(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 101965710 B
(45)授权公告日 2015.08.19

(21)申请号 200980106136.8
(22)申请日 2009.01.20
(30)优先权数据
12/035,531 2008.02.22 US
(85)PCT国际申请进入国家阶段日
2010.08.20
(86)PCT国际申请的申请数据
PCT/US2009/031451 2009.01.20
(87)PCT国际申请的公布数据
WO2009/105302 EN 2009.08.27
(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 H·沈 A·A·哈萨恩 Y·陆
T·W·库纳尔 A·T·巴隆 D·吴
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨洁 钱静芳
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04W 12/10(2009.01)
G06Q 30/02(2012.01)
(56)对比文件
CN 1631010 A,2005.06.22,说明书第4页第7行-第9页第5行,附图1、6.
CN 1757195 A,2006.04.05,说明书第4页第18行-第9页第17行,附图1.
审查员 肖瑜

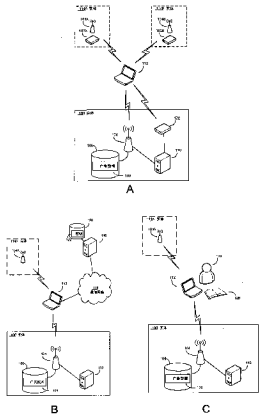
权利要求书1页 说明书15页 附图10页

(54)发明名称

用于无线网络的认证机制

(57)摘要

一种用于传送诸如广告等内容的无线网络的安全技术和安全机制。根据各示例性技术,可以响应于来自客户机设备的请求来传送包括未经请求的内容(例如,广告数据)的控制消息,而在其他示例性技术中,该控制消息可以在没有来自客户机设备的任何请求的情况下传送。在一些示例性实现中,可以使用诸如公钥密码算法等安全机制来保护传输。在这些技术中的实现公钥密码的一些技术中,需要用户从不同于传送加密广告的无线接入点的源来检索公钥(例如,传送这些广告的商业实体中的标牌或终端,或从web服务),以使该用户可以确认加密内容来自与检索到的公钥相匹配的源并因而确认无线接入点的真实性。



CN 101965710 B

1. 一种操作客户机设备 (112) 来显示与一实体相关的内容的方法，所述方法包括：

从不同于无线接入点的源获取对应于所述无线接入点的信任信息，其中所获取的信任信息包括所述无线接入点的公钥；

从所述无线接入点接收包含所述内容的加密消息，但所述客户机设备不连接到由所述无线接入点提供访问的任何网络；

基于所获取的信任信息来验证所述无线接入点的身份，其中所述验证基于使用所述信任信息中的公钥成功地解密了从所述无线接入点接收到的所述加密消息；以及

将经解密的消息中包含的所述内容的至少一部分显示给用户。

2. 如权利要求 1 所述的方法，其特征在于，所述验证动作包括向所述无线接入点传送至少一个消息 (306)。

3. 如权利要求 2 所述的方法，其特征在于，所述实体 (100) 是商场或购物中心，并且所述信任信息是所述商场和 / 或该商场中的商家的一个或多个信任信息片段。

4. 如权利要求 1 所述的方法，其特征在于，所述获取基于近场通信。

5. 如权利要求 1 所述的方法，其特征在于，获取所述信任信息包括从担当信任信息的储存库的 web 服务 (116) 获取所述信任信息。

6. 如权利要求 1 所述的方法，其特征在于，获取所述信任信息的动作包括用户 (124) 在从目录获取了所述信任信息之后输入它。

7. 如权利要求 1 所述的方法，其特征在于，所接收的加密消息包括无线接入点的位置数据。

8. 一种在客户机设备上执行的用于显示与一实体相关的内容的系统，所述系统包括：

用于从不同于无线接入点的源获取对应于所述无线接入点的信任信息的装置，其中所获取的信任信息包括所述无线接入点的公钥；

用于从所述无线接入点接收包含所述内容的加密消息的装置，但所述客户机设备不连接到由所述无线接入点提供访问的任何网络；

用于基于所获取的信任信息来验证所述无线接入点的身份的装置，其中所述验证基于使用所述信任信息中的公钥成功地解密了从所述无线接入点接收到的所述加密消息；以及

用于将经解密消息中包含的所述内容的至少一部分显示给用户的装置。

9. 如权利要求 8 所述的系统，其特征在于，所述内容是描述所述无线接入点的位置的位置数据。

用于无线网络的认证机制

[0001] 发明背景

[0002] 常规基于 web 的广告框架通常通过连接向基于 web 的服务的消费者发送广告，该连接是客户机设备已通过网络建立的与主存该基于 web 的服务的服务器的连接。例如，服务器的所有者 / 管理员可以配置该服务器响应于客户机设备的用户将统一资源定位符 (URL) 输入到该客户机设备来向该客户机设备发送带有广告的网页。该广告可以是文本 / 图像 / 视频 / 音频数据的形式，并可以嵌入在网页中，或可以是在显示客户机设备所访问的网页之前向用户显示的初始网页。

[0003] 在这样的广告框架中，广告在基于 web 的服务（例如，网站）与该基于 web 的服务的用户之间进行交换。用户的客户机设备与之相连并且该客户机设备通过其访问该基于 web 的服务的网络对控制网页内容的参与有限，并且因此具有向客户机设备的用户提供广告的有限能力。相反，一些网络实现替换的、互补广告框架，例如向连接到该网络的客户机设备的用户发送包含广告的网页的那些框架。这些网络所实现的广告框架例如可能需要网络的用户在首次连接到该网络时查看初始网页，或可能使用该网络周期性地向客户机设备发送包含广告的网页。

[0004] 发明概述

[0005] 用于无线网络的常规广告框架在其向用户发送广告的能力方面受到限制，因为广告只可发送给具有与该无线网络的已建立连接的客户机设备和 / 或从该无线网络请求数据的客户机设备。如果广告可以发送给未连接到无线网络的客户机设备，则广告可到达更多用户并且做广告的商家可以吸引更多顾客或更多收益。

[0006] 然而，使客户机设备能够开放地接受来自它们未连接到的网络的未经请求的内容可使这些设备的用户对各种风险开放。例如，不合需要的广告（例如，色情广告）可能由用户不感兴趣的组织发送，或由冒充该用户感兴趣的组织的恶意一方发送。在没有标识发送广告和其他内容的网络的任何安全机制和 / 或方法的情况下，这样的不合需要的广告可能被客户机设备接收并被显示给用户，并且可对用户造成冒犯或侮辱。

[0007] 除广告框架之外的框架也可以从能够向客户机设备发送未经请求的内容中获益，并且进而，这些客户机设备可以从标识发送未经请求的内容的网络的安全机制和 / 或方法中获益。例如，无线接入点可以将它们自己的位置数据发送给跟踪它们自己位置的客户机设备，并且确认这些无线接入点的身份可以防止恶意各方广播欺骗性位置数据。

[0008] 本文公开了用于发送诸如广告等内容的无线网络的安全技术和安全机制的各种原理。根据各示例性技术中的一些技术，可以响应于来自客户机设备的请求来传送包括未经请求的内容（例如，广告数据）的控制消息，而在其他示例性技术中，该控制消息可以在没有来自客户机设备的任何请求的情况下传送。在一些示例性实现中，可以使用诸如公钥密码算法等安全机制来保护传输。在这些技术中的实现公钥密码的一些技术中，需要用户从不同于传送加密广告的无线接入点的源（例如，传送这些广告的商业实体中的标牌或终端，或从 web 服务）来检索公钥，以使该用户可以确认加密内容来自与检索到的公钥相匹配的源并因而确认无线接入点的真实性。

[0009] 在一个实施例中，提供了一种操作客户机设备来显示与商业服务相关的广告信息的方法。该方法包括获取无线接入点的信任信息，基于该信任信息来验证来自该无线接入点的控制传输的真实性，并且至少部分地基于该验证动作来将控制消息中包含的至少一个商业服务的广告选择性地显示给用户。

[0010] 在另一实施例中，提供了用计算机可执行指令编码的至少一个计算机可读介质，该计算机可执行指令在被执行时使得计算机执行一种用于确认来自与一实体相关联的无线接入点的控制传输的真实性的方法。该方法包括获取该实体的信任信息，使用该信任信息来验证来自无线接入点的控制传输的真实性，并且至少部分地基于该验证动作来选择性地使用该控制传输的内容。

[0011] 在又一实施例中，提供了一种用于在无线网络中发送控制消息的装置。该装置包括存储信任信息和内容的至少一个数据存储，适用于构造包括内容的控制传输并使用该信任信息对该控制传输的至少一部分进行加密的至少一个处理器，以及用于发送控制传输的通信电路。

[0012] 附图简述

[0013] 附图不旨在按比例绘制。在附图中，各个附图中示出的每一完全相同或近乎完全相同的组件由同样的标号来表示。出于简明的目的，不是每个组件在每张附图中均被标号。在附图中：

[0014] 图 1A 是本文公开的用于发送、接收、以及验证控制消息的真实性的技术中的一些而非全部技术可以在其中操作的示例性计算机系统的示图，该计算机系统包括可从中读取实体的信任信息的自助服务终端；

[0015] 图 1B 是本文公开的用于发送、接收、以及验证控制消息的真实性的技术中的一些而非全部技术可以在其中操作的示例性计算机系统的示图，该计算机系统包括主存可从中检索信任信息的网站的 web 服务器；

[0016] 图 1C 是本文公开的用于发送、接收、以及验证控制消息的真实性的技术中的一些而非全部技术可以在其中操作的示例性系统的示图，该系统包括可从中检索信任信息的纸质目录；

[0017] 图 2 是实现本文公开的原理中的一些的可由计算机系统实现来用于在无线网络和客户机设备之间交换关于商业服务的信息的说明性过程的流程图；

[0018] 图 3 是实现本文公开的原理中的一些的用于确认无线网络的无线接入点的真实性的一种示例性技术的流程图；

[0019] 图 4 是实现本文公开的原理中的一些的用于确认从无线网络的无线接入点接收到的控制消息的真实性的一种示例性技术的流程图；

[0020] 图 5 是实现本文公开的原理中的一些的用于确认从无线网络的无线接入点接收到的控制消息的真实性的另一示例性技术的流程图；

[0021] 图 6 是实现本文公开的原理中的一些的可由无线接入点用来发送控制消息的示例性技术的流程图；

[0022] 图 7 是可以实现本文公开的技术中的一些而非全部技术的用于发送和验证控制消息的真实性的示例性无线接入点的框图；以及

[0023] 图 8 是可以实现本文公开的技术中的一些而非全部技术的用于接收和验证从无

线网络的无线接入点接收到的控制消息的真实性的示例性客户机设备的框图。

[0024] 详细描述

[0025] 申请人明白，商家和消费者都可从用于使基于计算机的广告对例如接近可使用被广告服务的位置的消费者可用的简单机制中受益。例如，用户可以获悉商家所提供的廉价销售或特别促销。同样，用户可以获悉商家所提供的服务来在进入该商家的场所之前确定该用户是否对该商家所提供的服务感兴趣。

[0026] 相反，广告客户可使广告聚焦于接近它们的处所并且因而最可能进行购买的潜在顾客。例如，具有无线网络的餐厅可通过向射程内的客户机设备发送该餐厅的每日特价的描述来设法吸引更多顾客。常规广告框架不能以此方式传送广告。尽管能够向大量用户发送广告，但常规框架被限于向已通过无线接入点连接到无线网络的客户机设备的、向该无线网络请求数据的用户显示广告。这样的常规框架不能够向未连接到该无线网络的用户显示广告或不能够向不知道请求信息的用户通知有该用户附近的商家的广告可用。

[0027] 申请人认识到向未连接到该商家所操作的无线网络的客户机设备的用户对商家的服务（包括诸如销售一种或多种产品等服务）作广告的需求。如果商家能够将向其无线网络射程内的所有客户机设备而非只是连接到该无线网络的客户机设备对其产品或服务作广告，则广告将能够到达更广泛的受众并且商家可能吸引更多顾客和更多收益。此外，处于无线网络射程内的客户机设备的用户是最可能的潜在顾客组，因为在他们接收到所发送的广告时他们在商家附近。

