(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 104247369 A
(43)申请公布日 2014.12.24

(21)申请号 201380020574.9

(22)申请日 2013.02.22

(30)优先权数据
61/601,620 2012.02.22 US
61/637,834 2012.04.24 US
61/670,226 2012.07.11 US
61/693,169 2012.08.24 US
61/701,457 2012.09.14 US
61/713,239 2012.10.12 US
61/716,373 2012.10.19 US
61/717,964 2012.10.24 US
61/728,677 2012.11.20 US
61/745,395 2012.12.21 US
61/745,308 2012.12.21 US
13/773,336 2013.02.21 US

(85)PCT国际申请进入国家阶段日
2014.10.17

(86)PCT国际申请的申请数据
PCT/US2013/027409 2013.02.22

(87)PCT国际申请的公布数据
WO2013/126759 EN 2013.08.29

(71)申请人 高通股份有限公司
地址 美国加利福尼亚

(72)发明人 C·S·沃斯特 N·尚 P·托马斯 S·A·斯普里格 M·霍尔菲尔德 I·H·麦克莱恩

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04W 12/02*(2006.01)
*H04L 9/18*(2006.01)
*G01S 1/02*(2006.01)
*H04W 84/22*(2006.01)
*G06Q 30/02*(2006.01)
*H04L 29/08*(2006.01)

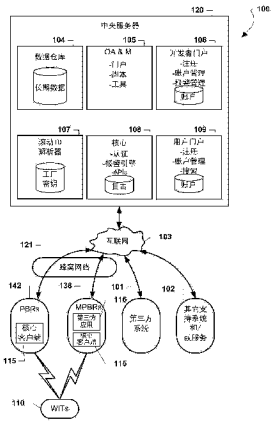
权利要求书26页 说明书70页 附图40页

(54)发明名称

用于使设备标识符变模糊的方法和设备

(57)摘要

用于在无线标识发射机(110)与中央服务器(120)之间同步模糊的标识信息,以支持该模糊的标识信息向中央服务器的单向传输的方法、系统和设备。该无线标识发射机(110)可以是被配置为例如通过蓝牙®通告,对包括模糊的标识符的消息进行广播,以便由附近的邻近广播接收机(138、142)接收,并经由可能还包括位置信息的目击消息来中继给中央服务器(120)的紧凑设备。中央服务器(120)可以对接收的识别码进行解码,以识别无线标识发射机。无线标识发射机可以通过将识别信息与递增的随机数进行连接,对连接后的信息进行加密,并对加密后的信息进行截短,来生成消息数据。替代地,可以使用中央服务器知道的伪随机函数和密钥,对连接后的标识信息进行加密。中央服务器可以将接收的数据与预先计算的加密数据进行比较。



CN 104247369 A

1. 一种用于服务器安全地识别包括模糊信息的消息的发起方的方法，包括：

将共享密钥与同无线标识发射机相对应的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

使用流式加密算法和所述共享密钥对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

判断所述解码后的设备标识符是否与同所述共享密钥相关联的设备标识符相匹配；以及

当所述解码后的设备标识符与同所述无线标识发射机相关联的所述设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

2. 根据权利要求 1 所述的方法，其中，所述消息还包括随机数，其中使用流式加密算法和所述共享密钥对所提取的滚动标识符进行解码以生成解码后的设备标识符包括：使用流式加密算法、从所述消息中提取的所述随机数和所述共享密钥，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符。

3. 根据权利要求 1 所述的方法，其中，所述流式加密算法是 AES-CTR 密码。

4. 根据权利要求 1 所述的方法，其中，所述共享密钥的大小为 128 比特。

5. 根据权利要求 1 所述的方法，其中，使用流式加密算法和所述共享密钥对所提取的滚动标识符进行解码以生成解码后的设备标识符，还包括：对在加密之前连接到所述设备标识符的数据进行解码。

6. 一种用于无线标识发射机发送模糊信息，以实现标识信息的单向传输的方法，包括：

对所述无线标识发射机中的随机数进行初始化；

通过使用所述随机数和与服务器共享的密钥以流式加密算法对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增。

7. 根据权利要求 6 所述的方法，其中，所述定期地广播的消息还包括所述随机数。

8. 根据权利要求 6 所述的方法，其中，所述随机数表示由所述无线标识发射机生成的非重复数字，其中，在每次需要改变所述设备标识符编码时，改变所述非重复数字的值。

9. 根据权利要求 6 所述的方法，其中，所述流式加密算法是 AES-CTR 密码。

10. 根据权利要求 6 所述的方法，其中，所述消息是大小为 80 个比特或更小的单个分组，并且其中，所述密钥是 128 个比特。

11. 根据权利要求 6 所述的方法，其中，生成所述滚动标识符包括：将要发送的数据连接到所述设备标识符，并且使用所述随机数和与服务器共享的所述密钥以所述流式加密算法对所连接的标识符和数据进行编码。

12. 一种用于服务器安全地识别包括模糊信息的消息的发起方的方法，包括：

将共享的密钥与随机数和用于无线标识发射机的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

对所述随机数进行递增，以表示所述服务器的当前时间；

使用所述共享密钥、所述随机数以及伪随机函数，对所述设备标识符进行编码，以生成服务器加密的数据；

判断所述服务器加密的数据是否与所提取的滚动标识符相匹配；以及

当所述服务器加密的数据与所提取的滚动标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

13. 根据权利要求 12 所述的方法，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

14. 根据权利要求 12 所述的方法，其中，对所述随机数进行递增以表示所述服务器的当前时间，包括：基于所述消息中包括的信息，对所述随机数进行计算，以便与邻近广播接收机从所述无线标识发射机接收广播的时间相对应。

15. 根据权利要求 12 所述的方法，还包括：从所接收的消息中提取随机数，其中，对所述设备标识符进行编码使用了从所接收的消息中提取的随机数。

16. 一种用于无线标识发射机发送模糊信息，以实现标识信息的单向传输的方法，包括：

对所述无线标识发射机中的随机数进行初始化；

通过使用伪随机函数以便基于所述随机数和与服务器共享的密钥，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

17. 根据权利要求 16 所述的方法，其中，通过使用伪随机函数来生成滚动标识符，包括：将要发送的数据连接到所述设备标识符，并且基于所述随机数和与服务器共享的所述密钥，使用所述伪随机函数对所述连接后的设备标识符和数据进行编码。

18. 根据权利要求 16 所述的方法，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

19. 一种用于服务器安全地识别包括模糊信息的消息的发起方的方法，包括：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，使用流式加密算法、所述第一密钥以及与所提取的编码的随机数相匹配的预先计算的编码随机数相关联的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的一个随机数不匹配时，使用所述流式加密算法、所述第一密钥、以及与所述无线标识发射机相关联的初始随

机数，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符；以及

当所述解码后的设备标识符与所述无线标识发射机的设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

20. 根据权利要求 19 所述的方法，其中，所述第一密钥和所述第二密钥具有相同的值。

21. 一种用于无线标识发射机发送模糊信息，以实现标识信息的单向传输的方法，包括：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的第一密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数；

使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

22. 一种用于服务器安全地识别消息的发起方的方法，包括：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

使用流式加密算法与所述第一密钥、所述当前随机数和所述设备标识符，预先计算多个编码的设备标识符；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，将所提取的滚动标识符与所述多个预先计算的编码的设备标识符进行比较；以及

当所提取的滚动标识符与所述多个预先计算的编码的设备标识符中的任一个相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

23. 一种用于服务器安全地识别消息的发起方的方法，包括：

使用加密算法、共享密钥、初始随机数以及与无线标识发射机相关联的设备标识符，生成多个初始模型有效载荷，其中所述加密算法是与所述无线标识发射机共享的；

使用所述加密算法、所述共享密钥、当前随机数以及与所述无线标识发射机相关联的所述设备标识符，来生成多个当前模型有效载荷；

接收所述消息，所述消息包括具有模糊的标识信息的有效载荷；

将所接收的消息的有效载荷与所述多个当前模型有效载荷进行比较；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的一个相匹配时，识别所述无线标识发射机；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的任一个都不匹配时，将

所接收的消息的有效载荷与所述多个初始模型有效载荷进行比较；

当所接收的消息的有效载荷与所述多个初始模型有效载荷中的一个相匹配时，识别所述无线标识发射机；以及

当所接收的消息的有效载荷与初始模型有效载荷和当前模型有效载荷中的至少一个相匹配时，对与所述无线标识发射机相关联的所述当前随机数进行更新。

24. 一种用于无线标识发射机接收输入消息的方法，所述方法包括：

在第一时段，经由短距离无线传输，来定期地广播用于指示接收输入传输的可用性的消息；

响应于所述第一时段到期，在第二时段期间，接收链路通告消息；

基于所接收的链路通告消息中的信息，与邻近广播接收机协商链路；

对所述协商的链路进行认证；以及

经由所述协商的链路，来处理输入消息，并且

其中，所述协商的链路是经由蓝牙配对来执行的。

25. 根据权利要求 24 所述的方法，其中，所述输入消息包括以下各项中的至少一项：固件更新、配置信息、触发信号和软件指令。

26. 根据权利要求 24 所述的方法，其中，所述第一时段是由以下各项中的至少一项来定义的：所述无线标识发射机上的定时器、时钟信号、以及从所述邻近广播接收机接收的消息。

27. 一种被配置为安全地识别包括模糊信息的消息的发起方的服务器，包括：

用于将共享密钥与同无线标识发射机相对应的设备标识符进行关联的单元；

用于接收包括滚动标识符的所述消息的单元；

用于从所接收的消息中提取所述滚动标识符的单元；

用于使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码，以生成解码后的设备标识符的单元；

用于判断所述解码后的设备标识符是否与同所述共享密钥相关联的设备标识符相匹配的单元；

用于当所述解码后的设备标识符与同所述无线标识发射机相关联的设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机的单元。

28. 根据权利要求 27 所述的服务器，其中，所述消息还包括随机数，并且其中，用于使用流式加密算法和所述共享密钥对所提取的滚动标识符进行解码以生成解码后的设备标识符的单元包括：用于使用流式加密算法、从所述消息中提取的随机数和所述共享密钥，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符的单元。

29. 根据权利要求 27 所述的服务器，其中，所述流式加密算法是 AES-CTR 密码。

30. 根据权利要求 27 所述的服务器，其中，所述共享密钥的大小为 128 个比特。

31. 根据权利要求 27 所述的服务器，其中，用于使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码以生成解码后的设备标识符的单元还包括：用于对在加密之前连接到所述设备标识符的数据进行解码的单元。

32. 一种被配置为发送模糊信息，以实现标识信息的单向传输的无线标识发射机，包括：

用于对所述无线标识发射机中的随机数进行初始化的单元；

用于通过使用所述随机数和与服务器共享的密钥，以流式加密算法对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符的单元；

用于使用短距离无线传输，来定期地广播包括所述滚动标识符的消息的单元；以及

用于按照预先定义的时间间隔，对所述随机数进行递增的单元。

33. 根据权利要求 32 所述的无线标识发射机，其中，所述定期地广播的消息还包括所述随机数。

34. 根据权利要求 32 所述的无线标识发射机，其中，所述随机数表示由所述无线标识发射机生成的非重复数字，在每次需要改变所述设备标识符编码时，改变所述非重复数字的值。

35. 根据权利要求 32 所述的无线标识发射机，其中，所述流式加密算法是 AES-CTR 密码。

36. 根据权利要求 32 所述的无线标识发射机，其中，所述消息是大小为 80 个比特或更小的单个分组，并且其中所述密钥是 128 个比特。

37. 根据权利要求 32 所述的无线标识发射机，其中，用于生成所述滚动标识符的单元包括：用于将要发送的数据连接到所述设备标识符，并且使用所述随机数和与服务器共享的所述密钥，以所述流式加密算法对连接后的标识符和数据进行编码的单元。

38. 一种被配置为安全地识别包括模糊信息的消息的发起方的服务器，包括：

用于将共享密钥与随机数和用于无线标识发射机的设备标识符进行关联的单元；

用于接收包括滚动标识符的所述消息的单元；

用于从所接收的消息中提取所述滚动标识符的单元；

用于对所述随机数进行递增以表示所述服务器的当前时间的单元；

用于使用所述共享密钥、所述随机数和伪随机函数，对所述设备标识符进行编码，以生成服务器加密的数据的单元；

用于判断所述服务器加密的数据是否与所提取的滚动标识符相匹配的单元；以及

用于当所述服务器加密的数据与所提取的滚动标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机的单元。

39. 根据权利要求 38 所述的服务器，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

40. 根据权利要求 38 所述的服务器，其中，用于对所述随机数进行递增以表示所述服务器的当前时间的单元包括：用于基于所述消息中包括的信息，对所述随机数进行计算，以便与邻近广播接收机从所述无线标识发射机接收广播的时间相对应的单元。

41. 根据权利要求 38 所述的服务器，还包括：用于从所接收的消息中提取随机数的单元，其中，用于对所述设备标识符进行编码的单元使用从所接收的消息中提取的所述随机数。

42. 一种被配置为发送模糊信息，以实现标识信息的单向传输的无线标识发射机，包括：

用于对所述无线标识发射机中的随机数进行初始化的单元；

用于通过使用伪随机函数，以便基于所述随机数和与服务器共享的密钥，对与所述无

线标识发射机相关联的设备标识符进行编码，来生成滚动标识符的单元；

用于使用短距离无线传输，来定期地广播包括所述滚动标识符的消息的单元；以及

用于按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间的单元。

43. 根据权利要求 42 所述的无线标识发射机，其中，用于通过使用伪随机函数来生成滚动标识符的单元包括：用于将要发送的数据连接到所述设备标识符，并且基于所述随机数和与服务器共享的所述密钥，使用所述伪随机函数对连接后的设备标识符和数据进行编码的单元。

44. 根据权利要求 42 所述的无线标识发射机，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

45. 一种被配置为安全地识别包括模糊信息的消息的发起方的服务器，包括：

用于将无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联的单元；

用于使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数的单元；

用于接收包括滚动标识符和编码的随机数的所述消息的单元；

用于从所接收的消息中提取所述编码的随机数的单元；

用于从所接收的消息中提取所述滚动标识符的单元；

用于将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较的单元；

用于当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，使用流式加密算法、所述第一密钥、以及与所提取的编码的随机数相匹配的预先计算的编码随机数相关联的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符的单元；

用于当所提取的编码的随机数与所述多个预先计算的编码的随机数中的一个随机数不匹配时，使用所述流式加密算法、所述第一密钥、以及与所述无线标识发射机相关联的所述初始随机数，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符的单元；以及

用于当所述解码后的设备标识符与所述无线标识发射机的所述设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机的单元。

46. 根据权利要求 45 所述的服务器，其中，所述第一密钥和所述第二密钥具有相同的值。

47. 一种被配置为发送模糊信息，以实现标识信息的单向传输的无线标识发射机，包括：

用于对所述无线标识发射机中的随机数进行初始化的单元；

用于通过与服务器共享的第一密钥、和所述随机数以及流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符的单元；

用于通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数的单元；

用于使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息的单元；以及

用于按照预先定义的时间间隔对所述随机数进行递增，以便维持所述无线标识发射机的当前时间的单元。

48. 一种被配置为安全地识别消息的发起方的服务器，包括：

用于将无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联的单元；

用于使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数的单元；

用于使用流式加密算法与所述第一密钥、所述当前随机数和所述设备标识符，来预先计算多个编码的设备标识符的单元；

用于接收包括滚动标识符和编码的随机数的所述消息的单元；

用于从所接收的消息中提取所述编码的随机数的单元；

用于从所接收的消息中提取所述滚动标识符的单元；

用于将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较的单元；

用于当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个随机数相匹配时，将所提取的滚动标识符与所述多个预先计算的编码的设备标识符进行比较的单元；以及

用于当所提取的滚动标识符与所述多个预先计算的编码的设备标识符中的任一个相匹配时，将所接收的消息的发起方识别成所述无线标识发射机的单元。

49. 一种被配置为识别消息的发起方的服务器，包括：

用于使用加密算法、共享密钥、初始随机数以及与无线标识发射机相关联的设备标识符，来生成多个初始模型有效载荷的单元，其中所述加密算法是与所述无线标识发射机共享的；

用于使用所述加密算法、所述共享密钥、当前随机数以及与所述无线标识发射机相关联的设备标识符，来生成多个当前模型有效载荷的单元；

用于接收所述消息的单元，所述消息包括具有模糊的标识信息的有效载荷；

用于将所接收的消息的有效载荷与所述多个当前模型有效载荷进行比较的单元；

用于当所接收的消息的有效载荷与所述多个当前模型有效载荷中的一个相匹配时，识别所述无线标识发射机的单元；

用于当所接收的消息的有效载荷与所述多个当前模型有效载荷中的任一个都不匹配时，将所接收的消息的所述有效载荷与所述多个初始模型有效载荷进行比较的单元；

用于当所接收的消息的所述有效载荷与所述多个初始模型有效载荷中的一个相匹配时，识别所述无线标识发射机的单元；以及

用于当所接收的消息的所述有效载荷与初始模型有效载荷和当前模型有效载荷中的至少一个相匹配时，对与所述无线标识发射机相关联的所述当前随机数进行更新的单元。

50. 一种被配置为接收输入消息的无线标识发射机，包括：

用于在第一时段，经由短距离无线传输来定期地广播用于指示接收输入传输的的可用

性的消息的单元；

用于响应于所述第一时段到期，在第二时段期间，接收链路通告消息的单元；

用于基于在所接收的链路通告消息中的信息，与邻近广播接收机协商链路的单元；

用于对所协商的链路进行认证的单元；以及

用于经由所协商的链路来处理输入消息的单元，

其中，所协商的链路是经由蓝牙配对来执行的。

51. 根据权利要求 50 所述的无线标识发射机，其中，所述输入消息包括以下各项中的至少一项：固件更新、配置信息、触发信号和软件指令。

52. 根据权利要求 50 所述的无线标识发射机，其中，所述第一时段由以下各项中的至少一项来定义的：所述无线标识发射机上的定时器、时钟信号、以及从所述邻近广播接收机接收到的消息。

53. 一种被配置为安全地识别包括模糊信息的消息的发起方的服务器，包括：

存储器；以及

耦接到所述存储器的服务器处理器，其中，所述服务器处理器被服务器处理器可执行指令配置为执行包括以下各项的操作：

将共享的密钥与同无线标识发射机相对应的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

判断所述解码后的设备标识符是否与同所述共享密钥相关联的所述设备标识符相匹配；以及

当所述解码后的设备标识符与同所述无线标识发射机相关联的所述设备标识符相匹配时，将所接收的消息的所述发起方识别成所述无线标识发射机。

54. 根据权利要求 53 所述的方法，其中，所述消息还包括随机数，并且其中所述服务器处理器被服务器处理器可执行指令配置为执行操作，使得使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码以生成解码后的设备标识符，包括：使用流式加密算法、从所述消息中提取的随机数和所述共享密钥，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符。

