(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0021079
(43) 공개일자 2015년02월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/12 (2009.01) *H04W 12/08* (2009.01)
H04W 4/08 (2009.01) *H04W 88/18* (2009.01)
H04W 88/16 (2009.01)
(21) 출원번호 10-2014-7036507
(22) 출원일자(국제) 2013년04월19일
심사청구일자 2014년12월26일
(85) 번역문제출일자 2014년12월26일
(86) 국제출원번호 PCT/JP2013/002661
(87) 국제공개번호 WO 2014/002351
국제공개일자 2014년01월03일
(30) 우선권주장
JP-P-2012-147983 2012년06월29일 일본(JP)

(71) 출원인
닛본 덴끼 가부시끼가이샤
일본국 도쿄도 미나도꾸 시바 5쪼메 7방 1고
(72) 발명자
장, 시아오웨이
일본 108-8001 도쿄도 미나또꾸 시바 5쪼메 7-1 닛본 덴끼 가부시끼가이샤 내
프라사드, 아난드 라하와
일본 108-8001 도쿄도 미나또꾸 시바 5쪼메 7-1 닛본 덴끼 가부시끼가이샤 내
(74) 대리인
양영준, 박충범

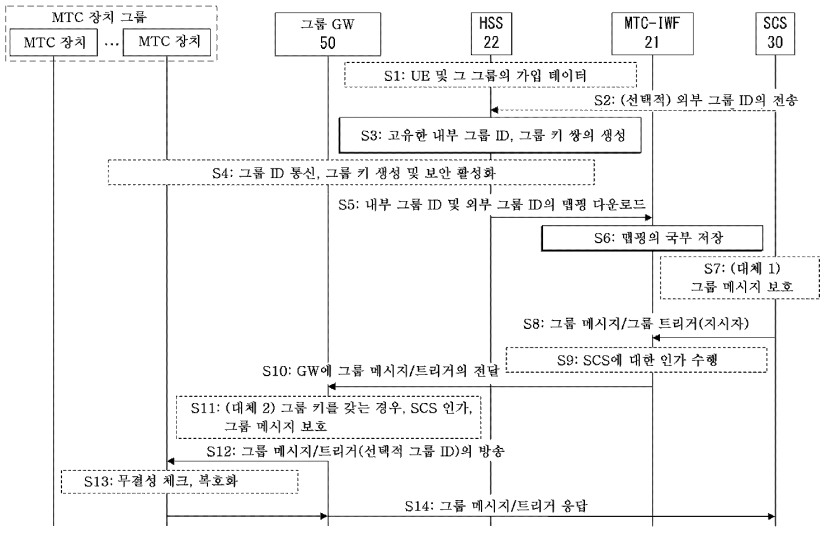
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 **M2M의 그룹 기반 특징에 대한 보안 업데이트**

(57) 요 약

코어 네트워크 내에 위치하는 네트워크 노드(21)는, 코어 네트워크 외부에 위치하는 송신원(30)으로부터 메시지를 수신한다. 이 메시지는 코어 네트워크에 연결된 하나 이상의 MTC 장치의 그룹에 메시지가 어드레스되는 지의 여부를 나타내는 지시자를 포함한다. 네트워크 노드(21)는 메시지가 그룹에 어드레스되는 것을 지시자가 나타내는 경우, 송신원(30)을 인가하기로 결정한다. 또한, 메시지는 그룹에 메시지가 어드레스되는지의 여부를 식별하기 위한 ID를 포함한다. MTC 장치는, ID가 MTC 장치 자체에 할당된 ID와 일치하지 않는 경우, 메시지를 폐기하기로 결정한다. 또한, MTC 장치는 공유된 그룹 키 쌍을 이용하여 송신원(30)과 통신한다.

대 표 도



특허청구의 범위

청구항 1

코어 네트워크 내에 위치한 네트워크 노드로서,

상기 코어 네트워크 외부에 위치한 송신원으로부터 메시지를 수신하기 위한 수신 수단 - 상기 메시지는 상기 코어 네트워크에 연결된 하나 이상의 MTC(머신 타입 통신) 장치의 그룹에 상기 메시지가 어드레스되는지의 여부를 나타내는 지시자를 포함함 -; 및

상기 메시지가 상기 그룹에 어드레스되는 것을 상기 지시자가 나타내는 경우, 상기 송신원을 인가하기로 결정하기 위한 판정 수단을 포함하는, 네트워크 노드.

청구항 2

제1항에 있어서, 상기 지시자는 상기 메시지가 상기 송신원과 통신하도록 상기 그룹을 트리거하는지를 더 나타내는, 네트워크 노드.

청구항 3

제1항 또는 제2항에 있어서,

상기 메시지는 상기 그룹을 식별하기 위해 상기 송신원에 대한 외부 ID(식별자)를 더 포함하고,

상기 네트워크 노드는,

상기 MTC 장치들의 어드레스들을 식별하기 위한 내부 ID 및 상기 외부 ID의 맵핑을 저장하기 위한 기억 수단;

상기 맵핑을 사용하여, 상기 메시지 내의 상기 대응하는 내부 ID에 상기 외부 ID를 맵핑하기 위한 맵핑 수단; 및

상기 MTC 장치들에 상기 메시지를 방송할 수 있는 네트워크 요소에 상기 메시지를 전송하기 위한 전송 수단을 더 포함하는, 네트워크 노드.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 네트워크 노드는 MTC-IWF(MTC-연동 기능)를 포함하는, 네트워크 노드.

청구항 5

코어 네트워크에 연결되어, 제1항 내지 제4항 중 어느 한 항에 따른 네트워크 노드에 의해 전송된 메시지를 수신하도록 구성된, MTC(머신 타입 통신) 장치.

청구항 6

코어 네트워크 외부에 위치되어, 제1항 내지 제4항 중 어느 한 항에 따른 네트워크 노드에 메시지를 송신하고, 상기 메시지 내에 상기 지시자를 포함하도록 구성된, 네트워크 노드.

청구항 7

제6항에 있어서,

상기 코어 네트워크 외부에 위치한 상기 네트워크 노드가, SCS(서비스 역량 서버) 또는 SME(단문 메시지 엔티티)를 포함하는, 네트워크 노드.

청구항 8

코어 네트워크 내에 위치하는 네트워크 노드를 제어하는 방법으로서,

상기 코어 네트워크 외부에 위치한 송신원으로부터 메시지를 수신하는 단계 - 상기 메시지는 상기 코어 네트워

크에 연결된 하나 이상의 MTC(머신 타입 통신) 장치의 그룹에 상기 메시지가 어드레스되는지의 여부를 나타내는 지시자를 포함함 -; 및

상기 메시지가 상기 그룹에 어드레스되는 것을 상기 지시자가 나타내는 경우, 상기 송신원을 인가하기로 결정하는 단계를 포함하는, 네트워크 노드 제어 방법.

