(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102204304 B
(45)授权公告日 2014.07.30

(21)申请号 200980144623.3
(22)申请日 2009.11.03
(30)优先权数据
61/111,240 2008.11.04 US
12/359,987 2009.01.26 US
(85)PCT国际申请进入国家阶段日
2011.05.03
(86)PCT国际申请的申请数据
PCT/US2009/063044 2009.11.03
(87)PCT国际申请的公布数据
WO2010/053889 EN 2010.05.14
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 H·沈 X·蒋 A·巴纳基 H·刘 T·曼德哈纳
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 胡利鸣
(51)Int.Cl.
H04W 12/04(2006.01)
H04W 88/08(2006.01)
审查员 张玉娟

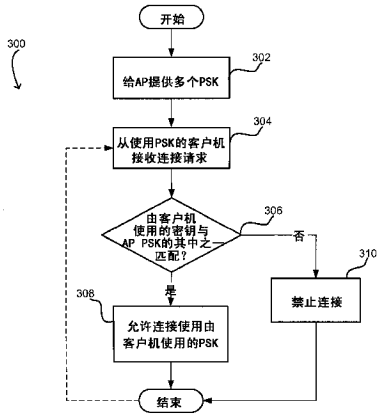
权利要求书2页 说明书13页 附图7页

(54)发明名称

对接入点中的多个预先共享的密钥的支持

(57)摘要

一种操作被配置成支持多个预先共享的密钥的接入点(AP)的方法。给与AP相关联的各个客户机设备提供密钥。为了鉴别客户机设备，AP判断多个所支持的预先共享的密钥(PSK)(如果存在的话)中的哪一个匹配包括从客户机设备接收的密钥的信息。当该信息匹配时，允许客户机设备连接到AP。给AP提供多个预先共享的密钥允许从AP有选择地断开所关联的客户机设备。移除受AP支持的多个预先共享的密钥的PSK和断开使用此PSK的客户机设备不断开使用不同的密钥来接入AP的剩余的客户机设备。此外，当PSK的寿命过期时，移除该PSK并断开每一个使用该PSK的客户机设备。



CN 102204304 B

1. 一种操作被配置成接入点（102）的设备的方法，给所述接入点提供（302）多个预先共享的密钥（218、220），且所述方法包括：

从至少一个客户机设备（106、108、110、112、210）接收（304）对到所述接入点的连接的请求，所述请求包括用密钥（107、109、111、113）生成的部分；

判断（306）所述部分是否包括与用来自被提供给所述接入点的所述多个预先共享的密钥中的密钥生成的信息匹配的信息，其中所述多个预先共享的密钥具有不同的寿命和/或复杂性，并且其中所述多个预先共享的密钥包括至少一个用户友好格式的预先共享的密钥，所述至少一个用户友好格式的预先共享的密钥被用于具有降低的安全要求的连接；

当判断所述部分的所述信息匹配用来自所述多个预先共享的密钥（218、220）的所述密钥生成的信息时，允许（308）所述连接；以及

当判断所述部分的所述信息不匹配用来自所述多个预先共享的密钥（218、220）的所述密钥生成的信息时，禁止（310）所述连接。

2. 如权利要求 1 所述的方法，其特征在于，所述多个预先共享的密钥包括长期预先共享的密钥（516）和短期预先共享的密钥（512）中的至少一个。

3. 如权利要求 1 所述的方法，其特征在于，还包括，响应于对从所述多个预先共享的密钥（218、220）移除所选择的预先共享的密钥的请求（402、404）：

从所述多个预先共享的密钥移除（406）所选择的预先共享的密钥；

判断（408、410）所述至少一个客户机设备是否使用所选择的预先共享的密钥；以及

当判断所述至少一个客户机设备使用所选择的预先共享的密钥时，断开（412）所述至少一个客户机设备。

4. 如权利要求 3 所述的方法，其特征在于，对移除所选择的预先共享的密钥的所述请求由用户经由用户界面执行（402）的。

5. 如权利要求 3 所述的方法，其特征在于：

所述多个预先共享的密钥中的密钥具有与其关联的生存时间值（220），以及

响应于判断（404）所选择的预先共享的密钥的生存时间过期而生成对移除所选择的预先共享的密钥的所述请求。

6. 如权利要求 1 所述的方法，其特征在于：接收所述请求包括根据 WPA（710）或 WPA2 协议（610）接收所述请求。

7. 如权利要求 6 所述的方法，还包括：

当允许所述连接时，根据所述 WPA（722、730）或 WPA2（622）协议发送进一步消息。

8. 如权利要求 1 所述的方法，其特征在于，还包括，当所述至少一个客户机设备包括被连接到所述接入点的多个客户机设备（106、108、110、112、210）时：

移除（406、214）与所述多个客户机中的至少一个客户机设备相关联的所述预先共享的密钥；以及

在不中断到所述多个客户机设备中的其他客户机设备的连接的情况下有选择地中止到所述多个客户机中的所述至少一个客户机设备的所述连接（412）。

9. 如权利要求 8 所述的方法，其特征在于，移除所述预先共享的密钥包括当预先共享的密钥的寿命过期（404）时和/或当从所述多个预先共享的密钥移除（402）由所述至少一个客户机设备使用的预先共享的密钥时，移除所述预先共享的密钥。

10. 如权利要求 1 所述的方法，其特征在于，还包括，当判断所述预先共享的密钥匹配来自所述多个预先共享的密钥的所述密钥时，为所述至少一个客户机设备生成组密钥（232）。

11. 一种被配置成接入点（102）的装置，所述装置包括：

被配置成存储多个预先共享的密钥（220）的计算机存储器（218）；

被配置成从至少一个客户机设备（106、108、110、112、210）接收（304）对到所述接入点的连接的请求的接口（208），所述请求包括用密钥生成的信息；以及

被配置成如下的控制组件（216）：

判断（306）用所述密钥生成的所述信息是否匹配用来自所述多个预先共享的密钥的密钥生成的信息，其中所述多个预先共享的密钥具有基于给客户机设备提供所述多个预先共享的密钥的用户容忍度而选择的不同的寿命和 / 或复杂性，并且其中所述多个预先共享的密钥包括至少一个用户友好格式的预先共享的密钥，所述至少一个用户友好格式的预先共享的密钥被用于具有降低的安全要求的连接；

当判断用所述密钥生成的所述信息匹配用来自所述多个预先共享的密钥的所述密钥生成的所述信息时，允许（308）所述连接；以及

当判断用所述密钥生成的所述信息不匹配用来自所述多个预先共享的密钥的所述密钥生成的所述信息时，禁止（310）所述连接。

12. 如权利要求 11 所述的装置，其特征在于，所述计算机存储器还包括：

被配置成存储被连接到所述接入点的客户机设备的信息（226、228、230、232）的多个数据结构（222、224A、224B、224C），来自所述多个数据结构的每一数据结构（224A、224B、224C）存储客户机设备的标识符（226）和由所述客户机设备使用的预先共享的密钥（228）。

13. 如权利要求 11 所述的装置，其特征在于：

用所述密钥生成的所述信息包括消息的签名，所述消息包括所述请求（610）；以及

判断用所述密钥生成的所述信息是否匹配用来自所述多个预先共享的密钥的所述密钥生成的信息包括使用用来自所述多个预先共享的密钥的密钥生成的信息来计算（614、714）所述消息的签名。

14. 如权利要求 11 所述的装置，其特征在于，所述控制组件被配置成，响应于对从所述多个预先共享的密钥移除所选择的预先共享的密钥的请求（402、404）：

从所述多个预先共享的密钥移除（406）所选择的预先共享的密钥；

判断（408、410）所述至少一个客户机设备是否使用所选择的预先共享的密钥；以及

当判断所述至少一个客户机设备使用所选择的预先共享的密钥时，指示断开（412）所述至少一个客户机设备。

15. 如权利要求 11 所述的装置，其特征在于，所述接入点包括允许 Wi-Fi 的设备（602、702）且所述至少一个客户机设备包括允许 Wi-Fi 的客户机设备（600、700）。

对接入点中的多个预先共享的密钥的支持

[0001] 背景

[0002] 现今，各种计算机设备能够无线地通信。例如，诸如个人计算机、个人数字助理、蜂窝式电话、打印机、扫描仪和其他等的移动计算设备可以使用用于无线联网的 IEEE 802.11 标准在无线局域网 (WLAN) 上通信。为了接入无线网络，计算机设备或其他客户机设备可以与被配置成接入点 (AP) 的设备无线地“关联”，该被配置成接入点 (AP) 的设备然后向客户机设备提供对系统或网络资源的接入。AP 可以被实现为被专门配置成提供网络接入的专用设备，或者可以通过编程执行其他功能的计算机来实现。在通过计算机编程来实现时，接入点可以被称为“软 AP”。类似于“硬 AP”，软 AP 提供对其的接入的资源可以包括被连接到网络的其他设备，且在一些实例中可以包括在充当软 AP 的计算机内的应用程序或其他元素。

[0003] 为了允许安全通信，客户机设备和 AP 通过交换秘密信息来手动地相互鉴别。如果交换是成功的，则 AP 允许客户机设备连接到网络。秘密信息可以是预先共享的密钥。如果使用了预先共享的密钥，则向 AP 和所关联的无线客户机设备提供用于鉴别的相同的预先共享的密钥。

[0004] 例如，根据 WPA 和 WPA2 鉴别和密钥交换协议，在尝试接入网络时，客户机设备向 AP 提供用其预先共享的密钥生成的信息。如果 AP 可以使用其预先共享的密钥的副本来鉴别该信息，则客户机被鉴别。预先共享的密钥可以被用于导出临时会话密钥、用于数据加密和解密以及用于其它目的。

[0005] 按照惯例，如果使用了预先共享的密钥，则 AP 使用单个预先共享的密钥来与客户机设备关联。因而，与相同的 AP 相关联的所有客户机设备共享相同的预先共享的密钥。

[0006] 概述

[0007] 本发明者已经认识到并明白，无线联网的角色可能改变，并且，可以由支持多个预先共享的密钥并可以自动地为寻求网络或系统接入的每一设备标识适当的预先共享的密钥的接入点提供较好匹配用户期望的操作。

[0008] 在从多个不同类型的设备接收连接请求的接入点中，客户机设备可以具有对于预先共享的密钥 (PSK) 的不同要求以及用于给设备提供复杂密钥的不同的用户容忍度。因而，接入点中的多个预先共享的密钥可以具有不同的寿命和复杂性。作为具体的示例，打印机和其他固定客户机设备可以与 AP 维持长期连接。因为可能仅不频繁地给这些设备提供预先共享的密钥，复杂密钥可以被用于维持安全而无需显著的用户负担。相比之下，个人数字助理和其他移动设备可能仅需要到 AP 的短期连接，可以使用被用户输入到移动设备的密钥来发起该短期连接。对于这样的连接，可以使用较不复杂的密钥，这是因为如果密钥被用于短的连接则存在较少的危害网络安全的风险。通过使用较不复杂的密钥，减少了给设备提供服务的用户负担。