[0028] 然而，申请人另外认识到，使客户机设备能够在不验证网络和/或内容的真实性的情况下从邻近网络开放地接收内容并将该内容显示给用户使用户对各种风险开放。例如，可能显示用户不感兴趣的广告，和/或可能显示冒犯用户的广告。例如，逛购物中心的用户可能走进销售该用户感到不合需要（例如，色情出版物）商品的商家的范围内，并且该用户可能对该商家的任何广告感到不合需要或冒犯。此外，如果客户机设备向用户显示所有接收到的广告，则恶意第三方可以建立欺骗性无线网络并发送广告，这些广告看来是合法源但实际上是客户机设备将自动地显示给用户的冒犯和/或不合需要的图像和/或文本。

[0029] 另外，申请人认识到，除广告框架之外的框架可以从通过无线网络向客户机设备发送未经请求的内容中获益，并且这些客户机设备可以从在接受该内容之前确认这些网络的身份中获益。例如，广播指示无线接入点的位置的数据的无线接入点对尝试查明其自己位置的、处于该无线接入点的射程内的客户机设备而言是有用的。然而，当在没有用于确认无线接入点和/或无线网络的身份的任何适当技术的情况下，在这一场景中，客户机设备对接受来自恶意第三方的欺骗位置数据开放。与客户机设备无线地交换信息的其他框架也可类似地从本文公开的技术中获益。

[0030] 申请人因此认识到对用于无线网络的、使客户机设备能够在接受来自该无线网络的未经请求的信息之前确认该无线网络的身份的安全机制的需求。安全机制可以准许用户和/或客户机设备验证来自无线接入点的包含内容（例如，广告、位置数据、或其他信息）的控制消息的真实性。作为替换或补充，安全机制可被用来在将内容显示给用户之前验证包括发送控制消息的一个或多个无线接入点或任何合适框架的任何其他组件的无线网络的真实性。另外，安全机制可以准许用户限制该用户希望客户机设备使用的内容（例如，选

择来显示给用户的内容）。

[0031] 鉴于以上描述，设计了针对用于确认无线网络的身份的安全机制的各种技术。在一种示例性技术中，用户接收一个或多个商业实体的信任信息，使用该信任信息来验证一个或多个控制传输或网络组件的真实性，以及基于该确认的成功来选择性地显示来自这些商业实体的一个或多个控制传输中包含的内容。

[0032] 任何合适的传输可以是根据本文描述的原理中的一个或多个的控制传输。例如，诸如通告传输等层 2 控制传输可包括关于无线接入点的任何合适的信息，包括使得接收到该控制传输的客户机设备能够打开到无线接入点的连接的一个或多个网络特性。通告传输可以是例如无线接入点根据电气和电子工程师协会 (IEEE)802.11 无线协议向该无线接入点射程内的所有客户机设备周期性地广播的信标、响应于客户机设备所发送的对控制信息的请求而发送到该客户机设备的探查响应、或无线接入点所发送的任何其他合适的通告传输。客户机设备向无线接入点发送的控制传输可以是任何合适的传输，如请求关于无线接入点和 / 或无线网络的控制信息的可以包括或不包括测试数据的探查、任何合适类型的认证测试消息、和 / 或任何其他合适的传输。

[0033] 在本文描述的一些而非全部实现中，安全技术可被实现成单向或双向公钥加密算法。在其中确实使用公钥加密的实现中，可以使用诸如流行的 Rivest-Shamir-Adleman(RSA) 公钥算法等任何合适的公钥算法，但本发明不限于实现任何特定安全技术或任何特定公钥算法。

[0034] 在一些实现中，诸如实现公钥密码的那些实现，用户或客户机设备可以从诸如书籍、签名、密钥服务、电子密钥提供器、使用诸如近场通信 (NFC) 协议等一个或多个协议通信的自助服务终端或其他设备或任何其他合适的源等“带外”源（即，与通过无线网络本身不同的源）来获取信任信息。在一些实现中，该信任信息可以是与无线网络或无线接入点相关联的公钥和 / 或证书授权机构所批准的公钥构架 (PKI) 证书。如以下详细描述的，具有无线网络或无线接入点的信任信息的客户机设备可以用任何合适的方式来使用该信任信息以确认该无线接入点和 / 或无线网络的身份。

[0035] 例如，在实现本文描述的原理中的一些的一些技术中，无线接入点可以发送使用与客户机设备检索到的作为信任信息的一部分或全部的公钥相对应的私钥加密的控制传输。在一些实现中，控制传输可被整个地加密，而在替换传输中，只发送控制传输净荷（例如，诸如广告数据等内容或包括一个或多个内容片段的信息元素）的一部分或全部。如果客户机设备能够使用公钥来正确地解密控制消息，则该客户机设备可以确认该控制消息是使用与该检索到的公钥相对应的私钥加密的，并且因此发送该加密控制消息的无线接入点是该客户机设备期望从中接收信息的无线接入点。

[0036] 作为补充或替换，在一些实现中，客户机设备可以交换一个或多个测试传输作为控制传输以测试无线接入点和 / 或无线网络的真实性。例如，客户机设备可以使用信任信息（例如，检索到的公钥）来加密测试数据，并将加密测试数据发送到无线接入点。如果响应于该测试传输从无线接入点接收到的控制传输包含正确的测试数据，则客户机设备可以确认该无线接入点能够正确地解码该传输，并且如此，该无线接入点具有与该公钥相对应的私钥并且是该客户机设备期望与之通信的无线接入点。可以通过向测试数据添加其他信息来提供更高的安全性。这一其他信息可以是任何合适的信息，如客户机设备的公钥，并且

无线接入点所发送的回复可以使用该客户机设备的公钥来加密发送。或者，测试数据可以是现时值或其他唯一符号（例如，唯一文本或发射时间），以使得即使来自无线接入点的控制传输被截取、记录、并从欺骗设备重新广播（使得该欺骗设备看起来是真实的），客户机设备也可以通过使用用于避免重放攻击的一种或多种技术来检测到该控制传输是“重放”的，如通过注意到应当是唯一符号的重复或发射时间中的异常延迟（即，当前时间与控制传输的声称发射时间之间的极差可以暗示控制传输在发射时间被记录并由欺骗设备在稍后的时间重新广播）。

[0037] 应当明白，这些技术仅仅是可实现本文描述的原理的技术的例示，并且本文描述的用于确认无线网络的身份的原理可以使用任何合适的安全机制用任何合适的方式来实现，因为本发明在这一方面没有限制。

[0038] 还应当明白，可以用任何合适的方式来格式化控制传输以包含任何一个或多个合适类型的内容（例如，广告数据和 / 或位置数据）。用于将内容封装在控制传输的各信息元素中的示例性技术在共同待审的美国申请 11/973,589（“Advertising framework for wireless networks（用于无线网络的广告框架）”）和 11/973,590 中讨论（“Transmitting location data in wireless networks（在无线网络中发送位置数据）”）。这些申请描述使用 IEEE 802.11 无线通信协议的各信息元素以及其他格式来在诸如信标和探查响应等控制传输中包括广告和位置数据。然而，本文描述的原理可以使用以任何合适的方式合并内容的任何合适的控制传输来实现，并且不限于本文描述的技术。

[0039] 本文描述的技术可以用包括一个或多个无线网络的任何合适的系统来实现，每一个无线网络都包括一个或多个无线接入点和供客户机设备获取无线网络的信任信息的任何合适的装置，因为本发明在这一方面没有限制。以下描述实现本文描述的原理中的一些的三个示例性系统。

[0040] 图 1A 示出了本文公开的技术中的一些可在其中操作的示例性系统。应当明白，本发明的各实施例可以在任何合适的系统中操作，并且不限于在图 1A 所示的说明性系统中实现。

[0041] 图 1A 的系统包括处于三个无线接入点 104、104A 和 104B 的射程内的示例性客户机设备 112。图 1A 所示的这些无线接入点中的每一个都与一实体相关联，如实体 100、实体 114、以及实体 116。在本发明的一些实施例中，实体可以是商业实体，如商家、商家集合或协会、非盈利性 / 公共组织、或其他商业实体，但可以明白，本发明的各实施例不限于用商业实体来实现。另外，应当明白，如此处所使用的，包括商业实体在内的“实体”可以是任何单个实体，如个人、群体、组织、或商家，或多个人、多个群体、多个组织、多个商家的任何组合，或以任何合适的方式彼此相关联的任何其他实体（例如，作为共享基础设施（如处于一个购物中心中）的商家协会或商家群）。应当明白，尽管以下描述了其中为简明起见该实体被描述为诸如商家或购物中心等商业实体的各示例，但本发明不限于用任何一个或多个特定类型的实体来实现。

[0042] 图 1A 以实体 100 示出根据本发明的各实施例的实体（包括诸如实体 114A 和 114B 等实体）的示例性实现。实体可包括至少一个无线接入点 104，该无线接入点 104 可通信耦合到与该无线接入点 104 相关联的数据存储 106 和服务器 110。数据存储 106 可以是任何合适的计算机可读介质，并可以是无线接入点 104 的组件，或可以直接耦合或通过一个

或多个任何合适的有线和/或无线通信介质耦合到无线接入点 104。如图 1A 所示，在一些实现中，数据存储 106 可以存储包括广告数据在内的、可由无线接入点 104 检索并发送的信息。广告数据 108 可以是可由无线接入点 104 发送的任何一种或多种合适类型的数据，包括例如描述文本、图像、音频、或视频、或其任何组合的数据。广告数据 108 可以是描述与实体 100 相关联的一个或多个服务的单个广告的数据，或可以是描述与实体 100 相关联的一个或多个服务的多个广告的数据。应当明白，如上所述，广告数据仅仅是可由无线网络的无线接入点发送的各类型数据的例示，并且可以发送任何合适的一个或多个类型的信息，因为本发明在这一方面没有限制。

[0043] 服务器 110 可以是用于存储要提供给连接到无线接入点 104 的客户机设备的信息（例如，数据和/或指令）的任何合适的计算装置。尽管图 1 将服务器 110 示为与无线接入点 104 和数据存储 106 分开，但在本发明的一些实施例中，服务器 110 可以是无线接入点 104 的组件和/或可以被实现为担当服务器 110 和数据存储 106 两者的包括一个或多个计算机可读介质的电子设备。在所示实施例中，服务器 110 连接到只要设备与无线接入点 104 相关联并获得对网络的访问权就可访问的网络。然而，应当明白，图 1A 的系统仅仅是示例性的，并且本发明不需要提供广告数据或其他内容的无线接入点最终支持到其他连网设备的连接。

[0044] 在一些实现中，服务器 110 所存储的信息可包括与数据存储 106 所存储的广告数据 108 所描述的一个或多个广告相关的信息。与该一个或多个广告相关的信息可以是任何合适的信息，包括例如描述广告数据 108 所广告的一个或多个产品或服务的一个或多个网页。在所示实施例中，数据存储 106 可不完全定义广告数据 108 所描述的广告的内容。然而，例如，这样的广告可包含指向服务器 110 的 URL 以使用户可选择通过无线接入点 104 或任何其他合适的网络连接到服务器 110，从而获得与所广告的服务相关的信息。

[0045] 无线接入点 104 可以是根据一个或多个无线连网协议生成信号的任何合适的无线信号生成器。例如，无线接入点可以是根据针对无线局域网 (WLAN) 的电气和电子工程师学会 (IEEE)802.11 标准操作的 WiFi 接入点，可以是根据任何合适的无线广域网 (WWAN) 协议（例如，全球移动通信系统 (GSM)）、诸如蓝牙等个域网 (PAN) 协议、诸如微波存取全球互通 (WiMAX) 协议和超宽带 (UWB) 协议等其他协议、或任何其他合适的无线协议来操作 WWAN 的蜂窝样式无线接入点。在具有多个无线接入点的实体中，这些无线接入点可以根据同一无线协议来操作或可以根据不同的无线协议来操作。

