(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104704790 A
(43)申请公布日 2015.06.10

(21)申请号 201380046867.4
(22)申请日 2013.09.12
(30)优先权数据
2012-201693 2012.09.13 JP
(85)PCT国际申请进入国家阶段日
2015.03.09
(86)PCT国际申请的申请数据
PCT/JP2013/005398 2013.09.12
(87)PCT国际申请的公布数据
WO2014/041806 EN 2014.03.20
(71)申请人 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 李兰 孙志湧
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/04(2006.01)

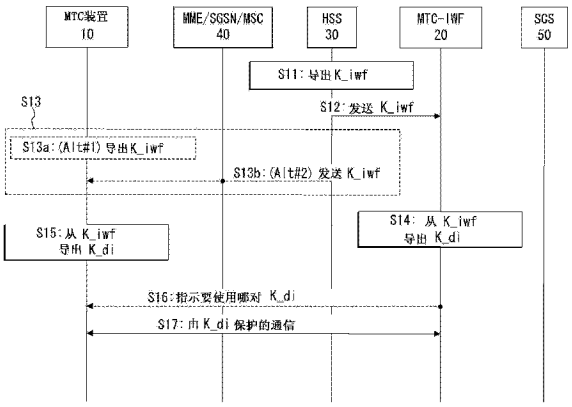
权利要求书4页 说明书6页 附图7页

(54)发明名称

机器型通信系统中的密钥管理

(57)摘要

MTC装置(10)和MTC交互工作功能MTC-IWF(20)形成通信系统，并且彼此进行通信。在该通信系统中，在MTC装置(10)和MTC-IWF(20)之间安全地共享根密钥(K_iwf)。MTC装置(10)和MTC-IWF(20)使用根密钥(K_iwf)来分别导出用于保护通信的临时密钥(K_di(K_di_conf，K_di_int))。临时密钥提供完整性保护和保密性。根密钥可以被HSS或ME/SGSN/MSC导出，并且被提供到MTC-IWF。MTC-IWF也可以基于所接收的密钥导出处理来导出根密钥。所述的系统有益于在MTC系统中的小数据发送的安全性。



CN 104704790 A

1. 一种通信系统，包括：

MTC（机器型通信）装置；以及

MTC-IWF(MTC 交互工作功能)，所述 MTC-IWF(MTC 交互工作功能）与所述 MTC 装置进行通信，

其中，在所述 MTC 装置和所述 MTC-IWF 之间安全地共享根密钥，并且

其中，所述 MTC 装置和所述 MTC-IWF 使用所述根密钥来分别导出用于保护在所述 MTC 装置和所述 MTC-IWF 之间的所述通信的临时密钥。

2. 根据权利要求 1 所述的通信系统，其中，所述临时密钥包括用于在所述 MTC 装置和所述 MTC-IWF 之间传送的消息的完整性保护和完整性检查中的至少一个的完整性密钥。

3. 根据权利要求 2 所述的通信系统，其中，所述 MTC 装置通过使用所述完整性密钥来执行所述消息的完整性保护和完整性检查中的至少一个，并且根据所述完整性检查的结果来执行 MTC-IWF 授权。

4. 根据权利要求 1 至 3 中的任何一项所述的通信系统，其中，所述临时密钥包括保密性密钥，所述保密性密钥用于加密和解密在所述 MTC 装置和所述 MTC-IWF 之间传送的消息。

5. 根据权利要求 1 至 4 中的任何一项所述的通信系统，其中，通过位于所述 MTC 装置所附接到的核心网络内的不同网络实体来进行所述通信。

6. 根据权利要求 1 至 5 中的任何一项所述的通信系统，

其中，以下述方式来执行根密钥的所述共享：

所述 MTC-IWF 接收由位于所述 MTC 装置所附接到的核心网络内布置的不同网络实体导出的根密钥；并且

所述 MTC 装置通过所述 MTC 装置本身导出根密钥，或者在所述 MTC 装置和不同的网络实体之间建立 NAS 和 / 或 AS 安全上下文之后接收来自所述不同的网络实体的所导出的临时密钥。

7. 根据权利要求 1 至 5 中的任何一项所述的通信系统，

其中，以下述方式来执行根密钥的所述共享：

所述 MTC-IWF 从位于所述 MTC 装置所附接到的核心网络内的不同网络实体接收材料，并且通过使用所述材料来导出根密钥；并且

所述 MTC 装置通过所述 MTC 装置本身来导出根密钥。

8. 根据权利要求 6 或 7 所述的通信系统，其中，所述不同的网络实体包括 HSS（归属订户服务器）。

9. 根据权利要求 6 或 7 所述的通信系统，其中，所述不同的网络实体包括 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）。

10. 根据权利要求 1 至 5 中的任何一项所述的通信系统，其中，以下述方式来执行根密钥的所述共享：所述 MTC-IWF 和所述 MTC 装置共享公共值，并且独立地通过使用所述公共值来导出根密钥。

11. 一种 MTC-IWF(MTC 交互工作功能)，包括：

通信部件，所述通信部件用于与 MTC（机器型通信）装置进行通信；

共享部件，所述共享部件用于与所述 MTC 装置安全地共享根密钥；以及

导出部件，所述导出部件用于通过使用所述根密钥来导出用于保护在所述 MTC 装置和

所述 MTC-IWF 之间的所述通信的临时密钥。

12. 根据权利要求 11 所述的 MTC-IWF，其中，所述导出部件被配置为导出用于从所述 MTC 装置接收的消息的完整性保护和完整性检查中的至少一个的完整性密钥作为所述临时密钥中的一个。

13. 根据权利要求 11 或 12 所述的 MTC-IWF，其中，所述导出部件被配置为导出用于加密要向所述 MTC 装置发送的消息并且用于加密从所述 MTC 装置接收的消息的保密性密钥作为所述临时密钥中的一个。

14. 根据权利要求 11 至 13 中的任何一项所述的 MTC-IWF，其中，所述通信部件被配置为通过位于所述 MTC 装置所附接到的核心网络内的不同网络实体来进行所述通信。

15. 根据权利要求 11 至 14 中的任何一项所述的 MTC-IWF，其中，所述共享部件被配置为接收由位于所述 MTC 装置所附接到的核心网络内的不同网络实体导出的根密钥。

16. 根据权利要求 11 至 14 中的任何一项所述的 MTC-IWF，其中，所述共享部件被配置为：

从位于所述 MTC 装置所附接到的核心网络内的不同网络实体接收材料；并且

通过使用所述材料来导出根密钥。

17. 根据权利要求 11 至 14 中的任何一项所述的 MTC-IWF，其中，所述共享部件被配置为：

与所述 MTC 装置共享公共值；并且

使用所述公共值来导出根密钥。

18. 一种 MTC（机器型通信）装置，包括：

通信部件，所述通信部件用于与 MTC-IWF(MTC 交互工作功能）进行通信；

共享部件，所述共享部件用于与所述 MTC-IWF 安全地共享根密钥；以及

导出部件，所述导出部件用于通过使用所述根密钥来导出用于保护在所述 MTC 装置和所述 MTC-IWF 之间的所述通信的临时密钥。

19. 根据权利要求 18 所述的 MTC 装置，其中，所述导出部件被配置为导出用于从所述 MTC-IWF 接收的消息的完整性保护和完整性检查中的至少一个的完整性密钥作为所述临时密钥中的一个。

