[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/28 (2006.01)
H04L 9/12 (2006.01)
H04L 9/30 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410080583.X

[45] 授权公告日 2007 年 9 月 19 日

[11] 授权公告号 CN 100338919C

[22] 申请日 2004.10.8
[21] 申请号 200410080583.X
[30] 优先权
[32] 2003.10.2 [33] KR [31] 03-68837
[73] 专利权人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 韩声休 金明宣 赵贞衍 崔良林
[56] 参考文献
US6584096B1 2003.6.24
US6198479B1 2001.3.6
US6580950B1 2003.6.17
US6393467B1 2002.5.21
审查员 郭风顺

[74] 专利代理机构 北京铭硕知识产权代理有限公司
代理人 郭鸿禧

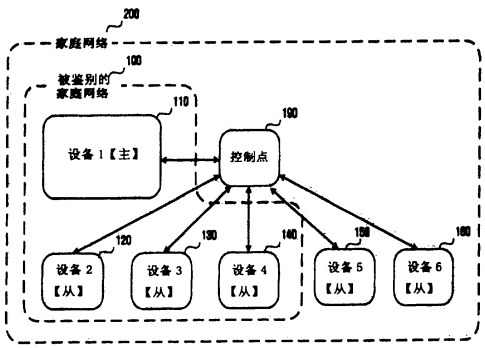
权利要求书 2 页 说明书 11 页 附图 12 页

[54] 发明名称

基于公共密钥构建域并通过通用即插即用执行该域的方法

[57] 摘要

一种在基于公共密钥体系结构中构建用于防止内容被未授权的第三人非法使用的唯一域，并使用通用即插即用(UPnP)将被创建的域应用到家庭网络中的方法。本发明的方法包括：选择作为主设备工作的被控设备中的一个，并且确定被选设备作为主设备；在这种其他被控设备从被确定的主设备接收秘密信息块并且创建证书的方式下执行设备鉴别；和通过在被鉴别的被控设备之中选择一个或多个设备来确定从设备。



1、一种基于公共密钥构建域并使用通用即插即用实施该域的方法，从而在家庭网络中在基于公共密钥的体系结构中可创建唯一域，以允许仅仅被授权的用户使用内容，包括:

(a) 选择作为主设备工作的被控设备中的一个，并且确定被选的被控设备中的一个作为主设备;

(b)由所确定的主设备基于证书对其它被控设备执行设备鉴别，其中，所述证书由所述被控设备使用从主设备接收的秘密信息块来创建；和

(c)通过在被鉴别的被控设备之中选择一个或多个设备来确定从设备。

2、如权利要求 1 所述的方法，其中，步骤(a)包括:

通知控制点被控设备被连接;

由控制点获得被控设备的设备信息和数字版权管理信息;

通过使用数字版权管理信息在被控设备之中选择主设备；和

将被选主设备的被控设备中的一个设置为主模式并且向被控设备提供设备列表。

3、如权利要求 1 所述的方法，其中步骤(b)包括:

由被确定的主设备从外部服务器接收秘密信息块;

向除了主设备之外的被控设备传送接收到的秘密信息块;

使用被传送的秘密信息块提取秘密值并创建证书；和

在接收到被创建的证书、设备 ID 和公共密钥之后，检验证书并准备被鉴别设备的列表。

4、如权利要求 1 所述的方法，其中，步骤(c)包括:

如果在步骤(b)中被鉴别的设备不具有域属性，则将在步骤(b)中被鉴别的设备的列表显示给用户;

在所列的设备之中选择从设备;

接收被选的从设备的列表并且创建域 ID 和域密钥；和

使用公共密钥加密域 ID 和域密钥。

5、如权利要求 1 所述的方法，其中，在通用即插即用中的控制点的一个或多个功能可由主设备接管，并且控制点涉及与用户界面有关的任务。

6、如权利要求 2 所述的方法，其中，控制点接管所述步骤中的一个或多

个。

7、如权利要求 1 所述的方法，其中，在通过从主设备获得管理者鉴别信息来执行管理者鉴别之后，主设备和从设备被确定。

8、如权利要求 1 所述的方法，其中，通过经由用户界面用户选择的方法来执行选择主设备和从设备。

基于公共密钥构建域并通过通用即插即用执行该域的方法

本申请要求于2003年10月2日在韩国知识产权局提交的10-2003-0068837号韩国专利申请的优先权，该申请全部公开于此以资参考。

技术领域

本发明涉及存在于域(domain)中的设备的鉴别，更具体地说，涉及在基于公共密钥的体系结构中构建用于防止内容被未授权的第三人非法使用的唯一域并使用通用即插即用(UPnP)将构建的域应用到家庭网络中的方法。

背景技术

随着数字和通信技术的日益发展，多种例如音频或视频材料的内容已经变得普及。已经提出了多种用于防止内容被非法复制和未授权传播的技术。具体地说，已开发了通过其用于加密内容并且仅特定的设备能使用预定的规则解密被加密的内容的技术。例如，这些技术包括DVD内容扰码系统、可记录媒体的内容拷贝保护(content protection for recordable media, CPRM)、数字发送内容保护(digital transmission content protection, DTCP)、高清晰内容保护(high definition content protection, HDCP)、内容保护系统体系结构(content protection system architecture, CPSA)、和数字版权管理(digital rights management, DRM)等。

具体地说，随着家庭网络领域的发展，已经提出多个用于保护家庭网络上的内容的技术。这些技术的典型例子包括:由汤姆逊(Thomson)公司提出的“智能版权(SmartRight)”、由西高(Sysco)公司提出的“OCCAM (公开的条件内容访问管理)”、或由IBM公司提出的“xCP (可扩展内容保护)集群协议”。

“智能版权”是通过其使组成家庭网络的每一设备具有包括公共密钥证书的智能卡，并通过使用这些智能卡在这些设备之间交换证书来创建用于家庭网络的密钥的技术。

“OCCAM”是通过其家庭中的各个设备能通过使用用于每一内容的唯一的“票”使用内容的技术。

"xCP 集群协议"是基于广播加密的技术，通过该技术，采用称作"集群"的域的概念，并且属于同一集群的设备能够自由地使用这些设备间的内容。

如图 1 所示，传统的域管理包括在被鉴别的家庭域 100 内部的主(master)设备 110 和从(slave)设备 120、130 和 140。在主设备和从设备之间执行域管理。参照图 2 将对依照这样主设备和从设备的配置基于 'xCP 集群协议' 再现内容的处理进行描述。该处理可被粗略地分为以下步骤：集群形成处理(S201)、设备鉴别处理(S202)、内容加密处理(S202)、内容解密处理(S204)。以下将对其进行详细地描述。最初连接给定家庭网络的服务器创建用于家庭网络的绑定 ID(以下称为"ID_b")(S200)。ID_b 可以是服务器的唯一的标识符，其在制造该服务器的时候建立，或者由用户任意建立。当 ID_b 被如此建立时，形成用 ID_b 识别的集群。

当设备想使用存在于服务器中的内容时，该设备通过使用其自己的设备密钥设置从媒体密钥块(MKB)中提取媒体密钥(以下称为"K_m")(S210)。其后，该设备通过使用在步骤 210 中提取的"K_m" 以及其自己的标识符 ID_p 来创建其自己的唯一密钥 K_p (S212)。

当该设备想要通过设备鉴别时，其请求该服务器鉴别该设备本身(214)。

具体地说，该设备将其自己的唯一"ID_p"、表明设备种类的"类型"、以及该"类型"和使用"K_p"获得的 ID_p 的哈希值(hash value)，即 $h=MAC(ID_p \| 类型)K_p$，发送到存在于该集群中的服务器或存在于该家庭网络外部的鉴别服务器。

该服务器从 K_m 和 ID_p 获得 K_p'，并且检查使用 K_p' 获得的哈希值 $h'=MAC(ID_p \| 类型)K_p'$ 是否与已经从该设备接收到的值 h 相同。

如果确定值 h 与值 h'相等，则该服务器发送通过使用 K_p 加密 ID_b 获得的 $E(ID_b)K_p$ 以及该设备的唯一标识符 ID_p 到该设备，然后将 ID_p 添加到该服务器的鉴别表"auth.tab"中。通过从自该服务器接收的 $E(ID_b)K_p$ 中提取 ID_b 可完成对该设备的鉴别(S216)。

在该设备鉴别完成后，该服务器加密将被传输到该设备的内容(S203)。使用 ID_b、auth.tab 和 K_m，绑定密钥(以下称为"K_b")被首先创建(S220)。这里，K_b 满足诸如 $K_b=H[ID_b \oplus H[auth.tab], K_m]$ 的方程式。

在 K_b 被创建以后，该服务器使用用于保护内容的标题密钥(以下称为"K_t")加密内容(S222)。同时，每一内容包含包括复制控制信息、关于该内容是否

允许被分发到外部的信息、使用该内容的权限、和有效的使用周期等用法规则(usage rule, UR)信息。使用 K_b，UR 信息和 K_t 被加密，以生成 $E(K_t \oplus H[UR] K_b)$(S224)。

