[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00
H04L 9/12

[12] 发明专利申请公开说明书

[21] 申请号 200410006804.9

[43] 公开日 2004 年 10 月 13 日

[11] 公开号 CN 1536808A

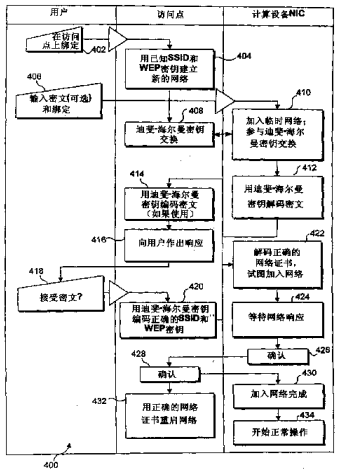
[22] 申请日 2004.2.18
[21] 申请号 200410006804.9
[30] 优先权
[32] 2003. 2.20 [33] US [31] 10/370，192
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 C·M·拉扎斯
M·D·奇尔德斯顿
N·R·S·马利克
[74] 专利代理机构 上海专利商标事务所
代理人 张政权

权利要求书 5 页 说明书 13 页 附图 7 页

[54] 发明名称 简化加密网络的装置和方法

[57] 摘要

以最少的用户交互动作使计算设备能够连接到安全网络。 计算设备的用户或授权能控制对安全网络的访问的人能够发起绑定步骤，以使计算设备能够加入网络。 然后在网络的访问点和计算设备网络接口卡(NIC)之间建立临时的备用网络。 然后把网络证书(可任选地是加密的)发送到计算设备 NIC。 由计算设备 NIC 对这些参数解密(如果它们是加密的)并利用这些解密的参数来连接到安全网络。 任选地，可以把一密文加密并传送到访问点，并在访问点提供这些参数给计算设备之前被验证。 该密文确保第三方不会被不正当地授权访问安全网络。



ISSN1008-4274

1．一种用于将计算设备加入安全网络的方法，其特征在于，包括以下步骤：

使用户发起将计算设备加入到安全网络的过程；

响应于将计算设备加入到安全网络的发起过程，在计算设备和安全网络的访问点之间建立备用的通信链路；

将加入安全网络所必须的证书发送到计算设备；以及

使用由计算设备所接收的证书来将该计算设备加入到安全网络。

2．如权利要求 1 所述的方法，其特征在于，还包括以下步骤：

对安全网络上的通信所需的证书进行加密，建立加密的消息；

在备用网络上将加密的消息传送给计算设备；以及

在计算设备处解密所述加密的消息以恢复证书。

3．如权利要求 2 所述的方法，其特征在于，还包括以下步骤：

确定加密密钥，该加密密钥用于加密证书以建立加密的消息，并用于对加密的消息进行解密以恢复证书。

4．如权利要求 2 所述的方法，其特征在于，使用公共和私有密钥组合来加密和解密证书。

5．如权利要求 2 所述的方法，其特征在于，使用迪斐-海尔曼密钥交换来加密和解密证书。

6．如权利要求 1 所述的方法，其特征在于，还包括以下步骤：

使用户在计算设备上输入密文，所述密文对于访问点处的被授权能够选择性地使计算设备加入安全网络的人来说是已知的；

在计算设备处加密该密文，生成加密的密文消息；

将该加密的密文消息传送给访问点；以及

在访问点对该加密的密文消息解密以恢复密文，使得所述的人能够判断如此恢复出的密文是否正确，从而防止可能截取备用网络上的通信的中间第三方被不正当地授权以在安全网络上通信。

7．如权利要求 1 所述的方法，其特征在于，还包括使用户通过计算设备

发起加入安全网络的过程的步骤。

8．如权利要求 1 所述的方法，其特征在于，还包括使用户通过访问点发起加入安全网络的过程的步骤。

9．一种存储有用于执行权利要求 1 的步骤的机器指令的存储媒体。

10．一种用于有选择地自动地使计算设备加入安全网络的方法，其特征在于，包括以下步骤：

在计算设备和安全网络上使用的访问点上启动绑定选项的激活；

响应于绑定选项被激活，自动地在计算设备和访问点之间产生安全的加密通信链路；

在得到将计算设备加入安全网络的授权许可之后，选择性地将安全加密消息从访问点传送到计算设备，所述加密消息传递将计算设备加入安全网络所需的证书；

在计算设备处对加密消息进行解密以恢复证书；

在计算设备处使用证书来将计算设备加入到安全网络。

11．如权利要求 10 所述的方法，其特征在于，自动地产生加密的无线网络的步骤包括产生用于在加密的通信链路上的通信的加密密钥的步骤。

12．如权利要求 10 所述的方法，其特征在于，还包括以下步骤：

使用户在计算设备上输入密文，所述密文对于能够选择性地授权计算设备加入安全网络的人来说是已知的；

在传送给访问点的安全的加密消息中加密该密文；以及

在访问点对该安全的加密消息解密以恢复密文，使得所述人能够判断已知的密文是否被实际恢复，如果没有，则防止可能已截取该加密消息的中间第三方被不正当地授权以在安全网络上通信。

13．如权利要求 10 所述的方法，其特征在于，所述自动地产生加密的通信链路的步骤包括采用迪斐-海尔曼密钥交换的步骤。

14．如权利要求 10 所述的方法，其特征在于，自动地产生加密的通信链路的步骤包括采用私有/公共密钥用于加密和解密通信信息的步骤。

15．如权利要求 10 所述的方法，其特征在于，还包括当把计算设备加入到安全网络时中断该安全网络上的其它通信的步骤。

16. 如权利要求 10 所述的方法，其特征在于，所述

启动绑定选项的激活的步骤包括显示图形用户界面选项来将计算设备绑定到安全网络的步骤。

17. 如权利要求 10 所述的方法，其特征在于，所述证书包括服务设置标识符 SSID 和线路等效保密 WEP 密钥。

18. 如权利要求 10 所述的方法，其特征在于，所述证书包括无线保护访问 WPA 密钥。

19. 一种存储有用于执行权利要求 10 的步骤的机器指令的存储媒体。

20. 一种用于加入安全网络的系统，包括：

存储有多条机器指令的存储器；

网络通信接口；以及

耦合至存储器和网络通信接口的处理器，所述处理器执行所述机器指令，使得所述处理器执行多个功能，这些功能包括：

使用户发起将计算设备加入到安全网络的过程；

参与在计算设备和安全网络的访问点之间建立备用的通信链路；

接收来自访问点的在备用的通信链路上加入安全网络所需的证书；以及

在计算设备上使用证书来将计算设备加入到安全网络。

21. 如权利要求 20 所述的系统，其特征在于，所述机器指令还使得所述处理器对来自访问点的用于在安全加密消息中向计算设备传递证书的加密消息进行解密。

22. 如权利要求 20 所述的系统，其特征在于，所述网络接口包括无线网络通信设备。

23. 如权利要求 20 所述的系统，其特征在于，所述机器指令还使得所述处理器使用户输入密文，该密文被包含于在备用通信链路上向访问点的安全的加密传送中，所述密文对于授权能许可计算设备加入安全网络的人来说是已知的。

24. 如权利要求 20 所述的系统，其特征在于，所述机器指令使得所述处理器能够使用迪斐-海尔曼密钥交换与访问点建立备用通信链路。

25. 如权利要求 20 所述的系统，其特征在于，所述机器指令使得所述处理器能够使用私有/公共密钥与访问点建立备用通信链路。

26. 如权利要求 20 所述的系统，其特征在于，还包括显示器，其中所述机器指令还使得所述处理器在所述显示器上的用户界面中显示绑定选项，可选择性地激活所述绑定选项来发起对安全网络的连接。

