



(12)发明专利

(10)授权公告号 CN 102598794 B

(45)授权公告日 2016.08.03

(21)申请号 201080050270.3

埃斯特班·劳尔·托雷斯

(22)申请日 2010.07.23

(74)专利代理机构 北京东方亿思知识产权代理
有限责任公司 11258

(30)优先权数据

代理人 李晓冬

12/613,784 2009.11.06 US

(85)PCT国际申请进入国家阶段日

(51)Int.Cl.

2012.05.04

H04W 48/08(2006.01)

(86)PCT国际申请的申请数据

H04L 29/06(2006.01)

PCT/US2010/043005 2010.07.23

(87)PCT国际申请的公布数据

(56)对比文件

W02011/056272 EN 2011.05.12

CN 101461277 A, 2009.06.17,

(73)专利权人 思科技术公司

CN 101461277 A, 2009.06.17,

地址 美国加利福尼亚州

WO 2007/080490 A1, 2007.07.19,

CN 1592313 A, 2005.03.09,

(72)发明人 马克·克里斯彻尔

JP 特开2002-41961 A, 2002.02.08,

詹姆斯·爱德华·伯恩斯

审查员 贾斌

南希·卡姆-温恩特

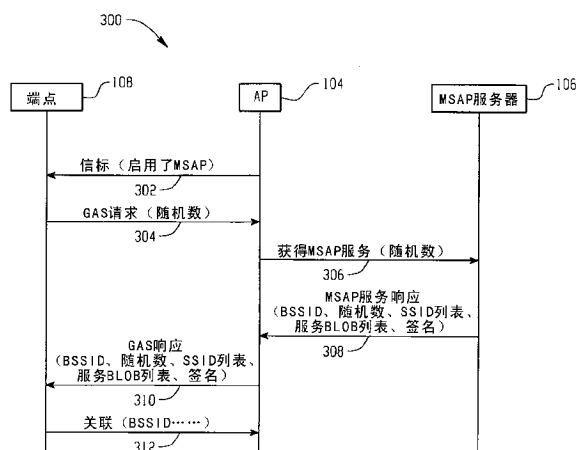
权利要求书2页 说明书8页 附图5页

(54)发明名称

管理员注册认证服务

(57)摘要

在一示例实施例中,这里描述的是一种装置,包括被配置来发送和接收数据的收发信机以及耦合到该收发信机的逻辑。该逻辑被配置为根据由无线收发信机接收的信标来确定发送该信标的相关无线设备是否支持用来广告来自相关无线设备的可用服务的协议。该逻辑被配置为响应于确定相关无线设备支持该协议,经由无线收发信机发送对来自相关无线设备的可用服务的请求。该逻辑被配置为经由无线收发信机接收对该请求的响应,该响应包括签名。该逻辑被配置为通过确认该签名包括以加密方式与服务数据绑定的网络数据来验证该响应。



1. 一种用于对广告服务进行认证的设备, 包括:

用于从接入网络提供商接收信号的装置, 所述信号包括指明所述接入网络提供商具有用来广告可用网络服务的移动服务广告能力的数据;

用于根据所述信号确定所述接入网络提供商支持用来广告可用服务的协议的装置;

用于从所述接入网络提供商请求可用服务的列表的装置;

用于接收对所述请求的响应的装置, 所述响应包括签名, 其中所述签名包括由服务提供商提供的第一签名和由所述接入网络提供商提供的第二签名; 以及

用于验证所述响应的装置, 其中验证所述响应包括确认所述签名包括以加密方式与服务数据绑定的网络数据。

2. 根据权利要求1所述的设备, 其中, 对可用服务的请求包括随机数; 并且用于验证所述响应的装置被配置为检验所述签名包括所述随机数。

3. 根据权利要求1所述的设备, 其中, 所述网络数据包括服务集标识符。

4. 根据权利要求1所述的设备, 其中, 所述网络数据包括对应于所广告的服务的服务集标识符。

5. 根据权利要求1所述的设备, 其中, 所述网络数据包括对应于多个所广告的服务的多个服务集标识符。

6. 根据权利要求1所述的设备, 其中, 所述网络数据包括域名。

7. 根据权利要求1所述的设备, 其中, 所述网络数据包括网络接入标识符。

8. 根据权利要求1所述的设备, 其中, 所述网络数据包括同类扩展服务集标识符。

9. 根据权利要求1所述的设备, 其中, 所述服务数据包括图标图像。

10. 根据权利要求1所述的设备, 其中, 所述服务数据包括引用图标的数据。

11. 根据权利要求1所述的设备, 其中, 所述服务数据包括服务提供商身份。

12. 根据权利要求1所述的设备, 其中, 所述服务数据包括服务统一资源定位符。

13. 根据权利要求1所述的设备, 其中, 所述服务数据包括公共密钥。

14. 根据权利要求1所述的设备, 其中, 所述服务数据包括由证书机构签名的证书; 并且所述设备进一步包括:

用于对所述证书进行验证的装置。

15. 根据权利要求1所述的设备, 其中, 所述服务数据包括由注册机构签名的证书; 并且所述设备进一步包括:

用于对所述证书进行验证的装置。

16. 一种用于对广告服务进行认证的方法, 包括:

从接入网络提供商接收信号, 所述信号包括指明所述接入网络提供商具有用来广告可用网络服务的移动服务广告能力的数据;

根据所述信号确定所述接入网络提供商支持用来广告可用服务的协议;

从所述接入网络提供商请求可用服务的列表;

接收对所述请求的响应, 所述响应包括签名, 其中所述签名包括由服务提供商提供的第一签名和由所述接入网络提供商提供的第二签名; 以及

验证所述响应, 其中验证所述响应包括确认所述签名包括以加密方式与服务数据绑定的网络数据。

17. 根据权利要求16所述的方法, 其中, 对可用服务的请求包括随机数; 并且验证所述响应还包括检验所述签名包括所述随机数。
18. 根据权利要求16所述的方法, 其中, 所述网络数据包括服务集标识符。
19. 根据权利要求16所述的方法, 其中, 所述网络数据包括对应于所广告的服务的服务集标识符。
20. 根据权利要求16所述的方法, 其中, 所述网络数据包括对应于多个所广告的服务的多个服务集标识符。
21. 根据权利要求16所述的方法, 其中, 所述网络数据包括域名。
22. 根据权利要求16所述的方法, 其中, 所述网络数据包括网络接入标识符。
23. 根据权利要求16所述的方法, 其中, 所述网络数据包括同类扩展服务集标识符。
24. 根据权利要求16所述的方法, 其中, 所述服务数据包括图标图像。
25. 根据权利要求16所述的方法, 其中, 所述服务数据包括引用图标的数据。
26. 根据权利要求16所述的方法, 其中, 所述服务数据包括服务提供商身份。
27. 根据权利要求16所述的方法, 其中, 所述服务数据包括服务统一资源定位符。
28. 根据权利要求16所述的方法, 其中, 所述服务数据包括公共密钥。
29. 根据权利要求16所述的方法, 其中, 所述服务数据包括由证书机构签名的证书; 并且所述方法进一步包括:
对所述证书进行验证。
30. 根据权利要求16所述的方法, 其中, 所述服务数据包括由注册机构签名的证书; 并且所述方法进一步包括:
对所述证书进行验证。