55. 根据权利要求 53 所述的服务器，其中，所述流式加密算法是 AES-CTR 密码。

56. 根据权利要求 53 所述的服务器，其中，所述共享密钥的大小为 128 个比特。

57. 根据权利要求 53 所述的服务器，其中，所述服务器处理器被服务器处理器可执行指令配置为执行操作，使得使用流式加密算法和所述共享密钥对所提取的滚动标识符进行解码以生成解码后的设备标识符还包括：对在加密之前连接到所述设备标识符的数据进行解码。

58. 一种被配置为发送模糊的信息，以实现标识信息的单向传输的无线标识发射机，包括：

存储器；以及

耦接到所述存储器的处理器，其中所述处理器被处理器可执行指令配置为执行包括下

面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过使用所述随机数和与服务器共享的密钥，以流式加密算法对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增。

59. 根据权利要求 58 所述的无线标识发射机，其中，所述定期广播的消息还包括所述随机数。

60. 根据权利要求 58 所述的无线标识发射机，其中，所述随机数表示由所述无线标识发射机生成的非重复数字，在每次需要改变所述设备标识符编码时，改变所述非重复数字的值。

61. 根据权利要求 58 所述的无线标识发射机，其中，所述流式加密算法是 AES-CTR 密码。

62. 根据权利要求 58 所述的无线标识发射机，其中，所述消息是大小为 80 个比特或更小的单个分组，并且其中所述密钥是 128 个比特。

63. 根据权利要求 58 所述的无线标识发射机，其中，所述处理器被处理器可执行指令配置为执行操作使得生成所述滚动标识符包括：将要发送的数据连接到所述设备标识符，并且使用所述随机数和与服务器共享的所述密钥，以所述流式加密算法对所连接的标识符和数据进行编码。

64. 一种被配置为安全地识别包括模糊信息的消息的发起方的服务器，包括：

存储器；以及

耦接到所述存储器的服务器处理器，其中所述服务器处理器被服务器处理器可执行指令配置为执行包括下面各项的操作：

将共享密钥与随机数和用于无线标识发射机的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

对所述随机数进行递增，以表示所述服务器的当前时间；

使用所述共享密钥、所述随机数和伪随机函数，对所述设备标识符进行编码，以生成服务器加密的数据；

判断所述服务器加密的数据是否与所提取的滚动标识符相匹配；以及

当所述服务器加密的数据与所提取的滚动标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

65. 根据权利要求 64 所述的服务器，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

66. 根据权利要求 64 所述的服务器，其中，所述服务器处理器被服务器处理器可执行指令配置为执行操作使得对所述随机数进行递增以表示所述服务器的当前时间包括：基于所述消息中包括的信息，对所述随机数进行计算，以便与邻近广播接收机从所述无线标识发射机接收广播的时间相对应。

67. 根据权利要求 64 所述的服务器，其中，所述服务器处理器被服务器处理器可执行

指令配置为执行还包括以下的操作：

从所接收的消息中提取随机数，其中，对所述设备标识符进行编码使用了从所接收的消息中提取的所述随机数。

68. 一种被配置为发送模糊信息，以实现标识信息的单向传输的无线标识发射机，包括：

存储器；以及

耦接到所述存储器的处理器，其中，所述处理器被处理器可执行指令配置为执行包括以下各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的密钥，以伪随机函数，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

69. 根据权利要求 68 所述的无线标识发射机，其中，所述服务器处理器被服务器处理器可执行指令配置为执行操作使得通过使用伪随机函数来生成滚动标识符包括：将要发送的数据连接到所述设备标识符，并且基于所述随机数和与服务器共享的所述密钥，使用所述伪随机函数对所连接的设备标识符和数据进行编码。

70. 根据权利要求 68 所述的无线标识发射机，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

71. 一种被配置为识别包括模糊信息的消息的发起方的服务器，包括：

存储器；以及

耦接到所述存储器的服务器处理器，其中所述服务器处理器被服务器处理器可执行指令配置为执行包括下面各项的操作：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，使用流式加密算法、所述第一密钥、以及与所提取的编码的随机数相匹配的预先计算的编码随机数相关联的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的一个不匹配时，使用所述流式加密算法、所述第一密钥、以及与所述无线标识发射机相关联的初始随机数，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符；以及

当所述解码后的设备标识符与所述无线标识发射机的所述设备标识符相匹配时，将所

接收的消息的所述发起方识别成所述无线标识发射机。

72. 根据权利要求 71 所述的服务器，其中，所述第一密钥和所述第二密钥具有相同的值。

73. 一种被配置为发送模糊信息以实现标识信息的单向传输的无线标识发射机，包括：

存储器；以及

耦接到所述存储器的处理器，其中，所述处理器被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的第一密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数；

使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

74. 一种被配置为安全地识别消息的发起方的服务器，包括：

存储器；以及

耦接到所述存储器的服务器处理器，其中所述服务器处理器被服务器处理器可执行指令配置为执行包括下面各项的操作：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

使用流式加密算法和所述第一密钥、所述当前随机数和所述设备标识符，来预先计算多个编码的设备标识符；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，将所提取的滚动标识符与所述多个预先计算的编码的设备标识符进行比较；

当所提取的滚动标识符与所述多个预先计算的编码的设备标识符中的任一个相匹配时，将所接收的消息的所述发起方识别成所述无线标识发射机。

75. 一种被配置为安全地识别消息的发起方的服务器，包括：

存储器；以及

耦接到所述存储器的服务器处理器，其中所述服务器处理器被服务器处理器可执行指令配置为执行包括下面各项的操作：

使用加密算法、共享密钥、初始随机数和与无线标识发射机相关联的设备标识符，生成

多个初始模型有效载荷，其中，所述加密算法是与所述无线标识发射机共享的；

使用所述加密算法、所述共享密钥、当前随机数和与所述无线标识发射机相关联的设备标识符，来生成多个当前模型有效载荷；

接收所述消息，所述消息包括具有模糊的标识信息的有效载荷；

将所接收的消息的有效载荷与所述多个当前模型有效载荷进行比较；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的一个相匹配时，识别所述无线标识发射机；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的任一个都不匹配时，将所接收的消息的有效载荷与所述多个初始模型有效载荷进行比较；

当所接收的消息的所述有效载荷与所述多个初始模型有效载荷中的一个相匹配时，识别所述无线标识发射机；以及

当所接收的消息的所述有效载荷与初始模型有效载荷和当前模型有效载荷中的至少一个相匹配时，对与所述无线标识发射机相关联的所述当前随机数进行更新。

76. 一种被配置为接收输入的消息的无线标识发射机，包括：

存储器；以及

耦接到所述存储器的处理器，其中所述处理器被处理器可执行指令配置为执行包括下面各项的操作：

在第一时段，经由短距离无线传输，来定期地广播用于指示接收输入传输的可用性的消息；

响应于所述第一时段到期，在第二时段期间，接收链路通告消息；

基于在所接收的链路通告消息中的信息，与邻近广播接收机协商链路；

对所协商的链路进行认证；以及

经由所协商的链路，来处理所述输入消息，

其中，所协商的链路是经由蓝牙配对来执行的。

77. 根据权利要求 76 所述的无线标识发射机，其中，所述输入消息包括下面各项中的至少一项：固件更新、配置信息、触发信号和软件指令。

78. 根据权利要求 76 所述的无线标识发射机，其中，所述第一时段是由下面各项中的至少一项来定义的：所述无线标识发射机上的定时器、时钟信号、以及从所述邻近广播接收机接收的消息。

79. 一种具有存储在其上的服务器可执行指令的非临时性服务器可读存储介质，所述服务器可执行指令被配置为使得服务器执行用于所述服务器安全地识别包括模糊信息的消息的发起方的操作，所述操作包括：

将共享密钥与同无线标识发射机相对应的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

判断所述解码后的设备标识符是否与同所述共享密钥相关联的所述设备标识符相匹配；以及

当所述解码后的设备标识符与同所述无线标识发射机相关联的所述设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

80. 根据权利要求 79 所述的非临时性服务器可读存储介质，其中，所述消息还包括随机数，并且其中，所存储的服务器可执行指令被配置为使服务器执行操作，使得使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码以生成解码后的设备标识符，包括：使用流式加密算法、从所述消息中提取的随机数和所述共享密钥，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符。

81. 根据权利要求 79 所述的非临时性服务器可读存储介质，其中，所述流式加密算法是 AES-CTR 密码。

82. 根据权利要求 79 所述的非临时性服务器可读存储介质，其中，所述共享密钥的大小为 128 个比特。

83. 根据权利要求 79 所述的非临时性服务器可读存储介质，其中，所存储的服务器可执行指令被配置为使服务器执行操作，使得使用流式加密算法和所述共享密钥，对所提取的滚动标识符进行解码以生成解码后的设备标识符，还包括：对在加密之前连接到所述设备标识符的数据进行解码。

84. 一种具有存储在其上的处理器可执行软件指令的非临时性处理器可读存储介质，其中所述处理器可执行软件指令被配置为使得处理器执行用于无线标识发射机发送模糊信息，以实现标识信息的单向传输的操作，所述操作包括：

对所述无线标识发射机中的随机数进行初始化；

通过使用所述随机数和与服务器共享的密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增。

85. 根据权利要求 84 所述的非临时性处理器可读存储介质，其中，所述定期地广播的消息还包括所述随机数。

86. 根据权利要求 84 所述的非临时性处理器可读存储介质，其中，所述随机数表示由所述无线标识发射机生成的非重复数字，其中在每次需要改变所述设备标识符的编码时，改变所述非重复数字的值。

87. 根据权利要求 84 所述的非临时性处理器可读存储介质，其中，所述流式加密算法是 AES-CTR 密码。

88. 根据权利要求 84 所述的非临时性处理器可读存储介质，其中，所述消息是大小为 80 比特或更小的单个分组，并且其中所述密钥是 128 个比特。

89. 根据权利要求 84 所述的非临时性处理器可读存储介质，其中，所存储的服务器可执行指令被配置为使服务器执行操作，使得生成所述滚动标识符包括：将要发送的数据连接到所述设备标识符，并且使用所述随机数和与服务器共享的所述密钥，以所述流式加密算法对所连接的标识符和数据进行编码。

90. 一种具有存储在其上的服务器可执行指令的非临时性服务器可读存储介质，其中所述服务器可执行指令被配置为使得服务器执行用于所述服务器安全地识别包括模糊信息的消息的发起方的操作，所述操作包括：

将共享密钥与随机数和用于无线标识发射机的设备标识符进行关联；

接收包括滚动标识符的所述消息；

从所接收的消息中提取所述滚动标识符；

对所述随机数进行递增，以表示所述服务器的当前时间；

使用所述共享密钥、所述随机数和伪随机函数，对所述设备标识符进行编码，以生成服务器加密的数据；

判断所述服务器加密的数据是否与所提取的滚动标识符相匹配；以及

当所述服务器加密的数据与所提取的滚动标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

91. 根据权利要求 90 所述的非临时性服务器可读存储介质，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

92. 根据权利要求 90 所述的非临时性服务器可读存储介质，其中，所述服务器可执行指令被配置为使所述服务器执行操作，使得对所述随机数进行递增以表示所述服务器的当前时间，包括：基于所述消息中包括的信息，对所述随机数进行计算，以便与邻近广播接收机从所述无线标识发射机接收广播的时间相对应。

93. 根据权利要求 90 所述的非临时性服务器可读存储介质，其中，所述服务器可执行指令被配置为使服务器执行还包括下面的操作：

从所接收的消息中提取随机数，其中对所述设备标识符进行编码使用了从所接收的消息中提取的所述随机数。

94. 一种具有存储在其上的处理器可执行软件指令的非临时性处理器可读存储介质，其中所述处理器可执行软件指令被配置为使得处理器执行用于无线标识发射机发送模糊的信息，以实现标识信息的单向传输的操作，所述操作包括：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的密钥，以伪随机函数对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

95. 根据权利要求 94 所述的非临时性服务器可读存储介质，其中，所述处理器可执行指令被配置为使处理器执行操作，使得通过使用伪随机函数来生成滚动标识符包括：将要发送的数据连接到所述设备标识符，并基于所述随机数和与服务器共享的所述密钥，使用所述伪随机函数对所连接的设备标识符和数据进行编码。

96. 根据权利要求 94 所述的非临时性处理器可读存储介质，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

97. 一种具有存储在其上的服务器可执行指令的非临时性服务器可读存储介质，其中所述服务器可执行指令被配置为使得服务器执行用于所述服务器安全地识别包括模糊信息的消息的发起方的操作，所述操作包括：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任何一个相匹配时，使用流式的加密算法、所述第一密钥、以及与所提取的编码的随机数相匹配的预先计算的编码随机数相关联的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的一个不匹配时，使用所述流式加密算法、所述第一密钥、以及与所述无线标识发射机相关联的所述初始随机数，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符；以及

当所述解码后的设备标识符与所述无线标识发射机的所述设备标识符相匹配时，将所接收的消息的所述发起方识别成所述无线标识发射机。

98. 根据权利要求 97 所述的非临时性服务器可读存储介质，其中，所述第一密钥和所述第二密钥具有相同的值。

99. 一种具有存储在其上的处理器可执行软件指令的非临时性处理器可读存储介质，其中所述处理器可执行软件指令被配置为使得处理器执行用于无线标识发射机发送模糊信息，以实现标识信息的单向传输的操作，所述操作包括：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的第一密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数；

使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间。

100. 一种具有存储在其上的服务器可执行指令的非临时性服务器可读存储介质，其中所述服务器可执行指令被配置为使得服务器执行用于所述服务器安全地识别消息的发起方的操作，所述操作包括：

将用于无线标识发射机的设备标识符与初始随机数、当前随机数、第一密钥和第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

使用流式加密算法与所述第一密钥、所述当前随机数和所述设备标识符，预先计算多个编码的设备标识符；

接收包括滚动标识符和编码的随机数的所述消息；

从所接收的消息中提取所述编码的随机数；

从所接收的消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，将所提取的滚动标识符与所述多个预先计算的编码的设备标识符进行比较；

当所提取的滚动标识符与所述多个预先计算的编码的设备标识符中的任一个相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

101. 一种具有存储在其上的服务器可执行指令的非临时性服务器可读存储介质，其中所述服务器可执行指令被配置为使得服务器执行用于使所述服务器安全地识别消息的发起方的操作，所述操作包括：

使用加密算法、共享密钥、初始随机数和与无线标识发射机相关联的设备标识符，生成多个初始模型有效载荷，其中所述加密算法是与所述无线标识发射机共享的；

使用所述加密算法、所述共享密钥、当前随机数和与所述无线标识发射机相关联的所述设备标识符，生成多个当前模型有效载荷；

接收所述消息，所述消息包括具有模糊的标识信息的有效载荷；

将所接收的消息的有效载荷与所述多个当前模型有效载荷进行比较；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的一个相匹配时，识别所述无线标识发射机；

当所接收的消息的有效载荷与所述多个当前模型有效载荷中的任一个都不匹配时，将所接收的消息的所述有效载荷与所述多个初始模型有效载荷进行比较；

当所接收的消息的所述有效载荷与所述多个初始模型有效载荷中的一个相匹配时，识别所述无线标识发射机；以及

当所接收的消息的所述有效载荷与初始模型有效载荷和当前模型有效载荷中的至少一个相匹配时，对与所述无线标识发射机相关联的所述当前随机数进行更新。

102. 一种具有存储在其上的处理器可执行软件指令的非临时性处理器可读存储介质，其中所述处理器可执行软件指令被配置为使得处理器执行用于无线标识发射机接收输入消息的操作，所述操作包括：

在第一时段，通过短距离无线传输，来定期地广播用于指示接收输入传输的可用性的消息；

响应于所述第一时段到期，在第二时段期间，接收链路通告消息；

基于所接收的链路通告消息中的信息，与邻近广播接收机协商链路；

对所协商的链路进行认证；

经由所协商的链路，来处理输入消息，

其中，所协商的链路是经由蓝牙配对来执行的。

103. 根据权利要求 102 所述的非临时性处理器可读存储介质，其中，所述输入消息包括下面各项中的至少一项：固件更新、配置信息、触发信号和软件指令。

104. 根据权利要求 102 所述的非临时性处理器可读存储介质，其中，所述第一时段是由以下各项中的至少一项来定义的：所述无线标识发射机上的定时器、时钟信号、以及从所述邻近广播接收机接收的消息。

105. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；

耦接到所述第一存储器和所述第一收发机的第一处理器，其被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过所述第一收发机，使用短距离无线传输，来定期地广播包括所述滚动标识符和所述随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

通过所述第二收发机，从所述无线标识发射机接收包括所述滚动标识符和所述随机数的所述消息；

通过所述网络设备，向所述服务器发送包括所述滚动标识符和所述随机数的目击消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面各项的操作：

将所述密钥与和所述无线标识发射机相对应的所述设备标识符进行关联；

接收包括所述滚动标识符和所述随机数的所述目击消息；

从所接收的目击消息中提取所述随机数和所述滚动标识符；

使用所述流式加密算法、所述密钥和所提取的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

判断所述解码后的设备标识符是否与同所述密钥相关联的所述设备标识符相匹配；以及

当所述解码后的设备标识符与同所述无线标识发射机相关联的所述设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

106. 根据权利要求 105 所述的系统，其中，所述流式加密算法是 AES-CTR 密码。

107. 根据权利要求 105 所述的系统，其中，所述密钥的大小为 128 个比特。

108. 根据权利要求 105 所述的系统，其中，所述随机数表示所述无线标识发射机生成的非重复数字，其中在需要对所述设备标识符的编码进行改变的每一次，对所述非重复数字的值进行改变。

109. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；以及

第一处理器，其耦接到所述第一存储器和所述第一收发机，并且所述第一处理器被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与服务器共享的密钥，以伪随机函数，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过所述第一收发机，使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以维持所述无线标识发射机的当前时间，

并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

通过所述第二收发机，从所述无线标识发射机接收包括所述滚动标识符的所述消息；

通过所述网络设备，向所述服务器发送包括所述滚动标识符的目击消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面各项的操作：

将所述密钥与所述随机数以及用于所述无线标识发射机的所述设备标识符进行关联；

从所述邻近广播接收机接收包括所述滚动标识符的所述目击消息；

从所接收的目击消息中提取所述滚动标识符；

对所述随机数进行递增，以表示所述服务器的当前时间；

使用所述密钥、所述随机数和所述伪随机函数，对所述设备标识符进行编码，以生成服务器加密的数据；

判断所述服务器加密的数据是否与所提取的滚动标识符相匹配；以及

当所述服务器加密的数据与所提取的滚动标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

110. 根据权利要求 109 所述的系统，其中，所述伪随机函数是键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 中的一个。

111. 根据权利要求 109 所述的系统，其中，所述服务器被服务器可执行指令配置为执

行操作使得对所述随机数进行递增以表示所述服务器的当前时间，包括：基于所述目击消息中包括的信息，对所述随机数进行计算，以便与邻近广播接收机从所述无线标识发射机接收所述消息的时间相对应。

112. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；以及

第一处理器，其被耦接到所述第一存储器和所述第一收发机，并且所述第一处理器被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与所述服务器共享的第一密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数；

通过所述第一收发机，使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间，以及

并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

通过所述第二收发机，从所述无线标识发射机接收包括所述滚动标识符和所述编码的随机数的所述消息；

通过所述网络设备向所述服务器发送包括所述滚动标识符和所述编码的随机数的目击消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面各项的操作：