[0009] 为了支持不同的持续时间的密钥，根据本发明的一些实施方式的接入点可以被配置成在不断开正使用其他 PSK 的其他客户机设备的情况下移除一些 PSK。以此方式，可以在不中断与 AP 具有长期连接的设备的情况下移除短期 PSK。

[0010] 为了促进在 AP 和所关联的客户机设备之间的通信，本发明的实施方式提供将 AP

配置成支持多个预先共享的密钥 (PSK)。可以给与 AP 相关联的各个客户机设备提供多个 PSK 的其中之一。因而，根据本发明的一些实施方式，尽管多于一个的客户机设备仍然可以共享 PSK，但 AP 在给定的时刻支持多于一个的 PSK 以便鉴别其所关联的客户机设备。当客户机设备尝试经由 AP 接入网络时，AP 判断使用多个受支持的 PSK 中的哪一个 PSK 来鉴别客户机设备。AP 和客户机设备可以将这些 PSK 用于在例如使用 IEEE 802.11 标准的 Wi-Fi ® 技术的 WLAN 上进行通信。

[0011] 在本发明的一些实施方式中，与 AP 相关联的客户机设备可以被分组，且属于相同的组的设备共享 PSK。由形成一个组的客户机设备使用的 PSK 的移除在不影响使用不同的 PSK 的其他组中的客户机设备对网络的接入的情况下终止此组中的设备对网络的接入。

[0012] 给 AP 提供多个 PSK 允许 AP 被配置成支持不同类型的 PSK。例如，不同的寿命和复杂性的 PSK 可以由 AP 在给定的时刻采用。一些 PSK 可以是短的且适合于由人类用户输入。一些 PSK 可以频繁地改变且可以支持瞬时网络接入。其他可以是长的，以便为长期连接提供较好的安全性。

[0013] 前述是本发明的非限制性概述，本发明由所附权利要求界定。

[0014] 附图简述

[0015] 附图不预期按比例绘制。各图中，各种图中示出的每一相同的或接近相同的组件由类似的数字表示。为清晰起见，并非在每一附图中标记每一组件。各图中：

[0016] 图 1 是其中可以实现本发明的一些实施方式的计算环境的简图；

[0017] 图 2 是根据本发明的一些实施方式被配置成接入点的设备内的组件的框图；

[0018] 图 3 是根据本发明的一些实施方式操作接入点的过程的流程图；

[0019] 图 4 是根据本发明的一些实施方式移除被提供给接入点的预先共享的密钥的过程的流程图；

[0020] 图 5A-5C 是根据本发明的一些实施方式给接入点提供预先共享的密钥的过程期间所使用的用户界面的简图；

[0021] 图 6 是示出根据本发明的一些实施方式在使用 Wi-Fi 受保护接入 2(Wi-Fi Protected Access 2,WPA2) 协议的接入点和客户机设备之间的密钥交换过程的简图；以及

[0022] 图 7 是示出根据本发明的一些实施方式在使用 Wi-Fi 受保护接入 (WPA) 协议的接入点和客户机设备之间的密钥交换过程简图。

[0023] 详细描述

[0024] 在无线通信中，被配置成接入点 (AP) 的设备和客户机设备可以手动地使用某些秘密信息来相互鉴别。该信息可以包括预先共享的密钥 (PSK)。

[0025] 本发明者已经认识到并明白，客户机设备可以具有来自 PSK 的不同要求以及用于给设备提供复杂密钥的不同用户容忍度。因而，可以通过使得客户机设备用户将不同类型的 PSK 用于 AP 接入来改善用户体验。例如，不同的密钥可以具有适用于到 AP 的给定连接的寿命和复杂性。例如，PSK 可以是被临时地使用短期密钥，且具有允许由客户机设备的用户容易地键入密钥的用户友好的格式。短期密钥可以例如由被允许经由 AP 接入因特网短的时间周期的膝上型计算机用户或 PDA 用户使用。通过使用较不复杂的密钥减少了给客户机提供 AP 接入的用户负担，且安全风险是低的，这是因为密钥可以在短的时间之后过期。作为另一示例，PSK 也可以是更复杂且具有更长寿命的长期密钥。例如，固定的打印机或扫描

仪可以与 AP 维持长期通信，且可以因而利用用户更难以输入的长期密钥。

[0026] 本发明者已经进一步认识到且明白，可以通过将 AP 配置成支持多个预先共享的密钥 (PSK) 来促进 AP 的操作和在 AP 和所关联的客户机设备之间的通信。给 AP 提供多个 PSK 允许从 AP 有选择地断开所关联的客户机设备。因而，移除受 AP 支持的多个 PSK 中的 PSK 和断开已经使用该 PSK 来鉴别 AP 的客户机设备并不断开使用不同的 PSK 来接入 AP 的剩余的客户机设备。

[0027] 进一步，当两个或更多个客户机设备形成其中各设备共享 PSK 的组时，PSK 的移除在不影响使用不同的 PSK 的其他组中的客户机设备的网络接入的情况下终止此组中的设备到网络的接入。

[0028] 为了支持不同寿命的密钥，AP 可以根据本发明的一些实施方式被配置成在不断开与 AP 可以具有长期连接的其他客户机设备的情况下移除一些 PSK。因而，当 PSK 的寿命过期时，从 AP 有选择地移除 PSK。

[0029] 本发明的一些实施方式提供操作被配置成 AP 的设备的方法，其中给 AP 提供多个 PSK。当客户机设备尝试连接到 AP 时，AP 从客户机设备接收对连接的请求。该请求可以包括基于被存储在客户机设备上的密钥而被加密、签署或以另外方式处理的信息。AP 可以判断客户机设备是否已经访问有效的预先存储的密钥以便生成该信息，并且，如果是这样，则判断使用多个受支持的 PSK 中的哪一个 PSK。为了做出此判断，AP 可以将作为对连接的请求的部分而从客户机设备接收的信息与基于来自被提供给 AP 的多个 PSK 的 PSK 而生成的相似信息进行比较。

[0030] 可以使用任何合适的方法给 AP 提供多个 PSK。例如，为了存储各个 PSK，AP 可以经由可以由应用程序或用户界面响应于用户输入或任何其他合适的方式调用的编程接口接收调用。

[0031] 根据本发明的一些实施方式，AP 从被存储在 AP 上的多个 PSK 移除所选择的 PSK。AP 可以作为对 API 的调用、通过用户界面的用户输入、PSK 的寿命的终结和其他事件的结果而移除 PSK。在移除 PSK 时，AP 可以判断被连接到 AP 的任何客户机设备是否使用所选择的 PSK 来形成连接。当找到这样的设备时，AP 可以在不断开使用不同的 PSK 来鉴别 AP 的客户机设备的情况下断开它们。AP 可以支持一个或多个 API，AP 可以通过这些 API 来请求移除密钥。这样的请求可以由应用程序、通过用户界面响应于用户输入或以任何其他合适的方式生成。

[0032] 进一步，PSK 的移除可以由在 AP 本身内的控件元素触发。例如，当所选择 PSK 的寿命过期时，可以从被存储在 AP 上的多个 PSK 移除所选择的 PSK。如果被连接到 AP 的任何客户机设备使用所选择的 PSK，则 AP 可以在不断开使用不同的 PSK 来鉴别 AP 的客户机设备的情况下断开它们。

[0033] 图 1 示出其中多个计算设备使用无线网络 104 与被配置成接入点的设备 102 通信的联网计算环境 100。网络 104 可以是例如无线局域网 (WLAN)。设备 102 可以是例如被配置成“软 AP”的计算机。但是，AP 可以是硬件 AP，或者被配置成执行允许客户机设备根据无线协议接入资源的协议的其他无线设备。例如，可以利用可以使用受 IEEE 802.11 标准支持的 Wi-Fi ®技术来操作的 AP。

[0034] 在所示出的示例中，如图所示，四个客户机设备与接入点 102 无线地通信 :扫描仪

106、打印机 108、膝上型计算机 110 和 PDA 112。设备可以是移动的、固定的或实现移动操作模式和固定操作模式两者。尽管示出了四个计算设备，但任何数量或类型的计算设备可以根据本发明的实施方式与接入点通信，且出于简单起见而示出四个设备。

[0035] 在这里，AP 102 被配置成支持多个 PSK。与 AP 102 相关联的客户机设备 106、108、110 和 112 中的每一个都存储 PSK。因而，在此示例中，设备 106、108、110 和 112 中的每一个包括各自的 PSK，分别在框 107、109、111 和 113 中图示地示出。例如，扫描仪 106 和打印机 108 两者都包括密钥 1，膝上型计算机 110 包括密钥 2 且 PDA 112 包括密钥 3。因而，尽管扫描仪 106 和打印机 108 共享被称为密钥 1 的 PSK，但膝上型计算机 110 和 PDA 112 包括不同的 PSK，这示出了 AP 102 在给定的时刻支持多于一个的 PSK 以便鉴别其所关联的客户机设备。

[0036] 与 AP 相关联的客户机设备可以被分组，且属于相同的组的设备共享 PSK。图 1 示出扫描仪 106 和打印机 108 具有相同的 PSK。因而，这些设备可以形成组。根据一些实施方式，移除由形成一个组的客户机设备使用的 PSK 在不影响使用不同的 PSK 的其他组中的客户机设备的网络接入的情况下终止该组中的设备的网络接入。

[0037] 与 AP 相关联的客户机设备可以具有对于 PSK 的不同要求和用于给客户机设备提供复杂密钥的不同用户容忍度。因而，AP 中的多个 PSK 可以具有不同的寿命和复杂性。例如，图 1 中示出的扫描仪 106 和打印机 108 可以是与 AP 102 维持长期连接的固定设备。因为可以仅不频繁地向这些设备提供 PSK，复杂的或“强的”密钥可以被用于维持安全而没有用户负担。相比之下，诸如膝上型计算机 110 和 PDA 112 等的移动设备可以仅需要到 AP 102 的短期连接，该短期连接可以由将密钥输入到移动设备的用户发起。对于这样的短期连接，可以使用较不复杂的、用户友好的、或“简易的”密钥，这是因为，如果在未经授权方可以识别短期密钥或将它用于未经授权的目的之前可以移除短期密钥，则存在较少的危害网络安全的风险。然而，通过使用有益于移动设备的用户的需要记住和每当移动设备连接到网络时手动输入 PSK 的较不复杂的密钥，因而减少了给设备提供服务的用户负担。

[0038] 因而，密钥 1、2 和 3 中的每一个可以是不同的类型。类型可以反映密钥的寿命的持续时间、密钥的复杂性或其他特性。例如，密钥 1、2 和 3 可以各自具有不同的“生存时间”(TTL) 特性。但是，应明白，TTL 仅是跟踪密钥的寿命的方法的一个示例，且可以以任何其他合适的方式定义寿命。

