



(12)发明专利

(10)授权公告号 CN 104811920 B

(45)授权公告日 2018.09.11

(21)申请号 201510127800.4

(22)申请日 2009.09.28

(65)同一申请的已公布的文献号

申请公布号 CN 104811920 A

(43)申请公布日 2015.07.29

(30)优先权数据

2008-259997 2008.10.06 JP

(62)分案原申请数据

200980139671.3 2009.09.28

(73)专利权人 佳能株式会社

地址 日本东京都大田区下丸子3丁目30番2号

(72)发明人 后藤史英 坂井达彦

(74)专利代理机构 北京魏启学律师事务所

11398

代理人 魏启学

(51)Int.Cl.

H04W 8/00(2009.01)

H04W 12/04(2009.01)

H04W 12/06(2009.01)

H04W 28/18(2009.01)

H04W 68/00(2009.01)

H04W 72/00(2009.01)

H04W 84/18(2009.01)

H04W 84/20(2009.01)

(56)对比文件

CN 1606891 A,2005.04.13,

CN 1666558 A,2005.09.07,

WO 2006071650 A2,2006.07.06,

WO 2008093817 A1,2008.08.07,

US 20070197238 A1,2007.08.23,

WO 2008050622 A1,2008.05.02,

审查员 张芑

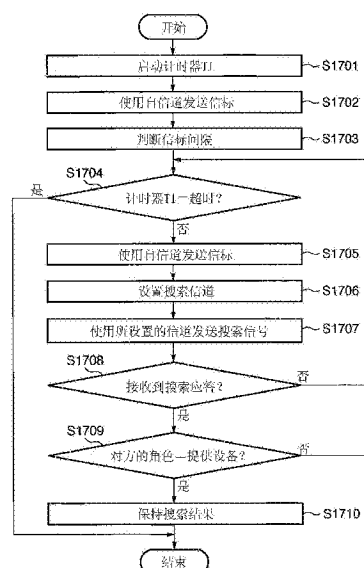
权利要求书3页 说明书20页 附图17页

(54)发明名称

通信设备和通信设备的控制方法

(57)摘要

本发明涉及一种能与通信网络连接的通信设备及该通信设备的控制方法,其中,使用分配给该通信设备的通信信道来通知该通信设备的存在,然后设置能在通信网络中使用的通信信道之中的不同于所分配的通信信道的一个通信信道,并且使用所设置的通信信道搜索用作用于提供通信参数的提供设备的通信对方设备。该通信设备重复地执行通知处理和搜索处理,并且每当执行一次或多次重复时,改变搜索处理中所使用的通信信道。



1. 一种通信设备,其特征在于,包括:
执行部件,用于执行共享通信参数的共享处理;
搜索部件,用于在包括第一通信信道和第二通信信道的多个信道中进行搜索,并且在结束所述第一通信信道的搜索的情况下,在与该第一通信信道不相邻的所述第二通信信道中搜索要执行所述共享处理的通信对方设备;以及
等待接收部件,用于进行等待接收来自通信对方设备的搜索信号的等待接收处理,
其中,所述等待接收部件所进行的所述等待接收处理的时间段的长度是可变的。
2. 根据权利要求1所述的通信设备,其特征在于,
所述等待接收部件使用由所述通信设备设定的规定通信信道进行所述等待接收处理,
所述通信设备在所述等待接收部件进行了所述等待接收处理之后,将动作从该等待接收处理切换为所述搜索部件的搜索。
3. 根据权利要求1所述的通信设备,其特征在于,
还具有显示部件,该显示部件在所述执行部件所进行的所述共享处理成功的情况下,显示表示所述共享处理成功的信息。
4. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,
还具有接收用于指示与通信对方设备之间形成网络的用户操作的部件,
在检测出所述用户操作之后通过所述搜索部件的搜索而检测出通信对方设备、或者由通信对方设备检测出所述通信设备的情况下,开始所述共享处理。
5. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,
还具有接收用于指示与通信对方设备之间形成网络的用户操作的部件,
根据检测出所述用户操作来开始所述搜索部件的搜索。
6. 根据权利要求1所述的通信设备,其特征在于,
还具有在上述通信设备与通信对方设备之间确定角色的确定部件,
在所述共享处理中,在由所述确定部件确定的角色为第一角色的情况下,将所述通信参数提供给所述通信对方设备。
7. 根据权利要求6所述的通信设备,其特征在于,
在所述共享处理中,在由所述确定部件确定的角色为第二角色的情况下,从所述通信对方设备接收所述通信参数。
8. 根据权利要求6或7所述的通信设备,其特征在于,
所述确定部件将从通信对方设备接收到的信息和与所述通信设备有关的信息进行比较,根据比较结果来确定角色。
9. 根据权利要求6或7所述的通信设备,其特征在于,
由所述通信设备发送的信息中包含表示由所述确定部件确定的角色的信息。
10. 根据权利要求1所述的通信设备,其特征在于,
所述搜索部件使用可使用的通信信道中的预定的通信信道搜索通信对方设备。
11. 根据权利要求1所述的通信设备,其特征在于,
在所述等待接收部件等待接收搜索信号的期间,所述搜索部件不进行搜索信号的发送。
12. 根据权利要求1所述的通信设备,其特征在于,

由所述通信设备发送的信息中包含表示能够执行所述共享处理的信息、或者表示正在执行所述共享处理的信息。

13. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述搜索部件搜索发送表示具有通信参数的自动设定处理功能、或者正在执行通信参数的自动设定处理的信息的通信对方设备。

14. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

还具有处理部件,该处理部件进行用于使其它通信对方设备加入在所述通信设备与所述通信对方设备之间构建的网络的处理。

15. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述第二通信信道是从所述第一通信信道错开三个信道得到的信道。

16. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述搜索部件通过一个通信信道在通信网络上发送搜索信号,通过该一个通信信道从其它通信设备接收搜索应答信号,由此进行通信对方设备的搜索。

17. 根据权利要求16所述的通信设备,其特征在于,

所述搜索部件还具备判断部件,该判断部件根据接收到的所述搜索应答信号,判断发送了该搜索应答信号的通信对方设备是否是提供通信参数的提供设备。

18. 根据权利要求2所述的通信设备,其特征在于,

随机地确定由所述等待接收部件等待接收搜索信号的时间段的长度。

19. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

通过符合IEEE802.11系列的无线通信来进行所述搜索部件的搜索处理。

20. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述通信参数包含服务集标识符即SSID、加密方法、加密密钥、认证方法和认证密钥中的至少一个。

21. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述通信参数包含SSID、加密方法、加密密钥、认证方法和认证密钥。

22. 根据权利要求21所述的通信设备,其特征在于,

所述认证方法为WPA认证方法、WPA-PSK认证方法、WPA2认证方法以及WPA2-PS认证方法中的任一个。

23. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述通信参数是用于进行无线通信的参数。

24. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

所述通信参数是用于进行符合IEEE802.11标准系列的无线通信的参数。

25. 根据权利要求1至3中的任一项所述的通信设备,其特征在于,

在所述通信设备与执行了所述共享处理的通信对方设备之间执行四次握手。

26. 根据权利要求1所述的通信设备,其特征在于,

所述搜索部件通过发送探测请求和接收探测应答来搜索所述通信对方设备,在接收到作为搜索信号的探测请求的情况下,所述等待接收部件发送探测应答。

27. 一种通信设备的控制方法,其特征在于,包括以下步骤:

第一搜索步骤,在第一通信信道中搜索要执行共享通信参数的共享处理的通信对方设

备；

第二搜索步骤，在结束所述第一搜索步骤中的所述第一通信信道的搜索的情况下，在与该第一通信信道不相邻的第二通信信道中搜索要执行所述共享处理的通信对方设备；

执行步骤，与在所述第一搜索步骤或所述第二搜索步骤中检测出的通信对方设备之间执行所述共享处理；以及

等待接收步骤，进行等待接收来自通信对方设备的搜索信号的等待接收处理，其中，所述等待接收步骤中的所述等待接收处理的时间段的长度是可变的。

通信设备和通信设备的控制方法

[0001] 本申请是申请日为2009年09月28日、国家申请号为200980139671.3、发明名称为“通信设备和通信设备的控制方法”的PCT申请(国际申请号为PCT/JP2009/067283)的分案申请。

技术领域

[0002] 本发明涉及一种通信设备和通信设备的控制方法。

背景技术

[0003] 在以符合IEEE802.11标准系列的无线LAN为代表的无线通信中,在使用之前必须设置许多设置项。例如,这些设置项包括诸如作为网络标识符的SSID、加密方法、加密密钥、认证方法和认证密钥等的进行无线通信所需的通信参数,并且手动输入这些参数对于用户来说非常不便。

[0004] 因此,不同厂家提出了允许用户在无线设备中容易地设置通信参数的自动设置方法。利用这些自动设置方法,一个设备使用在要连接的设备之间所预先确定的程序和消息来向其它设备提供通信参数,从而自动设置通信参数。

[0005] 日本特开2006-311139号公报(以下称为专利文献1)公开了无线LAN自组织(ad hoc)模式的通信(以下称为自组织通信)中的自动通信参数设置处理的例子。Wi-Fi CERTIFIED for Wi-Fi Protected Setup:Easing the User Experience for Home and Small Office Wi-Fi Networks,<http://www.wi-fi.org/wp/wifi-protected-setup>(以下称为非专利文献1)公开了“Wi-Fi保护设置”(Wi-Fi Protected Setup,以下缩写为WPS)作为接入点(基站)和站(终端站)之间的自动通信参数设置处理的行业标准规范。另外,基于IEEE P802.11i标准的Wi-Fi保护访问增强安全实现(以下称为非专利文献2)公开了“Wi-Fi保护访问”(Wi-Fi Protected Access,以下缩写为WPA)作为无线通信连接处理中的加密方法、加密密钥、认证方法和认证密钥等的行业标准规范。

[0006] 对于WPS,由于预先确定了用于提供通信参数的设备(以下称为提供设备)和用于接收通信参数的设备(以下称为接收设备)的角色,因而还唯一确定了通信参数的传送方向。

[0007] 然而,当没有预先确定提供设备和接收设备的角色时,不能唯一确定通信参数的传送方向。在这种情况下,当用户选择作为提供设备要使用的设备和作为接收设备要使用的设备时,用户的可操作性降低。

[0008] 此外,当选择多个设备作为提供设备时,接收设备不能区分要向其接收通信参数的提供设备。

[0009] 在向多个设备之间已建立的网络添加新设备时,也可能发生上述问题。在这种情况下,希望已是该网络的加入者的设备用作提供设备、并且作为预期加入者的新设备接收该网络的通信参数。然而,由于未预先确定提供设备和接收设备的角色,因而在作为预期加入者的新设备中不能设置适当的通信参数。

[0010] 不仅在无线通信的通信参数中可能发生上述问题,而且在需要设备间的通信设置的有线通信的通信参数中也可能发生上述问题。

发明内容

[0011] 本发明的一个实施例提供一种通信设备及其控制方法,其中,即使当在自动通信参数设置处理中没有预先确定角色,该通信设备也可以在不降低用户可操作性的情况下,设置适当的通信参数。

[0012] 根据本发明的一个方面,提供一种能与通信网络连接的通信设备,该通信设备包括:通知部件,用于使用分配给所述通信设备的通信信道来通知所述通信设备的存在;搜索部件,用于设置能在所述通信网络中使用的通信信道之中的不同于所分配的通信信道的一个通信信道,并且使用所设置的通信信道来搜索用作用于提供通信参数的提供设备的通信对方设备;以及控制部件,用于控制所述通知部件和所述搜索部件以交替地重复通知处理和搜索处理,并且每当执行一次或多次所述重复时,改变所述搜索部件所使用的通信信道。

[0013] 根据本发明的另一方面,提供一种能与通信网络连接的通信设备,该通信设备包括:通知部件,用于响应于自动通信参数设置处理的开始指示,使用能在所述通信网络中使用的通信信道之中的预定通信信道来通知所述通信设备的存在;搜索部件,用于使用所述预定通信信道来搜索用作用于提供通信参数的提供设备的通信对方设备;设置部件,用于与所述搜索部件所发现的通信对方设备执行所述自动通信参数设置处理;以及恢复部件,用于在完成所述自动通信参数设置处理之后,将通信信道恢复成开始所述自动通信参数设置处理之前的通信信道。

[0014] 根据本发明的另一方面,提供一种能与通信网络连接的通信设备的控制方法,该控制方法包括:通知步骤,用于使用分配给所述通信设备的通信信道来通知所述通信设备的存在;搜索步骤,用于设置能在所述通信网络中使用的通信信道之中的不同于所分配的通信信道的一个通信信道,并且使用所设置的通信信道来搜索用作用于提供通信参数的提供设备的通信对方设备;以及控制步骤,用于控制所述通知步骤和所述搜索步骤以交替地重复通知处理和搜索处理,并且每当执行一次或多次所述重复时,改变所述搜索步骤中所使用的通信信道。

[0015] 根据本发明的另一方面,提供一种能与通信网络连接的通信设备的控制方法,该控制方法包括:通知步骤,用于响应于自动通信参数设置处理的开始指示,使用能在所述通信网络中使用的通信信道之中的预定通信信道来通知所述通信设备的存在;搜索步骤,用于使用所述预定通信信道来搜索用作用于提供通信参数的提供设备的通信对方设备;设置步骤,用于与在所述搜索步骤中所发现的通信对方设备执行所述自动通信参数设置处理;以及恢复步骤,用于在完成所述自动通信参数设置处理之后,将通信信道恢复成开始所述自动通信参数设置处理之前的通信信道。

[0016] 通过以下参考附图对典型实施例的说明,本发明的其它特征将变得明显。

附图说明

[0017] 图1是示出根据本发明实施例的通信设备的结构的框图;

[0018] 图2是示出根据本发明实施例的设备的软件功能的框图;

- [0019] 图3是示出根据本发明实施例的第一网络结构的图；
- [0020] 图4是示出根据本发明实施例的设备A和B的操作的序列图；
- [0021] 图5是示出根据本发明实施例的第二网络结构的图；
- [0022] 图6是示出根据本发明实施例的提供设备的通知处理操作的流程图；
- [0023] 图7是示出根据本发明实施例的代理应答操作的流程图；
- [0024] 图8是示出根据本发明实施例的通信参数自动设置操作的流程图；
- [0025] 图9是示出根据本发明实施例的设备A、B和C的操作的序列图；
- [0026] 图10是支持的认证和加密方法的表；
- [0027] 图11是密钥交换算法中拥有的密钥和密钥交换序列的对照表；
- [0028] 图12是密钥交换处理的序列图(编号1)；
- [0029] 图13是密钥交换处理的序列图(编号2)；
- [0030] 图14是密钥交换处理的序列图(编号3)；
- [0031] 图15是密钥交换处理的序列图(编号4)；
- [0032] 图16是示出密钥交换算法选择算法的流程图；
- [0033] 图17是示出根据本发明第一实施例的提供设备发现处理操作的流程图；
- [0034] 图18是示出根据本发明第二实施例的提供设备发现处理操作的流程图；
- [0035] 图19是示出一般提供设备发现处理操作的时序图；以及
- [0036] 图20是示出根据本发明的提供设备发现处理操作的时序图。

具体实施方式

[0037] 第一实施例

[0038] 下面参考附图详细说明根据本实施例的通信设备。以下说明使用符合IEEE802.11系列的无线LAN系统的例子,但是通信模式不一定限于符合IEEE802.11的无线LAN。

[0039] 下面说明适于本实施例的事例的硬件结构。

[0040] 图1是示出根据本发明的实施例的能与通信网络连接的通信设备(提供设备或接收设备)的结构的例子的框图。附图标记101表示整个设备。附图标记102表示通过执行存储在存储单元103中的计算机程序而控制整个设备的控制单元。控制单元102还执行与其它设备的通信参数设置控制。附图标记103表示存储要由控制单元102执行的计算机程序和诸如通信参数等的各种类型的信息的存储单元。当控制单元102执行存储在存储单元103中的计算机程序时,实现后面所述的各种操作。

[0041] 附图标记104表示进行无线通信所使用的无线单元。附图标记105表示显示单元,其中,显示单元105进行各种显示,并具有如LCD或LED那样可输出在视觉上可感知的信息或者如扬声器那样可输出可听信息的功能。