20. 根据权利要求 19 所述的 MTC 装置，进一步包括：

通过使用所述完整性密钥对于所述消息的完整性保护和完整性检查中的至少一个的授权部件，并且用于根据所述检查的结果来授权所述 MTC-IWF。

21. 根据权利要求 18 至 20 中的任何一项所述的 MTC 装置，其中，所述导出部件被配置为导出保密性密钥作为所述临时密钥中的一个，所述保密性密钥用于加密要向所述 MTC-IWF 发送的消息，并且用于解密从所述 MTC-IWF 接收的消息。

22. 根据权利要求 18 至 21 中的任何一项所述的 MTC 装置，其中，所述通信部件被配置为通过位于所述 MTC 装置所附接到的核心网络内的不同网络实体来进行所述通信。

23. 根据权利要求 18 至 22 中的任何一项所述的 MTC 装置，其中，所述共享部件被配置为，在所述 MTC 装置和所述不同网络实体之间建立 NAS 和 / 或 AS 安全上下文之后，通过位于所述 MTC 装置所附接到的核心网络内布置的不同网络实体来接收根密钥。

24. 根据权利要求 18 至 22 中的任何一项所述的 MTC 装置，其中，所述共享部件被配置

为：

与所述 MTC-IWF 共享公共值；并且

通过使用所述公共值来导出根密钥。

25. 一种网络实体，所述网络实体位于 MTC（机器型通信）装置所附接到的核心网络内，所述网络实体包括：

导出部件，所述导出组件用于导出根密钥；以及

发送部件，所述发送部件用于向与所述 MTC 装置进行通信的 MTC-IWF（MTC 交互工作功能）发送所述根密钥。

26. 根据权利要求 25 所述的网络实体，其中，所述发送部件被配置为在所述 MTC 装置和所述网络实体之间建立 NAS（非接入层）和 / 或 AS（接入层）安全上下文之后，进一步向所述 MTC 装置发送所述根密钥。

27. 一种网络实体，所述网络实体位于 MTC（机器型通信）装置所附接到的核心网络内，所述网络实体包括：

发送部件，所述发送部件用于向与所述 MTC 装置进行通信的 MTC-IWF（MTC 交互工作功能）发送使所述 MTC-IWF 导出根密钥的材料。

28. 根据权利要求 25 至 27 中的任何一项所述的网络实体，包括 HSS（归属订户服务器）。

29. 根据权利要求 25 至 27 中的任何一项所述的网络实体，包括 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）。

30. 一种控制 MTC-IWF（MTC 交互工作功能）中的操作的方法，所述方法包括：

与 MTC（机器型通信）装置进行通信；

与所述 MTC 装置安全地共享根密钥；以及

通过使用所述根密钥来导出用于保护在所述 MTC 装置和所述 MTC-IWF 之间的所述通信的临时密钥。

31. 一种控制在 MTC（机器型通信）装置中的操作的方法，所述方法包括：

与 MTC-IWF（MTC 交互工作功能）进行通信；

与所述 MTC-IWF 安全地共享根密钥；以及

通过使用所述根密钥来导出用于保护在所述 MTC 装置和所述 MTC-IWF 之间的所述通信的临时密钥。

32. 一种控制位于 MTC（机器型通信）装置所附接到的核心网络内的网络实体中的操作的方法，所述方法包括：

导出根密钥；以及

向与所述 MTC 装置进行通信的 MTC-IWF（MTC 交互工作功能）发送所述根密钥。

33. 根据权利要求 32 所述的方法，进一步包括：

在所述 MTC 装置和所述网络实体之间建立 NAS（非接入层）和 / 或 AS（接入层）安全上下文之后，向所述 MTC 装置发送所述根密钥。

34. 一种控制位于 MTC（机器型通信）装置所附接到的核心网络内的网络实体中的操作的方法，所述方法包括：

向与所述 MTC 装置进行通信的 MTC-IWF（MTC 交互工作功能）发送使所述 MTC-IWF 导出

根密钥的材料。

机器型通信系统中的密钥管理

技术领域

[0001] 本发明涉及在MTC(机器型通信)系统中的密钥管理。

背景技术

[0002] 如在NPL 1中所述,应当研究在MTC装置和MTC-IWF(MTC交互工作功能)之间的接口上的安全。然而,还没有完成该研究。当前,没有在3GPP(第三代合作伙伴极化)SA3中的MTC装置和MTC-IWF之间的接口上的安全解决方案。

[0003] 引用列表

[0004] 非专利文献

[0005] 非专利文献1:3GPP TR 33.868,"Security aspects of Machine-Type Communications;(Release 11)",v0.9.0,2012-07,Clause 4

发明内容

[0006] 技术问题

[0007] 如上所述,在MTC装置和MTC-IWF之间要求安全的通信。

[0008] MTC-IWF支持授权SCS(服务能力服务器)和授权来自包括触发器的SCS的控制平面请求。MTC-IWF也向MTC装置传递来自SCS的消息(例如,触发消息)。在中间的人和重放攻击可能在MTC装置和MTC-IWF之间的接口上发生。而且,MME(移动性管理实体)不必具有关于SCS和它转发的消息内容的了解。因此,合理的是,具有在MTC装置和MTC-IWF之间的端到端安全性。

[0009] 对于问题的解决方案

[0010] 为了解决上述问题,根据本发明的第一示例性方面的一种通信系统包括:MTC装置;以及,与所述MTC装置进行通信的MTC-IWF。在该系统中,在所述MTC装置和所述MTC-IWF之间安全地共享根密钥。所述MTC装置和所述MTC-IWF使用所述根密钥来分别导出用于保护所述通信的临时密钥。

[0011] 而且,根据本发明的第二示例性方面的一种MTC-IWF包括:通信部件,用于与MTC装置进行通信;共享部件,用于与所述MTC装置安全地共享根密钥;以及,导出部件,用于通过使用所述根密钥来导出临时密钥以保护所述通信。

[0012] 而且,根据本发明的第三示例性方面的一种MTC装置包括:通信部件,用于与MTC-IWF进行通信;共享部件,用于与所述MTC-IWF安全地共享根密钥;以及,导出部件,用于通过使用所述根密钥来导出临时密钥以保护所述通信。

[0013] 而且,根据本发明的第四示例性方面的一种网络实体被布置在MTC装置所附接到的核心网络内。该网络实体包括:导出部件,用于导出根密钥;以及,发送部件,向与所述MTC装置进行通信的MTC-IWF发送所述根密钥。

