(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 106105142 A
(43)申请公布日 2016.11.09

(21)申请号 201580014720.6

(22)申请日 2015.06.24

(30)优先权数据
62/016,450 2014.06.24 US
62/063,135 2014.10.13 US
62/115,601 2015.02.12 US
62/141,853 2015.04.02 US

(85)PCT国际申请进入国家阶段日
2016.09.19

(86)PCT国际申请的申请数据
PCT/US2015/037549 2015.06.24

(87)PCT国际申请的公布数据
WO2015/200558 EN 2015.12.30

(71)申请人 谷歌公司
地址 美国加利福尼亚州

(72)发明人 马丁·A·特伦
格兰特·M·埃里克森
克里斯托弗·A·博罗什
杰伊·D·洛格

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 李佳 穆德骏

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/00(2009.01)
H04W 12/06(2009.01)

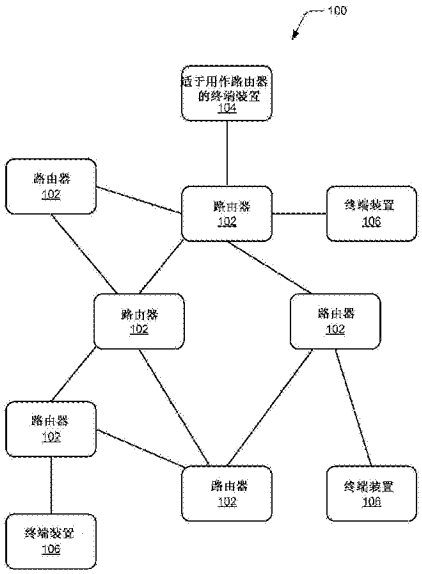
权利要求书19页 说明书42页 附图21页

(54)发明名称

网状网络调试

(57)摘要

在网状网络调试的实施例中，调试装置在所述调试装置与网状网络的边界路由器之间建立安全的调试通信会话，以安全地建立网络通信会话以用于将一个或多个加入装置加入到所述网状网络。所述调试装置能够激活针对所述网状网络的加入，并且从加入装置接收用于加入到所述网状网络的请求。所述调试装置能够在所述调试装置与所述加入装置之间建立安全的加入者通信会话，使用加密装置标识符来对所述加入装置进行认证，并且将所述加入装置加入到所述网状网络。



CN 106105142 A

1.一种将加入装置安全地加入到网状网络的方法,所述方法包括:

在加入者路由器处,从请求加入所述网状网络的所述加入装置接收消息;

将所接收到的消息转发到所述网状网络的调试装置;

从所述调试装置接收用于所述加入装置加入所述网状网络的授权;以及

向所述加入装置传送网络信息,所述网络信息有效地使得所述加入装置能够加入所述网状网络。

2.如权利要求1所述的方法,还包括:

从所述加入装置接收信标请求;以及

从所述加入者路由器向所述加入装置传送信标,所述信标提供所述网状网络能够用于加入的指示。

3.如权利要求2所述的方法,其中,所述传送所述信标有效地使得所述加入装置能够在所述加入装置与所述加入者路由器之间建立本地链路。

4.如前述权利要求中的任一项所述的方法,其中,所述接收所述消息以及所述转发所接收到的消息是使用数据报传输层安全DTLS来执行的。

5.如权利要求1至3中的任一项所述的方法,其中,所述接收所述消息以及所述转发所接收到的消息是使用用户数据报协议UDP来执行的。

6.如前述权利要求中的任一项所述的方法,其中:

从所述加入装置接收到的所述消息包括:能够用来对所述加入装置进行认证的加密装置标识符;

所述加入装置是使用Juggling口令认证密钥交换J-PAKE来认证的;以及

所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话。

7.如前述权利要求中的任一项所述的方法,其中,所述将所接收到的消息转发到所述调试装置包括:在所述加入者路由器与所述调试装置之间的通信路径中,通过所述网状网络的一个或多个路由器来转发所接收到的消息。

8.如权利要求7所述的方法,其中,所述一个或多个路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器,并且其中,所述调试装置附连到所述外部网络。

9.一种被实现为加入者路由器的网状网络装置,所述网状网络装置包括:

网状网络接口,所述网状网络接口被配置成用于网状网络中的通信;

用于实现调试应用的存储器和处理器系统,所述调试应用被配置成:

经由所述网状网络接口从请求加入所述网状网络的加入装置接收消息;

将所接收到的消息转发到所述网状网络的调试装置;

从所述调试装置接收用于所述加入装置加入所述网状网络的授权;以及

开始向所述加入装置传送网络信息,所述网络信息有效地使得所述加入装置能够加入所述网状网络。

10.如权利要求9所述的网状网络装置,其中,所述调试应用被配置成:

经由所述网状网络接口,从所述加入装置接收信标请求;以及

开始从所述加入者路由器向所述加入装置传送信标,所述信标提供所述网状网络能够用于加入的指示。

11.如权利要求10所述的网状网络装置,其中,所述信标有效地使得所述加入装置能够

在所述加入装置与所述加入者路由器之间建立本地链路。

12.如权利要求9至11中的任一项所述的网状网络装置，其中，所述调试应用被配置成使用数据报传输层安全DTLS来接收所述消息并且转发所接收到的消息。

13.如权利要求9至11中的任一项所述的网状网络装置，其中，所述调试应用被配置成使用用户数据报协议UDP来接收所述消息并且转发所接收到的消息。

14.如权利要求9至13中的任一项所述的网状网络装置，其中：

从所述加入装置接收到的所述消息包括能够用来对所述加入装置进行认证的加密装置标识符；

所述加入装置是使用Juggling口令认证密钥交换J-PAKE来认证的；以及

所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话。

15.如权利要求9至14中的任一项所述的网状网络装置，其中，所述调试应用被配置成在所述加入者路由器与所述调试装置之间的通信路径中，通过所述网状网络的一个或多个路由器来转发所接收到的消息。

16.如权利要求15所述的网状网络装置，其中，所述一个或多个路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器，并且其中，所述调试装置附连到所述外部网络。

17.一种网状网络系统，包括：

加入装置，所述加入装置被配置成请求加入网状网络；以及

加入者路由器，所述加入者路由器被配置成：

从请求加入所述网状网络的所述加入装置接收消息；

将所接收到的消息转发到所述网状网络的调试装置；

从所述调试装置接收用于所述加入装置加入所述网状网络的授权；以及

向所述加入装置传送网络信息，所述网络信息有效地使得所述加入装置能够加入所述网状网络。

18.如权利要求17所述的网状网络系统，其中，所述加入者路由器被配置成：

从所述加入装置接收信标请求；以及

向所述加入装置传送信标，所述信标提供所述网状网络能够用于加入的指示，并且所述信标有效地使得所述加入装置能够在所述加入装置与所述加入者路由器之间建立本地链路。

19.如前述权利要求中的任一项所述的网状网络系统，其中

从所述加入装置接收到的所述消息包括能够用来对所述加入装置进行认证的加密装置标识符；

所述加入装置是使用Juggling口令认证密钥交换J-PAKE来认证的；以及

所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话。

20.如权利要求17至19中的任一项所述的网状网络系统，其中，所述加入者路由器被配置成：在所述加入者路由器与所述调试装置之间的通信路径中，通过所述网状网络的一个或多个路由器来将所接收到的消息转发到所述调试装置，并且其中，所述路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器。

21.一种将加入装置安全地加入到网状网络的方法，所述方法包括：

在加入者路由器处，从请求加入所述网状网络的所述加入装置接收DTLS-客户端Hello消息；

将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中；

将所述DTLS中继接收通知消息传送到所述网状网络的调试装置；

从所述调试装置接收DTLS中继传送通知消息；

向所述加入装置传送所述DTLS中继传送通知消息的内容，所述内容有效地使得所述加入装置能够加入所述网状网络；

从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示；

从所述调试装置接收密钥加密密钥KEK，所述KEK是在所述调试装置与所述加入装置之间共享的；以及

响应于接收到所述指示，使用所述KEK来将所述网络证书从所述加入者路由器传送到所述加入装置，以使所述网络证书的通信安全。

22.如权利要求21所述的方法，还包括：

从所述加入装置接收信标请求；以及

从所述加入者路由器向所述加入装置传送信标。

23.如权利要求22所述的方法，其中，所述信标包括网络名称、和操纵数据，所述操纵数据指示被允许加入所述网状网络的一个或多个加入装置。

24.如权利要求21至23中的任一项所述的方法，其中，利用用户数据报协议UDP从所述加入装置接收所述DTLS-客户端Hello消息。

25.如权利要求21至24中的任一项所述的方法，其中，所述DTLS中继接收通知消息包括：

所述加入装置的地址；

所述加入者路由器的地址；以及

所接收到的DTLS-客户端Hello消息。

26.如权利要求21至25中的任一项所述的方法，其中，所述DTLS中继传送通知消息包括：

所述加入装置的所述地址；

所述加入者路由器的所述地址；以及

DTLS-Hello验证消息。

27.如权利要求21至26中的任一项所述的方法，其中，所述将所述DTLS中继传送通知消息的所述内容传送到所述加入装置有效地在所述调试装置与所述加入装置之间建立安全的通信会话。

28.如权利要求27所述的方法，其中，所述安全的通信会话能够用来执行所述加入装置的配备。

29.如权利要求21所述的方法，还包括：

对从加入装置传送到所述调试装置的DTLS中继接收通知消息的传输应用速率限制。

30.一种为实现为加入者路由器的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于在网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

经由所述网状网络接口，从请求加入所述网状网络的加入装置接收DTLS-客户端Hello消息；

将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中；

开始将所述DTLS中继接收通知消息传送到所述网状网络的调试装置；

从所述调试装置接收DTLS中继传送通知消息；

开始向所述加入装置传送所述DTLS中继传送通知消息的内容，所述内容有效地使得所述加入装置能够加入所述网状网络；

从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示；

从所述调试装置接收密钥加密密钥KEK，所述KEK是在所述调试装置与所述加入装置之间共享的；以及

响应于所述指示，开始使用所述KEK来将所述网络证书从所述加入者路由器传送到所述加入装置，以使所述网络证书的通信安全。

31.如权利要求30所述的网状网络装置，其中，所述调试应用被配置成：

经由所述网状网络接口从所述加入装置接收信标请求；以及

开始从所述加入者路由器向所述加入装置传送信标。

32.如权利要求30所述的网状网络装置，其中，所述调试应用被配置成利用用户数据报协议UDP来从所述加入装置接收所述DTLS-客户端Hello消息。

33.如权利要求30至32中的任一项所述的网状网络装置，其中：

所述DTLS中继接收通知消息包括：

所述加入装置的地址；

所述加入者路由器的地址；

所接收到的DTLS-客户端Hello消息；并且其中

所述DTLS中继传送通知消息包括：

所述加入装置的所述地址；

所述加入者路由器的所述地址；以及

DTLS-Hello验证消息。

34.如权利要求30至33中的任一项所述的网状网络装置，其中，传送到所述加入装置的所述DTLS中继传送通知消息的所述内容有效地在所述调试装置与所述加入装置之间建立安全的通信会话。

35.如权利要求30至34中的任一项所述的网状网络装置，其中，所述安全的通信会话能够用来执行所述加入装置的配备。

36.一种网状网络系统，包括：

加入装置，所述加入装置被配置成请求加入网状网络；以及

加入者路由器，所述加入者路由器被配置成：

从请求加入所述网状网络的所述加入装置接收DTLS-客户端Hello消息；

将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中；

将所述DTLS中继接收通知消息传送到所述网状网络的调试装置；

从所述调试装置接收DTLS中继传送通知消息；

向所述加入装置传送所述DTLS中继传送通知消息的内容，

所述内容有效地使得所述加入装置能够加入所述网状网络；

从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示；

从所述调试装置接收密钥加密密钥KEK，所述KEK是在所述调试装置与所述加入装置之间共享的；以及

响应于所述指示，使用所述KEK来将所述网络证书从所述加入者路由器传送到所述加入装置，以使所述网络证书的通信安全。

37.如权利要求36所述的网状网络装置，其中，所述加入者路由器被配置成：

从所述加入装置接收信标请求；以及

从所述加入者路由器向所述加入装置传送信标。

38.如权利要求37所述的网状网络装置，其中，所述信标包括网络名称和操纵数据，所述操纵数据指示被允许加入所述网状网络的一个或多个加入装置。

39.如权利要求36所述的网状网络装置，其中，所述加入者路由器被配置成利用用户数据报协议UDP来从所述加入装置接收所述DTLS-客户端Hello消息。

40.如权利要求36至39中的任一项所述的网状网络装置，其中：

所述DTLS中继接收通知消息包括：

所述加入装置的地址；

所述加入者路由器的地址；

所接收到的DTLS-客户端Hello消息；并且其中

所述DTLS中继传送通知消息包括：

所述加入装置的所述地址；

所述加入者路由器的所述地址；以及

DTLS-Hello验证消息。

41.一种对调试装置进行授权的方法，所述调试装置要成为调试者来对要加入网状网络的一个或多个加入装置进行调试，所述方法包括：

在边界路由器处，从所述调试装置接收要成为所述网状网络的所述调试者的请愿；

将所接收到的请愿传送到所述网状网络的领导者装置；

从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；以及

响应于所述接收到所述响应，向所述调试装置传送对所述请愿的接受或拒绝的指示。

42.如权利要求41所述的方法，还包括：

由所述边界路由器通告所述网状网络对于调试装置的可用性，所述接收所述请愿是响应于所述调试装置接收到所述通告。

43.如前述权利要求中的任一项所述的方法，还包括：

在所述边界路由器处，从所述调试装置接收用于安全连接到所述边界路由器的请求。

44.如权利要求43所述的方法，其中，所述安全连接使用数据报传输层安全DTLS来建立。

45.如权利要求41至44中的任一项所述的方法，其中，所述传送对所述请愿的接受的所述指示建立安全的调试会话。

46.如权利要求41至45中的任一项所述的方法，还包括：

向所述边界路由器注册所述调试装置的身份以建立安全的调试通信会话，所述注册包括向所述边界路由器提供加密调试证书，其中，所述加密调试证书是从由用户输入到所述调试装置的调试证书导出的。

47.如权利要求46所述的方法，其中，所述边界路由器包括能够用来向所述网状网络认证所述调试装置的所述加密调试证书的副本。

48.如权利要求47所述的方法，其中：

所述加密调试证书的所述副本是先前从所述调试证书导出的；

所述调试证书被注入到所述网状网络中导出了所述加密调试证书的所述副本的所述领导者装置中；以及

所述领导者装置将所述加密调试证书的所述副本安全地传递到所述边界路由器。

49.一种被实现为边界路由器的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

经由所述网状网络接口，从调试装置接收要成为所述网状网络的调试者以对要加入所述网状网络的一个或多个加入装置进行调试的请愿；

开始将所接收到的请愿传送到所述网状网络的领导者装置；

从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；以及

响应于所接收到的对所述请愿的响应，开始向所述调试装置传送对所述请愿的所述接受或拒绝的指示。

50.如权利要求49所述的网状网络装置，其中：

所述调试应用被配置成通告所述网状网络对于调试装置的可用性，并且响应于所述调试装置接收到所通告的可用性而接收所述请愿；以及

所通告的可用性是使用包括多播域名系统mDNS的服务发现协议来执行。

51.如前述权利要求中的任一项所述的网状网络装置，其中：

所述调试应用被配置成从所述调试装置接收安全地连接到所述边界路由器的请求；以及

使用数据报传输层安全DTLS来建立安全的连接。

52.如权利要求49至51中的任一项所述的网状网络装置，其中：

所述领导者装置对所述请愿的所述接受授权所述调试装置成为所述网状网络的所述调试者；

对所述请愿的所述接受使得所述领导者装置能够更新内部状态，所述内部状态跟踪所述网状网络的活动调试者，将所述网状网络的准许加入标志设置为真，并且在所述网状网络内传播调试数据集；以及所传送的对所述请愿的所述接受的指示建立安全的调试会话。

53.如权利要求49至52中的任一项所述的网状网络装置，其中：

所述调试应用被配置成：向所述边界路由器注册所述调试装置的身份以建立安全的调试通信会话，包括提供给所述边界路由器的加密调试证书；

所述加密调试证书是从由用户输入到所述调试装置的调试证书导出的；以及

所述边界路由器包括能够用来向所述网状网络认证所述调试装置的所述加密调试证

书的副本。

54.如权利要求49至52中的任一项所述的网状网络装置，其中，所述调试装置和所述边界路由器通过除所述网状网络以外的网络进行通信。

55.如权利要求54所述的网状网络装置，其中，其他网络是Wi-Fi网络或以太网网络中的一个。

56.一种网状网络系统，包括：

调试装置，所述调试装置被配置成请愿成为调试者来对要加入网状网络的一个或多个加入装置进行调试；以及

边界路由器，所述边界路由器被配置成：

从所述调试装置接收要成为所述网状网络的所述调试者的请愿；

将所接收到的请愿传送到所述网状网络的领导者装置；

从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；以及

向所述调试装置传送对所述请愿的所述接受或拒绝的指示。

57.如权利要求56所述的网状网络系统，其中，所述边界路由器被配置成通告所述网状网络对于调试装置的可用性，并且响应于所述调试装置接收到所述通告而接收所述请愿。

58.如前述权利要求中的任一项所述的网状网络系统，其中，所述调试装置和所述边界路由器通过除所述网状网络以外的网络进行通信。

59.如权利要求58所述的网状网络系统，其中，其他网络是Wi-Fi网络或以太网网络中的一个。

60.如权利要求56至59中的任一项所述的网状网络系统，其中，所述边界路由器被配置成传送对所述请愿的所述接受的所述指示，以建立安全的调试会话。

61.一种由网状网络的领导者装置实现的方法，所述方法包括：

由领导者装置接收用于接受调试装置作为调试者来对要加入所述网状网络的加入装置进行调试的请愿；

确定接受还是拒绝所接收到的请愿；

传送包括所述确定的指示的响应；以及

响应于所述确定是接受而更新内部状态，所述内部状态跟踪所述网状网络的活动调试者。

62.如权利要求61所述的方法，还包括：

从所述调试装置接收用于开始所述网状网络的加入模式的命令。

63.如权利要求62所述的方法，还包括：

在所述网状网络内传播调试数据集。

64.如权利要求63所述的方法，其中，所述调试数据集包括：

调试者会话标识符；

调试者时间戳；

加密调试者证书；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许。

65.如权利要求64所述的方法，还包括：

从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书。

66.如权利要求65所述的方法，其中，所述加密调试证书的导出通过应用密钥导出函数来执行，所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列。

67.如权利要求65所述的方法，还包括：

向所述边界路由器发送所述加密调试证书的副本，有效地使得所述边界路由器能够向所述网状网络认证所述调试装置。

68.如权利要求64所述的方法，其中，当所述调试者在所述网状网络上是活动的时，所述调试数据集还包括所述边界路由器的位置。

69.一种被实现为网状网络的领导者装置的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于所述网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

经由所述网状网络接口，接收用于接受调试装置作为调试者来对要加入所述网状网络的加入装置进行调试的请愿；

确定接受还是拒绝所接收到的请愿；

开始传送响应，所述响应包括确定接受还是拒绝所接收到的请愿的指示；以及

响应于所述确定是对所接收到的请愿的接受而更新内部状态，所述内部状态跟踪所述网状网络的活动调试者。

70.如权利要求69所述的网络网状装置，其中，所述调试应用被配置成从所述调试装置接收用于开始所述网状网络的加入模式的命令。

71.如权利要求70所述的网状网络装置，其中，所述调试应用被配置成在所述网状网络内传播调试数据集。

72.如权利要求71所述的网状网络装置，其中，所述调试数据集包括：

调试者会话标识符；

调试者时间戳；

加密调试者证书；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；

所述调试应用还被配置成：从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书，其中，所述加密调试证书的导出通过应用密钥导出函数来执行，所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列。

73.如权利要求72所述的网状网络装置，其中，所述调试应用被配置成向所述边界路由器发送所述加密调试证书的副本，有效地使得所述边界路由器能够向所述网状网络认证所述调试装置。

74.如权利要求72所述的网状网络装置，其中，当所述调试者在所述网状网络上是活动的时，所述调试数据集还包括所述边界路由器的位置。

75.一种网状网络系统，包括：

调试装置，所述调试装置被配置成请愿成为调试者来对要加入网状网络的一个或多个加入装置进行调试；以及

所述网状网络的领导者装置，所述领导者装置被配置成：

接收用于接受所述调试装置作为所述调试者来对要加入所述网状网络的所述加入装置进行调试的请愿；

确定接受还是拒绝所接收到的请愿；

传送包括关于接受还是拒绝所接收到的请愿的确定的指示的响应；以及

响应于所述确定是接受而更新内部状态，所述内部状态跟踪所述网状网络的活动调试者。

76.如权利要求75所述的网状网络系统，其中，所述领导者装置被配置成从所述调试装置接收用于开始所述网状网络的加入模式的命令。

77.如权利要求76所述的网状网络系统，其中，所述领导者装置被配置成在所述网状网络内传播调试数据集。

78.如权利要求77所述的网状网络系统，其中，所述调试数据集包括：

调试者会话标识符；

调试者时间戳；

加密调试者证书；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；

所述领导者装置还被配置成从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书，其中，所述加密调试证书的导出通过应用密钥导出函数来执行，所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列。

79.如权利要求78所述的网状网络系统，其中，所述领导者装置被配置成向所述边界路由器发送所述加密调试证书的副本，有效地使得所述边界路由器能够向所述网状网络认证所述调试装置。

80.如权利要求78所述的网状网络系统，其中，当所述调试者在所述网状网络上是活动的时，所述调试数据集还包括所述边界路由器的位置。

81.一种安全地建立网络通信会话以用于将一个或多个加入装置加入到网状网络的方法，所述方法包括：

在调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话；

激活针对所述网状网络的加入；

由所述调试装置从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求；

在所述调试装置与所述加入装置之间建立安全的加入者通信会话；以及

将所述加入装置加入到所述网状网络。

82.如权利要求81所述的方法，其中，所述建立所述安全的调试通信会话包括：

从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿；以及

从所述领导者装置接收对所述请愿的接受的指示。

83.如前述权利要求中的任一项所述的方法，其中，所述激活针对所述网状网络的加入包括：所述调试装置开始加入模式，所述加入模式致使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求。

84.如权利要求81至82中的任一项所述的方法，其中，所述激活针对所述网状网络的加

入包括：向领导者装置发送用于使所述网状网络变得能够加入的管理消息，所述管理消息有效地使得所述领导者装置能够更新所述网状网络的网络数据，并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置，所述网络数据包括所述网状网络能够用于加入的指示。

85.如权利要求81至84中的任一项所述的方法，还包括：

使用加密装置标识符来对所述加入装置进行认证。

86.如权利要求85所述的方法，其中，所述从所述加入装置中的一个加入装置接收用于加入所述网状网络的所述请求是经由加入者路由器接收的，所述方法还包括：

向所述加入者路由器传送所述加入装置将被委托接收所述网状网络的网络证书和密钥加密密钥KEK的指示，所述KEK是在所述调试装置与所述加入装置之间共享的，所述传送有效地使得所述加入者路由器能够使用所接收到的KEK来将所述网络证书安全地传送到所述加入装置，以将所述加入装置调试到所述网状网络。

87.如权利要求81所述的方法，其中，所述从所述加入装置接收所述请求包括：接收所述加入装置的加密装置标识符，并且其中，所述加密装置标识符是使用Jugglin口令认证密钥交换J-PAKE从所述加入装置的装置标识符导出的。

88.如权利要求87所述的方法，其中，所述建立所述安全的加入者通信会话包括：

由所述调试装置确定从所述加入装置接收到的所述加密装置标识符和由所述调试装置从所述装置标识符的副本所导出的加密装置标识符相匹配，所述装置标识符的所述副本是作为从用户向所述调试装置的输入而接收的；以及

使用所述加密装置标识符作为共享秘密来使所述加入者通信会话安全。

89.一种被实现为调试装置的网状网络装置，所述调试装置用于将一个或多个加入装置加入到网状网络，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于所述网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

在所述调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话；

激活针对所述网状网络的加入；

经由所述网状网络接口，从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求；

在所述调试装置与所述加入装置之间建立安全的加入者通信会话；以及

将所述加入装置加入到所述网状网络。

90.如权利要求89所述的网状网络装置，其中，所述调试应用被配置成：

从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿；以及

从所述领导者装置接收对所述请愿的接受的指示。

91.如前述权利要求中的任一项所述的网状网络装置，其中，所述调试应用被配置成通过开始加入模式来所述激活针对所述网状网络的加入，所述加入模式致使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求。

92.如权利要求89至90中的任一项所述的网状网络装置，其中，所述调试应用被配置成通过向领导者装置发送用于使所述网状网络变得能够加入的管理消息来所述激活针对所

述网状网络的加入，所述管理消息使得所述领导者装置能够更新所述网状网络的网络数据，并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置，所述网络数据包括所述网状网络能够用于加入的指示。

93.如权利要求89所述的网状网络装置，其中，从所述加入装置接收的所述请求包括所述加入装置的加密装置标识符，并且其中，所述加密装置标识符是使用Juggling口令认证密钥交换J-PAKE从所述加入装置的装置标识符导出的。

94.如权利要求93所述的网状网络装置，其中，所述调试应用被配置成建立所述安全的加入者通信会话，还被配置成：

确定从所述加入装置接收到的所述加密装置标识符和由所述调试装置从所述装置标识符的副本所导出的加密装置标识符相匹配，所述装置标识符的副本是作为从用户向所述调试装置的输入而接收的；以及

使用所述加密装置标识符作为共享秘密来使所述加入者通信会话安全。

95.如权利要求89至92中的任一项所述的网状网络装置，其中，所述调试应用被配置成转发来自所述加入装置的用于加入所述网状网络的所述请求，所述请求被所述网状网络中的一个或多个路由器装置转发到所述调试装置。

96.一种网状网络系统，包括：

一个或多个加入装置，所述一个或多个加入装置被配置成请求加入网状网络；以及

所述网状网络的调试装置，所述调试装置被配置成：

在所述调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话；

激活针对所述网状网络的加入；

从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求；

在所述调试装置与所述加入装置之间建立安全的加入者通信会话；以及

将所述加入装置加入到所述网状网络。

97.如权利要求96所述的网状网络系统，其中，用于建立所述安全的调试通信会话的所述调试装置被配置成：

从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿；以及

从所述领导者装置接收对所述请愿的接受的指示。

98.如前述权利要求中的任一项所述的网状网络系统，其中，所述调试装置被配置成通过开始加入模式来所述激活针对所述网状网络的加入，所述加入模式致使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求。

99.如权利要求96至97中的任一项所述的网状网络系统，其中，所述调试装置被配置成通过向领导者装置发送用于使所述网状网络变得能够加入的管理消息来所述激活针对所述网状网络的加入，所述管理消息使得所述领导者装置能够更新所述网状网络的网络数据，并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置，所述网络数据包括所述网状网络能够用于加入的指示。

100.如权利要求96所述的网状网络系统，其中，所述调试装置被配置成：

经由加入者路由器，从所述加入装置中的一个加入装置所述接收用于加入所述网状网络的所述请求；以及

向所述加入者路由器传送所述加入装置将被委托接收所述网状网络的网络证书和密钥加密密钥KEK的指示，所述KEK是在所述调试装置与所述加入装置之间共享的，所传送的指示使得所述加入者路由器能够使用所接收到的KEK来将所述网络证书安全地传送到所述加入装置，以将所述加入装置调试到所述网状网络。

101.一种在网状网络中配备加入装置的方法，所述方法包括：

在调试装置与所述网状网络的边界路由器之间建立调试通信会话；

在所述加入装置与所述调试装置之间建立加入者通信会话；

向所述加入装置发送调试信息，所述调试信息能够由所述加入装置使用来加入所述网状网络；

从所述加入装置接收调试者应用的位置的指示；以及

执行所述调试者应用，以配备所述加入装置。

102.如权利要求101所述的方法，还包括：

利用所接收到的指示来检索所述调试者应用。

103.如前述权利要求中的任一项所述的方法，其中，所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL。

104.如权利要求103所述的方法，其中，所述调试者应用通过互联网从云服务中检索。

105.如权利要求103所述的方法，其中，所述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中。

106.如权利要求101至105中的任一项所述的方法，还包括：

响应于完成所述加入装置的所述配备，使所述加入装置的调试结束，所述结束有效地使得所述加入装置能够加入所述网状网络。

107.如权利要求101所述的方法，其中，所述加入装置的所述配备包括：更新所述加入装置上的软件。

108.如权利要求101所述的方法，其中，所述加入装置的所述配备包括：将所述加入装置链接到云服务上的用户账户。

109.如权利要求101所述的方法，其中，所述加入装置的所述配备包括：配置所述加入装置。

110.如权利要求109所述的方法，其中，所述配置是与所述网状网络中的其它装置有关的本地配置。

111.一种被实现为调试装置的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

在所述调试装置与所述网状网络的边界路由器之间建立调试通信会话；

在所述加入装置与所述调试装置之间建立加入者通信会话；

向所述加入装置发送调试信息，所述调试信息能够由所述加入装置使用来加入所述网状网络；

从所述加入装置接收调试者应用的位置的指示；以及

执行所述调试者应用以配备所述加入装置。

112.如权利要求111所述的网状网络装置，其中，所述调试应用被配置成利用所接收到

的指示来检索所述调试者应用。

113.如前述权利要求中的任一项所述的网状网络装置，其中，所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL。

114.如权利要求113所述的网状网络装置，其中，所述调试者应用通过互联网从云服务中检索。

115.如权利要求113所述的网状网络装置，其中，所述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中。

116.一种网状网络系统，包括：

加入装置，所述加入装置被配置成请求加入网状网络；以及

所述网状网络的调试装置，所述调试装置被配置成：

在所述调试装置与所述网状网络的边界路由器之间建立调试通信会话；

在所述加入装置与所述调试装置之间建立加入者通信会话；

向所述加入装置发送调试信息，所述调试信息能够由所述加入装置使用来加入所述网状网络；

从所述加入装置接收调试者应用的位置的指示；以及

执行所述调试者应用以配备所述加入装置。

117.如权利要求116所述的网状网络系统，其中，所述调试应用被配置成利用所接收到的指示来检索所述调试者应用。

118.如前述权利要求中的任一项所述的网状网络系统，其中，所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL。

119.如权利要求118所述的网状网络系统，其中，所述调试者应用通过互联网从云服务中检索。

120.如权利要求118所述的网状网络系统，其中，所述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中。

121.一种识别被允许加入网状网络的装置的方法，所述方法包括：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及

将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够识别所述装置被允许加入所述网状网络。

122.如权利要求121所述的方法，其中，所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16。

123.如前述权利要求中的任一项所述的方法，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

124.如权利要求121至123中的任一项所述的方法，其中，所述确定所述网状网络的所述操纵数据还包括：确定附加装置标识符的所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联。

125.如权利要求121至124中的任一项所述的方法，其中，所述传播所述操纵数据有效

地使得所述装置能够区分所述网状网络和其它网络。

126.如权利要求125所述的方法，其中，所述其它网络是IEEE802.15.4网络。

127.如权利要求121所述的方法，其中，所述操纵数据指示调试者在所述网状网络上是活动的。

128.一种被实现为调试装置的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及

将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够识别所述装置被允许加入所述网状网络。

129.如权利要求128所述的网状网络装置，其中，所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16。

130.如前述权利要求中的任一项所述的网状网络装置，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

131.如权利要求128至130中的任一项所述的网状网络装置，其中，用于确定所述网状网络的所述操纵数据的所述调试应用被配置成：确定附加装置标识符的所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联。

132.如权利要求128至131中的任一项所述的网状网络装置，其中，所述操纵数据能够由所述装置使用来区分所述网状网络和其它网络。

133.如权利要求132所述的网状网络装置，其中，所述其它网络是IEEE 802.15.4网络。

134.如权利要求128所述的网状网络装置，其中，所述操纵数据指示调试者在所述网状网络上是活动的。

135.一种网状网络系统，包括：

加入装置，所述加入装置被配置成请求加入网状网络；以及

所述网状网络的调试装置，所述调试装置被配置成：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及

将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够识别所述装置被允许加入所述网状网络。

136.如权利要求135所述的网状网络系统，其中，所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16。

137.如前述权利要求中的任一项所述的网状网络系统，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

138.如权利要求135至137中的任一项所述的网状网络系统，其中，用于确定所述网状

网络的所述操纵数据的所述调试装置被配置成：确定附加装置标识符的所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联。

139.如权利要求135至138中的任一项所述的网状网络系统，其中，所述操纵数据使得所述装置能够区分所述网状网络和其它网络。

140.如权利要求135所述的网状网络系统，其中，所述操纵数据指示调试者在所述网状网络上是活动的。(优先于GP-22882-01)

141.一种识别被允许加入网状网络的装置的方法，所述方法包括：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及

将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的所述值的集合与在所述装置处确定的值的第二集合进行比较，以识别所述装置被允许加入所述网状网络。

