

(12) 发明专利

(10) 授权公告号 CN 101385032 B

(45) 授权公告日 2010.08.25

(21) 申请号 200780005764.8

(22) 申请日 2007.02.15

(30) 优先权数据

06290257.2 2006.02.15 EP

(85) PCT申请进入国家阶段日

2008.08.15

(86) PCT申请的申请数据

PCT/EP2007/001336 2007.02.15

(87) PCT申请的公布数据

W02007/093426 EN 2007.08.23

(73) 专利权人 汤姆森许可贸易公司

地址 法国布洛涅-比郎库尔

(72) 发明人 阿兰·迪朗

(74) 专利代理机构 中科专利商标代理有限责任

公司 11021

代理人 戎志敏

(51) Int. Cl.

G06F 21/00(2006.01)

H04L 29/06(2006.01)

H04L 12/28(2006.01)

H04N 7/00(2006.01)

(56) 对比文件

CN 2603581 Y, 2004.02.11, 全文.

EP 1564621 A1, 2005.08.17, 全文.

审查员 崔哲

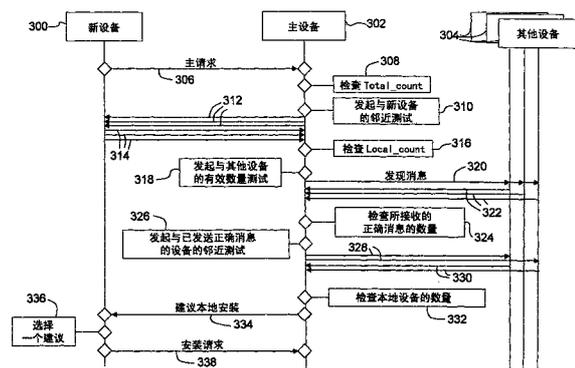
权利要求书 2 页 说明书 9 页 附图 5 页

(54) 发明名称

用于控制授权域中安装的设备数量的方法和装置

(57) 摘要

通过主设备功能,控制授权域中安装的设备数量。该主设备存储:在 AD 中安装的设备的总数的上限值 Totaljimit;在主设备的本地附近安装的设备总数的上限值 Localjimit,以及与所述主设备远程安装的设备总数的上限值 Remotejimit。该主设备也存储以下当前值:AD 中所述主设备本地附近安装的设备数量 Local_count;以及 AD 中与所述主设备远程安装的设备数量 Remote_count。当要在 AD 中安装新设备时,关于当前值检查该上限值,并检查该设备是否在该主设备的本地附近,以授权或不授权在 AD 中本地或远程安装该设备。



1. 一种用于控制包含至少一个主设备 (200) 的授权域 (1) 中安装的设备 (21、22、23、24、31、41、42、51) 的数量的方法, 所述主设备能够存储以下数量的上限值:

- 在所述授权域中安装的设备总数 Total_limit;
- 在所述主设备本地附近安装的设备总数 Local_limit;
- 与所述主设备远程安装的设备总数 Remote_limit;
- 授权域中在所述主设备本地附近安装的设备数量 Local_count; 以及
- 授权域中与所述主设备远程安装的设备数量 Remote_count;

所述主设备还能够存储授权域中安装的设备总数 Total_count, 或者根据 Local_count 和 Remote_count 来计算 Total_count; 当所述主设备接收到来自新设备的安装请求时, 所述方法包括以下步骤:

验证 (502) Total_count 尚未达到 Total_limit, 以及

在成功验证的情况下, 检查 (506、510) 所述新设备是否是在所述主设备的本地附近, 以及

在发现所述新设备是本地设备的情况下, 在允许本地安装之前, 验证 (520) Local_count 尚未达到 Local_limit;

在发现所述新设备是远程设备的情况下, 在允许远程安装之前, 验证 (516) Remote_count 尚未达到 Remote_limit。

2. 如权利要求 1 所述的方法, 其中, 所述上限值 Local_limit 大于所述上限值 Remote_limit。

3. 如权利要求 1 或 2 中任一项所述的方法, 其中, 所述上限值 Total_limit 大于所述上限值 Local_limit 和 Remote_limit 之和。

4. 如权利要求 1 所述的方法, 其中,

所述方法还包括以下步骤: 在发现新设备是本地设备而且数量 Local_count 等于或大于 Local_limit 的情况下, 检查授权域中安装的且此时在所述主设备的本地附近连接的设备的数量是否大于数量 Local_count 的预定有效数量;

其中, 只有所述检查为肯定时才本地安装所述新设备。

5. 如权利要求 4 所述的方法, 其中, 检查授权域中安装的且此时在所述主设备的本地附近连接的设备的数量是否大于 Local_count 的预定有效数量的步骤包括:

向授权域中的所有设备广播发现消息, 所述发现消息包含授权域标识符和随机数;

从授权域中的设备接收包含所述随机数和响应设备的标识符的消息, 所述消息由鉴权数据保护;

使用鉴权数据验证所接收的消息的有效性; 以及

针对从授权域中的设备接收到的每条有效消息, 检查发送该有效消息的设备是否在所述主设备的本地附近;

对所述主设备本地附近的发送有效消息的设备的数量进行计数; 以及

检查所述数量是否大于 Local_count 的预定有效数量。

6. 如权利要求 4 或 5 中任一项所述的方法, 其中, Local_count 的预定有效数量为 Local_count 的一半。

7. 如权利要求 4 至 5 中任一项所述的方法, 其中, 所述预定有效数量基于授权域中安装

的设备的总数 Total_count 而不是 Local_count。

8. 如权利要求 4 至 5 中任一项所述的方法,其中:

当本地安装新设备时,增大 Local_count ;或

当远程安装新设备时,增大 Remote_count。

9. 如权利要求 8 所述的方法,其中,只有在新设备能够消费和 / 或导出内容时,才增大 Local_count 或 Remote_count。

10. 如权利要求 9 所述的方法,其中,在新设备能够消费和导出内容时,把 Local_count 或 Remote_count 增大一个单位。

11. 如权利要求 9 所述的方法,其中,

当发现远程安装到授权域中的设备在所述主设备的本地附近时,增大 Local_count 并同时减小 Remote_count。

12. 如权利要求 4 至 5 中任一项所述的方法,其中,所述方法还包括将主设备功能在两个装置之间分割的步骤,

所述分割步骤包括在两个主设备之间分割上限值 Total_limit、Local_limit 和 Remote_limit 以及当前值 Local_count 和 Remote_count。

13. 如权利要求 12 所述的方法,其中,主设备功能的授权分割的数量被限制为预定数量。

14. 一种包含主设备功能的装置 (200),用于控制授权域 (1) 中安装的设备 (21、22、23、34、31、41、42、51) 的数量,所述装置包括:

存储器 (202),能够存储以下数量的上限值:

- 在所述授权域中安装的设备总数 Total_limit ;

- 在所述主设备本地附近安装的设备总数 Local_limit ;以及

- 与所述主设备远程安装的设备总数 Remote_limit ;

并能够存储以下数量的当前值:

- 授权域中在所述主设备本地附近安装的设备数量 Local_count ;以及

- 授权域中与所述主设备远程安装的设备数量 Remote_count ;以及

其中所述存储器还能够存储授权域中安装的所有设备的总数 Total_count,或者所述主设备包括用于根据 Local_count 和 Remote_count 来计算 Total_count 的装置;

用于从新设备接收安装请求的装置;

用于验证 Total_count 尚未达到 Total_limit 的装置;

用于在成功验证的情况下检查所述新设备是否在所述主设备的本地附近的装置;

用于在发现所述新设备是本地设备的情况下、在允许本地安装之前验证 Local_count 尚未达到 Local_limit 的装置;以及

用于在发现所述新设备是远程设备的情况下、在允许远程安装之前验证 Remote_count 尚未达到 Remote_limit 的装置。

用于控制授权域中安装的设备数量的方法和装置

技术领域

[0001] 本发明一般地涉及通信网络中的内容保护,更具体地,涉及授权域管理。

背景技术

[0002] 近来,授权域(AD)的概念被定义为属于同一个家庭的成员的用于接收、存储或消费内容的设备集合。在这里的上下文中,家庭不应被视为单个位置(主住宅)。实际上,授权域可以包括位于度假住宅、汽车中的设备或甚至手持设备。

[0003] 图1示出了授权域1的示例,包括位于主住宅2中的设备集合:数字电视21、个人电脑23、游戏控制台24和存储单元22;另一台数字电视31位于第二住宅3中;可以带出住宅的如个人数字助理41和便携式播放器42之类的移动设备,以及位于汽车5中的移动设备51(例如便携式视频播放器)。可以以多种方式向授权域中的设备传递内容:例如它可以是经由天线6接收的广播内容;它可以是经由如因特网7之类的开放网络接收到的宽带的、按需提供的内容,或它可以是存储在如光盘8之类的介质上的内容。

[0004] 过去几年中,多个工作组(例如TV-Anytime论坛或DVB-CPT-DVB组织的数字视频广播内容保护技术分组)致力于授权域概念的工作。产业也已经提出了实现解决方案,如SmartRight™建议(关于它的信息可以在www.smartright.org上找到)。

[0005] 在授权域中,通常根据其内容所扮演的角色来区分设备。例如,在SmartRight™系统中,内容经由接入设备(也称为获取设备)进入授权域,该内容被存储在存储实体中,并由表现设备消费或导出。类似的功能实体在DVB-CPCM系统(“CPCM”代表“内容保护和拷贝管理”)中定义,当前由DVB-CPT规定,并在图2中示出。

[0006] 在图2中,由内容提供者提供的输入内容110,经由获取点101进入授权域100。这个实体对输入内容执行一些处理,以获得授权域1指定的内容120。该AD指定内容120可以由存储实体102存储在授权域中,以供以后消费。该内容可以由处理实体103处理(例如,进行压缩以将该内容传递至低分辨率设备)。最终,可以经由消费点104消费该AD指定内容,在消费点104中,该内容被呈现(例如以声音和图像的形式)给用户,以获得所谓的消费内容130。该AD指定内容也可以经由导出点105导出,以获得导出内容140,该导出内容140不再由授权域规则保护,而是优选地由另一个系统保护。当然,可以在单个装置中实现两个或更多上述功能(例如,具有内部硬盘的机顶盒同时是获取点和存储实体;具有模拟输出的集成数字电视是消费点和导出点)。

[0007] 应注意,若内容提供者要求AD指定内容与获得该内容的授权域绑定(例如在输入内容所附的使用权中),则AD指定内容与获得该内容的授权域绑定。这意味着,该授权域中的每个消费点可以消费这样的AD指定内容,而不同授权域的任何设备都不能消费该内容。

[0008] 因此,授权域管理对于限制授权域的大小和/或范围非常重要。实际上用户可能对未限制的授权域感兴趣,以便能够与其他人分享其内容,但是,内容提供者要求将授权域的大小仅限制在单个家庭的成员的需要之内。

[0009] 一个基本的解决方案可以是,限制一个授权域中的总的设备数量,但是,难以估计

单个家庭的“正常的”设备数量。此外，只对设备的数量计数具有不利的副作用。例如，两个 1MByte 的存储实体（例如 USB 钥匙）将被计为两个设备，而一个 10GByte 的存储实体（例如硬盘驱动器）将仅被计为一个设备。

[0010] 因此，需要一种安全解决方案，用于限制授权域的大小 / 范围，这种解决方案对大多数诚实的用户是透明的，大多数诚实的用户不会注意到它，但该解决方案可以防止欺诈用户绕开它。

发明内容

[0011] 本发明的目的是提供一种用于控制包含至少一个主设备的授权域中安装的设备数量的方法，所述主设备能够存储以下数量的上限值：

[0012] - 在授权域中安装的设备总数 Total_limit；

[0013] - 在主设备本地附近安装的设备总数 Local_limit；

[0014] - 与所述主设备远程安装的设备总数 Remote_limit；

[0015] 当所述主设备接收到来自新设备的安装请求时，所述方法包括以下步骤：

[0016] 验证尚未达到 Total_limit，以及

[0017] 在验证成功的情况下，检查该新设备是否是在所述主设备的本地附近，以及

[0018] 在发现新设备是本地设备的情况下，在允许本地安装之前，

[0019] 验证尚未达到 Local_limit；

[0020] 在发现新设备是远程设备的情况下，在允许远程安装之前，

[0021] 验证尚未达到 Remote_limit。

[0022] 根据本发明的具体实施例：

[0023] - 上限值 Local_limit 大于上限值 Remote_limit；

[0024] - 上限值 Total_limit 大于上限值 Local_limit 和 Remote_limit 之和。

[0025] 根据另一个实施例，所述主设备还能够存储以下数量的当前值：授权域中所述主设备本地附近安装的设备数量 Local_count；以及与所述主设备远程安装的设备数量 Remote_count；以及所述方法还包括以下步骤：在发现新设备是本地设备且 Local_count 的数量等于或大于 Local_limit 的情况下，检查授权域中安装且此时在所述主设备的本地附近连接的设备的数量是否大于 Local_count 的预定有效数量 (quorum)；其中，只有所述检查成功时才本地安装所述新设备。

[0026] 根据其他具体实施例：

[0027] - 在本地安装新设备时，增大 Local_count；或在远程安装新设备时，增大 Remote_count；

[0028] - 只有在新设备能够消费和 / 或导出内容时，才增大 Local_count 或 Remote_count；

[0029] - 在新设备能够消费和导出内容时，把 Local_count 或 Remote_count 增大一个单位；

[0030] - 当发现远程安装到授权域中的设备在所述主设备的本地附近时，增大 Local_count 并同时减小 Remote_count；

[0031] - 所述方法还包括将主设备功能在两个装置之间分割的步骤，所述分割步骤包括

在两个主设备之间分割上限值 Total_limit、Local_limit 和 Remote_limit 以及当前值 Local_count 和 Remote_count。

[0032] 本发明的目的还在于提供一种包含主设备功能的装置,所述主设备功能用于控制授权域中安装的设备的数量,所述装置包括:

[0033] 存储器,能够存储以下数量的上限值:在授权域中安装的设备的总数 Total_limit;在主设备本地附近安装的设备的总数 Local_limit;与所述主设备远程安装的设备的总数 Remote_limit;

