(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105229966 A
(43)申请公布日 2016.01.06

(21)申请号 201480029713.9
(22)申请日 2014.05.23
(30)优先权数据
61/827,490 2013.05.24 US
14/284,785 2014.05.22 US
(85)PCT国际申请进入国家阶段日
2015.11.23
(86)PCT国际申请的申请数据
PCT/US2014/039301 2014.05.23
(87)PCT国际申请的公布数据
WO2014/190241 EN 2014.11.27
(71)申请人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 S·P·阿伯拉翰 G·切瑞安 J·马利宁
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 袁逸
(51)Int.Cl.
H04L 9/32(2006.01)

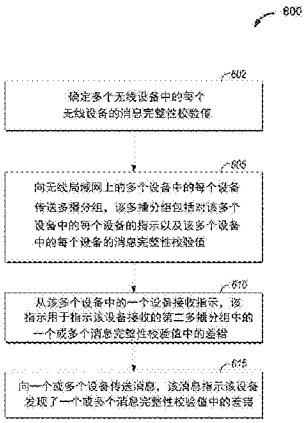
权利要求书3页 说明书11页 附图8页

(54)发明名称

用于具有消息认证的广播WLAN消息的系统和方法

(57)摘要

本文中包含用于具有消息认证的多播无线局域网消息的系统、方法和设备。该方法包括确定多个无线设备中的每一个无线设备的消息完整性校验值。该方法进一步包括向无线局域网上的多个设备中的每一个设备传送多播分组，该多播分组包括对该多个设备中的每个设备的指示以及该多个设备中的每个设备的消息完整性校验值。



CN 105229966 A

1. 一种无线通信的方法，包括：

确定多个无线设备中的每一个无线设备的消息完整性校验值；以及

向无线局域网上的多个设备中的每一个设备传送多播分组，所述多播分组包括对所述多个设备中的每一个设备的指示以及所述多个设备中的每一个设备的消息完整性校验值。

2. 如权利要求 1 所述的方法，其特征在于，对所述多个设备中的每一个设备的所述指示包括所述多个设备中的每一个设备的关联标识和媒体接入控制地址中的至少一者。

3. 如权利要求 1 所述的方法，其特征在于，确定所述消息完整性校验值包括基于以下一者或多者来确定消息完整性校验值：所述多播分组的帧报头、所述多播分组中的数据、对所述多个设备中的一个设备的指示、以及所述多播分组的计数器模式密码块链式消息认证码协议报头中的成对瞬态密钥和伪随机噪声序列号。

4. 如权利要求 1 所述的方法，其特征在于，所述多个无线设备中的每一个无线设备的消息完整性校验值包括少于 8 个八位位组的缩短消息完整性校验值。

5. 如权利要求 1 所述的方法，其特征在于，所述多播分组包括帧主体，所述多播分组的所述帧主体内包括数据长度字段。

6. 如权利要求 1 所述的方法，其特征在于，所述多播分组包括具有翻转的保留位或者翻转的保留位组合的计数器模式密码块链式消息认证码协议报头，所述翻转的保留位或翻转的保留位组合被配置成允许所述多个设备将所述多播分组识别为具有发送者认证的多播分组。

7. 如权利要求 1 所述的方法，其特征在于，进一步包括：

从所述多个设备中的至少一个设备接收指示，所述指示用于指示由所述设备接收到的第二多播分组中的一个或多个消息完整性校验值中的差错；以及

向一个或多个设备传送消息，所述消息指示所述至少一个设备发现了一个或多个消息完整性校验值中的差错。

8. 如权利要求 7 所述的方法，其特征在于，所述消息包括去往所述一个或多个设备以禁用所述网络中的多播分组服务的指令。

9. 如权利要求 7 所述的方法，其特征在于，所述消息包括去往所述一个或多个设备以更改所述一个或多个设备的单播密钥的指令。

10. 如权利要求 1 所述的方法，其特征在于，确定所述消息完整性校验值包括通过用群临时密钥加密所述多播分组中的数据来生成第一消息完整性校验值，以及随后基于所述第一消息完整性校验值确定多个无线设备中的每个无线设备的消息完整性校验值。

11. 一种无线通信装置，包括：

发射机，其配置成：

确定多个无线设备中的每一个无线设备的消息完整性校验值；以及

向无线局域网上的多个设备中的每一个设备传送多播分组，所述多播分组包括对所述多个设备中的每一个设备的指示以及所述多个设备中的每一个设备的消息完整性校验值。

12. 如权利要求 11 所述的装置，其特征在于，对所述多个设备中的每一个设备的所述指示包括所述多个设备中的每一个设备的关联标识和媒体接入控制地址中的至少一者。

13. 如权利要求 11 所述的装置，其特征在于，确定所述消息完整性校验值包括基于以下一者或多者来确定消息完整性校验值：所述多播分组的帧报头、所述多播分组中的数据、

对所述多个设备中的一个设备的指示、以及所述多播分组的计数器模式密码块链式消息认证码协议报头中的成对瞬态密钥和伪随机噪声序列号。

14. 如权利要求 11 所述的装置，其特征在于，所述多个无线设备中的每一个无线设备的消息完整性校验值包括少于 8 个八位位组的缩短消息完整性校验值。

15. 如权利要求 11 所述的装置，其特征在于，所述多播分组包括帧主体，所述多播分组的所述帧主体内包括数据长度字段。

16. 如权利要求 11 所述的装置，其特征在于，所述多播分组包括具有翻转的保留位或者翻转的保留位组合的计数器模式密码块链式消息认证码协议报头，所述翻转的保留位或翻转的保留位组合被配置成允许所述多个设备将所述多播分组识别为具有发送者认证的多播分组。

17. 如权利要求 11 所述的装置，其特征在于，进一步包括 ：

接收机，其配置成从所述多个设备中的至少一个设备接收指示，所述指示用于指示由所述设备接收到的第二多播分组中的一个或多个消息完整性校验值中的差错 ；以及

所述发射机进一步配置成向一个或多个设备传送消息，所述消息指示所述至少一个设备发现了一个或多个消息完整性校验值中的差错。

18. 如权利要求 17 所述的装置，其特征在于，所述消息包括去往所述一个或多个设备以禁用所述网络中的多播分组服务的指令。

19. 如权利要求 17 所述的装置，其特征在于，所述消息包括去往所述一个或多个设备以更改所述一个或多个设备的单播密钥的指令。

20. 如权利要求 11 所述的装置，其特征在于，确定所述消息完整性校验值包括通过用群临时密钥加密所述多播分组中的数据来生成第一消息完整性校验值，以及随后基于所述第一消息完整性校验值确定多个无线设备中的每个无线设备的消息完整性校验值。

21. 一种无线通信设备，包括 ：

用于确定多个无线设备中的每一个无线设备的消息完整性校验值的装置 ；以及

用于向无线局域网上的多个设备中的每一个设备传送多播分组的装置，所述多播分组包括对所述多个设备中的每一个设备的指示以及所述多个设备中的每一个设备的消息完整性校验值。

22. 如权利要求 21 所述的设备，其特征在于，所述用于确定所述消息完整性校验值的装置包括用于基于以下一者或多者来确定消息完整性校验值的装置 ：所述多播分组的帧报头、所述多播分组中的数据、对所述多个设备中的一个设备的指示、以及所述多播分组的计数器模式密码块链式消息认证码协议报头中的成对瞬态密钥和伪随机噪声序列号。

23. 如权利要求 21 所述的设备，其特征在于，所述多个无线设备中的每一个无线设备的消息完整性校验值包括少于 8 个八位位组的缩短消息完整性校验值。

24. 如权利要求 21 所述的设备，其特征在于，进一步包括 ：

用于从所述多个设备中的至少一个设备接收指示的装置，所述指示用于指示由所述设备接收到的第二多播分组中的一个或多个消息完整性校验值中的差错 ；以及

用于向一个或多个设备传送消息的装置，所述消息指示所述至少一个设备发现了一个或多个消息完整性校验值中的差错。

25. 如权利要求 24 所述的设备，其特征在于，所述消息包括去往所述一个或多个设备

以禁用所述网络中的多播分组服务或更改所述一个或多个设备的单播密钥的指令。

26. 一种包括指令的非瞬态计算机可读介质，所述指令在被执行时使得设备中的处理器执行一种无线通信的方法，所述方法包括：

确定多个无线设备中的每一个无线设备的消息完整性校验值；以及

向无线局域网上的多个设备中的每一个设备传送多播分组，所述多播分组包括对所述多个设备中的每一个设备的指示以及所述多个设备中的每一个设备的消息完整性校验值。

27. 如权利要求 26 所述的计算机可读介质，其特征在于，确定所述消息完整性校验值包括基于以下一者或多者来确定消息完整性校验值：所述多播分组的帧报头、所述多播分组中的数据、对所述多个设备中的一个设备的指示、以及所述多播分组的计数器模式密码块链式消息认证码协议报头中的成对瞬态密钥和伪随机噪声序列号。

28. 如权利要求 26 所述的计算机可读介质，其特征在于，所述多个无线设备中的每一个无线设备的所述消息完整性校验值包括少于 8 个八位位组的缩短消息完整性校验值。

29. 如权利要求 26 所述的计算机可读介质，其特征在于，进一步包括：

从所述多个设备中的至少一个设备接收指示，所述指示用于指示由所述设备接收到的第二多播分组中的一个或多个消息完整性校验值中的差错；以及

向一个或多个设备传送消息，所述消息指示所述至少一个设备发现了一个或多个消息完整性校验值中的差错。

30. 如权利要求 29 所述的计算机可读介质，其特征在于，所述消息包括去往所述一个或多个设备以禁用所述网络中的多播分组服务或更改所述一个或多个设备的单播密钥的指令。

用于具有消息认证的广播 WLAN 消息的系统和方法

[0001] 背景

[0002] 领域

[0003] 本申请一般涉及无线通信，且更具体地涉及用于具有消息认证的广播无线局域网(WLAN)消息的系统、方法和设备。

背景技术

[0004] 在许多电信系统中，通信网络被用于在若干个空间上分开的交互设备之间交换消息。网络可根据地理范围来分类，该地理范围可以例如是城市区域、局部区域、或者个人区域。此类网络会分别被指定为广域网(WAN)、城域网(MAN)、局域网(LAN)、或个域网(PAN)。网络还根据用于互连各种网络节点和设备的交换/路由技术(例如，电路交换-分组交换)、用于传输的物理介质的类型(例如，有线-无线)、和所使用的通信协议集(例如，网际协议集、SONET(同步光学联网)、以太网等)而有所不同。