[0039] 根据本发明的一些实施方式，当客户机设备尝试经由 AP 接入网络时，AP 判断使用多个受支持的 PSK 中的哪一个 PSK 来鉴别客户机设备。如图 1 中所示出，AP 102 包括存储 114 或以另外方式与存储 114 相关联，存储 114 包括受 AP 支持的 PSK。在此示例中，AP 102 被示出为支持被图示地示出为密钥 1、2 和 3 的三个 PSK。然而，AP 102 可以支持任何数量的不同的类型的 PSK，本发明的实施方式在这一方面不受限制。此外，尽管存储 114 被示出为包括被存储在客户机设备 106、108、110 和 112 上的全部 PSK，但应理解，客户机设备可以具有不受 AP 102 支持的 PSK。而且，AP 102 可以包括不被存储在所关联的客户机设备中的任何客户机设备上的 PSK。

[0040] 图 2 示出包括在根据本发明的一种实施方式被配置成 AP 102 的计算机内的示例性组件的系统 200。AP 102 经由在 AP 102 内其他组件控制的网络接口 208 与一个或多个客户机设备 210 无线通信。AP 102 可以经由计算设备 204 而被配置，计算设备 204 可以是

诸如台式计算机、膝上型计算机、PDA 或可以执行应用程序、响应用户输入或以另外方式执行控制功能的任何其他设备等的任何设备。应明白，计算设备 204 可以包括在这样的情况中在计算设备 204 内提供软 AP 的功能的 AP 102。如果 AP 102 是软 AP，则图 2 中的组件中的一些可以被实现为在计算机存储介质中的计算机软件或者被处理器（未示出）执行。但是，AP 102 可以以任何合适的方式实现，包括“硬”AP 中的固件。

[0041] 在所示出的示例中，AP 102 包括用于添加和移除 PSK 的接口，作为示例，仅示出添加密钥 API 212(Add Key API 212) 和移除密钥 API 214(Remove Key API 214)。尽管示出了两个 API，但任何数量或类型的 API 可以被用于管理在 AP 102 内的 PSK。可以由控制逻辑 216(Control Logic 216) 提供受 AP 102 支持的 PSK 的添加和移除以及 AP 102 的其他功能，例如判断客户机设备是否与 AP 102 共享 PSK。应明白，控制逻辑 216 可以包括根据本发明的一些实施方式控制 AP 102 的操作的任何数量的合适的组件。

[0042] 被提供给 AP 102 的 PSK 被存储在 AP 102 的计算机存储器内的 PSK 存储 218 中。在所示出的实施方式中，该存储器是非易失性存储器，但是可以使用任何合适的存储器。

[0043] 可以任何合适的方式组织关于 PSK 的信息。在这里，PSK 存储 218 包括密钥表 220，该密钥表 220 维护关于当前被存储在 AP 102 上的 PSK 信息。应明白，PSK 存储 218 可以包括其他合适的组件。例如将经由通过添加密钥 API 212 的调用提供给 AP 102 的 PSK 添加到 PSK 存储。

[0044] 应注意，密钥表 220 可以具有对密钥的数量及其可以存储的所关联的数据的限制。在这样的实施方式中，仅当没有达到对密钥表 220 可以存储的 PSK 的数量的限制时，PSK 才可以被添加到密钥表 220。但是，应明白，PSK 可以被存储成可以被扩大为接受任意数量的密钥的列表或存储器结构，以使得在一些实施方式中不存在对 PSK 的数量的限制。

[0045] 当从 AP 102 移除 PSK 时，例如，一旦经由移除密钥 API 214 接收到指令，就从 PSK 存储 218 移除 PSK。

[0046] 如图 2 中所示出，被存储在密钥表 220 中的 n 个密钥中的每一个具有作为示例仅被示出为生存时间 (TTL) 的各自的持续时间。应明白，可以以任何其他合适的方式定义密钥的持续时间。如上面所讨论，PSK 可以具有不同的持续时间且可以在它们的各个 TTL 终结时就被移除。在其 TTL 终结时移除 PSK 可以经由移除密钥 API 214 来管理。

[0047] 替代地，在其 TTL 终结时移除密钥可以由控制逻辑 216 或任何其他合适的组件触发。在所示出的实施方式中，无论移除是通过 API 214 由命令触发还是由控制逻辑 216 发起的触发器触发，对移除密钥的处理都是相同的。但是，在一些实施方式中，可以取决于用于移除 PSK 的触发器而执行不同的处理。应明白，密钥表 220 可以存储与 PSK 相关联的其他信息，且出于简单起见示出包括 TTL 的列。

[0048] 当客户机设备尝试经由 AP 或 AP 上的应用程序接入网络时，在 AP 内的诸如例如控制逻辑 216 之类的合适的组件判断使用多个受支持的 PSK 中的哪一个 PSK 来形成与客户机设备的连接。例如，在图 1 中所示出的示例中，AP 102 可以判断被指示为被存储在 AP 102 处的密钥 1 的 PSK 可以被用于形成与使用密钥 1 的膝上型计算机的连接。

[0049] 当膝上型计算机 110 形成与 AP 102 的连接时，用于形成该连接的密钥可以被记录在 AP 102 上。AP 102 还包括存储作为示例被示出为 224A-224C 的数据结构的连接存储 222(Connections Store 222)。各个数据结构包括与受 AP 102 支持的连接相关联的数据。

例如，数据结构 224A 包括用于在 AP 102 和诸如例如图 1 中所示出的设备 106、108、110 和 112 中的任何的客户机设备之间的连接的数据。数据结构 224A 可以包括任何合适的字段。因而，数据结构 224A 包括与之建立连接的客户机设备的标识符，在这里被示出为客户机 ID 226。该数据结构也包括指示在 AP 102 和客户机设备之间共享的密钥的字段 PSK 228。PSK 可以被用于导出诸如会话密钥等的其他信息，且被用于在 AP 102 和客户机设备之间的密钥交换期间的数据加密和解密。该所导出的信息也可以被存储。因而，连接存储 222 可以存储用于给定连接的会话密钥 230 和可选的组密钥 232。应明白，与连接相关的其他信息可以被记录在数据结构 224A 中，且仅出于示出目的示出四个元素 226-232。

[0050] 数据结构 224B 和 224C 包括关于在 AP 102 和所关联的客户机设备之间的其他连接的类似信息。例如，数据结构 224A 可以存储关于在 AP 102 和图 1 中所示出的扫描仪 106 之间的连接的信息，而数据结构 224B 和 224C 可以分别包括关于在 AP 102 和膝上型计算机 110 以及 PDA 112 之间的连接的信息。尽管连接存储 222 被示出为仅包括三种数据结构，但应明白，用于被连接到 AP 102 的各个客户机设备的数据结构可以被存储在连接存储 222 中。当客户机设备形成连接时，控制逻辑 216 可以将数据结构添加到连接存储 222。当从 AP 102 断开客户机设备时，可以从连接存储 222 移除相应的数据结构。

[0051] 如上面所讨论，本发明的实施方式提供操作被提供多个 PSK 的 AP 的方法。当客户机设备尝试接入资源时，AP 从客户机设备接收对到其的连接的请求。使用被提供给客户机设备的密钥生成此请求的至少部分。然后，AP 判断是否使用 PSK 的其中之一来生成该请求。如果是这样，则可以连接、鉴别客户机设备，且可以基于所标识的 PSK 建立连接。如果不是，则不鉴别客户机且不建立连接。在所示出的实施方式中，通过判断该请求是否包含于可以用来自被提供给 AP 的 PSK 的密钥生成的信息匹配的信息，AP 判断客户机设备是否具有其 PSK 的其中之一。如果存在匹配，则 AP 允许该连接。否则，该连接被禁止。

[0052] 图 3 是根据本发明的一些实施方式操作接入点的过程的流程图。当设备被配置成 AP（例如，AP 102）时或者在任何其他合适的时刻，过程 300 开始。在框 302，可以给 AP 提供多个 PSK。可以使用任何合适的方法给 AP 提供 PSK。例如，为了添加各个密钥，AP 可以接收标识要存储在 AP 中的密钥的通过编程接口（例如，添加密钥 API 212）的调用。可以响应于经由用户界面或以任何其他合适的方式接收的输入而发生通过这样的 API 的调用。

[0053] 除了为各个 PSK 提供值之外，提供 PSK 可以包括指定密钥的持续时间或密钥的其他特性。可以通过与密钥本身相同的 API 或以任何其他合适的方式来提供这样的信息。如上面所讨论，客户机设备可以具有对于 PSK 的不同的要求。因而，本发明的实施方式提供不同的寿命和复杂性的 PSK 的使用。在一种实施方式中，PSK 可以是 256 位数字或 8 个字节到 63 个字节长的密码短语。然而，应明白，本发明的实施方式在这一方面不受限制，且可以利用任何合适的长度和格式的 PSK。PSK 可以具有可以基于给客户机设备提供密钥的用户容忍度而选择的不同的寿命和复杂性。因而，PSK 可以是被临时地使用的短期密钥（例如，具有短的 TTL），并具有允许客户机设备的用户容易地输入密钥的用户友好的格式。短期密钥可以是包括字母数字字符的序列的密码。短期密钥可以由例如被允许经由 AP 接入因特网短的时间周期的膝上型计算机用户使用。PSK 也可以是长期密钥，长期密钥更复杂，且具有更长的寿命持续时间（例如，具有长的 TTL），且可以被提供给与 AP 维持长期连接的客户机设备。例如，固定的打印机可以与 AP 维持长期通信，且因而可以利用长期密钥。用户更

难以输入长期密钥。

[0054] 所提供的密钥可以被存储起来以供 API 稍后使用，包括供在 AP 重启之后使用。被提供给 AP 的 PSK 可以被存储在例如图 2 中所示出的 PSK 存储 218 中。各个 PSK 可以具有其所关联的 TTL 以及也被存储在 PSK 存储 218 中的其他特性。应明白，在任何合适的时刻，可以给 AP 提供多个 PSK。例如，在不同的时刻，不同的 PSK 可以被提供给 AP。

[0055] 在框 304 中，AP 从客户机设备接收（例如，经由图 2 中所示出的网络接口 208）对到 AP 的连接的请求。该请求可以在任何时刻被发送，且可以是以已知的连接的格式或任何其他合适的格式。而且，所请求的网络接入可以是出于任何期望的目的。例如，客户机设备可以请求连接以便经由 AP 接入网络上的资源。而且，客户机设备可以发送对接入 AP 上的应用程序的请求。应明白，客户机设备可以出于其他目的而发送对到 AP 的该连接的请求，本发明的实施方式在这一方面不受限制。可以用被存储在客户机设备上的密钥生成该请求的一部分。

[0056] 在判决框 306 中，AP（例如，控制逻辑 216）判断，对于来自被提供给 AP 的多个 PSK 的各个 PSK，用密钥生成的请求的部分是否包括与用来自多个 PSK 的 PSK 生成的信息匹配的信息。用密钥生成的请求的部分可以是例如包括该请求的消息的签名。在 WPA 和 WPA2 协议中，签名可以是由客户机设备计算的且在下面更详细地描述的消息完整性编码 (MIC)。但是，从密钥导出的任何信息都可以指示客户机具有 PSK。可以签署、加密、散列化、或以另外方式用该密钥或另一密钥或用该密钥生成的代码处理该信息。

