(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107306267 A
(43)申请公布日 2017.10.31

(21)申请号 201610262789.7

(22)申请日 2016.04.25

(71)申请人 西门子公司
地址 德国慕尼黑

(72)发明人 张洁 蓝培 丹尼尔·博芬西彭

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 李慧

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/46(2006.01)

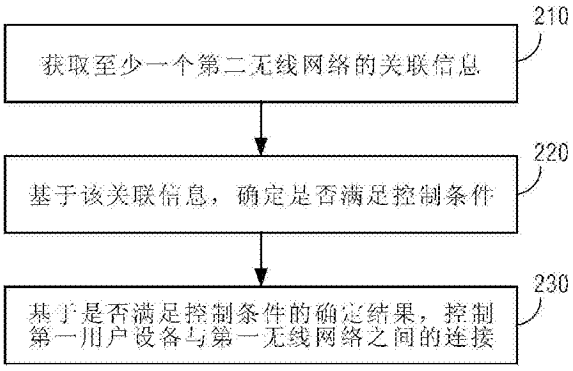
权利要求书2页 说明书8页 附图3页

(54)发明名称

用于控制无线网络访问的方法和装置

(57)摘要

本发明实施例提供了用于控制无线网络访问的方法和装置。该方法包括:获取至少一个第二无线网络的关联信息,关联信息用于指示当前连接到至少一个第二无线网络的用户设备;基于关联信息,确定是否满足控制条件,控制条件包括指定用户设备已经连接到至少一个第二无线网络;以及基于是否满足控制条件的确定结果,控制第一用户设备与第一无线网络之间的连接。可见,本发明实施例提供了一种新的网络访问控制方案,与现有技术中涉及密码的认证方式相比,能够更为灵活而且更为有效地实现网络访问控制目的,从而能够防止不受监管的网络访问。



CN 107306267 A

1.一种用于控制无线网络访问的方法,包括:

获取至少一个第二无线网络的关联信息,所述关联信息用于指示当前连接到所述至少一个第二无线网络的用户设备;

基于所述关联信息,确定是否满足控制条件,所述控制条件包括指定用户设备已经连接到所述至少一个第二无线网络;以及

基于是否满足所述控制条件的确定结果,控制第一用户设备与第一无线网络之间的连接。

2.根据权利要求1所述的方法,其中,所述获取所述至少一个第二无线网络的关联信息包括:

从公共存储资源读取由所述至少一个第二无线网络存储的所述关联信息。

3.根据权利要求1所述的方法,其中,所述获取所述至少一个第二无线网络的关联信息包括:

获取所述关联信息,其中所述关联信息是从所述至少一个第二无线网络接收的。

4.根据权利要求1至3中任一项所述的方法,其中,所述控制所述第一用户设备与所述第一无线网络之间的连接包括:

准许所述第一用户设备与所述第一无线网络之间的连接;或者

拒绝所述第一用户设备与所述第一无线网络之间的连接。

5.根据权利要求4所述的方法,其中,所述准许所述第一用户设备与所述第一无线网络之间的连接包括以下各项操作中的至少一项:

激活所述第一无线网络;或者

启用所述第一无线网络的白名单,所述白名单包括所述第一用户设备,其中所述白名单所包括的用户设备对所述第一无线网络具有访问权限。

6.根据权利要求4所述的方法,其中,所述拒绝所述第一用户设备与所述第一无线网络之间的连接包括以下各项操作中的至少一项:

去激活所述第一无线网络;或者

启用所述第一无线网络的黑名单,其中所述黑名单包括所述第一用户设备,其中,所述黑名单所包括的用户设备对所述第一无线网络不具有访问权限。

7.一种用于控制无线网络访问的装置,包括:

获取模块,用于获取至少一个第二无线网络的关联信息,所述关联信息用于指示当前连接到所述至少一个第二无线网络的用户设备;

判断模块,用于基于所述关联信息,确定是否满足控制条件,所述控制条件包括指定用户设备已经连接到所述至少一个第二无线网络;以及

控制模块,用于基于所述判断模块关于是否满足所述控制条件的确定结果,控制第一用户设备与第一无线网络之间的连接。

8.根据权利要求7所述的装置,其中,所述获取模块进一步用于:

从公共存储资源读取由所述至少一个第二无线网络存储的所述关联信息。

9.根据权利要求7所述的装置,其中,所述获取模块进一步用于:

获取所述关联信息,其中所述关联信息是从所述至少一个第二无线网络接收的。

10.根据权利要求7至9中任一项所述的装置,其中,所述控制模块进一步用于:

准许所述第一用户设备与所述第一无线网络之间的连接;或者

拒绝所述第一用户设备与所述第一无线网络之间的连接。

11.根据权利要求10所述的装置,其中,用于准许所述第一用户设备与所述第一无线网络之间的连接的所述控制模块进一步用于执行以下各项操作中的至少一项:

激活所述第一无线网络;或者

启用所述第一无线网络的白名单,所述白名单包括所述第一用户设备,其中所述白名单所包括的用户设备对所述第一无线网络具有访问权限。

12.根据权利要求10所述的装置,其中,用于拒绝所述第一用户设备与所述第一无线网络之间的连接的所述控制模块进一步用于执行以下各项操作中的至少一项:

去激活所述第一无线网络;或者

启用所述第一无线网络的黑名单,其中所述黑名单包括所述第一用户设备,其中,所述黑名单所包括的用户设备对所述第一无线网络不具有访问权限。

13.一种用于控制无线网络访问的装置,包括:

存储器;以及

处理器,用于执行权利要求1至6中任一项所包括的操作。

14.一种机器可读介质,其上存储有可执行指令,当所述可执行指令被执行时,使得机器执行权利要求1至6中任一项所包括的操作。

用于控制无线网络访问的方法和装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及用于控制无线网络访问的方法和装置。

背景技术

[0002] 出于安全等的目的，可能希望控制某些用户对特定无线网络的访问。例如，在企业环境中，可能希望控制企业访客对企业无线网络的访问；在家庭环境中，可能希望控制孩子对家庭无线网络的访问；在工业控制环境中，可能希望在某些情况下限制生产设备与无线网络的连接；在培训环境中，可能希望控制学生对培训环境中的无线网络的访问，进而限制培训设备与无线网络的连接等。

[0003] 目前，对无线网络的访问控制一般通过认证方式来实现，例如，针对无线局域网(Wireless Local Area Network，WLAN)可以采用Wi-Fi保护访问2(Wi-Fi Protected Access2，WPA2)方式来实现访问控制。具体而言，用户在希望访问无线网络时需要提供相应的密码或密钥，在由服务器对密码或密钥进行认证之后，该用户可以对该网络进行访问。或者进一步地，该密码或密钥可以是在某一时间段内有效的，或者其可以是通过短消息服务发送给该用户。

[0004] 然而，现有的这种方式并不能达到理想的访问控制目的。例如，如果访问无线网络的密码或者密钥遭到泄露或者传播，那么就无法达到网络访问控制的目的。比如，在上述例子的场景下，孩子在获知家庭无线网络的密码或密钥之后，可以在没有父母监管的情况下而访问家庭无线网络。因此，需要改进的网络访问控制方案。

发明内容

[0005] 考虑到现有技术的上述问题，本发明的实施例提供了用于控制无线网络访问的方法和装置，能够实现更为灵活且有效的网络访问控制目的。

[0006] 根据本发明实施例的一种用于控制无线网络访问的方法，包括：获取至少一个第二无线网络的关联信息，所述关联信息用于指示当前连接到所述至少一个第二无线网络的用户设备；基于所述关联信息，确定是否满足控制条件，所述控制条件包括指定用户设备已经连接到所述至少一个第二无线网络；以及基于是否满足所述控制条件的确定结果，控制第一用户设备与第一无线网络之间的连接。

[0007] 其中，所述获取所述至少一个第二无线网络的关联信息包括：从公共存储资源读取由所述至少一个第二无线网络存储的所述关联信息。

[0008] 其中，所述获取所述至少一个第二无线网络的关联信息包括：获取所述关联信息，其中所述关联信息是从所述至少一个第二无线网络接收的。

[0009] 其中，所述控制所述第一用户设备与所述第一无线网络之间的连接包括：准许所述第一用户设备与所述第一无线网络之间的连接；或者拒绝所述第一用户设备与所述第一无线网络之间的连接。

[0010] 其中，所述准许所述第一用户设备与所述第一无线网络之间的连接包括以下各项

操作中的至少一项：激活所述第一无线网络；或者启用所述第一无线网络的白名单，所述白名单包括所述第一用户设备，其中所述白名单所包括的用户设备对所述第一无线网络具有访问权限。

[0011] 其中，所述拒绝所述第一用户设备与所述第一无线网络之间的连接包括以下各项操作中的至少一项：去激活所述第一无线网络；或者启用所述第一无线网络的黑名单，其中所述黑名单包括所述第一用户设备，其中，所述黑名单所包括的用户设备对所述第一无线网络不具有访问权限。

[0012] 根据本发明实施例的一种用于控制无线网络访问的装置，包括：获取模块，用于获取至少一个第二无线网络的关联信息，所述关联信息用于指示当前连接到所述至少一个第二无线网络的用户设备；判断模块，用于基于所述关联信息，确定是否满足控制条件，所述控制条件包括指定用户设备已经连接到所述至少一个第二无线网络；以及控制模块，用于基于所述判断模块关于是否满足所述控制条件的确定结果，控制第一用户设备与第一无线网络之间的连接。

[0013] 其中，所述获取模块进一步用于：从公共存储资源读取由所述至少一个第二无线网络存储的所述关联信息。

[0014] 其中，所述获取模块进一步用于：获取所述关联信息，其中所述关联信息是从所述至少一个第二无线网络接收的。

[0015] 其中，所述控制模块进一步用于：准许所述第一用户设备与所述第一无线网络之间的连接；或者拒绝所述第一用户设备与所述第一无线网络之间的连接。

[0016] 其中，用于准许所述第一用户设备与所述第一无线网络之间的连接的所述控制模块进一步用于执行以下各项操作中的至少一项：激活所述第一无线网络；或者启用所述第一无线网络的白名单，所述白名单包括所述第一用户设备，其中所述白名单所包括的用户设备对所述第一无线网络具有访问权限。

[0017] 其中，用于拒绝所述第一用户设备与所述第一无线网络之间的连接的所述控制模块进一步用于执行以下各项操作中的至少一项：去激活所述第一无线网络；或者启用所述第一无线网络的黑名单，其中所述黑名单包括所述第一用户设备，其中，所述黑名单所包括的用户设备对所述第一无线网络不具有访问权限。

