[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/06
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 200510076210.X

[43] 公开日 2005 年 11 月 2 日

[11] 公开号 CN 1691672A

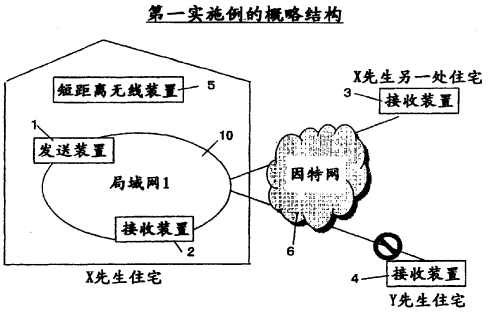
[22] 申请日 2005.3.4
[21] 申请号 200510076210.X
[30] 优先权
[32] 2004. 3. 5 [33] JP [31] 2004 - 063000
[71] 申请人 株式会社东芝
地址 日本东京都
[72] 发明人 矶崎宏 齐藤健 松下达之 上林达
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 吴丽丽

权利要求书 4 页 说明书 23 页 附图 16 页

[54] 发明名称 信息处理装置及信息处理方法

[57] 摘要

本发明谋求著作权保护，同时正规用户可以有效利用内容。 本发明具有接收来自短距离无线装置 X 的固有 ID 并注册到 ID 列表中的发送装置 A 和接收装置 B。 发送装置 A 和接收装置 B 在传送内容时，检查通信对象目的地具有的固有 ID 是否与自身装置内 ID 列表的固有 ID 一致，仅在固有 ID 一致的场合才进行内容传送。 接受从接收装置来的代理 ID 检查请求的桥接装置根据发送装置所具有的证明书检查装置类别，仅在发送装置不是桥接装置的场合，才进行认证、密钥交换处理。 由此，可以仅在有限的范围内允许内容的传送，谋求内容的著作权保护。



ISSN1008-4274

1. 一种信息处理装置，其特征在于，具有：

存储关于各个信息处理装置的、可以公开的第一固有信息和与上述第一固有信息成对的非公开的第二固有信息的固有信息存储设备，

从上述第一通信装置接收第一通信装置所具有的上述第一固有信息和作为希望和上述第一通信装置通信的目的地的第二通信装置的地址信息的代理确认要求接收设备，

检查上述第一通信装置所具有的上述第一固有信息是否登录到上述固有信息存储设备上的第一检查设备，

检查上述第二通信装置是否具有在上述固有信息存储设备中存储的上述第一固有信息的第二检查设备，

在通过上述第一检查设备判定为登录了并通过第二检查设备判定为具有的场合确认上述第二通信装置的装置类别的装置类别确认设备，

对应上述装置类别确认设备的确认结果，决定是否向上述第二通信装置发送上述第一通信装置所具有的上述第二固有信息的固有信息发送决定设备。

2. 权利要求1所述的信息处理装置，其特征在于，

具有接收从第三通信装置发送的上述第三通信装置的可公开的第一固有信息和与该第一固有信息成对的被加密的第二固有信息的第一接口设备，

通过网络在上述第一和第二通信装置之间传送上述第三通信装置的第一固有信息和与该第一固有信息成对的被加密的第二固有信息的第二接口设备，

上述固有信息存储设备存储在上述第一接口设备中接收的上述第一以及第二固有信息。

3. 权利要求1或者2所述的信息处理装置，其特征在于，

具有在通过上述第一检查设备检查为登录了的场合，向上述第二通信装置发送上述固有信息存储设备中存储的上述第一固有信息，要求上述第二通信装置检查是否具有上述固有信息存储设备中存储的上述第一固有信息的检查请求设备，和

响应上述检查请求设备接收上述第二通信装置进行的检查结果的检查结果接收设备，

上述第二检查设备，根据使用上述检查结果接收设备接收的结果检查上述第二通信装置是否具有上述固有信息存储设备中存储的上述第一固有信息。

4. 权利要求 1 到 2 中任何一项所述的信息处理装置，其特征在于，上述固有信息确认设备存储和位于规定的限制距离内的通信装置之间进行通信的上述信息处理装置具有的第一以及第二固有信息。

5. 权利要求 1 到 2 中任何一项所述的信息处理装置，其特征在于，

上述装置类别确认设备基于在多个通信装置间交换上述第一固有信息进行检查的结果，确认上述第二通信装置是否是进行信息的中继控制的信息中继装置，

在通过上述装置类别确认设备确认是上述信息中继装置的场合，上述固有信息发送决定设备决定不向上述第二通信装置发送上述第一通信装置具有的上述第二固有信息。

6. 权利要求 5 所述的信息处理装置，其特征在于，

具有在通过上述装置类别确认设备确认为上述第二通信装置是信息中继装置的场合，在从上述第一通信装置到达上述第二通信装置之间，计量通过其他的信息中继装置进行的信息中继的次数的次数计量设备，

在通过上述次数计量设备计量的次数在规定次数以内的场合，上述固有信息发送设备对上述第二通信装置发送上述第二固有信息，在超过上述规定次数的场合，禁止对上述第二通信装置发送上述第二固有信息。

7. 权利要求 5 所述的信息处理装置，其特征在于，具有：

在通过上述装置类别确认设备确认为上述第二通信装置是信息中继装置的场合，检测从上述第一通信装置到达上述第二通信装置之间的路径的路径检测设备，

检查通过上述路径检测设备检测出的路径的大小是否小于等于规定大小的大小检查设备，

在通过上述大小检查设备检查为小于等于上述规定大小的场合，对上述第二通信装置发送用上述路径检测设备检测出的路径和上述第一通信装置具有的上述第二固有信息，在检查为比上述规定大小大的场合，不向上述第二通信装置发送上述路径以及上述第二固有信息的中继信息发送设备。

8. 一种信息处理装置，其特征在于，具有：

通过网络和第一通信装置之间传送加密的内容的第一接口设备，

接收从第二通信装置发送的可公开的第一固有信息和与上述第一固有信息成对的加密的第二固有信息的第二接口设备，

存储在上述第二接口设备接收的上述第一及第二固有信息的固有信息存储设备，

对上述第一通信装置进行信息的发送请求的信息发送请求设备，

检查具有可公开的固有信息的上述第一通信装置是否被检索的第一检索设备，

在通过上述第一检索设备检查为未被检索的场合，根据和上述第一发送装置之间交换上述第一固有信息后的检查结果检索中继信息的信息中继装置的第二检索设备，

通过上述信息中继装置检测直到到达上述第一发送装置的路径的路径检测设备，

检查通过上述路径检测设备检测出来的路径的大小是否小于等于规定大小的大小检查设备，

在通过上述大小判断检查检查为小于等于上述规定大小的场合，对通过上述第二检索设备所检索的上述信息中继装置发送上述固有信息和上述第一通信装置的地址信息的代理确认请求设备。

9. 一种信息处理方法，其特征在于，包括步骤：

从上述第一通信装置接收第一通信装置具有的上述第一固有信息和作为希望和上述第一通信装置通信的目的地的第二通信装置的地址信息，

检查上述第一通信装置具有的上述第一固有信息是否存储在上述固有信息存储设备中，所述固有信息存储设备存储关于各个信息处理装置的可公开的第一固有信息和与上述第一固有信息成对的非公开的第二固有信息，

检查上述第二通信装置是否具有在上述固有信息存储设备中存储的上述第一固有信息，

在上述第一固有信息存储在上述固有信息存储设备中、且上述第二通信装置具有在上述固有信息存储设备中存储的上述第一固有信息的场合，确认上述第二通信装置的装置类别，

对应上述第二通信装置的装置类别的确认结果，决定是否向上述第二通信

装置发送上述第一通信装置具有的上述第二固有信息。

10. 一种信息处理方法，其特征在于，包括步骤:

使用第一接口设备、通过网络在和第一通信装置之间传送加密的内容，

通过上述第二接口设备，接收从第二通信装置发送的可公开的第一固有信息和与上述第一固有信息成对的加密的第二固有信息，存储在上述第二接口设备接收的上述第一及第二固有信息，

对上述第一通信装置进行信息的发送请求，

检查具有可公开的固有信息的上述第一通信装置是否被检索，

在上述第一通信装置未被检索的场合，检索用于中继和上述第一发送装置的通信的信息中继装置，

检测通过上述信息中继装置直到到达上述第一发送装置的路径，

检查上述检测出来的路径的大小是否小于等于规定大小，

在小于等于上述规定大小的场合，对上述信息中继装置发送上述固有信息和上述第一通信装置的地址信息。

信息处理装置及信息处理方法

技术领域

本发明涉及传送谋求著作权保护所必要的各种内容的信息处理装置、接收装置以及信息处理方法。

背景技术

近年来，伴随计算机网络的普及和数字化，称为数字信息家电的产品正在普及。另外，伴随地面波数字广播的开始，可以预想对应数字广播的电视机或者机顶盒、DVD 录像机等今后会更加普及。这些数字家电如果用网络连接的话，使用者就可以经由网络享受各种内容，利用价值很大。

这里，内容是指各种数字数据，例如在 MPEG2 或者 MPEG4 等动态图像数据或声音数据，另外文本数据或者静止图像数据等的文件、数据等。由这种数字数据组成的内容具有不会劣化、可以容易复制这样的优点，但是其反面是对于内容的著作权必须注意。例如，考虑从某发送装置向接收装置发送应该保护著作权的内容的场合。交换应该保护著作权的内容的范围，希望限制在一定的范围内，例如限制在著作权法第 30 条的个人利用的范围内等的正当的权限的范围内，或者比这更窄的范围内，而超过该范围不能和第三者交换内容。

关于通过这些的登录处理的内容的分发范围限制方法，在例如特开 2002—194491 号公报等公开的文献中详细说明。

但是，在用 IP（因特网协议）进行 AV 数据传送的场合，因为 IP 可以传送不受电缆长度等物理制约的数据，因此容易产生著作权法上的问题。亦即，在 IP 中，说到 VPN（Virtual Private Network），在逻辑上连接远方 IP 网络伙伴的技术广泛普及，使用该技术，可以使在 A 地区 X 先生住宅的家庭网络上连接的设备逻辑上连接在（物理上离开 A 地区的）B 地区的 Y 先生住宅的家庭网络内，传送 AV 数据。因此，X 先生住宅的内容不封闭在 X 先生住宅内的家庭网络内，地处远方的 Y 先生也能够连接 X 先生住宅的家庭网络，阅览 X 先生拥有的内容。

发明内容

本发明是鉴于上述问题提出的，其目的是在提供谋求著作权保护的基础上识别内容的传送而谋求内容的有效利用的信息处理装置以及信息处理方法。

为解决上述课题，本发明提供一种信息处理装置，其特征在于，具有：存储关于各个信息处理装置的、可以公开的第一固有信息和与上述第一固有信息成对的非公开的第二固有信息的固有信息存储设备，从上述第一通信装置接收第一通信装置所具有的上述第一固有信息和作为希望和上述第一通信装置通信的目的地的第二通信装置的地址信息的代理确认要求接收设备，检查上述第一通信装置所具有的上述第一固有信息是否登录到上述固有信息存储设备上的第一检查设备，检查上述第二通信装置是否具有在上述固有信息存储设备中存储的上述第一固有信息的第二检查设备，在通过上述第一检查设备判定为登录了并通过第二检查设备判定为具有的场合确认上述第二通信装置的装置类别的装置类别确认设备，对应上述装置类别确认设备的确认结果，决定是否向上述第二通信装置发送上述第一通信装置所具有的上述第二固有信息的固有信息发送决定设备。

本发明提供一种信息处理装置，其特征在于，具有：通过网络和第一通信装置之间传送加密的内容的第一接口设备，接收从第二通信装置发送的可公开的第一固有信息和与上述第一固有信息成对的加密的第二固有信息的第二接口设备，存储在上述第二接口设备接收的上述第一及第二固有信息的固有信息存储设备，对上述第一通信装置进行信息的发送请求的信息发送请求设备，检查具有可公开的固有信息的上述第一通信装置是否被检索的第一检索设备，在通过上述第一检索设备检查为未被检索的场合，根据和上述第一发送装置之间交换上述第一固有信息后的检查结果检索中继信息的信息中继装置的第二检索设备，通过上述信息中继装置检测直到到达上述第一发送装置的路径的路径检测设备，检查通过上述路径检测设备检测出来的路径的大小是否小于等于规定大小的大小检查设备，在通过上述大小判断检查检查为小于等于上述规定大小的场合，对通过上述第二检索设备所检索的上述信息中继装置发送上述固有信息和上述第一通信装置的地址信息的代理确认请求设备。

根据本发明，因为仅在满足规定条件的场合才在第一以及第二通信装置之

间进行通信，能够一面谋求著作权保护，一面在不同通信装置之间进行内容的传送，谋求内容的有效利用和提高用户的方便性。

附图说明

图 1 是表示包含涉及本发明的信息处理装置的信息处理系统的概略构成的一个示例的方框图。

图 2 是说明通过设备的登录限制内容分发范围的方法的概念图。

图 3 是表示短距离无线装置 X 的内部结构的一个示例的方框图。

图 4 是表示发送装置 A 的内部结构的一个示例的方框图。

图 5 是表示接收装置的内部结构的一个示例的方框图。

图 6 是表示在 ID 列表管理部 28、38 中存储的短距离 ID 列表的一个示例的图。

图 7 是表示 ID 登录阶段的处理步骤的一个示例的序列图。

图 8 是表示内容传送阶段的处理步骤的一个示例的序列图。

图 9 是表示内容传送阶段的处理序列的其他的序列的图。

图 10 是表示对应图 9 的序列图的发送装置 A 的内部结构的一个示例的方框图。

图 11 是表示对应图 9 的序列图的接收装置的内部结构的一个示例的方框图。

图 12 是说明使用多个短距离无线装置 X 在发送装置 A 和接收装置上登录 ID 的场合的问题点的图。

图 13 是说明使用桥接装置限制内容的分发范围的方法的概念图。

图 14 是表示根据本实施例的桥接装置的内部结构的方框图。

图 15 是表示证明书的格式的一个示例的图。

图 16 是表示和图 14 的桥接装置进行通信的发送装置 A 的内部结构的一个示例的方框图。

图 17 是表示和图 14 的桥接装置进行通信的接收装置的内部结构的一个示例的方框图。

图 18 是表示本实施例的内容传送阶段的处理步骤的一个示例的序列图。

图 19 是接续图 18 的序列图。

图 20 是在发送装置 A 和接收装置之间设置两个桥接装置的场合的概念结构图。

图 21 是表示在设置两个桥接装置的场合内容传送阶段的处理序列的一个示例的图。

图 22 是表示桥接装置作为家庭内服务器工作的场合的信息处理系统的概略结构的图。

图 23 是表示根据第二实施例的桥接装置的内部结构的一个示例的方框图。

图 24 是表示在设置两个桥接装置的场合内容传送阶段的处理序列的一个示例的图。

图 25 是表示图 22 的桥接装置 Y 的详细的处理步骤的流程图。

图 26 是表示涉及本实施例的接收装置 B 的一个实施例的概略结构的方框图。

图 27 是表示涉及本实施例的接收装置的处理序列的一个示例的流程图。

图 28 是表示公开固有 ID 关系表的一个示例的图。

图 29 是表示路径列表的一个示例的图。

图 30 是表示接收装置 B 向桥接装置 Y 发送的代理 ID 检查请求命令的一个示例的图。

图 31 是表示桥接装置 Y 向桥接装置 X 发送的代理 ID 检查请求命令的一个示例的图。

图 32 是表示在第四实施例中的桥接装置的概略结构的一个示例的方框图。

图 33 是表示桥接装置 X、Y 进行路径列表的大小检查的场合的处理序列的一个示例的序列图。

图 34 是表示桥接装置 X 的处理序列的一个示例的流程图。

具体实施方式

以下参照附图说明本发明的一个实施例。

（第一实施例）

图 1 是表示包含涉及本发明的信息处理装置的信息处理系统的概略构成的一个示例的方框图。图 1 的信息处理系统，以在个人欣赏范围内主要发送接收 AV 数据为目的，具有在局域网 10 上连接的可发送内容的发送装置 1、可接收