27. 如权利要求 20 所述的系统，其特征在于，所述证书包括服务设置标识符 SSID 和线路等效保密 WEP 密钥。

28. 如权利要求 20 所述的系统，其特征在于，所述证书包括无线保护访问 WPA 密钥。

29. 一种用于便于将计算设备加入安全网络的系统，其特征在于，包括：

存储有多条机器指令的存储器；

网络通信接口；以及

耦合至存储器和网络通信接口的处理器，所述处理器执行所述机器指令，使得所述处理器执行多个功能，所述功能包括：

使用户能发起将计算设备加入到安全网络的过程；

参与建立与计算设备的备用通信链路；

使用该备用通信链路，向计算设备发送在安全网络上通信所需的证书；以及

使用证书，响应于计算设备的加入请求，将计算设备加入到安全网络。

30. 如权利要求 29 所述的系统，其特征在于，所述处理器、网络通信接口、存储器组成安全网络上的访问点。

31. 如权利要求 29 所述的系统，其特征在于，所述机器指令还使得所述处理器加密证书，以生成在所述备用通信链路上传送给计算设备的加密的消息。

32. 如权利要求 29 所述的系统，其特征在于，所述机器指令还使得所述处理器：

接收来自计算设备的传递密文的加密消息；

对该加密消息解密以恢复密文；以及

将密文与已知密文比较，如果密文与已知密文匹配，则选择性地确定要把证书传送给计算设备，并且如果密文与已知密文不匹配，则检测未经授权的第三方试图加入安全网络。

33. 如权利要求 29 所述的系统，其特征在于，所述机器指令使得所述处理器能够使用迪斐-海尔曼密钥交换与计算设备建立备用通信链路。

34. 如权利要求 24 所述的系统，其特征在于，所述机器指令使得所述处理器能够使用私有/公共密钥与计算设备建立备用通信链路。

35. 如权利要求 29 所述的系统，其特征在于，还包括显示器，其中所述机器指令还使得所述处理器在所述显示器上的用户界面中显示绑定选项，可选择性地激活所述绑定选项来发起将计算设备加入到安全网络。

36. 如权利要求 29 所述的系统，其特征在于，所述证书包括服务设置标识符 SSID 和线路等效保密 WEP 密钥。

37. 如权利要求 29 所述的方法，其特征在于，所述证书包括无线保护访问 WPA 密钥。

简化加密网络的装置和方法

技术领域

本发明一般涉及将第一计算设备连接到网络，具体来说，涉及以最少的用户输入来启动由授权用户通过第二计算设备输入的判决以便于自动地将第一计算设备连接到加密安全网络，用户控制对该网络的存取访问。

背景技术

当在家庭和小型企业中使用无线网络用于将计算机和其它类型的计算设备互相连接或用于访问因特网时，无线网络一般不利用所用的无线网络接口卡（NIC）和访问点所配备的加密能力。大多数用户发现，对于家庭或小型企业来说，建立安全的加密网络太困难，因为与设置安全加密无线网络有关的任务常常不是这些用户所熟知的技能。即使最初建立了安全加密无线网络，但是当用户想对该安全加密无线网络添加新的计算机或其它设备时，就会产生问题。每次把一个新的计算机或其它类型的计算设备添加到安全加密无线网络时，用户必须打开该新设备上的无线NIC卡的用户接口，输入正确的网络名称以及在该网络上当前所采用的其它参数，并确定和输入正确的26个字符的网络密钥，以把该新的计算设备添加到安全加密无线网络。如果输入了错误的参数，例如错误的线路等效保密（WEP）密钥，该计算设备就不能成功地连接到安全无线网络。在经历了管理常规安全加密无线网络的挫折之后，大多数用户仅仅把他们的网络运行于未加密模式，而没有任何加密安全保护。运行于先前未接触过的已有无线网络附近的计算机上当前的操作系统，如微软的 WINDOWS XP，会自动地检测无线网络，并且仅当该网络是未加密的情况下，能够无需提供配置参数而把计算机连接到该网络。虽然以这种方式连接未加密的无线网络是非常便捷的，但是它使得网络过于开放，从而具有无线访问接口设备的计算机的未授权的用户无需获得许可就能够方便地加入无线网络。结果，网络用户的私有文件可被在该无线网络范围内的未授权的用户访问。

可以清楚地看到，希望以安全的加密模式来运行无线网络以避免他人的未授

权的访问。然而，大多数无线网络组件的制造商以设置用于未加密操作的默认模式来经销他们的产品。为了使用户更容易地加入加密网络，某些现有技术无线 NIC 或其它无线网络接口设备允许用户输入一短语，随后以预定的算法对该短语进行散列，来确定网络的加密密钥。只要无线网络上的所有无线网络组件都是同一个制造商的，如果用户正确地想起并输入先前所选择的短语，该方法就会提供正确的 WEP 密钥。然而，使用短语来确定网络密钥同样使黑客能够获得访问安全的加密无线网络的机会。此外，无线网络产品的不同制造商使用不同的散列算法，从而在不同制造商的无线网络产品上输入正确的短语可能不会导致该设备确定出正确的网络密钥。

近来，Wi-Fi 联盟已开始发展 802.11i 标准的无线保护访问（WPA）规范，将用于数据加密和网络访问控制。对于加密来说，WPA 采用暂时密钥完整性协议（TKIP），它使用与 WEP 相同的算法，但以不同的方式构成网络密钥并提供改进的网络安全性。对于访问控制，WPA 将使用 IEEE 802.1x 协议，该协议是最近刚完成的标准，用于控制对有线和无线 LAN 的登录。在要对 WPA 采用的方法中，各用户将具有其自己的加密密钥，该密钥可被设置成周期性地改变。在公司环境中，可由鉴别服务器来处理鉴别，从而比能够使用 WEP 密钥的用户还多的用户能够得到处理。对于较小的或家庭网络，可使用“预共享密钥”模式，它不需要鉴别服务器，并且如果用户系统上的预共享密钥与无线访问点的密钥匹配，则用户就能够登录到网络。

虽然在最初建立安全加密无线网络（这是微软公司生产的无线组件的默认模式）和在提高加密的网络的安全性方面取得了进步，但是仍然存在有关把新的计算设备连接到安全加密无线网络的问题。因此，显然需要更简单的方法来将新的计算设备连接到无线网络，避免用户回忆或输入 WEP 或 WPA 密钥，并仅仅需要授权控制对无线网络访问的人来判决是否允许把该新的计算设备连接到安全网络。希望以规定的或限制的时间来授权新的设备连接到安全无线网络。当向新的计算设备提供连接到安全无线网络所必须的参数时，该新的计算设备与用于控制访问安全无线网络的访问点之间的通信也应该是安全的，并且最好采取步骤来阻止第三方截取通信和伪装成能够连接到该安全无线网络的该新的计算设备的用户。可以清楚地看到，该方法不限于安全无线网络，而是适用于其它类型的安全网络。

发明内容

采用本发明来使将计算设备连接到现有安全网络的过程自动化。作为要求控制对网络访问的人手工地提供标识符和安全密钥的替代，采用一种相对简化的自动化过程，它仅仅要求计算设备的用户或授权加入网络的许可的人非常少的输入。希望加入网络的计算设备的用户或者授权能许可计算设备加入网络的人能够发起该自动化的过程。在计算设备上和安全网络上的访问点上，激活绑定选项。响应于该激活的绑定选项，在计算设备和访问点之间自动地产生了安全的加密通信链路。假设授权允许计算设备加入网络，安全的加密消息较佳地是从访问点发送到计算设备。加密的消息传递计算设备加入安全网络所需的证书。计算设备对该加密消息进行解密，以恢复加入网络所需的证书，如 SSID 和 WEP 密钥或 WPA 密钥。然后，计算设备使用证书连接到安全网络。

自动地产生加密的无线网络的步骤较佳地包括产生在加密的通信链路上的通信中所使用的加密密钥。例如，该加密密钥可以是来自私有/公共密钥集的私有密钥，或可以是使用迪斐-海尔曼（Diffie-Hellman）密钥交换而产生的密钥。

任选地，可以有用户在计算设备上输入密文。该密文对于授权将计算设备加入到安全网络的人来说也是已知的。该密文包含于发送到访问点的安全的加密消息中，在访问点加密的消息被解密以恢复密文。位于访问点的授权将计算设备连接到网络的人（处于访问点）能够确定所知的密文是否是从加密的消息中实际恢复的。如果不是，中间的第三方就可能已截取该加密的消息，通过检测该截取和诡计企图，就可以防止第三方加入该安全网络。

除非安全网络使用允许网络上并行通信链路的协议，当把计算设备连接到安全网络时，安全网络上的正常通信将中断。

较佳地，启动绑定选项激活的步骤将包括显示图形用户界面选项，以把计算设备绑定到安全网络。

本发明的另一方面针对用于允许加入安全网络的系统。该系统包括存储有机器指令的存储器和网络通信接口。处理器耦合至该网络通信接口和存储器，并执行机器指令，使得处理器执行与上述方法中的计算设备所实施的功能一致的功能。类似地，根据本发明的一种能够使计算设备加入安全网络的系统包括存储器、网络通信接口、以及执行机器指令的处理器，使得处理器执行与上述

