(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107786966 B
(45)授权公告日 2020.11.03

(21)申请号 201711098437.3
(22)申请日 2013.04.19
(65)同一申请的已公布的文献号
申请公布号 CN 107786966 A
(43)申请公布日 2018.03.09
(30)优先权数据
2012-147983 2012.06.29 JP
(62)分案原申请数据
201380034460.X 2013.04.19
(73)专利权人 日本电气株式会社
地址 日本东京
(72)发明人 张晓维
阿南德·罗迦沃·普拉萨德
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 孙志湧 穆德骏
(51)Int.Cl.
H04W 4/70(2018.01)
H04W 4/08(2009.01)
H04W 12/08(2009.01)
H04L 29/06(2006.01)

(56)对比文件
US 2011243261 A1,2011.10.06
CN 102804882 A,2012.11.28
WO 2012064932 A1,2012.05.18
WO 2011087826 A1,2011.07.21
US 2012064932 A1,2012.03.15
WO 2012018130 A1,2012.02.09
3GPP Organizational Partners.Architecture enhancements to facilitate communications with packet data networks and applications.《3GPP Technical Specification》.2012,第1页-第27页.
3rdGeneration Partnership Project.System Improvements for Machine-Type Communications.《3GPP Technical Specification》.2012,第1页-第165页.

审查员 杨露

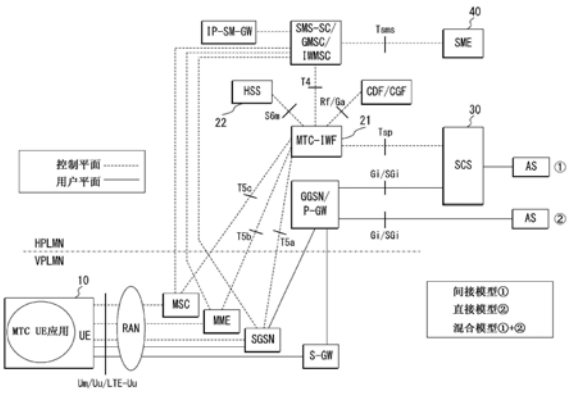
权利要求书3页 说明书8页 附图4页

(54)发明名称

用于M2M中的基于组的特征的安全性的更新

(57)摘要

一种用于移动通信的系统,包括:形成组的多个UE;RAN(无线接入网络);SCS(服务能力服务器);第一节点;以及第二节点;其中,所述SCS将包括外部组ID的消息发送到所述第一节点,所述第一节点检验所述SCS被授权以发送所述消息,所述第一节点将内部组ID发送到所述第二节点,以及所述第二节点经由所述RAN将组消息广播到位于特定地理区域中的所述多个UE。



CN 107786966 B

1.一种移动通信系统,包括:

形成组的多个设备;

SCS(服务能力服务器);

第一节点;以及

第二节点;

其中:

所述SCS将组消息发送到所述第一节点,所述组消息包括外部组ID和识别所述组消息的信息,

所述第一节点检验所述SCS被授权以发送所述组消息,

在将所述组消息转发到所述第二节点时,所述第一节点将所述外部组ID映射到所述组消息中的相应内部组ID,

所述第二节点将所转发的组消息广播到所述多个设备的目标组,以及

所述多个设备中的每个接收所述组消息中的所述内部组ID。

2.根据权利要求1所述的移动通信系统,其中,所述第一节点存储所述内部组ID和所述外部组ID之间的所述映射。

3.根据权利要求1所述的移动通信系统,其中,所述外部组ID在所述SCS和HSS(归属订户服务器)之间的接口上使用。

4.根据权利要求1所述的移动通信系统,其中,所述组消息包括地理区域信息。

5.一种移动通信系统的方法,所述移动通信系统包括形成组的多个设备、SCS(服务能力服务器)、第一节点、以及第二节点,所述方法包括:

将组消息从所述SCS发送到所述第一节点,所述组消息包括外部组ID和识别所述组消息的信息;

由所述第一节点检验所述SCS被授权以发送所述组消息;

在将所述组消息转发到所述第二节点时,由所述第一节点将所述外部组ID映射到所述组消息中的相应内部组ID;

将所转发的组消息从所述第二节点广播到所述多个设备的目标组;以及

由所述多个设备中的每个接收所述组消息中的所述内部组ID。

6.一种移动通信系统中的第一节点,所述移动通信系统包括形成组的多个设备、SCS(服务能力服务器)、以及第二节点,所述第一节点包括:

接收器,所述接收器被配置为从所述SCS接收组消息,所述组消息包括外部组ID和识别所述组消息的信息;

控制器,所述控制器被配置为检验所述SCS被授权以发送所述组消息;以及

发射器,所述发射器被配置为将所述组消息转发到所述第二节点,

其中,在转发到所述第二节点时,所述控制器将所述外部组ID映射到所述组消息中的相应内部组ID,

所述第二节点将所转发的组消息广播到所述多个设备的目标组,以及

所述多个设备中的每个接收所述组消息中的所述内部组ID。

7.根据权利要求6所述的第一节点,其中,所述第一节点存储所述内部组ID和所述外部组ID之间的所述映射。

8.根据权利要求6所述的第一节点,其中,所述外部组ID在所述SCS和HSS(归属订户服务器)之间的接口上使用。

9.根据权利要求6所述的第一节点,其中,所述组消息包括地理区域信息。

10.一种移动通信系统中的第一节点的方法,所述移动通信系统包括形成组的多个设备、SCS(服务能力服务器)、以及第二节点,所述方法包括:

从所述SCS接收组消息,所述组消息包括外部组ID和识别所述组消息的信息;