[0005] 当网络元件是移动的并由此具有动态连通性需求时，或者在网络架构以自组织(ad hoc)拓扑结构而非固定拓扑结构来形成的情况下，无线网络往往是优选的。无线网络使用无线电、微波、红外、光等频带中的电磁波以非制导传播模式来采用无形的物理介质。在与固定的有线网络相比较时，无线网络有利地促成用户移动性和快速的现场部署。

[0006] 无线网络中的设备可在彼此之间传送/接收信息。该信息可包括分组，其在一些方面可被称为数据单元。各分组可包括帮助通过网络来路由分组、标识分组中的数据、处理分组等的开销信息(例如，报头信息、分组性质等)，以及可能在分组的有效载荷中携带的数据(例如，用户数据、多媒体内容等)。在一些情形中，可以传送广播分组，其中相同的数据被同时传送给无线网络中的多个设备。

[0007] 概述

[0008] 本发明的系统、方法和设备各自具有若干方面，其中并非仅靠任何单一方面来负责其期望属性。在不限制如由所附权利要求所表达的本发明的范围的情况下，现在将简要地讨论一些特征。在考虑此讨论后，并且尤其是在阅读题为“详细描述”的章节之后，将理解本发明的特征如何提供包括降低传送数据分组中的有效载荷中的开销的优点。

[0009] 本公开的一方面提供了一种无线通信方法，包括：确定多个无线设备中的每一个无线设备的消息完整性校验值；以及向无线局域网上的多个设备中的每一个设备传送多播分组，该多播分组包括对该多个设备中的每一个设备的指示和该多个设备中的每一个设备的消息完整性校验值。

[0010] 对该多个设备中的每一个设备的指示可以包括该多个设备中的每个设备的关联标识和媒体接入控制地址中的至少一者。确定消息完整性校验值可包括基于以下一者或多者来确定消息完整性校验值：多播分组的帧报头、多播分组中的数据、对该多个设备中的一个设备的指示、以及多播分组的计数器模式密码块链式消息认证码协议报头中的成对瞬态密钥和伪随机噪声序列号。多个无线设备中的每一个无线设备的消息完整性校验值可包括少于8个八位位组的缩短消息完整性校验值。多播分组可在该多播分组的帧主体内包括数

据长度字段。多播分组可包括具有翻转的保留位或者翻转的保留位组合的计数器模式密码块链式消息认证码协议报头，该翻转的保留位或翻转的保留位组合被配置成允许该多个设备将该多播分组识别为具有发送者认证的多播分组。

[0011] 该方法还可包括从多个设备中的一个设备接收指示，该指示用于指示该设备接收到的第二多播分组中的一个或多个消息完整性校验值中的差错；以及向一个或多个设备传送消息，其指示该设备发现了一个或多个消息完整性校验值中的差错。该消息可包括去往一个或多个设备以禁用网络中的多播分组服务的指令，或者可以包括去往一个或多个设备以更改该一个或多个设备的单播密钥的指令。确定消息完整性校验值可包括通过用群临时密钥加密多播分组中的数据来生成第一消息完整性校验值，以及随后基于第一消息完整性校验值确定多个无线设备中的每个无线设备的消息完整性校验值。

[0012] 本公开的另一方面提供了一种无线通信装置，包括发射机，其配置成确定多个无线设备中的每一个无线设备的消息完整性校验值；以及向无线局域网上的多个设备中的每一个设备传送多播分组，该多播分组包括对该多个设备中的每一个设备的指示和该多个设备中的每一个设备的消息完整性校验值。

[0013] 在一方面，本公开提供了一种无线通信设备，包括：用于确定多个无线设备中的每一个无线设备的消息完整性校验值的装置；以及用于向无线局域网上的多个设备中的每一个设备传送多播分组的装置，该多播分组包括对该多个设备中的每一个设备的指示和该多个设备中的每一个设备的消息完整性校验值。

[0014] 在另一方面，本公开提供了一种非瞬态计算机可读介质，包括当被执行时使得设备中的处理器执行一种无线通信方法的指令，该方法包括：确定多个无线设备中的每一个无线设备的消息完整性校验值；以及向无线局域网上的多个设备中的每一个设备传送多播分组，该多播分组包括对该多个设备中的每一个设备的指示和该多个设备中的每一个设备的消息完整性校验值。

[0015] 附图简述

[0016] 图 1 解说了其中可采用本公开的各方面的无线通信系统的示例。

[0017] 图 2 示出了可在图 1 的无线通信系统内采用的示例性无线设备的功能框图。

[0018] 图 3 解说了具有消息认证的多播帧格式分组。

[0019] 图 4 解说了具有消息认证的另一多播帧格式分组。

[0020] 图 5A 示出了用于传送具有消息认证的分组的示例性方法的流程图。

[0021] 图 5B 示出了用于传送具有使用公钥和私钥的消息认证的分组的另一示例性方法的流程图。

[0022] 图 6 示出了用于传送具有消息认证的分组的另一示例性方法的流程图。

[0023] 图 7 示出了用于接收具有消息认证的分组的示例性方法的流程图。

[0024] 图 8 示出了用于接收具有消息认证的分组的另一示例性方法的流程图。

[0025] 详细描述

[0026] 以下参照附图更全面地描述本新颖系统、装置和方法的各种方面。然而，本教义公开可用许多不同的形式来实施并且不应被解释为被限定于本公开通篇所给出的任何特定结构或功能。确切而言，提供这些方面是为了使本公开将是透彻和完整的，并且其将向本领域技术人员完全传达本公开的范围。基于本文中的教导，本领域技术人员应领会到，本公开

的范围旨在覆盖本文中公开的这些新颖的系统、设备和方法的任何方面，不论其是独立实现的还是与本发明的任何其他方面组合实现的。例如，可以使用本文所阐述的任何数目的方面来实现装置或实践方法。另外，本发明的范围旨在覆盖使用作为本文中所阐述的本发明各种方面的补充或者与之不同的其他结构、功能性、或者结构及功能性来实践的装置或方法。应当理解，本文披露的任何方面可以由权利要求的一个或多个要素来实施。

[0027] 尽管本文描述了特定方面，但这些方面的众多变体和置换落在本公开的范围之内。尽管提到了优选方面的一些益处和优点，但本公开的范围并非旨在被限定于特定益处、用途或目标。相反，本公开的各方面旨在宽泛地适用于不同的无线技术、系统配置、网络、和传输协议，其中一些藉由示例在附图和以下对优选方面的描述中解说。详细描述和附图仅仅解说本公开而非限定本公开，本公开的范围由所附权利要求及其等效技术方案来定义。

[0028] 无线网络技术可包括各种类型的无线局域网 (WLAN)。WLAN 可被用于采用广泛使用的联网协议来将近旁设备互连在一起。本文中所描述的各个方面可应用于任何通信标准，诸如 WiFi、或者更一般地 IEEE 802.11 无线协议族中的任何成员。

[0029] 在一些实现中，WLAN 包括作为接入无线网络的组件的各种设备。例如，可以存在两种类型的设备：接入点（“AP”）和客户端（也称为站或“STA”）。一般而言，AP 用作 WLAN 的中枢或基站，而 STA 用作 WLAN 的用户。例如，STA 可以是膝上型计算机、个人数字助理 (PDA)、移动电话等。在一示例中，STA 经由遵循 WiFi（例如，IEEE 802.11 协议）的无线链路连接到 AP 以获得至因特网或至其他广域网的一般连通性。在一些实现中，STA 也可被用作 AP。

[0030] 接入点 (“AP”) 还可包括、被实现为或被称为 B 节点、无线电网络控制器 (“RNC”)、演进型 B 节点、基站控制器（“BSC”）、基收发机站（“BTS”）、基站（“BS”）、收发机功能（“TF”）、无线电路由器、无线电收发机或其他某个术语。

[0031] 站（“STA”）还可包括、被实现为、或被称为接入终端（“AT”）、订户站、订户单元、移动站、远程站、远程终端、用户终端、用户代理、用户设备、用户装备或其他某个术语。在一些实现中，接入终端可包括蜂窝电话、无绳电话、会话发起协议（“SIP”）话机、无线本地环路（“WLL”）站、个人数字助理（“PDA”）、具有无线连接能力的手持式设备、或连接至无线调制解调器的其他某种合适的处理设备。因此，本文所教导的一个或多个方面可被纳入到电话（例如，蜂窝电话或智能电话）、计算机（例如，膝上型设备）、便携式通信设备、手持机、便携式计算设备（例如，个人数据助理）、娱乐设备（例如，音乐或视频设备、或卫星无线电）、游戏设备或系统、全球定位系统设备、或被配置成经由无线介质通信的任何其他合适的设备中。如以上所讨论的，本文中所描述的特定设备可实现例如 IEEE 802.11 标准。

[0032] 图 1 解说了可以在其中采用本公开的各方面的无线通信系统 100 的示例。无线通信系统 100 可按照无线标准（例如 802.11ah 标准）来操作。无线通信系统 100 可包括与 STA 106 通信的 AP 104。

[0033] 可以将各种过程和方法用于无线通信系统 100 中在 AP 104 与 STA 106 之间的传输。例如，可以根据 OFDM/OFDMA（正交频分多址）技术在 AP 104 与 STA 106 之间发送和接收信号。如果是这种情形，则无线通信系统 100 可以被称为 OFDM/OFDMA 系统。替换地，可以根据 CDMA（码分多址）技术在 AP 104 与 STA 106 之间发送和接收信号。如果是这种情形，则无线通信系统 100 可被称为 CDMA 系统。

[0034] 促成从 AP 104 至一个或多个 STA 106 的传输的通信链路可被称为下行链路(DL)108，而促成从一个或多个 STA 106 至 AP 104 的传输的通信链路可被称为上行链路(UL)110。替换地，下行链路 108 可被称为前向链路或前向信道，而上行链路 110 可被称为反向链路或反向信道。

