



(12) 发明专利

(10) 授权公告号 CN 111066014 B

(45) 授权公告日 2024. 03. 15

(21) 申请号 201880057232.7
(22) 申请日 2018.07.02
(65) 同一申请的已公布的文献号
申请公布号 CN 111066014 A
(43) 申请公布日 2020.04.24
(30) 优先权数据
2017-131568 2017.07.04 JP
(85) PCT国际申请进入国家阶段日
2020.03.04
(86) PCT国际申请的申请数据
PCT/JP2018/025118 2018.07.02
(87) PCT国际申请的公布数据
W02019/009263 JA 2019.01.10
(73) 专利权人 株式会社宙连
地址 日本东京都世田谷区玉川四丁目5番6号

(72) 发明人 安川健太 片山晓雄
(74) 专利代理机构 上海华诚知识产权代理有限公司 31300
专利代理师 刘煜
(51) Int.Cl.
G06F 21/44 (2006.01)
G06F 21/45 (2006.01)
G06F 21/62 (2006.01)
(56) 对比文件
JP 2007241985 A, 2007.09.20
JP 2008028600 A, 2008.02.07
US 2017034644 A1, 2017.02.02
CN 104303484 A, 2015.01.21
US 8594628 B1, 2013.11.26
审查员 张天洋

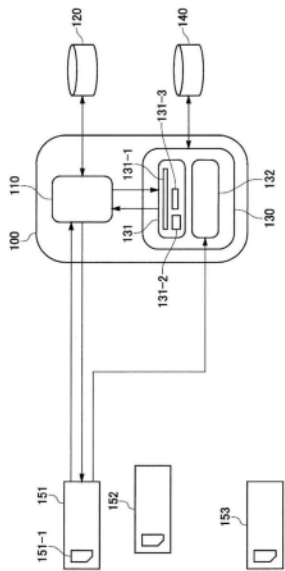
权利要求书2页 说明书6页 附图4页

(54) 发明名称

用于远程地管理设备的装置、方法及其程序

(57) 摘要

本发明提供一种用于远程地管理多个设备的装置、方法及其程序,使得容易地进行对各设备的认证信息的初始设定。首先,通信装置(110)经由蜂窝网络从设备(151)接收设备(151)的设备ID以及存储在SIM卡(151-1)中的识别码或与其对应的ID(S201)。接着,通信装置(110)根据需要访问数据库(120),获取与识别码或识别码对应的ID相关联的顾客ID(S202)。管理装置(130)使用这些ID来生成用于设备(151)的凭证(S203)。该凭证通过管理装置(110),经蜂窝网络被发送给设备(151)(S204)。接收到包含凭证的初始设定信息的设备(151)使用它在与第二管理装置(132)之间建立安全连接。



1. 一种用于远程地管理设备的方法,其特征在于,包括:

连接到蜂窝网络的通信装置经由所述蜂窝网络从存储有用于连接到所述蜂窝网络的识别码的设备接收所述识别码或与其对应的ID以及初始设定请求的步骤;

根据所述通信装置接收到所述识别码或与其对应的所述ID以及所述初始设定请求这一情况,第一管理装置生成用于所述设备的凭证的步骤;

所述第一管理装置经由所述蜂窝网络向所述设备发送初始设定信息的步骤,所述初始设定信息包含所述凭证或与所述凭证对应的认证信息、以及用于所述设备连接到能够经由所述蜂窝网络以外的网络与所述设备通信的第二管理装置的连接目的地信息;以及

在所述第一管理装置发送所述初始设定信息之后,所述第二管理装置对所述设备进行管理的步骤,

其中,所述初始设定信息用于将所述设备经由除了能够通过所述识别码连接的所述蜂窝网络以外的网络连接所述第二管理装置。

2. 根据权利要求1所述的方法,其特征在于,

所述识别码包括IMSI。

3. 根据权利要求1或2所述的方法,其特征在于,

所述识别码存储在SIM卡中。

4. 根据权利要求1所述的方法,其特征在于,

所述连接目的地信息是所述第二管理装置的连接目的地URL。

5. 一种用于远程地管理设备的方法,其特征在于,包括:

连接到蜂窝网络的通信装置经由所述蜂窝网络从与网关相连接的设备接收所述网关的识别码或与其对应的ID以及初始连接请求的步骤,该网关存储有用于连接到所述蜂窝网络的所述识别码;

根据所述通信装置接收到所述识别码或与其对应的所述ID以及所述初始设定请求这一情况,第一管理装置生成用于所述设备的凭证的步骤;