청구항 9

코어 네트워크에 연결된 MTC(머신 타입 통신) 장치로서,

상기 코어 네트워크로부터 메시지를 수신하기 위한 수신 수단 - 상기 메시지는 하나 이상의 MTC 장치의 그룹에 상기 메시지가 어드레스되는지의 여부를 식별하기 위한 ID(식별자)를 포함함 -; 및

상기 ID가 상기 MTC 장치 자체에 할당된 ID와 일치하지 않는 경우, 상기 메시지를 폐기하기로 결정하기 위한 판정 수단을 포함하는, MTC(머신 타입 통신) 장치.

청구항 10

코어 네트워크 내에 위치되어, 제9항에 따른 MTC 장치에 메시지를 전송하고 상기 메시지 내에 상기 ID를 포함하도록 구성되는, 네트워크 노드.

청구항 11

제10항에 있어서,

상기 네트워크 노드는 MTC-IWF(MTC-연동 기능)를 포함하는, 네트워크 노드.

청구항 12

코어 네트워크 외부에 위치되어, 상기 코어 네트워크를 통해 제9항에 따른 상기 MTC 장치에 메시지를 전송하고 상기 메시지 내에 상기 ID를 포함하도록 구성되는, 네트워크 노드.

청구항 13

제12항에 있어서,

상기 네트워크 노드는 SCS(서비스 역량 서버) 또는 SME(단문 메시지 엔티티)를 포함하는, 네트워크 노드.

청구항 14

코어 네트워크에 연결된 MTC(머신 타입 통신) 장치의 제어 방법으로서,

상기 코어 네트워크로부터 메시지를 수신하는 단계 - 상기 메시지는 하나 이상의 MTC 장치의 그룹에 상기 메시지가 어드레스되는지의 여부를 식별하기 위한 ID(식별자)를 포함함 -; 및

상기 ID가 상기 MTC 장치 자체에 할당된 ID와 일치하지 않는 경우, 상기 메시지를 폐기하기로 결정하는 단계를 포함하는, MTC(머신 타입 통신) 장치의 제어 방법.

청구항 15

메시지를, 코어 네트워크 외부에 위치된 상기 메시지의 송신원으로부터, 상기 코어 네트워크에 연결된 하나 이상의 MTC(머신 타입 통신) 장치의 그룹에 중계하는 게이트웨이로서,

상기 송신원과 통신을 안전하게 행하기 위해 상기 MTC 장치들의 상기 그룹에 대한 그룹 키 쌍을 취득하기 위한 취득 수단; 및

상기 그룹 키들을 이용하여 상기 메시지를 중계하기 위한 중계 수단을 포함하는, 게이트웨이.

청구항 16

제15항에 있어서,

상기 중계 수단은,

상기 그룹 키들로 상기 메시지를 검증하고;

상기 검증 실패시에 상기 메시지를 폐기하도록 구성되는, 게이트웨이.

청구항 17

제15항 또는 제16항에 있어서,

상기 게이트웨이는 상기 MTC 장치들이 무선으로 연결되는 기지국에 배치되는, 게이트웨이.

청구항 18

제15항 또는 제16항에 있어서,

상기 게이트웨이는 상기 MTC 장치들이 무선으로 연결되는 하나 이상의 기지국에 연결된 네트워크 구성 요소에 배치되는, 게이트웨이.

청구항 19

코어 네트워크에 연결된 MTC(머신 타입 통신) 장치로서,

상기 코어 네트워크 외부에 위치되어, 하나 이상의 MTC 장치의 그룹에 어드레스된 메시지를 송신하는 송신원과 안전하게 통신을 행하기 위해 그룹 키 쌍을 취득하기 위한 취득 수단; 및

상기 그룹 키들을 이용하여 상기 송신원과 통신하기 위한 통신 수단을 포함하는, MTC(머신 타입 통신) 장치.

청구항 20

코어 네트워크 외부에 위치되어, 상기 코어 네트워크를 통해 제19항에 따른 MTC 장치와 통신하고, 상기 통신을 위해 상기 그룹 키들을 사용하도록 구성되는, 네트워크 노드.

청구항 21

제20항에 있어서,

상기 네트워크 노드는, SCS(서비스 역량 서버) 또는 SME(단문 메시지 엔티티)를 포함하는, 네트워크 노드.

청구항 22

메시지를, 코어 네트워크 외부에 위치된 상기 메시지의 송신원으로부터, 상기 코어 네트워크에 연결된 하나 이상의 MTC(머신 타입 통신) 장치의 그룹에 중계하는 게이트웨이를 제어하는 방법으로서,

상기 송신원과 통신을 안전하게 행하기 위해 상기 MTC 장치들의 그룹에 대한 그룹 키 쌍을 취득하는 단계; 및

상기 그룹 키들을 이용하여 상기 메시지를 중계하는 단계를 포함하는, 게이트웨이의 제어 방법.

청구항 23

코어 네트워크에 연결된 MTC(머신 타입 통신) 장치를 제어하는 방법으로서,

상기 코어 네트워크 외부에 위치되어, 하나 이상의 MTC 장치의 그룹에 어드레스된 메시지를 송신하는 송신원과 안전하게 통신을 행하기 위해 그룹 키 쌍을 취득하는 단계; 및

상기 그룹 키들을 이용하여 상기 송신원과 통신하는 단계를 포함하는, MTC(머신 타입 통신) 장치의 제어 방법.

명 세 서

기 술 분 야

[0001] 본 발명은, 새롭게 비특허 문헌 1에 기재된 구조를 갖는 머신 타입 통신(MTC)을 기반으로 하는 그룹에 대한 보안 솔루션에 관한 것이다. 이러한 솔루션은 그룹 메시지가 송신될 때 SCS(서비스 역량 서버)에 적합한 인가를 행하기 위해 MTC-IWF(MTC-연동 기능)을 지원할 수 있다. 본 발명은 또한 안전하게 그룹 메시지를 전달하고 방송하는 메커니즘에 관한 것이다.

배 경 기 술

[0002] 그룹 기반 특징의 연구는 3GPP 릴리즈 12(예를 들어, 비특허 문헌 2 참조)에서 시작되고, 새로운 구조는 비특허 문헌 1에서 연구되고 있다. 본 출원의 발명자가 특허 문헌 1에서 제안한 그룹 게이트웨이(GW)의 개념으로, 본 발명은 새로운 구조에서 그것을 확장한다.

[0003] SCS는 MTC-IWF의 네트워크 노드에 그룹 메시지를 전송하고, MTC-IWF는 MTC 장치의 타겟 그룹에 그룹 메시지를 전달한다. 메시지는 하나 초과의 MTC 장치를 타겟으로 하고 네트워크와 통신하기 위해 이들 장치를 트리거할 수 있다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 국제 특허 공보 WO 2012/018130

비특허문헌

[0005] (비특허문헌 0001) 3GPP TS 23.682, "Architecture enhancements to facilitate communications with packet data networks and applications (Release 11)", v11.1.0, 2012-06

(비특허문헌 0002) 3GPP TR 23.8xy, "Machine-Type and other Mobile Data Applications Communications Enhancements; (Release 12)", V0.1.0, 2012-05

(비특허문헌 0003) 3GPP TR 33.868, "Security aspects of Machine-Type Communications; (Release 11)", v0.8.0

발명의 내용

해결하려는 과제

[0006] 그러나, 본 출원의 발명자는 사기성 그룹 메시지가 네트워크에 대한 DoS(서비스 거부) 공격을 일으킬 수 있다는 문제를 찾아냈다. 비 특허 문헌 3에 기재된 MTC 장치에 대한 공격이 여기에서도 유효하다는 점에 유의해야 한다.