管理员注册认证服务

[0001] 相关申请的交叉引用

[0002] 本申请基于并要求2009年11月6日递交的序号为12/613,784的美国专利申请的优先权。

技术领域

[0003] 本公开一般地涉及对通过网络而广告的服务的认证。

背景技术

[0004] 诸如管理员服务(Concierge Service)之类的移动服务广告协议创建了一些非常有趣的机会,允许诸如智能电话之类的下一代设备自动呈现由无线局域网(WLAN)提供的服务,而无需用户执行复杂的设备配置。例如,采用移动管理员服务的WLAN可以连同网络服务的提供商来广告网络服务。接收广告的移动设备可以在移动设备上输出(例如,显示和/或提供音视觉信号)所广告的服务,从而允许与移动设备相关联的用户访问所广告的服务。但是,还产生了滥用的可能,例如,欺骗性的应用可能化装为合法应用,欺骗性的应用可以用来引诱垃圾邮件攻击的潜在的受害人和/或潜在的弱点。

附图说明

[0005] 结合于此并且形成说明书的一部分的附图示出了示例实施例。

[0006] 图1示出了根据示例实施例而配置的无线局域网的示例。

[0007] 图2示出了根据示例实施例而配置的具有服务提供商的无线局域网的示例。

[0008] 图3示出了无线移动单元从无线局域网接收广告服务的示例信号图。

[0009] 图4示出了无线移动单元从包括服务提供商的无线局域网接收广告服务的示例信号图。

[0010] 图5是可以实现示例实施例的移动设备的框图。

[0011] 图6是可以实现示例实施例的服务器的框图。

[0012] 图7示出了可以实现示例实施例的计算机系统的示例。

[0013] 图8示出了移动设备执行的获取网络广告服务的方法的示例。

[0014] 图9示出了服务器执行的提供广告服务的方法的示例。

具体实施方式

[0015] 示例实施例的概述

[0016] 下面给出了示例实施例的简要概述,以提供对示例实施例的一些方面的基本理解。该概述不是示例实施例的广泛概述。目的既不在于标识出示例实施例的关键或者必需元件,也不在于描绘出所附权利要求的范围。唯一目的在于以简要形式给出示例实施例的一些概念,作为随后给出的更详细的描述的序言。

[0017] 根据示例实施例,这里公开了一种装置,包括被配置来发送和接收数据的收发信

机以及耦合到该收发信机的逻辑。该逻辑被配置为根据由收发信机接收的信号来确定发送该信号的相关设备是否支持用来广告可从相关设备获得的可用服务的协议。该逻辑被配置为响应于确定相关设备支持该协议,经由收发信机发送对来自相关设备的可用服务的请求。该逻辑被配置为经由收发信机接收对该请求的响应,该响应包括签名。该逻辑被配置为通过确认该签名包括以加密方式与服务数据绑定的网络数据来验证该响应。

[0018] 根据示例实施例,这里公开了一种装置,包括被配置来发送和接收数据的接口以及耦合到该接口的逻辑。该逻辑被配置为从该接口接收获取广告服务请求。该逻辑被配置为生成对该获取广告请求的响应,该响应包括签名,该签名包括以加密方式与服务数据绑定的网络数据。该逻辑被配置为经由该接口发送对获取广告请求的响应。

[0019] 根据示例实施例,这里公开了一种方法,包括:从接入网络提供商接收诸如信标或者探测响应之类的信号。该方法还包括:根据该信号来确定接入网络提供商是否支持用来广告可用服务的协议。从接入网络提供商请求可用服务的列表。对该请求的响应被接收,该响应包括签名。该响应被验证,其中验证该响应的步骤包括确认该签名包括以加密方式与服务数据绑定的网络数据。

[0020] 示例实施例的描述

[0021] 该描述提供了不被用于限制所附权利要求的范围的示例。附图一般地指示出了示例的特征,其中应该理解和明白的是,相同的标号被用来指代相似的元件。说明书中提到的“一个实施例”或者“实施例”或者“示例实施例”是指所描述的特定特征、结构或者特性被包括在这里描述的至少一个实施例中,而不是意味着该特征、结构或者特性存在于这里描述的所有实施例中。

[0022] 在示例实施例中,当非接入点(AP)无线台站(STA)位于接入点的范围中时,预先关联服务广告被递送到该无线台站。每个服务由定义服务类型的服务描述符、网络入口点(例如,服务集标识符或者说“SSID”)、用于终端用户的队列(例如,图标)、用于获取服务的统一资源定位符(URL)等来描述。在示例实施例中,第2层标识符(SSID)被绑定到第7层元素(例如URL),以对广告的来源进行认证。如这里所使用的,层支持开放系统互连(OSI)模型。例如,第1层是物理层,第2层是管理设备与共享介质的交互的数据链路层(媒体访问控制(MAC)层是第2层的子层),第3层是网络层(第3层协议的最公知的示例是互联网协议“IP”),并且第7层是应用层。

[0023] 在特定实施例中,当非AP STA做出对服务列表的请求时,该STA包括用于标识该特定请求的随机数(nonce)。基础设施网络中的节点创建包括服务列表的响应,包括来自该非AP STA的随机数(用于重放保护),并且利用私用密钥对该响应进行签名。

[0024] 任何适当的受信签名实体可以被用在这里描述的示例实施例中。例如,受信签名实体可以根植于诸如Verisign、Thawte等公共证书机构(CA)中。作为另一示例,受信签名实体可以根植于诸如Cisco(本发明的受让人)、IBM等私有证书机构中。作为又一示例,受信签名实体可以是诸如T-Mobile、AT&T、Boingo等网络接入提供商。作为再一示例,受信签名实体可以是应用服务提供商(例如,Target、Westfield、Best Buy、Frys等)。

[0025] 服务描述符的验证允许STA和AP在STA加入网络之前对所广播的所有服务进行验证,并且有选择地报告欺骗性的服务。适当地利用安全管理员能力,AP和STA可以报告它们在它们的环境中检测到的欺骗性的服务。无法通过验证的图标(服务)不被呈现给终端用