[0034] 所述存储器能够存储以下数量的当前值:授权域中所述主设备本地附近安装的设备的数量 Local_count;以及授权域中与所述主设备远程安装的设备的数量 Remote_count;

[0035] 用于实现上述控制授权域中新设备的安装的方法的装置。

附图说明

[0036] 现在参照附图,仅以示例的方式描述本发明的各个特征及其优选实施例,其中:

[0037] 图 1,上文已经讨论过,示出了典型的授权域的示例;

[0038] 图 2,之前已经讨论过,示出了授权域中的不同类型的设备;

[0039] 图 3 示出了被称为主设备的具体设备的框图;

[0040] 图 4 示出了在本地安装的具体示例中,要在授权域中安装的新设备与该 AD 的主设备以及该 AD 的其他设备之间所交换的消息;

[0041] 图 5 和图 6 分别示出了要在授权域中安装的新设备和该授权域的主设备的状态图。

具体实施方式

[0042] 在根据本发明来管理的授权域中,处理三个不同的大小计数:

[0043] - 一个 (Local_count) 针对在本地安装的设备的数量;

[0044] - 一个 (Remote_count) 针对从远程位置安装的设备的数量;

[0045] - 一个 (Total_count) 针对授权域中安装的设备的总数 (该 Total_count 实际上是前两者的总和)。

[0046] 优选地,对于这些计数,只考虑执行消费点或导出点功能的设备。

[0047] 这些计数由主设备维护,所述主设备是授权域中唯一能够安装消费和导出点的设备。获取点、存储和处理实体可以由授权域中的任何设备安装。

[0048] 该主设备功能可以由授权域中任何设备来实现,优选地,被实现为 AD 中的单个设备。如图 3 所示,主设备是设备 200,包括安全处理器 (CPU 201) 和安全存储器 202。可以使用智能卡或 TCPA 类型的平台来实现这些组件的安全性 (在图 3 中以虚线矩形代表) (TCPA 代表“可信计算机平台联盟”)。对于安全存储和处理也存在模糊 (obfuscation) 技术。这些技术可以单独使用,或与智能卡或 TCPA 结合。安全存储器 202 能够存储用于该主设备 200 所属的授权域的 Local_count 和 Remote_count。在一个实施例中,安全存储器 202 也存储 Total_count。选择性地,在存储器 202 中,Total_count 不作为单独的计数存储;每次需要检查 AD 中安装的设备的总数时,从其他两个计数推导出 Total_count。

[0049] CPU 201 能够执行实现下文说明的方法的程序,以控制 AD 的大小 / 范围。

[0050] 主设备 200 还包括网络接口 203,用于永久或暂时与住宅网络和 / 或开放网络连接,从而与 AD 的其他设备通信。网络接口 203 能够实现已知的有线和 / 或无线传送协议,如 IP、IEEE 1394 或 802.11b。优选地,主设备 200 也包括用户接口 204。

[0051] 给定设备的本地或远程位置的概念相对于主设备来定义。例如,在图 1 所示的授权域中,若主设备是 PC 23,则作为一种消费点的 DTV121 将被计入主设备 23 中存储的 Local_count,而 DTV231 将被计入主设备 23 中存储的 Remote_count。至于作为另一种消费点的便携式播放器 42,若其在 AD 中登记时对于主设备 23 而言是本地设备,则它将被认为是本地的(并被计入 Local_count)。这没有妨碍该便携式设备以后移出主住宅 2 之后的使用。我们将在以后看到,在选择性实施例,可以将主设备功能分割到两个或更多设备中,这些设备优选地彼此远离。

[0052] 对于上述 3 个计数中的每一个,还定义了上限并存储在主设备中。这些限制是:

[0053] -Total_limit 为高(正常的用户永远不会达到该限制);

[0054] -针对远程安装的设备的限制 Remote_limit 为低(以控制远程安装);

[0055] -针对本地安装的设备的限制 Local_limit 合理;以及

[0056] -Remote_limit 与 Local_limit 的和应远小于总限制。

[0057] 当 AD 的主设备接收到在该 AD 中安装新设备的请求时,适用以下规则:

[0058] 若 Total_count 达到 Total_limit,则拒绝该安装。

[0059] 若新设备是远程设备,而 Remote_count 达到 Remote_limit,则拒绝该安装。

[0060] 若新设备是本地设备,而 Local_count 等于或大于 Local_limit,则进行有效数量测试。该测试在于检查此时在主设备附近连接的 AD 的设备的数量。对此,主设备在其所连接的网络上广播消息,并只接受来自该 AD 且位于该主设备附近的设备的响应。仅当所接收的响应的数量表示 Local_count 的特定有效数量时,有效数量测试才通过。若该测试失败,则拒绝新设备的安装。选择性地,该有效数量测试可以基于 Total_count 的特定有效数量。

[0061] 在所有其他情况下,进行新设备的安装。Total_count 增加。若新设备在该主设备的附近,则 Local_count 也增加,否则 Remote_count 增加。

[0062] 上限值 Total_limit、Remote_limit 和 Local_limit 由独立的授权方确定,该授权方决定哪个数量对于“正常”用户而言是合理的。优选地在制造过程中,对可能用作主设备的所有设备输入这些限制。该独立授权方还定义了授权代理规则,所述规则授权代理(例如设备中的软件模块或特定用户)在一旦得到验证时更新这些上限值。当用户受到一个或多个上限值的影响时,该用户可以请求经验证的授权代理增大一个或多个上限值。

[0063] 应注意,主设备功能可以从 AD 中的一个设备转移到 AD 中的另一个设备。优选地,这样的转移只可以在本地进行,或应限制远程转移的次数。在这种情况下,当前计数和上限值也应被转移给新的主设备。

[0064] 当家庭中的用户决定从授权域中移除一个设备时(例如将其售出或将其借给该家庭之外的用户),根据由主设备所检测到的所移除的设备的位置,减小 Local_count 或 Remote_count,也减小 Total_count。当一个设备丢失或被盗时,它不能再与主设备交换消息,因此不能与主设备执行邻近测试(用于检测设备的位置,将在以后描述)。在这种情况下,优选地,我们选择减小 Local_count。也减小 Total_count。应注意,若相关计数

(Remote_count 或 Local_count) 已经为 0, 则减小另一个计数。

[0065] 在本发明的一个实施例中, 提供了一种机制 (将在以后详细描述), 若例如一个远程安装的设备之后被发现为本地的 (例如, 在度假期间带走的便携式播放器首先是与主设备远程安装的, 接着与主住宅的住宅网络连接), 则该机制用于重新平衡 Local_count 和 Remote_count。

[0066] 如上所述, 也可以将控制功能一分为二 (或更多), 以在一个授权域中获得两个或更多主设备。在这种情况下, 也应在主设备之间分割三个计数 Local_count、Remote_count 和 Total_count 以及上限值 Local_limit、Remote_limit 和 Total_limit。例如, 在分割之后, 两个主设备的 Local_count1 和 Local_count2 之和应等于先前唯一的主设备的 Local_count。主设备之间的计数的平衡可以自动决定 (例如在主设备之间相等地共享), 或可以由执行主设备分割的 AD 的用户来决定。优选地, 为主设备功能的分割的数量设置上限, 并且该上限与其他计数和上限值一起存储在主设备的安全存储器中。