检验所述SCS被授权以发送所述组消息;以及

将所述组消息转发到所述第二节点,

其中,在转发到所述第二节点时,将所述外部组ID映射到所述组消息中的相应内部组ID,

所述第二节点将所转发的组消息广播到所述多个设备的目标组,以及

所述多个设备中的每个接收所述组消息中的所述内部组ID。

11.移动通信系统中的多个设备,所述移动通信系统包括SCS(服务能力服务器)、第一节点、以及第二节点,所述多个设备包括:

控制器,所述控制器被配置为形成组;

接收器,所述接收器被配置为从所述第二节点接收组消息,

其中:

所述SCS将所述组消息发送到所述第一节点,所述组消息包括外部组ID和识别所述组消息的信息,

所述第一节点检验所述SCS被授权以发送所述组消息,

在将所述组消息转发到所述第二节点时,所述第一节点将所述外部组ID映射到所述组消息中的相应内部组ID,

所述第二节点将所转发的组消息广播到所述多个设备的目标组,以及

所述多个设备中的每个接收所述组消息中的所述内部组ID。

12.根据权利要求11所述的多个设备,其中,所述第一节点存储所述内部组ID和所述外部组ID之间的所述映射。

13.根据权利要求11所述的多个设备,其中,所述外部组ID在所述SCS和HSS(归属订户服务器)之间的接口上使用。

14.根据权利要求11所述的多个设备,其中,所述组消息包括地理区域信息。

15.一种移动通信系统中的形成组的多个设备的方法,所述移动通信系统包括SCS(服务能力服务器)、第一节点、以及第二节点,所述方法包括:

形成组;以及

从所述第二节点接收组消息,

其中:

所述SCS将所述组消息发送到所述第一节点,所述组消息包括外部组ID和识别所述组消息的信息,

所述第一节点检验所述SCS被授权以发送所述组消息,

在将所述组消息转发到所述第二节点之后,所述第一节点将所述外部组ID映射到所述组消息中的相应内部组ID,

所述第二节点将所转发的组消息广播到所述多个设备的目标组,以及

所述多个设备中的每个接收所述组消息中的所述内部组ID。

用于M2M中的基于组的特征的安全性的更新

[0001] 本申请是于2014年12月26日进入中国国家阶段的、PCT申请号为PCT/JP2013/002661、国际申请日为2013年4月19日、中国申请号为201380034460.X、发明名称为“用于M2M中的基于组的特征的安全性的更新”的申请的分案申请。

技术领域

[0002] 本发明涉及用于具有在NPL 1中新提供的架构的基于组的机器类通信(MTC)的安全性解决方案。该解决方案可以支持MTC-IWF(MTC-互通功能),以当从其发送组消息时,执行对SCS(服务能力服务器)的适当授权。本发明还涉及安全地递送和广播组消息的机制。

背景技术

[0003] 在3GPP版本12中发起了基于组的特征的研究(参见例如NPL2),并且在NPL 1中研究了新架构。通过本申请的发明人在PTL 1中提出的组网关(GW)的概念,本发明在新架构中对其进行扩展。

[0004] SCS将组消息发送到MTC-IWF的网络节点,并且MTC-IWF将组消息转发到MTC设备的目标组。该消息针对多于一个的MTC设备,并且可以触发这些设备与网络进行通信。

[0005] 引用列表

[0006] 专利文献

[0007] PTL1:国际专利公开No.WO2012/018130

[0008] 非专利文献

[0009] NPL1:3GPP TS23.682,"Architecture enhancements to facilitate communications with packet data networks and applications(Release 11)",v11.1.0,2012-06

[0010] NPL 2:3GPP TR 23.8xy,"Machine-Type and other Mobile Data Applications Communications Enhancements;(Release 12)",V0.1.0,2012-05

[0011] NPL 3:3GPP TR 33.868,"Security aspects of Machine-Type Communications;(Release 11)",v0.8.0

发明内容

[0012] 技术问题

[0013] 然而,本申请的发明人已经发现了下述问题:欺诈组消息可能导致对网络的DoS(拒绝服务)攻击。注意,在NPL3中描述的对MTC设备的攻击在此也有效。

[0014] 因此,MTC-IWF应当执行SCS授权,以查看具体地当消息包含触发时,其是否可以发送组消息。

[0015] 对问题的解决方案

[0016] 为了解决上述问题,根据本发明的第一示例性方面的网络节点位于核心网内。该网络节点包括:接收装置,用于从位于核心网外的发射源接收消息,该消息包括指示消息是

否被寻址到附连到核心网的一个或多个MTC(机器类通信)设备组的指示符;以及确定装置,用于当指示符指示消息被寻址到该组时,确定对发射源进行授权。

[0017] 而且,根据本发明的第二示例性方面的方法提供了一种控制位于核心网内的网络节点的方法。该方法包括:从位于核心网外的发射源接收消息,该消息包括指示消息是否被寻址到附连到核心网的一个或多个MTC设备组的指示符;以及当指示符指示该消息被寻址到该组时,确定对发射源进行授权。

[0018] 而且,根据本发明的第三示例性方面的MTC设备包括:接收装置,用于从核心网接收消息,该消息包括用于识别消息是否被寻址到一个或多个MTC设备组的ID(标识符);以及确定装置,用于当ID与分配用于MTC设备本身的ID不一致时,确定丢弃该消息。

[0019] 而且,根据本发明的第四示例性方面的方法提供了一种控制附连到核心网的MTC设备的方法。该方法包括:从核心网接收消息,该消息包括用于识别消息是否被寻址到一个或多个MTC设备组的ID;以及当ID与分配用于MTC设备本身的ID不一致时,确定丢弃该消息。