户,并且可以被有选择地向网络静默地标记。

[0026] 图1示出了根据示例实施例而配置的无线局域网100的示例。网络100包括服务提供商网络102和与服务提供商网络102无线通信的移动设备108。服务提供商网络102包括接入点(AP)104和耦合到AP 104的与移动服务广告协议(MSAP)兼容的服务器106。如在这里所使用的,MSAP是管理将通过网络边缘(在这个示例中是AP 104)来广告的、由较高的层(在OSI模型中)提供的服务的协议。电气和电子工程师协会当前颁布了标准IEEE 802.11u,网络100在示例实施例中可以采用该标准。注意,尽管这里的描述描述了移动设备108与接入点104进行无线通信,但是本领域技术人员应该很容易理解的是,移动设备108和接入点104之间的通信链路可以是有线链路或者无线和有线通信链路的组合。

[0027] 在示例实施例中,AP 104发送诸如信标和对探测的响应之类的信号,从而广告其支持用来广告来自可以通过AP 104接入的网络102的可用服务的广告(诸如,IEEE 802.11u获取广告服务“GAS”、MSAP或类似类型的)协议。移动设备108接收信标(或者探测响应),并且可以确定AP 104(这里也称为接入网络提供商或者“ANP”)支持广告协议。作为响应,移动设备108可以向AP 104发送对服务的请求(例如,“GAS”请求)。AP 104将该请求转发给MSAP服务器106。

[0028] MSAP服务器106生成对请求的响应。该响应包括网络数据和服务数据。MSAP服务器106还生成以加密方式绑定网络数据和服务数据的签名,该签名被包括在响应中。例如,MSAP可以构建包括随机数、服务数据、网络数据、以及被定义为RSA的消息完整性校验(MIC)的经认证响应(MSAP服务器私有密钥,SHA-256(随机数|服务数据|网络数据)),其中,RSA是Rivest,Shamir,&Adleman算法,SHA-256是安全散列算法,256比特。该响应被发送给AP 104。该响应被从AP 104转发到移动设备108。

[0029] 移动设备108在接收到响应时对响应进行验证。在示例实施例中,移动设备108被配置为通过确认签名包括以加密方式与服务数据绑定的网络数据来对响应进行验证。根据示例实施例的一方面,如果响应被验证为可信的,则移动设备108将允许与AP 104进行通信。例如,在MSAP应用中,如果响应是有效的,则移动设备108将允许由AP 104发送的广告被处理。例如,图标可以被显示在用户界面上,或者音频信号可以被输出。

[0030] 在特定实施例中,移动设备108可以判决是否进行关联,并且可以选择AP 104上的、映射到移动设备108所寻求的服务的服务集标识符(SSID)(因为可能存在不止一个由AP提供的服务)。对签名的验证(还可能在服务提供商所包括的服务数据中存在对服务进行验证的签名)有助于提供服务有效性和缓解网络钓鱼攻击的进一步的证据。这两个签名的组合可以提供对抗网络钓鱼攻击的“完全确认”。例如,由服务提供商提供的第一签名是主要证据,并且由ANP(例如,这个示例中的AP104)提供的第二签名用于证明ANP被授权来提供该服务并且已经通过将请求者所提供的经认证的随机数包括在内而将其响应绑定到请求。

[0031] 但是,如果由AP 104发送的响应不是有效的,则移动设备将停止与AP 104进行通信。例如,移动设备108将禁止向用户界面显示图标。这提供了对抗网络钓鱼攻击和对抗垃圾邮件的保护。

[0032] 在示例实施例中,由移动节点108发送给AP 104的对可用服务的请求包括随机数。MSAP服务器108被进一步配置为将随机数包括在签名中。在对响应进行验证时,移动设备108检验签名是否包括随机数。

[0033] 在一示例实施例中,网络数据包括基本服务集标识符(BSSID)。在另一示例实施例中,网络数据包括对应于所广告的服务的服务集标识符(SSID)。在又一示例实施例中,网络数据包括对应于多个所广告的服务的多个服务集标识符(SSID)。在又一示例实施例中,网络数据包括域名。在又一示例实施例中,网络数据包括网络接入标识符(NAI)。在再一示例实施例中,网络数据包括同类扩展服务集标识符(HESSID)。在又一示例实施例中,网络数据包括诸如可扩展认证协议(EAP)方法和/或证书类型之类的802.11关联能力。其他示例实施例包括前述数据的组合。

[0034] 在一示例实施例中,服务数据包括图标图像和/或用于获取图标图像的引用。在另一示例实施例中,服务数据包括服务提供商身份。在又一示例实施例中,服务数据包括服务统一资源定位符(URL)。在又一示例实施例中,服务数据包括公共密钥。在一示例实施例中,服务数据包括由证书机构签名的证书。在另一示例实施例中,服务数据包括由注册机构签名的证书。其他示例实施例包括前述数据的组合。

[0035] 在一示例实施例中,在服务数据包括由证书机构签名的证书的情况下,移动设备108被进一步配置为对证书进行验证。在另一示例实施例中,在服务数据包括由注册机构签名的证书的情况下,移动设备108被进一步配置为对证书进行验证。

[0036] 图2示出了具有包括服务提供商(在这个示例中是MSAP服务提供商)204(例如,服务器)的服务提供商网络202的无线局域网200的示例。MSAP服务提供商204可以被用来配置和/或更新MSAP服务器106。在示例实施例中,服务提供商从(例如,管理员)证书机构/注册机构(CA/RA)获取有效的x.509证书,其中该证书被用来证明MSAP服务提供商的提供服务数据中所定义的服务的授权。MSAP服务器106从(例如,管理员)CA/RA获取有效的x.509证书,以证明MSAP服务器106被授权来提供MSAP服务并且向前运载服务提供商204的用在广告交换中的服务数据。可以在MSAP服务器106和MSAP服务提供商204之间建立信赖关系,以允许对服务数据的带外动态更新。可选地,更新可以不是动态的,并且是通过其他手段获取的。在示例实施例中,在MSAP服务器106和接入网络提供商(ANP——在该示例中为了简单而被示出为AP 104)之间建立了信赖关系。安全通信通道可以被建立在MSAP服务器106和AP104之间,因此AP 104将把服务广告请求转发给MSAP服务器106,并把来自MSAP服务器106的响应转发给移动设备(或者端点)108。在示例实施例中,在网络配置期间,在MSAP服务器106处定义MSAP服务与AP 104的能力(例如,BSSID、SSID、MSAP领域的)的绑定关系。在示例实施例中,利用用于启用MSAP并且选择通过预先规定的证书而验证了的MSAP服务的策略(例如,证书)来配置移动设备108。