[0067] 在选择性实施例中, 在分割其他计数和上限值时, 无需分割上限值 Total_count。同样, 应注意, 与远程转移受到限制或可以仅限于本地转移的主设备功能转移相反, 优选地, 允许主设备功能在远程设备之间分割。实际上, 分割主要关心的是允许每个 AD 位置中都有具有主设备的用户。

[0068] 在图 4 中, 我们示出了在授权域中安装新设备 300 的示例, 该授权域已经安装有主设备 302 和其他设备 304。当与住宅网络连接时, 在步骤 306, 新设备 300 在该网络上广播主请求 (Master Request) 消息, 请求主设备应答。网络的其他设备只有当其为为主设备时才应答。在图 4 中, 我们假定主设备 302 接收到主请求消息。接着, 在步骤 308, 主设备检查 Total_count 的值。若 Total_count 小于上限值 Total_limit, 则在步骤 310, 主设备发起与该新设备的邻近测试, 以得知对于该主设备的位置来说该新设备应计为本地设备还是远程设备。

[0069] 优选地, 邻近测试使用一种用于安全测量两个设备之间基于时间的距离的方法, 该方法在当前的欧洲专利申请的申请人于 2005 年 6 月 20 日提出申请的欧洲专利申请 No. 05300494.1 中公开。为此, 主设备 302 向该新设备 300 发送一系列“ping”命令 312, 并等待“ping”响应 314。对于每个接收到的响应 314, 主设备计算相关联的被称为往返时间 (RTT) 的基于时间的距离。若该主设备获得了一个小于给定限制 (例如 7ms) 的 RTT, 则它认为该新设备在其本地附近, 并向该新设备发送另一消息 (图 4 中未示出) 以请求鉴权数据 (如在上述专利申请中所解释)。主设备验证该新设备响应该请求而发送的鉴权数据, 以确认用于计算 RTT 的 ping 响应的源。若主设备进行的所有这些验证都成功, 则认为该新设备是本地设备。否则, 认为该新设备是远程设备。

[0070] 若该新设备是远程设备, 则主设备检查 Remote_count。若 Remote_count 小于 Remote_limit, 则主设备向该新设备建议远程安装。否则 (Remote_count 大于或等于 Remote_limit), 主设备向该新设备发送消息, 发信号通知拒绝该安装。

[0071] 若该新设备是本地设备 (如图 4 的示例中的情况), 则主设备检查 (步骤 316) Local_count。若 Local_count 小于 Local_limit, 则向该新设备建议本地安装。在 Local_count 大于或等于 Local_limit 的情况下, 主设备发起与网络中的其他设备的有效数量测试 (图 4 中的步骤 318): 它首先在网络上广播发现消息 320。优选地, 该发现消息包含随机

数 R (由主设备产生或获得) 以及授权域标识符 AD_ID 作为质询。每个授权域一旦建立就具有该 AD 的所有安装设备都知道的唯一标识符 AD_ID。

[0072] 当 AD 中的其他设备 304 接收到该发现消息时, 它们使用消息 322 应答, 该消息 322 包括其自身的标识符 Device_ID 以及根据随机数 R 及其自身的标识符 Device_ID 使用密钥计算出的鉴权数据。优选地, 使用 HMAC-SHA1 函数以及授权域的密钥 AD_key 计算该鉴权数据。在授权域中, 所有安装的设备通常共享指定用于该 AD 的密钥 :AD_key。选择性地, 可以使用在安全验证通道 (SAC) 中建立的并在主设备和计算应答消息 322 的设备 304 之间共享的会话密钥来计算鉴权数据。

[0073] 接着, 主设备 302 检查所接收的应答的有效性 (通过验证消息 322 中的鉴权数据), 以确保它只接收来自该授权域的设备响应, 主设备 302 检查 (步骤 324) 正确应答的数量是否足够通过有效数量测试。例如, 若有效数量的比值是 1/2, 则应出现一半数量的本地设备 (即 Local_count/2)。因此, 在步骤 324 检查所接收的正确应答的数量是否大于 Local_count/2。若检查成功, 则主设备 302 在步骤 326 发起与发送正确应答 322 的每个其他设备 304 的邻近测试。如之前所解释的那样进行邻近测试: 从主设备向每个有关的其他设备 304 发送 “ping” 命令 328, 从每个其他设备接收 “ping” 响应 330, 并在主设备中利用鉴权数据来检查该响应。

[0074] 接着, 主设备对通过邻近测试的 (即在其本地附近的) 所有设备进行计数, 并检查 (步骤 332) 该数量是否大于有效数量所需的数量 (即在上述示例中是否大于 Local_count/2)。若通过有效数量测试 (如图 4 所示的示例), 则主设备向该新设备建议本地安装 (步骤 334)。否则, 主设备向该新设备发送消息, 发信号通知拒绝该安装。

[0075] 当该新设备从一个或多个主设备 (在控制功能在两个或更多设备之间分割的情况下) 接收到安装建议时, 它要求用户选择一个建议 (步骤 336), 优选地, 用户选择优先于建议本地安装的主设备。接着, 该新设备向所选择的主设备发送安装请求 (步骤 338), 然后安装过程开始 (更新主设备中的计数、向成为域设备的该新设备发送该授权域的标识符 AD_ID 以及可能地还有密钥 AD_key, 等等)。

[0076] 现在参照图 5, 从请求被安装到 AD 中的新设备的立场, 解释授权域大小管理的协议。

[0077] 首先, 该设备处于 “新设备” 状态 400。从这个状态, 当它第一次与住宅网络连接时, 它广播 401 主请求消息。接着, 它启动 402 超时 T_v 并在预定的时间 T_v 期间等待 403。在这个等待中, 若该设备接收到邻近测试请求 (例如以 “ping” 命令的形式), 则它与发送该请求的主设备进行邻近测试 405, 并返回等待状态 403。应注意, 若多个主设备应答主请求消息, 则在该超时期满之前, 可能进行多个邻近测试。当预定的时间 T_v 期满 406 时, 该设备检查 407 其是否接收到来自主设备的任何响应。若接收到 408 响应, 则该设备检查 409 是否接收到本地安装建议。若主设备没有建议 410 本地安装, 则该设备检查 411 是否接收到远程安装建议。若没有建议 412 远程安装, 则意味着该设备只从响应其主请求消息的主设备接收到否定应答 (安装被拒绝)。在这种情况下, 优选地, 应将该失败 (通过该设备的用户接口) 通知给用户, 然后该设备返回 “新设备” 状态 400。

[0078] 若向该设备建议远程安装 413 或本地安装 414, 则它让用户选择一个建议 415, 并与发送该安装建议的主设备运行安装协议, 以进入 “域设备” 状态 416。选择性地, 在该设备

没有用户接口的情况下,可以采用自动选择。

[0079] 当在超时 T_v 期满之后没有接收到 418 响应的情况下,该设备建议用户创建新的网络。若用户接受,则该设备 419 在进入“主设备”状态 420 之前,随机选择 AD_key 并初始化计数 ($Local_count = 1$; $Remote_count = 0$ 以及 $Total_count = 1$)。