142.如权利要求141所述的方法，其中，所述确定所述操纵数据包括：

对所述装置标识符应用第一散列函数，以产生第一散列值；

对所述装置标识符应用第二散列函数，以产生第二散列值；

对所述第一散列值执行模运算，以确定所述布隆过滤器中的第一位字段位置；

对所述第二散列值执行所述模运算，以确定所述布隆过滤器中的第二位字段位置；

将所述布隆过滤器的所述第一位字段位置中的值设置为一；以及将所述布隆过滤器的所述第二位字段位置中的所述值设置为一。

143.如权利要求142所述的方法，其中，所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI。

144.如权利要求142所述的方法，其中，所述模运算的除数是所述布隆过滤器的位阵列的长度。

145.如前述权利要求中的任一项所述的方法，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

146.如权利要求141至144中的任一项所述的方法，其中，所述装置标识符是所述EUI-64的最低有效二十四位。

147.如权利要求141至146中的任一项所述的方法，其中，所述确定所述网状网络的所述操纵数据还包括：确定附加装置标识符的所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联。

148.如权利要求141所述的方法，还包括：

将所述操纵数据的所述值设置成零值，这禁用了针对所述网状网络的加入。

149.如权利要求141所述的方法，还包括：

将所述操纵数据中的所有位字段值设置成值为一，以指示所述网状网络对任何装置来说是能够加入的。

150.一种被实现为调试装置的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及

将所述操纵数据传播到所述网状网络中的一个或多个路由器，所述传播有效地使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的所述值的集合与在所述装置处确定的值的第二集合进行比较，以识别所述装置被允许加入所述网状网络。

151.如权利要求150所述的网状网络装置，其中，所述调试应用被配置成：

对所述装置标识符应用第一散列函数，以产生第一散列值；

对所述装置标识符应用第二散列函数，以产生第二散列值；

对所述第一散列值执行模运算，以确定所述布隆过滤器中的第一位字段位置；

对所述第二散列值执行所述模运算，以确定所述布隆过滤器中的第二位字段位置；

将所述布隆过滤器的所述第一位字段位置中的值设置为一；以及

将所述布隆过滤器的所述第二位字段位置中的所述值设置为一。

152.如权利要求151所述的网状网络装置，其中，所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI。

153.如权利要求151所述的网状网络装置，其中，所述模运算的除数是所述布隆过滤器的位阵列的长度。

154.如前述权利要求中的任一项所述的网状网络装置，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

155.一种网状网络系统，包括：

加入装置，所述加入装置被配置成请求加入网状网络；以及

调试装置，所述调试装置被配置成：

确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及

将所述操纵数据传播到所述网状网络中的一个或多个路由器，所述传播有效地使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的所述值的集合与在所述装置处确定的值的第二集合进行比较，以识别所述装置被允许加入所述网状网络。

156.如权利要求155所述的网状网络系统，其中，所述调试装置被配置成：

对所述装置标识符应用第一散列函数，以产生第一散列值；

对所述装置标识符应用第二散列函数，以产生第二散列值；

对所述第一散列值执行模运算，以确定所述布隆过滤器中的第一位字段位置；

对所述第二散列值执行所述模运算，以确定所述布隆过滤器中的第二位字段位置；

将所述布隆过滤器的所述第一位字段位置中的值设置为一；以及

将所述布隆过滤器的所述第二位字段位置中的所述值设置为一。

157.如权利要求156所述的网状网络系统，其中，所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI。

158.如权利要求156所述的网状网络系统，其中，所述模运算的除数是所述布隆过滤器的位阵列的长度。

159.如权利要求155至158中的任一项所述的网状网络系统，其中，所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

160.如权利要求155所述的网状网络系统，其中，用于确定所述网状网络的所述操纵数据的所述计算装置被配置成：确定附加装置标识符的所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加加入者装置相关联。

161.一种更新网状网络的节点中的调试数据的方法，所述方法包括：

在所述网状网络中的节点装置处接收调试数据集；

将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述节点装置中的调试数据集中的存储时间戳进行比较；

根据所述比较，确定所述存储时间戳比所接收到的时间戳更近；以及

响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

162.如权利要求161所述的方法，还包括：

根据所述比较，确定所接收到的时间戳比所述存储时间戳更近；以及

响应于所述确定所接收到的时间戳比所述存储时间戳更近，更新所存储的调试数据集，以和所接收到的调试数据集匹配。

163.如前述权利要求中的任一项所述的方法，其中，所接收到的调试数据集包括：

所接收到的时间戳；

调试证书；

所述网状网络的网络名称；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许。

164.如权利要求163所述的方法，其中，所接收到的时间戳包括时间值以及所述时间值对于协调世界时间UTC是能够追踪的的指示。

165.如权利要求161至164中的任一项所述的方法，其中，所述节点装置和所述领导者装置被先前调试到所述网状网络，并且其中，先前调试将相同的调试数据集存储在所述节点装置和所述领导者装置中。

166.如权利要求165所述的方法，其中，所述节点装置中所存储的调试数据集在所述网状网络的分割之后被更新，所述分割将所述网状网络分成多个分区，其中，所述网状网络的第一分区包括所述领导者装置，并且其中，所述网状网络的第二分区包括所述节点装置。

167.如权利要求166所述的方法，其中，所述分割停止所述网状网络上在所述节点装置与所述领导者装置之间的通信。

168.如权利要求166所述的方法，其中，所述在所述节点装置处接收所述调试数据集发

生在所述网状网络的所述第一分区和所述第二分区的合并之后，所述合并重新建立所述网状网络上在所述节点装置与所述领导者装置之间的通信路径。

169.如权利要求161至168中的任一项所述的方法，其中，所述节点装置是路由器装置或适于用作路由器的装置。

170.一种被实现为路由器的网状网络装置，所述网状网络装置包括：

网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；

用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：

接收调试数据集；

将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述路由器中的调试数据集中的存储时间戳进行比较；

根据所述比较，确定所述存储时间戳比所接收到的时间戳更近；以及

响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

171.如权利要求170所述的网状网络装置，其中，所述调试应用被配置成：

根据所述比较，确定所接收到的时间戳比所述存储时间戳更近；以及

响应于确定所接收到的时间戳比所述存储时间戳更近，更新所存储的调试数据集，以和所接收到的调试数据集匹配。

172.如前述权利要求中的任一项所述的网状网络装置，其中，所接收到的调试数据集包括：

所接收到的时间戳；

调试证书；

所述网状网络的网络名称；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许。

173.如权利要求172所述的网状网络装置，其中，所述接收时间戳包括时间值以及所述时间值对于协调世界时间UTC是能够追踪的的指示。

174.如权利要求170至173中的任一项所述的网状网络装置，其中，所述路由器和所述领导者装置被先前调试到所述网状网络，并且其中，先前调试将相同的调试数据集存储在所述路由器和所述领导者装置中。

175.如权利要求174所述的网状网络装置，其中，所述路由器中所存储的调试数据集在所述网状网络的分割之后被更新，所述分割将所述网状网络分成多个分区，其中，所述网状网络的第一分区包括所述领导者装置，并且其中，所述网状网络的第二分区包括所述路由器。

176.一种网状网络系统，包括：

领导者装置，所述领导者装置被配置成维持所述网状网络的调试数据；以及

路由器装置，所述路由器装置被配置成：

接收调试数据集；

将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述路由器中的调试数据集中的存储时间戳进行比较；

根据所述比较，确定所述存储时间戳比所接收到的时间戳更近；以及

响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

177.如权利要求176所述的网状网络系统，其中，所述路由器装置被配置成：

根据所述比较，确定所接收到的时间戳比所述存储时间戳更近；以及

响应于确定所接收到的时间戳比所述存储时间戳更近，更新所存储的调试数据集，以和所接收到的调试数据集匹配。

178.如前述权利要求中的任一项所述的网状网络系统，其中，所接收到的调试数据集包括：

所接收到的时间戳；

调试证书；

所述网状网络的网络名称；以及

安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许。

179.如权利要求178所述的网状网络系统，其中，所接收到的时间戳包括时间值以及所述时间值对于协调世界时间UTC是能够追踪的的指示。

180.如权利要求176所述的网状网络系统，其中，所述路由器和所述领导者装置被先前调试到所述网状网络，并且其中，所述先前调试将相同的调试数据集存储在所述路由器和所述领导者装置中。

网状网络调试

[0001] 发明人

[0002] Martin A.Turon

[0003] Grant M.Erickson

[0004] Christopher A.Boross

[0005] Jay D.Logue

[0006] 相关申请的交叉引用

[0007] 本申请根据美国法典第35条119(e)款要求2014年6月24日提交的美国临时专利申请序号62/016,450的优先权。本申请还要求2014年10月13日提交的美国临时专利申请序号62/063,135的优先权。本申请还要求2015年2月12日提交的美国临时专利申请序号62/115,601的优先权。本申请还要求2015年4月2日提交的美国临时专利申请序号62/141,853的优先权。

背景技术

[0008] 为了感测环境条件、控制设备并且向用户提供信息和警报，使用无线网状网络来将装置彼此连接并且连接到基于云的服务日益流行。然而，网状网络上的许多装置被设计成在电池电力上操作达延长时间段，这限制装置中的可用计算、用户接口和无线电资源。附加地，为了确保网状网络的安全，加入并在网状网络上操作的装置的身份被认证，并且网状网络内的通信基于被调试到装置中的证书而被加密。然而，随着网状网络的普遍性和规模不断增长，调试技术限制了对调试的用户体验的质量、将装置加入到正确的网状网络的准确性、将证书安全地注入到装置中、以及在调试期间将特定于装置和特定于应用的信息配备到装置中。

发明内容

[0009] 本发明内容被提供来引入网状网络调试的简化概念。简化概念在下面在具体实施方式中被进一步描述。本发明内容不旨在识别所要求保护的主题的必要特征，也不旨在用于在确定所要求保护的主题的范围时使用。

[0010] 描述了通常与在网状网络中加入节点有关的网状网络调试。在实施例中，加入者路由器能够从加入装置接收信标请求，然后从加入者路由器向加入装置传送信标，其中该信标提供网状网络能够用于加入的指示。所传送的信标还使得加入装置能够在该加入装置与加入者路由器之间建立本地链路。加入者路由器从请求加入网状网络的加入装置接收消息。从加入装置接收到的消息能够包括可用来对使用Juggling口令认证密钥交换(J-PAKE)或任何其它适合的密码套件来认证的加入装置进行认证的装置标识符，并且认证有效地在调试装置与加入装置之间建立安全的通信会话。加入者路由器将所接收到的消息转发到网状网络的调试装置，这能够包括在加入者路由器与调试装置之间的通信路径中通过网状网络的一个或多个路由器来转发所接收到的消息。在实施方式中，路由器中的一个路由器可以是将网状网络连接到外部网络的边界路由器，并且调试装置附连到外部网络。加入者路

由器然后从调试装置接收用于加入装置加入网状网络的授权，并且加入者路由器向加入装置传送网络信息，其中该网络信息使得加入装置能够加入网状网络。

[0011] 描述了通常与在网状网络中加入节点有关的网状网络调试。在实施例中，加入者路由器能够从加入装置接收信标请求，然后从加入者路由器向加入装置传送信标，其中该信标提供网状网络可用于加入的指示。所传送的信标还使得加入装置能够在该加入装置与加入者路由器之间建立本地链路。加入者路由器在被传送到网状网络的调试装置的DTLS中继接收通知消息中中继来自请求加入网状网络的加入装置的DTLS-客户端Hello消息。加入者路由器从调试装置接收DTLS中继传送通知消息，并且向加入装置传送该DTLS中继传送通知消息的内容，其中所述内容使得加入装置能够加入网状网络并且有效地在调试装置与加入装置之间建立安全的通信会话。加入者路由器从调试装置接收加入装置将被委托接收网状网络的网络证书的指示，并且接收在调试装置与加入装置之间共享的密钥加密密钥KEK。加入者路由器然后使用KEK来在媒体访问控制MAC层对消息进行加密和认证而将网络证书以及其它必要的网络参数从加入者路由器传送到加入装置以安全地传递网络证书。安全的通信会话可用来执行加入装置的配备。

[0012] 描述了通常与建立调试会话有关的网状网络调试。在实施例中，边界路由器从调试装置接收用于成为调试者以将装置加入到网状网络的请愿。边界路由器通告网状网络对于调试装置的可用性。响应于接收到通告，调试者响应于调试装置接收到通告而发送请愿。边界路由器能够将所接收到的请愿传送到网状网络的领导者装置，并且从该领导者装置接收对请愿的响应，其中该响应指示对请愿的接受或拒绝。边界路由器向调试装置传送对请愿的接受或拒绝的指示。请愿由领导者装置接受对调试装置进行授权以成为网状网络的调试者并且安全的调试会话被建立。对请愿的接受还使得领导者装置能够更新内部状态，所述内部状态跟踪网状网络的活动调试者，使得能够通过网状网络加入，传递被允许加入网状网络的装置的集合，并且在网状网络内传播调试数据集。

[0013] 在网状网络调试的其它方面中，边界路由器还能够注册调试装置的身份以建立安全的调试通信会话，包括向边界路由器提供硬化的(例如，加密散列的)调试证书，其中，经硬化的调试证书是从由用户输入到调试装置的调试证书通行码导出的。边界路由器包括可用来向网状网络对调试装置进行认证的加密调试证书的副本，其中加密调试证书的副本是先前从调试证书导出的。调试证书被注入到网状网络的导出了加密调试证书的副本的领导者装置中，并且领导者装置将加密调试证书的副本安全地传递到边界路由器。

[0014] 描述了通常与建立调试会话有关的网状网络调试。在实施例中，网状网络的领导者装置接收用于接受调试装置作为调试者来对要加入网状网络的加入装置进行调试的请愿。领导者装置能够确定接受还是拒绝所接收到的请愿，并且随着所接收到的请愿被接受还是拒绝的指示而向调试装置传送响应。关于接受还是拒绝从调试装置接收到的请愿的确定可以包括确保对网状网络来说存在单个活动调试者。响应于所接收到的请愿被接受的确定，领导者装置能够更新内部状态，所述内部状态跟踪网状网络的活动调试者。

[0015] 在网状网络调试的其它方面中，领导者装置能够从调试装置接收用于针对网状网络开始加入模式的命令，并且在网状网络内传播调试数据集。能够从在领导者装置的调试期间被注入到该领导者装置中的调试证书导出经硬化的调试证书。领导者装置能够向边界路由器发送加密调试证书的副本，使得边界路由器能够向网状网络认证调试装置。

[0016] 描述了通常与管理多个调试会话有关的网状网络调试。在实施例中，调试装置在该调试装置与网状网络的边界路由器之间建立安全的调试通信会话，以安全地建立网络通信会话以用于将一个或多个加入装置加入到网状网络。安全的调试通信会话由调试装置用来向网状网络的领导者装置发送用于请求接受调试装置作为网状网络的活动调试者的请愿，并且从领导者装置接收对请愿的接受的指示。调试装置能够激活针对网状网络的加入，并且接收来自要加入到网状网络的加入装置的请求。为了激活针对网状网络的加入，调试装置能够开始加入模式，所述加入模式使网状网络中的路由器通告网状网络正在接受加入请求。

[0017] 在网状网络调试的其它方面中，调试装置还能够向领导者装置发送用于使网状网络变得可加入的管理消息，其中该管理消息使得领导者装置能够更新网状网络的网络数据。管理消息能够包括操纵数据，所述操纵数据指示被允许加入到网状网络的加入装置。网络数据然后被传播到网状网络中的路由器装置，其中网络数据包括网状网络可用于加入的指示。加入装置与调试装置建立安全的加入者通信会话。调试装置使用加入装置的装置预共享密钥PSKd来对加入装置进行认证，并且将加入装置加入到网状网络。能够通过调试装置确定从加入装置接收到的加密装置标识符和由调试装置从作为调试装置的输入从用户接收到的装置标识符的副本所导出的加密装置标识符匹配、并且使用加密装置标识符作为共享秘密来使加入者通信会话安全而建立安全的加入者通信会话。

[0018] 能够经由加入者路由器从加入装置接收用于加入网状网络的请求，并且调试装置向加入者路由器发送加入装置将被委托接收网状网络的网络证书以及在调试装置与加入装置之间共享的密钥加密密钥(KEK)的指示。经由加入者路由器到加入装置的传输有效地使得加入者路由器能够使用所接收到的KEK来将网络证书安全地传送到加入装置以将加入装置调试到网状网络。从加入装置接收到的请求能够包括加入装置的加密装置标识符，其中加密装置标识符是使用Juggling口令认证密钥交换(J-PAKE)从加入装置的装置标识符导出的。

[0019] 描述了通常与提供加入装置有关的网状网络调试。在实施例中，调试装置能够在该调试装置与网状网络的边界路由器之间建立调试通信会话，并且还在加入装置与调试装置之间建立加入者通信会话。调试装置然后能够向加入装置发送调试信息，其中该调试信息可由加入装置用来加入网状网络。调试装置从加入装置接收调试者应用的位置的指示，利用所接收到的指示来检索调试者应用，并且执行调试者应用以配备加入装置。

[0020] 描述了通常与搜寻和操纵有关的网状网络调试。在实施例中，网状网络的调试装置能够确定网状网络的操纵数据，其中该操纵数据是与被允许加入网状网络的装置相关联的装置标识符的指示。调试装置然后能够将操纵数据从网状网络的调试装置传播到网状网络中的一个或多个路由器，并且操纵数据指示调试者在网状网络上是活动的。调试装置传播操纵数据使得一个或多个路由器能够在信标消息中传送操纵数据，并且该操纵数据有效地使得与装置标识符相关联的装置能够识别该装置被允许加入网状网络。在实施方式中，操纵数据是作为IEEE64位扩展唯一标识符(EUI-64)的装置标识符的16位循环冗余校验(CRC16)。调试装置能够通过针对与被允许加入网状网络的附加装置相关联的附加装置标识符来确定操纵数据而确定网状网络的操纵数据。调试装置传播操纵数据有效地使得所述装置能够区分网状网络和其它网络，其中其它网络是IEEE 802.15.4网络。

[0021] 描述了通常与搜寻和操纵有关的网状网络调试。在实施例中，网状网络的调试装置能够确定网状网络的操纵数据，其中该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示，并且该指示被表示为在布隆过滤器(bloom filter)中表示装置标识符的值的集合。调试装置然后能够将操纵数据从网状网络的调试装置传播到网状网络中的一个或多个路由器。传播操纵数据使得路由器能够在信标消息中传送操纵数据，其中该操纵数据使得与装置标识符相关联的装置能够将布隆过滤器中的值的集合与在该装置处确定的值的第二集合进行比较以识别该装置被允许加入网状网络。

[0022] 在网状网络调试的其它方面中，调试装置通过对装置标识符应用第一散列函数以产生第一散列值并且对装置标识符应用第二散列函数以产生第二散列值来确定操纵数据。装置标识符可以是IEEE 64位扩展唯一标识符(EUI-64)，其中装置标识符是EUI-64的最低有效二十四位。在实施方式中，第一散列函数和第二散列函数是循环冗余校验(CRC)，其中第一散列函数是CRC16-CCITT，并且第二散列函数是CRC16-ANSI。调试装置然后对第一散列值执行模运算以确定布隆过滤器中的第一位字段位置，并且对第二散列值执行模运算以确定布隆过滤器中的第二位字段位置。用于模运算的除数可以是布隆过滤器的位阵列的长度。调试装置能够将布隆过滤器的第一位字段位置中的值设置为一，并且将布隆过滤器的第二位字段位置中的值设置为一。调试装置能够将操纵数据中的位字段值中的全部设置成值为一以指示网状网络对任何装置来说是可加入的。替选地，调试装置能够将操纵数据的位字段值设置成值为零，这禁用针对网状网络的加入。

[0023] 描述了通常与在网状网络中划分节点有关的网状网络调试。在实施例中，网状网络中的节点装置接收调试数据集，并且将所接收到的调试数据集中的时间戳与被存储在节点中的调试数据集中的存储时间戳进行比较。节点装置能够根据比较确定存储时间戳比接收时间戳更近，并且作为响应，向网状网络的领导者装置传送消息，其中该消息包括所存储的调试数据集。领导者装置接受所存储的调试数据集作为网状网络的最近的调试数据集，并且将所存储的调试数据集传播到网状网络。替选地，节点装置能够确定接收时间戳比存储时间戳更近，并且响应于确定，更新所存储的调试数据集以和所接收到的调试数据集匹配。

[0024] 在网状网络调试的其它方面中，所接收到的调试数据集包括接收时间戳、调试证书、网状网络的网络名称以及指示哪些安全相关操作在网状网络中被允许的安全策略。接收时间戳包括时间值以及该时间值可追踪到协调世界时间(UTC)的指示。在实施例中，节点装置和领导者装置被先前调试到网状网络，并且先前调试将相同的调试数据集存储在节点装置和领导者装置中。能够在停止通过网状网络的节点装置与领导者装置之间的通信的网状网络的分割之后更新节点装置中所存储的调试数据集。分割使网状网络分开并且网状网络的第一分区包括领导者装置，并且网状网络的第二分区包括节点装置。节点装置能够在网状网络的第一分区和第二分区的合并之后接收调试数据集，其中所述合并在通过网状网络的节点装置与领导者装置之间重新建立通信路径。

附图说明

[0025] 参考以下附图描述网状网络调试的实施例。相同的附图标记在整个附图中被用来引用相同的特征和组件：

[0026] 图1图示其中能够实现网状网络调试的各种实施例的示例网状网络系统。

[0027] 图2图示其中能够实现网状网络调试的各种实施例的示例环境。

[0028] 图3A至图3D图示具有根据网状网络调试的实施例所实现的装置的示例网状网络环境的简化版本。

[0029] 图4图示根据网状网络调试的实施例的网状网络环境中的装置之间的数据事务的示例。

[0030] 图5图示根据网状网络调试的实施例的具有所建立的调试者会话和所建立的加入者会话的调试环境的示例。

[0031] 图6图示根据网状网络调试的实施例的用于建立调试者会话的网状网络环境中的装置之间的数据事务的示例。

[0032] 图7图示根据网状网络调试的实施例的用于建立加入者会话的网状网络环境中的装置之间的数据事务的示例。

[0033] 图8图示根据网状网络调试的实施例的使用布隆过滤器来对加入装置的装置标识符进行编码而生成的操纵数据的示例。

[0034] 图9图示根据网状网络调试的实施例的划分网状网络的示例。

[0035] 图10图示根据本文中所描述的技术的实施例的如通常与在网状网络中加入节点有关的网状网络调试的示例方法。

[0036] 图11图示根据本文中所描述的技术的实施例的如通常与在网状网络中加入节点有关的网状网络调试的另一示例方法。

[0037] 图12图示根据本文中所描述的技术的实施例的如通常与在网状网络中建立调试会话有关的网状网络调试的示例方法。

[0038] 图13图示根据本文中所描述的技术的实施例的如通常与在网状网络中建立调试会话有关的网状网络调试的另一示例方法。

[0039] 图14图示根据本文中所描述的技术的实施例的如通常与在网状网络中管理多个调试会话有关的网状网络调试的示例方法。

[0040] 图15图示根据本文中所描述的技术的实施例的如通常与在网状网络中配备加入装置有关的网状网络调试的示例方法。

[0041] 图16图示根据本文中所描述的技术的实施例的如通常与在网状网络中搜寻和操纵有关的网状网络调试的示例方法。

[0042] 图17图示根据本文中所描述的技术的实施例的如通常与在网状网络中搜寻和操纵有关的网状网络调试的另一示例方法。

[0043] 图18图示根据本文中所描述的技术的实施例的如通常与在网状网络中划分节点有关的网状网络调试的示例方法。

[0044] 图19图示根据本文中所描述的技术的实施例的其中能够实现网状网络的示例环境。

[0045] 图20图示根据本文中所描述的技术的一个或多个实施例的能够在网状网络环境中实现的示例网状网络装置。

[0046] 图21图示具有能够实现网状网络调试的实施例的示例装置的示例系统。

具体实施方式

[0047] 无线网状网络是具有以网状拓扑连接的无线节点的通信网络，所述网状拓扑为网状网络内的业务提供可靠且冗余的通信路径的。无线网状网络使用多个无线电链路、或跳来在网状网络内的装置之间转发业务。这为相比于由单个无线电链路所覆盖的区域大的区域提供覆盖范围。

[0048] 无线网状网络能够基于专有技术、或基于标准的技术。例如，无线网状网络可以基于IEEE 802.15.4标准，所述IEEE 802.15.4标准定义物理(PHY)层和媒体访问控制(MAC)层特征和服务以用于由在网状网络栈的更高层处的应用使用。上层应用使用这些标准定义的服务来跨网状网络实现应用级安全通信(例如，加密和认证)。

[0049] 虽然用于网状网络的基于标准的技术为安全通信提供服务，但是这些技术并未为网状网络的安全调试提供完整的解决方案。基于标准的解决方案可以假设装置是在安全网状网络带外调试的，并且留给应用开发人员设计。例如，带外调试解决方案包括在加入装置试图做出到网状网络的基于无线电的连接之前通过有线连接注入网络证书。替选地，网络证书在网状网络形成时通过不安全的无线电链路来发送。

[0050] 通过网状网络安全地调试加入装置消除了对专门调试工具的需要、加入装置上用于证书注入的附加接口、以及通过不安全的通信链路来传送证书的风险。各种实施例提供网状网络调试技术来改进加入网状网络的装置的调试。

[0051] 在连接到互联网的网络中使用的认证技术能够依靠使用由证书机构所发布的证书。证书能够被核实以对网络上的另一装置的身份进行认证。与互联网上的装置不同，网状网络中的装置可能不能够访问连接互联网的、基于证书的认证以便对用于调试的装置进行认证。描述了在无需外部证书机构的情况下向网状网络提供对调试装置和加入装置的安全认证的网状网络调试技术。

[0052] 用于网状网络的标准提供用于使网状网络内的通信安全的服务，诸如定义用于网状网络中的装置之间的通信的网络密钥(网络主密钥)和MAC层加密技术。然而，将证书(诸如网络密钥)插入到加入网状网络的装置中超出标准定义的PHY和MAC服务的范围。常常，在加入装置试图连接到网状网络之前使用用于初始地将证书加载到加入装置中的带外技术。描述了在通过网状网络的调试期间向加入装置安全地传递网络证书的网状网络调试技术。

[0053] 针对网状网络而设计的许多装置具有有限的用户接口能力，或者没有用户接口能力。网状网络装置上的有限的用户接口使加入装置的键入信息(诸如通行码、装置标识符、和/或装置地址)对用户来说麻烦且易出错。描述了在将加入装置调试到网状网络期间提高用户效率和数据输入准确性的网状网络调试技术。

[0054] 随着使用网状网络的系统变得日益普遍，可能需要在网状网络的调试期间添加许多加入装置。尤其当需要调试或者再调试大量的加入装置时，许多网状网络装置的有限资源和用户接口导致长且代价高的调试。描述了提高将加入装置调试到网状网络的可伸缩性的网状网络调试技术。

[0055] 无线网状网络可以使用许可或未许可(也被称为免许可或无许可)无线电谱。标准(诸如IEEE 802.15.4)定义了使得多个网状网络能够在未许可谱的带内操作的未许可无线电谱(诸如信道频率)、信道带宽、数据速率、调制、接入技术等的使用。描述了在多个网状网

络共享相同的无线电谱和/或底层工业标准联网协议的环境中将加入装置安全地加入到正确的网状网络的网状网络调试技术。

[0056] 除在调试期间将网络证书插入到加入装置中之外，对加入装置来说可能需要附加配备，以便更新或者配置加入装置以用于在网状网络中使用。这个配备可能需要信息的安全通信，诸如将加入装置链接到云服务的用户账户等。描述了用于在调试期间安全地配备加入装置的网状网络调试技术。

[0057] 虽然能够在任何数目的不同环境、系统、装置、和/或各种配置中实现所描述的用于网状网络调试的系统和方法的特征和构思，但是在以下示例装置、系统、和配置的场境中对网状网络调试的实施例进行描述。

[0058] 图1图示其中能够实现网状网络调试的各种实施例的示例网状网络系统100。网状网络100是包括路由器102、适于用作路由器的终端装置104、以及终端装置106的无线网状网络。路由器102、适于用作路由器的终端装置104、以及终端装置106各自包括网状网络接口以用于通过网状网络通信。路由器102通过网状网络接口来接收和传送分组数据。路由器102还跨网状网络100路由业务。如在下面所讨论的，路由器102以及适于用作路由器的终端装置104能够假设各种角色、和角色的组合，以便在网状网络100内调试。

[0059] 适于用作路由器的终端装置104位于网状网络拓扑的叶节点处，并且并未活动地将业务路由到网状网络100中的其它节点。适于用作路由器的装置104能够在该适于用作路由器的装置104连接到附加装置时成为路由器102。终端装置106是能够使用网状网络100来通信但是缺少除简单地转发到其父路由器102之外的在网状网络100中路由业务的能力的装置。例如，电池供电的传感器是一种终端装置106。

[0060] 路由器102、适于用作路由器的终端装置104、以及终端装置106包括被用来将这些装置的身份认证为网状网络100的成员的网络证书。路由器102、适于用作路由器的终端装置104、以及终端装置106还使用网络证书来对网状网络中的通信进行加密。

[0061] 图2图示其中能够实现网状联网调试技术的各种实施例的示例环境200。该环境200包括网状网络100，其中一些路由器102正在网状网络100中执行特定角色。如由虚线所图示的网状网络100内的装置正在使用网络证书通过网状网络100安全地通信。在网状网络100外部示出的装置不具有网状网络100的网络证书的副本，并且不能够使用网状网络层安全来安全地通信。

[0062] 边界路由器202(也被称为网关和/或边缘路由器)是路由器102中的一个。边界路由器202包括用于与网状网络100外部的外部网络通信的第二接口。边界路由器202通过外部网络连接到接入点204。例如，接入点204可以是以太网路由器、Wi-Fi接入点，或用于桥接不同类型的网络的任何其它适合的装置。接入点204连接到诸如互联网的通信网络206。经由通信网络206连接的云服务208提供与网状网络100内的装置有关的服务并且/或者使用网状网络100内的装置来提供服务。作为示例而非限制，云服务208提供包括将终端用户装置(诸如智能电话、平板等)连接到网状网络100中的装置、处理在网状网络100中获取的数据并将其呈现给终端用户、将一个或多个网状网络100中的装置链接到云服务208的用户账户、配备并更新网状网络100中的装置等的应用。

[0063] 选择调试新装置加入网状网络100的用户能够使用经由接入点204的外部网络技术连接到边界路由器202的调试装置210来调试该新装置。调试装置210可以是具有适合的

用户接口和通信能力以按调试者的角色操作来将装置加入到网状网络100的任何计算装置，诸如智能电话、平板、笔记本计算机等。为了成为网状网络100的调试者，调试装置210请愿成为调试者，如在下面更详细地描述的。

[0064] 加入装置212是用户选择要加入到网状网络100的任何适于用作路由器的终端装置104或终端装置106。在调试之前，加入装置212尚未接收到网状网络100的网络证书并且不能够被向网状网络100认证或者通过网状网络100安全地通信。如在下面详细地描述的，在调试期间，加入装置212执行加入者(或加入装置)的角色。

[0065] 路由器102中的一个在对要加入网状网络100的加入装置212进行调试期间执行加入者路由器214的角色。加入者路由器214的角色能够由在加入装置212的一个无线电链路内的任何路由器102来执行。如在下面详细地描述的，加入者路由器214向加入装置212提供仅本地无线电链路以用于加入者会话。

[0066] 路由器102中的一个执行网状网络100的领导者216的角色。领导者216管理路由器标识符指派，并且领导者216是网状网络100的网络配置信息的中央仲裁者。领导者216还控制哪一个调试装置210在任何给定时间被接受为网状网络100的单一活动调试者。

[0067] 如图2中所示的环境200示出了仅执行上面所描述的各种角色中的单个角色的装置。如在下面示出并描述的图3A至图3D通过示例而不限制地图示网状网络调试技术的调试角色的其它分配。

[0068] 图3A图示示例环境200的简化版本300，其中为了简洁起见示出了仅具有特定于调试的角色的那些装置。在这个示例中，图3A中的每个装置正在网状网络调试的实施例中执行单个调试的角色。图3A还图示在调试过程期间使用的通信链路。在已经被加入到网状网络100的装置之间使用安全的网状通信链路302。建立不安全的仅本地无线电链路304来将加入装置212连接到加入者路由器214，以用于将加入装置212调试到网状网络100。外部网络306具有如所示的通信链路，诸如通过外部网络的边界路由器202与调试装置210之间的点对点链路308。

[0069] 图3B还图示示例环境200的简化版本320，并且示出作为边界路由器202附加地执行合并器路由器214的角色的边界/加入者路由器322。图3C还图示示例环境200的简化版本340，并且示出作为附加地执行调试装置210的角色的边界路由器202的调试者/边界路由器342。在这个示例中，调试者/边界路由器342包括网状网络接口。调试者/边界路由器342还可以被称为网上调试者，因为该调试者/边界路由器342连接到网状网络100。