[0042] 附图标记106表示给出用于开始通信参数设置处理的触发的设置按钮。控制单元102在检测到用户对设置按钮106的操作时执行后面所述的处理。

[0043] 附图标记107表示天线控制单元,并且附图标记108表示天线。附图标记109表示允许用户进行各种输入的输入单元。

[0044] 图2是示出在后面所述的通信参数设置操作中要由下面所述的各个设备执行的软件功能块的结构的例子的框图。

[0045] 附图标记201表示整个设备。附图标记202表示通信参数自动设置功能块。在本实施例中,通信参数自动设置功能块202自动设置诸如作为网络标识符的SSID、加密方法、加密密钥、认证方法和认证密钥等的进行无线通信所需的通信参数。

[0046] 附图标记203表示接收与各种通信相关联的包的包接收单元。包接收单元203接收信标(通知信号)。附图标记204表示发送与各种通信相关联的包的包发送单元。包发送单元204发送信标。注意,信标附加有发送源设备的各种类型的信息(自信息)。

[0047] 附图标记205表示控制诸如探测请求等的设备搜索信号的发送的搜索信号发送单元。注意,探测请求还可以被表示为搜索想要的网络所使用的网络搜索信号。搜索信号发送单元205发送探测请求。搜索信号发送单元205还发送作为所接收到的探测请求的应答信号的探测响应。

[0048] 附图标记206表示控制从其它设备接收诸如探测请求等的设备搜索信号的搜索信号接收单元。搜索信号接收单元206接收探测请求。另外,搜索信号接收单元206接收探测响应。注意,设备搜索信号和其应答信号附加有发送源设备的各种类型的信息(自信息)。

[0049] 附图标记207表示控制网络连接的网路控制单元。网路控制单元207执行例如与无线LAN自组织网络的连接处理。

[0050] 在通信参数自动设置功能块中,附图标记208表示控制自动通信参数设置处理中的各种协议的自动设置控制单元。

[0051] 附图标记209表示向对方设备提供通信参数的通信参数提供单元。通信参数提供单元209在自动设置控制单元208的控制下,执行自动通信参数设置处理(后面说明)中的提供处理。附图标记210表示从对方设备接收通信参数的通信参数接收单元。通信参数接收单元210在自动设置控制单元208的控制下,执行自动通信参数设置处理(后面说明)中的接收处理。

[0052] 自动设置控制单元208还判断自开始自动通信参数设置处理之后所经过的时间段是否超过设置处理的限制时间。当判断为经过的时间段超过限制时间时,在自动设置控制单元208的控制下中止设置处理。

[0053] 附图标记211表示判断在自动通信参数设置处理中的角色的角色判断单元。角色判断单元211执行后面所述的角色判断处理。

[0054] 附图标记212表示控制与自动通信参数设置处理的开始和完成通知相关联的设置的设置通知控制单元。设置通知控制单元212执行后面所述的提供设备中的开始通知消息、开始通知应答消息和完成通知消息的发送/接收处理。

[0055] 附图标记213表示控制信标(通知信号)的发送定时的信标控制单元。下面说明IEEE802.11无线LAN的自组织网络中的信标发送算法。

[0056] 在自组织网络下,在构成该网络的所有设备间以自主分布方式发送信标。由最初创建自组织网络的设备确定信标发送间隔(信标周期),并且通常以约100ms的间隔从任意设备发送信标。注意,当任意一个设备开始发送信标时,形成自组织网络。

[0057] 通过被称为竞争窗口(随机数生成范围,以下被缩写为CW)的参数来控制信标发送定时。当到达信标发送定时时,网络中的各设备计算从0到CW的范围内的随机值(CWrand)。将通过该CWrand乘以预定恒定间隔(时隙时间)所获得的时间段设置为信标发送之前的等待时间段(延后时间段)。

[0058] 由于信标发送之前的等待时间段按照时隙时间而减小,因而当等待时间段达到0时,发送信标。如果设备在发送信标之前从其它设备接收到信标,则该设备中止信标的发送处理。

[0059] 利用该控制,可以避免从各个设备所发送的信标的冲突。由于自组织网络上的各个设备在从0到CW的范围内选择随机数,因而构成该网络的设备中的选择最小CWrand的设备发送信标。

[0060] 例如,当在各个设备中设置相同CW作为初始值时,各个设备具有相等的信标发送概率,作为结果,各个设备每单位时间发送信标的次数变得几乎相同。换句话说,各个设备的信标发送频率(发送比)变得相同。

[0061] 另一方面,当网络上的一个设备将CW设置成小于初始值的值时,该设备发送信标的概率变得高于其它设备。也就是说,可以将CW表示为用于确定发送信标的概率或每单位时间发送信标的次数所使用的参数。

[0062] 另外,可以将CW表示为用于确定各设备所发送的信标的发送比所使用的参数。此外,还可以将CW表示为用于确定信标发送定时或信标发送之前的等待时间段所使用的参数。

[0063] 注意,CW值可以在从CWmin(最小值)到CWmax(最大值)的范围内改变。在设置CWmin时,使每单位时间发送信标的次数最大化。在各设备中,将CWinit(>CWmin)设置为初始值,并且在不执行自动通信参数设置处理时,使用该初始值来发送信标。

[0064] 图3是示出通信设备A 300(以下称为设备A)和通信设备B301(以下称为设备B)的图。所有这些设备均具有以上图1和2所示的结构。

[0065] 在没有确定设备A或设备B是用作通信参数提供设备还是接收设备的状态下,这两个设备分别创建网络A 302(以下称为网络A)和网络B 303(以下称为网络B)。

[0066] 设备A和B相互发现,并且判断哪一设备用作提供设备。结果,用作提供设备的设备向用作接收设备的设备提供通信参数。

[0067] 网络A和B是分别由设备A和B所创建的自组织网络。自组织网络被称为IBSS(独立基本服务集),并且使用BSSID作为网络标识符来区分各个网络。BSSID是采用由创建网络的设备所生成的随机值的网络标识符。注意,SSID是在设备可预先设置的网络标识符或者可被用户设置为任意值的网络标识符,并且不同于BSSID。通过上述说明可知,BSSID不是通过自动通信参数设置处理从提供设备提供给接收设备的通信参数。

[0068] 图4是示出在设备A和B上按下设置按钮106时的处理序列的例子的图,并且在设备A和B之间执行自动通信参数设置处理。

[0069] 当在设备A和B上分别按下设置按钮106时,设备A创建唯一网络A(F401),并且设备B也创建唯一网络B(F402)。假定较早按下设备B的设置按钮106,并且设备B首先创建网络。

[0070] 将设备A和B中的每一个设置为“候选提供设备”,这表示它们的工作角色(以下称为角色)既未被确定为提供设备也未被确定为接收设备(F403、F404),并且作为确定工作角色之前的限制时间而启动计时器T1(F405、F406)。

[0071] 设备A和B发送信标(通知信号)(F407、F408)。信标信号包括用于通知设备在所创建的网络中具有自动通信参数设置处理功能或者正在进行自动设置处理的信息元素。另外,信标还可以包括表示作为当前角色的“候选提供设备”的信息元素。

[0072] 由于这些信标包括与网络A和B相对应的不同的BSSID,因而接收到信标的设备可以识别该信标的发送源设备所属的网络。

[0073] 随后,设备B发送搜索信号A(F409)。搜索信号A还包括表示该设备具有自动通信参数设置处理功能或正在进行自动设置处理的信息元素、以及表示作为当前角色的“候选提供设备”的信息元素,如在信标中一样。

[0074] 在接收到从设备B发送的搜索信号A时,设备A向设备B发送搜索应答信号A(F410)。搜索应答信号A还包括表示该设备具有自动通信参数设置处理功能或正在进行自动设置处理的信息元素、以及表示作为当前角色的“候选提供设备”的信息元素,如在信标和搜索信号A中一样。

[0075] 当设备B的计时器T1在未检测到提供设备之前达到超时(F411),设备B设置“提供设备”作为其工作角色(F412)。

[0076] 这次,设备A发送搜索信号A(F413)。从设备A所发送的搜索信号A也包括表示该设备具有自动通信参数设置处理功能或正在进行自动设置处理的信息元素、以及表示作为当前角色的“候选提供设备”的信息元素。

[0077] 在接收到从设备A所发送的搜索信号A时,设备B向设备A发送搜索应答信号B(F414)。搜索应答信号B包括表示该设备具有自动通信参数设置处理功能或正在进行自动设置处理的信息元素、以及当前角色,如在信标和搜索信号A中一样。此时,由于设备B确定“提供设备”作为其工作角色,因而搜索应答信号B包括表示“提供设备”的信息元素。除表示作为角色的“提供设备”的信息元素以外,还可以添加表示该设备准备提供通信参数就绪的信息元素。

[0078] 设备A接收到从设备B所发送的搜索应答信号B,并且确认设备B的角色为“提供设备”、并且设备B准备提供通信参数就绪。因此,设备A停止计时器T1(F415),设置“接收设备”作为其角色(F416),并且加入由设备B所创建的网络B(F417)。然后,设备A和B可以交换在通信参数自动设置协议处理中要交换的通信消息(协议消息)。

[0079] 注意,自动设置协议处理意为交换预先设置的各种通信消息以从提供设备向接收设备提供通信参数的处理。注意,WPS将该协议处理称为“注册协议”(参考非专利文献1)。在本实施例的以下说明中,为了简化,接收设备向提供设备发送通信参数设置启动消息,并且提供设备响应于该消息执行向接收设备的通信参数提供处理。然后,在完成通信参数提供处理时,提供设备发送通信参数设置完成消息。

[0080] 当设备A在F417加入网络B时,由于在设备A中未设置诸如加密密钥和认证密钥等的通信参数,因而设备A和B不能进行使用加密和认证的通信。

[0081] 注意,在设备A和B之间确定通信参数提供设备或接收设备的角色时,使用搜索信号和搜索应答信号。

[0082] 然而,代替交换搜索信号和搜索应答信号,可以使用相互交换的信标的信息来确定角色。

[0083] 当设备A加入由设备B创建的网络时,设备A向设备B发送通信参数设置启动消息(F418),并且作为提供设备的设备B执行向作为接收设备的设备A的通信参数提供处理(F419)。在完成通信参数提供处理时,设备B向设备A发送通信参数设置完成消息(F420)。然后,完成通信参数设置处理,并且在设备A和B之间共享通信参数。

[0084] 然后,设备A和B使用共享的通信参数执行通信连接处理(F421)。

[0085] 注意,由于在结束通信参数设置处理的同时开始通信连接处理,因而设备A和B可以在不强迫用户进行任何操作的情况下相互通信。在这种情况下,设备可以发送明确表示开始通信连接处理的连接请求信号。在自组织模式下,尽管与基础架构模式不同,不执行关联处理,但是在接收到连接请求信号时,可以快速识别作为连接的请求源的设备。

[0086] 在本实施例中,设备B向设备A发送网络B的通信参数,并且使用这些通信参数执行通信连接处理。在这种情况下,当设备A向设备B发送连接请求信号时,设备B可以检测到设备A加入网络B,并且还可以容易地获得加入者的数量。

[0087] 在开始通信连接处理之前,设备可以确认用户是否开始连接,并且可以根据用户操作开始通信连接处理。例如,在完成通信参数设置处理时,显示单元105可以显示提示用户选择是否开始连接的消息,并且可以根据来自输入单元109的用户输入开始通信连接处理。

[0088] 设备B可以向设备A发送表示不同于网络B的网络的通信参数。例如,设备B可以向设备A提供使用网络C进行通信所需的通信参数,并且设备A和B可以在该提供处理之后使用网络C相互通信。在这种情况下,设备A或B可以响应于检测到网络C上的其它设备作为触发,开始通信连接处理。

[0089] 图8是示出在设备A和B上按下设置按钮106、确定了设备A和B的工作角色即提供设备和接收设备、然后执行自动通信参数设置处理时所执行的操作序列的例子的流程图。

[0090] 下面参考该流程图说明通过这两个设备所执行的控制。

[0091] 按下设置按钮106以表示开始通信参数设置处理(S801)。

[0092] 设置按钮106被按下了的设备检查自身当前是否已是网络的加入者(S802)。当设备使用通过与其它设备已进行的通信参数设置处理所共享的通信参数构成网络时,该设备是该网络的加入者。如果设备已是网络的加入者,则该设备设置“提供设备”作为其角色,以控制其它新设备加入正加入的网络(S815)。设备然后开始发送包括例如表示角色为“提供设备”的信息的信标(S816)。

[0093] 此后,在从作为网络的预期加入者的新设备接收到通信参数设置启动消息时,设备开始通信参数提供处理(S817)。也就是说,在步骤S817所开始的通信参数提供处理中,当设备已是网络的加入者时,该设备提供自身作为加入者的网络的通信参数。注意,当设备当前已是网络的加入者时,该设备启动图6所示的开始通知处理(后面说明)。假定信标(通知信号)、搜索信号(探测请求)和搜索应答信号(探测响应)包括以下信息元素作为依赖于信号的必须元素或选项:

[0094] • 通知设备具有自动通信参数设置处理功能或正在进行自动设置处理的信息元素;

[0095] • 表示设备的角色的信息元素;以及

[0096] • 表示提供功能是否是活动的信息元素。

[0097] 如果在步骤S802判断为设备没有加入任何网络,则该设备自身创建网络以确定工作角色(S803),设置“候选提供设备”作为角色(S804),并且启动后面所述的提供设备发现处理(S805)。注意,设备在步骤S803利用任意无线LAN信道创建网络。注意,无线LAN信道是在无线LAN的通信中授权使用的通信信道(频道)。例如,在符合IEEE802.11g的无线LAN的情

况下,在日本可使用从1ch到13ch的通信信道。后面将参考图17、19和20说明步骤S805的提供设备发现处理。

[0098] 作为提供设备发现处理的结果,如果发现了以“提供设备”作为其角色的设备(S806),该设备设置“接收设备”作为其角色(S807),并且加入由该提供设备所创建的网络(S808)。在该设备加入该网络后,该设备开始发送包括表示角色是“接收设备”的信息的信标(S809)。注意,由于该设备此时没有接收到从提供设备所提供的任何通信参数,因而不能在其已成为加入者的网络中进行使用加密和认证的通信。已成为该网络的加入者的设备向提供设备发送通信参数设置启动消息以请求提供通信参数,并且开始来自提供设备的通信参数的接收处理(S810)。

[0099] 另一方面,如果作为提供设备发现处理的结果,未能发现以“提供设备”作为其角色的设备(S806),则该设备设置“提供设备”作为其角色(S815)。然后,该设备开始发送包括表示角色是“提供设备”的信息的信标(S816),并且在接收到来自接收设备的通信参数设置启动消息时,开始通信参数提供处理(S817)。在步骤S817开始的通信参数提供处理中,如果该设备不是任何网络的加入者,则该设备提供在步骤S803所创建的网络的通信参数。

[0100] 另一方面,角色是“接收设备”且已开始来自提供设备的通信参数的接收处理的设备确认是否完成通信参数的接收处理(S811)。如果完成了通信参数的接收处理,则该设备通过控制显示单元105在LCD上显示消息、使LED闪烁或发光、改变LED的颜色或者生成任意声音,来进行表示通信参数设置处理成功的显示以使得可被用户识别(S814),从而结束该处理(S822)。如果发生了错误(S812),则该设备通过类似地控制显示单元105在LCD上显示消息、使LED闪烁或发光、改变LED的颜色或者生成任意声音,来通知该错误以使得可被用户识别(S813),从而结束该处理(S822)。

[0101] 另一方面,角色是“提供设备”且已开始通信参数提供处理的设备确认是否完成通信参数提供处理(S818)。如果完成了通信参数提供处理,则该设备通过控制显示单元105在LCD上显示消息、使LED闪烁或发光、改变LED的颜色或者生成任意声音,来进行表示通信参数设置处理成功的显示以使得可被用户识别,从而结束该处理(S822)。如果发生了错误(S819),则该设备通过控制显示单元105在LCD上显示消息、使LED闪烁或发光、改变LED的颜色或者生成任意声音,来通知该错误以使得可被用户识别(S820),从而结束该处理(S822)。