[0018] 从上述可以看出，本发明实施例提供了一种新的网络访问控制方案，与现有技术中涉及密码的认证方式相比，能够更为灵活而且更为有效地实现网络访问控制目的，从而防止不受监管的网络访问。另外，本发明实施例所提供的技术方案无需对网络硬件进行额外修改，也不需要增加额外的网络设备，因此成本低且容易实现。

附图说明

[0019] 本发明的其它特征、特点、优点和益处通过以下结合附图的详细描述将变得更加显而易见。

[0020] 图1A是可应用本发明实施例的场景的一个例子的示意图。

[0021] 图1B是可应用本发明实施例的场景的另一例子的示意图。

[0022] 图1C是可应用本发明实施例的场景的另一例子的示意图。

[0023] 图2是根据本发明一个实施例的用于控制无线网络访问的方法的示意性流程图。

[0024] 图3是根据本发明一个实施例的用于控制无线网络访问的装置的示意图。

[0025] 图4是根据本发明一个实施例的用于控制无线网络访问的装置的示意图。

具体实施方式

[0026] 已知的是，接入点(Access Point，AP)可以被配置为提供多个虚拟无线网络。例如，单个AP可以被配置为提供一个或多个虚拟无线网络，多个AP可以被配置为多个虚拟无线网络或者共同提供一个虚拟无线网络。可以为多个虚拟无线网络分别设置不同的网络标识符。例如，在IEEE 802.11标准中，这样的网络标识符可以称为扩展服务集标识符(Extended Service Set Identifier，ESSID)。那么，不同的用户设备可以基于ESSID来选择相应的虚拟无线网络进行接入，从而进行网络访问。本发明实施例所提供的技术方案正是基于这样的前提。

[0027] 首先，通过例子来说明本发明实施例可应用的场景。应注意，以下例子只是为了帮助本领域技术人员更好地理解本发明实施例，而非限制本发明实施例的范围。

[0028] 图1A是可应用本发明实施例的场景的一个例子的示意图。例如，图1A所示的场景可以是家庭网络环境。该场景可以包括AP 110A以及有线骨干网，其中AP 110A可以连接到有线骨干网，由此AP 110可以提供网络访问服务。

[0029] 在图1A的例子中，假设AP 110A可以被配置为支持虚拟无线网络120A-1和120A-2。虚拟无线网络120A-1和120A-2可以分别具有不同的ESSID。

[0030] 各个用户设备可以基于ESSID来选择相应的虚拟无线网络，向AP 110A发起关联请求。AP 110A在接收到关联请求后，可以对关联请求进行认证等，在认证通过后接受用户设备的请求。由此，用户设备就接入该相应的虚拟无线网络。

[0031] 例如，在图1A的例子中，用户设备130A-1可以接入无线网络120A-1进行网络访问，而用户设备130A-2和130A-3可以接入无线网络120A-2进行网络访问。

[0032] 应当理解的是，为了便于描述，在图1A示出一个AP提供两个虚拟无线网络。而实际情况中通常可能存在多个AP。如上所述，多个AP可以被配置为提供多个虚拟无线网络或者共同提供一个虚拟无线网络。在某些较小型的网络中，这些AP本身均具有对用户设备的关联请求等的相关处理能力(例如，认证等)，而且它们之间可以通过有线或者无线的方式相互通信，以便交换与通信处理相关的信息。此外，这些AP还可以通过访问公共的网络存储资源来实现与通信处理相关的信息的交互。

[0033] 在大型网络情况下，为了便于管理，通常设置有一个或多个AP控制器。每个AP控制器可以管理多个AP。在这种情况下，对用户设备的关联请求等的处理功能可以由AP控制器来实现，而AP本身可以不需要具备这样的能力。因此，AP在接收到用户设备的关联请求之后，可以将关联请求转发给AP控制器进行处理。另外，在存在AP控制器的情况下，AP之间也可以不进行相互通信，它们可以将与通信处理相关的信息上报给AP控制器，由AP控制器进行统一管理。

[0034] 下面将通过例子来说明这样的场景。应当理解的是，为了便于描述，在图1B和图1C中以两个AP为例来进行说明。

[0035] 图1B是可应用本发明实施例的场景的另一例子的示意图。例如，图1B所示的场景可以是企业网络环境等。如图1B所示，该场景可以包括两个AP，即AP 110B和AP 110C。AP

110B和AP 110C均可以连接到有线骨干网(图中未示出),从而可以提供网络访问服务。

[0036] 在图1B的例子中,假设AP 110B和AP 110C可以被配置为提供三个虚拟无线网络120B-1、120B-2和120B-3。如图1B所示,虚拟无线网络120B-2可以由AP 110B和AP 110C共同提供,虚拟无线网络120B-1可以由AP 110B提供,而虚拟无线网络120B-3可以由AP 110C提供。其中,这三个虚拟无线网络可以分别具有不同的ESSID。

[0037] 各个用户设备可以基于ESSID来选择相应的虚拟无线网络,然后向提供该虚拟无线网络的AP发起关联请求。在从用户设备接收到关联请求之后,AP可以进行认证等处理,在认证通过之后,AP可以与用户设备相关联,从而通过相应的虚拟无线网络来为该用户设备提供网络访问服务。

[0038] 例如,在图1B中,用户设备130B-1可以接入无线网络120B-1进行网络访问,用户设备130B-2和130B-3可以接入无线网络120B-2进行网络访问,而用户设备130B-4可以接入无线网络120B-3进行网络访问。