方法所描述的访问点所执行的方法步骤相对应的功能。

附图说明

参考下述结合附图的详细描述，将能够更容易地理解和明白本发明的上述诸方面和附带的许多优点。附图中：

图 1 是适用于实施本发明的示例性计算环境的示意性框图；

图 2 是本发明可适用的示例性安全无线网络的框图；

图 3 是实施本发明的以及用于将计算设备连接到安全无线网络的网络访问设备的轴测图；

图 4 是实施本发明的访问点的轴测图；

图 5 是一般地说明为加入安全无线网络而响应于计算设备（或计算设备的 NIC）上的绑定“按钮”被激活而执行的步骤的示图；

图 6 是一般地说明起动计算设备连接到安全无线网络，而响应于访问点上的绑定“按钮”被激活而执行的步骤的示图；

图 7 是说明根据本发明将计算设备连接到安全无线网络所执行的步骤的详细示图；

图 8A 是包括用于起动将计算设备连接到安全无线网络的绑定控制的访问点的示例性图形用户界面；以及

图 8B 是包括用于起动将计算设备连接到安全无线网络的绑定控制的 NIC（或与无线网络通信的其它设备）的示例性图形用户界面。

具体实施方式

示例性的操作环境

图 1 以及下面的讨论意图提供对实施本发明的合适的计算环境的简要的、全面的描述。虽然并非必要，但是将用如无线访问设备和/或计算设备所执行的程序模块之类的计算机可执行指令的一般环境来描述本发明的一部分，这些无线访问设备和/或计算设备例如带有网络接口卡或类似组件的个人计算机（PC）。一般来说，程序模块包括例行程序、程序、对象、组件、数据结构等等，他们执行特定的任务或实现特定的抽象数据类型。除了把 PC 连接到安全

无线网络之外，本领域的技术人员将理解到可以采用本发明来把其它计算设备连接到安全无线网络，这些设备包括游戏控制台、电视机机顶盒、多处理器系统、网络个人计算机、小型计算机、大型计算机、工业控制设备、汽车设备、航空设备、外围设备、手持设备、袖珍个人计算设备、适于连接到网络的数字蜂窝电话、以及其它基于微处理器的或可编程的消费电子产品。还可以在分布式计算环境中实施本发明，在分布式计算环境中，由通过通信网络链接的远程处理设备来执行任务。在分布式计算环境中，程序模块可位于本地和远程存储设备中。

参考图 1，用于实施本发明的示例性的计算环境包括通用 PC 20 形式的通用计算设备。PC 20 配备有处理单元 21、系统存储器 22 以及系统总线 23。系统总线将包括系统存储器的各种系统组件连接到处理单元 21，并可以是各种总线结构中的任一种类型，包括存储器总线或存储器控制器、外围总线、使用多种总线结构体系中的任一种的局部总线。系统存储器包括只读存储器（ROM）24 和随机存取存储器（RAM）25。基本输入/输出（BIOS）系统 26 存储在 ROM 24 中，BIOS 中包含了诸如在启动期间运行的基本例行程序以帮助在 PC 20 内部的元件之间传送信息。

PC 20 还包括用于对硬盘（未示出）进行读写的硬盘驱动器 27、用于对可移除的磁盘 29 进行读写的磁盘驱动器 28、以及用于对诸如光盘只读存储器（CD-ROM）或其它光媒体之类的可移除的光盘 31 进行读写的光盘驱动器 30。硬盘驱动器 27、磁盘驱动器 28 以及光盘驱动器 30 分别通过硬盘驱动器接口 32、磁盘驱动器接口 33 以及光盘驱动器接口 34 而连接到系统总线 23。各驱动器及其相关的计算机可读媒体提供对用于 PC 20 的计算机可读机器指令、数据结构、程序模块以及其它数据的非易失性存储。虽然这里所描述的示例性环境采用硬盘、可移除的磁盘 29 和可移除的光盘 31，但是本领域的技术人员应理解到在示例性操作环境中还可以使用能够存储可由计算机存取访问的数据的其它类型的计算机可读媒体，如磁带盒、闪存卡、数字视频盘、贝努利（Bernoulli）盒式磁带、随机存取存储器（RAM）、ROM 等等。可在硬盘、磁盘 29、光盘 31、ROM 24 或 RAM 25 上存储若干程序模块，包括操作系统 35（任选地可包括一个或多个设备驱动器）、一个或多个应用程序 36（如启动程序）、

其它程序模块 37 以及程序数据 38。

用户可通过诸如键盘 40 和指针设备 42 之类的输入设备向 PC 20 输入命令和信息。其它输入设备（未示出）可包括话筒、操纵杆、游戏手柄、卫星反射器、扫描仪、数字照相机等等。这些或其它输入设备通常通过耦合至系统总线的输入/输出（I/O）设备接口 46 而连接到处理单元 21。诸如打印机（未示出）之类的输出设备也可通过耦合至系统总线的 I/O 设备接口 46 而连接到处理单元 21。术语“I/O 设备接口”意图包含用于串行端口、并行端口、游戏端口、键盘端口、PS/2 端口、USB 端口和/或其它 I/O 端口的各种接口。类似地，监视器 47 或其它类型的显示设备也可通过诸如视频适配器 48 之类的适当接口而连接到系统总线 23，并可用于显示图形用户界面、应用程序界面、Web 网页和/或其它信息。除了监视器之外，PC 通常还连接到其它外围输出设备（未示出），如扬声器（通过声卡或其它音频接口（未示出））。

PC 20 较佳地工作于使用对一个或多个远地的其它计算设备的逻辑连接的联网环境中，这些远程计算设备诸如其它局域网（LAN）计算机或在安全无线网络中连接在一起的计算设备（在本图中未示出），也可能是通过有线网络连接的其它计算设备，如远程计算机 50。其它 LAN 计算机和远程计算机 50 一般可以是另一台 PC、和/或服务器，并一般配置成非常类似于 PC 20。可在安全无线网络中连接的其它类型的计算设备至少还包括处理器和用于存储机器指令的存储器。对其它计算设备的逻辑连接还包括诸如因特网之类的广域网（WAN）52，它较佳地使用诸如 TCP/IP 之类的已知的 WAN 协议。这些联网环境在办公室、企业范围的计算机网络、企业内部互联网以及因特网之中是常见的。

当用于 LAN 联网环境时，PC 20 通过网络接口或适配器 53，也可以是无线 NIC，连接到 LAN 段 51。当用于 WAN 联网环境时，PC 20 一般通过调制解调器 54 或其它装置在 WAN 52 上建立通信连接。调制解调器 54，它可以是外置的或内置的，但出于示例性的目的，下述的调制解调器主要是宽带调制解调器，如 xDSL 调制解调器、电缆调制解调器或其它高速调制解调器。PC 20 通常通过 LAN 段 51、网关 55 以及 WAN 段 56 而从外部连接到调制解调器 54。WAN 段 56 一般包括标准 LAN 段，但较佳地是仅包括访问 WAN 52 的 LAN 段。将理解到所示的网络连接是示例性的，可使用用于在通信中链接计算机的其它手段。在许多情

况下，PC 20 是膝上型或其它类型的便携式计算设备，网络接口 53 将包括个人计算机存储器卡国际协会（PCMCIA）NIC 卡，该卡包括用于与访问点进行无线通信的电子电路。应注意到 PC 20 还可通过网络接口 53（一般是以太网端口）连接到访问点（未示出），并将用于显示用户界面对话框，便于通过 PC 20 授权能够使另一计算设备连接到安全无线网络。

示例性安全无线网络

虽然本发明不限于使用无线网络，但本发明可能最初被用于连接计算设备到这样的一种网络上。然而，必须强调的是，可采用本发明来把计算设备连接到几乎任何类型的安全网络，下面关于用于无线网络的描述并不是对本发明的限制。

图 2 例示了示例性的安全无线网络 100。在该相对简单的示例性无线网络中，较佳地是通过以太网电缆 109 把访问点 102 耦合到交换器和网关的组合体 110。访问点 102 包括传送和接收用于在安全无线网络 100 上通信的无线信号的天线 104。例如，访问点可使用符合电气和电子工程师协会（IEEE）802.11b 规范、802.11a 规范、80211g 规范或其它适当的无线网络规范的射频信号进行通信。PC 106 耦合至网关和交换器 110 的另一以太网端口，但还可通过诸如安装在 PC 106 内的总线上的无线通信卡之类的无线连接来进行耦合连接。提供显示器 108 用于向 PC 106 的用户显示图形和文本。