[0070] 图3D还图示示例环境200的简化版本360，并且示出作为附加地执行加入者路由器214和调试装置210的角色的边界路由器202的调试者/边界路由器/加入者路由器362。图3A至图3D图示网状网络调试角色的可能组合的例子，其中任何适于用作路由器的终端装置104装置能够执行多个角色(除加入装置212的角色外)。

[0071] 图4通过示出在网状网络100中正在执行各种网状网络调试角色的装置之间的事务来图示调试过程400。调试过程400在调试装置210(例如移动电话)根据来自边界路由器202的通告402发现网状网络100可用于调试者时开始。调试装置210然后使用调试者的预共享密钥(PSKc)来与边界路由器202建立安全的套接字连接。这个安全的连接建立调试会话404。可能一次存在仅一个活动调试者，所以调试装置210通过向边界路由器202发送请愿406来向领导者216请愿成为网状网络100的活动调试装置210，所述请愿406进而被边界路

由器202作为请求408转发到领导者216。

[0072] 如果领导者216接受调试装置210作为活动调试者，则该领导者向边界路由器202发送请愿响应410，所述边界路由器202进而向该调试装置发送请愿响应412。领导者216还通过在网状网络100上传播更新的网络数据414来向网状网络100上的装置指示存在活动调试者。

[0073] 一旦作为调试者活动，调试装置210就使得能实现针对网状网络100的加入。可选地，调试装置210提供指示期望加入网状网络100的加入装置212的装置标识符的操纵数据。调试装置210还可以查询并设置诸如网络名称和安全配置的网络参数。

[0074] 加入装置212向加入者路由器214发送用于建立加入者会话的请求416，所述加入者路由器214然后将来自加入装置212的请求418中继到边界路由器202。应该注意，中继请求418可以在加入者路由器214与边界路由器202之间由网状网络中的任何数目的路由器102转发。边界路由器202向调试装置210转发用于建立加入者会话的请求420。调试装置210向边界路由器202发送对针对加入者会话的请求的响应422，所述边界路由器202进而将该响应424中继到加入者路由器214。加入者路由器214在426处完成加入者会话的建立。为了简洁起见图4中的加入者会话的建立是以简化方式示出的；附加中继的DTLS消息可以作为DTLS握手的一部分被交换来建立加入者会话。

[0075] 如在416至426处所示，加入装置212和调试装置210利用加入装置212的装置预共享密钥(PSKd)使用数据报传输层安全(DTLS)或传输层安全(TLS)来执行握手。如在下面详细地描述的，握手是经由网状网络100通过中继执行的。调试装置210从自网状网络100带外接收到的(通常通过调试装置210的用户接口(诸如通过扫描QR码或条形码)而键入的)加入装置证书导出PSKd。一旦握手完成，从PSKd产生的共享秘密就被用来建立加入者会话并且将网状网络100的网络证书从加入者路由器214传递给加入装置212。可选地，除传递网状网络100的网络证书之外，调试者会话和加入者会话还可以被用来配备加入者，如在428处所示。

[0076] 图5图示具有所建立的调试者会话和所建立的加入者会话的调试环境500。调试者会话502是从调试装置210到边界路由器202的安全通信隧道。加入者会话504是从调试装置210到加入装置212的安全通信隧道。为了简洁起见，省略了其它网状通信链路和外部网络通信链路。

[0077] 第一装置配对

[0078] 为了将装置加入到网状网络100，第一装置被调试来建立用于调试装置加入网状网络100的调试证书以及用于网状网络100的安全操作的网络证书。调试装置210连接到可以为任何适于用作路由器的终端装置104的第一装置。第一装置是在网状网络100带外调试的。可以使用任何适合的连接(诸如USB、自组织Wi-Fi、蓝牙、点对点IEEE802.15.4等)来将第一装置连接到调试装置210。

[0079] 一旦调试装置210连接到第一装置，该调试装置就将用于网状网络100的PSKc和网络名称编程到第一装置中。如在上面并在下面所描述的，PSKc被用来向网状网络100认证调试装置210并且建立调试会话。网络名称具有人类可读的形式，与Wi-Fi网络中的服务集标识符(SSID)类似。一旦第一装置被调试，该第一装置就成为网状网络100的领导者216。第一装置形成网状网络100，包括确定网状网络100的唯一个域网标识符(PAN ID)和唯一扩展

PAN ID(XPANID)以及网状网络100的网络密钥。

[0080] PSKc是从调试证书导出的，所述调试证书是由管理网状网络100的用户键入到调试装置210中的人为可调节通行码。调试证书被硬化(例如，通过多次密码散列)以导出由领导者216和调试装置210所存储的PSKc。任何适合的密码散列技术可以被用来导出PSKc。

[0081] 为了改进PSKc的安全，可以应用密码技术来相对于由用户键入的等效人为可调节的调试证书通行码来增加在所导出的PSKc中的调试证书的平均信息量。通过使用密钥展开，能够将所导出的密钥安全地存储在嵌入式节点上，该嵌入式节点可能被以物理方式损害的，而用户的通行码不会被损害。这是有用的，因为用户常常将通行码重新用于多个网站和账户。例如，任何适合的密码技术(诸如应用多次密钥散列)被用来使密钥展开。例如，基于口令的密钥导出函数2(PBKDF2)能够被用来应用基于高级加密标准密码的消息认证码伪随机函数-128(AES-CMAC-PRF-128)。例如，可以像等式1中所示的那样导出PSKc。

[0082] PSKc＝PBKDF2(PRF,P,S,c,dkLen) (1)

[0083] 其中，PRF是要由PBKDF2使用的类型伪随机函数，P是调试证书，S是密码函数的盐(例如，诸如与网络名称级联的网络类型的串)，c是PRF的迭代次数，并且dkLen是所导出的密钥(PSKc)的期望长度。

[0084] 建立调试会话

[0085] 图6通过示出调试装置210、边界路由器202、与领导者216之间的事务来图示建立调试者会话的过程600。网状网络100可以具有有限数目的活动调试装置210，但是可以存在能够执行调试者的角色的多个潜在的调试装置210。领导者216负责确保对网状网络100来说仅存在活动调试者的有限集。作为示例而非限制，活动调试者的有限集可以限于单个活动调试者。为了成为活动调试者，调试装置210请愿领导者216成为网状网络的调试者。

[0086] 在602处，边界路由器202在外部网络接口上通告网状网络100可用于调试装置210。边界路由器202可以在服务发现协议内响应于多播请求(即，扫描或查询)而做出通告。例如，可以使用任何适合的服务发现(诸如多播域名服务(mDNS))来完成通告602。具体地，对于无线网络，边界路由器202经由统一资源定位符(URL)使用DNS服务发现(DNS-SD)来通告调试服务。查找服务器然后将对可访问的所有不同的无线网络、网状网络100的网络名称、以及调试端口做出响应。

[0087] 调试装置210通过为调试装置210与边界路由器202之间的调试会话请求安全的连接来对来自边界路由器202的通告做出响应604。例如，能够以任何适合的方式建立调试会话，诸如使用PSKc来建立使用DTLS或TLS的调试会话。作为示例而非限制，调试装置210和边界路由器202交换DTLS消息606-616以向网状网络100识别和认证调试装置，并且为调试者会话建立安全的连接。

[0088] 调试会话可以使用任何适合的网络端口，诸如作为调试会话的源端口和目的地端口两者的用户数据报协议(UDP)或传输控制协议(TCP)端口。例如，调试会话使用在网络发现期间发现的调试端口。每个边界路由器202能够指派调试端口或者使用默认调试端口。

[0089] 为了成为网状网络100的活动调试者，调试装置210请愿618领导者216以请求成为调试者。使用调试会话，调试装置210向边界路由器202发送用于成为网状网络100的活动调试者的请愿620。边界路由器202将请愿622转发到领导者216。例如，在调试装置210被认证和识别之后，边界路由器202向领导者216单播调试者请愿请求消息620(例如，COMM_

PET.req)。调试者请愿请求作为请求调试装置210被接受为网状网络100的活动调试装置210的请求622(例如,作为LEAD_PET.req)被边界路由器202转发到领导者216。例如,调试者请愿请求消息(包括调试者标识串)被通过网状网络100安全地发送。

[0090] 领导者216确定对网状网络100来说是否存在活动调试者。如果存在活动调试者,则领导者拒绝来自调试装置210的请愿。如果对网状网络100来说不存在活动调试者,则领导者216接受来自调试装置210的请愿。如果调试数据集反映存在活动调试者以及调试装置210的身份,则领导者216更新其副本。领导者216将网状网络100的准许加入标志设置为真。领导者216然后将网络数据以及经更新的调试数据集传播624到网状网络100,这指示网状网络100是可加入的。

[0091] 例如,领导者216将通过接受或者拒绝调试装置210作为网状网络100的活动调试者来对调试者请愿请求消息做出响应。在接受时,领导者216将用新调试者信息更新其网络数据的副本,将准许加入标志设置为真,并且使用任何适合的协议(诸如低功率有损网络多播协议(MPL))或者多播MLE-UPDATE消息来通过网状网络100传播经更新的网络数据和调试数据集。

[0092] 潜在的加入者路由器214(即,路由器102以及适于用作路由器的终端装置104)存储由领导者216所传播的经更新的网络信息和调试数据集。经更新的网络信息和调试数据集允许与调试装置210的直接通信以用于在调试任何加入装置212时使用。调试数据集包括边界路由器定位符(RLOC),所述边界路由器定位符(RLOC)允许任何装置向正作为活动调试者的代理的当前的活动边界路由器202发送消息。

[0093] 在确定接受还是拒绝来自调试装置210的请愿之后,领导者216以其对边界路由器202的决定的指示进行响应626。边界路由器202向调试装置210发送响应628,响应628包括领导者216接受或者拒绝请愿的决定的指示。例如,领导者216向边界路由器202发送指示该领导者216接受或者拒绝调试装置210作为网状网络100的活动调试者的决定的领导者请愿响应消息(例如,LEAD_PET.rsp)。响应于从领导者216接收到领导者请愿响应消息,边界路由器202将向调试装置210发送指示领导者216接受或者拒绝调试装置210作为网状网络100的活动调试者的决定的调试者请愿响应消息(例如,COMM_PET.rsp)。

[0094] 替选地,如在630处所示,领导者216在接受调试装置210成为活动调试者的请愿之后,将准许加入标志设置为真,但是等待接收包括来自调试装置210的指示的设置管理数据请求消息632(例如,MGMT_SET.req)以允许领导者216将经更新的网络数据传播到网状网络100。领导者216用设置管理数据响应消息634(例如,MGMT_SET.rsp)回复调试装置,以肯定用于传播经更新的网络数据的请求。领导者216将网络数据以及经更新的调试数据集传播636到网状网络100,这指示网状网络100是可加入的。

[0095] 在调试装置210发送设置管理数据请求消息(Set Management Data Request message)以允许领导者216传播经更新的网络信息之前,调试装置210可以管理网状网络100,诸如配置装置、改变网络设置等,而无需使网状网络100可加入。调试数据集包括调试会话标识符、调试数据集时间戳、和PSKc。当调试装置210是网状网络100上的活动调试者时,调试数据集还包括边界路由器202的位置。当网状网络100是可加入的时,调试数据集还包括指示哪些加入装置212被允许加入网状网络100的操纵数据。当网状网络100是可加入的时,网状网络100中的路由器102将准许加入标志和操纵数据包括在由路由器102所传送

的信标中。

[0096] 调试装置210可以包括网状网络接口，从而使得调试装置210能够作为网状网络100上的本机调试者操作。当在信标中设了本机调试者位并且调试装置210包括网状网络接口时，调试装置210可以请愿领导者216成为网状网络100的活动调试者。

[0097] 一旦被接受为活动调试者，调试装置210就可以使用设置管理数据请求消息(Set Management Data Request message)和得到管理数据响应消息(Get Management Data Request message)来管理网络以得到和设置网状网络100的网络参数。网络参数包括网状网络100的PSKc、网络名称、网络密钥、网络密钥顺序号、网络PAN ID、网络扩展PAN ID、网络唯一本地地址(ULA)和/或无线电信道。设想了附加的管理能力，诸如用于从网状网络100中驱逐出先前加入的装置的设施。设置管理数据请求消息和得到管理数据响应消息是通过调试会话经由边界路由器202中继到领导者216的。因为用于得到和设置网络参数命令的消息影响全局全网络状态，所以这些消息被转发到领导者216并且由领导者216存储。任何装置能够将用于获得网络信息的请求直接寻址到领导者216并且避免多跳寻址。

[0098] 建立加入者会话

[0099] 为了将新装置安全地调试到网状网络100，在调试装置210与加入装置212之间建立加入者会话。加入者会话是在调试装置210与加入装置212之间通过网状网络100的通信隧道。加入装置证书是被用来认证加入装置212有资格加入网状网络100的人为可调节的通行码。加入装置证书通过任何适合的带外机制在加入装置212与调试装置210之间被传递。例如，可以通过采用包括在调试装置210中的相机来扫描位于加入装置212上的QR码或条形码、通过将加入装置212的序列号键入到调试装置210的用户接口中等来传递加入装置证书。

[0100] 图7通过示出调试装置210、边界路由器202、加入者路由器214与加入装置212之间的事务来图示建立加入者会话的过程700。在一些实施例中，建立加入者会话始于加入装置212扫描无线电信道，诸如IEEE 802.15.4规范中所定义的信道，以找到要加入的潜在的网状网络100。加入装置212向在信道扫描期间找到的每个网状网络100发出信标请求702，所有网状网络100将对该信标请求702做出响应。

[0101] 例如，加入装置212通过在每个信道上传送802.15.4MAC-BEACON.request来执行主动扫描。响应于接收到信标请求，加入者路由器214传送包括用于协助加入装置212发现要加入的正确的网状网络100的操纵数据的信标响应704。加入者路由器214传送将操纵数据包括在802.15.4 MAC-BEACON.response的有效负荷中的802.15.4 MAC-BEACON.response。在下面更详细地描述生成、传送、并使用操纵数据的细节。一旦加入装置212已经找到要加入的网状网络100，该加入装置212就建立到加入者路由器214的仅本地无线电链路，其是不安全的点对点通信链路。

[0102] 例如，加入装置212通过配置从自信道扫描接收到的信标搜集的MAC层网络参数(例如，信道、PAN ID等)来建立到加入者路由器214的仅本地无线电链路706。加入装置212在加入者路由器214的不安全的接口(例如，端口号5684″:coaps″)上向加入者端口(例如，UDP端口)发送分组以建立仅本地无线电链路。还在信标中传递加入者端口。如果加入者端口丢失，则默认端口被加入装置212使用。

[0103] 加入装置212向加入者路由器214发送用于加入网状网络100的请求。在收到用于

加入网状网络100的请求后，加入者路由器214发送对加入到调试装置210的权限的请求。加入者路由器214在不安全的加入者端口上转发由加入装置212所发送的所有业务。加入者路由器214不处理或者理解被调试装置210所理解的DTLS握手的内容。在一些实施例中，加入者路由器214可以在其存储器中存储调试装置210或边界路由器202(该调试装置210的代理)的位置，从另一装置(例如，领导者216或边界路由器202)或某个其它位置(例如，远程服务)中检索调试装置210的位置。PSKd被用来向网状网络100认证加入装置212并且使调试装置210与加入装置212之间的加入者会话安全。PSKd是从加入装置证书导出的。

[0104] 在一些实施例中，可以使用DTLS以及认证协议(诸如Juggling口令认证密钥交换(J-PAKE)、安全远程口令(SRP)协议、和/或任何其它适合的口令认证密钥交换协议)来建立加入者会话。例如，使用NIST P-256椭圆曲线的J-PAKE椭圆曲线变体(EC-JPAKE)可以被用于认证和密钥协定。与PSKd一起使用J-PAKE证明正在调试加入装置212的用户物理上占有加入装置212，以及证明调试装置210通过加入者会话连接到正确的加入装置212。

[0105] 加入者路由器214将通过加入者会话从加入装置212接收到的用于加入网状网络100的请求转发到调试装置210。在授权加入网状网络100后，网络密钥被使用加入者会话从调试装置210安全地转移到加入装置214。

[0106] 例如，加入装置212可以向加入者路由器214发送加入者标识消息来为加入装置212提供人类可读的名称。加入者路由器214使用调试者前缀、泛播地址、或边界路由器定位符来将加入者标识消息中的信息封装在中继消息中并且将该中继消息转发到边界路由器202。在收到中继消息后，边界路由器202将发送方地址(在这种情况下是加入者路由器214的地址)附加到在中继消息结尾的下一个中继地址的列表，并且通过加入者会话来转发该中继消息。

[0107] 例如，加入装置212使用DTLS和UDP向加入者路由器214发送握手消息708。加入者路由器214将DTLS握手消息710中继到边界路由器202以用于递送给调试装置210。加入者路由器214不知道已中继的DTLS握手消息的内容。加入者路由器214基于同意上面所描述的加入者UPD端口来过滤通过不安全的仅本地无线电链路从加入装置212接收到的已接收到的DTLS握手消息。加入者路由器214中继在所指定的加入者UDP端口上接收到的所有消息。加入者路由器214可以速率限制不安全消息的转发，以防止网状网络100上的拒绝服务(DOS)攻击。

[0108] 通过另一个示例，加入装置212最初通过向加入者路由器214发送DTLS-客户端Hello消息来向调试装置210识别它本身。这个初始DTLS-客户端Hello旨在允许调试装置210给加入装置212指派DTLS cookie以用于在调试交换的剩余部分期间使用。加入者路由器214将DTLS-客户端Hello UDP有效负荷封装在DTLS中继接收通知消息(例如，RLY_RX.ntf)中，从而添加作为中继跳的已封装分组的源地址，在这种情况下是加入装置212的链路本地64位地址。DTLS cookie被发送到加入装置212，加入装置212然后将所述DTLS cookie返回给调试装置210以确保加入装置212是原来的。

[0109] 加入者路由器214还将其地址作为中继点添加到DTLS中继接收通知消息。加入者路由器214将DTLS中继接收通知消息发送到边界路由器202。边界路由器202在收到DTLS中继接收通知消息时，通过调试会话将该DTLS中继接收通知消息712转发到调试装置210。

[0110] 基于从加入装置212接收到的加入者标识消息，调试装置210使用该加入者标识消

息来基于PSKd发起DTLS-Hello验证消息。在714处，DTLS-Hello验证消息和DTLS中继传送通知消息(例如，RLY_TX.ntf)被发送到边界路由器202。在716处，边界路由器202将DTLS-Hello验证消息和DTLS中继传送通知消息中继到加入者路由器214。在718处，加入者路由器214将DTLS-Hello验证消息发送到加入装置212。

[0111] 替选地，调试装置210可以具有将要被调试的多个加入装置212的信息。调试装置210在从多个加入装置212中的特定一个接收到DTLS-客户端Hello消息后，检查发送了DTLS-客户端Hello消息的加入装置212的IEEE 64位扩展唯一标识符(EUI-64)地址。调试装置210在将被调试的多个加入装置212的信息中查找PSKd，以针对特定加入装置212继续DTLS握手。调试装置210经由加入者路由器214将组合的DTLS-ServerHello、DTLS-ServerKeyEx和DTLS-ServerHelloDone中继回到加入装置212。在完成这个DTLS握手后，加入者会话的建立完成。

[0112] 一旦调试装置210已经对加入装置212进行了认证，调试装置210就把网状网络100的网络证书委托给加入装置212。例如，调试装置210从边界路由器202请求网络证书，并且通过加入者会话在通过DTLS中继传送通知消息在调试会话上传输的加入者委托消息中将网络证书发送到加入装置212。替选地，调试装置210使用密钥交换密钥(KEK)作为调试装置210与加入装置212之间的共享秘密来把网状网络100的网络证书委托给加入装置212。KEK被发送到加入装置212的加入者路由器214，并且被用来对网络证书进行加密以便通过仅本地无线电链路传输。

[0113] 加入装置配备

[0114] 当加入装置212被加入到网状网络100时，加入装置212还可能需要配备。配备可以包括更新加入装置212中的固件、配置加入装置212、提供与网状网络100上的其它装置有关的本地配置、将加入装置212链接到云服务208上的用户账户、将加入装置212链接到基于云的应用服务器等。虽然仍然被建立，但是调试者会话和加入者会话被用来在加入装置212使用网络证书来加入网状网络100之前提供用于配备加入装置212的安全的连接。

[0115] 加入装置212发送要由调试装置210执行以执行加入装置212的配备的调试者应用的位置的指示。位置的指示可以被用来在调试装置210的存储器中查找调试者应用，或者可以由调试装置210用来从云服务208中检索调试者应用。指示可以具有任何适合的形式，例如统一资源定位符(URL)。当加入装置212的配备结束时，加入装置212终止加入者会话和仅本地无线电链路。加入装置212使用网络证书来加入网状网络100。

[0116] 操纵数据

[0117] 无线网状网络可以共享无线电谱。标准(诸如IEEE 802.15.4)定义了使得多个网络能够在无线电谱的带内操作的多个信道。附加地，当存在许多装置要调试到网状网络100时，期望使用信标中的操纵数据来高效地传递许多加入装置212的多个装置标识符，以协助加入装置212搜寻正确的网状网络100来加入。描述了在多个网状网络共享相同的无线电谱和/或底层工业标准联网协议的环境中将多个加入装置212安全地加入到正确的网状网络100的网状网络调试技术。

[0118] 当调试装置210获得期望的加入装置212的PSKd和EUI-64 MAC地址时，调试装置210构造将向所期望的加入装置212发信号通知要加入哪一个网状网络100的操纵数据。该操纵数据将包括用于区分网状网络100和其它基于802.15.4的网络的一些方式、用于传递

是否在网状网络100上存在活动调试者的方式、以及用于指定哪些加入装置212当前被允许加入网状网络100的方式。

[0119] 操纵数据由调试装置210确定并且指示被允许加入网状网络100的一个或多个加入装置212的装置标识符。调试装置210将操纵数据传播到网状网络100中的路由器102。路由器102进而将操纵数据包括在网状网络100的信标中，随着网状网络100是可加入的并且潜在的加入装置212是否被允许加入网状网络100的指示而发送该信标以将操纵数据提供给潜在的加入装置212。例如，如上面所讨论的，调试装置210获得所期望的加入装置212的PSKd和EUI-64 MAC地址。根据这个EUI-64，调试装置210构造操纵数据以向所期望的加入装置212发信号通知所期望的加入装置212被允许加入网状网络100。

[0120] 在另一个示例中，操纵数据可以包括被允许加入网状网络100的加入装置212的16位循环冗余校验(CRC16)编码的EUI-64地址的列表。CRC16在CRC16编码地址中的两个不同的EUI-64地址之间的冲突机率低的情况下提供EUI-64地址的紧凑表示。CRC16的使用使得适当的加入装置212能够高效地找到要加入的正确的网状网络100，同时通过减小加入装置212的装置标识符的所需信标有效负荷的大小来高效地使用网状网络100的资源。

[0121] 在多个网状网络100具有活动调试者的情况下，加入装置212通过从主动扫描中收集信标来搜寻正确的网状网络100。加入装置212丢弃从非网状网络收集的信标、具有错误协议的信标、具有错误版本的信标、具有错误XPANID的信标、具有错误网络名称的信标、和/或具有其中加入被禁用的信标的信标。加入装置212在已收集的信标的操纵数据中对与加入装置212的装置标识符具有确切匹配的所收集的信标进行优先级排序，并且按照最好信号强度的顺序对匹配的、所收集的信标进行次优先级排序。加入装置212试图加入优先网络，一次一个(如上所述)，直到加入装置212成功地加入网状网络100为止。如果加入装置耗尽网络的优先列表而未成功地加入网状网络100，则加入装置212可以执行主动扫描以立即或者在延迟时段之后开始再次搜寻网状网络100。

[0122] 操纵数据指导哪些加入装置212可以或者可以不试图加入网状网络100。附加地，可以将操纵数据中的所有位设置成值为零以指示网状网络100不可用于加入。替选地，可以将操纵数据中的所有位设置成值为一以指示网状网络100可用于由任何加入装置212加入。

[0123] 一些调试装置210可能缺少用于通过扫描QR码容易地提取EUI-64和加入装置证书的资源。在这种情况下，当确定操纵数据时，EUI-64的最低有效24位被用作加入装置212的装置标识符。信标中的S位表示加入装置212的短或长装置标识符是否被用来确定操纵数据。当EUI-64被用作用于确定操纵数据的装置标识符时，S位被设置成值为零。当EUI-64的最低有效24位被用作用于确定操纵数据的装置标识符时，S位被设置成值为一。

[0124] 图8图示被用来将加入装置212的装置标识符编码到操纵数据中的使用布隆过滤器来生成的操纵数据的示例800。布隆过滤器在不同的装置标识符的已编码值之间的冲突概率低的情况下提供对装置标识符的高效编码。要包括在操纵数据中的每个装置标识符802由第一散列函数804编码以产生第一散列值并且由第二散列函数806编码以产生第二散列值。例如，第一散列函数804是CRC16-CCITT并且第二散列函数806是CRC16-ANSI。装置标识符802是加入装置212的EUI-64。替选地，EUI-64的二十四个最低有效位被用作装置标识符802。

[0125] 对第一散列值并且对第二散列值执行模运算808。用于模运算的除数是布隆过滤

器的位阵列810的长度(位阵列810中的位位置被示出在812处,并且位值被示出在814处)。位阵列中的每个位在确定操纵数据之前被初始化成值为零。每个模运算的结果确定位阵列中的位置。位阵列中两个确定的位置中的值被设置成值为一,并且两个确定的位字段提供到装置标识符的映射。

[0126] 例如,对于假想的装置标识符802,对第一散列函数804的结果执行模运算808对装置标识符802来说结果是值为三。对第二散列函数806的结果执行模运算808对装置标识符802来说结果是值为六。在位位置三(3)和六(6)处的值被设置成值为一以指示假想的装置标识符802的经布隆过滤的值。

[0127] 加入装置212还计算表示加入装置212的装置标识符的布隆过滤器位位置。加入装置212确定所计算出的位位置是否两个都将操纵数据中一的值包含在所收集的信标中。肯定的确定向加入装置212指示该加入装置212被允许加入网状网络100。布隆过滤器的位阵列中的位的值可以全部被设置成值为一以指示任何加入装置212被允许加入网状网络100。将布隆过滤器位阵列中的所有位设置成值为零指示对网状网络100来说不存在活动调试者并且网状网络100不可用于加入。在当特定加入装置未被允许加入时指示特定加入装置212被允许加入网状网络100的误报概率很低的情况下,布隆过滤器匿名为装置标识符提供紧凑表示,同时允许适当的加入装置212高效地找到要加入的正确的网状网络100。

[0128] 用于布隆过滤器的参数是:k,用来将装置标识符散列的散列函数的数目;m,布隆过滤器的位阵列中的位的数目;以及n,要在操纵数据中表示的加入装置212的数目。作为示例而非限制,参数k被设置为二,指示使用了两个散列函数,诸如具有多项式0x1021的CRC16-CCITT以及具有多项式0x8005的CRC16-ANSI。设想了k、散列函数和多项式的其它值。

[0129] 能够计算布隆过滤器的冲突概率p如下:

[0130] $$p = \left(1 - e^{\left(-k\frac{n}{m}\right)}\right)^k \qquad (2)$$

[0131] 调试装置212可以设置如在操纵数据中得到相当低的冲突概率所需的位阵列的长度m。布隆过滤器的使用允许操纵数据缩放以支持在维持低冲突概率的同时将大量的加入装置212加入到网状网络100。下表示出了当m=127(即,16个字节)时n以及冲突概率p的各种值:

[0132]

n	p
1	0.000
2	0.001
3	0.002
4	0.004
5	0.006
10	0.021
12	0.030
20	0.073
25	0.106
30	0.142

50	0.297
100	0.629
200	0.916
1000	1.000

[0133] 为了加入大量的加入装置212(例如,1000个),调试装置210可以将大型集分解成较小集,使得每个较小集在操纵数据中具有较低的冲突(误报)概率。

[0134] 跨网状网络分区管理调试数据

[0135] 图9图示当网状网络100的分割或划分已经发生时的网状网络100。例如,路由器102中的一个可能已失去电力,导致网状网络100的分割,这妨碍网状网络100的一个分区或段与另一分区进行通信。另一方面,无线电干扰可能已经在网状网络100的引起网状网络100的分割的一部分中阻塞了通信。当网状网络100分成两个网络段902和904时,网络段904将为段904选择领导者,并且还可以接受与段902的调试者不同的段904的调试者。这些段中的任何一个或两个可以在分割期间更新网络证书。

[0136] 网状网络100能够清楚地且可靠地划分成两个根本不同的段,当两个分区之间具有连接性时该两个根本不同的段是全功能网络。分区能够继续被完全包含在连续分区内的任何未完成的通信并且能够继续正常的密钥旋转。两个网状网络分区(原来单个网状网络100的一部分)能够在两个分区之间的连接性被恢复时自主地合并。

[0137] 如果调试证书在分割期间在网络段902中改变了,则当在网络段902与网络段904之间恢复连接性时,调试证书改变将被传播到网络段904内的装置。换句话说,在一些实施例中,调试证书被更新为最近采用的证书。然而,如果网络段902和网络段904两者对不同的调试者进行授权,并且在分割期间接收到新且不同的调试证书,则可能更难以确定最近的证书。

[0138] 调试证书在被先前分段但现在合并的任何两个网状网络段之间的解决方案将最近改变的调试数据集传播到网状网络100中的装置。如果在段902上存在改变,则用户认为他或她正在改变整个网状网络100上的调试证书,但是由于划分,仅在有效地改变段902上的证书。在某个以后的时间点,段902和段904合并。因为段904上的原始证书紧跟分段之后保持不变,而段902上的证书被改变,所以经合并的段假设新证书在分段期间建立在段902上。如果在分割期间存在对段904上的调试证书的改变,则对段904做出的改变被传播到合并之后的段902中的装置。

[0139] 在两个用户在分割期间改变相应的两个段902和904上的调试证书的情况下,这两个用户各自认为它们正在改变整个网状网络100上的调试证书。然而,因为网状网络100被分段,所以两个用户能够将本身建立为网络调试者并且改变它们相应的网络段上的调试证书。在某个以后的时间点,段902和段904合并,但是可能不知道来自两个段的哪一个领导者将胜过经合并的网状网络的领导者。胜过的领导者可能不具有最近改变的调试证书的副本。因为调试证书在两个段上独立地改变,所以具有最近更新的调试证书的段优先。

[0140] 为了确定两个中的哪一个网络证书最近,调试数据集包括时间戳信息以及用于在网状网络合并时解决调试证书之间的差异的调试证书。时间戳信息使得网状网络100中的节点能够确定对任何段中的调试证书的最近更新,并且使网状网络100中的装置中的调试数据集与最近更新的调试证书同步。

[0141] 时间戳信息包括时间戳以及该时间戳可追踪到协调世界时间(UTC)还是网状网络100内的相对时间基准的指示。例如,如果调试装置210是诸如能够访问网络时间(诸如使用网络时间协议(NTP)、对通过蜂窝网络提供的时间的访问、来自全球定位系统(GPS)接收器的定时信息等)的智能电话或计算机的装置,则该时间戳可追踪到UTC。作为示例而非限制,时间戳可追踪到UTC,时间戳以可追踪到已知纪元的秒为单位(例如,以自UNIX®时间开始以来的2^{-15}秒为单位)来表达。当时间戳是UTC可追踪时间时,指示(诸如U位)被设置来指示该时间戳可追踪到UTC。

[0142] 如果调试装置210是诸如本机调试者的不能够访问UTC可追踪时间的嵌入式系统,则时间戳包含相对时间值。相对时间值是通过使用如由领导者216提供的时间戳的先前值并且将时钟滴答的增量加到先前时间戳以为经更新的调试数据集产生时间戳来确定的。作为示例而非限制,时间滴答可以是从本机调试者的32kHz时钟导出的亚秒时间滴答的15位表示。当时间戳是相对时间时,指示(诸如U位)被设置成值为零,以指示该时间戳被表达为相对时间。相对时间的时间戳的增量允许对调试数据的改变被检测到。当分区合并时,如果调试时间戳中的一个可追踪到UTC并且秒是相对时间,则具有UTC可追踪时间戳的调试数据将被给予较高优先级。

[0143] 如果时间戳在被在分割期间单独地更新的调试证书之间是相同的,则替选手段可以被用来断开时间戳之间的联结。在一些实施例中,可以执行字典式比较(例如,memcmp)以确定哪一个证书是更近的。在某些实施例中,可以对网络段进行优先级排序,使得将在时间戳之间的联结的情况下采用对一个网络段上的调试证书的改变。例如,具有边界路由器202的网络段可以被视为最高优先级段,使得如果网络段902和904各自接收到包括相同时间戳的调试证书改变,则将在两个段的调试数据集中的相同时间戳值的情况下采用网络段902改变中的改变。