[0007] 따라서, MTC-IWF는, 특히 메시지가 트리거를 포함할 때, 그룹 메시지를 송신할 수 있는지 알아보기 위해 SCS 인가를 수행해야 한다.

과제의 해결 수단

[0008] 상기 과제를 해결하기 위해, 본 발명의 제1 실시 형태에 따른 네트워크 노드는 코어 네트워크 내에 위치된다. 이 네트워크 노드는, 코어 네트워크에 연결된 하나 이상의 MTC 장치의 그룹에 메시지가 어드레스되는지의 여부를 나타내는 지시자를 포함하는 메시지를, 코어 네트워크 외부에 위치된 송신원으로부터 수신하기 위한 수신 수단; 및 메시지가 그 그룹에 어드레스되는 것을 지시자가 나타내는 경우, 송신원을 인가하기로 결정하기 위한 판정 수단을 포함한다.

[0009] 또한, 본 발명의 제2 실시 형태에 따른 방법은, 코어 네트워크 내에 위치하는 네트워크 노드를 제어하는 방법을 제공한다. 이 방법은, 코어 네트워크 외부에 위치한 송신원으로부터 메시지를 수신하는 단계- 상기 메시지는 코어 네트워크에 연결된 하나 이상의 MTC 장치의 그룹에 메시지가 어드레스되는지의 여부를 나타내는 지시자를 포함-; 및 메시지가 그 그룹에 어드레스되는 것을 지시자가 나타내는 경우, 송신원을 인가하기로 결정하는 단계를 포함한다.

[0010] 또한, 본 발명의 제3 실시 형태에 따른 MTC 장치는, 메시지가 하나의 이상의 MTC 장치의 그룹에 어드레스되는지의 여부를 식별하기 위한 ID(식별자)를 포함하는 메시지를 코어 네트워크로부터 수신하기 위한 수신 수단; 및 ID가 MTC 장치 자체에 할당된 ID와 일치하지 않는 경우, 메시지를 폐기하기로 결정하기 위한 판정 수단을 포함

한다.

[0011] 또한, 본 발명의 제4 실시 형태에 따른 방법은, 코어 네트워크에 연결된 MTC 장치를 제어하는 방법을 제공한다. 이 방법은, 메시지가 하나 이상의 MTC 장치의 그룹에 어드레스되는지의 여부를 식별하기 위한 ID를 포함하는 메시지를 코어 네트워크로부터 수신하는 단계; 및 ID가 MTC 장치 자체에 할당된 ID와 일치하지 않는 경우, 메시지를 폐기하기로 결정하는 단계를 포함한다.

[0012] 또한, 본 발명의 제5 실시 형태에 따른 게이트웨이는, 코어 네트워크 외부에 위치된 메시지의 송신원으로부터 메시지를, 코어 네트워크에 연결된 하나 이상의 MTC 장치의 그룹에 중계한다. 이 게이트웨이는, 안전하게 송신원과 통신을 수행하기 위해 MTC 장치의 그룹에 대한 그룹 키 쌍을 취득하는 취득 수단; 및 그룹 키를 이용하여 메시지를 중계하기 위한 중계 수단을 포함한다.

[0013] 또한, 본 발명의 제6 실시 형태에 따른 MTC 장치는, 코어 네트워크 외부에 위치되어, 하나 이상의 MTC 장치의 그룹에 어드레스된 메시지를 송신하는 송신원과 통신을 안전하게 행하기 위해 그룹 키 쌍을 취득하는 취득 수단; 및 그룹 키를 이용하여 송신원과 통신하는 통신 수단을 포함한다.

[0014] 또한, 본 발명의 제7 실시 형태에 따른 방법은, 코어 네트워크 외부에 위치된, 메시지의 송신원으로부터 메시지를, 코어 네트워크에 연결된 하나 이상의 MTC 장치의 그룹에 중계하는 게이트웨이를 제어하는 방법을 제공한다. 이 방법은, 송신원과 통신을 안전하게 수행하기 위해 MTC 장치의 그룹에 대한 그룹 키 쌍을 취득하는 단계; 및 상기 그룹 키를 이용하여 메시지를 중계하는 단계를 포함한다.

[0015] 또한, 본 발명의 제8 실시 형태에 따른 방법은, 코어 네트워크에 연결된 MTC(머신 타입 통신) 장치를 제어하는 방법을 제공한다. 이 방법은, 코어 네트워크 외부에 위치되어 하나 이상의 MTC 장치의 그룹에 어드레스된 메시지를 송신하는 송신원과 통신을 안전하게 행하기 위해 그룹 키 쌍을 취득하는 단계; 및 상기 그룹 키를 이용하여 송신원과 통신하는 단계를 포함한다.

발명의 효과

[0016] 본 발명에 의하면, 특히 메시지가 트리거를 포함할 때, 그룹 메시지를 송신할 수 있는지 알아보기 위해 SCS 인가를 수행하는 것이 가능하다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시 형태에 따른 시스템 구조의 일례를 나타내는 블록도이다.

도 2는 본 발명의 실시 형태에 따른 시스템 내의 MTC 장치에서 종료된 그룹 메시지의 일례를 나타내는 시퀀스도이다.

도 3은 본 발명의 실시 형태에 따라 위치된 네트워크 노드의 구성 예를 나타내는 블록도이다.

도 4는 본 발명의 실시 형태에 따른 MTC 장치의 구성 예를 나타내는 블록도이다.

도 5는 본 발명의 실시 형태에 따른 게이트웨이의 구성 예를 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 1. 논의

[0019] SA2는 TR 23.8xy v0.1.0 "Machine-Type and other Mobile Data Applications Communications Enhancements (Release 12)"에 기재된 그룹 기반 특징에 대한 연구를 시작했다. SA3는 SA2가 제공한 구조 요구 사항에 따라 릴리즈 12에 대한 보안 과제를 공부해야한다.

[0020] SA2로부터의 그룹 기반 메시징에 대한 구조 요구 사항은 하기와 같이 주어진다:

[0021] - 네트워크는 특별한 지리적 영역에 위치한 MTC 그룹의 멤버들에 SCS로부터의 그룹 메시지를 분배하는 메커니즘을 제공한다.

[0022] - 그룹 기반 메시징 특징은 이러한 특징을 사용하지 않는 UE에 대해서는 새로운 추가 기능을 필요로 하지 않는다.

[0023] - 시스템은 그룹 기반 메시징 기능을 사용하는 UE가 UE에 어드레스된 분산 그룹 메시지를 효율적으로 인식할 수

있는 메커니즘을 지원한다.