内容的接收装置2、3、4、和短距离无线装置5。短距离无线装置5通过与发送装置1和接收装置2的短距离通信，可以进行通信，作为一种方式可以考虑遥控器。

在图1中表示的是在X先生住宅内有短距离无线装置5和连接在局域网10上的发送装置1和接收装置2，在X先生的另一处住宅内有接收装置3，在Y先生住宅内有接收装置4，表示出以因特网6连接X先生住宅内的局域网10、X先生的另一处住宅内的接收装置3、和Y先生住宅内的接收装置4的例子，但是发送装置1和接收装置2～4的配置和连接形式不限于图1所示的情形。例如，也可以在连接在因特网6上连接的局域网10和接收装置2～4的路径上存在路由器。

作为图1的局域网10的物理层以及链路层，可以采用遵照IEEE 802.11的无线LAN、以太网（注册商标）、IEEE1394等各种形式。在作为局域网10的网络层使用因特网协议（IP）的场合，可以是Ipv4，也可以是Ipv6。另外，在局域网10上也可以连接发送装置1、接收装置2以外的装置，不过为简化起见在这里省略。

这里，所谓在图1的信息处理系统中传送的内容，指例如MPEG2、MPEG4那样的动态图像数据、MP3那样的声音数据、或者文本数据或图像数据那样的文档等数字内容。这里为使说明简单，考虑在进行著作权保护的基础上应该传送的数字内容（以下简称内容）的情况。

这里考虑从发送装置1向接收装置2～4发送内容的情况。这时应该注意的是内容的著作权。如上所述，该内容交换的范围希望限制在一定的范围内，例如著作权法第30条的个人利用的范围内等的正当的权限的范围内，或者比这更窄的范围内，禁止超出该范围，例如在和其他人之间的内容交换。亦即，应该允许从X先生拥有的发送装置1向接收装置2、3传送内容，而不允许向拥有者不同的接收装置4传送内容。

作为把分发范围限定在一定分发内的方法，在发送装置2和接收装置之间预先设置“登录”的步骤，登录相互的装置、一方的装置、或者第三装置的ID，只许可在登录的装置之间的内容传送。进而考虑把可能登录的范围作为物理的范围，在未进行登录的装置间不允许内容传送、把加密的内容解密的结构。

图2是说明通过设备的登录限制内容分发范围的方法的概念图。短距离无

线装置X具有在设备内固有的不能改写的ID(固有ID),具有向发送装置A和接收装置B发送该固有ID的功能。接收来自短距离无线装置X的ID的发送装置A和接收装置B在自身装置的ID列表中登录固有ID的值。发送装置A和接收装置B在传送内容时,检查通信对象目的地所具有的固有ID是否和自身装置的ID列表中的固有ID一致,仅在固有ID一致的场合进行内容的传送。

例如,假设短距离无线装置X的固有ID的值是"x",因为接收来自该短距离无线装置X的固有ID"x"的发送装置A和接收装置B具有相互相同的固有ID,因此可以进行内容的传送。具有短距离无线装置Y的固有ID"y"的接收装置C在ID列表中具有固有ID"y"而不具有"x",接收装置C不能接收来自发送装置A的内容。

图3是表示短距离无线装置X的内部结构的一个示例的方框图。图3的短距离无线装置X具有为进行与发送装置和接收装置的短距离无线通信而执行物理层处理以及数据链路层处理的短距离无线接口部11、进行与发送装置和接收装置之间的认证、密钥交换处理的短距离无线认证、密钥交换处理部12、ID管理部13和短距离无线加密处理部14。

ID管理部13,管理作为短距离无线装置X的固有ID的秘密固有ID以及公开固有ID并且进行向发送装置A和接收装置B发送这些秘密固有ID以及公开固有ID的控制。短距离无线加密处理部14使用短距离无线认证、密钥交换处理结果得到的密钥,加密秘密固有ID。

公开固有ID是和秘密固有ID成对的值,例如可以使用以秘密固有ID为基础的SHA1等公知的单方向杂散函数计算。秘密固有ID和公开固有ID在短距离无线装置X内是固有的值,可以由许可机构发行保证其唯一性,也可以使用制造短距离无线装置X的设备销售商使用不具有同一值的秘密固有ID和不具有公开固有ID那样的十分大的值而能够在概率上保证唯一性。此外,希望秘密固有ID不能从其他的装置上不正当地取得、改变。这里,所谓"不正当"意味许可机构或者设备销售商等具有分配ID权限的特定组织以外的第三者未经许可而进行变更。

图4是表示发送装置A的内部结构的一个示例的方框图。图4的发送装置A具有:为和接收装置B进行通信而执行物理层处理以及数据链路层处理的网络接口部21;为和接收装置B进行内容的收发而执行网络层、传输层处理的包

处理部22、和接收装置B进行认证、密钥交换处理的认证、密钥交换处理部23；为和短距离无线装置X在短距离无线上进行通信而执行物理层处理以及数据链路层处理的短距离无线接口部24；和短距离无线装置X之间进行认证、密钥交换处理的短距离无线认证、密钥交换处理部25、使用短距离无线认证、密钥交换处理的结果得到的密钥解密短距离无线装置X的秘密固有ID的短距离无线密码处理部26；判别在自身装置的ID列表中是否登录了从网络接口部21输入的接收装置B具有的ID列表中的值的ID登录判别处理部27；或者从短距离无线接口部24输入短距离无线装置X的秘密固有ID登录在ID列表中、或者根据ID登录判别处理部27的请求向接收装置B输出ID列表的ID列表管理部28；加密发送内容的密码处理部29；存储内容、供给包处理部的内容供给部30。

在以下的例子中，用包处理部22处理的信息设想为使用因特网协议执行的信息。另外，所谓短距离无线例如设想为使用红外线或者无线标签（RF标签）的无线，但是未必限定为无线。

这里重要的是，在网络接口部21中处理的信息是在逻辑地址空间中进行处理的信息，不限定在物理范围内。另一方面，短距离无线接口部24，限定红外线或者无线标签、或者（不是无线）IC卡、磁卡等可交换的信息在物理范围内。

图5是表示接收装置的内部结构的一个示例的方框图。图5的接收装置，类似图4的发送装置A的内部结构，与图4的发送装置A的不同之处在于，代替内容供给部30具有内容处理部39；没有ID登录判别处理部，在密码处理部37上连接为用于加密ID列表向发送装置A发送的ID列表管理部38。

此外，发送装置A和接收装置B具有的ID列表管理部28、38，只要在短距离无线认证、密钥交换处理部25、35上认证为通信对象是正当的设备的场合，就具有从短距离无线装置X接收秘密固有ID、在ID列表上追加相应固有ID的功能。

图6是表示在ID列表管理部28、38中存储的短距离ID列表的一个示例的图。ID列表由必须项和可选项构成。作为必须项，具有短距离无线装置X的秘密固有ID和公开固有ID，作为可选项，具有登录ID列表的登录日期时间、发送装置A或者接收装置的网络接口部的MAC地址或IP地址等设备中通用的固有信息。

此外，设ID列表可以记录有限个数（例如N个）的秘密固有ID。亦即，

ID 列表管理部 28、38 具有用于存储 ID 列表的 RAM 区域。

ID 列表管理部 28、38，在从通信对象接收秘密固有 ID 后，在 ID 列表中追加该秘密固有 ID，但是在此时秘密固有 ID 已经在 ID 列表中存在的场合，则什么也不做。此外，在有作为可选项的登录日期时间的场合，也可以更新该日期时间。

另外，通过存储器容量等的物理限制或者许可等的逻辑限制，也可以限制 ID 列表管理部可存储的秘密固有 ID 的个数。在这种场合，也可以在已经记录 N 个秘密固有 ID 的场合，显示用于催促选择是拒绝追加新的秘密固有 ID，还是在有作为可选项的登录日期时间的场合、在删除最老的登录日期时间的秘密固有 ID 后追加该秘密固有 ID，还是用户删除哪个秘密固有 ID 的消息，删除任意的秘密固有 ID。

此外，在这里，所谓认证、密钥交换处理，是指接收装置以及短距离无线装置 X 相互认证是否是从某许可机构正确地接受许可的设备，在确认是正当的设备的场合，生成共同的密钥的处理。认证的方法中可以使用 ISO/IEC 9798-3 或者 ISO/IEC 9798-2 那样众所周知的方法。另外，密码处理部 29、37 或者短距离无线密码处理部 14、26、36，通过认证处理，通过共有的密钥，具有加密内容、ID 列表乃至秘密固有 ID 的功能，但是作为用于加密、解密这些数据的加密算法，也可以使用 AES 或者 DES 等众所周知的方法。

下面说明在发送装置 A、接收装置 B 以及短距离无线装置 X 之间进行的内容的传送处理步骤。从发送装置 A 向接收装置 B 传送内容时的处理分为“ID 登录阶段”和“内容传送阶段”这两个阶段。

“ID 登录阶段”是对发送装置 A 或者接收装置 B 登录短距离无线装置 X 的固有 ID 的阶段。图 7 相当于这一阶段。

在“内容传送阶段”中，发送装置 A 和接收装置 B 在传送内容前进行是否具有相互共同的短距离无线装置 X 的 ID 的检查，在具有同一短距离无线装置 X 的 ID 的场合，许可传送内容，在不具有的场合，拒绝传送内容。图 8 相当于这一阶段。

这样，“ID 登录阶段”一定先于“内容传送阶段”进行。另外，在“ID 登录阶段”使用发送装置 A、接收装置 B、短距离无线装置 X，但是在“内容传送阶段”中只使用发送装置 A、接收装置 B。

首先叙述ID登录阶段的处理。图7是表示"ID登录阶段"的处理序列的一个示例的图，表示到在短距离ID列表中记录短距离无线装置X的秘密固有ID的步骤。

以下，为省略说明，说明对于发送装置A登录ID的处理。首先，发送装置A对于短距离无线装置X发送秘密固有ID请求（步骤S1）。基于这一请求，短距离无线装置X和发送装置A相互进行是否是正当的设备的认证处理，随后进行密钥交换处理（步骤S2）。在认证失败的场合，进行规定的错误处理，不进行以后的处理。

在认证成功的场合（步骤S3，S4），亦即如果相互能够确认是正当的设备的话，则短距离无线装置X向发送装置A发送秘密固有ID和公开固有ID（步骤S5）。此时，在通信路径上为了不改变秘密固有ID希望通过认证、密钥交换处理使用共有的密钥加密发送。

发送装置A接收秘密固有ID后，在发送装置A内的ID列表中追加秘密固有ID（步骤S6）。

此外，公开固有ID未必加密发送，和秘密固有ID成对追加到ID列表中。在接收装置B中登录短距离无线装置X的ID的场合，也可以以同样的步骤进行。

此外，这一系列的处理，使用发送装置A、接收装置B以及短距离无线装置X各自具有的短距离无线接口部11，通过短距离无线进行。

通过以上的处理，发送装置A和接收装置B可以在各ID列表中设置短距离无线装置X中固有的ID。

此外，在图7中，表示从发送装置A对于短距离无线装置X发送秘密固有ID请求的例子，但是与其相反，也可以从短距离无线装置X向发送装置A发送秘密固有ID请求，开始短距离无线认证、密钥交换请求。

另外，在发送装置A或者接收装置的ID列表超过可能记录的个数的场合，有（1）删除最初登录的短距离无线装置X的秘密固有ID，记录新输入的秘密固有ID的方法，（2）给发送装置A或者接收装置返回错误的方法，（3）催促用户删除哪个秘密固有ID的方法，（4）组合这些的方法。

下面，详细叙述内容传送阶段。图8是表示"内容传送阶段"的处理序列的一个示例的图。首先，接收装置B对于发送装置A发送内容接收请求（步骤S11）。

基于该请求，发送装置A和接收装置B进行认证、密钥交换处理（步骤S12）。如果认证、密钥交换处理正常结束，在发送装置A和接收装置B之间密钥共有的话，则接收装置B使用该共有的密钥加密在自身装置中保存的ID列表后发送（步骤S13）。

接收接收装置B的ID列表的发送装置A，从接收的ID列表中进行是否包含与在自身装置的ID列表中包含的秘密固有ID相同的秘密固有ID的检索处理（步骤S14）。

在这一场合，在ID登录阶段，在接收装置B的ID列表中包含短距离无线装置X的秘密固有ID“x”，而且因为在发送装置A的ID列表中也包含短距离无线装置X的秘密固有ID“x”，因此这一检索处理成功。检索处理成功的话，将通知这一意思的消息向接收装置B发送后（步骤S15），发送装置A开始内容的传送（步骤S16）。

图9是表示内容传送阶段的处理序列的其他的序列的图。首先，接收装置B将从ID列表中只添加公开固有ID的列表和内容接收请求一起发送给发送装置A（步骤S21）。

发送装置A接收该请求和ID列表后，从相应ID列表中进行是否包含与在自身装置的ID列表中包含的公开固有ID相同的公开固有ID的检索处理（步骤S22）。在这一场合，在ID登录阶段，因为在接收装置B的ID列表中包含短距离无线装置X的公开固有ID“xxyyzz”，而且在发送装置A的ID列表中也包含短距离无线装置X的公开固有ID“xxyyzz”，因此公开固有ID“xxyyzz”的值一致，该检索处理成功。

检索处理成功的话，把通知检索处理成功的意思和在哪个公开固有ID上成功的消息向接收装置B发送（步骤S23）。

其后，发送装置A和接收装置B进行认证、密钥交换处理（步骤S24）。此时，使用对应相应公开固有ID的秘密固有ID“x”生成加密、解密内容的密钥（步骤S25，S26）。使用该密钥发送装置A加密内容、开始传送（步骤S27）。

此外，在图9的方法中，图8的序列中使用的发送装置A和接收装置的结构有若干不同。图10是表示对应图9的序列图的发送装置A的内部结构的一个示例的方框图，图11是表示对应图9的序列图的接收装置的内部结构的一个示例的方框图。

图10的发送装置A和在图4中图示的发送装置A的不同点是，因为从接收装置B发送的登录用公开ID列表不被加密，因此ID登录判别处理部27不和密码处理部29连接而是和包处理部22连接。

图11的接收装置和图5的不同点是，因为向发送装置A发送的公开固有ID列表不需要加密，因此ID列表管理部38连接包处理部。

通过执行图9的处理，在ID列表的收发中不需要加密，可以使设备的结构简单。因为ID检查处理先于认证、密钥交换处理，所以如果尝试连接彼此ID不一致的设备，则在ID检查处理中当作错误，能够避免进行不需要的认证、密钥交换处理。

如果是使用短距离无线装置X和正当的步骤来实施登录处理的发送装置A或者接收装置的话，则应该具有同一公开固有ID“xxyyzz”和秘密固有ID“x”的组。因此，公开固有ID“xxyyzz”以明文收发，但是考虑假设某恶意的第三者想绕过该检查处理，即使用通信路径改变公开固有ID，也不能在不共有秘密固有ID的装置间生成同一密钥，不能正确加密、解密内容。

此外，内容传送阶段中的这一系列的处理在和在内容收发中使用的同一接口中进行。

根据以上的步骤，在内容传送阶段，只有在同一短距离无线装置X中登录的发送装置A和接收装置才可以进行内容传送。

在上述的例子中，说明了接收装置发送ID列表，发送装置比较自身装置内的ID列表和从接收装置接收的ID列表的处理，但是，也可以是与此相反的结构，即接收装置比较ID列表。在这一场合，ID登录判别处理部不在发送装置中设置而在接收装置中设置。当然，发送装置和接收装置都装备ID登录判别处理部也可以。

在上述的例子中，说明使用一个短距离无线装置X，在发送装置和接收装置内登录ID的例子。但是，考虑住宅内存在多个短距离无线装置X的场合。在这种场合，在某一住宅内，存在由于不同的短距离无线装置X登录的多个设备区域，有不同设备群伙伴不能通信的可能。

