(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 103891329 B
(45)授权公告日 2017.11.28

(21)申请号 201180074388.4
(22)申请日 2011.10.25
(65)同一申请的已公布的文献号
申请公布号 CN 103891329 A
(43)申请公布日 2014.06.25
(85)PCT国际申请进入国家阶段日
2014.04.24
(86)PCT国际申请的申请数据
PCT/IB2011/054765 2011.10.25
(87)PCT国际申请的公布数据
WO2013/061114 EN 2013.05.02
(73)专利权人 诺基亚技术有限公司
地址 芬兰埃斯波
(72)发明人 T·萨沃莱南 B·加伯尔
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅
(51)Int.Cl.
H04W 12/06(2006.01)
H04L 12/24(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101563883 A,2009.10.21,
US 2010071040 A1,2010.03.18,
US 2005243872 A1,2005.11.03,
CN 1677978 A,2005.10.05,
CN 1677978 A,2005.10.05,
审查员 刘婧

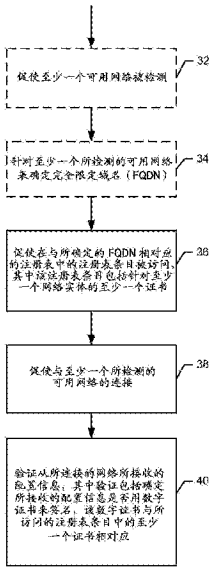
权利要求书5页 说明书11页 附图3页

(54)发明名称

用于保护主机配置消息的方法

(57)摘要

提供了一种用于验证使用例如受信任协议、诸如Hostspot2.0的接入网络的方法、装置和计算机程序产品。在这个方面，提供了一种方法，该方法包括：促使至少一个可用网络被检测。该方法可以进一步包括针对该至少一个所检测的可用网络来确定完全限定域名(FQDN)。该方法可以进一步包括促使在与所确定的FQDN相对应的注册表中的注册表条目被访问，其中该注册表条目包括针对至少一个网络实体的至少一个证书。该方法可以进一步包括验证从所连接的网络所接收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的至少一个证书相对应。



CN 103891329 B

1.一种用于无线通信的方法,包括:

促使至少一个可用网络被检测;

针对所述至少一个所检测的可用网络,确定完全限定域名(FQDN);

促使从与所确定的FQDN相对应的注册表下载注册表条目,其中所述注册表条目包括针对至少一个网络实体的至少一个证书;

促使与所述至少一个所检测的可用网络的连接;以及

验证从所连接的网络所接收的配置信息,其中验证包括确定所接收的配置信息是否用数字证书来签名,所述数字证书与所下载的注册表条目中的所述至少一个证书相对应,

其中所述注册表条目从受信任网络注册表被下载,所述受信任网络不同于所检测的可用网络,并且其中所述配置信息从所述至少一个网络实体被接收。

2.根据权利要求1所述的方法,其中所述至少一个网络实体包括针对服务提供商的路由器、动态主机配置协议(DHCP)服务器或域名系统(DNS)服务器中的至少一个。

3.根据权利要求1所述的方法,进一步包括:接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息,其中所述签名进一步包括属于移动终端的标识或随机数中的至少一项。

4.根据权利要求1所述的方法,进一步包括:接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息,其中所述消息进一步包括被用来签名所述消息的公共密钥的哈希,以依据签名所述消息的服务提供商记录来确定网络实体。

5.根据权利要求1所述的方法,进一步包括:接收路由器通告、DHCP或DHCPv6消息,以及确定所接收的路由器通告、DHCP或DHCPv6消息是否来自经验证的合法网络实体,并且在所接收的消息包含网络单元的有效签名的实例中促使与经验证的接入网络的连接,所述网络单元被授权给与所述接入网络相关联的至少一个移动终端的IP供应。

6.根据权利要求1所述的方法,其中在网络实体在所述注册表中具有对应的证书、或者网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书的实例中,所述网络实体被授权。

7.根据权利要求1所述的方法,其中IPv6头部选项被定义为通过所指配的IP地址以及属于客户端的标识或随机数而在路由器通告中携带签名。

8.根据权利要求4所述的方法,其中所述签名包括至少一个字段,其中所述字段中的一个字段包括生成所述数字签名的实体的FQDN。

9.根据权利要求1所述的方法,其中路由器请求包含由所述路由器通告所签名的字段中的链路层地址选项或随机数选项中的至少一个。

10.根据权利要求1所述的方法,其中DHCPv6消息包含被配置为携带哈希和签名的认证选项。

11.根据权利要求1至10中任一项所述的方法,进一步包括:在签名被验证并且存在以下各项之一的实例中接受IP地址配置信息:所述网络实体在所述注册表中具有对应的证书或者所述网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书。

12.一种用于无线通信的装置,包括:

处理器,以及

包括软件的存储器,所述存储器与所述软件被配置为与所述处理器一起促使所述装置

至少：

促使至少一个可用网络被检测；

针对所述至少一个所检测的可用网络，确定完全限定域名(FQDN)；

促使从与所确定的FQDN相对应的注册表下载注册表条目，其中所述注册表条目包括针对至少一个网络实体的至少一个证书；

促使与所述至少一个所检测的可用网络的连接；以及

验证从所连接的网络所接收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，所述数字证书与所下载的注册表条目中的所述至少一个证书相对应，

其中所述注册表条目从受信任网络注册表被下载，所述受信任网络不同于所检测的可用网络，并且其中所述配置信息从所述至少一个网络实体被接收。

13.根据权利要求12所述的装置，其中所述至少一个网络实体包括针对服务提供商的路由器、动态主机配置协议(DHCP)服务器或域名系统(DNS)服务器中的至少一个。

14.根据权利要求12所述的装置，其中包括计算机程序代码的所述至少一个存储器进一步被配置为与所述至少一个处理器一起促使所述装置：接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息，其中所述签名进一步包括属于移动终端的标识或随机数中的至少一项。

15.根据权利要求12所述的装置，其中包括计算机程序代码的所述至少一个存储器进一步被配置为与所述至少一个处理器一起促使所述装置：接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息，其中所述消息进一步包括被用来签名所述消息的公共密钥的哈希，以依据签名所述消息的服务提供商记录来确定网络实体。

16.根据权利要求12所述的装置，其中包括计算机程序代码的所述至少一个存储器进一步被配置为与所述至少一个处理器一起促使所述装置：接收路由器通告、DHCP或DHCPv6消息，并且确定所接收的路由器通告、DHCP或DHCPv6消息是否来自经验证的合法网络实体，并且在所接收的消息包含网络单元的有效签名的实例中促使与经验证的接入网络的连接，所述网络单元被授权给与所述接入网络相关联的至少一个移动终端的IP供应。

17.根据权利要求12所述的装置，其中在网络实体在所述注册表中具有对应的证书、或者网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书的实例中，所述网络实体被授权。

18.根据权利要求12所述的装置，其中IPv6头部选项被定义为通过所指配的IP地址以及属于客户端的标识或随机数而在路由器通告中携带签名。

19.根据权利要求18所述的装置，其中签名包括至少一个字段，其中所述字段中的一个字段包括生成所述数字签名的实体的FQDN。

20.根据权利要求12所述的装置，其中路由器请求包含由所述路由器通告所签名的字段中的链路层地址选项或随机数选项。

21.根据权利要求12所述的装置，其中DHCPv6消息包含被配置为携带哈希和签名的认证选项。

22.根据权利要求12至21中任一项所述的装置，其中包括计算机程序代码的所述至少一个存储器进一步被配置为与所述至少一个处理器一起促使所述装置：在签名被验证并且存在以下各项之一的实例中接受IP地址配置信息：所述网络实体在所述注册表中具有对应