将用于所述无线标识发射机的所述设备标识符与初始随机数、当前随机数、与所述无线标识发射机共享的第一密钥、以及第二密钥进行关联；

使用伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

从所述邻近广播接收机接收包括所述滚动标识符和所述编码的随机数的所述目击消息；

从所接收的目击消息中提取所述编码的随机数；

从所接收的目击消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，使用所述流式加密算法、所述第一密钥、以及与所提取的编码的随机数相匹配的预先计算的编码随机数相关联的存储的随机数，对所提取的滚动标识符进行解码，以生成解码后的设备标识符；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的一个不匹配时，使用所述流式加密算法、所述第一密钥、以及与所述无线标识发射机相关联的所述初始随机数，对所提取的滚动标识符进行解码，以生成所述解码后的设备标识符；

当所述解码后的设备标识符与所述无线标识发射机的所述设备标识符相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

113. 根据权利要求 112 所述的系统，其中，所述第一密钥和所述第二密钥具有相同的值。

114. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；以及

第一处理器，其耦接到所述第一存储器和所述第一收发机，并且所述第一处理器被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与所述服务器共享的第一密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过使用伪随机函数和与所述服务器共享的第二密钥，对所述随机数进行编码，以生成编码的随机数；

通过所述第一收发机，使用短距离无线传输，来定期地广播包括所述滚动标识符和所述编码的随机数的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，以便维持所述无线标识发射机的当前时间，

并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

通过所述第二收发机，从所述无线标识发射机接收包括所述滚动标识符和所述编码的

随机数的所述消息；

通过所述网络设备，向所述服务器发送包括所述滚动标识符和所述编码的随机数的目击消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面各项的操作：

将用于所述无线标识发射机的所述设备标识符与初始随机数、当前随机数、所述第一密钥和第二密钥进行关联；

使用所述伪随机函数与所述第二密钥和所述当前随机数，预先计算多个编码的随机数；

使用所述流式加密算法与所述第一密钥、所述当前随机数和所述设备标识符，来预先计算多个编码的设备标识符；

从所述邻近广播接收机接收包括所述滚动标识符和所述编码的随机数的所述目击消息；

从所接收的目击消息中提取所述编码的随机数；

从所接收的目击消息中提取所述滚动标识符；

将所提取的编码的随机数与所述多个预先计算的编码的随机数进行比较；

当所提取的编码的随机数与所述多个预先计算的编码的随机数中的任一个相匹配时，将所提取的滚动标识符与所述多个预先计算的编码的设备标识符进行比较；

当所提取的滚动标识符与所述多个预先计算的编码的设备标识符中的任一个相匹配时，将所接收的消息的发起方识别成所述无线标识发射机。

115. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；

第一处理器，其耦接到所述第一存储器和所述第一收发机，并且所述第一处理器被处理器可执行指令配置为执行包括下面各项的操作：

对所述无线标识发射机中的随机数进行初始化；

通过所述随机数和与所述服务器共享的密钥，以流式加密算法，对与所述无线标识发射机相关联的设备标识符进行编码，来生成滚动标识符；

通过所述第一收发机，使用短距离无线传输，来定期地广播包括所述滚动标识符的消息；以及

按照预先定义的时间间隔，对所述随机数进行递增，

并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

通过所述第二收发机，从所述无线标识发射机接收包括所述滚动标识符的所述消息；

通过所述网络设备，向所述服务器发送包括所述滚动标识符的目击消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面各项的操作：

使用所述加密算法、所述密钥、初始随机数和与所述无线标识发射机相关联的所述设备标识符，生成多个初始模型有效载荷，其中所述加密算法是与所述无线标识发射机共享的；

使用所述加密算法、所述密钥、当前随机数和与所述无线标识发射机相关联的所述设备标识符，生成多个当前模型有效载荷；

从所述邻近广播接收机接收所述目击消息，其中所述目击消息包括具有模糊的标识信息的有效载荷；

将所接收的目击消息的所述有效载荷与所述多个当前模型有效载荷进行比较；

当所接收的目击消息的所述有效载荷与所述多个当前模型有效载荷中的一个相匹配时，识别所述无线标识发射机；

当所接收的目击消息的所述有效载荷与所述多个当前模型有效载荷中的任一个都不匹配时，将所接收的目击消息的所述有效载荷与所述多个初始模型有效载荷进行比较；

当所接收的目击消息的所述有效载荷与所述多个初始模型有效载荷中的一个相匹配时，识别所述无线标识发射机；以及

当所接收的消息的所述有效载荷与初始模型有效载荷和当前模型有效载荷中的至少一个相匹配时，对与所述无线标识发射机相关联的所述当前随机数进行更新。

116. 一种系统，包括：

服务器；

无线标识发射机；以及

邻近广播接收机，

其中，所述无线标识发射机包括：

第一存储器；

第一收发机，其配置为：广播能够由所述邻近广播接收机进行接收的短距离无线信号；以及

第一处理器，其耦接到所述第一存储器和所述第一收发机，并且所述第一处理器被处理器可执行指令配置为执行包括下面各项的操作：

在第一时段，使用所述第一收发机，通过短距离无线传输，来定期地广播用于指示接收输入传输的可用性的消息；

响应于所述第一时段到期，在第二时段期间，接收链路通告消息；

基于所接收的链路通告消息中的信息，与所述邻近广播接收机协商链路，其中所协商的链路是通过蓝牙配对来执行的；

对所协商的链路进行认证；以及

经由所协商的链路，来处理输入消息，

并且其中，所述邻近广播接收机包括：

第二存储器；

第二收发机，其配置为与所述无线标识发射机交换短距离无线信号；

网络设备，其配置为与所述服务器交换信号；

第二处理器，其耦接到所述第二存储器、所述第二收发机和所述网络设备，并且所述第二处理器被处理器可执行指令配置为执行包括下面各项的操作：

使用所述网络设备，从所述服务器接收消息；

接收用于指示所述无线标识发射机可用于接收所述输入传输的广播消息；

基于所接收的广播消息中指示的所述可用性，发送所述链路通告消息；

基于所述链路通告消息中的所述信息，与所述无线标识发射机协商所述链路，其中所协商的链路是经由蓝牙配对来执行的；

对所协商的链路进行认证；以及

通过所协商的链路，从所述服务器向所述无线标识发射机发送所述消息，

并且其中，所述服务器被服务器可执行指令配置为执行包括下面的操作：向所述邻近广播接收机发送所述消息。

117. 根据权利要求 116 所述的系统，其中，向所述无线标识发射机发送的所述消息包括下面各项中的至少一项：固件更新、配置信息、触发信号和软件指令。

118. 根据权利要求 116 所述的系统，其中，所述第一时段是由下面各项中的至少一项来定义的：所述无线标识发射机上的定时器、时钟信号、以及来自所述邻近广播接收机的第二消息。

119. 一种用于第一通信设备使用蓝牙在安全性提高的情况下进行通信的方法，包括：

与第二通信设备建立通信链路；

存储与所述第二通信设备共享的随机数；

通过所述通信链路，接收用于指示滚动的蓝牙机器地址的消息；

使用所述随机数和与所述第二通信设备共享的加密算法，生成所述第二通信设备的预期的蓝牙机器地址；

将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较；

当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，对所接收的消息进行处理；以及

响应于确定需要进行随机数更新，对所述随机数进行递增。

120. 根据权利要求 119 所述的方法，还包括：

当所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址不匹配时，对所述随机数改变预先定义的一组偏移值；

基于所述改变的随机数，生成新的预期的蓝牙机器地址，以便在一个时段期间，与所接收的消息中的所述滚动的蓝牙机器地址进行比较；以及

当在所述时段期间没有找到匹配时，忽略所接收的消息。

121. 一种被配置为使用蓝牙在安全性提高的情况下进行通信的第一通信设备，包括：

用于与第二通信设备建立通信链路的单元；

用于存储与所述第二通信设备共享的随机数的单元；

用于通过所述通信链路，接收用于指示滚动的蓝牙机器地址的消息的单元；

用于使用所述随机数和与所述第二通信设备共享的加密算法，生成所述第二通信设备的预期的蓝牙机器地址的单元；

用于将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较的单元；

用于当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，对所接收的消息进行处理的单元；以及

用于响应于确定需要进行随机数更新，对所述随机数进行递增的单元。

122. 根据权利要求 121 所述的第一通信设备，还包括：

用于当所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址不匹配时，对所述随机数改变预先定义的一组偏移值的单元；

用于基于所述改变的随机数，生成新的预期的蓝牙机器地址，以便在一个时段期间，与所接收的消息中的所述滚动的蓝牙机器地址进行比较的单元；以及

用于当在所述时段期间没有找到匹配时，忽略所接收的消息的单元。

123. 一种被配置为使用蓝牙在安全性提高的情况下进行通信的第一通信设备，包括：

存储器；以及

处理器，其耦接到所述存储器，其中所述处理器被处理器可执行指令配置为执行包括下面各项的操作：

与第二通信设备建立通信链路；

存储与所述第二通信设备共享的随机数；

通过所述通信链路，接收用于指示滚动的蓝牙机器地址的消息；

使用所述随机数和与所述第二通信设备共享的加密算法，生成所述第二通信设备的预期的蓝牙机器地址；

将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较；

当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，对所接收的消息进行处理；以及

响应于确定需要进行随机数更新，对所述随机数进行递增。

124. 根据权利要求 123 所述的第一通信设备，其中，所述处理器被处理器可执行指令配置为执行还包括下面各项的操作：

当所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址不匹配时，对所述随机数改变预先定义的一组偏移值；

基于所述改变的随机数，生成新的预期的蓝牙机器地址，以便在一个时段期间，与所接收的消息中的所述滚动的蓝牙机器地址进行比较；以及

当在所述时段期间没有找到匹配时，忽略所接收的消息。

125. 一种具有存储在其上的处理器可执行软件指令的非临时性处理器可读存储介质，其中所述处理器可执行软件指令被配置为使得处理器执行用于第一通信设备使用蓝牙在安全性提高的情况下进行通信的操作，所述操作包括：

与第二通信设备建立通信链路；

存储与所述第二通信设备共享的随机数；

通过所述通信链路，接收用于指示滚动的蓝牙机器地址的消息；

使用所述随机数和与所述第二通信设备共享的加密算法，生成所述第二通信设备的预期的蓝牙机器地址；

将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较；

当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，对所接收的消息进行处理；以及

响应于确定需要进行随机数更新，对所述随机数进行递增。

126. 根据权利要求 125 所述的非临时性处理器可读存储介质，其中，所述处理器可执行软件指令执行的操作还包括下面各项：

当所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址不匹配时，对所述随机数改变预先定义的一组偏移值；

基于所述改变的随机数，生成新的预期的蓝牙机器地址，以便在一个时段期间，与所接收的消息的所述滚动的蓝牙机器地址进行比较；以及

当在所述时段期间没有找到匹配时，忽略所接收的消息。

127. 一种用于使用蓝牙在安全性提高的情况下进行通信的方法，包括：

在第一通信设备中，与第二通信设备建立通信链路；

存储与所述第二通信设备共享的随机数；

使用所述随机数和与所述第一通信设备共享的加密算法，在所述第二通信设备中生成滚动的蓝牙机器地址；

使用所述滚动的蓝牙机器地址，从所述第二通信设备向所述第一通信设备发送消息；

通过所述通信链路，在所述第一通信设备中接收用于指示所述滚动的蓝牙机器地址的所述消息；

使用所述随机数和与所述第二通信设备共享的所述加密算法，在所述第一通信设备中生成所述第二通信设备的预期的蓝牙机器地址；

将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较；

当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，在所述第一通信设备中对所接收的消息进行处理；以及

响应于确定需要进行随机数更新，对所述随机数进行递增。

128. 一种系统，包括：

第一通信设备，以及

第二通信设备，

其中，所述第一通信设备包括：

第一存储器；以及

第一收发机，其配置为广播能够由所述第二通信设备进行接收的短距离无线信号，并被处理器可执行指令配置为执行包括下面各项的操作：

与所述第二通信设备建立通信链路；

存储与所述第二通信设备共享的随机数；

通过所述通信链路，接收用于指示滚动的蓝牙机器地址的消息；

使用所述随机数和与所述第二通信设备共享的加密算法，生成所述第二通信设备的预期的蓝牙机器地址；

将所接收的消息中的所述滚动的蓝牙机器地址与所述预期的蓝牙机器地址进行比较；

当所接收的消息中的所述滚动的蓝牙机器地址与所述第一通信设备生成的所述预期的蓝牙机器地址相匹配时，对所接收的消息进行处理；以及

响应于确定需要进行随机数更新，对所述随机数进行递增，并且其中，所述第一通信设备包括：

第二存储器；以及

第二收发机，其配置为广播能够由所述第一通信设备进行接收的短距离无线信号，并被处理器可执行指令配置为执行包括下面各项的操作：

与所述第一通信设备建立所述通信链路；

存储与所述第一通信设备共享的所述随机数；

使用所述随机数和与所述第一通信设备共享的所述加密算法，生成所述滚动的蓝牙机器地址；

使用所述滚动的蓝牙机器地址，向所述第一通信设备发送所述消息；

通过所述通信链路，从所述第二通信设备接收输入消息；以及

响应于确定需要进行随机数更新，对所述随机数进行递增。

# 用于使设备标识符变模糊的方法和设备

[0001] 相关申请

[0002] 本申请要求享受以下美国临时申请的优先权：

[0003] 2012 年 2 月 22 日提交的美国临时申请 No.61/601,620(113445P1)，

[0004] 2012 年 4 月 24 日提交的美国临时申请 No.61/637,834(113445P2)，

[0005] 2012 年 8 月 24 日提交的美国临时申请 No.61/693,169(113445P3)，

[0006] 2012 年 7 月 11 日提交的美国临时申请 No.61/670,226(122183P1)，

[0007] 2012 年 9 月 14 日提交的美国临时申请 No.61/701,457(124489P1)，

[0008] 2012 年 10 月 12 日提交的美国临时申请 No.61/713,239(124489P2)，

[0009] 2012 年 10 月 19 日提交的美国临时申请 No.61/716,373(124460P1)，

[0010] 2012 年 10 月 24 日提交的美国临时申请 No.61/717,964(124642P1)，

[0011] 2012 年 11 月 20 日提交的美国临时申请 No.61/728,677(124614P1)，

[0012] 2012 年 12 月 21 日提交的美国临时申请 No.61/745,395(122183P2)，

[0013] 2012 年 12 月 21 日提交的美国临时申请 No.61/745,308(113445P4)，

[0014] 故以引用方式将所有这些申请的全部内容并入本文。

[0015] 此外，本申请还涉及与本申请同时提交的、题目为“Platform for Wireless Identity Transmitter and System Using Short-Range Wireless Broadcasts”的美国专利申请 No.__/___,___(律师案卷号为 No.113445)，故以引用方式将其全部内容并入本文。

## 背景技术

[0016] 最近几年，蜂窝和无线通信设备已经飞速增长。更好的通信硬件、更大的网络和更可靠的协议，推动了这种增长。如今的智能电话包括相机、GPS 接收机、蓝牙®收发机，当然，蜂窝通信能力（例如，LTE、3G 和 / 或 4G 网络接入）使设备能够与互联网建立数据通信链路。智能电话在当今社会已非常普及。另外，智能电话中的组件和能力现在一般人都能负担得起，这使得这些能力可部署在其它类型的设备中。

[0017] 已经提出了众多解决方案，以便有助于利用蜂窝设备和无线设备的人员或资产的定位。这些系统中的大部分涉及开发可穿戴设备，所述可穿戴设备向服务器传输该可穿戴设备的位置。其它方面涉及在可穿戴设备和蜂窝设备之间建立无线连接。这些系统有成本、有效性和实用性的问题，这些问题会限制它们的可行性。此外，非故意的各方可以对发送用于指示用户身份或其它唯一信息的无线信息的方案进行跟踪，造成安全问题。例如，恶意方可以例如通过使用分组嗅探器来捕获包括用户身份的无线消息，并可以通过对以明文发送的数据进行分析，以确定这些消息的来源。

## 发明内容

[0018] 各个实施例提供了用于基于广播标识分组来定位无线标识发射机的系统、设备和方法，其中以滚动方式对这些广播标识分组进行编码、加密或者以其它方式模糊，以便提供一定级别的安全性和匿名性。无线标识发射机可以是被配置为使用诸如蓝牙®低功耗

(LE) 之类的短距离无线信令技术，来广播唯一的和安全的识别码的紧凑设备。这些标识广播分组（“广播消息”）可以被在物理上位于附近的邻近广播接收机 (PBR) 进行接收，其中 PBR 可以是专用接收机、配置有 PBR 应用的智能电话、配置有 PBR 应用的平板计算机和静止接收机，这里仅仅举出几个例子。由于无线标识发射机使用短距离无线信号来广播其标识符，因此当邻近广播接收机接收到广播消息（以及所包括的标识符）时，该邻近广播接收机自己的位置可以向该无线标识发射机提供大致位置。使用远距离无线网络和 / 或互联网，邻近广播接收机可以将所接收的标识符连同其它相关联信息（例如，时间和位置）作为目击消息向中央服务器进行发送或者上传。这形成了中央服务器上的记录的目击的数据库，其中该数据库可以呈现无线标识发射机的历史信息和主动更新的位置（或者邻近性）信息。

[0019] 为了保护隐私和防止特定无线标识发射机的未授权跟踪，可以以中央服务器已知但未被授权的系统难以预测的方式，对广播消息中的标识符进行定期地改变（或者“滚动”）。在一个实施例中，无线标识发射机可以在该发射机和中央服务器之间，对随机数或计数器进行同步，以使得能够向中央服务器广播模糊的标识信息。可以对广播消息中的有效载荷数据进行加密或者随机化以防止被非故意拦截，并被中央服务器接收以进行处理。无线标识发射机可以使用仅仅只有该无线标识发射机和中央服务器才知道的密钥和函数，对标识信息和时钟、随机数或计数器信息进行加密。通过在中央服务器和无线标识发射机之间维持松散同步的随机数或计数器，中央服务器可以基于接收的消息，生成预期的来自该无线标识发射机的消息内容，并进行比较。如果中央服务器在存储的信息和接收的消息数据之间发现了匹配，则中央服务器可以推断对所接收的消息进行广播的无线标识发射机的标识。替代地，中央服务器可以使用存储的密钥、设备标识、以及随机数或计数器信息，与伪随机函数来生成数据，并与接收的消息进行比较。中央服务器可以避免用于对接收消息的无线标识发射机进行识别的蛮力比较。

[0020] 附近的邻近广播接收机可以记录接收的广播消息，并可以定期地发送目击消息。通过利用邻近广播接收机（例如，智能电话、静止接收机等等），将所接收的广播消息与当前时间和位置进行关联的能力，中央服务器可以维持针对无线标识发射机的位置踪迹（类似于面包屑的痕迹），其可以用于定位或者缩小对特定设备的搜索。通过对该标识符进行模糊（在一些实施例中，其包括对蓝牙标识符进行模糊或者随机化），可以防止未被授权的实体跟踪这些无线标识发射机。