图12是说明使用多个短距离无线装置X在发送装置和接收装置上登录ID的场合的问题点的图。在图12中，通过短距离无线装置X在发送装置A和接收装置B中登录ID“x”。另外，通过短距离无线装置Y在接收装置C和发送装

置D中登录ID"y"。因为发送装置A和接收装置B具有同一短距离无线装置X的ID，因此可以进行内容的收发。同样，接收装置C和发送装置D也可以进行内容的收发。但是，因为发送装置A和接收装置C、发送装置D登录的ID不同，因此不能进行内容的收发。

为解决这一问题，考虑直接把不共有同一秘密固有ID的发送装置A和接收装置B通过认证桥接装置使通信成为可能的方法。

图13是说明使用桥接装置限制内容的分发范围的方法的概念图。在图13中表示短距离无线装置X的ID在发送装置A、接收装置B以及桥接装置上登录，且短距离无线装置Y的ID在接收装置C、未图示的发送装置D以及桥接装置上登录的状态。亦即，在桥接装置的ID列表中登录短距离无线装置X和短距离无线装置Y双方的ID。通过经由该桥接装置，发送装置A可以和接收装置C和未图示的发送装置D进行通信。

但是，无限制允许桥接的话，存在多个利用者有意共有桥接装置，通过因特网在桥接装置上分发到许多段，由此进行无限制内容分发的危险性。因此在本实施例中，通过限制在桥接装置之间的连接，回避无限制的桥接。

图14是表示根据本实施例的桥接装置的内部结构的方框图。图14的桥接装置，具有：为了进行与发送装置A和接收装置B的通信而执行的物理层处理和数据链路层处理的网络接口部41；为了进行与发送装置A和接收装置B的认证、密钥交换处理用的信息的收发而执行的网络层、传输层处理的包处理部42；执行与发送装置A和接收装置B的认证、密钥交换处理的认证、密钥交换处理部43；为了在短距离无线上和短距离无线装置X进行通信而执行的物理层处理和数据链路层处理的短距离无线接口部44；和短距离无线装置X之间执行认证、密钥交换处理的短距离无线认证、密钥交换处理部45；使用短距离无线认证、密钥交换处理的结果得到的密钥，解密短距离无线装置X的秘密固有ID的短距离无线密码处理部46；判别从网络接口部输入的发送装置A或接收装置B具有的ID列表中的值是否在自身装置的ID列表中登录的ID登录判别处理部47；从短距离无线接口部11输入短距离无线装置X的秘密固有ID，在ID列表中登录，或者根据ID登录判别处理部47的请求向发送装置A或者接收装置B输出ID列表的ID列表管理部48；密码处理部49。

认证、密钥交换处理部43具有：接收来自接收装置B的代理ID检查请求、

将其意思通知 ID 列表管理部 48 的代理 ID 检查请求接收部 51、用于向发送装置 A 发送 ID 检查请求的 ID 检查请求发送部 52、查验通信对象的证明书进行通信对象是否是桥接装置的判别的证明书检查部 63。

发送装置、接收装置以及桥接装置在自身装置内具有用于证明是从某特定许可机构正确接受许可的设备的证明书。该证明书例如在认证、密钥交换处理部内设置。

图 15 是表示证明书的格式的一个示例的图。证明书包含：版本号、表示认证方式的识别的认证类别、通过许可机构各装置唯一接受的 ID、认证、密钥交换用的公开密钥、识别是何种装置的装置类别、为证明这些信息未被改变许可机构授予的签名。这里重要的是装置类别。该装置类别用于区别具有证明书的装置是发送装置 A、接收装置还是桥接装置。因为在图 15 中表示了桥接装置的证明书的一个示例，所以装置类别是“桥接装置”。

图 16 是表示和图 14 的桥接装置进行通信的发送装置 A 的内部结构的一个示例的方框图。图 16 的发送装置 A，其认证、密钥交换处理部的结构和图 10 的不同，具有接收来自桥接装置的 ID 检查请求，进行规定动作的代理 ID 检查处理部 56。

图 17 是表示和图 14 的桥接装置进行通信的接收装置的内部结构的一个示例的方框图。图 17 的接收装置，在图 11 的接收装置的结构上，新增加在内容传送阶段中对发送装置 A 的 ID 检查处理失败的场合，检索由同一短距离无线装置 X 登录的桥接装置的桥接装置检索处理部 57。另外，认证、密钥交换处理部 33 具有对桥接装置发送 ID 检查请求的代理 ID 检查请求处理部 58。

下面说明本实施例的内容传送阶段。这里，举例说明图 13 的发送装置 A、桥接装置以及接收装置 C。在发送装置 A 中，通过短距离无线装置 X 令 ID 登录处理成功，在 ID 列表中登录作为短距离无线装置 X 的秘密固有 ID 的“x”。在接收装置 C 中，通过短距离无线装置 Y 令 ID 登录处理成功，在 ID 列表中登录作为短距离无线装置 Y 的秘密固有 ID 的“y”。

另一方面，在桥接装置中，会与短距离无线装置 X 和 Y 双方进行 ID 登录处理，在自身装置的 ID 列表中登录秘密固有 ID“x”和“y”双方，考虑在该状态下从发送装置 A 向接收装置 C 发送内容的情况。

图 18 和图 19 是表示本实施例的内容传送阶段的处理序列的一个示例图。

首先，接收装置C，对发送装置A发送内容接收请求和自身装置的秘密公开ID（步骤S31）。发送装置A，基于从接收装置C接收的内容接收请求比较自身装置ID列表和从接收装置C接收的ID列表，检索一致的秘密公开ID（步骤S32）。在这一场合，因为发送装置A和接收装置C不用同一短距离无线装置X进行ID登录阶段的处理，所以不具有共同的公开固有ID，该处理失败（步骤S33，S34）。

接着，接收装置C，检索在ID列表中具有与在发送装置A的ID列表中包含的秘密固有ID相同的秘密固有ID的桥接装置（步骤S35）。如果检索成功，则接收装置C对桥接装置发送委托代理进行ID检查处理的代理ID检查请求、自身装置的ID列表、再加上作为内容传送的通信对象的发送装置A的地址（步骤S36）。

接收这些消息的桥接装置，首先比较自身装置的ID列表和从接收装置C接收的ID列表，检索一致的公开固有ID（步骤S37）。在这一场合，因为接收装置C和桥接装置用同一短距离无线装置Y进行ID登录阶段的处理，所以在ID列表中包含秘密固有ID“y”，该检索处理成功（步骤S38）。

桥接装置，对接收装置C通知同意代理ID检查的委托这一意思（步骤S39），为向发送装置A传达用代理进行ID检查请求，对发送装置A发送ID检查请求和桥接装置具有的ID列表（步骤S40）。

从桥接装置接收ID列表的发送装置A，比较自身装置的ID列表和相应ID列表，检索一致的公开固有ID（步骤S41）。在这一场合，因为发送装置A和桥接装置用同一短距离无线装置X执行ID阶段的处理，所以在ID列表中包含秘密固有ID“x”，该检索处理成功（步骤S42）。发送装置A向桥接装置发送发送代理ID检查成功的消息（步骤S43），桥接装置对接收装置C发送代理ID检查成功的意思的消息（步骤S44）。

接着，桥接装置和发送装置A、桥接装置和接收装置C进行各自的认证、密钥交换处理（步骤S45，S46）。

此时，桥接装置检查从各装置接收的证明书的装置类别字段（步骤S47）。如果装置类别是发送装置A或者接收装置C，则继续处理。在装置类别是桥接装置的场合进行中断处理。由此，可以防止在桥接装置间进行认证、密钥交换处理。

在该例中，因为桥接装置进行认证、密钥交换处理的对象是发送装置A和接收装置C，因此认证、密钥交换处理成功，桥接装置将和接收装置C共同的秘密固有ID“X”使用在和发送装置A之间进行的认证、密钥交换生成的密钥加密并向发送装置A发送（步骤S48）。由此，发送装置A和接收装置C暂时共有共同的秘密固有ID“x”。

其后，发送装置A和接收装置C进行认证处理（步骤S49），使用秘密固有ID“x”生成用于加密、解密内容的密钥（步骤S50，S51），开始内容的收发（步骤S52）。

此外，在图18和图19中，表示接收装置C和发送装置A一旦进行ID检查，在其失败后接收装置C检索桥接装置的处理步骤的例子，但是在接收装置C预先知道未和发送装置A共有ID的场合，也可以不需要进行该ID检查处理，从桥接装置的检索处理开始处理。

图20是在发送装置A和接收装置之间设置两个桥接装置X、Y的场合的概念结构图。在图20中，使用短距离无线装置X登录发送装置A和桥接装置X，使用短距离无线装置Y登录桥接装置X和桥接装置Y，使用短距离无线装置Z登录桥接装置Y和接收装置B。

亦即，表示桥接装置X在ID列表中注册短距离无线装置X的秘密固有ID“x”和短距离无线装置Y的秘密固有ID“y”、桥接装置Y在ID列表中注册短距离无线装置Y的秘密固有ID“y”和短距离无线装置Z的秘密固有ID“z”的状态。这里，考虑从发送装置A经由桥接装置X和桥接装置Y向接收装置B发送内容的场合。

图21是表示在设置两个桥接装置X、Y的场合的内容传送阶段的处理序列的一个示例图。因为关于前半部分的处理执行和图18同样的处理，因此在这里省略，仅说明桥接装置Y发送ID列表的处理以后的处理。桥接装置Y基于接收装置B的代理ID检查请求，向桥接装置X发送ID检查请求和自身装置的ID列表（步骤S61）。桥接装置X比较自身装置的ID列表和从桥接装置Y发送来的ID列表，检索一致的秘密固有ID（步骤S62）。这里，因为秘密固有ID“y”是共同的值，所以检查处理成功，桥接装置X对桥接装置Y发送ID检查成功的意思的消息（步骤S64），桥接装置Y对接收装置B发送代理ID检查成功的意思的消息（步骤S65）。

其后，桥接装置X和桥接装置Y开始认证、密钥交换处理（步骤S66，S67），但是因为桥接装置X、Y具有的证明书的装置类别字段是桥接装置，所以处理中止（步骤S68），桥接装置Y对桥接装置X和接收装置B发送错误消息（步骤S69，S70）。

另外，在该例中表示具有和在接收装置B中登录的秘密固有ID同一值的桥接装置判别证明书的装置类别的例子，但是，这之外也可以考虑（a）桥接装置X进行判别处理对桥接装置X返回结果的方法，（b）桥接装置X、Y双方执行判别处理的方法等。

根据以上的步骤，在内容传送阶段中可以避免桥接装置彼此进行认证、密钥交换处理，在发送装置A和接收装置B进行通信时，可以避免等于或大于两个的桥接装置进行内容的收发。

此外，在进行以上的通信时，可以作为类似IP（因特网协议）那样的网络层的包收发，也可以作为数据链路层的帧收发。进而在使用IP的场合，接收装置C向桥接装置发送的地址信息也可以是IP地址。

在图18和图19中，发送装置A和桥接装置、桥接装置和接收装置C、发送装置A和接收装置C进行各自的认证、密钥交换处理，但是，此时为确认在进行认证、密钥交换处理的各装置间存在于逻辑上以及物理上规定的范围内，也可以发送装置A把IP头标的TTL的值低于一个规定的数，发送认证、密钥交换处理的消息，或者测定发送装置A和接收装置C之间的往复应答时间，在超过一定的时间那样的场合中止认证、密钥交换处理。

此外，在该例中叙述了内容发送请求或者代理ID检查请求从接收装置发送的处理步骤，但是，本实施例不限定与此，也可以采取从发送装置A向接收装置C发送的步骤。

另外，在该例中采取使用作为秘密值的秘密固有ID的值生成用于加密、解密内容的密钥那样的形态，但是，本实施例中接收装置C能否接收从发送装置A正确解码的内容是关键，因此，也可以执行与迄今叙述的认证、密钥交换处理不同的第二认证、密钥交换处理，在第二认证、密钥交换处理中进行是否共有秘密固有ID的检查，进而使用通过第二认证、密钥交换所共有的值生成用于加密、解密的密钥。

上述第一实施例在家庭内存在服务器的场合等特别有效。例如，在把短距

离无线装置X装配在具有发送装置和接收装置自身的控制功能的红外线遥控器等的一部分中的场合，一般把这些遥控器作为各装置的附属品销售。短距离无线装置X在家庭中仅按装置的装置的数目存在，用户自身如果不记得在哪个短距离无线装置X上登录哪个装置的话，则不能进行适当的分组。但是，如果假定有家庭内服务器的话，在家庭内设置新的装置时，使用附属该新装置的短距离无线装置X登录新装置和家庭内服务器。由此，可以把家庭内服务器视为桥接装置，看作是桥接新装置和现有的装置的装置。

图 22 是表示桥接装置作为家庭内服务器工作的场合的信息处理系统的概略结构的图。图22的各装置，通过各装置附属的短距离无线装置X登录。例如，发送装置A通过短距离无线装置A进行登录处理。此外，这种登录处理也可以在产品发运前预先由产品销售商进行。在设备利用者通过短距离无线装置B把登录有秘密固有 ID 的接收装置 B 连接到网络上时，仅通过使用短距离无线装置B登录桥接装置，接收装置B就可以和发送装置A通信。由此，可以削减用户本应进行的登录人工和时间。

这样，在第一实施例中，因为根据各装置具有的证明书调查装置类别，仅在不是桥接装置的场合进行认证、密钥交换处理，所以可以仅在有限范围内允许内容的传送，在谋求内容的著作权保护的同时能够进行内容的传送。

（第二实施例）

在第一实施例中，表示了在桥接装置用代理进行 ID 检查处理时，通过检查代理ID检查委托源的证明书的特定字段，防止多次进行桥接的方法。在第二实施例中，在装置间通过扩充执行的命令，限制桥接的次数。

图23是表示根据第二实施例的桥接装置的内部结构的一个示例的方框图。和图14的不同点是，具有接收包含转发数的代理ID检查的代理ID检查请求接收部 51；检查该转发、若小于等于规定数的话进行错误处理的代理 ID 检查请求判别部 61；把该转发数减去规定的数、向其他桥接装置发送代理 ID 检查请求的代理ID检查请求发送部62。

图 24 是表示在设置两个桥接装置的场合内容传送阶段的处理序列的一个示例的图。前半部分的处理因为和图18相同，所以在这里省略说明，说明关于图20中的桥接装置Y和接收装置B、以及桥接装置X和桥接装置Y的ID检查处理成功后的处理。

桥接装置X向桥接装置Y通知ID检查处理成功(步骤S81),其后桥接装置Y向接收装置B通知代理ID检查处理成功(步骤S82)。到此,可以和图18同样处理。其后,桥接装置X和桥接装置Y进行认证、密钥交换(步骤S83,S84),这里,桥接装置Y从桥接装置X的证明书识别通信对象是桥接装置(步骤S85),桥接装置X从桥接装置Y的证明书识别通信对象是桥接装置(步骤S86)。

和第一实施例不同,步骤S85、S86的判别处理,因为是以在判别认证处理的对象是否是桥接装置后变更发送的命令为目的,所以即使假定通信对象是桥接装置处理也仍然继续。

如果桥接装置Y判定认证处理的对象是桥接装置的话,则发送代理ID检查请求(步骤S87)。此时包含转发数。所谓转发数是从接收装置B到发送装置A进行代理ID检查时在判断到多少个桥接装置进行桥接为好时使用的值。

在桥接装置中减去规定的数(例如1),减得的结果小于等于规定的阈值的话,则拒绝代理ID请求(步骤S88)。在该例中,首先以N发送来自接收装置B的代理ID检查请求的转发数,其后桥接装置Y从N减去规定的数(这里是1)(N-1)。这里假设阈值为0,判定N-1是否比0大。