所述第一管理装置经由所述蜂窝网络向所述设备发送初始设定信息的步骤,所述初始设定信息包含所述凭证或与所述凭证对应的认证信息、以及用于所述设备连接到能够经由所述蜂窝网络以外的网络与所述设备通信的第二管理装置的连接目的地信息;以及

在所述第一管理装置发送所述初始设定信息之后,所述第二管理装置对所述设备进行管理的步骤,

其中,所述初始设定信息用于将所述设备经由除了能够通过所述识别码连接的所述蜂窝网络以外的网络连接所述第二管理装置。

6. 根据权利要求5所述的方法,其特征在于,

所述识别码包括IMSI。

7. 根据权利要求5或6所述的方法,其特征在于,

所述识别码存储在SIM卡中。

8. 根据权利要求5所述的方法,其特征在于,

所述连接目的地信息是所述第二管理装置的连接目的地URL。

9. 一种用于远程地管理设备的系统,其特征在于,

具备连接到蜂窝网络的通信装置、与所述通信装置连接的第一管理装置、以及能够经

由所述蜂窝网络以外的网络与所述设备通信的第二管理装置，

所述通信装置经由所述蜂窝网络从存储有用于连接到所述蜂窝网络的识别码的设备接收所述识别码或与其对应的ID以及初始设定请求，

所述第一管理装置进行如下处理：

根据接收到所述识别码或与其对应的所述ID以及所述初始设定请求这一情况，生成用于所述设备的凭证，

经由所述蜂窝网络向所述设备发送初始设定信息，所述初始设定信息包含所述凭证或与所述凭证对应的认证信息、以及用于所述设备连接到能够经由所述蜂窝网络以外的网络与所述设备通信的第二管理装置的连接目的地信息，

在所述第一管理装置发送所述初始设定信息之后，所述第二管理装置对所述设备进行管理，

其中，所述初始设定信息用于将所述设备经由除了能够通过所述识别码连接的所述蜂窝网络以外的网络连接到所述第二管理装置。

用于远程地管理设备的装置、方法及其程序

技术领域

[0001] 本发明涉及一种用于远程地管理设备的装置、方法及其程序。

背景技术

[0002] 随着传感技术、通信技术的发展,与计算机网络连接的设备增多,所有的事物都被网络化的Internet of Thing (物联网)的想法在普及。以下,不限于因特网,将经网络化的设备称为“IoT设备”。

[0003] IoT设备能够与网络连接来向服务器、存储器等发送收集到的数据,或者从服务器接收数据的传送。能够进行固件的更新、新的软件的安装,或者接收对现有软件的命令。当考虑在远程配备许多设备的情况时,通过与网络连接,能够动态地检测并管理这些设备的设定、状态等。

发明内容

[0004] 发明要解决的问题

[0005] 理论上,可能的这种设备管理在现实中是不容易的。即,为了在远程进行信息的收集、传送,必须在与用于进行管理的服务器之间建立安全的连接。作为一种方法,可以预先将用于以规定的通信方式进行通信的相同或对应的认证信息提供给管理服务器和设备双方,例如,在接通设备的电源时动作的软件使用该认证信息,来确立与管理服务器之间的连接。

[0006] 但是,在该方法中,必须在使用各设备之前预先对每个设备进行认证信息的设定,例如会导致制造工序中的工时增加,关系到成本的上升。今后,在2020年连接到因特网的物品的数量据说是200亿个或1000亿个的状况下,设备数量越爆炸性地增大,初始设定的成本也越增大。

[0007] 本发明是鉴于这样的问题点而完成的,其目的在于,在用于远程地管理多个设备的装置、方法及其程序中,容易地进行对各设备的认证信息的初始设定。

[0008] 用于解决问题的技术手段

[0009] 为了达成这样的目的,本发明的第1形态是一种用于远程地管理设备的方法,其特征在于,包括:经由蜂窝网络从存储有用于连接到所述蜂窝网络的识别码的设备接收包含所述设备的设备ID的初始设定请求以及所述识别码或与其对应的ID的步骤;根据所述识别码或与其对应的ID,获取与所述识别码相对应的顾客ID的步骤;使用所述顾客ID以及所述设备ID,生成用于所述设备的凭证的步骤;以及向所述设备发送包含所述凭证或与其对应的认证信息的初始设定信息的步骤。