[0020] 而且,根据本发明的第五示例性方面的网关将来自位于核心网外的消息的发射源的消息中继到附连至核心网的一个或多个MTC设备组。该网关包括:获取装置,用于获取用于该MTC设备组的组密钥对,以与发射源安全地进行通信;以及中继装置,用于通过使用组密钥来中继该消息。

[0021] 而且,根据本发明的第六示例性方面的MTC设备包括:获取装置,用于获取用于与位于核心网外的发射源安全地进行通信的组密钥对,并且发射寻址到一个或多个MTC设备组的消息;以及通信装置,用于通过使用组密钥与发射源进行通信。

[0022] 而且,根据本发明的第七示例性方面的方法提供了一种控制将来自位于核心网外的消息的发射源的消息中继到附连到核心网的一个或多个MTC设备组的方法。该方法包括:获取用于该MTC设备组的组密钥对,以与发射源安全地进行通信;以及通过使用组密钥来中继该消息。

[0023] 而且,根据本发明的第八示例性方面的方法提供了一种控制附连到核心网的MTC(机器类通信)设备的方法。该方法包括:获取用于与位于核心网外的发射源安全地进行通信的组密钥对,并且发射寻址到一个或多个MTC设备组的消息;以及通过使用组密钥与发射源进行通信。

[0024] 本发明的有益效果

[0025] 根据本发明,特别是当消息包含触发时,能够执行SCS授权以查看其是否可以发送组消息。

附图说明

[0026] 图1是示出根据本发明的示例性实施例的系统架构的示例的框图。

[0027] 图2是示出根据本发明的示例性实施例的在系统中的MTC设备处终止的组消息的示例的序列图。

[0028] 图3是示出根据本发明的示例性实施例所放置的网络节点的配置示例的框图。

[0029] 图4是示出根据本发明的示例性实施例的MTC设备的配置示例的框图。

[0030] 图5是示出根据本发明的示例性实施例的网关的配置示例的框图。

具体实施方式

[0031] 1.讨论

[0032] SA2已经开始了对TR 23.8xy v0.1.0"Machine-Type and other Mobile Data Applications Communications Enhancements(Release 12)"中的基于组的特征的研究。SA3应当根据SA2提供的架构需要来研究用于版本12的安全性问题。

[0033] 以下给出用于来自SA2的基于组的消息的架构要求：

[0034] -网络将提供用于将组消息从SCS分配给位于特定地理区域中的MTC组的那些成员的机制。

[0035] -基于组的消息收发特征将不需要用于不使用该特征的UE的附加新功能。

[0036] -系统将支持使用基于组的消息收发特征的UE可以有效地识别寻址到UE的所分配的组消息的机制。

[0037] -系统将提供使SCS发送组消息的接口。该接口应当能够承载以下信息：

[0038] -组消息的应用层内容，

[0039] -期望组消息用于的组标识，以及

[0040] -组消息应当被分配的地理区域和RAT。

[0041] -针对从对分配的组消息进行响应的设备得到的负载来保护系统。

[0042] -将在GERAN、UTRAN和E-UTRAN接入中支持基于组的消息收发。

[0043] 根据当前架构，可以假设MTC-IWF从SCS接收组消息，并且将其转发到MTC设备的目标组。

[0044] 通过组消息，可以触发多个MTC设备来进行响应。因此，与对单个MTC设备的触发可能导致的问题相比，未授权的组消息可能产生更严重的问题。如MitM攻击和重放攻击的被认为用于非组消息的其他处理在此还应用放大效果。因此

[0045] -网络将执行SCS是否可以将组消息发送到目标组的授权。为此，MTC-IWF应该能够使组消息与其他消息进行区分。

[0046] -组消息应该具有机密性和完整性保护，并且接收该消息的MTC设备应该能够对其进行验证。

[0047] -网络应该提供使位于3GPP网络外的用于SCS的装置与目标组进行通信的装置。当SCS发送组消息时，使用组标识。类似于UE标识，在3GPP网络中使用的组标识将不通过外部接口被发送，并且不由3GPP网络外的节点所知。这适用于位于3GPP网络外的SCS。

[0048] 通过以上分析，对基于MTC组的特征的安全性要求如下推断：

[0049] -MTC-IWF将验证SCS是否被授权以将组消息发送到给定MTC组。

[0050] -MTC-IWF将能够使组(触发)消息与其他消息区分。

[0051] -分配给MTC设备组的组消息应该具有机密性、完整性保护和中继保护。

[0052] -接收组消息的MTC设备应该能够验证组消息是否是从授权的SCS发送的。

[0053] -组ID应该被暴露于位于3GPP网络外的节点。这还包括在3GPP网络外的SCS。

[0054] 2.建议

[0055] 我们建议SA3

[0056] 1)研究用于基于组的特征的处理和安全性要求

[0057] 2)包括以上在用于版本12的TR 33.868中的分析和安全性要求，以下在单独pCR中

给出。

[0058] 5.x关键问题-基于组的消息收发

[0059] 5.x.1问题细节

[0060] SA2开始研究TR 23.8xy(版本12)中的基于组的特征。根据当前架构,可以假设MTC-IWF从SCS接收组消息,并且将其转发到MTC设备的目标组。

[0061] 5.x.2处理

[0062] 通过组消息,可以触发多个MTC设备来进行响应。因此,与对单个MTC设备的触发可能导致的相比,未授权的组消息可能导致严重得多的问题。如MitM攻击和重放攻击的被认为用于非组消息的其他处理在此还可以应用放大效果。

