



(12) 发明专利申请

(10) 申请公布号 CN 115039377 A

(43) 申请公布日 2022. 09. 09

(21) 申请号 202180012515.1

(22) 申请日 2021.04.05

(30) 优先权数据

63/010,370 2020.04.15 US

(85) PCT国际申请进入国家阶段日

2022.08.03

(86) PCT国际申请的申请数据

PCT/US2021/025743 2021.04.05

(87) PCT国际申请的公布数据

W02021/211315 EN 2021.10.21

(71) 申请人 谷歌有限责任公司

地址 美国加利福尼亚州

(72) 发明人 马塞尔·M·M·容

大卫·拉扎罗夫

(74) 专利代理机构 中原信达知识产权代理有限
责任公司 11219

专利代理师 李佳 周亚荣

(51) Int.Cl.

H04L 9/08 (2006.01)

H04W 12/02 (2006.01)

H04W 12/03 (2006.01)

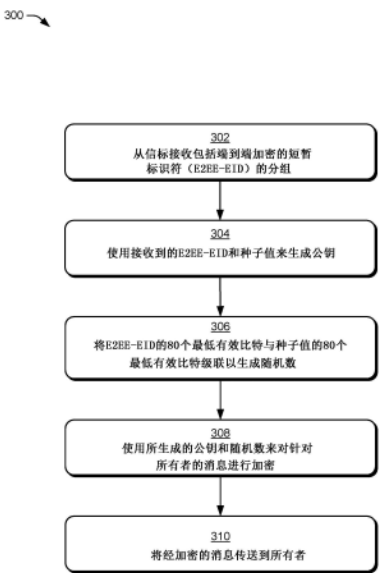
权利要求书2页 说明书12页 附图7页

(54) 发明名称

端到端加密的位置发现

(57) 摘要

本文档描述了确保对通过可能不可信的云服务转发的位置信息的端到端加密的方法、设备、系统和手段,该可能不可信的云服务用来将位置信息从观测设备转发到被观测设备的所有者。对位置信息的端到端加密保护位置信息的私密性,该位置信息由与所有者不相关联的观测器设备提供,因为位置信息遍历从观测器到所有者的网络节点。



1. 一种从观测器向所有者安全地传递消息的方法,所述方法包括,所述观测器:
从信标接收包括端到端加密的短暂标识符E2EE-EID的分组;
使用接收到的E2EE-EID和种子值来生成公钥;
将所述E2EE-EID的80个最低有效比特与所述种子值的80个最低有效比特级联以生成随机数;
使用所生成的公钥和所述随机数来对针对所述所有者的消息进行加密;以及
将经加密的消息传送到所述所有者。
2. 根据权利要求1所述的方法,进一步包括所述观测器:
生成针对所述所有者的所述消息。
3. 根据权利要求2所述的方法,进一步包括,所述观测器:
将所述观测器的位置包括在所述消息中,所述位置是当所述观测器从所述信标接收到所述分组时所述观测器的位置。
4. 根据前述权利要求中任一项所述的方法,其中,对针对所述所有者的消息进行加密包括,所述观测器:
使用AES-EAX-256加密来对所述消息进行加密。
5. 根据前述权利要求中任一项所述的方法,其中,使用接收到的E2EE-EID和种子值来生成公钥包括,所述观测器:
计算表示所述公钥的曲线上的点R。
6. 根据前述权利要求中任一项所述的方法,其中,所述分组是蓝牙通告分组,并且其中,所述蓝牙通告分组是在蓝牙通告信道上接收到的。
7. 一种由信标生成用于向所有者安全地传递消息的短暂标识符的方法,所述方法包括,所述信标:
确定在所述信标与所述所有者之间共享的身份密钥;
使用所述身份密钥和时间值来生成端到端加密的短暂标识符E2EE-EID;
生成包括所述E2EE-EID的信标分组;以及
传送所述信标分组,所述信标分组能够由观测器使用来向所述所有者传送安全消息。
8. 一种电子设备,包括:
无线收发器;
处理器;以及
指令,所述指令能够由所述处理器执行以将所述电子设备配置成执行根据权利要求1至7中的任一项所述的方法。
9. 根据权利要求8所述的电子设备,其中,所述电子设备是信标,并且其中,所述信标是以下各项之一:固定安装的信标、能够贴附到可移动对象的资产标签、由个人携带的个人标签、无线耳塞、智能手表、相机、移动电话或移动计算设备。
10. 根据权利要求8所述的电子设备,其中,所述电子设备是观测器,并且其中,所述观测器是以下各项之一:智能电话、无线局域网(WLAN)接入点、家庭自动化中枢器、安全中枢器、HVAC中枢器、能源管理中枢器、智能扬声器、恒温器、危险探测器、联网相机、照明单元、照明控制器、入口接口设备、占用传感器、家庭自动化边界路由器、手持标签扫描器、或固定安装的标签扫描器。

11. 一种由所有者安全地接收来自观测器的消息的方法,所述方法包括,所述所有者:
从解析器检索所述消息,所述消息包括端到端加密的短暂标识符E2EE-EID;
使用接收到的E2EE-EID和种子值来生成公钥;
将所述E2EE-EID的80个最低有效比特与所述种子值的80个最低有效比特级联以生成随机数;以及
使用所生成的公钥和所述随机数来对接收到的消息进行解密。
12. 根据权利要求11所述的方法,其中,所述消息包括所述观测器的位置,所述位置是当所述观测器从生成所述E2EE-EID的信标接收到分组时所述观测器的位置。
13. 根据权利要求11或权利要求12所述的方法,其中,所述对接收到的消息进行解密包括,所述所有者:
使用AES-EAX-256解密来对所述消息进行解密。
14. 一种电子设备,包括:
处理器;以及
指令,所述指令能够由所述处理器执行以将所述电子设备配置成执行根据权利要求11至13中的任一项所述的方法。
15. 一种计算机可读存储介质,包括指令,所述指令响应于由处理器执行而使得执行如权利要求1至7和权利要求11至13中的任一项所述的方法。

端到端加密的位置发现

背景技术

[0001] 使用短暂标识符的信标系统被设计成让开发人员控制哪些客户端能够利用其信标信号。在信标与信标的所有者之间共享的短暂标识符和密钥使得解析器服务能够在观测器(sighter)向解析器服务发送短暂标识符时确定信标的所有者。信标的观测器与解析器之间的通信以及解析器与所有者之间的通信是安全的;然而,信标和/或观测器与所有者之间的任何通信是不安全的并且对解析器可见。

发明内容

[0002] 提供本发明内容来引入端到端加密的位置发现的简化构思。在下面在具体实施方式中进一步描述该简化构思。本发明内容不旨在标识所要求保护的主题的必要特征,它也不旨在用于确定所要求保护的主题的范围。

[0003] 在各方面中,描述了用于端到端加密的位置发现的方法、设备、系统和手段,其中,观测器从信标接收包括端到端加密的短暂标识符(E2EE-EID)的分组。观测器使用接收到的E2EE-EID和种子值来生成公钥。观测器将E2EE-EID的80个最低有效比特与种子值的80个最低有效比特级联以生成随机数。观测器使用所生成的公钥和随机数来针对所有者的消息进行加密,并且观测器将经加密的消息传送到所有者。

[0004] 在各方面中,描述了用于无线网络中的端到端加密的位置发现的方法、设备、系统和手段,其中,信标确定在信标与所有者之间共享的身份密钥。信标使用身份密钥和时间值来生成端到端加密的短暂标识符(E2EE-EID)。信标生成包括E2EE-EID的信标分组并且传送该信标分组,所传送的信标分组能够由接收信标分组的观测器使用来向所有者传送安全消息。

[0005] 在各方面,描述了用于无线网络中的端到端加密的位置发现的方法、设备、系统和手段,其中,所有者从解析器检索消息,该消息包括端到端加密的短暂标识符(E2EE-EID)。所有者使用接收到的E2EE-EID和种子值来生成公钥。所有者将E2EE-EID的80个最低有效比特与种子值的80个最低有效比特级联以生成随机数,并且所有者使用所生成的公钥和随机数来对接收到的消息进行解密。

[0006] 虽然能够在任何数目的不同环境、系统、设备和/或各种配置中实现所描述的用于端到端加密的位置发现的系统和方法的特征和构思,但是在以下示例设备、系统和配置的上下文中描述端到端加密的位置发现的实施例。

