(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 103621127 B
(45)授权公告日 2019.04.19

(21)申请号 201280029895.0

(22)申请日 2012.05.03

(65)同一申请的已公布的文献号
申请公布号 CN 103621127 A

(43)申请公布日 2014.03.05

(30)优先权数据
61/482,520 2011.05.04 US

(85)PCT国际申请进入国家阶段日
2013.12.17

(86)PCT国际申请的申请数据
PCT/US2012/036236 2012.05.03

(87)PCT国际申请的公布数据
WO2012/151351 EN 2012.11.08

(73)专利权人 马维尔国际贸易有限公司
地址 巴巴多斯圣米加勒

(72)发明人 P·A·兰伯特

(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)

(56)对比文件
US 2009/0217043 A1,2009.08.27,

审查员 邱德洁

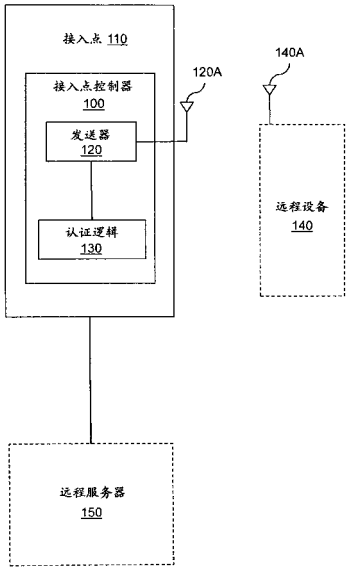
权利要求书2页 说明书8页 附图6页

(54)发明名称

用于无线认证的接入点控制器、方法及集成电路

(57)摘要

描述与使用信标消息的无线认证关联的系统、方法和其它实施例。根据一个实施例，一种接入点控制器包括被配置用于无线地发送信标消息的发送器。信标消息被配置用于向远程设备通报无线接入点可用于提供对网络的接入。信标消息包括标识用于无线接入点的公共密钥的安全标识符。



CN 103621127 B

1.一种接入点控制器,包括:

硬件逻辑,被配置为生成信标消息,在所述信标消息的计数器模式密码块链消息认证码协议(CCMP)报头中具有安全标识符;

发送器,被配置用于无线地发送所述信标消息,其中所述信标消息被配置用于向远程设备通报无线接入点可用于提供对网络的接入,并且其中所述信标消息包括标识用于所述无线接入点的公共密钥的安全标识符;以及

其中所述信标消息中的所述安全标识符被配置用于使得所述远程设备:

从第三方获得所述公共密钥,其中当所述远程设备从所述第三方获取所述公共密钥时,所述安全标识符和所述无线接入点的地址将所述无线接入点与所述公共密钥相关联;以及

通过使所述远程设备向所述无线接入点发送包括所述远程设备的用于认证交换的安全证书的回复来使所述远程设备发起与所述无线接入点的所述认证交换。

2.根据权利要求1所述的接入点控制器,包括:

认证单元,被配置用于确定从所述远程设备接收的响应于所述信标消息的所述回复是否包括用于完成与所述远程设备的所述认证交换的所述安全证书。

3.根据权利要求2所述的接入点控制器,其中所述认证单元被配置用于使用所述安全证书以确定用于与所述远程设备进行通信的加密密钥。

4.根据权利要求2所述的接入点控制器,其中所述认证单元被配置用于通过确定所述远程设备的加密随机数是否至少部分地基于用于所述无线接入点的所述公共密钥而被加密来确定所述回复是否包括所述安全证书,并且

其中所述回复是从所述远程设备向所述无线接入点发送的初始消息,而不存在居间消息。

5.根据权利要求1所述的接入点控制器,其中所述信标消息中的所述安全标识符被配置用于使所述远程设备通过使用所述无线接入点的所述公共密钥和来自所述信标消息的第一加密密文来认证所述无线接入点,并且其中所述信标消息使所述远程设备向所述无线接入点提供回复。

6.根据权利要求5所述的接入点控制器,其中所述信标消息被配置用于通过在所述远程设备中发起认证过程来使所述远程设备向所述无线接入点提供所述回复,并且其中所述回复包括完成所述无线接入点与所述远程设备之间的安全交换的第二加密密文。

7.根据权利要求1所述的接入点控制器,其中所述安全标识符是所述公共密钥的散列、所述公共密钥的标识符或者包括所述公共密钥的所述无线接入点的证书。

8.一种无线通信方法,包括:

生成信标消息,其中所述信标消息包括标识用于无线接入点的公共密钥的安全标识符,其中所述生成信标消息包括:将所述安全标识符包括在所述信标消息的计数器模式密码块链消息认证码协议报头中;

无线地发送所述信标消息以向远程设备通报所述无线接入点可用于提供网络接入;以及

使得所述远程设备:

从第三方获得所述公共密钥,其中当所述远程设备从所述第三方获取所述公共密钥

时，所述安全标识符和所述无线接入点的地址将所述无线接入点与所述无线接入点的所述公共密钥相关联；以及

通过在所述信标消息中发送所述安全标识符使所述远程设备发起与所述无线接入点的认证交换，其中从所述远程设备接收响应于所述信标消息的回复完成所述认证交换。

9.根据权利要求8所述的方法，包括：

确定从所述远程设备接收的响应于所述信标消息所述回复是否包括安全信息；以及

使用来自所述回复的所述安全信息来认证所述远程设备，其中所述安全信息完成加密密钥在所述远程设备与所述无线接入点之间的安全交换。

10.根据权利要求9所述的方法，还包括：

确定所述回复是否包括至少部分地基于用于所述无线接入点的所述公共密钥而被加密的所述远程设备的加密随机数，其中所述回复是来自所述远程设备、去往所述无线接入点的初始消息。

11.根据权利要求8所述的方法，其中所述信标消息中的所述安全标识符使所述远程设备使用所述无线接入点的所述公共密钥和来自所述信标消息的第一加密随机数来认证所述无线接入点，其中所述信标消息通过在所述远程设备中发起所述认证交换来使所述远程设备向所述无线接入点提供回复，并且其中所述回复包括完成所述无线接入点与所述远程设备之间的安全交换的第二加密随机数。

12.一种用于无线通信的集成电路，包括：

发送器，被配置用于无线地发送信标消息，其中所述信标消息被配置用于向远程设备通报无线接入点可用于提供对网络的接入，并且其中所述信标消息包括标识用于所述无线接入点的公共密钥的安全标识符，其中所述发送器被配置用于修改所述信标消息以在所述信标消息的计数器模式密码块链消息认证码协议报头中包括所述安全标识符；以及