[0024] - 시스템은 SCS가 그룹 메시지를 송신하기 위한 인터페이스를 제공한다. 이러한 인터페이스는 다음과 같은 정보를 운반할 수 있어야 한다:

[0025] - 그룹 메시지의 애플리케이션 계층 콘텐츠,

[0026] - 그룹 메시지가 의도되는 그룹 식별, 및

[0027] - 그룹 메시지가 분배되어야 하는 지리적 영역 및 RAT(s).

[0028] - 시스템은 분산된 그룹 메시지에 응답하는 장치들로 인한 과부하로부터 보호되어야 한다.

[0029] - 그룹 기반 메시징은 GERAN, UTRAN 및 E-UTRAN 액세스시에 지원되어야 한다.

[0030] 현재의 구조에 따르면, MTC-IWF가 SCS로부터 그룹 메시지를 수신하고, 이를 MTC 장치의 타겟 그룹에 전달한다고 가정할 수 있다.

[0031] 그룹 메시지로 인해, 다중 MTC 장치가 응답하도록 트리거될 수 있다. 따라서, 비인가 그룹 메시지는 단일 MTC 장치에 대한 트리거가 일으킬 수 있는 것에 비해 훨씬 더 심각한 문제를 일으킬 수 있다. 비 그룹 메시지에 대해 고려되었던 MitM 공격 및 재생 공격과 같은 다른 위협은 또한 증폭 효과를 여기에 적용한다. 따라서,

[0032] - 네트워크는 SCS가 타겟 그룹에 그룹 메시지를 보낼 수 있는지의 여부의 인가를 수행해야 한다. 이를 위해, MTC-IWF는 다른 메시지로부터 그룹 메시지를 구별할 수 있어야 한다.

[0033] - 그룹 메시지는 기밀성 및 무결성 보호를 받아야 하고, 메시지를 수신하는 MTC 장치는 이를 검증할 수 있어야 한다.

[0034] - 네트워크는 3GPP 네트워크의 외부에 위치하는 SCS가 타겟 그룹과 통신하기 위한 수단을 제공해야 한다. SCS가 그룹 메시지를 보낼 때 그룹 식별이 사용된다. UE 식별과 마찬가지로, 3GPP 네트워크에서 사용되는 그룹 식별은 외부 인터페이스를 통해 전송되지 말아야 하며, 3GPP 네트워크의 외부 노드에 알려지지 않아야 한다. 이는 3GPP 네트워크의 외부에 위치하는 SCS에 적용된다.

[0035] 상기 분석을 통해, MTC 그룹 기반 특징에 대한 보안 요구 사항은 다음과 같이 결론된다:

[0036] - MTC-IWF는 SCS가 주어진 MTC 그룹에 그룹 메시지를 송신하도록 인가되는 경우를 검증해야 한다.

[0037] - MTC-IWF는 다른 메시지로부터 그룹(트리거) 메시지를 구별할 수 있어야 한다.

[0038] - MTC 장치의 그룹에 분산되는 그룹 메시지는 기밀성, 무결성 보호 및 재생 보호가 있어야 한다.

[0039] - 그룹 메시지를 수신하는 MTC 장치는 인가된 SCS로부터 그룹 메시지가 전송되는 지를 검증할 수 있어야 한다.

[0040] - 그룹 ID는 3GPP 네트워크의 외부에 위치하는 노드에 노출되지 않아야 한다. 이는, 3GPP 네트워크의 외부에도 있는 SCS를 포함한다.

[0041] 2. 제안

[0042] SA3에 다음을 제안한다:

[0043] 1) 그룹 기반 특징에 대한 위협 및 보안 요구 사항을 연구

[0044] 2) 다음과 같이 별도의 pCR이 주어진 경우, 릴리즈 12의 TR 33.868에 상기 분석 및 보안 요구 사항을 포함.

[0045] 5.x 주요 이슈 - 그룹 기반 메시징

[0046] 5.x.1 이슈 세부 사항

[0047] SA2는 TR 23.8xy(릴리즈 12)에서 그룹 기반 특징에 대한 연구를 시작했다. 현재의 구조에 따르면, MTC-IWF가 SCS로부터 그룹 메시지를 수신하고, 이를 MTC 장치의 타겟 그룹에 전달한다고 가정할 수 있다.

[0048] 5.x.2 위협

[0049] 그룹 메시지로 인해, 다중 MTC 장치가 응답하도록 트리거될 수 있다. 따라서, 비인가 그룹 메시지는 단일 MTC 장치에 대한 트리거가 일으킬 수 있는 것에 비해 훨씬 더 심각한 문제를 일으킬 수 있다. 비 그룹 메시지에 대해 고려되었던 MitM 공격 및 재생 공격과 같은 다른 위협은 또한 증폭 효과를 여기에 적용한다.

[0050] 5.x.3 보안 요구 사항

[0051] - MTC-IWF는, SCS가 주어진 MTC 그룹에 그룹 메시지를 송신하도록 인가되는 지를 검증해야 한다.

[0052] - MTC-IWF는, 다른 메시지로부터 그룹(트리거) 메시지를 구별할 수 있어야 한다.

[0053] - MTC 장치의 그룹에 분산되어 있는 그룹 메시지는, 기밀성, 무결성 보호 및 재생 보호가 있어야 한다.

[0054] - 그룹 메시지를 수신하는 MTC 장치는, 인가된 SCS로부터 그룹 메시지가 전송되는 지를 검증할 수 있어야 한다.

[0055] - 그룹 ID는, 3GPP 네트워크의 외부에 위치하는 노드에 노출되지 않도록 해야한다. 이는, 3GPP 네트워크의 외부에도 있는 SCS를 포함한다.

[0056] 이하, 도 1 내지 5를 참조하여, 본 발명의 예시적인 실시 형태에 대하여 설명한다.

[0057] 도 1에 도시된 바와 같이, 본 실시 형태에 따른 시스템은, 코어 네트워크(3GPP 네트워크), RAN(무선 액세스 네트워크)을 통해 코어 네트워크에 연결되는 복수의 MTC 장치(10), 및 코어 네트워크 외부에 위치한 그룹 메시지 또는 그룹 트리거 소스로서 기능하는 SCS(30)와 SME(단문 메시지 엔티티)(40)를 포함한다. RAN은 복수의 기지국(즉, eNB들(진화된 노드 B들))에 의해 형성된다는 점에 유의해야 한다.

[0058] 그 중에서도, 각 MTC 장치(10)는, MTC를 Um/Uu/LTE-Uu 인터페이스를 통해 코어 네트워크에 접속하기 위한 UE이다. UE는 단일 또는 다중 MTC 애플리케이션을 호스팅할 수 있다. 외부 네트워크 내의 해당 MTC 애플리케이션은, 단일 또는 다중 AS들(애플리케이션 서버들) 상에서 호스팅된다.

[0059] 또한, SCS(30) 및 SME(40)는 MTC 장치들(10)과 통신하기 위해 코어 네트워크에 연결된다.