[0021] 在一些实施例中，无线标识发射机可以与邻近广播接收机和服务器进行单向通信，按照定期的时间间隔来广播消息，并且不接受响应消息，或者替代地从附近的设备接收配置设置。

## 附图说明

[0022] 并入本申请并且构成本说明书一部分的附图，描绘了本发明的示例性实施例，连同上面给出的概括描述以及下面给出的详细描述一起用于解释本发明的特征。

[0023] 图 1 是描绘适合在各种实施例中使用的网络组件的系统图。

[0024] 图 2 是描绘适合在各种实施例中使用的实施例架构的网络组件的通信系统图。

[0025] 图 3 是描绘用于从无线标识发射机广播标识符的实施例方法的处理流程图。

[0026] 图 4A 是描绘用于在执行启动操作之后进行无线标识发射机接收配置设置的实施例方法的处理流程图。

[0027] 图 4B 是描绘用于在执行启动操作之后，无线标识发射机接收配置设置，并且基于该配置设置来广播消息的实施例方法的处理流程图。

[0028] 图 5 是描绘用于无线标识发射机与邻近广播接收机执行双向无线通信的实施例方法的处理流程图。

[0029] 图 6 是描绘适合于在各种实施例中使用的移动的邻近广播接收机中的各种模块的组件图。

[0030] 图 7A- 图 7B 是描绘移动的邻近广播接收机将无线标识发射机的标识符连同其它数据（例如，时间或位置）进行中继的实施例方法的处理流程图。

[0031] 图 8 是根据各个实施例，用于响应于针对无线标识发射机的位置的用户请求的呼叫流程图。

[0032] 图 9 是描绘响应于第二段的实施例方法的处理流程图，所述第二段指示应当如何对来自无线设备的消息进行处理。

[0033] 图 10 是描绘基于与无线标识发射机的邻近性，响应于发送目击消息 (sighting message)，从中央服务器接收指令的实施例方法的处理流程图。

[0034] 图 11 是描绘移动的邻近广播接收机对针对特定无线标识发射机的警报进行响应的实施例方法的处理流程图。

[0035] 图 12 是根据各个实施例，用于通过发送警报，对针对无线标识发射机的位置的用户请求进行响应的呼叫流程图。

[0036] 图 13 是描绘适合于在各个实施例中使用的中央服务器里的各种模块的组件图。

[0037] 图 14 是描绘在各种实施例中使用的无线标识发射机注册过程的图。

[0038] 图 15A 和图 15B 是描绘用于中央服务器对从邻近广播接收机接收到的目击消息进行处理的实施例方法的处理流程图。

[0039] 图 16 是根据各个实施例，描绘无线标识发射机、邻近广播接收机和中央服务器之间的通信的呼叫流程图。

[0040] 图 17 是描绘用于响应于针对无线标识发射机的位置的用户请求，向位于所识别的扇区中的移动的邻近广播接收机发送警报的实施例方法的处理流程图。

[0041] 图 18 是描绘用于中央服务器判断邻近广播接收机是否已经丢失了无线标识发射机的实施例方法的处理流程图。

[0042] 图 19 是描绘用于服务器处理滚动标识符的实施例方法的处理流程图。

[0043] 图 20 是描绘由无线标识发射机和中央服务器对使用加密算法加密的滚动标识符进行发送和处理的实施例操作的处理流程图。

[0044] 图 21A 是描绘用于无线标识发射机使用加密算法来生成和广播滚动标识符有效载荷的实施例方法的处理流程图。

[0045] 图 21B 是描绘用于中央服务器使用加密算法来接收和处理滚动标识符有效载荷的实施例方法的处理流程图。

[0046] 图 22 是描绘无线标识发射机和中央服务器使用伪随机函数来发送和处理滚动标识符的实施例操作的处理流程图。

[0047] 图 23A 是描绘用于无线标识发射机使用伪随机函数来生成和广播滚动标识符有效载荷的实施例方法的处理流程图。

[0048] 图 23B 是描绘用于中央服务器使用伪随机函数来接收和处理滚动标识符有效载荷的实施例方法的处理流程图。

[0049] 图 24A 是描绘用于无线标识发射机生成和广播具有滚动标识符和编码的随机数或计数器的消息的实施例方法的处理流程图。

[0050] 图 24B- 图 24C 是描绘用于中央服务器对包括滚动标识符和编码的随机数或计数器的消息进行接收和处理的实施例方法的处理流程图。

[0051] 图 25A 是用于无线标识发射机通过协商的通信链路，与邻近广播接收机执行双向无线通信的实施例方法的处理流程图。

[0052] 图 25B 是用于邻近广播接收机通过协商的通信链路，向可用的无线标识发射机发送消息的实施例方法的处理流程图。

[0053] 图 25C 是用于无线标识发射机使用滚动的蓝牙 MAC 地址来发送消息，同时与移动设备进行配对的实施例方法 2570。

[0054] 图 25D 描绘了用于移动设备（例如，智能电话）使用滚动的蓝牙 MAC 地址，对从无线标识发射机接收的消息进行处理的实施例方法 2580。

[0055] 图 26A- 图 26B 是根据各种实施例的无线标识发射机的组件框图。

[0056] 图 27A- 图 27B 是根据各种实施例的邻近广播接收机的组件框图。

[0057] 图 28 是根据另外的实施例，来描绘包括标识信息的消息的消息格式图。

[0058] 图 29 是适合于在各种实施例中使用的移动设备的组件框图。

[0059] 图 30 是适合于在各种实施例中使用的服务器设备的组件框图。

## 具体实施方式

[0060] 现在参照附图来详细地描述各个实施例。只要有可能，在整个附图中使用相同的附图标记来指代相同或者类似的部件。对于特定示例和实现的提及只是用于说明目的，而不是旨在限制本发明或者权利要求的保护范围。

[0061] 本申请所使用的“示例性”一词意味着“用作例子、例证或说明”。本申请中描述为“示例性”的任何实现不一定被解释为比其它实现更优选或更具优势。

[0062] 本申请所使用的术语“移动设备”指代蜂窝电话、智能电话（例如，iPhone®）、连网板 (web-pad)、平板计算机、启用互联网的蜂窝电话、启用 WiFi 的电子设备、个人数据助理 (PDA)、膝上型计算机、个人计算机、以及配备有短距离无线电（例如，蓝牙®无线电、Peanut®无线电、WiFi 无线电等）的类似电子设备和广域网连接（例如，LTE、3G 或 4G 无线广域网收发机、或者与互联网的有线连接）。对特定类型的计算设备（如移动设备）的提及，并不旨在限制权利要求的保护范围，除非在权利要求中陈述了特定类型的移动设备。

[0063] 本申请所使用的术语“广播消息”指代无线标识发射机（下文定义）所广播的短距离无线广播信号，所述短距离无线广播信号可以包括与无线标识发射机和 / 或它们的用户相关联的标识信息（例如，标识符）。可以对这些标识符进行定期地改变和加密（即，滚动标识符）。在各个实施例中，广播消息可以包括其它识别信息，例如，蓝牙® MAC 地址和

计数器，它们也能够被加密。另外，广播消息可以包括元数据和其它数据，例如，进行发送的无线标识发射机的特性（例如，设备类型）、传感器数据和/或命令或其它指令。在各个实施例中，可以通过诸如蓝牙低功耗、WiFi、WiFi Direct、Zigbee®、Peanut®之类的无线通信协议和其它 RF 协议，来发送广播消息。在各个实施例中，由于某些短距离传输信道的高度不可靠性，广播消息可以是限于某个大小（例如，80 比特、10 个字节、20 个字节等）的单个分组传输。例如，实施例广播消息的有效载荷可以是总共 80 个比特，其包括指示电池状态信息的 4 比特和指示滚动标识符的 76 比特。再举一个例子，实施例广播消息可以包括表示随机数或者计数器的 20 比特和表示滚动标识符（例如，使用伪随机函数或者加密算法所生成）的 60 比特。

[0064] 本申请所使用的术语“无线标识发射机”指代被配置为定期地通过短距离无线发射机来发送广播消息的紧凑设备。无线标识发射机可以是移动的（例如，当携带到或者固定到移动的人或物时），或者替代地可以是静止的（例如，当安装在建筑物之中时）。无线标识发射机可以存储唯一的设备标识符（即，“设备 ID”）（例如，出厂 ID）并与该设备标识符相关联。在一个实施例中，该唯一设备标识符可以是长度 56 比特的代码。在各个实施例中，为了安全目的，当将唯一设备标识符连同其它数据（例如，随机数或计数器值）包括在广播消息之中作为“滚动标识符”时，可以对它们进行编码、加密或者以其它方式变模糊。无线标识发射机可以被配置为维持不准确的时间（例如，UTC）信息，例如通过将 30ppm 16kHz 晶体振荡器用作时钟。在整个本申请中描述了无线标识发射机，特别是参照图 26A- 图 26E 进行了描述。在本申请的各个附图和图形中，无线标识发射机可以被称为“WIT”或“WITs”。

[0065] 本申请所使用的术语“邻近广播接收机”指的是：被配置为接收例如由无线标识发射机发送的广播消息。在各个实施例中，邻近广播接收机可以是遍及整个场所（例如，建筑物、零售商店等）永久定位的静止设备（或者“静止的邻近广播接收机”），或者可以是被配置为作为邻近广播接收机（或者“移动的邻近广播接收机”）进行操作的移动设备。例如，智能电话可以被配置为接收广播消息，并作为移动的邻近广播接收机进行操作。将特定类型的计算设备称为邻近广播接收机，并不旨在限制权利要求的保护范围，除非在权利要求中记载了特定类型的设备。此外，除非另外指出，否则贯穿本申请对邻近广播接收机的提及，并不旨在将任何方法或系统限于特定类型的邻近广播接收机设备（例如，无线或静止）。贯穿本申请描述了邻近广播接收机，特别是参照图 27A- 图 27B 进行了描述。在本申请的各个附图和图形中，邻近广播接收机可以被称为“PBR”或“PBRs”，在附图中将移动的邻近广播接收机称为“MPBR”或“MPBRs”。

[0066] 本申请所使用的术语“标识收发机”和“无线标识收发机”指的是：被配置为接收和发送广播消息的设备。换言之，标识收发机可以用作邻近广播接收机和标识发射机二者。例如，智能电话可以被配置为：广播包括其唯一标识符的短距离信号，以及从附近的无线标识发射机接收广播消息。在整个本申请中，可以将各种操作描述成明显由无线标识发射机或者邻近广播接收机来执行，但是，本领域普通技术人员应当理解的是，被配置为作为标识收发机进行操作的设备可以被配置为执行相同操作中的任何或全部操作，因此，可以参照无线标识发射机或邻近广播接收机进行互换。

[0067] 本申请所使用的术语“目击消息”指代：响应于从无线标识发射机接收到广播消息，由邻近广播接收机向中央服务器发送的报告、信号和/或消息。目击消息可以是包括在

所接收的广播消息中的编码信息的一部分或全部的传输，其包括任何模糊或加密的信息，例如，无线标识发射机的标识符。另外，目击消息可以包括元数据和其它信息（或者“相关联的数据”），例如，进行发送的邻近广播接收机的标识信息（例如，设备 ID、第三方关系等）、邻近广播接收机是否与无线标识发射机配对、传输上下文信息（例如，指示该目击消息与警报或者注册的服务有关的代码）、与在邻近广播接收机上运行的软件或者应用有关的信息（例如，应用 ID）、位置信息、与场所中的已知区域有关的邻近性信息、以及时间戳数据。在一个实施例中，目击消息还可以包括认证信息（例如，密钥、许可证、特殊代码、数字证书等），中央服务器可以使用该认证信息来确认发送该目击消息的邻近广播接收机的标识（或者标识信息）。例如，目击消息可以包括来自哈希函数的代码，中央服务器可以对该代码进行解码以确保进行发送的邻近广播接收机与一个特定的注册服务相关联。在各个实施例中，可以在接收到广播（例如，当涉及警报时）之后，立即发送目击消息，对目击消息进行缓存、或者连同其它调度的传输一起调度。

[0068] 各种实施例提供了用于经由编码、加密或者其它方式进行模糊的标识符的短距离无线广播，来定位或跟踪无线标识发射机的方法、设备和系统。包括加密标识符的广播，可以由能够与一个或多个中央服务器进行通信的邻近广播接收机的网络（例如，蜂窝电话、移动设备或者静止的邻近广播接收机）进行接收。在各个实施例中，无线标识发射机可以是被配置为发送具有识别码的分组的紧凑设备，该识别码具有位于短距离无线广播的范围之内的任何邻近广播接收机能够接收的格式。由于无线标识发射机依赖于短距离无线信令（例如，诸如蓝牙低能量分组、光信号、声信号等短距离无线信号）来发送包括其标识符的广播消息，因此只有位于附近的邻近广播接收机才可以接收这些广播消息。因此，邻近广播接收机自己的位置可以提供该无线标识发射机在广播消息的接收时的大致位置。从无线标识发射机接收广播消息的每个邻近广播接收机，可以向中央服务器传送包括加密的无线标识发射机标识符的目击消息以进行处理。中央服务器可以对接收的目击消息中的经加密或模糊的信息（其包括滚动标识符）进行解码。

[0069] 在各个实施例中，无线标识发射机可以被配置为：通过难以对发射机进行跟踪的方式来定期地改变对设备标识符进行编码 / 加密的方式，或者改变该标识符本身（本文中被称为“滚动标识符”），同时使中央服务器能够对该无线标识发射机的唯一设备标识符（和其它识别信息）进行解码、解密或者以其它发送进行识别。例如，无线标识发射机可以被配置为：定期地广播包括该无线标识发射机的设备标识符（即，设备 ID）的编码版本的蓝牙分组。可能需要在广播消息中指示标识符的这种加密，以使中央服务器能可靠地识别广播消息的发起方无线标识发射机，同时强制第三方（例如，被动攻击者）只能通过猜测来确定该广播消息的来源。例如，如果标识符是静止的，则第三方可以对该标识符进行嗅探（例如，通过冒充邻近的广播接收机），随后使用该标识符来跟踪该无线标识发射机。如果第三方不知道用于生成加密的标识符的方式，则滚动标识符可以使得这种攻击是不可能的。

[0070] 由于单个分组广播消息不能够支持可以适应传统的非对称密钥加密的密文的有效载荷，因此在各个实施例中，标准的私 / 公钥对加密可能是不可用的。另外，无线标识发射机通常是只广播的设备，所以不存在传统的加密方案中通常需要的返回信道。因此，在各个实施例中，中央服务器可以通过预先设定对各个无线标识发射机来说唯一的共享密钥，来处理加密的消息有效载荷。在中央服务器处，这些密钥可以与各个无线标识发射机的唯

一设备标识符相关联，并可以用于对每个无线标识发射机所编码的数据（例如，标识符）进行解码。

[0071] 执行一种实施例方法，无线标识发射机可以使用流式加密算法（例如，AES-CTR）来加密其设备标识符、共享的密钥、以及随机数或计数器，在所述随机数或计数器为明文的情况下，广播包括加密数据的有效载荷。执行另一种实施例方法，无线标识发射机可以使用伪随机函数来加密设备标识符、共享的密钥、以及随机数或计数器，在所述随机数或计数器不为明文的情况下，广播包括加密数据的有效载荷。执行另一种实施例方法，无线标识发射机可以使用流式加密和伪随机函数加密的组合来生成要广播的有效载荷。在一个实施例中，无线标识发射机和中央服务器均可以具有用于在共同的时间尺度上生成标识符的密码安全伪随机数发生器或算法，使得在任何给定时刻，中央服务器都可以计算由特定的无线标识发射机所发送的标识符。

[0072] 在各个实施例中，无线标识发射机可以维持用于定期地递增随机数或计数器（或时钟数据），所述随机数或计数器（或时钟数据）表示经过的时间并且可以在各种加密方法中使用。当无线标识发射机上电时（或更换电池时），可以将该随机数或计数器设置为已知的初始值（例如，0）。随着无线标识发射机工作，该随机数或计数器可以定期地递增（例如，每隔几秒 / 分钟 / 小时进行一次递增）。如果无线标识发射机遇到不一致的功率（例如，电池被取出或更换），则可以对随机数或计数器进行重置。使用这种随机数或计数器，无线标识发射机可以被配置为：定期地广播具有加密的有效载荷的广播消息，所述加密的有效载荷包括变化的和加密的设备标识。在一个实施例中，加密的有效载荷可以包含设备的唯一标识符（即，设备 ID）和用于该无线标识发射机的当前随机数或计数器值的串接。在一个实施例中，无线标识发射机可以使用密钥，对串接的数据进行加密。按照变化的频率来广播有效载荷，邻近广播接收机或中央服务器可以接收该有效载荷以进行处理。

[0073] 在一个实施例中，中央服务器可以被配置为：通过将所接收的加密的有效载荷与对应于注册的无线标识发射机的预生成有效载荷（或者模型有效载荷）进行匹配，来识别无线标识发射机。基于在中央服务器与无线标识发射机之间的注册操作期间获得的信息，中央服务器可以存储关于每个无线标识发射机的唯一信息。例如，中央服务器可以基于注册通信，知道密钥、设备标识符（或设备 ID）、以及无线标识发射机的初始随机数或计数器值。使用这种存储的信息，中央服务器可以生成预期（或者很有可能）该无线标识发射机在一个时间段（例如，24 小时的时段）之内进行广播的一系列模型有效载荷。如果中央服务器接收到与这些模型有效载荷中的任何一个相匹配的有效载荷，则中央服务器可以确定起源的无线标识发射机的身份、以及该无线标识发射机中的松散准确的随机数或计数器值。可以基于每个注册的无线标识发射机的当前同步的随机数或计数器，来生成模型有效载荷（即，当前模型有效载荷）。在一个实施例中，中央服务器还可以通过保持模型有效载荷的窗，对无线标识发射机时钟歪斜（skew）进行调整。例如，中央服务器可以使用表示在期望的随机数或计数器之前和之后的时间的随机数或计数器值，来生成有效载荷。中央服务器还可以通过监测所接收的有效载荷随时间的变化，来确定无线标识发射机时钟的周期。在一个实施例中，中央服务器可以跟踪无线标识发射机的报告的随机数或计数器值的变化，并且可以报告针对一个特定的时间段来说，设备时钟如何不准确。

[0074] 还可以基于每个注册的无线标识发射机在注册操作期间所报告的初始随机数或

计数器值，来生成模型有效载荷（即，初始模型有效载荷）。当无线标识发射机断电并再次上电（例如，休息、更换电池等）时，无线标识发射机可以重置到原始的或者初始的随机数或计数器值。如果在中央服务器处接收的加密的有效载荷与任何当前模型有效载荷都不匹配，则中央服务器可以将所接收的加密的有效载荷与所存储的初始模型有效载荷进行比较。当中央服务器发现初始模型有效载荷与所接收的加密的有效载荷相匹配时（例如，无线标识发射机被重置时），中央服务器可以更新数据库，以指示相应的无线标识发射机的随机数或计数器被重置，因此与重置的无线标识发射机的时钟进行重新同步。