[0102] 图17是示出在执行图8的步骤S805的提供设备发现处理时的操作序列的例子的流程图。下面参考该流程图说明提供设备发现处理的控制。

[0103] 当开始提供设备发现处理时,该设备启动计时器T1(S1701)。该设备利用用于创建网络的通信信道(以下称为自信道)发送信标(通知信号)(S1702)。为了确定自信道中信标的发送间隔和其它通信信道中搜索信号(探测信号)的发送间隔,该设备确定自信道的信标间隔(S1703)。在发送搜索信号之后(在后述的步骤S1707的处理之后),该设备等待,直到根据信标间隔所确定的下一信标发送定时为止。

[0104] 该设备判断计时器T1是否达到超时(S1704)。如果计时器T1仍未达到超时,则该设备利用自信道发送信标(通知信号)(S1705)。注意,可以根据信标间隔的持续时间或比该持续时间更长的随机持续时间来确定信标发送时间段。

[0105] 该设备设置搜索信道(S1706)。在设置搜索信道时,该设备执行例如下面的处理。在日本符合IEEE802.11g的无线LAN的情况下,可以使用从1ch到13ch的信道作为无线LAN信

道。在本实施例中,如下执行信道设置处理。也就是说,在第一次搜索信道设置处理中,设置1ch。此后,每当执行步骤S1706的处理,以1ch为增量增大信道编号直到13ch。然后,在设置13ch之后的步骤S1706的处理中,再次设置1ch。注意,在美国,由于可使用信道1ch~11ch,因而当如在日本一样从1ch开始依次执行该设置处理时,在设置11ch之后的下一步骤S1706中,再次设置1ch。

[0106] 除用于以一个信道为增量来改变信道的方法以外,还可以使用用于跳着改变信道的方法。因IEEE802.11g的无线电特性的缘故,由于无线电波向相邻信道泄漏,该泄漏虽然微弱,但可以接收到相邻信道的其中一个中所发送的搜索信号,并且可以返回应答信号。因此,在第一次信道设置处理中,设置2ch设置为搜索信道,并且可以搜索从1ch到3ch的带宽。也就是说,在以所设置的通信信道为中心的三个信道的带宽上搜索通信对方设备。同样,在第二次信道设置处理中,设置5ch以搜索从4ch到6ch的带宽。此后,在第三次处理中设置8ch,在第四次处理中设置11ch,并且在第五次处理中设置13ch。在第六次处理中,要设置的信道回到2ch。可以使用这一搜索信道设置方法。

[0107] 注意,代替上述连续设置顺序,信道选择可以采用随机设置顺序,或者可以使用同一信道多次执行搜索处理。此外,除上述方法以外,还可以利用预定方法对信道进行分组,并且可以针对各个组来执行搜索处理。

[0108] 如上所述,步骤S1706的搜索信道设置处理是根据预定算法改变要设置的信道的处理。

[0109] 返回对图17所示流程图的说明。该设备使用在步骤S1706所设置的搜索信道在通信网络上发送搜索信号(探测请求)(S1707)。在发送该搜索信号之后,该设备等待接收搜索应答,直到下一信标发送定时为止(S1708)。如果在到达下一信标发送定时时没有接收到搜索应答,则处理返回到步骤S1704,以判断计时器T1的剩余时间段。如果计时器仍未达到超时,则该设备再次使用自信道重复从信标发送开始的处理。

[0110] 如果在步骤S1708接收到搜索应答,则该设备确认所接收到的搜索应答信号的内容,以判断对方设备的角色是否是“通信参数提供设备”(S1709)。如果对方设备的角色是“通信参数提供设备”,则该设备保持该搜索结果(S1710),并且结束提供设备发现处理。如果作为步骤S1709的判断处理的结果,对方设备的角色不是“提供设备”,则处理返回到步骤S1704,以判断计时器T1的剩余时间段。如果计时器仍未达到超时,则该设备再次使用自信道重复从信标发送开始的处理。注意,如果在步骤S1704,计时器T1达到了超时,则判断为未检测到提供设备,从而结束提供设备发现处理。

[0111] 通过执行上述提供设备发现处理,可以交替执行使用自信道的信标发送和使用其它信道的搜索处理。

[0112] 下面参考图19和20说明用于在改变发送信标所使用的信道和发送搜索信号并等待接收搜索应答信号所使用的信道时执行提供设备发现处理的例子、以及该处理的效果。

[0113] 图19是示出不执行图17所示的处理、并且在使用自信道的信标发送之后依次改变信道时探测提供设备的例子的图。设备A仅在时间段(a)期间使用自信道发送信标。此后,设备A在改变所有信道时发送搜索信号并且等待接收搜索应答,直到在时间段(b)期间发现提供设备为止。

[0114] 另一方面,如设备A一样,设备B同样仅在时间段(d)期间使用自信道发送信标。此

后,设备B在改变所有信道时发送搜索信号并且等待接收搜索应答,直到在时间段(e)期间发现提供设备为止。

[0115] 假定在时间段(b')期间,设备A使用设备B形成网络的信道来发送搜索信号并等待接收搜索应答信号。在这种情况下,由于设备B在时间段(b')期间不使用自信道发送任何信标,因而设备B不能从设备A接收到搜索信号,并且不能返回任何搜索应答信号。

[0116] 同样,假定在时间段(e')期间,设备B使用设备A形成网络的信道来发送搜索信号并等待接收搜索应答信号。在这种情况下一样,由于设备A在时间段(e')期间不使用自信道发送任何信标,因而设备A不能从设备B接收到搜索信号,并且不能返回任何搜索应答信号。

[0117] 这样,当这两个设备执行提供设备发现处理时,自信道的信标通知时间段短,并且使用自信道通知信标之前的间隔长。因此,设备A不能检测到设备B,并且设备B不能检测到设备A。

[0118] 因此,通过执行本实施例中所述的提供设备发现处理,可以降低发生这一状况的概率。图20是示出在设备A和B执行图17所示的提供设备发现处理时的例子的图。设备A在时间段(a)期间使用自信道发送信标。此后,设备A在时间段(b)期间使用第一信道执行搜索处理。设备A然后再次使用自信道发送信标(c),并使用第二信道执行搜索处理(d)。这样,设备A交替执行使用自信道的信标发送以及使用其它信道的搜索信号发送和搜索应答信号接收等待处理。

[0119] 如设备A一样,设备B同样执行相同处理。利用该处理,例如,设备A使用设备B形成网络的信道来执行搜索处理的时间段(d)与设备B通知信标的时间段(o)重叠。结果,当设备B响应于从设备A发送的搜索信号返回搜索应答信号时,设备A可以检测到设备B。

[0120] 同样,设备B使用设备A形成网络的信道来执行搜索处理的时间段(r)与设备A通知信标的时间段(g)重叠。结果,当设备A响应于从设备B发送的搜索信号返回搜索应答信号时,设备B可以检测到设备A。

[0121] 如上所述,通过执行本实施例中所述的提供设备发现处理,可以增大检测到对方通信设备的概率。

[0122] 注意,图17说明了通过等待接收对探测请求的探测响应来搜索开始通信参数设置处理的提供设备的方法(主动扫描)。由于正在执行通信参数设置处理的提供设备发送附加意味着自动通信参数设置处理的附加信息的信标,因而接收设备可以使用用于等待接收所发送的信标预定时间段的方法(被动扫描)。

[0123] 步骤S1709说明了判断所接收到的搜索应答信号的信息元素中所包括的对方的角色是否是“提供设备”的方法。当接收到的搜索应答信号的信息元素中所包括的对方的角色是“候选提供设备”时,可以使用搜索应答信号中所包括的信息判断是否确定“提供设备”作为角色。更具体地,例如,发送搜索应答信号的设备发送用于存储在按下设置按钮106之后经过的时间段的搜索应答信号。接收到该搜索应答信号的设备将搜索应答信号中所存储的经过的时间段与在按下其自身的设置按钮106之后经过的时间段进行比较。作为比较的结果,如果早于发送搜索应答信号的设备地按下了接收到搜索应答信号的设备的设置按钮106,则接收到搜索应答信号的设备设置“提供设备”作为角色,并且处理进入步骤S816。

[0124] 另一方面,作为比较的结果,如果早于接收到搜索应答信号的设备地按下了发送搜索应答信号的设备的设置按钮106,则接收到搜索应答信号的设备向发送搜索应答信号

的设备发送通知信号,并且接收到通知信号的设备可以设置“提供设备”作为角色。

[0125] 如上所述,当搜索应答信号包括做出用户操作以发出通信参数设置处理的开始指示的时间,并且所发现的通信对方设备未被确定为提供设备时,可以参考该时间确定哪一设备是提供设备。当搜索应答信号中所包括的时间早于向接收到搜索应答信号的设备发出通信参数设置处理的开始指示的时间时,确定通信对方设备为提供设备。利用该处理,可以快速确定提供设备。注意,要比较的信息不局限于在按下按钮106之后经过的时间段。例如,可以比较设备的MAC地址,或者可以比较搜索应答信号中所包括的定时同步功能(TSF)值。

[0126] 下面说明使用自动通信参数设置处理向已存在的自组织网络添加新设备的情况。注意,已存在的自组织网络表示通过多个设备使用执行通信参数设置处理的设备之间共享的通信参数所构成的自组织网络。

[0127] 图5是示出第一通信设备A 500(以下称为设备A)、第二通信设备B 501(以下称为设备B)、第三通信设备C 503(以下称为设备C)和网络502的图。设备A、B和C具有图1和2所示的上述结构。

[0128] 下面说明在设备C将要加入由设备A和B所构成的网络502时操作设备B和C的设置按钮的情况。

[0129] 图6是用于说明提供设备的通知处理操作的流程图。当在图8的步骤S802,设备已是网络的加入者时,该设备开始图6所示的处理。

[0130] 当开始该处理时,提供设备的信标控制单元213增大提供设备每单位时间的信标发送频率(发送比、发送次数)(S601)。

[0131] 注意,IEEE802.11无线LAN的自组织网络规定返回探测响应的设备是紧挨在接收到探测请求之前发送信标的设备。

[0132] 然后,在步骤S601,提供设备将CW设置成小于初始值的值。利用该设置,提供设备每单位时间发送信标的次数变得大于作为网络加入者的其它设备。结果,在作为预期加入者的新设备的提供设备搜索处理中(图8的步骤S805),可以在短的时间段内检测到来自提供设备的探测响应。

[0133] 这样,由于提供设备的信标发送频率增大,因而当作为预期加入者的新设备搜索提供设备时,该新设备可以更大可能地从提供设备接收到探测响应。当作为预期加入者的新设备通过被动扫描来搜索提供设备时,该新设备可以更大可能地从提供设备接收到信标。

[0134] 结果,可以降低在作为预期加入者的新设备未能检测到提供设备时经过了通信参数设置处理的限制时间的概率。当作为预期加入者的新设备可以在短的时间段内检测到提供设备时,可以缩短在完成通信参数提供处理之前所需的时间段。

[0135] 此后,提供设备广播用于通知开始自动通信参数设置处理的开始通知消息(S602)。注意,提供设备可以向作为网络的加入者的各设备单播该开始通知消息。还可以将该开始通知消息表示为用于通知开始操作的设备B是提供设备的消息。

[0136] 提供设备等待,直到由于错误终止所启动的提供处理(S606),完成向接收设备的通信参数提供处理(S603),或者该提供设备从其它设备接收到错误通知或完成通知消息(S605、S608)为止。

[0137] 如果提供处理成功,也就是说,如果完成向接收设备的通信参数提供处理(S603),

则提供设备广播完成通知消息(S604)。注意,提供设备可以向作为网络的加入者的各设备单播该完成通知消息。

[0138] 如果提供设备在步骤S604发送完成通知消息或者从其它设备接收到完成通知消息(S605),则处理跳到步骤S609。

[0139] 如果提供处理失败(S606),则提供设备广播错误通知消息(S607)。注意,提供设备可以向作为网络加入者的各设备单播错误通知消息。

[0140] 如果提供设备在步骤S607发送错误通知消息或从其它设备接收到错误通知消息(S608),则处理进入步骤S609。

[0141] 在步骤S609,提供设备的信标控制单元213将CW重新设置为初始值,以恢复在步骤S601增大的信标发送频率(S609)。注意,将CW向初始值的重新设置定时没有特别限制,只要在开始提供处理之后重新设置CW即可。也就是说,可以紧挨在开始处理之后,在完成提供处理之后,或者在错误之后,重新设置CW。如果紧挨在开始该处理之后重新设置CW,则由于信标发送频率(发送次数)降低,因而可以有效降低信标发送所需的消耗功率。在由于错误终止提供处理、向接收设备提供通信参数、或者从其它设备接收到通知消息之前,重复发送在步骤S602发送的开始通知消息。

[0142] 图7是用于说明作为除提供设备以外的网络的加入者的设备(设备A)的代理应答处理操作的流程图。当设备A接收到开始通知消息时,开始图7所示的处理。

[0143] 在检测到接收到开始通知消息时,设备A的自动设置控制单元208启动用于判断是否经过了在步骤S702~S707所述的处理的限制时间的计时器(S701)。

[0144] 然后,自动设置控制单元208改变要发送的信标和搜索应答信号(探测响应)中所包括的信息的内容(S702)。在步骤S702,自动设置控制单元208向要发送的信标和搜索应答信号添加唯一识别提供设备(设备B)所使用的识别信息。作为识别信息,例如,存储提供设备的MAC地址信息。这样,即使当不是提供设备的设备A返回搜索应答信号时,作为搜索信号的发送源的设备可以检测到提供设备的存在。

[0145] 信标控制单元213将CW设置为大于初始值的值(S703)以降低信标发送频率(发送比)。

[0146] 因此,作为除提供设备以外的网络的加入者的设备每单位时间发送信标的次数小于提供设备。结果,在作为预期加入者的新设备的提供设备搜索处理中(图8的步骤S805),可以在短时间段内检测到来自提供设备的探测响应。

[0147] 此后,设备A等待从提供设备发送的完成通知消息或错误通知消息(S704、S705)。在接收到通知消息时,设备A的信标控制单元213将CW重新设置(恢复)成初始值,以恢复在步骤S703降低的信标发送频率(S706)。此外,自动设置控制单元208将要发送的信标和搜索应答信号中要包括的信息的内容恢复成步骤S702的改变之前的内容(S707)。也就是说,自动设置控制单元208去除用于唯一识别提供设备(设备B)并被附加给要发送的信标和搜索应答信号的识别信息。

[0148] 注意,如果在步骤S701所设置的计时器达到了超时,则接收设备中止步骤S702~S707的处理。如果在计时器超时定时已进行了步骤S702~S707的处理,则如步骤S706和S707一样,执行重新设置处理。

[0149] 图9是用于解释本实施例中各个设备的操作的序列图。设备A通过自动通信参数设

置处理接收到从设备B提供的通信参数,并且已成为由这些通信参数所定义的网络502的加入者(F901)。设备C仍未进行通信参数提供处理。

[0150] 当用户操作设备B的设置按钮时,设备B启动图8所示的处理(F902)。由于设备B使用通过自动通信参数设置处理与设备A所共享的通信参数,已是网络502的加入者,因而设备B设置“提供设备”作为角色,并且开始通信参数提供处理(F902)。

[0151] 设备B启动图6所示的开始通知处理(F903)。在启动开始通知处理之后,设备B发送开始通知消息,并且增大信标发送频率(F904)。

[0152] 接收到开始通知消息的设备A启动图7所示的代理应答处理,并且降低信标发送频率(F905)。

[0153] 这样,当设备B增大信标发送频率并且设备A降低信标发送频率时,作为新的预期加入者的设备C可以在更短时间段内检测到作为提供设备的设备B。

[0154] 当用户操作设备C的设置按钮106时,设备C启动图8所示的处理。由于设备C不是网络的加入者,因而设备C执行用于创建网络及设置“候选提供设备”作为其角色等的处理,并然后开始提供设备搜索处理。注意,图9示出搜索处理和随后的处理,而没有示出它们之前的处理。设备C发送搜索信号以检测提供设备(F906)。