还考虑到，除了直接连接到网关和交换器 110 之外，访问点 102 可通过以太网电缆 109'而连接到 PC 106 的另一以太网端口（未示出）。在任何一种情况下，可由 PC 106 的用户（或通过使用安全无线网络的任何其它 PC 而由授权用户），使用管理程序或显示对访问点 102 的超文本标记语言（HTML）图形用户界面的 Web 浏览器界面来方便地进行管理。由于通过管理接口对无线网络进行改变会干扰计算机和访问点之间的通信，一般较佳的是使用具有对访问点直接线缆连接的计算机来管理访问点。如果通过以太网电缆而直接连接，在管理接口中对无线网络的改变就不可能产生计算机和访问点之间的通信损失。网关和交换器 110 一般还连接到电缆调制解调器或 ADSL 调制解调器，从而安全无线网络 100 可对因特网（或其它形式的公共或私有 WAN）进行宽带访问。

虽然安全无线网络可包括多个访问点，但如图 2 所示的简化的安全无线网

络仅具有一个访问点 102。该访问点提供与网络中的一个或多个其它计算设备进行安全无线通信。例如，包括外部天线 122 的无线网络接口设备 120 使用可任选地周期性改变的 WEP 密钥在安全无线网络上与访问点 102 通信。无线接口设备 120 包括可选的绑定按钮 124，下文会解释其功能。USB（或以太网）电缆 126 将无线网络接口设备连接到 PC 128，使得该 PC 能够通过访问点 102 在安全无线网络上与 PC 106(以及已连接到网络的其它计算设备)通信。PC 128 还连接到显示器 130。此外，PC 128 可宽带访问连有网关和交换器 110 的因特网（或其它 WAN）。

虽然本发明可能最初用于将诸如 PC 之类的计算设备连接到安全无线网络，但是还考虑到本发明可用于将其它类型的计算设备连接到安全无线网络。例如，如图 2 所示，蜂窝电话 132 也可连接到安全无线网络。同样显而易见的是，可使用诸如蓝牙之类的其它协议把蜂窝电话 132 连接到安全网络。根据本发明，诸如个人数字助理（PDA）、机顶盒、电子游戏机、娱乐设备、以及各种设备也同样都可连接到安全网络。

本发明便于将当前没有连接的计算设备连接到安全无线网络 100，使得该设备能够通过安全无线网络进行安全的无线通信。在图 2 所示的例子中，本发明可使示为具有显示器 116 的膝上型或便携式 PC 的客户计算机 112 以最少的用户交互动作来连接到安全无线网络 100。关于 PC 112 的术语“客户计算机”并非是限制性的，因为 PC 112 可以是以通常永久的方式正被加入安全无线网络的一台新的计算机。然而，由于对于具有便携式 PC 的朋友来说，访问一可运行安全无线网络 100 的住宅并希望将其 PC 连接到该无线网络以进行宽带因特网通信和/或与连接到该无线网络的其它计算机或计算设备通信，这是非常普通的，因此，在该例子中使用了该术语。在商业环境中，PC 112 可被看作为正被加入商业安全网络的另一台计算设备。如下所述，本发明使 PC 112 自动地连接到无线网络，PC 112 的用户无需知道为了将 PC 112 连接到网络而由安全网络所使用的 SSID 或 WEP 密钥(或 WPA 密钥)。PC 112 的用户和授权确定 PC 112 是否能够连接到安全无线网络 100 的人（可以是同一人）不需要记得在无线网络上所使用的 SSID 或 WEP 或 WPA 密钥。下面解释了关于自动地将 PC 112 连接到安全网络的步骤的细节。

图 3 示出了通过 USB 电缆 126 连接到 USB 连接器 140 的无线网络接口设备 120 的进一步细节。作为替代，USB 电缆 126 可用以太网电缆替代，而连接器可用适当的以太网连接器替代，以用于连接至计算设备上的 LAN 卡上的以太网端口。

图 4 例示了访问点 102 的进一步细节，它包括绑定按钮 142，该绑定按钮可选地包含于访问点 102 上，能够由授权确定另一计算设备是否能连接到安全无线网络的人来激活。除了使用无线网络接口设备 120 上的绑定按钮 124 或访问点 102 上的绑定按钮 142 之外，可以向连接至该访问点或无线网络接口设备的相关计算设备的用户显示图形用户界面中的软件绑定控制。可由用户选择性地激活软件绑定控制，以实现将计算设备连接到一临时的安全无线网络。

图 5 中所示的诸步骤 200 解释了当用户按下要被连接到安全无线网络的计算设备的无线网络接口设备 120 上的绑定按钮 124 或激活无线网络接口设备的图形用户界面上的软件绑定控制而启动过程时，本发明是如何用于将计算设备连接到安全无线网络的。在步骤 202 中选择绑定选项，使得在计算设备无线 NIC 上实施步骤 204。如这里所使用的，术语“NIC”意图包含插入通用 PC 的总线的类型的内部无线网络接口卡、通过 USB、以太网或其它通信端口连接到计算设备的网络接口设备、以及为计算设备提供无线接口的 PCMCIA 卡 114，如图 2 中所示的 PCMCIA 卡 114。

响应于用户所希望加入安全无线网络的计算设备上的绑定控制在步骤 204 被激活，绑定信号 206 就被传送到访问点。在步骤 208 中，授权能够确定是否将允许该计算设备连接到安全无线网络的人就随后能够选择性地按下绑定按钮。绑定按钮可以是硬件绑定按钮 142 或软件绑定控制。如果该人选择性地激活了该绑定控制，则在访问点执行绑定步骤 210。相应地，访问点将一绑定信号 212 发送回所述要连接到安全无线网络的计算设备。接着，步骤 214 执行密钥交换，以发起从访问点到计算设备的安全传送。密钥交换产生了一个加密密钥，使得访问点在步骤 216 中能够向计算设备发送传达 SSID 和 WEP 密钥的加密消息。在步骤 218 中，计算设备对 SSID 和 WEP 密钥进行解密，并确认对这些参数的接收。最后，访问点将确认消息 220 传送到计算设备。然后在步骤 222，计算设备使用其接收的来自访问点的 SSID 和 WEP 密钥进行对无线网络的连

接。在步骤224，访问点响应于发送到计算设备的SSID和WEP的传送，并接受所述连接，使得计算设备当前被加入到安全无线网络。现在，计算设备可与访问点和组成该安全无线网络的其它计算设备进行通信，并能够对该安全无线网络上所提供的其它网络连接进行访问。作为替代，在本发明中可使用 WPA 密钥或其它类型的网络证书，来自动地加入到使用该形式的证书的安全无线网络。

图6中所示的诸步骤300解释了当在访问点启动过程时，是如何把计算设备连接到安全无线网络的。在步骤302中，授权以确定计算设备是否将加入安全网络的人按下绑定按钮或选择该访问点的图形用户界面中的绑定控制。作为响应，绑定步骤304使得访问点向计算设备发送绑定信号306。接着，在步骤308，计算设备的用户（可以是与在步骤 302 中按下绑定按钮的同一个人）按下绑定按钮或选择计算设备的图形用户界面中的绑定控制，使其无线NIC开始绑定步骤310。作为响应，计算设备无线NIC向访问点传送一绑定信号312。在步骤314，访问点和计算设备执行密钥交换，以在步骤316中，在从访问点向计算设备传送的加密消息中提供加密诸如SSID和WEP密钥之类的网络证书的加密密钥。然后，在步骤 318，计算设备对消息解密以恢复网络证书，并确认对网络证书的接收。作为响应，在步骤 320，访问点将一确认消息发送回计算设备。最终，在步骤 324，计算设备使用该网络证书来加入安全无线网络，以及在步骤322中，访问点接受该连接和加入。

虽然图5和图6一般地说明了根据本发明的将计算设备加入到安全无线网络的步骤，但是图7中的框图400示出了该过程的细节。如果授权能够将计算设备添加到安全无线网络的人启动该过程，块402提供了要被执行的绑定步骤，可通过按下绑定按钮或选择在访问点的图形用户界面中提供的绑定控制来开始。在步骤404中，仅当在建立了将计算设备连接到安全无线网络的同时，使用一个新的临时的备用网络；当把计算设备连接到常规安全网络时，该备用网络仅由访问设备和计算设备所使用。在该步骤期间，采用已知的SSID和WEP密钥（或其它已知证书）来建立访问点和计算设备之间的备用网络。访问点和计算设备NIC都必须知道在该访问点和计算设备之间的临时的备用网络中所采用的已知SSID和WEP。