[0057] 当判断该信息匹配时，该过程分支到框 308，框 308 中允许在客户机设备和 AP 之间的连接。然后，该过程可以结束。作为允许该连接的一部分，AP 可以以本领域中已知的 AP 响应请求的相同方式响应该请求，但 AP 的响应可以基于在匹配来自客户机设备的请求中的信息之后选择的 PSK，且附加处理可以包括基于所标识的 PSK 生成会话密钥、组密钥或其他信息。允许连接也可以包括在连接存储 222 中创建数据结构，如上面所讨论。

[0058] 当判断该信息不匹配时，该过程转到框 310，框 310 中禁止该连接，且客户机设备不被准许接入资源。然后，该过程可以结束。应理解，当接收到来自客户机设备的对连接的另一请求时，过程 300 也可以返回到框 304，如图 3 中所示出。

[0059] 根据本发明的一些实施方式，可以从 AP 移除 PSK，即使它已经与一个或多个客户机设备相关联。可以例如在由用户或应用程序做出移除密钥的请求时发起移除。移除所选择的密钥的请求可以由用户经由 AP 上的用户界面或被用于配置 AP 的设备执行。

[0060] 进一步，当 PSK 的寿命过期时可以撤销 PSK。当撤销密钥时，可以有选择地断开在使用此 PSK 的一个或多个客户机设备之间的连接。不从 AP 断开被连接到 AP 并与 AP 共享不同的 PSK 的其他客户机设备。

[0061] 图 4 示出根据本发明的实施方式移除被提供给接入点的预先共享的密钥的过程 400。该过程可以在任何合适的点开始，且可以是编程接口的状态的连续监视的部分状态，诸如例如，图 2 中所示出的移除密钥 API 214 和 / 或在控制逻辑 216 内的触发任何 PSK 是否已经超过了它们的 TTL 的定期检查的计时组件。在判决框 402，该过程判断是否接收到指示 AP（例如，AP 102）移除所选择的 PSK 的用户输入。AP 或配置 AP 的设备（例如，计算设备 204）可以具有用户界面，该用户界面可以用于接收用户输入。

[0062] 当判断已经提供了指示 AP 移除所选择的 PSK 的用户输入时，该过程分支到框 406，

在框 406 中移除 PSK。如上面所讨论，可以从 PSK 存储 218 移除所选择的 PSK。以此方式，没有未来的连接可以基于所移除的 PSK。

[0063] 相反，当在判决框 402 判断没有提供用户输入时，该过程继续进行到框 404，在框 404 中判断与所选择的 PSK 相关联的生存时间 (TTL) 是否过期。如果该 TTL 过期，则该过程转到框 406，在框 406 中移除所选择的 PSK。当该 TTL 没有过期时，该过程返回到开始，如图 4 中所示出，其中该过程继续循环直到接收到通过 API 214 的输入或 TTL 过期。尽管判断是否提供指示 AP 移除所选择的 PSK 的用户输入和判断与所选择的 PSK 相关联的 TTL 是否过期被示出为两个相邻的步骤，但应明白，可以以任何次序或同时地或在任何时刻执行这些操作，本发明在这一方面不受限制。进一步，应明白，出于示出的简单起见，图 4 示出各步骤的顺序执行。图 4 中所示出的一个或多个操作可以作为分离的计算线程而被执行，以使得一些所示出的操作可以同时地或在分离的时刻发生。例如，当与 PSK 相关联的 TTL 过期时移除密钥可以在与处理通过 API 的调用分离的计算线程中被执行。

[0064] 在框 408，AP 搜索使用所选择的 PSK 的客户机设备。不考虑什么事件触发了 API 移除 PSK，移除 PSK 也可以包括终结在所移除 PSK 内形成的任何连接。因此，在图 2 中所示出的实施方式中，这样的设备可以通过在连接存储 222 中搜索来标识。但是，可以使用将连接关联到 PSK 的任何合适的机制。

[0065] 在判决框 410，可以判断一个或多个客户机设备是否使用所选择的 PSK。当找到这样的设备时，该过程继续进行到框 412，在框 412 中从 AP 断开这些客户机设备，这是因为它们使用的密钥已经被移除。进一步，对于被断开的各个连接，从连接存储 222 移除诸如被存储在连接存储 222 中的数据结构 224A-224C 的其中之一等的与该连接相关联的相应的数据结构。

[0066] 根据本发明的实施方式，在移除 PSK 时仅断开正在使用被选择为要移除的 PSK 的客户机设备。使用用于鉴别 AP 的不同的 PSK 的其他客户机设备保持被连接到 AP。

[0067] 当没有找到使用所选择的 PSK 的客户机设备时，该过程可以结束。然而，可以对被提供给 AP 的各个密钥重复过程 400，如图 4 中所示出。

[0068] 根据本发明的一些实施方式，经由 AP 或被用于配置 AP 的设备（例如，计算设备 204）上的用户界面向 AP 提供多个 PSK。尽管可以使用任何合适的提供机制，但图 5A-5C 示出根据本发明的实施方式用于提供 PSK 的示例性用户界面。图 5A 包括用户界面 500，该用户界面 500 包括添加密钥元素（例如，下推按钮或其他元素）和字段 504，在该字段 504 中用户可以输入密钥的值。用户界面 500 也包括指示用户可以选择密钥类型的选择密钥类型元素 506（例如，下推按钮或其他元素）。在所示出的实施方式中，支持两种密钥类型，即长期密钥类型和短期密钥类型。可以允许任何数量的各个类型的密钥。但是在一些实施方式中，AP 可以支持各个类型的密钥中的仅一种。因而，如作为示例在下拉菜单 508 中示出，用户可以选择所输入密钥是短期密钥还是长期密钥。

[0069] 图 5B 示出当用户已经通过选择下拉菜单 508 中的“短期密钥”选项（图 5B 中被示出为元素 512）选择短期密钥时的用户界面。类似地，图 5C 示出用户已经通过选择下拉菜单 508 中的“长期密钥”选项（图 5C 中被示出为元素 516）选择长期密钥。在一些实施方式中，长期密钥可以自动地生成而非由用户键入。

[0070] 不考虑所选择的密钥的类型，用户也可以通过合适的输入设备输入密钥的值。图

5B 和 5C 指示用于字段 510 中输入的短期密钥或者用于字段 514 中输入的长期密钥的值。图 5B 和 5C 图示地示出短期密钥 510 比长期密钥 516 短，且可以由用户更容易地输入。尽管图 5A-5C 示出两种类型的密钥，但应明白，可以采用多于两种类型的密钥，本发明在这一方面不受限制。此外，用户界面 500 可以包括任何其他合适的组件并显示任何文本的和视觉的格式的任何其他信息。例如，用户界面中可以包括其他组件，以便接收定义密钥的特性的输入。当如上面所示出输入密钥时，它可以被存储在图 2 中所示出的 PSK 存储 218 中的诸如密钥表 220 等的密钥表中。应注意，密钥表 220 可以具有条目的数量的限制。

[0071] 如上面所讨论，可以根据已知的协议使用 PSK。例如，PSK 可以被用于导出临时会话密钥，用于数据加密和解密和用于其他目的。进一步，不同于修改以在 AP 上支持多个 PSK，可以如本领域中已知的实现这些协议。图 6 和图 7 示出根据本发明的一些实施方式使用被提供给 AP 的 PSK 的密钥交换机制的两个示例。

[0072] 计算机设备日益使用基于 IEEE 802.11 标准的 Wi-Fi ®技术。Wi-Fi ®网络可以利用使用一个预先共享的密钥以供 AP 在给定的时刻鉴别和密钥交换的 Wi-Fi 受保护接入 (WPA 和 WPA2) 协议。应明白，在这里仅作为示例描述 WPA 和 WPA2 鉴别和密钥交换协议，且 AP 和客户机设备可以采用任何其他合适的鉴别和密钥交换协议。图 6 是示出根据本发明的一些实施方式在使用 Wi-Fi 受保护接入 2(WPA2) 协议的 AP 和客户机设备之间的密钥交换过程。图 6 示出在客户机设备 600 或恳求者一侧以及在 AP 602 的一侧或鉴别者执行的过程。客户机设备 600 可以是例如图 1 中所示出的任何设备。本领域中的技术人员可以注意到，在此示例中在客户机 600 内的处理与其中 AP 支持仅一个预先存储的密钥的密钥交换中的处理相同。

[0073] 在此示例中可以被称为 Wi-Fi 客户机设备或恳求者的客户机设备向 AP 602 发送连接的请求之后，该过程开始，但该过程可以由任何合适的事件触发。如上面所讨论，该过程包括消息的生成，该消息的一部分基于被存储在客户机设备上的密钥。然后，AP 判断被提供给它的多个 PSK 中的哪一个 PSK 可以被用于鉴别客户机设备。该 PSK 可以被用于密钥交换，如下面所描述。

[0074] 在 WPA2 协议中，使用局域网上的可扩展鉴别协议 (EAPOL)- 密钥 (Extensible Authentication Protocol over LANs(EAPOL)-KEY) 消息执行密钥交换。在框 604，AP 602 发送消息 1 EAPOL_ 密钥 (ANonce，单播)(EAPOL_KEY(ANonce，Unicast))，其可由客户机设备 600 在框 606 接收到。单播参数指示消息 1 仅被发送给客户机设备 600。ANonce 指示鉴别者现时，在此示例中，ANonce 是在 AP 602 处使用 WPA2 协议生成的任何合适的格式的随机数据。

[0075] 在框 606，客户机 600 接收消息 1。对于所示出的密钥交换，客户机设备 600 接着生成 SNonce(恳求者现时)，SNonce 也是任何合适的格式的随机数据。

[0076] 在框 608，客户机设备 600 使用其所存储的密钥从 ANonce 和 SNonce 计算成对瞬时密钥 (PTK)。在框 610，客户机 600 使用 PTK 发送消息 2 EAPOL_ 密钥 (SNonce，单播，MIC)(EAPOL_KEY(SNonce，Unicast，MIC))。单播参数指示消息 2 仅被发送给 AP 602。由 WPA2 协议实现的消息完整性编码 (MIC) 是通过检测该数据分组的有害修改来保护数据分组完整性的键控散列函数。MIC 可以是例如在被加密和被传送之前跨越整个非加密原始数据分组被计算的 8 字节的值。然而，MIC 可以是任何合适的格式和长度，本发明的实施方式在这

一方面不受限制。在这里，使用 PTK 生成 MIC，PTK 又是基于被存储在客户机 600 上的密钥而生成。因而，包含 MIC 的消息 2 的部分基于客户机 600 的所存储的密钥。具有所存储的密钥的副本的其他设备可以同样地生成相同的 MIC 值。但是，不带有客户机的所存储的密钥的副本的设备不能容易地生成相同的 MIC 值。