[0014] 而且,根据本发明的第五示例性方面的一种网络实体被布置在MTC装置所附接到的核心网络内。该网络实体包括发送部件,向与所述MTC装置进行通信的MTC-IWF发送用

于所述 MTC-IWF 导出根密钥的材料。

[0015] 而且，根据本发明的第六示例性方面的一种方法提供了一种控制在 MTC-IWF 中的操作的方法。该方法包括：与 MTC 装置进行通信；与所述 MTC 装置安全地共享根密钥；以及，通过使用所述根密钥来导出临时密钥以用于保护所述通信。

[0016] 而且，根据本发明的第七示例性方面的一种方法提供了一种控制在 MTC 装置中的操作的方法。该方法包括：与 MTC-IWF 进行通信；与所述 MTC-IWF 安全地共享根密钥；并且，通过使用所述根密钥来导出临时密钥以用于保护所述通信。

[0017] 而且，根据本发明的第八示例性方面的一种方法提供了一种控制在 MTC 装置所附接到的核心网络内布置的网络实体中的操作的方法。该方法包括：导出根密钥；并且，向与所述 MTC 装置进行通信的 MTC-IWF 发送所述根密钥。

[0018] 而且，根据权利要求的第九示例性方面的一种方法提供了一种控制在 MTC 装置所附接到的核心网络内布置的网络实体中的操作的方法。该方法包括：向与所述 MTC 装置进行通信的 MTC-IWF 发送用于所述 MTC-IWF 导出根密钥的材料。

[0019] 本发明的有益效果

[0020] 根据本发明，有可能解决上述问题，使得例如，可以实现下面的效果 (1) 至 (3)。

[0021] (1) 可以通过使用所提出的密钥保护在 MTC-IWF 和 UE（用户设备）之间的消息来提供端到端安全。

[0022] (2)UE 可以使用所提出的密钥通过从 MTC-IWF 发送的消息的完整性检查来执行 MTC-IWF 授权。

[0023] (3) 消息可以是服务节点 (MME/SGSN/MSC) 独立的。可以向 UE 传递从 MTC-IWF 发送的消息，甚至因为 UE 移动性或网络故障而改变服务节点。UE 不必再一次执行源认证和授权

附图说明

[0024] 图 1 是示出根据本发明的一个示例性实施例的通信系统的配置示例的框图。

[0025] 图 2 是示出根据所述示例性实施例的系统系统中的密钥分级的框图。

[0026] 图 3 是示出根据所述示例性实施例的通信系统的第一操作示例的时序图。

[0027] 图 4 是示出根据所述示例性实施例的通信系统的第二操作示例的时序图。

[0028] 图 5 是示出根据所述示例性实施例的通信系统的第三操作示例的时序图。

[0029] 图 6 是示出根据所述示例性实施例的 MTC-IWF 的配置示例的框图。

[0030] 图 7 是示出根据所述示例性实施例的 MTC 装置的配置示例的框图。

[0031] 图 8 是示出根据示例性实施例的网络实体的配置示例的框图。

具体实施方式

[0032] 以下，将参考图 1 至 8 来描述本发明的示例性实施例。

[0033] 如图 1 中所示，根据这个示例性实施例的通信系统包括核心网络 (3GPP 网络）和通过 RAN（无线电接入网）连接到核心网络的一个或多个 MTC 装置 10。注意，在这个示例性实施例中，MTC 装置的定义遵循在 NPL 1 中的那个：“MTC 装置是被配备用于机器型通信的 UE”。虽然省略了图示，但是 RAN 由多个校正（即，eNB（演进节点 B））形成。

[0034] MTC 装置 10 附接到核心网络。MTC 装置 10 可以容纳一个或多个 MTC 应用。在外部网络中的对应的 MTC 应用被容纳在一个或多个 AS(应用服务器)上。

[0035] 而且,核心网络包括 MTC-IWF 20。MTC-IWF 20 作为网络实体,其中继在 MTC 装置 10 和 SCS 50 之间的消息,SCS 50 连接到核心网络以与 MTC 装置 10 进行通信。核心网络包括作为其他网络实体的 HSS(归属订户服务器)30、MME、SGSN(服务 GPRS(通用分组无线电服务)支持节点)和 MSC(移动交换中心)等。在下面的说明中,有时将 MME、SGSN 和 MSC 称为"MME/SGSN/MSC",并且被符号 40 集体表示。通过 MME/SGSN/MSC 40 来进行在 MTC 装置 10 和 MTC-IWF 20 之间的通信。

[0036] 而且,对于这个示例性实施例作出几个假设如下:

[0037] -UE(MTC 装置 10)和核心网络(HSS 30、MME/SGSN/MSC40)已经相互认证。

[0038] -在 HSS 30、MME/SGSN/MSC 40 和 MTC-IWF 20 之间建立安全关联。

[0039] 本示例性实施例建议导出和分配 MTC-IWF 20 和 UE(MTC 装置 10)彼此共享的密钥。密钥用于在 MTC-IWF 20 和 UE(MTC 装置 10)之间的通信的保密性和完整性保护。

[0040] 具体地说,如图 2 中所示,本示例性实施例提出具有根密钥和临时密钥的密钥分级。根密钥 K_iwf 用于导出一对临时密钥 K_di(K_di_conf,K_di_int)。K_di_conf 是用于加密和解密在 MTC 装置 10 和 MTC-IWF 20 之间传送的消息的保密密钥。K_di_int 是用于保护和查看在 MTC 装置 10 和 MTC-IWF 20 之间传送的消息的完整性的完整性密钥。

[0041] 临时密钥的使用是因为对于临时密钥的任何攻击不导致在分级中的较高级处的临时密钥的折中,使得可以使用根密钥来重新导出新的密钥,该新的密钥继而减轻由折中的较低层密钥产生的问题。

[0042] 而且,MTC 装置 10 可以根据完整性检查的结果来授权 MTC-IWF20。具体地说,MTC 装置 10 当在完整性检查中成功时将 MTC-IWF 20 授权为真实的一个。在该情况下,有可能防止 MTC 装置 10 与伪装为真实者的 MTC-IWF 进行通信,即使当 MTC 装置 10 连接到假网络时。优选的是,这些完整性检查和认证被应用到漫游的 UE/MTC 装置。

[0043] 接下来,将详细描述这个示例性实施例的操作示例。

[0044] [1]. 根密钥 K_iwf 的导出和分配

[0045] HSS 30、MME/SGSN/MSC 40 或 MTC-IWF 20 可以导出 K_iwf。在图 3、4 和 5 中示出三种情况。

[0046] 可以以下面给出的两种方式来进行密钥分发。

[0047] (1) 分布式

[0048] (A) 如果未通过 MTC-IWF 20 本身导出根密钥,则给出的网络实体(HSS 30 或 MME/SGSN/MSC 40)向 MTC-IWF 发送密钥,并且