[0144] 根据网状网络调试的一个或多个实施例参考相应的图10至图18对示例方法1000至1800进行描述。通常,本文中所描述的组件、模块、方法和操作中的任一个能够使用软件、固件、硬件(例如,固定逻辑电路)、手工处理、或其任何组合来实现。可以在存储在计算机处理系统本地和/或远程的计算机可读存储器上的可执行指令的一般场境中描述示例方法的一些操作,并且实施方式能够包括软件应用、程序、函数等。替选地或此外,本文中所描述的功能性中的任一个能够至少部分地由一个或多个硬件逻辑组件(诸如而不限于现场可编程门阵列(FGPA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统(SoC)、复杂可编程逻辑器件(CPLD)等)来实现。

[0145] 图10图示如通常与在网状网络中加入节点有关的网状网络调试的(一个或多个)示例方法1000。对方法块进行描述的顺序不旨在被解释为限制,并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选的方法。

[0146] 在块1002处,从加入装置接收信标请求,并且在块1004处,从加入者路由器向加入装置传送信标,其中信标提供网状网络可用于加入的指示。例如,网状网络100中的加入者路由器214从加入装置212接收信标请求并且然后向该加入装置传送信标,其中信标提供网状网络100可用于加入的指示。所传送的信标有效地使得加入装置212能够在该加入装置与加入者路由器之间建立本地链路。

[0147] 在块1006处,从请求加入网状网络的加入装置接收消息。例如,网状网络100中的

加入者路由器214从请求加入网状网络的加入装置212接收消息。从加入装置212接收到的消息能够包括可用来对使用Juggling口令认证密钥交换(J-PAKE)来认证的加入装置进行认证的加密装置标识符，并且认证有效地在网状网络100的调试装置210与加入装置之间建立安全的通信会话。

[0148] 在块1008处，将所接收到的消息转发到网状网络的调试装置。例如，加入者路由器214将从加入装置212接收到的消息转发到网状网络100的调试装置210。在实施方式中，能够使用数据报传输层安全(DTLS)或者使用用户数据报协议(UDP)来接收和转发消息。附加地，加入者路由器214将所接收到的消息转发到调试装置210能够包括在加入者路由器214与调试装置210之间的通信路径中通过网状网络100的一个或多个路由器来转发所接收到的消息。在实施方式中，路由器中的一个可以是将网状网络100连接到外部网络的边界路由器202，并且调试装置附连到外部网络。

[0149] 在块1010处，接收对于要加入网状网络的加入装置的授权，并且在块1012处，向加入装置传送网络信息，该网络信息有效地使得加入装置能够加入网状网络100。例如，加入者路由器214从调试装置210接收对要加入网状网络100的加入装置212的授权，并且加入者路由器214向加入装置传送网络信息，其中该网络信息有效地使得加入装置212能够加入网状网络。

[0150] 图11图示如通常与在网状网络中加入节点有关的网状网络调试的(一个或多个)示例方法1100。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0151] 在块1102处，从加入装置接收信标请求，并且在块1104处，从加入者路由器向加入装置传送信标，其中信标提供网状网络可用于加入的指示。例如，网状网络100中的加入者路由器214从加入装置212接收信标请求并且然后向该加入装置传送信标，其中信标提供网状网络100可用于加入的指示。信标包括网状网络100的网络名称以及指示被允许加入该网状网络的一个或多个加入装置212的操纵数据。所传送的信标有效地使得加入装置能够在该加入装置与加入者路由器之间建立本地链路。

[0152] 在块1106处，从请求加入网状网络的加入装置接收DTLS-客户端Hello消息，并且在块1108处，将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中。例如，加入者路由器从请求加入网状网络100的加入装置212接收DTLS-客户端Hello消息并且将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中。能够利用用户数据报协议(UDP)从加入装置212接收DTLS-客户端Hello消息，并且DTLS中继接收通知消息包括加入装置212的地址、加入者路由器214的地址、以及所接收到的DTLS-客户端Hello消息。

[0153] 在块1110处，将DTLS中继接收通知消息传送到网状网络的调试装置。例如，加入者路由器将DTLS中继接收通知消息传送到网状网络100的调试装置210。在实施方式中，加入者路由器可以对从加入装置传送到调试装置210的DTLS中继接收通知消息的传输应用速率限制。

[0154] 在块1112处，从调试装置接收DTLS中继传送通知消息，并且在块1114处，向加入装置传送该DTLS中继传送通知消息的内容，其中该内容使得加入装置能够加入网状网络。例如，加入者路由器从调试装置210接收DTLS中继传送通知消息并且向加入装置212发送该DTLS中继传送通知消息的内容，其中该内容使得加入装置能够加入网状网络100并且该内

容有效地在调试装置210与加入装置之间建立安全的通信会话。DTLS中继传送通知消息包括加入装置212的地址、加入者路由器214的地址以及DTLS-Hello验证消息。

[0155] 在块1116处，从调试装置接收加入装置将被委托接收网状网络的网络证书的指示，并且在块1118处，接收在调试装置与加入装置之间共享的密钥加密密钥(KEK)。例如，加入者路由器214从调试装置210接收加入装置212将被委托接收网状网络100的网络证书的指示，以及接收在调试装置210与加入装置之间共享的密钥加密密钥(KEK)。

[0156] 在块1120处，使用KEK来将网络证书传送到加入装置以使网络证书的通信安全。例如，加入者路由器使用KEK来将包括网络主密钥的网络证书发送到加入装置212以使网络证书的通信安全，并且安全的通信会话可用来执行加入装置的配备。

[0157] 图12图示如通常与在网状网络中建立调试会话有关的网状网络调试的(一个或多个)示例方法1200。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0158] 在块1202处，通告网状网络对于调试装置的可用性，并且在块1204处，从调试装置接收要成为网状网络的调试者的请愿。例如，网状网络100的边界路由器202通告网状网络对于调试装置的可用性，并且从调试装置210接收要成为网状网络的调试者的请愿。能够响应于通告网状网络的可用性而从调试装置210接收请愿。调试装置210还能够请求安全地连接到边界路由器202，并且使用数据报传输层安全(DTLS)来建立安全的连接。附加地，调试装置210和边界路由器202能够通过除网状网络以外的网络(诸如通过Wi-Fi网络或以太网网络)通信。

[0159] 在块1206处，将所接收到的请愿传送到网状网络的领导者装置，并且在块1208处，从领导者装置接收对请愿的响应，该响应指示对请愿的接受或拒绝。例如，边界路由器202将从调试装置210接收到的请愿传送到网状网络100的领导者装置216，然后从领导者装置216接收对请愿的响应，其中该响应指示对请愿的接受或拒绝。能够使用作为多播域名系统(mDNS)的服务发现协议来执行通告。

[0160] 在块1210处，向调试装置传送对请愿的接受或拒绝的指示。例如，边界路由器202向调试装置210传送对请愿的接受或拒绝的指示，并且请愿由领导者装置216接受对要成为网状网络的调试者的调试装置210进行授权。对请愿的接受建立安全的调试会话，并且对请愿的接受使得领导者装置216能够更新跟踪网状网络的活动调试者的内部状态，将网状网络的准许加入标志设置为真，并且在网状网络内传播调试数据集。

[0161] 在块1212处，向边界路由器注册调试装置的身份以建立安全的调试通信会话。例如，边界路由器202向边界路由器202注册调试装置210的身份以建立安全的调试通信会话。注册调试装置210的身份包括向边界路由器202提供加密调试证书，其中，加密调试证书是从由用户输入到调试装置210的调试证书导出的。边界路由器202包括可用来向网状网络100对调试装置210进行认证的加密调试证书的副本，其中加密调试证书的副本是先前从调试证书导出的，该调试证书被注入到网状网络100的导出了加密调试证书的副本的领导者装置216中，并且领导者装置216将加密调试证书的副本安全地传递到边界路由器。

[0162] 图13图示如通常与在网状网络中建立调试会话有关的网状网络调试的(一个或多个)示例方法1300。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0163] 在块1302处，接收用于接受调试装置作为调试者来对要加入网状网络的加入装置进行调试的请愿。例如，网状网络100的领导者装置216接收用于接受调试装置210作为调试者来对要加入网状网络的加入装置212进行调试的请愿。该请愿是从通过网状网络连接到领导者装置216的边界路由器202接收的，并且调试装置210通过另一网络(诸如Wi-Fi网络和以太网网络)连接到边界路由器202。另外，使用边界路由器202与调试装置210之间的安全的通信会话来接收请愿，其中该安全的通信会话使用数据报传输层安全(DTLS)来建立。领导者装置216能够通过网状网络100从包括网状网络的网络接口的调试装置210接收请愿，并且调试装置210通过在网络信标中将本机调试者位设置为真来请愿成为调试者。调试装置210能够通过约束应用协议(CoAP)端口使用IEEE 802.15.4接口来将请愿传递到领导者装置。

[0164] 在块1304处，做出关于接受还是拒绝所接收到的请愿的确定，并且在块1306处，向调试装置传送响应，其带有关于所接收到的请愿被接受还是拒绝的指示。例如，领导者装置216确定接受还是拒绝所接收到的请愿，然后向调试装置210发送响应，其带有关于所接收到的请愿被接受还是拒绝的指示。领导者装置216基于确保对网状网络100来说存在单个活动调试者来确定接受还是拒绝所接收到的请愿。

[0165] 在块1308处，响应于所接收到的请愿被接受的确定而更新内部状态，所述内部状态跟踪网状网络的活动调试者。例如，领导者装置216更新内部状态，所述内部状态跟踪网状网络的活动调试者。

[0166] 在块1310处，从调试装置接收用于针对网状网络开始加入模式的命令，并且在块1312处，在该网状网络内传播调试数据集。例如，领导者装置216从调试装置210接收用于针对网状网络100开始加入模式的命令，并且在该网状网络内传播调试数据集。调试数据集包括调试者会话标识符、调试者时间戳、加密调试者证书、以及指示哪些安全相关操作在网状网络中被允许的安全策略。当调试者在网状网络100上活动时，调试数据集还包括边界路由器202的位置。当在网状网络中启用了加入模式时，调试数据集还包括指示加入装置212中的哪些被允许加入该网状网络的操纵数据。

[0167] 在块1314处，从在领导者装置的调试期间被注入到领导者装置216中的调试证书导出加密调试证书。例如，领导者装置216从在该领导者装置的调试期间被注入到该领导者装置中的调试证书导出加密调试证书。加密调试证书的导出通过应用密钥导出函数来执行，其中密钥导出函数使用基于密码的消息认证码(CMAC)来多次执行散列。在实施方式中，调试证书是人为可调节的通行码，并且加密调试证书的导出有效地使调试证书的长度展开。

[0168] 在块1316处，向边界路由器发送加密调试证书的副本，使得边界路由器能够向网状网络对调试装置进行认证。例如，领导者装置216向边界路由器202发送加密调试证书的副本，使得边界路由器202能够向网状网络认证调试装置210。

[0169] 图14图示如通常与在网状网络中管理多个调试会话有关的网状网络调试的(一个或多个)示例方法1400。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或供替选方法。

[0170] 在块1402处，在调试装置与网状网络的边界路由器之间建立安全的调试通信会话。例如，调试装置210在该调试装置与网状网络100的边界路由器202之间建立安全的调试

通信会话，以安全地建立网络通信会话以用于将一个或多个加入装置212加入到网状网络。调试装置210通过从该调试装置向网状网络100的领导者装置216发送用于请求接受调试装置210作为网状网络的活动调试者的请愿来建立安全的调试通信会话，并且该调试装置从该领导者装置接收对请愿的接受的指示。

[0171] 在块1404处，激活针对网状网络的加入。例如，调试装置通过开始使得网状网络中的一个或多个路由器通告网状网络正在接受加入请求的加入模式来激活针对网状网络的加入。调试装置210还能够通过向领导者装置216发送用于使网状网络变得可加入的管理消息来激活针对网状网络100的加入，其中管理消息使得领导者装置216能够更新网状网络的网络数据。该网络数据被传播到网状网络中的一个或多个路由器装置，其中该网络数据包括网状网络100可用于加入的指示。网络数据能够由路由器装置在信标中广播，并且管理消息包括指示调试装置210被配置成加入到网状网络的一个或多个加入装置212的操纵数据。

[0172] 在块1406处，从加入装置中的一个加入装置接收用于加入网状网络的请求。例如，调试装置210从加入装置212中的一个加入装置接收用于加入网状网络100的请求，并且可以经由加入者路由器接收该请求。调试装置210能够向加入者路由器214传送加入装置212将被委托接收网状网络100的网络证书以及在调试装置210与加入装置之间共享的密钥加密密钥(KEK)的指示。被传送到加入者路由器214的指示使得该加入者路由器能够使用所接收到的KEK来将网络证书安全地传送到加入装置212以将该加入装置调试到网状网络。从加入装置212接收到的请求能够包括加入装置的加密装置标识符，其中加密装置标识符是使用Jugglng口令认证密钥交换(J-PAKE)从加入装置的装置标识符导出的。

[0173] 在块1408处，在调试装置与加入装置之间建立安全的加入者通信会话。例如，调试装置210在该调试装置与加入装置212之间建立安全的加入者通信会话。调试装置210能够通过确定从加入装置212接收到的加密装置标识符和由调试装置210从作为调试装置的输入从用户接收到的装置标识符的副本导出的加密装置标识符匹配来建立安全的加入者通信会话，并且调试装置210将加密装置标识符用作共享秘密来使加入者通信会话安全。

[0174] 在块1410处，使用加密装置标识符来对加入装置进行认证，并且在块1412处，将加入装置加入到网状网络。例如，调试装置210使用加密装置标识符来对加入装置212进行认证，并且将加入装置212加入到网状网络。

[0175] 图15图示如通常与在网状网络中提供加入装置有关的网状网络调试的(一个或多个)示例方法1500。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0176] 在块1502处，在调试装置与网状网络的边界路由器之间建立调试通信会话。例如，网状网络100的调试装置210在调试装置210与网状网络的边界路由器202之间建立调试通信会话。在块1504处，在加入装置与调试装置之间建立加入者通信会话。例如，网状网络100的调试装置210在加入装置212与该调试装置之间建立加入者通信会话。

[0177] 在块1506处，向加入装置发送调试信息，其中该调试信息可由加入装置用来加入网状网络。例如，网状网络100的调试装置210向加入装置发送加入装置212能够使用来加入网状网络的调试信息。

[0178] 在块1508处，从加入装置接收调试者应用的位置的指示，并且在1510处，利用所接收到的指示来检索调试者应用。例如，调试装置210从加入装置接收调试者应用的位置指

示，其中所接收到的位置信息可以是统一资源定位符(URL)并且调试应用通过互联网从云服务中检索调试者应用。调试装置210还能够使用所接收到的URL来确定调试者应用是否被存储在该调试装置的存储器中。

[0179] 在块1512处，调试者应用被执行以配备加入装置。例如，调试装置210利用调试者应用来配备加入装置。加入装置212的配备能够包括更新该加入装置上的软件、将该加入装置链接到在云服务上的用户账户、和/或配置该加入装置，其中配置是与网状网络中的其它装置有关的本地配置。在块1514处，加入装置的调试结束，使得加入装置能够加入网状网络。例如，网状网络100的调试装置210使调试结束，使得加入装置212能够加入网状网络。

[0180] 图16图示如通常与在网状网络中搜寻和操纵有关的网状网络调试的(一个或多个)示例方法1600。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0181] 在块1602处，确定网状网络的操纵数据，其中该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示。例如，网状网络100的调试装置210确定网状网络的操纵数据，并且该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示。在实施方式中，操纵数据是作为IEEE 64位扩展唯一标识符(EUI-64)的装置标识符的16位循环冗余校验(CRC16)。调试装置210还可以通过针对与被允许加入网状网络的附加装置相关联的附加装置标识符来确定操纵数据而确定网状网络100的操纵数据。

[0182] 在块1604处，将操纵数据从网状网络的调试装置传播到网状网络中的路由器。例如，网状网络100的调试装置210将操纵数据传播到网状网络中的路由器，并且该操纵数据指示调试者在网状网络上活动。传播操纵数据使得路由器102能够在信标消息中传送该操纵数据，并且该操纵数据有效地使得与装置标识符相关联的装置能够识别该装置被允许加入网状网络。调试装置210传播操纵数据有效地使得装置能够区分网状网络和其它网络，其中其它网络是IEEE 802.15.4网络。

[0183] 图17图示如通常与在网状网络中搜寻和操纵有关的网状网络调试的(一个或多个)示例方法1700。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0184] 在块1702处，确定网状网络的操纵数据，其中该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示，并且该指示被表示为在布隆过滤器中表示装置标识符的值的集合。例如，网状网络100的调试装置210确定网状网络的操纵数据，并且该操纵数据包括被表示为在布隆过滤器中表示装置标识符的值的集合的指示。在实施方式中，调试装置210通过对装置标识符应用第一散列函数以产生第一散列值，并且对装置标识符应用第二散列函数以产生第二散列值来确定操纵数据。装置标识符可以是IEEE 64位扩展唯一标识符(EUI-64)，其中装置标识符是EUI-64的最低有效二十四位。在实施方式中，第一散列函数和第二散列函数是循环冗余校验(CRC)，其中第一散列函数是CRC16-CCITT，并且第二散列函数是CRC16-ANSI。

[0185] 调试装置210然后对第一散列值执行模运算以确定布隆过滤器中的第一位字段位置，并且对第二散列值执行模运算以确定布隆过滤器中的第二位字段位置。用于模运算的除数可以是布隆过滤器的位阵列的长度。调试装置210能够将布隆过滤器的第一位字段位置中的值设置为一，并且将布隆过滤器的第二位字段位置中的值设置为一。调试装置210能

够将操纵数据中的位字段值中的全部设置成值为一以指示网状网络对任何装置来说是可加入的。替选地，调试装置210能够将操纵数据的位字段值设置成值为零，这禁用针对网状网络的加入。

[0186] 在块1704处，将操纵数据从网状网络的调试装置传播到网状网络中的路由器。例如，网状网络100的调试装置210将操纵数据传播到网状网络中的路由器，并且该操纵数据指示调试者在网状网络上活动。传播操纵数据使得路由器102能够在信标消息中传送操纵数据，并且该操纵数据使得与装置标识符相关联的装置能够将布隆过滤器中的值的集合与在该装置处确定的值的第二集合进行比较以识别该装置被允许加入网状网络。

[0187] 图18图示如通常与在网状网络中划分节点有关的网状网络调试的(一个或多个)示例方法1800。对方法块进行描述的顺序不旨在被解释为限制，并且能够以任何顺序组合任何数目的所描述的方法块以实现方法或替选方法。

[0188] 在块1802处，在网状网络中的节点装置处接收调试数据集。例如，在网状网络100中的节点处的节点装置(例如，路由器102或终端装置106)接收包括接收时间戳、调试证书、网状网络的网络名称、以及指示哪些安全相关操作在网状网络中被允许的安全策略的调试数据集。接收时间戳包括时间值以及该时间值可追踪到协调世界时间(UTC)的指示。

[0189] 在块1804处，将被包括在所接收到的调试数据集中的接收时间戳与包括在被存储在节点装置中的调试数据集中的存储时间戳进行比较。例如，网状网络100中的节点装置将所接收到的调试数据集中的接收时间戳与包括在被存储在节点装置中的调试数据集中的存储时间戳进行比较。在实施例中，节点装置和领导者装置被先前调试到网状网络，并且先前调试将相同的调试数据集存储在节点装置和领导者装置中。能够在停止在节点装置与领导者装置之间的通过网状网络通信的网状网络的分割之后更新节点装置中所存储的调试数据集。分割使网状网络分开并且网状网络的第一分区包括领导者装置，而网状网络的第二分区包括节点装置。该节点装置能够在网状网络的第一分区和第二分区的合并之后接收调试数据集，其中合并重新建立在节点装置与领导者装置之间通过网状网络的通信路径。

[0190] 在块1806处，做出关于被包括在存储在节点装置中的调试数据集中的存储时间戳是否比包括在所接收到的调试数据集中的时间戳更近的确定。例如，基于比较(在块1806处)，节点装置确定被包括在存储在节点装置中的调试数据集中的存储时间戳是否比包括在所接收到的调试数据集中的时间戳更近。

[0191] 如果存储时间戳比接收时间戳更近(即，来自1806的“是”)，则在1808处，向网状网络的领导者装置传送消息，该消息包括所存储的调试数据集。例如，网状网络中的节点装置向网状网络100的领导者装置传送包括所存储的调试数据集的消息。所传送的消息使得领导者装置能够接受所存储的调试数据集作为网状网络的最近的调试数据集，并且将所存储的调试数据集传播到网状网络。替选地，如果接收时间戳比存储时间戳更近(即，来自1806的“否”)，则在1810处，更新所存储的调试数据集以和所接收到的调试数据集匹配。例如，网状网络中的节点装置更新所存储的调试数据集以和所接收到的调试数据集匹配。

[0192] 图19图示其中能够实现网状网络100(如参考图1所描述的)以及网状网络调试的实施例的示例环境1900。通常，环境1900包括作为具有针对网状网络中的通信而配置的任何数目的网状网络装置的智能家居或其它类型的结构的一部分所实现的网状网络100。例如，网状网络装置能够包括恒温器1902、危险检测器1904(例如，用于烟和/或一氧化碳)、相

机1906(例如,室内的和室外的)、照明单元1908(例如,室内的和室外的)以及被实现在结构1912内部和/或外部(例如,在智能家居环境中)的任何其它类型的网状网络装置1910。在这个示例中,网状网络装置还能够包括先前描述的装置中的任一个,诸如调试装置210、边界路由器202、加入者路由器214以及作为路由器102、终端装置106、和/或加入装置212所实现的装置中的任一个。

[0193] 在环境1900中,任何数目的网状网络装置能够被实现以用于无线互连以彼此以无线方式通信和交互。网状网络装置是模块化的、智能的、多感测的、连接网络的装置,其能够彼此和/或与中央服务器或云计算系统无缝地集成以提供各种有用的智能家居目标和实施方式中的任一个。参考图20示出并描述能够作为本文中所描述的装置中的任一个被实现的网状网络装置的示例。

[0194] 在实施方式中,恒温器1902可以包括检测环境气候特性(例如,温度和/或湿度)并且控制智能家居环境中的HVAC系统的Nest®学习恒温器。学习恒温器1902和其它智能装置通过捕获装置的占用设置来"学习"。例如,恒温器学习针对上午和晚上的优选温度设置点以及结构的占用者何时睡着或醒来以及占用者何时通常离开或在家。

[0195] 危险检测器1904能够被实现来检测危险物质或指示危险物质的物质(例如,烟、火、或一氧化碳)的存在。在无线互连的示例中,危险检测器1904可以检测烟的存在,其指示结构中的火,在此情况下首先检测到烟的危险检测器能够向已连接的网状网络装置中的全部网状网络装置广播低功率唤醒信号。其它危险检测器1904然后能够接收到所广播的唤醒信号并为了危险检测而开始高功率状态并且将接收警报消息的无线通信。另外,照明单元1908能够接收所广播的唤醒信号并且在已检测到危险的区域中激活以照射并识别问题区域。在另一示例中,照明单元1908可以诸如针对检测到的火或非法闯入用一种光照颜色激活以指示结构中的问题区域或区,并且用不同的光照颜色激活以指示安全区和/或离开结构的逃跑路线。

[0196] 在各种配置中,网状网络装置1910能够包括与连接网络的门锁系统协同起作用并且检测人接近于位置(诸如结构1912的外门)或者离开该位置并做出响应的入口接口装置。该入口接口装置能够基于某人是否已接近或者进入智能家居环境来与其它网状网络装置交互。入口接口装置能够控制门铃功能性、经由音频或视觉手段来通告人的接近或离开、并且控制安全系统上的设置,诸如以在占用者来去时激活或者去激活该安全系统。网状网络装置1910还能够包括其它传感器和检测器,诸如以检测环境照明条件、检测房间占用状态(例如,利用占用传感器)、并且控制一个或多个灯的电力和/或调光状态。在一些实例中,传感器和/或检测器还可以控制风扇(诸如吊扇)的电力状态和速度。另外,传感器和/或检测器可以检测房间或封闭空间中的占用,并且诸如在房间或结构被占用的情况下,控制电力到电插座或装置的供应。

[0197] 网状网络装置1910还可以包括连接的家电和/或受控系统(诸如冰箱、电炉和烘箱、洗衣机、烘干机、空调器、水池加热器、灌溉系统、安全系统等)以及其它电子和计算装置(诸如电视、娱乐系统、计算机、内部通信系统、车库开门器、吊扇、控制面板等)。当被插入时,家电、装置或系统能够将它本身通告给如上所述的网状网络,并且能够在智能家居中与网状网络的控件和装置自动地集成。应该注意,网状网络装置1910可以包括物理上位于结构外部但是在无线通信范围内的装置,诸如控制游泳池加热器或灌溉系统的装置。

[0198] 如上所述，网状网络100包括接口对接以用于与网状网络100外部的外部网络通信的边界路由器202。边界路由器202连接到接入点204，所述接入点204连接到诸如互联网的通信网络206。经由通信网络206连接的云服务208提供与网状网络100内的装置有关的服务并且/或者使用网状网络100内的装置来提供服务。作为示例，云服务208能够包括用于将终端用户装置(诸如智能电话、平板等)连接到网状网络100中的装置、处理在网状网络100中获取的数据并将其呈现给终端用户、将一个或多个网状网络100中的装置链接到云服务208的用户账户、配备并更新网状网络100中的装置等的应用。例如，用户能够使用连接网络的计算机或便携式装置(诸如移动电话或平板装置)来控制智能家居环境中的恒温器1902和其它网状网络装置。另外，网状网络装置能够经由边界路由器202和接入点204向任何中央服务器或云计算系统传递信息。能够使用各种定制或标准无线协议(例如，Wi-Fi、针对低功率的ZigBee、6LoWPAN等)中的任一个和/或通过使用各种定制或标准有线协议(CAT6以太网、HomePlug等)中的任一个来执行数据通信。

[0199] 网状网络100中的网状网络装置中的任一个网状网络装置能够用作低功率通信节点以在智能家居环境中创建网状网络100。网络的个体低功率节点能够定期地发出有关它们正在感测什么的消息，并且环境中的其它低功率节点除发出它们自己的消息之外还能够重复消息，从而在整个网状网络中从节点到节点(即，从装置到装置)传递消息。网状网络装置能够被实现来尤其在电池供电时保存电力、利用低低功率通信协议来接收消息、将这些消息转化为其它通信协议、并且将经转化的消息发送到其它节点和/或到中央服务器或云计算系统。例如，占用和/或环境光传感器能够检测房间中的占用者以及测量环境光，并且在环境光传感器检测到房间暗时以及在占用传感器检测到某人在房间中时激活光源。另外，传感器能够包括定期地发出有关房间的占用以及房间中光的量的消息(包括与占用传感器检测到人存在于房间中一致的即时消息)的低功率无线通信芯片(例如，ZigBee芯片)。如上面所提及的，可以使用网状网络来在智能家居环境内从节点到节点(即，智能装置到智能装置)以及通过互联网向中央服务器或云计算系统无线发送这些消息。

[0200] 在其它配置中，网状网络装置中的各种装置能够充当智能家居环境中的警报系统的“绊网(tripwires)”。例如，在犯罪者避开通过位于结构或环境的窗户、门以及其它进入点处的警报传感器的检测的情况下，仍然能够通过从网状网络中的低功率网状节点中的一个或多个低功率网状节点接收占用、运动、热、声音等消息来触发警报。在其它实施方式中，网状网络能够被用来随着人在结构中从房间转移到房间而自动地打开和关掉照明单元1908。例如，网状网络装置能够检测人通过结构的移动并且经由网状网络的节点传递对应的消息。使用指示哪些房间被占用的消息，接收到这些消息的其它网状网络装置能够相应地激活和/或去激活。如上面所参考的，网状网络还能够被利用来例如通过打开引向安全出口的适当照明单元1908在紧急情况下提供出口照明。还可以打开照明单元1908以指示沿着人应该行进以安全地离开结构的出口路线的方向。

[0201] 各种网状网络装置还可以被实现来与可穿戴计算装置集成并进行通信，诸如可以被用来识别和定位结构的占用者，并且相应地调整温度、照明、声音系统等。在其它实施方式中，RFID感测(例如，具有RFID手镯、项链、或钥匙圈的人)、合成视觉技术(例如，摄像机和面部识别处理器)、音频技术(例如，语音、声音模式、振动模式识别)、超声感测/成像技术、以及红外或近场通信(NFC)技术(例如，穿戴有红外或NFC能力的智能电话的人)连同根据所

感测到的关于占用者在结构或环境中的位置的信息得出有用结论的基于规则的推理引擎或人工智能技术一起。

[0202] 在其它实施方式中，服务机器人的个人舒适区域网络、个人健康区域网络、个人安全区域网络和/或其它这样的面向人类的功能性能够通过根据用于实现这些功能性的更好性能的基于规则的推理技术或人工智能技术与环境中的其它网状网络装置和传感器的逻辑集成来增强。在与个人健康区域有关的示例中，本系统能够连同基于规则的推理和人工智能技术一起(例如，使用网状网络装置和传感器中的任一个)检测家庭宠物是否朝向占用者的当前位置移动。类似地，能够通知危险检测器服务机器人温度和湿度水平在厨房中上升，并且根据环境烟水平的任何小增加最可能是由于烹饪活动而导致的而不是由于一般危险条件而导致的推理来暂时提升危险检测阈值，诸如烟检测阈值。针对任何类型的监测、检测、和/或服务而配置的任何服务机器人能够作为网状网络上的网状节点装置被实现，从而符合用于在网状网络上通信的无线互连协议。

[0203] 网状网络装置1910还可以包括针对智能家居环境中的结构的个体占用者中的每一个占用者的智能闹钟。例如，占用者能够为唤醒时间(诸如次日或下一周)定制并设置警报装置。人工智能能够被用来考虑占用者在它们睡去时对警报的响应，并且随着时间的推移而做出关于优选睡眠模式的推理。能够基于人的唯一签名在网状网络中跟踪个体占用者，所述人的唯一签名是基于从位于网状网络装置中的传感器(诸如包括超声传感器、无源IR传感器等的传感器)所获得的数据来确定的。占用者的唯一签名能够基于移动的模式、语音、身高、尺寸等的组合，以及使用面部识别技术。

[0204] 在无线互连的示例中，个体的唤醒时间能够与恒温器1902相关联以以高效方式控制HVAC系统，以便将结构预加热或者冷却至期望的睡眠和唤醒温度设置。能够随着时间的推移(诸如通过在人睡眠之前并在醒来时捕获恒温器中设置的温度)来学习优选设置。收集到的数据还可以包括人的生物计量指示，诸如呼吸模式、心率、移动等，据此基于这个数据与指示人何时实际上醒来的数据相结合地做出推理。其它网状网络装置能够使用该数据来提供其它智能家居目标，诸如调整恒温器1902以便把环境预加热或者冷却至期望的设置，并且打开或者关掉灯1908。

[0205] 在实施方式中，网状网络装置还能够被用于声音、振动、和/或运动感测，诸如以检测自来水并且基于水使用和消耗的算法和映射来确定关于智能家居环境中的水使用的推理。这能够被用来确定家居中的各个水源的签名或指纹，并且也被称为“音频指纹水使用”。类似地，网状网络装置能够被利用来检测有害害虫(诸如老鼠和其它啮齿动物)的以及通过白蚁、蟑螂和其它昆虫的细微声音、振动、和/或运动。本系统然后能够向占用者通知环境中的可疑害虫，例如采用告警消息来帮助便于早期检测和预防。

[0206] 图20图示根据如本文中所描述的网状网络调试的一个或多个实施例的能够作为网状网络中的网状网络装置中的任一个网状网络装置被实现的示例网状网络装置2000。该装置2000能够被集成有电子电路、微处理器、存储器、输入输出(I/O)逻辑控件、通信接口和组件、以及用于实现网状网络中的装置的其它硬件、固件和/或软件。另外，网状网络装置2000能够用各种组件(诸如用如参考图21中所示的示例装置进一步描述的任何数目的不同组件以及这些不同组件的组合)加以实现。

[0207] 在这个示例中，网状网络装置2000包括处理可执行指令的低功率微处理器2002和

高功率微处理器2004(例如,微控制器或数字信号处理器)。该装置还包括输入输出(I/O)逻辑控件2006(例如,以包括电子电路)。微处理器能够包括集成电路的组件、可编程逻辑器件、使用一个或多个半导体形成的逻辑器件、以及硅和/或硬件的其它实施方式,诸如作为芯片上系统(SoC)所实现的处理器和存储器系统。替选地或此外,该装置能够用可以用处理和控制电路实现的软件、硬件、固件或固定逻辑电路中的任何一个或组合来实现。低功率微处理器2002和高功率微处理器2004还能够支持装置的一个或多个不同的装置功能性。例如,高功率微处理器2004可以执行计算密集的运算,然而低功率微处理器2002可以管理诸如从一个或多个传感器2008检测危险或温度的不太复杂的过程。低功率处理器2002还可以为了计算密集的过程而唤醒或者初始化高功率处理器2004。