[0035] AP 104 可充当基站并提供基本服务区域 (BSA)102 中的无线通信覆盖。AP 104 连同与该 AP 104 相关联并使用该 AP 104 来通信的诸 STA 106 一起可被称为基本服务集(BSS)。应注意，无线通信系统 100 可以不具有中央 AP 104，而是可以作为 STA 106 之间的对等网络起作用。相应地，本文中所描述的 AP 104 的功能可替换地由一个或多个 STA 106 来执行。

[0036] 图 2 解说了可在无线通信系统 100 内可采用的无线设备 202 中使用的各种组件。无线设备 202 是可被配置成实现本文描述的各种方法的设备的示例。例如，无线设备 202 可包括 AP 104 或者各 STA 106 中的一个 STA。

[0037] 无线设备 202 可包括控制无线设备 202 的操作的处理器 204。处理器 204 也可被称为中央处理单元 (CPU)。可包括只读存储器 (ROM) 和随机存取存储器 (RAM) 两者的存储器 206 向处理器 204 提供指令和数据。存储器 206 的一部分还可包括非易失性随机存取存储器 (NVRAM)。处理器 204 通常基于存储器 206 内存储的程序指令来执行逻辑和算术运算。存储器 206 中的指令可以是可执行的以实现本文描述的方法。

[0038] 处理器 204 可包括用一个或多个处理器实现的处理系统或者可以是其组件。这一个或多个处理器可以用通用微处理器、微控制器、数字信号处理器 (DSP)、现场可编程门阵列 (FPGA)、可编程逻辑器件 (PLD)、控制器、状态机、选通逻辑、分立硬件组件、专用硬件有限状态机、或能够对信息执行演算或其他操纵的任何其他合适实体的任何组合来实现。

[0039] 处理系统还可包括用于存储软件的机器可读介质。软件应当被宽泛地解释成意指任何类型的指令，无论其被称作软件、固件、中间件、微代码、硬件描述语言、或是其他。指令可包括代码（例如，呈源代码格式、二进制代码格式、可执行代码格式、或任何其他合适的代码格式）。这些指令在由该一个或多个处理器执行时使处理系统执行本文描述的各种功能。

[0040] 无线设备 202 还可包括外壳 208，该外壳 208 可内含发射机 210 和接收机 212 以允许在无线设备 202 和远程位置之间进行数据的传送和接收。发射机 210 和接收机 212 可被组合成收发机 214。天线 216 可被附连至外壳 208 并且电耦合至收发机 214。无线设备 202 还可包括（未示出）多个发射机、多个接收机、多个收发机、和 / 或多个天线。

[0041] 无线设备 202 还可包括可被用于力图检测和量化由收发机 214 接收到的信号电平的信号检测器 218。信号检测器 218 可检测诸如总能量、每副载波每码元能量、功率谱密度之类的信号以及其它信号。无线设备 202 还可包括用于处理信号的数字信号处理器(DSP)220。DSP 220 可被配置成生成数据单元以供传输。在一些方面，数据单元可包括物理层数据单元 (PPDU)。在一些方面，PPDU 被称为分组。

[0042] 在一些方面，无线设备 202 可进一步包括用户接口 222。用户接口 222 可包括按键板、话筒、扬声器、和 / 或显示器。用户接口 222 可包括向无线设备 202 的用户传达信息和 / 或从该用户接收输入的任何元件或组件。

[0043] 无线设备 202 的各种组件可由总线系统 226 耦合在一起。总线系统 226 可包括例

如数据总线，以及除了数据总线之外还有电源总线、控制信号总线、和状态信号总线。本领域技术人员将领会，无线设备 202 的各组件可耦合在一起或者使用某种其他机制来接受或提供彼此的输入。

[0044] 尽管图 2 中解说了数个分开的组件，但本领域技术人员将认识到，这些组件中的一个或多个组件可被组合或者共同地实现。例如，处理器 204 可被用于不仅实现以上关于处理器 204 描述的功能性，而且还实现以上关于信号检测器 218 和 / 或 DSP 220 描述的功能性。另外，图 2 中解说的每个组件可使用多个分开的元件来实现。

[0045] 在一些方面，可能期望从 AP 104 向多个 STA 106 同时发送多播或广播帧。例如，在教室环境中，教师可能期望一次向所有学生发送广播分组，因为每个学生可能需要来自教师的相同指令或资料。还存在可能在 WLAN 网络（诸如 IEEE 802.11 协议网络）中期望广播或多播分组的多种其他环境。例如，广播或多播分组也可以用于实况流送、紧急消息接发、广告或其他应用。

[0046] 然而，当前的 Hotspot（热点）2.0 标准强烈地阻止多播帧，因为这些帧可能不包括足够的安全性特征。多播帧当前存在的一个问题是用于多播分组的当前协议容易受到“漏洞 196 攻击”，其中 STA 106 可以冒充 AP 104 并发送多播帧。此类弱点之所以可能存在，是因为当前多播帧中使用对称密钥，这意味着作为网络一部分的 STA 106 能够冒充 AP 104 来发送多播帧，并且其他 STA 106 将不能够区别是由 AP 104 发送的多播帧还是由冒充 AP 104 的 STA 106 发送的多播帧。此类冒充 STA 106 可以例如被用于地址解析协议 (ARP) 中毒，在其中冒充 STA 106 将其自身的 MAC 地址与 AP 104 的 MAC 地址相关联，从而拦截来自其他 STA 106 的数据帧。由此，提供合适的多播格式从而允许 STA 106 验证多播帧的发送者是 AP 104 并且在 WLAN 中启用更安全的广播和多播分组可能是有益的。

[0047] 图 3 解说了具有增强的安全性特征的多播帧格式分组 300。例如，该分组 300 可以被用于从 AP 104 发送到 STA 106 的任何多播或广播帧。例如，该分组 300 可以被用于数据帧以及被用于管理帧。在一些方面，针对分组 300 的每个部分所列出的八位位组数目可以变化。例如，针对分组 300 的每个部分所列出的八位位组数目仅仅是示例性的。

[0048] 多播帧格式分组 300 可以包括两个八位位组的帧控制 305 字段、两个八位位组的历时 ID 310 字段、以及三个各为六个八位位组的地址字段 315、320、325。多播帧格式分组 300 可进一步包括两个八位位组的序列控制字段 330、帧主体 335、以及四个八位位组的帧校验序列 (FCS)340。在一些方面，帧格式 300 的这些部分中的每个部分（除了帧主体）可以类似于先前的帧类型。帧主体 335 可包括计数器密码模式块链式消息认证码协议 (CCMP) 报头 345、数据长度 350、加密数据 355、基于群临时密钥（基于 GTK 的）的 MIC（消息完整性码）360、以及两个或更多个 AID 或 MAC（媒体接入控制）地址 365 和 MIC 370。

[0049] 在一些方面，CCMP 报头 345 和经加密的数据 355 可以如普通分组中那样基于 GTK 被创建。然而，格式 300 可以按多种方式与普通帧不同。首先，为了提供附加的安全性，对于帧所要去往的每个 STA 106，该 STA 106 的 AID 或 MAC 地址 365 可以连同每个 STA 的消息完整性校验 (MIC)370 一起被传送。这些元素通常可以在发送到 STA 106 的单播分组中被传送。在一些方面，每个 STA 106 的 MIC 370 可以基于帧报头、数据、STA 106 的 MAC 地址和 / 或 AID、以及 CCMP 报头 345 中的 STA 成对瞬态密钥 (PTK) 和 PN 序列号来生成。然而，在一些方面，改为基于 CCMP 报头 345 中的 PN 序列号以及为 GTK 生成的 MIC 来生成 MIC 可

能是有益的。不像仅包括对称密钥的先前多播帧格式，包括此类每 STA 的 MIC 370 可以防止漏洞 196 攻击。由此，为每个接收多播分组 300 的 STA 增加 AID 或 MAC 地址 365 和 MIC 370 可以允许多播或广播分组中增加的安全性。

[0050] 在一些方面，分组 300 的帧主体 335 可以包括数据长度字段 350。此类数据长度字段 350 在其他分组格式中可能是不需要的，因为分组的数据长度可以基于单播分组的历时字段 310 而推导出来。然而，在多播分组 300 中，数据的历时可能无法从历时字段 310 推导出来，因为多播分组 300 可能具有可变数目的 AID 或 MAC 地址 365 和可变数目的 MIC 370。由此，附加的数据长度字段 350 可以被用来指示多播分组中所包括的数据的长度。

[0051] 在一些方面，CCMP 报头 345 可以包括多个保留位。在一些方面，为了向 STA 指示分组是包含每 STA 的 MIC 的多播分组，其中一个保留位可以被用来指示具有分组格式 300 的经加密的 MPDU。例如，保留位的值可以被更改从而指示具有分组格式 300 的经加密的 MPDU。在一些方面，CCMP 报头 345 的位的组合可以被保留，并且所保留的位组合可以被选择从而向 STA 106 指示分组是根据分组格式 300 的经加密的多播分组。例如，位组合的值（诸如所保留的位组合）可以被更改从而指示该分组是根据分组格式 300 的经加密的多播分组。通过更改保留位或保留位组合，分组可以向接收设备指示该分组包括本文中所讨论的安全性特征和 / 或加密。在一些方面，图 3 中的每 STA 的 MIC 办法的一个缺陷可以是随着多播分组被传送到更大数目的 STA，需要更多的每 STA 的 AID 或 MAC 地址 365、以及更多的每 STA 的 MIC 370。由此，因为分组被传送到更多数目的 STA，因此可能需要随每个分组传送更大量的开销信息。

[0052] 在一些方面，降低通过在每个分组中包括每 STA 的 MIC 370 所产生的开销的一种可能方法可以包括减小每个 MIC 的大小。例如，在一些方面，每 STA 的 MIC 370 各自可以是 8 个八位位组。这个大小可以允许 2^{8*8} 个不同值。这可以使得冒充 STA 在假装 AP 104 传送分组时很难正确地猜到 STA MIC 370 的正确值。然而，为每个 STA 包括 8 个八位位组 MIC 会向每个分组增加相当大量的开销，特别是当多播分组 300 被传送给大量 STA 106 时。由此，提供较短的 MIC 370 可以是有利的。然而，较短的 MIC 370 一般可能具有更易被冒充设备猜到的缺点。可用以弥补多播分组 300 中的这一缺陷的一种方法是为接收该分组的每个 STA 106 提供较短的 MIC 370，并且允许 STA 106 藉以在该 STA 106 的 MIC 370 不正确的情况中警告其他 STA 106 的机制