其中所述信标消息中的所述安全标识符被配置用于通过使所述远程设备执行以下操作来：

从第三方获得所述公共密钥，其中当所述远程设备从所述第三方获取所述公共密钥时，所述安全标识符和所述无线接入点的地址将所述无线接入点与所述公共密钥相关联；以及

通过使得所述远程设备向所述无线接入点发送包括所述远程设备的安全证书的回复来发起与所述无线接入点的认证交换。

13.根据权利要求12所述的集成电路，还包括认证单元，所述认证单元被配置用于确定从所述远程设备接收响应于所述信标消息的所述回复是否包括完成与所述远程设备的所述认证交换的安全证书，其中所述认证单元被配置用于使用所述安全证书以确定用于与所述远程设备进行通信的加密密钥。

14.根据权利要求13所述的集成电路，其中所述认证单元被配置用于通过确定所述远程设备的加密随机数是否至少部分地基于用于所述无线接入点的所述公共密钥而被加密来确定所述回复是否包括所述安全证书，并且

其中所述回复是从所述远程设备向所述无线接入点发送的初始消息，而不存在居间消息。

用于无线认证的接入点控制器、方法及集成电路

[0001] 有关申请的交叉引用

[0002] 本专利公开内容要求于2011年5月4日提交的第61/482,520号美国临时申请的权益,其通过引用的方式全部并入于此。

背景技术

[0003] 这里提供的背景技术描述是为了一般性地呈现公开内容的背景的目的。当前发明人的工作(到在此背景技术部分描述的工作的程度)以及在提交时可能无法以其他方式作为现有技术衡量的本描述的诸多方面,既不被明确地也不被暗含地承认为本公开内容的现有技术。

[0004] 无线网络提供一种用于设备接入计算机网络的便利方式。许多不同设备的接入和从许多不同位置的接入在繁琐布线被无线连接能力取代时变得简单。然而随着无线网络的普及性增长,这一通信形式特有的安全问题最可能被利用。

[0005] 无线接入点(WAP)是允许无线设备连接到有线计算机网络的设备。无线通信呈现许多安全难题。例如无线接入点与无线客户端设备之间的通信易遭受恶意用户的窃听和攻击。为了提供防范这些威胁的安全性,设备通常加密无线通信。然而使用加密保护安全网络并非没有难题。定义无线接入点和客户端如何交互的协议不断改变并且经常配置起来困难和耗时。

[0006] 信息技术专业人员或者其他技术人员经常配置设备以用于无线接入。基本配置过程可以包括人工录入数据并且在设备之间交换配置信息。此外,一旦基本配置完成,设备的认证和连接可能由于在设备与无线接入点之间的通信多样性而缓慢。因而,连接到无线网络的方法可能是低效的。

发明内容

[0007] 在一个实施例中,一种接入点控制器包括被配置用于无线地发送信标消息的发送器。发送器被配置用于修改信标消息以包括安全标识符。信标消息包括标识用于无线接入点的公共密钥的安全标识符。信标消息被配置用于向远程设备通报无线接入点可用于提供对网络的接入。信标消息中的安全标识符被配置用于通过使远程设备向无线接入点发送包括远程设备的安全证书的回复来使远程设备发起与无线接入点的认证交换。

[0008] 在另一实施例中,信标消息中的安全标识符被配置用于使远程设备通过使用无线接入点的公共密钥和来自信标消息的第一加密密文(cryptographic secret)来认证无线接入点。信标消息被配置用于通过在远程设备中发起认证过程来使远程设备向无线接入点提供回复。回复是从远程设备向无线接入点发送的初始消息而无居间消息。在另一实施例中,回复包括完成在无线接入点与远程设备之间的安全交换的第二加密密文。在另一实施例中,安全标识符是无线接入点的公共密钥、公共密钥的散列(hash)、公共密钥的标识符或者包括公共密钥的无线接入点的证书。

[0009] 在另一实施例中,接入点控制器也包括认证逻辑。认证逻辑被配置用于确定从远

程设备接收的响应于信标消息的回复是否包括完成与远程设备的认证交换的安全信息。在另一实施例中，认证逻辑被配置用于使用安全信息以确定用于与远程设备进行通信的加密密钥。在另一实施例中，认证逻辑被配置用于通过确定远程设备的加密随机数(cryptographic nonce)是否至少部分地基于用于无线接入点的公共密钥而被加密来确定回复是否包括安全信息。

[0010] 在另一实施例中，一种方法包括生成信标消息。信标消息包括标识用于无线接入点的公共密钥的安全标识符。该方法也包括无线地发送信标消息以向远程设备通报无线接入点可用于提供网络接入。

[0011] 在另一实施例中，该方法通过在信标消息中发送安全标识符使远程设备发起与无线接入点的认证交换。从远程设备接收响应于信标消息的回复完成认证交换。

[0012] 在另一实施例中，该方法也包括确定从远程设备接收的响应于信标消息的回复是否包括安全信息。该方法包括使用来自回复的安全信息来认证远程设备。接收安全信息完成在远程设备与无线接入点之间的加密密钥的安全交换。

[0013] 在另一实施例中，该方法包括确定回复是否包括至少部分地基于用于无线接入点的公共密钥而被加密的远程设备的加密随机数。回复是来自远程设备、去往无线接入点的初始消息。

[0014] 在一个实施例中，信标消息中的安全标识符使远程设备使用无线接入点的公共密钥和来自信标消息的第一加密随机数来认证无线接入点。信标消息通过在远程设备中发起认证过程来使远程设备向无线接入点提供回复。回复包括完成无线接入点与远程设备之间的安全交换的第二加密随机数。

[0015] 在一个实施例中，一种集成电路包括被配置用于无线地发送信标消息的发送器。信标消息被配置用于向远程设备通报无线接入点可用于提供对网络的接入。信标消息包括标识用于无线接入点的公共密钥的安全标识符。信标消息中的安全标识符被配置用于通过使远程设备向无线接入点发送包括远程设备的安全证书的回复来使远程设备发起与无线接入点的认证交换。

[0016] 在另一实施例中，集成电路也包括被配置用于确定从远程设备接收的响应于信标消息的回复是否包括完成与远程设备的认证交换的安全信息的认证逻辑。在另一实施例中，认证逻辑被配置用于使用安全信息以确定用于与远程设备进行通信的加密密钥。认证逻辑被配置用于通过确定远程设备的加密随机数是否至少部分地基于用于无线接入点的公共密钥而被加密来确定回复是否包括安全信息。回复是从远程设备向无线接入点发送的初始消息，而不存在居间消息。

附图说明

[0017] 并入于说明书中并且构成说明书的部分的附图图示公开内容中的各种系统、方法和其它实施例。图中的所示单元边界(例如框、框组或者其它形状)代表边界的一个例子。在一些例子中，一个单元可以被设计为多个单元或者多个单元可以被设计为一个单元。在一些例子中，被示为另一单元的内部部件的单元以被实现为外部部件，并且反之亦然。另外，单元可以未按比例绘制。