[0077] 在框 612，AP 602 接收消息 2。在框 614，AP 602 使用被存储在 AP 602 上的多个 PSK 的其中之一从 ANonce 和 SNonce 计算 PTK。然后，在框 616，所计算的 PTK 被用于验证 MIC，如本领域中已知的。这样的验证可以通过将由 AP 602 生成的 MIC 与消息 2 中接收的 MIC 进行比较来执行。如果由 AP 602 使用的预先存储的密钥与由客户机 600 使用的密钥相同，则 MIC 应匹配。在判决框 618，AP 602（使用例如诸如图 2 中所示出的控制逻辑 216 等的组件）判断从客户机设备 600 接收的 MIC 是否匹配由 AP 602 计算的 MIC。当判断 MIC 不匹配 PTK 时，该过程分支到判决框 619，在判决框 619 中该过程基于是否还有要比较的 PSK 而分支。当不再存在 PSK 时（这意味着不存在对由客户机 600 使用的密钥的匹配），该过程分支到框 620，在框 620 中中断密钥交换过程，且客户机设备 600 不被允许接入所请求的资源并被从 AP 602 断开。

[0078] 如图 6 中所示出，对被存储在 AP 602 处的多个 PSK 中的每一个重复在框 614-618 执行的操作。因此，如果一个 PSK 不产生匹配，则该过程从框 619 循环回到 614。因而，AP 判断多个 PSK 中的哪一个（如果存在的话）匹配被存储在客户机设备上的密钥。

[0079] 当判断 MIC 匹配时，这指示 AP 602 已经找到匹配由客户机设备 600 使用的密钥的 PSK。因此，允许客户机设备 600 和 AP 602 之间的连接，且允许客户机设备接入资源。在此场景中，该过程分支到框 622。而且，可以在 AP 602 记录用于客户机设备 600 的 PSK 和所关联的信息。例如，创建诸如图 2 中所示出的数据结构 224A-224C 的其中之一等的数据结构并在在连接存储 222 中存储该数据结构。

[0080] 为了完成密钥交换过程，需要将 PTK 安装在客户机设备上。因而，在框 622，AP 602 发送指示客户机设备 600 安装 PTK 的消息 3 EAPOL_ 密钥（安装 PTK，单播，MIC，经加密的 GTK)(EAPOL_KEY(Install PTK,Unicast,MIC,Encrypted GTK))。根据可以可选地为客户机设备 600 创建的 WPA2 协议，GTK 指示成组临时密钥。使用 PSK 来生成 GTK，且该 GTK 可以用于将客户机设备 600 标识为一组设备的成员。AP 602 加密 GTK，且经加密的 GTK 作为消息 3 的一部分被发送给客户机设备 600。在框 624，客户机设备 600 接收消息 3 并将其发送 AP 602，在框 626，发送作为消息 4 EAPOL_ 密钥（单播，MIC)(EAPOL_KEY(Unicast,MIC)) 的肯定应答，在框 628，AP 602 接收到消息 4。然后，该过程可以结束。

[0081] 图 7 示出根据本发明的一些实施方式在使用 Wi-Fi 受保护接入 (WPA) 协议的 AP 和客户机设备之间的密钥交换过程。类似于在 WPA2 协议中，使用局域网上的可扩展鉴别协议 (EAPOL)- 密钥消息执行密钥交换。图 7 示出在客户机设备 700 上和在 AP 702 上执行的过程。客户机设备 700 可以是例如图 1 中所示出的任何设备。类似地，AP 702 可以是图 1 和图 2 中所示出的 AP 102。

[0082] 在 Wi-Fi 客户机设备 700 或恳求者连接到 AP 702 以便请求通过 AP 702 接入网络或其他资源之后，该过程可以开始。如上面所讨论，客户机设备 700 使用其密钥来生成到 AP 702 的消息的部分，然后 AP 702 判断被提供给它的多个 PSK 中的哪一个（如果存在的话）可以被用于鉴别客户机设备 700。PSK 可以被用于密钥交换，如下面所描述。

[0083] 在框 704，AP 702 发送消息 1 EAPOL_ 密钥 (ANonce，单播)(EAPOL_KEY(ANonce，Unicast))，在框 706，客户机设备 700 接收到消息 1。单播参数指示消息 1 仅被发送给客户机设备 700。ANonce 指示鉴别者现时，在此示例中，ANonce 是在 AP 602 处使用 WPA 协议生成的任何合适的格式的随机数据。在此示例中，客户机设备 700 生成 SNonce(恳求者现时)，SNonce 也是任何合适的格式的随机数据。

[0084] 在框 708，客户机设备 700 使用其所存储的密钥从 ANonce 和 SNonce 计算成对瞬时密钥 (PTK)，且在框 710 发送消息 2 EAPOL_ 密钥 (SNonce，单播，MIC，SSN IE)(EAPOL_KEY(SNonce，Unicast，MIC，SSN IE))，在框 712，AP 702 接收消息 2。单播参数指示消息 2 仅被发送给 AP 702。SSN IE 是根据 WPA 协议定义的消息 2 中的安全信息元素。消息完整性编码 (MIC) 如上所述定义，且包括基于被存储在客户机设备 700 上的密钥而生成的信息。

[0085] 在框 714，AP 702 使用被提供给 AP 702 的多个 PSK 的其中之一从 ANonce 和 SNonce 计算 PTK。然后，在框 716，所计算的 PTK 被用于验证 MIC，如本领域中已知的。这样的验证可以通过将比较由 AP 702 生成的 MIC 与消息 2 中所接收的 MIC 进行比较来执行。如果由 AP 702 使用的预先存储的密钥与由客户机 700 使用的密钥相同，则 MIC 应匹配。进一步，在判决框 718，AP 702(使用例如诸如图 2 中所示出的控制逻辑 216 等的组件) 判断从客户机设备 700 接收的 MIC 是否匹配由 AP 702 计算的 MIC。

[0086] 当判断 MIC 不匹配 PTK 时，该过程通过框 719 循环回到框 714，在框 714 中测试另一 PSK。如果没有 PSK 匹配，则该过程进行到其中中断密钥交换过程，且客户机设备 700 不被允许接入所请求的资源且从 AP 702 被断开。如图 7 中所示出，重复在框 714-718 执行的操作，直到找到匹配 PSK 或直到已经评估了被存储在 AP 702 处的全部多个 PSK。因而，AP 判断多个 PSK 中的哪一个 (如果存在的话) 匹配被存储在客户机设备上的密钥。

[0087] 当判断由 AP 702 生成的 MIC 匹配由客户机 700 生成的 MIC 时，该过程分支到框 722。此时，在 AP 702 记录用于客户机设备 700 的 PSK。例如，创建诸如图 2 中所示出的数据结构 224A-224C 的其中之一等的数据结构并在连接存储 222 中记录该数据结构。在框 722，AP 702 发送指示客户机设备 700 安装 PTK 的消息 3 EAPOL_ 密钥 (安装 PTK，单播，MIC，SSN IE)(EAPOL_KEY(Install PTK，Unicast，MIC，SSN IE))。在框 724，客户机设备 700 接收消息 3，安装 PTK，并将其发送给 AP 702，在框 726，发送指示 PTK 已经被安装的作为消息 4 EAPOL_ 密钥 (单播，MIC)(EAPOL_KEY(Unicast，MIC)) 的肯定应答。在框 728，AP 702 接收到消息 4。此时，完成了成对临时密钥的交换，且客户机设备 700 和 AP 702 被手动地鉴别。

[0088] IEEE 802.11 标准支持可以用于例如视频数据的分发的多播消息。WPA 协议支持为多播消息生成的不同于诸如 PTK 等的成对临时密钥的成组临时密钥。

[0089] 因而，在客户机设备 700 和 AP 702 之间建立的安全连接可以由 AP 702 用来发送包括由在 AP 702 生成的 WPA 协议实现的成组临时密钥 (GTK) 的消息。AP 702 加密该 GTK，且经加密的 GTK 作为消息 5EAPOL_ 密钥 (经加密的 GTK，GNonce，组，MIC)(EAPOL_KEY(Encrypted GTK，GNonce，Group，MIC)) 的一部分被发送给客户机设备 700。GNonce 是组现时，GNonce 是为该成组临时密钥生成而生成的随机数据，同时组参数指定消息 5 是被发送给客户机设备 700 所属的一组设备的多播消息。在框 732，客户机设备 700 接收消息 5 并安装 GTK。在框 734，客户机设备 700 向 AP 702 发送指示经加密的 GTK 已经被安装在客户机设备 700 上的肯定应答消息 6 EAPOL_ 密钥 (组，MIC)(EAPOL_KEY(Group，MIC))。这完

成了在客户机设备 700 和 AP 702 之间密钥交换过程。

[0090] 已经这样描述了本发明的至少一种实施方式的若干方面，应明白，本领域中的技术人员将容易地想起各种变更、修改和改进。

[0091] 这样的变更、修改和改进预期是本公开内容的部分，且预期是在本发明的精神和范围内。因此，前述的描述和图仅作为示例。

[0092] 可以以众多方式中的任何方式实现上面所描述的本发明的实施方式。例如，可以使用硬件、软件或其组合来实现各实施方式。在以软件实现时，无论是在单个计算机中提供还是在多个计算机当中分布，软件代码可以在任何合适的处理器或处理器的集合上执行。

[0093] 进一步，应明白，可以以诸如机架式计算机、台式计算机、膝上型计算机或平板计算机等的许多形式中的任何形式化具体化计算机。另外，计算机可以被嵌入在一般不被看作是计算机但具有合适的处理能力的设备中，包括个人数字助理 (PDA)、智能电话或任何其他合适的便携式或固定式电子设备。

[0094] 而且，计算机可以具有一个或多个输入和输出设备。这些设备可以被用来呈现用户界面以及其他。可以被用于提供用户界面的输出设备的示例包括用于输出的视觉呈现的打印机或显示屏以及用于输出的听觉呈现的扬声器或其他声音生成设备。可以用于用户界面的输入设备的示例包括键盘和诸如鼠标、触控板和数字化输入板等的指点设备。作为另一示例，计算机可以接收通过语音识别或以其他可听格式输入信息。

[0095] 这样的计算机可以由包括诸如企业网络或因特网等的局域网或广域网的以任何合适的形式的一个或多个网络互连。这样的网络可以基于任何合适的技术，且可以根据任何合适的协议操作，并可以包括无线网络、有线网络或光纤网络。

[0096] 而且，在此略述的各种方法或过程可以被编码为可在采用各种操作系统或平台中的任何一种的一个或多个处理器上执行的软件。另外，这样的软件可以使用许多合适的编程语言和 / 或编程或脚本工具中的任何来编写，且也可以被编译为在框架或虚拟机上执行的可执行机器语言代码或中间代码。