如果N-1小于或者等于0,则判定为检查处理失败,转移到错误处理(步骤S89)。另一方面,如果N-1比1大,则桥接装置Y对于桥接装置X进行代理ID检查请求(步骤S90)。此时转发数减1。然后,判定N-2是否比0大(步骤S91)。如果N-2小于或者等于0,则桥接装置X向桥接装置Y发送意思是检查处理失败的消息(步骤S92)。接收该消息的桥接装置Y向接收装置B通知检查处理失败(步骤S89)。

图25是表示图22的桥接装置Y的详细的处理步骤的流程图。首先,桥接装置Y和接收装置B之间执行ID检查处理(步骤S101),检查失败的话,进行错误处理(步骤S02)。检查成功的话,和发送装置A或者桥接装置(以下称通信对象)之间进行ID检查处理(步骤S103)。检查失败的话,进到步骤S102,检查成功的话,和通信对象之间进行认证处理(步骤S104)。

认证成功的话,判定通信对象是否是桥接装置X(步骤S105)。不是桥接装置X的话,判断是发送装置A,在步骤S103加密一致的秘密固有ID,向发送装置A发送(步骤S106)。如果是桥接装置X的话,则从接收装置B接收代

理 ID 检查请求（步骤 S107）。

接着，解密从接收装置 B 来的转发数 N（步骤 S108），取得转发数 N（步骤 S109）。接着，转发数减 1（步骤 S110），判定 N-1 是否比 0 大（步骤 S111）。如果 N-1 小于或者等于 0，则向接收装置 B 发送代理 ID 检查错误，同时向桥接装置 X 发送 ID 检查错误（步骤 S112）。如果 N-1 大于 0，则向桥接装置 X 发送代理 ID 检查（步骤 S113）。接着，向桥接装置 X 发送接收装置 B 具有的秘密固有 ID（步骤 S114）。

这样，在第二实施例中，通过包含用于限制在装置间收发的控制信息中的桥接装置的传送次数的转发数，可以灵活地限制从发送装置 A 直到到达接收装置 B 通过的桥接装置的数目。另外，根据本方法，无需在内容自身内嵌入转发数，可以抑制信息的传送量或者简化发送装置 A 和接收装置 B 的处理步骤。

再有，内容传送路径和认证路径不同是本实施例的特征。亦即，在接收装置 B 和桥接装置 Y、桥接装置 X 和发送装置 A 之间以无线等位速率低的网络连接，而接收装置 B 和发送装置 A 以有线的位速率高的网络连接那样的状况下，可以只用无线进行认证、而用有线进行实际的内容的传送。因此，桥接装置 X、Y 未必一定具有进行内容的高速传送的处理能力，可以削减桥接装置 X、Y 的制造成本。

（第三实施例）

在第一和第二实施例中，说明了限制桥接装置进行桥接的次数的方法，但是在本实施例中，其特征是接收装置在认证、密钥交换之前，限制桥接的次数。

此外，在本实施例中，如图 20 那样的设备的结构为例说明。亦即，设想接收装置 B 和发送装置 A 不共有直接共同的秘密固有 ID，而通过桥接装置 X 和桥接装置 Y 可以进行内容收发的场合。

图 26 是表示涉及本实施例的接收装置 B 的一个实施例的概略结构的方框图。和图 17 的不同点是，在桥接装置检索处理部 57 内，新设置制作用于发送 ID 代理检查请求记述直到发送装置 A 所经由的桥接装置的路径的路径表的路径表制作部 66、检查该路径表的大小是否小于或者等于规定大小的路径表大小判别部 67。

图 27 是表示涉及本实施例的接收装置 B 的处理序列的一个示例的流程图。接收装置 B 发行内容接收请求命令（步骤 S121），首先解析是对哪个发送装置

A 的命令（步骤 S122），接着，在自身的 ID 列表中进行是否包含和该发送装置 A 的 ID 列表中包含的秘密固有 ID 相同的 ID 的检索处理（步骤 S123）。

因为 ID 列表为图 6 所示那样的结构，因此作为检索的键可以使用发送装置 A 的 MAC 地址或者 IP 地址等通用的设备中固有的信息。如果接收装置 B 具有与发送装置 A 共同的秘密固有 ID 的话，则遵照图 8 所示的步骤，可以直接进行认证、密钥交换（步骤 S124）。在接收装置 B 和发送装置 A 不共有秘密固有 ID 的场合，通过桥接装置进行认证、密钥交换。

首先，接收装置 B 进行用哪个路径经由桥接装置可以和发送装置 A 间接进行认证、密钥交换的路径检索处理（步骤 S125～S127）。该路径检索由下述 3 个步骤组成：（1）取得公开固有 ID（步骤 S125），（2）制作公开固有 ID 关系表（步骤 S126），（3）制作路径列表（步骤 S127）。这里，所谓路径列表，是从接收装置 B 到达桥接装置 X 所需要采取的认证路径。

（1）在获取公开固有 ID 中，进行哪个设备通过哪个短距离无线装置 X 登录的信息收集。在该信息收集中可以使用公开固有 ID。公开固有 ID，因为对发送装置 A、接收装置 B、桥接装置以外的设备是不保密的值，所以例如可以使发送装置 A、桥接装置的 IP 地址或者 MAC 地址成对通过网络路径检索。作为这一检索手段，例如如果使用广播 IP 地址的话，则可以对于连接在同一子网内的装置发送委托公开固有 ID 的发送的消息，接收该消息的装置返送公开固有 ID、自身装置的 MAC 或者 IP 地址。

（2）在公开固有 ID 关系表的制作中，把在（1）公开固有 ID 获取中得到的、各 MAC 地址和公开固有 ID 的一览汇总成表。图 28 是图示公开固有 ID 关系表的一个示例的图。在图 28 中，所谓装置的地址，指例如装置的网络接口固有的 MAC 地址或者 IP 地址等。通过该公开固有 ID 关系表，了解哪个装置具有哪个秘密固有 ID，亦即哪个装置通过哪个短距离无线装置 X 登录。

（3）在路径列表制作中，使用在（2）中制成的公开固有 ID 关系表，检索从自身装置用怎样的路径发送代理 ID 检查请求的话可以和目的地的发送装置 A 共有密钥。例如，在图 28 所示的公开固有 ID 关系表中，可以明白从接收装置 B 到发送装置 A 可以按桥接装置 Y、桥接装置 X 的顺序进行认证、密钥交换，能够制作图 29 所示的路径列表。

下面检查不同接收制作的路径列表的大小（步骤 S128）。在图 29 所示的例

子中，到作为目的地的接收装置需要经过两个桥接装置。这里如果假定限制桥接装置的数目为 1 的话，则该大小检查失败，执行错误处理（步骤 S129）。另一方面，如果许可桥接装置的数目可以到两个，路径列表的大小在规定的量以内的话，则向桥接装置发送代理 ID 检查请求、公开固有 ID 列表、发送装置 A 地址（步骤 S130）。

图 30 是表示接收装置 B 向桥接装置 Y 发送的代理 ID 检查请求命令的一个示例的图。

图 30 的代理 ID 检查请求命令包含命令发送目的地地址（在这一场合为桥接装置 Y 的地址）、命令发送源地址（在这一场合为接收装置 B 的地址）、公开固有 ID 列表（在这一场合为 ZZ）、第一中继主机的地址（在这一场合为桥接装置 X 的地址）、和第二中继主机的地址（在这一场合为发送装置 A 的地址）。

桥接装置 Y，从接收装置 B 接收图 30 所示的命令，进行图 27 所示的处理后，对于桥接装置 X 发送代理 ID 检查请求命令。

图 31 是表示桥接装置 Y 向桥接装置 X 发送的代理 ID 检查请求命令的一个示例的图。图 31 的代理 ID 检查请求命令包含命令发送目的地地址（在这一场合为桥接装置 X 的地址）、命令发送源地址（在这一场合为桥接装置 Y 的地址）、公开固有 ID 列表（在这一场合为 YY 和 ZZ）、和第二中继主机的地址（在这一场合为发送装置 A 的地址）。

此外，在该例中表示了从接收装置 B 向发送装置 A 发送代理 ID 检查请求的例子，但是在从发送装置 A 向接收装置 B 发送代理 ID 检查请求的场合，这一桥接检索处理以及路径表大小检查处理在发送装置 A 中进行。

这样在第三实施例中，通过接收装置 B 限制路径列表的大小，可以在代理 ID 检查请求的发送或者认证、密钥交换之前限制桥接的次数。根据该实施例，可以避免不需要的代理 ID 检查请求的收发，可以减轻网络负荷以及设备的处理负荷。

（第四实施例）

在上述的第三实施例中，说明了接收装置 B 检查路径列表的大小后，如果小于或者等于规定的大小的话，则中止代理 ID 检查请求的发送的方法，在以下说明的第四实施例中，是桥接装置检查在认证、密钥交换处理后到此为止所通过的路径列表。在路径列表中，包含接收装置和桥接装置 Y 的 ID。作为路径列

表中包含的 ID 例如可以使用图 15 那样的认证、密钥交换处理时利用的证明书中包含的 ID 字段的值。

图 32 是表示在第四实施例中的桥接装置的概略结构的一个示例的方框图。和图 21 的不同点是在认证密钥交换处理部中具有路径列表检查部 68。

图 33 是表示桥接装置 X、Y 进行路径列表的大小检查的场合的处理序列的一个示例的序列图。在图 33 的处理之前，进行和图 18 或者图 22 同样的处理，不过在这里省略。

桥接装置 X 对桥接装置 Y 通知 ID 检查处理成功后（步骤 S141），桥接装置 Y 对接收装置 B 通知该意思（步骤 S142）。其后进行桥接装置 X、Y 之间的认证、密钥交换处理（步骤 S143），在桥接装置 Y 和接收装置之间也进行认证、密钥交换处理（步骤 S144）。此时，桥接装置 Y 从桥接装置 X 的证明书中识别桥接装置 X 是桥接装置（步骤 S145），进行路径列表的大小检查（步骤 S146）。

如果大小小于或者等于规定的大小，则桥接装置 Y 对桥接装置 X 进行代理 ID 检查请求（步骤 S147）。此时，加密路径列表和接收装置具有的秘密固有 ID 并发送。

桥接装置 X，进行从桥接装置 Y 发送的路径列表的大小检查（步骤 S148），如果大小小于或等于规定的大小，则和接收装置 B 之间进行认证、密钥交换处理（步骤 S149）。其后，桥接装置 X 和接收装置 B 使用共同的秘密固有 ID 生成密钥（步骤 S150，S151），发送加密的内容（步骤 S152）。

图 34 是表示桥接装置 X 的处理序列的一个示例的流程图。首先判定通信目的地是否是桥接装置（步骤 S161），不是桥接装置的话，在 ID 检查中加密一致的秘密固有信息并发送（步骤 S162）。

如果通信目的地是桥接装置的话，则接收从桥接装置 Y 来的代理 ID 检查请求（步骤 S163）。接着，解密接收的路径列表（步骤 S164），取得路径列表（步骤 S165）。在路径列表中包含接收装置和桥接装置 Y 的 ID。作为包含在路径列表中的 ID，例如可以使用图 15 那样的认证、密钥交换处理时利用的证明书中包含的 ID 字段的值。

判定路径列表的大小是否比规定大小大（步骤 S166），大的话，向桥接装置 Y 发送代理 ID 检查错误，还向通信目的地发送代理 ID 检查错误（步骤 S167）。

如果路径列表的大小小于或等于规定大小，则向通信目的地发送代理 ID

检查请求（步骤S168），从桥接装置Y向通信目的地发送接收装置B具有的秘密固有ID（步骤S169）。

这样，涉及第四实施例的接收装置，在同一短距离无线装置X上登录，向认证桥接数最小（或者登录最多设备）的桥接装置发送代理ID检查请求。这在网络结构动态变更的场合特别有意义。在家庭内网络设备中，在很多场合关断电源。因此，不限于在某特定的日期时间工作的桥接装置在其他的日子也工作。这样，即使在家庭内网络的结构动态变更的场合，根据本实施例，可以向认证桥接数最小的桥接装置发送代理ID检查请求，可以高效率地进行通信。

图1

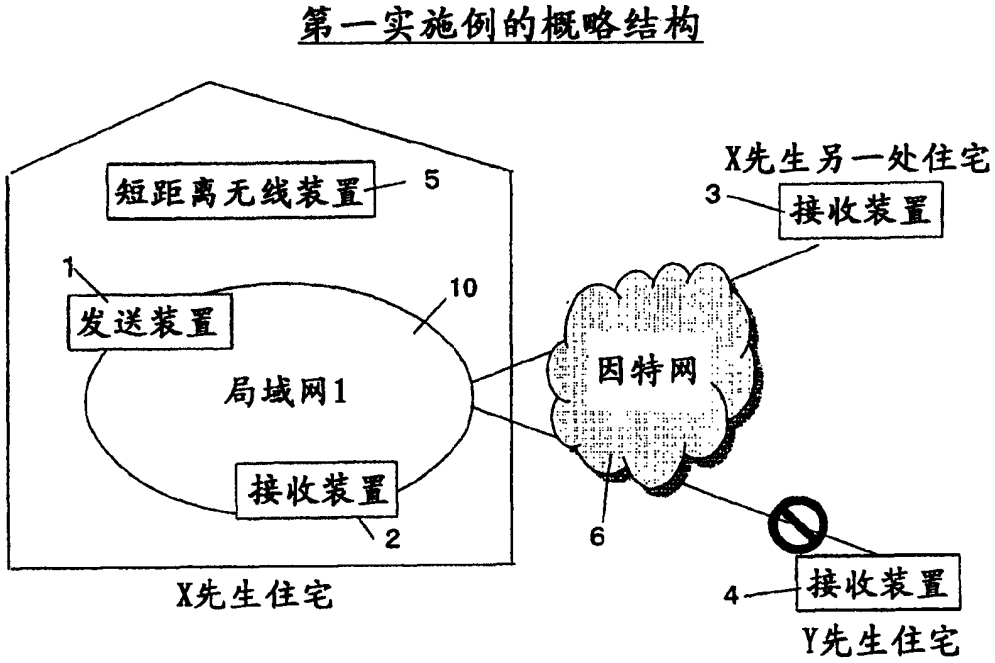

第一实施例的概略结构
短距离无线装置
5
X先生另一处住宅
3
接收装置
1
发送装置
10
局域网1
因特网
接收装置
2
6
4
接收装置
X先生住宅
Y先生住宅

图2

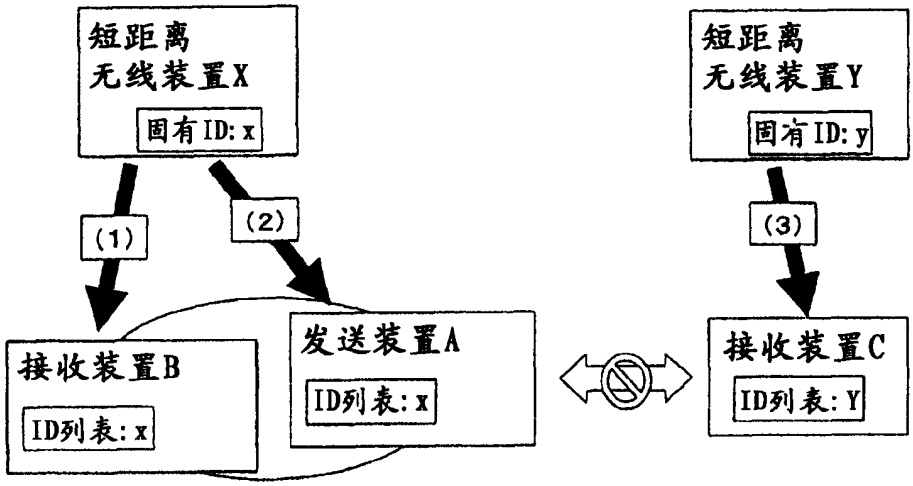

短距离
无线装置X
固有ID:x
短距离
无线装置Y
固有ID:y
(1)
(2)
(3)
接收装置B
ID列表:x
发送装置A
ID列表:x
接收装置C
ID列表:Y