[0049] (B)UE。

[0050] 注意,被发送到 UE 的密钥应当在在 MTC 装置 10 和网络(HSS 30 和 MME/SGSN/MSC 40)之间建立安全后,并且应当使用有效的安全上下文来保护该密钥。

[0051] (2) 同步

[0052] (A) 给定的网络实体(HSS 30 或 MME/SGSN/MSC 40)向 MTC-IWF 20 发送密钥,或者,MTC-IWF 20 本身导出根密钥。

[0053] (B)UE 导出相同的密钥。

[0054] [2]. 临时密钥

[0055] 临时密钥

[0056] 在导出根密钥后，UE(MTC 装置 10) 和 MTC-IWF 20 将导出用于保护在 MTC-IWF 20 和 UE(MTC 装置 10) 之间的通信的一对临时密钥。

[0057] 通过服务的 MTC-IWF 20 来进行在网络侧处的临时密钥导出。当 MTC-IWF 20 第一次需要与给定的 UE 进行通信时，它从根密钥导出一对或几对临时密钥。UE 以 MTC-IWF 20 进行的相同方式来导出相同的临时密钥。如果存在超过一对临时密钥，则 MTC-IWF 20 将向 UE 指示哪个用于该通信。并且，UE 将选择 MTC-IWF 20 指示的那个。

[0058] [3]. 用于密钥导出的输入参数

[0059] 可以将 K_iwf 导出如下。

[0060] (1) 可以从 CK(加密密钥)、IK(完整性密钥) 导出 K_iwf。在该情况下，它可以重新使用现有密钥分级的一部分。

[0061] (2) 可以从 Kasme(密钥访问安全管理实体) 导出 K_iwf。它可以重新使用现有的密钥分级的一部分。

[0062] (3) 可以从 3GPP 密钥分级独立地导出 K_iwf。

[0063] 其他值也被用作用于 K_iwf 导出的输入参数。

[0064] 可以使用 K_iwf 和其他输入参数来导出 K_di。

[0065] [4]. 密钥存储

[0066] 可以在 USIM(通用订户身份模块) 或 ME(移动设备) 的非易失性存储器中存储根密钥 (K_iwf) 和临时密钥 (K_di_con，K_di_int) 两者。

[0067] 随后参考图 3、4 和 5 来描述根密钥导出的 3 种情况。

[0068] 图 3 示出当 HSS 30 导出根密钥时的密钥导出和分配。

[0069] (S11)HSS 30 导出根密钥 K_iwf，并且以 CK、IK 作为输入密钥。

[0070] (S12)HSS 30 向 MTC-IWF 20 发送根密钥 K_iwf。

[0071] (S13)MTC 装置 10 导出相同的根密钥 K_iwf(S13a)，或者，HSS 30 向 MTC 装置 10 发送根密钥 K_iwf(S 13b)，这个应当在建立 NAS 和 / 或 AS 安全性后。

[0072] (S14)MTC-IWF 20 从 K_iwf 导出临时密钥。

[0073] (S15)MTC 装置 10 以 MTC-IWF 20 进行的相同方式从它具有的 K_iwf 导出相同的临时密钥。

[0074] (S16) 如果导出多对临时密钥，则 MTC-IWF 20 向 MTC 装置 10 指示它应当使用哪对临时密钥。

[0075] (S17) 通过一对临时密钥来保护在 MTC 装置和 MTC-IWF 之间传送的消息。

[0076] 图 4 示出当 MME/SGSN/MSC 40 导出根密钥时的密钥导出和分配。

[0077] (S21)MME/SGSN/MSC 40 导出根密钥 K_iwf，并且以 Kasme 作为输入密钥。

[0078] (S22)MME/SGSN/MSC 40 向 MTC-IWF 20 发送根密钥 K_iwf。

[0079] (S23)MTC 装置 10 导出相同的根密钥 K_iwf(S23a)，或者，MME/SGSN/MSC 40 向 MTC 装置 10 发送根密钥 K_iwf(S23b)，这应当在建立 NAS 和 / 或 AS 安全性之后。

[0080] (S24)MTC-IWF 20 从 K_iwf 导出临时密钥。

[0081] (S25)MTC 装置 10 以 MTC-IWF 20 进行的相同方式从它具有的 K_iwf 导出相同的临

时密钥。

[0082] (S26) 如果导出多对临时密钥，则 MTC-IWF 20 向 MTC 装置 10 指示它应当使用哪对临时密钥。

[0083] (S27) 通过一对临时密钥来保护在 MTC 装置 10 和 MTC-IWF 20 之间传送的消息。

[0084] 图 5 示出当 MTC-IWF 20 导出根密钥时的密钥导出和分配。

[0085] (S31)MME/SGSN/MSC 40 或 HSS 30 向 MTC-IWF 20 发送用于根密钥 K_iwf 导出的材料 (S31a)，或者，MTC 装置 10 和 MTC-IWF20 具有用于 K_iwf 导出的公共值 (S31b)。

[0086] (S32)MTC-IWF 20 导出根密钥 K_iwf。

[0087] (S33)MTC 装置 10 导出相同的根密钥 K_iwf。

[0088] (S34)MTC-IWF 20 从 K_iwf 导出临时密钥。

[0089] (S35)MTC 装置 10 以 MTC-IWF 20 进行的方式从它具有的 K_iwf 导出相同的临时密钥。

[0090] (S36) 如果导出多对临时密钥，则 MTC-IWF 20 向 MTC 装置 10 指示它应当使用的哪对临时密钥。

[0091] (S37) 通过一对临时密钥来保护在 MTC 装置 10 和 MTC-IWF 20 之间传送的消息。

[0092] 接下来，随后参考图 6 至 8 来描述根据这个示例性实施例的 MTC-IWF 20、MTC 装置 10 和网络实体 (HSS 30 或 MME/SGSN/MSC40) 的配置示例。

[0093] 如图 6 中所示，MTC-IWF 20 至少包括通信单元 21、共享单元 22 和导出单元 23。通信单元 21 与 MTC 装置 10 进行通信。共享单元 22 以在图 3 至 5 的任何一个中所示的方式来与 MTC 装置 10 安全地共享根密钥 K_iwf。导出单元 23 通过使用根密钥 K_iwf 导出临时密钥 K_di，以用于保护通信。结果，也可以在 MTC-IWF 20 和 MTC 装置 10 之间共享临时密钥 K_di。注意，这些单元 21 至 23 通过总线等彼此相互连接。这些单元 21 至 23 可以被例如下述部分构成 ：收发器，其分别与 HSS 30、MME/SGSN/MSC 40 和 SCS 50 进行通信 ；以及，控制器，其控制这些收发器以执行在图 3 中的步骤 S12、S14、S16 和 S17 至 S10 处所示的处理、在图 4 中的步骤 S22、S24、S26 处所示的处理、在图 5 中的步骤 S31、S32、S34、S36 和 S37 处所示的处理或与其等同的处理。