[0097] 在这一方面，本发明可以被具体化为用一个或多个程序编码的计算机可读介质（或多个计算机可读介质）（例如，计算机存储器、一个或多个软盘、紧致盘、光盘、磁带盒、闪速存储器、以现场可编程门阵列或其他半导体设备的电路构型、或其他有形计算机存储介质），当一个或多个程序在一个或多个计算机或其他处理器上执行时，执行实现上面讨论的本发明的各种实施方式的方法。一个或多个计算机可读介质可以是可移动的，以使得被存储在其上一个或多个程序或程序可以被加载到一个或多个不同的计算机或其他处理器，以便实现上面所讨论的本发明的各种方面。

[0098] 在此使用术语“程序”或“软件”来在一般意义上提及可以用来编程计算机或其他处理器以便实现上面所讨论的本发明的各种方面的任何类型的计算机代码或计算机可执行指令集。另外，应明白，根据此实施方式的一个方面，在被执行时执行本发明的方法的一个或多个计算机程序不需要驻留在单个计算机或处理器上，而是可以以模组方式分布在许多不同的计算机或处理器中，以便实现本发明的各种方面。

[0099] 计算机可执行指令可以是以许多形式，例如由一个或多个计算机或其他设备执行的程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。通常，在各种实施方式中，可以根据期望组合或分布程序模块的

功能。

[0100] 而且，数据结构可以被存储在以任何合适的形式的计算机可读介质中。出于示出的简单起见，数据结构可以被示出为具有通过数据结构中的位置相关的字段。这样的关系可以同样通过用传达个字段之间的关系的计算机可读介质中的位置来为各字段分配存储来获得。然而，任何合适的机制都可以被用于在数据结构的字段中的信息之间建立关系，包括通过使用指针、标签或在数据元素之间建立关系的其他机制。

[0101] 可以单独使用、组合使用或者以在前述所描述的实施方式中不具体讨论的各种排列使用本发明的各种方面，且因此本发明的各种方面在其应用方面不限于前述的描述中陈述的或各图中所示出的组件的细节和排列。例如，可以以任何方式将在一种实施方式中所描述的各方面与在其他实施方式中描述的各方面组合起来。

[0102] 而且，本发明可以被具体化为方法，已经提供了该方法的示例。可以以任何合适的方式排序作为该方法的部分而被执行的动作。因此，可以构建其中以不同于所阐述的次序执行各动作的实施方式，这些实施方式可以包括同时执行一些动作，即使在说明性的实施方式中被示出为顺序的动作。

[0103] 在权利要求中使用诸如“第一”、“第二”、“第三”等等的次序术语的来修改权利要求元素本身并不意味着一个权利要求元素相对于另一权利要求元素的任何优先级、优先权或次序、或者方法的动作被执行的时间顺序，而是仅被用作将具有某一名称的一个权利要求元素与具有相同名称的另一元素（只供次序术语使用）区分开来的标记，以便区分各权利要求元素。

[0104] 而且，在此使用的短语和术语是用于描述的目的，且不应被看作是限制。在此“包括(include)”、“包括(comprise)”或“具有”、“包含”、“涉及”和及其变体来意指包含其后所列出的项及其等效物以及附加的项。

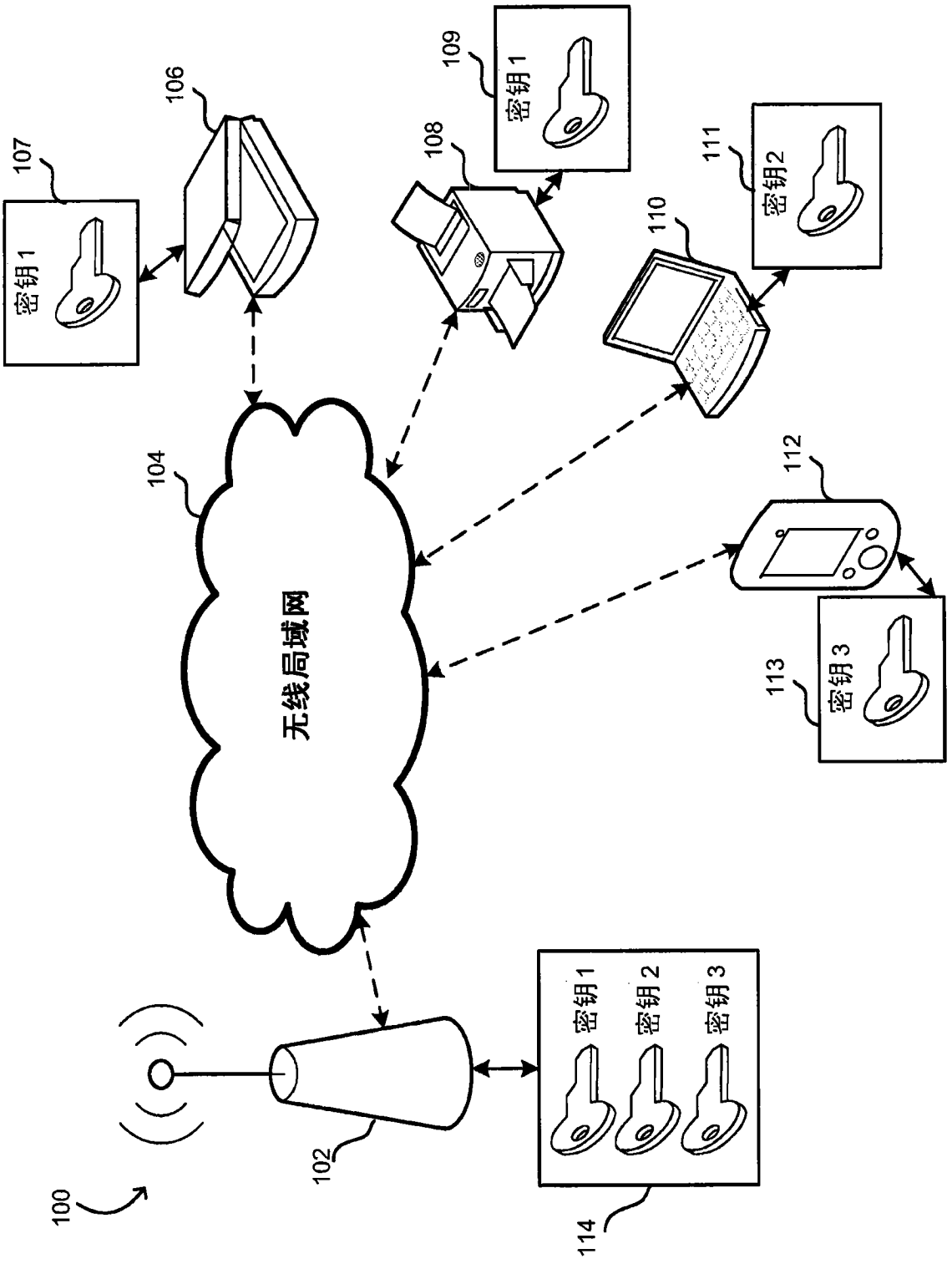

100
102
104
无线局域网
106
107
密钥1
108
109
密钥1
110
111
密钥2
112
113
密钥3
114
密钥1
密钥2
密钥3

图 1

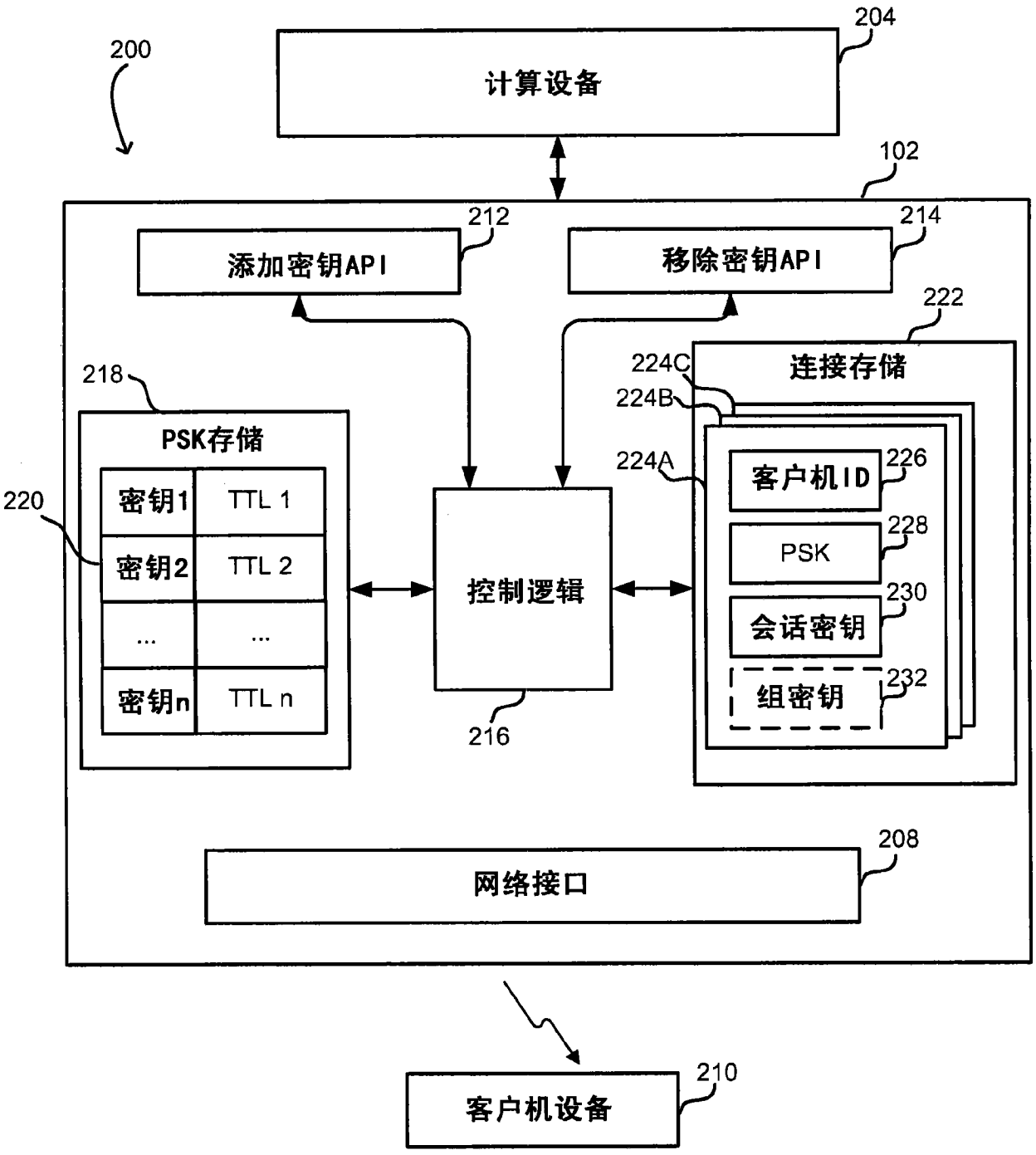

200
204
计算设备
102
212
添加密钥API
214
移除密钥API
222
连接存储
224C
224B
224A
218
PSK存储
220
密钥1
TTL 1
密钥2
TTL 2
...
...
密钥n
TTL n
控制逻辑
216
客户机ID
226
PSK
228
会话密钥
230
组密钥
232
208
网络接口
210
客户机设备