的证书或者所述网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书。

23.一种计算机可读存储器介质，具有存储在其上的程序代码，所述程序代码在由装置执行时促使所述装置至少：

促使至少一个可用网络被检测；

针对所述至少一个所检测的可用网络，确定完全限定域名(FQDN)；

促使从与所确定的FQDN相对应的注册表下载注册表条目，其中所述注册表条目包括针对至少一个网络实体的至少一个证书；

促使与所述至少一个所检测的可用网络的连接；以及

验证从所连接的网络所接收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，所述数字证书与所下载的注册表条目中的所述至少一个证书相对应，

其中所述注册表条目从受信任网络注册表被下载，所述受信任网络不同于所检测的可用网络，并且其中所述配置信息从所述至少一个网络实体被接收。

24.根据权利要求23所述的计算机可读存储器介质，其中所述至少一个网络实体包括针对服务提供商的路由器、动态主机配置协议(DHCP)服务器或域名系统(DNS)服务器中的至少一个。

25.根据权利要求23所述的计算机可读存储器介质，进一步包括在由所述装置执行时促使所述装置至少执行以下操作的程序代码：接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息，其中所述签名进一步包括属于移动终端的属于移动终端的标识或随机数中的至少一项。

26.根据权利要求23所述的计算机可读存储器介质，进一步包括在由所述装置执行时促使所述装置至少执行以下操作的程序代码：接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息，其中所述消息进一步包括被用来签名所述消息的公共密钥的哈希，以依据签名所述消息的服务提供商记录来确定网络实体。

27.根据权利要求23所述的计算机可读存储器介质，进一步包括在由所述装置执行时促使所述装置至少执行以下操作的程序代码：确定所接收的路由器通告、DHCP或DHCPv6消息是否来自经验证的合法网络实体，并且在所接收的消息包含网络单元的有效签名的实例中促使与经验证的接入网络的连接，所述网络单元被授权给与所述接入网络相关联的至少一个移动终端的IP供应。

28.根据权利要求23所述的计算机可读存储器介质，其中IPv6头部选项被定义为包含消息的签名。

29.根据权利要求23所述的计算机可读存储器介质，其中IPv6头部选项被定义为通过所指配的IP地址以及属于客户端的标识或随机数而在路由器通告中携带签名。

30.根据权利要求23所述的计算机可读存储器介质，其中签名包括至少一个字段，其中所述字段中的一个字段包括生成所述数字签名的实体的FQDN。

31.根据权利要求23所述的计算机可读存储器介质，其中路由器请求包含由所述路由器通告所签名的字段中的链路层地址选项或随机数选项。

32.根据权利要求23所述的计算机可读存储器介质，其中DHCPv6消息包含被配置为携带哈希和签名的认证选项。

33.根据权利要求23至32中任一项所述的计算机可读存储器介质，进一步包括在由所

述装置执行时促使所述装置至少执行以下操作的程序代码：在签名被验证并且存在以下各项之一的实例中接受IP地址配置信息：所述网络实体在所述注册表中具有对应的证书或者所述网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书。

34.一种用于无线通信的设备，包括：

用于促使至少一个可用网络被检测的装置；

用于针对所述至少一个所检测的可用网络，确定完全限定域名(FQDN)的装置；

用于促使从与所确定的FQDN相对应的注册表下载注册表条目的装置，其中所述注册表条目包括针对至少一个网络实体的至少一个证书；

用于促使与所述至少一个所检测的可用网络的连接的装置；以及

用于验证从所连接的网络所接收的配置信息的装置，其中验证包括确定所接收的配置信息是否用数字证书来签名，所述数字证书与所下载的注册表条目中的所述至少一个证书相对应，

其中所述注册表条目从受信任网络注册表被下载，所述受信任网络不同于所检测的可用网络，并且其中所述配置信息从所述至少一个网络实体被接收。

35.根据权利要求34所述的设备，其中所述至少一个网络实体包括针对服务提供商的路由器、动态主机配置协议(DHCP)服务器或域名系统(DNS)服务器中的至少一个。

36.根据权利要求34所述的设备，进一步包括：用于接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息的装置，其中所述签名进一步包括属于移动终端的标识或随机数中的至少一项。

37.根据权利要求34所述的设备，进一步包括：用于接收包括来自路由器、DHCP服务器或DNS服务器中至少一项的签名的消息的装置，其中所述消息进一步包括被用来签名所述消息的公共密钥的哈希，以依据签名所述消息的服务提供商记录来确定网络实体。

38.根据权利要求34所述的设备，进一步包括：用于接收针对主机的无线电通告的装置，其中所述无线电通告包括证书选项，所述证书选项包含针对用AAA服务器的认证来签名的路由器的证书。

39.根据权利要求34所述的设备，进一步包括：用于确定所接收的路由器通告、DHCP或DHCPv6消息是否来自经验证的合法网络实体并且在所接收的消息包含网络单元的有效签名的实例中促使与经验证的接入网络的连接的装置，所述网络单元被授权给与所述接入网络相关联的至少一个移动终端的IP供应。

40.根据权利要求34所述的设备，其中IPv6头部选项被定义为通过所指配的IP地址以及属于客户端的标识或随机数而在路由器通告中携带签名。

41.根据权利要求34所述的设备，其中在网络实体在所述注册表中具有对应的证书、或者网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书的实例中，所述网络实体被授权。

42.根据权利要求34所述的设备，其中签名包括至少一个字段，其中所述字段中的一个字段包括生成所述数字签名的实体的FQDN。

43.根据权利要求34所述的设备，其中路由器请求包含由所述路由器通告所签名的字段中的链路层地址选项或随机数选项。

44.根据权利要求34所述的设备，其中DHCPv6消息包含被配置为携带哈希和签名的认

证选项。

45.根据权利要求34至44中任一项所述的设备，进一步包括：用于在签名被验证并且存在以下各项之一的实例中接受IP地址配置信息的装置：所述网络实体在所述注册表中具有对应的证书或者所述网络实体具有由在所述注册表中具有对应的证书的实体所发出的证书。

用于保护主机配置消息的方法

技术领域

[0001] 本发明的一些实施例一般性地涉及通信技术，并且更特别地涉及在无线环境中保护主机配置消息。

背景技术

[0002] 主机(诸如移动终端)可以被配置为经由互联网协议(IP)版本6(v6)路由器通告(RA)或动态主机配置协议(DHCP)v6消息来接收地址配置信息，然而主机(诸如移动终端)可能不能够验证RA或DHCP消息的合法性。对验证该消息的合法性的这种无能力可能导致攻击，诸如流氓RA攻击。另外，在其中流氓DHCP服务器被使用的实例中，移动终端很可能将不能够确定DHCP服务器是否是为该网络指配IP地址的合法服务器。对验证所指配的IP地址的合法性的无能力可能允许攻击者以他们看来合适的方式错误地配置移动终端，例如，攻击者可能促使移动终端使用错误的源地址或者可能引导被错误配置的路由器/服务器向未检测的移动终端指配不正确的IP地址。在效果上，攻击者可以安排拒绝服务(denial-of-service)攻击和/或用于中间人(man-in-the-middle)攻击的设置主机的两者。备选地或另外地，当路由器或服务器发送RA/DHCP_供应消息(RA/DHCP_offer message)而这些RA/DHCP_供应消息泄漏到它们本不应该到的网络段中时，移动终端IP地址错误配置还可能在该路由器或DHCP服务器错误配置的情况中发生。