[0046] 如上所述，实现本文描述的原理中的一些的系统可以具有用于除通过无线接入点和无线网络本身之外（即，带外源）获取无线接入点和无线网络的信任信息的方法。在一些非优选实现中，信任信息可以从无线网络本身检索，但应当明白，带外源是优选的。

[0047] 在图 1A 的实施例中，实体 100 配备了客户机设备可从中检索信任信息的自助服务终端 102。自助服务终端 102 可以是例如位于实体 100 内或其附近的电子设备。在一些实现中，自助服务终端 102 可以是安装在商家入口处或者购物中心入口处或者商家或购物中心各处的位置处（例如安装在柱子或墙上）的、用户可以访问以检索该商家或购物中心的一个或多个信任信息片段的设备。客户机设备 112 可以与自助服务终端 102 通信以用任何合适的方式来检索信任信息。在一些实现中，客户机设备 112 可以使用诸如 WLAN 或 PAN 协议等任何合适的无线协议或者使用任何合适的近场通信 (NFC) 协议（例如，射频识别 (RFID)

技术）或者使用任何合适的有线或基于接触的通信技术来与自助服务终端 102 通信。例如，在一些实现中，用户可以从自助服务终端 102 检索要插入到客户机设备 112 的、客户机设备 112 可以从中复制信任信息或用户可以在商家或购物中心购物（或以其他方式与实体进行交互）时持有的存储器单元（例如，存储器卡）。如上所述，从自助服务终端 102 检索到的信任信息可以是任何合适的信任信息，如实体 100 的公钥或 PKI 证书。

[0048] 如图 1A 所示，接收来自一个或多个无线接入点 104、104A、以及 104B 的传输的客户机设备 112 可以是膝上型个人计算机。然而，应当理解，本发明的各实施例不限于用膝上型个人计算机来实现，而可以用用于接收无线信号的、移动或非移动的任何合适的电子设备来实现，如台式或膝上型个人计算机、个人数字助理 (PDA)、或智能电话。

[0049] 客户机设备 112 可以具有或不具有开放到一个或多个无线接入点 104、104A 和 104B 的连接，但处于无线接入点 104、104A 和 104B 中的每一个的射程内并能够接收来自无线接入点 104、104A 和 104B 的传输。如上所述，根据本发明的各实施例，接收到的来自无线接入点 104、104A 和 104B 的传输可包括任何合适的信息，包括数据存储 106 所存储的广告数据 108。根据一些说明性技术，无线接入点 104、104A 和 104B 所发送的并由客户机设备 112 接收的传输可以是层 2 控制传输。诸如通告传输等层 2 控制传输可包括关于无线接入点 104 的任何合适的信息，包括使得接收到该控制传输的客户机设备能够打开到无线接入点 104 的连接的一个或多个网络特性。如上所述，通告传输可以是例如无线接入点 104 根据 IEEE 802.11 无线协议向该无线接入点 104 射程内的所有客户机设备（包括客户机设备 112）周期性地广播的信标、响应于客户机设备 112 所发送的对控制信息的请求而发送到客户机设备 112 的探查响应、或无线接入点 104 所发送的任何其他合适的通告传输。

[0050] 在本发明的一些实施例中，无线接入点 104 可以将数据存储 106 所存储的广告数据 108 编码在控制传输中。如下更详细地讨论的，客户机设备 112 可适于接收包括内容（例如，广告数据 108 或任何其他合适的内容）的控制传输并从控制传输中读取该内容。一旦读取了该内容，则可以用任何合适的方式来处理该内容，如通过任何合适的用户界面向客户机设备 112 的用户提供广告数据 108 所描述的广告。在其中可实现本文描述的用于安全的技术的一些广告框架中，用户随后可以查看广告，并可以指示客户机设备 112 他或她想要关于该广告所描述的产品或服务的更多信息。客户机设备随后可以建立与发送用户指示他或她感兴趣的广告的无线接入点的连接（在客户机设备 112 尚不具有与该无线接入点的开放连接的情况下），并检索关于该广告所描述的一个或多个服务的任何合适的附加信息。该附加信息可包括包含关于该服务的更多信息的一个或多个网页或用户可从中预订或订购该服务的一个或多个网页。然而，应当明白，在实现本文描述的技术的一些广告框架中，该附加信息可以不是一个或多个网页，而改为是可以提供给客户机设备的用户的任何合适的附加信息。

[0051] 应当明白，图 1A 中的示例性计算机系统仅仅是说明性的，并且本发明的各实施例可以在包括任何合适数量的客户机设备、实体、以及无线接入点的任何合适的计算机系统中操作。此外，应当明白，实体和无线接入点不限于如图 1A 的示例中所示的那样来实现，因为本发明的各实施例可以用采用任何合适的硬件和 / 或软件的任何合适的实体来实现。

[0052] 图 1B 和 1C 示出实现本文描述的原理中的一些的技术可在其中操作的替换系统。如图 1B 和 1C 所示，实体 100′ 和 114A′ 基本上类似于图 1A 所示的实体，但这些实体未被

示为包括自助服务终端 102。相反，在图 1B 中，服务器 116 被示为通过包括一个或多个任何合适的有线和 / 或无线通信介质的通信网络 118 通信连接到客户机设备的用户 112。服务器 116 可以是用于以任何合适的方式提供一个或多个实体的信任信息的服务器，如通过可担当用于发行 PKI 证书的证书授权机构和 / 或任何一个或多个类型的信任信息的储存库的网站或者 web 服务诸如可从华盛顿州雷蒙德市的微软公司获得的 MSN 或 Windows Live 服务等。担当信任信息的储存库的网站可被构造成实体的信任信息的在线目录，类似于电话号码的在线目录。在诸如图 1B 的系统等系统中操作的技术中，客户机设备 112 的用户在访问实体之前可以检索该实体（例如，实体 100′ 或实体 114A′ ）的信任信息，以便用户不必从自助服务终端 102 检索信任信息或以便该实体不必提供自助服务终端 102。或者，客户机设备可以在访问实体的同时（例如，在商家购物时）通过经由与无线接入点 104 的无线网络不同的无线和 / 或有线网络（例如，通过接入 WWAN 网络）访问服务器 116 来检索信任信息。

[0053] 服务器 116 具有包括一个或多个实体的一个或多个信任信息片段 122（在图 1B 中被示为“密钥”，但不限于此）的数据存储 120。在该系统中操作的一些技术中，用户可以从服务器 116 请求单独实体的单独密钥，或可以按任何合适的组请求多个密钥，诸如特定地理位置中的各实体或处于特定地理位置的特定范围内的各实体、特定类型的各实体、和 / 或以特定方式彼此相关联的各实体（例如，指定购物中心内的所有商家）。

[0054] 图 1C 的系统示出客户机设备 112 可以检索一个或多个实体的信任信息的另一方式。在图 1C 的系统中，客户机设备 112 的用户 124 可以使用物理目录 126 来检索一个或多个实体 100 ‘的信任信息并随后通过任何合适的用户界面将该信任信息手动地输入到客户机设备 112。该目录可以用任何合适的方式来构造，如以类似于常规电话簿的书籍格式（如图 1C 所示）或可以在该实体内展示（例如，安装在墙上）或靠近该实体（例如，以类似于购物中心中的楼层图目录的格式或作为商家入口处的标牌）的列出信任信息的标牌。目录 126 可以提供一个或多个实体的信任信息。在其中目录 126 提供多个实体的信息的情况下，所列出的实体可以是任何合适的编组中的实体，如一个或多个特定类型的实体、特定地理区域内的实体、或根据任何其他编组。用户 124 可以在访问实体之前使用目录 126 来检索该实体的信任信息（例如，在其中目录 126 被构造成像电话簿一样的情况下），或可以在访问该实体时使用目录 126（例如，在其中目录 126 是标牌的情况下）。

[0055] 应当明白，在一些实现中，在一个系统中可以实现用于允许客户机设备检索信任信息的多种技术。例如，实体可以使其信任信息可通过 web 服务和 / 或目录获得，并可另外地提供可从中检索信任信息的一个或多个自助服务终端，并且也可以实现任何其他合适的技术，因为本发明不限于实现用于单独地或结合任何其他技术来提供或检索信任信息的任何单种技术。应当明白，本发明不限于用上述用于检索信任信息的说明性技术来执行，因为可以根据本文描述的原理来实现用于检索信任信息的任何合适的技术。

[0056] 图 2 示出实现本文描述的原理中的一些的用于在实体 100 的无线接入点 104 和客户机设备 112 之间传递内容（例如，广告形式的关于产品和 / 或服务的信息）的示例性过程 200。应当明白，过程 200 仅仅是说明性的，并且本发明不限于实现用于在无线接入点和客户机设备之间交换内容的任何一个或多个特定过程。如上所述，应当明白，尽管结合广告描述了过程 200，但这一类型的内容仅仅是说明性的，因为本发明不限于交换任何一个或多

个特定类型的内容。

[0057] 过程 200 在框 202 开始，在此实体（或与实体相关联的任何人或设备）指定同与该实体相关联的一个或多个服务相关的广告信息。如图 2 所示，该一个或多个服务可以是商业服务，如通过可由该实体执行的任何服务的产品销售。例如，如果该实体是餐厅，则该实体所提供的商业服务可以是提供食物并且关于该服务的广告可以描述该餐厅所提供的当天特价。如此处所使用的，术语“商业服务”不限于实体所提供的盈利性服务。商业服务可包括非盈利性或政府组织所进行的事件通告，如免费音乐会。

[0058] 根据实现本文描述的原理的一些技术，在框 202 指定广告信息可包括在与无线接入点相关联的数据存储中编码描述该指定商业服务的一个或多个广告的数据，而在其他实现中，指定商业服务可包括从预先配置的产品和 / 或服务列表中选择哪些产品和 / 或服务要作为指定商业服务。

[0059] 在框 204，无线接入点传送与商业服务的指定广告信息相关的广告数据。在一些实现中，框 204 所发送的传输可以是无线接入点所发送的控制传输的一部分，并且根据用于传送未经请求的内容的一些说明性技术，可以是诸如信标等周期性地向该无线接入点的射程内的所有客户机设备广播的通告传输。广告数据可以用任何合适的方式来合并到控制传输中。例如，在实现在 IEEE 802.11 无线网络中的技术中，广告数据可以包括在信标或探查响应的信息元素中，但本发明不限于这一示例性技术并可以用任何合适的方式将内容合并到控制传输中。

[0060] 在框 206，客户机设备检索实体（即，包括无线接入点的无线网络和 / 或无线接入点）的信任信息（例如，公钥或 PKI 证书）。这可以与动作 202 和 204 并行完成，在指定并传送广告信息的同时检索信任信息，或者这可以在完成动作 202 和 204 之后的任何合适的时间完成。检索信任信息可以用任何合适的方式来完成，如通过上述说明性技术中的任一种。信任信息可以从自助服务终端、持有一个或多个信任信息片段的服务器、信任信息的目录、和 / 或信任信息的任何其他合适的“带外”源来检索。

[0061] 在框 208，客户机设备 112 接收框 204 的包括广告数据的控制传输并对该传输执行任何合适的处理。根据本文描述的原理，这一处理包括使用框 210 中的信任信息来确认无线接入点的和 / 或该无线接入点连接到的无线网络的身份。框 210 的处理可以用任何合适的方式来完成，包括通过以下详细描述的过程 300、400 和 500 中的任一过程。

[0062] 在框 212，在框 210 的确认处理之后，取决于无线接入点是从中接收到控制传输的无线接入点还是客户机设备 112 期望从中接收内容的无线接入点（例如，无线接入点是真实的还是欺骗的），过程 200 产生分支。如果确定无线接入点是预期无线接入点，则在框 214，客户机设备通过例如经由合适的用户界面向该客户机设备的用户呈现广告数据来利用控制消息的内容，并且过程 200 结束。然而，如果在框 212 确定无线接入点不是预期无线接入点，则在框 216，在合适的一段时间（例如，几分钟、几天、直至客户机设备离开该无线接入点的射程、直至获取了新信任信息、永远、或任何其他合适的时间段）内忽略该无线接入点（以及它所传送的控制消息）。