图 2

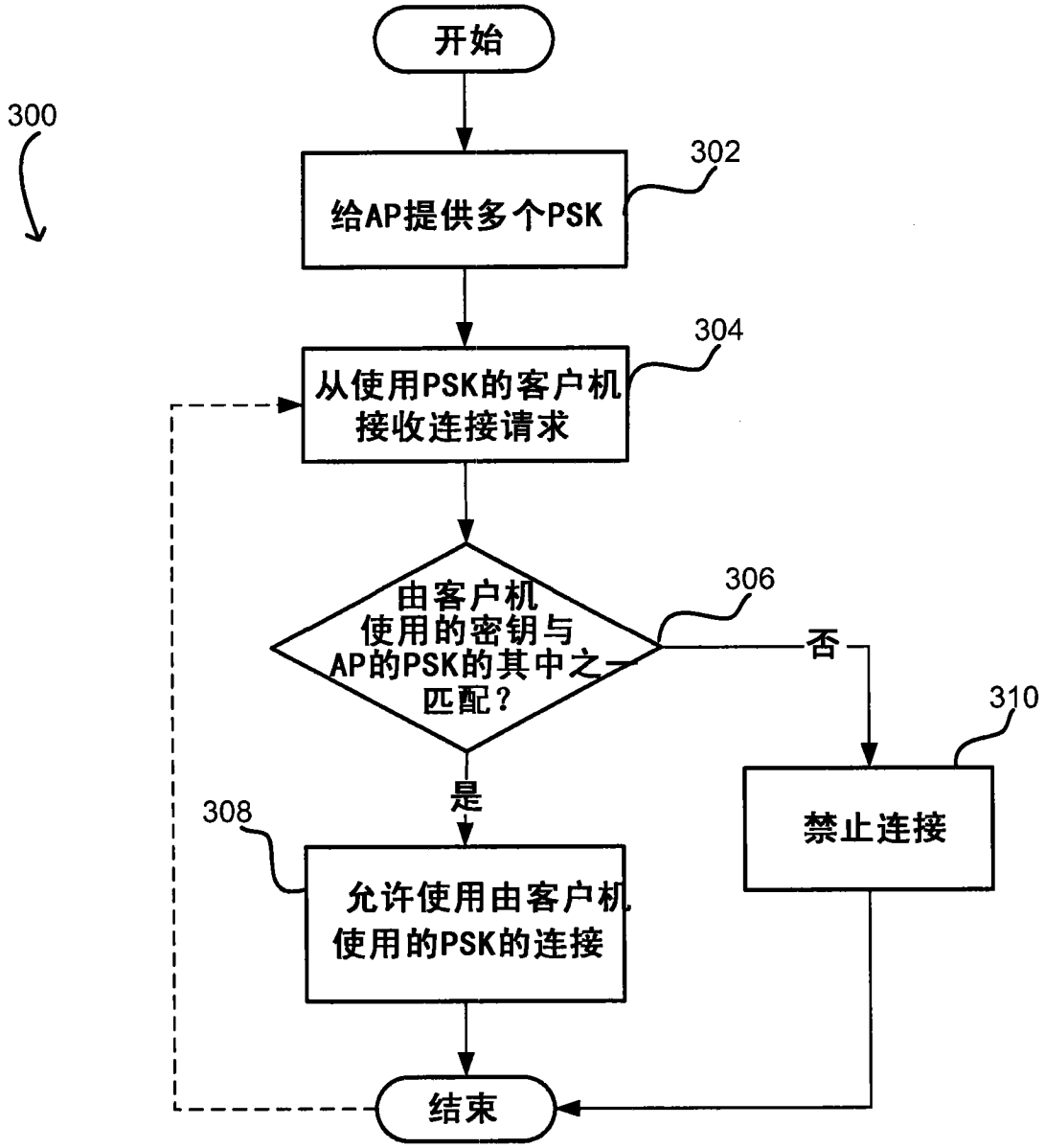

300
开始
302
给AP提供多个PSK
304
从使用PSK的客户机
接收连接请求
306
由客户机
使用的密钥与
AP的PSK的其中之一
匹配？
否
是
310
禁止连接
308
允许使用由客户机
使用的PSK的连接
结束

图 3

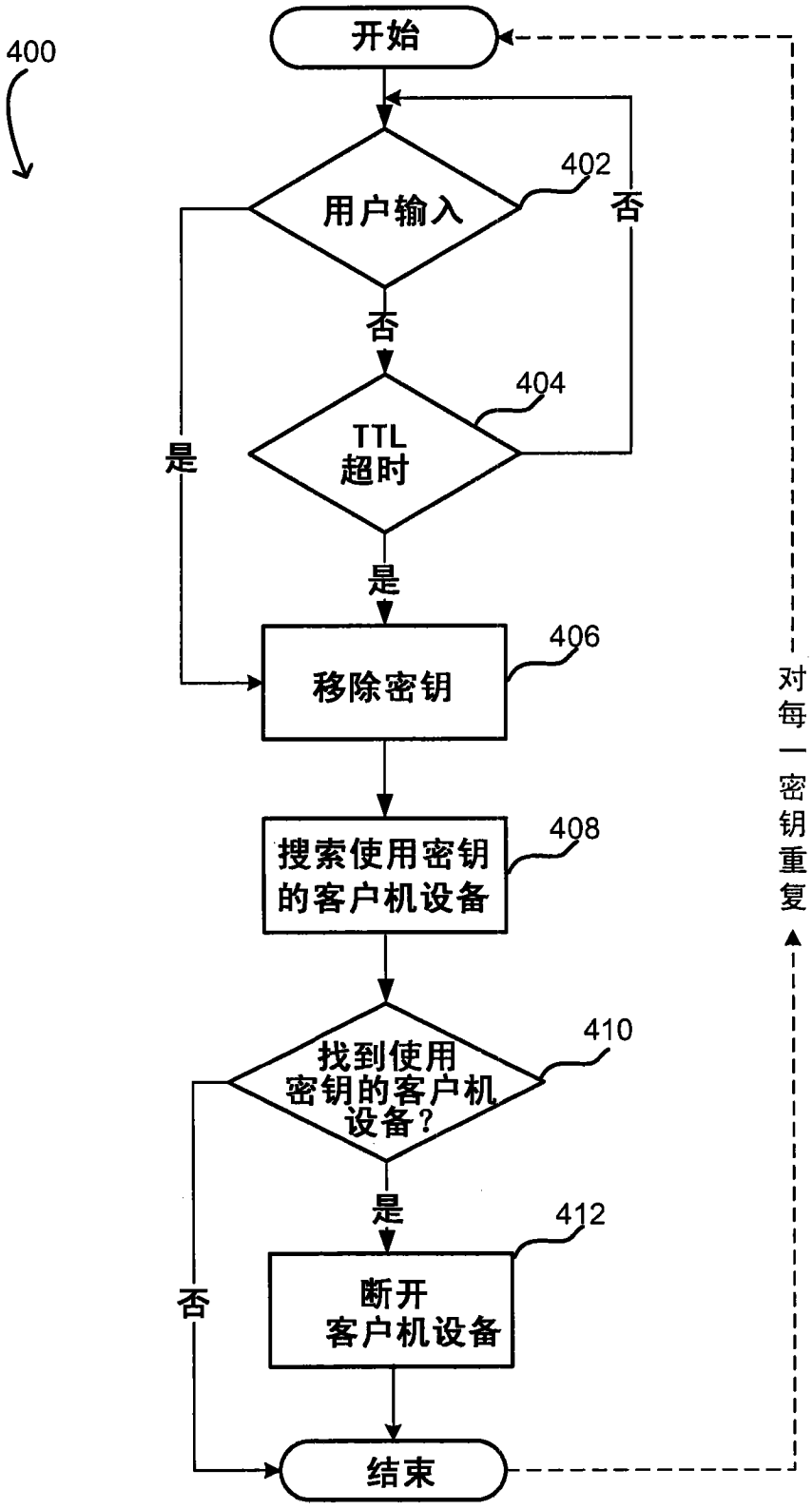

400
开始
用户输入
402
否
否
TTL
超时
404
是
是
移除密钥
406
搜索使用密钥
的客户机设备
408
找到使用
密钥的客户机
设备?
410
是
412
否
断开
客户机设备
结束
对每一密钥重复

图 4

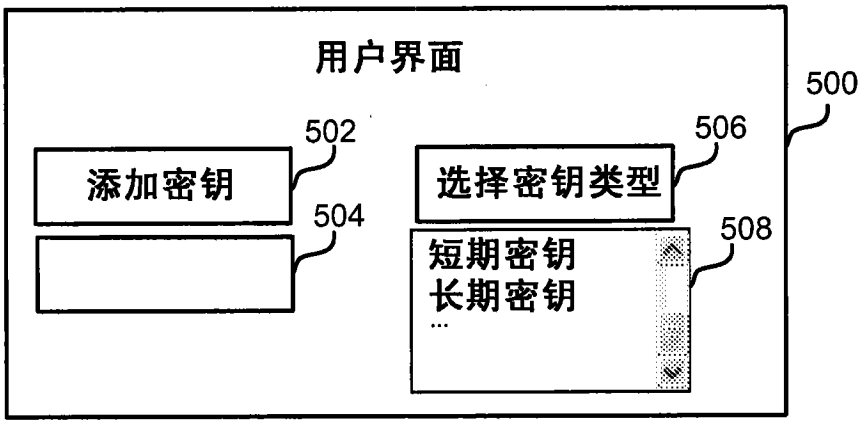

用户界面
500
502
添加密钥
504
506
选择密钥类型
508
短期密钥
长期密钥
...