[0003] 另外，服务集标识符(SSID)可信度也是一个问题。例如，对于攻击者而言越来越流行建立起具有如“Sprint”或“ATT”的名称的SSID，并且作为响应，用户可能加入这样的网络，认为它们是受信任的供应商和无线服务。

发明内容

[0004] 因此根据一个示例实施例提供了一种方法、装置和计算机程序产品，以便验证使用利用诸如Hotspot2.0类型网络部署的网络部署的接入网络。根据一个实施例，移动终端可以针对特定的接入网络(AN)来访问可信网络注册表，诸如Hotspot2.0注册表条目，该可信网络注册表与所发现的接入网络的完全限定域名(FQDN)相对应。使用该可信网络注册表(诸如Hotspot2.0注册表条目)，该移动终端可以针对经验证的AN来下载服务提供商记录，该记录可以包括由受信任当局所签名的证书。这些证书还可以识别当前正在经验证的AN上操作的经验证的路由器、DHCP服务器和/或DNS服务器。在一些示例实施例中，使用这些经验证的证书，该移动终端然后可以被配置为验证各种RA、DHCP消息等是合法的，并且进一步地该移动终端可以接入该经验证的AN。

[0005] 在这个方面，提供了一种方法，该方法包括：促使至少一个可用网络被检测。该方法可以进一步包括：针对该至少一个所检测的可用网络，确定完全限定域名(FQDN)。该方法可以进一步包括：促使在与所确定的FQDN相对应的注册表中的注册表条目被访问，其中该注册表条目包括用于至少一个网络实体的至少一个证书。该方法可以进一步包括：促使与该至少一个所检测的可用网络的连接。该方法可以进一步包括：验证从所连接的网络所接

收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的该至少一个证书相对应。

[0006] 一种示例装置可以包括至少一个处理器以及存储计算机程序代码的至少一个存储器，其中该至少一个存储器以及所存储的计算机程序代码被配置为与该至少一个处理器一起促使该装置来促使至少一个可用网络被检测。该至少一个存储器以及所存储的计算机程序代码进一步被配置为与该至少一个处理器一起促使该装置针对该至少一个所检测的可用网络来确定完全限定域名(FQDN)。该至少一个存储器以及所存储的计算机程序代码进一步被配置为与该至少一个处理器一起促使该装置来促使在与所确定的FQDN相对应的注册表中的注册表条目被访问，其中该注册表条目包括用于至少一个网络实体的至少一个证书。该至少一个存储器以及所存储的计算机程序代码进一步被配置为与该至少一个处理器一起促使该装置来促使与该至少一个所检测的可用网络的连接。该至少一个存储器以及所存储的计算机程序代码进一步被配置为与该至少一个处理器一起来促使该装置验证从所连接的网络所接收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的该至少一个证书相对应。

[0007] 在进一步的实施例中，提供了一种计算机程序产品，该计算机程序产品包括在其中存储有计算机可读程序指令的至少一个非瞬态计算机可读存储介质，这些计算机可读程序指令包括：被配置为促使至少一个可用网络被检测的程序指令。这些计算机可读程序指令还包括：被配置为针对该至少一个所检测的可用网络来确定完全限定域名(FQDN)的程序指令。这些计算机可读程序指令还包括：被配置为促使在与所确定的FQDN相对应的注册表中的注册表条目被访问的程序指令，其中该注册表条目包括用于至少一个网络实体的至少一个证书。这些计算机可读程序指令还包括：被配置为促使与该至少一个所检测的可用网络的连接的程序指令。这些计算机可读程序指令还包括：被配置为验证从所连接的网络所接收的配置信息的程序指令，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的该至少一个证书相对应。

[0008] 一种示例设备可以包括：用于促使至少一个可用网络被检测的装置。该设备还可以包括：用于针对该至少一个所检测的可用网络来确定完全限定域名(FQDN)的装置。该设备还可以包括：用于促使在与所确定的FQDN相对应的注册表中的注册表条目被访问的装置，其中该注册表条目包括用于至少一个网络实体的至少一个证书。该设备还可以包括：用于促使与该至少一个所检测的可用网络的连接的装置。该设备还可以包括：用于验证从所连接的网络所接收的配置信息的装置，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的该至少一个证书相对应。

附图说明

[0009] 已经如此一般性地描述了本发明的示例实施例，现在将对附图做出参考，这些附图不一定按比例绘制，并且其中：

[0010] 图1是具有可能经历主机配置消息并且可以从本发明的实施例受益的移动终端的系统的示意性表示；

[0011] 图2是根据本发明的一个实施例的可以由移动终端来体现的装置的框图；以及

[0012] 图3是图示了根据本发明的一个实施例所执行的操作的流程图。

具体实施方式

[0013] 现在将在下文中参考附图更完全地描述本发明，在这些附图中示出了这些发明的一些但不是全部的实施例。事实上，这些发明可以以许多不同的形式来体现并且不应当被解释为限制于本文所阐述的这些实施例；更确切地，这些实施例被提供以使得本公开内容将满足可适用的法律要求。贯穿全文，相似的标号指代相似的元件。

[0014] 如在本申请中所使用的，术语“电路”指代下列的所有：(a)仅硬件的电路实施方式(诸如仅模拟和/或数字电路中的实施方式)以及(b)电路和软件(和/或固件)的组合，诸如(如可适用的)：(i)(多个)处理器的组合或者(ii)(多个)处理器/软件的部分(包括一起工作以促使装置(诸如移动电话或服务器)执行各种功能的(多个)数字信号处理器、软件、和(多个)存储器)以及(c)需要软件或固件用于操作的电路，诸如(多个)微处理器或(多个)微处理器的一部分，即使该软件或固件不是物理存在的。

[0015] “电路”的这个定义应用至在本申请中对这个术语的所有使用，包括在任何权利要求中。作为进一步的示例，如在本申请中所使用的，术语“电路”还将覆盖仅处理器(或多个处理器)或处理器的一部分以及它的(或它们的)伴随软件和/或固件的实施方式。用于示例并且如果对特定的权利要求元素可适用，术语“电路”还将覆盖用于移动电话的基带集成电路或专用集成电路，或者在服务器、蜂窝网络设备、或其他网络设备中的类似集成电路。

[0016] 本发明的示例实施例的方法、装置以及计算机程序产品可以被配置为连同Hotspot2.0网络来操作。当前发明的示例实施例的示例移动终端可以被配置为，促使受信任网络实体(诸如Hotspot2.0注册表)被查询并且然后可以促使实体被下载，该实体可以包括下列非穷举的列表的至少一部分：热点的接入网络(AN)完全限定域名(FQDN)；AN授权、授权和记账(AAA)服务器认证；以及其他受信任网络单元，诸如Hotspot2.0特定元件，如Hotspot2.0网络实体的信任锚(例如，Hotspot2.0WiFi根CA)与发送者的(例如，接入网络路由器的)公共密钥之间的认证路径。在这个示例中，发送者可以是生成消息的网络实体(例如，诸如路由器、DHCP服务器、DNS服务器等等的网络实体)。

[0017] 在802.11(其由此通过引用而被并入)中被定义用以下载“热点在线签到提供商列表”L2元素的通用通告服务(GAS)接入网络查询协议(ANQP)过程具有下列内容：