[0010] 另外,本发明的第2形态是一种用于远程地管理设备的方法,其特征在于,包括:经由蜂窝网络接收从与网关相连接的设备发送来的所述设备的设备ID、以及所述网关的识别码或与其对应的ID来作为初始连接请求的步骤,该网关存储有用于连接到所述蜂窝网络的所述识别码,根据所述识别码或与其对应的ID,获取与所述识别码相对应的顾客ID的步骤;

使用所述顾客ID以及所述设备ID,生成用于所述设备的凭证的步骤;以及向所述设备发送包含所述凭证或与其对应的认证信息的初始设定信息的步骤。

[0011] 另外,本发明的第3形态的特征在于,在第1或第2形态中,所述识别码包含IMSI。

[0012] 另外,本发明的第4形态的特征在于,在第1至第3中的任一形态中,所述识别码存储在SIM卡中。

[0013] 另外,本发明的第5形态的特征在于,在第1至第4中的任一形态中,所述凭证是用于与有线网络连接的凭证。

[0014] 另外,本发明的第6形态的特征在于,在第1至第4中的任一形态中,所述凭证是用于与无线网络连接的凭证。

[0015] 另外,本发明的第7形态的特征在于,在第6形态中,所述无线网络是除了能够通过所述识别码连接的蜂窝网络以外的网络。

[0016] 另外,本发明的第8形态的特征在于,在第6或第7形态中,所述无线网络中的通信使用LwM2M协议。

[0017] 另外,本发明的第9形态的特征在于,在第1至第8中的任一形态中,所述凭证的发送通过所述蜂窝网络来进行。

[0018] 另外,本发明的第10形态的特征在于,在第1或第2形态中,所述接收以及发送在用于提供所述蜂窝网络中的通信的通信装置中进行,所述生成在用于管理所述设备的管理装置中进行,所述管理装置能够在蜂窝网络外与所述通信装置进行通信。

[0019] 另外,本发明的第11形态的特征在于,在第10形态中,所述获取在所述通信装置中进行。

[0020] 另外,本发明的第12形态的特征在于,在第10或第11形态中,所述初始设定信息包含所述管理装置的连接目的地信息。

[0021] 另外,本发明的第13形态的特征在于,在第12形态中,所述管理装置具有第一管理装置以及第二管理装置,所述生成在所述第一管理装置中进行,所述连接目的地信息是所述第二管理装置的连接目的地URL。

[0022] 另外,本发明的第14形态是一种用于使计算机执行用于远程地管理设备的方法的程序,其特征在于,所述方法包括:经由蜂窝网络从存储有用于连接到所述蜂窝网络的识别码的设备接收包含所述设备的设备ID的初始设定请求以及所述识别码或与其对应的ID的步骤;根据所述识别码或与其对应的ID,获取与所述识别码相对应的顾客ID的步骤;使用所述顾客ID以及所述设备ID,生成用于所述设备的凭证的步骤;以及向所述设备发送包含所述凭证或与其对应的认证信息的初始设定信息的步骤。

[0023] 另外,本发明的第15形态是一种用于远程地管理设备的装置,其特征在于,经由蜂窝网络从存储有用于连接到所述蜂窝网络的识别码的设备接收包含所述设备的设备ID的初始设定请求以及所述识别码或与其对应的ID,根据所述识别码或与其对应的ID,获取与所述识别码相对应的顾客ID,使用所述顾客ID以及所述设备ID,生成用于所述设备的凭证,向所述设备发送包含所述凭证或与其对应的认证信息的初始设定信息。

[0024] 发明的效果

[0025] 根据本发明的一形态,基于预先存储在作为管理对象的设备中的用于与蜂窝网络连接的IMSI等识别码,来生成用于该设备的凭证,并事后给予该凭证,由此,能够大幅容易

地进行用于与管理该设备用的管理装置之间的远程管理的安全连接所需的初始设定。

附图说明

- [0026] 图1是示出本发明的第1实施方式的管理系统的图。
- [0027] 图2是示出本发明的第1实施方式的方法的流程图。
- [0028] 图3是用于说明本发明的第1实施方式的方法中的初始设定请求的图。
- [0029] 图4是用于说明本发明的第1实施方式的方法中的初始设定信息的图。
- [0030] 图5是用于说明本发明的第2实施方式的管理对象设备的图。
- [0031] 图6是表示本发明的第3实施方式的网络控制台的图。

具体实施方式

[0032] 以下,参照附图详细说明本发明的实施方式。

[0033] (第1实施方式)

[0034] 图1示出了本发明的第1实施方式的管理系统。管理系统100具备:通信装置110,其通过蜂窝网络与多个设备151、152、153进行通信;以及管理装置130,其能够与通信装置110通信,用于管理多个设备151、152、153。设备的数量可以是1个或多个,图1示出了3台的例子,但不限于此。以下,以设备151为例进行说明。