图3

短距离无线装置X的概略结构

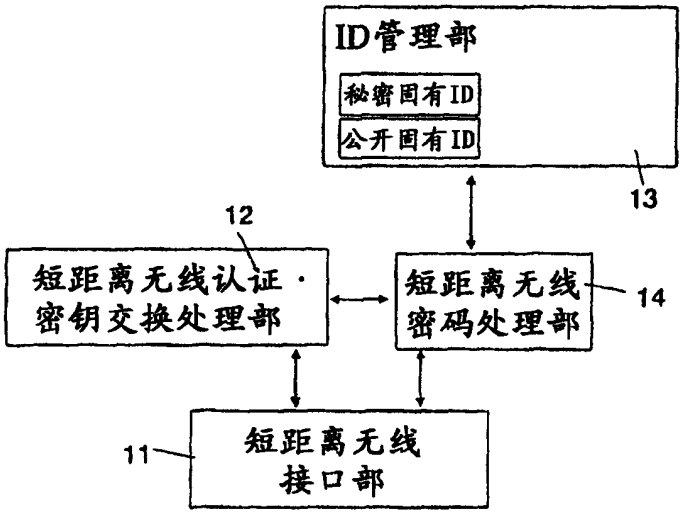


图4

发送装置A的概略结构

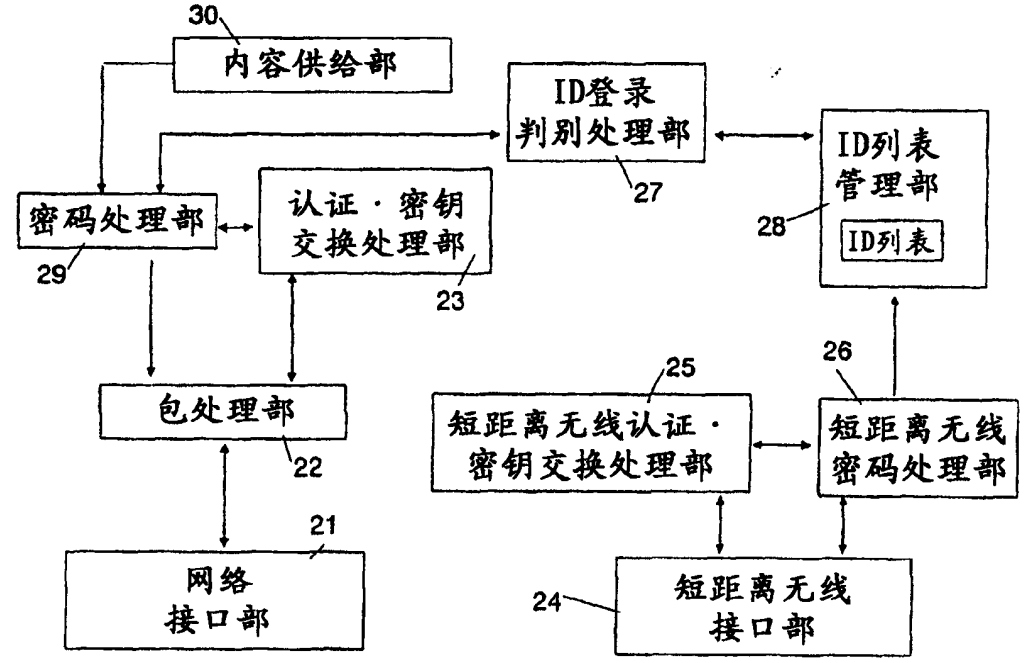


图5

接收装置B的概略结构

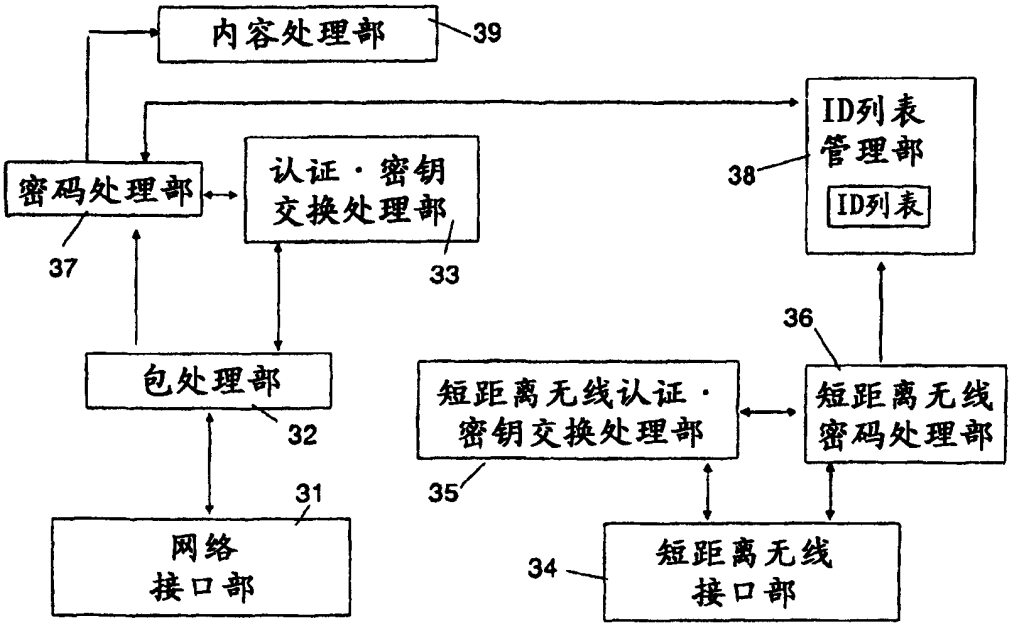


图6

ID列表

必选项		可选项	
公开 固有ID	秘密 固有ID	登录日期时间	设备中通用的 固有信息
XX	x	○月×日△时×分	XX:YY:ZZ:AA
AA	A	×月□日△时○分	AA:BB:CC:DD
EE	E	×月□日×时□分	EE:FF:00:11
…		…	

图7

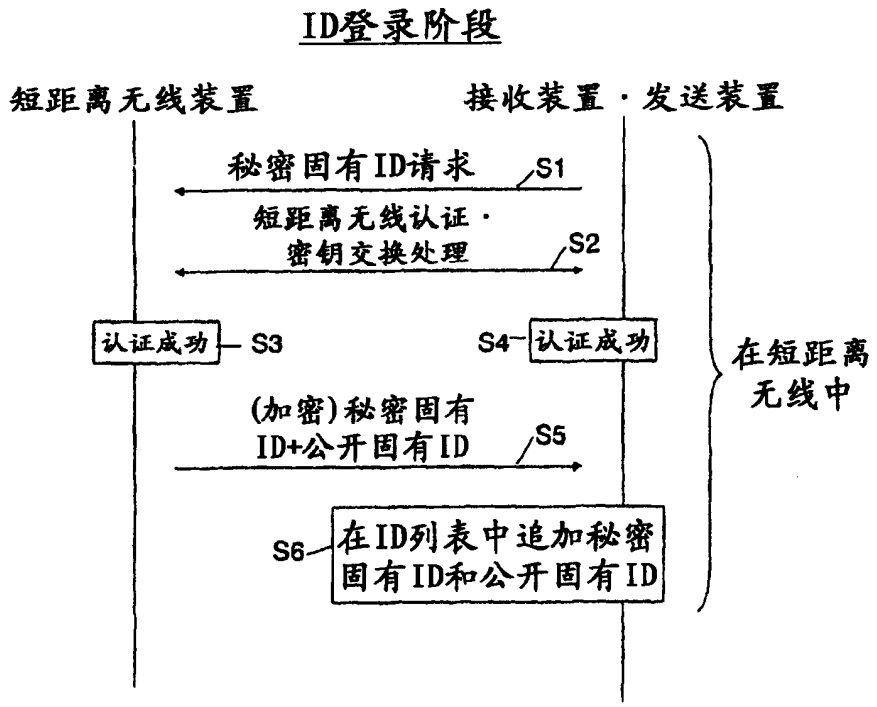

ID登录阶段
短距离无线装置
接收装置·发送装置
秘密固有ID请求
S1
短距离无线认证·
密钥交换处理
S2
认证成功
S3
S4
认证成功
在短距离
无线中
(加密)秘密固有
ID+公开固有ID
S5
S6
在ID列表中追加秘密
固有ID和公开固有ID

图8

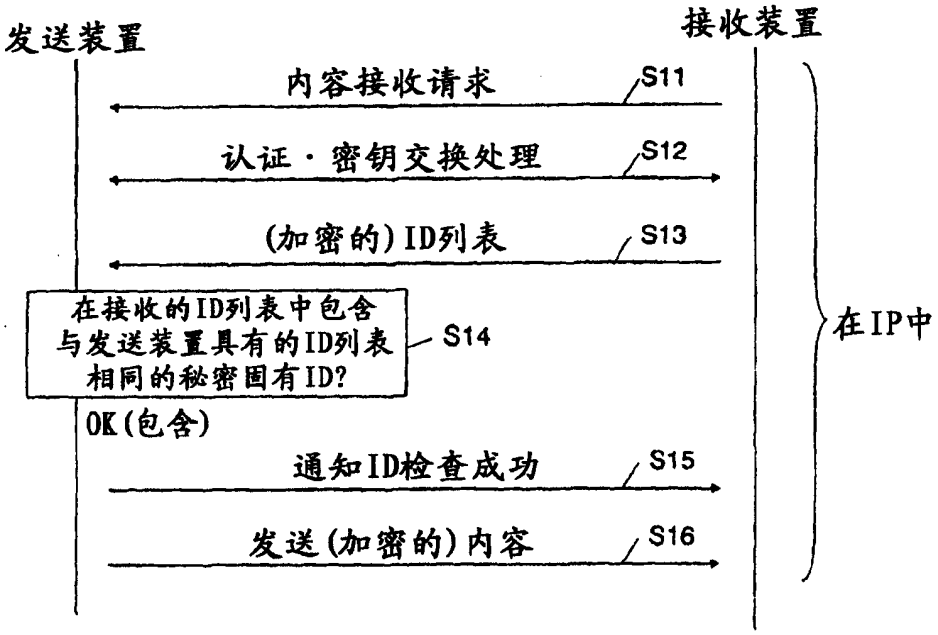

内容传送阶段
发送装置
接收装置
内容接收请求
S11
认证·密钥交换处理
S12
(加密的)ID列表
S13
在接收的ID列表中包含
与发送装置具有的ID列表
相同的秘密固有ID?
S14
OK(包含)
通知ID检查成功
S15
发送(加密的)内容
S16
在IP中

图9

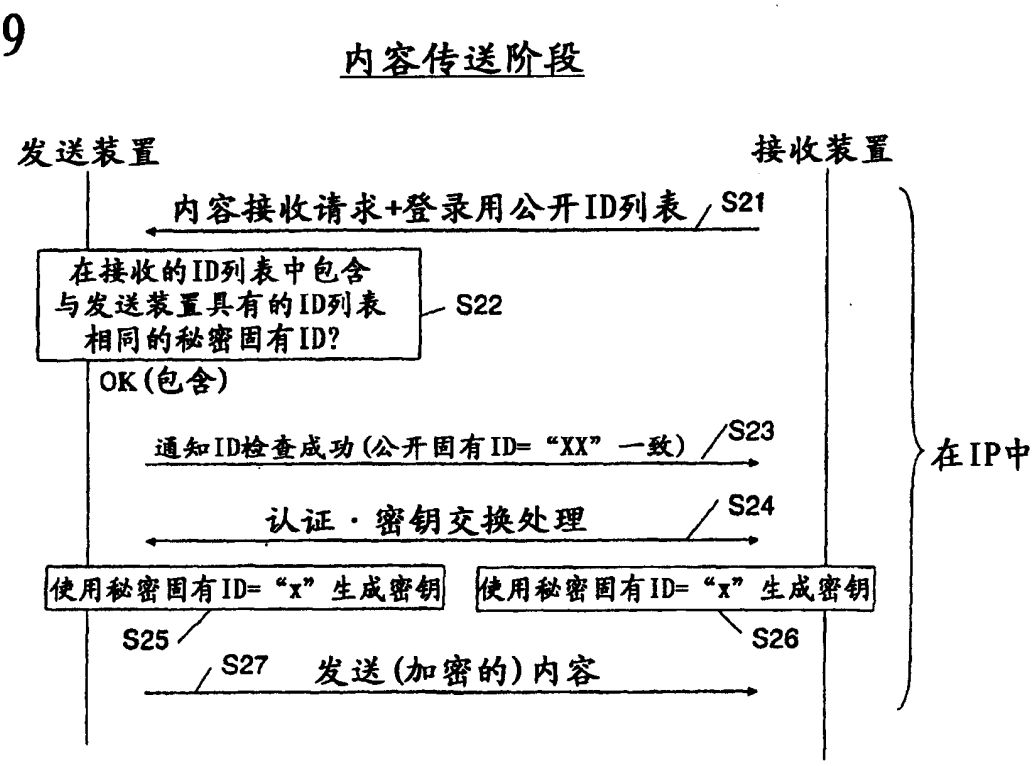

内容传送阶段
发送装置
接收装置
内容接收请求+登录用公开ID列表
S21
在接收的ID列表中包含
与发送装置具有的ID列表
相同的秘密固有ID?
S22
OK(包含)
通知ID检查成功(公开固有ID="XX"一致)
S23
认证·密钥交换处理
S24
使用秘密固有ID="x"生成密钥
使用秘密固有ID="x"生成密钥
S25
S26
S27
发送(加密的)内容
在IP中

图10

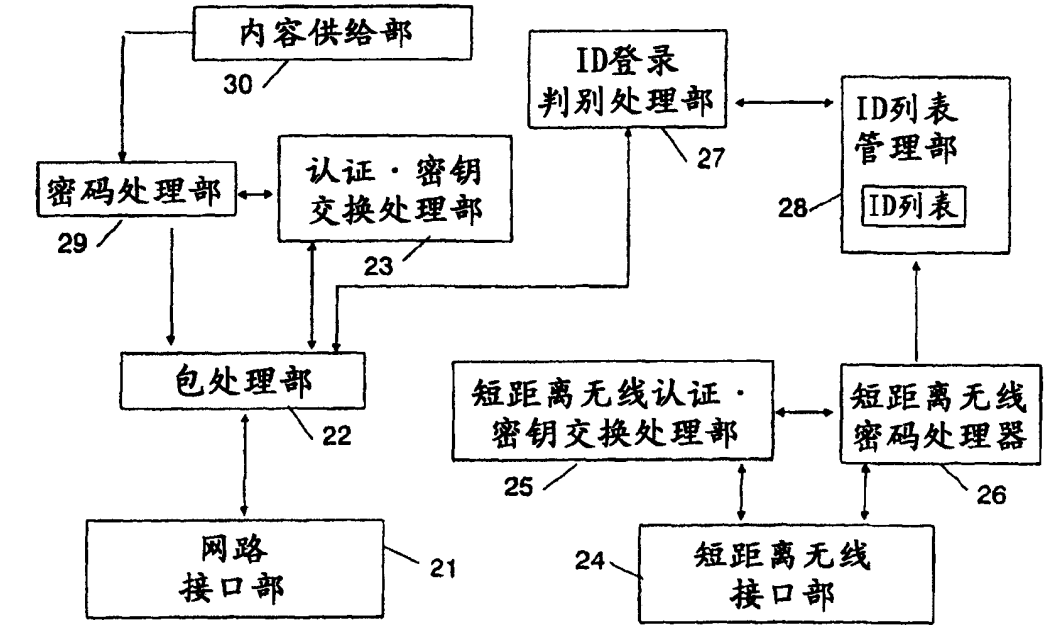

发送装置A的概略结构
内容供给部
30
ID登录
判别处理部
27
ID列表
管理部
28
ID列表
密码处理部
29
认证·密钥
交换处理部
23
包处理部
22
短距离无线认证·
密钥交换处理部
25
短距离无线
密码处理器
26
网路
接口部
21
24
短距离无线
接口部