[0075] 在无线标识发射机暂停一段时间，但没有对其用于生成加密的有效载荷的随机数或计数器进行重置的情形下，无线标识发射机后续生成的有效载荷可能与中央服务器中存储的预期的有效载荷不匹配（例如，当前模型有效载荷和初始模型有效载荷）。为了处理这种情形，当模型有效载荷和 / 或随机数或计数器值与所接收的加密的有效载荷不匹配时，中央服务器可以确定发生了暂停。中央服务器可以通过对数据库中表示的所有已知的和 / 或注册的无线标识发射机执行强力搜索，来识别该无线标识发射机，并基于记录的密钥和设备标识，来对所接收的加密的有效载荷进行解码。在一个实施例中，强力搜索可以只包括不具有中央服务器最近接收的广播有效载荷的无线标识发射机。

[0076] 为了本申请的说明目的，描述了用于解码、解密和以其它方式访问模糊的标识信息（例如，滚动标识符）的各种实施例方法，如中央服务器执行的用于将该信息与注册用户和 / 或注册设备进行关联。但是，本领域普通技术人员应当理解，具有授权的任何计算设备都可以被配置为执行这些操作，以解密无线标识发射机所广播的模糊的标识信息。例如，用户所采用的移动的邻近广播接收机（例如，智能电话），可以使用用于对滚动标识符进行解密、解码和以其它发送访问的各种方法，这些滚动标识符与该用户还拥有的无线标识发射机相关联。

[0077] 额外预防也是很重要的，以便防止安全漏洞，例如防止黑客攻击与中央服务器相关联的数据库，以及让注册用户（例如，商家、父母、儿童等等）安心和有信心：可以完全保护他们的隐私。可以通过下面方式，向在实施例系统中注册的参与方提供这种隐私保护：与涉及跟踪设备有关的其它信息和 / 或用户的邻近信息分开存储识别信息（例如，名称、地址、财务信息、医疗信息等等）。具体而言，为了避免注册的商家、客户、儿童或个人的个人信息的无意泄漏，实施例系统可以使用“双盲”架构。例如，这种双盲架构可以使用第一单元（例如，服务器、数据库或其它计算集线器），所述第一单元存储和访问与该邻近信息有关的信息或者注册用户的设备（例如，无线标识发射机、邻近广播接收机、标识收发机、移动设备等）的其它基于位置的数据。换言之，第一单元可以访问与目击消息相关联的信息，其中所述目击消息指示各个用户的设备的大致位置 / 邻近性。但是，第一单元可以不存储唯一标识的个人信息（例如，用户名称、地址和 / 或社会安全号码）。相反，第二单元可以存储该标识的个人信息，而无需被配置为访问如第一单元所使用的任何位置 / 邻近信息。第一单元和第二单元可以使用对在这两个单元中存储的数据进行连接的匿名标识符，而无需表明受保护的信息存储在哪个单元中。在一个实施例中，第一单元和第二单元可以由不同的实体（例如，服务提供商）进行维护，另外，提供识别信息的注册用户可以信任这些实体中的至少一个实体。

[0078] 在另外的实施例中，无线标识发射机可以被配置为：从邻近广播接收机接收输入

的传输。输入的传输可以包括固件更新或升级、软件指令、配置信息和其它数据，以便调整这些无线标识发射机的行为。无线标识发射机可以被配置为（或被调度为）：基于时钟信号、用户输入数据（例如，按键按下）或者接收的信号，来选择性地接收输入的传输。例如，从邻近广播接收机接收的触发信号，可以指示无线标识发射机激活其接收机以便接收后续的消息。具体而言，无线标识发射机可以被配置为从邻近的设备（例如，被配置为发送配置设置值的邻近广播接收机）接收配置设置。这些配置设置可以设置变化的频繁程度和 / 或无线标识发射机广播的发射功率标识符的参数。

[0079] 各个实施例利用已经到位的移动设备的大型基础设施。很多现代移动设备（例如，智能电话）已经配备有多个无线装置（其包括诸如蓝牙®无线装置之类的短距离无线装置），因此，这些现代移动设备可以被配置为与邻近广播接收机一样执行操作，从邻近的无线标识发射机接收识别码。通常，移动设备都配备有可以提供当前时间的时钟，以及（每当接收到无线标识发射机标识符）可以提供当前位置的 GPS 接收机。移动设备可以通过远距离网络连接（例如，蜂窝无线连接），经由目击消息向中央服务器传输这些识别码、时间和位置。因此，已经在使用或者即将被使用的大量移动设备中的很多移动设备可以被纳入成移动的邻近广播接收机，以便扩展各个实施例系统所能到达的范围。

[0080] 通过依赖远距离无线装置和邻近广播接收机的其它服务，来向中央服务器报告所接收的广播消息（或者“目击”）的位置和时间，无线标识发射机可以是相对较小、低廉和简单的设备（包括稍大于一个短距离无线装置（例如，蓝牙® LE 收发机））、以及电池。在各个实施例中，无线标识发射机还可以包括额外的短距离无线装置（例如，Peanut®无线装置）。在各个实施例中，无线标识发射机可以不包括用户接口、多个无线装置、全球定位系统 (GPS) 接收机、或者在移动设备上常见的其它特征。实施例无线标识发射机可能还消耗极少的电量，这允许它们能够在无需被频繁地充电或更换的情况下进行部署。这些特性使他们能理想地用于多种用途、以及在各种物理配置下实现。例如，可以容易地隐藏无线标识发射机，或者将其纳入到诸如纽扣、手表、鞋、公文包、背包、ID 徽章、衣服、产品包装之类的很多不同的个人物品之中。

[0081] 实施例方法、设备和系统可以用于多种目的。例如，各种实施例可以用于跟踪失踪的儿童、精神病人、宠物、老年痴呆症患者、自然灾害的受害者和试图营救他们的第一响应者等等。另外的实施例可以安装在高价值财物上，以便在物流系统中对该财物进行跟踪、监测边界区域运输（例如，进入 / 离开建筑工地）、以及跟踪该财物是否曾经被偷窃或者被报告丢失。实施例还可以用于对进入和离开控制区域的人员进行监测。各个实施例可以辅助或者补充安柏警戒系统，或者向警察提供信息。实施例还可以向私人或企业实体提供有价值的信息。

[0082] 无线标识发射机还可以用于传输信息（例如，传感器数据）或者提示邻近广播接收机采取特定的动作。在一些实施例中，无线标识发射机可以发送广播消息，所述广播消息指示要由邻近广播接收机（例如，蜂窝电话）执行的一个或多个行为，在该情况下，所述广播消息还可以包括与命令（即，命令标识符）或者该无线标识发射机的类型（即，设备类型标识符或设备类型信息）相对应的辅助段。接收该广播消息的邻近广播接收机可以基于识别码或者辅助码来采取动作。替代地，邻近广播接收机可以向中央服务器发送所接收的广

播消息，所述中央服务器可以向邻近广播接收机返回指令或者另一个编码以指示要执行的行为。

[0083] 在另外的实施例中，可以使用无线标识发射机来跟踪物品并指示资产何时离开或者进入邻近广播接收机的接收范围（或者其附近）。例如，可以在用户携带的邻近广播接收机周边建立个人地理围栏，使得当相关联的无线标识发射机离开或者进入该邻近广播接收机的接收范围内时，可以发送警报或者提醒消息。无线标识发射机邻近度的这种指示可以表现得像限制带，其可以用于跟踪儿童、箱包、钱包或手提包、停车场中的汽车等。在另一个实施例中，可以基于确定附近的邻近广播接收机和／或输入数据来确认跟踪的物品何时从邻近广播接收机的接收范围离开，从而在中央服务器中确定和记录无线标识发射机的监护链条。

[0084] 在另外的实施例中，无线标识发射机和邻近广播接收机可以被配置为使用诸如LTE-D、对等 LTE-D、WiFi 和 WiFi Direct 之类的各种无线技术来交换传输。在一个实施例中，无线标识发射机可以被配置为通过 WiFi 无线装置来广播消息，使得具有 WiFi 收发机的邻近广播接收机可以接收广播消息。在这些实施例中，无线标识发射机可以类似于 WiFi 接入点广播通告，使用 WiFi 传输来广播标识信息。例如，包括 WiFi 无线装置的无线标识发射机可以被配置为：通过具有低功耗的 WiFi 传输来发送广播消息，这样，接收范围是有限的，从而提供具有与蓝牙 LTE 传输相类似的距离的短距离无线信号。在针对无线标识发射机使用各种无线广播技术和通信协议时，具有有限能力的邻近广播接收机可能仍然能够对来自无线标识发射机的广播消息进行接收和处理。例如，被配置为操作成移动的邻近广播接收机、并包括 WiFi 收发机但不包括蓝牙 LE 无线装置的智能电话，可以对来自无线标识发射机的广播消息进行接收和处理，其中该无线标识发射机被配置为使用 WiFi 无线装置来广播短距离信号。在一个实施例中，无线标识发射机可以通过多个无线装置（例如，蓝牙 LE 收发机和低功耗 WiFi 收发机）进行广播，以便使更多模型的邻近广播接收机（例如，更多类型的智能电话）能够对目击消息进行接收和中继。

[0085] 在其它实施例中，无线标识发射机可以包括生成传感器数据的传感器，可以在广播消息中对所述传感器数据进行编码。这种传感器数据可以包括麦克风、相机、压力传感器、热传感器、加速计、湿度传感器、温度传感器、CO2 传感器等。邻近广播接收机可以使用或存储来自这些传感器的数据，或者中央服务器通过来自邻近广播接收机的目击消息来接收数据。

[0086] 各种实施例方法可以基于短距离无线广播消息的接收，来确定无线标识发射机位于邻近广播接收机的附近范围之内，反之亦然。此外，实施例可能不需要确定无线标识发射机和／或邻近广播接收机的确切位置，而是可以确定这些设备彼此之间的大致位置和／或相对位置。因此，在整个本申请中对确定位置和／或距离的提及，可以是用于确定信令设备之间的邻近度。

[0087] 在各个实施例中，公司、组织和机构（例如，学校、商店、公园、机场、购物商场、办公大厦等）可以部署静止的邻近广播接收机来接收和中继来自用户的无线标识发射机的广播消息。或者，一些场所可以部署静止的无线标识发射机，用户的移动的邻近广播接收机可以接收和中继广播消息。在另外的实施例中，一些场所可以使用邻近广播接收机和无线标识发射机，对来自携带无线标识发射机和／或移动的邻近广播接收机的用户的数据进行

接收、中继和处理。无论广播消息的来源是什么，中央服务器（或者本地计算设备）可以基于接收的目击消息，确定邻近广播接收机与无线标识发射机之间的近似邻接度。

[0088] 另外，基于与接收的目击消息有关的邻近广播接收机和无线标识发射机的标识，中央服务器可以被配置为：确定哪个设备与注册的服务（例如，零售商店）有关，哪个设备与用户（例如，一个用户）有关。本申请所使用的术语“注册的服务”可以指代：被注册、认证、有效或者中央服务器以其它方式知道的并且与目击消息有关的参与方或服务。注册的服务可以包括商家、零售商、服务、商店（例如，大型零售商，当地的咖啡馆等）、以及在中央服务器中注册的各种其它第三方。注册的服务还可以包括由中央服务器管理的已知例程、动作或服务（例如，特定的搜索或活动警报）、或者替代地，可以在移动设备上执行的应用（例如，第三方应用）。在一个实施例中，注册的服务还可以包括在中央服务器中注册成开发者的任何第三方。例如，注册的服务可以对应于一个商家，该商家在中央服务器中注册了邻近广播接收机。在一个实施例中，中央服务器还可以将使用移动的邻近广播接收机的注册用户（例如，用户）视为注册的服务，其中，这些移动的邻近广播接收机响应于从其它无线标识发射机（例如，位于零售商店内的商家的静止标识发射机）接收到广播消息，发送目击消息。

[0089] 为了说明目的，在结帐队列中等待的用户所携带的移动的邻近广播接收机（例如，被配置为操作成邻近广播接收机的智能电话），可以从放置在该零售商店内的收银机销售点设备顶端的无线标识发射机接收广播消息，并且可以向中央服务器发送目击消息。当接收到该目击消息时，中央服务器可以基于与滚动标识符相对应的简档，来确定无线标识发射机属于该零售商店，并且基于目击消息中的元数据里所包括的邻近广播接收机的标识符，来确定该移动的邻近广播接收机与用户简档相关联。根据该信息，中央服务器可以向该用户发送销售信息。

[0090] 图 1 描绘了可以在各种实施例中使用的示例性系统 100。通常而言，中央服务器 120 可以被配置为接收、存储和以其它方式处理与无线标识发射机 110 相对应的数据。中央服务器 120 可以被配置为经由互联网 103 与诸如邻近广播接收机 142、移动的邻近广播接收机 138、第三方系统 101 和其它支持系统和 / 或服务 102 之类的各种设备交换通信。无线标识发射机 110 可以广播可被附近的邻近广播接收机 142 和 / 或移动的邻近广播接收机 138 经由短距离无线信号进行接收的消息。邻近广播接收机 142、138 可以使用远距离通信，通过互联网 103 将接收的广播消息作为目击消息中继给中央服务器 120。例如，邻近广播接收机 142 和移动的邻近广播接收机可以使用蜂窝网络 121 来向中央服务器 120 发送目击消息。第三方系统 101 可以包括商家服务器、零售商店计算设备、与紧急服务相关联的计算设备。其它支持系统和 / 或服务 102 可以包括与各种技术相关联的计算设备，例如，用户使用的用于提供注册信息的计算设备、传输与用户有关的内容的系统（例如，Qualcomm Gimbal™）、以及提供特定于位置的信息的服务（例如，Qualcomm IZat™）。

[0091] 中央服务器 120 可以包括用于执行各种操作以处理数据（例如，从邻近广播接收机 142、138、第三方系统 101 或者其它支持系统和 / 或服务 102 接收的数据）的一些组件 104-109。具体而言，中央服务器 120 可以包括可存储长期数据（例如，压缩的用户数据、过去的位置信息等）的数据仓库组件 104。中央服务器 120 还可以包括操作、控制和管理（或 OA&M）组件 105，该操作、控制和管理组件 105 可以管理、处理和 / 或存储与用户门户接入相

关联的软件、脚本、工具（例如，软件工具、例行程序等等）、以及用于管理中央服务器 120 的任何其它单元。此外，中央服务器 120 还可以包括开发者门户组件 106，该开发者门户组件 106 可以存储开发者账户数据和执行注册、账户管理以及与开发者相关联的警报（或通知）管理例行程序，例如，进行注册以便与无线标识发射机 110 的用户进行交互的供应商或商家。中央服务器 120 还可以包括滚动标识符（或 ID）解析器组件，所述滚动标识符（或 ID）解析器组件可以存储与无线标识发射机 110 相关联的出厂密钥，以及执行操作、软件或例行程序，以便将接收的目击消息中的加密的、编码的、滚动或者以其它发送模糊的标识信息与附属的用户数据进行匹配。中央服务器 120 还可以包括用户门户组件 109，所述用户门户组件 109 可以存储用户账户数据，并且执行与用户（例如，与无线标识发射机 110 相关联的人）相关联的注册、账户管理和搜索例行程序。中央服务器 120 还可以包括核心组件 108，所述核心组件 108 可以处理目击消息，执行警报或通知引擎模块，处理应用程序编程接口（API）命令，以及与中央服务器 120 中的其它组件交换数据。下面参照图 13 来描述核心组件 108。

[0092] 在各个实施例中，组件 104-109 可以由中央服务器 120 中包括的、连接到中央服务器 120 的、或者以其它方式与中央服务器 120 相关联的计算设备、服务器、软件和 / 或电路来启用。例如，核心组件 108 可以是中央服务器 120 中包括的服务器刀片或者计算单元。再举一个例子，数据仓库组件 104 可以是远程云存储设备，中央服务器 120 通过互联网协议与该远程云存储设备进行通信。

[0093] 在一个实施例中，邻近广播接收机 142 和移动的邻近广播接收机 138 可以被配置为执行核心客户端模块 115，所述核心客户端模块 115 可以是使邻近广播接收机 142、138 能够处理从邻近无线标识发射机 110 接收的广播消息的软件、指令、例行程序、应用、操作或其它电路。核心客户端模块 115 还可以处理邻近广播接收机 142、138 和中央服务器 120 之间的通信，例如，发送目击消息和从中央服务器 120 接收返回消息。此外，移动的邻近广播接收机 138 可以被配置为执行第三方应用模块 116，所述第三方应用模块 116 可以涉及执行由各种第三方提供的软件指令、例行程序、应用或其它操作（例如，商家应用）。在一个实施例中，当被配置为在中央服务器 120 中注册的服务时，第三方应用模块 116 可以从核心客户端模块 115 接收各种数据。例如，在中央服务器 120 中注册的第三方应用可以被配置为：当移动的邻近广播接收机 138 的用户进入、逗留和 / 或离开特定的场所（例如，地理围栏、零售商店等）时，从核心客户端模块 115 接收通知。

[0094] 在另一个实施例中，移动的邻近广播接收机 138 可以被配置为接收和发送广播消息，其还可以称为“无线标识收发机”。例如，用户可以使用智能电话，该智能电话被配置为从附近的无线标识发射机 110 接收广播消息，以及包括与该用户相关联的识别信息的广播信号。

[0095] 图 2 描绘了可以在各种实施例中使用的示例性通信系统 200。通信系统 200 有效地使无线标识发射机 110（例如，蓝牙® LE 发射机）能够通过多个移动的邻近广播接收机 138 和 / 或静止的邻近广播接收机 142，向中央服务器 120 发送包括标识信息的广播消息，而无需协商直接通信链路。无线标识发射机的附近范围（或广播范围）内的任何邻近广播接收机可以自动地收集这些广播消息。例如，位于某个邻近范围之内的移动的邻近广播接

收机 138 可以接收由位于无线标识发射机 110 中的蓝牙®无线装置所发送的广播消息。

[0096] 通信系统 200 可以包括无线标识发射机 110。无线标识发射机 110 可以与各种对象相耦合。例如，其可以嵌入在手镯之中。无线标识发射机 110 可以发送短距离无线信号 114，例如，如上所述的广播消息。例如，该短距离无线信号 114 可以是分组的定期广播，该分组包括无线标识发射机的识别码。替代地，短距离无线信号 114 可以是尝试与可充当邻近广播接收机的多个移动设备 138 中的任何一个建立无线通信链路。附近的邻近广播接收机（例如，静止的邻近广播接收机 142 和 / 或移动的邻近广播接收机 138）可以接收短距离无线信号 114。

[0097] 短距离无线信号 114 可以根据多种通信协议中的任一种，例如，蓝牙®、蓝牙 LE®、Wi-Fi、红外无线、感应无线、超宽带 (UWB)、无线通用串行总线 (USB)、Zigbee®、Peanut ®、或者其它短距离无线技术或协议，这些技术或协议必须或可以被修改为（例如，通过限制发射功率）将它们的有效通信距离限制到相对较短的距离（例如，在约 100 米之内）。在一些实施例中，无线标识发射机 110 可以使用蓝牙® 4.0 协议（或之后的版本）中标准化的低能耗技术。例如，在一些实施例系统中，无线标识发射机 110 可以定期地广播标识分组（其被配置成如在蓝牙® 4.0 协议中描述的通告），并且附近的邻近广播接收机 142、138 可以根据该协议被配置为充当扫描器。