[0208] 一个或多个传感器2008能够被实现来检测诸如加速度、温度、湿度、水、电源、接近、外部运动、装置运动、声音信号、超声信号、光信号、火、烟、一氧化碳、全球定位卫星(GPS)信号、射频(RF)、其它电磁信号或电磁场等的各种特性。因此,传感器2008可以包括温度传感器、湿度传感器、危险相关传感器、其它环境传感器、加速度计、麦克风、相当于并包括相机(例如,电荷耦合器件或摄像机)的光学传感器、有源或无源辐射传感器、GPS接收器、以及射频标识检测器中的任何一个或组合。在实施方式中,网状网络装置2000可以包括一个或多个主传感器以及一个或多个辅传感器,诸如感测以装置的核心操作为中心的数据(例如,在恒温器中感测温度或者在烟检测器中感测烟)的主传感器,而辅传感器可以感测能够被用于能量效率目标或智能操作目标的其它类型的数据(例如,运动、光或声音)。

[0209] 网状网络装置2000包括存储器装置控制器2010和存储器装置2012,诸如任何类型的非易失性存储器和/或其它适合的电子数据存储装置。网状网络装置2000还能够包括各种固件和/或软件,诸如作为计算机可执行指令由存储器所保持的并且由微处理器所执行的操作系统2014。装置软件还可以包括实现网状网络调试的实施例的调试应用2106。网状网络装置2000还包括用于与另一装置或外围组件接口对接的装置接口2018,并且包括耦合网状网络装置的各种组件以用于组件之间的数据通信的集成数据总线2020。网状网络装置中的数据总线还可以作为不同的总线结构和/或总线架构中的任何一个或组合被实现。

[0210] 装置接口2018可以从用户接收输入并且/或者向用户提供信息(例如,作为用户接口),并且接收到的输入能够被用来确定设置。装置接口2018还可以包括对用户输入做出响应的机械或虚拟组件。例如,用户能够以机械方式移动滑动或可旋转组件,或者可以检测沿着触摸板的运动,并且这样的运动能够与装置的设置调整相对应。物理和虚拟可移动的用户接口组件能够允许用户沿着表观连续能谱的一部分设置设置。装置接口2018还可以从任何数目的外围设备(诸如按钮、小键盘、开关、麦克风、和成像器(例如,相机装置))接收输入。

[0211] 网状网络装置2000能够包括网络接口2022(诸如用于与网状网络中的其它网状网络装置通信的网状网络接口)以及用于网络通信(诸如经由互联网)的外部网络接口。网状网络装置2000还包括用于经由网状网络接口与其它网状网络装置以及多个不同的无线通信系统通信的无线的无线电系统2024。无线的无线电系统2024可以包括Wi-Fi、蓝牙™、移动宽带、和/或点对点IEEE 802.15.4。不同的无线电系统中的每一个无线电系统能够包括无线电装置、天线、以及针对特定无线通信技术而实现的芯片组。网状网络装置2000还包括电源2026,诸如电池并且/或者用于将装置连接到线电压。AC电源还可以被用来对装置的电池

充电。

[0212] 图21图示包括示例装置2102的示例系统2100，所述示例装置2102能够作为实现如参考先前的图1至图20所描述的网状网络调试的实施例的网状网络装置中的任一个网状网络装置被实现。示例装置2102可以是任何类型的计算装置、客户端装置、移动电话、平板、通信、娱乐、游戏、媒体重放、和/或其它类型的装置。另外，示例装置2102可以作为针对网状网络上的通信而配置的任何其它类型的网状网络装置(诸如恒温器、危险检测器、相机、灯单元、调试装置、路由器、边界路由器、加入者路由器、加入装置、终端装置、领导者、接入点、和/或其它网状网络装置)被实现。

[0213] 装置2102包括使得能实现装置数据2106(诸如在网状网络中的装置之间传递的数据、正被接收的数据、为广播而调度的数据、数据的数据分组、在装置之间同步的数据等)的有线和/或无线通信的通信装置2104。装置数据能够包括任何类型的通信数据以及由在装置上执行的应用所生成的音频、视频、和/或图像数据。通信装置2104还能够包括用于蜂窝电话通信和/或用于网络数据通信的收发器。

[0214] 装置2102还包括输入/输出(I/O)接口2108，诸如在装置、数据网络(例如，网状网络、外部网络等)与其它装置之间提供连接和/或通信链路的数据网络接口。I/O接口能够被用来将装置耦合到任何类型的组件、外围设备、和/或附属装置。I/O接口还包括能够经由其接收任何类型的数据、媒体内容、和/或输入(诸如到装置的用户输入，以及任何类型的通信数据以及从任何内容和/或数据源接收到的音频、视频和/或图像数据)的数据输入端口。

[0215] 装置2102包括可以至少部分地用硬件(诸如采用处理可执行指令的任何类型的微处理器、控制器等)实现的处理系统2110。该处理系统能够包括集成电路的组件、可编程逻辑器件、使用一个或多个半导体形成的逻辑器件、以及硅和/或硬件的其它实施方式，诸如作为芯片上系统(SoC)所实现的处理器和存储器系统。替选地或此外，该装置能够用可以用处理和控制电路加以实现的软件、硬件、固件或固定逻辑电路中的任何一个或组合来实现。装置2102还可以包括耦合该装置内的各种组件的任何类型的系统总线或其它数据和命令传送系统。系统总线能够包括不同的总线结构和架构以及控制线和数据线中的任何一个或组合。

[0216] 装置2102还包括计算机可读存储存储器2112，诸如能够由计算装置访问并且提供数据和可执行指令(例如，软件应用、模块、程序、功能等)的持久存储的数据存储装置。本文中所描述的计算机可读存储存储器排除传播信号。计算机可读存储存储器的示例包括易失性存储器和非易失性存储器、固定和可移动媒体装置、以及维持数据以用于计算装置访问的任何适合的存储器装置或电子数据存储。计算机可读存储存储器能够包括随机存取存储器(RAM)、只读存储器(ROM)、闪速存储器、以及以各种存储器装置配置的其它类型的存储存储器的各种实施方式。

[0217] 计算机可读存储存储器2112提供装置数据2106和各种装置应用2114(诸如采用计算机可读存储存储器作为软件应用被维持并且由处理系统2110执行的操作系统)的存储。装置应用还可以包括装置管理器，诸如任何形式的控制应用、软件应用、信号处理和控制模块、对特定装置而言为本机的代码、用于特定装置的硬件抽象层等。在这个示例中，装置应用还包括诸如当示例装置2102作为本文中所描述的网状网络装置中的任一个被实现时实现网状网络调试的实施例的调试应用2116。

[0218] 装置2102还包括为音频装置2120生成音频数据并且/或者为显示装置2122生成显示数据的音频和/或视频系统2118。音频装置和/或显示装置包括处理、显示、和/或以其它方式渲染音频、视频、显示、和/或图像数据的任何装置，诸如数字照片的图像内容。在实施方式中，音频装置和/或显示装置是示例装置2102的集成组件。替选地，音频装置和/或显示装置是示例装置的外部外围组件。在实施例中，可以在分布式系统中(诸如在平台2126中通过“云”2124)实现针对网状网络调试所描述的技术的至少一部分。云2124包括和/或表示用于服务2128和/或资源2130的平台2126。

[0219] 平台2126使硬件(诸如服务器装置(例如，被包括在服务2128中))和/或软件资源(例如，作为资源2130被包括)的底层功能性抽象化，并且将示例装置2102与其它装置、服务器等连接。资源2130还可以包括能够在远离示例装置2102的服务器上执行计算处理的同时被利用的应用和/或数据。附加地，服务2128和/或资源2130可以诸如通过互联网、蜂窝网络、或Wi-FI网络便于订户网络服务。平台2126还可以用来使资源抽象化和缩放以为针对经由该平台(诸如在具有在整个系统2100分布的功能性的互连装置实施例中)实现的资源2130的命令服务。例如，可以部分地在示例装置2102处以及经由使云2124的功能性抽象化的平台2126实现功能性。

[0220] 尽管已经用特定于特征和/或方法的语言描述了网状网络调试的实施例，然而所附权利要求的主题未必限于所描述的特定特征或方法。相反，特定特征和方法作为网状网络调试的示例实施方式被公开，并且其它等效的特征和方法旨在为在所附权利要求的范围内。另外，描述了各种不同的实施例，并且应当了解，能够独立地或者与一个或多个其它描述的实施例相结合地实现每个描述的实施例。

[0221] 一种将加入装置安全地加入到网状网络的方法包括：在加入者路由器处从请求加入所述网状网络的所述加入装置接收消息；将所接收到的消息转发到所述网状网络的调试装置；从所述调试装置接收用于所述加入装置加入所述网状网络的授权；以及向所述加入装置发送网络信息，所述网络信息有效地使得所述加入装置能够加入所述网状网络。

[0222] 替选地或除上面描述的方法之外，以下步骤中的任一个或组合：从所述加入装置接收信标请求；以及从所述加入者路由器向所述加入装置传送信标，所述信标提供所述网状网络能够用于加入的指示；所述发送所述信标有效地使得所述加入装置能够在所述加入装置与所述加入者路由器之间建立本地链路；所述接收所述消息以及所述转发所接收到的消息是使用数据报传输层安全(DTLS)来执行的；所述接收所述消息以及所述转发所接收到的消息是使用用户数据报协议(UDP)来执行的；从所述加入装置接收到的所述消息包括能够用来对所述加入装置进行认证的加密装置标识符，所述加入装置是使用Jugglling口令认证密钥交换(J-PAKE)来认证的，以及所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话；所述将所接收到的消息转发到所述调试装置包括在所述加入者路由器与所述调试装置之间的通信路径中通过所述网状网络的一个或多个路由器来转发所接收到的消息；以及所述一个或多个路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器，并且其中，所述调试装置附连到所述外部网络。

[0223] 一种作为加入者路由器所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：经由所述网状网络接口从请求加入所述网状网络

的加入装置接收消息;将所接收到的消息转发到所述网状网络的调试装置;从所述调试装置接收用于所述加入装置加入所述网状网络的授权;以及开始向所述加入装置传送网络信息,所述网络信息有效地使得所述加入装置能够加入所述网状网络。

[0224] 替选地或除上面描述的网状网络装置之外,以下各项中的任一项或组合:所述调试应用被配置成经由所述网状网络接口从所述加入装置接收信标请求,以及开始从所述加入者路由器向所述加入装置传送信标,所述信标提供所述网状网络能够用于加入的指示;所述信标有效地使得所述加入装置能够在所述加入装置与所述加入者路由器之间建立本地链路;所述调试应用被配置成使用数据报传输层安全(DTLS)来接收所述消息并且转发所接收到的消息;所述调试应用被配置成使用用户数据报协议(UDP)来接收所述消息并且转发所接收到的消息;从所述加入装置接收到的所述消息包括能够用来对所述加入装置进行认证的加密装置标识符,所述加入装置是使用Juggling口令认证密钥交换(J-PAKE)来认证的;以及所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话;所述调试应用被配置成在所述加入者路由器与所述调试装置之间的通信路径中通过所述网状网络的一个或多个路由器来转发所接收到的消息;以及所述一个或多个路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器,并且其中,所述调试装置附连到所述外部网络。

[0225] 一种网状网络系统包括:加入装置,所述加入装置被配置成请求加入网状网络;以及加入者路由器,所述加入者路由器被配置成:从请求加入所述网状网络的所述加入装置接收消息;将所接收到的消息转发到所述网状网络的调试装置;从所述调试装置接收用于所述加入装置加入所述网状网络的授权;以及向所述加入装置传送网络信息,所述网络信息有效地使得所述加入装置能够加入所述网状网络。

[0226] 替选地或除上面描述的网状网络系统之外,以下各项中的任一项或组合:所述加入者路由器被配置成:从所述加入装置接收信标请求,以及向所述加入装置传送信标,所述信标提供所述网状网络能够用于加入的指示,并且所述信标有效地使得所述加入装置能够在所述加入装置与所述加入者路由器之间建立本地链路;从所述加入装置接收到的所述消息包括能够用来对所述加入装置进行认证的加密装置标识符,所述加入装置是使用Juggling口令认证密钥交换(J-PAKE)来认证的,以及所述认证有效地在所述调试装置与所述加入装置之间建立安全的通信会话;以及所述加入者路由器被配置成在所述加入者路由器与所述调试装置之间的通信路径中通过所述网状网络的一个或多个路由器来将所接收到的消息转发到所述调试装置,并且其中,所述路由器中的一个路由器是将所述网状网络连接到外部网络的边界路由器。

[0227] 一种将加入装置安全地加入到网状网络的方法包括:在加入者路由器处从请求加入所述网状网络的所述加入装置接收DTLS-客户端Hello消息;将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中;将所述DTLS中继接收通知消息传送到所述网状网络的调试装置;从所述调试装置接收DTLS中继传送通知消息;向所述加入装置传送所述DTLS中继传送通知消息的内容,所述内容有效地使得所述加入装置能够加入所述网状网络;从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示;从所述调试装置接收在所述调试装置与所述加入装置之间共享的密钥加密密钥KEK;以及响应于接收到所述指示,使用所述KEK来将所述网络证书从所述加入者路由器传送到所述加

入装置以使所述网络证书的通信安全。

[0228] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：从所述加入装置接收信标请求，以及从所述加入者路由器向所述加入装置传送信标；所述信标包括网络名称和操纵数据，所述操纵数据指示被允许加入所述网状网络的一个或多个加入装置；所述利用用户数据报协议(UDP)从所述加入装置接收所述DTLS-客户端Hello消息(；所述DTLS中继接收通知消息包括：所述加入装置的地址、所述加入者路由器的地址以及所接收到的DTLS-客户端Hello消息；所述DTLS中继传送通知消息包括：所述加入装置的所述地址、所述加入者路由器的所述地址、以及DTLS-Hello验证消息；所述将所述DTLS中继传送通知消息的所述内容传送到所述加入装置有效地在所述调试装置与所述加入装置之间建立安全的通信会话；所述安全的通信会话能够用来执行所述加入装置的配备；以及对从加入装置传送到所述调试装置的DTLS中继接收通知消息的传输应用速率限制。

[0229] 一种作为加入者路由器所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：经由所述网状网络接口从请求加入所述网状网络的加入装置接收DTLS-客户端Hello消息；将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中；开始将所述DTLS中继接收通知消息传送到所述网状网络的调试装置；从所述调试装置接收DTLS中继传送通知消息；开始向所述加入装置传送所述DTLS中继传送通知消息的内容，所述内容有效地使得所述加入装置能够加入所述网状网络；从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示；从所述调试装置接收在所述调试装置与所述加入装置之间共享的密钥加密密钥KEK；以及响应于所述指示，开始使用所述KEK来将所述网络证书从所述加入者路由器传送到所述加入装置以使所述网络证书的通信安全。

[0230] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：经由所述网状网络接口从所述加入装置接收信标请求，以及开始从所述加入者路由器向所述加入装置传送信标；所述调试应用被配置成利用用户数据报协议(UDP)来从所述加入装置接收所述DTLS-客户端Hello消息；所述DTLS中继接收通知消息包括：所述加入装置的地址、所述加入者路由器的地址、所接收到的DTLS-客户端Hello消息，并且其中，所述DTLS中继传送通知消息包括：所述加入装置的所述地址、所述加入者路由器的所述地址以及DTLS-Hello验证消息；传送到所述加入装置的所述DTLS中继传送通知消息的所述内容有效地在所述调试装置与所述加入装置之间建立安全的通信会话；所述安全的通信会话可用来执行所述加入装置的配备。

[0231] 一种网状网络系统包括：加入装置，所述加入装置被配置成请求加入网状网络；以及加入者路由器，所述加入者路由器被配置成：从请求加入所述网状网络的所述加入装置接收DTLS-客户端Hello消息；将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中；将所述DTLS中继接收通知消息传送到所述网状网络的调试装置；从所述调试装置接收DTLS中继传送通知消息；向所述加入装置传送所述DTLS中继传送通知消息的内容，所述内容有效地使得所述加入装置能够加入所述网状网络；从所述调试装置接收所述加入装置将被委托接收所述网状网络的网络证书的指示；从所述调试装置接收在所述调试装置与所述加入装置之间共享的密钥加密密钥KEK；并且响应于所述指示，使用所述KEK来将所

述网络证书从所述加入者路由器传送到所述加入装置以使所述网络证书的通信安全。

[0232] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：从所述加入装置接收信标请求，以及从所述加入者路由器向所述加入装置传送信标；所述信标包括网络名称和操纵数据，所述操纵数据指示被允许加入所述网状网络的一个或多个加入装置；所述加入者路由器被配置成利用用户数据报协议(UDP)来从所述加入装置接收所述DTLS-客户端Hello消息；并且所述DTLS中继接收通知消息包括：所述加入装置的地址、所述加入者路由器的地址、所接收到的DTLS-客户端Hello消息，并且其中，所述DTLS中继传送通知消息包括：所述加入装置的所述地址、所述加入者路由器的所述地址以及DTLS-Hello验证消息。

[0233] 一种对于要成为调试者来对要加入网状网络的一个或多个加入装置进行调试的调试装置进行授权的方法包括：在边界路由器处从要成为所述网状网络的所述调试者的所述调试装置接收请愿；将所接收到的请愿传送到所述网状网络的领导者装置；从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；以及响应于所述接收到所述响应，向所述调试装置传送对所述请愿的所述接受或所述拒绝的指示。

[0234] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：由所述边界路由器通告所述网状网络对于调试装置的可用性，所述接收所述请愿响应于所述调试装置接收到所述通告；在所述边界路由器处从所述调试装置接收用于安全地连接到所述边界路由器的请求；安全的连接使用数据报传输层安全DTLS来建立；传送对所述请愿的接受的所述指示建立安全的调试会话；向所述边界路由器注册所述调试装置的身份以建立安全的调试通信会话，所述注册包括向所述边界路由器提供加密调试证书，其中，所述加密调试证书是从由用户输入到所述调试装置的调试证书导出的；所述边界路由器包括能够用来向所述网状网络认证所述调试装置的所述加密调试证书的副本；并且所述加密调试证书的所述副本是先前从所述调试证书导出的，所述调试证书被注入到所述网状网络的导出了所述加密调试证书的所述副本的所述领导者装置中，并且所述领导者装置将所述加密调试证书的所述副本安全地传递到所述边界路由器。

[0235] 一种作为边界路由器所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：经由所述网状网络接口从调试装置接收要成为所述网状网络的调试者来对要加入所述网状网络的一个或多个加入装置进行调试的调试装置的请愿；开始将所接收的请愿发送到所述网状网络的领导者装置；从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；并且响应于所接收到的对所述请愿的响应，开始向所述调试装置传送对所述请愿的所述接受或所述拒绝的指示。

[0236] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述调试应用被配置成通告所述网状网络对于调试装置的可用性，并且响应于所述调试装置接收到所通告的可用性而接收所述请愿，并且所通告的可用性使用包括多播域名系统mDNS的服务发现协议来执行；所述调试应用被配置成从所述调试装置接收安全地连接到所述边界路由器的请求，以及使用数据报传输层安全DTLS来建立安全的连接；由所述领导者装置接受所述请愿对所述调试装置进行授权以成为所述网状网络的所述调试者，对所述请愿的接受使得所述领导者装置能够更新内部状态，所述内部状态跟踪所述网状网络的活动调试者，

将所述网状网络的准许加入标志设置为真，并且在所述网状网络内传播调试数据集，并且所传送的对所述请愿的接受的指示建立安全的调试会话；所述调试应用被配置成向所述边界路由器注册所述调试装置的身份以建立安全的调试通信会话，包括提供给所述边界路由器的加密调试证书，所述加密调试证书是从由用户输入到所述调试装置的调试证书导出的，并且所述边界路由器包括可用来向所述网状网络认证所述调试装置的所述加密调试证书的副本；以及所述调试装置和所述边界路由器通过除所述网状网络以外的网络进行通信；并且另一个网络是Wi-Fi网络或以太网网络中的一个。

[0237] 一种网状网络系统，包括：调试装置，所述调试装置被配置成请愿成为调试者来对要加入网状网络的一个或多个加入装置进行调试；以及边界路由器，所述边界路由器被配置成：从所述调试装置接收要成为所述网状网络的所述调试者的所述调试装置的请愿；将所接收到的请求发送到所述网状网络的领导者装置；从所述领导者装置接收对所述请愿的响应，所述响应指示对所述请愿的接受或拒绝；并且向所述调试装置传送对所述请愿的接受或拒绝的指示。

[0238] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：所述边界路由器被配置成通告所述网状网络对于调试装置的可用性，并且响应于所述调试装置接收到所述通告而接收所述请愿；所述调试装置和所述边界路由器通过除所述网状网络以外的网络进行通信；另一个网络是Wi-Fi网络或以太网网络中的一个；以及所述边界路由器被配置成传送对所述请愿的接受的所述指示以建立安全的调试会话。

[0239] 一种由网状网络的领导者装置实现的方法包括：由领导者装置接收用于接受调试装置作为调试者来对要加入所述网状网络的加入装置进行调试的请愿；确定接受还是拒绝所接收到的请愿；传送包括所述确定的指示的响应；以及响应于所述确定为接受而更新内部状态，所述内部状态跟踪所述网状网络的活动调试者。

[0240] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：从所述调试装置接收用于针对所述网状网络开始加入模式的命令；在所述网状网络内传播调试数据集；所述调试数据集包括：调试者会话标识符、调试者时间戳、加密调试者证书以及安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书；所述加密调试证书的导出通过应用密钥导出函数来执行，所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列；向所述边界路由器发送所述加密调试证书的副本，有效地使得所述边界路由器能够向所述网状网络认证所述调试装置；以及当所述调试者在所述网状网络上活动时，所述调试数据集还包括所述边界路由器的位置。

[0241] 一种作为网状网络的领导者装置所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于所述网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：经由所述网状网络接口接收用于接受调试装置作为调试者来对要加入所述网状网络的加入装置进行调试的请愿；确定接受还是拒绝所接收到的请愿；开始传送响应，所述响应包括接受还是拒绝所接收到的请愿的确定的指示；以及响应于所述确定是对所接收到的请愿的接受而更新内部状态，所述内部状态跟踪所述网状网络的活动调试者。

[0242] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述调

试应用被配置成从所述调试装置接收用于针对所述网状网络开始加入模式的命令;所述调试应用被配置成在所述网状网络内传播调试数据集;所述调试数据集包括:调试者会话标识符、调试者时间戳、加密调试者证书以及安全策略,所述安全策略指示哪些安全相关操作在所述网状网络中被允许,所述调试应用还被配置成从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书,其中,所述加密调试证书的导出通过应用密钥导出函数来执行,所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列;所述调试应用被配置成向所述边界路由器发送所述加密调试证书的副本,有效地使得所述边界路由器能够向所述网状网络认证所述调试装置;以及当所述调试者在所述网状网络上活动时,所述调试数据集还包括所述边界路由器的位置。

[0243] 一种网状网络系统包括:调试装置,所述调试装置被配置成请愿成为调试者来对要加入网状网络的调试一个或多个加入装置进行调试;以及所述网状网络的领导者装置,所述领导者装置被配置成:接收用于接受所述调试装置作为所述调试者来调试所述加入装置以加入所述网状网络的请愿;确定接受还是拒绝所接收到的请愿;传送包括关于接受还是拒绝所接收到的请愿的确定的指示的响应;并且响应于所述确定为接受而更新内部状态,所述内部状态跟踪所述网状网络的活动调试者。

[0244] 替选地或除上面描述的网状网络系统之外,以下各项中的任一项或组合:所述领导者装置被配置成从所述调试装置接收用于针对所述网状网络开始加入模式的命令;所述领导者装置被配置成在所述网状网络内传播调试数据集;所述调试数据集包括:调试者会话标识符、调试者时间戳、加密调试者证书、以及安全策略,所述安全策略指示哪些安全相关操作在所述网状网络中被允许,所述领导者装置还被配置成从在所述领导者装置的调试期间被注入到所述领导者装置中的调试证书导出所述加密调试证书,其中,所述加密调试证书的导出通过应用密钥导出函数来执行,所述密钥导出函数使用基于密码的消息认证码CMAC来多次执行散列;所述领导者装置被配置成向所述边界路由器发送所述加密调试证书的副本,有效地使得所述边界路由器能够向所述网状网络认证所述调试装置;以及当所述调试者在所述网状网络上活动时,所述调试数据集还包括所述边界路由器的位置。

[0245] 一种安全地建立网络通信会话以便将一个或多个加入装置加入到网状网络的方法包括:在调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话;激活针对所述网状网络的加入;由所述调试装置从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求;在所述调试装置与所述加入装置之间建立安全的加入者通信会话;以及将所述加入装置加入到所述网状网络。

[0246] 替选地或除上面描述的方法之外,以下各项中的任一项或组合:建立所述安全的调试通信会话包括:从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿,以及从所述领导者装置接收对所述请愿的接受的指示;激活针对所述网状网络的加入包括所述调试装置开始加入模式,所述加入模式使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求;激活针对所述网状网络的加入包括向领导者装置发送用于使所述网状网络变得能够加入的管理消息,所述管理消息有效地使得所述领导者装置能够更新所述网状网络的网络数据,并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置,所述网络数据包括所述网状网络可用于加入的指示;使用加密装置标识符来对所述加入装置进行认证;从所述加

入装置中的一个加入装置接收用于加入所述网状网络的所述请求是经由加入者路由器接收的，所述方法还包括：向所述加入者路由器传送所述加入装置将被委托接收所述网状网络的网络证书和密钥加密密钥KEK的指示，所述密钥加密密钥KEK在所述调试装置与所述加入装置之间共享，所述传送有效地使得所述加入者路由器能够使用所接收到的KEK来将所述网络证书安全地传送到所述加入装置以将所述加入装置调试到所述网状网络；从所述加入装置接收所述请求包括接收所述加入装置的加密装置标识符，并且其中，所述加密装置标识符是使用Juggling口令认证密钥交换J-PAKE从所述加入装置的装置标识符导出的；建立所述安全的加入者通信会话包括：由所述调试装置确定从所述加入装置接收到的所述加密装置标识符和由所述调试装置所述装置标识符的副本所导出的加密装置标识符相匹配，所述装置标识符的副本是作为来自用户的到所述调试装置的输入而接收的，以及使用所述加密装置标识符作为共享秘密来使所述加入者通信会话安全。

[0247] 一种作为用于将一个或多个加入装置加入到网状网络的调试装置所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于所述网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：在所述调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话；激活针对所述网状网络的加入；经由所述网状网络接口从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求；在所述调试装置与所述加入装置之间建立安全的加入者通信会话；以及将所述加入装置加入到所述网状网络。

[0248] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述调试应用被配置成：从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿，并且从所述领导者装置接收对所述请愿的接受的指示；所述调试应用被配置成所述通过开始加入模式来激活针对所述网状网络的加入，所述加模式致使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求；所述调试应用被配置成所述通过向领导者装置发送用于使所述网状网络变得可加入的管理消息来激活针对所述网状网络的加入，所述管理消息使得所述领导者装置能够更新所述网状网络的网络数据，并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置，所述网络数据包括所述网状网络可用于加入的指示；从所述加入装置接收的所述请求包括所述加入装置的加密装置标识符，并且其中，所述加密装置标识符是使用Juggling口令认证密钥交换J-PAKE从所述加入装置的装置标识符导出的；所述调试应用被配置成建立所述安全的加入者通信会话还被配置成：确定从所述加入装置接收到的所述加密装置标识符和由所述调试装置从所述装置标识符的副本所导出的加密装置标识符相匹配，所述装置标识符的副本是作为来自用户的到所述调试装置的输入而接收的；并且使用所述加密装置标识符作为共享秘密来使所述加入者通信会话安全；所述调试装置被配置成转发来自要加入所述网状网络的所述加入装置的所述请求，所述请求被所述网状网络中的一个或多个路由器装置转发到所述调试装置。

[0249] 一种网状网络系统包括：一个或多个加入装置，所述一个或多个加入装置被配置成请求加入网状网络；以及所述网状网络的调试装置，所述调试装置被配置成：在所述调试装置与所述网状网络的边界路由器之间建立安全的调试通信会话；激活针对所述网状网络的加入；从所述加入装置中的一个加入装置接收用于加入所述网状网络的请求；在所述调

试装置与所述加入装置之间建立安全的加入者通信会话;并且将所述加入装置加入到所述网状网络。

[0250] 替选地或除上面描述的网状网络系统之外,以下各项中的任一项或组合:用于建立所述安全的调试通信会话的所述调试装置被配置成:从所述调试装置向所述网状网络的领导者装置发送用于请求接受所述调试装置作为所述网状网络的活动调试者的请愿,并且从所述领导者装置接收对所述请愿的接受的指示;所述调试装置被配置成所述通过开始加入模式来激活针对所述网状网络的加入,所述加入模式致使所述网状网络中的一个或多个路由器通告所述网状网络正在接受加入请求;所述调试装置被配置成所述通过向领导者装置发送用于使所述网状网络变得可加入的管理消息来激活针对所述网状网络的加入,所述管理消息使得所述领导者装置能够更新所述网状网络的网络数据,并且将所述网络数据传播到所述网状网络中的一个或多个路由器装置,所述网络数据包括所述网状网络能够用于加入的指示;所述调试装置被配置成:所述经由加入者路由器从所述加入装置中的一个加入装置接收用于加入所述网状网络的所述请求,以及向所述加入者路由器传送所述加入装置将被委托接收所述网状网络的网络证书和密钥加密密钥KEK的指示,所述密钥加密密钥KEK在所述调试装置与所述加入装置之间共享,所发送的指示使得所述加入者路由器能够使用所接收到的KEK来将所述网络证书安全地发送到所述加入装置以将所述加入装置调试到所述网状网络。

[0251] 一种在网状网络中提供加入装置的方法包括:在调试装置与所述网状网络的边界路由器之间建立调试通信会话;在所述加入装置与所述调试装置之间建立加入者通信会话;向所述加入装置发送调试信息,所述调试信息可由所述加入装置使用来加入所述网状网络;从所述加入装置接收调试者应用的位置的指示;以及执行所述调试者应用以提供所述加入装置。

[0252] 替选地或除上面描述的方法之外,以下各项中的任一项或组合:利用所接收到的指示来检索所述调试者应用;所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL;所述调试者应用通过互联网从云服务中检索;所述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中;响应于完成所述加入装置的所述配备,使所述加入装置的调试结束,所述结束有效地使得所述加入装置能够加入所述网状网络;所述加入装置的所述配备包括更新所述加入装置上的软件;所述加入装置的所述配备包括将所述加入装置链接到云服务上的用户账户;所述加入装置的所述配备包括配置所述加入装置;以及所述配置是与所述网状网络中的其它装置有关的本地配置。

[0253] 一种作为调试装置所实现的网状网络装置,所述网状网络装置包括:网状网络接口,所述网状网络接口被配置成用于网状网络中的通信;用于实现调试应用的存储器和处理器系统,所述调试应用被配置成:在所述调试装置与所述网状网络的边界路由器之间建立调试通信会话;在所述加入装置与所述调试装置之间建立加入者通信会话;向所述加入装置发送调试信息,所述调试信息可由所述加入装置使用来加入所述网状网络;从所述加入装置接收调试者应用的位置的指示;以及执行所述调试者应用以配备所述加入装置。

[0254] 替选地或除上面描述的网状网络装置之外,以下各项中的任一项或组合:所述调试应用被配置成利用所接收到的指示来检索所述调试者应用;所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL;所述调试者应用通过互联网从云服务中检索;所

述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中。

[0255] 一种网状网络系统包括：加入装置，所述加入装置被配置成请求加入网状网络；以及所述网状网络的调试装置，所述调试装置被配置成：在所述调试装置与所述网状网络的边界路由器之间建立调试通信会话；在所述加入装置与所述调试装置之间建立加入者通信会话；向所述加入装置发送调试信息，所述调试信息可由所述加入装置使用来加入所述网状网络；从所述加入装置接收调试者应用的位置的指示；以及执行所述调试者应用以配备所述加入装置。

[0256] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：所述调试应用被配置成利用所接收到的指示来检索所述调试者应用；所接收到的所述调试者应用的所述位置的指示是统一资源定位符URL；所述调试者应用通过互联网从云服务中检索；并且所述调试装置使用所接收到的URL来确定所述调试者应用是否被存储在所述调试装置的存储器中。

[0257] 一种标识被允许加入网状网络的装置的方法包括：确定所述网状网络的操纵数据，所述操作数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中发送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够标识所述装置被允许加入所述网状网络。