图11

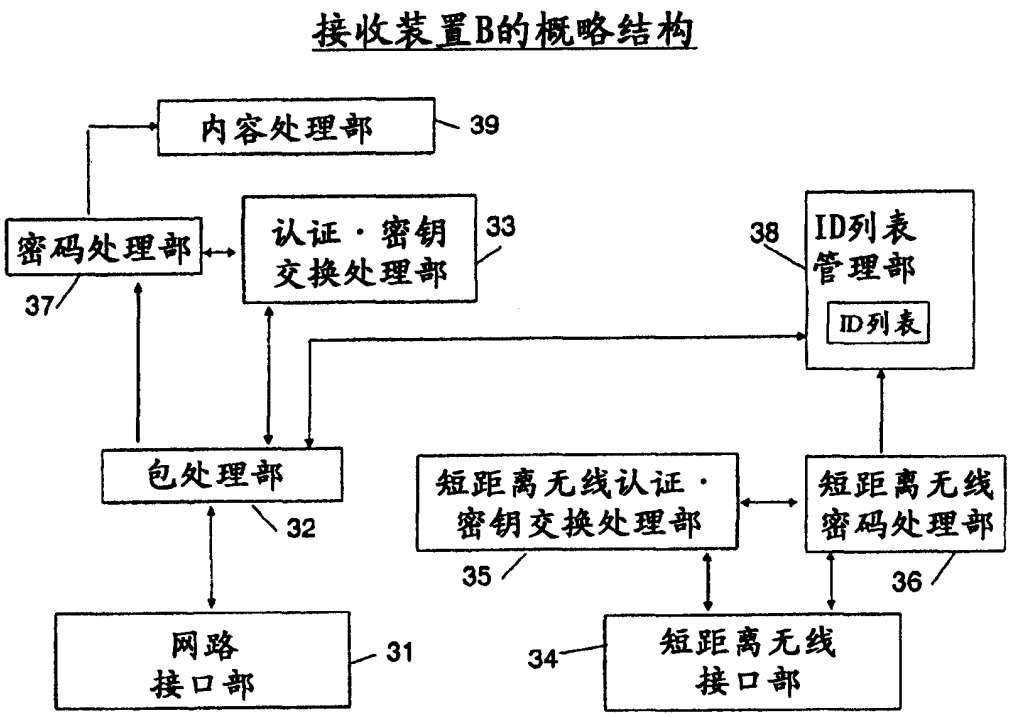

接收装置B的概略结构
内容处理部
39
密码处理部
37
认证·密钥
交换处理部
33
38
ID列表
管理部
ID列表
包处理部
32
短距离无线认证·
密钥交换处理部
35
短距离无线
密码处理部
36
网路
接口部
31
34
短距离无线
接口部

图12

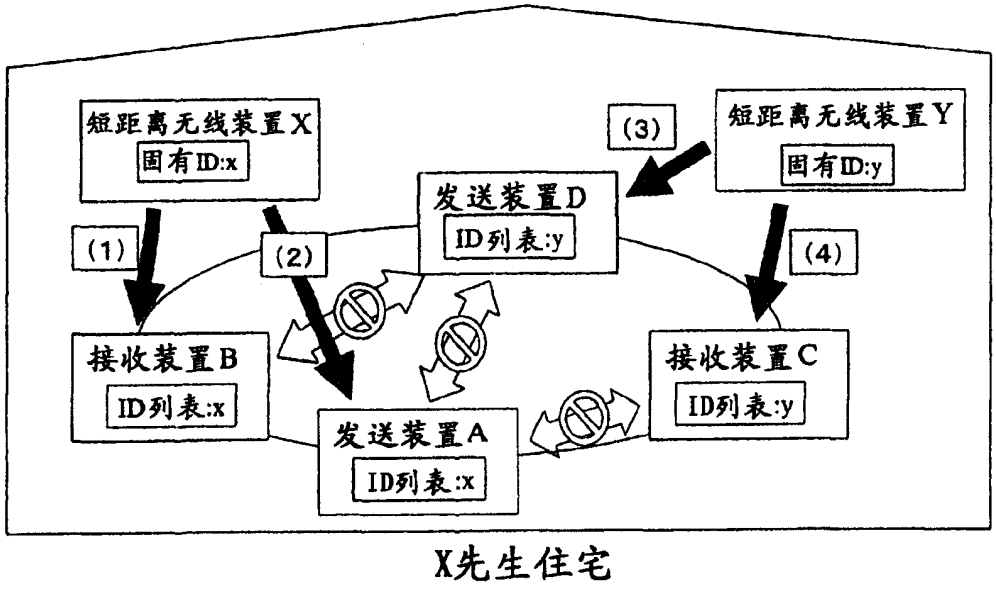
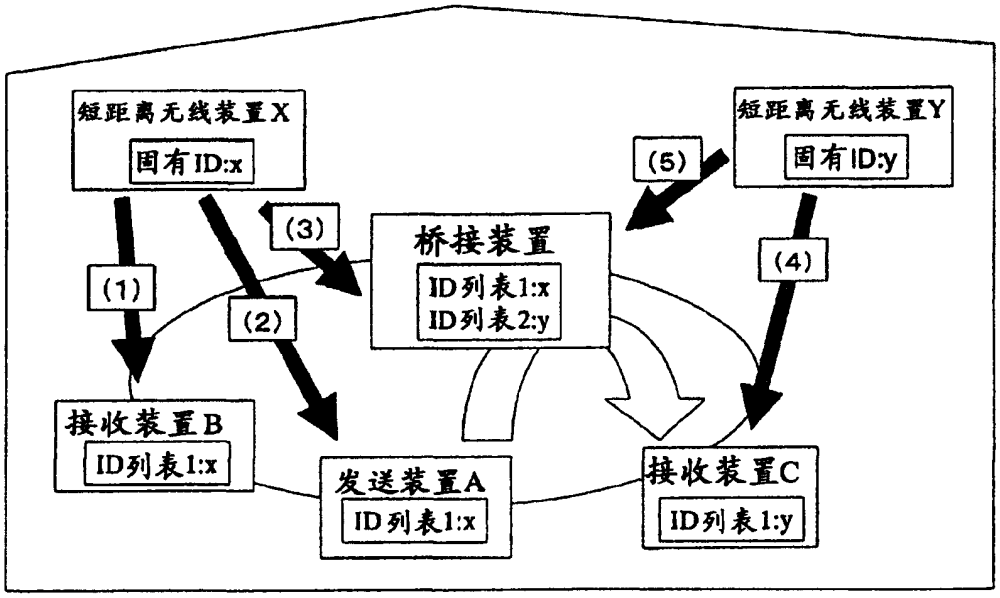

短距离无线装置X
固有ID:x
(3)
短距离无线装置Y
固有ID:y
发送装置D
ID列表:y
(1)
(2)
(4)
接收装置B
ID列表:x
接收装置C
ID列表:y
发送装置A
ID列表:x
X先生住宅

图13

桥接装置概念图



X先生住宅

图14

桥接装置的概略结构

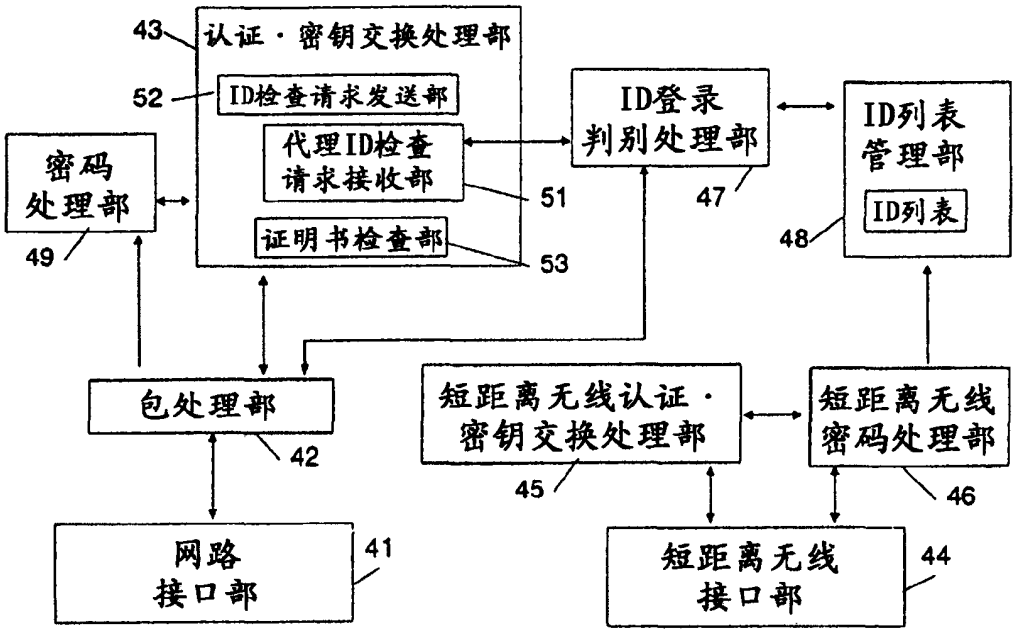


图15

证明书格式

版本号	1
认证类别	公开密钥方式
ID	AABBCC
公开密钥	XXXX
装置类别	桥接装置
签名	YYYYYYY

图16

发送装置A的概略结构

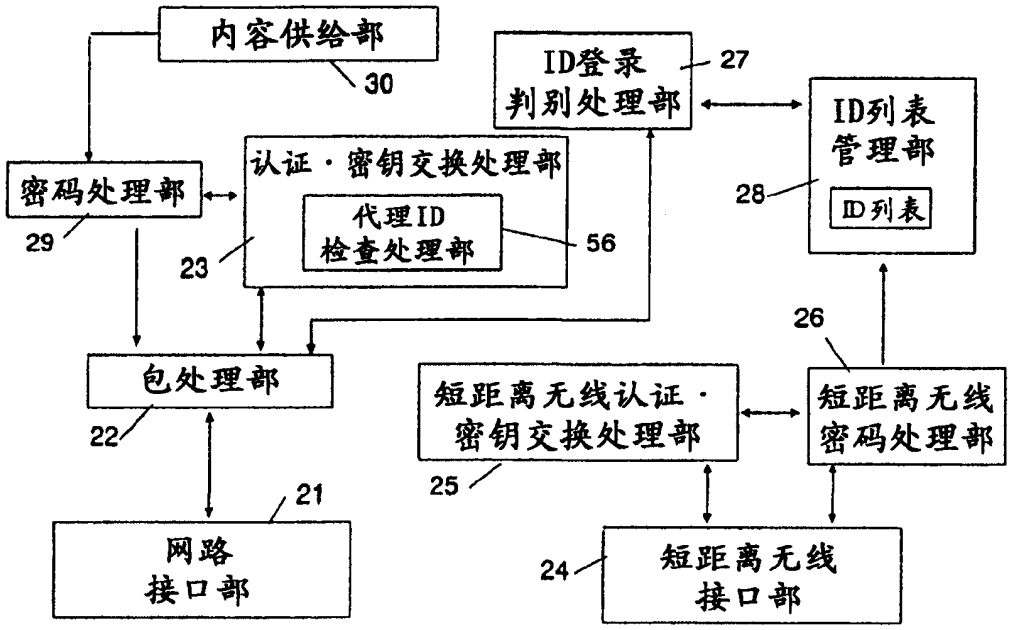


图17

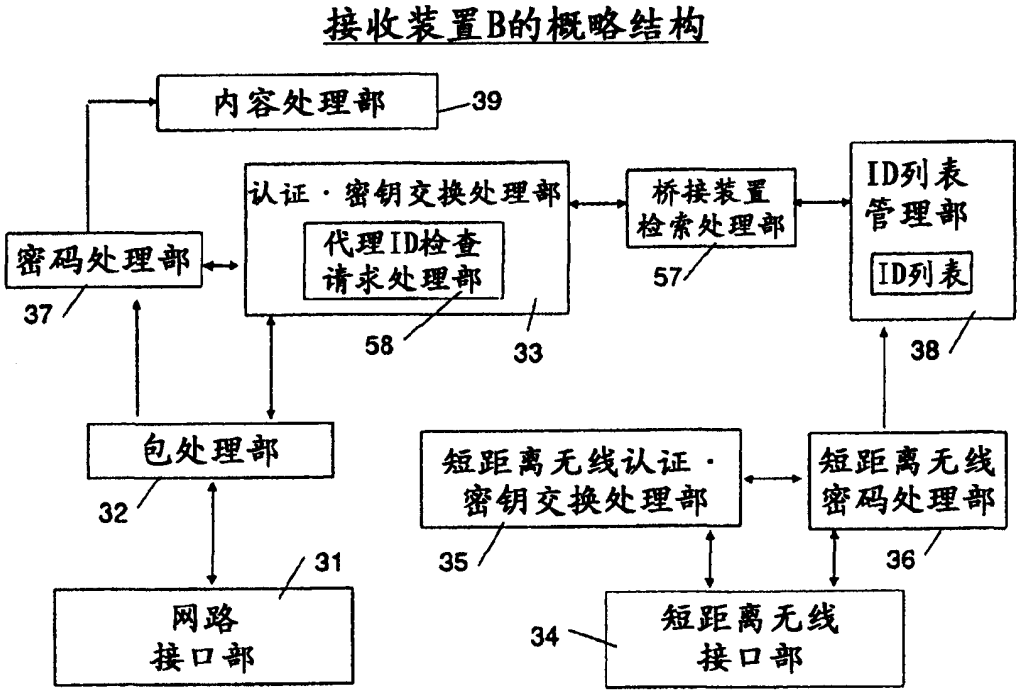

接收装置B的概略结构
内容处理部
39
认证·密钥交换处理部
代理ID检查
请求处理部
桥接装置
检索处理部
ID列表
管理部
ID列表
密码处理部
37
58
33
57
38
包处理部
32
短距离无线认证·
密钥交换处理部
短距离无线
密码处理部
35
36
31
网路
接口部
34
短距离无线
接口部

图18

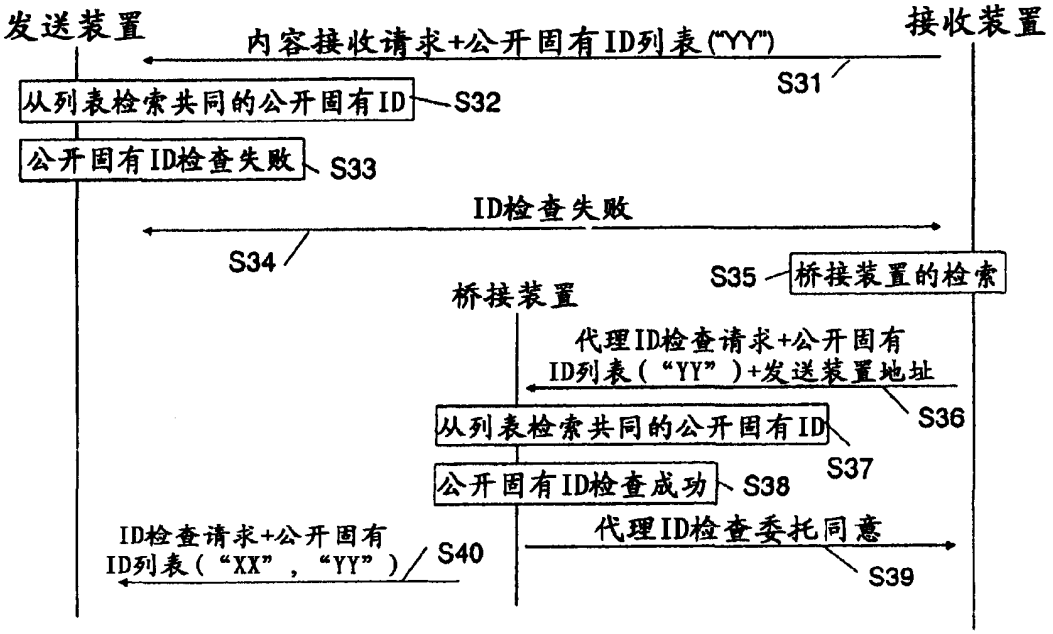

内容传送阶段(桥接)
发送装置
接收装置
内容接收请求+公开固有ID列表("YY")
S31
从列表检索共同的公开固有ID
S32
公开固有ID检查失败
S33
ID检查失败
S34
S35
桥接装置的检索
桥接装置
代理ID检查请求+公开固有
ID列表(“YY”)+发送装置地址
S36
从列表检索共同的公开固有ID
S37
公开固有ID检查成功
S38
ID检查请求+公开固有
ID列表(“XX”,“YY”)
S40
代理ID检查委托同意
S39