[0094] 而且，如图 7 中所示，MTC 装置 10 至少包括通信单元 11、共享单元 11 和导出单元 13。优选的是，MTC 装置 10 进一步包括授权单元 14。通信单元 11 与 MTC-IWF 20 进行通信。共享单元 12 以在图 3 至 5 的任何一个中所示的方式来与 MTC 装置 10 安全地共享根密钥 K_iwf。导出单元 13 通过使用根密钥 K_iwf 导出临时密钥 K_di，以用于保护通信。结果，也可以在 MTC 装置 10 和 MTC-IWF 20 之间共享临时密钥 K_di。授权单元 14 通过使用完整性密钥 K_di_int 来执行完整性检查，并且根据完整性检查的结果来授权 MTC-IWF 20。注意，这些单元 11 至 14 通过总线等彼此相互连接。这些单元 11 至 14 可以被例如下述部分构成 ：收发器，其通过 RAN 与核心网络无线地进行通信 ；以及，控制器，其控制该收发器以执行在图 3 中的步骤 S13 和 S15 至 S7 处所示的处理、在图 4 中的步骤 S23 和 S25 至 S27 处所示的处理、在图 5 中的步骤 S31、S33 和 S35 至 S37 处所示的处理或与其等同的处理。

[0095] 而且，如图 8 中所示，HSS 30 和 MME/SGSN/MSC 40 的每一个至少包括导出单元 31 和发送单元 32。导出单元 31 导出根密钥 K_iwf。发送单元 32 向 MTC-IWF 20 发送根密钥 K_iwf。在 MTC 装置 10 和 HSS 30 和 MME/SGSN/MSC 40 的每一个之间建立 NAS 和 / 或 AS 安

全上下文后，发送单元 32 也可以向 MTC 装置 10 发送根密钥 K_iwf。替代地，发送单元 32 向 MTC-IWF 20 发送用于根密钥 K_iwf 导出的材料。注意，这些单元 31 和 32 通过总线等彼此相互连接。这些单元 31 和 32 可以被例如下述部分构成：收发器，其与 MTC-IWF 20 进行通信；收发器，其在 MME/SGSN/MSC 40 的情况下与 RAN 进行通信；以及，控制器，其控制这些收发器以执行在图 3 中的步骤 S11 至 S13 处所示的处理、在图 4 中的步骤 S21 至 S23 处所示的处理、在图 5 中的步骤 S31 处所示的处理或与其等同的处理。