同时，设备从服务器接收"auth.tab"，并且使用以前提取的 K_m 和 ID_b 从 $K_b=H[ID_b \oplus H[auth.tab], K_m]$ 获得 K_b (230)。此外，在从 $E(K_t \oplus H[UR] K_b)$ 提取 K_t (S232)之后，使用提取的 K_t 解密从服务器接收的内容(S234)。

在如上描述的 xCP 集群协议的操作中，所有能够与该服务器通信的设备能够自动加入域而不需要选择将要加入该域的设备的处理。此外，因为 ID_b 是固定的，所以甚至当该设备在该域之外时，K_b、K_t 等的值也能被计算。然而，其不方便在于每当每个设备创建其的新 K_b 时，该设备应从服务器接收 auth.tab 来计算新的 K_b。因此，有必要通过建立唯一的家庭域并将用户引入设备鉴别来更安全的保护内容。

同时，DRM 在数字工业的发展中担任重要的部分，并且在家庭网络中也起着重要的作用。因此，在家庭网络中存在对于以上描述的执行域管理模型的增长的需求。如上所述，如图 1 所示，用于将域管理技术应用到家庭网络中的有关技术使用在家庭网络中主和从设备之间的直接通信方案。这种方案需要开发适合于各个域管理的通信协议。因此，问题在于与各个设备的兼容性恶化。因此，需要对有效地解决该问题的措施。近来，全世界的许多公司已经对作为家庭网络中间件出现的 UPnP(通用即插即用)感兴趣，并且生产许多支持 UPnP 的产品。UPnP 具有许多优点在于由于使用传统标准的互联网协议其能够无缝地融入现有网络中，并且不依赖于特定的操作系统、物理介质或诸如此类。然而，因为通过 UPnP 执行域管理的方法仍然未知，所以存在着对使用 UPnP 有效地执行域管理的方法的需求。

发明内容

本发明的目的在于解决有关技术中的问题。本发明的目的在于提供通过用户直接涉及构建域来更安全地构建独立于外部的域并且防止内容被第三人非法使用的方法。

本发明的另一目的在于提供一种当域构建方法应用到家庭网络中时，使用 UPnP 来执行更有效的域管理的方法。

根据用于实现该目的的本发明的一方面，提供了一种基于公共密钥创建

域并且通过 UPnP 执行该域从而在家庭网络中在基于公共密钥的体系中可创建唯一域，以允许仅仅被授权的用户使用内容的方法，包括：第一步骤，将可操作的被控设备中的一个选为主设备，并且确定被选设备为主设备；第二步骤，以其他被控设备从被确定的主设备接收秘密信息块并且创建证书的方式执行设备鉴别；和第三步骤，通过在被鉴别的被控设备之中选择一个或多个设备来确定从设备。

第一步骤可包括如下步骤：通知控制点被控设备被连接；由控制点获得被控设备的设备信息和 DRM 信息；通过使用 DRM 信息在被控设备之中选择主设备；和将被选为主设备的被控设备设置为主模式并且向被控设备提供设备列表。

第二步骤可包括如下步骤：由被确定的主设备从外部服务器接收秘密信息块；向除了主设备的被控设备传送接收到的秘密信息块；使用传送的秘密信息块提取秘密值并创建证书；和通过使用创建的证书、设备 ID 和公共密钥来检验证书并准备被鉴别设备的列表。

第三步骤可包括如下步骤：如果在第二步骤中被鉴别的设备不具有域属性，则将这些设备的列表显示给用户；在所列的设备之中选择从设备；接收被选的从设备的列表并且创建域 ID 和域密钥；和使用公共密钥加密域 ID 和域密钥。

在该方法中，在 UPnP 中的控制点的一些重要的功能可由主设备接管，并且控制点处理与用户界面有关的任务。

另外，在通过从主设备获得管理者鉴别信息执行管理者鉴别之后，主设备和从设备可被确定。

此外，可以通过用户界面由用户选择的方法来执行选择主设备和从设备。

附图说明

通过下面结合附图对给定的优选实施例进行的描述，本发明的上述和其他目的和特点将会变得更加清楚，其中：

图 1 显示传统的域管理配置；

图 2 是表示依照传统的主-从设备配置基于‘xCP 集群协议’再现内容的处理的流程图；

图 3 表示根据本发明在基于公共密钥的体系结构中构建域的方法；

图 4 是显示其中本发明的域构建方法被应用于 UPnP 的示例的方框图;

图 5 表示在控制点和被控设备之间执行的普通 UPnP 操作;

图 6 表示根据本发明第一实施例确定主设备的处理;

图 7 表示根据本发明第一实施例在图 6 中表示的处理之后执行的设备鉴别处理;

图 8 表示根据本发明第一实施例在图 7 中表示的处理之后执行的确定从设备的处理;

图 9A 显示用于接收用户的选择以选择主设备的用户界面;

图 9B 显示用于从用户接收管理器 ID 和口令以鉴别管理器的用户界面;

图 9C 显示用于接收用户的选择以选择从设备的用户界面;

图 10 表示根据本发明的第二实施例确定主设备的处理;

图 11 表示根据本发明第二实施例在图 10 中表示的处理之后执行的设备鉴别处理; 和

图 12 表示根据本发明第二实施例在图 11 中表示的处理之后执行的确定从设备的处理。

具体实施方式

以下，参照附图来说明本发明的实施例。

图 3 表示根据本发明在基于公共密钥体系结构中创建域的方法。

为了描述本发明的方便，假设请求提供内容的主设备向其传输内容的每个设备当其被生产时具有一套唯一秘密密钥和公共密钥或公共密钥创建功能。此时，该套秘密密钥用于从以广播加密方式提供的秘密信息块(以下称为“SIB”)中提取秘密值。SIB 是用于检验设备的撤销的信息。撤销的设备不能从 SIB 中提取想要得到的秘密值，而合法的设备可以提取公共秘密值。

在单一域中，存在涉及构建域的主设备 320。该主设备以广播加密的方式从外部服务器 310 接收 SIB(S332)。其后，以经有线或无线网络设备 330 通知主设备它们存在于该域或主设备 320 本身发现设备 330 的方式主设备 320 识别设备 330 的存在(S334)。

当主设备 320 通过将它们显示在主设备的显示单元上来向用户提供已经由主设备识别的设备 330 时，用户选择在所显示的设备之中的他想要向该域注册的设备 330(S336)。然后，主设备 320 将已经从外部服务器 310 接收的

SIB 发送到由用户选择的设备 330(S338)。每个接收到 SIB 的设备 330 从 SIB 提取秘密值(S340)，并且使用提取的秘密值准备用于其自己的公共密钥的证书(S342)。

当设备 330 的每一个将其自己的证书、唯一标识符(ID)和公共密钥发送到主设备 320 时(S344)，为了检验该设备是合法的设备，主设备检验证书以证实设备是合法设备(S346)。然后，主设备 320 准备其中记录有被鉴别设备的唯一标识符(IDs)和公共密钥的鉴别列表(S348)。可被鉴别的设备的数量受到用户的限制。

主设备 320 准备鉴别列表之后，主设备使用包括在鉴别列表中的关于设备的信息和由主设备本身创建的随机数来创建唯一域 ID 和域密钥(S350)。域 ID 是在仅仅属于由用户的选择而形成的域的设备之间共享的秘密密钥，并且每当在组成该域的成员中存在改变时，域 ID 同时被改变。域 ID 被用作区别一个域与其他域的鉴别器。

主设备 320 通过使用存在于域中的被鉴别的设备 330 各自的公共密钥来加密域 ID 和域密钥，然后将加密的域 ID 和域密钥传输到被鉴别的设备 330。设备 330 使用它们自己的秘密密钥来恢复域密钥(S354)。从而，用于使用内容的域最终形成。当共享内容的域形成时，主设备 320 使用依次使用域密钥加密的内容密钥来加密内容。当想要使用内容的设备使用域密钥解密加密的内容时，设备可使用该内容。

图 4 是显示其中本发明的域构建方法被应用于 UPnP 的示例的方框图。

每个被控设备 110 至 160 接收/发送命令，并且在控制点 190 的控制下也提供它们自己的服务。通过指定被控设备中的一个设备作为主设备 110 并在剩余的设备之中指定已经被用户选择的设备 120、130 和 140 作为从设备来构建域。在被控设备之中，没被指定为主或从设备的设备 150 和 160，即，不包括在该域中的设备被称作访客设备。主设备 110 和从设备 120 至 140 构建被鉴别的家庭域，并且控制点 190 和被控设备 110 至 160 构建作为一个整体的家庭网络 200。

图 5 表示在控制点和被控设备之间执行的普通 UPnP 操作。首先，执行寻址步骤。UPnP 连网基于其关键点是寻址功能的 TCP/IP 协议。每一设备应具有动态主机配置协议(DHCP)代理。当设备第一次连接到网络时，设备搜索 DHCP 服务器。如果存在 DHCP 服务器，那么设备使用分配至其的 IP 地址。

如果不存在可用的 DHCP 服务器，则设备使用“自动选择 IP(auto IP)”以取得地址。

下面，执行发现步骤。一旦设备连接到网络并且被分配了合适的地址，则发现操作可被执行。使用简单服务发现协议(SSDP)来处理发现操作。当设备被添加到网络中时，SSDP 执行把由设备提供的服务通知存在于网络中的控制点。

