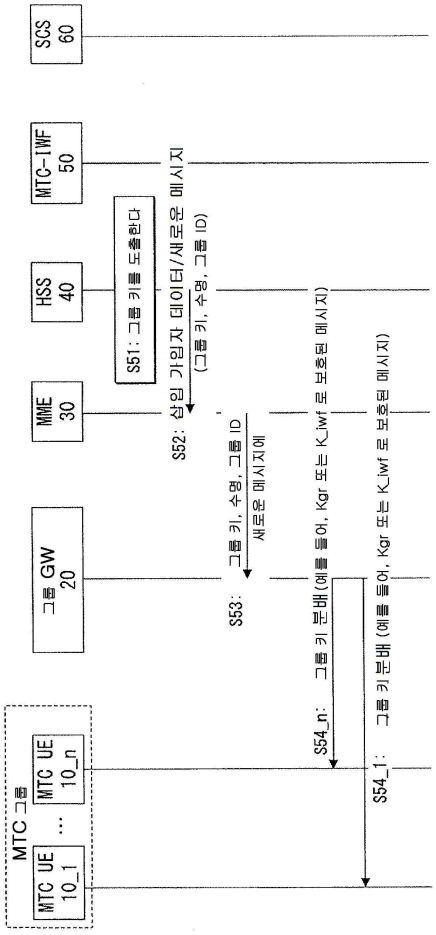
도면5


SCS 60
MTC-IWF 50
HSS 40
MME 30
그룹 GW 20
MTC 그룹
MTC UE 10_1
MTC UE 10_n
S31: 옵션1: HSS가 키를 도출한다
S31a: 그룹 키, 수명을 도출한다
S31b: 가입자 정보 업데이트 (그룹 키, 수명, 그룹 ID)
S32: 옵션2: MTC-IWF 가 키를 업데이트한다
S32a: 옵션: 도출 파라미터들을 취출한다
S32b: 그룹 키, 수명을 도출한다
S33: 그룹 ID, 그룹 키의 KSI 와 함께 그룹 키를 전송한다
S34_n: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S34_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

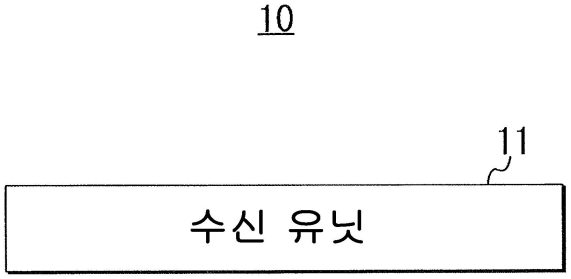
도면6


SCS 60
MTC-IWF (= 그룹 GW) 50A
HSS 40
MME 30
MTC 그룹
MTC UE 10_1
MTC UE 10_n
S41: 옵션1: HSS 가 키를 업데이트한다
S41a: 그룹 키, 수명을 도출한다
S41b: 가입자 정보 업데이트 (그룹 키, 수명, 그룹 ID)
S42: 옵션2: MTC-IWF 가 키를 업데이트한다
S42a: 옵션: 도출 파라미터들을 취출한다
S42b: 그룹 키, 수명을 도출한다
S44_n: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S44_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

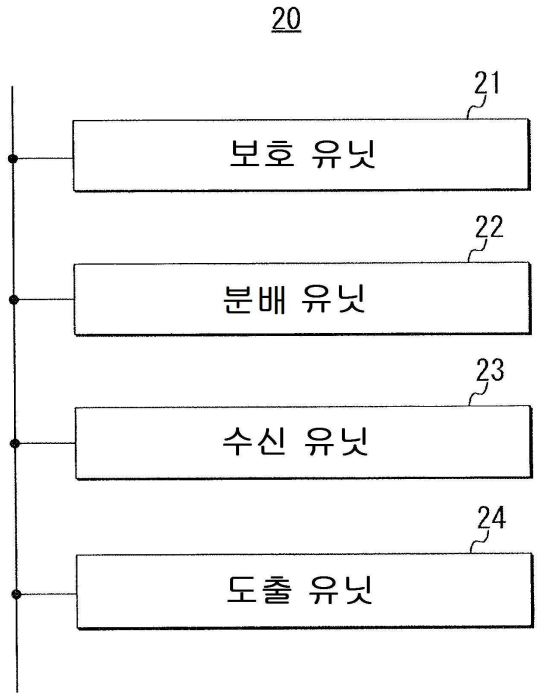
도면7


SCS 60
MTC-IWF 50
HSS 40
MME 30
그룹 GW 20
MTC 그룹
MTC UE 10_1
MTC UE 10_n
S51: 그룹 키를 도출한다
S52: 삽입 가입자 데이터/새로운 메시지 (그룹 키, 수명, 그룹 ID)
S53: 그룹 키, 수명, 그룹 ID 새로운 메시지에
S54_n: 그룹 키 분배(예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)
S54_1: 그룹 키 분배 (예를 들어, Kgr 또는 K_iwf 로 보호된 메시지)

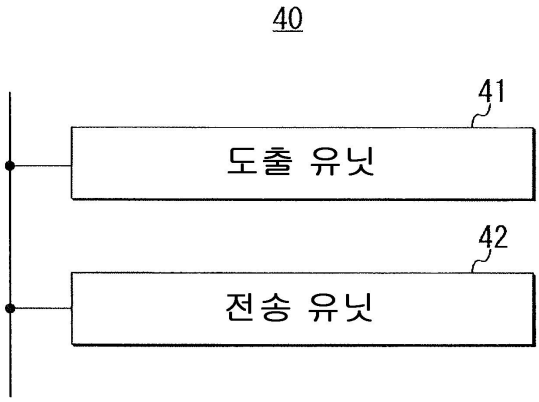
도면8


10
11
수신 유닛

도면9



도면10



도면11