[0063] 应当明白，过程 200 仅仅是实现本文描述的原理中的一些的技术的说明，并且本发明不限于实现诸如过程 200 等过程或执行过程 200 的一个或多个动作的任何特定过程。可以根据本文描述的原理来实现用于在与实体相关联的无线接入点和客户机设备之间交

换关于产品和/或服务的信息的任何合适的技术。例如，在替换技术中，尽管图2根据由商业实体进行广告的商业服务来描述过程200，但本发明的各实施例可由不是商业实体的实体来实现，并且如果像这样则与该实体相关联的产品和/或服务可以不是商业服务。另外，应当明白，一些替换技术可以用不同的次序来实现图2中所示的动作。作为示例，在根据本文描述的原理操作的一些技术中，客户机设备112可以在接收包括广告数据（或其他内容）的任何控制传输之前确认无线接入点102的身份，以使得可以在动作208之前执行上述确认无线接入点的和/或无线网络的身份的动作（即，动作210和212）。

[0064] 如以上结合过程200所述，确认无线接入点的和/或无线网络的身份（如在过程200的框210中）可以用任何合适的方式来完成。以下结合图3-5讨论用于确认无线接入点的和/或无线网络的身份的说明性技术。然而，应当明白，这些技术仅仅是可根据本文描述的原理实现的各类技术的示例，并且其他技术是可能的。

[0065] 图3示出可以确认无线接入点的身份的示例性过程300。如上所述，尽管结合广告和商业实体讨论了图3，但可以使用任何一个或多个合适类型的内容。

[0066] 过程300在框302开始，在此客户机设备检索一个或多个商业实体的信任信息。该信任信息可包括实体的公钥和/或PKI证书，并可以用任何合适的方式来检索，如从与该实体相关联的自助服务终端。在框304，客户机设备检测到它处于它拥有其信任信息的无线接入点的射程内（例如，通过将检测到的无线接入点的标识符与信任信息的标识符相比较）。在框306，客户机设备向无线接入点传送使用该信任信息加密的测试控制传输。该测试控制传输可包括任何合适的信息，并可包括质询短语和/或现时值。在测试控制传输中可以使用任何合适的消息（例如，随机或伪随机位串、诸如“Red trees are blue（红色的树是蓝色的）”等唯一文本、发射时间和/或发射位置、或任何其他合适的数据）。在根据图3的示例操作的一些技术中，测试控制传输的净荷还可包括客户机设备112的信任信息，如客户机设备的公钥/PKI证书和/或用户的公钥/PKI证书（以下为简明起见统称为客户机信任信息）。

[0067] 在框308，客户机设备响应于测试控制消息来从无线接入点接收控制传输。该响应控制传输可包括所发送的未加密的测试控制传输的内容，或在其中测试控制消息另外包括客户机信任信息的一些实现中，可以使用客户机信任信息进行加密来将该响应控制消息的内容发送回来。在接收到（并且，在一些技术中，进行解密）响应控制传输后，如果客户机设备确定该内容与加密并传送的内容（例如，测试控制传输的内容）相匹配，则客户机设备可以假定无线接入点持有与用其加密测试控制传输的内容的公钥相对应的私钥，并且因此该客户机设备与之交换消息的无线接入点是预期无线接入点。

[0068] 在框310，如果无线接入点是预期无线接入点（例如，如果无线接入点是真实的），则客户机设备可以认可来自该无线接入点的所有将来传输都是真实的，并且自由地使用控制消息的内容（例如，可以显示无线接入点传送给用户的广告），并且该过程结束。然而，如果在框310确定无线接入点不是预期无线接入点，则在框314，客户机设备可以在任何合适的时间段内忽略该无线接入点和来自该无线接入点的控制传输。

[0069] 在根据图3的示例操作的技术的一些实现中，包括内容（例如，广告数据）的控制消息可以不在加密的情况下传送，而是在未加密的情况下发送。在一些替换实现中，在过程300的认证技术之后，作为广播控制消息的替换或补充，无线接入点可以向客户机设备发送

使用客户机信任信息加密的控制消息。在其他实施例中，无线接入点所传送的包括内容的控制消息的全部或一部分都被使用该无线接入点的信任信息来加密，并且客户机设备将在使用该内容（例如，将该内容显示给用户）之前使用该信任信息解密每一消息。

[0070] 在实现本文描述的原理的一些技术中，对无线接入点的身份的确认可以仅依赖于对控制消息的正确解密，以用于确认无线接入点的和/或无线网络的身份。图 4 示出作为这些技术的说明的过程 400。如上所述，以下结合商业实体的广告描述了过程 400，但可根据本文描述的原理中的一些实现的技术可以交换任何一个或多个合适类型的信息来作为控制消息的内容。

[0071] 过程 400 在框 402 开始，在此客户机设备检索商业实体的信任信息。信任信息可以用任何合适的方式来检索，如通过从与商业实体相关联的自助服务终端读取信任信息。在框 404，客户机检测到它处于它拥有其信任信息的无线接入点的射程内（例如，通过将检测到的无线接入点的标识符与信任信息的标识符相比较），并且在框 406，从无线接入点接收控制传输（例如，信标或对客户机设备所发送的探查请求的响应）。

[0072] 在框 408，客户机设备 112 使用在框 402 检索到的信任信息来处理控制传输以确认无线接入点的身份。处理控制传输可包括使用信任信息来解密该控制传输。如果可以使用检索到的信任信息来正确地解密控制传输，则客户机设备 112 可以假定控制传输是使用与该信任信息的公钥相对应的私钥来加密的，并且因此该无线接入点是预期无线接入点并且该传输是真实的。

[0073] 在框 410，如果确定传输是真实的，则在框 412，可以用任何合适的方式来使用控制传输的内容，如通过提取广告并将其显示给用户，并且该过程结束。然而，如果在框 410 确定该传输不是真实的（即，未确认该传输来自预期无线接入点），则在框 414，在任何合适的时间段内忽略该无线接入点，并且该过程结束而不使用该内容。

[0074] 图 5 示出根据本文描述的原理中的一些来操作的替换过程 500。过程 500 在框 502 开始，在此客户机设备 112 检索商业实体的信任信息。该信任信息可以用任何合适的方式来检索，如通过从诸如服务器 116 等服务器检索该信任信息，该服务器在根据图 5 的示例操作的技术的一些实现中可实现担当证书授权机构和/或信任信息的储存库的 web 服务。在框 502 检索到的信任信息可以是单个信任信息片段，或可以是在任何合适的编组中检索到的多个信任信息片段。在一些实现中，可以响应于用户请求来检索信任信息，而在一些实现中，作为补充或替换，客户机设备 112 可以适用于响应于任何合适的刺激来自动地检索信任信息。该刺激可以是时间或位置（例如，在客户机设备检测到它在一实体的位置附近时）、对与一实体相关联的无线接入点的检测、从服务器 116 接收到的先前检索到的信任信息已被添加或改变的指示、或任何其他合适的刺激。

[0075] 在框 504，客户机设备 112 检测到它处于它拥有其信任信息的无线接入点的射程内（例如，通过将检测到的无线接入点的标识符与信任信息的标识符相比较），并且在框 506，从无线接入点接收控制传输（例如，信标或对客户机设备所发送的探查请求的响应）。

[0076] 在框 508，客户机设备 112 使用在框 502 检索到的信任信息来处理控制传输以确认无线接入点的身份。处理控制传输可包括使用信任信息来解密该控制传输。如果可以使用检索到的信任信息来正确地解密控制传输，则客户机设备 112 可以假定控制传输是使用与该信任信息的公钥相对应的私钥来加密的，并且因此该无线接入点是预期无线接入点并且

该传输是真实的。

[0077] 在框 510，如果确定传输是真实的，则在框 512，可以用任何合适的方式来使用控制传输的内容，如通过提取广告并将其显示给用户，并且该过程结束。然而，如果在框 510 确定该传输不是真实的（即，未确认该传输来自预期无线接入点），则在框 514，在任何合适的时间段内忽略该无线接入点，并且该过程结束而不使用该内容。

[0078] 应当明白，以上结合图 3-5 描述的技术仅仅是可实现本文描述的原理中的一些的用于确认无线网络和 / 或无线接入点的身份的各类技术的示例。应当明白，本发明不限于实现这些技术中的任何特定一种技术，且不限于实现任何技术，因为根据本文描述的原理可以实现任何合适的技术。

[0079] 尽管上述示例性技术集中于通过对使用信任信息加密的控制消息进行解密来确认无线接入点的和 / 或无线网络的身份，但本发明不限于此。可以实现以其他方式另外地或另选地确认无线网络的身份的各种技术，包括使用环境信息。例如，无线接入点或无线网络的信任信息可以是该无线接入点或无线网络的预期位置，并可以与当客户机设备处于无线接入点的射程内时的位置和 / 或来自无线接入点的控制传输中包括的位置信息相比较。以此方式，如果客户机设备在它未处于预期位置时检测到无线接入点，或如果控制传输中的位置信息不是预期位置信息，则检测到的无线接入点可能是欺骗的。可以使用的位置信息可以是任何合适的位置信息，如街道地址、建筑物内的位置、纬度 / 经度数据、和 / 或任何其他合适的位置信息。作为补充或替换，环境信息可包括控制传输的时间信息。时间信息可以例如被包括在描述控制传输被首次传送的时间的控制传输中。客户机设备在接收到该控制传输后，可以将该控制传输的时间信息与包括当前时间的信任信息相比较。该信任信息可被用来确定广播时间是否处于与当前时间的合理的差之内。例如，如果控制传输的广播时间与当前时间之间的差大于特定时间量（例如，10 秒），则客户机设备可以确定其受到重新广播控制传输的设备的回复攻击，并且确定检测到的无线接入点是欺骗性的。其他实施例可以实现用于确认无线接入点的和 / 或无线网络的身份的其他技术，因为本发明在这一方面没有限制。

[0080] 以上讨论了可由客户机设备用来实现本文描述的原理中的一些的各种技术。然而，应当明白，在实现本文描述的原理中的一个或多个的一些系统中，客户机设备连接到的无线网络的一个或多个元素可以执行根据这些原理的技术。图 6 示出根据这些原理中的一些的可由无线接入点实现的示例性过程 600。

[0081] 过程 600 在框 602 开始，在此无线接入点从数据存储检索本地信任信息。本地信任信息可包括任何合适的信任信息，如可在公钥密码算法中使用的私钥或任何其他合适的本地信任信息。在框 604，从数据存储 106 检索内容并将其编码在控制传输中，并且使用框 602 的本地信任信息来对控制传输进行加密。在框 604 加密的内容可以是任何合适的内容，如广告数据、位置数据、描述无线接入点和 / 或无线网络提供的一个或多个服务（例如，打印服务）的数据、或任何其他类型的信息。在框 606，无线接入点随后传送控制传输。在一些实现中，控制传输可以作为信标传送到该无线接入点的射程内的所有客户机设备，而在替换实现中，控制传输可以作为对无线接入点接收到的来自客户机设备的探查请求的响应或作为任何其他合适的控制传输来发送。

[0082] 实现本文描述的原理中的一个或多个的技术可以在多个计算机系统配置中的任

一个上实现，并且不限于任何特定类型的配置。图 7-8 示出本发明的各实施例可在其中操作的各种计算机系统，但其他系统也是可能的。应当理解，图 7-8 既不旨在是担当无线接入点或客户机设备的计算设备的必要组件的描绘，也不旨在是全面描绘。