[0018] 图1图示与使用信标消息的无线认证关联的接入点控制器的一个实施例。

[0019] 图2图示与使用信标消息的无线认证关联的方法的一个实施例。

[0020] 图3图示用于在无线认证交换中发送的消息的时序图的一个示例。

[0021] 图4图示用于在无线认证交换中发送的消息的时序图的另一示例。

[0022] 图5图示与无线认证关联的信标消息的一个实施例。

[0023] 图6图示与使用信标消息的无线认证关联的集成电路的一个实施例。

具体实施方式

[0024] 这里描述与使用信标消息的高效无线认证关联的示例方法、装置和其它实施例。例如无线接入点可以使用信标消息以向在无线接入点附近的远程设备通报无线接入点存在和可用。信标消息可以包括关于远程设备在连接到由无线接入点提供的无线网络时使用的该无线接入点的配置的信息。在一个实施例中，信标消息被配置用于通过在信标消息中包括安全信息来发起与远程设备的认证交换。以这一方式，附加信息被包括在信标消息中，并且无线接入点与远程设备之间交换的消息数目可以得以减少。作为以这一方式使用信标消息的结果，建立与无线接入点的连接可以在更少时间内发生。

[0025] 在一个实施例中，在信标消息中包括用于无线接入点的公共密钥。远程设备在接收到信标消息之后确定公共密钥存在，并且然后可以立即使用公共密钥来加密发送回无线接入点的回复。因此，在信标消息中包括公共密钥可以允许远程设备安全地与无线接入点进行通信而不交换多个不安全消息集合、因此更高效地传达信息以建立可信的安全连接。

[0026] 参照图1，示出与使用信标消息的高效无线认证关联的接入点控制器100的一个实施例。在以下示例中，考虑接入点控制器100是接入点110的部分并且接入点110为在接入点110的传输覆盖区(footprint)中存在的远程设备提供向计算机网络(例如远程服务器150)的接入。接入点控制器100至少包括用于控制经由天线120A的无线传输的发送器120和以下描述的用于认证远程设备的认证逻辑130。

[0027] 在附近远程设备(例如远程设备140)初始地进入接入点1 10的覆盖区(例如发送范围)时，远程设备未连接到无线网络并且并未得知接入点110的配置。为了让附近设备知道接入点110存在，接入点控制器100例如使发送器120经由天线120A(可以在内部和/或芯片的部分)通过无线网络发送信标消息。以这一方式，接入点110使用信标消息以通报无线网络的可用性并且向远程设备140提供用于通过接入点110连接到无线网络的发现信息。在一个实施例中，发现信息概括接入点100的配置和能力。

[0028] 在远程设备140在传输范围内时，远程设备140经由天线140A接收信标消息并且在尝试建立与接入点110的连接时使用发现信息以配置回复。与发现信息一起，接入点控制器100在信标消息中插入(一个或多个)安全标识符。

[0029] 通过在信标消息中包括安全标识符，信标消息使远程设备140在交换任何附加消息之前发起与接入点110的认证交换。以这一方式，接入点110可以避免例如在信标消息中未包括安全标识符则为了交换它而将出现的交换居间通信。因此，向信标消息添加安全标识符可以减少用于认证远程设备140并且建立与远程设备140的连接的时间，因为可以交换更少消息。

[0030] 在一个实施例中，发送器120被配置用于修改信标消息以包括安全标识符，或者发送器120可以重新设计信标消息中的现有字段以包括安全标识符。以这一方式，由安全标识

符体现的附加信息在向远程设备140发送时被包括在信标消息中。例如，远程设备140在回复信标消息时使用安全标识符。考虑到安全标识符可以向远程设备140提供信标消息原本不可用的附加信息。附加信息可以包括没有在接入点110与远程设备140之间的若干居间请求和回复就原本不会交换的信息。

[0031] 在一个实施例中，信标消息中的安全标识符是用于接入点110的公用/私用不对称密钥对的公共密钥。具有公共密钥允许远程设备140紧接在接收信标消息之后保护与接入点110的通信。因此，远程设备140可以使用来自信标消息的公共密钥来加密向接入点110发送的回复中的敏感信息而无需交换附加消息以获得公共密钥。另外，使用接入点110的公共密钥，远程设备140可以向接入点110发送敏感信息，该敏感信息可以用来根据信标消息直接构造安全共享密文并且在通信序列中及早防止窃听或者其它恶意入侵。

[0032] 用公共密钥修改的信标消息可以用于其它功能。在一个实施例中，远程设备140可以使用来自信标消息的公共密钥以在回复信标消息之前认证接入点110。以这一方式，远程设备140可以保证接入点110被信任而不是恶意设备(例如入侵者、诈骗者)。在认证接入点110时，远程设备140可以使用接入点110的公共密钥以解密信标消息中的消息认证码(MAC)、向第三方设备(例如远程服务器150)提供安全标识符用于验证、比对内部信任列表认证安全标识符等等。

[0033] 在其它实施例中，取代包含实际公共密钥，信标消息中的安全标识符可以是公共密钥的散列、公共密钥的标识符、接入点110的包括公共密钥的证书、从其取回公共密钥的位置等等。在安全标识符未包括公共密钥而代之以包括公共密钥的标识符时，远程设备140可以请求来自可以适当处理安全标识符的第三方服务器(例如远程服务器150)或者其它认证设备或者服务的公共密钥。因此，在一个实施例中，通过要求使用安全标识符从可信源取回公共密钥来向过程中集成附加安全性。因而，通过在信标消息中提供安全标识符，接入点110提供用于在设备之间高效建立安全通信和/或可信关系的健壮机制。

[0034] 在一个实施例中，由于远程设备140可以根据信标消息中的信息认证接入点110，所以远程设备140可以响应于信标消息而生成回复，这完成在接入点110与远程设备140之间的认证交换。认证交换例如是交换用于构造共享秘密密钥的密码信息、相互认证握手等等。例如，如果在从远程设备140接收回复时已经交换用于构造共享秘密密钥的信息，则认证交换完成。

[0035] 在接入点110接收回复时，认证逻辑130处理回复以确定回复是否为正确形式并且包括用于完成认证交换的某些信息(例如加密密钥信息)。例如认证逻辑130可以通过确定回复或者回复的部分是否用来自接入点110的公共密钥(将已经是信标消息的部分)而被加密来确定回复是否包括安全信息。在一个示例中，如果用公共密钥加密回复，则认证逻辑130将能够用密钥对的对应私用部分解密回复以揭示加密的信息。如果解密失败，则认证逻辑130知道加密未使用来自接入点110的公共密钥并且认证过程终止和/或不安全交换可能开始。

[0036] 如果解密成功，则在一个实施例中，认证逻辑130使用解密的信息以构造用于与远程设备140安全通信的共享对称加密密钥。此外，认证逻辑130可以认证远程设备140为可信的设备。为了认证远程设备140，认证逻辑130可以向执行认证、比较安全信息与已认证设备数据库等等的远程服务器150提供安全信息。在一个示例中，远程服务器150是为网络中的