下面，在 UPnP 连网之后执行描述操作。尽管控制点已经发现了设备，但是控制点仍然只具有关于设备的很少信息。如果控制点想要获得设备和其功能的详细信息并与设备交互，则控制点应从由相关设备提供的发现消息和 URL 检验对设备的描述。设备的 UPnP 描述采用 XML 表达，并且包括设备的制造商的唯一产品信息(例如，模型名称、序列号、制造商名称、制造商的 URL 等)。另外，这个描述还包括嵌入设备和服务以及用于控制、事件和表征的 URL 的列表。

在前述的寻址、发现和描述步骤之后，UPnP 步骤被实质地执行。通过用于控制、事件、和表征等的操作来执行 UPnP 步骤。在控制操作中，控制点获得设备的描述，然后执行对于设备的控制不可缺少的任务。为了控制设备，控制点向用于由设备提供服务的设备发送操作命令。为了这个目的，控制点向用于设备的服务的控制 URL(从设备描述可获得)发送合适的控制消息。控制消息使用简单对象存取协议(SOAP)也采用 XML 表达。响应于控制消息，相关服务然后提供特定操作值或默认代码。

在事件操作中，当每个设备由于命令的接收而使其状态发生改变时，其通过事件消息把状态改变通知控制点。事件消息包括一个或多个状态变量的名称和这些变量的当前值，并且采用 XML 表达并使用通用事件通知结构(GENA)格式化。事件的内容被周期地更新并且控制点被连续地通知事件的更新内容。另外，使用 GENA 可取消订阅。

至于表征操作，如果设备具有用于表征的 URL，则控制点可通过 URL 搜索页面并且在浏览器中装载页面。用户可使用页面控制设备或查阅设备的状态。这些功能可执行的水平取决于设备的表征页面和特定的功能。

图 6 至图 8 表示根据本发明的第一实施例执行的处理。在这些附图之中，图 6 表示确定主设备的处理。首先，所有被控设备 110 至 160 通过使用 SSDP 通知控制点 190 它们已经被连接到家庭网络(S601)。然后，控制点 190 通过

HTTP 从设备 110 至 160 获得设备信息和 DRM 信息(S602)。这里，设备信息是指用于在 UPnP 中使用的通用设备信息，并且 DRM 信息是指设备属性和设备模式。设备属性是用于确定被控设备是否可被作为在域中的主设备操作的值。另外，设备模式是能够确定设备当前被作为主设备、从设备还是访客设备操作的值。所有被控设备最初被设置为访客设备。其后，如果设备被设置为主设备或从设备，那么可改变设备模式的值。

从 DRM 信息的设备模式确定是否存在作为主设备操作的被控设备。如果不存在作为主设备操作的设备，则选择可被作为主设备操作的被控设备中的一个 (S603)。以这种通过控制点 190 的用户界面利用用户选择的方式完成将设备设置为主设备。在图 9A 中显示用户界面的示例。在用户界面中，显示作为主设备操作并且当前设置为访客设备的“主要网络点(nexus)”和“次要网络点”。为了选择主设备，用户简单的对用户想要指派其为主设备的设备中的一个打上标记。在当前的示例中，被控设备 1 110 被选为主设备。

下面，控制点 190 通过 SOAP 获得设置为主设备的被控设备 1 110 的管理者鉴别信息(S604)。这种管理者鉴别信息可从主设备的智能卡重新得到，并且需要确认已经选择主设备的用户是否是合法管理者的过程。控制点 190 通过使用管理者鉴别信息输出用户界面并从用户接收管理者 ID 和口令来执行管理者鉴别(S605)。图 9B 显示这种用户界面的一个示例。

管理者鉴别之后，控制点 190 设置被控设备 1 110 为域主设备，然后向被控设备 1 110 提供控制点 190 支配的设备列表(S606)。其后，被控设备 1 110 的设备模式值变为“主”。设置为主设备的被控设备 1 110 最初构建仅仅具有该设备本身作为成员的新域(S607)。

图 7 表示根据本发明第一实施例的在图 6 中表示的处理之后执行的设备鉴别处理。首先，域主设备 110 在这种在图 3 中表示的方式下通过外部服务器接收新的 SIB(S611)。控制点 190 然后通过使用 SOAP 向剩余的被控设备 120 至 160 传送具有存储在其中的 SIB 的 URL 信息(S612)。剩余被控设备 120 至 160 通过 HTTP 获得存在于 URL 中的 SIB(S613)。然后，被控设备使用获得的 SIB 提取秘密值，并且使用秘密值和它们自己的 ID 以及公共密钥来创建证书(S614)。这些证书被用于区分非法设备和合法设备。例如，如果其中仅仅由特定制造商生产的设备被批准为合法设备的鉴别方针被实施，则由除了特定制造商的其他制造商生产的设备将被当作非法设备对待。

其后，当控制点 190 通过 SOAP 向主设备 110 发送包含证书的 URL 信息(S615)时，主设备 110 通过使用 HTTP 从剩余被控设备 120 至 160 获得证书、设备 ID 和公共密钥(S616)。另外，主设备 110 检验获得的证书并准备被鉴别设备的列表(S617)。通过证书检验而被分类为非法设备的设备随后从该域中被排除，并且对它们来说不存在被指定为从设备的可能。

图 8 表示根据本发明第一实施例在图 7 中表示的处理之后执行的确定从设备的处理。首先，控制点 190 通过使用 SOAP 根据证书检验结果来对被批准为合法设备的设备 120 至 140 检验域属性(S621)。每个域属性可包括域密钥、属于域的设备的名称、属于该域的设备的数量等。如果设备不具有域属性，则控制点 190 通过用户界面显示这些设备的列表(S622)，并允许用户选择从设备(S623)。图 9C 表示显示合法设备 120 至 140 的列表的用户界面的示例。用户对在所列的设备之中用户希望包括于该域中的设备打上标记以选择从设备。与主设备的选择相反，用户可选择多个设备作为从设备。其后，在与图 6 中表示的主设备选择处理同样的方式下，管理者鉴别信息被获得(S624)并且管理者鉴别处理被执行 (S625)。

下面，控制点 190 通过 SOAP 向主设备 110 传送在所列设备之中选择的从设备的列表(S626)，并且通过 SOAP 将被选设备设置为从模式(S627)。已经被设置为从模式的设备具有“从”作为它们的设备模式值。然后，主设备 110 使用从设备列表创建域 ID 和域密钥(S628)。主设备使用用于从设备的公共密钥加密域 ID 和域密钥(S629)。

下面，控制点 190 通过 SOAP 从主设备将包含域属性值的 URL 信息传送到从设备(S630)。然后，从设备经由 HTTP 获得存在于 URL 中的域属性(S631)。域属性包括域密钥、属于该域的设备的名称、属于该域的设备的数量等。

图 10 至 12 表示根据本发明的第二实施例的处理。第二实施例与第一实施例的不同在于控制点 190 的一些重要的功能由主设备 110 接管。控制点 190 处理与用户界面有关的任务。作为结果，主设备 110 具有被控设备功能以及除了控制点 190 的剩余功能之外的控制点功能。因此，大大降低了控制点 190 的负荷。而且，即使控制点 190 是非法设备，从安全角度考虑，问题也不会发生。此外，即使主设备不具有用户界面也没有问题。

在这些附图之中，图 10 表示确定主设备的处理，其中设备 1 110 仅仅作为被控设备(CD)操作。因此，这个处理与确定根据第一实施例的图 6 中表示

的主设备的处理相同。从而，其重复的描述将被省略。

图 11 表示根据本发明第二实施例的在图 10 中表示的处理之后执行的设备鉴别处理。首先，控制点 190 通过 SOAP 通知主设备 110 设备鉴别处理开始(S711)。在这个处理中，主设备作为 CD 操作。然后，主设备 110(作为 CP 操作)使用 SOAP 将 SIB 直接传送到剩余被控设备 120 至 160(S712)。然后，剩余被控设备 120 至 160 使用接收到的 SIB 提取秘密值，并且使用秘密值和它们自己的设备 ID 以及公共密钥来创建证书(S713)。

接下来，剩余被控设备 120 至 160 通过 SOAP 将它们的证书、设备 ID 和公共密钥直接传送到主设备 100(作为控制点操作)(S714)。然后，主设备 110 检验接收到的证书并且准备鉴别设备的列表(S715)。通过证书检验分类为非法设备的设备随后从该域中被撤销，并且对它们来说不存在被指派为从设备的可能。然后，主设备 110(作为 CD 操作)通过使用 GENA 把利用事件消息的方式而被检验的设备的设备 ID 通知给控制点 190(S716)。然后，控制点 190 使用 SOAP 从主设备 110(作为 CD 操作)获得设备检验的结果(S717)，然后，通过用户界面显示关于设备是非法还是合法设备的检验结果(S718)。

图 12 表示根据本发明第二实施例的在图 11 中表示的处理之后执行的确定从设备的处理。首先，控制点 190 通过使用 SOAP 根据证书检验结果来检验被批准为合法设备的设备 120 至 140 的域属性(S721)。如果设备不具有域属性，则控制点 190 通过用户界面显示这些设备的列表(S722)，并且允许用户选择从设备(S723)。图 9C 表示显示合法设备 120 至 140 的列表的用户界面的示例。用户对在所列的设备之中用户希望包括于该域中的设备打上标记以选择从设备。其后，在与图 6 中表示的主设备选择处理同样的方式下，管理者鉴别信息被获得(S724)并且执行管理者鉴别处理(S725)。