[0035] 通信装置110除了可以是MNO(移动网络运营商)的通信装置,也可以是与MNO的通信基础设施连接来提供无线通信服务的形式的MVNO(移动虚拟网络运营商)的通信装置。在设备151中插入由MNO或MVNO提供的SIM卡151-1,经过基于HLR/HSS的验证,可以与通信装置110进行蜂窝网络中的通信。在本实施方式中,设备151与通信装置110之间的通信在蜂窝网络的核心网络中进行,通信装置110与管理装置130之间的通信在蜂窝网络外进行。

[0036] 在MNO和MVNO之间,还存在MVNE(移动虚拟通信服务提供商),其提供用于MVNO进行顺利运营的辅助服务,MVNE还具有用于与MNO的通信基础设施连接来提供无线通信服务的通信基础设施。在这种情况下,通信装置110成为MVNE的通信装置。另外,MVNE也提供SIM卡151-1。

[0037] 通信装置110能够与数据库120通信,在数据库120中,针对各SIM卡存储有IMSI等识别码或与其对应的ID与该SIM卡的使用者名、企业名等顾客ID的对应关系。通信装置110也可以具有自己的存储设备或存储介质(未图示)来代替访问数据库120,并在其中存储上述对应关系。

[0038] 在本说明书中,主要以SIM卡为例进行说明,但IMSI等识别码不仅存储在设备151所具有的物理性的SIM卡151-1中,还可以在嵌入至设备151中的半导体芯片(也称为“eSIM”)。上存储一个或多个IMSI,以及可以在设备151的模块内的安全区域中搭载软件,在该软件上存储一个或多个IMSI,设备151直接或间接地保持识别码的方式可以考虑各种方式。在本发明中,如下文所述,当使用预先存储在设备151中的用于连接到蜂窝网络的识别码来进行管理用的初始设定时,IMSI在蜂窝网络的连接阶段进行其可靠性的验证,并且随后的通信通过加密而具有高保密性,能够实现高度的安全。

[0039] 管理装置130能够与数据库140通信,数据库140如下文所述那样存储设备151的初始设定所需的数据。通信装置110可以具有自己的存储装置或存储介质来代替访问数据库

140,并在其中存储上述对应关系。如图1所示,管理装置130也可以分为用于进行管理所需的初始设定的第一管理装置131和用于进行初始设定后的管理的第二管理装置132,以下说明该例子,但也可以是同一装置。这种情况下,不进行在第一管理装置131和第二管理装置132之间进行的数据的收发或交接。通信装置110和管理装置130为同一装置时也同样。

[0040] 设备151可以是具有所需的通信功能的任意设备,只要具有用于连接到蜂窝网络的识别码即可。为了将电池余量、电波强度、动作状况等设备151中的传感结果发送给管理系统100,或者执行来自管理系统100的指令,要求能够执行基于C、Java (注册商标) 等编程语言的软件。以包装(ラップ)C的安装的形式,使用不同的编程语言(Ruby、Go、Javascript (注册商标) 等)的扩展也是可能的。例如,可以是安装有Linux (注册商标)、Android (注册商标) 等OS的设备。在设备151中配备管理装置130进行管理所需的最低限度或有限的软件,通过使管理装置130承担很多的处理,能够使设备151成为无效的设备。从这个观点来看,管理装置130优选至少将其一部分安装在云上,更优选地安装在公有云上或私有云上。作为具体例子,考虑在设备管理中在IP协议上使用LwM2M协议,使设备151具有LwM2M客户端,使第一管理装置131具有LwM2M引导服务器,使第二管理装置132具有LwM2M服务器的构成。

[0041] 在本说明书中说明的各设备不限于物理上单一的设备,可以是多个可相互访问的设备。另外,关于第一管理装置131,具备通信接口等通信部131-1、处理器、CPU等处理部131-2、以及包含内存、硬盘等存储装置或存储介质的存储部131-3,如图所示通过在处理部131-2中执行存储在可从存储部131-3或第一管理装置131访问的存储装置或存储介质中的用于进行各处理的程序,能够实现以下说明的各功能,关于其他设备,也能够通过同样的硬件实现。上述程序可以包括一个或多个程序,并且能够记录在计算机可读的存储介质中作为非临时性程序产品。