[0018]

在线签到(OSU)提供商长度	OSU FQDN长度	OSU FQDN	OSU_NAI(网络接入标识符)长度	OSU_NA1(可选的)	OSU服务器URI(统一资源标识符)长度	OSU服务器URI	OSU方法
八位组： 2	1	可变的	1	可变的	1	可变的	1

[0019] 尽管该方法、装置和计算机程序产品可以被实施在各种不同的系统中，图1中示出了这种系统的一个示例，其包括第一通信设备(例如，移动终端10)，第一通信设备能够经由网络实体12(诸如无线路由器、基站、节点B、演进型节点B(eNB)、WiFi站点或其他网络实体)与网络14(例如，核心网络)通信。尽管该网络可以根据有线或无线联网技术来配置，这些联网技术包括但不限于无线保真(Wi-Fi)；无线局域网(WLAN)技术、诸如电气和电子工程师协会(IEEE)802.11、802.16等等。

[0020] 可以被设想到、但是在当前的发明中不被要求的其他通信是诸如长期演进(LTE)或LTE-高级(LTE-A),其他网络可以支持本发明的实施例的该方法、装置和计算机程序产品,包括根据宽带码分多址(W-CDMA)、CDMA2000、全球移动通信系统(GSM)、通用分组无线电服务(GPRS)等来配置的那些网络。备选地或另外地,网络14可以包括可以经由对应的有线和/或无线接口相互通信的各种不同的节点、设备或功能的集合。例如,该网络可以包括一个或多个小区(包括网络实体12),每个小区可以服务各自的覆盖区域。服务小区和相邻小区可以是例如一个或多个蜂窝或移动网络或公共陆地移动网络(PLMN)的一部分。进而,其他设备、诸如处理设备(例如,个人计算机、服务器计算机等)可以经由网络耦合至移动终端10和/或其他通信设备。

[0021] 诸如移动终端10(也被称为用户设备(UE)、无线站(STA)等)的通信设备,可以经由网络实体12进而经由网络14与其他通信设备或其他设备通信。在一些情况下,通信设备可以包括用于向服务小区发射信号并且用于从服务小区接收信号的天线。

[0022] 在一些示例实施例中,移动终端10可以是移动通信设备,诸如举例而言,移动电话,便携式数字助理(PDA),寻呼机,膝上型计算机,或者多种其他手持或便携式通信设备、计算设备、内容生成设备、内容消费设备中的任何一个,或者它们的组合。如此,移动终端10可以包括一个或多个处理器,该一个或多个处理器可以独自地或者与一个或多个存储器组合地定义处理电路。该处理电路可以利用被存储在该存储器中的指令,以在这些指令被该一个或多个处理器执行时促使移动终端10以特定的方式操作或者执行特定的功能。移动终端10还可以包括通信电路和对应的硬件/软件,以实现与其他设备和/或网络14的通信。

[0023] 在一个实施例中,例如,移动终端10和/或网络实体12可以被体现为装置20或者以其他方式包括装置20,装置20由图2的框图一般性地表示。尽管装置20可以例如由移动终端10或网络实体12所采用,但是应当注意,下面所描述的这些组件、设备或元件可以不是强制性的并且因此在某些实施例中一些组件、设备或元件可以被省略。另外,一些实施例可以包括超出本文所示出并描述的那些组件、设备或元件的进一步的或者不同的组件、设备或元件。

[0024] 如在图2中所示出的,装置20可以包括处理电路22或者以其他方式与处理电路22通信,处理电路22可配置为根据本文所描述的示例实施例而执行动作。该处理电路可以被配置为根据本发明的示例实施例来执行数据处理、应用执行和/或其他处理和管理服务。在一些实施例中,该装置或该处理电路可以被体现为芯片或芯片组。换句话说,该装置或该处理电路可以包括一个或多个物理封装(例如,芯片),该一个或多个物理封装包括结构装配(例如,基板)上的材料、组件和/或接线。该结构装配可以提供物理强度、尺寸的节省、和/或针对包括在其上的组件电路的电相互作用的限制。该装置或该处理电路可以因此在一些情况下被配置为在单个芯片上实施本发明的实施例,或者将本发明的实施例实施为单个“片上系统”。如此,在一些情况下,芯片或芯片组可以构成用于执行一个或多个操作以用于提供本文所描述的功能的装置。

[0025] 在一个示例实施例中,处理电路22可以包括处理器24和存储器28,处理器24和存储器28可以与通信接口26并且在一些情况下与用户接口30通信,或者以其他方式控制通信接口26并且在一些情况下控制用户接口30。如此,该处理电路可以被体现为被配置(例如,用硬件、软件或硬件和软件的组合)为执行本文所描述的操作的电路芯片(例如,集成电路

芯片)。然而,在移动终端10的上下文中所采用的一些实施例中,该处理电路可以被体现为移动计算设备或其他移动终端的一部分。

[0026] 用户接口30(如果被实施)可以与处理电路22通信,以在用户接口处接收用户输入的指示,和/或向用户提供可听的、可视的、机械的或者其他输出。如此,该用户接口可以包括例如,键盘、鼠标、操纵杆、显示器、触摸屏、麦克风、扬声器、和/或其他输入/输出机制。装置20不需要总是包括用户接口。例如,在其中该装置被体现为网络实体12的实例中,该装置可以不包括用户接口。如此,该用户接口在图2中以虚线示出。

[0027] 通信接口26可以包括用于使得与其他设备和/或网络的通信成为可能的一个或多个接口机制。在一些情况下,该通信接口可以是如下的任何装置,诸如被配置为从网络14接收数据和/或向网络14发送数据的被体现在硬件或硬件和软件的组合中的设备或电路,和/或与处理电路22通信的任何其他设备或模块,诸如在移动终端10与网络实体12之间。在这个方面,该通信接口可以包括例如,用于使得与无线通信网络的通信成为可能的天线(或多个天线)以及支持硬件和/或软件,和/或用于支持经由电缆、数字订户线路(DSL)、通用串行总线(USB)、以太网或其他方法的通信的通信调制解调器或其他硬件/软件。

[0028] 在一个示例实施例中,存储器28可以包括一个或多个非瞬态存储器设备,诸如举例而言,固定的或者可移除的易失性和/或非易失性存储器。该存储器可以被配置为存储信息、数据、应用、指令等,以用于使得装置20能够根据本发明的示例实施例来执行各种功能。例如,该存储器可以被配置为缓存用于由处理器24处理的输入数据。另外地或备选地,该存储器可以被配置为存储用于由该处理器执行的指令。作为又另一个备选,该存储器可以包括可以存储各种文件、内容或数据集的多个数据库之一。除了该存储器的内容之外,应用可以被存储以用于由该处理器执行,以便执行与每个相应应用相关联的功能。在一些情况下,该存储器可以经由用于在该装置的组件之间传递信息的总线与该处理器通信。

[0029] 处理器24可以以多种不同的方式来体现。例如,该处理器可以被体现为各种处理装置,诸如微处理器或其他处理元件;协处理器;控制器或各种其他计算或处理设备,包括集成电路,诸如举例而言ASIC(专用集成电路)、FPGA(现场可编程门阵列)等中的一项或多项。在一个示例实施例中,该处理器可以被配置为处理被存储在存储器28中的或者该处理器以其他方式可访问的指令。如此,不论由硬件或者由硬件和软件的组合来配置,该处理器可以表示当相应地被配置时能够根据本发明的实施例来执行操作的实体(例如,以处理电路22的形式物理地体现在电路中)。因此,例如,当该处理器被体现为ASIC、FPGA等时,该处理器可以是用于进行本文所描述的操作的被具体配置的硬件。备选地,作为另一个示例,当该处理器被体现为软件指令的执行器时,这些指令可以具体地将该处理器配置为执行本文所描述的操作。