[0063] 5.x.3安全性要求

[0064] -MTC-IWF应该验证SCS是否被授权以将组消息发送到给定MTC组。

[0065] -MTC-IWF应该能够使组(触发)消息与其他消息区分。

[0066] -分配给MTC设备组的组消息应该具有机密性、完整性保护和重放保护。

[0067] -接收组消息的MTC设备应当能够验证组消息是否从授权SCS被发送。

[0068] -组ID应该不被暴露于位于3GPP网络外的节点。这还包括在3GPP网络外的SCS。

[0069] 此后,将参考图1至图5描述本发明的示例性实施例。

[0070] 如图1中所示,根据该示例性实施例的系统包括核心网(3GPP网络)、通过RAN(无线接入网)连接至核心网的多个MTC设备10、以及用作位于核心网外的组触发源或组消息的SCS 30和SME(短消息实体)40。注意,RAN由多个基站(即,eNB(演进的节点B))形成。

[0071] 其中,每个MTC设备10都是用于MTC经由Um/Uu/LTE-Uu接口连接至核心网的UE。UE可以托管一个或多个MTC应用。外部网络中的相应MTC应用被托管在一个或多个AS(应用服务器)上。

[0072] 而且,SCS 30和SME 40连接到核心网,以与MTC设备10进行通信。

[0073] 而且,核心网包括HPLMN(本地公用陆地移动网)中的MTC-IWF21和HSS(归属订户服务器)22。在核心网中,MTC-IWF 21用作从其发射源接收组消息或组触发的网络节点。通常,MTC-IWF 21接收还可以作为经由Tsp接口的来自SCS 30或者经由T4和Tsms接口的来自SME 40的组消息,并且将组消息转发至MME(移动管理实体)、SGSN(服务GPRS(通用分组无线电服务)支持节点)或MSC(移动交换中心),其用作经由T5b/T5a/T5c接口将组消息转发到MTC设备10的网络元件,使得组消息或组触发可以被路由到MTC设备10。HSS 22或MTC-IWF 21可以创建并且存储内部和外部组ID的映射,并且HSS22生成组密钥对(随后将描述)。组密钥中的一个被生成用于加密和解密,并且另一个被生成用于完整性保护。

[0074] 接下来,将参考图2详细地描述本示例性实施例的操作示例。图2示出了发送到MTC设备组的组消息的消息序列。在MTC设备组中存在多于一个的设备。

[0075] 在该示例性实施例中,假设在组GW(随后将描述)和网络以及组GW和MTC设备10之间已经执行了相互认证。注意,在PTL 1的单独发明中提出了一种网关,该网关负责接收组消息并且将组消息发送到MTC设备,并且发送用于与网络或SCS进行通信的MTC设备的级联消息。该示例性实施例提出了用于网关的一些新功能,并且其可以被部署在网络节点中或者是独立节点。

[0076] (1)组消息发送和接收

[0077] (A)SCS 30通过Tsp接口将组消息发送到MTC-IWF 21(步骤S8)。组消息包含组ID和地理区域信息(这在NPL 2中进行了描述)。另外,该消息包括指示消息是组消息还是非组消息的指示符。因此,MTC-IWF 21可以使组消息与非组消息相区分,由此能够执行对SCS 30的适当授权,如在以下(B)中描述的。而且,指示符可以指示组消息是否包含触发。在该情况下,MTC-IWF 21还可以使组触发与组消息或非组消息相区分。

[0078] (B)MTC-IWF 21执行对SCS 30的授权,以查看其是否可以将组消息发送到目标组(步骤S9)。这在MTC-IWF 21发送非组消息时应当是相同的授权过程。授权基于组ID、从SCS 30接收到的地理区域信息和由MTC-IWF 21从HSS 22检索到的授权数据的组信息。

[0079] (C)MTC-IWF 21将组消息转发至组GW 50(步骤S10)。组GW 50可以拥有多于一个的组。其可以是部署在如eNB/MME/MTC-IWF的任何网络节点上的虚拟功能或者独立节点。

[0080] (D)组GW 50将组消息广播至MTC设备的目标组(步骤S12)。在组GW 50被部署在eNB上的情况下,组消息仅在eNB和MTC设备之间广播。因此,能够避免核心网的拥塞。另一方面,在组GW 50被部署在用作连接到一个或多个基站的网络元件中的一个的MME上的情况下,能够通过多个区域来广播组消息,同时部分地减少核心网的拥塞。

[0081] (2)组ID、组密钥管理和组消息安全性

[0082] HSS 22生成用于该MTC设备组的唯一组ID(步骤S1和S3)。在步骤S3处,HSS 22可以生成组密钥。对于位于核心网(3GPP网络域)外的SCS 30,组ID不应该被暴露于SCS 30,由此HSS 22将具有组ID和外部使用组ID的映射。内部使用组ID可以被发送至现有NAS或AS消息内的组GW 50、MTC设备10(步骤S4)。

[0083] 可以存在生成外部组ID的两种方法。其可以通过HSS来创建,并且被提供给SCS 30。替代地,其可以由SCS 30创建,并且被提供给HSS 22(步骤S2)。以任何一种方法,HSS都将创建两个组ID的映射。

[0084] MTC-IWF 21从HSS 22下载映射(步骤S5),并且将其存储在本地(步骤S6)。而且,当在上述步骤S10处将组消息转发到组GW 50时,MTC-IWF 21参考映射,由此将外部组ID映射到组消息中的相应内部组ID。

[0085] 因此,在该示例性实施例中,内部组ID向核心网外隐藏。因此,能够防止欺诈组消息产生对核心网的攻击。而且,在源授权之后,仅使得外部组ID有效。因此,即使外部组ID被暴露于攻击者,也能够防止攻击。