[0039] 在图1B中所示的场景,假设不存在AP控制器,AP 110B与AP 110C之间可以相互通信,从而交互与通信处理相关的各种信息。

[0040] 在另一种实现方式中,AP 110B和AP 110C可以访问公共的网络存储资源。AP 110B和AP 110C可以将与通信处理相关的各种信息存储在公共的网络存储资源上,从而在AP 110B和AP 110C之间实现信息的共享。

[0041] 图1C是可应用本发明实施例的场景的另一例子的示意图。例如,图1C所示的场景可以是企业网络环境、工业控制环境或者培训环境等。如图1C所示,该场景可以包括两个AP,即AP 110D和AP 110E。AP 110D和AP 110E均可以连接到有线骨干网(图中未示出),从而可以提供网络访问服务。

[0042] 在图1C中,仍然假设AP 110D和AP 110E可以被配置为提供三个虚拟无线网络120C-1、120C-2和120C-3。如图1C所示,虚拟无线网络120C-2可以由AP 110D和AP 110E共同提供,虚拟无线网络120C-1可以由AP 110D提供,而虚拟无线网络120C-3可以由AP 110E提供。其中,这三个虚拟无线网络可以分别具有不同的ESSID。

[0043] 用户设备可以根据ESSID选择相应的虚拟无线网络进行接入。例如,在图1C中,用户设备130C-1可以连接到无线网络120C-1,用户设备130C-2和130C-3可以连接到无线网络120C-2,而用户设备130C-4可以连接到无线网络120C-3。

[0044] 与图1B的场景不同的是,图1C所示的场景中还可以包括AP控制器140。AP控制器140可以对AP 110D和AP 110E进行管理。在这种情况下,对关联请求的处理能力(例如,认证等)可以由AP控制器140来实现,而APAP 110D和AP 110E本身可以不需要具备这样的能力。例如,用户设备130C-1向提供虚拟无线网络120C-1的AP 110D发起的关联请求可以由该AP转发给AP控制器140。然后,AP控制器140对该关联请求进行认证等处理,在认证通过后准许该用户设备130C-1与AP 110D关联,从而使得该用户设备接入虚拟无线网络120C-1。

[0045] 另外,由于存在AP控制器140,AP 110D和AP 110E之间可以无需相互通信。AP 110D和AP 110E可以将与通信处理有关的信息均上报给AP控制器140,从而由AP控制器140进行统一处理。

[0046] 应当理解的是,在上述图1A、图1B和图1C中示出的AP数量及其支持虚拟无线网络的数量以及用户设备的数量仅是示例性的。本发明实施例中,可以存在更多或者更少的AP、

AP控制器、虚拟无线网络以及用户设备。

[0047] 出于安全等目的，可能需要控制特定用户对无线网络的访问。例如，假设图1A所示的场景是家庭网络环境，用户设备130A-1可以由孩子所使用，而用户设备130A-2可以由父母所使用。父母可能希望控制孩子对家庭无线网络的使用，例如，父母希望有父母在场时，孩子才能使用用户设备130A-1进行网络访问。因此，需要控制用户设备130A-1对该家庭无线网络的访问。

[0048] 再例如，假设图1B所示的场景是企业网络环境，无线网络120B-1、120B-2和120B-3中的一个或两个可以由企业员工使用，而剩余的无线网络可以由访客使用。比如，无线网络120B-2可以由企业员工使用，而无线网络120B-1和120B-3可以由访客使用。或者，无线网络120B-2和120B-3可以由企业员工使用，而无线网络120B-1可以由访客使用。同样可能出于安全等目的，希望控制访客对企业无线网络的访问。比如，需要控制访客的用户设备130B-1对无线网络120B-1的访问。

[0049] 再例如，假设图1C所示的场景是工业控制环境，其中无线网络120C-2用于连接各个生产设备130C-2和130C-3，而无线网络120C-1和120C-3可以由资深人员或者监督人员使用。此时，可能希望在资深人员或者监督人员在场的情况下，准许生产设备130C-2和130C-3与无线网络120C-2之间的连接，进而允许普通操作人员对这些生产设备进行操作。

[0050] 再例如，假设图1C所示的场景是培训环境，其中，无线网络120C-2和120C-3可以由学生使用，而无线网络120B-1可以由指导人员使用。同样可能出于安全等目的，希望在指导人员在场的情况下，学生才能使用无线网络120C-2或120C-3，或者进而使用连接到无线网络120C-2或120C-3的设备130C-2至130C-4中的任一个。

[0051] 那么，对于上述这些问题，本发明实施例提供了有效的解决方案。在下文中，将结合图2详细描述本发明实施例。

[0052] 图2是根据本发明一个实施例的用于控制无线网络访问的方法的示意性流程图。图2的方法可以由AP执行，也可以由AP控制器(如上所述，如果存在AP控制器的话)来执行。例如，该方法可以由图1A中的AP 110A或者图1B中的AP 110B、AP 110C、或者图1C中的AP控制器140来执行。

[0053] 如图2所示，在步骤210中，获取至少一个第二无线网络的关联信息，该关联信息用于指示当前连接到至少一个第二无线网络的用户设备。

[0054] 在步骤220中，基于该关联信息，确定是否满足控制条件，所述控制条件包括指定用户设备已经连接到至少一个第二无线网络。

[0055] 在步骤230中，基于是否满足所述控制条件的确定结果，控制第一用户设备与第一无线网络之间的连接。

[0056] 此处，第一无线网络和至少一个第二无线网络可以是AP所支持的虚拟无线网络。第一无线网络和至少一个第二无线网络可以由相同的AP提供，也可以分别由不同的AP提供。第一无线网络和至少一个第二无线网络中的每个无线网络均可以由一个或多个AP提供。例如，第一无线网络可以是由单个AP提供的网络，也可以是由多个AP共同提供的网络；每个第二无线网络可以是由单个AP提供的网络，也可以是由多个AP共同提供的网络。本发明实施例对此不作限定。另外，第一无线网络和至少一个第二无线网络可以属于同一物理网络，也可以属于不同的物理网络。