[0042] 图2是示出本发明的第1实施方式的方法的流程图。首先,通信装置110经由蜂窝网络从设备151接收设备151的设备名(有时也称为“端点”。)等设备ID以及存储在SIM卡151-1中的IMSI等识别码或TEID等与其对应的ID(S201)。作为一例,在接通设备151的电源时,在规定的软件动作且不具有用于与管理装置130连接的凭证的情况下,为了初始设定,也可以发送包含设备ID的初始设定请求,自动进行以下的处理。

[0043] 图3是用于说明从设备发送的初始设定请求的一例的图。从设备151发送基于CoAP/UDP/IP的各个协议的第一数据310作为初始设定请求,并且基于GTP/UDP/IP的各个协议的第二数据320被附加到蜂窝网络中,由通信装置110接收。在基于CoAP协议的CoAP区域中,“POST/bs”与端点一起被记述为基于LwM2M协议的引导请求。UDP区域中记述有在设备151中动作的软件的端口号,IP区域中记述有作为发送目的地的第一管理装置131的IP地址以及作为发送源的设备151的IP地址。

[0044] 设备151中插入有SIM卡,由于可以具有电话号码,所以可以收发SMS消息。基于LwM2M协议的消息可以在SMS上交换,在这种情况下,搬运CoAP消息的传输层代替UDP/IP成为SMS。

[0045] 接着,通信装置110根据需要访问数据库120,获取与识别码或识别码对应的ID相关联的顾客ID(S202)。在图3所示的数据结构的例子中,在第二数据320的GTP区域中包含与IMSI对应的TEID,可以使用该TEID获取顾客ID。通信装置110将获取到的顾客ID以及设备ID交给管理装置130,管理装置130使用这些ID,生成用于设备151的凭证(S203)。生成的用于

设备151的凭证或与其对应的认证信息与顾客ID以及设备ID相关联地登记在数据库140或存储部131-3中。这里所说的“凭证”是以ID、密码为代表的、用户的认证所用的信息的总称。

[0046] 这里,记述了在通信装置110中进行顾客ID的获取的处理,但也可以将通信装置110接收到的初始设定请求310直接或实质上直接地交给管理装置130,或者将必要的设备ID、IP地址等交给管理装置130,并在管理装置130中,参照IMSI等识别码或与其对应的ID与该SIM卡的使用者名、企业名等顾客ID的对应关系来进行顾客ID的获取。该对应关系除了访问数据库120来进行参照之外,也可以预先存储在数据库140中,访问数据库140来进行参照。

[0047] 该凭证或与其对应的认证信息通过通信装置110,经蜂窝网络发送给设备151(S204)。除了该凭证或与其对应的认证信息之外,包含作为设备151的连接目标的第二管理装置132的IP地址或主机名的连接目的地信息被发送给设备151,将这些信息称为初始设定信息。初始设定信息中包含的发送目的地信息以负荷分散等为目的,可以根据顾客ID以及设备ID的至少一方来选择。

[0048] 图4是用于说明从管理装置发送的初始设定信息的一例的图。从管理装置131发送基于CoAP/UDP/IP的各个协议的第一数据410作为初始设定信息,并且基于GTP/UDP/IP的各个协议的第二数据420被附加在蜂窝网络中,向设备151发送。在基于CoAP协议的CoAP区域中,除了IP地址之外,包括协议及端口号的连接目的地URL被记述为“coaps://<第二管理装置132的IP地址或主机名>:5684”来作为连接目的地信息。另外,CoAP区域在LwM2M协议中包含“201”等表示初始设定请求被适当处理的符号,根据接收到该符号这一情况,可以在设备151中进行之后的连接处理。UDP区域中记述有在设备151中动作的软件的端口号,IP区域中记述有作为发送目的地的设备151的IP地址以及作为发送源的第一管理装置131的IP地址。

[0049] 接收到包含凭证或与其对应的认证信息以及连接目的地信息的初始设定信息的设备151使用其在与第二管理装置132或管理装置130之间建立安全连接。

[0050] 这样,基于预先装配于设备151的用于连接到蜂窝网络的IMSI等识别码,生成用于设备151的凭证,并事后给予该凭证,由此,能够大幅容易地在设备151与管理装置130或管理系统100之间进行用于远程管理的安全连接所需的初始设定。

[0051] 此外,需要注意的是,假设如果没有如“仅基于××”、“仅根据××”、“仅在××的情况下”这样的“仅”的记载,则在本说明书中,还可以考虑附加的信息。

[0052] 另外,管理系统100以及数据库120、140的全部或一部分可以是云上或公有云或私有云上的实例。这里,在本说明书中,“云”是指能够在网络上根据需求动态地配置并提供CPU、内存、存储器、网络带宽等计算资源的系统。例如,可以通过AWS等来利用云。另外,“公有云”是指多个租户可利用的云。