[0053] 例如，任何 STA 106 一旦接收到具有错误 MIC 370 的多播帧时就可以向 AP 104 传送消息以告知其流氓实体正在传送多播帧。在一些方面，若 STA 106 接收到包含具有不同于期望值的值的 MIC 370 的分组，则 STA 106 可以警告 AP 104。AP 104 可以配置成确定这一差错是否是由于 STA 106 接收分组中的差错，或者该分组自身是否不是由 AP 104 发送的并且可能是由流氓实体（诸如冒充 STA）发送的。AP 104 一旦知晓此类流氓实体，就可以随后采取多种动作。例如，AP 104 可以停止 BSS 中的多播服务。AP 104 可以配置成广播告知所有设备有流氓设备正在传送多播帧的消息。该消息可以包括该帧的一些参数，从而允许设备丢弃来自流氓设备的帧。AP 104 也可以改变 BSS 中的设备的单播密钥。例如，AP 104 可以指令设备改变密钥，诸如设备用来确定消息是否是由 AP 104 发送的成对瞬态密钥 (PTK)。例如，若一个设备正在冒充 AP 104，则那个设备可能已经成功地将 MIC 370 传送到网络中的一些设备。相应地，若每个设备更改其单播密钥以使得冒充设备将无法在单播密

钥改变后向这些设备发送正确的 MIC 370 值可能是有益的，因为每个个体设备的 MIC 370 可以至少部分基于该设备的单播密钥。

[0054] 在一些方面，网络的安全性可以通过向每个 STA 106 提供较短 MIC 370 但还提供若接收到错误 MIC 370 则 STA 106 可警告 AP 104 的机制来改善。相比于向每个 STA 106 提供较长 MIC 370 且没有警告 AP 104 的反应机制，这也可以降低开销。例如，若五个 STA 106 各自接收到两个八位位组的 MIC 370，那么 5 个各为两个八位位组的 MIC 值 370 可有 2^{8*2*5} 种不同的可能组合。这高于单个八位位组 MIC 的不同值的数目 2^{8*8}。由此，提供短于 8 个八位位组的 MIC 370 可能是有益的，并且 MIC 大小的此类降低可能不会导致比较大 MIC 大小差的安全性。

[0055] 图 4 解说了具有增强的安全性特征的另一多播帧格式分组 400。例如，该分组 400 可以被用于从 AP 104 发送到 STA 106 的所有帧。例如，该分组 400 可以被用于数据帧和管理帧两者。在一些方面，针对分组 400 的每个部分所列出的八位位组数目可以不同于所列出的数目，所列出的数目可以仅是示例性的。

[0056] 多播帧格式分组 400 可以包括两个八位位组的帧控制 405 字段、两个八位位组的历时 ID 410 字段、以及三个各为六个八位位组的地址字段 415、420、425。分组 400 可进一步包括两个八位位组的序列控制字段 430、帧主体 435、以及四个八位位组的帧校验序列 (FCS) 440。在一些方面，帧格式 400 的这些部分中的每个部分（除了帧主体）可以类似于先前的帧类型。帧主体 435 可以包括计数器密码模式块链式消息认证码协议 (CCMP) 报头 445、经加密的数据 455 和数字签名 475。

[0057] 如同分组 300 一样，分组 400 除了帧主体 435 之外的所有分组部分可以类似于先前的分组。如同分组 300 一样，CCMP 报头 445 可以配置成包括去往 STA 106 的关于分组是多播分组 400 的指示。例如，CCMP 报头 445 可以包括从其保留值翻转的保留位从而指示该分组是多播分组 400。在一些方面，CCMP 报头 445 可以包括保留位组合，从而指示分组是多播分组 400。在一些方面，不像分组 300，分组 400 中可以不需要数据长度字段，因为数字签名 475 可以被定义成某个固定长度。由此，历时字段 410 单独就足以向 STA 106 指示经加密的广播数据 455 的历时。

[0058] 为了确保分组 400 是由 AP 104 传送而非由冒充 STA 106 传送，该分组 400 可包括数字签名 475。在一些方面，数字签名 475 可以基于公钥 / 私钥方案。在该方案中，可以使用基于每分组的数字签名 475。这可以包括将用 GTK 数据加密的数据进行散列，并且随后基于该数据的散列值来计算数字签名 475。在一些方面，数字签名 475 可以基于数据或者是数据的散列来计算。在一些方面，数字签名 475 也可以基于计数器模式密码块链式消息认证码协议 (CCMP) 报头 445 中的序列 (PN) 号。在一些方面，数字签名 475 也可以基于由 GTK 生成的 MIC 来生成。这在一些方面可能是有益的，因为这可以避免为整个数据计算数字签名 475，而为整个数据计算数字签名 475 可能更复杂。

[0059] 数字签名 475 可以随后被附加到帧。这种办法可以提供胜过其他办法的优势。例如，该办法可仅要求固定长度的单个数字签名 475，其可以小于如分组 300 中那样为每个 STA 106 附加多个个体 MIC。类似地，计算单个签名比计算个体 MIC 可以更简单，特别是在 STA 数目较大时。然而，这一办法也可具有一些缺点。例如，非对称加密（诸如用在公钥 / 私钥系统中的非对称加密）在计算上可能更复杂。这可能使得 STA 的逐分组验证更加困难。

此外，公钥 / 私钥对的生成可能是困难的。在该情况中，AP 104 可以充当其本身的证书权威机构，并且可能不得不动态地生成公钥 / 私钥对。这对于 AP 在计算上可能是复杂的。每个密钥对可以配置成在特定时间段之后过期，从而维持安全性，这可以要求生成新的公钥 / 私钥对。

[0060] 可以在分组 400 中使用的一种加密类型是椭圆曲线密码学 (ECC)。ECC 可以被用来生成数字签名 475，并且可以具有胜过其他技术的优势。例如，ECC 可以要求少量的计算开销。使用 ECC 生成数字签名 475 可以涉及在其他密码学领域中使用的方法。例如，如在用于公钥加密的 IEEE 1363 标准中所描述的，椭圆曲线数字签名算法 (ECDSA) 可以被用于加密数字签名 475。在一些方面，数字签名 475 可以至少部分基于诸如 NIST 特别出版物 800-56A，“Recommendation for Pair-Wire Key Establishment Schemes Using Discrete Logarithm Cryptography（使用离散对数密码术的对线密钥建立方案的建议）”以及 FIPS 出版物 186-3，“Digital Signature Standard(DSS)（数字签名标准 (DSS)）”中所公开的那些技术而生成，上述两者通过引用纳入于此。在一些方面，每个公钥 / 私钥对可以包括期满时间，该期满时间可以用 AP 104 的定时器同步功能 (TSF) 的形式来提供。

[0061] 为了使用公钥 / 私钥加密方法，公钥必须被提供给网络中的 STA 106。在提供公钥时，每个 STA 106 可以配置成验证其正在使用的公钥是由 AP 104 发送的。例如，AP 104 可以在经加密的单播帧中向 STA 106 传送公钥，其使用 STA 106 的 PTK 来加密。这可以允许 STA 106 确保密钥的发送者确实是 AP 104。

[0062] 图 5A 示出了用于传送具有消息认证的分组的示例性方法的流程图。在一些方面，该方法可以由 WLAN 网络上的 AP 104 在发送广播分组时完成。

[0063] 在框 505，AP 104 确定要传送到无线局域网上的多个设备的广播分组的数字签名，该数字签名使用非对称密码术来加密以使得该多个设备中的每一者能验证传送该广播分组的设备的身份。在一些方面，该数字签名可以使用椭圆曲线密码术来加密。在一些方面，用于确定的装置可以包括处理器或发射机。在一些方面，该方法进一步包括生成公钥 / 私钥对，其中公钥可以用来解密使用私钥加密的消息。在一些方面，这些公钥可以被传送到个体无线设备。为了防止对公钥传输的安全性攻击（诸如由冒充 AP 的其他设备所传送的假密钥），个别地向每个无线设备发送公钥而非在广播分组中发送可能是期望的。这在向设备发送第一公钥时可能尤其有用。在一些方面，AP 可以配置成在一些时间区间上生成公钥 / 私钥对，并且在生成了新密钥对之后向无线设备传送新公钥。如本文中所描述的，这些经更新的公钥的传输可以在广播分组中被传送到具有先前公钥的设备。然而，因为网络的新设备可能无法认证此类广播分组，因此将公钥单独地发送到网络上的新设备可能是有用的。

[0064] 在一些方面，每个公钥 / 私钥可以具有期满时间。例如，该期满时间可以与新公钥 / 私钥对被生成并且传送到网络中的设备的时间相一致。该期满时间可以用多种方式被传送到设备。例如，该期满时限可以作为定时器同步功能的一部分被传送到网络中的每个设备。

[0065] 在框 510，AP 104 在网络上传送广播分组，该广播分组包括该数字签名。在一些方面，该数字签名可以被包括在该分组的帧主体中的经加密数据之后。在一些方面，用于传送分组的装置可以包括发射机。

[0066] 图 5B 示出了用于传送具有使用公钥和私钥的消息认证的分组的另一示例性方法的流程图。在一些方面，该方法可以由 WLAN 网络上的 AP 104 在发送广播分组时完成。

[0067] 在框 520，方法 515 包括生成公钥和私钥。例如，公钥和私钥可以基于椭圆曲线密码术或另一形式的非对称密码术来生成。在一些方面，用于生成公钥和私钥的装置可以包括处理器。

[0068] 在框 525，方法 515 包括将公钥传送到多个设备中的一个设备，该公钥被配置成解密使用私钥加密的消息。例如，公钥和私钥可以是密钥对，从而公钥可以被用来解密使用私钥加密的消息。然而，由于非对称密码术的本质，公钥可能无法加密消息，因为这需要私钥。在一些方面，用于传送公钥的装置可包括发射机。在一些方面，传送公钥还可以包括传送公钥的期满时间，在期满时间之后公钥就不可以被使用。例如，期满定时器可以被包括在定时器同步功能中。