下面，控制点 190 通过 SOAP 向主设备 110(作为 CD 操作)传送在所列设备之中选择的从设备 120 至 140 的列表(S726)。然后，主设备 110 使用从设备的列表创建域 ID 和域密钥(S727)。然后，主设备使用用于从设备的公共密钥加密域 ID 和域密钥(S728)。主设备 110(作为控制点操作)通过 SOAP 将被选设备直接设置为从模式，然后传送被设置的设备的域属性(S729)。

根据本发明，其优点在于，通过使用其中用户直接涉及构建域并且使用鉴别列表和作为输入值得随机数因此改变取决于属于该域的成员的变化来创建域密钥的基于公共密钥的体系结构可构建独立于外部的域，从而更安全地

限制内容的使用。

另外，根据本发明，其优点在于因为在 UPnP 中实施的通信方法可被用作将域管理技术应用到家庭网络中的通信方法，所以没必要在域中的成员之间开发新的通信方法。另外，本发明具有的优点在于包括在家庭网络中的设备可被更容易地鉴别，通过使用标准互联网协议不需根据特定操作系统或物理介质即可无缝的融入传统网络，并且与支持 UPnP 的所有设备的兼容性可被实现。

尽管本发明的实施例是结合附图来描述的，但是对于本领域的技术人员应该理解，在不调整或改变其的技术精神和本质特征的情况下，可实施本发明。因此，应该明白上述的实施例在所有方面不是限制性的而是示例性的。本发明的范围应受到所附权利要求的限定，并且从本发明的精神和范围进行的所有改变或修改以及其等同物应解释为落入本发明的范围。

图 1

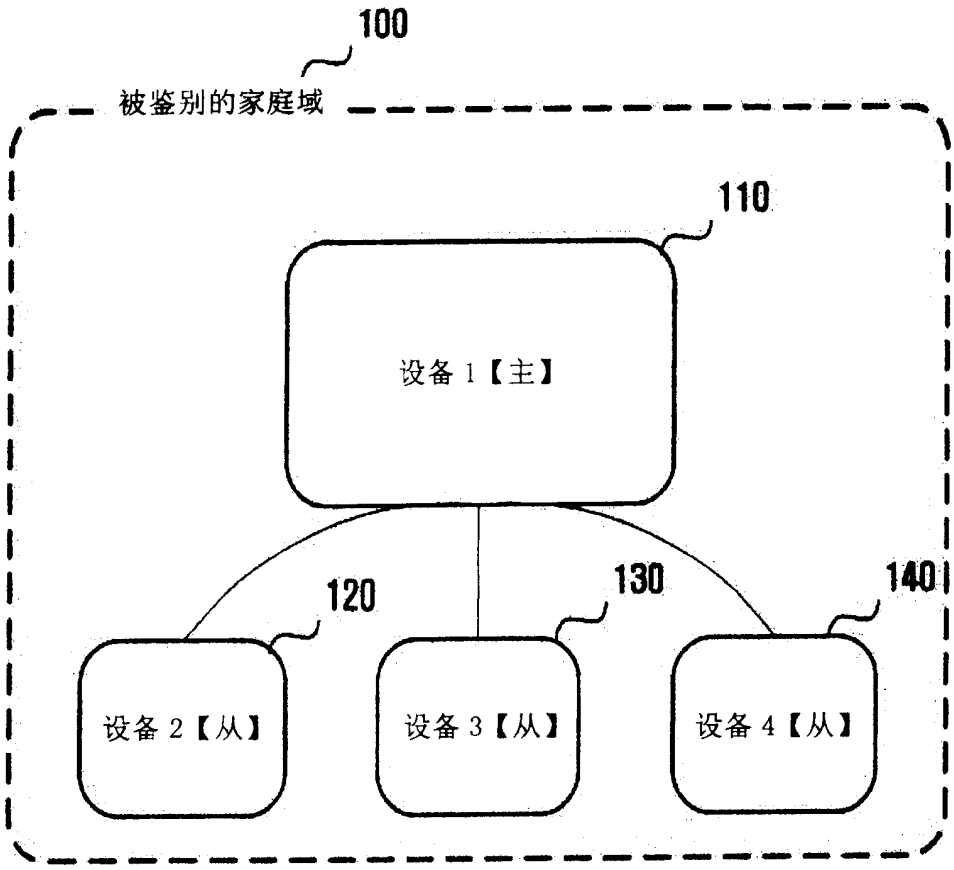


图 2

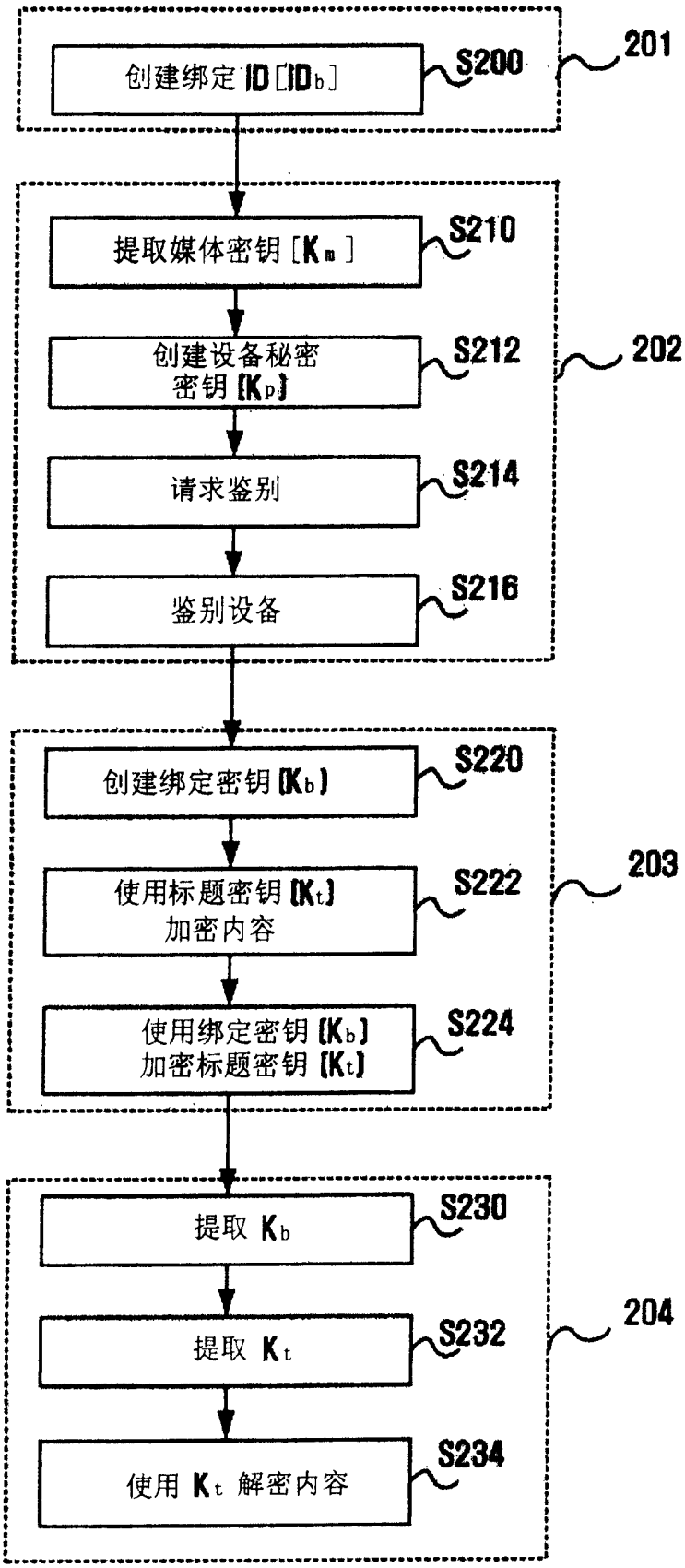

创建绑定 ID[IDb]
S200
201
提取媒体密钥[Km]
S210
创建设备秘密密钥[Kp]
S212
202
请求鉴别
S214
鉴别设备
S216
创建绑定密钥[Kb]
S220
使用标题密钥[Kt]加密内容
S222
203
使用绑定密钥[Kb]加密标题密钥[Kt]
S224
提取 Kb
S230
提取 Kt
S232
204
使用 Kt 解密内容
S234