[0258] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64；所述确定所述网状网络的所述操纵数据还包括针对附加装置标识符来确定所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联；所述传播所述操纵数据有效地使得所述装置能够区分所述网状网络和其它网络；所述其它网络是IEEE 802.15.4网络；以及所述操纵数据指示调试者在所述网状网络上是活动的。

[0259] 一种作为调试装置所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：确定所述网状网络的操纵数据，所述操作数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中发送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够识别所述装置被允许加入所述网状网络。

[0260] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64；用于确定所述网状网络的所述操纵数据的所述调试应用被配置成针对附加装置标识符来确定所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联；所述操纵数据可由所述装置使用来区分所述网状网络和其它网络；所述其它网络是IEEE 802.15.4网络；以及所述操纵数据指示调试者在所述网状网络上是活动的。

[0261] 一种网状网络系统包括：加入装置，所述加入装置被配置成请求加入网状网络；以及所述网状网络的调试装置，所述调试装置被配置成：确定所述网状网络的操纵数据，所述操作数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联；以及将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中传送所述操纵数据，所述操纵数据有效地使得与所述装置标识符相关联的所述装置能够识别所述装置被允许加入所述网状网络。

[0262] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：所述操纵数据包括所述装置标识符的16位循环冗余校验CRC16；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64；用于确定所述网状网络的所述操纵数据的所述调试装置被配置成针对附加装置标识符来确定所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联；所述操纵数据使得所述装置能够区分所述网状网络和其它网络；所述操纵数据指示调试者在所述网状网络上是活动的。

[0263] 一种识别被允许加入网状网络的装置的方法包括：确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及将所述操纵数据从所述网状网络的调试装置传播到所述网状网络中的一个或多个路由器，所述传播使得所述一个或多个路由器能够在信标消息中发送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的值的集合与在所述装置处确定的值的第二集合进行比较以识别所述装置被允许加入所述网状网络。

[0264] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：确定所述操纵数据包括：对所述装置标识符应用第一散列函数以产生第一散列值，对所述装置标识符应用第二散列函数以产生第二散列值，对所述第一散列值执行模运算以确定所述布隆过滤器中的第一位字段位置，对所述第二散列值执行所述模运算以确定所述布隆过滤器中的第二位字段位置，将所述布隆过滤器的所述第一位字段位置中的值设置为一，并且将所述布隆过滤器的所述第二位字段位置中的值设置为一；所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI；用于所述模运算的除数是所述布隆过滤器的位阵列的长度；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64；所述装置标识符是所述EUI-64的最低有效二十四位；确定所述网状网络的所述操纵数据还包括针对附加装置标识符来确定所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加装置相关联；将所述操纵数据的值设置成值为零，这禁用针对所述网状网络的加入；将所述操纵数据中的所有位字段值设置成值为一以指示所述网状网络对任何装置来说是能够加入的。

[0265] 一种作为调试装置所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用存储器和处理器系统，所述调试应用被配置成：确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及将所述操纵数据传播到所述网状网络中的一个或多个路由器，所述传播有效地使得所述一个或多个路由器能够在信标

消息中发送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的值的集合与在所述装置处确定的值的第二集合进行比较以识别所述装置被允许加入所述网状网络。

[0266] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述调试应用被配置成：对所述装置标识符应用第一散列函数以产生第一散列值，对所述装置标识符应用第二散列函数以产生第二散列值，对所述第一散列值执行模运算以确定所述布隆过滤器中的第一位字段位置，对所述第二散列值执行所述模运算以确定所述布隆过滤器中的第二位字段位置，将所述布隆过滤器的所述第一位字段位置中的值设置为一，并且将所述布隆过滤器的所述第二位字段位置中的值设置为一；所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI；用于所述模运算的除数是所述布隆过滤器的位阵列的长度；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64。

[0267] 一种网状网络系统包括：加入装置，所述加入装置被配置成请求加入网状网络；以及调试装置，所述调试装置被配置成：确定所述网状网络的操纵数据，所述操纵数据包括装置标识符的指示，所述装置标识符与被允许加入所述网状网络的装置相关联，并且所述指示被表示为在布隆过滤器中表示所述装置标识符的值的集合；以及将所述操纵数据传播到所述网状网络中的一个或多个路由器，所述传播有效地使得所述一个或多个路由器能够在信标消息中发送所述操纵数据，所述操纵数据使得与所述装置标识符相关联的所述装置能够将所述布隆过滤器中的值的集合与在所述装置处确定的值的第二集合进行比较以识别所述装置被允许加入所述网状网络。

[0268] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：所述调试装置被配置成：对所述装置标识符应用第一散列函数以产生第一散列值，对所述装置标识符应用第二散列函数以产生第二散列值，对所述第一散列值执行模运算以确定所述布隆过滤器中的第一位字段位置，对所述第二散列值执行所述模运算以确定所述布隆过滤器中的第二位字段位置，将所述布隆过滤器的所述第一位字段位置中的值设置为一，并且将所述布隆过滤器的所述第二位字段位置中的值设置为一；所述第一散列函数和所述第二散列函数是循环冗余校验CRC，所述第一散列函数是CRC16-CCITT，并且所述第二散列函数是CRC16-ANSI；用于所述模运算的除数是所述布隆过滤器的位阵列的长度；所述装置标识符是IEEE 64位扩展唯一标识符EUI-64；用于确定所述网状网络的所述操纵数据的所述计算装置被配置成针对附加装置标识符来确定所述操纵数据，所述附加装置标识符与被允许加入所述网状网络的附加加入者装置相关联。

[0269] 一种更新网状网络的节点中的调试数据的方法包括：在所述网状网络中的节点装置处接收调试数据集；将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述节点装置中的调试数据集中的存储时间戳进行比较；根据所述比较确定所述存储时间戳比所述接收时间戳更近；以及响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

[0270] 替选地或除上面描述的方法之外，以下各项中的任一项或组合：根据所述比较确

定所述接收时间戳比所述存储时间戳更近，并且响应于所述确定所述接收时间戳比所述存储时间戳更近，更新所存储的调试数据集以和所接收到的调试数据集匹配；所接收到的调试数据集包括：所述接收时间戳、调试证书、所述网状网络的网络名称以及安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；所述接收时间戳包括时间值以及所述时间值可追踪到协调世界时间UTC的指示；所述节点装置和所述领导者装置被先前调试到所述网状网络，并且其中，先前调试将相同的调试数据集存储在所述节点装置和所述领导者装置中；所述节点装置中所存储的调试数据集在所述网状网络的分割之后被更新，所述分割将所述网状网络分成多个分区，其中，所述网状网络的第一分区包括所述领导者装置，并且其中，所述网状网络的第二分区包括所述节点装置；所述分割停止通过所述网状网络的所述节点装置与所述领导者装置之间的通信；在所述节点装置处接收所述调试数据集发生在所述网状网络的所述第一分区和所述第二分区的合并之后，所述合并通过所述网状网络在所述节点装置与所述领导者装置之间重新建立通信路径；以及所述节点装置是路由器装置或适于用作路由器的装置。

[0271] 一种作为路由器所实现的网状网络装置，所述网状网络装置包括：网状网络接口，所述网状网络接口被配置成用于网状网络中的通信；用于实现调试应用的存储器和处理器系统，所述调试应用被配置成：接收调试数据集；将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述路由器中的调试数据集中的存储时间戳进行比较；根据所述比较确定所述存储时间戳比所述接收时间戳更近；以及响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

[0272] 替选地或除上面描述的网状网络装置之外，以下各项中的任一项或组合：所述调试应用被配置成：根据所述比较确定所述接收时间戳比所述存储时间戳更近，以及响应于所述接收时间戳比所述存储时间戳更近的确定，更新所存储的调试数据集以和所接收到的调试数据集匹配；所接收到的调试数据集包括：所述接收时间戳、调试证书、所述网状网络的网络名称、以及安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；所述接收时间戳包括时间值以及所述时间值对于协调世界时间UTC是能够追踪的的指示；所述路由器和所述领导者装置被先前调试到所述网状网络，并且其中，先前调试将相同的调试数据集存储在所述路由器和所述领导者装置中；以及所述路由器中所存储的调试数据集在所述网状网络的分割之后被更新，所述分割将所述网状网络分成多个分区，其中，所述网状网络的第一分区包括所述领导者装置，并且其中，所述网状网络的第二分区包括所述路由器。

[0273] 一种网状网络系统包括：领导者装置，所述领导者装置被配置成维持所述网状网络的调试数据；以及路由器装置，所述路由器装置被配置成：接收调试数据集；将包括在所接收到的调试数据集中的时间戳与包括在被存储在所述路由器中的调试数据集中的存储时间戳进行比较；根据所述比较确定所述存储时间戳比所述接收时间戳更近；并且响应于所述确定，向所述网状网络的领导者装置传送消息，所述消息包括所存储的调试数据集并且有效地使得所述领导者装置能够接受所存储的调试数据集作为所述网状网络的最近的调试数据集，并且将所存储的调试数据集传播到所述网状网络。

[0274] 替选地或除上面描述的网状网络系统之外，以下各项中的任一项或组合：所述路由器装置被配置成：根据所述比较确定所述接收时间戳比所述存储时间戳更近，以及响应于所述接收时间戳比所述存储时间戳更近的确定，更新所存储的调试数据集以和所接收到的调试数据集匹配；所接收到的调试数据集包括：所述接收时间戳、调试证书、所述网状网络的网络名称、以及安全策略，所述安全策略指示哪些安全相关操作在所述网状网络中被允许；所述接收时间戳包括时间值以及所述时间值对于协调世界时间UTC是能够追踪的的指示；以及所述路由器和所述领导者装置被先前调试到所述网状网络，并且其中，先前调试将相同的调试数据集存储在所述路由器和所述领导者装置中。

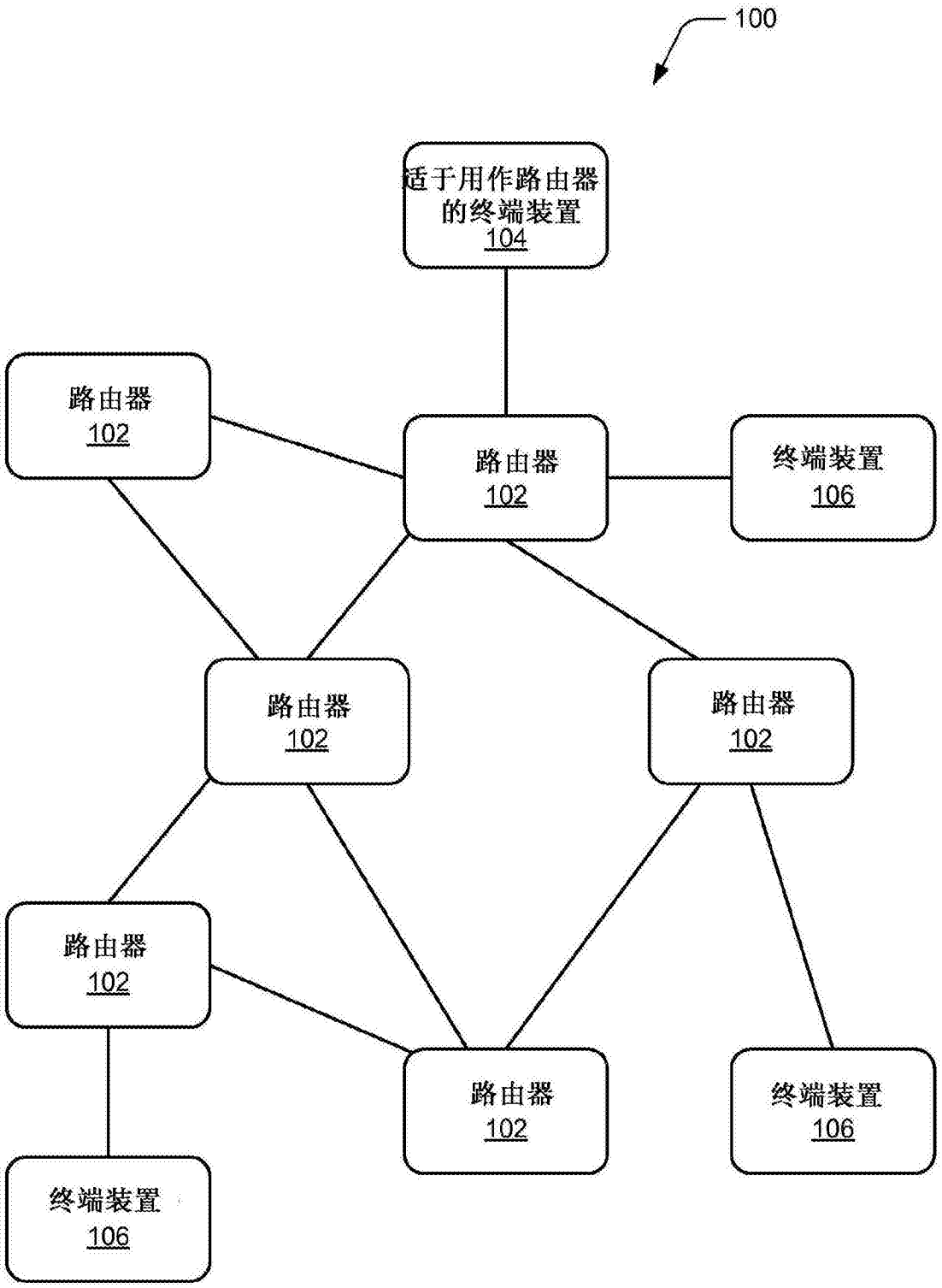

100
适于用作路由器的终端装置 104
路由器 102
路由器 102
终端装置 106
路由器 102
路由器 102
路由器 102
路由器 102
终端装置 106
终端装置 106

图1

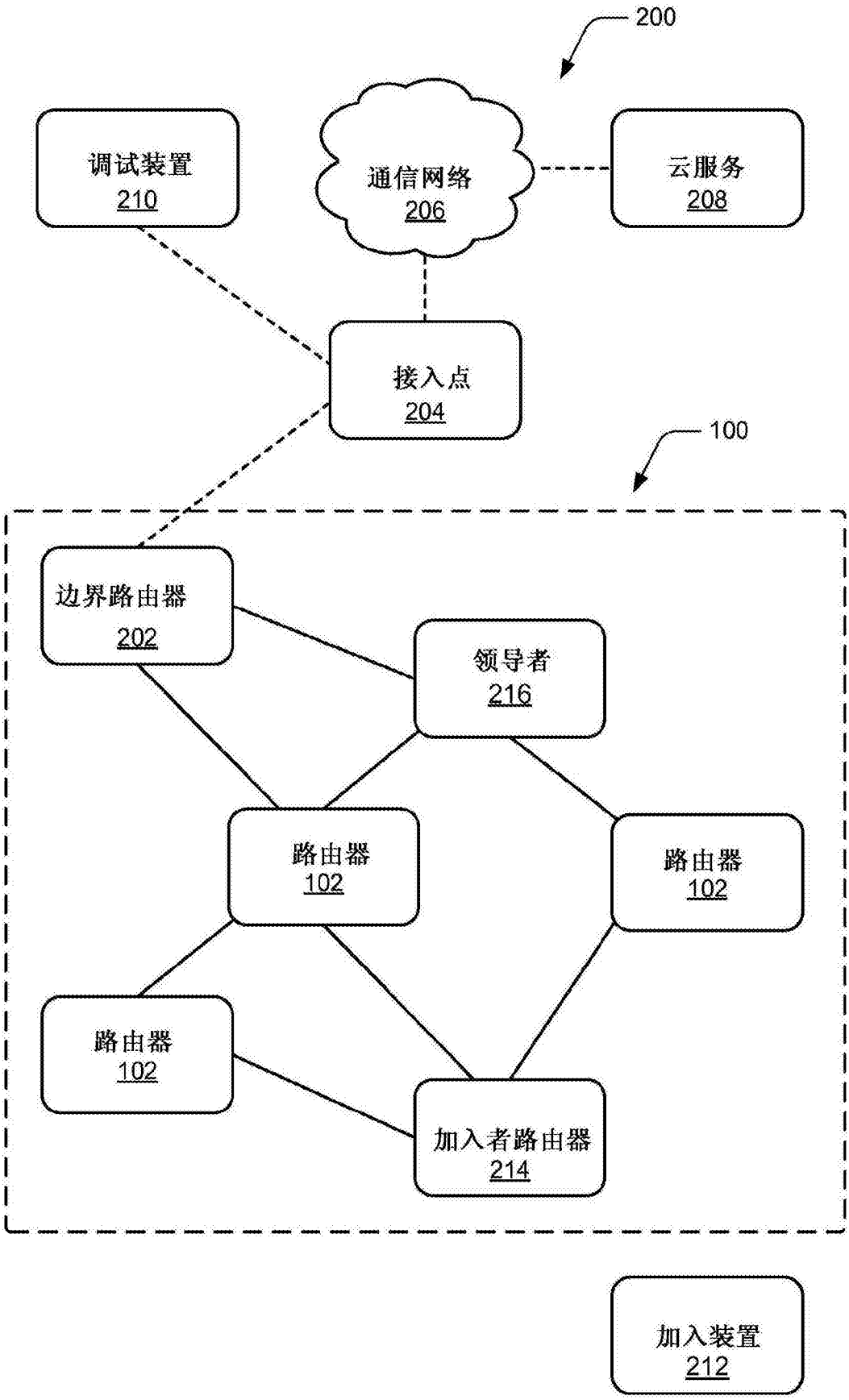

200
调试装置
210
通信网络
206
云服务
208
接入点
204
100
边界路由器
202
领导者
216
路由器
102
路由器
102
路由器
102
加入者路由器
214
加入装置
212

图2

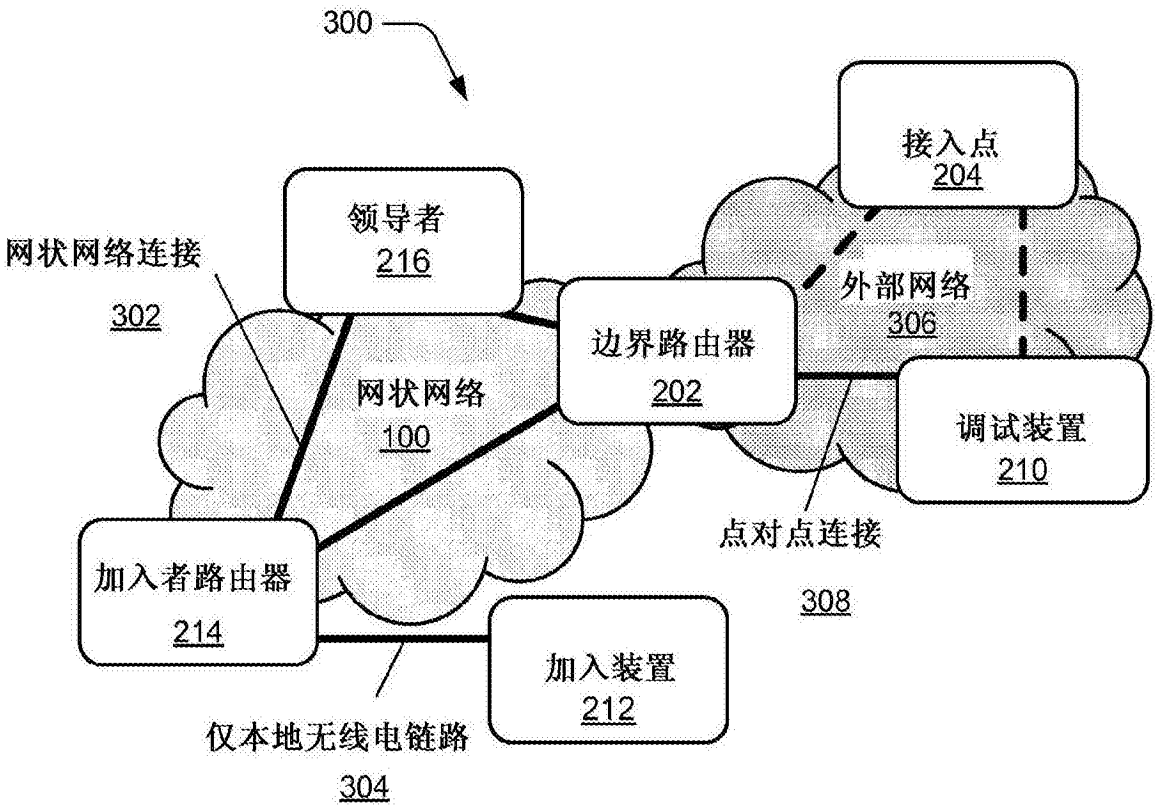

300
接入点
204
领导者
216
网状网络连接
302
外部网络
306
边界路由器
202
网状网络
100
调试装置
210
点对点连接
308
加入者路由器
214
加入装置
212
仅本地无线电链路
304

图3A

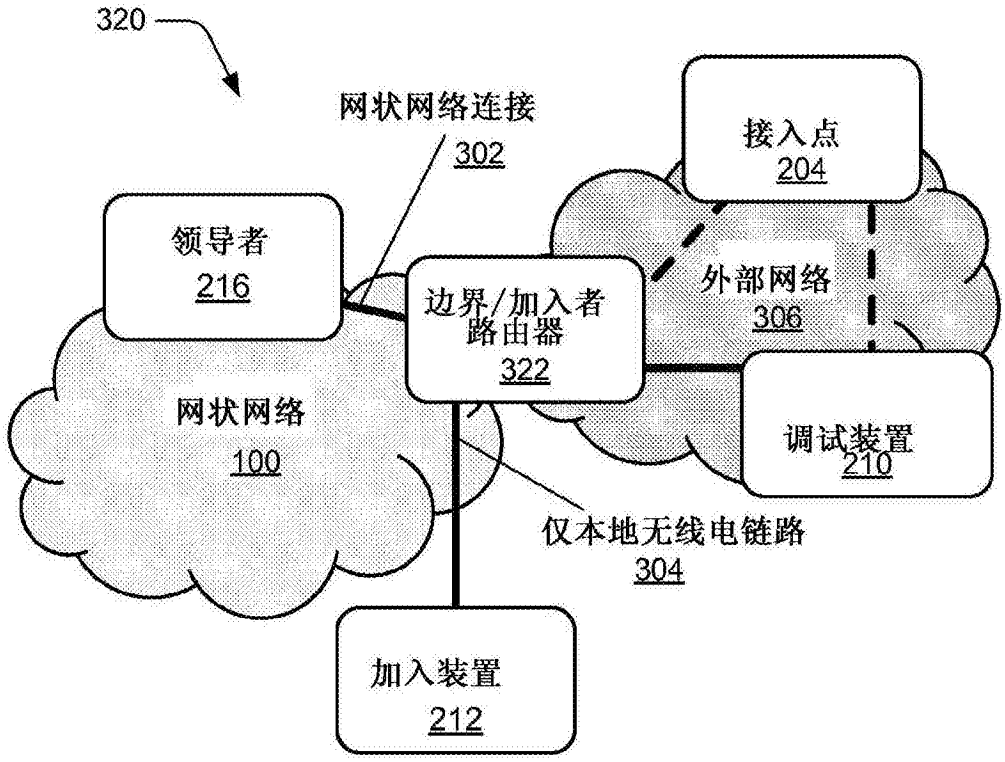

320
网状网络连接
302
接入点
204
领导者
216
外部网络
306
边界/加入者
路由器
322
网状网络
100
调试装置
210
仅本地无线电链路
304
加入装置
212

图3B

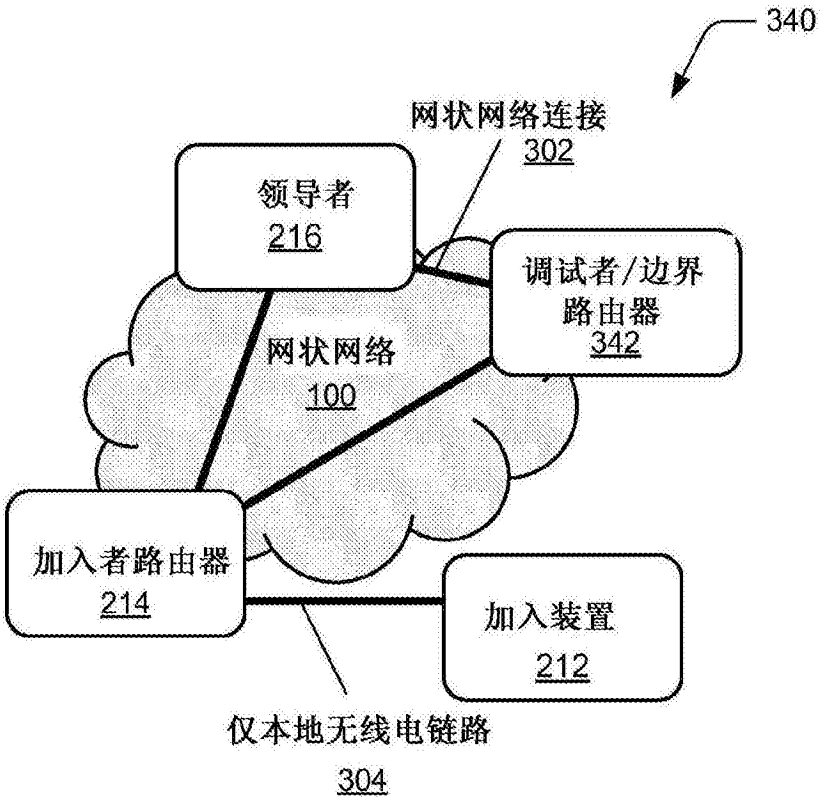

340
网状网络连接
302
领导者
216
调试者/边界
路由器
342
网状网络
100
加入者路由器
214
加入装置
212
仅本地无线电链路
304

图3C

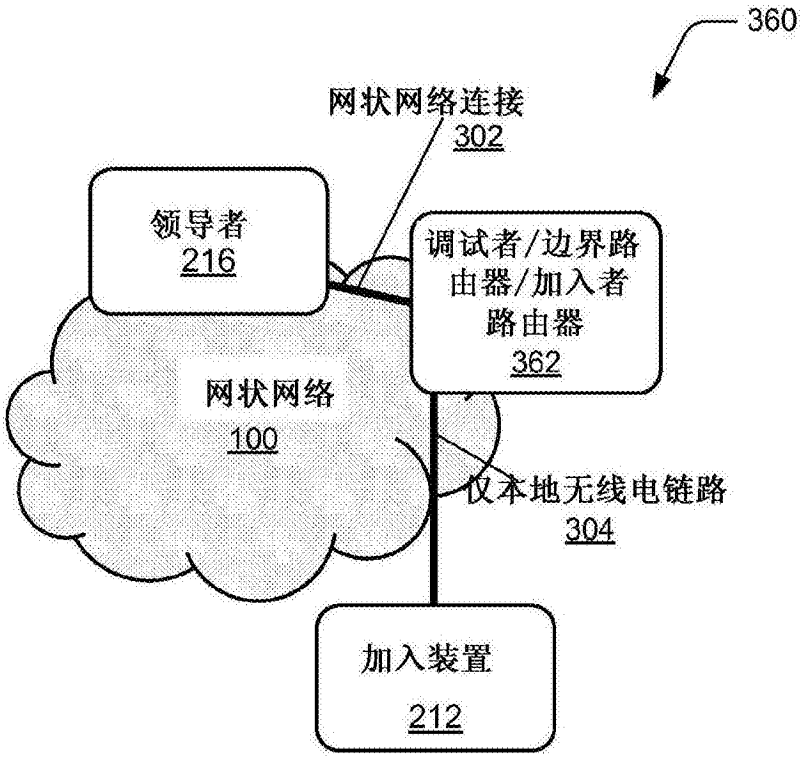

360
网状网络连接
302
领导者
216
调试者/边界路
由器/加入者
路由器
362
网状网络
100
仅本地无线电链路
304
加入装置
212

图3D

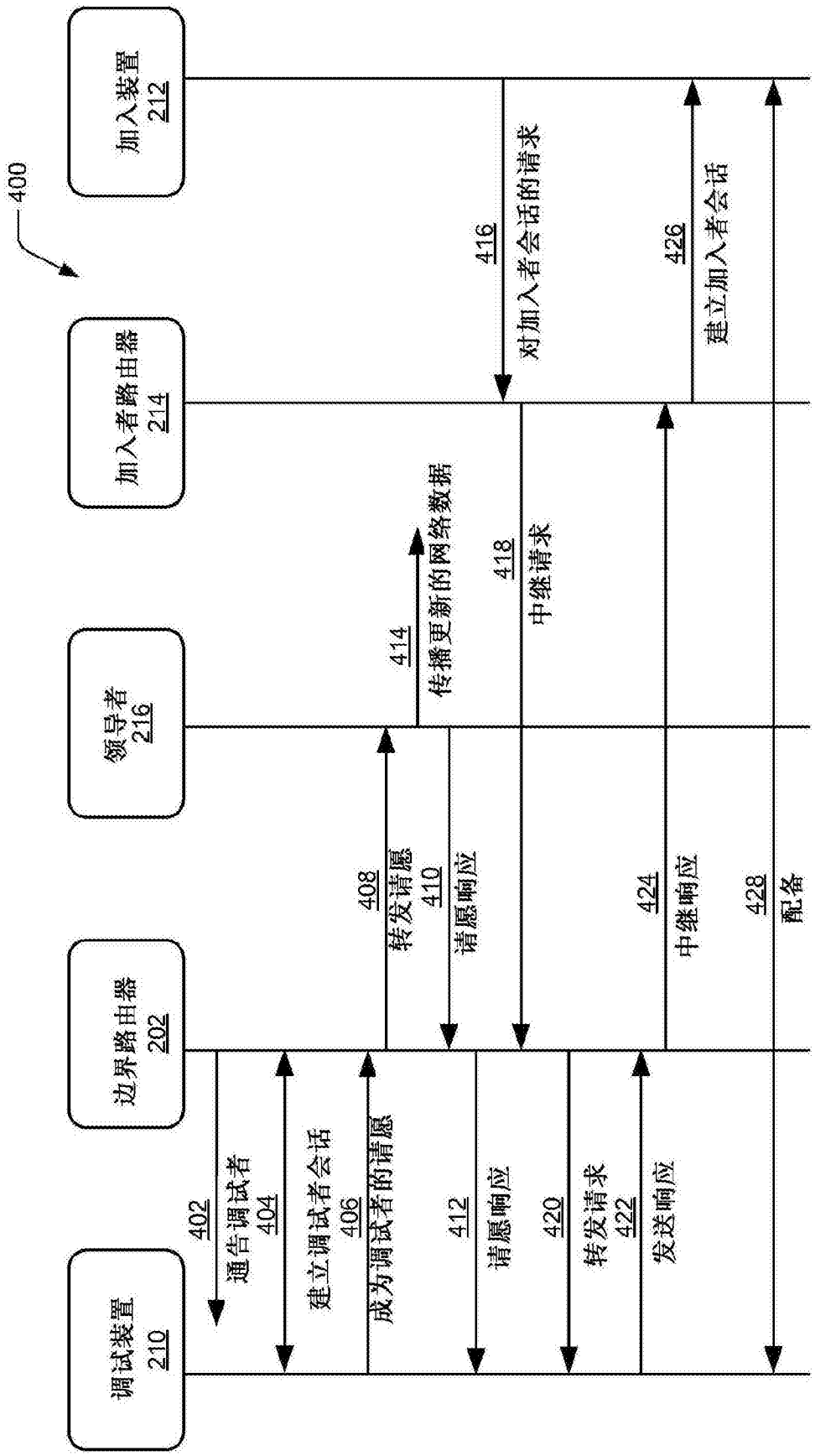

400
调试装置 210
边界路由器 202
领导者 216
加入者路由器 214
加入装置 212
402 通告调试者 404
建立调试者会话 406
成为调试者的请愿 408
转发请愿 410
请愿响应 412
传播更新的网络数据 414
中继请求 418
对加入者会话的请求 416
转发请求 422
发送响应 420
中继响应 424
建立加入者会话 426
配备 428