[0069] 在框 530，方法 515 包括确定要传送到无线局域网上的多个设备的广播分组的数字签名，该数字签名使用非对称密码术来加密以使得该多个设备中的每一者能验证传送该广播分组的设备的身份，其中确定该数字签名包括使用私钥来确定该数字签名。在一些方面，用于确定数字签名的装置可以包括处理器。

[0070] 在框 535，方法 515 包括在网络上传送广播分组，该广播分组包括该数字签名。在一些方面，用于传送广播分组的装置可包括发射机。

[0071] 图 6 示出了用于传送具有消息认证的分组的另一示例性方法的流程图。在一些方面，该方法可以由无线设备（诸如网络上与一个或多个 STA 106 处于通信中的 AP 104）完成。

[0072] 在框 602，AP 104 确定多个无线设备中的每一个无线设备的消息完整性校验值。例如，AP 104 可以希望将多播分组传送给该多个无线设备中的每个无线设备。相应地，为了允许那些设备验证多播消息的发送者，AP 104 可以确定每个设备的 MIC 值。在一些方面，用于确定 MIC 值的装置可以包括处理器。

[0073] 在框 605，AP 104 向无线局域网上的多个设备中的每一个设备传送多播分组，该多播分组包括对该多个设备中的每个设备的指示以及该多个设备中的每个设备的消息完整性校验值。在一些方面，用于传送的装置可包括发射机。在一些方面，该指示可以是标识多播分组要去往的每个设备的一个或多个 MAC 地址或 AID。在一些方面，消息完整性校验值可以是小于 8 个八位位组的缩短消息完整性校验。例如，使用此类缩短的值可以允许分组中包含 MIC 的部分以较少时间被传送，并且由此具有比使用具有较大大小的 MIC 值少的开销。

[0074] 在框 610，AP 104 接收来自该多个设备中的一个设备的指示，其指示了该设备所接收的第二多播分组中的一个或多个消息完整性校验值中的差错。在一些方面，该指示可以由 AP 104 用来确定其他设备是否可能冒充 AP 104。例如，当设备确定分组中的给定消息完整性校验值并不是其应为的值时，该指示可以被接收。这可以意味着除 AP 104 以外的设备传送了该分组。在一些方面，用于接收的装置可包括接收机。

[0075] 在框 615，AP 104 向一个或多个设备传送消息，指示设备发现了分组中一个或多个消息完整性校验值中的差错。例如，若 AP 104 确定设备在框 610 中所接收的分组并不是由 AP 104 所发送的，那么 AP 104 可以警告其他设备有冒充 STA，告知其他设备丢弃冒充分

组，关闭BSS中的多播服务，和/或更改网络中的一个或多个设备的单播密钥。在一些方面，用于传送的装置可包括发射机。

[0076] 图7示出了用于接收具有消息认证的分组的示例性方法的流程图。在一些方面，该方法可以由无线设备（诸如网络上与AP 104处于通信中的STA 106）完成。

[0077] 在框705，STA 106在无线局域网上接收广播分组，该广播分组包括数字签名。在一些方面，用于接收的装置可包括接收机。

[0078] 在框710，STA 106使用公钥来解密数字签名从而验证传送该分组的设备的身份。在一些方面，用于解密的装置可包括处理器或接收机。

[0079] 图8示出了用于接收具有消息认证的分组的示例性方法的流程图。在一些方面，该方法可以由无线设备（诸如网络上与AP 104处于通信中的STA 106）完成。

[0080] 在框805，STA 106接收要传送给无线局域网上的多个设备的广播分组，该分组包括对该多个设备中的每个设备的指示以及该多个设备中的每个设备的消息完整性校验值。在一些方面，用于接收的装置可包括接收机。

[0081] 在框810，STA 106至少部分基于对该多个设备中的每个设备的指示以及该多个设备中的每个设备的消息完整性校验值来验证传送该分组的设备的身份。在一些方面，用于验证的装置可包括处理器或接收机。在一些方面，若传送该分组的设备的身份不能够被验证，则STA 106可以配置成传送指示消息中的消息完整性校验值中的差错的指示。在一些方面，用于传送的装置可包括发射机。

[0082] 如本文所使用的，术语“确定”涵盖各种各样的动作。例如，“确定”可包括演算、计算、处理、推导、研究、查找（例如，在表、数据库或其他数据结构中查找）、探知及诸如此类。而且，“确定”可包括接收（例如，接收信息）、访问（例如，访问存储器中的数据）及诸如此类。而且，“确定”还可包括解析、选择、选取、确立及类似动作。另外，如本文中所使用的“信道宽度”可在某些方面涵盖或者还可称为带宽。

[0083] 上面描述的方法的各种操作可由能够执行这些操作的任何合适的装置来执行，诸如各种硬件和/或软件组件、电路、和/或模块。一般而言，在附图中所解说的任何操作可由能够执行这些操作的相对应的功能性装置来执行。

[0084] 结合本公开所描述的各种解说性逻辑框、模块、以及电路可用设计成执行本文所描述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列信号(FPGA)或其他可编程逻辑器件(PLD)、分立的门或晶体管逻辑、分立的硬件组件或其任何组合来实现或执行。通用处理器可以是微处理器，但在替换方案中，该处理器可以是任何市售的处理器、控制器、微控制器或状态机。处理器还可以被实现为计算设备的组合，例如DSP与微处理器的组合、多个微处理器、与DSP核心协同的一个或多个微处理器、或任何其它此类配置。

[0085] 在一个或多个方面中，所描述的功能可在硬件、软件、固件或其任何组合中实现。如果在软件中实现，则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。计算机可读介质包括计算机存储介质和通信介质两者，包括促成计算机程序从一地向另一地转移的任何介质。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限定，这样的计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储、磁盘存储或其他磁存储设备、或能用于携带或存储指令或数据结构形式的期望程序代

码且能被计算机访问的任何其他介质。任何连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线 (DSL)、或诸如红外、无线电、以及微波之类的无线技术从 web 网站、服务器、或其它远程源传送而来，则该同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之中。如本文中所使用的盘 (disk) 和碟 (disc) 包括压缩碟 (CD)、激光碟、光碟、数字多用碟 (DVD)、软盘和蓝光碟，其中盘 (disk) 往往以磁的方式再现数据，而碟 (disc) 用激光以光学方式再现数据。因此，在一些方面，计算机可读介质可包括非暂态计算机可读介质（例如，有形介质）。另外，在一些方面，计算机可读介质可包括暂态计算机可读介质（例如，信号）。上述的组合应当也被包括在计算机可读介质的范围内。

[0086] 本文所公开的方法包括用于实现所描述的方法的一个或多个步骤或动作。这些方法步骤和 / 或动作可以彼此互换而不会脱离权利要求的范围。换言之，除非指定了步骤或动作的特定次序，否则具体步骤和 / 或动作的次序和 / 或使用可以改动而不会脱离权利要求的范围。

[0087] 所描述的功能可在硬件、软件、固件或其任何组合中实现。如果在软件中实现，则各功能可以作为一条或多条指令存储在计算机可读介质上。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限定，这样的计算机可读介质可包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储、磁盘存储或其他磁存储设备、或能用于携带或存储指令或数据结构形式的期望程序代码且能被计算机访问的任何其他介质。如本文中所使用的盘 (disk) 和碟 (disc) 包括压缩碟 (CD)、激光碟、光碟、数字多用碟 (DVD)、软盘、和蓝光® 碟，其中盘 (disk) 常常磁性地再现数据，而碟 (disc) 用激光来光学地再现数据。

[0088] 因此，一些方面可包括用于执行本文中给出的操作的计算机程序产品。例如，此种计算机程序产品可包括其上存储（和 / 或编码）有指令的计算机可读介质，这些指令能由一个或多个处理器执行以执行本文中所描述的操作。对于一些方面，计算机程序产品可包括包装材料。

[0089] 软件或指令还可以在传输介质上传送。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线 (DSL)、或诸如红外、无线电、以及微波等无线技术从 web 站点、服务器或其他远程源传送而来的，则该同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电以及微波等无线技术就被包括在传输介质的定义里。

[0090] 此外，应当领会，用于执行本文中所描述的方法和技术的模块和 / 或其它恰适装置能由用户终端和 / 或基站在适用的场合下载和 / 或以其他方式获得。例如，此类设备能被耦合至服务器以促成用于执行本文中所描述的方法的装置的转移。替换地，本文所述的各种方法能经由存储装置（例如，RAM、ROM、诸如压缩碟 (CD) 或软盘等物理存储介质等）来提供，以使得一旦将该存储装置耦合至或提供给用户终端和 / 或基站，该设备就能获得各种方法。此外，可利用适于向设备提供本文中所描述的方法和技术的任何其他合适的技术。

[0091] 将理解，权利要求并不被限定于以上所解说的精确配置和组件。可在以上所描述的方法和装置的布局、操作和细节上作出各种改动、更换和变形而不会脱离权利要求的范围。