图 3

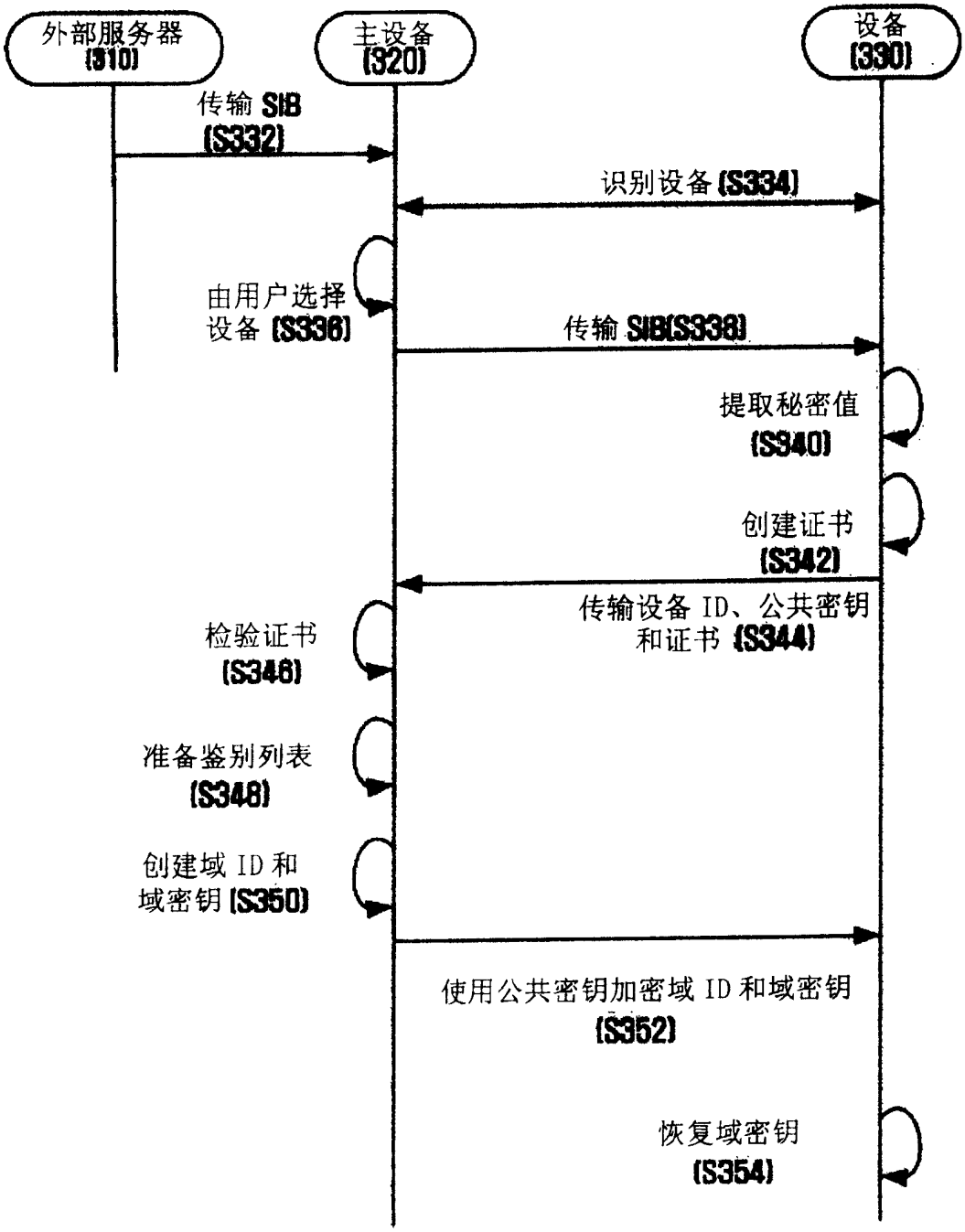
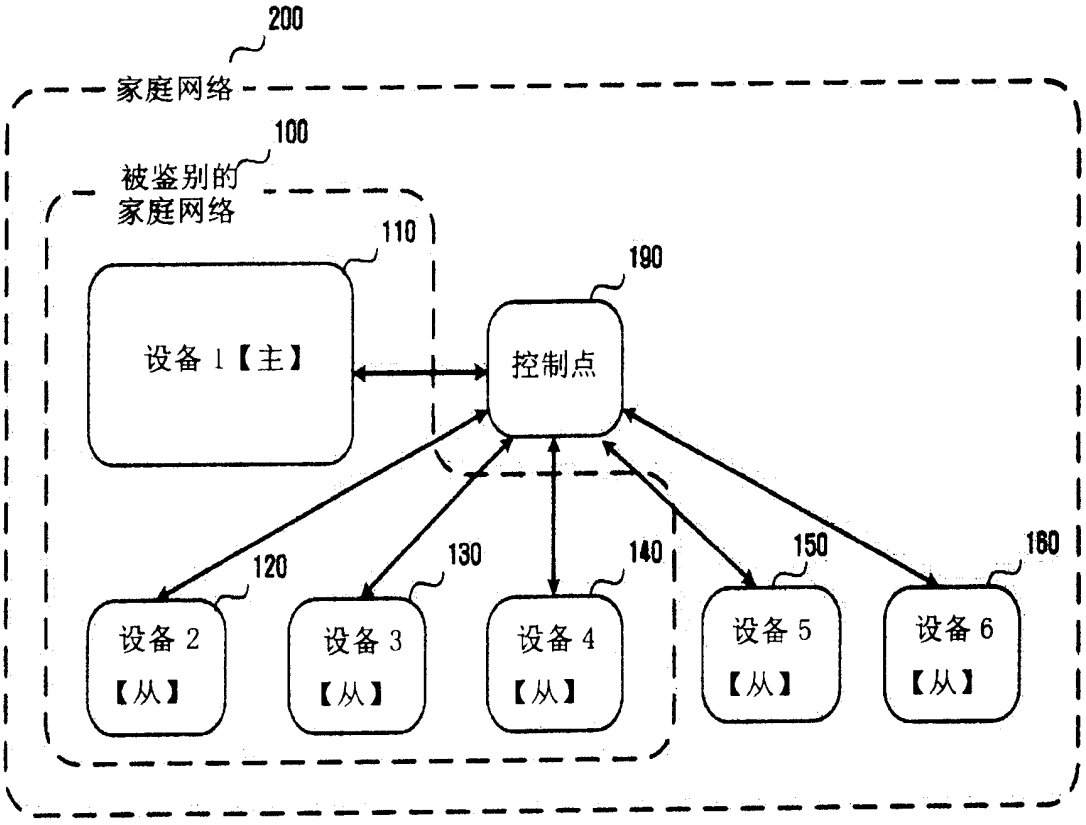

外部服务器 (310)
主设备 (320)
设备 (330)
传输 SIB (S332)
识别设备 (S334)
由用户选择设备 (S336)
传输 SIB(S338)
提取秘密值 (S340)
创建证书 (S342)
传输设备 ID、公共密钥和证书 (S344)
检验证书 (S346)
准备鉴别列表 (S348)
创建域 ID 和域密钥 (S350)
使用公共密钥加密域 ID 和域密钥 (S352)
恢复域密钥 (S354)

图 4


200
家庭网络
100
被鉴别的
家庭网络
110
设备 1【主】
190
控制点
120
设备 2
【从】
130
设备 3
【从】
140
设备 4
【从】
150
设备 5
【从】
160
设备 6
【从】

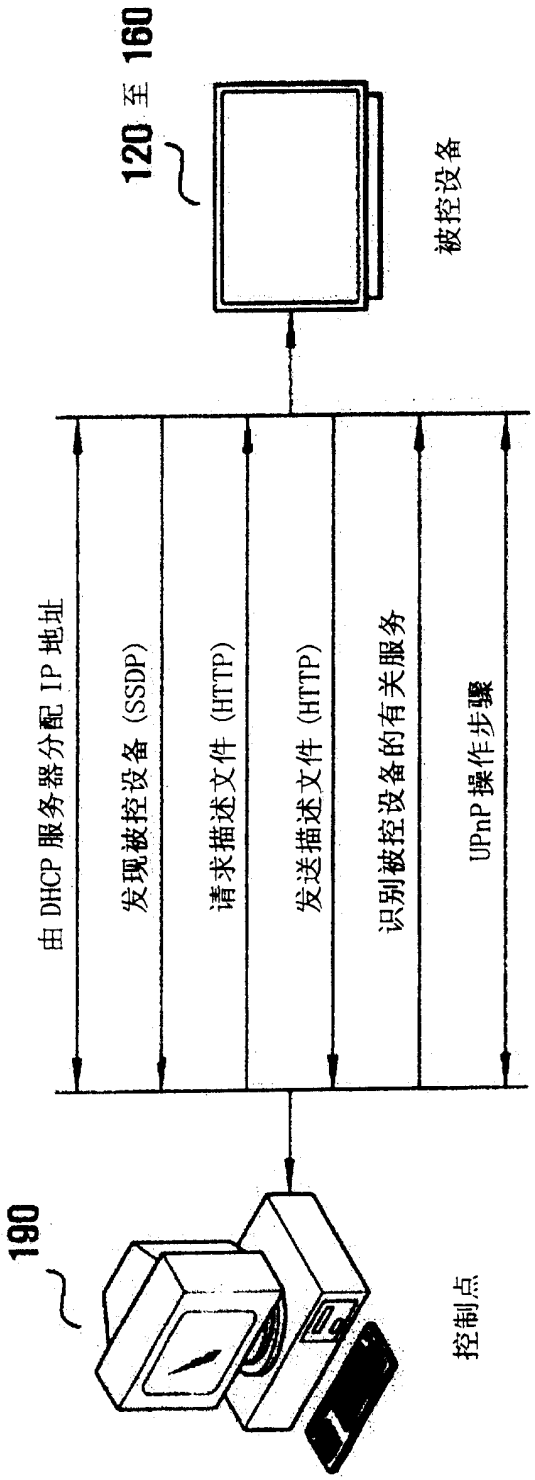

120 至 160
被控设备
由 DHCP 服务器分配 IP 地址
发现被控设备 (SSDP)
请求描述文件 (HTTP)
发送描述文件 (HTTP)
识别被控设备的有关服务
UPnP 操作步骤
190
控制点