[0096] 注意，本发明不限于上述示例性实施例，并且显然，本领域内的普通技术人员可以基于权利要求的引用来来作出各种修改。

[0097] 如上所述的示例性实施例的整体或一部分可以被描述为但是不限于下面的补充说明。

[0098] （补充说明 1）

[0099] 提出了新的密钥分级，用于在 MTC-IWF 和 UE/MTC 装置之间的安全通信。它包括下面的部分。

[0100] (A) 用于导出一对临时密钥的根密钥。

[0101] (B) 包括保密性和完整性密钥的一对临时密钥，用于保护在 MTC-IWF 和 UE/MTC 装置之间的通信

[0102] （补充说明 2）

[0103] 在用于在 3GPP MTC 架构中的密钥管理的现有消息中的新的消息或新的参数。

[0104] （补充说明 3）

[0105] 在所建立的 NAS 和 / 或 AS 安全上下文上提供了在 MTC-IWF 和 UE/MTC 装置之间的安全通信

[0106] （补充说明 4）

[0107] 可以通过执行从 MTC-IWF 接收的消息的完整性检查的 UE/MTC 装置实现 MTC-IWF 授权。这也适用于漫游的 UE/MTC 装置。

[0108] 本申请基于并且要求优先权权益于在 2012 年 9 月 13 日提交的日本专利申请 No. 2012-201693，其公开通过引用被整体并入在此。

[0109] 附图标记列表

[0110] 10 MTC 装置

[0111] 11、21 通信单元

[0112] 12、22 共享单元

[0113] 13、23、31 导出单元

[0114] 14 授权单元

[0115] 20 MTC-IWF

[0116] 30 HSS

[0117] 32 发送单元

[0118] 40 MME/SGSN/MSC

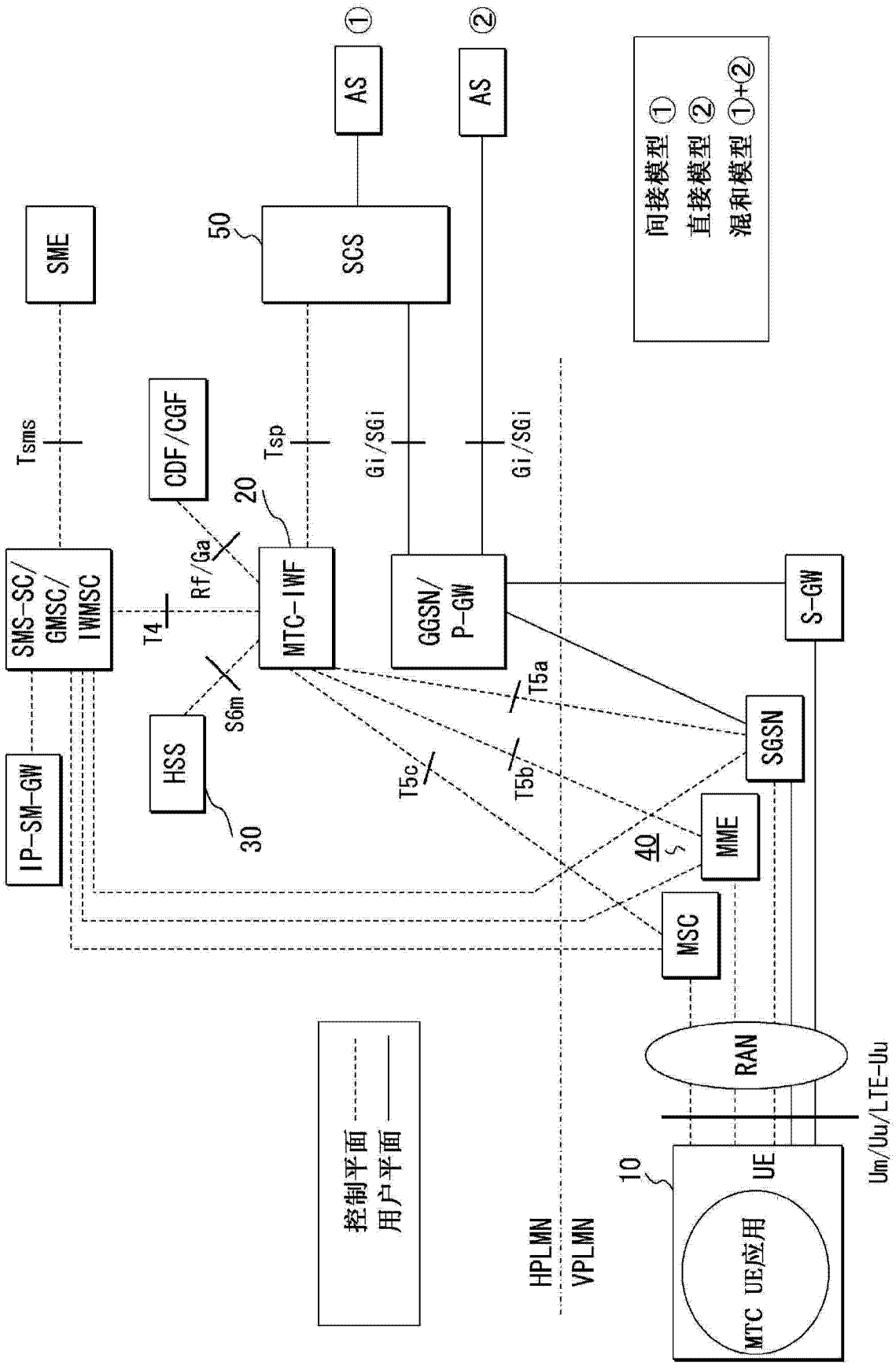

AS
①
AS
②
间接模型 ①
直接模型 ②
混和模型 ①+②
SME
50
SCS
Tsms
CDF/CGF
Tsp
Gi/SGi
Gi/SGi
20
SMS-SC/
GMSC/
IWMSC
Rf/Ga
MTC-IWF
GGSN/
P-GW
S-GW
T4
T5a
S6m
HSS
SGSN
T5c
T5b
30
40
IP-SM-GW
MME
MSC
RAN
控制平面
用户平面
HPLMN
VPLMN
10
UE
Um/Uu/LTE-Uu
MTC UE应用

图 1

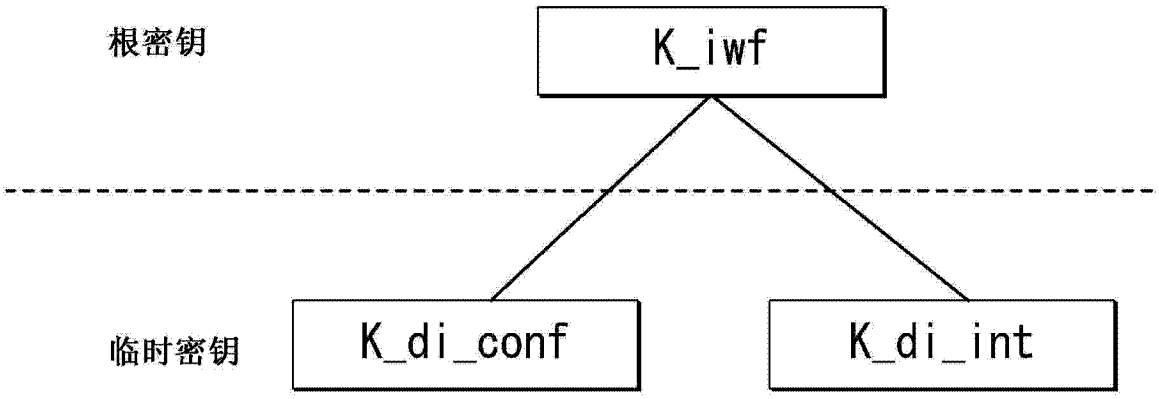


图 2

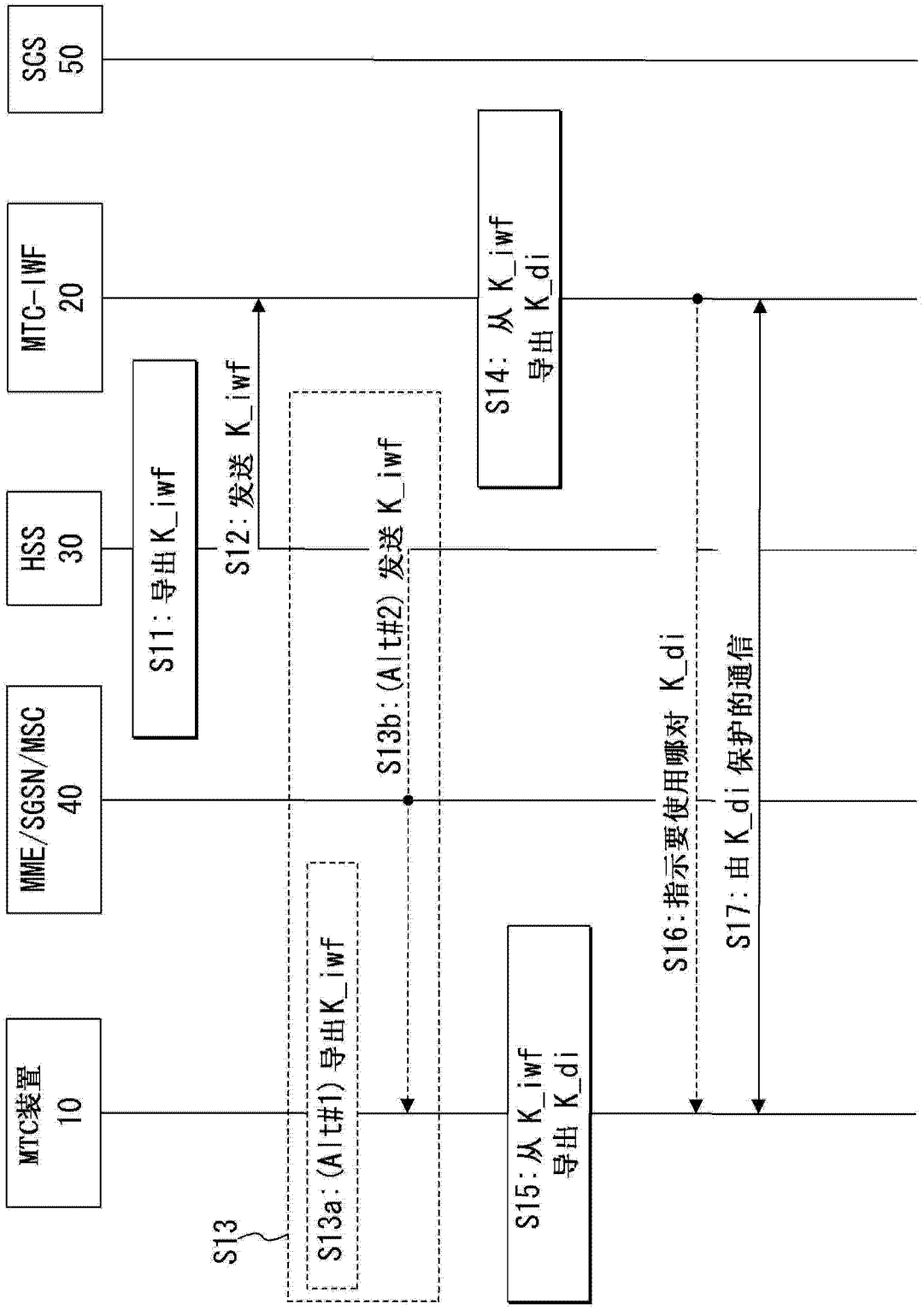

SCS 50
MTC-IWF 20
HSS 30
MME/SGSN/MSC 40
MTC装置 10
S11：导出K_iwf
S12：发送 K_iwf
S13
S13a：(A|t#1) 导出K_iwf
S13b：(A|t#2) 发送 K_iwf
S14：从 K_iwf 导出 K_di
S15：从 K_iwf 导出 K_di
S16：指示要使用哪对 K_di
S17：由 K_di 保护的通信