计算机提供集中认证、授权和记账管理的远程认证拨号用户服务(RADIUS)服务器。

[0037] 在一个实施例中,回复中的安全信息可以例如是远程设备140的公共密钥、远程设备140的安全证书如可信的证书、用于安全密钥协商的加密随机数等等。例如考虑认证交换可以包括交换用于构造秘密对称密钥的安全信息。在一个实施例中,接入点110和远程设备140使用秘密对称密钥以加密并且由此保护通信以防被窃听和其它有害入侵。秘密对称密钥可以是按组瞬态密钥(GTK)或者为了维持密钥的完整性而保持私用的其它对称密钥。因此,信标消息可以包括在构造这样的密钥时使用的第一加密密文(例如第一加密随机数)。

[0038] 此外,来自远程设备140的回复可以包括用于构造秘密对称密钥的第二加密密文(例如第二加密随机数)。在认证交换期间在远程设备140与接入点110之间交换的数据可以是符合Diffie-Helman密钥交换、可扩展认证协议(EAP)、IEEE 802.1X、IEEE 802.11i、IEEE 802.11ai、WiFi保护的接入(WPA)、WPA2(例如WPA2 4路握手)、健壮安全网络(RSN)协议等等的数据。因而,一旦远程设备140响应于信标消息而提供回复,如果回复包括正确信息,则认证交换有效地完成。

[0039] 将结合图2讨论认证交换和使用信标消息以传达安全标识符的更多细节。图2图示与使用信标消息的高效无线认证关联的方法200。从方法200由无线接入点(例如接入点110)实施和执行以通过无线网络建立与远程设备(例如远程设备140)的安全连接这样的视角讨论图2。应当理解方法200可以支持并行地与在接入点的覆盖区内的多个远程设备的交换。提供以下关于单个远程设备的讨论作为示例。

[0040] 在方法200的210处,接入点生成信标消息。在一个实施例中,为了生成信标消息,接入点可以通过添加附加字段或者通过重新指派现有字段以包括安全标识符来修改标准信标消息(例如IEEE802.11信标帧)。根据接入点实施的用于认证远程设备的协议,安全标识符可以是用于无线接入点的公用/私用密钥对的公共密钥的标识符、公共密钥本身和/或其它安全信息。

[0041] 在220处,接入点无线地发送信标消息。在一个实施例中,无线地发送信标消息包括发送信标消息为广播或者多播传输以便向在接入点的附近的远程设备(例如远程设备140)提供信标消息。如先前说明的那样,信标消息向监听并且能够建立与无线网络的连接的远程设备通报接入点的存在和可用。以这一方式,信标消息可以传达远程设备在尝试建立与接入点的连接时使用的发现消息。

[0042] 在一个实施例中,通过在信标消息中提供安全标识符,接入点可以引起远程设备发起与接入点的认证交换。然而在一个实施例中,为了远程设备发起认证交换,远程设备先需要识别信标消息包括安全标识符。因而,远程设备可以被配置用于处理信标消息并且在回复信标消息之前校验安全标识符。以这一方式,远程设备可以认证接入点和/或在对信标消息的回复中提供安全信息以完成认证交换。

[0043] 例如在远程设备被配置用于参与高效认证交换时,来自远程设备的响应于信标消息(包括安全标识符)的回复将包括安全信息。接入点然后使用安全信息(例如远程设备的安全证书、加密密文)以认证远程设备和/或构造共享秘密密钥。秘密密钥例如是可以在构造加密密钥时使用的伪随机数、随机数或者其它信息。

[0044] 在方法200的230处,接入点从远程设备接收对信标消息的回复。在一个实施例中,在接收回复时,接入点尚未知远程设备是否已经基于来自信标消息的安全标识符而发起认

证交换。然而在240处，该方法确定回复是否包括指示认证交换的安全信息或者例如回复是否包括如下信息，该信息指示远程设备正在请求根据次级策略连接。

[0045] 在一个实施例中，在240处，接入点通过使用用于接入点的公用/私用密钥对的私用密钥解密回复的部分(例如有效载荷)来确定回复是否包括安全信息。备选地，回复可以包括指示是否包括安全信息的字段。在240处如果回复包括安全信息，则接入点进行至250，其中接入点尝试认证远程设备。如果认证远程设备，则方法200进行至260，其中建立并且完成连接。因此，如果远程设备用正确安全信息回复，则可以仅需在接入点与远程设备之间交换两个消息以完成认证交换。将参照图3讨论通信交换的序列的示例。

[0046] 参照图3，图示通信序列300。序列300是在接入点110与远程设备140之间的传输交换。在序列300中，接入点110发送包括如先前讨论的安全标识符的信标消息310。这里，远程设备140被配置用于在接收具有安全标识符的信标消息时发起认证序列。因此，认证交换通过远程设备140使用在来自信标消息310的安全标识符中包括的信息认证接入点110来在远程设备中开始。

[0047] 在远程设备140认证接入点110之后，构造回复320以包括远程设备140的安全证书。安全证书例如用于接入点110在认证远程设备140时使用和/或用于构造共享密文。远程设备140然后可以加密回复320或者回复320的部分(例如有效载荷)以掩盖所包括的安全信息。远程设备然后向接入点110发送回复320以完成认证交换。如序列300中所示，可以在设备之间发送具有可选第三消息的两个消息以共享秘密密钥并且相互认证，该第三消息是认证交换的完成确认330。

[0048] 对照而言，如果对信标消息的回复不是以适当形式(例如未包括安全证书)，则如图4的序列400中所示备选次级交换可能出现。

[0049] 图4图示如下示例，在该示例中，远程设备140未被配置用于参与高效认证交换或者另外选择未参与高效交换。在任一情况下，跟随的消息系列更复杂并且可能消耗比如图3中所示序列300更多的时间。例如序列400始于可以包括安全标识符的信标消息410以在远程设备140中发起认证交换。

[0050] 然而在序列400中，远程设备140例如用未包括安全信息和/或未恰当加密的认证请求420回复。因此，接入点110确定(例如在图2中的方法200的240)安全信息不存在并且继续发送指示可用认证方法的回复430。通过向远程设备140发送消息430，设备可以发现并且协商两个设备支持的协议。然而回复430已经代表在设备之间的交换复杂性增加。例如回复430比图3的序列300中的交换超过一个消息。此外，在发送回复430时，设备尚未完成协商待使用的公共协议，而序列300在这一传输次数完成。序列400中的其余传输(例如440、450、460、470)图示可以出现的消息序列的一个示例，该消息序列用于建立与在序列300中实现的连接相似的连接而传输比序列300更多，因为在序列400中未使用信标消息中的安全标识符。传输440、450、460、470代表公共认证过程并且这里将不具体加以讨论。提供它们仅为了与图2和3的过程和序列比较来示范它们的相对复杂性和消息数目。