图 5

图 6

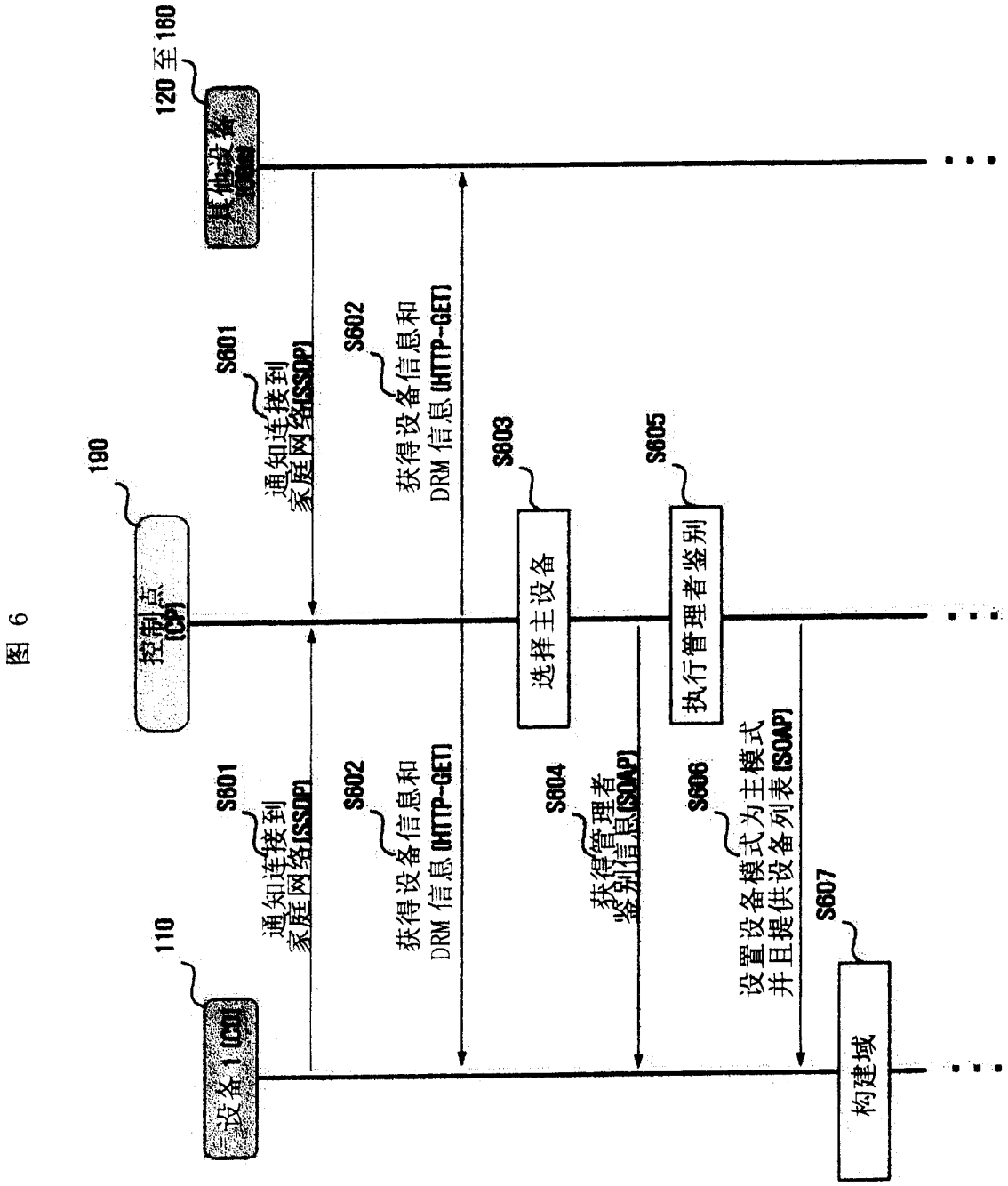

120 至 160
190
110
控制点 (CP)
设备 1 (CD)
S601
通知连接到家庭网络(SSDP)
S602
获得设备信息和 DRM 信息 (HTTP-GET)
S603
选择主设备
S604
获得管理者鉴别信息 (SOAP)
S605
执行管理者鉴别
S606
设置设备模式为主模式并且提供设备列表 (SOAP)
S607
构建域

图 7

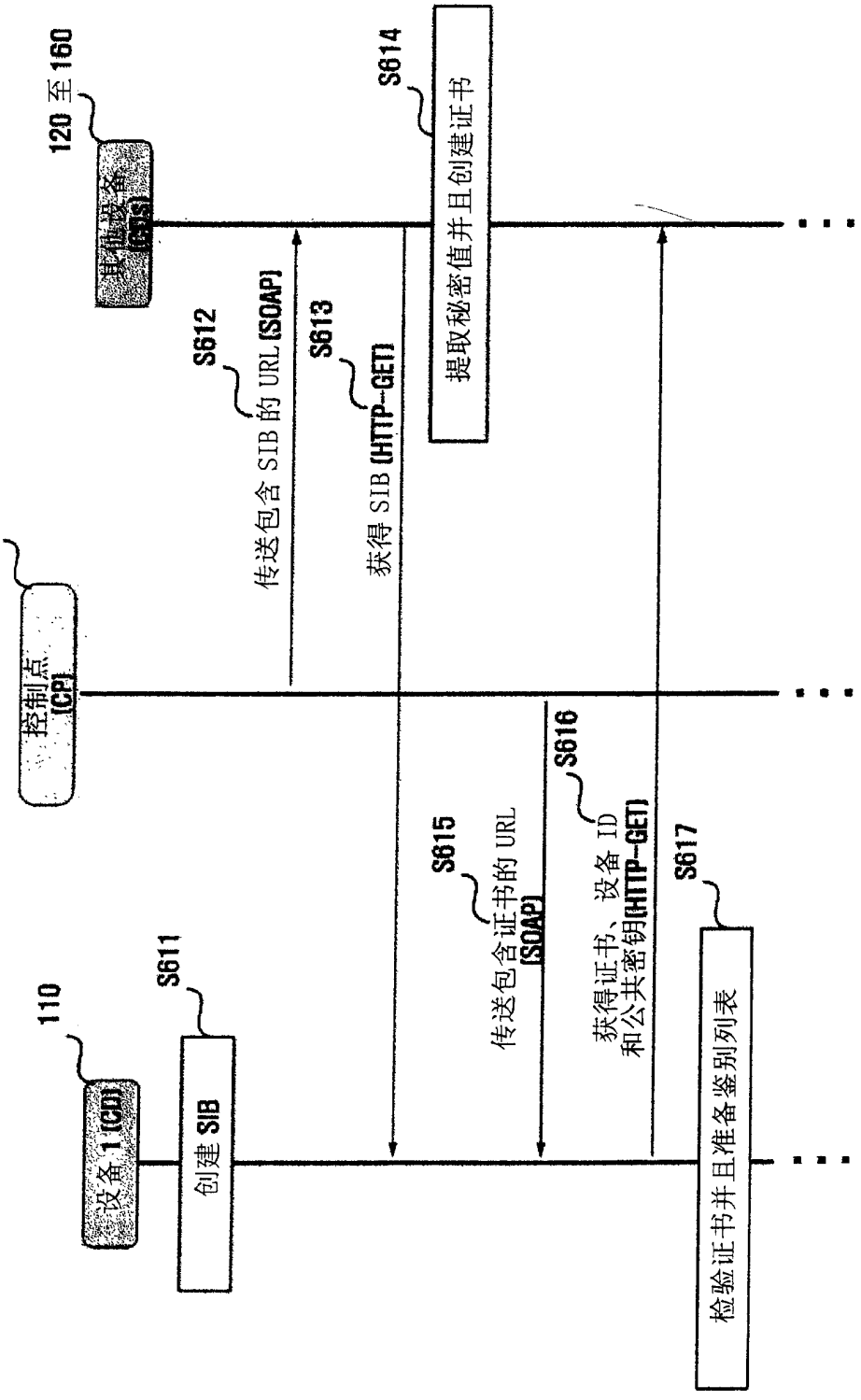

120 至 160
其他设备 (DIS)
S614
提取秘密值并且创建证书
S612
传送包含 SIB 的 URL [SOAP]
S613
获得 SIB [HTTP-GET]
190
控制点 (CP)
S615
传送包含证书的 URL [SOAP]
S616
获得证书、设备 ID 和公共密钥 [HTTP-GET]
S617
检验证书并且准备鉴别列表
110
设备 1 (CD)
S611
创建 SIB