图19

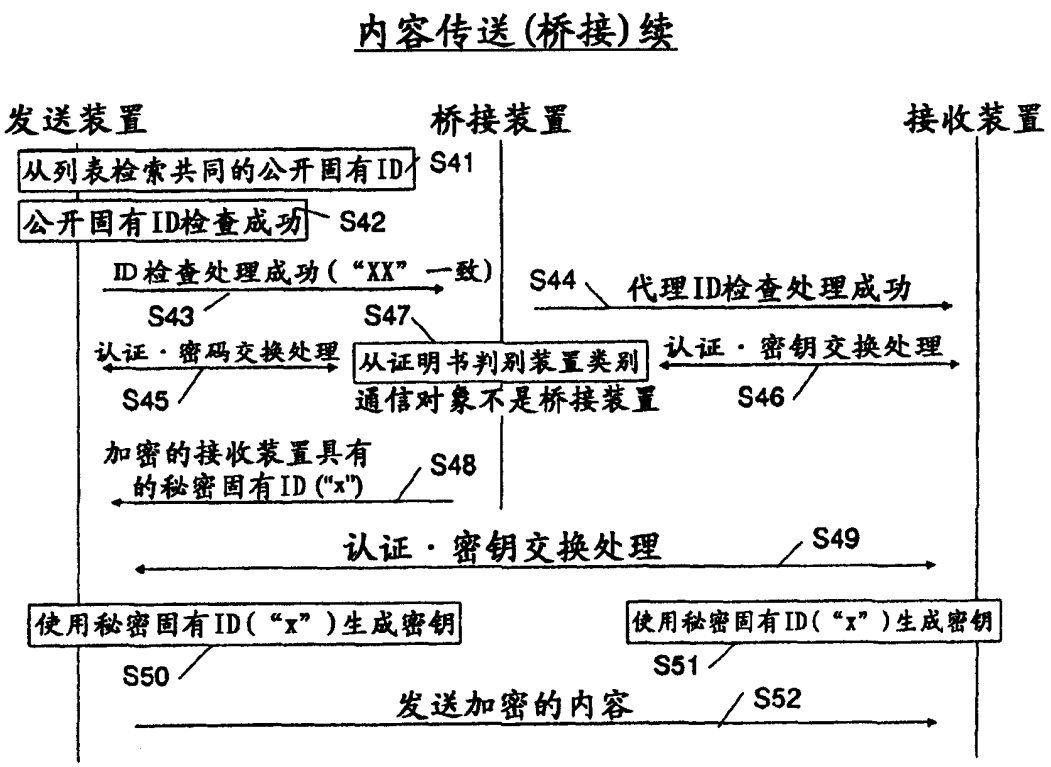

内容传送(桥接)续
发送装置
桥接装置
接收装置
从列表检索共同的公开固有ID
S41
公开固有ID检查成功
S42
ID检查处理成功(“XX”一致)
S43
S44
代理ID检查处理成功
S47
认证·密码交换处理
S45
从证明书判别装置类别
通信对象不是桥接装置
认证·密钥交换处理
S46
加密的接收装置具有的秘密固有ID(“x”)
S48
认证·密钥交换处理
S49
使用秘密固有ID(“x”)生成密钥
S50
使用秘密固有ID(“x”)生成密钥
S51
发送加密的内容
S52

图20

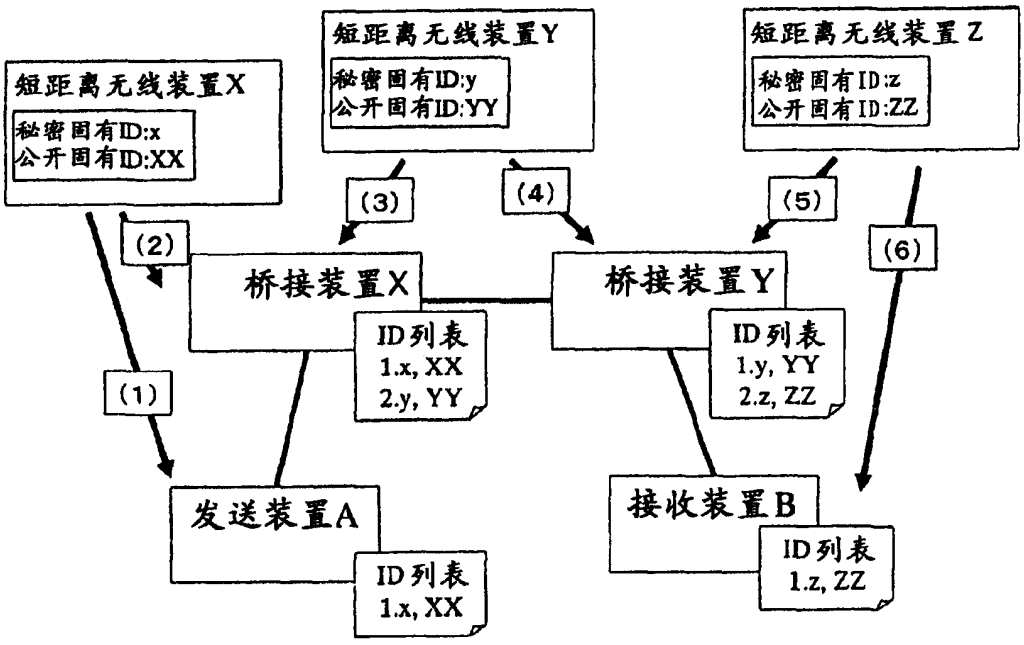

设备固有ID关系图
短距离无线装置X
秘密固有ID:x
公开固有ID:XX
短距离无线装置Y
秘密固有ID:y
公开固有ID:YY
短距离无线装置Z
秘密固有ID:z
公开固有ID:ZZ
(1)
(2)
(3)
(4)
(5)
(6)
桥接装置X
桥接装置Y
ID列表
1.x, XX
2.y, YY
ID列表
1.y, YY
2.z, ZZ
发送装置A
ID列表
1.x, XX
接收装置B
ID列表
1.z, ZZ

图21

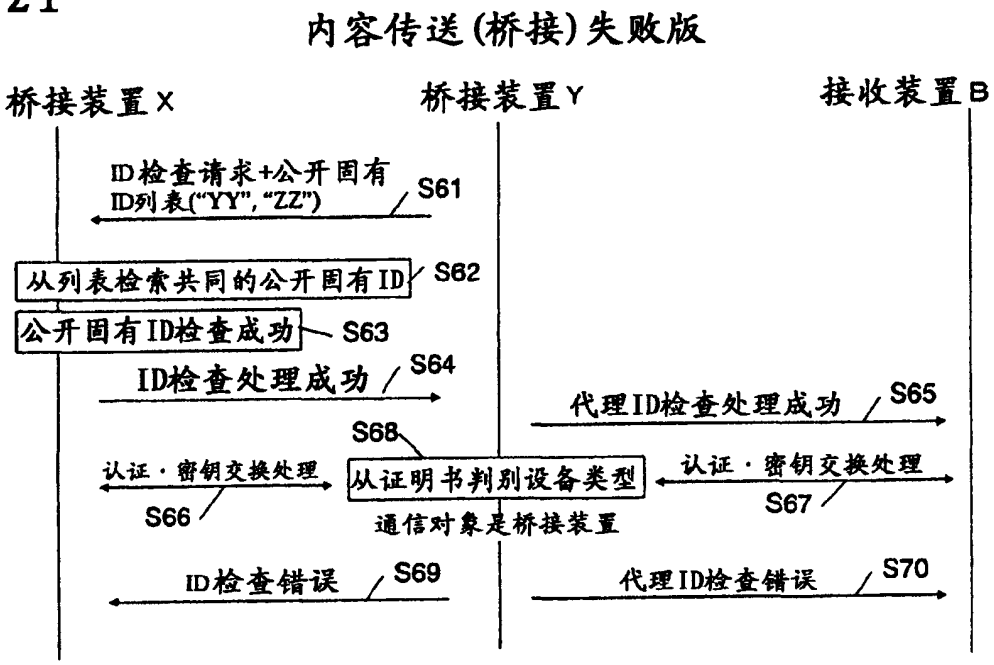

内容传送(桥接)失败版
桥接装置X
桥接装置Y
接收装置B
ID检查请求+公开固有ID列表("YY","ZZ")
S61
从列表检索共同的公开固有ID
S62
公开固有ID检查成功
S63
ID检查处理成功
S64
代理ID检查处理成功
S65
S68
认证·密钥交换处理
从证明书判别设备类型
认证·密钥交换处理
S66
S67
通信对象是桥接装置
ID检查错误
S69
代理ID检查错误
S70

图22

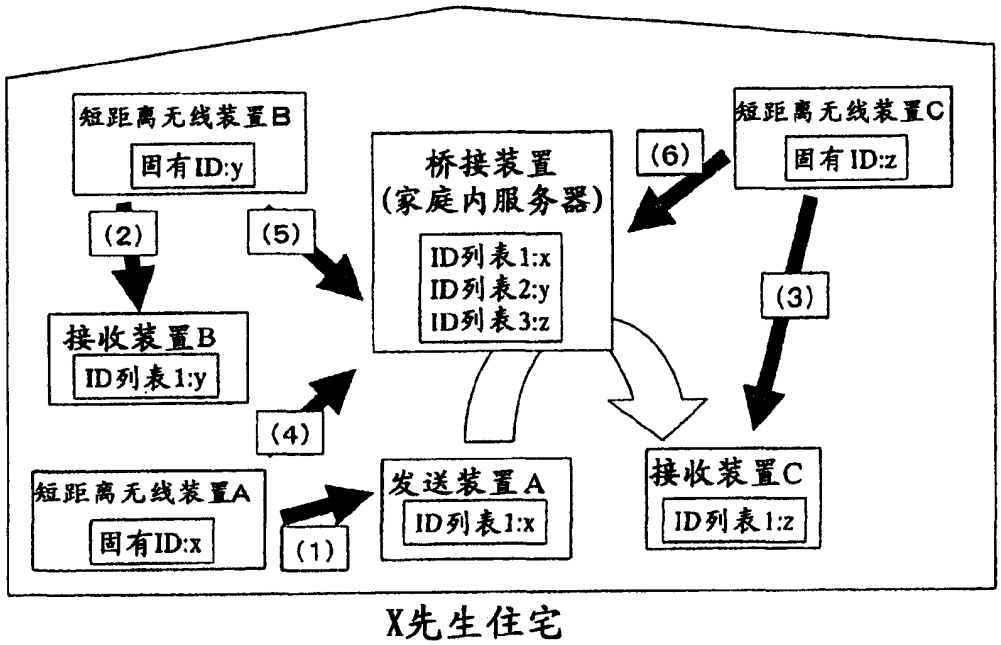

桥接装置概念图
短距离无线装置B
固有ID:y
桥接装置
(家庭内服务器)
ID列表1:x
ID列表2:y
ID列表3:z
短距离无线装置C
固有ID:z
(2)
(5)
(6)
(3)
接收装置B
ID列表1:y
(4)
短距离无线装置A
固有ID:x
(1)
发送装置A
ID列表1:x
接收装置C
ID列表1:z
X先生住宅

图23

桥接装置的概略结构

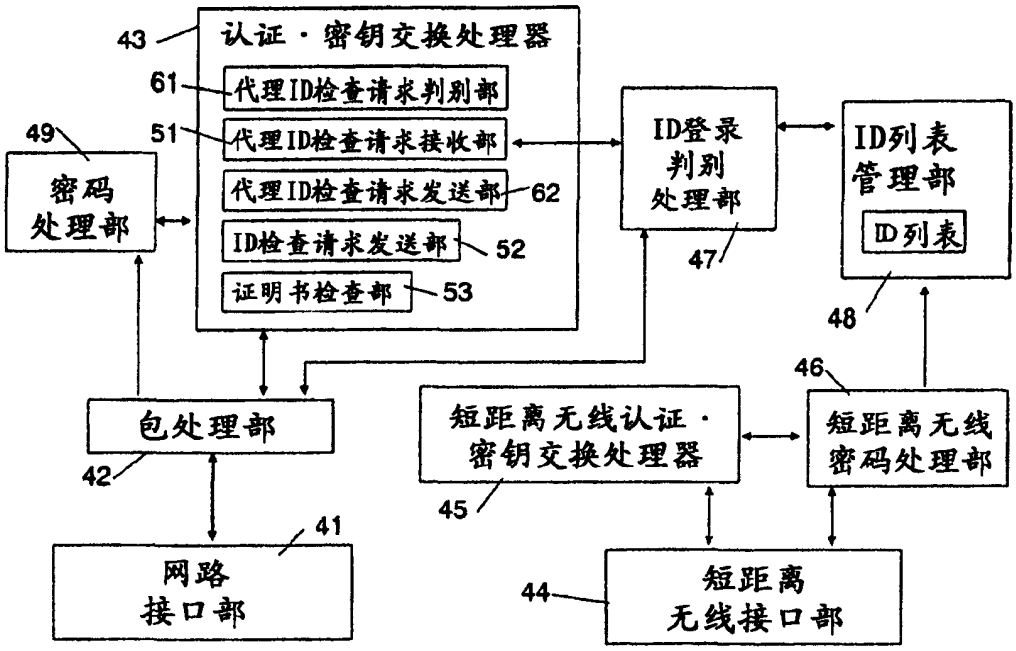


图24

内容传送(桥接)