[0155] 在网络502上,设备A或B响应于从设备C发送的搜索信号返回搜索应答信号(F907a、F907b)。

[0156] 当设备A返回搜索应答信号时,设备A返回用于存储作为提供设备的设备B的识别信息(MAC地址)的搜索应答信号(F907b)。当设备B返回搜索应答信号时,设备B返回用于存储表示其是提供设备的信息的搜索应答信号(F907a)。这样,即使当设备C接收到来自网络502上的任何设备的搜索应答信号时,设备C可以确保检测到作为提供设备的设备B。

[0157] 在检测到存在提供设备时,设备C设置“接收设备”作为其角色(F908)。然后,设备C加入网络502,并且从作为提供设备的设备B接收在网络502上进行通信所需的通信参数(F909)。

[0158] 在设备B向设备C提供通信参数之后,设备B向设备A发送完成通知消息(F910)。在发送完成通知消息之后,设备B恢复在F903增大的信标发送频率。在接收到完成通知消息时,设备A恢复在F905降低的信标发送频率。

[0159] 如上所述,用户可以通过仅操作设置按钮106来自动控制设备C来加入网络502。

[0160] 注意,图9说明了操作设备B的设置按钮106的情况。另外,可以假定操作设备A的设置按钮106的情况。即使当操作设备A的设置按钮106时,由于设备A经由图8的步骤S802变成提供设备,因而可以以与图9相同的方式将设备C添加到网络502。

[0161] 利用上述处理,通信设备可以容易地共享通信参数。如上所述,通过操作设备A和B的设置按钮106,在设备A和B之间执行通信连接处理以构成网络502。

[0162] 如上所述,可以在完成通信参数设置处理之后自动开始通信连接处理,或者可以响应于设置按钮106的再次按下操作或通过输入单元109所输入的连接命令来开始通信连接处理。

[0163] 注意,通信连接处理根据共享的通信参数的认证方法和加密方法而不同。

[0164] 在本实施例中,例如,作为认证方法和加密方法所采用的组合如图10所示。

[0165] 开放认证是被定义为IEEE802.11标准的“开放系统认证(Open System

Authentication)”的认证方法,并且详细情况请参考IEEE802.11标准。共享认证是被定义为IEEE802.11和IEEE802.11i标准的“共享密钥认证(Shared Key Authentication)”的认证方法,并且使用WEP协议作为加密方法。

[0166] 注意,“WEP”是“有线等效保密(Wired Equivalent Privacy)”的缩写,并且详细情况请参考IEEE802.11或IEEE802.11i标准。另外,WPA认证方法、WPA-PSK认证方法、WPA2认证方法和WPA2-PSK认证方法是Wi-Fi联盟所规定的认证方法的标准。这些方法基于IEEE802.11i标准中的RSNA(鲁棒安全网络关联(Robust Security Network Association))。

[0167] “TKIP”是“Temporal Key Integrity Protocol(临时密钥集成协议)”的缩写。另外,“CCMP”是“具有CBC-MAC协议的CRT(CTR with CBC-MAC Protocol)”的缩写,并且使用AES协议作为加密方法。“AES”是“高级加密标准(Advanced Encryption Standard)”的缩写。

[0168] 这些方法的详细情况请参考Wi-Fi联盟规范或测试规范。WPA-PSK和WPA2-PSK认证方法是使用预共享密钥的认证方法。WPA和WPA2认证方法需要利用单独准备的认证服务器的用户认证,并且从该认证服务器获取通信信道的加密密钥。这些方法的详细情况请参考IEEE802.11i标准。

[0169] 连接处理方法根据认证方法而不同。当前可支持的认证方法包括六种不同方法,即开放认证、共享认证、WPA认证、WPA-PSK认证、WPA2认证和WPA2-PSK认证,如该表所示。在这些方法中,WPA认证和WPA2认证以及WPA-PSK认证和WPA2-PSK认证在本质上是相同的认证方法。为此,将WPA和WPA2认证方法及WPA2和WPA2-PSK认证方法当作为相同方法,并且下面将介绍四种不同认证方法(开放、共享、WPA和WPA-PSK)。

[0170] 然而,由于WPA认证需要从外部设置的独立认证服务器,并且利用该认证服务器执行认证处理,因而当如本发明一样所有通信设备在相等的立场下工作时,需要复杂处理。因此,不给出对WPA认证的说明。

[0171] 在本实施例中,下面将分别说明开放认证、共享认证和WPA-PSK认证。

[0172] 首先说明开放认证。在开放认证中,通信设备设置通过自动通信参数设置处理所共享的通信参数,并且搜索相互的设备以构成IBSS网络。

[0173] 下面说明共享认证。由于IEEE802.11和IEEE802.11i规范包括对共享认证的详细说明,因而不给出该说明。在进行共享认证时,必须确定请求方和应答方。

[0174] 在基础架构模式下,STA(站)作为请求方而工作,并且AP(接入点)作为应答方而工作。另一方面,在自组织模式下,不存在AP。为此,为了实现在IBSS网络中的共享密钥认证,STA必须包括应答方功能和请求方/应答方角色判断算法。

[0175] 请求方/应答方角色判断算法可以采用与后面所述的WPA-PSK认证中的申请方/认证方角色判断算法的方法相同的方法。例如,在自动通信参数设置处理中,通信参数提供设备可以用作应答方,并且通信参数接收设备可用作请求方。

[0176] 最后,说明WPA-PSK认证。在IEEE802.11i和WPA中标准化WPA-PSK认证,并且还规定IBSS网络中的操作方法。图12说明IEEE802.11i中规定的序列。详细情况请参考IEEE802.11i标准,并且下面进行概略说明。

[0177] 假定存在完成自动通信参数设置处理的设备A和B。在完成自动通信参数设置处理

之后,自动使用自动设置的通信参数或者响应于用户操作,执行通信连接处理。

[0178] 设备A和B搜索相互的对方(F1201)。如果这些设备可以相互识别,则设备A和B中具有较大MAC地址的一个用作认证方,并且另一设备用作申请方。然后,设备A和B执行第一次四次握手处理(4-way handshake processing)和组密钥握手处理(group key handshake processing)(F1202和F1203)。

[0179] 注意,四次握手处理是如下的机制:在认证方和请求方之间交换随机数、并且针对每一会话基于预共享密钥生成被称为对偶密钥的单播包的加密密钥。组密钥握手处理是发送认证方所拥有的多播包或广播包的加密密钥的机制。

[0180] 此后,设备A和B交换认证方和申请方的角色,并且再次执行四次握手处理和组密钥握手处理(F1204和F1205)。利用以上处理,允许设备A和B进行加密通信。

[0181] 这样,在完全符合IEEE802.11i规范的方法的情况下,由于多次重复四次握手处理和组密钥握手处理,因而总体处理变得冗余。由于执行冗余处理和角色判断算法,因而在完成连接之前需要很长时间。因此,还可以使用用于减少冗余处理并缩短处理时间的方法。

[0182] 存在一些这样的方法,并且在这种情况下,说明下面的四种方法:

[0183] 第一种方法:将四次握手处理组合成一次;

[0184] 第二种方法:将组密钥组合成每一网络一个。

[0185] 第三种方法:将所有组密钥和对偶密钥组合成一个;以及

[0186] 第四种方法:在自动通信参数设置处理中一起执行密钥交换。

[0187] 图11示出上述四种方法的密钥交换序列的次数的不同以及拥有的对偶密钥和组密钥的数量。

[0188] 首先说明拥有的密钥的数量。当包括 n 个通信设备的自组织IBSS网络完全符合IEEE802.11i时,需要与其它的通信设备的数量一样多的 $n-1$ 个对偶密钥。对于组密钥,除与其它通信设备的数量一样多的组密钥以外,还总共需要两个组密钥,即该设备的当前组密钥和紧挨着的前一组密钥。因此,总共需要 $n+1$ 个组密钥。需要设备的两个组密钥的原因是:根据组密钥握手进度状况,在过渡时间段在同一网络中存在具有不同组密钥的设备。

[0189] 在第一种方法中,仅减少序列的数量,并且拥有的密钥的数量保持不变。

[0190] 在第二种方法中,类似地需要 $n-1$ 个对偶密钥,并且总共仅需要一个组密钥。

[0191] 在第三种方法中,由于完全不变地使用组密钥作为对偶密钥,因而对偶密钥的数量变成0,并且仅拥有一个组密钥。

[0192] 在第四种方法中,类似地需要 $n-1$ 个对偶密钥。由于各个设备可以拥有组密钥,或者总共拥有一个组密钥,因而基于情况可能需要 $n+1$ 个组密钥或仅一个组密钥。

[0193] 下面说明每一其它设备执行的密钥交换序列的数量。在完全符合IEEE802.11i的方法的情况下,如使用图12所述的一样,执行四次握手处理两次并且执行组密钥握手处理两次。

[0194] 在第一种方法中,将作为冗余处理执行四次握手处理的次数减少到1。仍执行组密钥握手处理两次。

[0195] 在第二种方法中,由于在网络中仅使用一个组合的组密钥,因而仅需要将该密钥发布给新终端。因此,执行组密钥握手处理一次。另外,根据第一种方法可以执行四次握手处理一次,或者根据IEEE802.11i标准以两种方式执行四次握手处理两次。

[0196] 在第三种方法中,由于使用预先设置的一个密钥作为对偶密钥和组密钥,因而不执行密钥交换序列。

[0197] 在第四种方法种,由于在WPS自动通信参数设置处理中进行相当于密钥交换处理的处理,因而不执行独立的四次握手处理。将组密钥握手处理执行任意次数。

[0198] 如参考图11所述一样,与完全符合IEEE802.11i标准的上述方法相比,这些方法在密钥交换序列的数量和拥有的密钥的数量方面具有优点。

[0199] 下面使用序列图详细说明上述四种方法。

[0200] 下面参考图13说明第一种方法。

[0201] 假定存在完成自动通信参数设置处理的设备A和B。在完成自动通信参数设置处理之后,自动使用自动设置的通信参数或者响应于用户操作,执行通信连接处理。

[0202] 设备A和B搜索相互的对方(F1301)。如果这些设备可以相互识别,并且设备A和B中具有较大MAC地址的一个用作认证方,并且另一设备用作申请方。然后,设备A和B执行四次握手处理和一个组密钥握手处理(F1302和F1303)。

[0203] 此后,设备A和B交换认证方和申请方的角色,并且再次执行组密钥握手处理(F1304)。利用上述处理,允许进行通信。

[0204] 如上所述,利用第一种方法,将IEEE802.11i规范中每一设备对两次执行的四次握手处理的次数减少成1。

[0205] 由于需要四次握手处理在执行四次握手处理的通信设备之间来共享对偶密钥,因而,如果连续执行该处理两次,则不能提高安全性,这导致冗余处理。因此,在第一种方法中,改变传统方法,将执行四次握手处理的次数减少成1,从而缩短正常连接处理所需的时间。

[0206] 下面参考图14说明第二种方法。假定存在完成自动通信参数设置处理的设备A和B。在完成自动通信参数设置处理之后,自动使用自动设置的通信参数或者响应于用户操作,执行通信连接处理。

[0207] 设备A和B搜索相互的对方(F1401)。如果这些设备可以相互识别,则设备A和B中具有较大MAC地址的一个用作认证方,并且另一设备用作申请方。然后,设备A和B执行四次握手处理和组密钥握手处理(F1402和F1403)。利用上述处理,允许进行通信。

[0208] 在IEEE802.11i规范中,对于各个通信设备设置不同的组密钥。然而,在第二种方法中,仅使用每一网络的一个组合的组密钥。

[0209] 对各个通信信道准备对偶密钥,但是每一网络一般使用一个组密钥。结果,在符合IEEE802.11i的方法中必须执行两次的组密钥握手处理可以仅需要执行一次。由于仅设置一个组密钥,因而由于对于发送广播包和多播包的各设备不必保持不同密钥,因而这类包的加密/解密处理变得简单。

[0210] 第三种方法与参考非专利文献2所述的WPA-None(可选IBSS全球预共享密钥系统)相同。

[0211] 由于上述文献详细说明了WPA-None,因而没有给出对其的详细说明。在正常WPA中,通过四次握手处理向作为对偶密钥的源的元素应用随机数以生成会话密钥。另一方面,在WPA-None中,完全不变地应用作为对偶密钥的源的元素作为会话密钥。

[0212] 也就是说,第三种方法的大的特性特征在于不执行密钥交换处理。因此,与针对每

一连接都生成会话密钥的正常WPA连接处理相比,安全性变低。因此,当采用该方法时,对每一连接都启动自动通信参数设置处理,并且对每一连接都随机生成共享的通信参数的通信密钥,从而提高安全性。

[0213] 下面参考图15说明第四种方法。如前面使用图4所述,执行自动通信参数设置处理中的通信对方搜索处理和角色判断处理(F1501)。随后,通过自动通信参数设置处理,将通信参数从通信参数提供设备传送给通信参数接收设备(F1502)。在F1502的处理期间,与通信参数设置处理同时执行在传统方法中不执行的密钥交换处理。

[0214] 在同时执行时,例如,还使用通信参数设置处理的消息交换处理中所使用的随机数作为密钥交换处理的随机数。因此,在结束F1502时的定时,设备A和B共享对偶密钥。在完成自动通信参数设置处理之后,执行组密钥交换处理(F1503)。如上所述,第四种方法的特征在于,在自动通信参数设置处理中,一起执行密钥交换处理。

[0215] 利用第四种方法,由于即使在同一网络中设备之间的对偶密钥也不同,因而可以提高安全性。由于在通信参数设置处理中执行相当于四次握手处理的处理,因而可以缩短总连接时间。

[0216] 在该说明中,单独执行组密钥交换处理。然而,当在通信参数设置处理中还执行组密钥交换处理时,可以进一步缩短总连接时间。

[0217] 对于包括符合IEEE802.11i的方法的上述5种方法,系统可以选择这些方法中的一个,并且可以提供表示通信参数中所包括的要使用的方法的信息。另外,可以根据自动通信参数设置处理的模式动态切换这些方法。

[0218] 下面参考图16说明根据自动通信参数设置处理的模式动态切换这些方法的情况。

[0219] 假定通过自动通信参数设置处理选择需要密钥交换处理的WPA-PSK或WPA2-PSK等作为通信参数。在这种情况下,判断为网络中已使用的密钥交换方法(S1601)。利用该判断处理,如果已选择了任意密钥交换方法(S1601-2为“是”),则完全不变地使用该方法。如果没有特别选择方法(S1601-2为“否”),则判断为自动通信参数设置处理模式。

[0220] 处理模式包括例如下面的模式:永久使用通过自动通信参数设置处理所设置的通信参数、或者使用通信参数作为临时会话信息。例如,在永久使用所设置的通信参数的处理模式(当在切断电源后再次进行无线通信时使用相同通信参数的模式)的情况下,选择确保高安全性的方法(例如,第一种方法或第四种方法)。在使用通信参数作为临时会话信息的模式(在切断电源时清除或使所设置的通信参数无效的模式)的情况下,可以选择使处理负荷优先于安全性的方法(例如,第二种方法或第三种方法)。

[0221] 如果基于处理模式没有确定要使用的密钥交换方法(步骤S1602-2为“否”),则判断同一网络中包括的通信设备的数量(S1603)。然后,基于通信设备的数量选择适当的密钥交换方法(S1604)。例如,在两个通信设备的情况下,选择完全符合IEEE802.11i的方法或者第一种或第四种方法。在三个或更多个通信设备的情况下,可以选择第二种或第三种方法。

[0222] 如上所述,根据本实施例,当操作作为网络的加入者的设备的设置按钮时,该设备用作提供设备并执行通信参数提供处理。为此,当用户在不管作为网络的加入者的设备是提供设备还是接收设备的情况下选择任意设备时,新设备都可以接收到所提供的通信参数。

[0223] 也就是说,在无需选择任何提供设备的情况下,通过操作任意设备的设置按钮,都

可以将新设备添加至网络。由于在完成提供处理之后恢复增大的信标发送频率,因而可以降低信标发送所需的消耗功率。注意,当紧挨在开始通信参数提供处理之后恢复信标发送频率时,可以更有效地降低信标发送所需的消耗功率。