附图说明

[0007] 参考以下附图描述端到端加密的位置发现的实施例。在整个附图中使用相同的数字来引用相似的特征和组件:

[0008] 图1图示能够在其中实现端到端加密的位置发现的各种实施例的示例环境。

[0009] 图2图示根据端到端加密的位置发现的各方面的设备之间的示例数据和控制事务。

- [0010] 图3图示根据本文描述的技术的实施例的端到端加密的位置发现的示例方法。
- [0011] 图4图示根据本文描述的技术的实施例的端到端加密的位置发现的示例方法。
- [0012] 图5图示根据本文描述的技术的实施例的端到端加密的位置发现的示例方法。
- [0013] 图6图示根据本文描述的技术的一个或多个实施例的能够在网络环境中实现的示例网络设备。
- [0014] 图7图示根据本文描述的技术的一个或多个实施例的能够在网络环境中实现的示例信标设备。

具体实施方式

[0015] 本文档描述了确保对通过可能不可信的云服务转发的位置信息的端到端加密的方法、设备、系统和手段,该可能不可信的云服务用来将位置信息从观测设备转发到被观测设备的所有者。对位置信息的端到端加密保护位置信息的私密性,该位置信息由与所有者不相关联的观测器设备提供,因为位置信息遍历从观测器到所有者的网络节点。

[0016] 许多电子设备在它们操作诸如耳塞、智能手表、智能电话、相机、跟踪标签等的设备时通告短程无线信号。使用合适的无线技术和协议,所通告的无线信号使诸如智能电话、网络连接的扬声器、家庭自动化中枢器(hub)、安全中枢器等接收器能够标识这些电子设备。如果接收器意识到其位置(例如,地理位置),则接收器能够上传从电子设备接收到通告的信号的位置以及电子设备的身份。例如,接收器能够将电子设备被观测的位置上传到服务(例如,基于云的服务),以允许电子设备的所有者在所有者将电子设备放错地方的情况下查询电子设备的位置。

[0017] 然而,必须考虑电子设备的所报告的位置信息的私密性和设备的身份,以便防止不良行为者可能获得和利用此信息。让电子设备在通告传输中广播不变的标识符能够使得任何人都能够跟踪电子设备,包括可能使用该信息来跟踪携带电子设备的人(诸如拥有电子设备的人)或电子设备可以被贴附到的任何对象。

[0018] 像Eddystone-EID和FastPair的协议引入了通过让电子设备基于预先确定的机制通告包括轮换标识符的消息以允许所有者(并且仅允许所有者)标识电子设备来保护电子设备的身份的私密性的技术。然而,能够将附加的保护添加到这些方法中以使电子设备的所报告的位置对除了所有者以外的所有人保密。

[0019] 例如,诸如低功耗蓝牙(Bluetooth LE,BLE)信标的低功率无线信标在信标分组(例如,通告信道协议数据单元(PDU))中传送信息。信标可以传送能够直接标识的广播信息,诸如未加密的数据,或者广播每隔几分钟改变的标识符,诸如短暂标识符(短暂ID,EID)。短暂标识符能够由与个别信标身份密钥(短暂身份密钥或EIK)的所有者解析成有用信息。尽管以下讨论经常提及BLE,但是BLE是为了简单而讨论的示例无线技术,但也可以将本文讨论的短暂标识符以类似的方式应用于另一无线技术(例如,超宽带(UWB)、无线局域网(WLAN)、近场通信(NFC)、个域网(PAN)、IEEE 802.15.4、ZigBee、Thread等)。

[0020] 示例环境

[0021] 图1图示能够在其中实现端到端加密的位置发现的各种实施例的示例环境100。环境100包括信标110、观测器120、解析器130和所有者140。信标110是诸如BLE信标、头戴式耳机等的定期地广播(例如,传送)信标分组的设备,如102处所示。观测器(或观察器)120是能

够接收信标分组并且将接收到的分组转发到解析器服务的设备,诸如智能电话,如104处所示。例如,观测器120经由因特网150将接收到的分组转发到解析器服务130。在此示例中,因特网150表示将观测器120、解析器130和/或所有者140互连的有线网络和/或无线网络、局域网和/或广域网的任何组合。诸如基于云的解析器服务(解析服务)的解析器130将接收到的EID与共享密钥和相关联的所有者的散列值进行比较以确定正确的所有者并且将接收到的分组转发到正确的所有者140,如106处所示。替换地或附加地,所有者140能够针对与所有者140相关联的任何信标110向解析器130查询从观测器120接收到的分组或消息。所有者140是与信标110相关联的设备或服务,诸如智能电话、计算机或基于云的服务。所有者140可以拥有一个或多个信标110并且存储用于那些信标110中的每一个信标的共享密钥。

[0022] 端到端加密的位置发现能够与如图1所图示的被配置用于通信的任何合适的设备一起使用。所有者140能够是任何所有者计算系统。信标110能够是与所有者计算系统相关联的任何设备。从设备到所有者计算系统的通信是匿名的(通过隐藏设备和所有者计算系统两者的身份)并且涉及路由系统(例如,解析器130)以将匿名性解析成所有者计算系统和设备的标识并且将设备连接到所有者计算系统。观测器120能够是作为中间设备的任何观测器系统,该中间设备不管匿名性如何都从设备接收信标分组并且向其所有者计算系统发送关于对设备的观测的观测信息。观测信息对除所有者计算系统之外的解析器(和任何其它网络节点)保密。

[0023] 信标110是定期地传送(广播)信标分组(例如,BLE通告分组)的设备,该信标分组包括从在信标110与所有者140之间共享的共享密钥(EIK)生成的短暂标识符(EID)以及由信标110生成该EID的时间。信标110以信标110及其所有者140已知的轮换速率计算新EID。信标110可能具有有限的计算和电力资源并且在有限范围上广播信标分组。观测器120能够从信标110接收信标分组并且能够访问较远程网络(例如,广域网,WAN)。观测器120能够通过较远程网络连接到基于云的服务,诸如解析器130。这使得观测器120能够将接收到的信标分组转发到基于云的解析器130。解析器130能够是设备(服务器)或形成基于云的服务的设备的集合。解析器130存储所有者140和那些所有者的相关联的EID的集合。解析器130将接收到的来自信标分组的EID与其存储的EID的集合进行比较以确定接收到的信标分组的相关联的所有者140。一旦针对接收到的信标分组标识了所有者140,解析器130就能够将信标分组转发到该分组的正确的所有者140。

[0024] 在信标110的初始化时,信标110和所有者140使用椭圆曲线Diffie-Hellman密钥协商协议来交换在信标110与所有者140之间共享的密钥(EIK),如108处所示。共享的EIK使得解析器130能够基于时间从EID中解析信标110的身份并且将来自信标110和/或观测器120的消息导向所有者140。观测器120与解析器130之间的通信以及解析器130与所有者140之间的通信使用传输层安全(TLS)来保证。然而,信标110和/或观测器120与所有者140之间的任何通信对解析器130可见。添加从观测器120到所有者140的安全(加密的)端到端通信信道使用解析器130作为不能访问观测器120与所有者140之间的消息的经加密的有效载荷的路由元件来为从信标110和/或观测器120到所有者140的消息提供保密。

[0025] 端到端加密的位置发现

[0026] 在各方面中,当信标110与所有者140配对时,信标110和所有者140(例如,通过使用智能电话上的应用)发起共同状态并且如上所述商定共享的256比特的对称身份密钥

(EIK)。信标110和所有者140还确定用于轮换信标110包括在由信标110传送的广播分组中的端到端加密的短暂标识符(E2EE-EID)的值的频率(例如,轮换周期)。信标110包括内部时钟。例如,信标110能够维持以一秒间隔递增的内部时钟。从这些参数(轮换周期、身份密钥和来自时钟的当前时间),信标110和所有者140(或拥有这三个参数的任何设备)能够定义伪随机数生成器,其输出对拥有这些参数的任何人来说都是能够预测的。

[0027] 端到端加密的位置发现协议使用这种伪随机数生成器机制。通过使用256比特高级加密标准(AES)电子码本(ECB)(AES-ECB-256)来生成随机数,以对表1中图示的数据结构进行加密:

字节偏移	字段	描述
0 - 10	填充	值 = 0xFF
11	K	轮换周期指数
12-15	TS[0]...TS[3]	信标时间计数器,采用 32 比特大端格式。K 个最低比特被清除。
16 - 26	填充	值 = 0x00
27	K	轮换周期指数
28 - 31	TS[0]...TS[3]	信标时间计数器,采用 32 比特大端格式。K 个最低比特被清除。

[0030] 表1

[0031] 数据结构的AES-ECB-256的结果是表示为r的256比特数字。对于以下计算,SECP160R1的椭圆曲线域参数(F_p 、n和G)(如在SEC 2中所定义的:推荐的椭圆曲线域参数,版本1.0,2000年9月20日)被用于本文的椭圆曲线加密(ECC)操作。

[0032] 通过计算下式, r' 被投影到有限域 F_p :

$$[0033] \quad r = r' \bmod n \quad (1)$$

[0034] 通过下式来计算R:

$$[0035] \quad R = r * G \quad (2)$$

[0036] 这是表示正在使用的公钥的曲线上的点。信标通告 R_x ,其是R的x坐标,作为其E2EE短暂标识符。请注意, R_x 为20个字节长,以适合放入标准BLE通告信道PDU中。

[0037] E2EE-EID帧在通告信道PDU中被编码为与Eddystone服务通用独特标识符(UUID)相关联的服务数据块。在表2中图示了E2EE-EID帧布局。

[0038]	字节偏移	字段	描述
	0	帧类型	值 = 0x40
	1	E2EE-EID[0]	能够被用于导出加密密钥的 20 字节的短暂标识符。
[0039]	2	E2EE-EID[1]	
	...	...	
	20	E2EE-EID[19]	

[0040] 表2

[0041] 端到端加密的位置发现加密

[0042] 为了对消息 m 进行加密(例如,消息是观测器120从信标110接收到通告分组的所报告的位置),已经从信标110接收到 R_x 的观测器120在 F_p 中生成随机数 s ,如上所述。

[0043] 观测器120从随机数和ECC基点 G 计算种子 S :

[0044] $S = s * G$ (3)

[0045] 观测器120通过在曲线方程中进行替换并从可能的结果中挑选任意 R_y 值来从接收到的 R_x 计算表示公钥的曲线上的点 R :

[0046] $R = (R_x, R_y)$ (4)

[0047] 观测器120计算公钥 k :

[0048] $k = \text{HKDFSAH256}((s * R)_x)$ (5)

[0049] 其中, $(s * R)_x$ 是曲线乘法结果的 x 坐标。

[0050] UR_x 和 LR_x 分别是 R_x 的高(最高有效)80比特和低(最低有效)80比特(以大端格式)。类似地, US_x 和 LS_x 分别是 S 的高80比特和低80比特(以大端格式)。

[0051] 观测器120计算随机数,其中:

[0052] 随机数 = $LR_x || LS_x$ (6)

[0053] 观测器120计算 (m', tag) , 其中:

[0054] $(m', \text{tag}) = \text{AESEAX256ENC}(k, \text{随机数}, m)$ (7)

[0055] 观测器120向所有者140发送消息,在该消息中包括 UR_x 、 S_x 、 m' 和 tag 。该消息可以经由诸如解析器130的不可信节点转发。

[0056] 端到端加密的位置发现解密

[0057] 拥有身份密钥和轮换周期指数的所有者设备140从观测器120接收消息并对该消息进行解密。已经接收到 UR_x 的所有者140获得 UR_x 所基于的信标时间计数器值并计算如上定义的 r 的预期值。

[0058] 所有者140计算:

[0059] $R = r * G$ (8)

[0060] 并且验证与从观测器120接收到的消息中提供的 UR_x 值的匹配。

[0061] 所有者140通过在曲线方程中进行替换并从可能的结果中挑选任意 S_y 值来计算种子 S :

[0062] $S = (S_x, S_y)$ (9)

[0063] 所有者140计算公钥k:

[0064] $k = \text{HKDFSHA256}((r*S)_x)$ (10)

[0065] 其中, $(r*S)_x$ 是曲线乘法结果的x坐标。

[0066] 所有者140计算随机数:

[0067] 随机数 = $LR_x || LS_x$ (11)

[0068] 所有者140计算消息的解密值m:

[0069] $m = \text{AESEAX256DEC}(k, \text{随机数}, m', \text{tag})$ (12)

[0070] 位置发现系统

[0071] 当用户购买支持端到端加密的位置发现的信标设备(例如,独立信标设备、包括信标的设备、除了支持其他蓝牙配置文件之外还支持信标传输的蓝牙设备等)时,用户供应信标设备以配置端到端加密的位置发现。例如,用户通过如上所述设置身份密钥和轮换周期使用用户设备(例如,智能电话或计算设备)上的应用来发起供应。身份密钥在信标设备(信标110)与用户设备(所有者140)之间共享,但对系统中的诸如观测器120和解析器130的其他设备保密。尽管解析器130(例如,基于云的解析器服务)不知道身份密钥,但使解析器130意识到信标110和相关联的所有者140的存在。例如,供应应用向解析器130提供信标110和所有者的相关联的身份140,该解析器130转而以任何合适的方式存储这些身份以供以后使用,以针对从观测器120接收到的消息解析所有者140的身份。信标110是能够存储身份密钥、维持时钟时间、生成E2EE-EID、并传送包括E2EE-EID的信标分组的任何设备。例如,信标110可以是固定安装的信标、能够贴附到可移动对象的资产标签、由个人携带的个人标签、无线耳塞、智能手表、相机、移动电话、移动计算设备等等。

[0072] 所有者设备140定期地预先计算(例如,每天)该时段(例如,接下来的24小时)的预期短暂标识符,如上所述。所有者设备140然后截断预先计算的短暂标识符。例如,所有者设备140将预先计算的短暂标识符截断到任何合适的长度,诸如保留等于公钥长度的一半的最低有效比特的数目。在另一示例中,所有者设备140截断预先计算的短暂标识符以保留预先计算的短暂标识符的80个最低有效比特。所有者设备140然后将截断的预先计算的短暂标识符上传到解析器130。解析器130将截断的预先计算的短暂标识符与先前存储的信标110和所有者140的相关联的身份相关联,以供以后用于解析从一个或多个观测器120接收到的消息的所有权。

[0073] 观测器120是能够接收和解码信标分组以恢复信标110的标识符、生成和加密消息(如上所述)、并且将消息传递到解析器130的任何设备。例如,观测器设备120包括智能电话、无线局域网(WLAN)接入点、家庭自动化中枢器、安全中枢器、HVAC中枢器、能量管理中枢器、智能扬声器、恒温器、危险检测器(例如,用于烟雾和/或一氧化碳)、联网相机、照明单元、照明控制器、入口接口设备、占用传感器、家庭自动化边界路由器、手持(例如,移动)标签扫描器、固定安装的标签扫描器,或诸如连接的电器和/或可控系统的任何其他类型的无线网络设备,诸如冰箱、炉灶和烤箱、洗衣机、烘干机、空调、泳池加热器、灌溉系统、安全系统等等,以及其他电子和计算设备,诸如电视、娱乐系统、计算机、对讲系统、车库门开启器、吊扇、控制面板等。

[0074] 解析器130使用作为由观测器120发送的消息有效载荷的一部分包括的部分标识

符 UR_x 以确定在消息中报告的观测是特定信标110的观测。解析器130将所报告的观测与特定信标110相关联并存储接收到的消息和消息与特定信标110的关联。虽然解析器130能够解析与接收到的消息相关联的信标110,但是解析器130不能对消息内容进行解密以确定信标观测的位置。解析器130可以是任何设备(例如,计算机服务器)或形成基于云的服务的设备的集合。

[0075] 因为解析器130不知道身份密钥,所以解析器130不能预测未来的EID,并且在没有来自所有者140的截断的预先计算的短暂标识符的定期更新的情况下,解析器130不能跟踪信标110。解析器130不能欺骗虚假位置,因为整个公钥不可用于解析器130,并且解析器130不能用于中间人攻击,因为解析器130无法访问身份密钥。