图 8

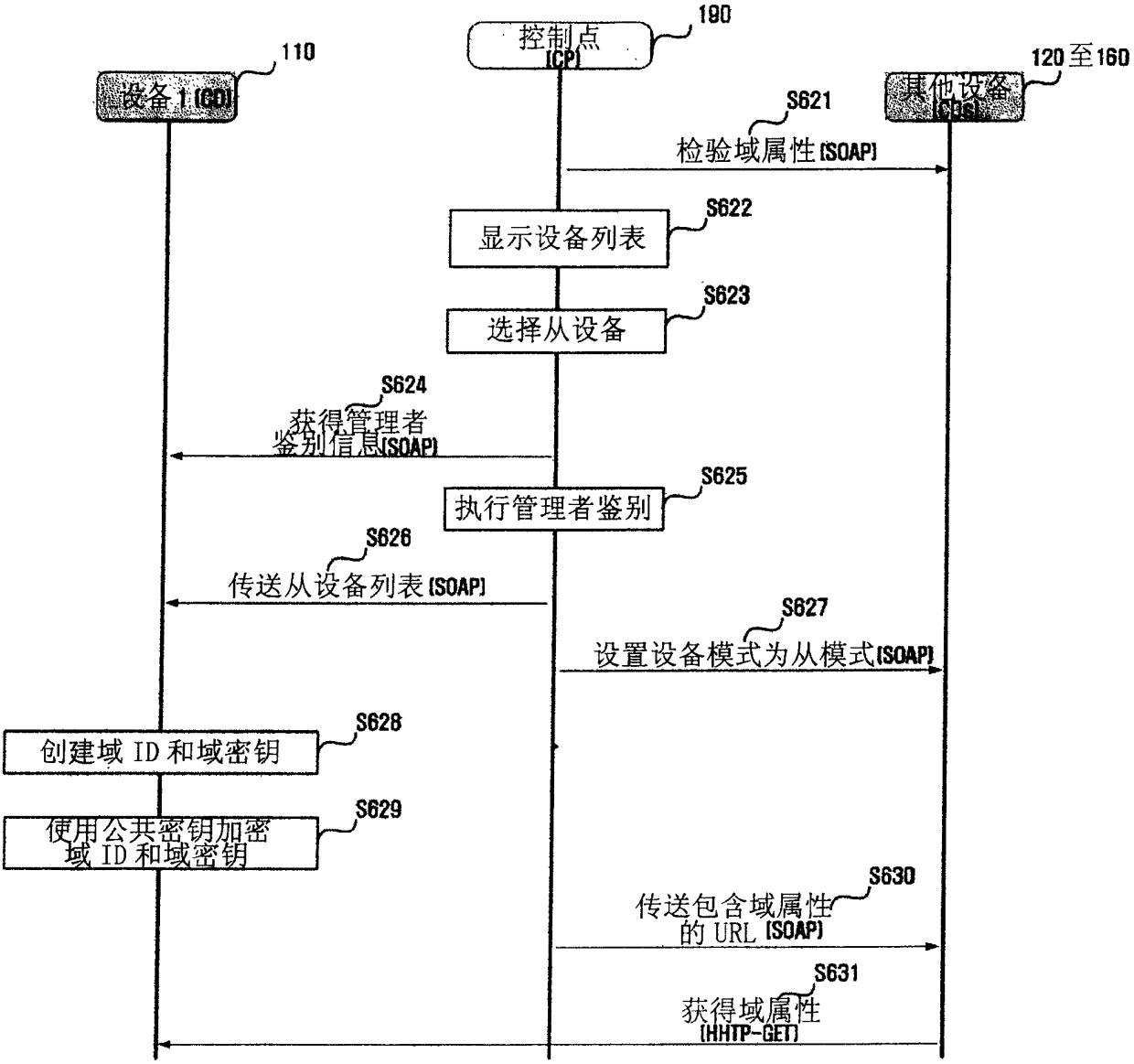

190
控制点
[CP]
110
设备 1 [GO]
120 至 160
其他设备
[GO]
S621
检验域属性 [SOAP]
S622
显示设备列表
S623
选择从设备
S624
获得管理者
鉴别信息 [SOAP]
S625
执行管理者鉴别
S626
传送从设备列表 [SOAP]
S627
设置设备模式为从模式 [SOAP]
S628
创建域 ID 和域密钥
S629
使用公共密钥加密
域 ID 和域密钥
S630
传送包含域属性
的 URL [SOAP]
S631
获得域属性
[HHTP-GET]

图 9A

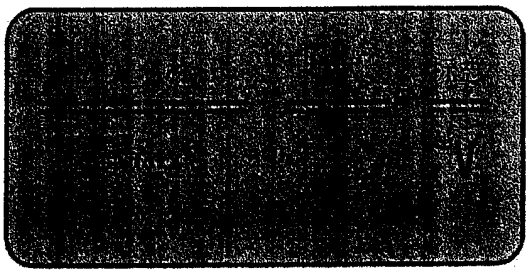


图 9B

图 9C

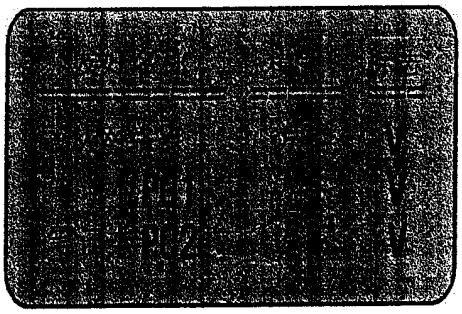


图 10

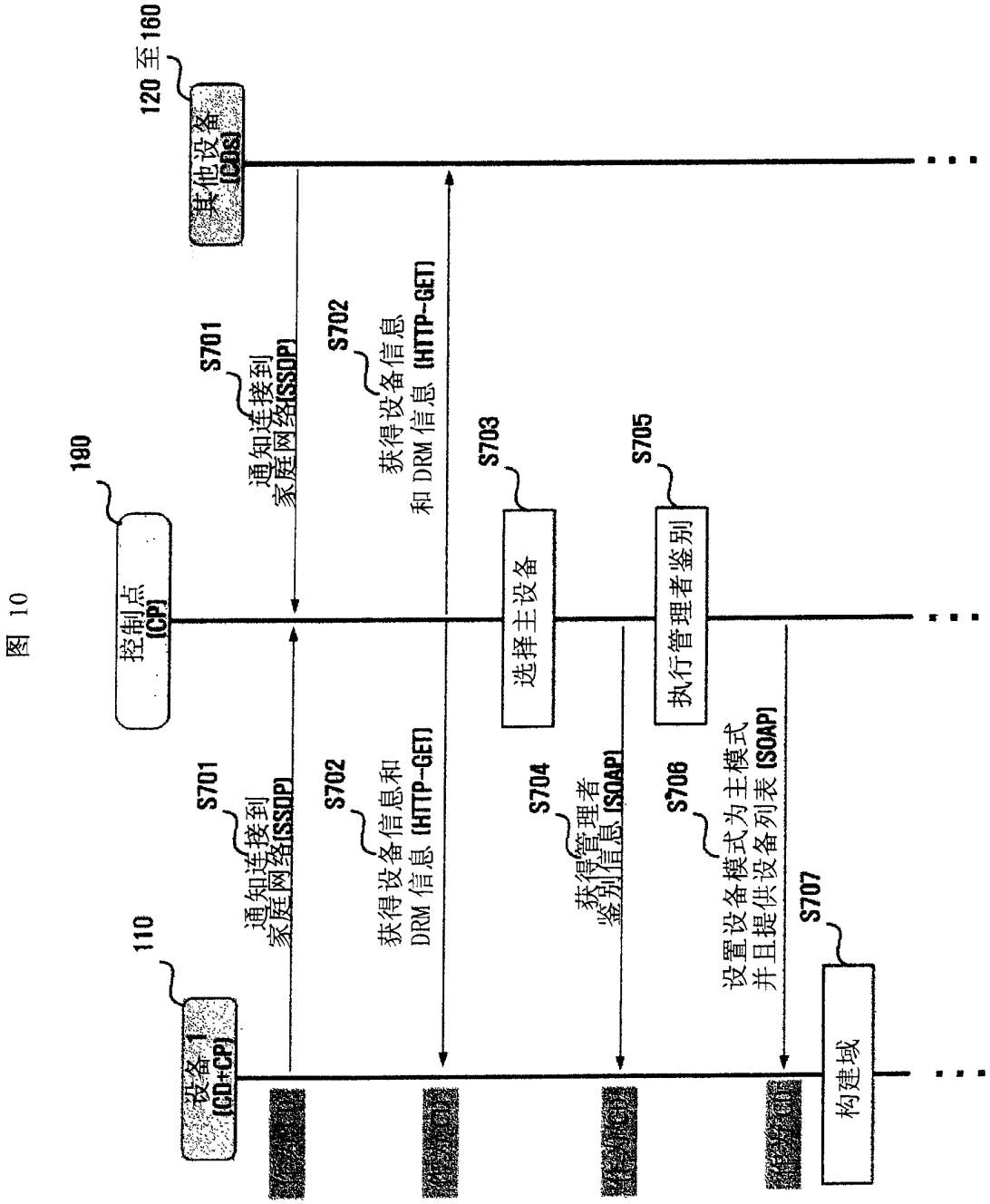

120 至 160
其他设备 (DMS)
180
控制点 (CP)
110
设备 1 (CD+CP)
S701
通知连接到家庭网络(SSDP)
S702
获得设备信息和 DRM 信息 (HTTP-GET)
S703
选择主设备
S704
获得管理者鉴别信息 (SOAP)
S705
执行管理者鉴别
S706
设置设备模式为主模式并且提供设备列表 (SOAP)
S707
构建域