[0037] 图3示出了无线移动单元用来从无线局域网接收广告服务的示例信号图300。信号图300是针对图1中所示的网络100的,但是也可以在图2所示的网络200中实现。移动设备(端点)108从AP 104接收信标302。信标302包括指明其支持广告服务的数据(在该示例中为MSAP,但是任何适当的协议可以被以这种方式来广告)。移动设备108发送从AP 104获取可用服务的请求304。在该示例中,请求304是通用广告服务(GAS)请求。为了额外的安全性,随机数可以被包括在请求304中。这可以对重放攻击产生保护。

[0038] 由AP 104发送的信号306将请求304转发给MSAP服务器106。在该示例中,信号306是获取MSAP服务请求,其具有由移动设备108发送的随机数。

[0039] MSAP服务器106生成对来自移动设备108并且由AP 104转发的获取可用服务的请

求的响应。在该示例中,该响应包括基本服务集标识符(BSSID)、在原始请求中由移动设备108发送的随机数、对应于可用服务的SSID列表、其他的网络数据和服务数据(例如,二进制大型对象“BLOB”列表)、以及签名。签名将网络数据和服务数据绑定。例如,签名可以绑定BSSID、SSID列表、随机数以及其他的网络数据和服务数据。例如,签名可以由RSA生成(MSAP服务器私有密钥,(SHA-256(随机数|服务数据|网络数据)))。响应(在这个示例中是包括BSSID、随机数、SSID列表、服务BLOB列表以及签名的MSAP服务响应)被转发给AP 104,如信号308所示。AP然后将来自MSAP服务器106的响应(在本示例中为GAS响应)转发给移动设备108,如信号310所示。

[0040] 移动设备308对信号310进行验证。如果信号310是可信的,则移动设备可以继续与AP 104通信。例如,利用在MSAP服务响应中指示出的SSID,移动设备108可以与AP 104相关联,如信号312所示。作为另一示例,移动设备可以在用户界面(未示出)上提供输出,并且如果指明服务已被选择的输入被接收到,则移动设备108可以使用对应于所选择的服务的SSID而与AP 104相关联。但是,如果信号308无法通过验证,则移动设备108可以停止与AP 104通信。

[0041] 图4示出了无线移动单元从包括外部服务提供商的无线局域网接收广告服务的示例信号图400。在该示例中,MSAP服务器和服务提供商(SP)之间存在关系。信号图400是使用采用了MSAP服务提供商204的图2中的网络200示出的。MSAP服务提供商204可以向MSAP服务器106发送MSAP服务配置和/或更新,如信号402所示出的。信号402可以适当地包括多个信号。MSAP服务配置/更新可以在任何时间被在带外发送,所以信号402不应该被解释为仅以图4中所示的次序出现。

[0042] 图5是可以实现示例实施例的移动设备500的框图。移动设备500适合于实现移动设备108(图1-4)的功能。移动设备502包括无线收发信机502,该无线收发信机被配置为发送和接收无线信号。耦合到无线收发信机的逻辑504被配置为经由无线收发信机502发送和接收数据。逻辑504可以被配置为实现参考移动设备108(图1-4)在这里描述的功能。例如,移动设备500可以经由无线收发信机502接收信号(例如,被动地接收信标,或者通过发送探测信号并且等待对探测信号的响应来主动接收信号)。逻辑504可以根据信标来确定信标的来源是否支持诸如MSAP之类的网络广告协议或者与所提出的802.11u协议兼容的协议。逻辑504还可以使用代表可用服务的数据来帮助选择与网络的连接(例如,哪个AP和利用哪个SSID)。逻辑504然后可以经由无线收发信机502发送信号,以请求可用服务。逻辑504还可以生成包括在经由无线收发信机502发送的信号中的随机数。对请求的响应可以经由无线收发信机502而被接收。逻辑504可以通过采用任何适当的技术(诸如,这里描述的技术)来对响应进行认证。例如,逻辑504可以确定响应是否包含以加密方式绑定了网络数据(诸如,信标的来源的BSSID)和服务数据(诸如图标或者对用来广告服务的信标的引用)的签名。逻辑504可以配置有检验签名的证书。在特定实施例中,逻辑504配置了用于广告服务器(诸如,MSAP服务器)的公共密钥。在特定实施例中,逻辑504可以基于在服务广告处理中获取的数据来选择与网络的连接(或者网络)。例如,逻辑504可以确定是继续留在使用指定SSID的AP,还是移动到不同的AP(甚至不同的网络)。

[0043] 图6是可以实现示例实施例的服务器600的框图。服务器600适合于实现诸如MSAP服务器106(图1-4)之类的广告服务器。服务器600包括用于发送和接收信号的接口(收发信

机)602和用于实现这里描述的功能的逻辑604。在示例实施例中,服务器600包括与接入网络提供商(ANP,诸如图1-4中的AP 104)和服务提供商(诸如图2和图4中的服务提供商204)通信的单个接口。在替代实施例中,接口602包括多个接口。例如,第一接口可以被用于与ANP通信,第二接口被用于与服务提供商通信。

[0044] 在示例实施例中,逻辑604被配置为经由接口602从服务提供商接收配置和/或更新数据。配置和/或更新数据可以在任何时间被在带外接收。

[0045] 在示例实施例中,逻辑604被进一步配置为对对于广告服务的请求进行响应。例如,如图3中描述的获取MSAP服务请求。逻辑604可以被配置为生成可用服务的列表。该列表可以与ANP的BSSID和其他网络数据(例如,对应于可用服务的SSID)绑定。例如,信息可以被进行散列(SHA-256),并且签名可以是使用私有密钥通过RSA加密而生成的。逻辑604然后经由接口602发送响应。

[0046] 图7示出了可以实现示例实施例的计算机系统700的示例。计算机系统700适合于实现逻辑504(图5)和/或逻辑604(图6),该逻辑可以被用于实现移动设备108(图1-4)和服务器106(图104)的功能。

[0047] 计算机系统700包括总线702或者用于传送信息的其他通信机制、以及与总线702耦合的用于处理信息的处理器704。计算机系统700还包括诸如随机存取存储器(RAM)或者耦合到总线702的其他动态存储设备之类的主存储器706,用于存储将由处理器704执行的指令和信息。主存储器706还可以被用于在将被处理器704执行的指令的执行期间存储临时变量或者其他中间信息。计算机系统700还包括只读存储器(ROM)708或者耦合到总线702的其他静态存储设备,用于存储用于处理器704的静态信息和指令。诸如磁盘或者光盘之类的存储设备710被提供并被耦合到总线702,用于存储信息和指令。