[0098] 蓝牙®协议和蓝牙®设备（例如，蓝牙 LE 设备）具有相对较短的有效通信距离，广泛用于所部署的通信和计算设备中，具有满足各种实施例的发现和报告需求的标准通告或配对过程，并呈现出低功耗，这使得该协议能理想地用于各种实施例的多种应用。由于该原因，在本文的大部分示例中提到了蓝牙®和蓝牙 LE 协议和设备，以用于说明目的。但是，权利要求的保护范围不应限于蓝牙®或蓝牙 LE 设备和协议，除非在权利要求书中具体记载。例如，可以在无线标识发射机 110 中包括 Peanut® 收发机，并且可以使用 Peanut® 收发机来发送双向通信，在该情况下，邻近广播接收机 142、138 也被配置为使用 Peanut® 短距离无线传输。

[0099] 通信系统 200 可以包括多个静止的邻近广播接收机 142，该静止的邻近广播接收机 142 可以由整个区域、建筑物或者场所中的政府机关、商家或各种第三方进行部署。这些静止的邻近广播接收机 142 可以是专门针对无线标识发射机 110 来设计的（或者除了包括诸如交通信号灯、实用变压器等其它主要功能，还包括这种跟踪功能）。静止的邻近广播接收机 142 可以位于一个地区中的战略位置，例如，形成关于一个社区的周界、和 / 或位于交通流量高的区域中（例如，主叉路口和高速公路入口匝道）。静止的邻近广播接收机 142 可以与局域网 202（例如，WiFi 网络）进行通信，局域网 202 可以包括互联网接入服务器 140，该互联网接入服务器 140 提供与互联网 103 的连接 148。静止的邻近广播接收机 142 可以通过有线或无线链路 146，连接到局域网 202。在各种实施例中，静止的邻近广播接收机 142 可以被包含在互联网接入服务器 140 之中、或者位于互联网接入服务器 140 的附近。例如，静止的邻近广播接收机 142 可以是互联网接入服务器 140 中的组件，或者替代地，其可以放

置在互联网接入服务器 140 的顶端或旁边。在一个实施例中，静止的邻近广播接收机 142 可以位于一个地区中的战略位置，例如形成关于一个社区的周界，和 / 或位于交通流量高的区域（例如，沿着零售商店的过道，处于大厦的入口等）。在一个实施例中，静止的邻近广播接收机 142 可以具有额外的功能。例如，静止的邻近广播接收机 142 还可以充当零售商店中的收银机、销售点设备、和 / 或显示单位，或者被包括在这些部件之中。

[0100] 此外，通信系统 200 还可以包括被配置为充当移动的邻近广播接收机 138 的一个或多个移动设备。移动的邻近广播接收机 138 可以是典型的移动设备或者智能电话，它们经由与一个或多个基站 134 的远距离无线链路 136 与蜂窝网络 121 进行通信，其中所述一个或多个基站 134 通过有线或无线连接 158 耦接到一个或多个网络操作中心 132。这些蜂窝网络 121 可以使用诸如 3G、4G 和 LTE 之类的各种技术。网络操作中心 132 可以通过蜂窝网络 121 来管理语音呼叫和数据业务，并且网络操作中心 132 通常可以包括一个或多个服务器 130，或者可以通过有线或无线连接 156 来连接到一个或多个服务器 130。服务器 130 可以提供与互联网 103 的连接 154。在各种实施例中，移动的邻近广播接收机 138 可以是移动设备，该移动设备被应用或者其它软件模块配置为充当邻近广播接收机，以便通过互联网 103 的方式，将从无线标识发射机 110 接收的广播消息（即，目击消息）中继报告给中央服务器 120。在一个实施例中，静止的邻近广播接收机 142 也可以经由与基站 134 的远距离无线链路 136，与蜂窝网络 121 进行通信。

[0101] 邻近广播接收机 138、142 可以被配置为通过互联网 103，向中央服务器 120 报告与无线标识发射机 110 的联系（或目击）。例如，邻近广播接收机 142 可以向中央服务器 120 发送目击消息，该目击消息包括与无线标识发射机 110 的用户的标识相对应的滚动标识符。邻近广播接收机 138、142 每次从无线标识发射机 110 接收到标识符，该标识符就可以与该连接的时间以及邻近广播接收机 138、142 的位置进行关联，并可以将该信息发送给中央服务器 120（例如，在目击消息中）。在一些实施例中，可以将联系的标识符、时间和位置存储在邻近广播接收机 138、142 的存储器（或者中间服务器 130、140）中以便稍后报告（例如，响应于中央服务器 120 的查询消息广播或多播）。此外，中央服务器 120 可以将由目击消息所报告的位置信息存储在数据库中，其可以用于定位、跟踪或者以其它方式监测无线标识发射机 110 的移动。

[0102] 在一个实施例中，移动的邻近广播接收机 138 可以被配置为与静止接收机设备 142 交换短距离无线信号 189。换言之，移动的邻近广播接收机 138 可以被配置为操作成无线标识收发机，该无线标识收发机能够从无线标识发射机 110 接收短距离无线信号 114（即，广播消息），以及发送短距离无线信号 189 以便由邻近广播接收机 142 进行接收。

[0103] 在一个实施例中，邻近广播接收机 138、142 可以向无线路由器 185（例如，作为局域网 202 的一部分）发送无线信号 188，该无线路由器 185 可以提供与互联网 103 的连接 187。例如，静止的邻近广播接收机 142 可以向 WiFi 无线路由器 185 发送目击消息，该目击消息包括来自无线标识发射机 110 所发送的广播消息的数据。

[0104] 中央服务器 120 还可以连接到互联网 103，从而允许在邻近广播接收机 142、138 与中央服务器 120 之间进行通信。如上所述，中央服务器 120 可以包括多个组件、刀片或者其它模块，以便处理从邻近广播接收机 142、138 所接收的目击消息和数据。另外的实施例可以在中央服务器 120 和移动设备网络组件中的任何一个（例如，网络操作中心 132）之间提

供直接连接（没有示出），以便更直接地连接邻近广播接收机 142、138 和中央服务器 120。

[0105] 此外，通信系统 200 还可以包括诸如家庭或工作中的个人计算机之类的计算终端 124，用户可以通过使用计算终端 124 来经由互联网 103 与中央服务器 120 进行通信。这些终端 124 可以允许用户（例如，父母、警察、消防员、医护人员、以及其他政府机构）对设备（例如，无线标识发射机 110）进行注册，访问中央服务器 120 上的跟踪记录，和 / 或请求中央服务器 120 发起对特定的无线标识发射机 110 的搜索。在一个实施例中，用户可以例如通过访问 web 门户和 / 或与中央服务器 120 相关联的用户账户，使用这些终端 124 来注册无线标识发射机 110、邻近广播接收机 142、138（例如，被配置为执行与中央服务器相关联的客户端软件的智能电话）和 / 或标识收发机（没有示出）。类似地，诸如商家之类的第三方可以使用终端 124 来注册无线标识发射机 110、邻近广播接收机 142、138（例如，被配置为执行客户端软件并向中央服务器中继广播的静止接收机）和 / 或标识收发机（没有示出）。

[0106] 基于邻近广播接收机 138、142 在一个场所中的位置，多个邻近广播接收机 138、142 可以位于无线标识发射机 110 的广播区域之内，并可以同时接收广播消息。中央服务器 120 可以检测到邻近广播接收机 138、142 同时地（或者在某个时间段之内）发送用于指示从无线标识发射机接收到广播消息的目击消息。可以使用这种同时的目击消息，来确定与无线标识发射机在广播时有关的更精确的邻近信息。

[0107] 通信系统 200 可以以被动信息收集模式和 / 或主动搜索模式进行操作。在被动信息收集模式中，邻近广播接收机 138、142 可以对来自任何无线标识发射机 110 的广播进行连续监听，通过目击消息（例如，包括标识符、时间和位置的传输）向中央服务器 120 报告所有标识符接收事件。当没有执行任何主动搜索时（即，没有人正在查找特定的无线标识发射机 110），可以将无线标识发射机 110 的目击或者从无线标识发射机 110 接收的广播消息存储在邻近广播接收机 138、142 或中央服务器 120 的存储器中，以便在稍后时间进行访问。为了保护隐私，可以依据被跟踪的人或资产，将这种存储的数据保存一段有限的时间（例如，一天、一周或者一个月）。随后，如果发现人或资产丢失了，则可以立刻访问所存储的数据，以便定位和跟踪相关联的无线标识发射机 110，或者至少确定其最后报告的位置。

[0108] 在被动跟踪模式的修改中，每个邻近广播接收机 138、142 可以在一段有限的时间保存与从无线标识发射机 110 接收到的广播消息（或者联系）相对应的 ID、时间和位置。替代地，可以将这种信息存储在连接到这些邻近广播接收机 138、142 的服务器 130、140 中。随后，如果发现与无线标识发射机 110 相关联的人或资产丢失，则中央服务器 120 可以发起搜索，查询邻近广播接收机 138、142（或者服务器 130、140）以下载它们存储的数据（例如，指示与无线标识发射机 110 的联系的数据库），以用于分析并存储在中央服务器 120 的数据库中。

[0109] 在一个实施例中，为了限制对民用移动设备（其被配置为操作成移动的邻近广播接收机 138）的要求，可以只在静止的邻近广播接收机 142 上实施被动跟踪模式。虽然这种设备的数量越少，意味着无线标识发射机 110 的跟踪可能越不有效，但该实施例可能仍然能够接收广播消息，从而跟踪通过交通流量高的区域（例如，交叉路口、高速公路入 / 出匝道、公交车站、机场等）的无线标识发射机 110。

[0110] 在被动信息收集模式 / 实施例中，用户可以使用通信系统 200 来请求特定的无线标识发射机 110 的位置，例如通过从终端 124 向中央服务器 120 发送请求。例如，母亲可以

登录她的家用计算机终端 124，请求她的孩子的背包中的无线标识发射机 110 的位置。该请求可以包括与该无线标识发射机 110 相对应的序列号、代码或者其它标识符。中央服务器 120 可以搜索在所存储的标识消息中的序列号、代码或者其它标识符，并且返回与输入信息相匹配的任何报告的位置，以及通过目击消息来报告这些位置的时间。在另外的实施例中，父母输入的序列号或代码与所请求的无线标识发射机 110 在广播消息中传输的、并且在由邻近广播接收机 138、142 提交的目击消息中向中央服务器 120 中继的标识符，可以是交叉引用的。以此方式，即使对数据进行连续地收集，也只有被授权的用户（即，知道与特定的无线标识发射机 110 相关联的访问码、密码或者其它密码的人）能够获得关于给定的无线标识发射机 110 的信息。

[0111] 在主动搜索模式 / 实施例中，中央服务器 120 可以指示邻近广播接收机 138、142 主动地搜索特定的无线标识发射机 110（即，“目标”无线标识发射机）。可以响应于从终端 124 接收的请求，发起主动搜索。这种请求可以包括用于特定无线标识发射机 110 的标识符，或者可以交叉链接到无线标识发射机 110 的标识符的账号 / 姓名。中央服务器 120 可以例如通过广播或者多播向邻近广播接收机 138、142 发送激活消息，所述激活消息可以指示邻近广播接收机 138、142 对特定的无线标识发射机 110 进行搜索，并且该激活消息可以包括目标无线标识发射机 110 的标识符（即，目标设备 ID）。例如，与针对一个目标无线标识发射机 110 的主动搜索相对应的激活消息，可以包括 ：该无线标识发射机 110 以不可预测的方式（但中央服务器 120 知道该方式）来定期改变的滚动标识符。在一个实施例中，中央服务器 120 发送、广播或者多播的激活消息，可以只发送给位于特定的扇区之内或者位于与特定位置的给定距离之内的邻近广播接收机 138、142。替代地，该激活消息可以标识特定的扇区或者与特定位置的距离，以使邻近广播接收机 138、142 能够基于它们自己已知的位置来判断该激活消息是否可应用于它们。以此方式，可以将该搜索关注于给定的区域，例如，涵盖无线标识发射机 110 的最后已知位置或者目击者目击位置的扇区。通过以此方式对搜索进行关注，不需要对不位于搜索扇区之内的邻近广播接收机 138、142 进行激活。

[0112] 在主动搜索模式 / 实施例中，响应于从中央服务器 120 接收到包括目标设备 ID 的激活消息，并确定自己位于所标识的搜索扇区之内，邻近广播接收机 138、142 可以配置它们的短距离无线装置（例如，蓝牙无线装置）来监听具有标识符的广播消息。换言之，邻近广播接收机 138、142 可以被视为进行主动搜索，可以查找该激活消息中所包括的标识符（即，目标设备 ID），或者尝试与标识符进行配对。在不依赖于与无线标识发射机进行配对的实施例中，将接收的广播消息中的标识符与激活消息中的目标设备 ID 进行匹配的邻近广播接收机 138、142，可以通过经由有线链路 146 或远距离无线链路 136 发送的目击消息，迅速地向中央服务器 120 报告该事件。在依赖于无线标识发射机和邻近广播接收机之间的消息的配对或交换的实施例中，邻近广播接收机 138、142 可以监听并只完成通信握手或者与广播该目标设备 ID 的设备进行配对，并且忽略其它配对尝试。在该替代性实施例中，当处于主动搜索模式中时，可以保护邻近广播接收机 138、142，以免与未授权设备进行配对。此外，只要邻近广播接收机 138、142 接收到设备 ID，就可以在主动搜索模式下对配置过程进行修改，以终止通信链路，在主动搜索模式下，进一步保护以防止与未授权设备进行配对。在主动搜索模式 / 实施例中，接收目标设备 ID 的邻近广播接收机 138、142 可以通过与互联网 103 的有线或无线链路，迅速地向中央服务器 120 报告事件。如上所述，这种报告可

以包括邻近广播接收机 138、142 的位置、以及接收到该标识符的时间（如果没有立即发送该报告的话）。在主动搜索模式 / 实施例中，可以将中央服务器 120 所接收的每个目击消息（例如，以在地图中显示更新位置指示符的网页形式）报告给感兴趣的人或机构。

[0113] 此外，在主动搜索模式 / 实施例中，授权用户（例如，警察、FBI、消防 / 救援或者其它机构的人员）可以使用通信系统 200 来激活针对特定的无线标识发射机 110 的搜索（例如，通过使用终端 124 来向中央服务器 120 提供目标设备 ID、以及搜索位置或要搜索的扇区）。例如，发现她的孩子失踪的母亲可以给警察打电话，并向警察提供她的孩子的衣服中隐藏的无线标识发射机 110 的标识符。在激活搜索的情况下，中央服务器 120 可以向位于初始目标搜索扇区内的邻近广播接收机 138、142 发送警报（或者指示已经激活针对无线标识发射机的搜索的消息）。随后，中央服务器 120 可以激活用于呈现搜索区域的地图的网页，并进行近似实时地维护，从而当接收到有关的目击消息时，在地图上显示报告的位置信息。随后，授权用户可以访问该网站（或者服务器提供的其它信息），以协调人力搜索工作。

[0114] 当然，在发起了主动搜索时，可以使用在被动模式中在邻近广播接收机 138、142 中收集和存储的信息或者在中央服务器的数据库中的信息，例如以便识别初始搜索位置或扇区，跟踪最近的位置和移动，提供 / 显示目击消息所报告的位置的历史，其中可以将这些信息与近似实时的搜索报告进行组合。

[0115] 图 3 描绘了用于在无线标识发射机 110（其在图 3 中称为“WIT”）、邻近广播接收机 142 和中央服务器 120 中实现的实施例方法 300。在方框 302 中，无线标识发射机 110 可以广播包括标识符的消息，例如，如上所述的广播消息。例如，无线标识发射机 110 可以广播蓝牙 LE 通告分组，该蓝牙 LE 通告分组包括如本申请所述的滚动标识符。在方框 302 中，这可以通过无线标识发射机 110 中的微控制器来完成，其中该微控制器确定到了广播其标识符的时间，配置适当的广播消息（例如，根据蓝牙® 4.0 协议中针对蓝牙 LE 设备所规定的通告分组），并通过短距离无线装置来发送该分组。

[0116] 在各个实施例中，无线标识发射机广播的消息（即，广播消息）可以包括标识符段（例如，滚动标识符）。在各个实施例中，该广播消息还可以包括额外的段（例如，类型段）。该类型段可以指示无线标识发射机的类型。例如，可以销售无线标识发射机以用于各种目的，例如，儿童安全设备、狗项圈或者商店防盗标签。无线标识发射机可以基于意图目的而具有不同的类型段（例如，一个代码用于儿童安全装置、第二个代码用于狗项圈等）。类型段可以是静态的，并由制造商进行设置，而该标识符的剩余部分对于每个设备来说是唯一的，其可以如下所述地进行滚动。用户也可以对类型段进行改变，例如，当由于不同的目的或者应用，对无线标识发射机进行重置时。

[0117] 在其它实施例中，广播消息还可以包括 :具有用于由邻近广播接收机来实现的指令或命令的一个或多个静态或动态段。这些命令段也可以被传递，以指示中央服务器或者其它网络设备。类似于类型段，命令段可以被设置或者是静态的，或者可以基于各种状况（例如，来自一个或多个邻近广播接收机的配对或数据）而随时间发生变化。无线标识发射机的用户也可以对这些命令设置进行配置。第二段或者另外的段也可以指示无线标识发射机的状态。例如，第二段可以指示剩余的电量或者在电池耗尽之前估计的剩余时间。邻近广播接收机或者中央服务器可以解释该状态并作出相应地响应。

[0118] 返回到图 3，在方框 304 中，无线标识发射机 110 可以进入休眠模式。例如，在广

播具有标识符的广播消息之后，无线标识发射机 110 可以被配置为进入省电状态，其中该省电状态可以持续一段预先定义的时间。在各个实施例中，无线标识发射机 110 可以休眠一段预先定义的时间、从不休眠、或者在基于各种输入所确定的不同时间中休眠。在方框 306，无线标识发射机 110 可以从休眠模式苏醒（例如，在预先定义的持续时间到期之后）。在方框 308 中，无线标识发射机 110 可以根据某种算法（例如，滚动标识符算法），生成新的设备标识符。例如，无线标识发射机 110 可以使用伪随机函数或者流式加密算法（例如，AES-CTR）来生成滚动标识符，如下所述。随后，无线标识发射机 110 可以返回到方框 302 以进行再次广播。在一个实施例中，该广播消息可以包含用于指示该无线标识发射机的用于接收消息的可用性的、定时、计数器、递减计数、或调度信息。例如，该广播消息可以指示无线标识发射机将在规定的时间窗内接收输入的配置消息。在各个实施例中，方框 302-308 中的操作可以由标识收发机来执行（例如，被配置为操作成标识发射机和邻近广播接收机的智能电话）。