[0224] 当在容易且安全地提供通信参数之后将新设备添加至网络时,增加了与密钥交换算法有关的选项,并且自动判断并设置密钥交换算法,因而降低了形成网络时的用户压力。另外,可以安全、容易且快速地形成网络。

[0225] 第二实施例

[0226] 在第一实施例中,在使用图17所述的提供设备发现处理中,设备交替执行利用其无线LAN信道的信标发送处理和利用其它无线LAN信道的提供设备发现处理。利用该处理,该设备和其它设备可以容易地检测到相互的设备。相反,第二实施例说明利用预定无线LAN信道执行提供设备发现处理的例子。

[0227] 图18是示出第二实施例中要执行的提供设备发现处理的操作序列的例子的流程图。

[0228] 下面参考该流程图说明提供设备发现处理的控制。

[0229] 设备响应于自动通信参数设置处理的开始指示(按下设置按钮106),开始使用图8所述的处理,并且开始步骤S805的提供设备发现处理。在开始提供设备发现处理之后,该设备启动计时器T1(S1801)。

[0230] 该设备将无线LAN信道从当前无线LAN信道改变成预定无线LAN信道(S1802)。注意,作为预定无线LAN信道,可以使用通信网络中可使用的通信信道中的预定的一个。作为预定无线LAN信道,可以使用通信网络中可使用的通信信道中在正常通信中不使用的通信信道。可以使用不同的通信信道作为正常通信所使用的通信信道和提供设备发现处理所使用的通信信道,从而可以在不影响其它设备之间的通信的情况下,执行提供设备发现处理。

[0231] 在改变无线LAN信道之后,该设备开始信标(通知信号)发送处理(S1803)。在开始信标发送处理之后,假定该设备使用基于IEEE802.11标准的信标间隔来执行信标发送控制,并且周期性保持发送信标信号。

[0232] 该设备判断计时器T1是否达到超时(S1804)。如果计时器T1仍未达到超时,则该设备发送搜索信号(探测请求)(S1805)。在发送搜索信号之后,该设备判断是否接收到搜索应答(S1806)。如果未接收到搜索应答,则处理返回到步骤S1804以判断计时器T1的剩余时间段。如果计时器仍未到达超时,则该设备再次重复从搜索信号发送开始的处理。

[0233] 如果在步骤S1806接收到搜索应答,则该设备确认所接收到的搜索应答信号的内容,以判断对方设备的角色是否是“通信参数提供设备”(S1807)。如果对方设备的角色是“通信参数提供设备”,则该设备保持该搜索结果(S1808),从而结束提供设备发现处理。

[0234] 作为步骤S1807的判断处理的结果,如果对方设备的角色不是“通信参数提供设备”,则处理返回到步骤S1804,以判断计时器T1的剩余时间段。如果计时器仍未达到超时,则该设备再次重复从搜索信号发送开始的处理。注意,如果在步骤S1804计时器T1达到了超时,则该设备判断为未检测到提供设备,从而结束提供设备发现处理。

[0235] 注意,使用预定通信信道执行通过步骤S810的通信参数接收处理和步骤S817的通信参数提供处理所执行的自动通信参数设置处理。因此,当处理从步骤S802进入步骤S815时,在步骤S815,将预定通信信道设置为通信信道。在通信参数提供处理成功或者被由于错

误而终止之后,将通信信道恢复成开始自动通信参数设置处理之前的通信信道。在本实施例中,例如,在步骤S820和S821恢复通信信道。另外,当由于错误而终止通信参数接收处理时,可以将通信信道恢复成开始自动通信参数设置处理之前的通信信道。在本实施例中,例如,可以在步骤S813恢复通信信道。

[0236] 如上所述,根据本实施例,由于利用预定无线LAN信道执行提供设备发现处理,因而可以非常快速地检测到提供设备。在自动通信参数设置处理期间可以中断通信连接处理。然而,由于提供设备发现处理快速结束,因而可以缩短通信连接处理的中断时间段。

[0237] 说明了本发明的优选实施例,但是它们是为了说明本发明的例子,并且本发明的范围不仅仅局限于这些实施例。在不脱离本发明的范围的情况下可以进行这些实施例的各种变形例。

[0238] 在以上实施例所述的例子中,改变CW值以将提供设备每单位时间发送信标的次数增大得大于其它设备。然而,可以使用其它参数,只要提供设备可以将发送信标的次数增大得大于其它设备。例如,如果可以改变信标发送间隔(信标周期),则提供设备减小信标发送间隔,从而增大每单位时间发送信标的次数。

[0239] 在上述说明中,将CW改变得大于或小于初始值。由于各个设备不一定具有相同的CW初始值,因而,如果在可改变的范围内将CW改变成最小值(CWmin)或者最大值(CWmax),则可以更可靠地改变信标发送频率(次数)。开始通知消息被描述为用于通知开始自动通信参数设置处理的消息。

[0240] 然而,还可以将开始通知消息表示为用于通知设置按钮106的操作的消息或者用于允许提供设备向其它接收设备提供通信参数的消息。

[0241] 以符合IEEE802.11的无线LAN作为例子给出了以上说明。然而,对于诸如无线USB、MBOA、**Bluetooth®**、UWB和ZigBee等的其它无线介质也可以执行本发明。另外,对于诸如有线LAN等的有线通信介质也可以执行本发明。

[0242] 注意,“MBOA”是“多频带OFDM联盟(Multi Band OFDM Alliance)”的缩写。另外,UWB包括无线USB、无线1394和WINET等。

[0243] 作为通信参数举例说明了网络标识符、加密方法、加密密钥、认证方法和认证密钥。然而,可以使用其它种类的信息,或者在上述通信参数中可包括其它种类的信息。

[0244] 如上所述,根据本发明,即使当在自动通信参数设置处理中没有预先确定角色时,可以在无需用户选择角色的情况下,适当执行通信参数设置处理和网络加入处理。

[0245] 其它实施例

[0246] 还可以利用读出并执行记录在存储器装置上的程序以进行上述实施例的功能的系统或设备的计算机(或者CPU或MPU等装置)和通过下面的方法实现本发明的方面,其中,利用系统或设备的计算机通过例如读出并执行记录在存储器装置上的程序以进行上述实施例的功能来进行上述方法的步骤。为此,例如,通过网络或者通过用作存储器装置的各种类型的记录介质(例如,计算机可读介质)将该程序提供给计算机。

[0247] 尽管参考典型实施例说明了本发明,但是应该理解,本发明不局限于所公开的典型实施例。所附权利要求书的范围符合最宽的解释,以包含所有这类修改、等同结构和功能。