[0048] 在示例实施例中,例如,当计算机系统700被用于实现移动设备108时,计算机系统700可以经由总线702耦合到诸如阴极射线管(CRT)或者液晶显示器(LCD)之类的显示器712,用于向计算机用户显示信息。诸如包括字母数字键和其他按键的键盘之类的输入设备714耦合到总线702,用于向处理器704传送信息和命令选择。另一种类型的用户输入设备是诸如鼠标、轨迹球、触摸屏或者光标方向键之类的光标控件716,用于向处理器704传送方向信息和命令选择并且用于控制显示器712上的光标移动。该输入设备一般具有两个轴上的两个自由度,允许设备在平面中指定位置的第一轴(例如,x)和第二轴(例如,y)。

[0049] 示例实施例的一个方面涉及使用计算机系统700来认证移动设备广告。根据示例实施例,认证移动设备广告的处理由计算机系统700响应于处理器704执行主存储器706中包含的一个或多个指令的一个或多个序列而提供。这些指令可以被从诸如存储设备710之类的另一计算机可读介质读入到主存储器706中。主存储器706中包含的指令序列的执行使得处理器704执行这里描述的处理步骤。多处理布置中的一个或多个处理器可以被用来执行主存储器706中包含的指令序列。在替代实施例中,硬连线电路可以被代替软件指令或者结合软件指令使用,来实现示例实施例。所以,这里描述的实施例不限于硬件电路和软件的任何特定组合。

[0050] 这里使用的术语“计算机可读介质”是指参与向处理器704提供用于执行的指令的任何介质。这种介质可以采用很多形式,包括但不限于非易失性介质和易失性介质。非易失性介质例如包括诸如存储设备710之类的光盘或磁盘。易失性介质包括诸如主存储器706之

类的动态存储器。普通形式的计算机可读介质例如包括软盘、柔性盘、硬盘、磁卡、纸带、具有孔洞图案的任何其他物理介质、RAM、PROM、EPROM、FLASH PROM、CD、DVD、或者任何其他存储器芯片或者卡盒、或者计算机可以从其进行读取的任何其他介质。

[0051] 在将一个或多个指令的一个或多个序列运载到处理器704以供执行时，可以涉及各种形式的计算机可读介质。例如，指令最初可以被承载在远程计算机的磁盘上。远程计算机可以将指令装载到其动态存储器中，并且使用调制解调器在电话线上发送指令。计算机系统700本地的调制解调器可以在电话线上接收数据，并且使用红外发送机将数据转换为红外信号。耦合到总线702的红外检测器可以接收在红外信号中运载的数据，并且将数据放置在总线702上。总线702将数据运载到主存储器706，处理器704从主存储器706取回并且执行指令。主存储器706所接收到的指令可以可选地在被处理器706执行之前或者之后存储在存储设备710上。

[0052] 计算机系统700还包括耦合到总线702的通信接口718。通信接口718提供双向数据通信，该双向数据通信将计算机系统700耦合到与本地网络720相连的网络链路720。这使得计算机系统700能够与其他设备通信。

[0053] 例如，通信接口718可以是局域网(LAN)卡，用于提供与兼容LAN的数据通信连接。作为另一示例，通信接口718可以是综合服务数字网(ISDN)卡或者调制解调器，用于提供与相应类型的电话线的数据通信连接。无线链路也可以被实现。在任何这样的实施方式中，通信接口718发送和接收运载了代表各种类型的信息的数字数据流的电、电磁或者光信号。

[0054] 鉴于以上所述的结构和功能性特征，参考图8和图9将更好地理解根据示例实施例的方法。虽然为了说明的简要，图8和图9的方法被示出并被描述为连续执行，但是将理解和明白的是，示例实施例不受所示出的次序的限制，因为某些方面可以以不同于这里所示出和描述的次序发生和/或与其他方面同时发生。另外，可能并不需要所有示出的特征来实现这里描述的方法。这里描述的方法被适当地改编以用硬件、软件或者它们的组合来实现。

[0055] 图8示出了由移动设备执行的获取网络广告服务的方法800的示例。方法800可以由这里的图1-4中所描述的移动设备108实现。

[0056] 在802，包括以下数据的信号被接收：该数据指明信号的来源(例如，ANP或者AP)具有用来广告可用网络服务的移动服务(诸如管理员)广告能力。该信号可以是信标或者向探测信号发送的响应。

[0057] 在804，对可用服务的请求被发送给信标的来源(例如，ANP或者AP)。该请求可以是通用广告服务请求。在特定实施例中，该请求包括随机数。

[0058] 在806，对请求的响应被接收。在示例实施例中，该响应包括ANP的BSSID、随机数、网络数据、服务数据以及签名。网络数据和服务数据可以包括这里描述的很多不同类型的数据。例如，网络数据可以包括服务提供商的域名，并且服务数据可以包括URL、图标和/或对图标的引用。

[0059] 在808，接收到响应的设备对签名进行验证。在示例实施例中，使用用于响应的来源(例如，诸如MSAP服务器之类的服务器)的公共密钥来对签名进行验证。在示例实施例中，接收到响应的设备确定签名是否包括以加密方式绑定到服务数据的网络数据。在特定实施例中，接收设备检验签名是否包括在对可用服务的请求中发送的随机数。

[0060] 如果在808，响应被确定是无效的，则在810，通信被终止(中止)。在管理员环境中，

这防止了流氓设备在移动设备上呈现图标并广告服务。这还可以防止网络钓鱼攻击和/或垃圾邮件。

[0061] 如果在810,响应被确定是有效的,则在812,用于确定网络选择的通信可以继续运行。例如,在管理员环境中,图标或者其他输出(诸如,视频、音频、音视觉输出等)可以经由用户接口而被输出。如果指示出对特定服务的选择的输入被接收到,则移动设备可以使用用于所选择的服务的BSSID和SSID来与ANP相关联。

[0062] 图9示出了由服务器执行的提供可以从相关网络获得的广告服务的方法900的示例。方法900可以由图1-4中描述的MSAP服务器106执行。

[0063] 在902,服务器对ANP进行配置,以广告可用服务。例如,可以向AP提供包括在由AP发送的信标的数据,用来广告网络支持广告协议(诸如,MSAP)。在特定实施例中,ANP可以被更新。