[0119] 如上所述，在方框 308 中使用的算法（或者滚动标识符算法）可以生成设备或系统很难预测或识别的滚动标识符，所述设备或系统不知道该无线标识发射机 110 的标识（例如，MAC 或蓝牙 ID）、解码密钥和 / 或用于生成滚动标识符的算法。如下面参照图 19 所讨论的，中央服务器 120（其被配置为具有算法（或解码算法）或解码密钥，并且拥有该无线标识发射机 110 标识）可以使用该滚动标识符来确定相应的账户或设备标识。虽然方法 300 示出了滚动标识符在每一次苏醒和广播循环都发生变化（作为一个例子），但在其它实施例中，可以不太频繁地改变该标识符（例如，每一分钟改变一次、每一小时改变一次等）。在这些实施例中，只按照规定的时间间隔来执行在方框 308 中生成新标识符的操作，使得在苏醒之后的其它时间（即，方框 306），无线标识发射机 110 可以返回到方框 302 来广播该标识符。下文讨论了用于生成滚动标识符或者其它编码的标识符的各种算法。

[0120] 方法 300 还描绘了可以在邻近广播接收机 142 中实施的操作。在方框 312，邻近广播接收机 142 可以从无线标识发射机 110 接收所述广播消息。当邻近广播接收机 142 位于无线标识发射机 110 的附近范围之内时（即，位于通信范围之内），可以接收该广播消息。当接收到具有包括的标识符的广播消息时，邻近广播接收机 142 可以分析所接收的广播消息中的报头或元数据，以及解析和评估该广播消息中的各种数据。在一个实施例中，该广播消息可以包含加密的和非加密的数据，其中邻近广播接收机 142 可以被配置为对该数据进行解密或者以其它方式进行访问，也可以不被配置为对该数据进行解密或者以其它方式进行访问。在方框 314 中，邻近广播接收机 142 可以向中央服务器 120 发送目击消息，所述目击消息包括标识符、位置信息、以及与广播消息的接收相对应的时间。可以通过无线广域网（例如，耦接到互联网的蜂窝数据网络）来完成这种传输。在各个实施例中，方框 312 和 314 中的操作可以由静止的邻近广播接收机、移动的邻近广播接收机、或者替代地标识收发机（例如，被配置为操作成发射机和接收机二者的智能电话）来执行。

[0121] 通常，目击消息可以包括元数据或报头信息，这些元数据或报头信息可以描述由邻近广播接收机 142 接收的广播消息（例如，消息大小、主题的指示符等））、例如邻近广播接收机标识（例如，代码、用户名等）、邻近广播接收机 142 关于该服务器所关联的服务的指示（例如，邻近广播接收机 142 参与针对特定的供应商、商家、区域等的跟踪程序））、以及接收这些广播消息时的状况。例如，目击消息可以包括所接收的广播消息的信号强度信

息。在一个实施例中，目击消息可以各自包括用于描述目击消息的通用主题、题材或者原因的代码、标志或者其它指示符。例如，该目击消息可以包含用于指示与活动警报的关系的标志。

[0122] 另外，目击消息可以包括邻近广播接收机 142 的位置信息。具体而言，目击消息可以指示与位置有关的网络专用信息。例如，目击消息可以指示小区站点（例如，小区站点 ID）、蜂窝网络塔（例如，小区塔 ID）、或者移动的邻近广播接收机在接收广播消息时与之通信的其它无线网络。此外，目击消息可以基于来自全球定位系统 (GPS) 的数据或邻近广播接收机 142 中所包括的码片，包括更精细的位置信息。例如，邻近广播接收机 142 可以确定该邻近广播接收机 142 在接收到广播消息时的 GPS 信息（即，GPS 坐标），其将这些坐标包括在相应的目击消息中。在一个实施例中，目击消息还可以包括来自该邻近广播接收机 142 中的各种传感器（例如，加速计、陀螺仪、磁力计等等）的传感器数据。此外，目击消息可以包括：用于确认该目击消息是否来自已知的、注册的或者在其它方面中有效的邻近广播接收机 142 的合法性的认证信息。例如，在目击消息中包括的认证信息可以包括在该邻近广播接收机和中央服务器 120 之间共享的密码、证书或者哈希数据。

[0123] 在各个实施例中，邻近广播接收机 142 可以通过将数据和各种信息附加到从无线标识发射机 110 接收的广播消息中，来生成目击消息。在一个实施例中，目击消息可以包括接收的广播消息的完整部分，或者替代地只包括该邻近广播接收机 142 确定为具有意义的所接收的广播消息的一部分。例如，在生成相应的目击消息之前，邻近广播接收机 142 可以从广播消息中提取特定的报头或者元数据信息。再举一个例子，邻近广播接收机 142 可以对广播消息中的数据进行压缩、简略、截短和 / 或概括。在另一个实施例中，邻近广播接收机 142 可以简单地将接收的广播消息重新定向、中继或者重新发送给中央服务器。

[0124] 可以通过诸如无线蜂窝网络、被配置为通过互联网协议进行通信的局域网、远距离无线通信链路或者短距离无线之类的无线或有线通信链路，来发送目击消息。例如，邻近广播接收机 142 可以在互联网上经由蜂窝网络向中央服务器发送目击消息。再举另一个例子，邻近广播接收机 142 可以通过有线以太网连接来发送目击消息。

[0125] 返回到图 3，方法 300 还描绘了可以在中央服务器 120 中实现的操作。在方框 322 中，中央服务器 120 可以从邻近广播接收机 142 接收所述目击消息。在方框 324 中，中央服务器 120 可以将该目击消息所指示的标识符与无线标识发射机 110 进行关联。中央服务器 120 可以将该目击消息中的标识符与用户注册 / 生成的账户进行关联。可以通过以下方式来完成该标识符与特定的无线标识发射机 110 或者用户账户的关联：将该标识符与同无线标识发射机 110 或者用户账户相对应的代码数据库进行比较，以确定应当存储来自该目击消息的信息（例如，位置信息）的数据库记录。由于在一些实施例中，无线标识发射机 110 标识符频繁地改变（滚动），因此该过程可能涉及：将在该目击消息中接收的标识符与由伪随机数发生器算法所生成的几种可能的序列码进行比较，或者应用将所接收的标识符作为输入并输出相应的账户号的逆算法。在方框 326 中，中央服务器 120 可以将来自目击消息的数据（例如，位置信息和时间数据）存储在数据库中。例如，中央服务器 120 可以基于评估所接收的目击消息，来确定邻近广播接收机 142 在接收到广播消息时的位置，并可以将该数据存储在链接到无线标识发射机 110 或者其用户 / 所有者的数据库中。

[0126] 在方框 340 中，中央服务器 120 可以响应于该目击消息，执行一个动作，例如，向接

收者发送消息，发送优惠券和 / 或计算报酬。在一个实施例中，中央服务器 120 可以向接收者（例如，邻近广播接收机 142）发送返回消息，该返回消息包括用于指示邻近广播接收机 142 如何对所接收的广播消息进行响应的指令、软件或代码。例如，该返回消息可以指示邻近广播接收机 142 发送链接通告消息。对于来自中央服务器的这些消息的接收方可以包括各种设备和参与方，其包括 :注册服务的计算设备（例如，商家、紧急救援人员）、用户的移动设备、以及邻近广播接收机（例如，接收该广播消息的邻近广播接收机 142）。在另一个实施例中，中央服务器 120 可以使用存储的数据来识别无线标识发射机 110 何时进入指定的区域、处于指定的区域之中和 / 或离开指定的区域。换言之，中央服务器 120 可以识别何时无线标识发射机 110 来到附近，在附近逗留，或者离开邻近广播接收机 142 的附近。

[0127] 图 4A 描绘了用于在执行启动操作之后，无线标识发射机（在图 4A 中被称为“WIT”）接收配置设置的实施例方法 400。通常，无线标识发射机可以只执行单向通信，广播用于由邻近广播接收机进行接收的信号。但是，无线标识发射机可以被配置为 :选择性地参与同具有类似的短距离无线信令能力（例如，蓝牙 LE 收发机）的其它设备的双向通信。具体而言，在初始化操作（或者“启动”）之后，无线标识发射机可以被配置为从邻近广播接收机接收输入的短距离无线通信。例如，当更换电池时或者第一次插入电池时，无线标识发射机可以在一段预先定义的时间段（例如，六十秒）中接受输入的蓝牙分组。替代地，无线标识发射机可以接收输入的消息，作为功率循环的一部分（例如，在无线标识发射机重启之后的六十秒内进行接收）。

[0128] 这种输入的短距离无线通信可以包括 :用于设置该无线标识发射机为了执行各种功能而使用的配置参数的值的指令、软件、固件、命令或其它代码。具体而言，输入的通信可以包括配置设置（或者值），无线标识发射机可以使用这些配置设置（或者值）来设置或者修改与发送广播消息相关联的已建立的配置参数，这些已建立的配置参数包括该无线标识发射机的标识信息。在一个实施例中，包括配置设置的输入通信，可以是不需要发送方与接收方（即，无线标识发射机）之间进行配对操作的蓝牙信号（例如，设置器或者获得器）。换言之，输入的通信可以是非配对的蓝牙通告。

[0129] 配置参数可以包括 :用于发送广播消息的发送时间间隔（即，无线标识发射机应当以何种频率广播包括其标识的分组）、以及用于发送广播消息的发射功率（即，当进行广播时，要使用什么信号强度）。例如，接收的配置设置可以通过有助于该无线标识发射机的准确跟踪，同时节省电池电量的方式，来改变该无线标识发射机广播其标识符的时间间隔（即，广播频率）。由于设置发射功率配置参数可能影响无线标识发射机的电池服务寿命（例如，更长的时间间隔可以包括更长的休眠模式，因此降低了功耗），所以这可能是较为重要的。在一个实施例中，配置参数还可以包括 :能由制造商或者管理方（例如，中央服务器）进行设置或者修改的调试参数。无线标识发射机所执行的软件或算法可以使用该调试参数，该调试参数可以指示无线标识发射机应当何时生成要广播的新标识符（例如，用于生成新的滚动标识符或者蓝牙 MAC 地址标识符的时间间隔）。在另一个实施例中，具有配置设置的输入通信可以包括 :用于指示该无线标识发射机改变在广播消息中表示的数据的命令（例如，通过进入 / 退出编码模式）。替代地，输入的通信可以包括 :用于无线标识发射机缩短其广播信号距离以模拟近场通信 (NFC) 的指令。

[0130] 在方框 402 中，无线标识发射机可以进行启动。换言之，可以对无线标识发射机提

供能量、初始化和以其它方式配置，以便从冬眠、睡眠、休眠或者以其它方面中从去活动状态恢复操作。在各个实施例中，可以响应于用户输入（例如，按钮按下）、无线标识发射机中的电池的插入、或者接收短距离无线信号（例如，激活信号），来执行启动操作。在方框 403 中，可以激活该无线标识发射机的短距离无线装置。这种激活可以通过定时器或者通过微控制器确定自从执行了启动操作以来的持续时间已经到期来完成，或者与启动操作同时地进行。在一个实施例中，短距离无线装置的激活可以是方框 402 中的启动操作的例行程序。

[0131] 在方框 404 中，无线标识发射机可以广播配置消息，该配置消息用于指示存在能够在该无线标识发射机中设置的配置参数。例如，该配置消息可以包括无线标识发射机的标识（标识符），以及后续的短距离无线信号可以设置、修改或者初始化某些数量或者类型的配置参数的指示。在一个实施例中，该配置消息可以包括：可用于被设置的配置参数列表（例如，发送时间间隔）。

[0132] 在替代的实施例中，该配置消息可以包括：用于指示无线标识发射机可用于接收配置设置的指示符。在该实施例中，任何响应的设备（例如，附近的邻近广播接收机）可以发送用于请求配置参数列表的响应（例如，蓝牙 LE 信号）。响应于接收到该请求，移动的邻近广播接收机可以发送包括配置参数列表的第二消息。

[0133] 在判断框 406 中，无线标识发射机可以判断：在例如来自附近的邻近广播接收机或者标识收发机的短距离无线信号中，是否接收到配置设置。无线标识发射机可以对短距离无线装置进行监测，以判断是否从邻近的设备接收到响应。响应可以具有该无线标识发射机微控制器能够识别的简单响应分组或脉冲的形式，或者替代地，是根据蓝牙 LE 协议的通告。如果接收到配置设置（即，判断框 406 ＝“是”），则在方框 408 中，无线标识发射机可以基于所接收的配置设置来设置参数。例如，无线标识发射机可以设置用于指示其发送广播消息的频率的值。如果没有接收到配置设置（即，判断框 406 ＝“否”），或者如果无线标识发射机执行方框 408 中的操作，则在判断框 410 中，无线标识发射机可以判断配置时段是否已流逝。例如，无线标识发射机可以对计数器或定时器进行评估，以判断自执行启动操作以来，是否已流逝了预先定义数量的秒（例如，60 秒）。如果该配置时段还没有流逝（即，判断框 410 ＝“否”），则在可选框 411 中，无线标识发射机可以等待一段时间（例如，很多的毫秒、秒等），随后可以继续方框 404 中的操作。

[0134] 但是，如果该配置时段已流逝（即，判断框 410 ＝“是”），则在方框 302’中，无线标识发射机可以基于配置参数来广播包括标识符的消息。例如，响应于从附近的邻近广播接收机接收到配置设置（或者值），无线标识发射机可以按照配置参数设置所指示的信号强度，来发送广播消息。在可选框 412 中，无线标识发射机可以基于这些配置参数（例如，发送时间间隔配置参数），进入休眠一段时间。在方框 308 中，无线标识发射机可以根据某种算法来生成新的设备标识符（例如，滚动标识符），并且可以继续执行方框 302’中的操作。

[0135] 在替代的实施例中，无线标识发射机可以被配置为：基于时钟时序（或者时钟信号）、检测到的来自用户的输入（例如，检测到的按键按下）、或者先前接收的信号中的信息（例如，从邻近广播接收机接收的消息可以指示该无线标识发射机在特定的未来时间中成为可用于后续消息），接收来自邻近广播接收机的输入消息。

[0136] 图 4B 描绘了一种用于在执行启动操作之后，无线标识发射机（在图 4B 中被称为“WIT”）接收配置设置，并且基于该配置设置来广播消息的实施例方法 450。该方法 450 类

似于上面所描述的方法 400，除了无线标识发射机被配置为基于配置参数来生成不同的标识符（例如，滚动标识符）和 / 或蓝牙机器地址（即，BT MAC 地址），其中该配置参数可以根据来自附近的邻近广播接收机的配置消息来设置。通常，当无线标识发射机被配置为通过蓝牙无线装置（例如，蓝牙 LE 等）来发送广播消息时，蓝牙信号或分组可以包含指示用于发送信号的蓝牙设备的信息。基于从附近的邻近广播接收机接收的调试集值，无线标识发射机可以被配置为 :按照变化的时间间隔，改变在广播消息中所指示的标识符和 / 或蓝牙 MAC 地址。

[0137] 在方框 402 中，无线标识发射机可以启动。在方框 403 中，可以激活该无线标识发射机的短距离无线装置。在方框 404 中，无线标识发射机可以广播配置消息，该配置消息用于指示存在可以在该无线标识发射机中设置的配置参数。在判断框 406 中，无线标识发射机可以判断在例如来自附近的邻近广播接收机或者标识收发机的短距离无线信号中，是否接收到配置设置。如果接收到配置设置（即，判断框 406 =“是”），则在方框 408 中，无线标识发射机可以基于所接收的配置设置来设置参数。如果没有接收到配置设置（即，判断框 406 =“否”），或者如果无线标识发射机执行方框 408 中的操作，则在判断框 410 中，无线标识发射机可以判断配置时段是否已流逝完。如果该配置时段还没有流逝（即，判断框 410 =“否”），则在可选框 411 中，无线标识发射机可以等待一段时间（例如，很多毫秒、秒等），随后可以继续方框 404 中的操作。但是，如果该配置时段已流逝（即，判断框 410 =“是”），则在方框 302’中，无线标识发射机可以基于配置参数来广播包括标识符的消息。

[0138] 在判断框 452 中，无线标识发射机可以判断其是否需要新的蓝牙 MAC 地址。换言之，无线标识发射机可以对配置参数进行评估，以确定其必须生成新的蓝牙 MAC 地址的频率，所述新的蓝牙 MAC 地址用于采用蓝牙 LE 协议的广播消息。因此，无线标识发射机可以被配置为使用滚动蓝牙 MAC 地址。在一个实施例中，无线标识发射机可以比较所存储的信息，其中该信息指示自上一次生成蓝牙 MAC 地址以来流逝的时间（或者广播的数量）。替代地，无线标识发射机可以针对每一次广播，生成新的蓝牙 MAC 地址。如果需要新的蓝牙 MAC 地址（即，判断框 452 =“是”），则在方框 454 中，无线标识发射机可以生成新的蓝牙 MAC 地址。在一个实施例中，无线标识发射机可以使用在蓝牙协议中提供的命令（例如，API 调用或者命令），来生成新的蓝牙 MAC 地址。另外，新的蓝牙 MAC 地址可以是不可解析的、随机的、或者在其它方面中，缺少任何接收设备可以用来联系该无线标识发射机的信息。例如，邻近广播接收机可以不使用在广播消息中指示的蓝牙 MAC 地址，来指示与该无线标识发射机的响应传输或配对。

[0139] 在另一个实施例中，为了支持邻近广播接收机与无线标识发射机之间的配对通信（例如，通过蓝牙配对），可以通过一种算法来生成新的蓝牙 MAC 地址，使得接收广播消息的接收方邻近广播接收机可以确定无线标识发射机的实际蓝牙 MAC 地址。换言之，可以使用已知的算法、密钥、加密、或者无线标识发射机和被授权与该无线标识发射机建立配对通信的已授权或相关联的邻近广播接收机所知道的其它技术，来生成新的蓝牙 MAC 地址。在各种实施例中，下面参照图 20-24B 所描述的方法可以由无线标识发射机和邻近广播接收机来执行，以便通过与无线标识发射机和中央服务器可以对滚动标识符进行解码相类似的方式，对广播消息中所指示的模糊的蓝牙 MAC 地址进行解码。

[0140] 如果不需要新的蓝牙 MAC 地址（即，判断框 452 =“否”），或者在方框 454 中生成

新的蓝牙MAC地址，则在判断框456中，该无线标识发射机设备可以判断是否需要新的设备标识符（例如，滚动标识符）。类似于新的蓝牙MAC地址，无线标识发射机可以对配置参数进行评估，以确定何时生成新的滚动标识符。例如，存储的配置参数可以指示：每隔一秒钟、一分钟或者在一小时之后，需要新的设备滚动标识符。如果需要新的标识符（即，判断框456＝“是”），则在方框308中，无线标识发射机可以根据某种算法来生成新的设备标识符（例如，滚动标识符）。如果不需要新的设备标识符（即，判断框456＝“否”），或者如果在方框308中根据该算法生成了新的设备标识符，则在可选框412中，无线标识发射机可以基于这些配置参数，进入休眠一段时间，并可以继续执行方框302’中的操作。