[0086] 当组消息被广播到该MTC设备组时,需要安全性。该示例性实施例建议使用组密钥对以用于组消息机密性和完整性保护。

[0087] 在MTC设备和组GW与网络相互认证之后,应当执行组密钥管理和安全性激活(步骤S4)。组密钥用于MTC组中的所有MTC设备以具有组密钥。该组密钥对于组中的所有MTC设备均是相同的,并且其由它们与组GW 50并且可以选地与发送组消息的其他终端共享。

[0088] 存在网络节点可以具有相同组密钥和组消息如何被发送的几个选择:

[0089] (A)MTC设备-组GW

[0090] 在组GW 50和SCS 30之间传送的组消息可以由IPsec或其他现有网络安全性解决方案来保护。组GW 50使用组密钥来保护组消息,并且将其广播到目标组MTC设备。在步骤S4处,MTC设备和组GW 50从HSS 22获取组密钥,使得组密钥在MTC设备和组GW 50之间共享。

[0091] (B)MTC设备-SCS(步骤S7)

[0092] 在该情况下,组GW 50将转发组消息并且按原样广播组消息。另一方面,MTC设备如上述(A)那样获取组密钥。而且,在授权之后,SCS 30通过MTC-IWF 21从HSS 22获取组密钥,使得组密钥在MTC设备和SCS 30之间共享。因此,能够在MTC设备和SCS 30之间提供端到端安全性。MTC设备可以执行对SCS 30的授权。

[0093] (C)MTC设备-组GW-SCS(步骤S11)

[0094] 在该情况下,组GW 50和SCS 30之间的通信可以通过组密钥来保护。组GW 50可以通过组密钥执行对SCS 30的授权,并且MTC设备不需要执行授权。如上述(A)和(B)那样,组密钥在MTC设备、组GW 50和SCS 30之间共享。而且,组GW通过共享的组密钥来验证组消息(解密和完整性检验),由此当验证失败时,丢弃组消息。在该情况下,能够避免广播其本身。

[0095] (3)可以通过或不通过组ID广播的组消息

[0096] 当组ID被包括在组消息中时,MTC设备侦听该消息,但是仅接收包含与其具有的相同组ID的消息,然后MTC设备执行完整性检验,并且通过共享的组密钥来解密该消息(步骤S13和S14)。当组ID与被分配用于MTC设备本身的组ID不一致时,MTC设备丢弃该组消息。在该情况下,MTC设备不需要验证组消息。因此,能够减少MTC设备上的处理负载。

[0097] 另一方面,当不包括组ID时,MTC设备侦听所有广播,并且执行完整性检验和解密,并且仅响应其可以验证的广播。

[0098] 如图3中所示,MTC-IWF 21至少包括接收单元11和确定单元212。接收单元211从SCS 30或SME 40接收包括上述指示符的组消息或组触发。当指示符指示组消息或组触发时,确定单元211确定授权SCS 30或SME 40。除了这些单元211和212之外,MTC-IWF 21可以包括存储单元213、映射单元214以及转发单元215。存储单元213存储上述映射。映射单元214通过使用映射将外部组ID映射到组消息或组触发中的相应内部组ID。转发单元215将组消息或组触发转发到MME/SGSN/MSC中的一个,使得组消息或组触发被广播到MTC设备。注意,这些单元211至215通过总线等彼此连接。

[0099] 这些单元211至215可以通过例如分别与HSS 22、MME/SGSN/MSC、SCS 30和SME 40进行通信的收发器、以及控制这些收发器执行在图2中的步骤S5、S6和S8至S10处所示的处理或者与其等效的处理的控制器来配置。

[0100] 而且,如图4中所示,MTC设备10中的每一个都至少包括接收单元101和确定单元102。接收单元101从核心网接收包括上述组ID的组消息或者组触发。当组ID与用于MTC设备10本身中的每一个的组ID不一致时,确定单元102确定丢弃组消息或组触发。代替或者除了这些单元101和102之外,MTC设备10中的每一个可以包括获取单元103和通信单元104。获取单元103从例如HSS 20获取组密钥。通信单元104通过使用组密钥与SCS 30或SME 40进行通信。注意,这些单元101至104通过总线等彼此连接。

[0101] 这些单元101至104可以通过例如通过RAN与核心网无线地进行通信的收发器、以及控制该收发器执行图2中的步骤S4和S12至S14处所示的处理或者等效于其的处理的控制器来配置。

[0102] 而且,如图5中所示,在将组GW 50部署为独立节点的情况下,组GW 50至少包括获取单元501和中继单元502。获取单元501从例如HSS 20获取组密钥。中继单元502通过使用组密钥来中继组消息或组触发。注意,这些单元501和502通过总线等彼此连接。

[0103] 这些单元501和502可以通过例如分别与MTC-IWF 21、HSS 22和MME/SGSN/MSC/RAN

进行通信的收发器、以及控制这些收发器执行图2中的步骤S4和S10至S12处所示的处理或等效于其的处理的控制器来配置。

[0104] 虽然说明被省略，但是除了安装在典型的SCS和SME中的每一个上的功能之外，SCS 30和SME 40中的每一个都包括将上述指示符包括在组消息或组触发中的功能、将上述组ID包括在组消息或组触发中的功能、以及通过上述组密钥与该MTC设备组进行通信的功能中的至少一个。

[0105] 注意，本发明不限于上述示例性实施例，并且明显地，各种修改可以基于权利要求的叙述由本领域技术人员作出。

[0106] 以上公开的整个或部分示例性实施例可以被描述为但不限于以下补充注释。

[0107] (补充注释1)