[0051] 图5图示信标消息500的一个实施例，该信标消息包括无线接入点可以使用的如先前讨论的安全标识符。当然，不同协议可以具有不同信标消息配置，因此本系统和方法可以被相应地调整而不受所示示例限制。信标消息500可以包括字段序列。在一个示例中，字段序列包括介质访问控制(MAC)报头505、具有密码块链消息认证码的计数器模式协议(CCMP)

报头515、信标帧体525和帧校验序列(FCS)字段530。

[0052] MAC报头505包括一系列子字段(例如508、509、510等)。MAC报头505的子字段包括用来在网络中的节点之间发送分组的信息。应当理解在不同实施例中,MAC报头505可以包括如适合于实施并且如与实施的标准(例如IEEE 802.11-2007标准或者其它标准)兼容的更多或者更少字段。

[0053] MAC报头505子字段508-510可以是地址字段。例如地址字段508包括48位目的地MAC地址。地址字段509包括发送分组的AP的48位MAC地址。地址字段510是发起分组的设备的48位MAC地址。地址字段510指示分组的原有源。地址字段508、509和510指示参与发送和接收分组的设备的2层MAC地址。地址字段509例如指示广播目的地地址。以这一方式,向在无线接入点的传输范围内的远程设备传达信标消息500。

[0054] 在一个实施例中,CCMP报头515可以用来指示用来发起与远程设备的认证交换的安全标识符。CCMP报头515可以包括在六个分组编号字段516、517、520、521、522和523之间划分的48位分组编号。分组编号字段可以是用作安全标识符的一个要素。CCMP报头515也包括保留字段518和密钥ID字段519。密钥ID字段519和保留字段518也可以用于安全标识符。在其它实施例中,其它字段可以用于安全标识符,或者可以向信标消息添加附加字段以容纳安全标识符。

[0055] 在一个实施例中,密钥ID字段519与源地址和/或接入点地址组合用作安全标识符。例如密钥ID字段519和接入点源地址的组合可以用来向接入点绑定公共密钥。远程设备可以使用这一组合以验证可信接入点。应当理解在其它实施例中,CCMP报头515可以包括如适合于实施并且如与选择的标准(例如IEEE 802.11-2007标准或者其它实施的标准)兼容的更多或者更少字段。在一个实施例中,在信标消息中简单地包括CCMP报头可以服务于充当安全标识符。此外,在其它实施例中,在信标消息500中可以不包括CCMP报头。

[0056] 继续信标消息500,信标体525是信标消息500的包括发现信息的部分并且也可以包括安全标识符。FCS字段530包括用于保证信标消息500不包括任何错误的错误校验段。在一个实施例中,FCS530包括用于信标消息500的循环冗余校验(CRC)值。

[0057] 图6图示用单独集成电路和/或芯片配置的来自图1的接入点控制器100的一个附加实施例。在这一实施例中,体现来自图1的发送器120为单独集成电路610。此外,在单独的集成电路630上体现认证逻辑130。也在单独的集成电路620上体现天线120A。经由连接路径连接电路以传达信号。尽管图示集成电路610、620和630为单独集成电路,但是可以将它们集成到公共电路板600中。此外,可以将集成电路610、620和630集成为比所示电路更少的集成电路或者分成更多的集成电路。此外,在另一实施例中,可以将集成电路610和630中所示的发送器120和认证逻辑130组合成单独的专用集成电路。在其它实施例中,可以体现与发送器120和认证逻辑130关联的功能的部分为可由处理器执行并且存储在非瞬态存储器中的固件。

[0058] 下文包括这里运用的所选术语的定义。定义包括落入术语的范围内并且可以用于实施的部件的各种示例和/或形式。示例并非旨在于限制。术语的单数和复数形式二者可以在定义内。

[0059] 引用“一个实施例”、“实施例”、“一个示例”、“示例”等指示这样描述的实施例或者示例可以包括特定特征、结构、特性、性质、单元或者限制,但是并非每个实施例或者示例必

然包括该特定特征、结构、特性、性质、单元或者限制。另外，反复使用短语“在一个实施例中”虽然可以、但是未必指代相同实施例。

[0060] “逻辑”如这里所用包括但不限于用于执行功能或者动作和/或引起来自另一逻辑、方法和/或系统的功能或者动作的硬件、固件、在非瞬态介质上存储或者在机器上执行的指令和/或各项的组合。逻辑可以包括被编程用于执行公开的功能中的一个或者多个功能的微处理器、分立逻辑(例如ASIC)、模拟电路、数字电路、编程的逻辑器件、包含指令的存储器设备等。逻辑可以包括一个或者多个门、门组合或者其它电路部件。在描述多个逻辑时，可以有可能向一个物理逻辑中并入多个逻辑。类似地，在描述单个逻辑时，可以有可能使该单个逻辑分布在多个物理逻辑之间。可以使用逻辑单元中的一个或者多个逻辑单元来实施这里描述的部件和功能中的一个或者多个部件和功能。

[0061] 尽管出于说明简化的目的而示出和描述所示方法为一系列的块。但是方法不受块的顺序限制，因为一些块可以按与示出和描述的顺序不同的顺序和/或与其它块并行地出现。另外，可以使用比所有所示块少的块来实施示例方法。可以组合块或者将块分离成多个部件。另外，附加和/或备选方法可以运用附加的未图示的块。

[0062] 在具体实施方式或者权利要求中运用术语“包括(include)”的程度上，它旨在于以与术语“包括(comprise)”在该术语在运用时解释为权利要求中的过渡词时相似的方式有包含意义。

[0063] 尽管已经通过描述示例来举例说明示例系统、方法等并且尽管已经以相当多的细节描述示例，但是申请人的意图并非是约束或者以任何方式使所附权利要求的范围限于这样的细节。当然不可能出于描述这里描述的系统、方法等的目的而描述每个可设想的部件或者方法组合。因此，公开内容不限于示出和描述的具体细节、代表的装置和示例。因此，本申请旨在于涵盖落入所附权利要求的范围内的变更、修改和变化。