图 11

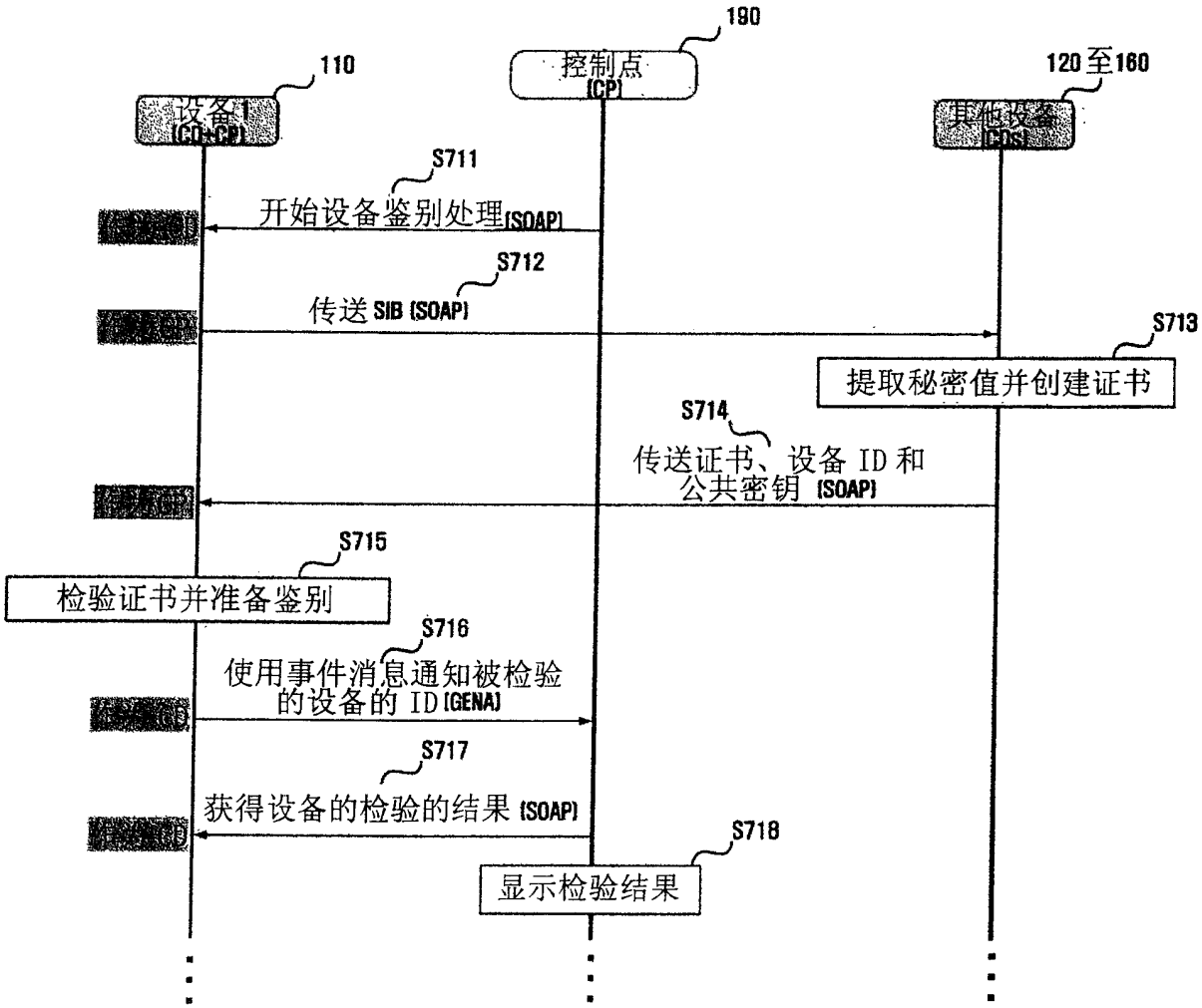
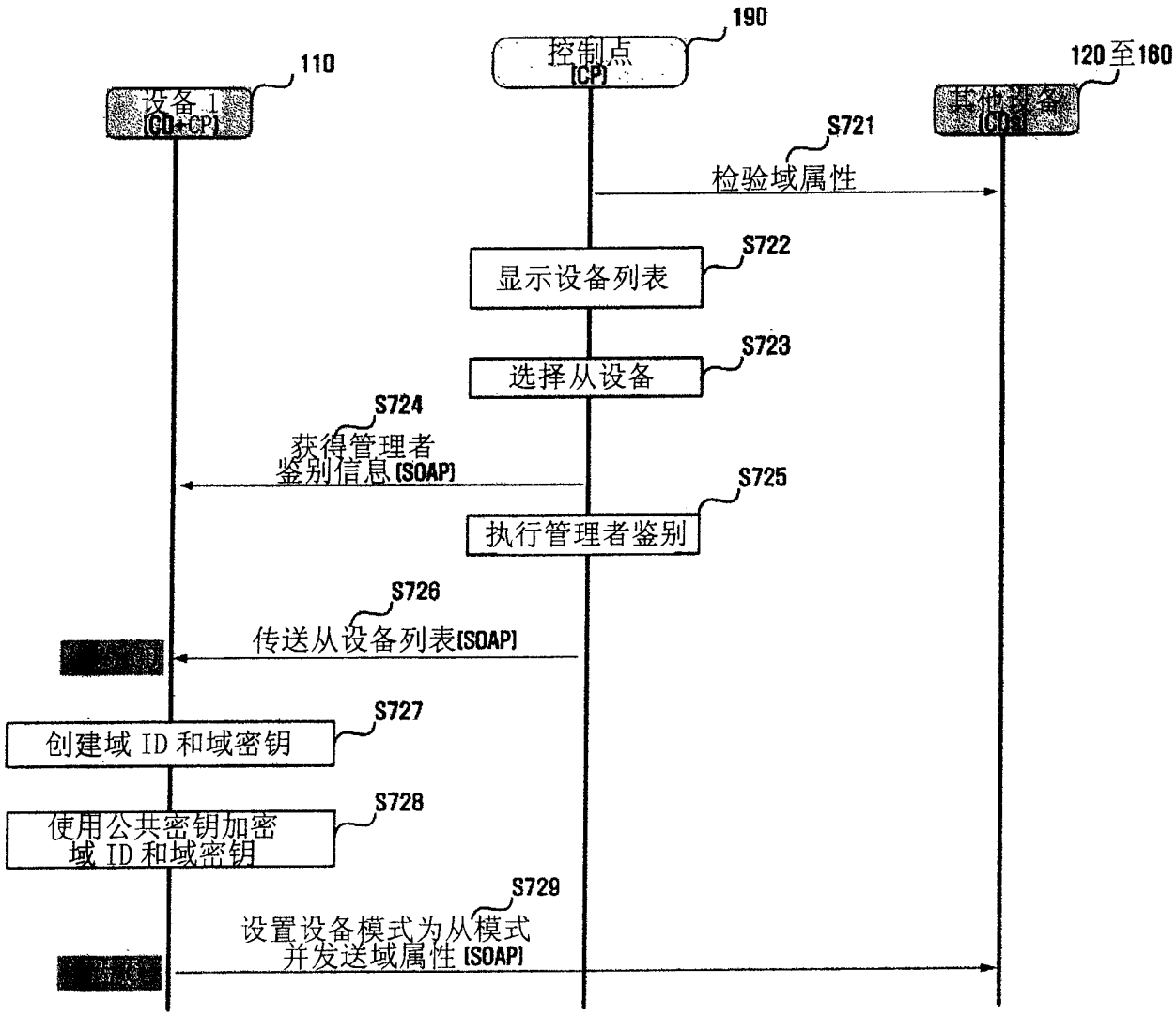

190
控制点
(CP)
110
设备1
(CD+CP)
120至160
其他设备
(CDs)
S711
开始设备鉴别处理(SOAP)
S712
传送 SIB (SOAP)
S713
提取秘密值并创建证书
S714
传送证书、设备 ID 和
公共密钥 (SOAP)
S715
检验证书并准备鉴别
S716
使用事件消息通知被检验
的设备的 ID (GENA)
S717
获得设备的检验的结果 (SOAP)
S718
显示检验结果

图 12


190
控制点
(CP)
110
设备 1
(CD+CP)
120 至 160
其他设备
(CD)
S721
检验域属性
S722
显示设备列表
S723
选择从设备
S724
获得管理者
鉴别信息 (SOAP)
S725
执行管理者鉴别
S726
传送从设备列表(SOAP)
S727
创建域 ID 和域密钥
S728
使用公共密钥加密
域 ID 和域密钥
S729
设置设备模式为从模式
并发送域属性 (SOAP)