[0064] 在904,服务器接收对可用服务的请求。例如,该请求可以是通用广告服务请求。在特定实施例中,该请求还包括随机数。

[0065] 在906,对请求的响应被生成。该响应一般包括可用服务的列表。该列表可以包括服务集标识符,其中服务集标识符与各个可用服务相关联。另外,该响应可以包括最初接收到请求的ANP的BSSID。该请求还可以包括诸如图标(或者用于获得图标的引用)、服务提供商身份、服务URL、公共密钥、MSAP服务器身份、由CA/RA签名的证书之类的其他服务数据。网络数据可以包括BSSID、可以提供所广告的服务的SSID的SSID列表、诸如域名、NAI和/或HESSID之类的网络身份、和/或诸如可扩展认证协议(EAP)方法、证书类型之类的802.11关联能力等。在示例实施例中,服务器构建包括随机数、服务数据、网络数据和可以被定义为RSA的MIC的经认证响应(服务器私有密钥,SHA-#比特(随机数|服务数据|网络数据))。

[0066] 在908,响应被转发。例如,该响应可以被转发给AP,以供转发给发送了请求的移动设备。

[0067] 以上描述了示例实施例。当然,不可能描述组件或方法的每种可以想到的组合,但是本领域普通技术人员将认识到,示例实施例的很多进一步的组合和置换都是可能的。尽管以上描述描述了无线网络,但是本领域技术人员应该很容易明白,仅为了容易说明而描述了无线网络,这里描述的原理也适用于有线网络。因此,本申请意图包括落入所附权利要求的精神和范围内的所有这样的变形、修改和改变,所附权利要求的精神和范围根据它们被公平地、合法地、公正地授予的宽度来解释。