[0060] 또한, 코어 네트워크는 HPLMN(홈 공용 지상 모바일 네트워크)에서 MTC-IWF(21) 및 HSS(홈 가입자 서버)(22)를 포함한다. 코어 네트워크에 있어서, MTC-IWF(21)는 송신원으로부터 그룹 메시지 또는 그룹 트리거를 수신하는 네트워크 노드로서 기능한다. 통상적으로, MTC-IWF(21)는 Tsp 인터페이스를 통해 SCS(30)로부터 또는 T4 및 Tsms 인터페이스를 통해 SME(40)로부터 그룹 트리거일 수도 있는 그룹 메시지를 수신하고, T5b/T5a/T5c 인터페이스를 통해 MTC 장치(10)에 그룹 메시지를 전달하는 네트워크 요소로서 기능하는 MME(이동성 관리 엔티티), SGSN(서빙 GPRS(일반 패킷 무선 서비스) 지원 노드) 또는 MSC(모바일 스위칭 센터)에 그룹 메시지를 전달하여, 그룹 메시지 또는 그룹 트리거가 MTC 장치(10)에 라우팅될 수 있도록 한다. HSS(22) 또는 MTC-IWF(21)는 내부 및 외부 그룹 ID의 맵핑을 생성하고 저장할 수 있으며, HSS(22)는 그룹 키 쌍(후술함)을 생성한다. 그룹 키 중 하나는 암호화 및 복호화를 위해 생성되고, 다른 하나는 무결성 보호를 위해 생성된다.

[0061] 다음에, 본 실시 형태의 동작 예는 도 2를 참조하여 상세하게 설명한다. 도 2는 MTC 장치의 그룹에 전송하는 그룹 메시지의 메시지 시퀀스를 도시한다. MTC 장치 그룹 내에는 하나 초과의 장치가 있다.

[0062] 본 실시 형태에서, 상호 인증이 그룹 GW(후술함)와 네트워크와의 사이 및 그룹 GW와 MTC 장치(10) 사이에서 행해졌다고 가정한다. 그룹 메시지를 수신하고 이를 MTC 장치에 전송하며, 네트워크 또는 SCS와 통신하는 MTC 장치에 대해 연결 메시지를 송신할 책임이 있는 게이트웨이는, 특허문헌 1의 별도의 발명에서 제안되었다는 점에 유의해야 한다. 이러한 실시 형태는 게이트웨이에 대한 몇 가지 새로운 기능을 제안하며, 이는 네트워크 노드 내에 배치되거나 독립적인 노드가 될 수 있다.

[0063] (1) 그룹 메시지 전송 및 수신

[0064] (A) SCS(30)는 MTC-IWF(21)에 Tsp 인터페이스를 통해 그룹 메시지를 전송한다(단계 S8). 그룹 메시지는 그룹 ID 및 지리 영역 정보(이는 비특허문헌 2에서 설명된다)를 포함한다. 또한, 메시지는 메시지가 그룹 메시지 또는 비 그룹 메시지인지를 나타내는 지시자를 포함한다. 따라서, MTC-IWF(21)는 비 그룹 메시지로부터 그룹 메시지를 구별할 수 있으므로, 다음의 (B)에서 설명한 바와 같이 SCS(30)에 적절한 인가를 수행할 수 있게 된다. 또한, 지시자는 그룹 메시지가 트리거를 포함하고 있는지의 여부를 나타낼 수 있다. 이 경우, MTC-IWF(21)는 또한, 그룹 메시지 또는 비 그룹 메시지로부터 그룹 트리거를 구별할 수 있다.

[0065] (B) MTC-IWF(21)는 타겟 그룹에 그룹 메시지를 보낼 수 있는 지를 알아보기 위해, SCS(30)에 대한 인가를 수행한다(단계 S9). 이는, MTC-IWF(21)가 비 그룹 메시지를 송신할 때 동일한 인가 절차이어야 한다. 인가는 그룹 ID, SCS(30)로부터 수신된 지리 영역 정보, 및 HSS(22)로부터 MTC-IWF(21)에 의해 검색된 인가 데이터의 그룹 정보에 기초한다.

[0066] (C) MTC-IWF(21)는 그룹 GW(50)에 그룹 메시지를 전달한다(단계 S10). 그룹 GW(50)는 하나 초과의 그룹을 소

유할 수 있다. 이는, eNB/MME/MTC-IWF와 같은 소정의 네트워크 노드, 또는 독립적인 노드에 배치된 가상 기능일 수 있다.

[0067] (D) 그룹 GW(50)는 MTC 장치의 타겟 그룹에 그룹 메시지를 방송한다(단계 S12). 그룹 GW(50)가 eNB에 배치된 경우에, 그룹 메시지는 eNB와 MTC 장치 사이에서만 방송된다. 따라서, 코어 네트워크의 혼잡을 회피할 수 있다. 한편, 그룹 GW(50)가 하나 이상의 기지국에 접속된 네트워크 요소들 중 하나로서 기능하는 MME에 배치된 경우에는, 코어 네트워크의 혼잡을 부분적으로 감소시키면서 다수의 영역에 걸쳐 그룹 메시지를 방송할 수 있다.

[0068] (2) 그룹 ID, 그룹 키 관리 및 그룹 메시지 보안

[0069] HSS(22)는 MTC 장치의 그룹에 대한 고유 그룹 ID를 생성한다(단계 S1 및 S3). 단계 S3에서, HSS(22)는 그룹 키를 생성할 수 있다. 코어 네트워크(3GPP 네트워크 도메인)의 외측에 위치되는 SCS(30)에 대해서, 그룹 ID는 SCS(30)에 노출되지 않아야 하므로, HSS(22)는 그룹 ID 및 외부 사용 그룹 ID의 맵핑을 가질 것이다. 내부 사용 그룹 ID는 MTC 장치들(10), 기존 NAS 또는 AS 메시지 내의 그룹 GW(50)에 전송될 수 있다(단계 S4).

[0070] 외부 그룹 ID를 생성하는 두 가지 방법이 있을 수 있다. 이는, HSS(22)에 의해 생성되고 SCS(30)에 제공될 수 있다. 대안적으로, 이는 SCS(30)에 의해 생성되고 HSS(22)에 제공될 수 있다(단계 S2). 어느 쪽이든, HSS는 두 그룹 ID의 맵핑을 생성하게 된다.

[0071] MTC-IWF(21)는 HSS(22)로부터 맵핑을 다운로드하고(단계 S5), 이를 국지적으로 저장한다(단계 S6). 또한, 상기 단계 S10에서 그룹 GW(50)에 그룹 메시지를 전달할 시에, MTC-IWF(21)는 맵핑을 참조하므로, 그룹 메시지 내의 대응하는 내부 그룹 ID에 외부 그룹 ID를 맵핑한다.

[0072] 따라서, 이 예시적인 실시 형태에서, 내부 그룹 ID는 코어 네트워크 외부로부터 숨겨진다. 따라서, 사기성 그룹 메시지가 코어 네트워크에 공격을 일으키는 것을 방지할 수 있다. 또한, 외부 그룹 ID는 단지 소스 인가 후에만 유효하게 된다. 따라서, 외부 그룹 ID가 공격자에게 노출된다 하더라도, 공격을 방지할 수 있다.