[0076] 信标设备110的所有者140然后能够向解析器130查询信标110的最后已知位置。解析器130然后将经加密的位置转发到所有者140。替换地或附加地,解析器130能够当消息被接收时将消息转发到或定期地批量地将消息转发到所有者140。给定消息中的时间戳,所有者140能够在那时推断信标110的预期的私钥并执行解密算法,如上所述。

[0077] 图2图示根据端到端加密的位置发现的各方面的设备之间的数据和控制事务。尽管为了图示清楚起见而未图示,但是可以实现对图2中图示的消息的各种确认以确保端到端加密的位置发现的可靠操作。

[0078] 在205处,并且如上所述,在信标的供应期间将信标110与所有者140配对。配对包括共享用于端到端加密的位置发现的密钥。在210处,信标基于当前时间来生成E2EE-EID。

[0079] 在215处,信标110生成信标分组。信标110将E2EE-EID包括在信标分组中。注意,基于E2EE-EID的预定轮换速率,信标110针对轮换的每个连续循环(在图2中未图示)重复210和215的操作。在220处,信标110传送信标分组。信标110可以在轮换的每个循环期间传送信标分组一次或多次。

[0080] 在225处,在从信标110接收到信标分组之后,观测器120生成要向所有者140发送的消息。任选地,观测器120可以将附加分组括在消息中,诸如当接收到信标分组时观测器的位置。在230处,观测器向解析器130发送消息。

[0081] 在235处,解析器130基于时间从E2EE-EID中解析信标110的身份并且将该身份与所有者140和那些所有者的相关联的E2EE-EID的集合进行比较。如果解析器针对接收到的消息标识所有者140,则解析器在240处将消息转发到所有者140。在245处,所有者对接收到的消息进行解密。

[0082] 示例方法

[0083] 根据端到端加密的位置发现的一个或多个实施例参考相应的图3至图5描述示例方法300-500。描述方法框的次序不旨在被解释为限制,并且能够跳过或以任何次序组合任何数目的所描述的方法框以实现方法或替代方法。通常,本文描述的组件、模块、方法和操作中的任何组件、模块、方法和操作能够使用软件、固件、硬件(例如,固定逻辑电路)、手动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存储器(介质)上的可执行指令的一般上下文中描述示例方法的一些操作,并且实现方式能够包括软件应用、程序、函数等。替换地或另外,本文描述的功能性中的任何功能性能能够至少部分地由诸如但不限于以下各项的一个或多个硬件逻辑组件执行:现场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、片上系统系统(SoC)、复杂可编程逻辑

器件 (CPLD) 等。

[0084] 图3图示如通常与从观测器向所有者安全地传递消息相关的端到端加密的位置发现的示例方法300。在框302处,观测器(例如,观测器120)从信标(例如,信标110)接收包括端到端加密的短暂标识符(E2EE-EID)的分组。

[0085] 在框304处,观测器使用接收到的E2EE-EID和种子值来生成公钥(例如,公钥k)。在框306处,观测器将E2EE-EID的80个最低有效比特与种子值的80个最低有效比特级联以生成随机数。

[0086] 在框308处,观测器使用所生成的公钥和随机数来对针对所有者的消息进行加密。在框310处,观测器将经加密的消息传送到所有者。例如,观测器经由解析器130将消息转发到所有者140。

[0087] 图4图示如通常与由信标生成用于向所有者安全地传递消息的短暂标识符相关的端到端加密的位置发现的示例方法400。在框402处,信标(例如,信标110)确定在信标与所有者之间分享的身份密钥。在框404处,信标使用身份密钥和时间值来生成端到端加密的短暂标识符(E2EE-EID)。

[0088] 在框406处,信标生成包括E2EE-EID的信标分组。在框408处,信标传送信标分组,该信标分组能够由观测器(例如,观测器120)使用来向所有者传送安全消息。

[0089] 图5图示如通常与由所有者安全地接收来自观测器的消息相关的端到端加密的位置发现的示例方法500。在框502处,所有者(例如,所有者140)从解析器(例如,解析器130)检索消息,该消息包括端到端加密的短暂标识符(E2EE-EID)。在框504处,所有者使用接收到的E2EE-EID和种子值来生成公钥。

[0090] 在框506处,所有者将E2EE-EID的80个最低有效比特与种子值的80个最低有效比特级联以生成随机数。在框508处,所有者使用所生成的公钥和随机数来对接收到的消息进行解密。

[0091] 示例设备

[0092] 图6图示根据如本文所描述的端到端加密的位置发现的一个或多个实施例的能够作为网络中的网络设备中的任何网络设备被实现的示例网络设备600,诸如信标110、观测器120、解析器130或所有者140。网络设备600能够与电子电路系统、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其它硬件、固件和/或软件集成以在网络中实现该设备。

[0093] 在此示例中,网络设备600包括处理可执行指令的低功率微处理器602和/或高功率微处理器604(例如,微控制器或数字信号处理器)。该设备也包括输入-输出(I/O)逻辑控件606(例如,以包括电子电路系统)。微处理器能够包括集成电路、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/或硬件中的其它实现方式的组件,诸如作为片上系统(SoC)实现的处理器和存储器系统。替换地或另外,该设备能够用软件、硬件、固件、或可以用处理和控制电路实现的固定逻辑电路系统中的任何一个或它们的组合加以实现。低功率微处理器602和高功率微处理器604也能够支持设备的一个或多个不同的设备功能性。例如,高功率微处理器604可以执行计算密集的操作,而低功率微处理器602可以管理不太复杂的过程,诸如从一个或多个传感器608检测危险或温度。低功率处理器602也可以唤醒或初始化高功率处理器604以进行计算密集的过程。

[0094] 可以包括和实现一个或多个传感器608以检测各种性质,诸如加速度、温度、湿度、水、供电、接近度、外部运动、设备运动、声音信号、超声信号、光信号、火、烟雾、一氧化碳、全球定位卫星(GPS)信号、射频(RF)、其它电磁信号或场等。因此,传感器608可以包括以下各项中的任何一个或它们的组合: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、适于并包括相机(例如,电荷耦合器件或视频相机)的光传感器、主动或被动辐射传感器、GPS接收器和射频标识检测器。在实现方式中,网络设备600可以包括一个或多个主要传感器以及一个或多个次要传感器,诸如感测以设备的核心操作为中心的数据(例如,感测恒温器中的温度或感测烟雾检测器中的烟雾)的主要传感器,而次要传感器可以感测其它类型的数据(例如,运动、光或声音),这些数据能够被用于能源效率目标或智能操作目标。

[0095] 网络设备600包括存储器设备控制器610和存储器设备612,诸如任何类型的非易失性存储器和/或其它合适的电子数据存储设备。网络设备600也能够包括各种固件和/或软件,诸如由存储器作为计算机可执行指令维护并且由微处理器执行的操作系统614。设备软件也可以包括消息收发应用616,该消息收发应用实现端到端加密的位置发现的实施例。网络设备600也包括设备接口618,该设备接口用于与另一设备或外围组件进行接口,并且包括集成数据总线620,该集成数据总线耦合无线网络设备的各种组件以在组件之间进行数据通信。也可以将无线网络设备中的数据总线实现为不同的总线结构和/或总线架构中的任何一种或它们的组合。

[0096] 设备接口618可以从用户接收输入并且/或者向用户提供信息(例如,作为用户界面),而且接收到的输入能够用于确定设定。设备接口618也可以包括对用户输入做出响应的机械或虚拟组件。例如,用户能够机械地移动滑动或可旋转组件,或者可以检测沿着触摸板的运动,并且此类运动可以对应于设备的设定调整。物理和虚拟可移动用户界面组件能够允许用户沿着表现连续体的一部分设置设定。设备接口618也可以从任何数目的外围设备如按钮、键区、开关、麦克风和成像器(例如,相机设备)接收输入。

[0097] 网络设备600能够包括网络接口622,诸如用于与无线网络中的其它无线网络设备进行通信的无线网络接口,以及用于诸如经由因特网进行网络通信的外部网络接口。网络设备600也包括用于经由无线网络接口与其它无线网络设备进行无线通信并且用于多个不同的无线通信系统的无线的无线电系统624。无线的无线电系统624可以包括Wi-Fi、Bluetooth™、BLE、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能够包括为特定无线通信技术实现的无线电设备、天线和芯片组。网络设备600也包括电源626,诸如电池和/或将设备连接到线路电压。AC电源也可以用于对设备的电池充电。