[0083] 图 7 示出说明性无线接入点 104。无线接入点 104 包括处理器 702、网络适配器 704、以及计算机可读介质 706。网络适配器 704 可以是使得无线接入点 104 能够通过任何合适的计算网络来与任何其他合适的计算设备进行通信的任何合适的硬件和 / 或软件。该计算网络可以是用于在两个或更多个计算机之间交换数据的任何合适的一个或多个有线和 / 或无线通信介质，包括因特网。例如，该计算网络可以至少部分是根据诸如 IEEE802.11、GSM、蓝牙、WiMAX、UWB、和 / 或任何其他合适的协议等任何合适的无线连网协议操作的无线网络。在本发明的一些实施例中，无线接入点 104 可包括两个网络适配器 704，以使无线接入点 104 能够与两个不同的通信网络——例如，有线计算网络和无线计算网络——进行通信并在这两者之间交换数据。计算机可读介质 706 适用于存储要由处理器 702 处理的数据和 / 或要由处理器 702 执行的指令。处理器 702 能够处理数据和执行指令。这些数据和指令可被存储在计算机可读介质 706 上，并且可以例如允许在无线接入点 104 的各组件之间进行通信。

[0084] 根据本文描述的示例性技术中的一些，图 1A、1B 和 1C 的数据存储 106 可被实现为计算机可读介质 706，并且存储在计算机可读介质 706 上的数据和指令可包括接入点固件 708，接入点固件 708 可以是由处理器 702 执行来指示无线接入点 104 执行任何合适的功能的软件，这些功能诸如从数据存储中检索内容（例如，广告数据 710 或其他合适的内容）以供传输，将该内容编码在控制传输中，以及生成控制传输。计算机可读介质 706 还可以存储诸如广告数据 710（即，广告数据 108）等内容。广告数据 710 可以是可由无线接入点 104 发送的任何一种或多种合适类型的数据，包括例如描述文本、图像、音频、或视频、或其任何组合的数据。广告数据 710 可以是描述与关联于无线接入点 104 的实体相关联的一个或多个服务的单个广告的数据，或可以是描述与一实体相关联的一个或多个服务的多个广告的数据。在本发明的各实施例中，该实体可以是商业实体（例如，商家）并且服务可以是商业服务。如上所述，应当明白，根据本文描述的原理中的一个或多个，广告数据仅仅是可由无线接入点 104 传送的各类型数据的说明。

[0085] 根据本文描述的示例性技术中的一些，计算机可读介质 706 还可持有无线接入点 104 和 / 或该无线接入点连接到的无线网络的信任信息 712。信任信息 712 可以是任何合适的信任信息，如无线接入点 104 和 / 或无线网络的要在公钥密码算法中使用的私钥。然而，应当明白，任何合适的信任信息都可以用作信任信息 712，包括例如环境信息，因为私钥仅仅是可以用作根据本文描述的原理的信任信息的各类型信息的说明。

[0086] 图 8 示出根据本文描述的原理的可被实现为客户机设备的示例性客户机设备 112。如上所述，任何合适的移动或非移动计算设备都可以用作客户机设备 112。客户机设备 110 可以是为多个目的而设计并供用户使用的计算设备，如台式个人计算机、膝上型个人计算机、服务器、个人数字助理 (PDA)、智能 / 移动电话、或任何其他合适的电子设备。或者，客户机设备 110 可以是不旨在供用户通常使用或旨在用于单个目的或有限目的的任何计算设备，如服务器或机架式连网设备。

[0087] 客户机设备 112 包括处理器 802、网络适配器 804、以及计算机可读介质 808。网络

适配器804可以是使得客户机设备112能够通过任何合适的计算网络来与任何其他合适的计算设备进行通信的任何合适的硬件和/或软件。该计算网络可以是用于在两个或更多个计算机之间交换数据的任何合适的一个或多个有线和/或无线通信介质，包括因特网。例如，该计算网络可以至少部分是根据诸如IEEE 802.11、GSM、蓝牙、WiMAX、UWB、和/或任何其他合适的协议等任何合适的无线连网协议操作的无线网络。网络适配器804还可包括允许网络适配器804与在客户机设备112上执行的应用程序之间的交互的应用程序接口(API)806。API 806可以向客户机设备112上的应用程序提供可执行功能，以使这些应用程序可以请求网络适配器804开始监视来自无线接入点的传输，提供来自传输的内容（例如，广告数据、位置数据、或任何其他合适的内容），请求来自无线接入点的附加信息，或任何其他合适的功能。计算机可读介质806适用于存储要由处理器802处理的数据和/或要由处理器802执行的指令。处理器802能够处理数据和执行指令。这些数据和指令可以存储在计算机可读介质806上，并且例如可以启用客户机设备112的各组件之间的通信。

[0088] 根据本发明的一些实施例，存储在计算机可读介质808上的数据和指令可包括用户界面810，通过该用户界面可以向用户呈现网络适配器804接收到的控制传输的内容（例如，广告数据和/或关于所广告的产品或服务的附加信息）。用户界面810可以用任何合适的格式来呈现内容。在客户机设备112的一些实施例中，用户界面810可以是操作系统的组件或客户机设备112的固件，而在本发明的替换实施例中，用户界面910可以是独立应用程序或一段应用程序，从而可在该应用程序内显示并使用该内容。

[0089] 根据本文描述的原理中的一个或多个，客户机设备112的计算机可读介质808还可包括信任信息812的数据存储。信任信息812可以是一个或多个无线接入点和/或无线网络的一个或多个信任信息片断，并可包括任何一个或多个合适类型的信任信息。例如，如上所述，该信任信息可以是无线接入点和/或无线网络的公钥和/或PKI证书，和/或可以是诸如无线接入点和/或无线网络的时间或位置数据等环境信息。

[0090] 计算机可读介质808还可包括用于使用信任信息812来测试网络适配器804接收到的控制消息以确定无线接入点和/或无线网络的真实性的验证模块814。验证模块814可以实现任何合适的技术，包括但不限于上述示例性技术中的任何一个或多个。在一些实现中，验证模块814可以合并到客户机设备112的操作系统中，而在替换实现中，验证模块814可以与操作系统分开实现，例如实现成在客户机设备112上执行的独立应用程序或以任何其他合适的方式来实现。

[0091] 可以用多种方式中的任一种来实现本发明的上述实施例。例如，可使用硬件、软件或其组合来实现各实施例。当使用软件实现时，该软件代码可在无论是在单个计算机中提供的还是在多个计算机之间分布的任何合适的处理器或处理器集合上执行。

[0092] 此外，应当理解，计算机可以用多种形式中的任一种来具体化，如机架式计算机、台式计算机、膝上型计算机、或平板计算机。另外，计算机可以具体化在通常不被认为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电子设备。

[0093] 同样，计算机可以具有一个或多个输入和输出设备。这些设备主要可被用来呈现用户界面。可被用来提供用户界面的输出设备的示例包括用于可视地呈现输出的打印机或显示屏和用于可听地呈现输出的扬声器或其他声音生成设备。可被用作用户接口的输入设

备的示例包括键盘和诸如鼠标、触摸板和数字化桌等定点设备。作为另一示例，计算机可以通过语音识别或以其他可听格式来接收输入信息。

[0094] 这些计算机可以通过任何合适形式的一个或多个网络来互连，包括作为局域网或广域网，如企业网络或因特网。这些网络可以基于任何合适的技术并可以根据任何合适的协议来操作，并且可以包括无线网络、有线网络或光纤网络。

[0095] 而且，此处略述的各种方法可被编码为可在采用各种操作系统或平台中任何一种的一个或多个处理器上执行的软件。此外，这样的软件可使用多种合适的程序设计语言和/或常规程序设计或脚本工具中的任何一种来编写，而且它们还可被编译为可执行机器语言代码或在框架或虚拟机上执行的中间代码。

[0096] 就此，本发明可被具体化为用一个或多个程序编码的一个或多个计算机存储介质（例如，计算机存储器、一个或多个软盘、紧致盘、光盘、磁带、闪存、现场可编程门阵列或其他半导体器件中的电路配置等），当这些程序在一个或多个计算机或其他处理器上执行时，它们执行实现本发明的上述各个实施例的方法。这一个或多个计算机可读介质可以是便携的，使得其上存储的一个或多个程序可被加载到一个或多个不同的计算机或其他处理器上以便实现本发明上述的各个方面。

[0097] 此处以一般的意义使用术语“程序”或“软件”来指可被用来对计算机或其他处理器编程以实现本发明上述的各个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，应当理解，根据本实施例的一个方面，当被执行时实现本发明的方法的一个或多个计算机程序不必驻留在单个计算机或处理器上，而是可以按模块化的方式分布在多个不同的计算机或处理器之间以实现本发明的各方面。

[0098] 计算机可执行指令可以具有可由一个或多个计算机或其他设备执行的各种形式，诸如程序模块。一般而言，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。通常，在各实施例中，程序模块的功能可以视需要组合或分散。

[0099] 本发明的各个方面可单独、组合或以未在前述实施例中具体讨论的各种安排来使用，从而并不将其应用限于前述描述中所述或附图中所示的组件的细节和安排。例如，可使用任何方式将一个实施例中描述的各方面与其他实施例中描述的各方面组合。

[0100] 在权利要求书中使用诸如“第一”、“第二”、“第三”等序数词来修饰权利要求元素本身并不意味着一个权利要求元素较之另一个权利要求元素的优先级、先后次序或顺序、或者方法的各动作执行的时间顺序，而仅用作将具有某一名字的一个权利要求元素与（若不是使用序数词则）具有同一名字的另一元素区分开的标签以区分各权利要求元素。

[0101] 同样，此处所使用的短语和术语是出于描述的目的而不应被认为是限制。此处对“包括”、“包含”、或“具有”、“含有”、“涉及”及其变型的使用旨在包括其后所列的项目及其等效物以及其他项目。

[0102] 至此描述了本发明的至少一个实施例的若干方面，可以理解，本领域的技术人员可容易地想到各种更改、修改和改进。这样的更改、修改和改进旨在是本发明的一部分，且旨在处于本发明的精神和范围内。因此，上述描述和附图仅用作示例。