[0092] 尽管上述内容针对本公开的各方面，然而可设计出本公开的其他和进一步的方面而不会脱离其基本范围，且其范围是由所附权利要求来确定的。

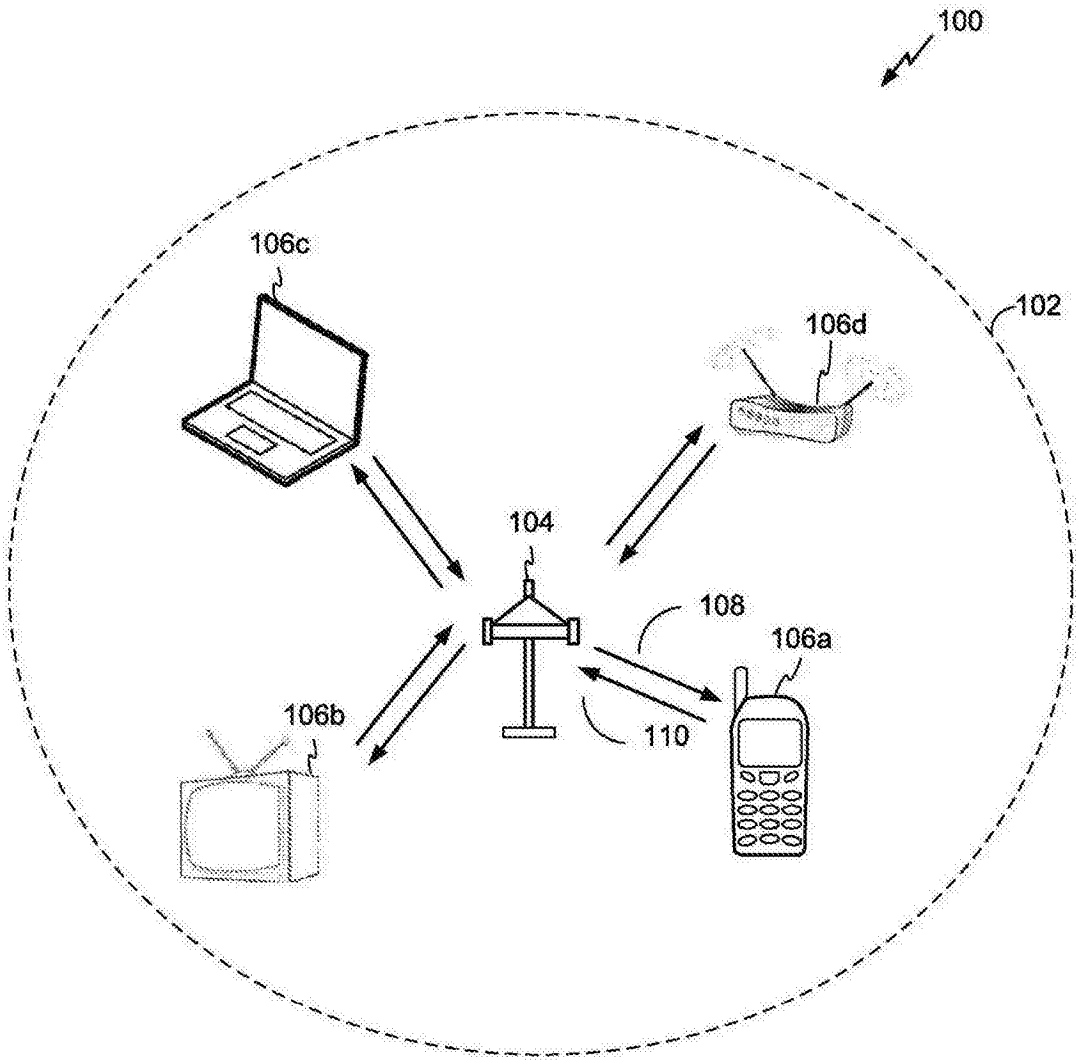


图 1

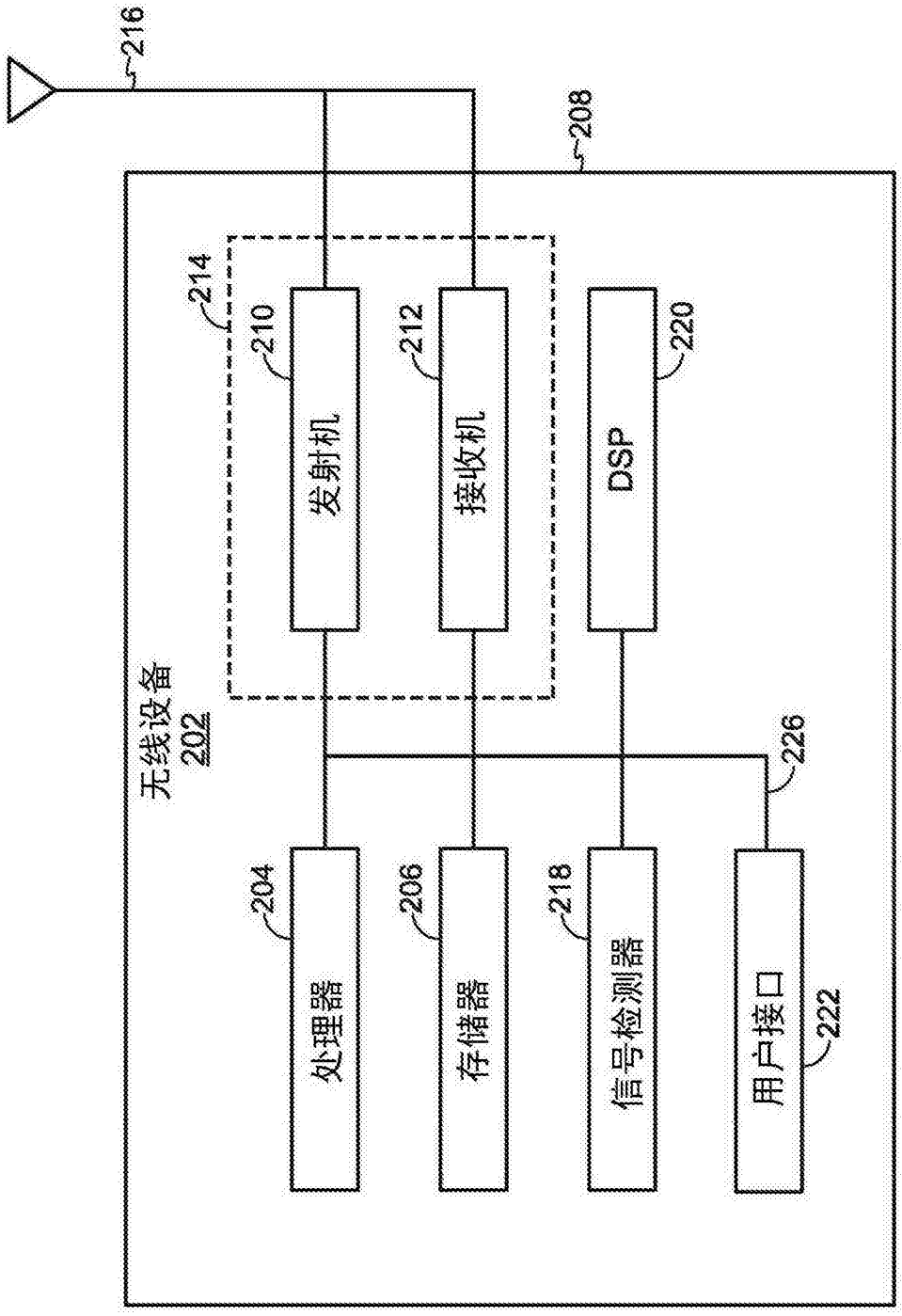

216
208
214
210
发射机
212
接收机
220
DSP
无线设备
202
226
204
处理器
206
存储器
218
信号检测器
222
用户接口

图 2

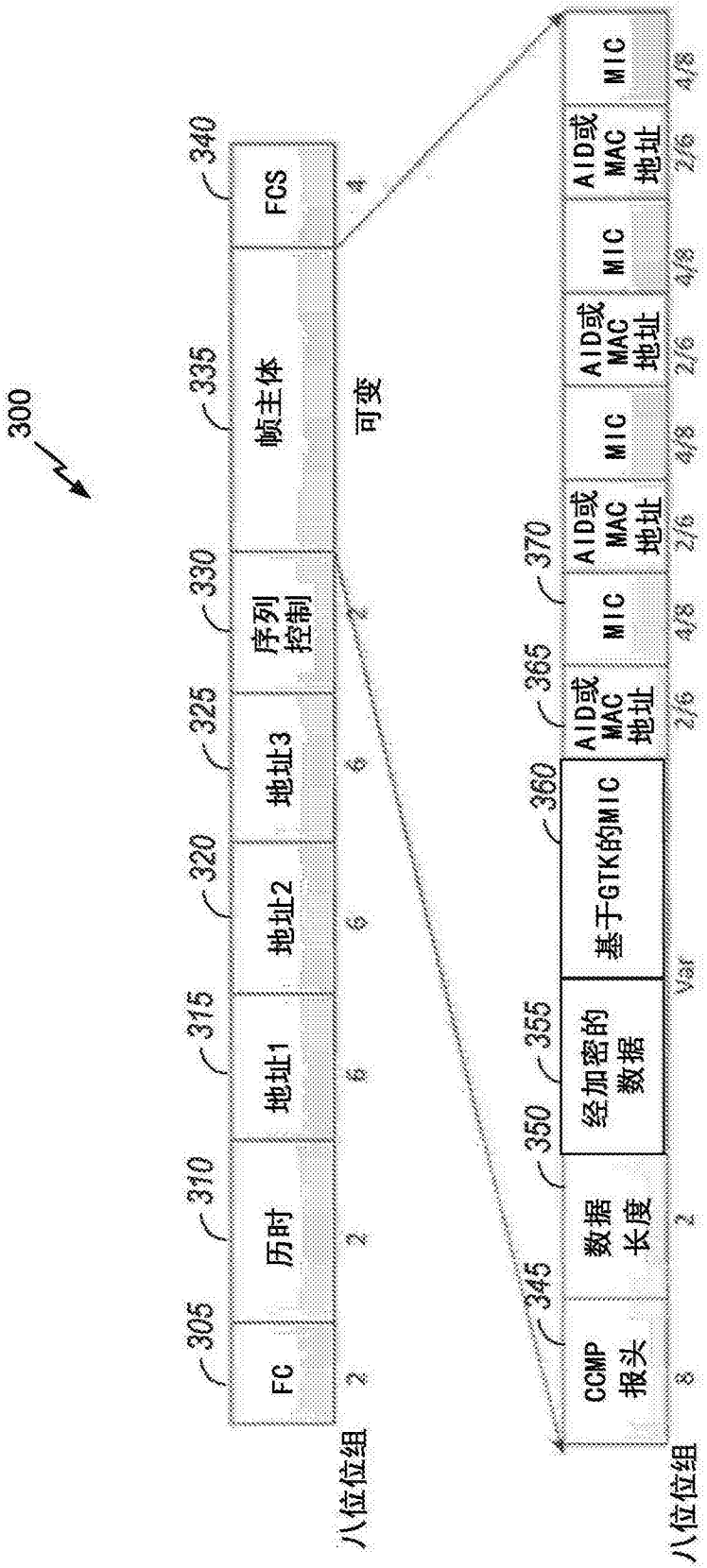

300
305
FC
2
310
历时
2
315
地址1
6
320
地址2
6
325
地址3
6
330
序列控制
2
335
帧主体
可变
340
FCS
4
八位位组
345
CCMP报头
8
350
数据长度
2
355
经加密的数据
Var
360
基于GTK的MIC
8
365
AID或MAC地址
2/6
MIC
4/8
370
AID或MAC地址
2/6
MIC
4/8
AID或MAC地址
2/6
MIC
4/8
AID或MAC地址
2/6
MIC
4/8
八位位组