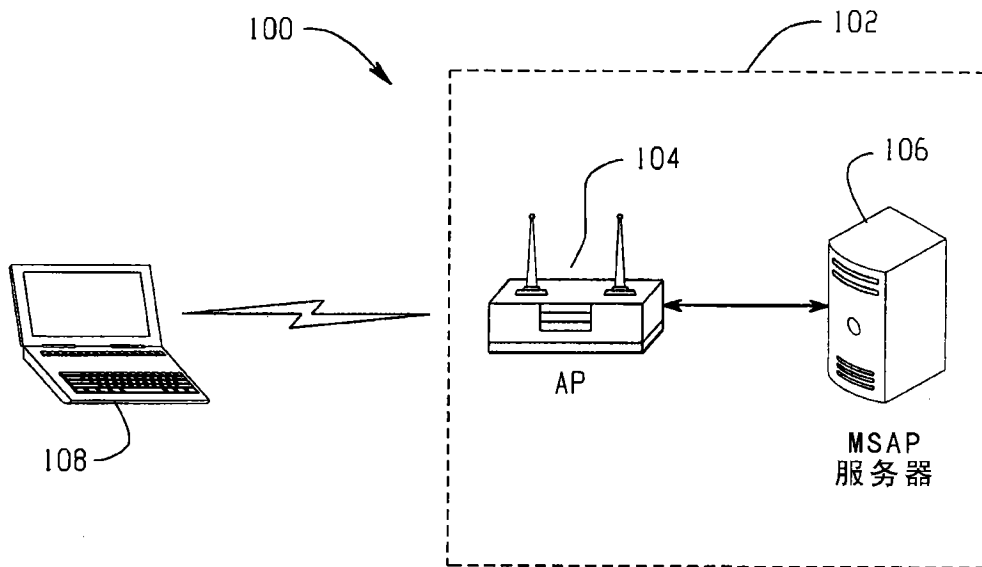


图1

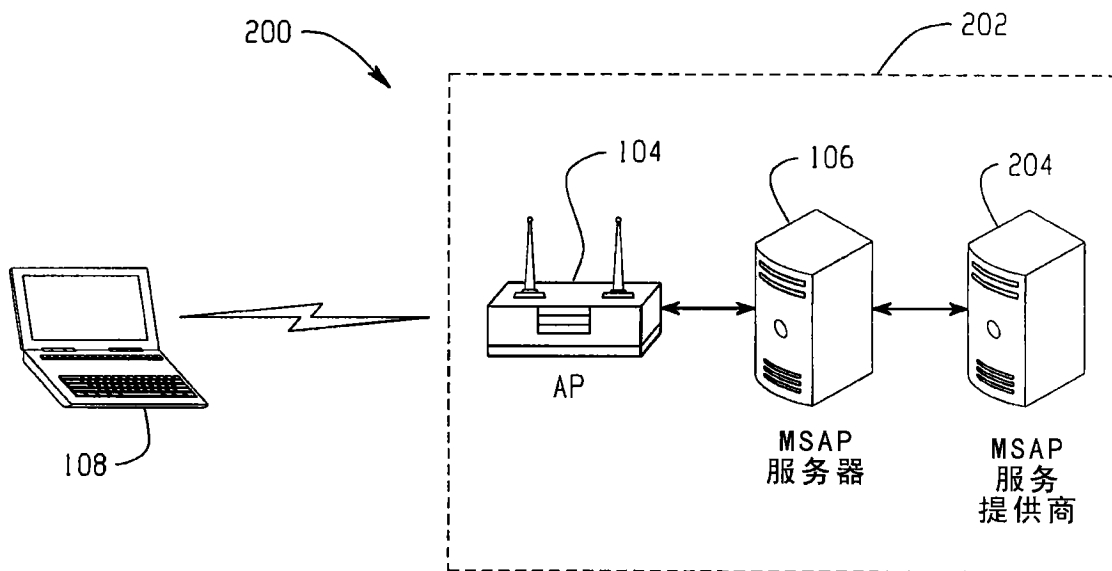


图2

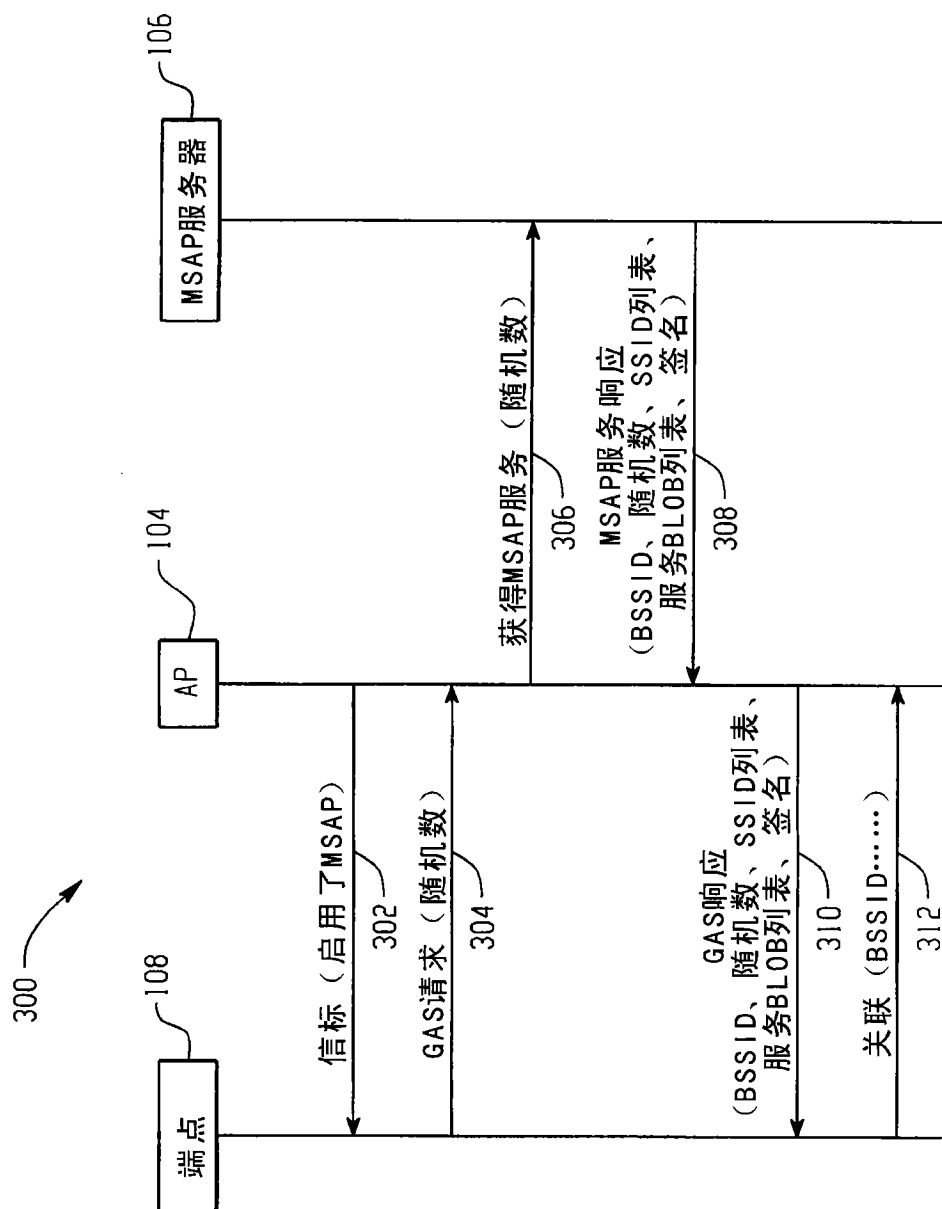


图3

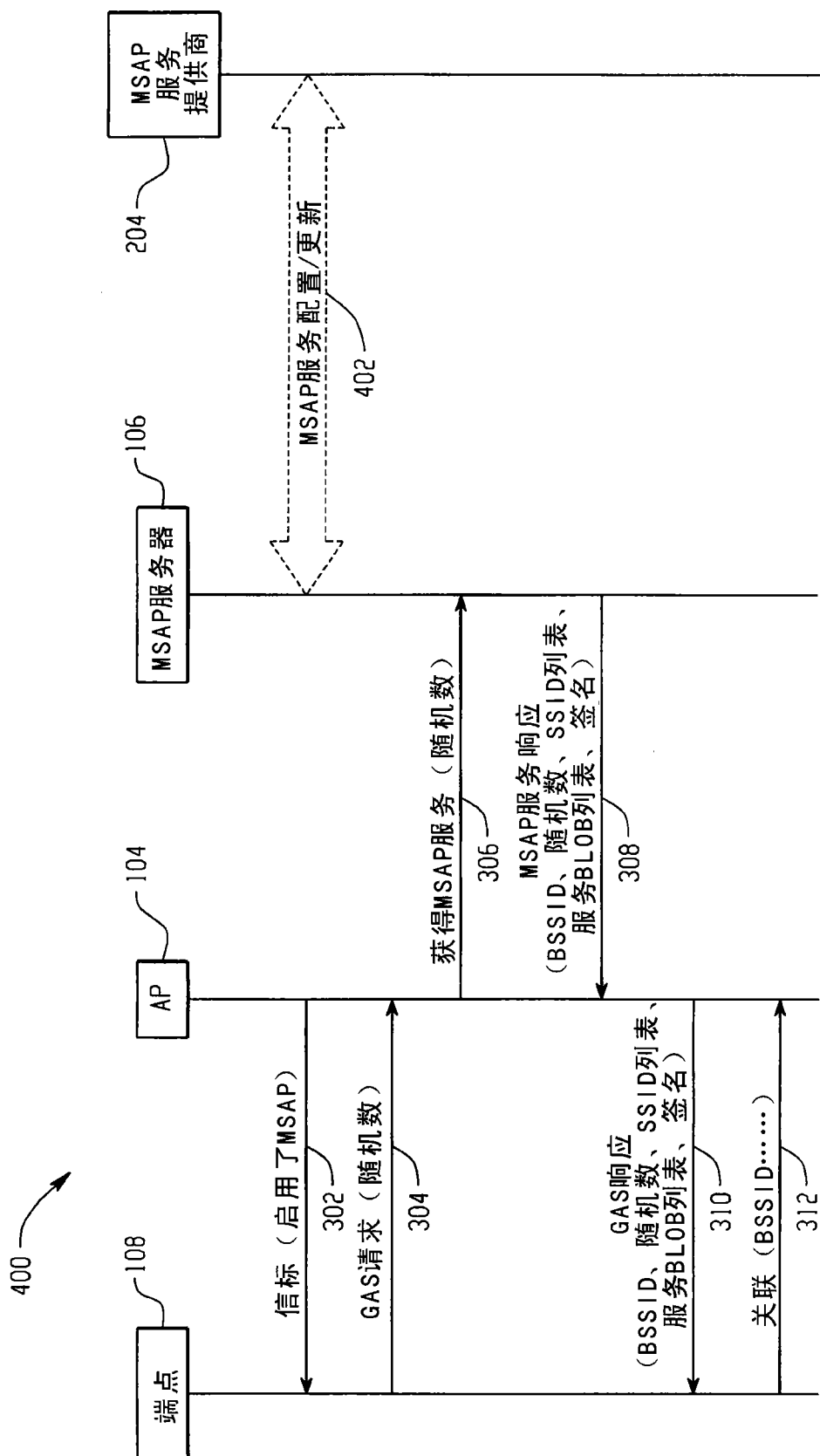
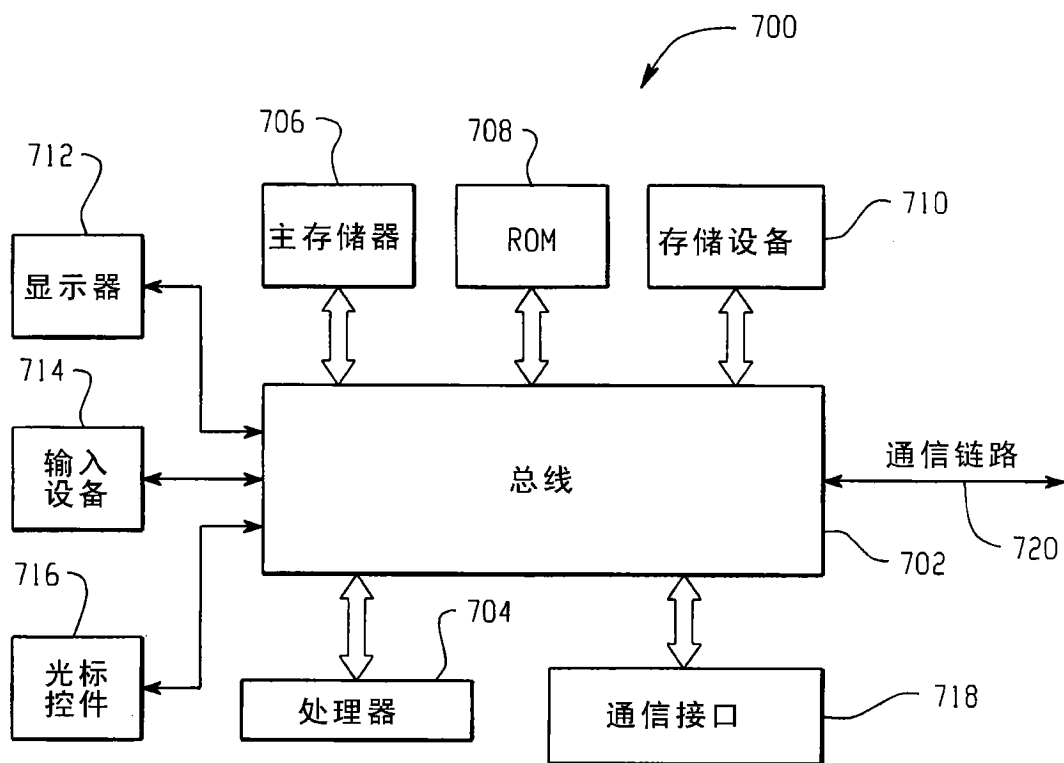
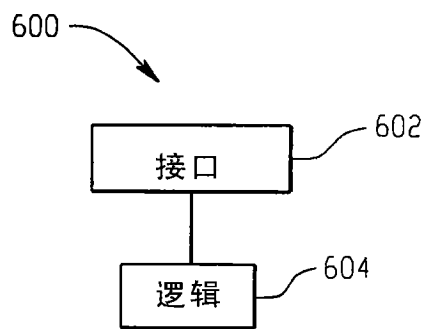
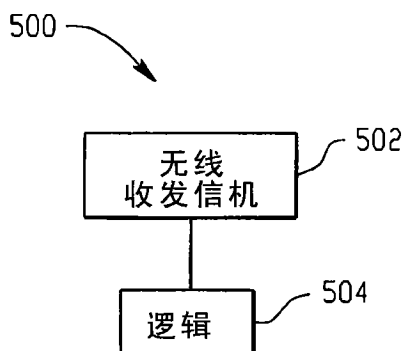