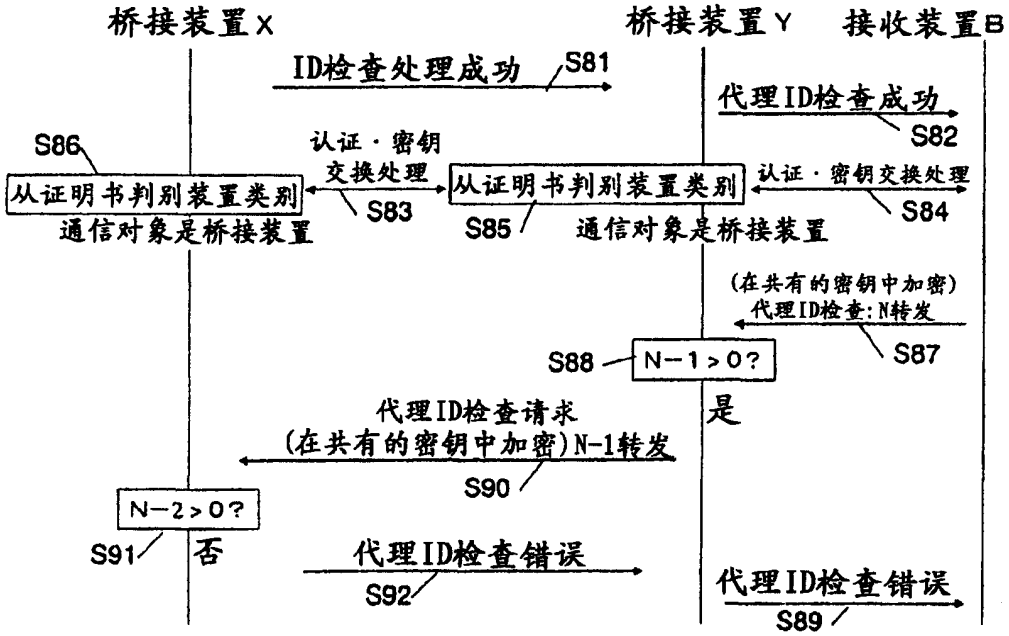


图25

桥接装置Y的处理内容

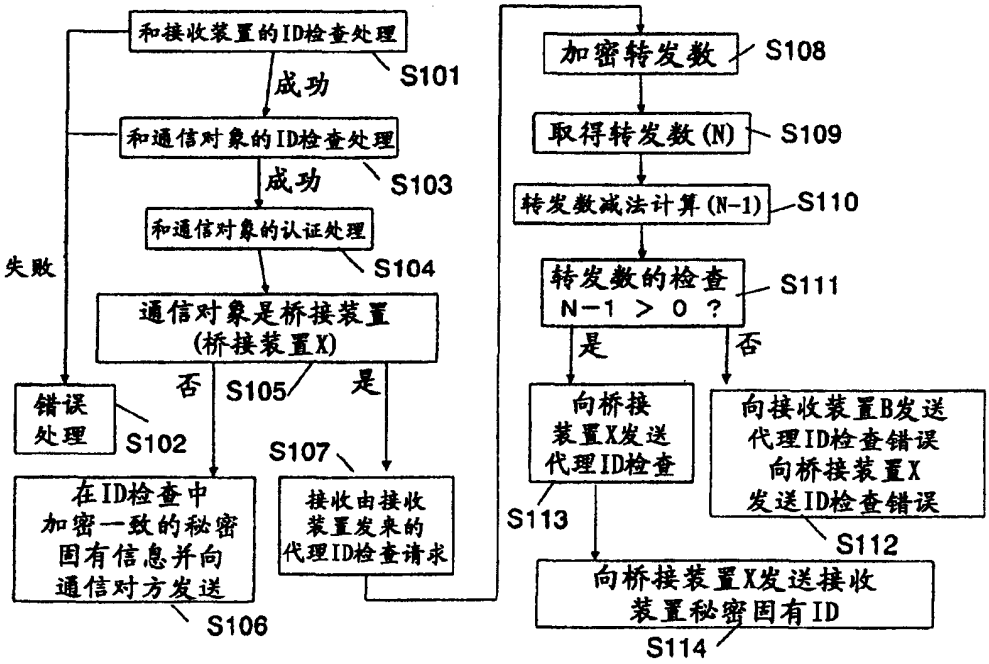


图26

接收装置B的概略结构

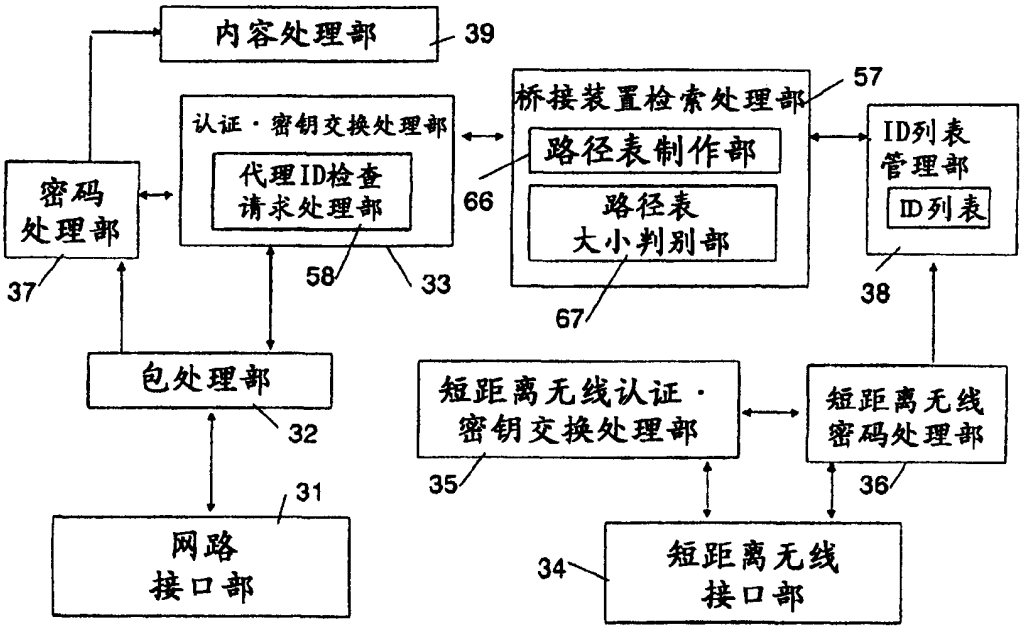


图27

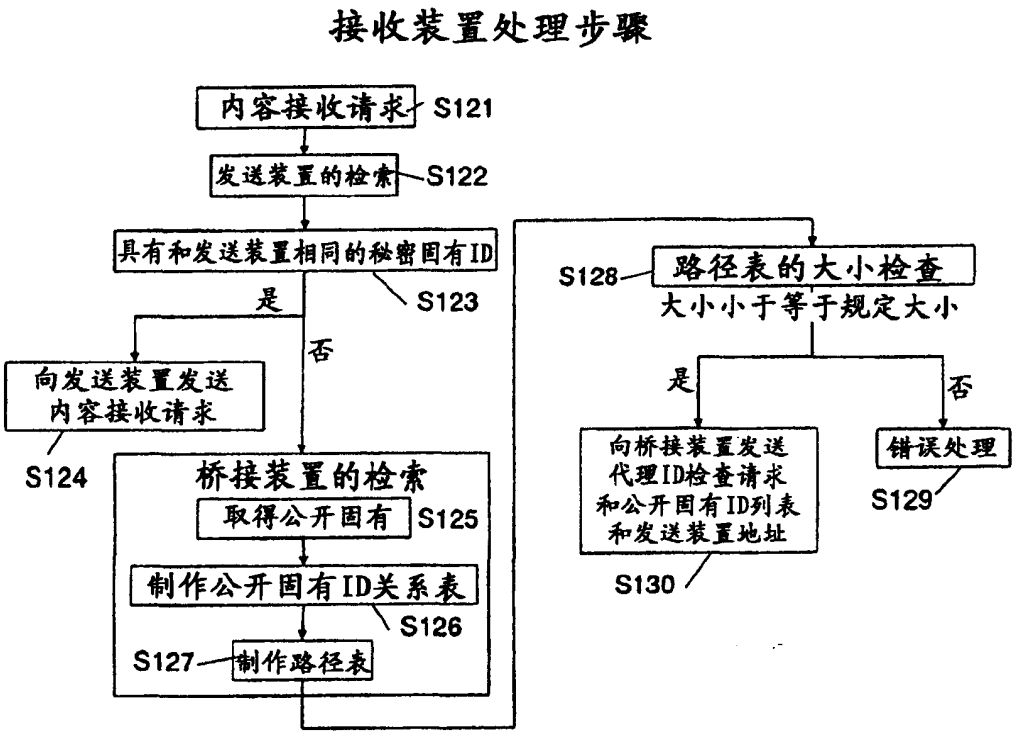


图28

公开固有ID关系表

装置的地址	公开固有ID
B	ZZ
Y	ZZ
Y	YY
X	YY
X	XX
A	XX
…	

图29

路径表

路径顺序	装置的地址	公开固有ID
1	Y	XX
2	X	CC
3	A	DD

图30

代理ID检查请求命令
(接收装置B)

命令发送目的地地址 =Y	命令发送源地址 =B	公开固有ID列表 ("ZZ")	第一中继主机的地址 =X	第二中继主机的地址 =A

图31

代理ID检查请求命令
(桥接装置Y)

命令发送目的地地址 =X	命令发送源地址 =Y	公开固有ID列表 ("YY, ZZ")	第二中继主机的地址 =A

图32

桥接装置的概略结构

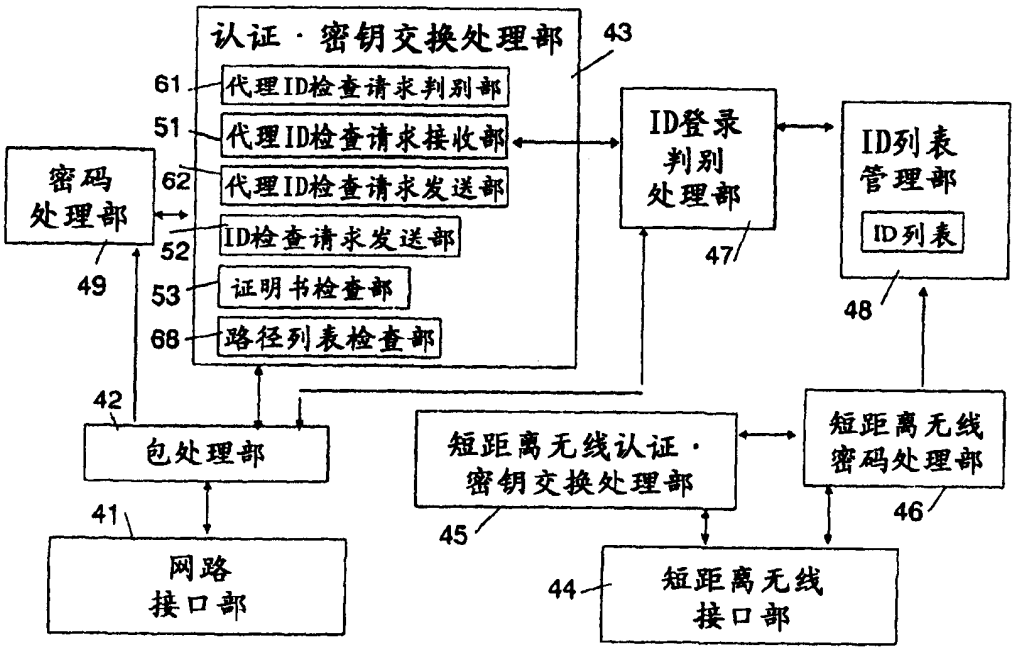


图33

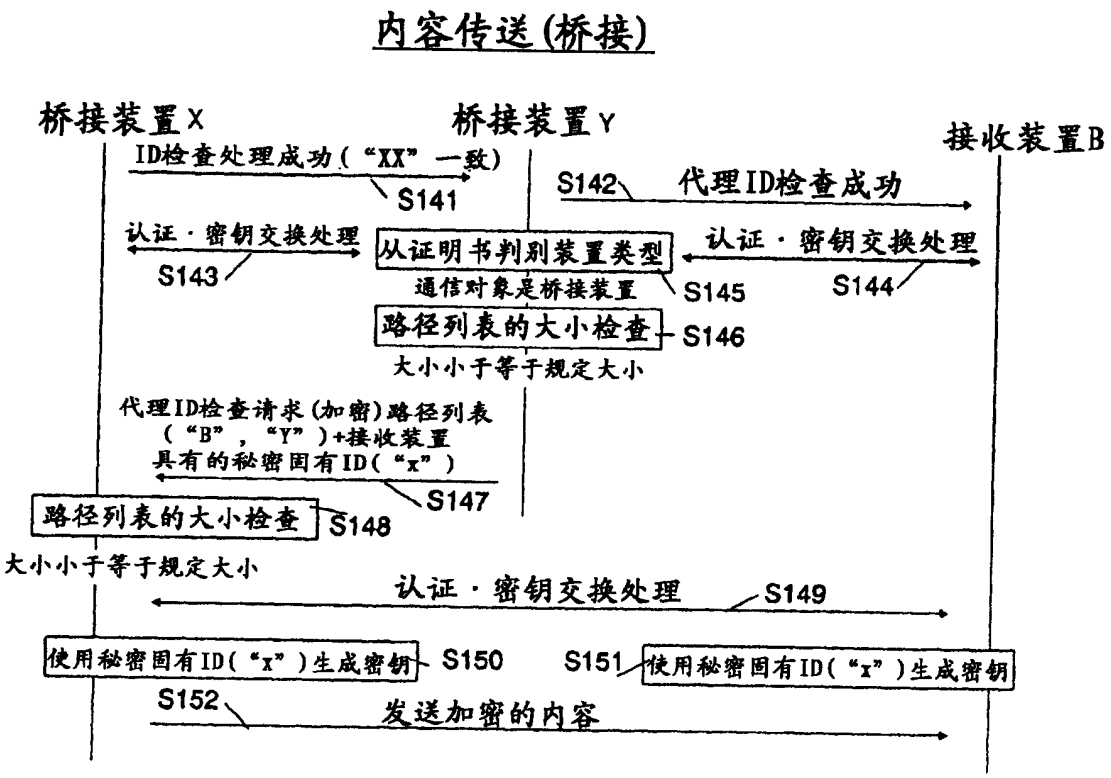
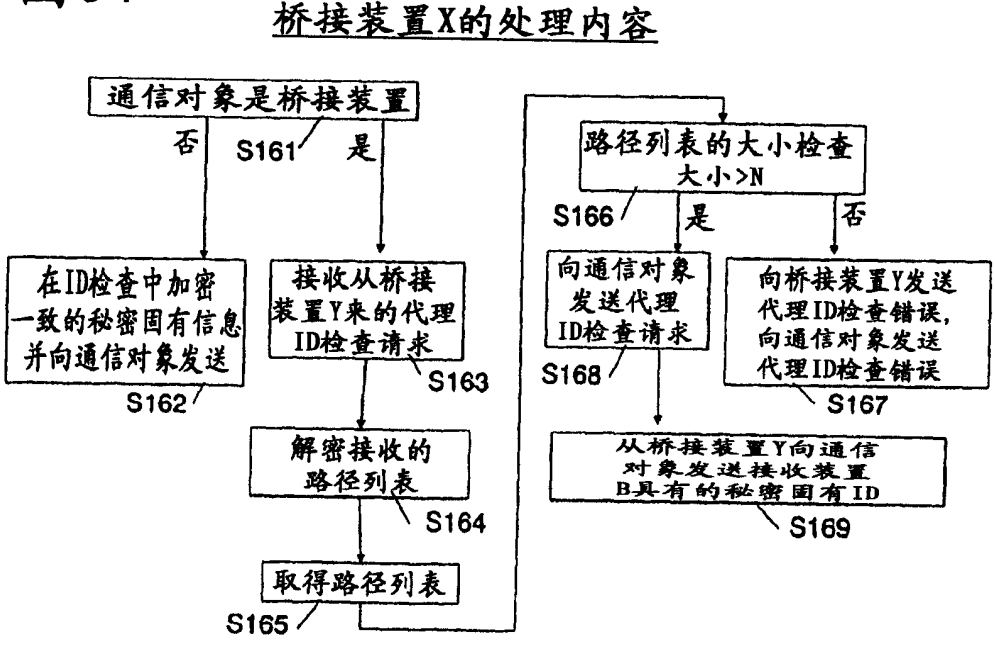

内容传送(桥接)
桥接装置X
桥接装置Y
接收装置B
ID检查处理成功(“XX”一致)
S141
S142
代理ID检查成功
认证·密钥交换处理
S143
从证明书判别装置类型
认证·密钥交换处理
S144
通信对象是桥接装置
S145
路径列表的大小检查
S146
大小小于等于规定大小
代理ID检查请求(加密)路径列表
(“B”,“Y”)+接收装置
具有的秘密固有ID(“x”)
S147
路径列表的大小检查
S148
大小小于等于规定大小
认证·密钥交换处理
S149
使用秘密固有ID(“x”)生成密钥
S150
S151
使用秘密固有ID(“x”)生成密钥
S152
发送加密的内容

图34


桥接装置X的处理内容
通信对象是桥接装置
否
S161
是
在ID检查中加密
一致的秘密固有信息
并向通信对象发送
S162
接收从桥接
装置Y来的代理
ID检查请求
S163
解密接收的
路径列表
S164
取得路径列表
S165
路径列表的大小检查
大小>N
S166
是
否
向通信对象
发送代理
ID检查请求
S168
向桥接装置Y发送
代理ID检查错误,
向通信对象发送
代理ID检查错误
S167
从桥接装置Y向通信
对象发送接收装置
B具有的秘密固有ID
S169