图 3

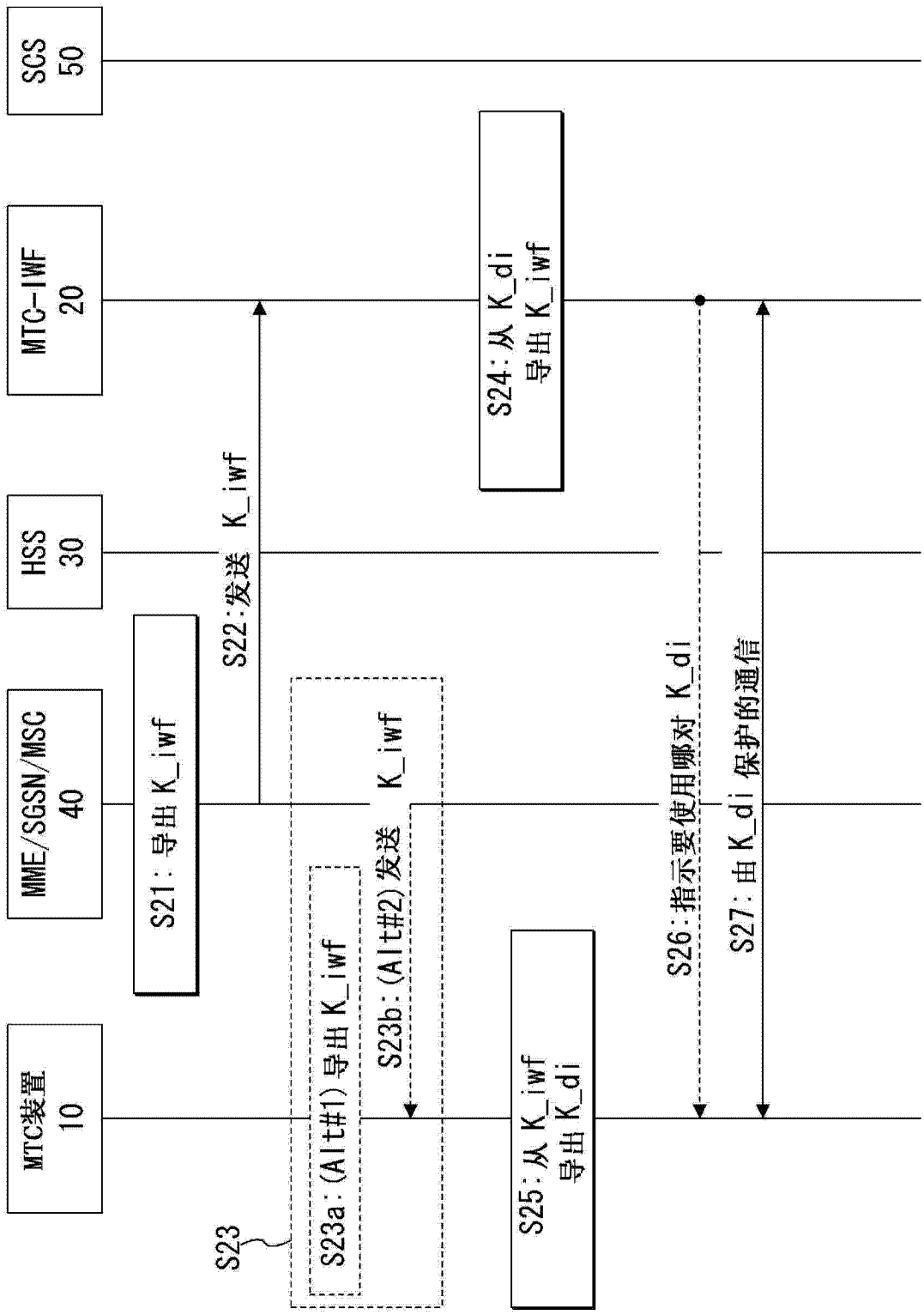

SCS 50
MTC-IWF 20
HSS 30
MME/SGSN/MSC 40
MTC装置 10
S21：导出 K_iwf
S22：发送 K_iwf
S23
S23a：(Alt#1) 导出 K_iwf
S23b：(Alt#2) 发送 K_iwf
S24：从 K_di 导出 K_iwf
S25：从 K_iwf 导出 K_di
S26：指示要使用哪对 K_di
S27：由 K_di 保护的通信