作为替代，计算设备的用户能够发起绑定步骤。在步骤 406，用户任选地可输入诸如短语或字之类的密文，该密文对于该用户和授权能够将该计算设备加入安全无线网络的人来说都是已知的。使用常规的键盘或其它输入设备将该密文输入到计算设备上。如果计算设备的用户发起了该过程，则授权能够确定是否要把该计算设备加入到安全网络的人将遵循步骤 402。在任一种情况下，在建立了新的临时的备用网络之后，步骤 408 提供访问点和计算设备 NIC 卡执行迪斐-海尔曼（Diffie-Hellman）密钥交换。迪斐-海尔曼密钥交换对于确定加密密钥来说是较佳的，该加密密钥将用于在步骤 404 中建立的备用网络上，以使得访问点产生加密消息来将 SSID 和 WEP 密钥传送给计算设备。然后，计算设备使用密钥对消息解密以恢复网络证书，如 SSID 和 WEP 密钥。然而，还要考虑到私有/公共密钥集也可用于加密/解密步骤。

在步骤 410 中，计算设备加入由访问点在步骤 404 建立的临时的备用网络。此外，计算设备参与与访问点的迪斐-海尔曼密钥交换。接着，在步骤 412 中，计算设备使用已开发的迪斐-海尔曼密钥来对密文（如果它被使用）进行加密。提供由计算设备用迪斐-海尔曼密钥进行加密的密文的目的是，检测可能截取计算设备间的通信的第三方并防止第三方未经授权而加入该安全无线网络。由于只有计算设备的用户和授权能够使计算设备连接到安全无线网络的人知道密文，因此，第三方计算设备就不能成功地把它表示成被授权加入安全网络的计算设备。

如果使用密文，在步骤 414 中，在访问点使用迪斐-海尔曼密钥对该密文进行解密。然后在步骤 416 把该解密的密文呈现给授权能使计算设备连接到网络的人。在步骤 418 中，该人判断该密文是否被正确解密。如果该密文是正确的，则在步骤 420 中，访问点使用迪斐-海尔曼密钥对安全无线网络的正确的网络证书（如 SSID 和 WEP 密钥）进行加密。然后，含有网络证书的加密的消息经临时的备用网络被传送给计算设备 NIC，后者对该消息进行解密以恢复正确的网络证书。在步骤 422，计算设备 NIC 使用网络证书来加入安全无线网络。步骤 424 提供了计算设备 NIC 等待来自安全无线网络的响应。在步骤 426，计算设备向访问点发送确认消息，作为响应，访问点在步骤 428 将一确认消息发送回计算设备。在步骤 430 中，计算设备连接到安全无线网络。相应地，访问点响

应来自步骤 428 的确认消息，并在步骤 432 中以先前提供给计算设备的正确的网络证书（如 SSID 和 WEP 密钥，或 WPA 密钥）重启安全无线网络。此后，在步骤 434 中，计算设备开始正常的操作，能够与安全无线网络上的各个其它计算设备通信，并在可能的情况下访问宽带连接。

如果授权能将计算设备连接到安全无线网络的人决定拒绝这种连接企图，则可以通过不进行在步骤 404 将计算设备绑定到临时的备用网络而中断该过程。作为替代，在步骤 418 中，该人可以选择不接受密文或在步骤 420 中不传送把计算设备加入安全无线网络所需的加密的网络证书（如 SSID 和 WEP 密钥或 WPA 密钥）。密文的使用防止了未被真正授权的第三方使用诡计来连接安全无线网络。作为替代，计算设备可以使用由受信任的第三方（如 VeriSign 公司）的验证证书把核准的数字签名发送给访问点。

图 8A 例示了包含绑定控制 442 和退出控制 444 的图形用户界面对话框 440。图 8A 中所示的图形用户界面对话框设于管理访问点的 PC 或其它计算设备上。应理解到图形用户界面对话框 440 仅仅是示例性的，可以替换地采用许多不同的形式和格式来使用户将计算设备绑定到安全无线网络。如果计算设备的用户已发起将计算设备连接到安全无线网络，则列表框 446 将示出计算设备。在多个此类设备请求加入安全无线网络而待决的情况下，管理访问点的用户可以在选择性地激活绑定控制 442 之前选择列表框 446 中所包含的计算设备之一。

图 8B 例示了向计算设备的用户显示的示例性用户界面对话框 450，以便于连接到安全无线网络。计算设备的 NIC 会检测和识别在列表框 452 中运行的任何可访问的无线网络。图示了一个名为“工作组”的示例性安全无线网络。用户可随后通过选择绑定控制 456 发起连接过程，或通过激活绑定控制 456 来响应访问点向计算设备发送绑定信号。还提供了退出控制 458。由于公司环境可具有多个安全无线网络，计算设备的用户可在激活绑定控制之前选择列表框 452 中的特定的一个安全无线网络。

向计算设备提供的加入安全网络的授权可以是临时性的。安全网络的网络密钥（如 WEP 密钥或 WPA 密钥）可周期性地改变。从而，计算设备下一次置于安全无线网络的范围内时，仍然需要连接到网络。从而，可以仅在规定的或

限制的时间（即直到网络的网络密钥改变为止）授权对加入网络的许可。

虽然连同实施本发明的较佳形式及其改进描述了本发明，但是本领域的普通技术人员将理解到可对本发明作出的许多其它改进都在本发明的范围之内。因此，本发明的范围并不限于上述的描述。