[0108] 诸如HSS的网络节点针对每个组创建唯一内部使用组ID。

[0109] (补充注释2)

[0110] HSS将组ID发送至MTC设备的所有组成员和组GW。组GW可以是部署在网络节点中的功能或者是独立节点。

[0111] (补充注释3)

[0112] 外部组ID以及其对唯一内部使用组ID的映射：

[0113] HSS保持外部组ID和仅在网络中使用的唯一组ID的映射。外部组ID可以通过HSS或者通过组订阅的SCS来分配。

[0114] (补充注释4)

[0115] MTC-IWF经由接口S6m下载组ID映射，并且将其存储在本地。新颖性是接口的修改。

[0116] (补充注释5)

[0117] 生成用于加密和完整性保护的组密钥对。对于组内的所有MTC设备，该组密钥对是相同的。组GW和/或SCS可以具有相同的组密钥。

[0118] (补充注释6)

[0119] 组消息中的指示符使得例如MTC-IWF的网路实体可以使其与其他非组消息相区分。指示符使IWF区分组触发消息与非触发组消息。这有助于MTC-IWF执行适当的授权。

[0120] (补充注释7)

[0121] 组GW将组消息广播到该MTC设备组，其由组密钥对来保护，使得仅适当的MTC设备可以接收并且读取组消息。

[0122] (补充注释8)

[0123] 组消息可以以如下所示的两种方式中的一个来进行广播：

[0124] (A)包含组ID:MTC设备检验广播中的组ID，如果广播中的组ID与其保持的组ID相同，则将使用(组ID相关)组密钥来执行完整性检验并且解密该消息。