图 5A

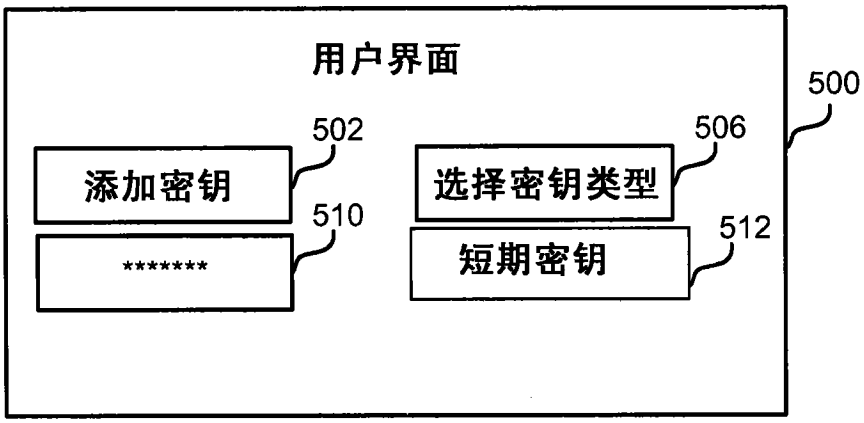

用户界面
500
502
添加密钥
510
****
506
选择密钥类型
512
短期密钥

图 5B

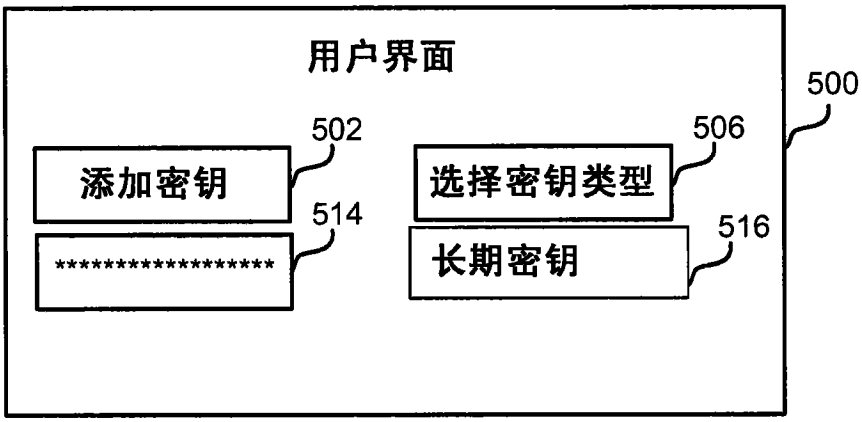

用户界面
500
502
添加密钥
514
****
506
选择密钥类型
516
长期密钥

图 5C

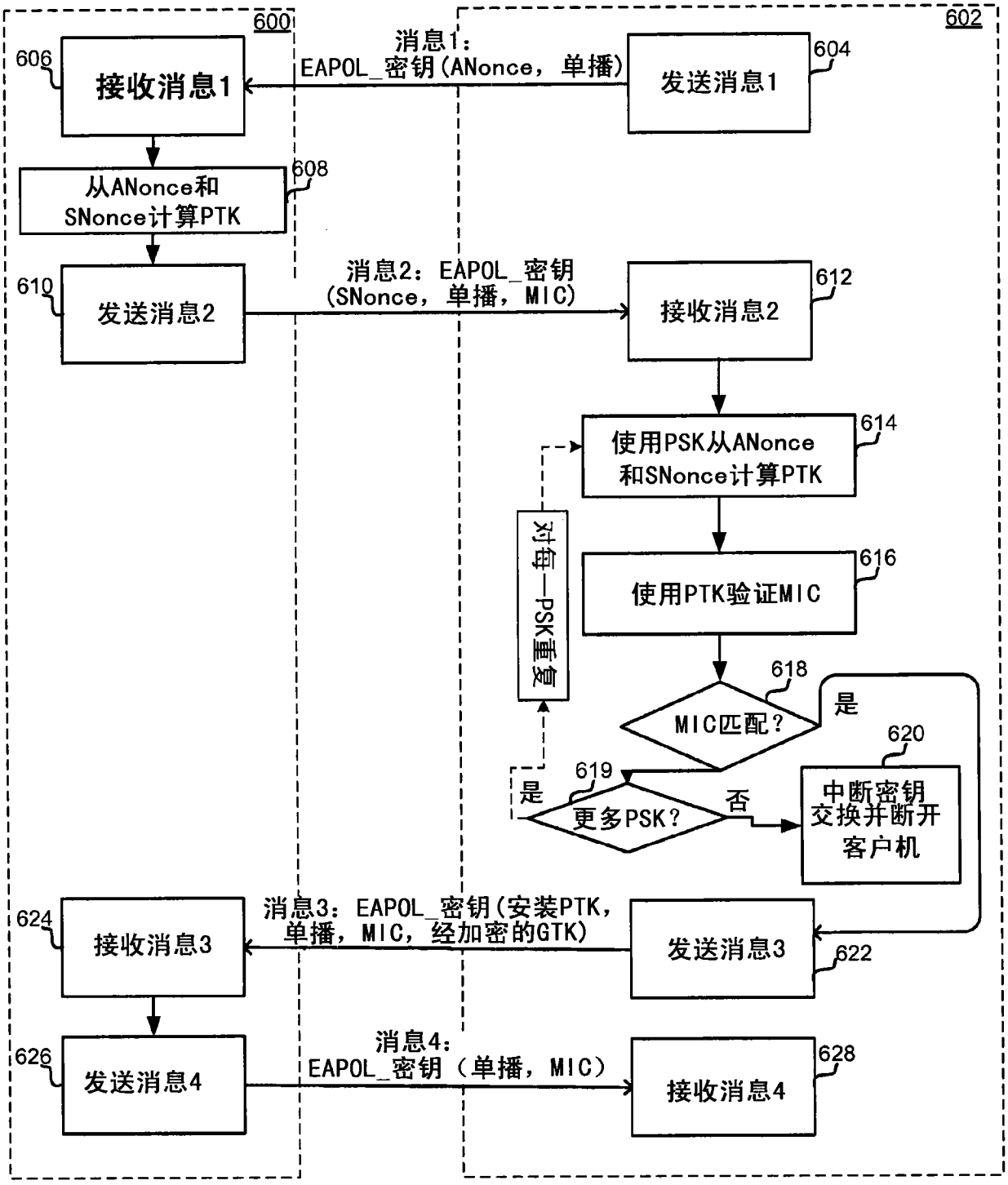

600
602
606
接收消息1
消息1：
EAPOL_密钥(ANonce，单播)
发送消息1
604
从ANonce和
SNonce计算PTK
608
610
发送消息2
消息2：EAPOL_密钥
(SNonce，单播，MIC)
接收消息2
612
使用PSK从ANonce
和SNonce计算PTK
614
对每一PSK重复
使用PTK验证MIC
616
618
MIC匹配？
是
620
619
是
更多PSK？
否
中断密钥
交换并断开
客户机
624
接收消息3
消息3：EAPOL_密钥(安装PTK，
单播，MIC，经加密的GTK)
发送消息3
622
626
发送消息4
消息4：
EAPOL_密钥（单播，MIC）
接收消息4
628

图 6

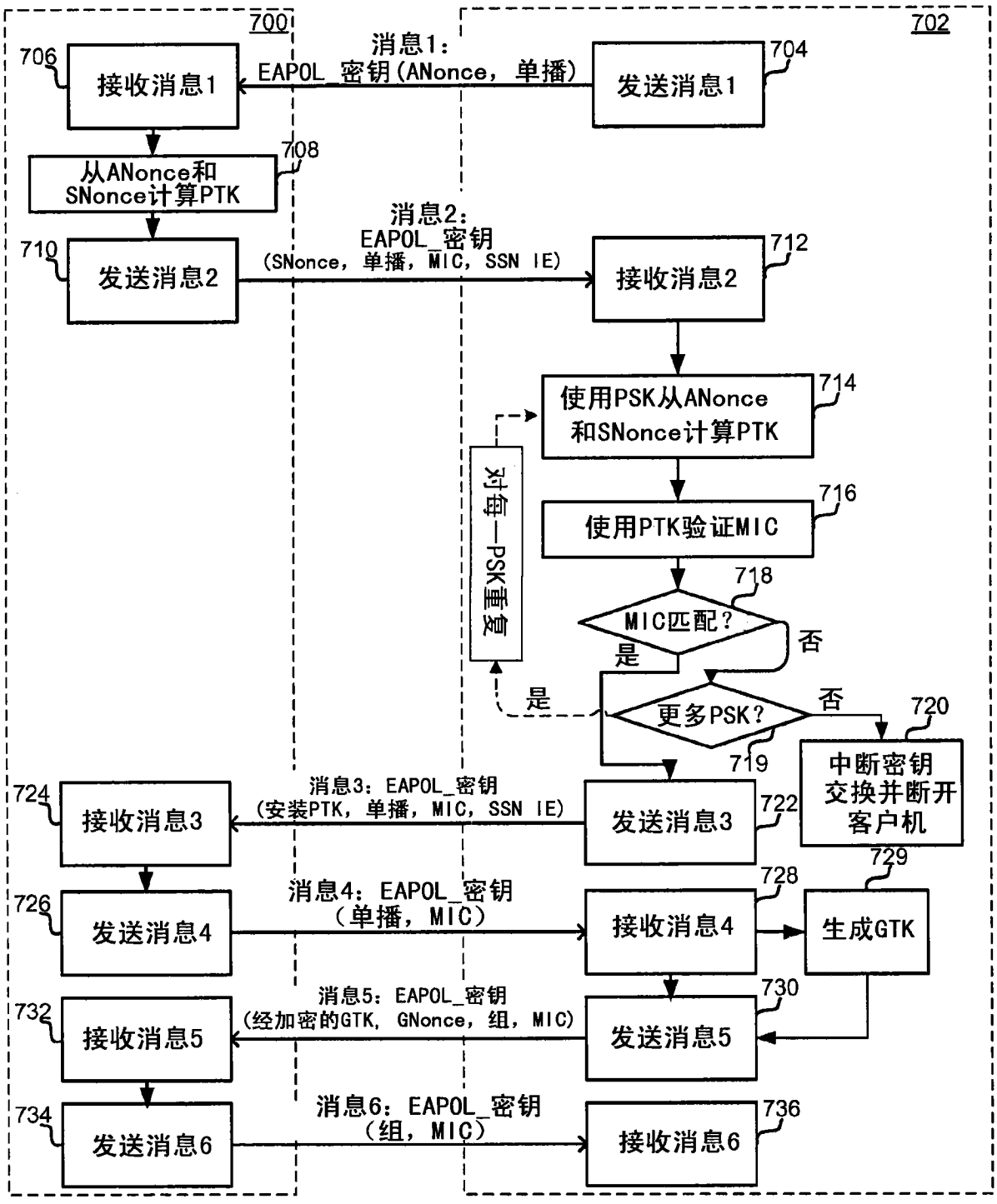

700
702
706
接收消息1
消息1：
EAPOL_密钥(ANonce，单播)
发送消息1
704
708
从ANonce和
SNonce计算PTK
710
发送消息2
消息2：
EAPOL_密钥
(SNonce，单播，MIC，SSN IE)
接收消息2
712
使用PSK从ANonce
和SNonce计算PTK
714
对每一PSK重复
使用PTK验证MIC
716
718
MIC匹配？
否
是
是
更多PSK？
否
720
719
中断密钥
交换并断开
客户机
724
接收消息3
消息3：EAPOL_密钥
(安装PTK，单播，MIC，SSN IE)
发送消息3
722
729
726
发送消息4
消息4：EAPOL_密钥
（单播，MIC）
接收消息4
728
生成GTK
732
接收消息5
消息5：EAPOL_密钥
(经加密的GTK，GNonce，组，MIC)
发送消息5
730
734
发送消息6
消息6：EAPOL_密钥
（组，MIC）
接收消息6
736

图 7