[0248] 本申请要求2008年10月6日提交的日本2008-259997号专利申请的优先权,其全部

内容通过引用包含于此。

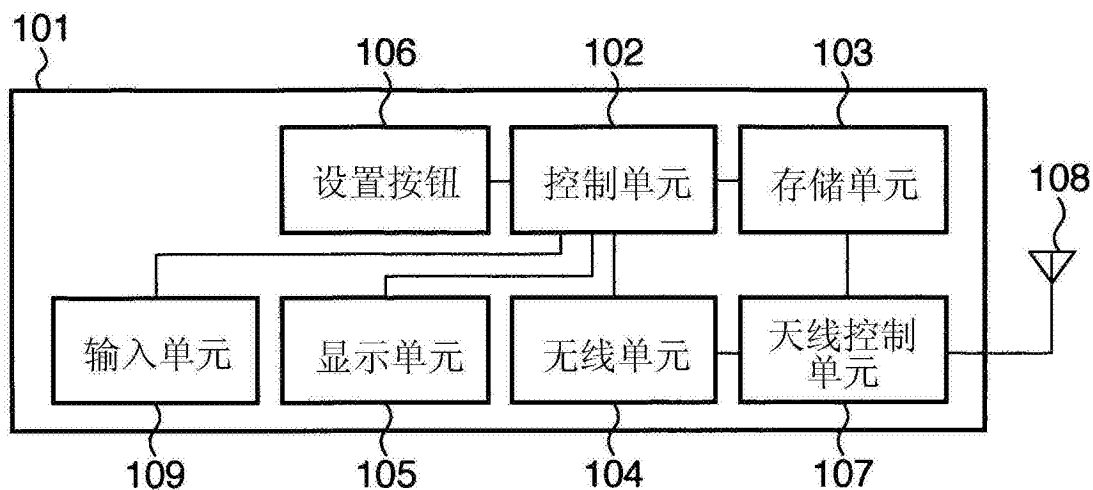


图1

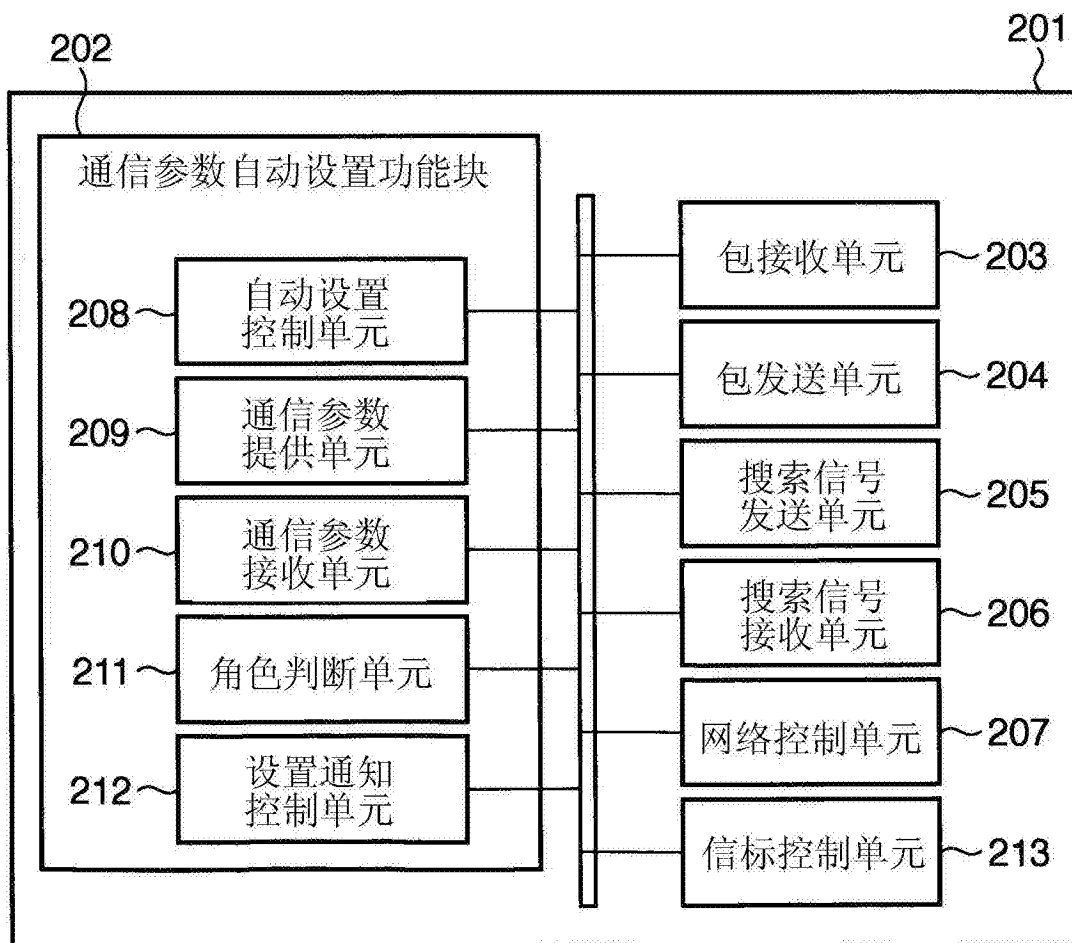


图2

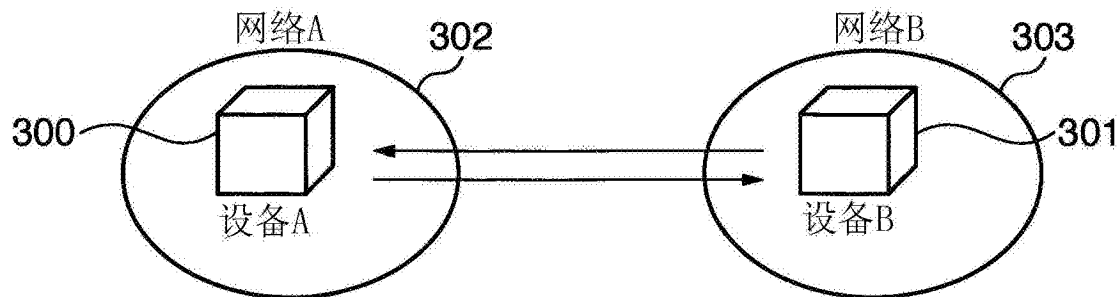


图3

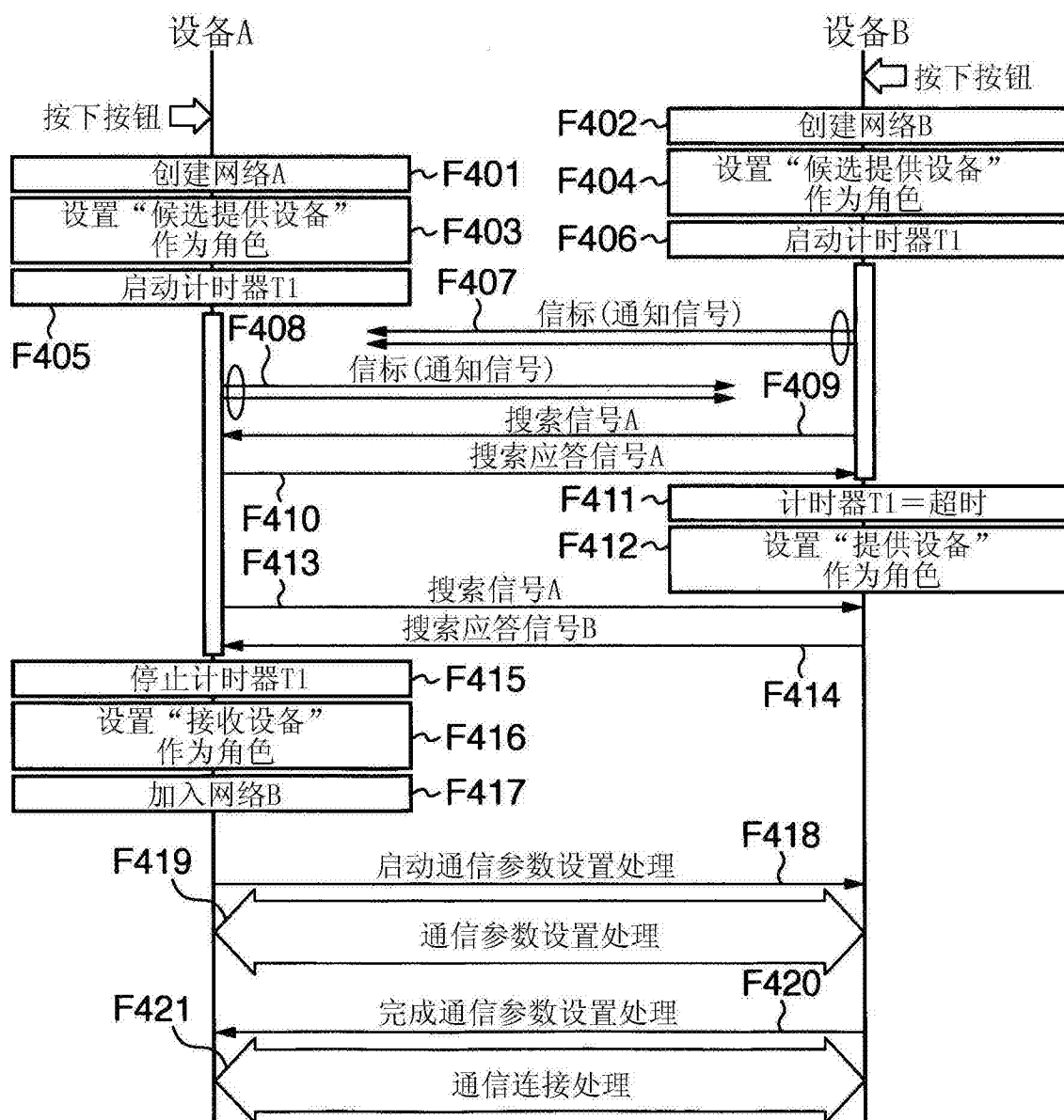


图4

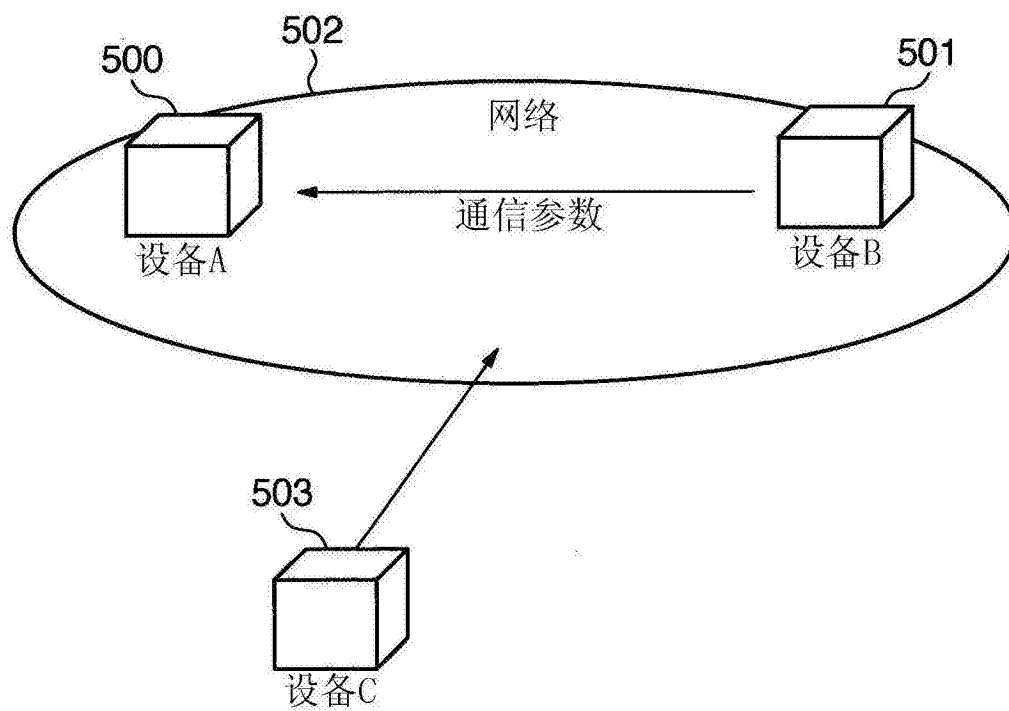


图5

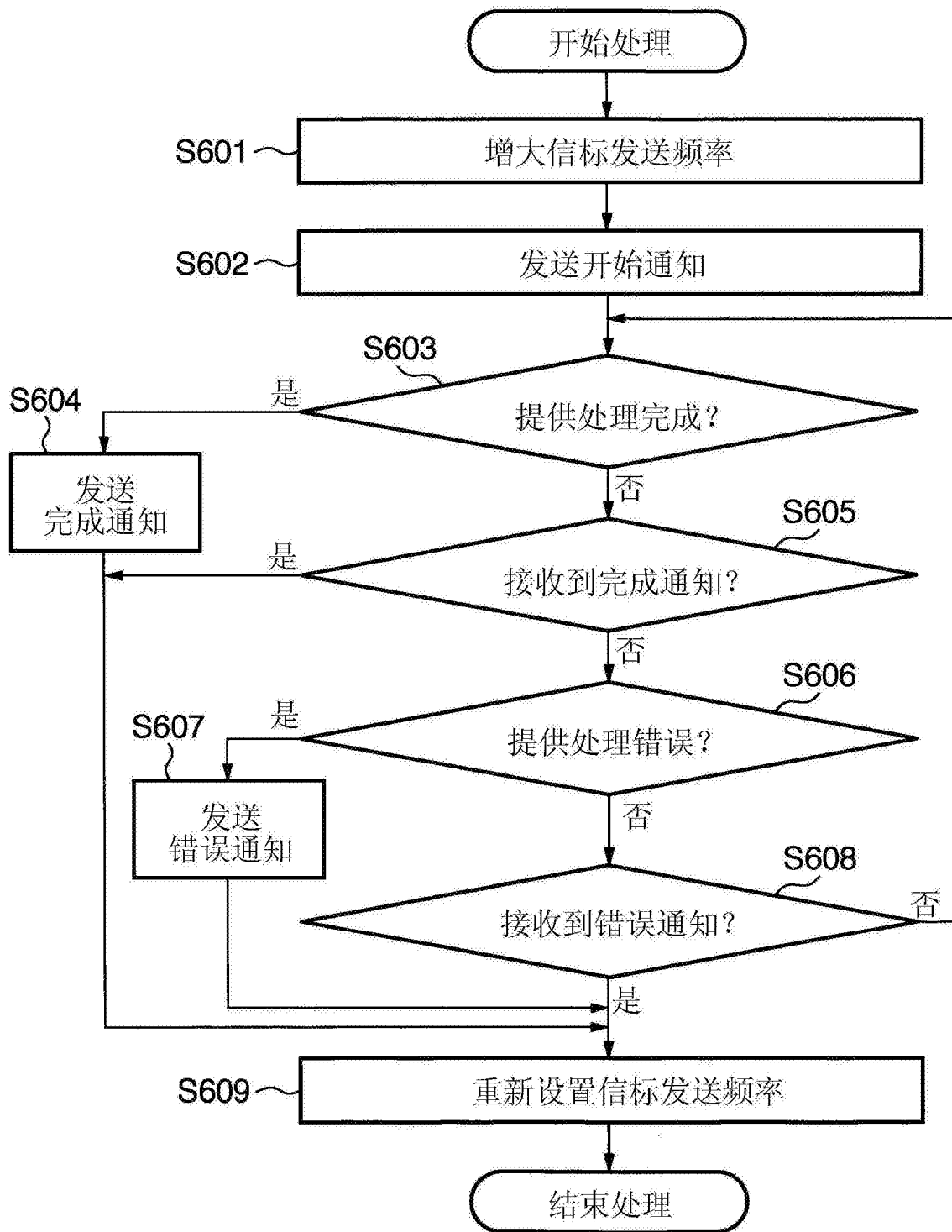


图6

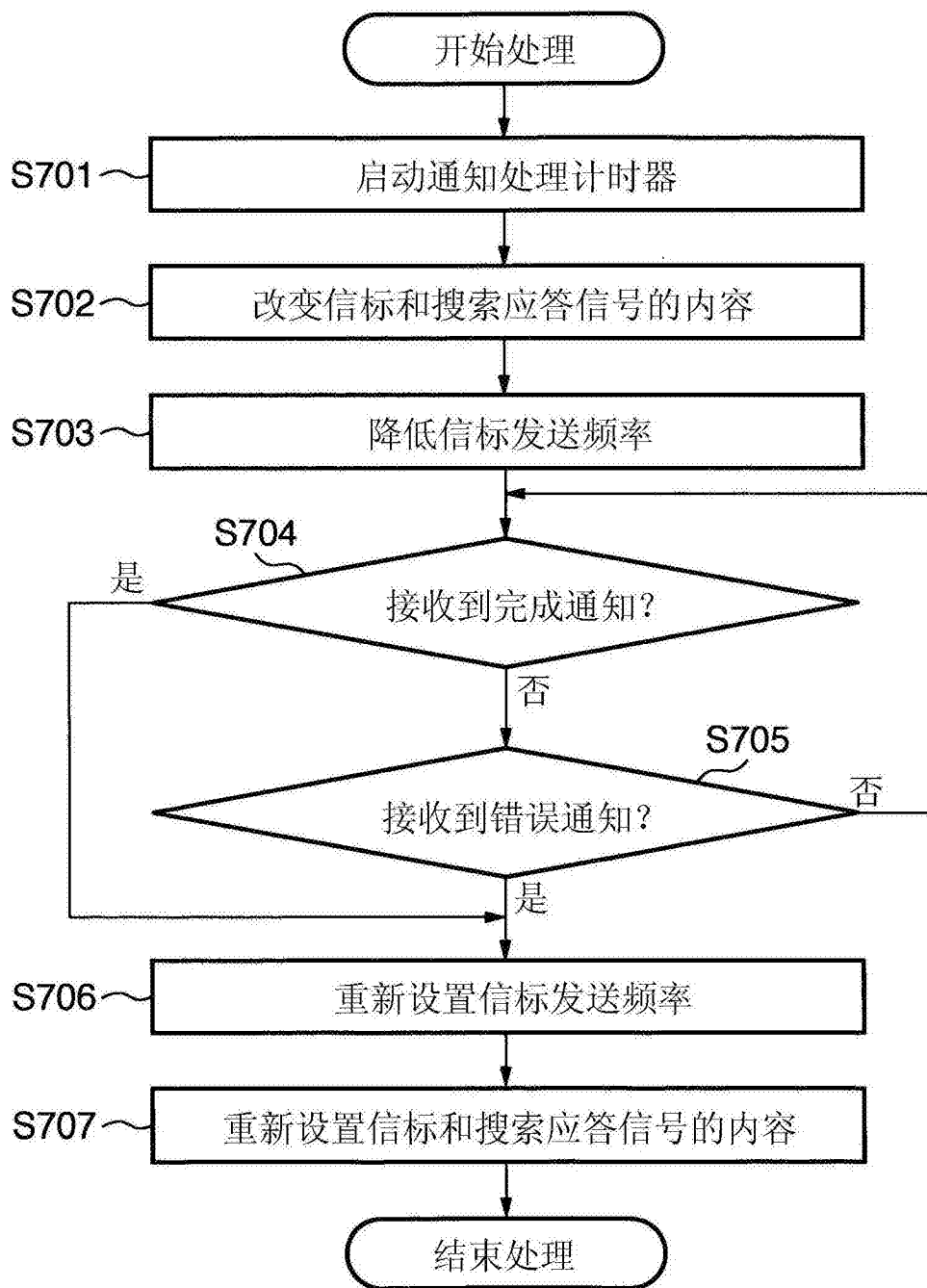


图7

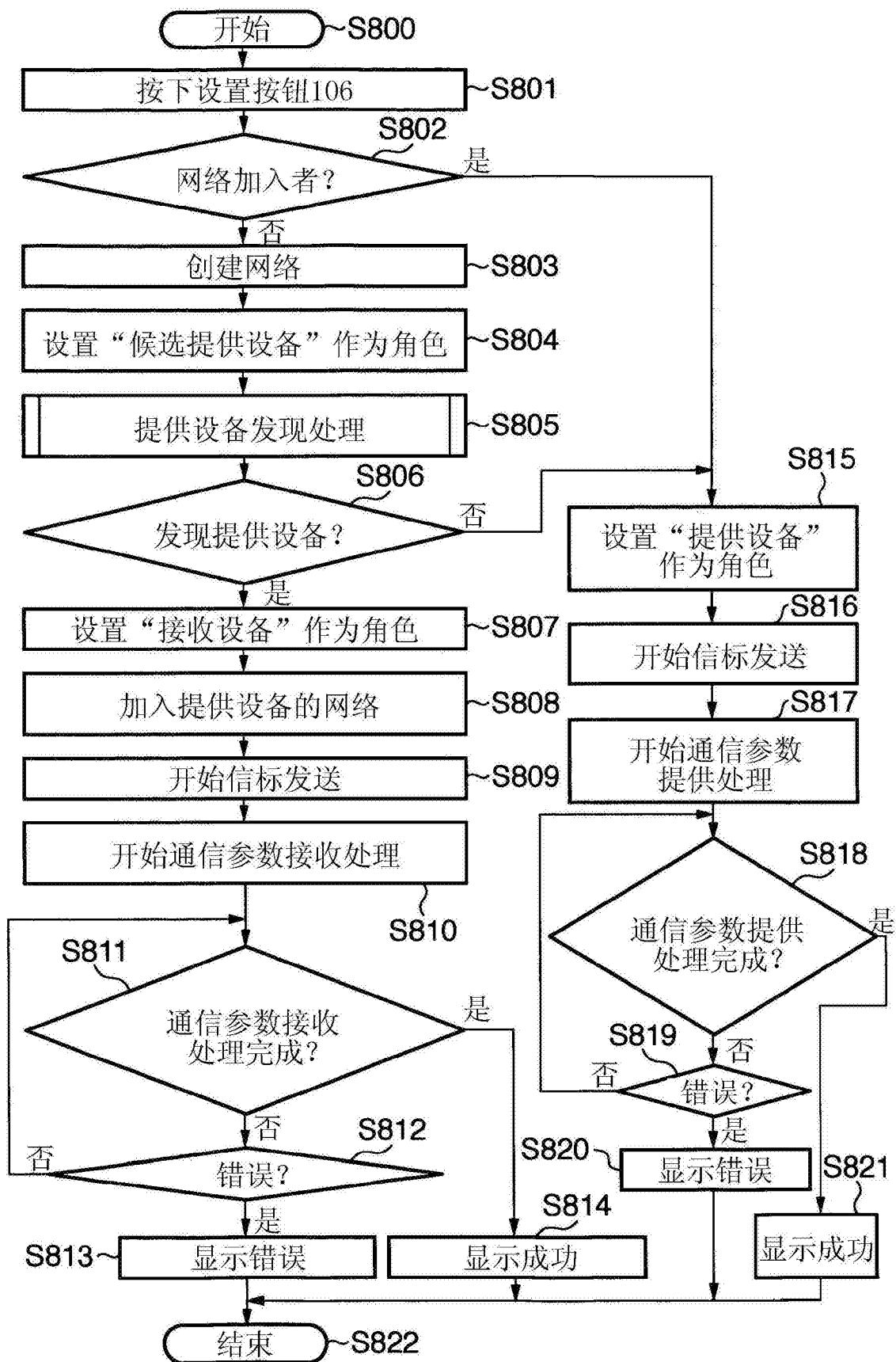


图8

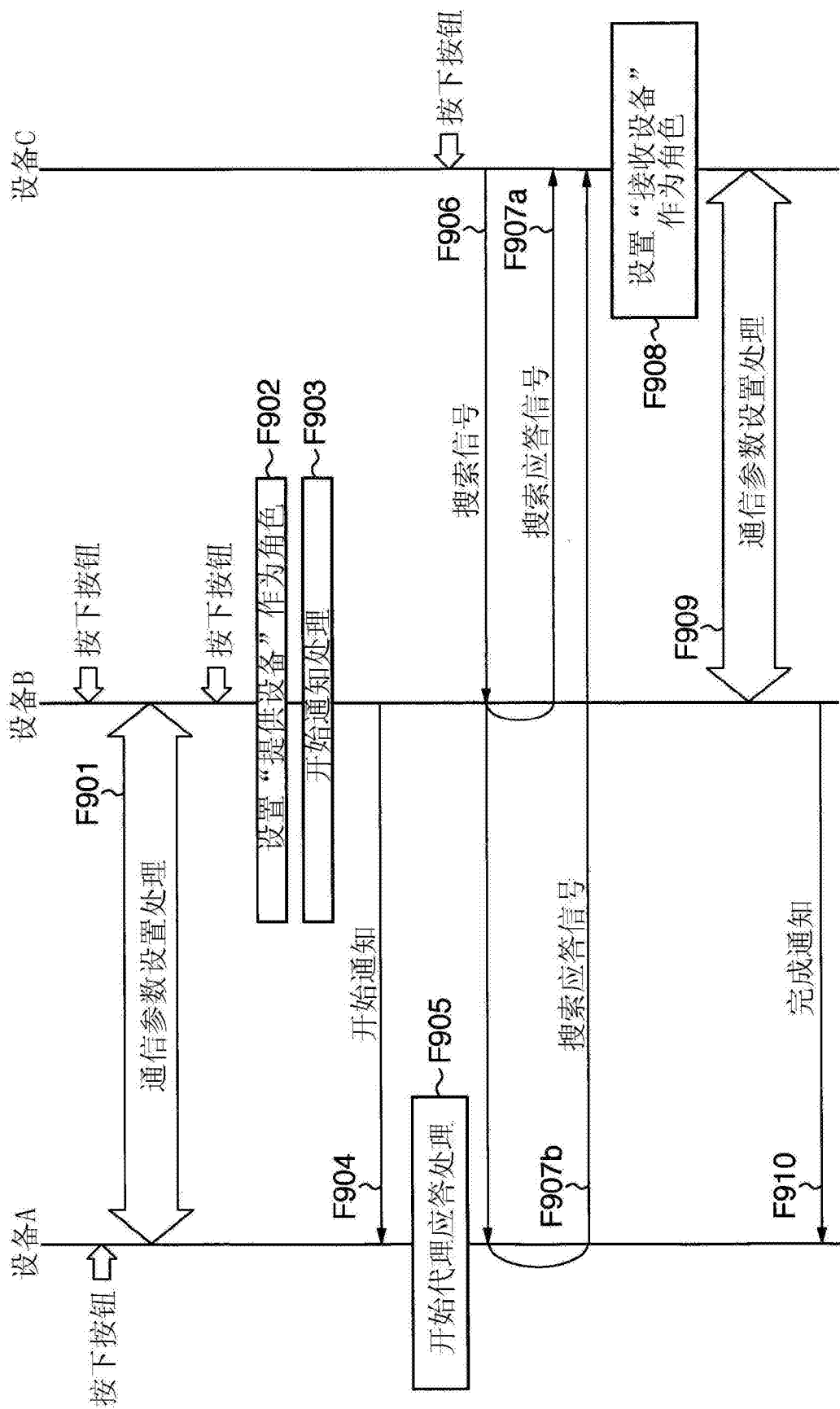


图9

支持的认证/加密方法

认证方法	加密方法
开放	不加密
	WEP
共享	WEP
WPA	TKIP
	CCMP
WPA-PSK	TKIP
	CCMP
WPA2	TKIP
	CCMP
WPA2-PSK	TKIP
	CCMP