[0098] 图7图示根据如本文所描述的端到端加密的位置发现的一个或多个实施例的能够作为网络中的信标设备110被实现的示例信标设备700。信标设备700能够与电子电路系统、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其它硬件、固件和/或软件集成以在网络中实现该设备。

[0099] 在此示例中,信标设备700包括处理可执行指令的一个或多个处理器702(例如,微控制器或数字信号处理器)。该设备也包括输入输出(I/O)逻辑控件704(例如,以包括电子电路系统)。处理器能够包括集成电路、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/或硬件中的其它实现方式的组件,诸如作为片上系统(SoC)实现的处理器

和存储器系统。替换地或另外,该设备能够用软件、硬件、固件、或可以用处理和电路来实现的固定逻辑电路系统中的任何一种或组合加以实现。

[0100] 任选地或附加地,可以包括和实现一个或多个传感器706以检测各种性质,诸如加速度、温度、湿度、水、供电、接近度、外部运动、设备运动、声音信号、超声信号、光信号、火、烟雾、一氧化碳、全球定位卫星 (GPS) 信号、射频 (RF)、其它电磁信号或场等。因此,传感器706可以包括以下各项中的任何一个或它们的组合: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、适于并包括相机(例如,电荷耦合器件或视频相机)的光传感器、主动或被动辐射传感器、GPS接收器和射频标识检测器。在实现方式中,信标设备700可以包括一个或多个主要传感器以及一个或多个次要传感器,诸如感测以设备的核心操作为中心的数据(例如,感测恒温器中的温度或感测烟雾检测器中的烟雾)的主要传感器,而次要传感器可以感测其它类型的数据(例如,运动、光或声音),这些数据能够被用于能源效率目标或智能操作目标。

[0101] 信标设备700包括存储器708,诸如任何类型的非易失性存储器和/或其它合适的电子数据存储设备。信标设备700也能够包括各种固件和/或软件,诸如操作系统710,该操作系统由存储器作为计算机可执行指令维护并且由处理器执行。设备软件也可以包括实现端到端加密的位置发现的实施例的信标应用712。任选地或附加地,信标设备700也包括设备接口714,该设备接口用于与另一设备或外围组件进行接口。信标设备700包括集成数据总线716,该集成数据总线耦合信标设备的各种组件以在组件之间进行数据通信。也可以将信标设备中的数据总线实现为不同的总线结构和/或总线架构中的任何一种或组合。

[0102] 设备接口714可以从用户接收输入并且/或者向用户提供信息(例如,作为用户界面),而且接收到的输入能够用于确定设定。设备接口714也可以包括对用户输入做出响应的机械或虚拟组件。例如,用户能够机械地移动滑动或可旋转组件,或者可以检测沿着触摸板的运动,并且此类运动可以对应于设备的设定调整。物理和虚拟可移动用户界面组件能够允许用户沿着表现连续体的一部分设置设定。设备接口714也可以从任何数目的外围设备如按钮、键区、开关、麦克风和成像器(例如,相机设备)接收输入。

[0103] 信标设备700能够包括用于无线通信的无线的无线电系统818。无线的无线电系统718可以包括Wi-Fi、Bluetooth™、BLE、移动宽带和/或点对点IEEE 802.15.4。无线的无线电系统718能够包括为特定无线通信技术实现的无线电设备、天线和芯片组。信标设备700也包括电源720,诸如电池和/或将设备连接到线路电压。AC电源也可以用于对设备的电池充电。

[0104] 在下文中描述了一些示例:

[0105] 示例1:一种从观测器向所有者安全地传递消息的方法,所述方法包括所述观测器:

[0106] 从信标接收包括端到端加密的短暂标识符 (E2EE-EID) 的分组;

[0107] 使用接收到的E2EE-EID和种子值来生成公钥;

[0108] 将所述E2EE-EID的80个最低有效比特与所述种子值的80个最低有效比特级联以生成随机数;

[0109] 使用所生成的公钥和所述随机数来针对所述所有者的消息进行加密;以及

[0110] 将经加密的消息传送到所述所有者。

- [0111] 示例2:根据示例1所述的方法,进一步包括所述观测器:
- [0112] 生成针对所述所有者的所述消息。
- [0113] 示例3:根据示例2所述的方法,进一步包括所述观测器:
- [0114] 将所述观测器的位置包括在所述消息中,所述位置是当所述观测器从所述信标接收到所述分组时所述观测器的位置。
- [0115] 示例4:根据前述示例中任一项所述的方法,其中,所述对针对所述所有者的消息进行加密包括所述观测器:
- [0116] 使用AES-EAX-256加密来对所述消息进行加密。
- [0117] 示例5:根据前述示例中任一项所述的方法,其中,所述使用接收到的E2EE-EID和种子值来生成公钥包括所述观测器:
- [0118] 计算表示所述公钥的曲线上的点R。
- [0119] 示例6:根据前述示例中任一项所述的方法,其中,所述分组是蓝牙通告分组,并且其中,所述蓝牙通告分组是在蓝牙通告信道上接收到的。
- [0120] 示例7:一种由信标生成用于向所有者安全地传递消息的短暂标识符的方法,所述方法包括所述信标:
- [0121] 确定在所述信标与所述所有者之间共享的身份密钥;
- [0122] 使用所述身份密钥和时间值来生成端到端加密的短暂标识符 (E2EE-EID) ;
- [0123] 生成包括所述E2EE-EID的信标分组;以及
- [0124] 传送所述信标分组,所述信标分组能够由观测器使用来向所述所有者传送安全消息。
- [0125] 示例8:一种电子设备,包括:
- [0126] 无线收发器;
- [0127] 处理器;以及
- [0128] 指令,所述指令能够由所述处理器执行以将所述电子设备配置成执行根据示例1至7中的任一项所述的方法。
- [0129] 示例9:根据示例8所述的电子设备,其中,所述电子设备是信标,并且其中,所述信标是以下各项之一:固定安装的信标、能够贴附到可移动对象的资产标签、由个人携带的个人标签、无线耳塞、智能手表、相机、移动电话或移动计算设备。
- [0130] 示例10:根据示例8所述的电子设备,其中,所述电子设备是观测器,并且其中,所述观测器是以下各项之一:智能电话、无线局域网 (WLAN) 接入点、家庭自动化中枢器、安全中枢器、HVAC中枢器、能源管理中枢器、智能扬声器、恒温器、危险探测器、联网相机、照明单元、照明控制器、入口接口设备、占用传感器、家庭自动化边界路由器、手持标签扫描器、或固定安装的标签扫描器。
- [0131] 示例11:一种由所有者安全地接收来自观测器的消息的方法,所述方法包括所述所有者:
- [0132] 从解析器检索所述消息,所述消息包括端到端加密的短暂标识符 (E2EE-EID) ;
- [0133] 使用接收到的E2EE-EID和种子值来生成公钥;
- [0134] 将所述E2EE-EID的80个最低有效比特与所述种子值的80个最低有效比特级联以生成随机数;以及

[0135] 使用所生成的公钥和所述随机数来对接收到的消息进行解密。

[0136] 示例12:根据示例11所述的方法,其中,所述消息包括所述观测器的位置,所述位置是当所述观测器从生成所述E2EE-EID的信标接收到分组时所述观测器的位置。

[0137] 示例13:根据示例11或示例12所述的方法,其中,所述对接收到的消息进行解密包括所述所有者:

[0138] 使用AES-EAX-256解密来对所述消息进行解密。

[0139] 示例14:一种电子设备,包括:

[0140] 处理器;以及

[0141] 指令,所述指令能够由所述处理器执行以将所述电子设备配置成执行根据示例11至13中的任一项所述的方法。

[0142] 示例15:一种计算机可读存储介质,包括指令,响应于由处理器执行,所述指令使如权利要求1至7和权利要求11至13中的任一项中叙述的方法被执行。

[0143] 尽管已经用特定于特征和/或方法的语言描述了端到端加密的位置发现的实施例,但是所附权利要求的主题不一定限于所描述的特定特征或方法。相反,特定特征和方法被公开为端到端加密的位置发现的示例实现方式,并且其它等同特征和方法旨在为在所附权利要求的范围内。此外,描述了各种不同的实施例,并且应当领会,能够独立地或连同同一个或多个其它描述的实施例一起实现每个描述的实施例。