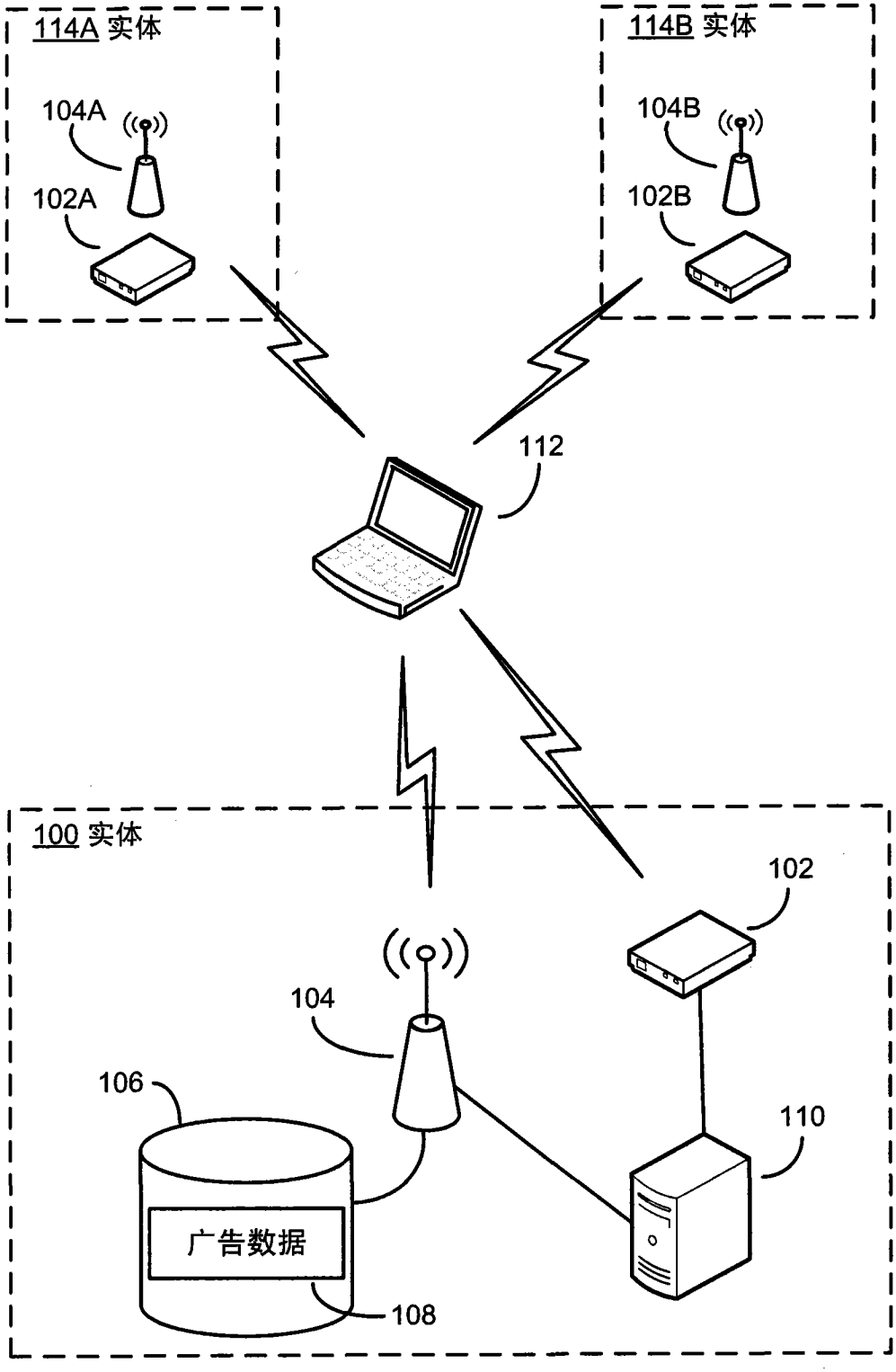

114A 实体
104A
102A
114B 实体
104B
102B
112
100 实体
102
104
106
110
广告数据
108

图 1A

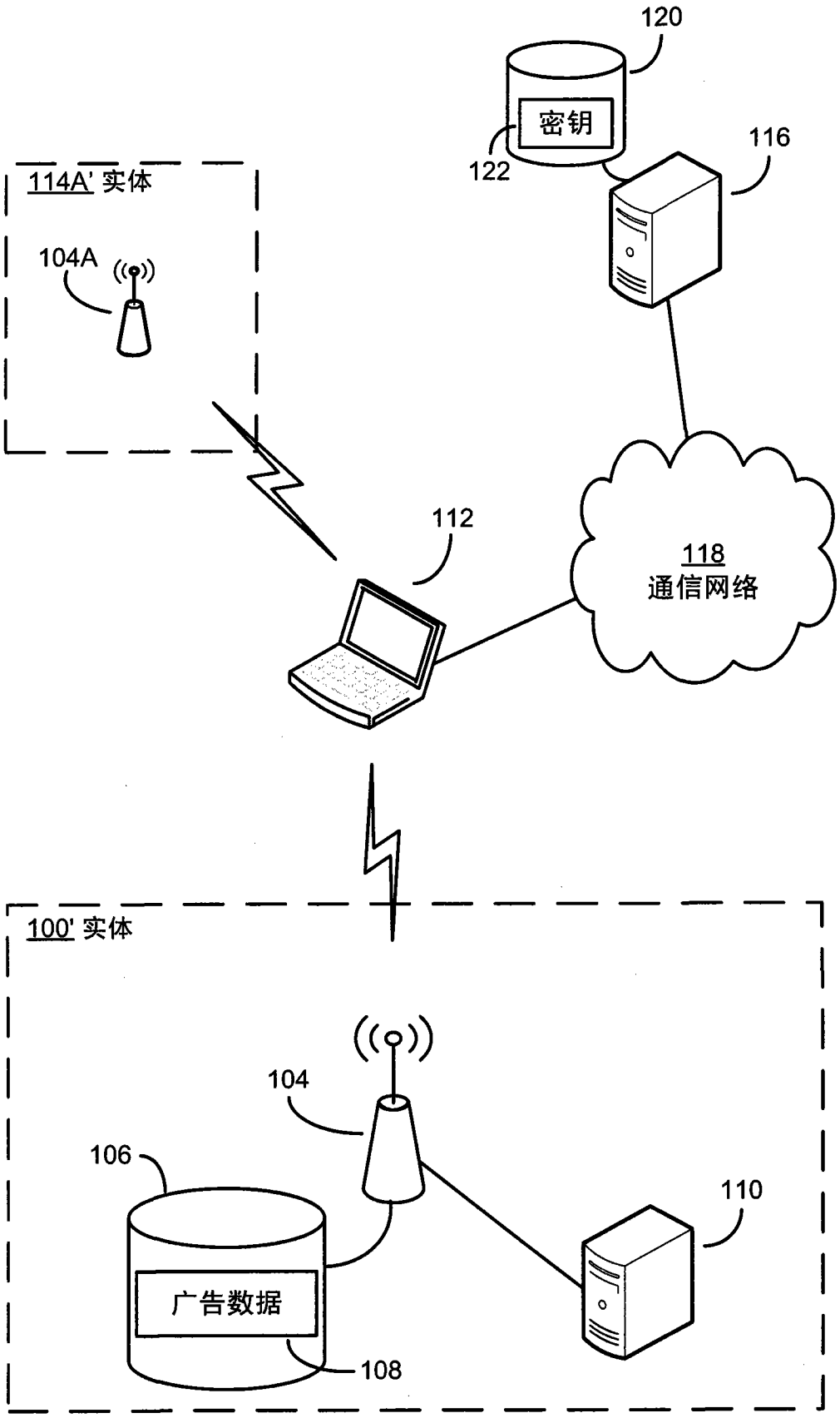

120
密钥
122
116
114A' 实体
104A
112
118
通信网络
100' 实体
104
106
110
广告数据
108

图 1B

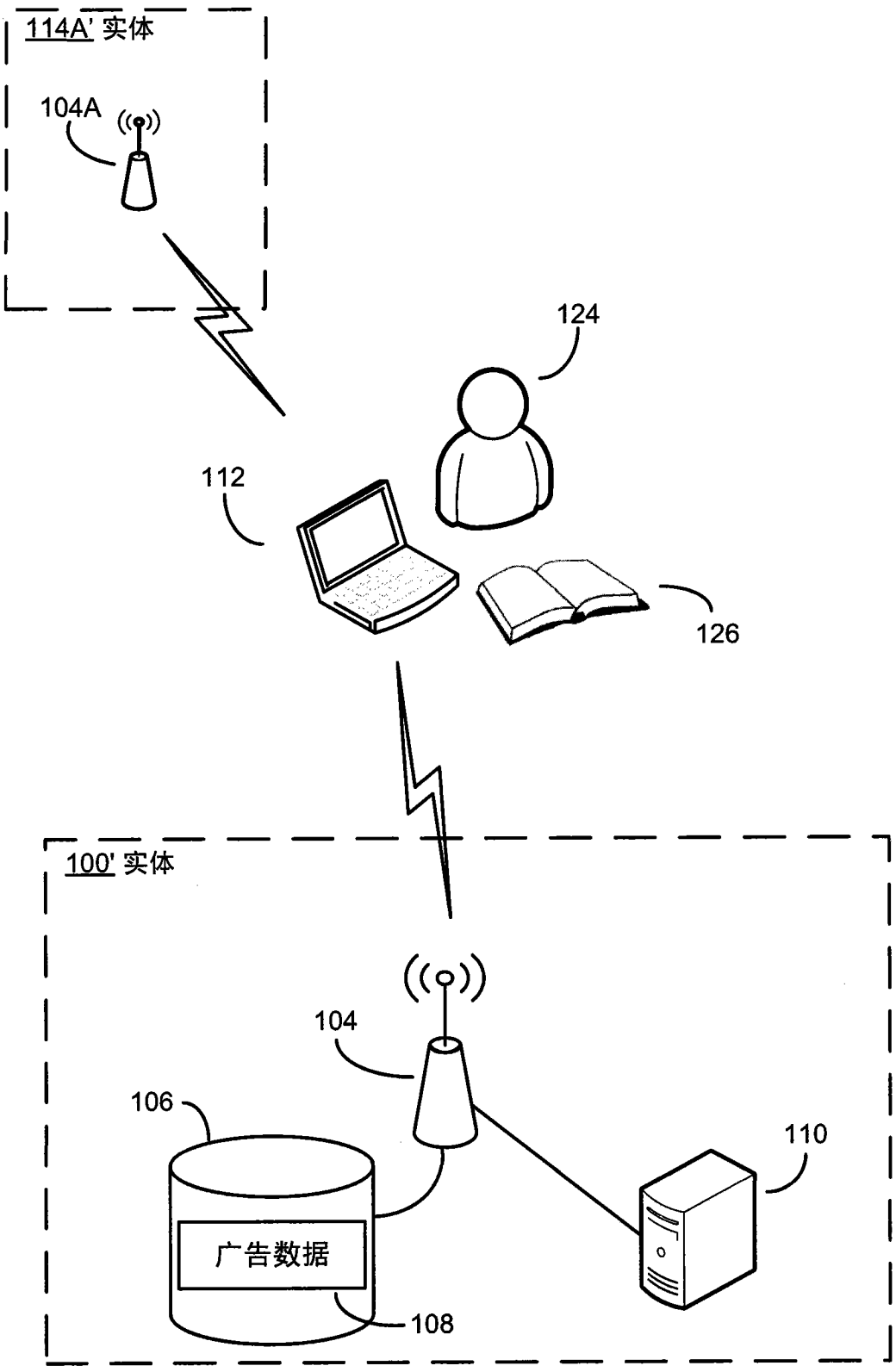


图 1C

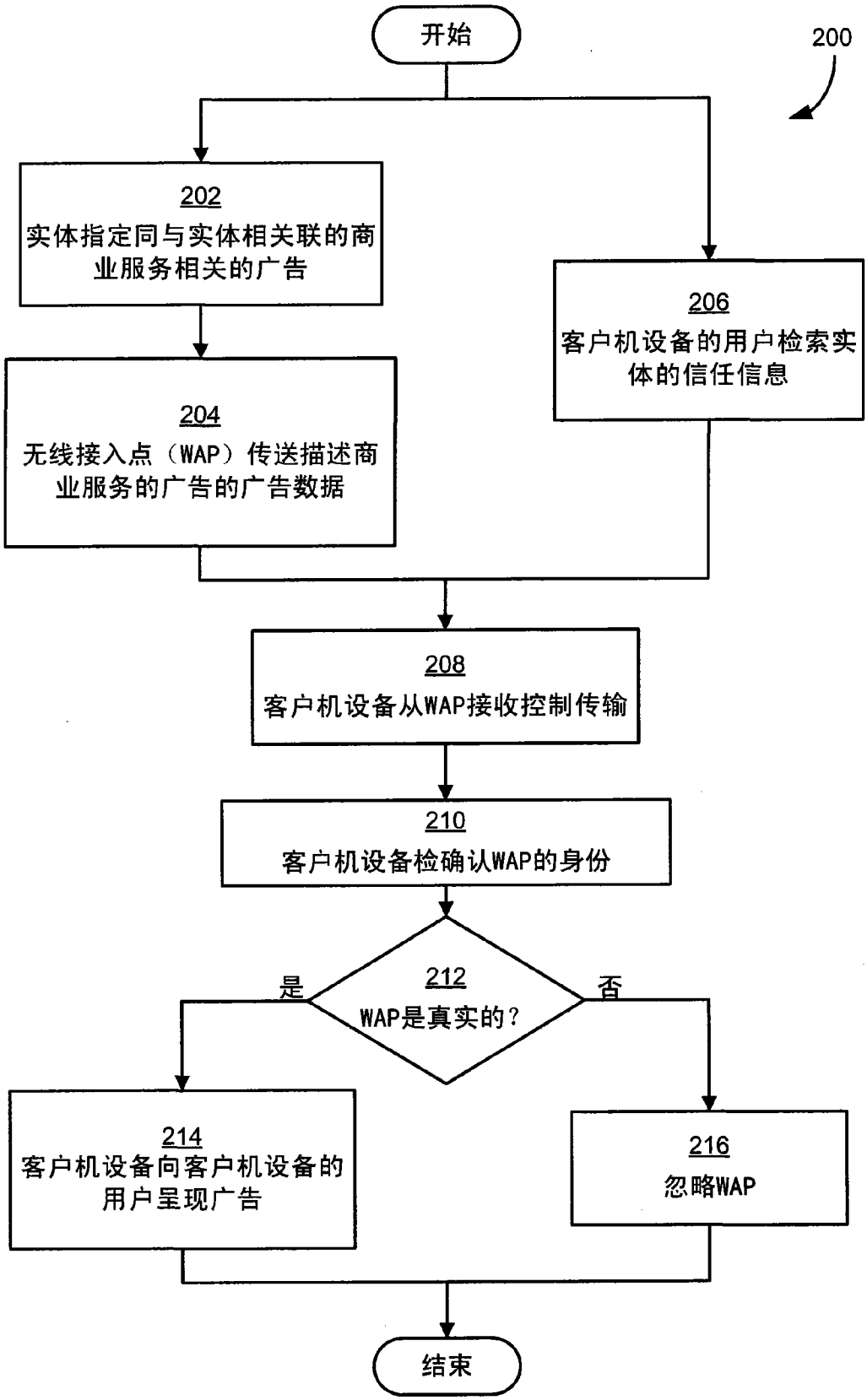

开始
200
202
实体指定同与实体相关联的商业服务相关的广告
204
无线接入点（WAP）传送描述商业服务的广告的广告数据
206
客户机设备的用户检索实体的信任信息
208
客户机设备从WAP接收控制传输
210
客户机设备检确认WAP的身份