[0073] 그룹 메시지가 MTC 장치의 그룹에 방송될 때 보안이 필요하다. 본 실시 형태는 그룹 메시지 기밀성 및 무결성 보호를 위해 그룹 키 쌍을 사용할 것을 제안하고 있다.

[0074] MTC 장치와 그룹 GW가 네트워크와 상호 인증된 후, 그룹 키 관리 및 보안 활성화가 수행되어야 한다(단계 S4). 그룹 키는 MTC 그룹 내의 모든 MTC 장치들이 그룹 키를 갖게 하기 위한 것이다. 이 그룹 키는 그룹 내의 모든 MTC 장치에서 동일하고, 이것은 그들에 의해 그룹 GW(50) 및 선택적으로 그룹 메시지가 전송되는 다른 단부와 공유된다.

[0075] 어느 네트워크 노드가 동일한 그룹 키를 가질 수 있고 어떻게 그룹 메시지가 전송되는 지에 대한 몇 가지 옵션이 있다:

[0076] (A) MTC 장치 - 그룹 GW

[0077] 그룹 GW(50)와 SCS(30) 사이에서 전달되는 그룹 메시지는 IPsec 또는 다른 기존 네트워크 보안 솔루션에 의해 보호될 수 있다. 그룹 GW(50)는 그룹 메시지를 보호하기 위해 그룹 키를 사용하며, 이를 타겟 그룹 MTC 장치들에 방송한다. 단계 S4에서, 그룹 키들이 MTC 장치들과 그룹 GW(50) 사이에서 공유되도록, MTC 장치들 및 그룹 GW(50)는 HSS(22)로부터 그룹 키들을 취득한다.

[0078] (B) MTC 장치 - SCS(단계 S7)

[0079] 이 경우, 그룹 GW(50)는 그룹 메시지를 전달하고 그대로 방송하게 된다. 한편, MTC 장치들은 상기 (A)에서와 같이 그룹 키들을 취득한다. 또한, 인가 후, 그룹 키들이 MTC 장치들과 SCS(30) 사이에서 공유되도록, SCS(30)는, MTC-IWF(21)를 통해 HSS(22)로부터 그룹 키들을 취득한다. 따라서, MTC 장치들과 SCS(30) 사이에 엔드-투-엔드 보안을 제공할 수 있다. MTC 장치는 SCS(30)에 대한 인가를 수행할 수 있다.

[0080] (C) MTC 장치 - 그룹 GW - SCS(단계 S11)

[0081] 이 경우, 그룹 GW(50)와 SCS(30) 사이의 통신은 그룹 키에 의해 보호될 수 있다. 그룹 GW(50)는 그룹 키로 SCS(30)에 대한 인가를 수행할 수 있고, MTC 장치는 인가를 수행할 필요가 없다. 상기 (A)와 (B)에서와 같이, 그룹 키들은 MTC 장치들, 그룹 GW(50)와 SCS(30) 간에 공유된다. 또한, 그룹 GW는 공유된 그룹 키로 그룹 메시지(해독 및 무결성 체크)를 검증하므로, 검증 실패시 그룹 메시지를 폐기한다. 이 경우, 방송 자체를 회피할 수 있다.

[0082] (3) 그룹 ID를 갖거나 갖지 않고 방송될 수 있는 그룹 메시지

[0083] 그룹 ID가 그룹 메시지에 포함되는 경우, MTC 장치는 메시지를 청취하지만, 그것이 갖고 있는 동일한 그룹 ID를 포함하는 메시지만을 수신한 다음, MTC 장치는 무결성 체크를 수행하며 공유된 그룹 키로 메시지를 해독한다(단계 S13 및 S14). 그룹 ID가 MTC 장치 자체에 할당된 그룹 ID와 일치하지 않는 경우, MTC 장치는 그룹 메시지를 폐기한다. 이 경우, MTC 장치는 그룹 메시지를 검증할 필요가 없다. 따라서, MTC 장치에서의 처리 부하를 저감할 수 있다.

[0084] 한편, 그룹 ID가 포함되어 있지 않은 경우, MTC 장치는 모든 방송을 청취하고 무결성 체크 및 복호화를 수행하며 단지 그것이 검증할 수 있는 것에만 응답한다.

[0085] 도 3에 도시된 바와 같이, MTC-IWF(21)는 적어도 수신 유닛(211) 및 판정 유닛(212)을 포함한다. 수신 유닛(211)은, SCS(30) 또는 SME(40)로부터 상기 지시자를 포함하는 그룹 메시지 또는 그룹 트리거를 수신한다. 판정 유닛(211)은, 지시자가 그룹 메시지 또는 그룹 트리거를 나타낼 때, SCS(30) 또는 SME(40)를 인가하기로 결정한다. 이들 유닛(211, 212) 외에, MTC-IWF(21)는 기억 유닛(213), 맵핑 유닛(214) 및 전송 유닛(215)을 포함할 수 있다. 기억 유닛(213)은 상기 맵핑을 저장한다. 맵핑 유닛(214)은 맵핑을 이용하여, 그룹 메시지 또는 그룹 트리거 내의 대응하는 내부 그룹 ID에 외부 그룹 ID를 맵핑한다. 전송 유닛(215)은, 그룹 메시지 또는 그룹 트리거가 MTC 장치들에 방송되도록, MME/SGSN/MSC 중 하나에 그룹 메시지 또는 그룹 트리거를 전송한다. 이들 유닛(211 내지 215)은 버스 등을 통해 상호 연결되어 있다는 점에 유의해야 한다.

[0086] 이들 유닛(211 내지 215)은, 예를 들어, HSS(22)와 각각 통신을 행하는 트랜시버, MME/SGSN/MSC, SCS(30)와 SME(40), 및 도 2의 단계 S5, S6 및 S8 내지 S10에서 도시된 프로세스 또는 이와 동등한 프로세스를 실행하기 위해 이들 트랜시버를 제어하는 제어기에 의해 구성될 수 있다.

[0087] 또한, 도 4에 도시된 바와 같이, MTC 장치(10)의 각각은, 적어도 수신 유닛(101) 및 판정 유닛(102)을 포함한다. 수신 유닛(101)은 코어 네트워크로부터 상술한 그룹 ID를 포함하는 그룹 메시지 또는 그룹 트리거를 수신한다. 판정 유닛(102)은, 그룹 ID가 MTC 장치들(10) 자체의 각각에 대한 그룹 ID와 일치하지 않을 때, 그룹 메시지 또는 그룹 트리거를 폐기하기로 결정한다. 또는 이들 유닛(101 및 102)에 추가하여 대용으로서, MTC 장치(10) 각각은, 취득 유닛(103) 및 통신 유닛(104)을 포함할 수 있다. 취득 유닛(103)은 예를 들어, HSS(20)로부터 그룹 키들을 취득한다. 통신 유닛(104)은 그룹 키들을 이용하여 SCS(30) 또는 SME(40)와 통신한다. 이들 유닛(101 내지 104)은 버스 등을 통해 상호 연결되어 있다는 점에 유의해야 한다.