[0053] (第2实施方式)

[0054] 在第1实施方式中,设备151是管理对象,但在本发明的第2实施方式中,将存储有用于连接到蜂窝网络的识别码的设备151作为网关,将与设备151连接的从属设备501、502、503作为管理对象。这里,作为例示,示出3台的例子。

[0055] 在设备151从从属设备501接收到从属设备501的设备ID的情况下,例如如果以图3所例示的数据结构来考虑,则将在第一数据的IP区域310中记述的发送源的IP地址变换为网关的自己的IP地址后,作为初始设定请求发送给通信装置110。在IP地址转换的同时,UDP

层的端口也会被转换。此后与第1实施方式相同。在设备151接收到向从属设备501发送的初始设定信息的情况下,进行IP地址的逆变换,将该初始设定信息中包含的凭证或与其对应的认证信息以及连接目的地信息交给从属设备501。

[0056] (第3实施方式)

[0057] 在第二管理装置132或管理装置130中执行的来自设备151的信息的确认、对设备151的控制等管理功能例如可以通过设置API来提供给外部。另外,也可以设置网络控制台。图6是能够在网络浏览器上显示的网络控制台600的一例。

[0058] 符号说明

[0059] 100:管理系统

[0060] 110:通信装置

[0061] 120:数据库

[0062] 130:管理装置