100 →

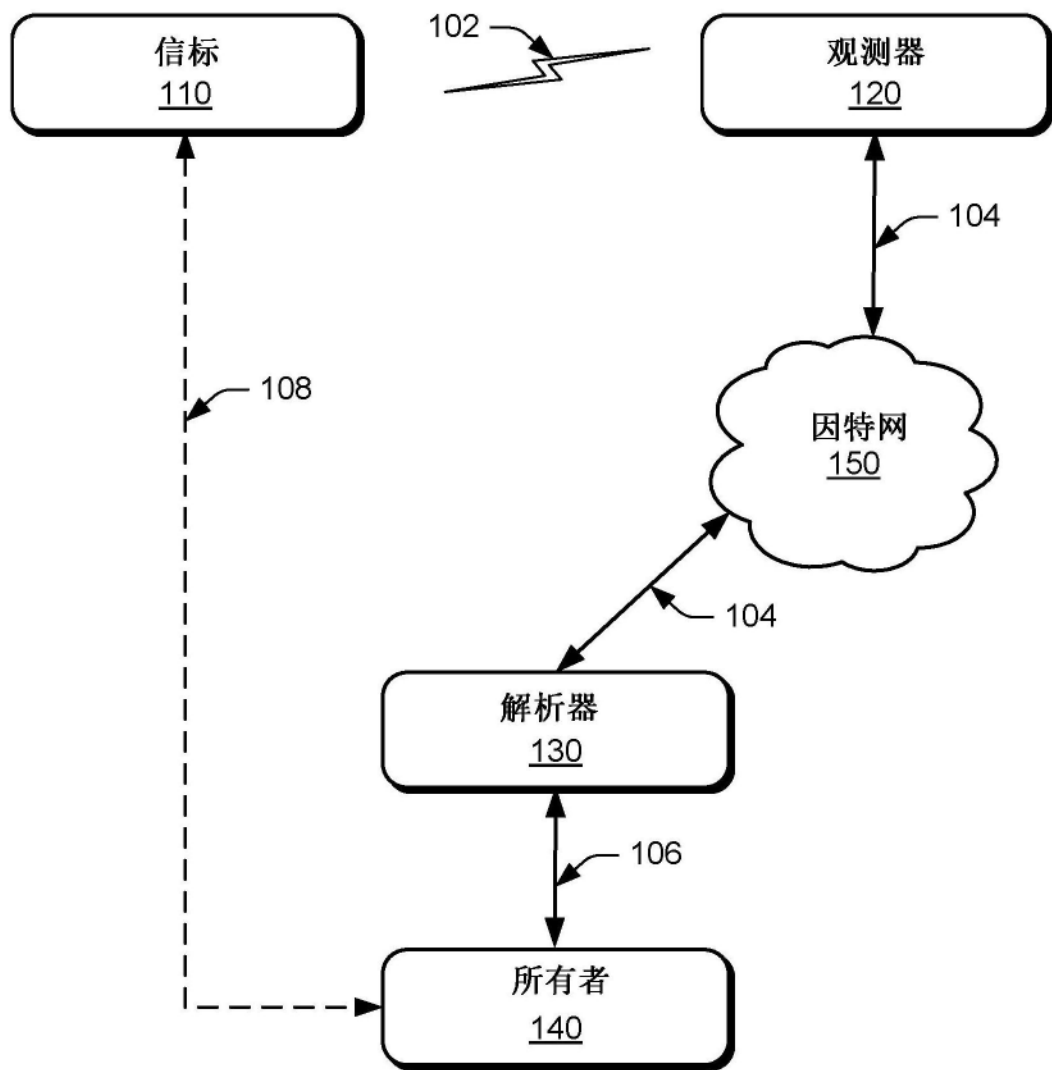


图1

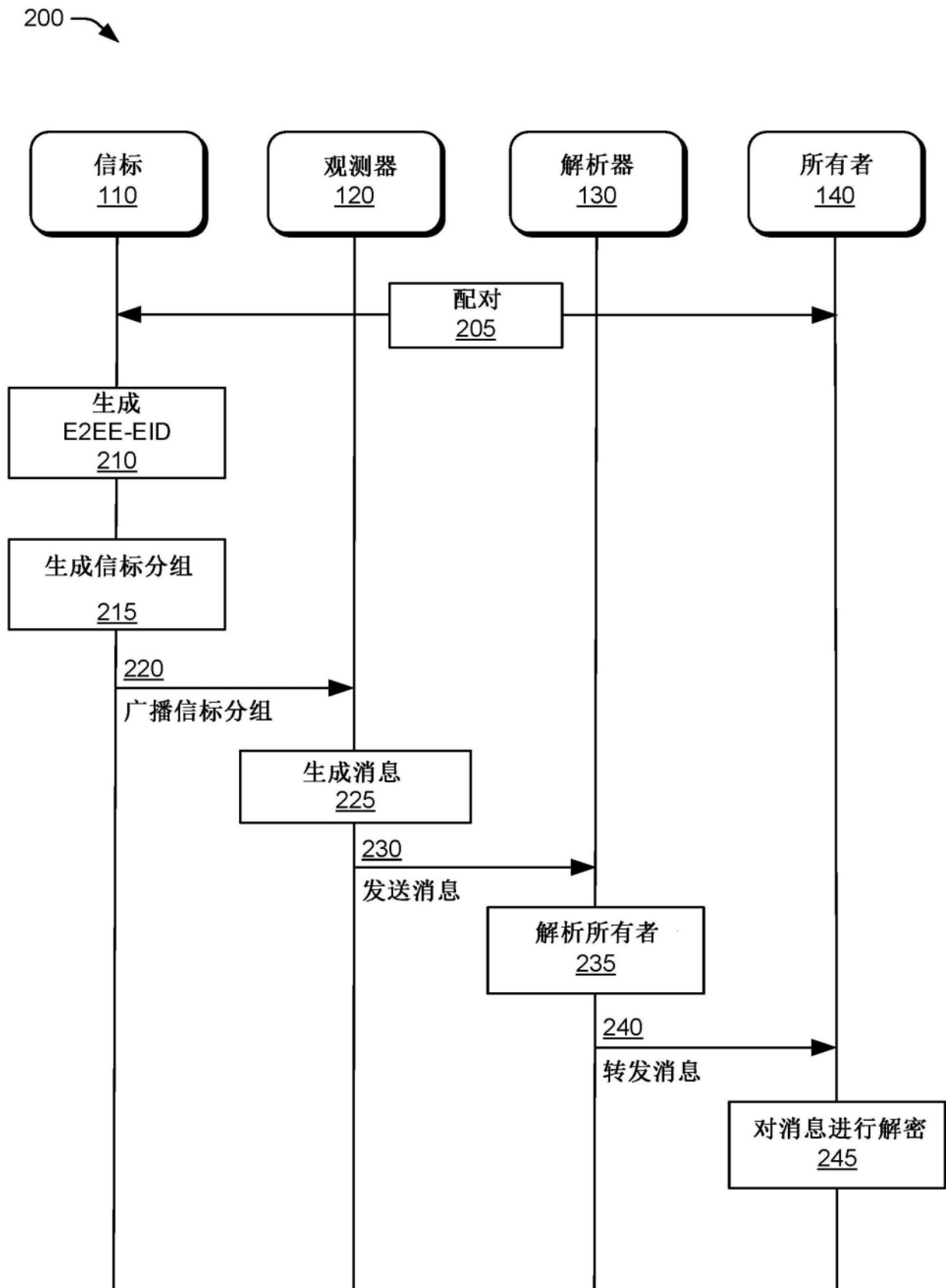


图2