212
WAP是真实的？
是
否
214
客户机设备向客户机设备的用户呈现广告
216
忽略WAP
结束

图 2

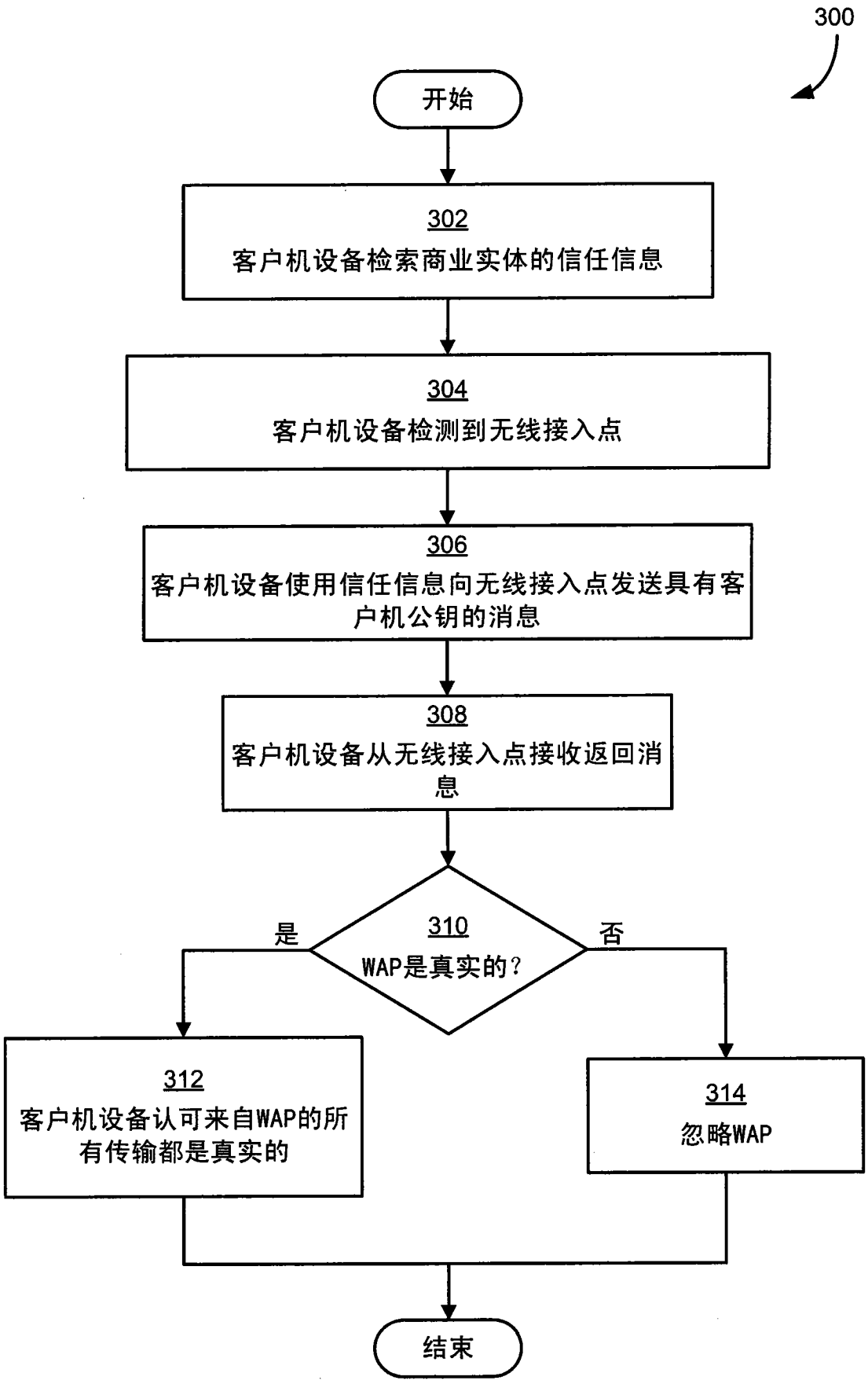

300
开始
302
客户机设备检索商业实体的信任信息
304
客户机设备检测到无线接入点
306
客户机设备使用信任信息向无线接入点发送具有客户机公钥的消息
308
客户机设备从无线接入点接收返回消息
310
WAP是真实的?
是
否
312
客户机设备认可来自WAP的所有传输都是真实的
314
忽略WAP
结束

图 3

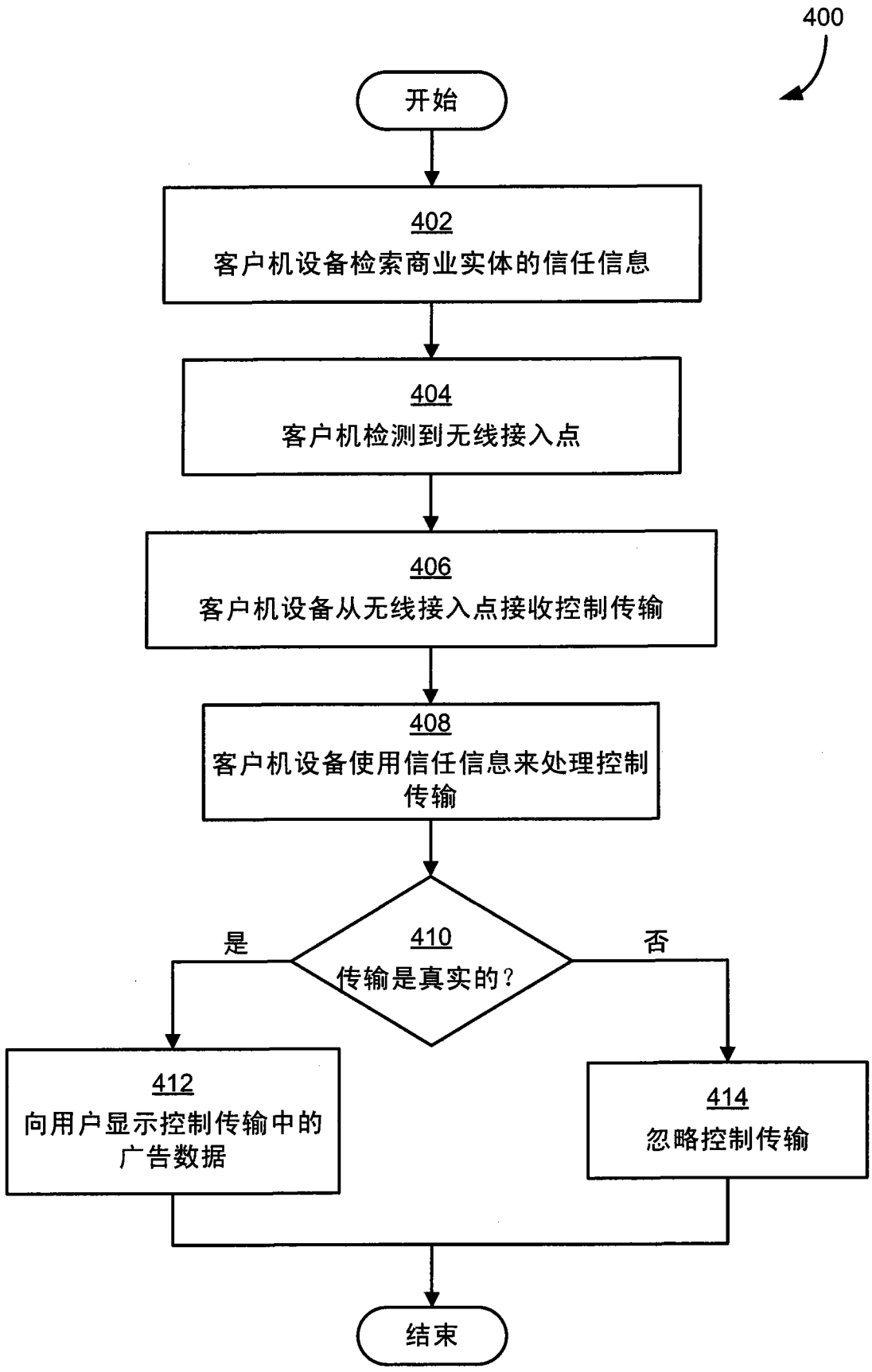

400
开始
402
客户机设备检索商业实体的信任信息
404
客户机检测到无线接入点
406
客户机设备从无线接入点接收控制传输
408
客户机设备使用信任信息来处理控制传输
410
传输是真实的？
是
否
412
向用户显示控制传输中的广告数据
414
忽略控制传输
结束