图4

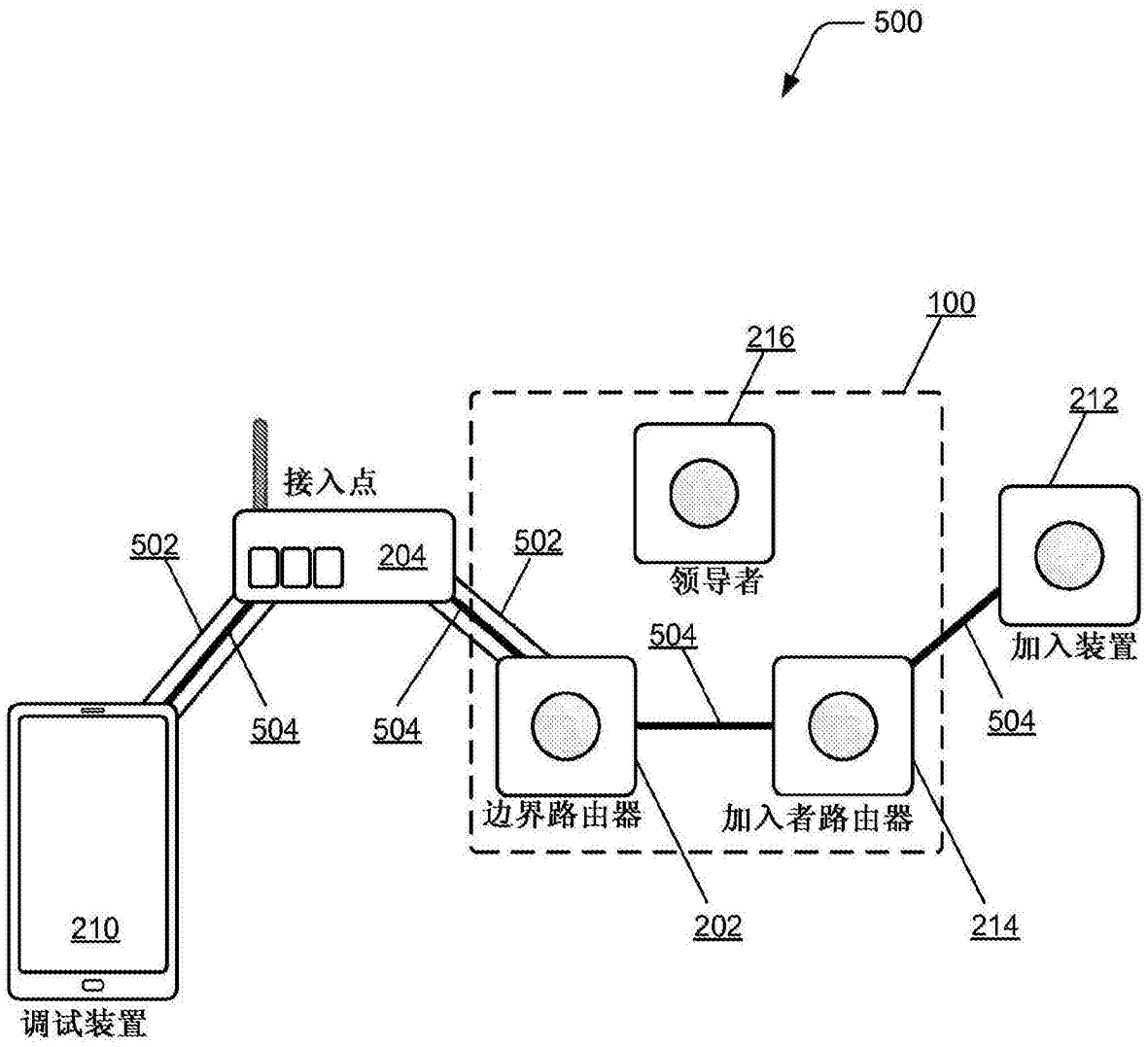

500
100
216
212
接入点
502
204
502
领导者
504
加入装置
504
504
504
边界路由器
加入者路由器
210
202
214
调试装置

图5

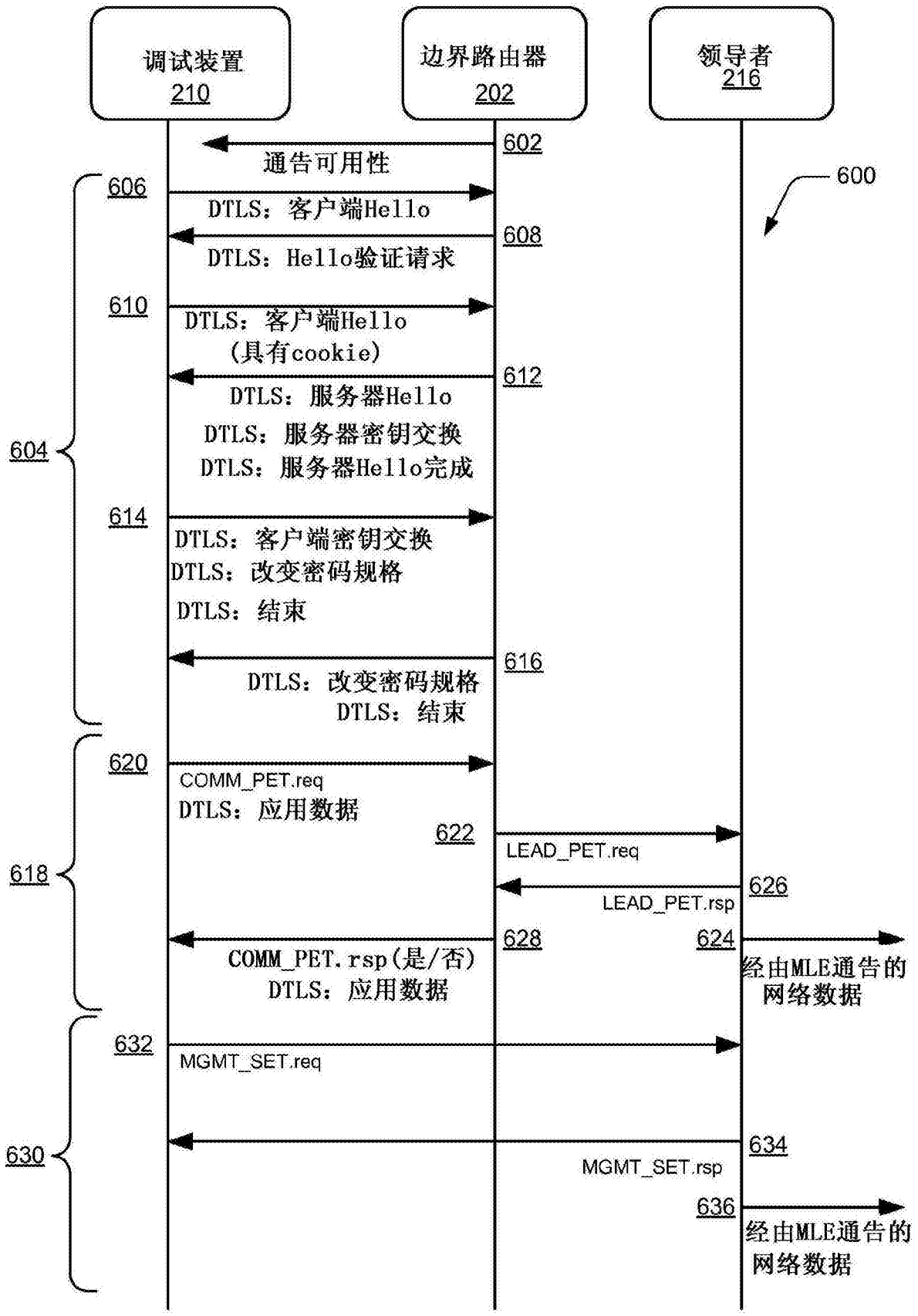

调试装置
210
边界路由器
202
领导者
216
600
602
通告可用性
606
DTLS：客户端Hello
608
DTLS：Hello验证请求
610
DTLS：客户端Hello
(具有cookie)
612
DTLS：服务器Hello
DTLS：服务器密钥交换
DTLS：服务器Hello完成
604
614
DTLS：客户端密钥交换
DTLS：改变密码规格
DTLS：结束
616
DTLS：改变密码规格
DTLS：结束
620
COMM_PET.req
DTLS：应用数据
622
LEAD_PET.req
618
626
LEAD_PET.rsp
628
624
COMM_PET.rsp(是/否)
DTLS：应用数据
经由MLE通告的
网络数据
632
MGMT_SET.req
630
634
MGMT_SET.rsp
636
经由MLE通告的
网络数据

图6

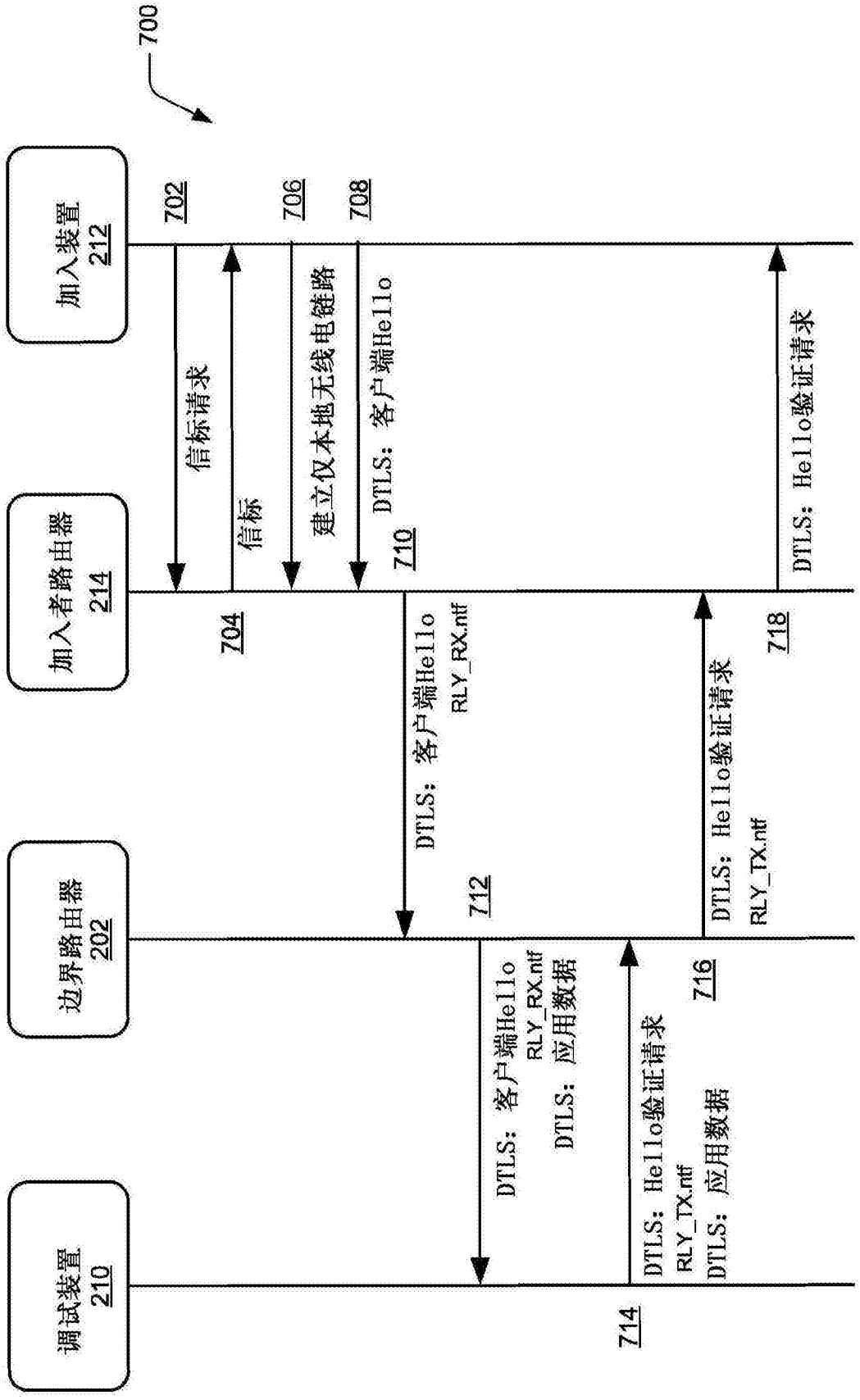

700
加入装置 212
加入者路由器 214
边界路由器 202
调试装置 210
702
704
706
708
710
712
714
716
718
信标请求
信标
建立仅本地无线电链路
DTLS：客户端Hello
DTLS：客户端Hello RLY_RX.ntf
DTLS：客户端Hello RLY_RX.ntf DTLS：应用数据
DTLS：Hello验证请求 RLY_TX.ntf DTLS：应用数据
DTLS：Hello验证请求 RLY_TX.ntf
DTLS：Hello验证请求

图7

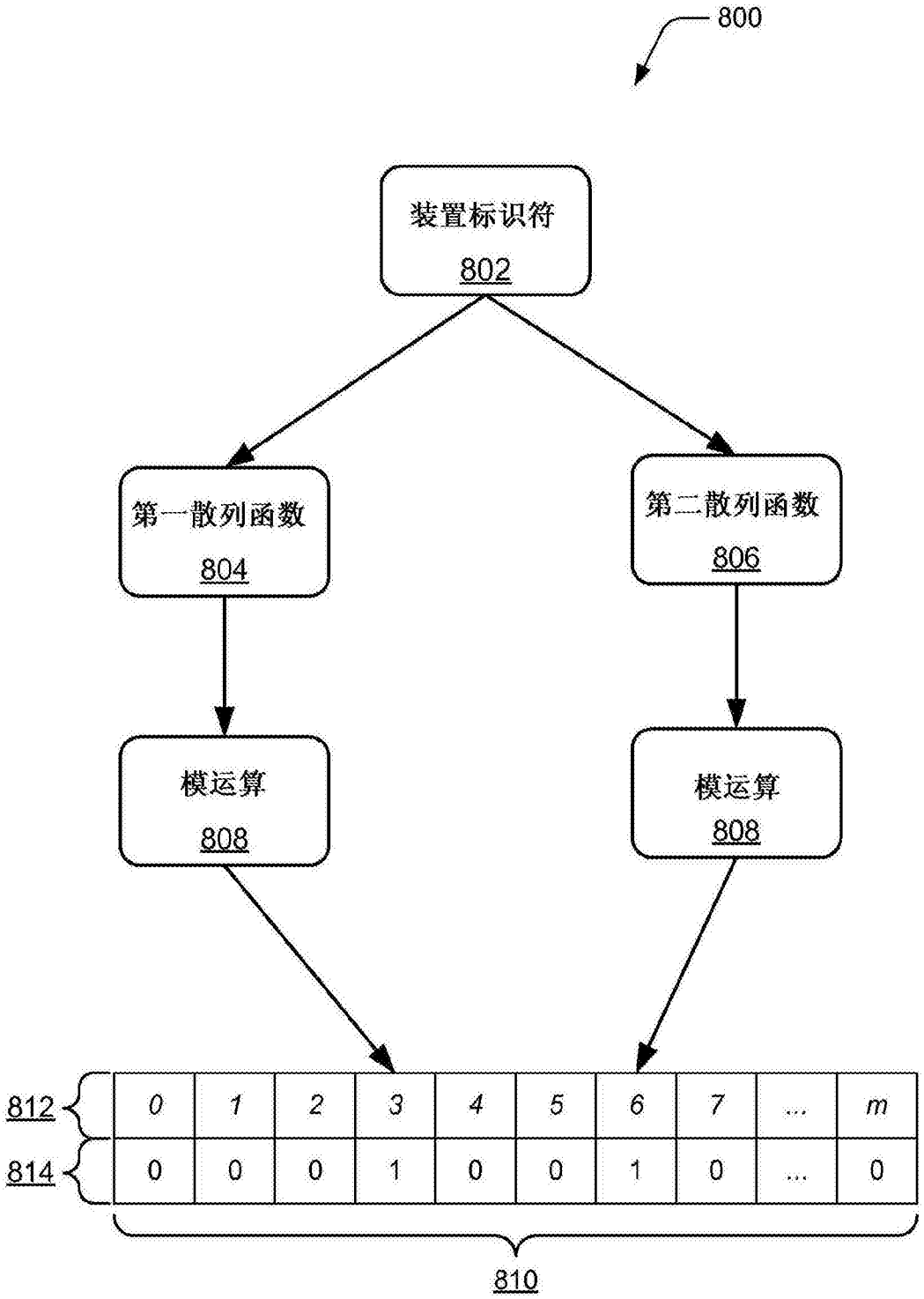

800
装置标识符
802
第一散列函数
804
第二散列函数
806
模运算
808
模运算
808
812
814
0 1 2 3 4 5 6 7 ... m
0 0 0 1 0 0 1 0 ... 0
810

图8

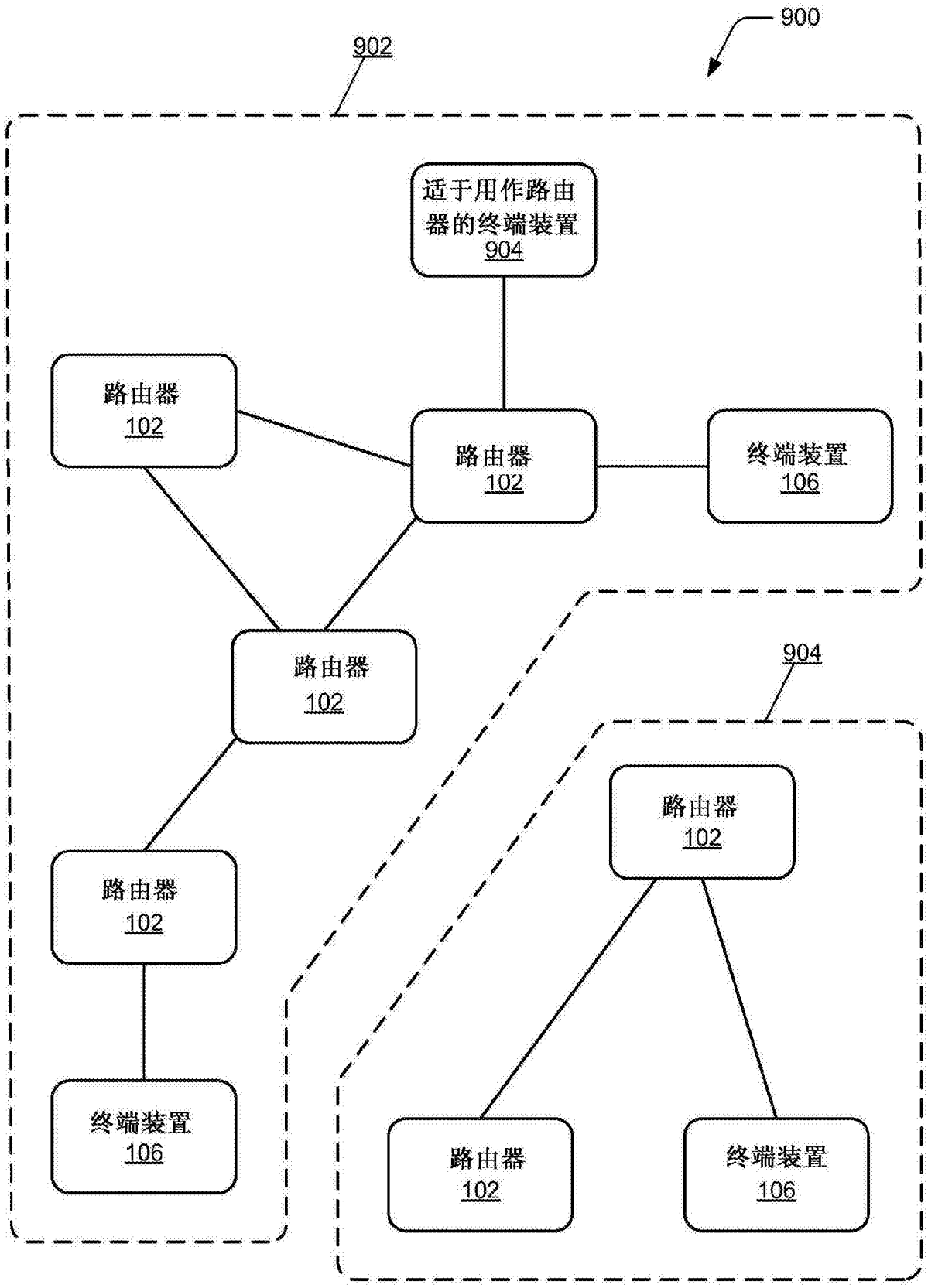

900
902
适于用作路由器的终端装置
904
路由器
102
路由器
102
终端装置
106
路由器
102
路由器
102
终端装置
106
904
路由器
102
路由器
102
终端装置
106

图9

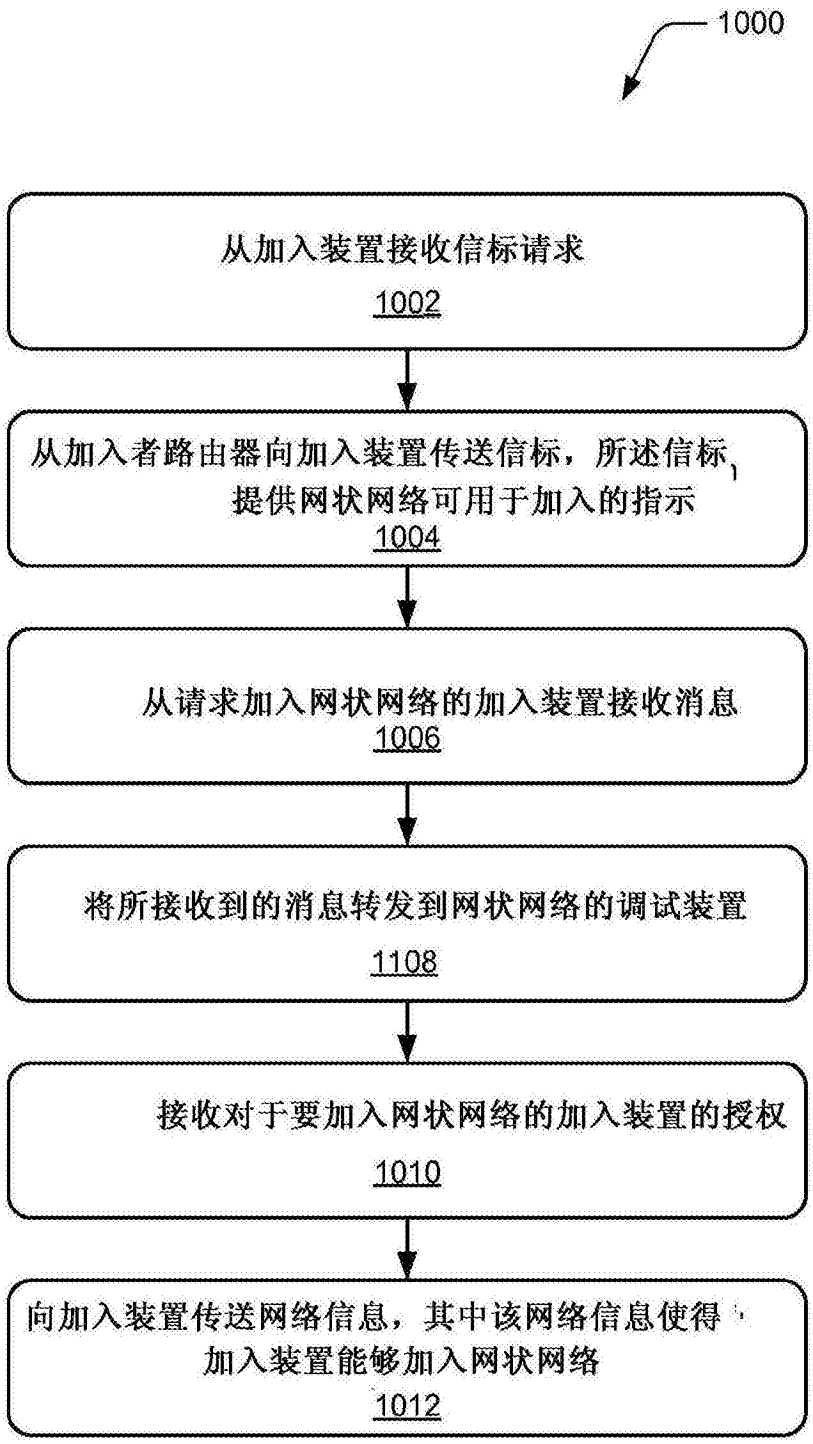

1000
从加入装置接收信标请求
1002
从加入者路由器向加入装置传送信标，所述信标提供网状网络可用于加入的指示
1004
从请求加入网状网络的加入装置接收消息
1006
将所接收到的消息转发到网状网络的调试装置
1108
接收对于要加入网状网络的加入装置的授权
1010
向加入装置传送网络信息，其中该网络信息使得加入装置能够加入网状网络
1012

图10

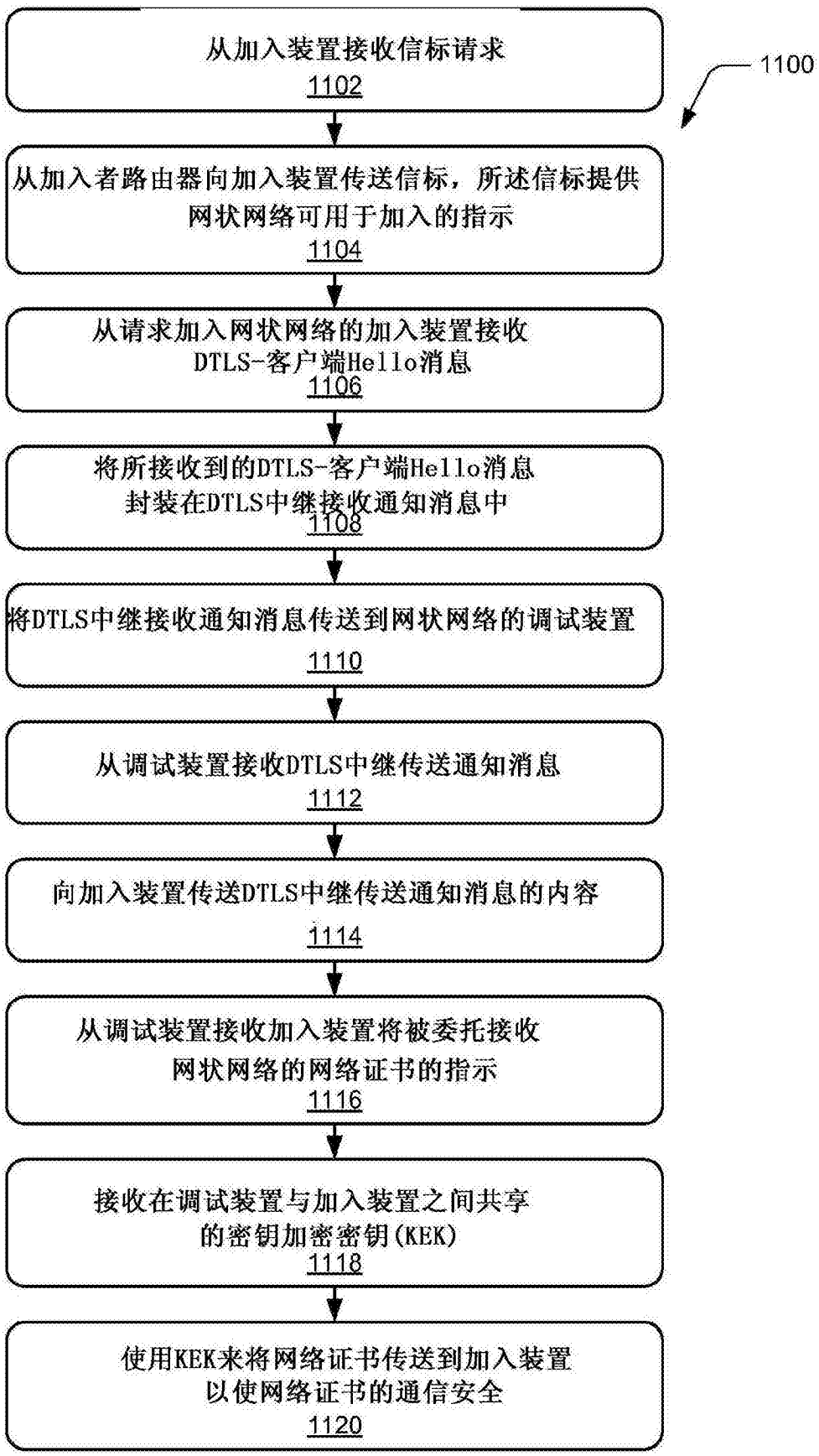

1100
从加入装置接收信标请求
1102
从加入者路由器向加入装置传送信标，所述信标提供网状网络可用于加入的指示
1104
从请求加入网状网络的加入装置接收DTLS-客户端Hello消息
1106
将所接收到的DTLS-客户端Hello消息封装在DTLS中继接收通知消息中
1108
将DTLS中继接收通知消息传送到网状网络的调试装置
1110
从调试装置接收DTLS中继传送通知消息
1112
向加入装置传送DTLS中继传送通知消息的内容
1114
从调试装置接收加入装置将被委托接收网状网络的网络证书的指示
1116
接收在调试装置与加入装置之间共享的密钥加密密钥(KEK)
1118
使用KEK来将网络证书传送到加入装置以使网络证书的通信安全
1120

图11

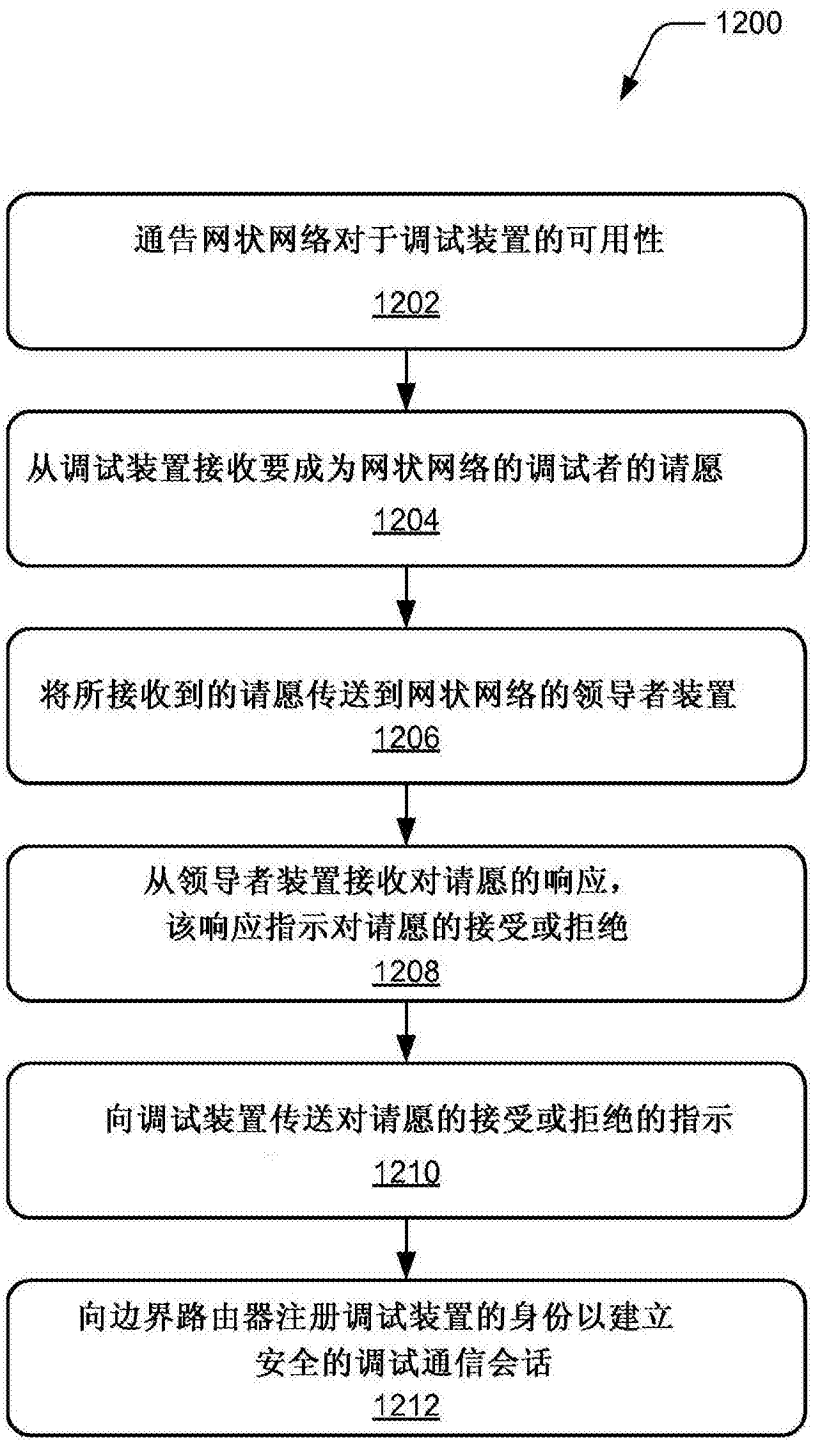

1200
通告网状网络对于调试装置的可用性
1202
从调试装置接收要成为网状网络的调试者的请愿
1204
将所接收到的请愿传送到网状网络的领导者装置
1206
从领导者装置接收对请愿的响应，
该响应指示对请愿的接受或拒绝
1208
向调试装置传送对请愿的接受或拒绝的指示
1210
向边界路由器注册调试装置的身份以建立
安全的调试通信会话
1212