[0080] 现在,参照图 6,从主设备的立场,解释授权域大小管理协议。优选地,该协议在主设备的安全处理器中执行。

[0081] 该协议从“主设备”状态 500 开始,此时主设备从请求被安装到授权域中一个新设备接收控制请求。该主设备首先将 $Total_count$ 与上限值 $Total_limit$ 进行比较 502。在 $Total_count$ 大于或等于 $Total_limit$ 的情况下,该主设备向做出请求的新设备发送 504 消息,通知该新设备安装被拒绝,然后该主设备返回“主设备”状态 500。

[0082] 当 $Total_count$ 小于 $Total_limit$ 时,如之前所解释的,该主设备发起 506 与该新设备的邻近测试。若在预定的时间 T_v 508 期满之前没有从该新设备接收到响应,则认为该新设备是远程设备。当在邻近测试期间从该新设备接收到至少一个响应时,该主设备检查 510 该新设备是远程的 (512) 还是本地的 (514)。若该新设备是远程的,则检查 516 $Remote_count$ 。若 $Remote_count$ 小于上限值 $Remote_limit$,则向该新设备发送 518 远程安装建议。否则 ($Remote_count$ 等于或大于 $Remote_limit$),则向该新设备发送 504 安装拒绝消息,然后该主设备返回“主设备”状态 500。

[0083] 若该新设备是本地的,则检查 520 $Local_count$ 。若 $Local_count$ 小于 $Local_limit$,则向该新设备发送 522 本地安装建议。否则 ($Local_count$ 等于或大于 $Local_limit$),则该主设备通过在网络上广播发现消息并启动超时 T 来发起 524 有效数量测试。接着,该主设备在预定的时间 T 期间等待 526。在等待期间,若接收 528 到任何其他设备的响应,则该主设备验证 530 响应消息中的鉴权数据 (例如之前所解释的使用 HMAC-SHA1 计算的消息鉴权码),以检查该响应是否由属于该授权域的设备发送。若该验证失败,则忽略 523 该响应消息,该主设备返回等待状态 526。若该验证 530 成功,则该响应消息被计为 534 正确,然后该主设备返回等待状态 526。

[0084] 当预定的时间 T 期满 536,将所接收到的正确响应消息的数量与通过该测试所需的有效数量进行比较 538。若该有效数量是例如 $Total_count$ 的一半,则检查 538 正确消息的数量是否大于 $Total_count/2$ 。作为选择性的优选实施例,通过该测试所需的有效数量是 $Local_count$ 的一半。若该检查失败,则应向该设备发送 504 安装拒绝消息,然后该主设备返回“主设备”状态 500。否则 (成功检查 538),与发送正确响应消息的每个设备执行 540 邻近测试。在这些测试结束时,只对在主设备本地附近的设备进行计数,以验证 542 有效数量 (即,如图 6 所示,本地设备的数量大于 $Total_count/2$,或在选择性实施例中,大于 $Local_count/2$)。若有效数量测试最终成功,则向该新设备发送 522 本地安装建议;否则发送 504 安装拒绝消息。

[0085] 当发送了远程安装建议 518 或本地安装建议 522 时,该主设备启动另一个超时 T_w ,并等待 544 来自该新设备的响应。当该预定的时间 T_w 期满时,该主设备检查 546 是否从该新设备接收到请求安装的任何响应。若接收到安装请求,则该主设备与该新设备运行 548 安装协议;否则,该主设备返回“主设备”状态 500。

[0086] 以下给出针对授权域的上限值的示例:

[0087] -Total_limit :20 个设备

[0088] -Local_limit :6 个设备

[0089] -Remote_limit :2 个设备

[0090] - 主设备分割数量的上限 :2。

[0091] 两个授权的远程安装（与两个授权的主设备分割一起）使用户能够在其主住宅和其他两个住宅中拥有主设备。在这种授权域中，移动设备（包括车载设备）可以在上述任何位置中本地安装。

[0092] 根据上述值，分割的示例如下。我们假定，在 AD 生存期间的一个时间，计数的当前值如下：

[0093] -Total_count :9 个设备

[0094] -Local_count :8 个设备（在这种情况下，由于 Local_count > Local_limit，我们假定通过有效数量测试已安装 2 个设备）

[0095] -Remote_count :1 个设备

[0096] - 主设备分割数量 :0。

[0097] 这意味着，此时，未发生主设备分割，已经远程安装了一个设备（例如在第二住宅中的电视机）并本地安装了 8 个设备（例如 4 台电视机、一台在主室中——主设备，一台在厨房，且每个卧室一台、1 台 DVD 播放器在汽车中，2 台 PC 和一台便携式播放器）。我们假定，一个用户 Alice 要在她的第二住宅中也安装一台 PC。当然，她可以远程安装它，但是这将意味着以后她再也不能安装远程设备。因此，她更希望在她的主室中的电视机和在她的第二住宅中的电视机之间分割主设备功能。为此，她为计数和上限值设定了以下新的值：

[0098] - 用于主室中的主设备 TV 的新上限值 :Total_limit = 15, Local_limit = 4, Remote_limit = 2, 最大主设备分割 = 2；

[0099] - 用于第二住宅中新的主设备的上限值 :Total_limit = 5, Local_limit = 2, Remote_limit = 0, 最大主设备分割 0；

[0100] - 用于主室的主设备 TV 的新计数 :Total_count = 8, Local_count = 8, Remote_count = 0, 主设备分割 = 1；

[0101] - 用于第二住宅中的新的主设备的新计数 :Total_count = 1, Local_count = 1, Remote_count = 0, 主设备分割 = 0。

[0102] 根据这些值，Alice 能够毫无问题地在其第二住宅中安装多达 4 个设备。应注意，在第二住宅中要安装的第二个设备的安装将不需要通过有效数量测试，而以下则需要（由于将会达到 Local_limit）。

[0103] 现在给出重新平衡的示例。我们假定该用户 Alice 拥有与上述相同的配置（分割前）。计数器的值如下：

[0104] -Total_count :9 个设备

[0105] -Local_count :8 个设备

[0106] -Remote_count :1 个设备

[0107] - 主设备分割数量 :0。

[0108] 在出差期间，她购买了一台新的便携式播放器（另一台是她的女儿的），当然，她等不及回家再享受她的新设备。因此，她远程安装该设备（计数器的新的值是：

[0109] -Total_count :10 个设备

[0110] -Local_count :8 个设备

[0111] -Remote_count :2 个设备

[0112] - 主设备分割数量 :0)。

[0113] 当她回到家时,她将该便携式播放器连接到她的住宅网络。主设备电视机检测到设备已连接,并发现该设备是本地地连接到该网络。它数出 9 个设备(我们假定此时汽车就在房子前)而本地设备的当前计数只有 8。因此,该主设备认定,一个远程安装的设备现在变为本地,并决定在满足以下条件之一的情况下更新计数:

[0114] -Local_count 小于 Local_limit 或

[0115] -若 Local_count 等于或大于 Local_limit,并且如之前所解释的有效数量测试通过(例如基于 Local_count 的一半)。

[0116] 在这种情况下,Local_count 被设置为当前存在的本地设备的数量,而 Remote_count 被设置为总计数和(新的)本地计数之间的差:

[0117] -Total_count :10 个设备

[0118] -Local_count :9 个设备

[0119] -Remote_count :1 个设备

[0120] - 主设备分割数量 :0。

[0121] 多亏重新平衡机制,Alice 仍享有安装远程设备的可能性。若没有该机制,Alice 要等到回到家才能安装她的新便携式播放器,以便不失去该可能性。

[0122] 本发明的优点如下:

[0123] - 高灵活性:正常的用户能够不受限制的安裝移动设备,以及第二住宅中的设备;

[0124] - 对远程安装的控制:在多个远程位置安装设备的能力方面,限制不诚实的用户;

[0125] - 安全:不容易绕开该解决方案。

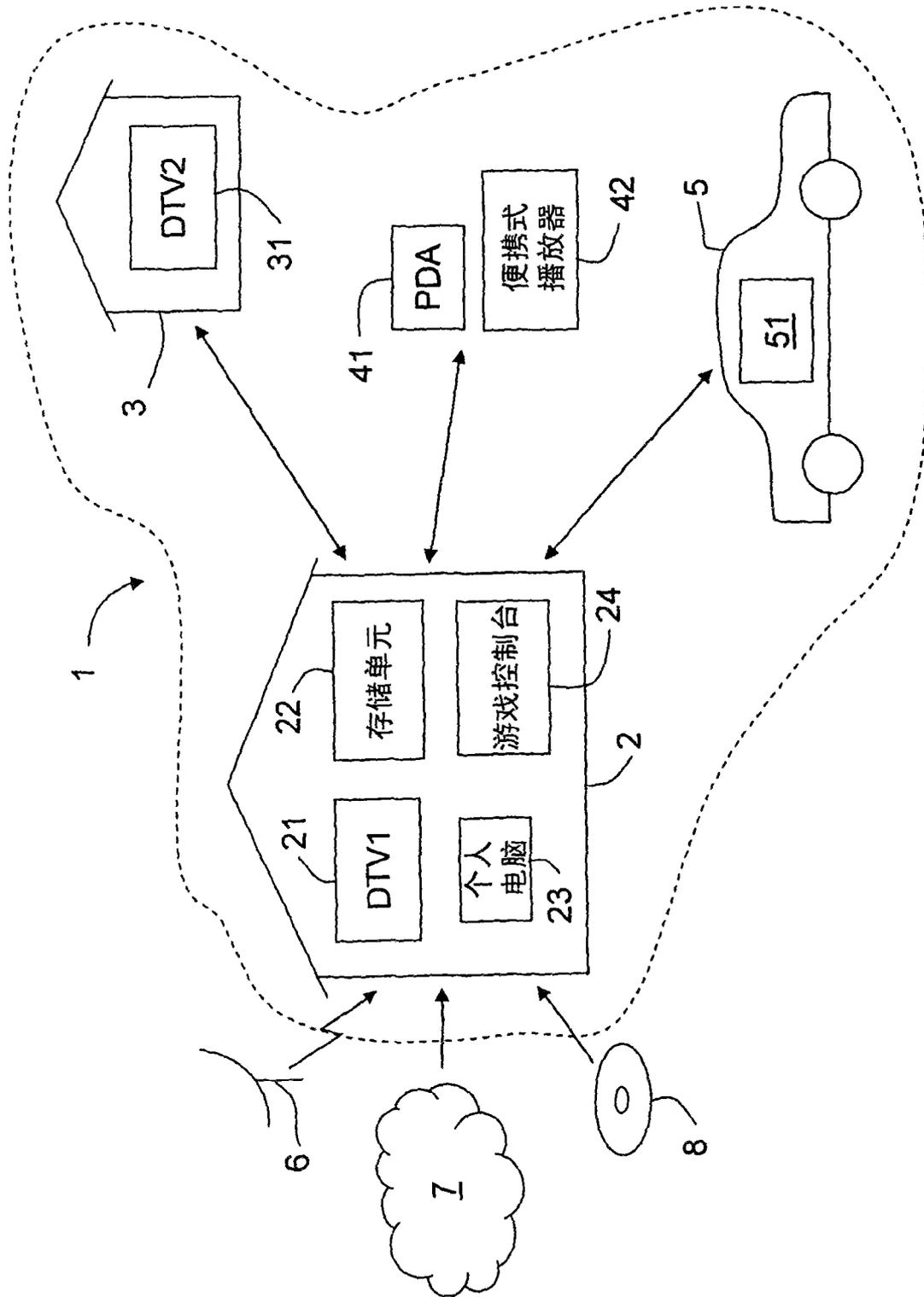


图1

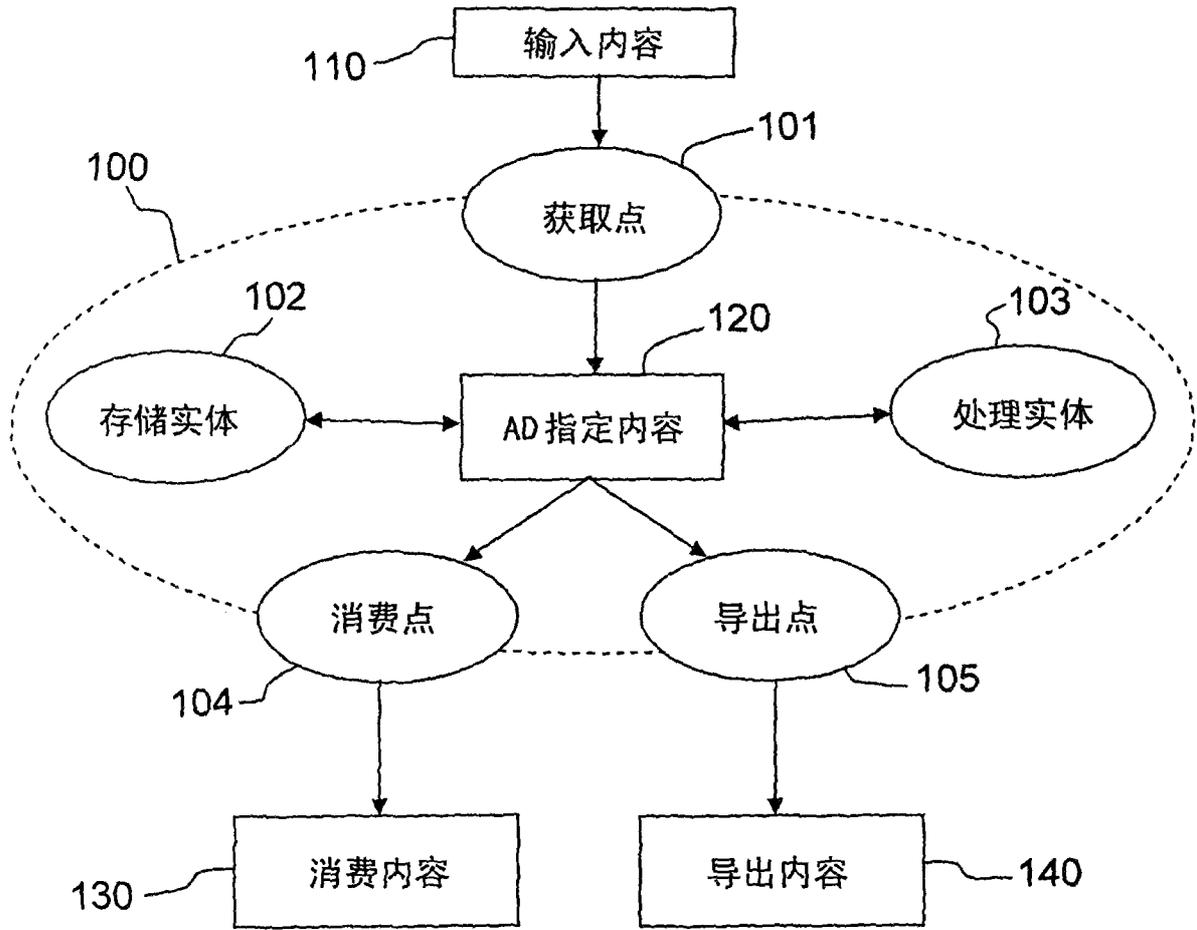