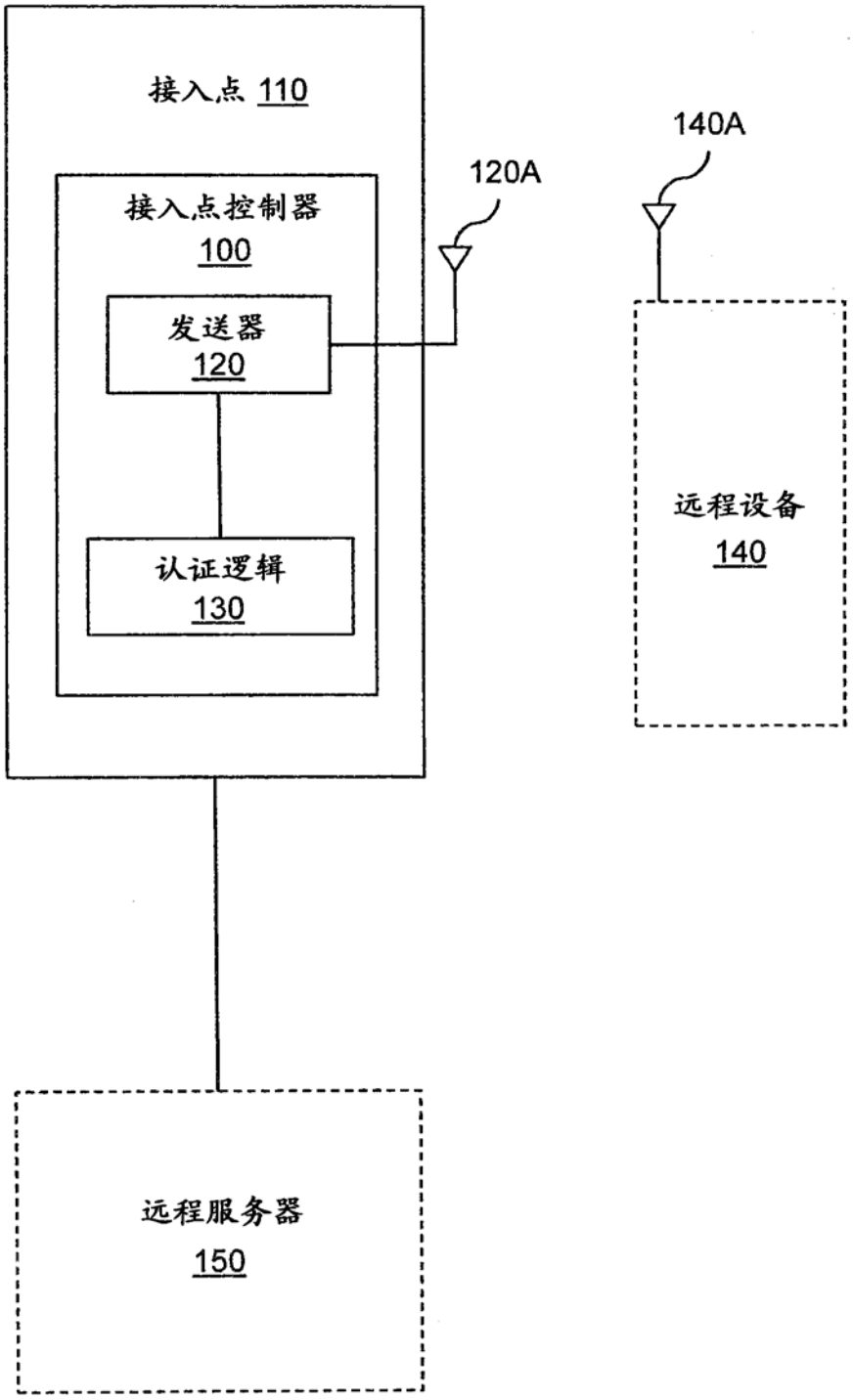

接入点 110
接入点控制器
100
发送器
120
认证逻辑
130
120A
140A
远程设备
140
远程服务器
150

图1

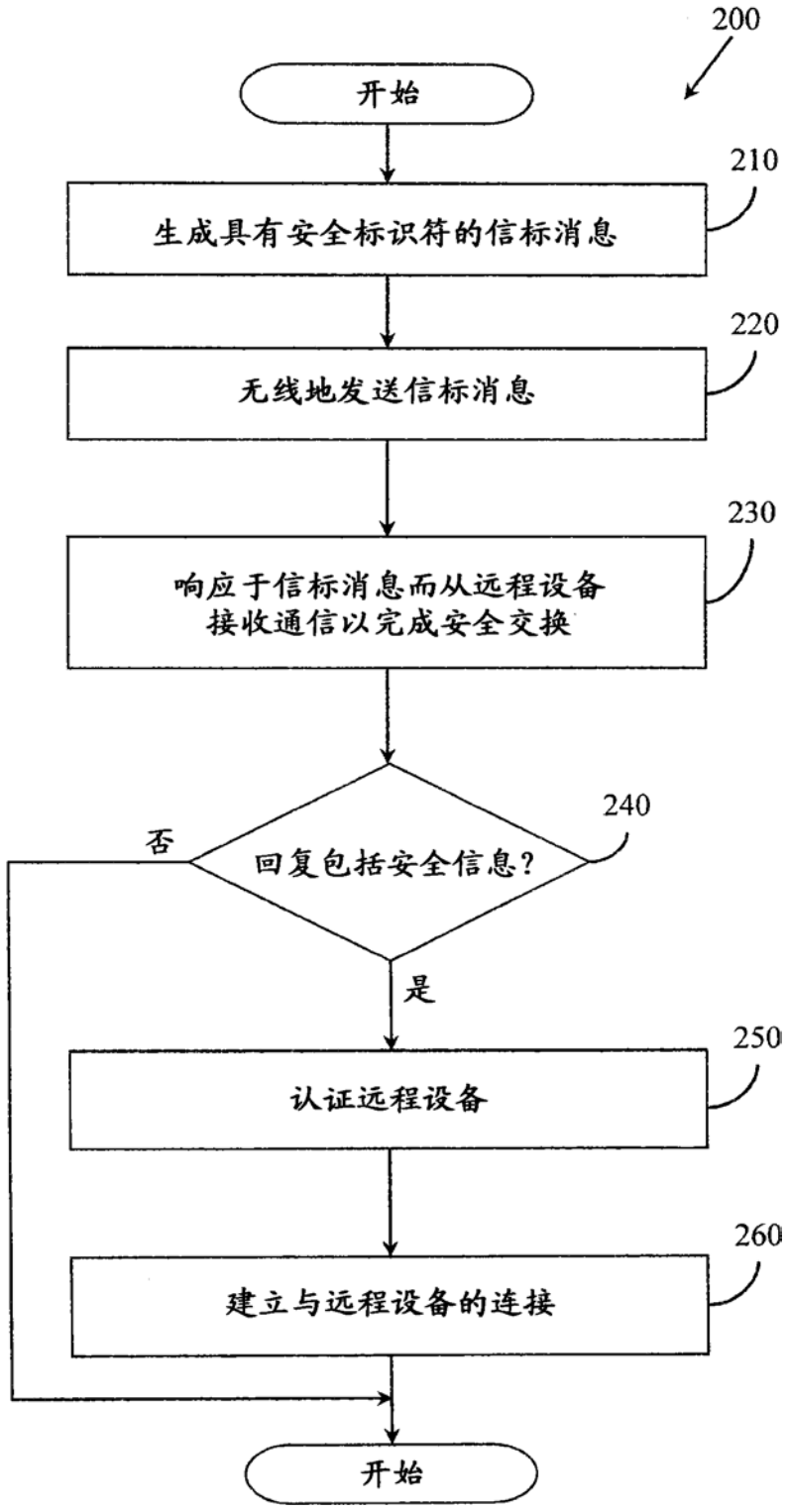

200
开始
210
生成具有安全标识符的信标消息
220
无线地发送信标消息
230
响应于信标消息而从远程设备
接收通信以完成安全交换
240
回复包括安全信息?
否
是
250
认证远程设备
260
建立与远程设备的连接
开始