[0125] (B)不包含组ID:MTC设备通过其组密钥检验所有广播消息。

[0126] 本申请基于并且要求于2012年6月29日提交的日本专利申请No.2012-147983的优先权的权益，其公开通过引用合并于此。

[0127] 附图标记列表

[0128] 10 MTC设备

[0129] 21 MTC-IWF

[0130] 22 HSS

[0131] 30 SCS

[0132] 40 SME

[0133] 50 组GW

[0134] 101、211 接收单元

[0135] 102、212 确定单元

[0136] 103、501 获取单元

[0137] 104 通信单元

[0138] 213 存储单元

[0139] 214 映射单元

[0140] 215 转发单元

[0141] 502 中继单元

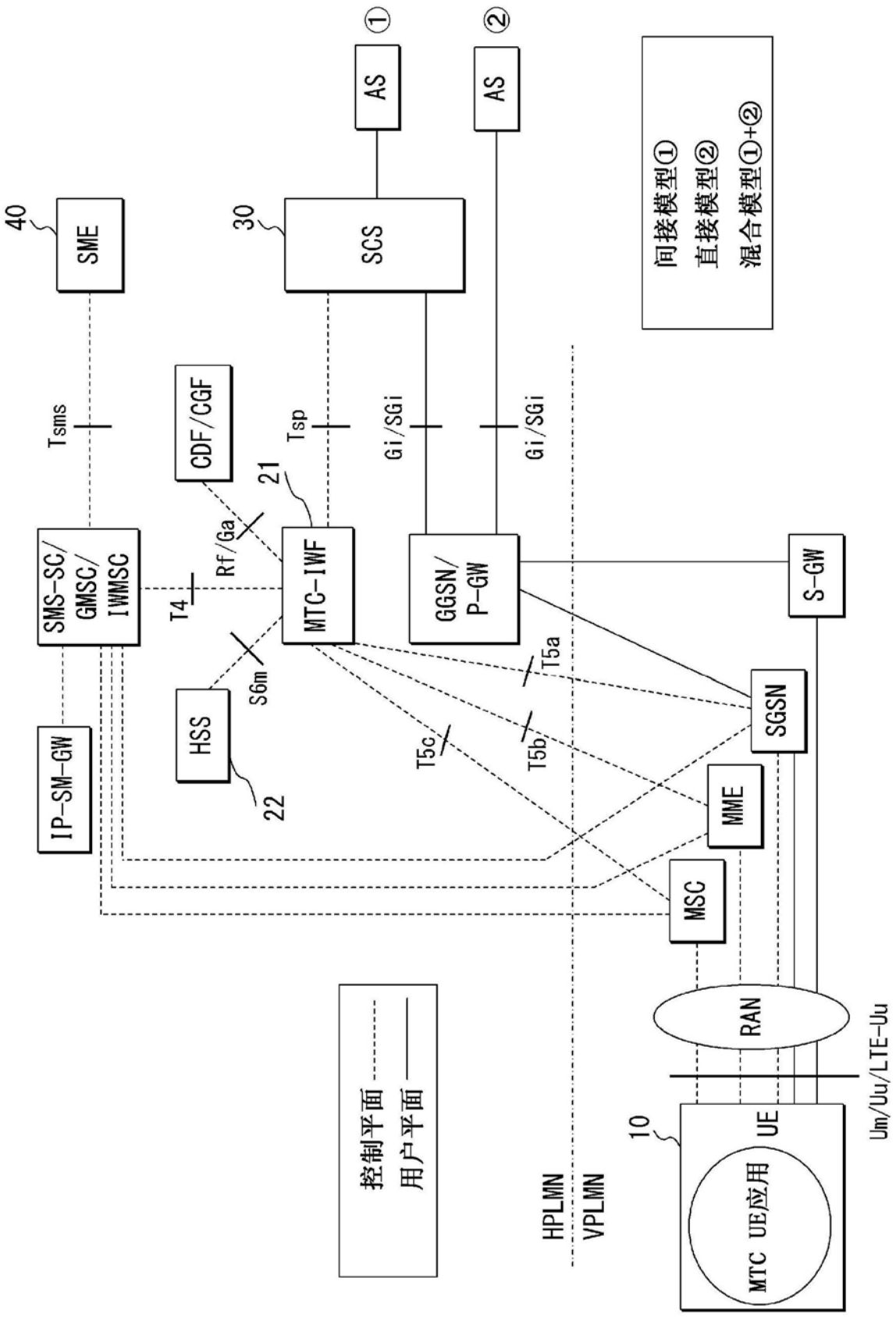

①
②
AS
AS
40
SME
30
SCS
间接模型①
直接模型②
混合模型①+②
Tsms
CDF/CGF
Tsp
Gi/SGi
Gi/SGi
21
SMS-SC/
GMSC/
IWMSC
Rf/Ga
T4
MTC-IWF
GGSN/
P-GW
S-GW
S6m
T5a
HSS
22
T5c
T5b
SGSN
IP-SM-GW
MME
MSC
RAN
Um/Uu/LTE-Uu
10
UE
MTC UE应用
控制平面
用户平面
HPLMN
VPLMN

图1

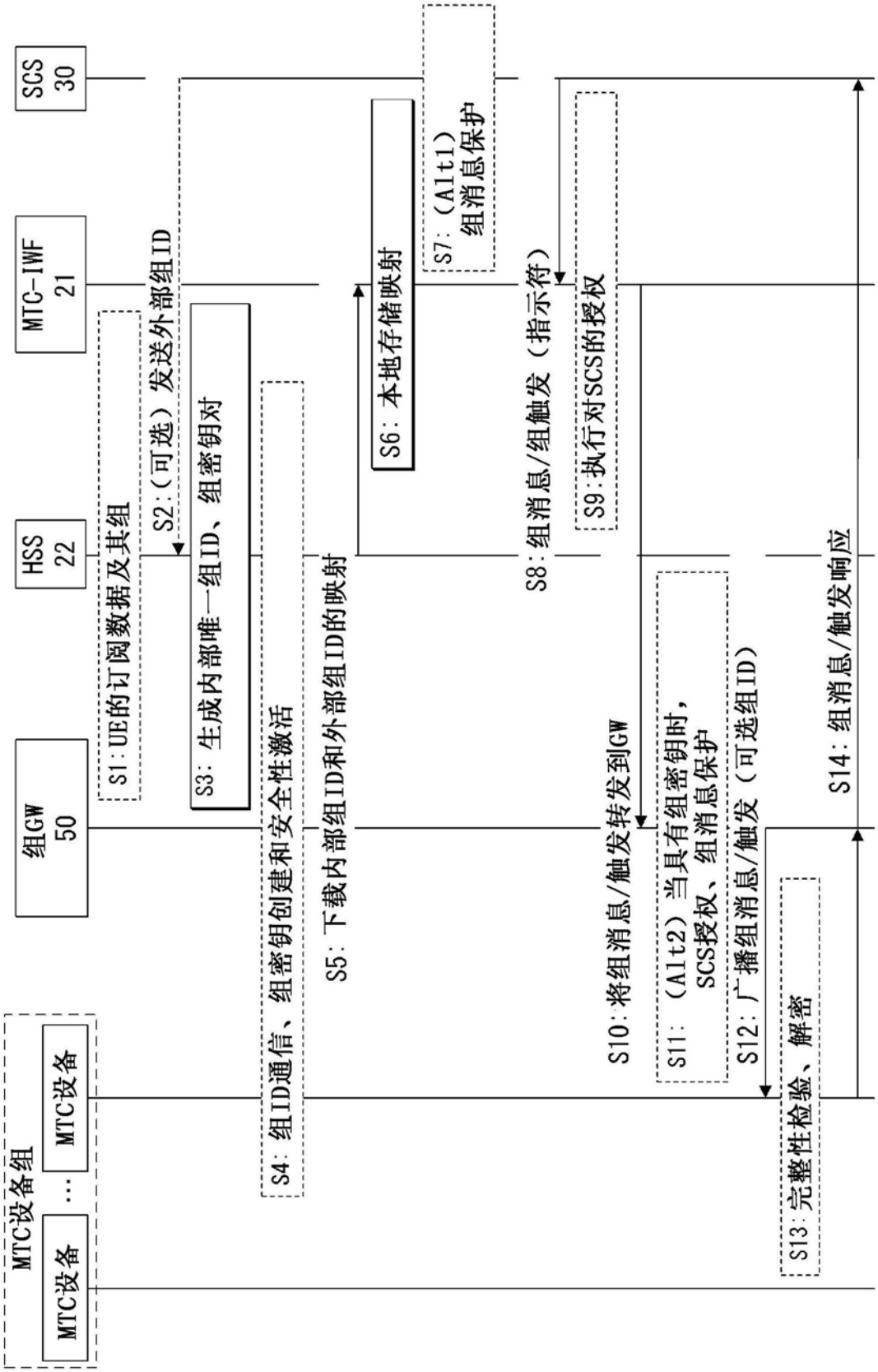

MTC设备组
MTC设备
…
MTC设备
组GW
50
HSS
22
MTC-IWF
21
SCS
30
S1:UE的订阅数据及其组
S2:(可选)发送外部组ID
S3: 生成内部唯一组ID、组密钥对
S4: 组ID通信、组密钥创建和安全性激活
S5: 下载内部组ID和外部组ID的映射
S6: 本地存储映射
S7: (A1t1)
组消息保护
S8:组消息/组触发(指示符)
S9:执行对SCS的授权
S10:将组消息/触发转发到GW
S11: (A1t2)当具有组密钥时,
SCS授权、组消息保护
S12:广播组消息/触发(可选组ID)
S13:完整性检验、解密
S14: 组消息/触发响应