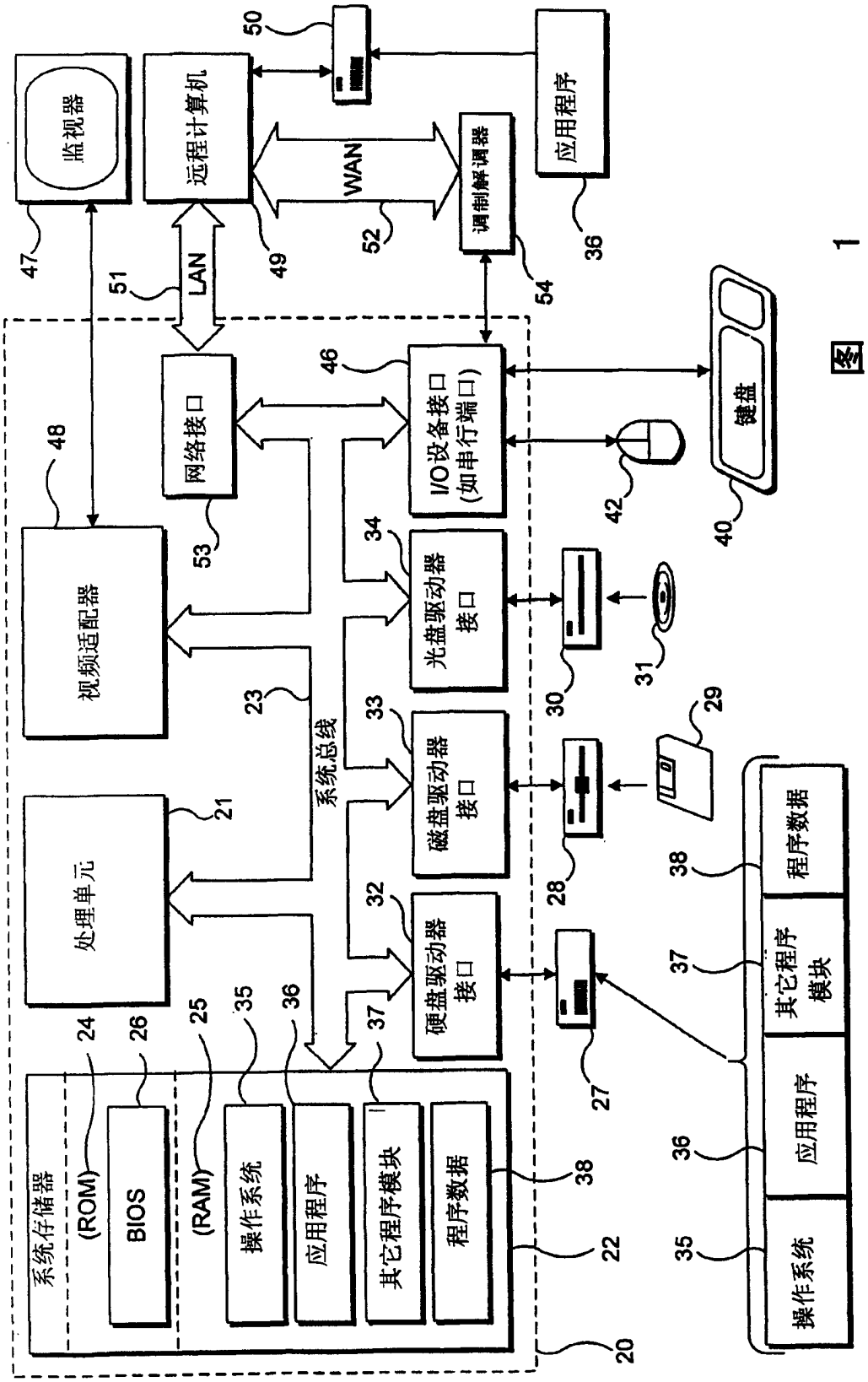

监视器
远程计算机
50
应用程序
WAN
调制解调器
47
51
LAN
49
52
54
36
网络接口
46
I/O设备接口
(如串行端口)
48
键盘
42
40
视频适配器
53
34
光盘驱动器
接口
31
30
23
系统总线
33
磁盘驱动器
接口
29
处理单元
21
32
28
38
硬盘驱动器
接口
37
27
其它程序
模块
程序数据
系统存储器
(ROM)
BIOS
24
26
(RAM)
操作系统
应用程序
其它程序模块
程序数据
25
35
36
37
38
22
20
36
应用程序
35
操作系统

图 1

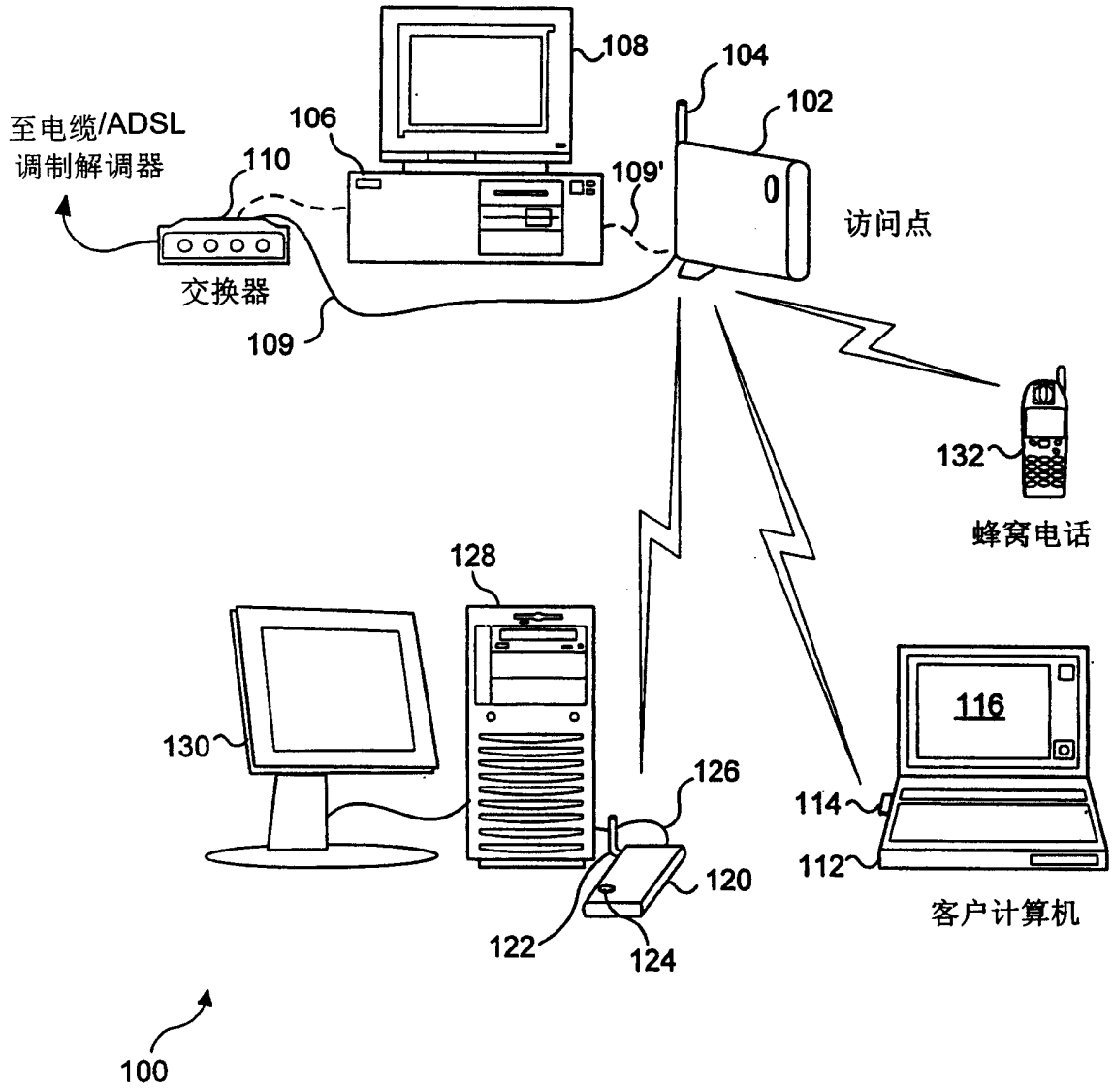

至电缆/ADSL
调制解调器
110
106
108
104
102
109'
访问点
交换器
109
132
蜂窝电话
128
130
126
120
122
124
116
114
112
客户计算机
100