图 3

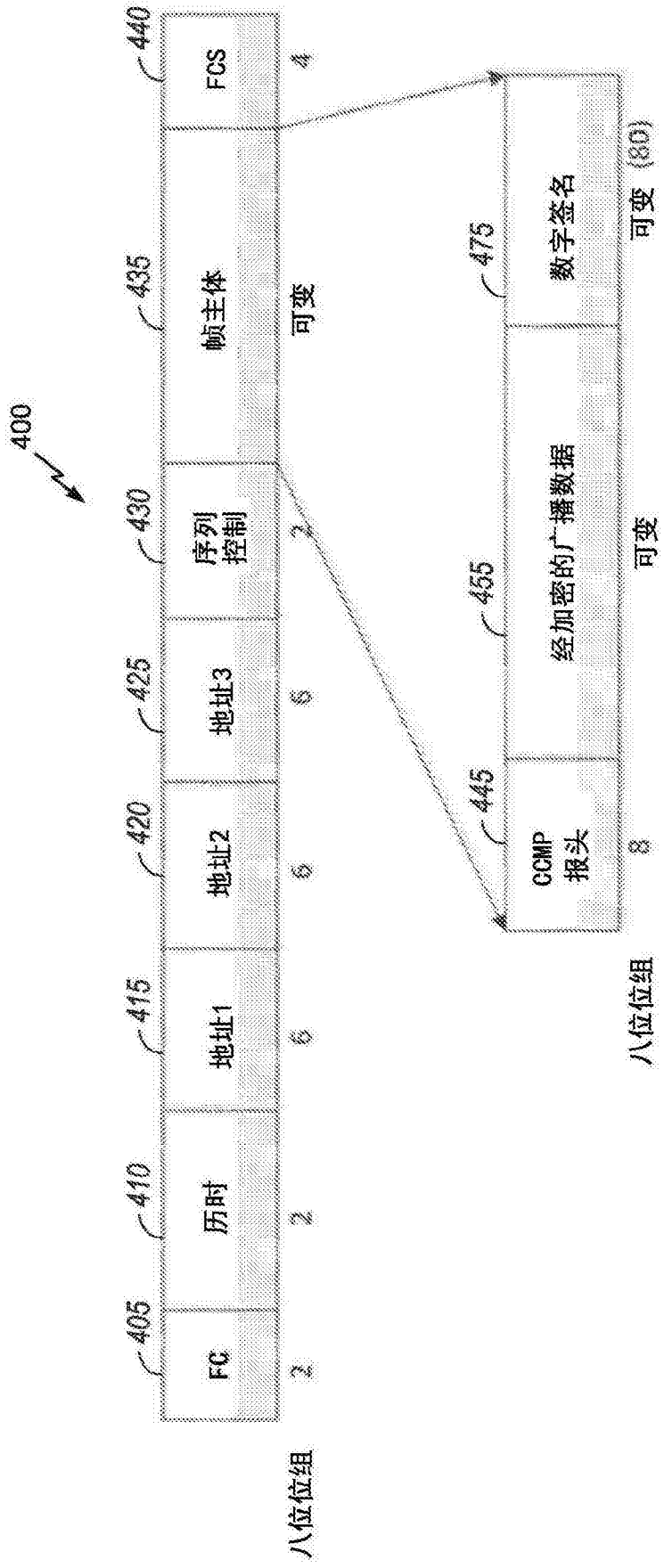

400
405
FC
2
410
历时
2
415
地址1
6
420
地址2
6
425
地址3
6
430
序列控制
2
435
帧主体
可变
440
FCS
4
八位位组
445
CCMP报头
8
455
经加密的广播数据
可变
475
数字签名
可变 (80)
八位位组

图 4

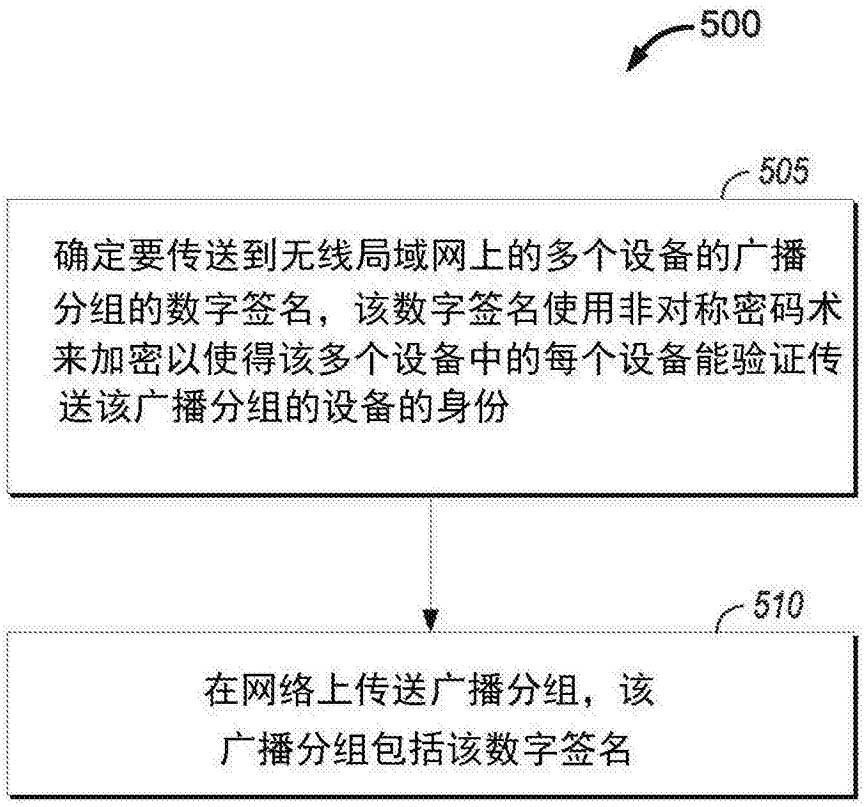

500
505
确定要传送到无线局域网上的多个设备的广播分组的数字签名，该数字签名使用非对称密码术来加密以使得该多个设备中的每个设备能验证传送该广播分组的设备的身份
510
在网络上传送广播分组，该广播分组包括该数字签名

图 5A

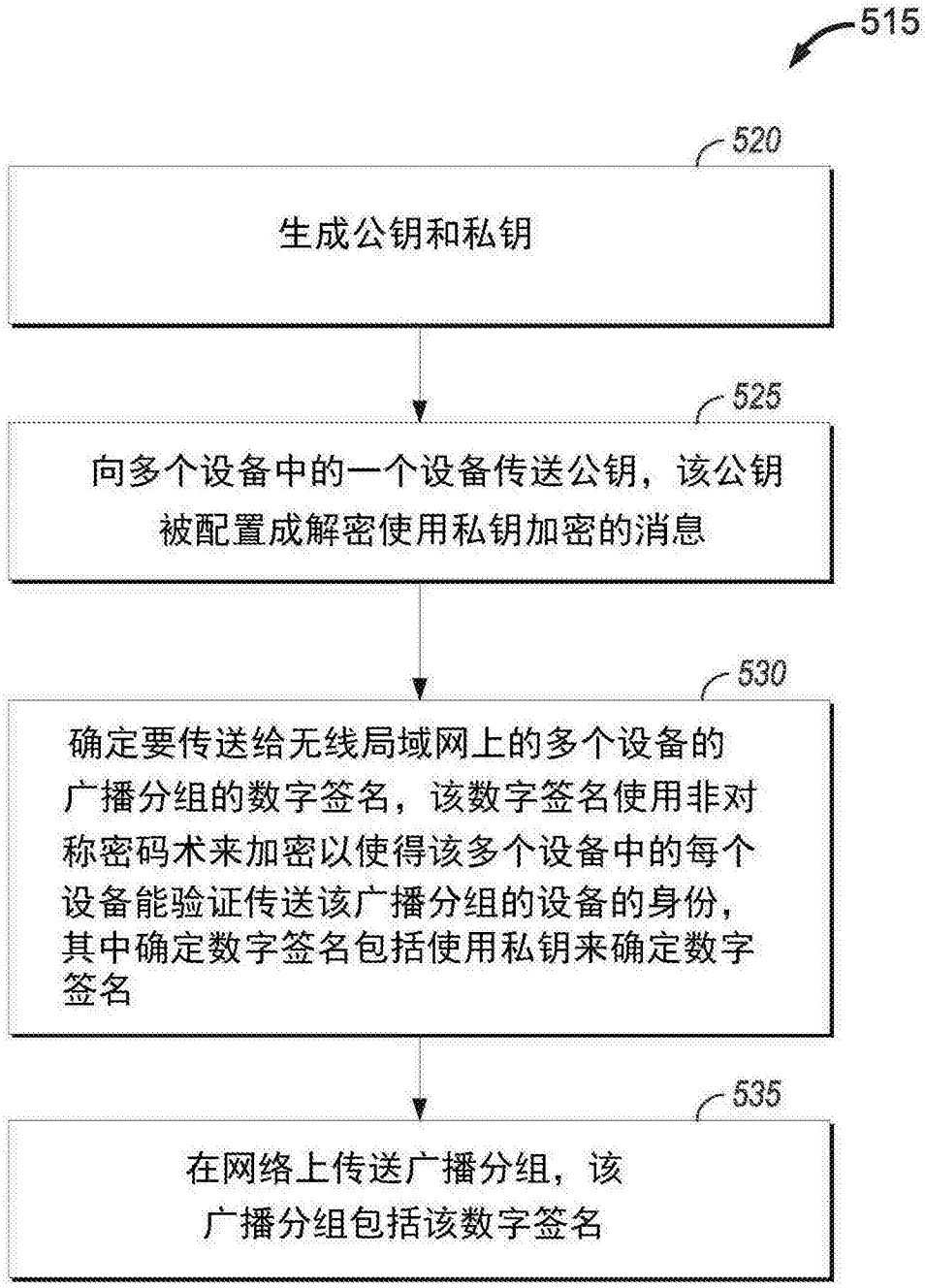

515
520
生成公钥和私钥
525
向多个设备中的一个设备传送公钥，该公钥被配置成解密使用私钥加密的消息
530
确定要传送给无线局域网上的多个设备的广播分组的数字签名，该数字签名使用非对称密码术来加密以使得该多个设备中的每个设备能验证传送该广播分组的设备的身份，其中确定数字签名包括使用私钥来确定数字签名
535
在网络上传送广播分组，该广播分组包括该数字签名