图 4

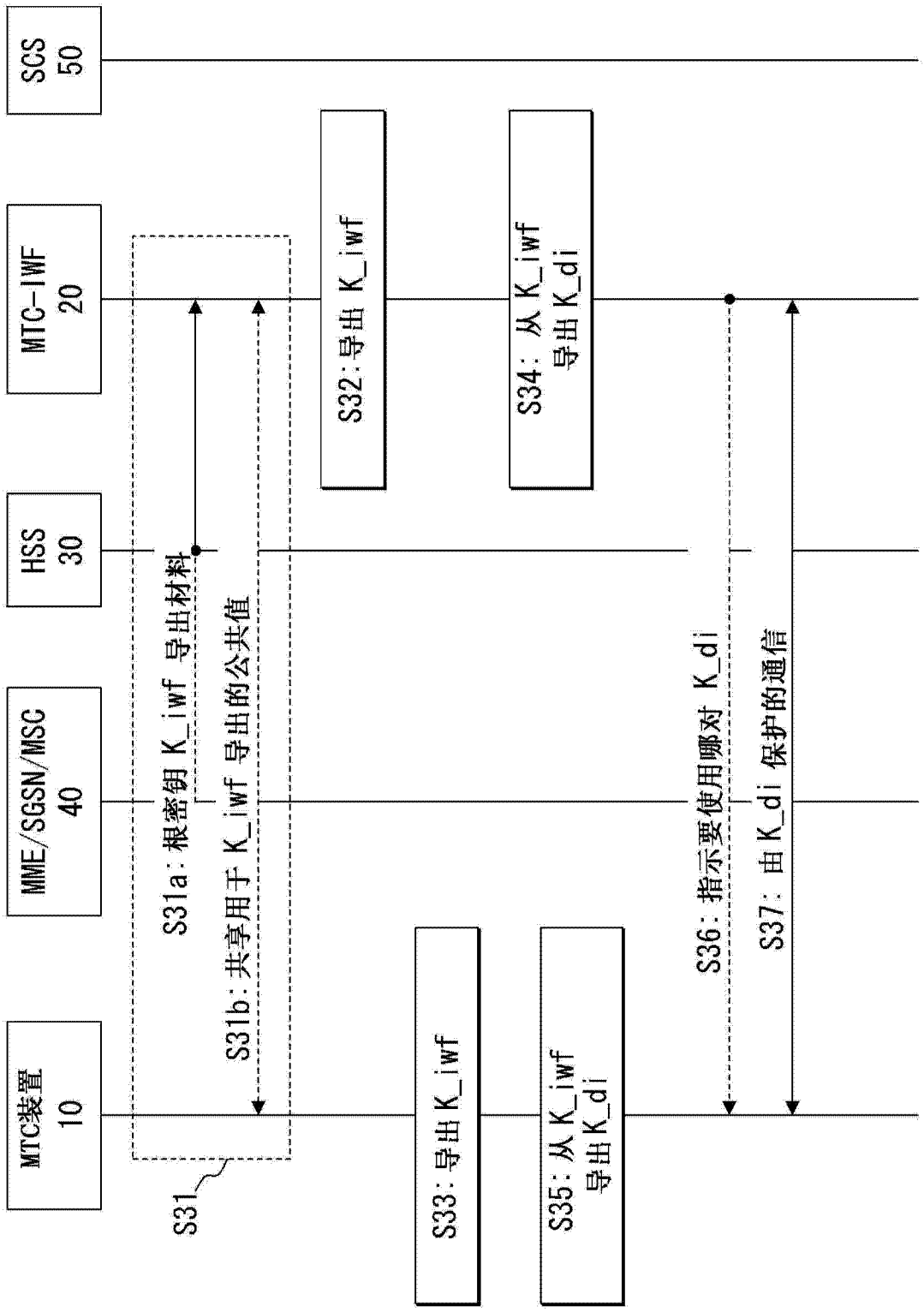

SCS 50
MTC-IWF 20
HSS 30
MME/SGSN/MSC 40
MTC装置 10
S31a：根密钥 K_iwf 导出材料
S31b：共享用于 K_iwf 导出的公共值
S31
S32：导出 K_iwf
S33：导出 K_iwf
S34：从 K_iwf 导出 K_di
S35：从 K_iwf 导出 K_di
S36：指示要使用哪对 K_di
S37：由 K_di 保护的通信

图 5

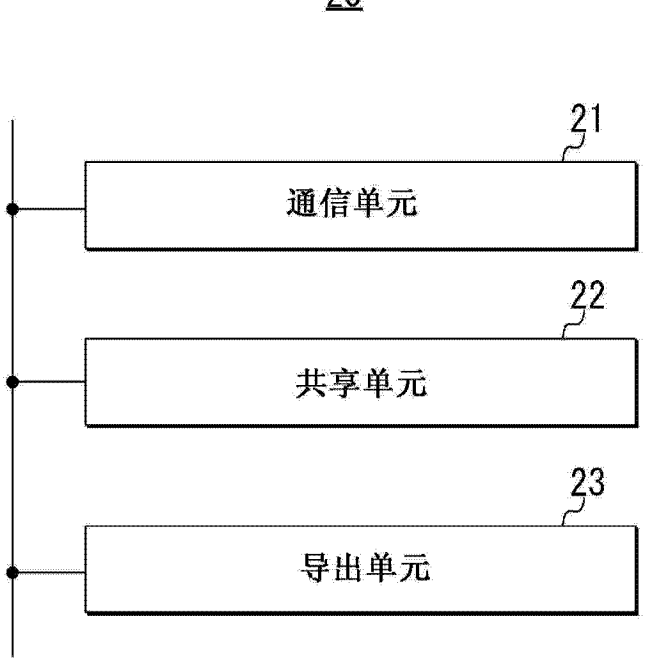


图 6

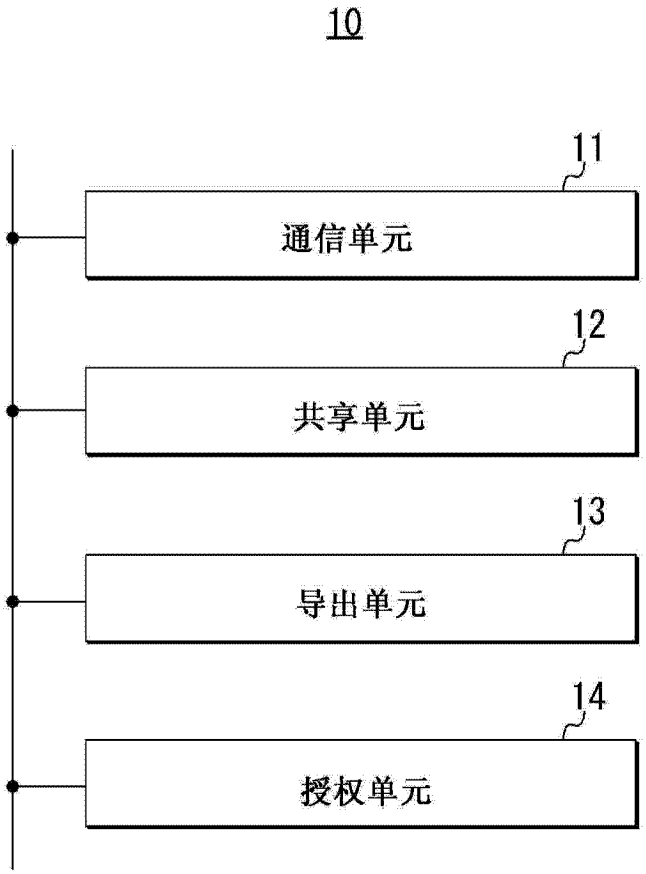


图 7

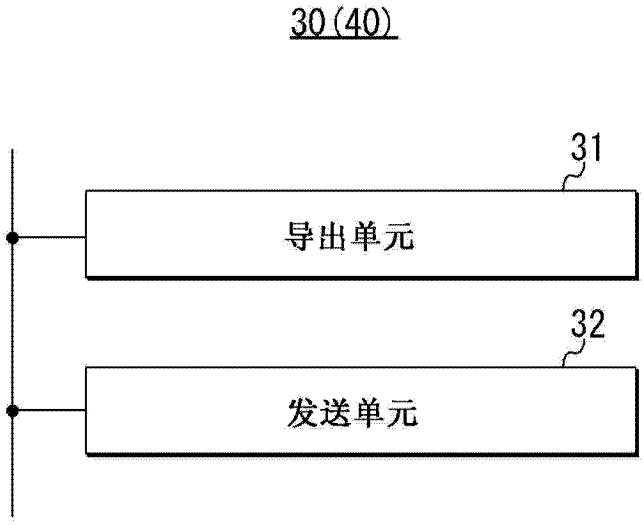


图 8