图12

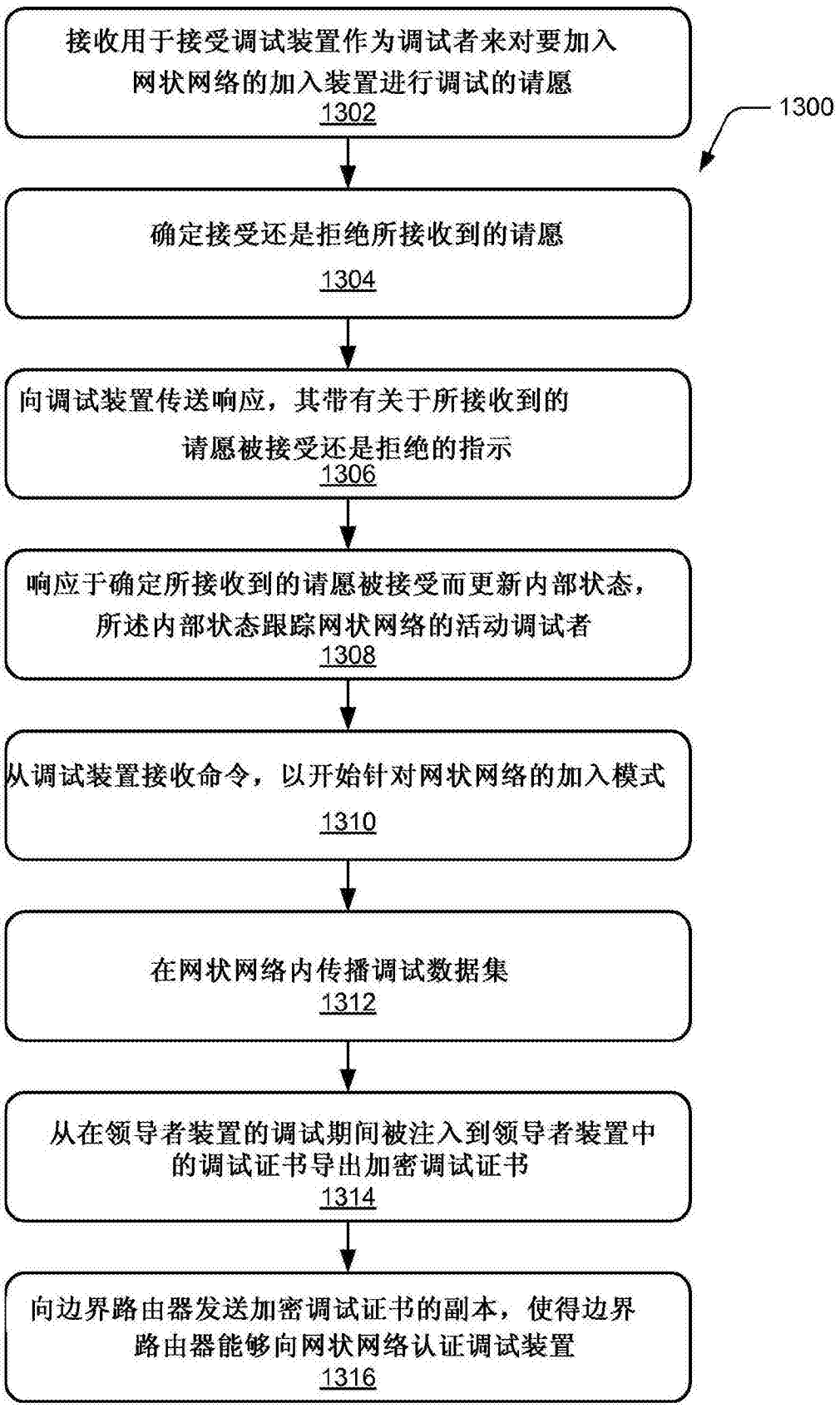

接收用于接受调试装置作为调试者来对要加入网状网络的加入装置进行调试的请愿
1302
1300
确定接受还是拒绝所接收到的请愿
1304
向调试装置传送响应，其带有关于所接收到的请愿被接受还是拒绝的指示
1306
响应于确定所接收到的请愿被接受而更新内部状态，所述内部状态跟踪网状网络的活动调试者
1308
从调试装置接收命令，以开始针对网状网络的加入模式
1310
在网状网络内传播调试数据集
1312
从在领导者装置的调试期间被注入到领导者装置中的调试证书导出加密调试证书
1314
向边界路由器发送加密调试证书的副本，使得边界路由器能够向网状网络认证调试装置
1316

图13

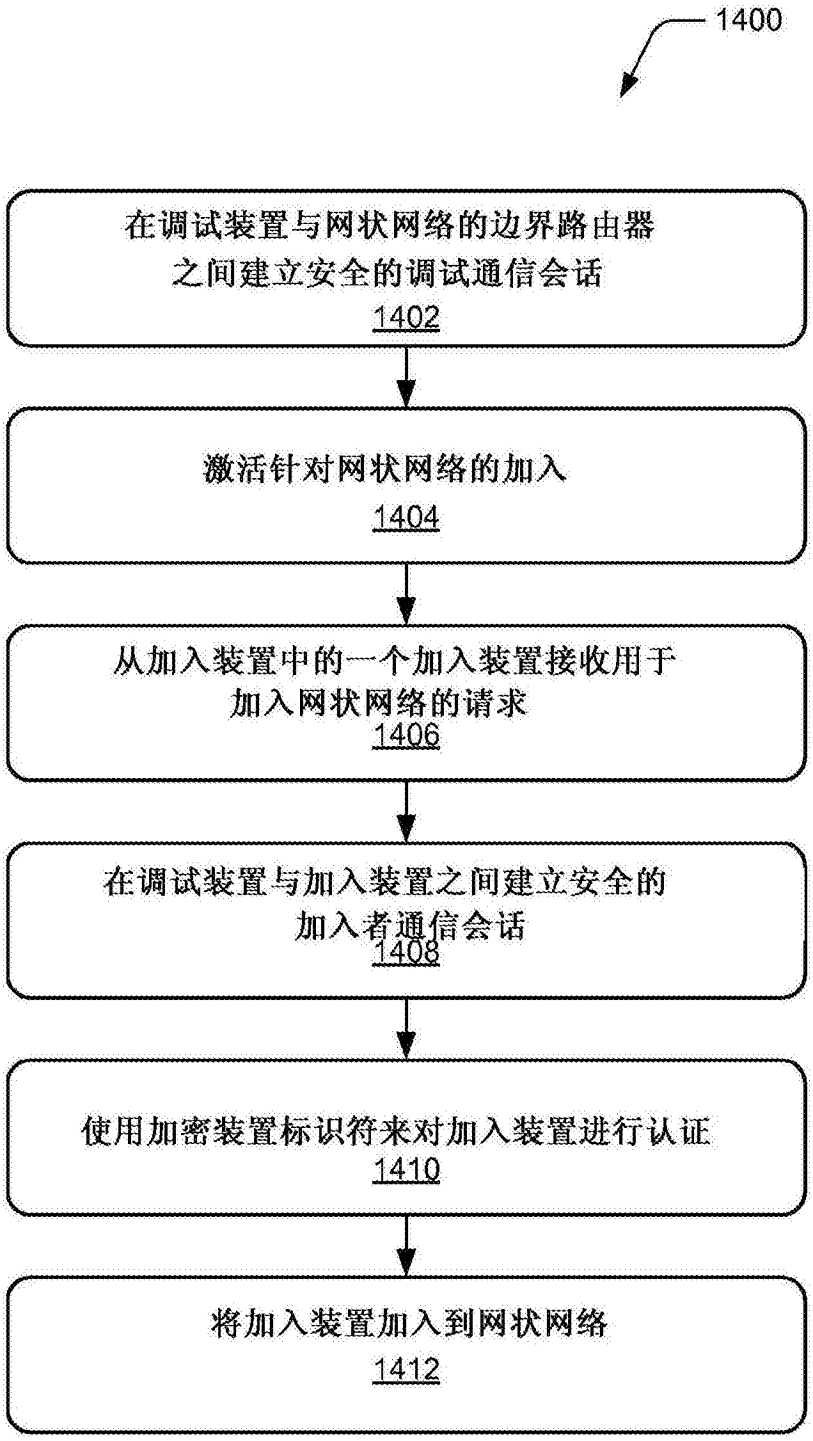

1400
在调试装置与网状网络的边界路由器之间建立安全的调试通信会话
1402
激活针对网状网络的加入
1404
从加入装置中的一个加入装置接收用于加入网状网络的请求
1406
在调试装置与加入装置之间建立安全的加入者通信会话
1408
使用加密装置标识符来对加入装置进行认证
1410
将加入装置加入到网状网络
1412

图14

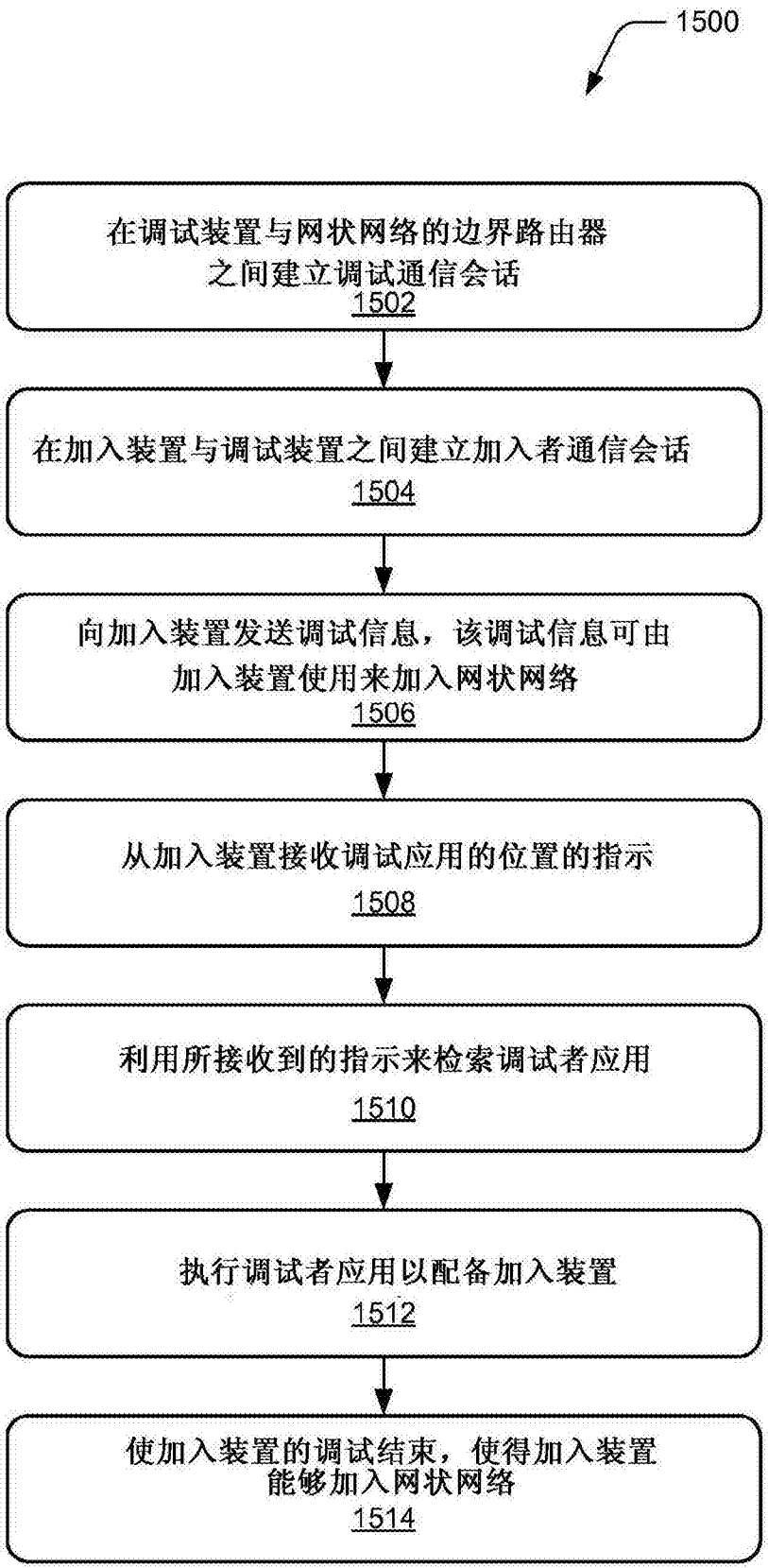

1500
在调试装置与网状网络的边界路由器之间建立调试通信会话
1502
在加入装置与调试装置之间建立加入者通信会话
1504
向加入装置发送调试信息，该调试信息可由加入装置使用来加入网状网络
1506
从加入装置接收调试应用的位置的指示
1508
利用所接收到的指示来检索调试者应用
1510
执行调试者应用以配备加入装置
1512
使加入装置的调试结束，使得加入装置能够加入网状网络
1514

图15

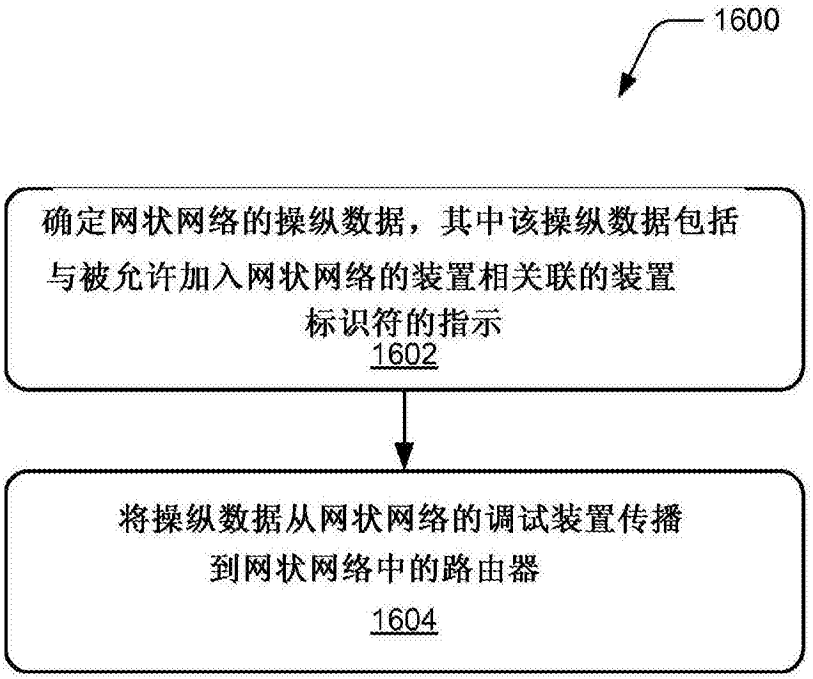

1600
确定网状网络的操纵数据，其中该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示
1602
将操纵数据从网状网络的调试装置传播到网状网络中的路由器
1604

图16

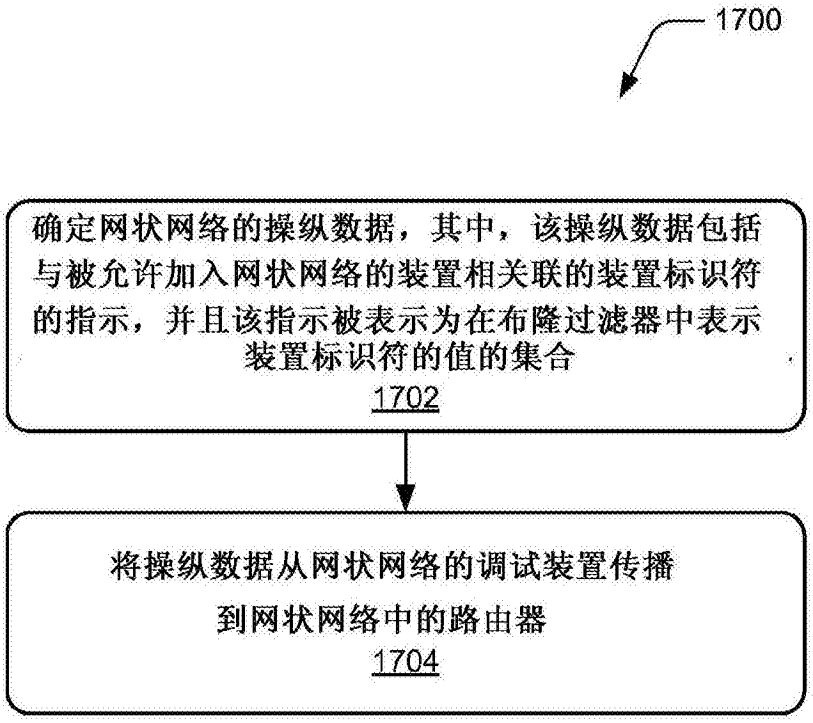

1700
确定网状网络的操纵数据，其中，该操纵数据包括与被允许加入网状网络的装置相关联的装置标识符的指示，并且该指示被表示为在布隆过滤器中表示装置标识符的值的集合
1702
将操纵数据从网状网络的调试装置传播到网状网络中的路由器
1704

图17

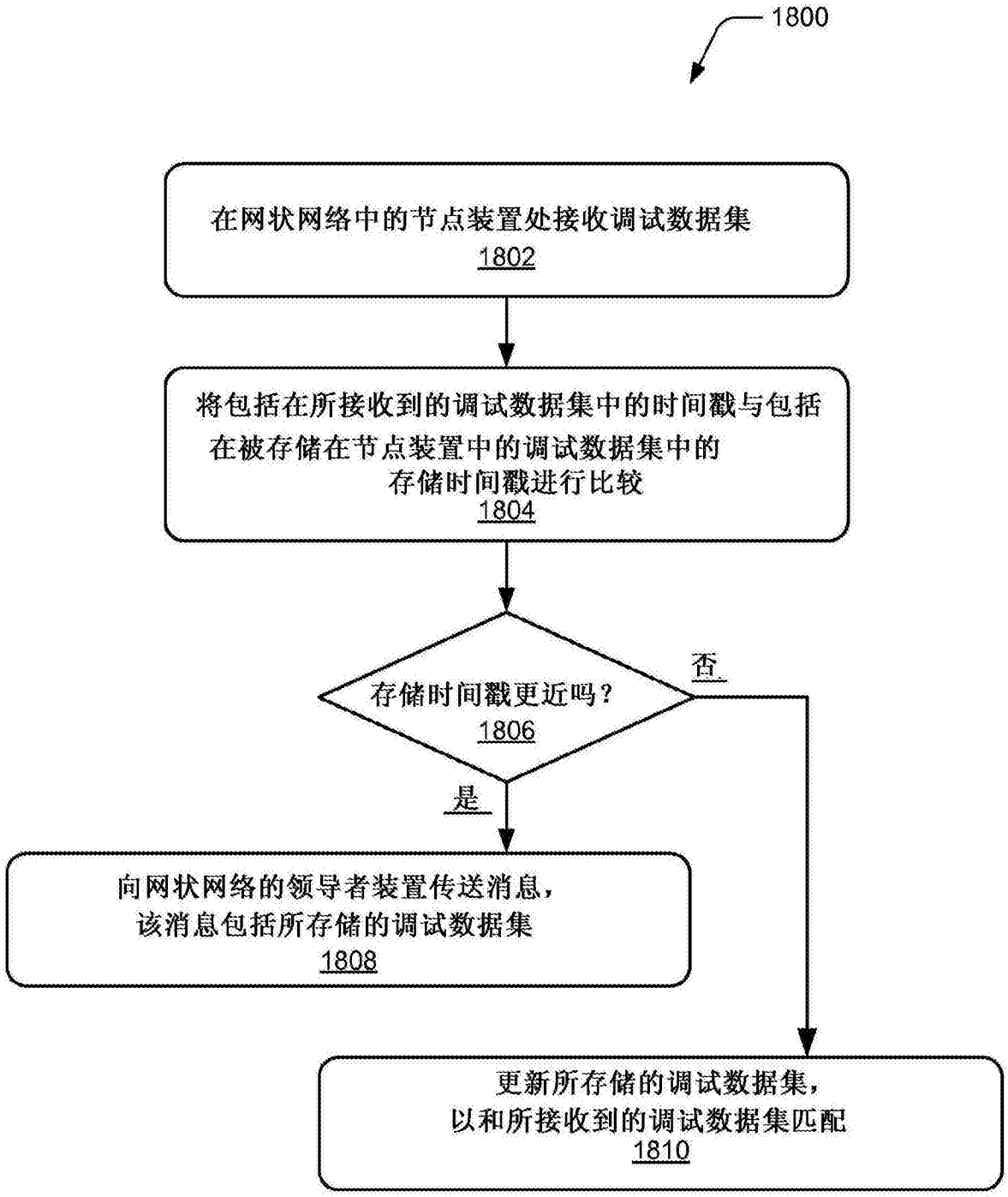

1800
在网状网络中的节点装置处接收调试数据集
1802
将包括在所接收到的调试数据集中的时间戳与包括
在被存储在节点装置中的调试数据集中的
存储时间戳进行比较
1804
存储时间戳更近吗？
1806
否
是
向网状网络的领导者装置传送消息，
该消息包括所存储的调试数据集
1808
更新所存储的调试数据集，
以和所接收到的调试数据集匹配
1810

图18

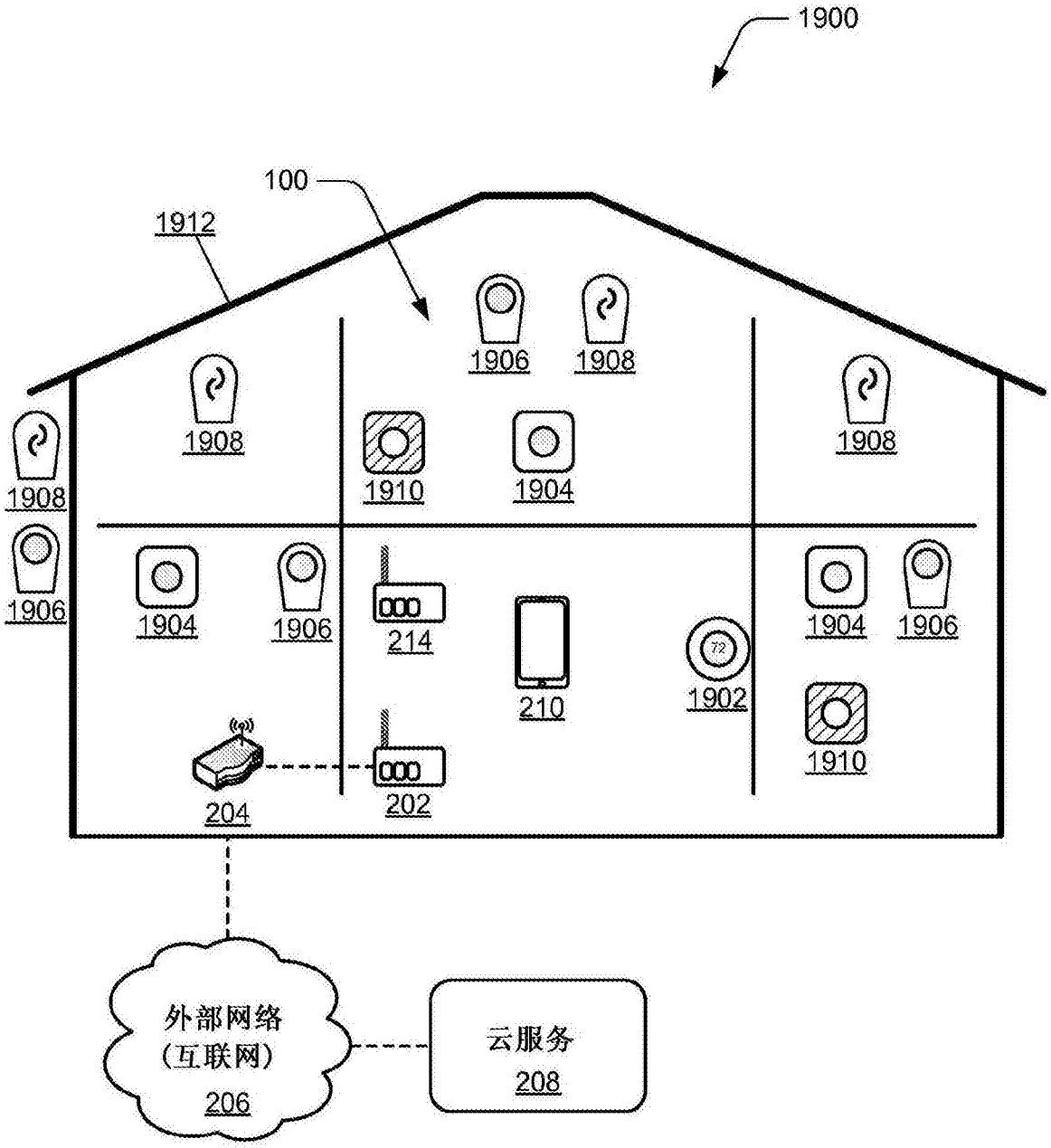

1900
100
1912
1906
1908
1908
1908
1908
1910
1904
1906
1904
1906
214
1904
1906
210
1902
1910
204
202
外部网络
(互联网)
206
云服务
208

图19

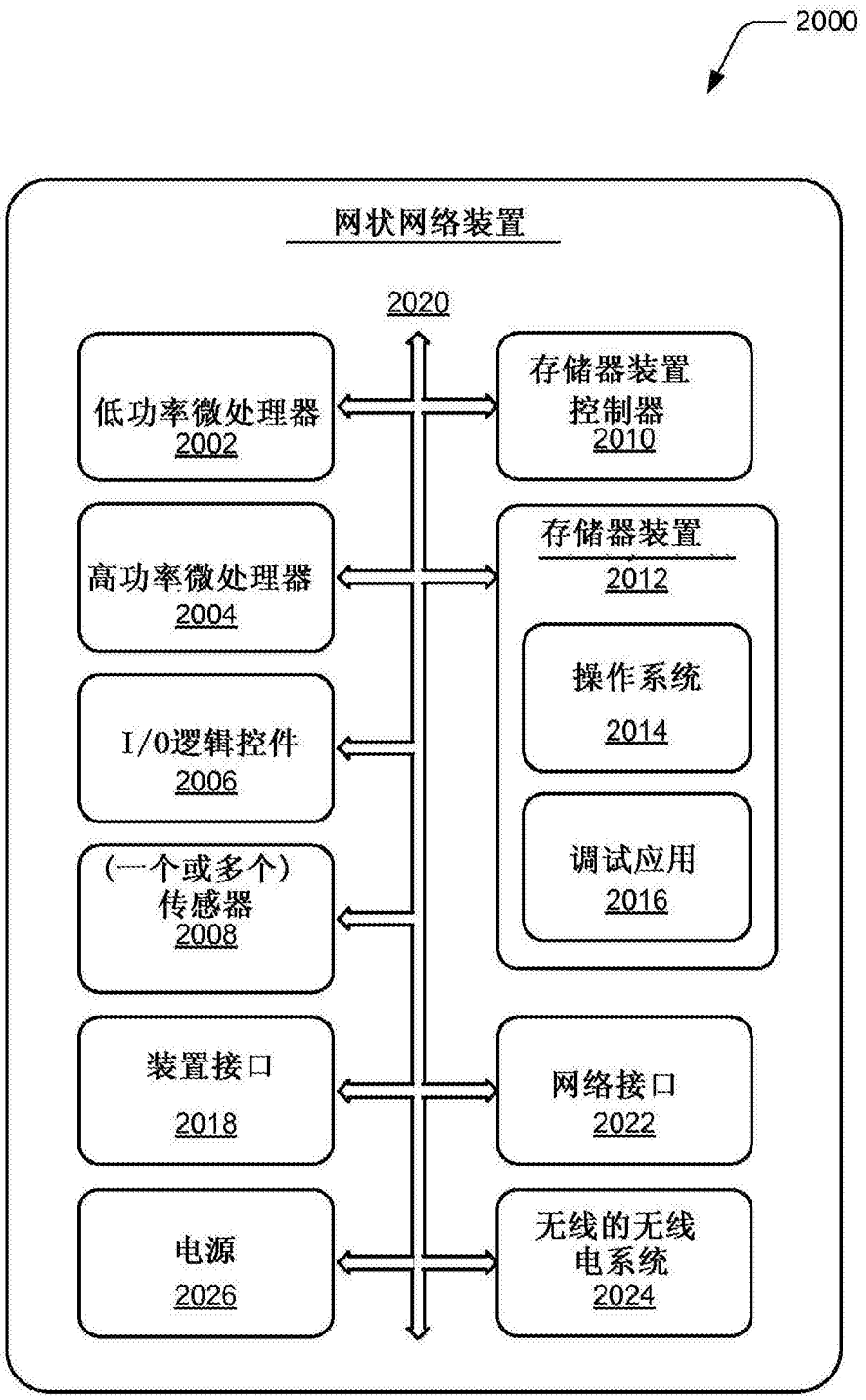

2000
网状网络装置
2020
低功率微处理器
2002
高功率微处理器
2004
I/O逻辑控件
2006
(一个或多个)
传感器
2008
装置接口
2018
电源
2026
存储器装置
控制器
2010
存储器装置
2012
操作系统
2014
调试应用
2016
网络接口
2022
无线的无线
电系统
2024

图20

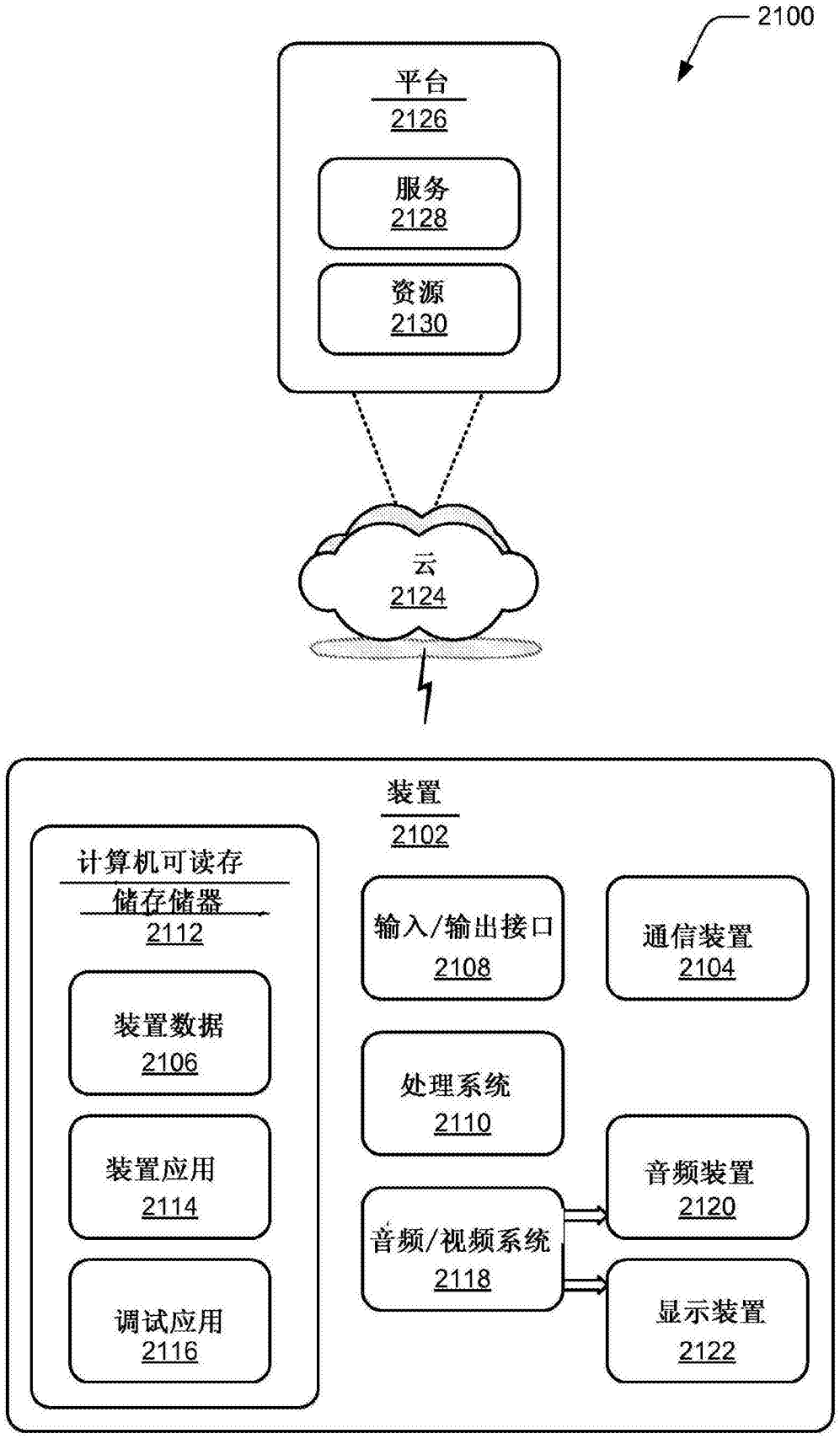

2100
平台
2126
服务
2128
资源
2130
云
2124
装置
2102
计算机可读存储存储器
2112
装置数据
2106
装置应用
2114
调试应用
2116
输入/输出接口
2108
处理系统
2110
音频/视频系统
2118
通信装置
2104
音频装置
2120
显示装置
2122

图21