图10

保持的密钥的数量			
方法	对偶密钥	组密钥	总数
IEEE802.11i全部规范	$n-1$	$n+1$	$2n$
(1) 减少序列	$n-1$	$n+1$	$2n$
(2) 减少密钥	$n-1$	1	n
(3) WPA-None	0	1	1
(4) 通过WPS握手的 WPA密钥交换	$n-1$	$n+1$ 或1	$2n$ 或 n

每一其它设备所执行的密钥交换的数量		
方法	四次握手	组密钥握手
IEEE802.11i全部规范	2	2
(1) 减少序列	1	2
(2) 减少密钥	1或2	1
(3) WPA-None	0	0
(4) 通过WPS握手的 WPA密钥交换	0	0或1或2

图11

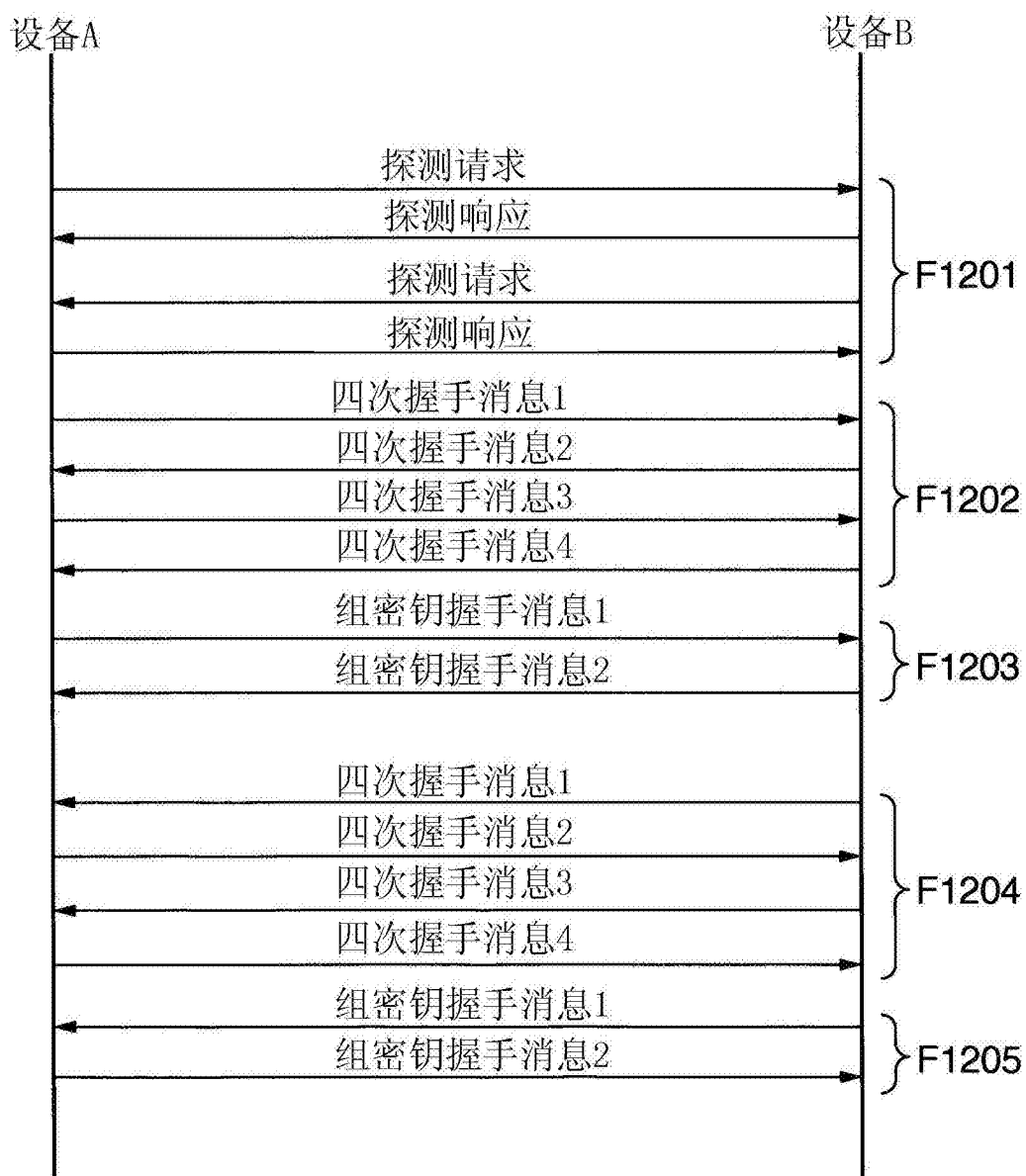


图12