图4



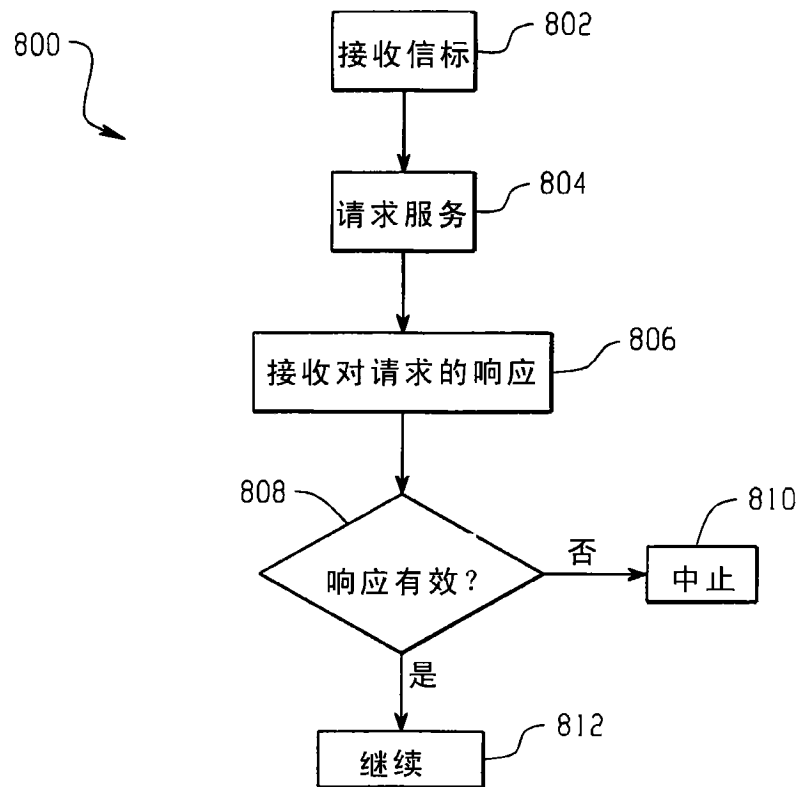


图8

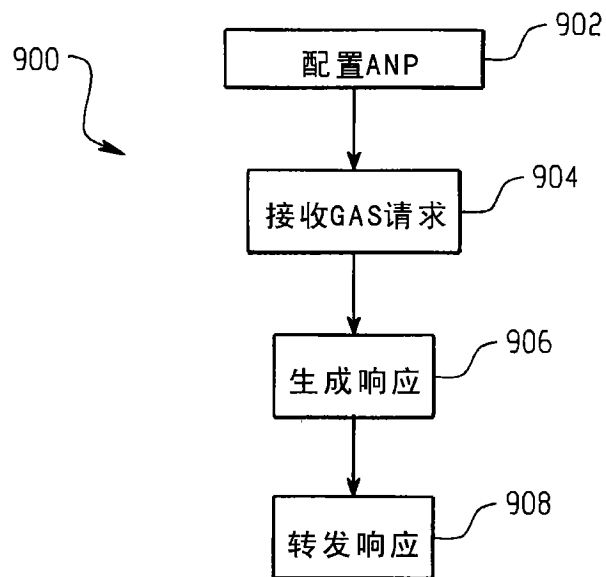


图9