图 2

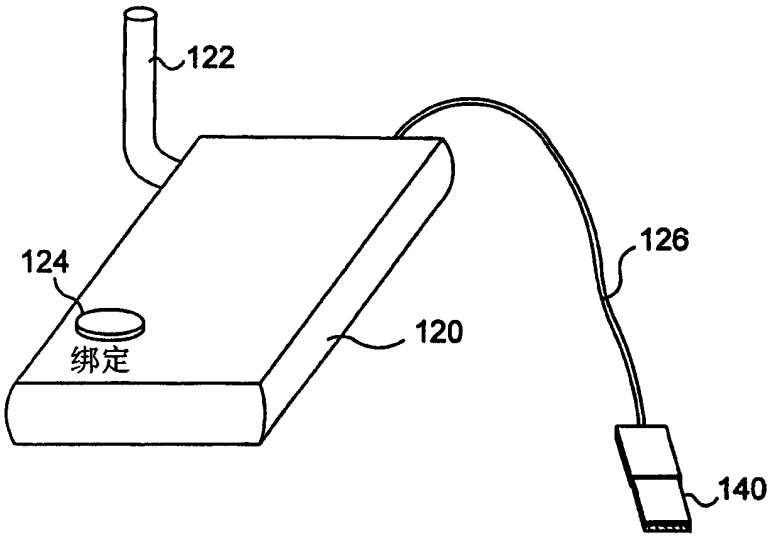


图 3

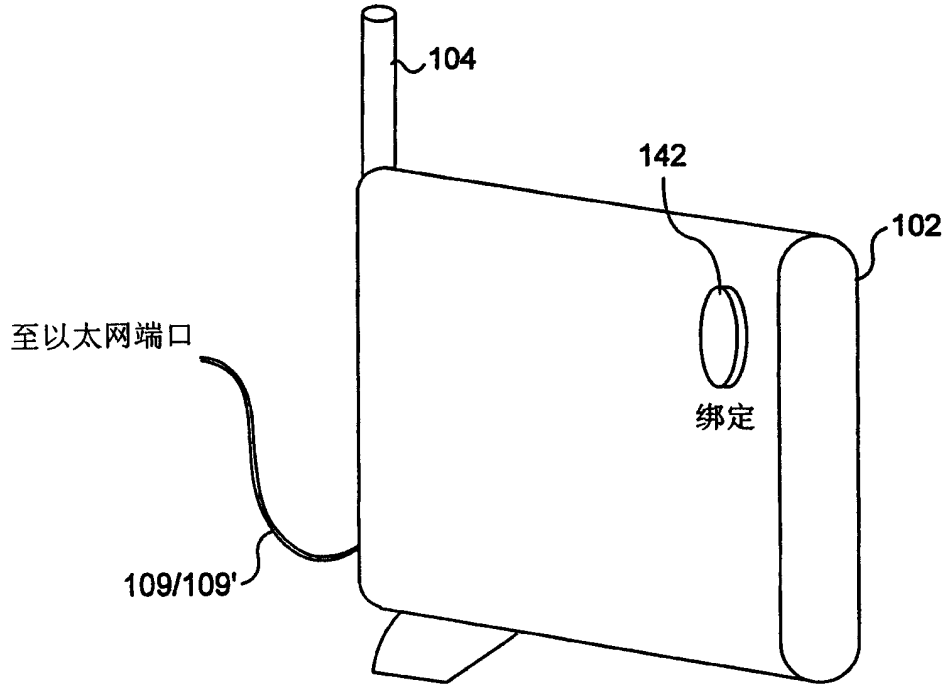


图 4

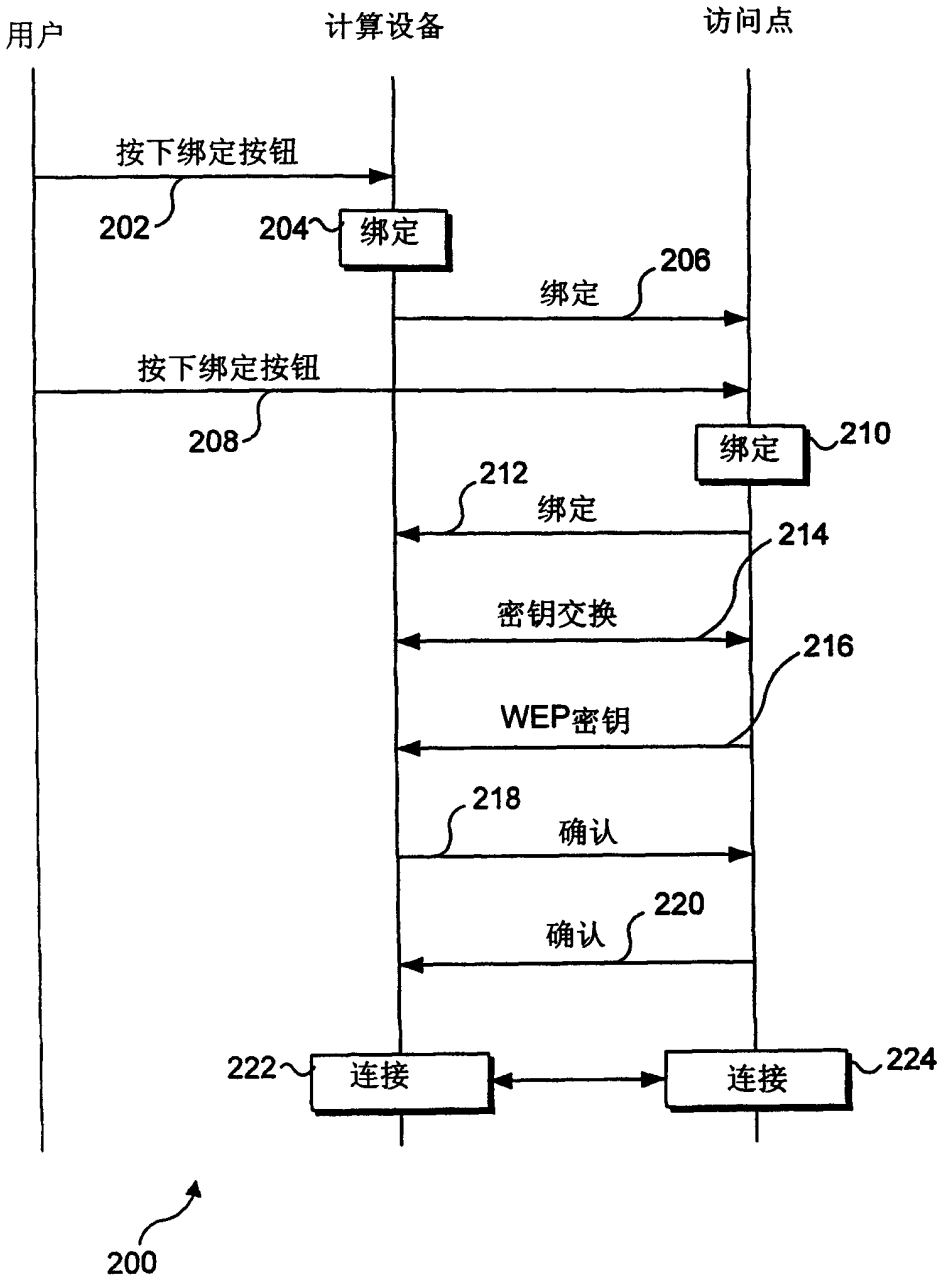

用户
计算设备
访问点
按下绑定按钮
202
204
绑定
206
绑定
按下绑定按钮
208
绑定
210
212
绑定
214
密钥交换
216
WEP密钥
218
确认
220
确认
222
连接
连接
224
200

图 5

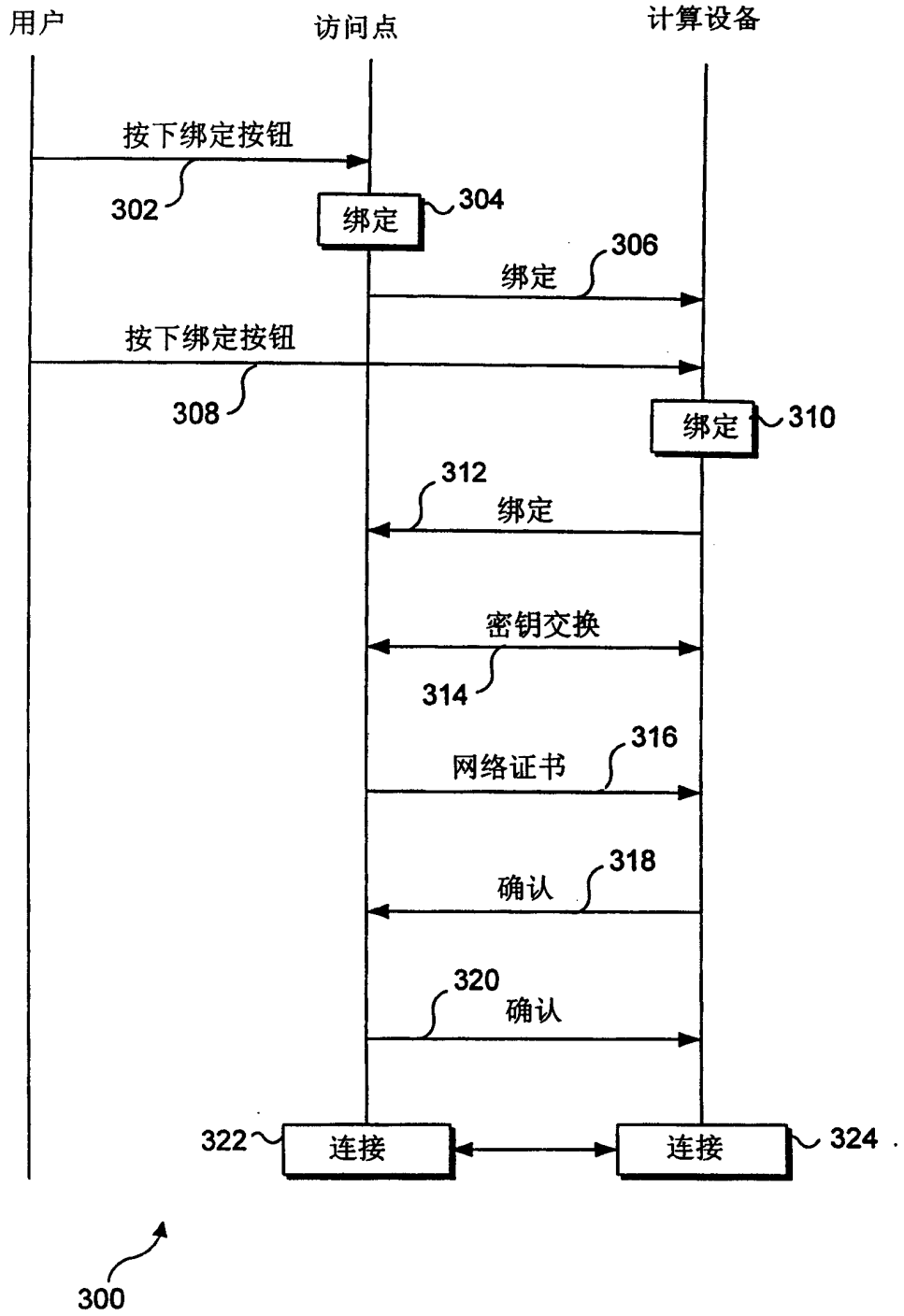

用户
访问点
计算设备
按下绑定按钮
302
绑定
304
306
绑定
按下绑定按钮
308
绑定
310
312
绑定
密钥交换
314
316
网络证书
确认
318
320
确认
322
连接
连接
324
300