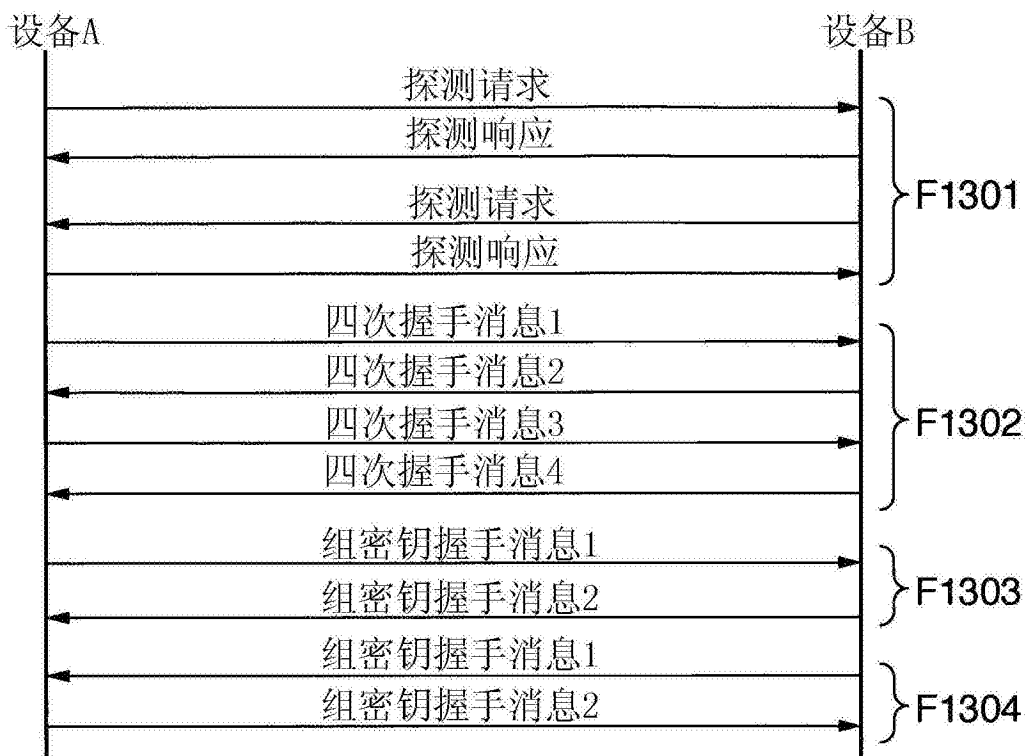


图13

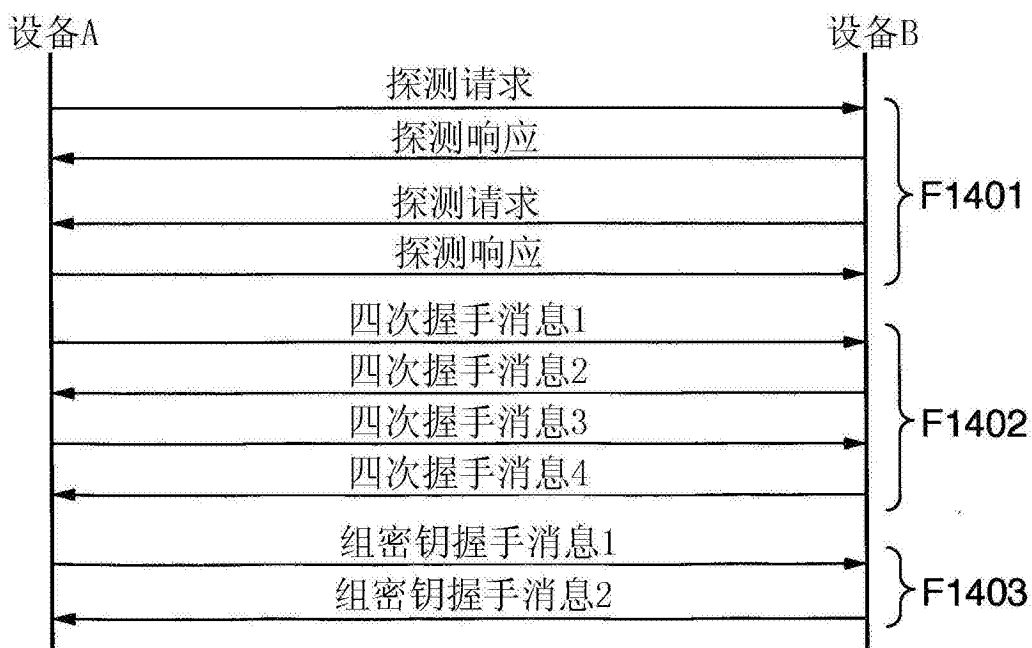


图14

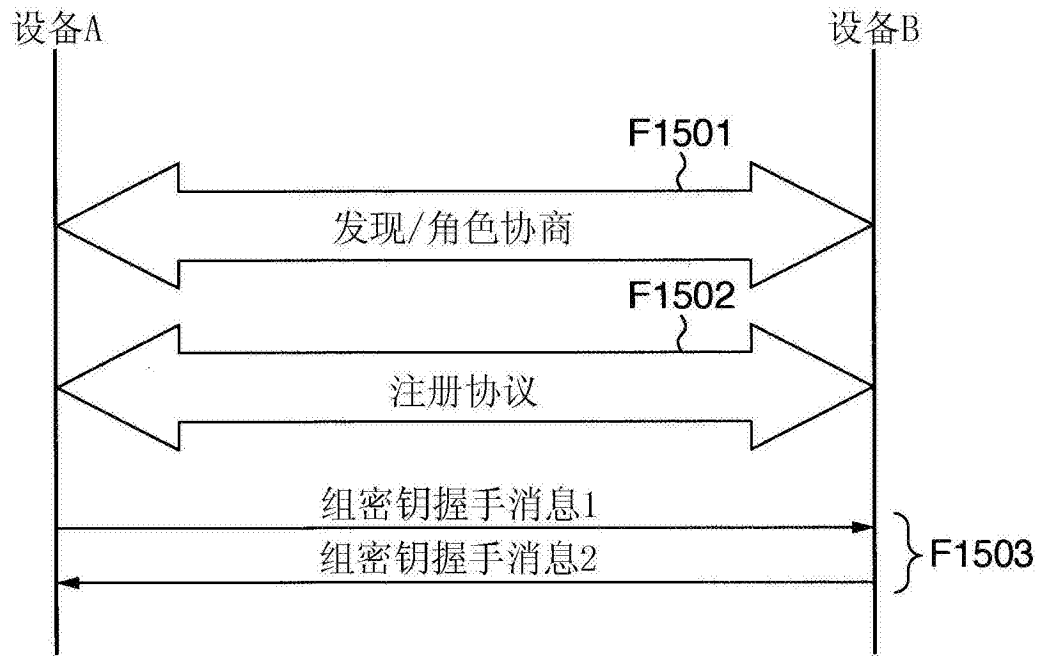


图15

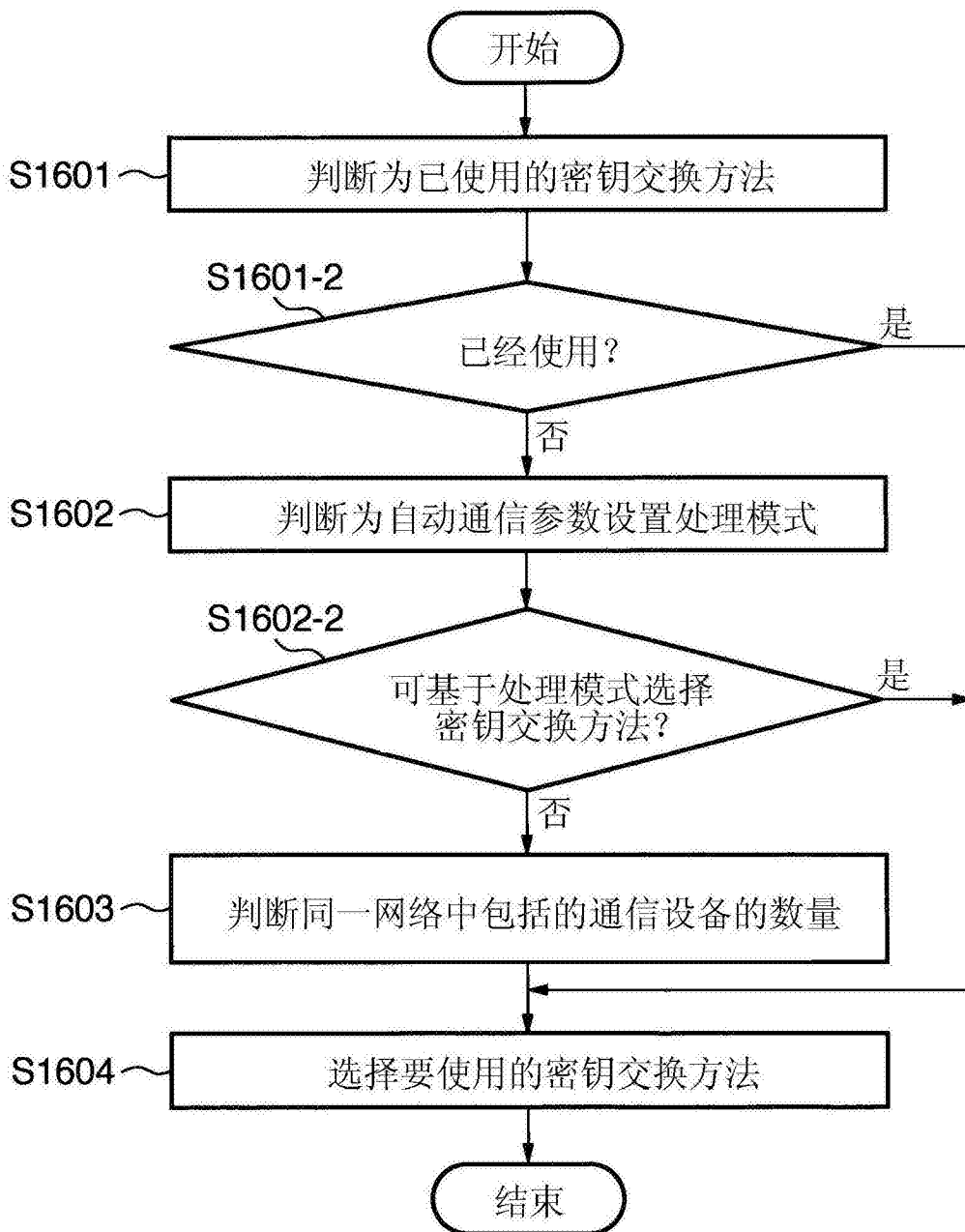


图16

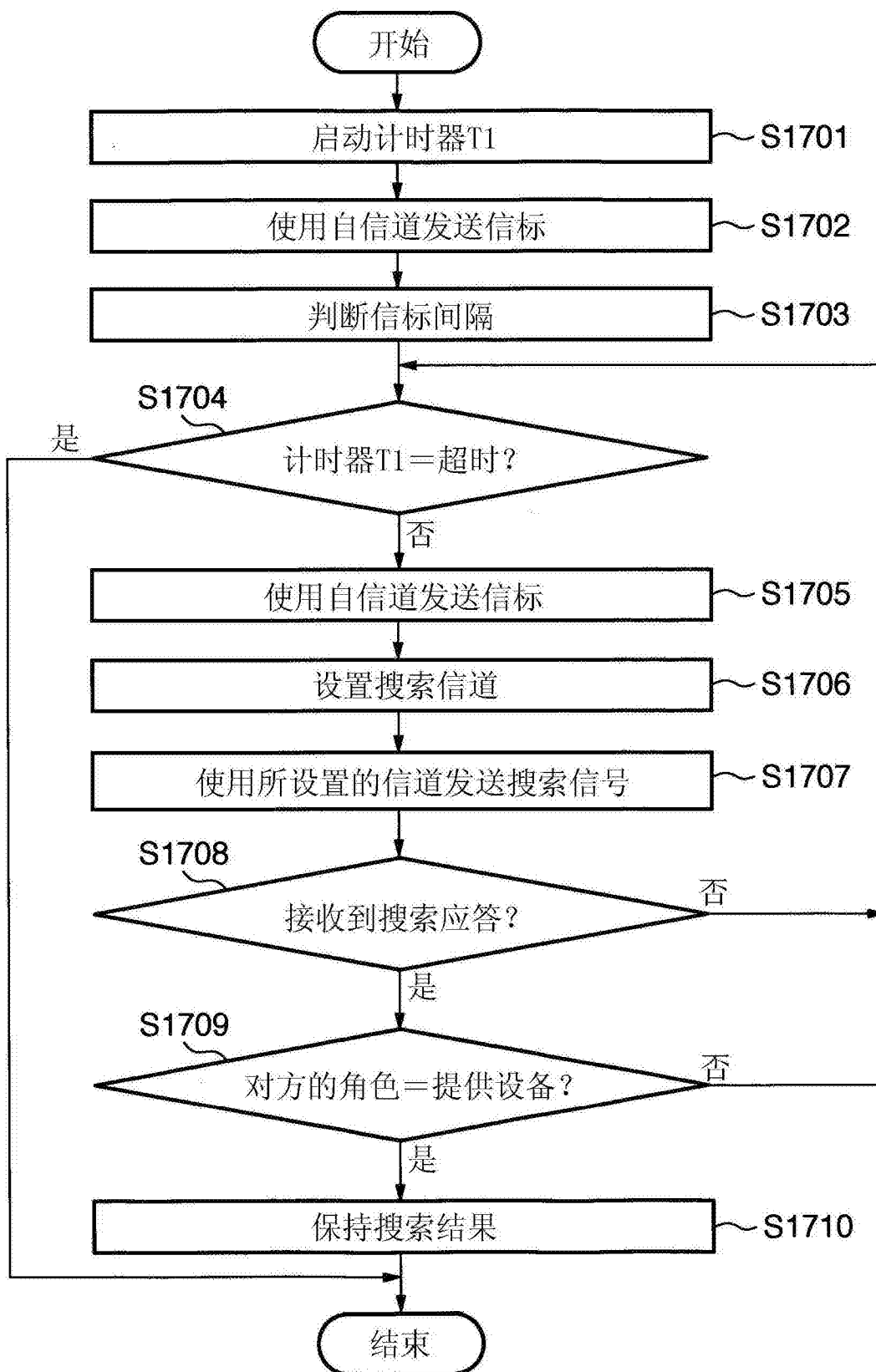


图17

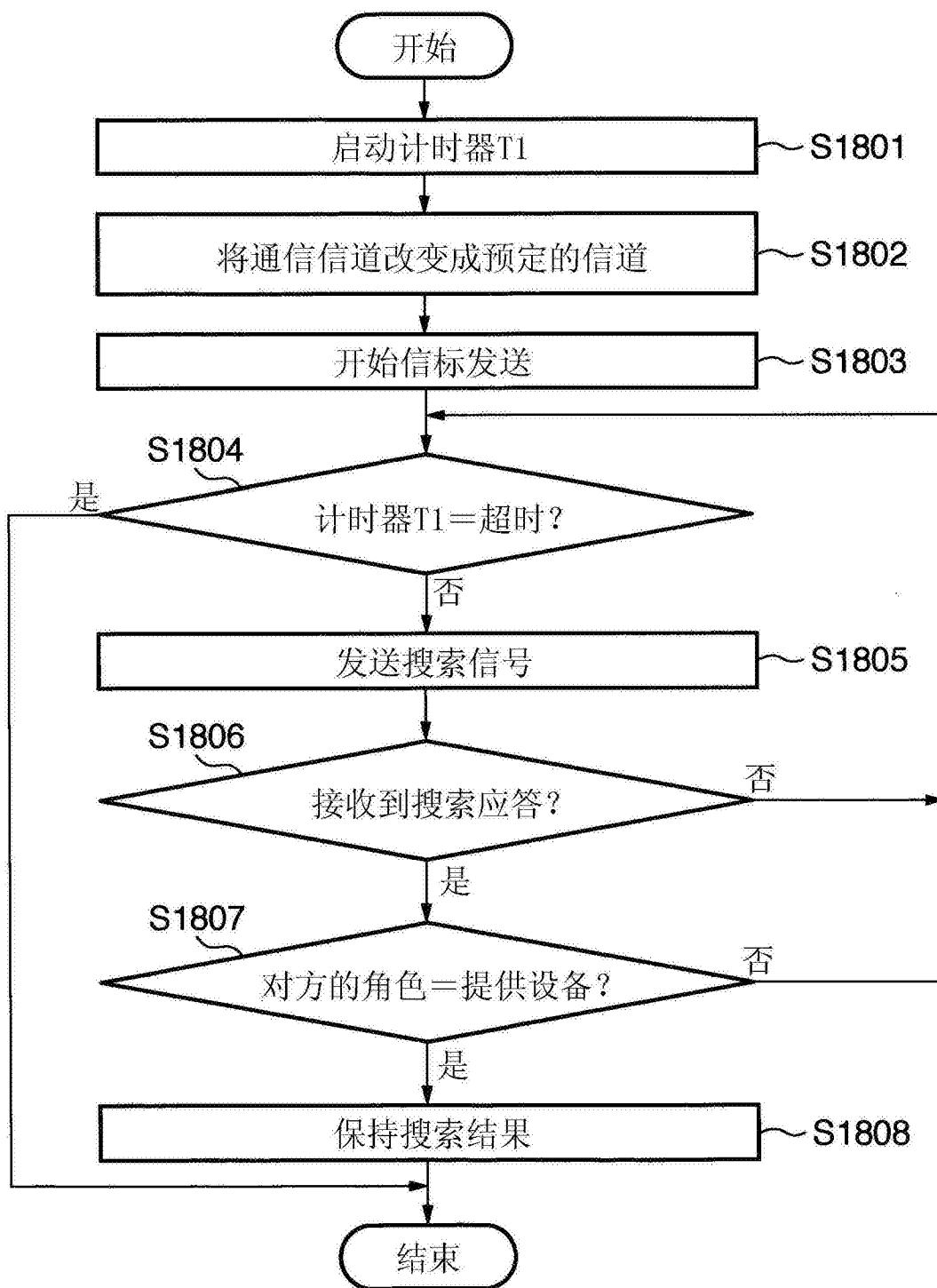


图18

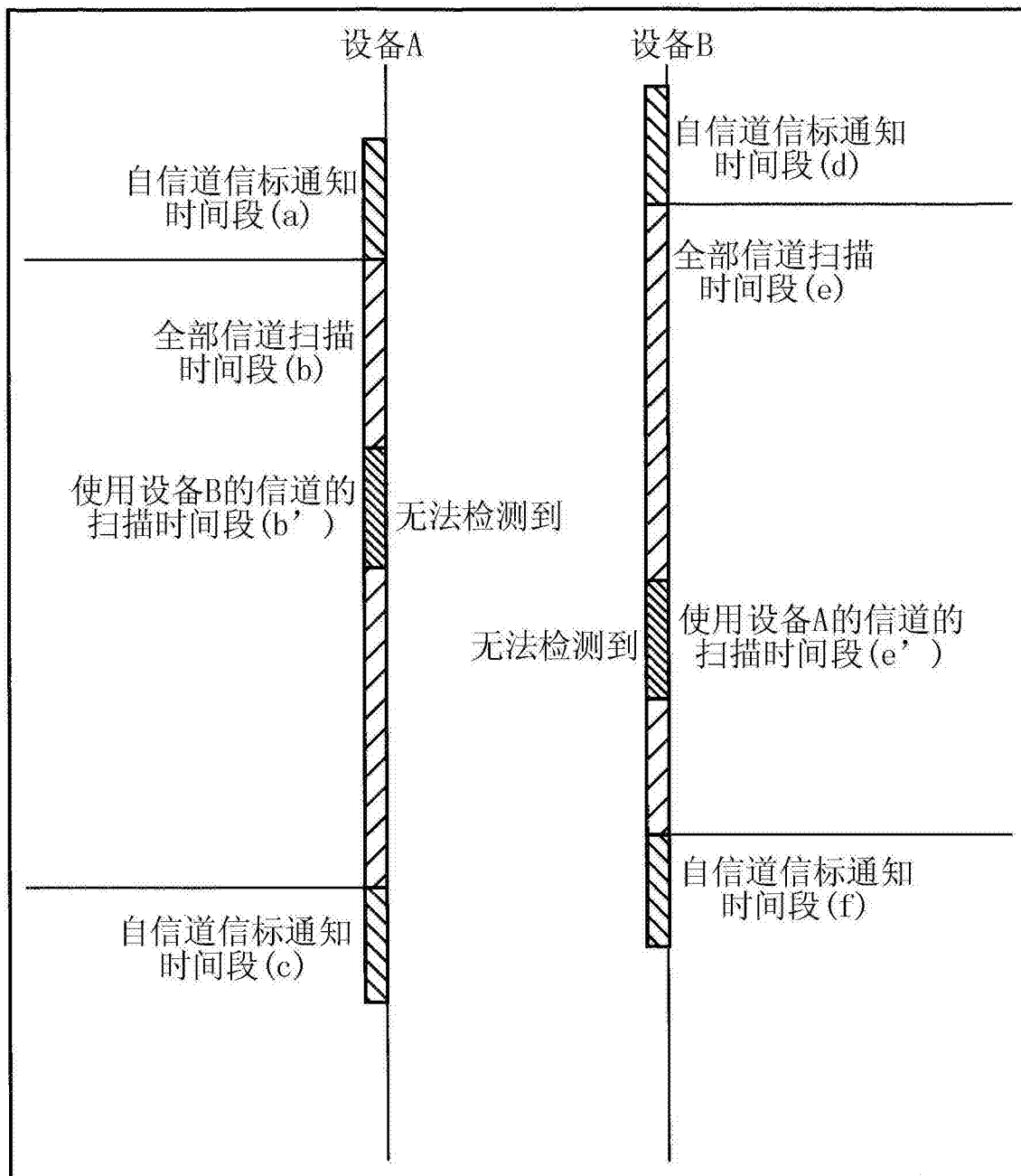


图19

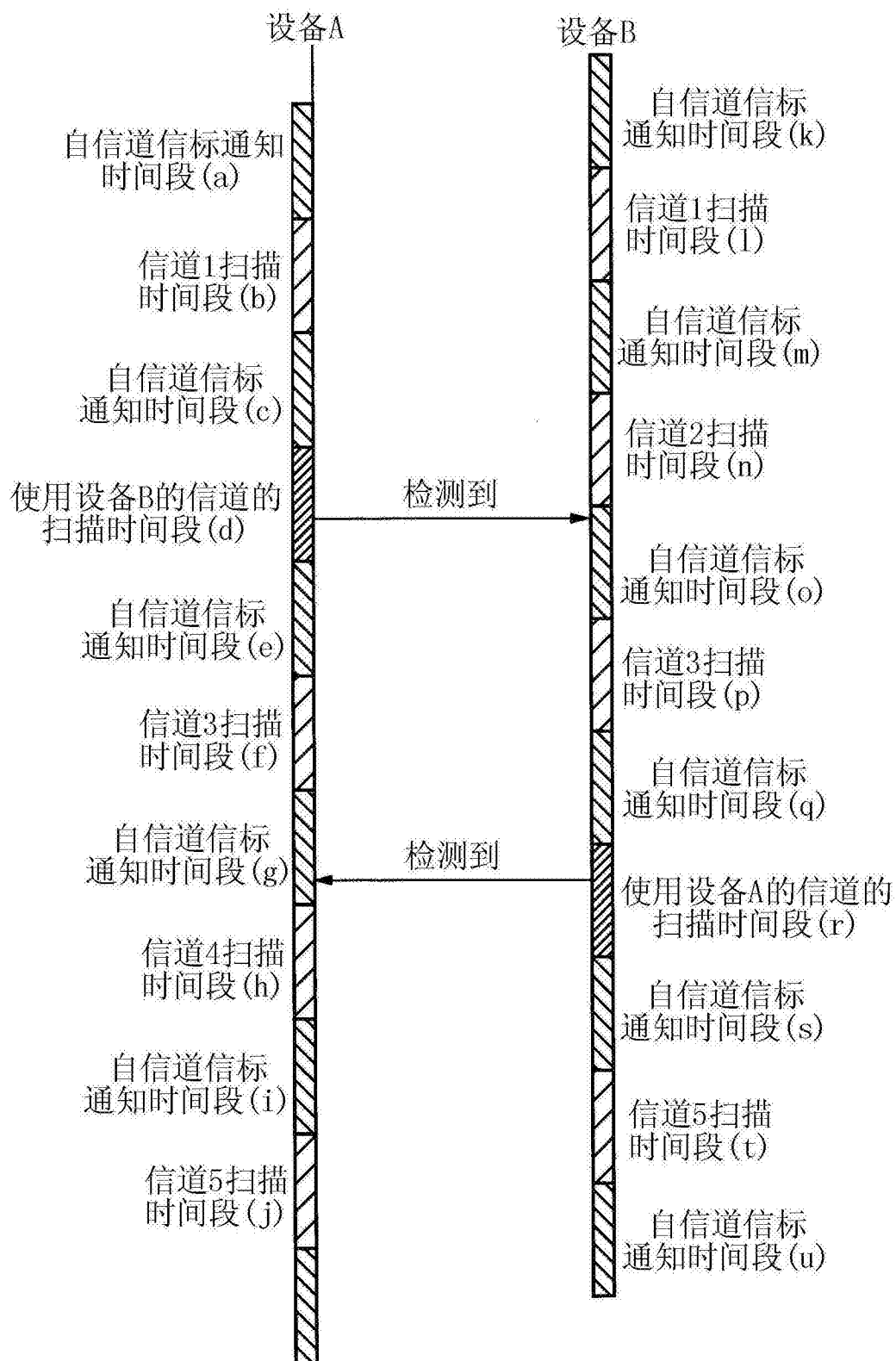


图20