图 5B

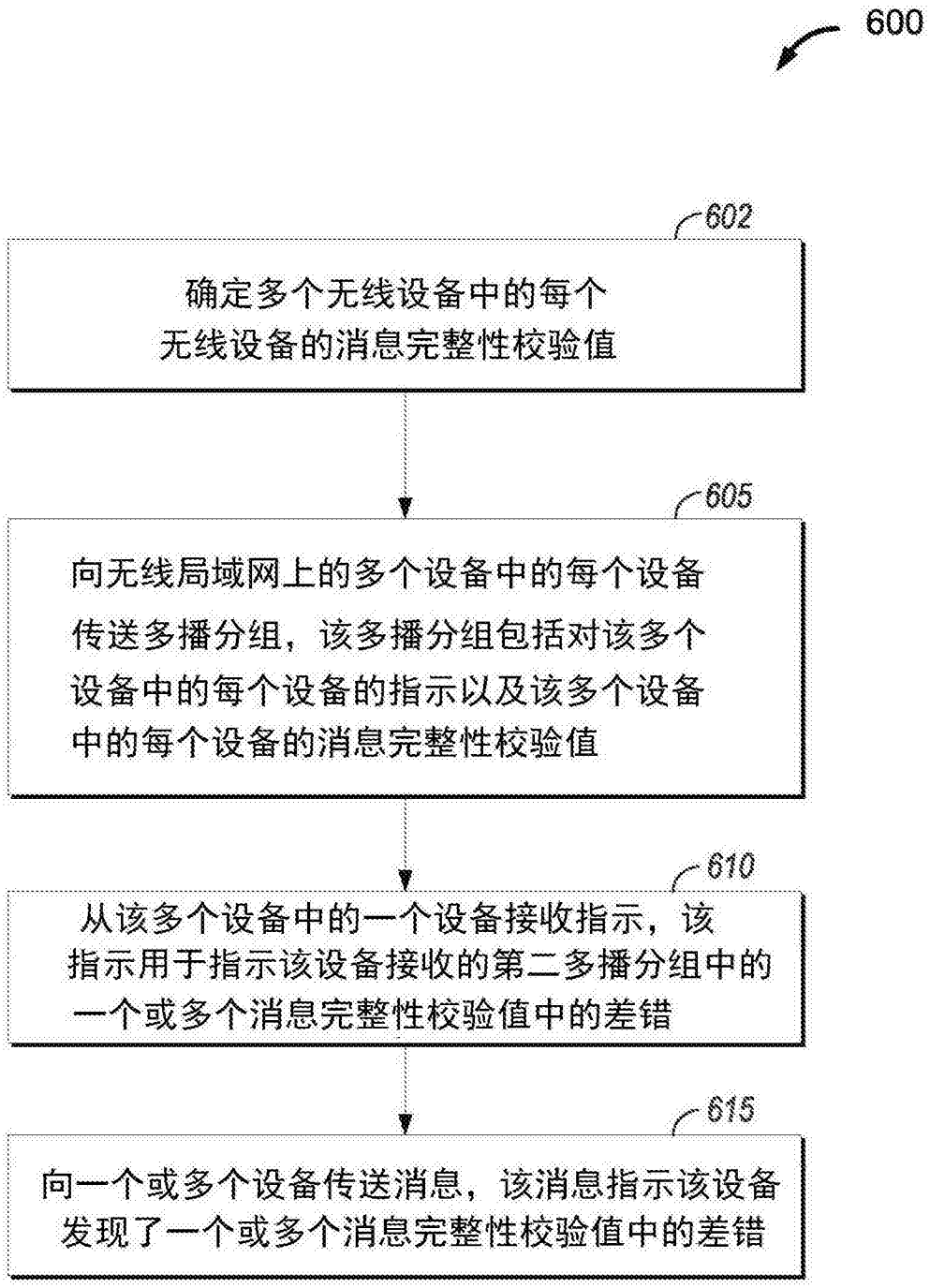

600
602
确定多个无线设备中的每个无线设备的消息完整性校验值
605
向无线局域网上的多个设备中的每个设备传送多播分组，该多播分组包括对该多个设备中的每个设备的指示以及该多个设备中的每个设备的消息完整性校验值
610
从该多个设备中的一个设备接收指示，该指示用于指示该设备接收的第二多播分组中的一个或多个消息完整性校验值中的差错
615
向一个或多个设备传送消息，该消息指示该设备发现了一个或多个消息完整性校验值中的差错

图 6

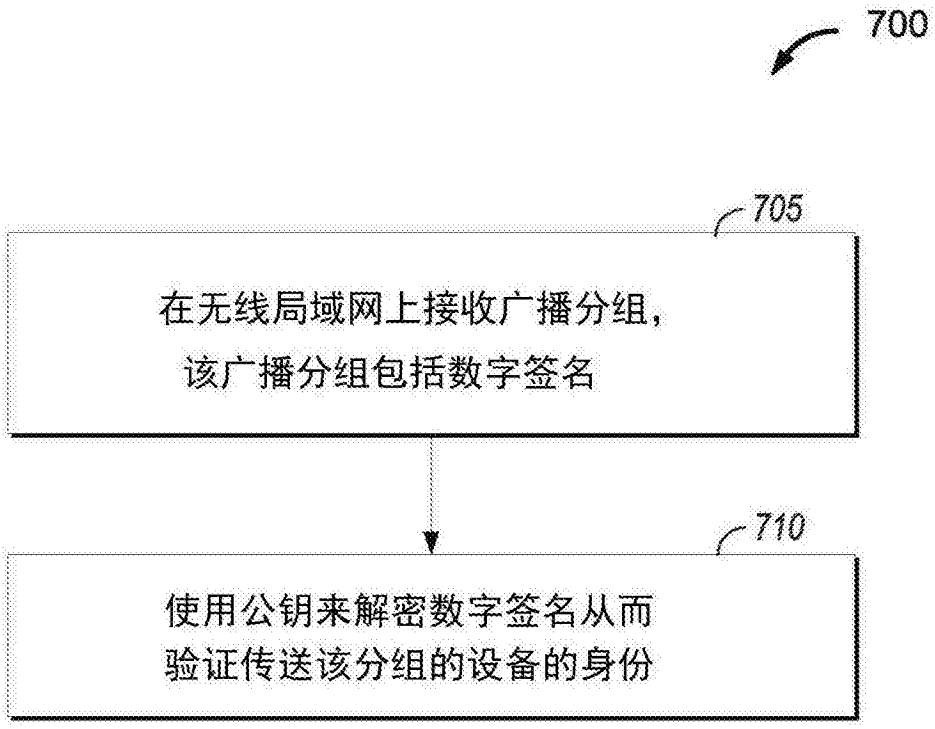

700
705
在无线局域网上接收广播分组，
该广播分组包括数字签名
710
使用公钥来解密数字签名从而
验证传送该分组的设备的身份

图 7

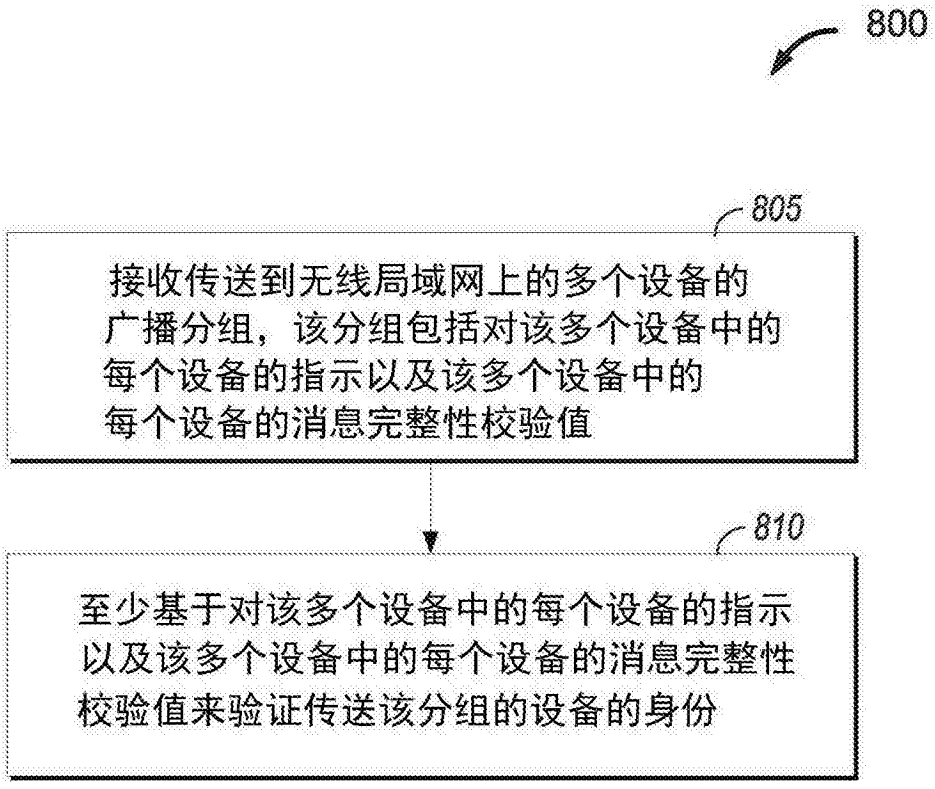

800
805
接收传送到无线局域网上的多个设备的
广播分组，该分组包括对该多个设备中的
每个设备的指示以及该多个设备中的
每个设备的消息完整性校验值
810
至少基于对该多个设备中的每个设备的指示
以及该多个设备中的每个设备的消息完整性
校验值来验证传送该分组的设备的身份

图 8