图 6

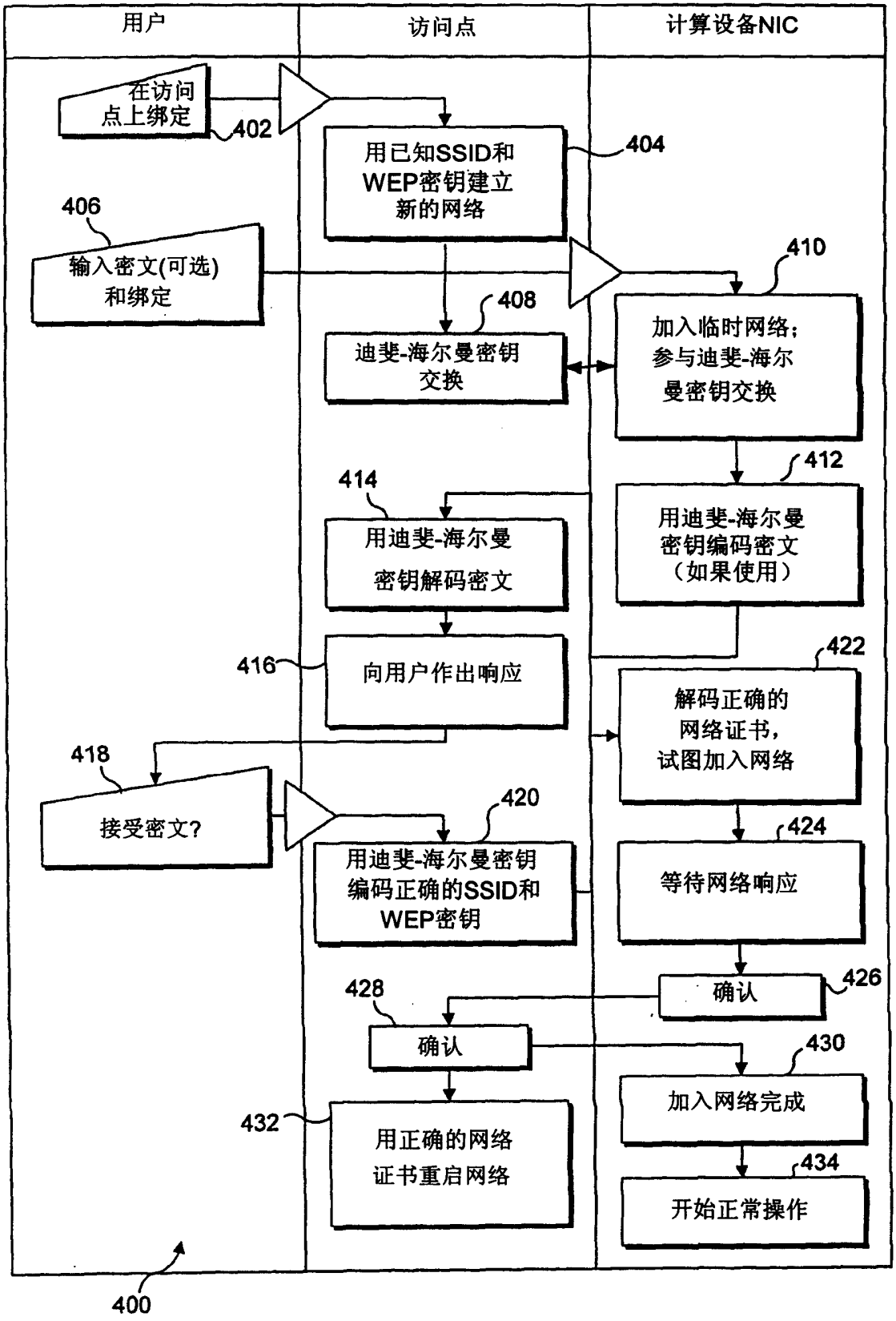

用户
访问点
计算设备NIC
在访问点上绑定
402
用已知SSID和WEP密钥建立新的网络
404
406
输入密文(可选)和绑定
410
408
迪斐-海尔曼密钥交换
加入临时网络；参与迪斐-海尔曼密钥交换
412
414
用迪斐-海尔曼密钥解码密文
用迪斐-海尔曼密钥编码密文（如果使用）
416
向用户作出响应
422
解码正确的网络证书，试图加入网络
418
接受密文?
420
424
用迪斐-海尔曼密钥编码正确的SSID和WEP密钥
等待网络响应
426
确认
428
确认
430
加入网络完成
432
用正确的网络证书重启网络
434
开始正常操作
400

图 7

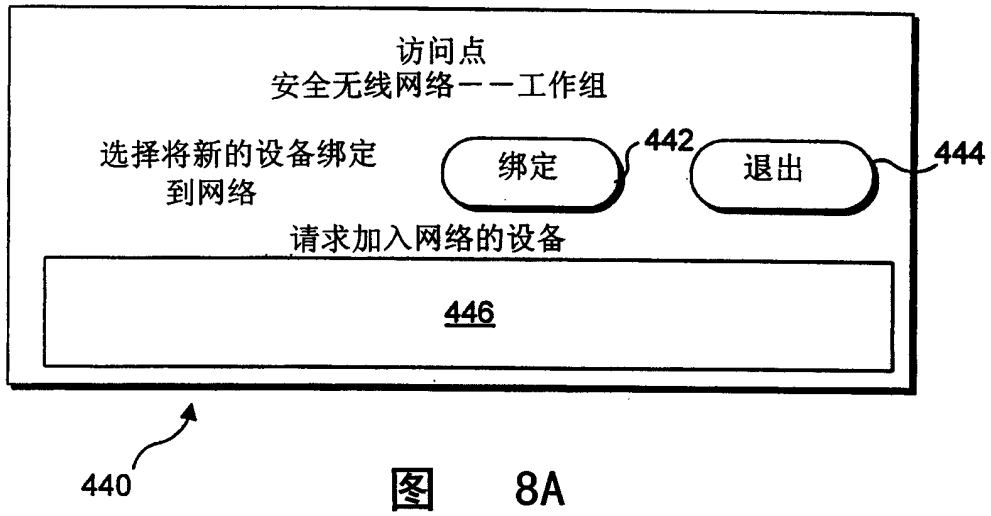

访问点
安全无线网络——工作组
选择将新的设备绑定到网络
绑定
442
退出
444
请求加入网络的设备
446
440

图 8A

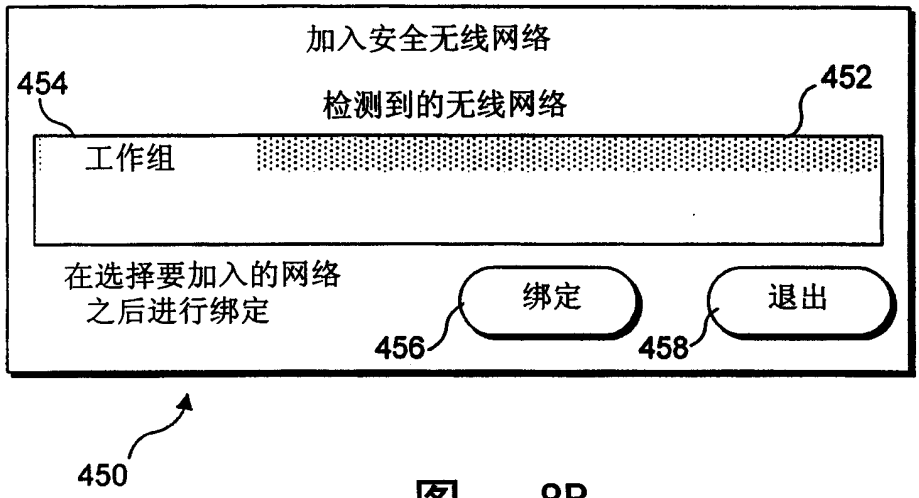

加入安全无线网络
454
检测到的无线网络
452
工作组
在选择要加入的网络之后进行绑定
绑定
456
退出
458
450

图 8B