[0030] 图3是图示了由根据所图示的本发明的实施例的方法、装置和计算机程序产品(诸如图2的装置20)所执行的操作的流程图。将理解,该流程图的每个框以及该流程图中的框的组合,可以由各种装置来实施,各种装置诸如硬件、固件、处理器、电路和/或与包括一个或多个计算机程序指令的软件的执行相关联的其他设备。例如,上面所描述的过程中的一个或多个过程可以由计算机程序指令来体现。在这个方面,体现上面所描述的这些过程的这些计算机程序指令可以由将本发明的实施例所体现的装置的存储器设备28来存储并且由该装置中的处理器24来执行。如将认识到的,任何这样的计算机程序指令可以被加载到

计算机或其他可编程装置(例如,硬件)上以产生一个机器,使得该作为结果的计算机或其他可编程装置提供对流程图(多个)框中所指定的功能的实施。这些计算机程序指令还可以被存储在非瞬态计算机可读存储存储器中,这可以指令计算机或其他可编程装置以特定的方式运行,使得被存储在该计算机可读存储存储器中的这些指令产生一种制造品,它的执行实施了流程图(多个)框中所指定的功能。这些计算机程序指令还可以被加载到计算机或其他可编程装置上,以促使一系列操作被执行在该计算机或其他可编程装置上,以产生一种计算机实施的过程,使得执行在该计算机或其他可编程装置上的这些指令提供操作以用于实施流程图(多个)框中所指定的功能。如此,图3的这些操作,当被执行时,将计算机或处理电路转变为被配置为执行本发明的示例实施例的特定机器。因此,图3的这些操作定义了用于将计算机或处理电路22(例如,处理器)配置为执行示例实施例的算法。在一些情况下,通用计算机可以被提供具有该处理器的一个实例,该处理器的实例执行图3该算法以将该通用计算机变换为执行示例实施例的特定机器。

[0031] 因此,该流程图的框支持用于执行所指定的功能的装置的组合以及用于执行所指定的功能的操作的组合。还将理解,该流程图的一个或多个框,以及该流程图中的框的组合,能够由执行所指定的功能的基于专用硬件的计算机系统或者专用硬件和计算机指令的组合来实施。

[0032] 在一些实施例中,上面的这些操作中的某些操作可以如下面所描述的被修改或被进一步扩大。此外,在一些实施例中,还可以包括附加的可选操作(它的一个示例在图3中以虚线示出)。应当认识到,下面的这些修改、可选添加或扩大可以独自地被包括或者与本文所描述的特征之中的任何其他特征组合地与上面的这些操作一起被包括。

[0033] 现在参考图3,一种方法、装置和计算机程序产品被配置为确定所发现的感兴趣的网络是否为被授权的网络,以便使得示例移动终端与实现示例网络实体之间的连接。如操作32中所示出的,装置20可以包括诸如处理电路22、处理器24、通信接口26等的器件,以用于促使至少一个可用网络被检测到。在一个实施例中,使用诸如处理电路22、处理器24、通信接口26等器件的装置20可以根据802.11规范而针对感兴趣的网络来扫描。在一些示例实施例中也可以使用其他无线或有线规范。

[0034] 在其中诸如处理电路22、处理器24、通信接口26等发现了感兴趣的网络(例如AN)的实例中,处理电路22、处理器24、通信接口26等可以促使查询被传输,该查询初始在线签名(OSU)提供商列表被下载并且被存储在存储器26中。备选地或另外地,OSU提供商列表可以被远程地存储或者被存储在存储器28中。

[0035] 在示例实施例中,处理电路22、处理器24、通信接口26等还可以针对所发现的感兴趣的网络以及相关的服务提供商记录来下载和/或访问FQDN。参见操作34。在一些示例实施例中,FQDN和SP从注册表(例如,受信任网络注册表,Hotspot2.0注册表等)被下载和/或被访问,并且SP的证书可以由受信任当局签名,诸如由WiFi联盟RootCA签名。SP记录在一些示例实施例中可以包含但不限于:SP的名称、SP的FQDN、SP的图标、以及SP AAA服务器和签名服务器的证书。在示例实施例中,SP记录可以被扩展以包括用于多个网络实体的证书,该多个网络实体提供与该感兴趣的网络的连接,诸如但不限于,网络实体(例如,路由器、DHCP服务器和/或DNS服务器)。

[0036] 备选地或另外地,在尝试接入感兴趣的网络之前,移动终端可以尝试收集受信任

网络注册表实体，诸如Hotspot2.0注册表实体。参见操作36。在移动终端关联至Hotspot2.0AN(例如，使用层2作为运输来访问注册表，如例如WiFi联盟(WFA)规范中所定义的；或者使用已有的因特网连接(例如，经由3G等))之前，处理电路22、处理器24、通信接口26可以促使针对Hotspot2.0注册表实体的请求被访问。受信任网络(诸如Hotspot2.0网络)、SP记录还可以在任意时间被预先配置或者被下载并且被存储在移动终端的存储器中，诸如存储器28(例如，SP记录一旦被生成并且由WiFi Root CA签名就可以然后成为自包含的不可修改的数据片)。

[0037] 通过示例的方式，利用由网络的AAA服务器发给网络实体(例如，路由器、DHCP_服务器、DNS等)的证书，该网络实体可以然后使用例如它的来自该证书的私人密钥来签名例如RA、DHCP、和/或DNS_消息。该网络实体，诸如，可以使用该移动终端的媒体接入控制(MAC)地址或者由该移动终端在用以生成签名的请求中所提供的随机数。在一些示例实施例中，从该网络实体被传输给移动终端的响应消息中的该签名，可以被添加至和/或附加至地址、前缀、FQDN和/或向该移动终端所提供的其他配置。该签名还可以通过向该移动终端所提供的配置信息来生成，例如生成该签名(存在于它的证书中)的该实体的FQDN和/或属于该移动终端的标识或随机数。该响应还可以包含被用来签名该消息的该实体的公共密钥的哈希，以允许该移动终端容易识别来自SP记录的哪个实体签名了该响应消息。

[0038] 备选地或另外地，路由器请求(RS)可以包含链路层地址选项和/或随机数选项，其然后可以被包括在由生成了该数字签名的实体所签名的字段(诸如FQDN字段)中。在DHCP的实例中，由该移动终端所发送的该移动终端的MAC地址和/或随机数(nonce)可以是所生成的签名的一部分。DHCP或者DHCPv6消息还可以包含如下的网络单元的有效签名，该网络单元被授权向与该接入网络相关联的至少一个移动终端来供应IP。

[0039] 备选地或另外地，处理电路22、处理器24、通信接口26可以被配置为接收RA和/或DHCP响应，该RA和/或DHCP响应可以包含携带发送者的证书的选项。证书在这个实例中可以存在于注册表中，或者可以使用存在于注册表条目中的AAA服务器的证书来签名。在签名RA或DHCPv6消息中所使用的这些证书可以由AAA服务器或者具有由SP的AAA服务器所发出的证书的任何备选中间实体来发出并且签名。在其中存在中间实体的实例中，这些中间实体的证书可以是注册表中的SP记录的一部分。