[0057] 在上述步骤210中，获取至少一个第二无线网络的关联信息可以通过多种方式来实现。

[0058] 在一种实现方式中，在步骤210中，可以从公共存储资源读取由所述至少一个第二无线网络存储的关联信息。该公共存储资源是第一无线网络和至少一个第二无线网络能够共同访问的。例如，提供第二无线网络的AP可以将其关联信息存储在公共存储资源，这样，提供第一无线网络的AP就能够获知当前连接到至少一个第二无线网络的用户设备。在另一实现方式中，上述关联信息可以是从至少一个第二无线网络接收的。该关联信息可以是预先从至少一个第二无线网络接收的，例如，在步骤210之前，AP控制器或者提供第一无线网络的AP可以从至少一个第二无线网络接收关联信息，然后将该关联信息存储在本地。这样，在第一用户设备请求访问第一无线网络时，AP控制器或者提供第一无线网络的AP可以从本地读取该关联信息。此外，该关联信息也可以是在需要判断是否满足控制条件时从至少一个第二无线网络接收的。

[0059] 在步骤230中，控制第一用户设备与第一无线网络之间的连接可以包括准许第一用户设备与第一无线网络之间的连接，或者拒绝第一用户设备与第一无线网络之间的连接。

[0060] 在一种实现方式中，准许第一用户设备与第一无线网络之间的连接可以包括以下各项中的至少一项：激活第一无线网络；或者启用第一无线网络的白名单(Whitelist)，白名单包括第一用户设备，其中白名单所包括的用户设备对第一无线网络具有访问权限。例如，白名单中可以包含具有访问权限的用户设备的介质访问控制标识符(Media Access Control Identifier,MAC ID)。这样，通过第一用户设备的MAC ID便可以确定第一用户设备是否在第一无线网络的白名单中。

[0061] 在另一实现方式中，拒绝第一用户设备与第一无线网络之间的连接可以包括以下各项中的至少一项：去激活第一无线网络；或者启用第一无线网络的黑名单(Blacklist)，其中黑名单包括第一用户设备，其中，黑名单所包括的用户设备对第一无线网络不具有访问权限。例如，黑名单可以包括不具有访问权限的用户设备的MAC ID。

[0062] 在某些情况下，激活/去激活第一无线网络这种方式相比启用白名单/黑名单的方式而言更容易实现。这是因为，白名单/黑名单的设定可能需要预先知道用户设备的MAC ID。然而，对于可能存在大量潜在用户设备的情况下，难以获取其MAC ID。

[0063] 另外，应当理解的是，是否满足控制条件的确定结果与控制第一用户设备与第一无线网络之间的连接的操作的关系可以根据实际情况来设定。例如，在确定满足控制条件的情况下，可以准许或者拒绝第一用户设备与第一无线网络之间的连接；在确定不满足控制条件的情况下，可以准许或者拒绝第一用户设备与第一无线网络之间的连接。本发明实施例对此并不限定。

[0064] 由此，还可以理解的是，上述控制步骤可以简单地表示为：如果<控制条件>满足，则执行<控制操作>。其中，控制操作可以包括以下各项中的至少一项：激活第一无线网络；去激活第一无线网络；启用第一无线网络的白名单；启用第一无线网络的黑名单。

[0065] 其中，控制条件可以是根据实际需要而预先设定的，并且可以存储在AP或者AP控制器上。该条件也可以理解为指定用户设备已经与提供至少一个第二无线网络的AP关联。此处，指定用户设备的数量可以大于等于一。

[0066] 该控制条件实际上可以理解为包括一个或多个子条件。每个子条件可以表示为“用户设备组关联到AP组”。用户设备组可以是一个用户设备，也可以是由和(AND)、或(OR)、异或(XOR)、非(NOT)等逻辑关系定义的多个用户设备。AP组可以是单个AP、或由某一特定ESSID指定的一组AP、或者由其各自的MAC ID指定的一组AP等。此外，多个子条件之间的关系可以是和、或、异或、非等逻辑关系。

[0067] 此外，第一无线网络可以与第二无线网络之间共享控制条件。也就是说，各个AP之间可以共享控制条件，从而实现期望的系统行为。

[0068] 从上述可以看出，由于控制条件和控制操作均可以根据实际需求灵活地设定，因此能够灵活地实现网络访问控制目的。

[0069] 为了帮助本领域技术人员更好地理解本发明实施例，下面将结合图1A的例子来详细描述本发明实施例的实现过程。

[0070] 假设图1A所示的场景是家庭网络环境。AP 110A提供的无线网络120A-2具有ESSID“主网络”，无线网络120A-1具有ESSID“孩子网络”。可以针对这两个网络分别配置不同的WPA密码。在该场景中，假设父母使用用户设备130A-2或者130A-3，而孩子使用用户设备130A-1。其中，父母的用户设备130A-2或者130A-3默认连接到“主网络”。