图 4

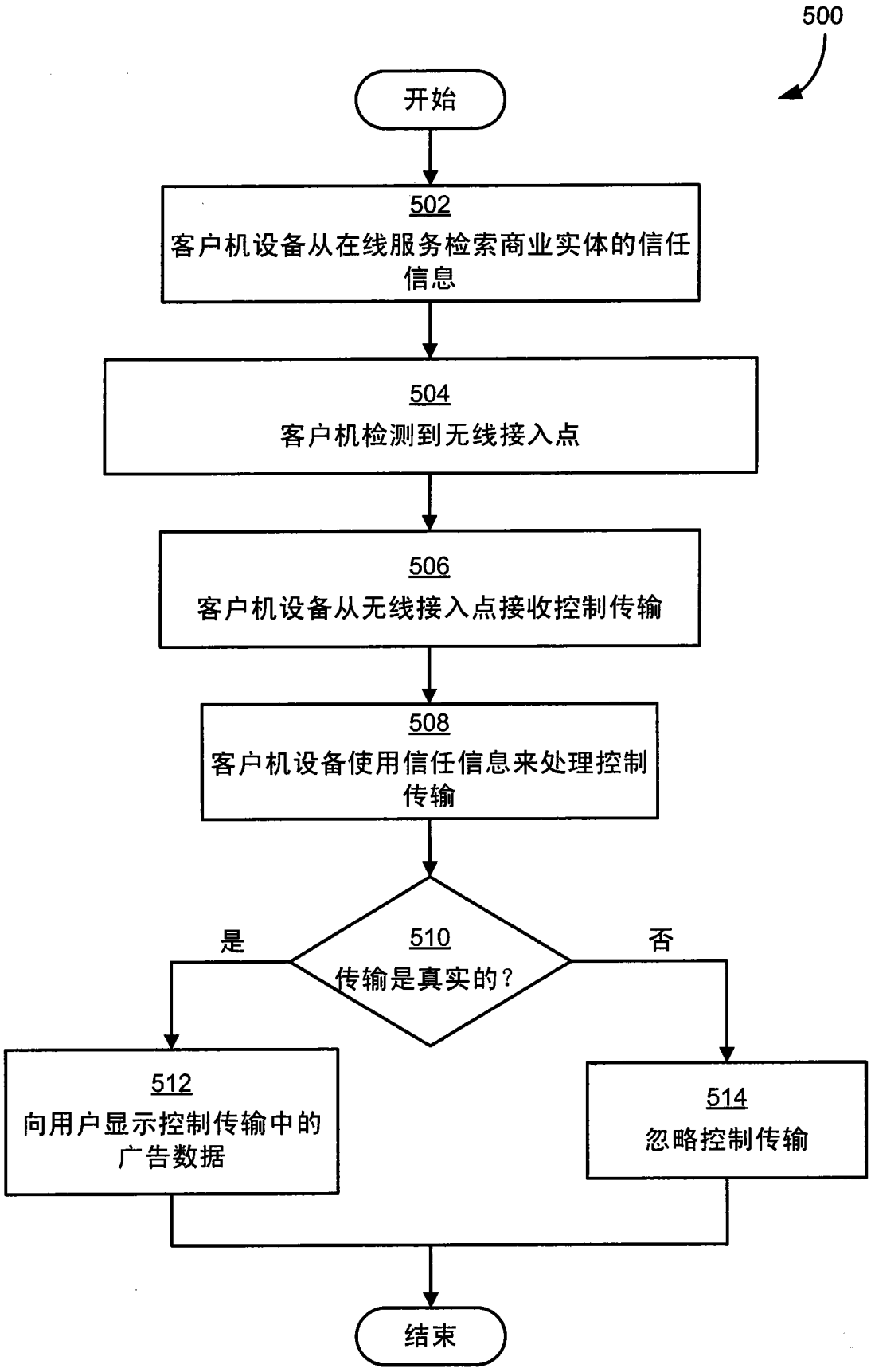

500
开始
502
客户机设备从在线服务检索商业实体的信任信息
504
客户机检测到无线接入点
506
客户机设备从无线接入点接收控制传输
508
客户机设备使用信任信息来处理控制传输
510
传输是真实的？
是
否
512
向用户显示控制传输中的广告数据
514
忽略控制传输
结束

图 5

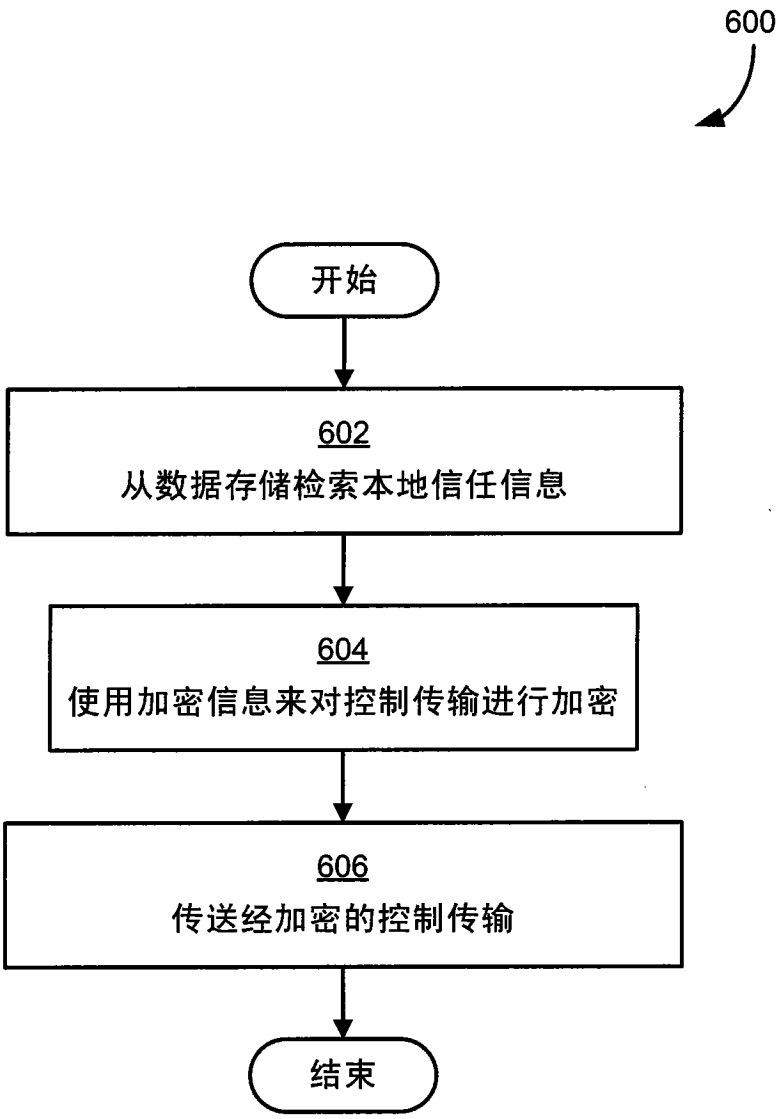

600
开始
602
从数据存储检索本地信任信息
604
使用加密信息来对控制传输进行加密
606
传送经加密的控制传输
结束

图 6

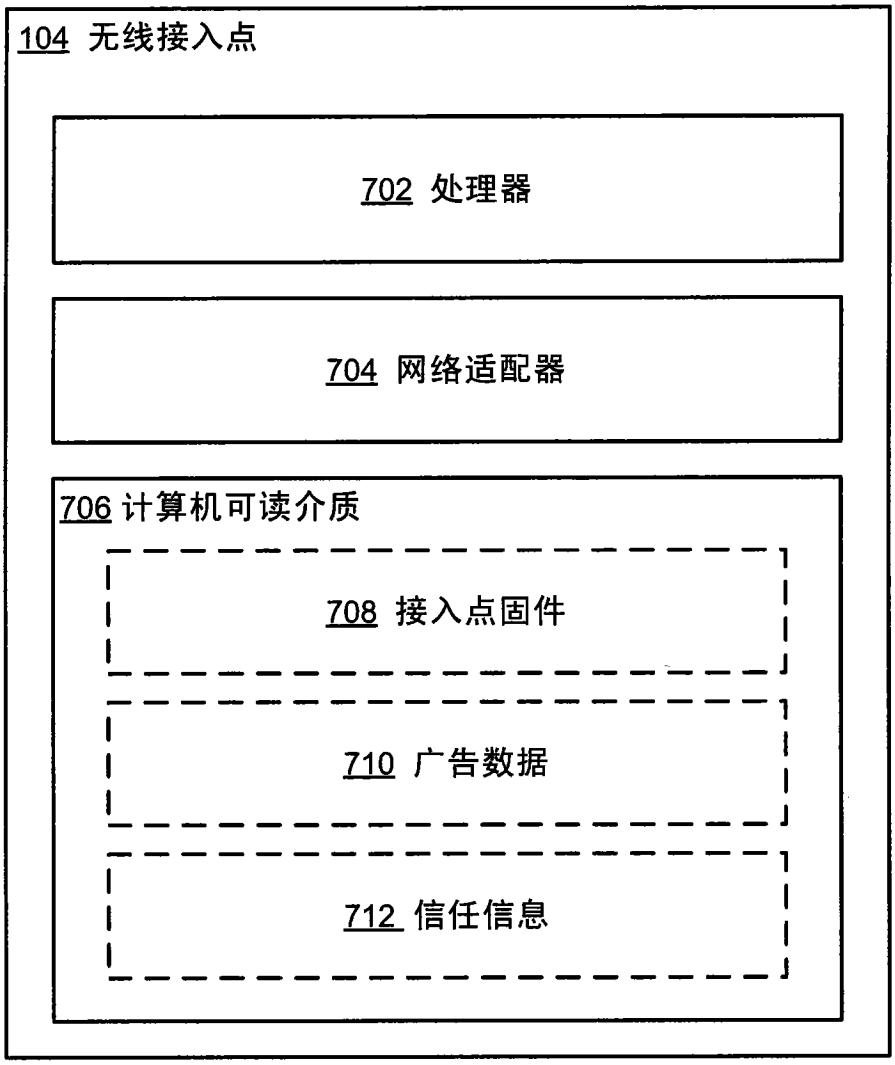

104 无线接入点
702 处理器
704 网络适配器
706 计算机可读介质
708 接入点固件
710 广告数据
712 信任信息

图 7

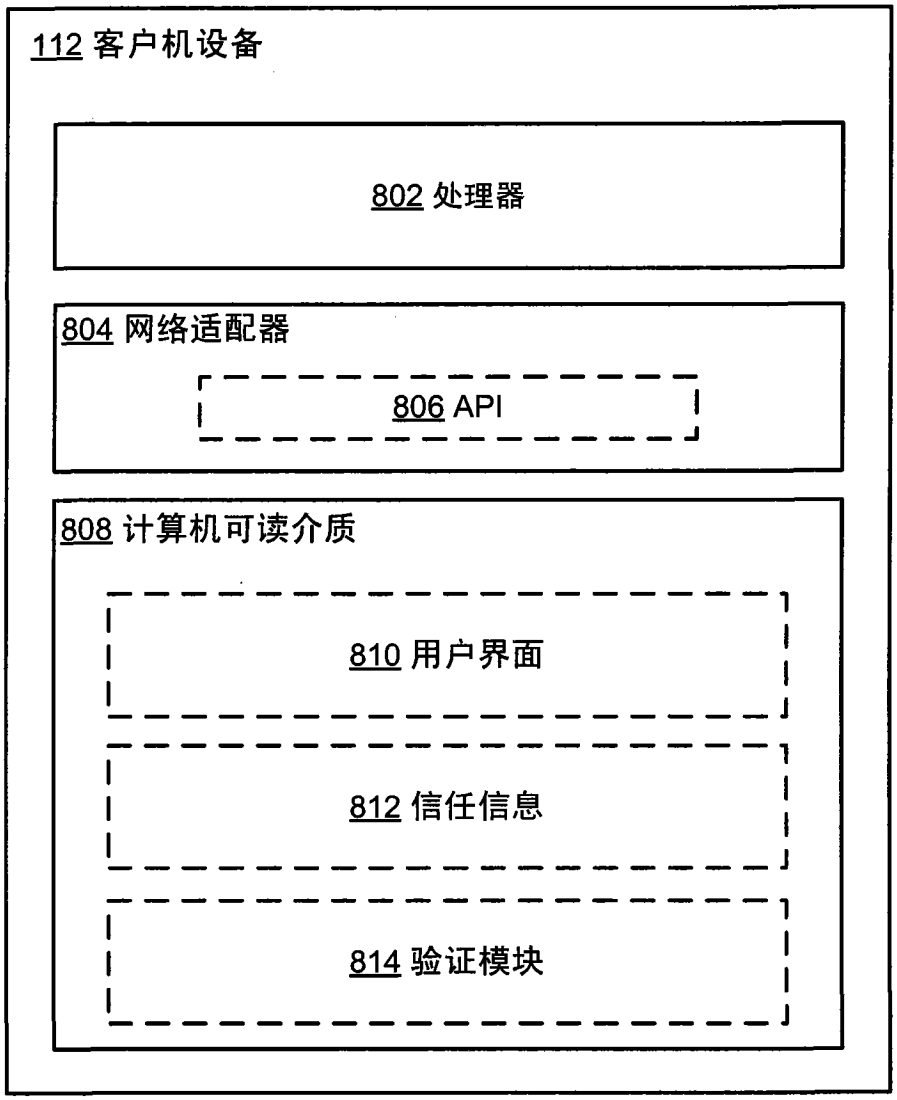

112 客户机设备
802 处理器
804 网络适配器
806 API
808 计算机可读介质
810 用户界面
812 信任信息
814 验证模块

图 8