[0088] 이들 유닛(101 내지 104)은, 예를 들어, RAN을 통해 코어 네트워크와 무선으로 통신을 행하는 트랜시버, 및 도 2의 단계 S4 및 S12 내지 S14에 도시된 프로세스 또는 이와 동등한 프로세스를 실행하기 위해 이러한 트랜시버를 제어하는 제어기에 의해 구성될 수 있다.

[0089] 또한, 도 5에 도시된 바와 같이, 독립적인 노드로서 그룹 GW(50)를 배치하는 경우에, 그룹 GW(50)는 적어도 취득 유닛(501) 및 중계 유닛(502)을 포함한다. 취득 유닛(501)은 예를 들어, HSS(20)로부터 그룹 키들을 취득한다. 중계 유닛(502)은 그룹 키들을 이용하여 그룹 메시지 또는 그룹 트리거를 중계한다. 이들 유닛(501 및 502)은 버스 등을 통해 상호 연결되어 있다는 점에 유의해야 한다.

[0090] 이들 유닛(501 및 502)은 예를 들어, MTC-IWF(21)와 각각 통신을 행하는 트랜시버, HSS(22)와 MME/SGSN/MSC/RAN, 및 도 2의 단계 S4 및 S10 내지 S12에서 도시된 프로세스 또는 이와 동등한 프로세스를 실행하기 위해 이들 트랜시버를 제어하는 제어기에 의해 구성될 수 있다.

[0091] 도시는 생략하지만, SCS(30) 및 SME(40)의 각각은, 각각의 전형적인 SCS 및 SME에 탑재된 기능에 부가하여, 그룹 메시지 또는 그룹 트리거 내에 상기 지시자를 포함하는 기능, 그룹 메시지 또는 그룹 트리거 내에 상기 그룹 ID를 포함하는 기능, 및 상기 그룹 키들을 이용하여 MTC 장치들의 그룹과 통신하는 기능 중 적어도 하나를 포함한다.

[0092] 본 발명은 상기 실시 형태에 한정되는 것은 아니고, 다양한 변형이 특허 청구 범위에 기초하여 당업자에 의해 이루어질 수 있음이 명백하다는 점에 유의해야 한다.

[0093] 상기 개시된 실시 형태들의 전부 또는 일부가, 이에 제한되는 것은 아니지만, 다음의 추가 사항으로 설명될 수 있다.

[0094] (부기 1)

[0095] HSS 등의 네트워크 노드는 각각의 그룹에 대한 고유 내부 사용 그룹 ID를 생성한다.

[0096] (부기 2)

[0097] HSS는 모든 MTC 장치의 그룹 멤버와 그룹 GW에 그룹 ID를 전송한다. 그룹 GW는 네트워크 노드에 배치된 기능이거나 독립적 노드일 수 있다.

[0098] (부기 3)

[0099] 외부 그룹 ID와 고유 내부 사용 그룹 ID에 대한 맵핑:

[0100] HSS는 네트워크 내에서만 사용되는 고유 그룹 ID 및 외부 그룹 ID의 맵핑을 유지한다. 외부 그룹 ID는 그룹이 가입하는 HSS에 의해 또는 SCS에 의해 할당될 수 있다.

[0101] (부기 4)

[0102] MTC-IWF는 인터페이스 S6m를 통해 그룹 ID 맵핑을 다운로드하고, 이를 국부적으로 저장한다. 신규성은 인터페이스의 변형이다.

[0103] (부기 5)

[0104] 암호화 및 무결성 보호를 위한 그룹 키 쌍이 생성된다. 그룹 키 쌍은 그룹 내의 모든 MTC 장치에 대해 동일하다. 그룹 GW 및/또는 SCS는 동일한 그룹 키를 가질 수 있다.

[0105] (부기 6)

[0106] 그룹 메시지 내의 지시자는, 네트워크 엔티티, 예를 들어 MTC-IWF가 다른 비-그룹 메시지로부터 구별할 수 있게 한다. 지시자는 IWF가 비-트리거 그룹 메시지로부터 그룹 트리거 메시지를 구별하게 한다. 이는, MTC-IWF가 적절한 인가를 수행하는 데 도움이 된다.

[0107] (부기 7)

[0108] 그룹 GW는 MTC 장치의 그룹에 그룹 메시지를 방송하고, 적절한 MTC 장치만이 그룹 메시지를 수신하고 판독할 수 있도록, 그룹 키 쌍에 의해 보호된다.

[0109] (부기 8)

[0110] 그룹 메시지는 하기의 두 가지 방법 중 하나로 방송될 수 있다:

[0111] (A) 그룹 ID를 포함한다: MTC 장치가 방송 중인 그룹 ID를 체크하고, 그것이 그가 보유하는 그룹 ID와 동일한 경우, 무결성 체크를 수행하고, (그룹 ID 관련) 그룹 키를 이용하여 메시지를 해독한다.

[0112] (B) 그룹 ID를 포함하지 않는다: MTC 장치는 단지 모든 방송 메시지를 그것의 그룹 키로 체크한다.

[0113] 이러한 애플리케이션은 2012년 6월 29일에 출원된 일본 특허 출원 제 2012-147983호에 기초하여 우선권을 주장하며, 그 개시 내용은 참고 문헌으로 본원에 인용된다.