图2

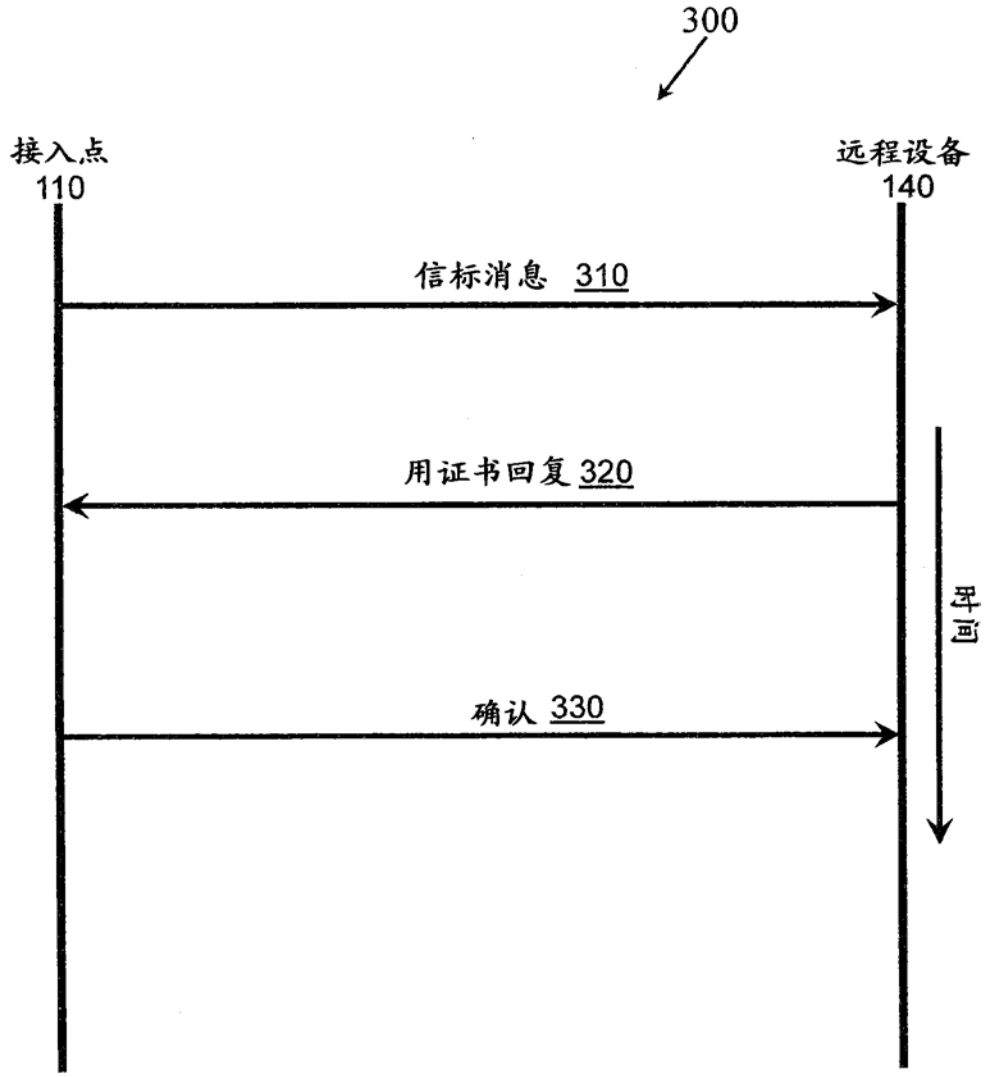


图3

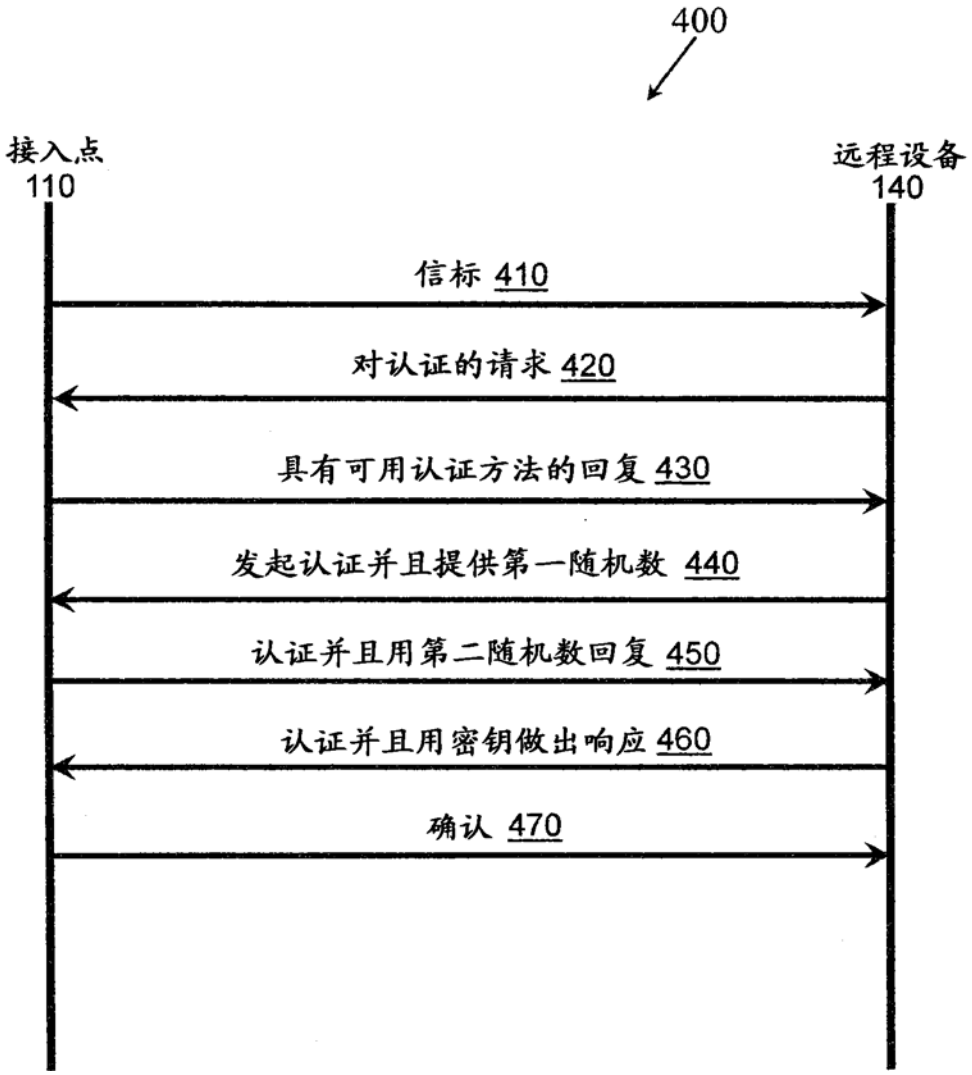

400
接入点
110
远程设备
140
信标 410
对认证的请求 420
具有可用认证方法的回复 430
发起认证并且提供第一随机数 440
认证并且用第二随机数回复 450
认证并且用密钥做出响应 460
确认 470