[0040] 备选地或另外地，在其中受信任网络(诸如Hotspot2.0的感兴趣的网络)具有许多网络实体(诸如路由器)的实例中，DHCP服务器可以不具有受信任网络注册表(诸如Hotspot2.0注册表)中的所有这些网络实体的证书中的每个证书。因此，被配置为由移动终端可访问的受信任注册表可以具有AAA服务器证书，并且因此在其中网络实体(诸如路由器)向主机提供RA的实例中，RA可以具有证书选项，该证书选项包含与AAA服务器的证书一起签名的路由器的证书。

[0041] 在示例实施例中，在移动终端已经访问和/或下载了上面所提到的所发现的感兴趣网络的FQDN中的至少一个之后，受信任证书等、处理电路22、处理器24、通信接口26等可以然后促使与网络实体的连接。参见操作38。在一些示例实施例中，受信任证书等、处理电路22、处理器24、通信接口26等验证从该网络实体所接收的RA和/或DHCP/DHCPv6消息是合法的。参见操作40。例如，处理电路22、处理器24、通信接口26可以促使IPv6RS或DHCP(v6)请求被发出，并且路由器/服务器可以然后以RA或DHCP(v6)供应来回复，RA或DHCP(v6)供应可

以由例如先前从注册表所下载的路由器/服务器证书来签名。

[0042] 在一个实施例中，装置20可以包括诸如处理电路22、处理器24、通信接口26等的装置，可以确定IP地址信息是否来自属于所发现的感兴趣网络的实体以及它是否为被授权发出IP配置相关消息的实体。在确定IP配置消息是否来自被授权的实体中，处理电路22、处理器24可以使用所访问和/或所下载的证书信息来验证所接收的RA或DHCP消息来自受信任且被授权的来源。

[0043] 一种示例验证方法可以包括，在如下的实例中，在该实例中移动终端成功地从受信任网络注册表(诸如Hotspot2.0注册表)获取SP记录并且成功地验证了所接收的RS/RA消息包含IP地址的数字签名以及属于特定移动终端(例如，客户设备)的随机数或标识，以及该数字签名由如下的实体生成，该实体的数字证书是存在的，或者该数字签名由存在于注册表中的实体所发出。

[0044] 另一种示例验证方法可以包括IPv6头部选项，诸如目的地选项，其可以被定义为包含消息的签名。IPv6头部选项可以进一步被定义为通过术语该客户端的所指配的IP地址和标识或随机数而在路由器通告中携带签名。这种方法的附加益处是不理解这个验证框架的示例移动终端可以忽略该认证选项并且仍然可以被配置为在受信任网络上操作。

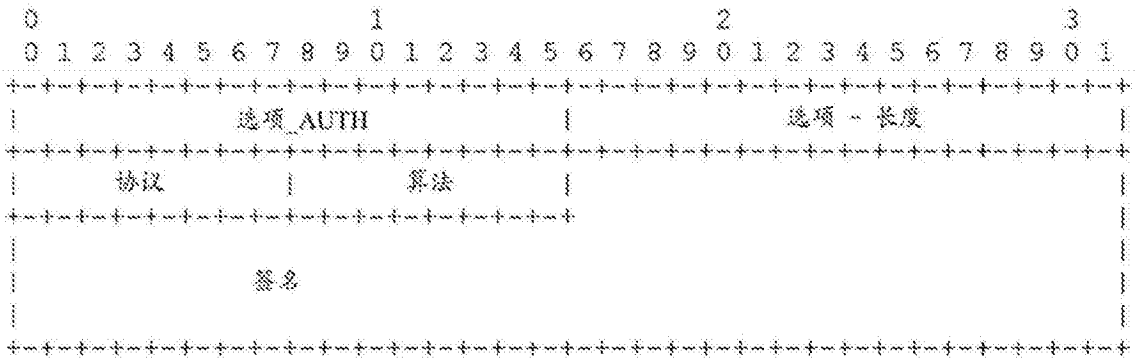
[0045] 在一个示例实施例中，在其中主机(诸如移动终端)(例如从不同的发送者)接收到已签名和未签名的配置信息两者的实例中，该主机(诸如该移动终端)可以然后确定使用来自受信任和被授权方的信息。备选地或另外地，主机可以被配置使得它仅接受来自(诸如所选择的接入网络/网络类型中的)受信任方的信息。因此，在一个实例中，签名被验证并且签名证书的网络实体是网络实体中的如下的一个网络实体，该网络实体的证书在注册表中或者由其证书在该注册表中的实体发出，在该实例中，移动终端10可以然后使用例如处理器24来决定是否接受IP地址配置信息。这样的配置可以例如缓解如下的攻击，在这些攻击中攻击者能够阻挡示例移动终端与示例网络实体之间的通信。验证IP地址是从被授权的网络实体所接收的保护了该移动终端免于由于无意的路由器/服务器误配置而被误配置。

[0046] 在一些示例实施例中，诸如网络实体12的网络实体可以被配置为发出RA。这些网络实体可以然后进一步被配置为，基于所定义的RA选项或者备选地基于在例如能够被重新使用的安全邻居发现(SEND)协议(SEND定义在RFC3971中，RFC3971通过引用并入本文)中所定义的密钥哈希、数字签名以及随机数选项，来提供认证选项。在一些示例实施例中，通过多个字段来生成签名，这些字段中的一个字段是生成该签名的实体的FQDN。备选地或另外地，在其中发送者的证书不在注册表中的实例中，RA将需要具有附加选项，携带该发送者的证书(其也需要是被包括在签名生成中的字段的一部分)。

[0047] 在示例实施例中，DHCP(v6)可以根据本文所描述的系统和方法而被使用。为了使对DHCP(v6)的使用成为可能，认证协议可以由示例网络实体定义为携带哈希和签名。可以使用处理电路22、处理器24、通信接口26等，将支持受信任网络的移动终端(诸如支持Hotspot2.0的移动终端)配置为，每当移动终端促使DHCP发现消息或DHCP请求消息被发出时，促使针对来自服务器的DHCP认证选项的请求。

[0048] 一种示例验证方法可以包括，DHCPv6认证选项(参见例如RFC3315章节22.11，其通过引用被并入)可以被定义用于特定的受信任网络，诸如Hotspot2.0框架。备选地或另外地，备选的DHCPv6选项可以被定义，这样的认证包括但不限于：

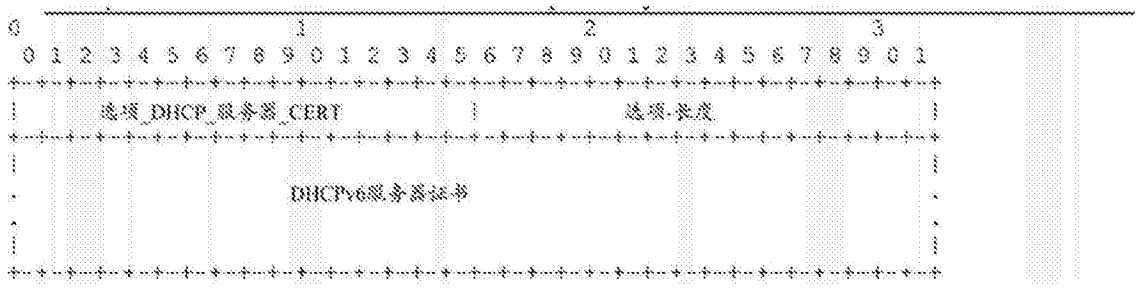
[0049]