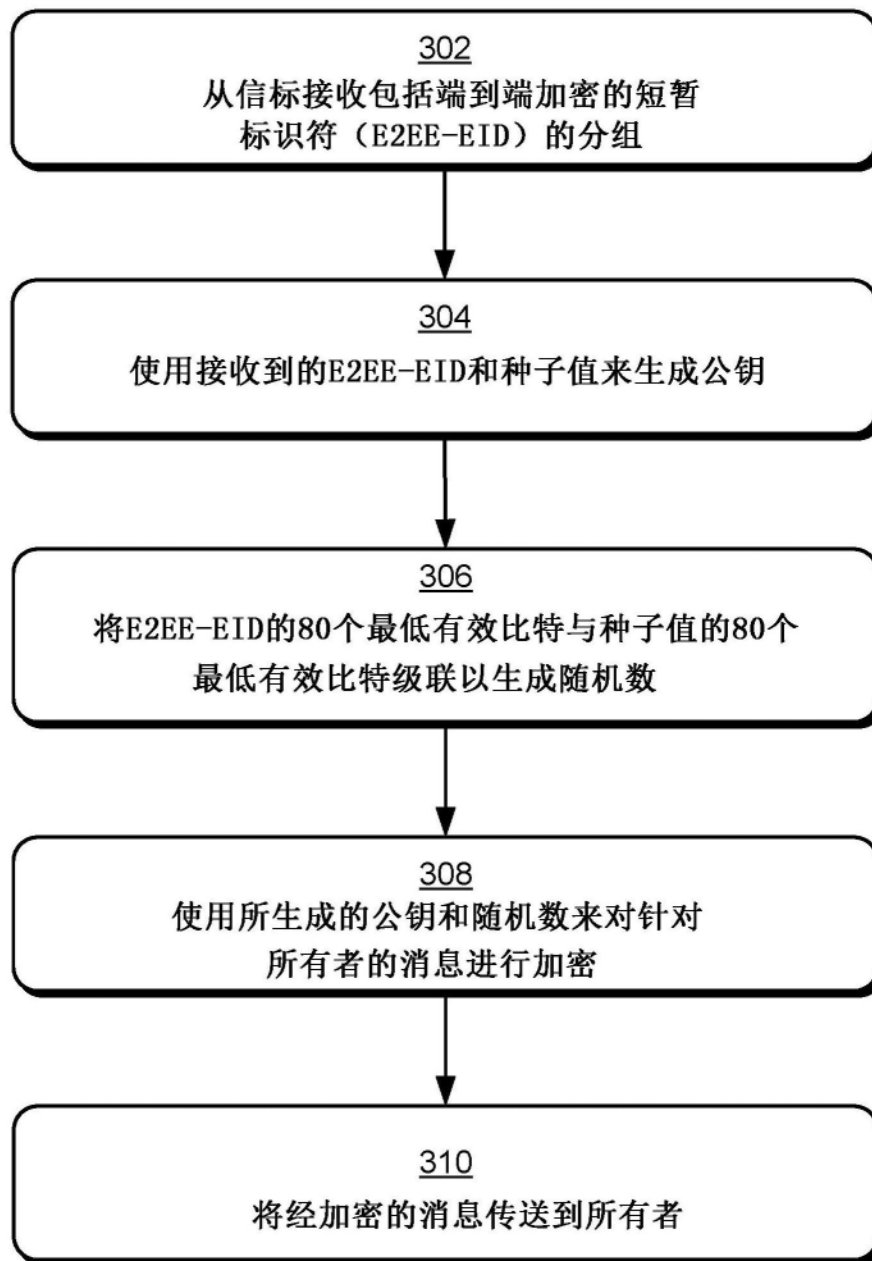
300 

图3

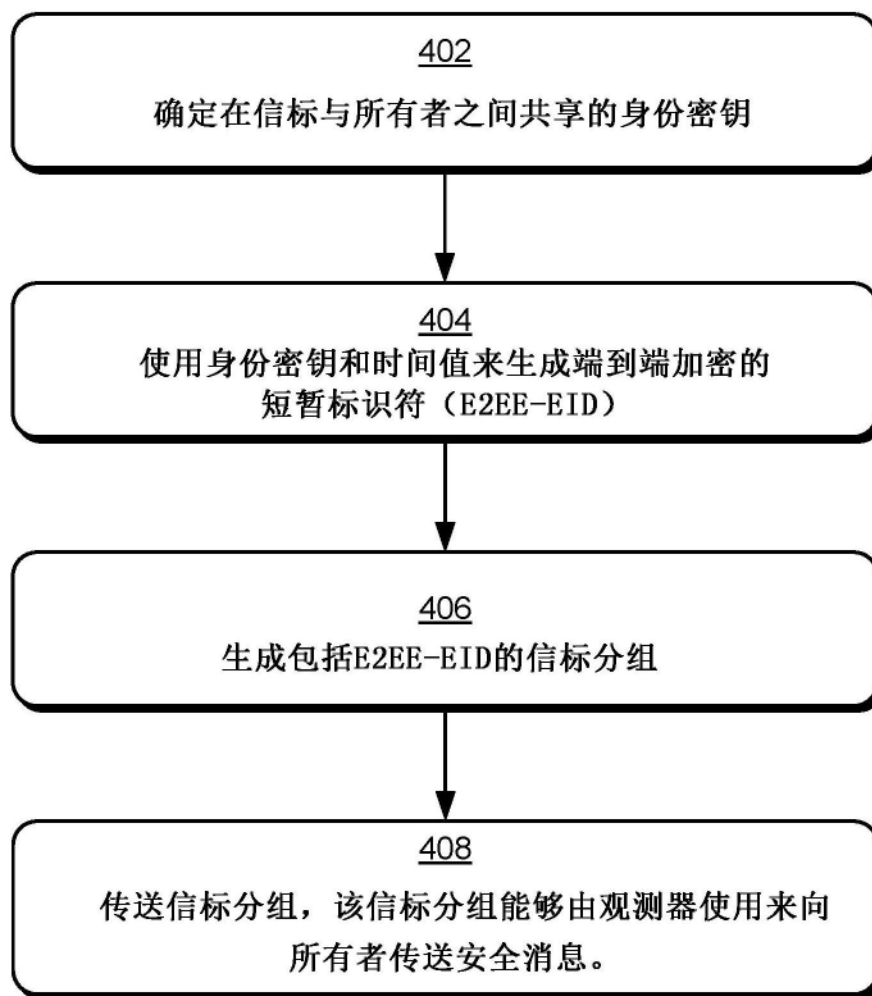
400 

图4

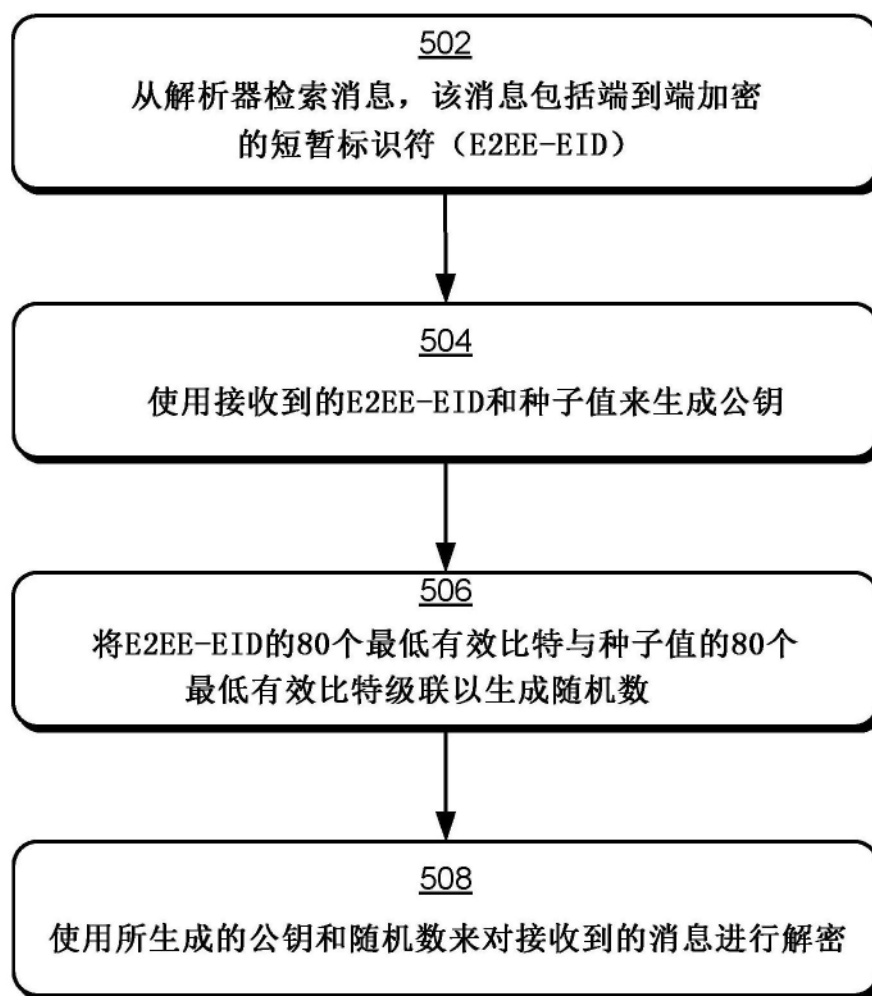