图4

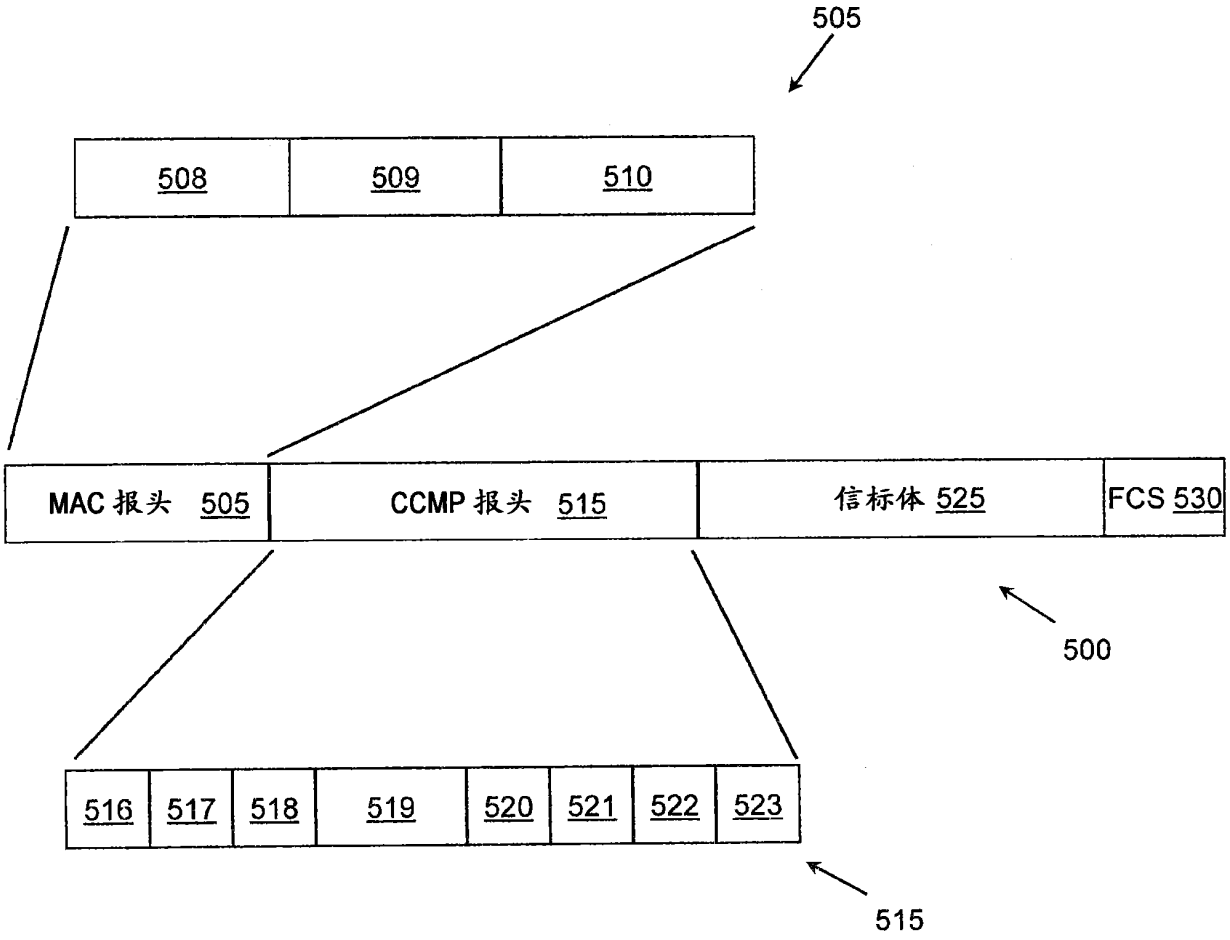

505
508
509
510
MAC 报头 505
CCMP 报头 515
信标体 525
FCS 530
500
516
517
518
519
520
521
522
523
515

图5

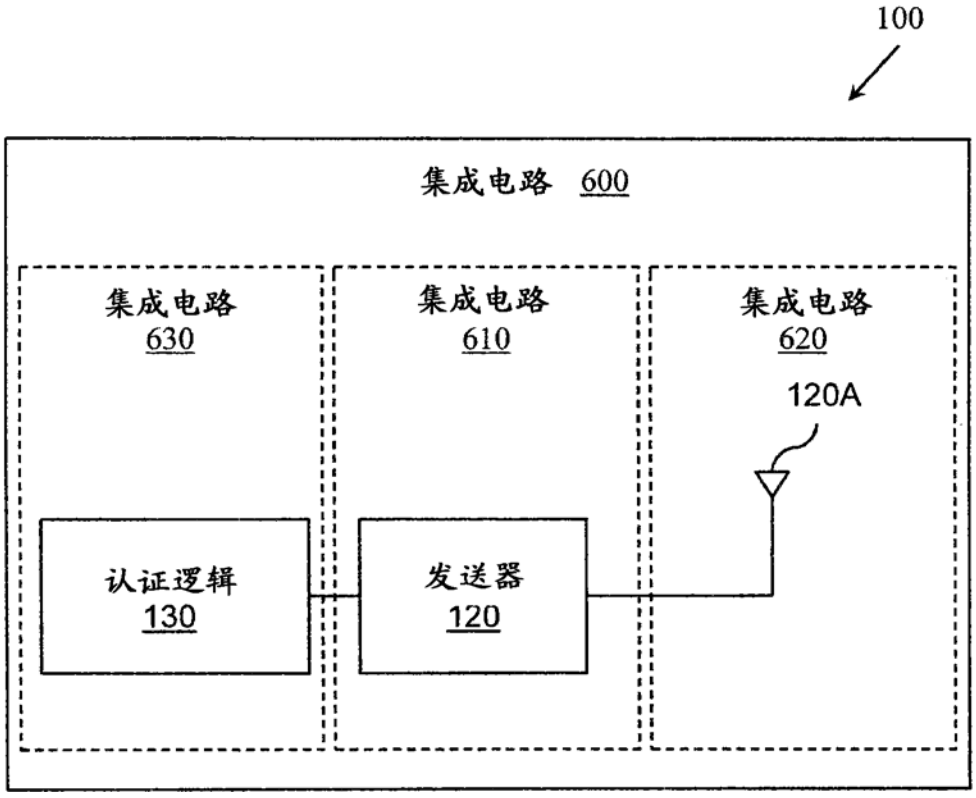


图6