图 2

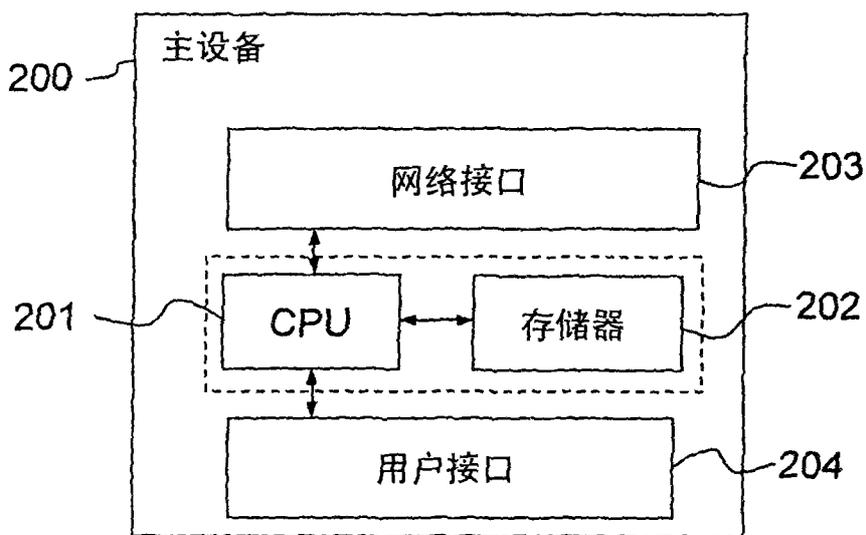


图 3

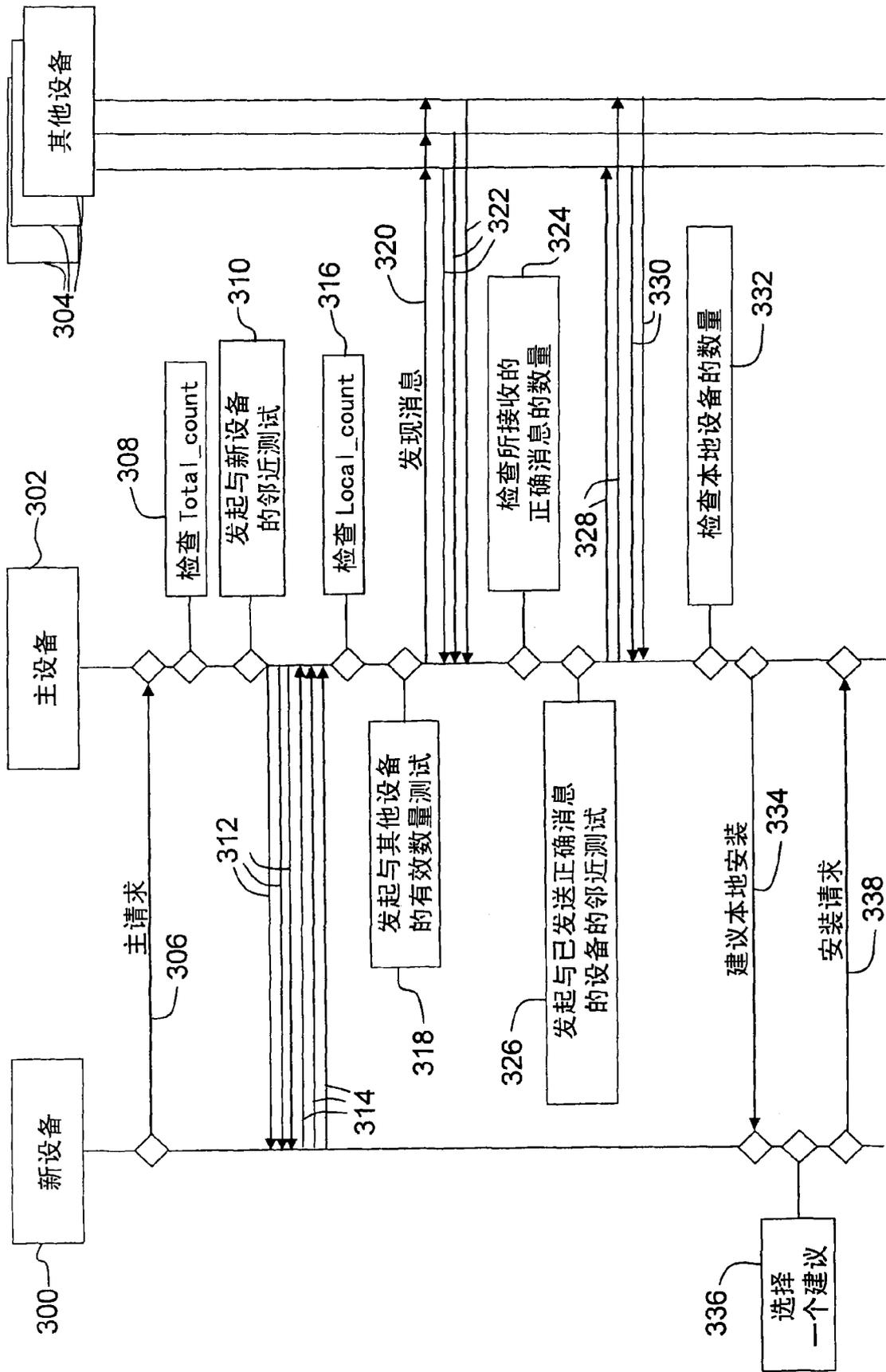


图 4

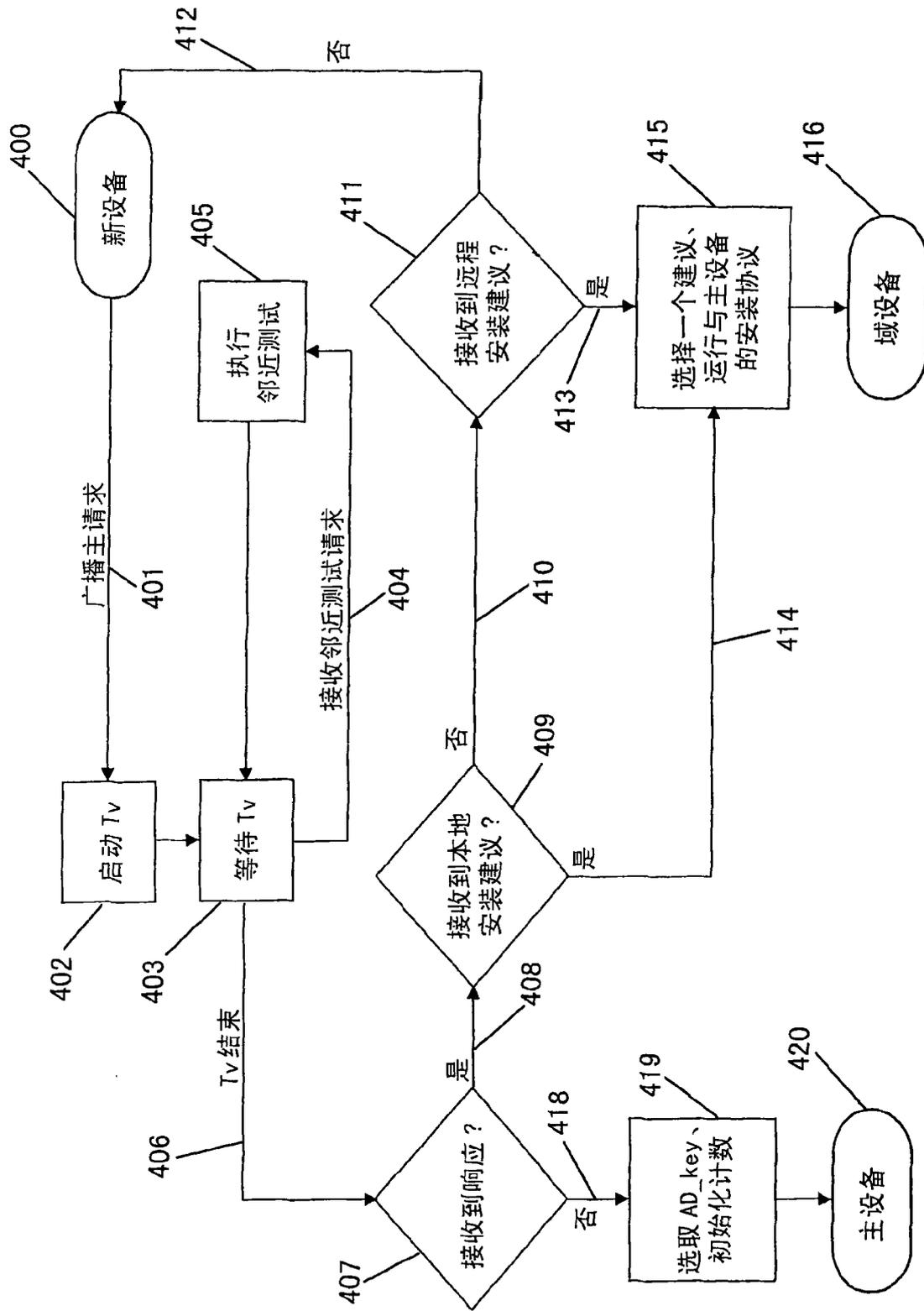


图 5

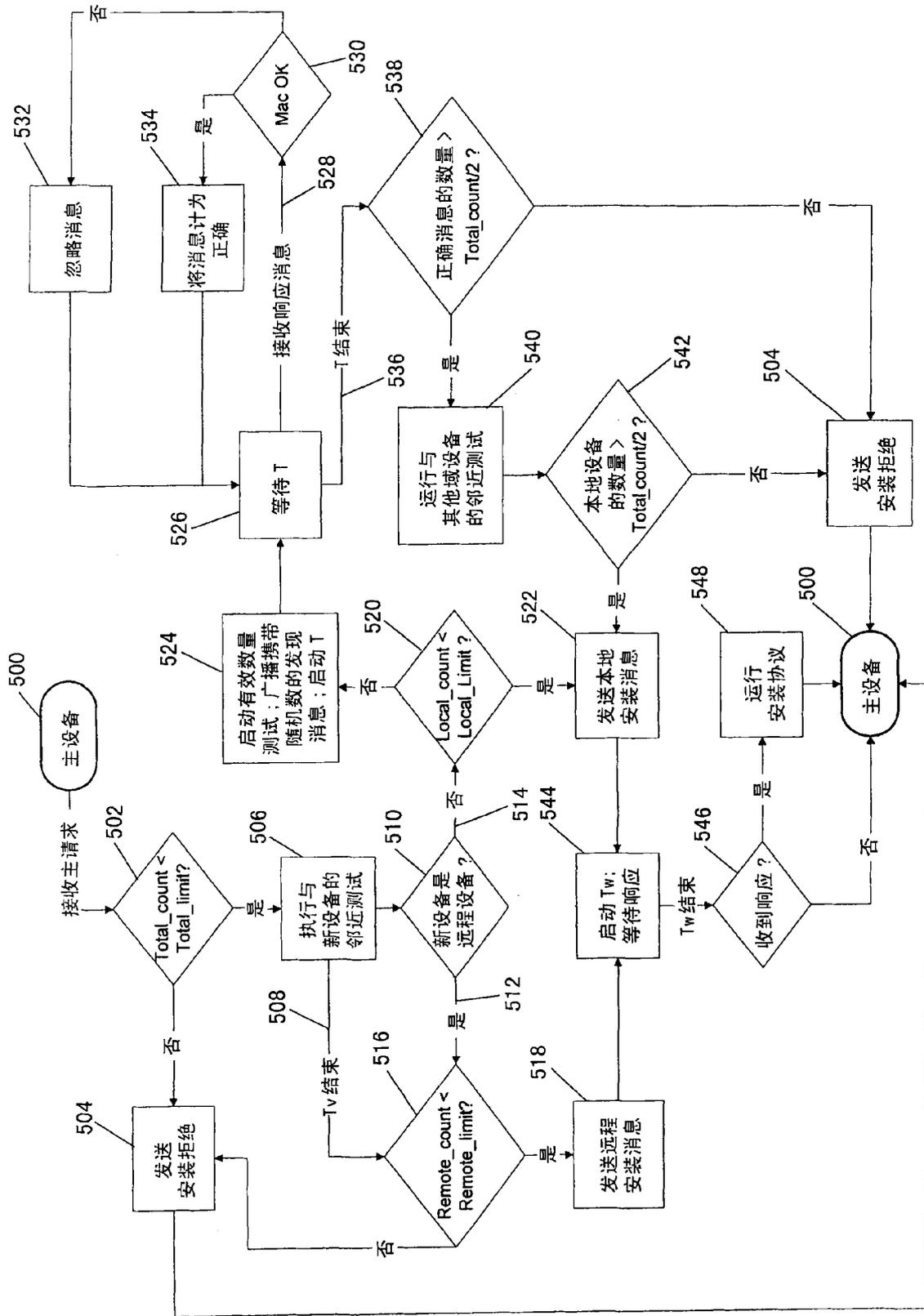


图 6