[0071] 假设控制条件被预先设定为父母的用户设备130A-2和130A-3中的至少一个连接到无线网络120A-2，并且预先设定当控制条件满足时，准许孩子的用户设备130A-1连接到“孩子网络”。例如，该关系可以表示为：如果<用户设备130A-2的MAC ID>或者<用户设备130A-3的MAC ID>关联到“主网络”，则激活“孩子网络”。

[0072] 那么，当确定用户设备130A-2或者130A-3中的至少一个已经连接到“主网络”时，可以激活“孩子网络”。此时，孩子可以通过输入“孩子网络”的WPA密码，使得其用户设备130A-1接入“孩子网络”。

[0073] 由此可以看出，当父母其中一人在家时，“孩子网络”将是活动的，从而为孩子的用户设备130A-1提供网络访问服务。然而，如果父母均离开家庭网络的覆盖范围，也就是说，用户设备130A-2和130A-3均没有连接到“主网络”时，“孩子网络”将被去激活。此时“主网络”仍是活动的。而一旦父母中的至少一人返回到家中，“孩子网络”将被再次激活，由此孩子可以再次通过用户设备130A-1使用“孩子网络”。

[0074] 可见，通过该技术方案，能够简单且有效地实现父母对孩子使用家庭网络的控制，从而防止非监管的网络访问。

[0075] 再例如，假设图1B所示的场景是企业网络环境，其中，无线网络120B-2可以由企业员工使用，而无线网络120B-1和120B-3可以由访客使用。控制条件可以被设定为员工的用户设备130B-2和130B-2连接到无线网络120B-2，并且假设当满足控制条件时，准许访客的用户设备连接到第一无线网络。这样，当访客的用户设备130B-1访问无线网络120B-1时，或者当访客的用户设备130B-4访问无线网络120B-3时，企业员工可以对此进行监管。

[0076] 再例如，在培训环境下，利用本发明实施例提供的技术方案，可以使得学生在老师或者指导人在场的情况下对该环境下进行无线网络访问；在工厂环境中，可以使得在监督者在场的情况下准许生产设备与无线网络的连接，由此操作人员可以在监督者监管的情况下对生产设备进行操作；等等。

[0077] 通过上述描述可以看出，本发明实施例提供了一种新的网络访问控制方案，与现

有技术中涉及密码的认证方式相比，能够更为灵活而且更为有效地防止不受监管的网络访问。另外，本发明实施例所提供的技术方案无需对网络硬件进行额外修改，也不需要增加额外的网络设备，因此成本低且容易实现。

[0078] 现在参照图3，其是根据本发明一个实施例的用于控制无线网络访问的装置的示意图。图3所示的装置300可以利用软件、硬件(例如集成电路或DSP等)或软硬件结合的方式来实现。图3的装置300的一个例子可以是上述图1A中的AP 110A或者图1B中的AP 110B、AP 110C、或者图1C中的AP控制器140。

[0079] 如图3所示，装置300包括获取模块310、判断模块320和控制模块330。获取模块310用于获取至少一个第二无线网络的关联信息，关联信息用于指示当前连接到至少一个第二无线网络的用户设备。判断模块320用于基于关联信息，确定是否满足控制条件，控制条件包括指定用户设备已经连接到至少一个第二无线网络。控制模块330用于基于判断模块320关于是否满足控制条件的确定结果，控制第一用户设备与第一无线网络之间的连接。

[0080] 在一种实现方式中，获取模块310进一步用于从公共存储资源读取由至少一个第二无线网络存储的关联信息。

[0081] 在另一实现方式中，获取模块310进一步用于获取关联信息，其中关联信息是从至少一个第二无线网络接收的。

[0082] 在另一实现方式中，控制模块330进一步用于准许第一用户设备与第一无线网络之间的连接；或者拒绝第一用户设备与第一无线网络之间的连接。

[0083] 在另一实现方式中，为了准许第一用户设备与第一无线网络之间的连接，控制模块330进一步用于执行以下各项操作中的至少一项：激活第一无线网络；或者启用第一无线网络的白名单，白名单包括第一用户设备，其中白名单所包括的用户设备对第一无线网络具有访问权限。

[0084] 在另一实现方式中，为了拒绝第一用户设备与第一无线网络之间的连接，控制模块330进一步用于执行以下各项操作中的至少一项：去激活第一无线网络；或者启用第一无线网络的黑名单，其中黑名单包括第一用户设备，其中，黑名单所包括的用户设备对第一无线网络不具有访问权限。

[0085] 现在参见图4，其是根据本发明一个实施例的用于控制无线网络访问的装置的示意图。如图4所示，装置400可以包括用于存储可执行指令的存储器410和与存储器410连接的处理器420，其中，处理器420可以执行前述装置300的各个模块所执行的操作。

[0086] 本发明实施例还提供一种机器可读介质，其上存储可执行指令，当该可执行指令被执行时，使得机器实现处理器420的操作。

[0087] 上文通过附图和优选实施例对本发明进行了详细展示和说明，然而本发明不限于这些已揭示的实施例，本领域技术人员从中推导出来的其它方案也在本发明的保护范围之内。