选项-代码	选项_AUTH （代码 TBD）
选项-长度	2+签名的长度
协议	Hotspot 2.0证书框架（或者某些事物，tbd）
算法	在认证协议中所使用的算法一被定义为
签名	如所描述的数字签名

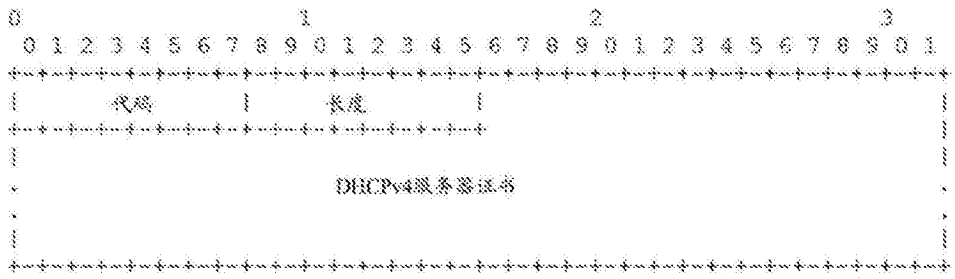
示例DHCP认证选项可以以“算法”、“重放检测”、以及“认证信息”字段而被定义在因特网工程任务组（IETF）规范中。

示例DHCPv6和DHCPv4服务器证书选项可以包括但不限于：



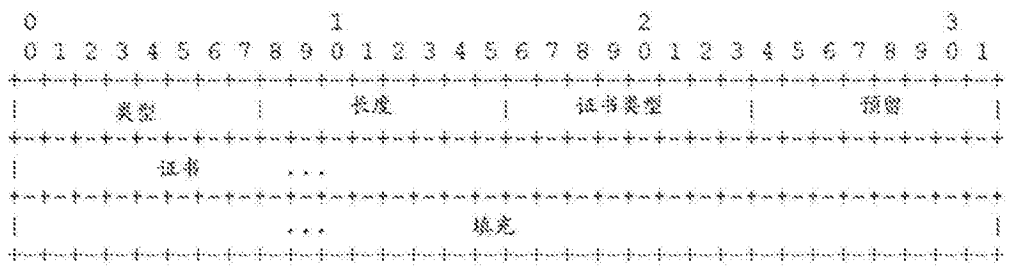
选项_DHCP_服务器_CERT	选项代码
选项-长度	证书的长度
DHCPv6服务器证书	证书

[0050]



代码	选项代码TBD
长度	证书的长度
DHCPv4服务器证书	证书

这里是用于SEND（RFC3971）中所定义的证书选项的可能的新证书认证类型定义（新的事物用组体）、另一个选项是以类似的结构定义完全新的选项：



类型

16

长度

选项的长度（包括类型、长度、证书类型、填充长度、以及证书字段），可以以8位组的单元为单位。

证书类型

在证书字段中所包括的证书的类型。这个规范定义了用于这个字段的合法值，诸如，但不限于：

1	X.509v3证书，如下面所规定的
2	X.509 Hotspot 2.0发送者证书

预留

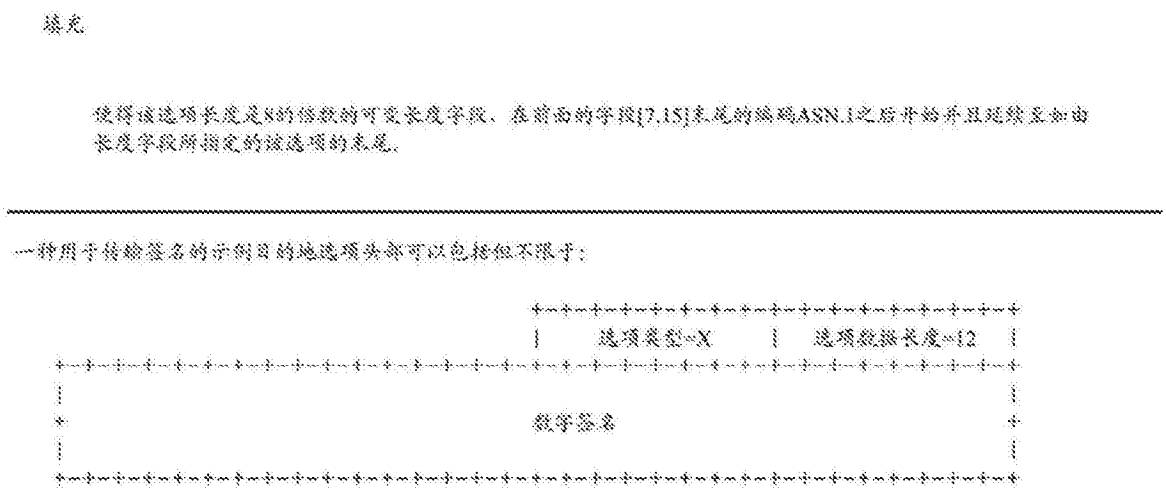
用于未来使用而预留的8比特字段。该值可以由发送者初始化为零并且可以被接收者忽略。

证书

在其中证书类型字段被设置为1的实例中，该证书字段可以包含X.509v3证书[7]。

当该证书类型字段被设置为2时，该证书字段可以包含受信任网络证书、诸如Hotspot 2.0证书。

[0051]



[0052] 得到前述描述和相关联的附图中所提出的教导的益处，这些发明所属领域的技术人员将会想到本文所阐述的这些发明的许多修改和其他实施例。因此，将理解，这些发明将不限制于所公开的这些特定实施例，并且修改和其他实施例旨在为被包括在所附权利要求的范围内。此外，尽管前述的描述和相关联的附图在元件和/或功能的某些示例组合的背景中描述了示例实施例，但是应当认识到，不偏离所附权利要求的范围，备选的实施例可以提供元件和/或功能的不同组合。在这个方面，例如，与上面明确描述的那些组合不同的元件和/或功能的组合也被考虑为可以在所附权利要求中的一些权利要求中阐述。尽管本文采用了特定的术语，但是它们仅在一般性和描述性的意义上被使用，并且不用于限制的目的。