[0063] 131:第一管理装置

[0064] 131-1:通信部

[0065] 131-2:处理部

[0066] 131-3:存储部

[0067] 132:第二管理装置

[0068] 140:数据库

[0069] 151、152、153:设备

[0070] 151-1:SIM卡

[0071] 310:第一数据

[0072] 320:第二数据

[0073] 410:第一数据

[0074] 420:第二数据

[0075] 501、502、503:从属设备

[0076] 600:网络控制台。

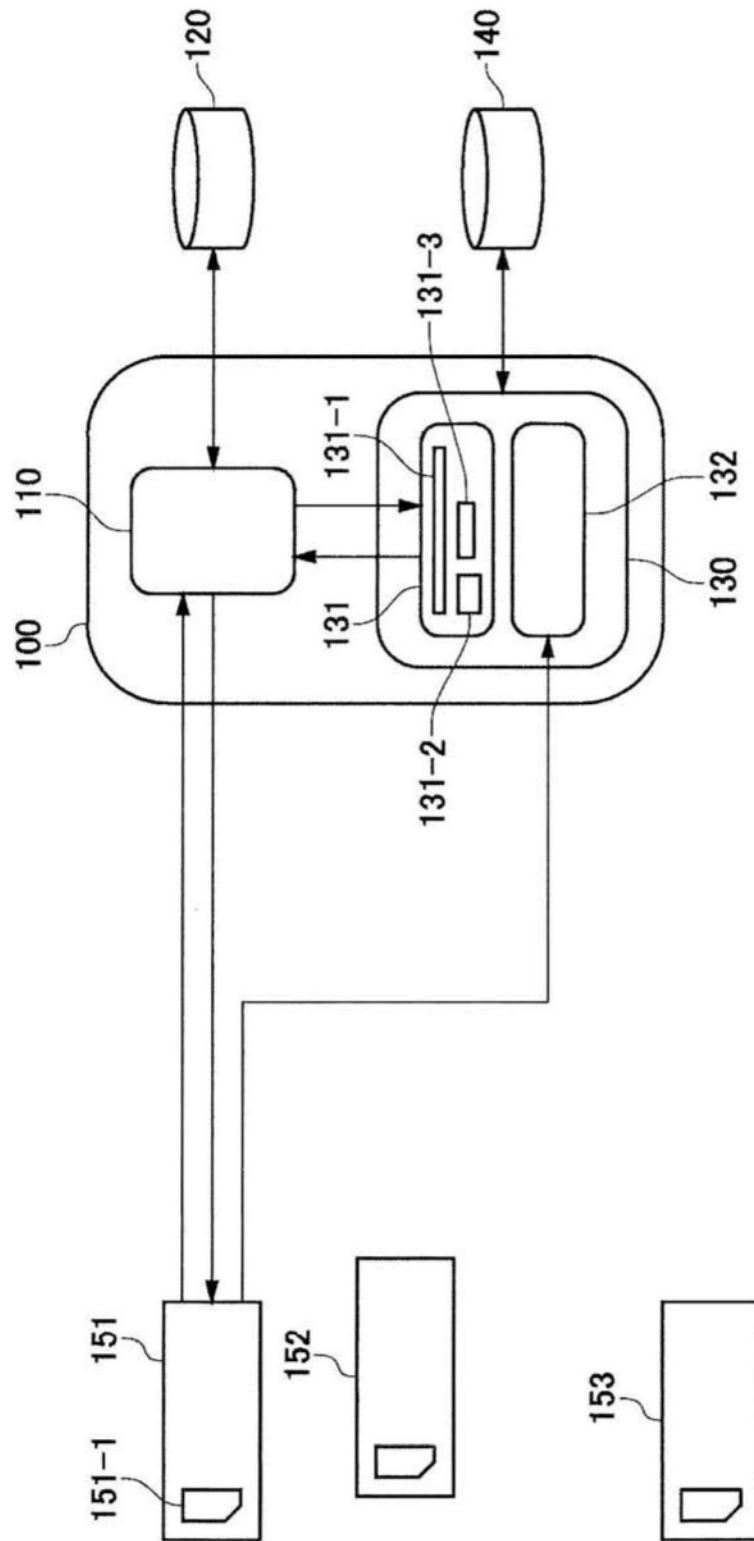


图1

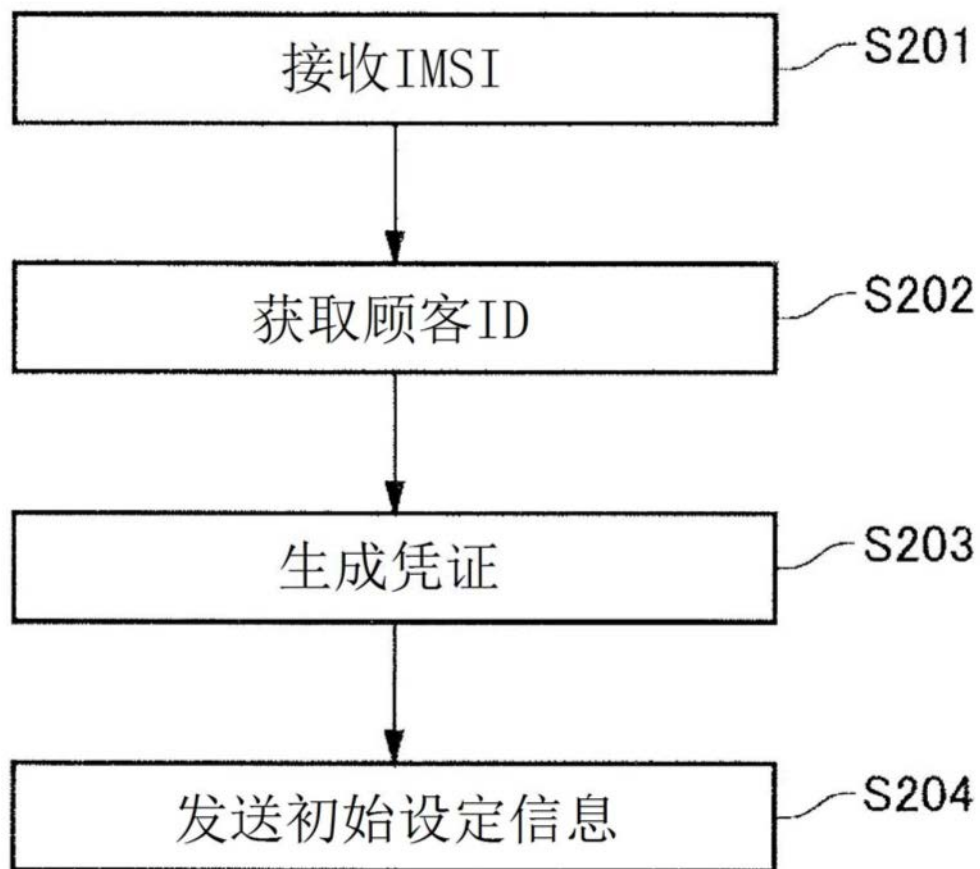


图2

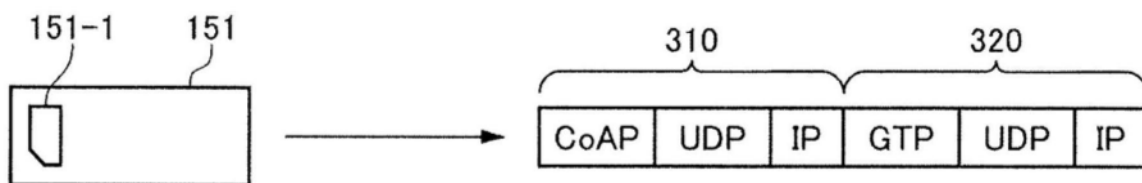


图3

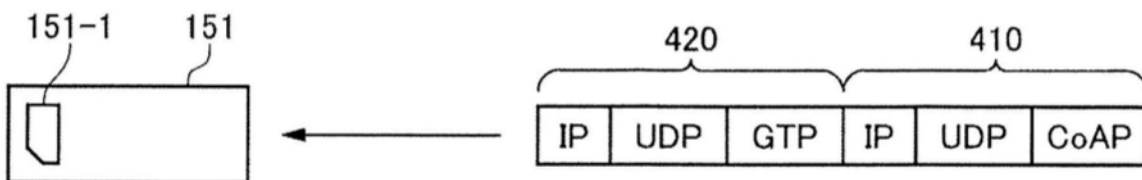


图4

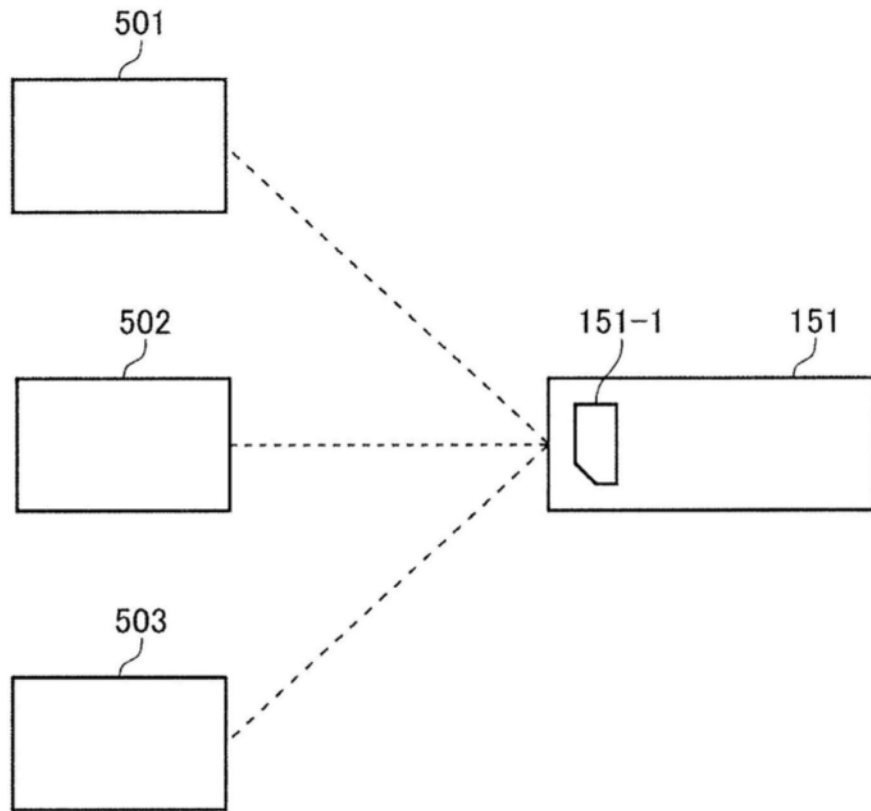


图5

LWM2M访问控制

2

设备 3

600

实例 (instance) 0

制造商 ? Leshan演示设备

型号 ? 模型 500

序列号 ? LT-500-000-0001

固件版本 ? 1.0.0

重新启动 ?

恢复出厂设置 ?

可用电源 ?

电源电压 ?

电源电流 ?

电池电量 ?

内存清理 ?

错误代码 ?

重置错误代码 ?

当前时间 ?

UTC偏移量 ?

时区 ?

支持的绑定和模式 ?

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

不监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

监视

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

执行

写

写

写

写

写

写

写

写

写

写

写

写

写

写

写

写

写

读

读

读

读

读

读

读

读

读

读

读

读

读

读

读

读

读

/3/0/0

/3/0/1

/3/0/2

/3/0/3

/3/0/4

/3/0/5

/3/0/6

/3/0/7

/3/0/8

/3/0/9

/3/0/10

/3/0/11

/3/0/12

/3/0/13

/3/0/14

/3/0/15

/3/0/16

11%

210793KB

Jun 21,2017 7:08:27 AM

+09

亚洲/东京

U

600

图6