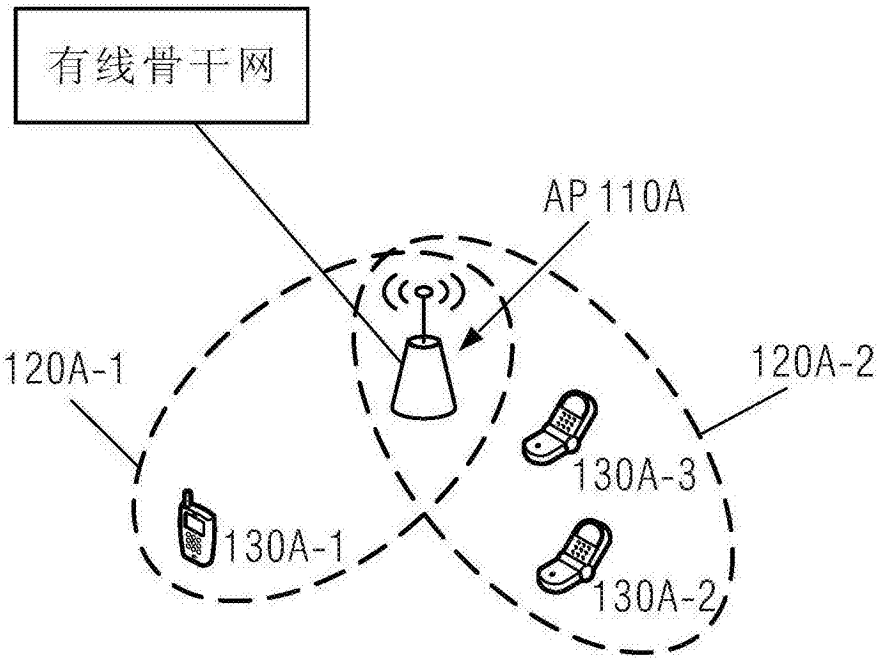

有线骨干网
AP 110A
120A-1
120A-2
130A-3
130A-1
130A-2

图1A

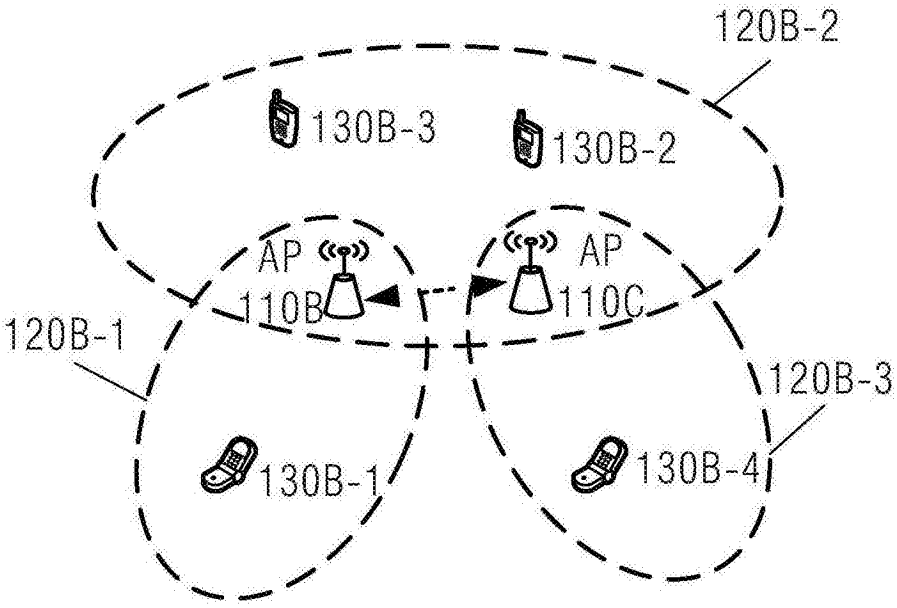

120B-2
130B-3
130B-2
AP
110B
AP
110C
120B-1
120B-3
130B-1
130B-4

图1B

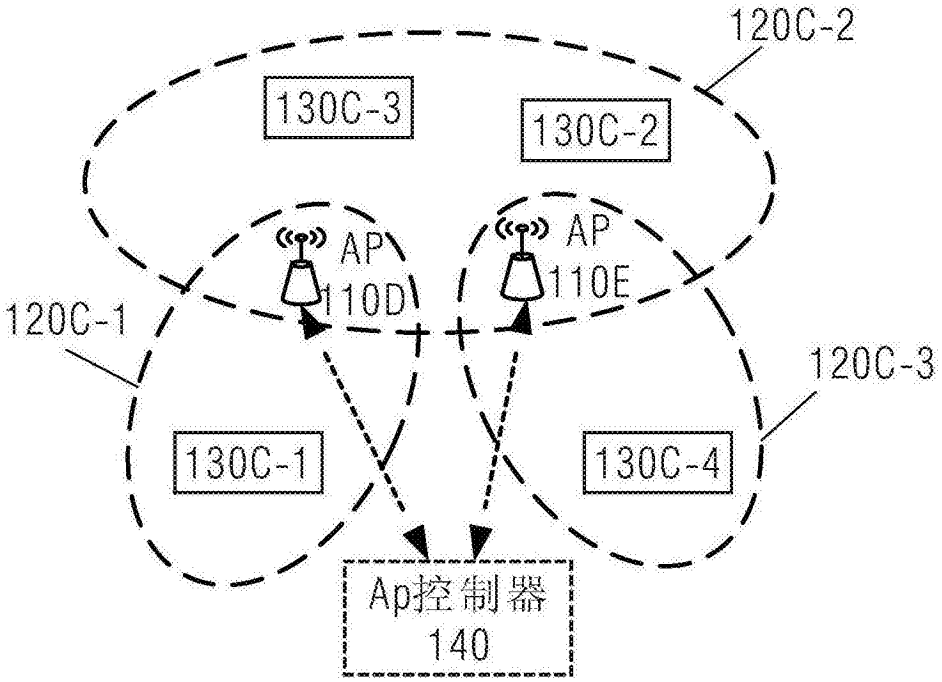

120C-2
130C-3
130C-2
AP
110D