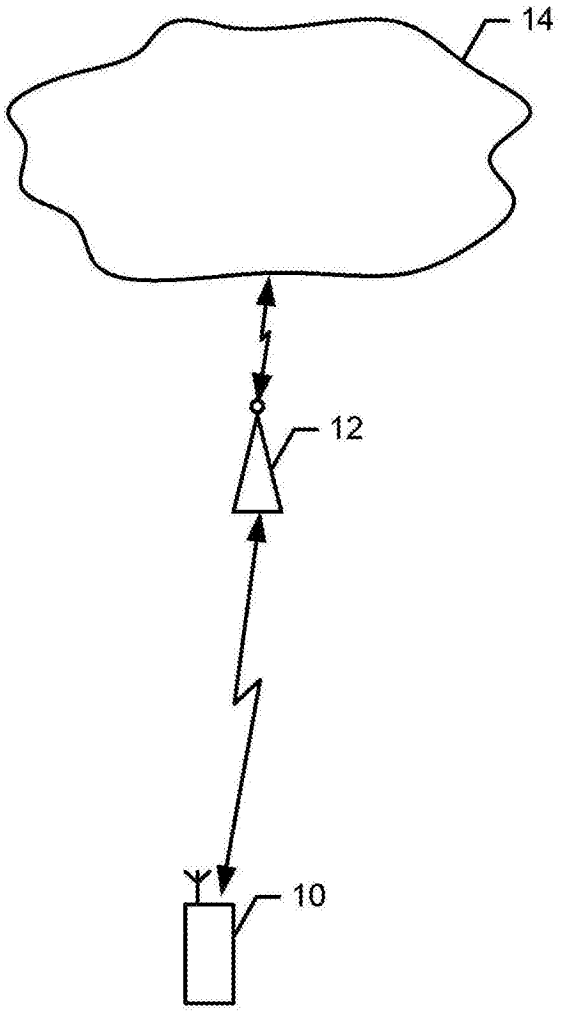


图1

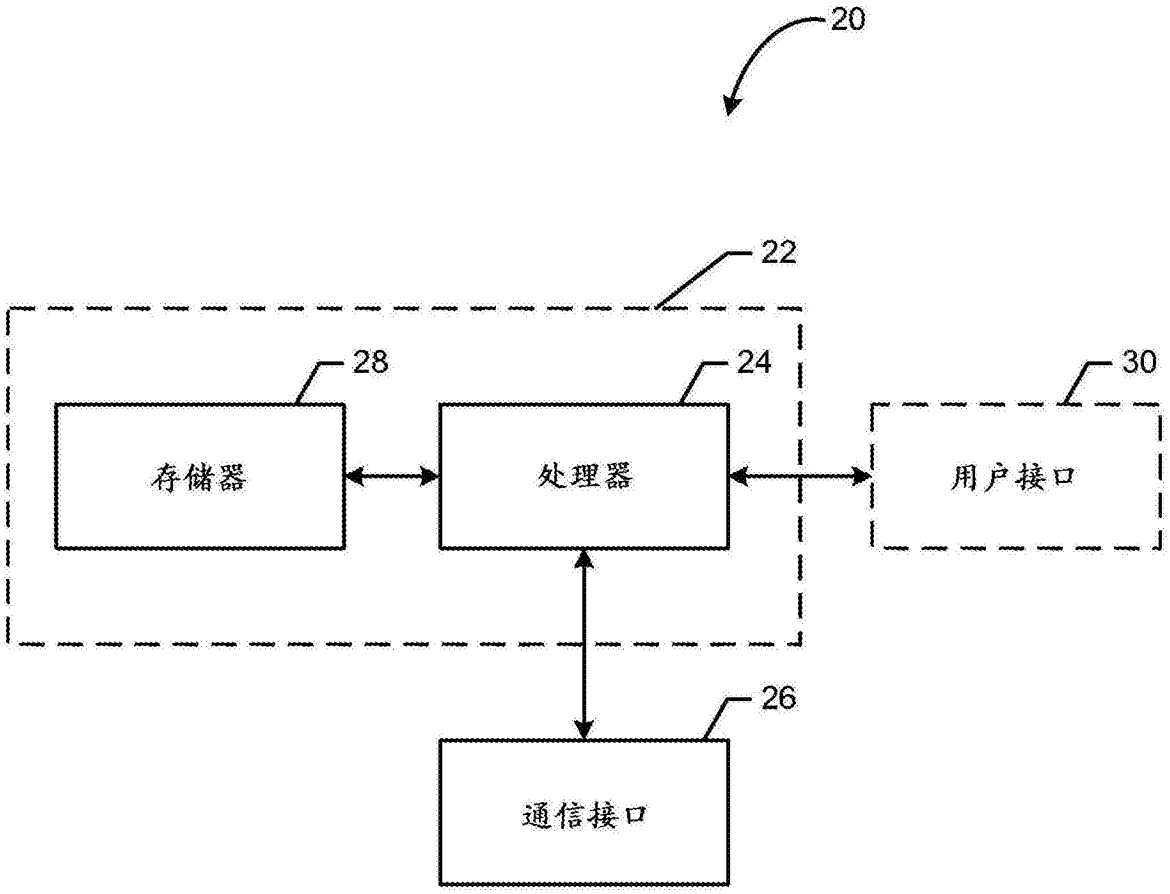


图2

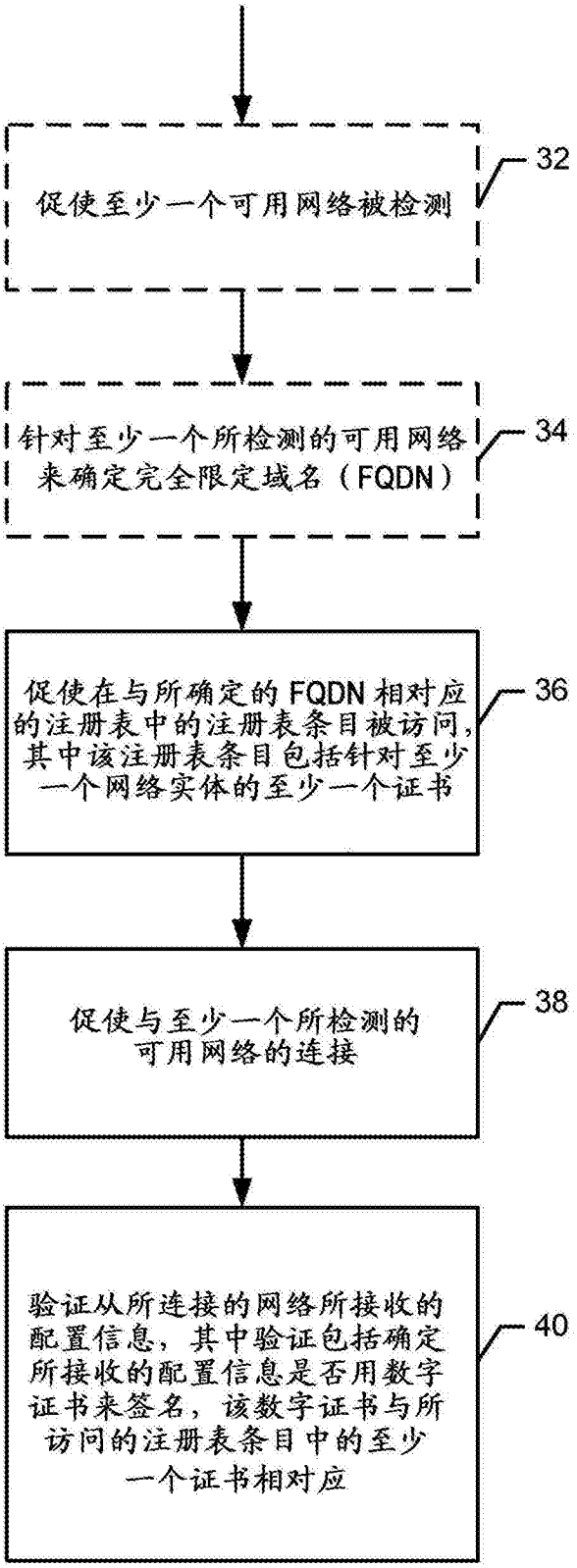

促使至少一个可用网络被检测
32
针对至少一个所检测的可用网络来确定完全限定域名（FQDN）
34
促使在与所确定的 FQDN 相对应的注册表中的注册表条目被访问，其中该注册表条目包括针对至少一个网络实体的至少一个证书
36
促使与至少一个所检测的可用网络的连接
38
验证从所连接的网络所接收的配置信息，其中验证包括确定所接收的配置信息是否用数字证书来签名，该数字证书与所访问的注册表条目中的至少一个证书相对应
40

图3