부호의 설명

[0114] 10: MTC 장치

21: MTC-IWF

22: HSS

30: SCS

40: SME

50: 그룹 GW

101, 211: 수신 유닛

102, 212: 판정 유닛

103, 501: 취득 유닛

104: 통신 유닛

213: 기억 유닛

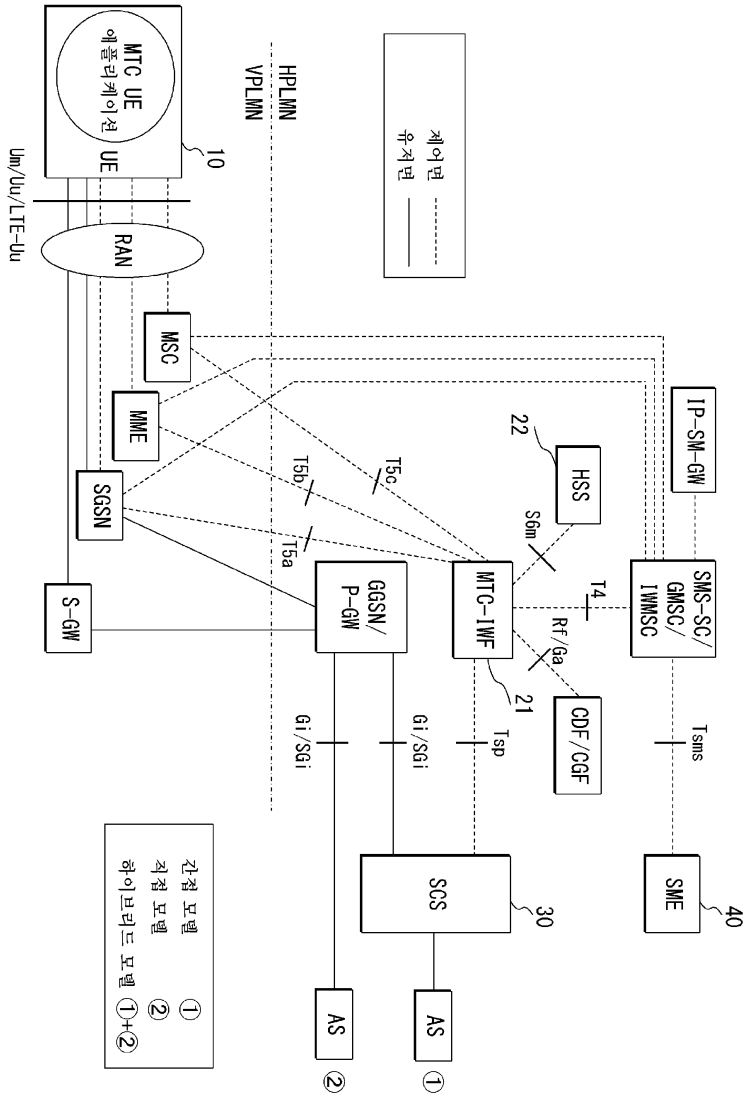
214: 맵핑 유닛

215: 전송 유닛

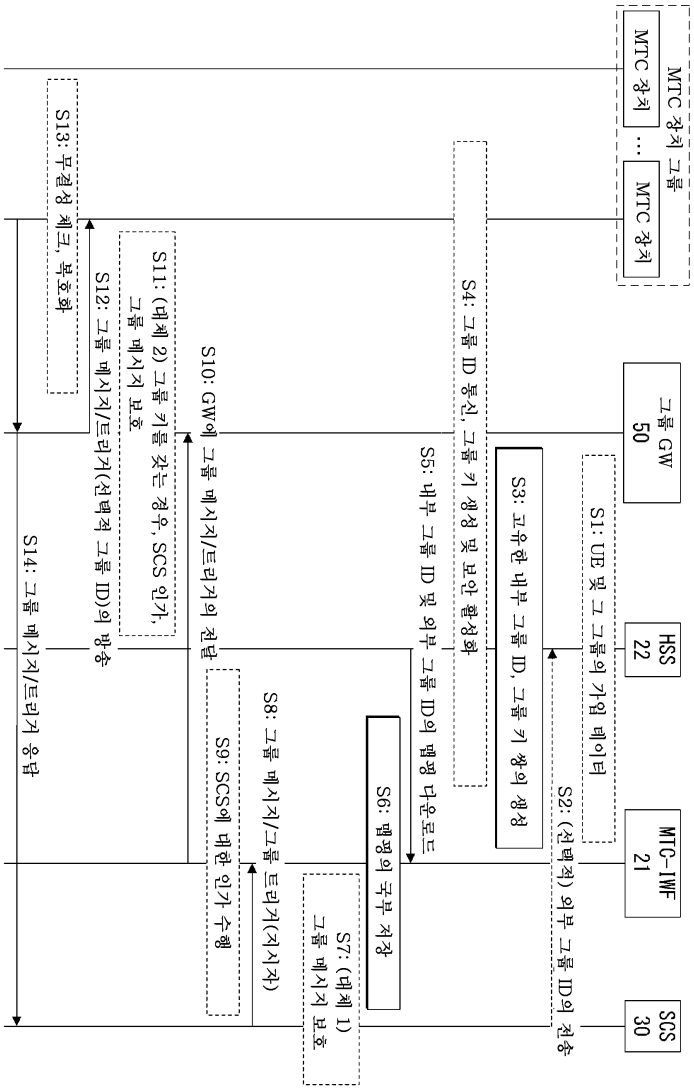
502: 중계 유닛

도면

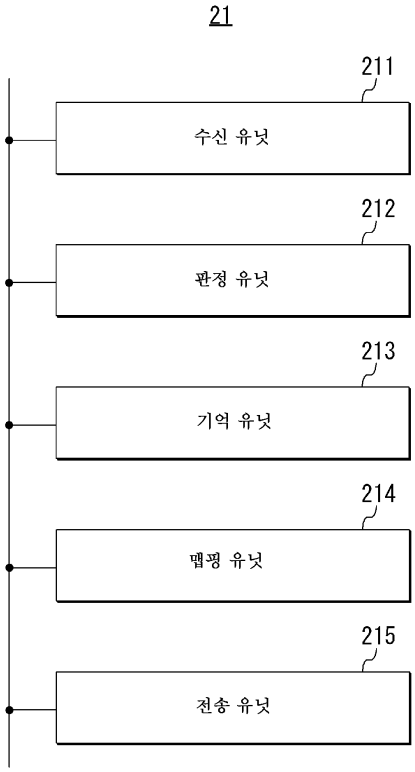
도면1



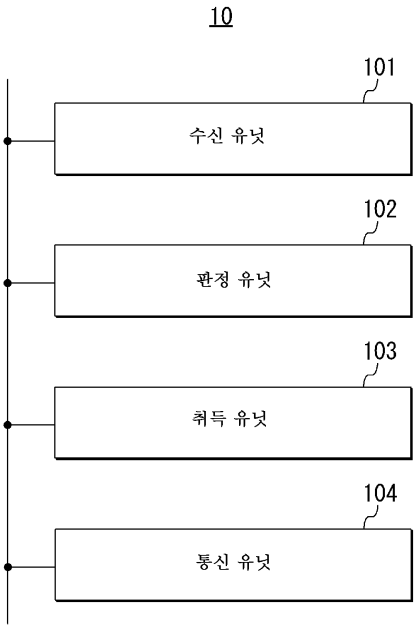
도면2


MTC 장치 그룹
MTC 장치
MTC 장치
그룹 GW 50
HSS 22
MTC-IWF 21
SCS 30
S1: UE 및 그 그룹의 가입 데이터
S2: (선택적) 외부 그룹 ID의 전송
S3: 고유한 내부 그룹 ID, 그룹 키 쌍의 생성
S4: 그룹 ID 통신, 그룹 키 생성 및 보안 활성화
S5: 내부 그룹 ID 및 외부 그룹 ID의 맵핑 다운로드
S6: 맵핑의 국부 저장
S7: (대체 1) 그룹 메시지 보호
S8: 그룹 메시지/그룹 트리거(지시자)
S9: SCS에 대한 인가 수행
S10: GW에 그룹 메시지/트리거의 전달
S11: (대체 2) 그룹 키를 갖는 경우, SCS 인가, 그룹 메시지 보호
S12: 그룹 메시지/트리거(선택적 그룹 ID)의 방송
S13: 무결성 체크, 복호화
S14: 그룹 메시지/트리거 응답

도면3


21
211
수신 유닛
212
판정 유닛
213
기억 유닛
214
맵핑 유닛
215
전송 유닛

도면4


10
101
수신 유닛
102
판정 유닛
103
취득 유닛
104
통신 유닛

도면5