AP
110E
120C-1
120C-3
130C-1
130C-4
Ap控制器
140

图1C

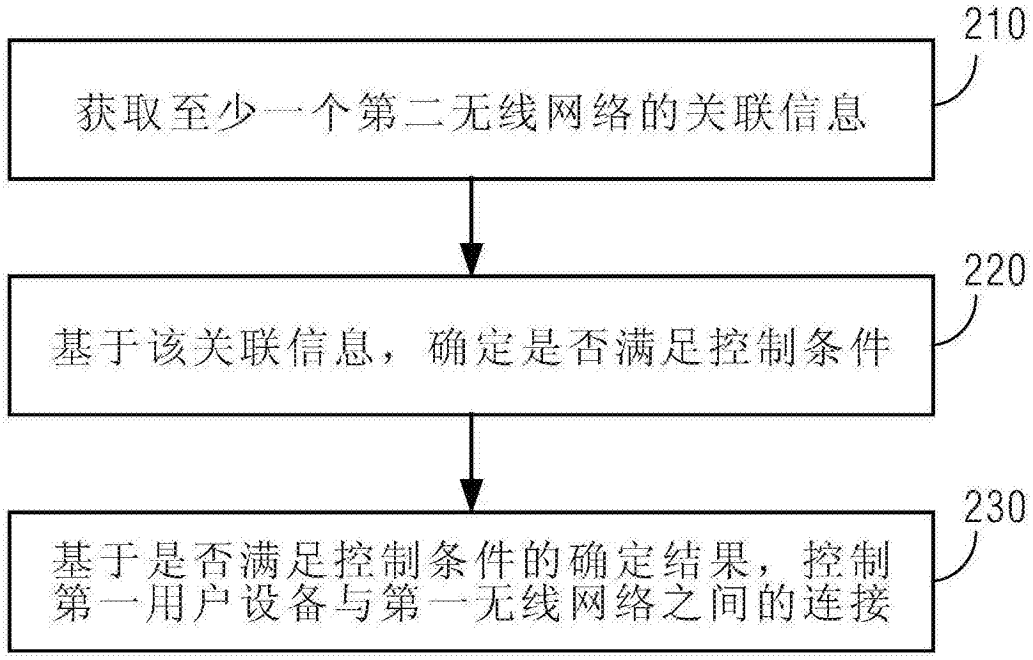

210
获取至少一个第二无线网络的关联信息
220
基于该关联信息，确定是否满足控制条件
230
基于是否满足控制条件的确定结果，控制第一用户设备与第一无线网络之间的连接

图2

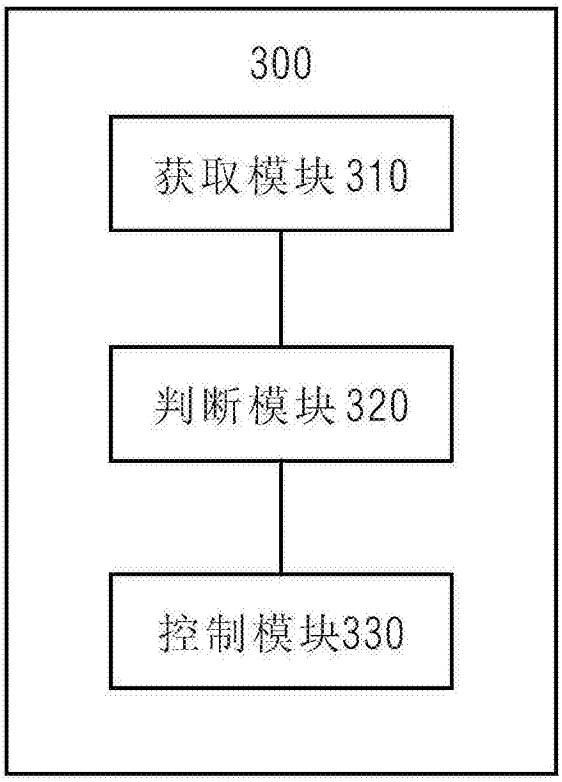


图3

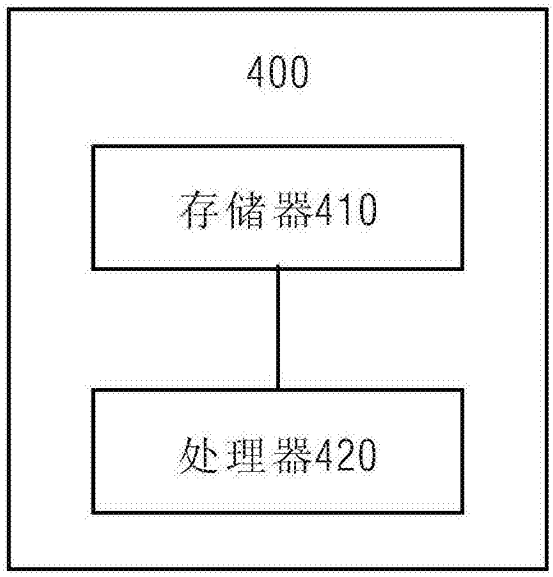


图4