500 

图5

600 →

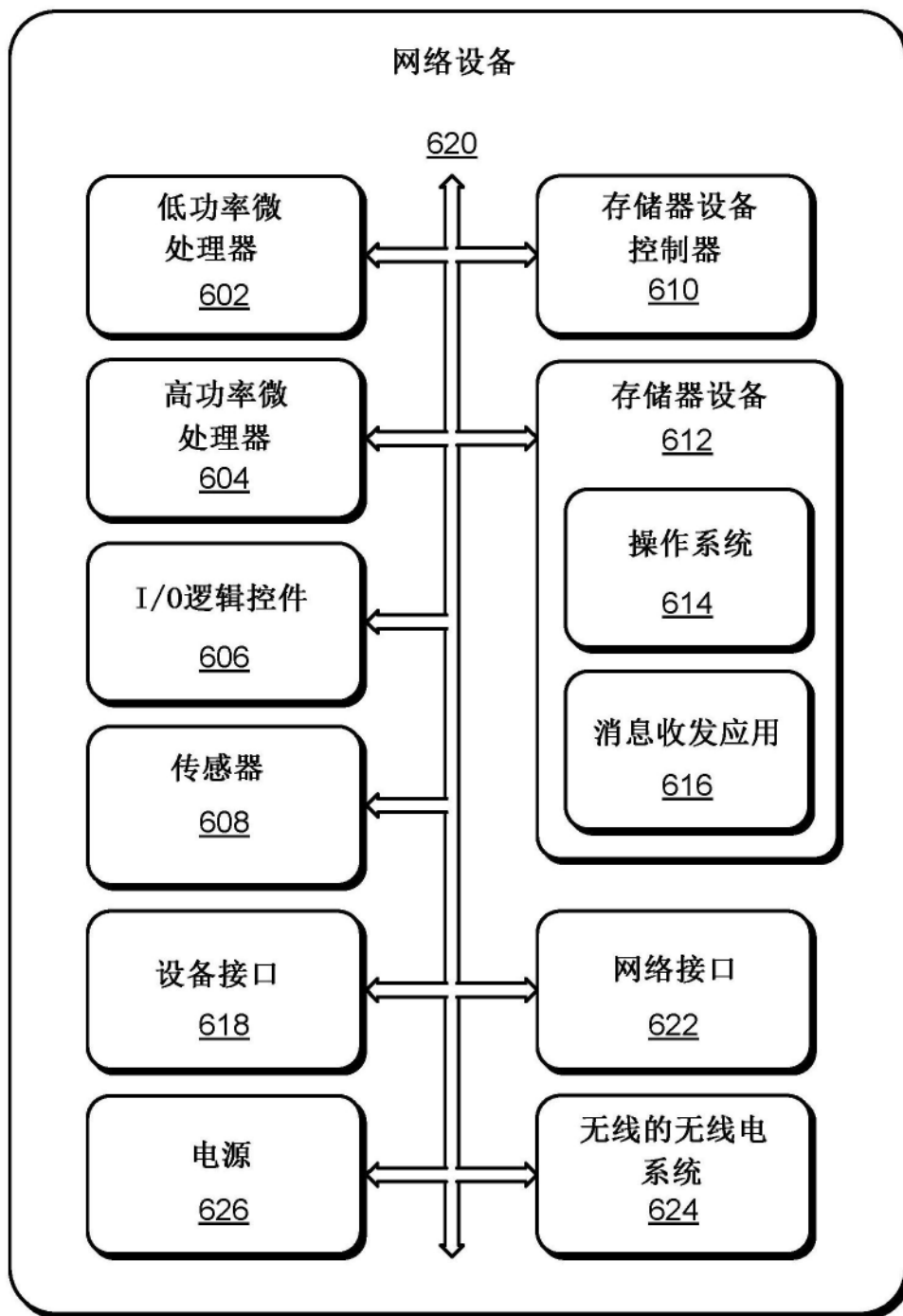


图6

700 →

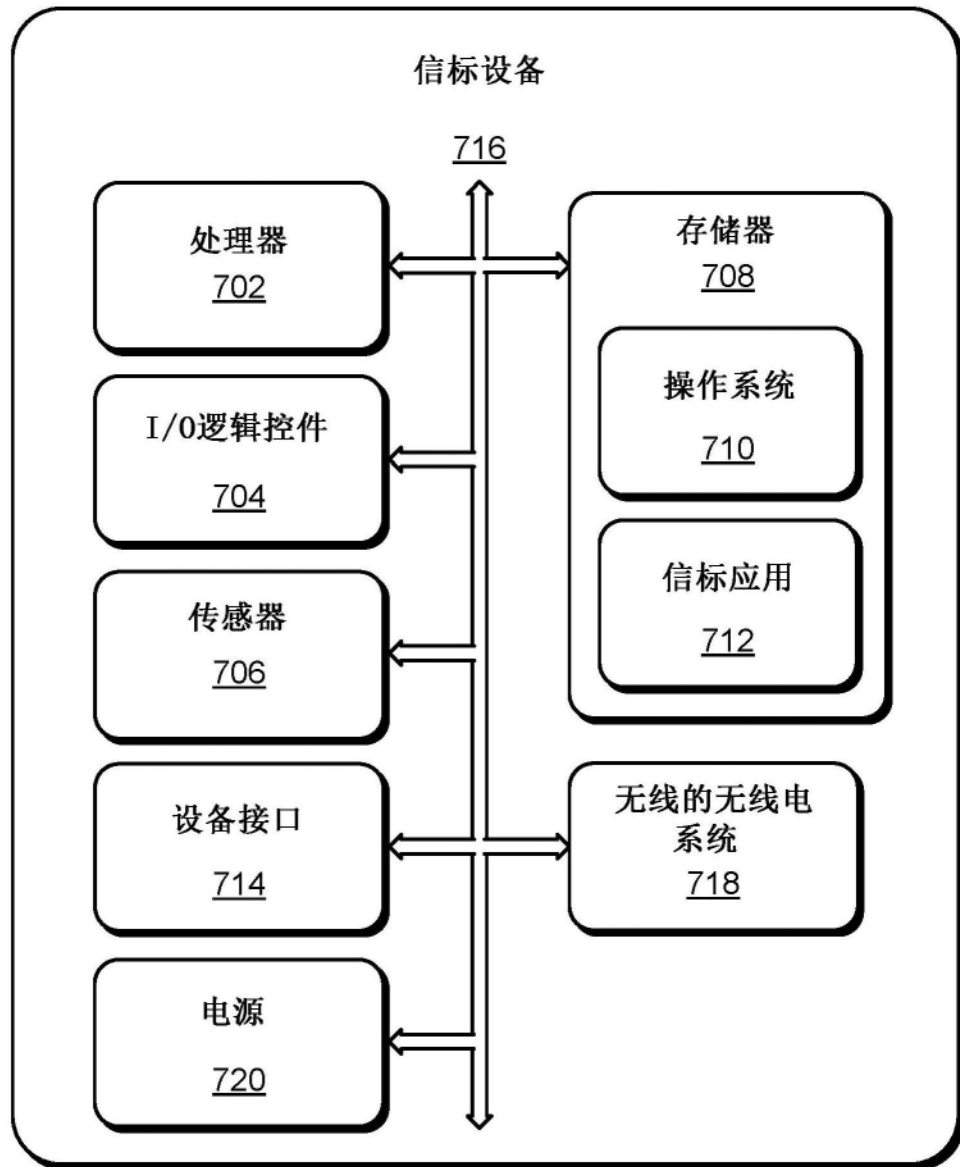


图7