图2

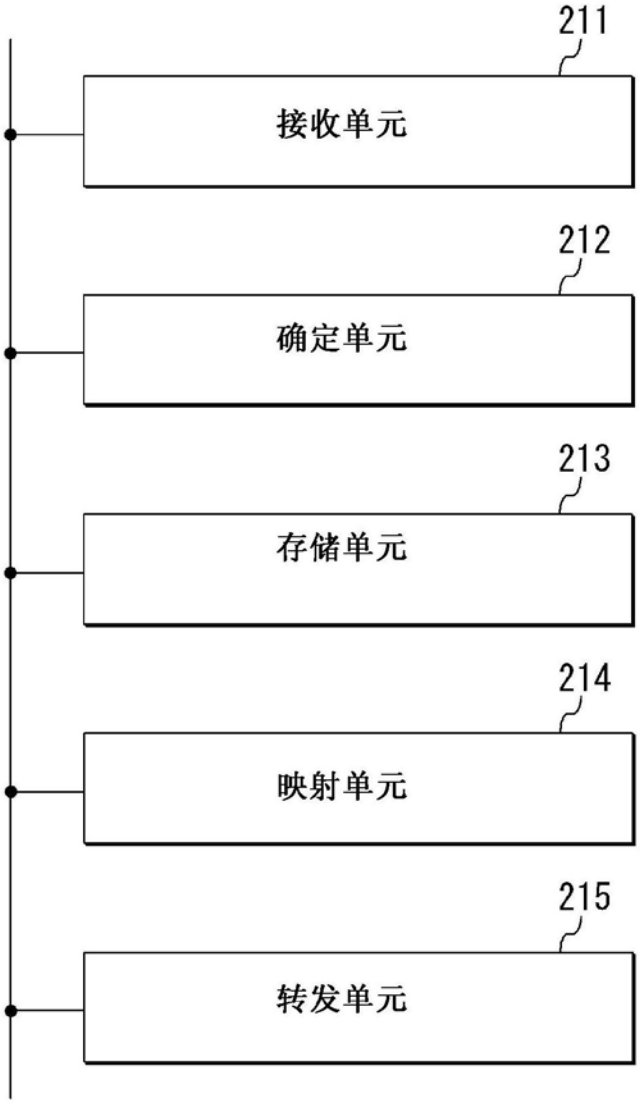


图3

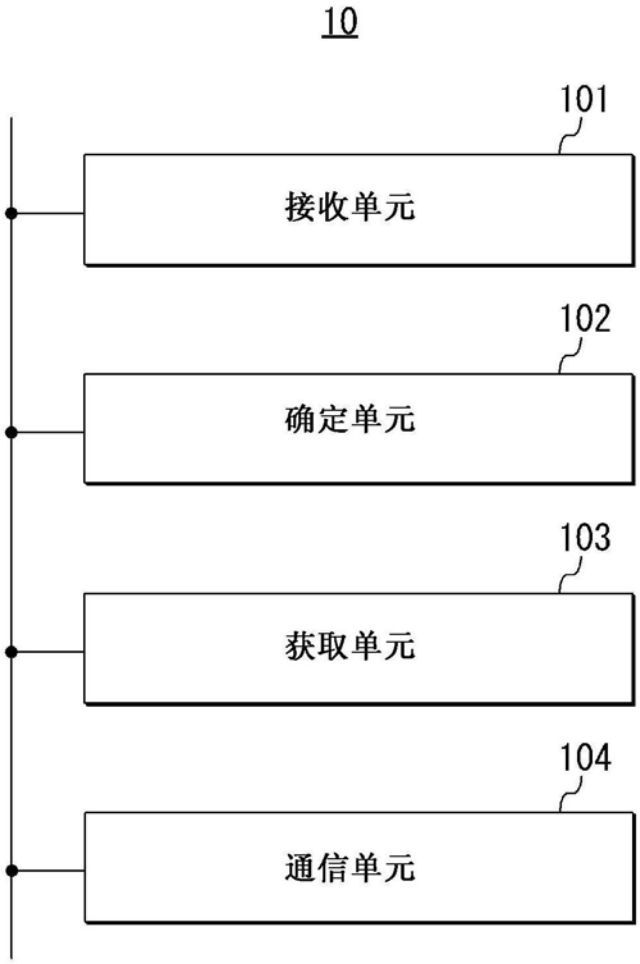


图4

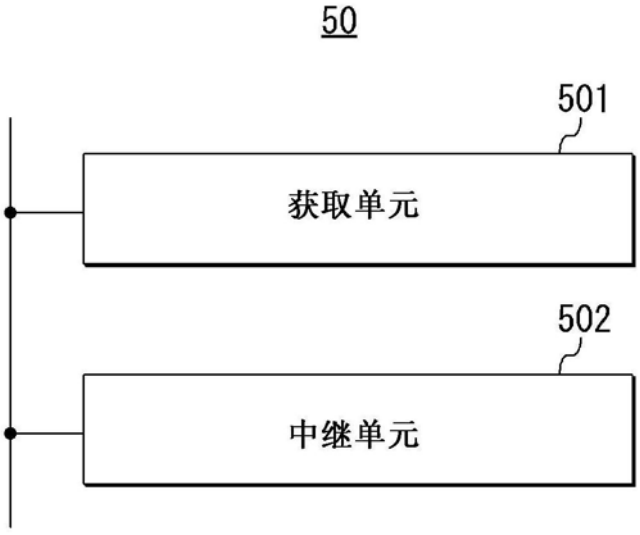


图5