[0141] 图5描绘了用于无线标识发射机执行与邻近广播接收机的双向无线通信的实施例方法550。如上所述，无线标识发射机可以通常用于单向信令，例如发送广播消息以便由邻近广播接收机进行接收、使用和中继。但是，无线标识发射机可以被配置为进行双向通信，以便接收用于指示发射机执行某些操作（例如，激活传感器）的固件、软件指令或者触发信号、配置数据和无线标识发射机可以用于发送广播消息的其它信息。这种双向通信可用于包括短距离无线收发机（例如，蓝牙®无线装置）的无线标识发射机。但是，无线标识发射机可以被配置为：选择性地参与同邻近广播接收机的双向通信，以将功耗减到最小，使电池服务寿命最大化。在一个实施例中，无线标识发射机可以广播消息，该消息用于向邻近广播接收机指示：该无线标识发射机可用于从邻近广播接收机接收消息的时间段，并且该无线标识发射机可以在有限的时间段或者预先定义的时间段内接收消息。

[0142] 在方框552中，无线标识发射机可以对计数器进行重置，例如，设置计数器变量以指示该无线标识发射机可能不接收消息的时段的起点（或初始化）。在方法550的操作期间，可以将计数器重置为零值，并可以递增到预先定义的数量。替代地，可以将该计数器重置或者初始化成预先定义的数值，并向下递减到零值。使用计数器变量，仅仅只是一种用于无线标识发射机确定何时将自身配置为接收消息的非限制性示例技术。在替代的实施例中，无线标识发射机可以替代地基于时钟定时（或者时钟信号）、检测到的来自用户的输入（例如，检测到的按键按下）、先前接收的信号中的信息（例如，从邻近广播接收机接收的消息可以指示该无线标识发射机在特定的未来时刻成为可用于后续消息）、或者功率循环（例如，一个这种时间可以是在无线标识发射机的初始启动或重启之后的六十秒），来确定该无线标识发射机何时可用于接收输入的消息。

[0143] 在一个实施例中，无线标识发射机可以粗略地与各个邻近广播接收机（例如，智能电话、整个场所的监听无线装置等）和/或中央服务器具有时钟同步、或者维持各个邻近广播接收机和/或中央服务器已知并粗略跟踪的随机数或计数器变量。例如，当无线标识发射机被激活时（例如，开启、通过插入电池进行初始化等），用户可以在中央服务器中注册该无线标识发射机，其中所述中央服务器存储该无线标识发射机标识以及使该中央服务器能够估计该无线标识发射机中的随机数或计数器值或时钟定时的信息。在一个实施例中，这种随机数或计数器变量或者时钟同步可以用于消除无线标识发射机标识的歧义，和/或用作用于模糊的或编码的消息的解密密钥。下面进一步描述这些注册和同步操作。

[0144] 在方框554中，无线标识发射机可以生成包括标识信息、计数器、以及可用于接收消息的时间的消息。所生成的消息可以包括关于该无线标识发射机的标识（例如，序列码/号、用户名或者滚动标识符）的信息。在一个实施例中，可以对所生成的消息进行加密、编

码或者以其它方式进行模糊，以防止邻近广播接收机确定该无线标识发射机和 / 或其用户的标识。例如，所生成的消息可以使用仅仅该无线标识发射机和中央服务器知道但邻近广播接收机不知道的滚动标识符或者代码。

[0145] 此外，所生成的消息还可以包括：用于指示当该无线标识发射机可以用于接受邻近广播接收机的通信时的时间或状况的信息。例如，该消息可以描述计数器的当前值或者指示向下递减的定时器，所述向下递减的定时器显示该无线标识发射机何时可用。在另一个实施例中，所生成的消息可以包括：用于邻近广播接收机实现对该无线标识发射机的成功传输的指令。例如，所生成的消息可以包含：用于邻近广播接收机向该无线标识发射机发送的任何消息的规范（例如，所需要的代码、内容、传递时间等）。

[0146] 在方框 556 中，发射机可以通过短距离无线传输（例如，蓝牙 LE 分组）来广播所生成的消息。如果邻近广播接收机位于短距离广播的范围之内，则该邻近广播接收机可以对广播进行接收和处理，如下面参照图 11 所描述的。

[0147] 无线标识发射机可以在每个计数器时间周期，对所生成的相同消息进行多次定期地广播。换言之，在对计数器变量值进行修改之前，无线标识发射机可以不止一次广播所生成的消息。在判断框 558 中，无线标识发射机可以判断预先定义的计数器时间周期是否已经到期。如果该计数器时间周期还没有到期（即，判断框 558 =“否”），则无线标识发射机可以在方框 556 中继续对所生成的消息进行定期地广播。

[0148] 如果该计数器时间周期已到期（即，判断框 558 =“是”），则在方框 560 中，无线标识发射机可以对该计数器进行递增，在判断框 562 中，基于该计数器值来判断该无线标识发射机是否成为可用于接收消息。例如，无线标识发射机可以将当前计数器变量值与预先定义的最大（或最小）计数器值进行比较。如上所述，在各种其它实施例中，无线标识发射机可以基于在该无线标识发射机中存储的时间或指令的其它评估，来确定用于接收消息的可用性。

[0149] 如果不可用于接收消息（即，判断框 562 =“否”），则无线标识发射机可以继续执行方框 554 中的操作，以生成要广播的新消息。如果无线标识发射机可用于接收消息（即，判断框 562 =“是”），则在方框 564 中，无线标识发射机可以对输入消息进行监听，例如通过针对输入的短距离无线传输，对接收机电路进行监测，在方框 566 中，无线标识发射机可以例如使用在该无线标识发射机中的处理器或无线调制解调器上运行的软件或操作，对任何接收的输入消息进行处理。

[0150] 在判断框 568 中，无线标识发射机可以判断该接收时间段是否已经到期。换言之，无线标识发射机可以判断是否仍然可以接收到输入消息。用于接收输入消息的时间段，可以是基于由无线标识发射机所维持的计数器变量、时钟信号指示、或者接收的消息中的信息。如果该接收时间段还没有到期（即，判断框 568 =“否”），则无线标识发射机可以在方框 564 中，继续对输入消息进行监听。但是，如果该接收时间段已到期（即，判断框 568 =“是”），则无线标识发射机可以通过返回到方框 552 来重复该过程。

[0151] 图 6 是移动的邻近广播接收机 138 中的各模块的图 600。如上所述，邻近广播接收机可以包括静止的邻近广播接收机（例如，在建筑物周边布置的专用设备）和移动的邻近广播接收机 138（例如，被配置为执行操作以便从无线标识发射机 110 接收广播消息并经由远距离通信（例如，经由 WiFi 或蜂窝网络）通过互联网 103 向中央服务器 120 发送目击消

息的移动设备）。下面在移动的邻近广播接收机 138 中的单元的背景下，描述各种模块和组件，但在各个实施例中，任何邻近广播接收机（例如，静止的邻近广播接收机）可以包括类似的模块和 / 或组件。

[0152] 移动的邻近广播接收机 138 可以包括核心客户端模块 115，该核心客户端模块 115 可以是用于处理从附近的无线标识发射机 110 接收的广播消息的软件、指令、例行程序、应用、操作或其它电路。核心客户端模块 115 还可以处理邻近广播接收机 142、138 和中央服务器 120 之间的通信，例如，发送目击消息和从中央服务器 120 接收返回消息。例如，核心客户端模块 115 可以操作成在没有与用户进行交互的情况下，执行诸如上传或发送目击消息之类的操作的后台服务。

[0153] 核心客户端模块 115 可以包括 API 组件 606，所述 API 组件 606 对应于与广播消息和 / 或目击消息有关的应用程序编程接口数据、代码或其它命令。例如，当对从无线标识发射机 110 接收的蓝牙 LE 通告分组进行监听时，邻近广播接收机可以 API 组件 606。再举一个例子，API 组件 606 可以用于注册移动的邻近广播接收机 138，以便接收通知、警报、或者与无线标识发射机 110 相对应的其它通信。核心客户端模块 115 还可以包括用于对接收的广播消息进行处理的授权系统组件 608。例如，移动的邻近广播接收机 138 可以支持针对授权请求的 oAuth 和针对批准的通信合作伙伴的 xAuth。核心客户端模块 115 还可以包括无线装置专用的目击接收机组件 610（用于处理蓝牙 LE、LTE-D、WiFi 和其它通信的组件），操作、管理和维护（或 OA&M）模块 612，无线标识发射机网络管理器组件 614，与存储的前瞻标识符有关的事件注册组件 616，以及目击管理器组件 618。在一个实施例中，事件注册组件 616 可以存储从中央服务器 120 下载的并与特定的无线标识发射机 110 相对应的多个滚动标识符，例如，可以与无线标识发射机 110 在某个时间窗期间广播的可能的滚动标识符相匹配的一组滚动标识符。

[0154] 类似于很多现代的移动设备，移动的邻近广播接收机 138 可以被配置为执行第三方应用（或“apps”），因此可以包括第三方应用模块 116，该第三方应用模块 116 可以执行、管理和以其它方式执行与各种第三方（例如，商家）所提供的应用有关的软件指令和例行程序。例如，第三方应用模块 116 可以从核心客户端模块 115 接收各种数据，以便由各种第三方应用使用。为了说明目的，与在中央服务器 120 中注册的百货商店有关的第三方应用可以被配置为：当该移动的邻近广播接收机 138 的用户进入、保持和 / 或离开该百货商店（例如，该商店的地理围栏）时，从核心客户端模块 115 接收通知。在一个实施例中，为了优化目的，通过第三方应用模块 116 执行的应用或者 apps 可以注册或者以其它方式被配置为：当特定的无线标识发射机位于附近时，或者替代地离开附近时，从核心客户端模块 115 接收通知。例如，应用可以提前在核心客户端模块 115 中进行注册，以接收用于指示特定的无线标识发射机是进入附近、在附近逗留（例如，待在附近并且不移动）还是离开附近的事件通知。

[0155] 移动的邻近广播接收机 138 还可以包括操作系统和平台模块 620，以便执行各种操作和管理电路（例如，短距离信号接收机电路）。具体而言，操作系统和平台模块 620 可以包括：用于使用蓝牙低功耗 (LE) 协议来处理通信的蓝牙 LE 模块 624、用于处理与各种蜂窝网络和类似的远距离无线网络（例如，LTE-D 等）相对应的通信的蜂窝网络模块 626。操作系统和平台模块 620 还可以包括：可以跟踪时间并生成时间戳数据的时间服务组件 628、

可以维持低精度位置数据或者替代地更高精度 GPS（或 A-GPS）位置数据的位置服务组件 630、存储组件 632、以及用于通过 WiFi 或其它无线网络来实现通信的无线广域网 / 无线局域网组件 622。

[0156] 在一个实施例中，核心客户端模块 115 可以向中央服务器请求无线标识发射机标识符的集合（例如，感兴趣列表上的所有发射机的滚动标识符、用于一个用户所拥有的所有发射机的标识符等）。这些集合可以与当前使用中的、以及预期在某个时间段将使用的无线标识发射机相对应。

[0157] 图 7A 描绘了可以在邻近广播接收机（例如，静止的邻近广播接收机或者移动的邻近广播接收机）上实现的实施例方法 700。在判断框 702 中，邻近广播接收机可以判断是否接收到广播消息。例如，邻近广播接收机可以开始对无线标识发射机的广播通告分组或者配对尝试进行监听。如上面所讨论的，在被动模式 / 实施例中，邻近广播接收机可以持续地处于监测模式，或者响应于从中央服务器接收到警报（或者搜索激活消息），开始监听特定的标识符。在发生配对的实施例中，如果邻近广播接收机被设置为在不使用密钥的情况下与任何无线标识发射机相配对，则可以通过使用根据与该无线标识发射机的先前配对所保存的密钥，或者通过使用从中央服务器接收到的密钥，自动地建立配对。如果邻近广播接收机没有接收到广播消息（即，判断框 702 ＝“否”），则邻近广播接收机可以继续执行判断框 702 中的操作。

[0158] 如果邻近广播接收机接收到广播消息（即，判断框 702 ＝“是”），则在方框 704 中，邻近广播接收机可以基于来自所接收的广播消息的信息和其它相关联的数据来生成目击消息。具体而言，该目击消息可以包括 :特定于发送所接收的广播消息的无线标识发射机的标识符（例如，滚动标识符（即，已编码的设备标识符）、MAC 地址、或者可以用于识别该特定的无线标识发射机的其它唯一码。在替代的实施例中，作为配对过程的一部分，可以接收无线标识发射机的标识符。其它相关联的数据可以包括与该广播消息的接收有关的各种信息，例如，该邻近广播接收机接收到该广播消息的时间、位置信息、该邻近广播接收机的标识信息、有关的服务（例如，相关联的商家）和信号强度信息。换言之，邻近广播接收机可以将关于当前状况的数据（例如，时间戳、GPS 坐标、最靠近的基站的小区 ID 等）与广播消息和 / 或无线标识发射机的标识符进行关联。可以用各种类型的数据结构中的任何一种来存储该数据，例如，具有以下各项的数组 :自发生与每一个标识符相对应的目击开始起的、与时间戳和 GPS 坐标相关联的一个或多个标识符。在一个实施例中，该目击消息可以包括可以由中央服务器用来证实邻近广播接收机的标识的认证数据（例如，数字证书或代码）。例如，在该目击消息的元数据之内，邻近广播接收机可以包括仅仅该邻近广播接收机和中央服务器知道的特殊哈希码。

[0159] 在方框 706 中，邻近广播接收机可以例如通过蜂窝（例如，LTE、3G 或 4G 网络）或者如上面参照图 2A-2B 所讨论的其它网络和互联网，向中央服务器发送目击消息。在通过发送目击消息来报告联系事件之后，邻近广播接收机可以迅速地返回以执行判断框 702 中的操作，等待来自无线标识发射机的进一步广播。这使邻近广播接收机能够持续地向中央服务器报告联系事件。

[0160] 图 7B 描绘了可以在邻近广播接收机（例如，静止的邻近广播接收机或者移动的邻近广播接收机）上实施的实施例方法 750。方法 750 可以类似于方法 700，除了邻近广播接

收机可以执行方法750以便对于指示该邻近广播接收机已经遇到的蓝牙机器(MAC)地址所广播的接收的广播消息进行忽略。在一个实施例中,可以响应于接收到由执行上述方法450的无线标识发射机所发送的广播消息,来执行方法750。通过执行方法750,邻近广播接收机可以避免通过目击消息将极度冗余的信息中继给中央服务器,这样可以增加被配置为使用内部电池的邻近广播接收机的电池效率,并且减少不必要的中央服务器工作负载。

[0161] 在判断框702中,邻近广播接收机可以判断是否接收到广播消息。如果邻近广播接收机没有接收到广播消息(即,判断框702=“否”),则邻近广播接收机可以继续执行判断框702中的操作。如果邻近广播接收机接收到广播消息(即,判断框702=“是”),则在判断框752中,邻近广播接收机可以判断其是否已经从相同的蓝牙MAC地址接收到消息。邻近广播接收机可以将所接收的消息中指示的蓝牙MAC地址,与与先前接收的蓝牙MAC地址相对应的存储的蓝牙MAC地址列表进行比较。在一个实施例中,邻近广播接收机可以将所接收的MAC地址与一段时间(例如,一分钟、一小时等)内的其它接收地址进行比较,或者替代地,可以将所接收的MAC地址与先前接收的任何/所有地址进行比较。

[0162] 如果邻近广播接收机已经从相同的蓝牙MAC地址接收到消息(即,判断框752=“是”),则邻近广播接收机可以继续执行判断框702中的操作。但是,如果邻近广播接收机没有从相同的蓝牙MAC地址接收到消息(即,判断框752=“否”),则在方框754中,邻近广播接收机可以存储所接收的消息的蓝牙MAC地址。例如,邻近广播接收机可以将蓝牙MAC地址存储在数据表中,其中该数据表还可以包含接收的时间、以及关于所接收的广播消息的其它信息。在方框704中,邻近广播接收机可以基于来自所接收的广播消息的信息和其它相关联的数据,来生成目击消息。在方框706中,邻近广播接收机可以向中央服务器发送目击消息。当通过发送目击消息来报告了联系事件时,邻近广播接收机可以迅速地返回以执行判断框702中的操作,等待来自无线标识发射机的进一步广播。

[0163] 图8是描绘各种实施例期间的通信的呼叫流程图800。无线标识发射机110可以向邻近广播接收机(例如,移动的邻近广播接收机(如,移动设备、蜂窝电话等)或者如上所述的各种其它邻近广播接收机发送短距离广播消息802(例如,蓝牙LE信号)。广播消息802可以包含针对无线标识发射机的标识符。邻近广播接收机可以将该无线标识发射机的标识符连同任何相关联的数据(例如,时间戳、GPS坐标、小区ID等)作为目击消息804,发送(或者上传)给中央服务器120。中央服务器120可以接收目击消息804,并且存储来自一个或多个邻近广播接收机的多个不同标识符。

[0164] 在一些实施例中,可以在不具有任何用户个人数据的情况下,向中央服务器发送(或者上传)标识符和相关联的数据,以保护隐私。在尝试利用个人移动电话的各种实施例中,电话用户可以选择加入(opt-in),作为移动的邻近广播接收机。但是,如果这些电话用户害怕个人可识别数据也将被发送给中央服务器,则可以拒绝选择加入。因此,在这些个人移动设备(即,移动的邻近广播接收机)上安装的用于上传接收到的标识符的应用,可以禁止传输可标识该移动的邻近广播接收机的个人数据或其它数据。

[0165] 中央服务器120可以从用户设备(例如,终端124或移动设备)接收用户请求806,该用户请求806请求无线标识发射机的位置。可以在登录到与特定的无线标识发射机的账户之后,用户可以发送该请求。例如,各无线标识发射机可以注册有认证用户,使得仅仅在该认证用户登录到安全账户之后,才能够发送针对注册的无线标识发射机的位置的请求

806。

[0166] 在接收到用户请求 806 之后，中央服务器 120 可以对通过目击消息所接收的先前报告的无线标识发射机标识符进行遍历搜索，以发现与所请求的无线标识发射机的标识符的任何匹配。在响应 808 中，可以向用户报告任何匹配。响应 808 还可以包括目击消息 804 中的相关联的数据（例如，时间戳、GPS 坐标、小区 ID）。用户可以使用该相关联的数据来帮助定位或跟踪该无线标识发射机（例如，母亲可以在失踪孩子的无线标识发射机所报告的最新位置寻找这个孩子）。

[0167] 图 9 描绘了用于包括类型或命令段的实施例方法 900。在方框 902 中，邻近广播接收机可以从无线标识发射机（在图 9 中被称为“WIT”）接收广播消息（例如，广播通告分组）。在替代的实施例中，可以通过配对所建立的连接，或者作为配对过程的一部分，来发送该消息。该广播消息可以包含标识符段、以及其它的段或代码（例如，类型段或命令段）。在方框 904 中，邻近广播接收机可以基于所接收的广播消息中的该代码，来执行动作。在各个实施例中，该动作可以包括邻近广播接收机能够执行的任何操作。例如，邻近广播接收机可以基于类型段或者命令段，向消息或标识符分配不同的优先级水平（例如，与来自商店的安全标签相比，儿童安全设备具有更高的优先级）。可以首先将所接收的具有较高优先级的消息或者标识符发送给中央服务器，或者最后从邻近广播接收机的本地记录中删除。

[0168] 邻近广播接收机可以基于类型或者命令段，对广播消息或者标识符进行不同处理。例如，在将消息发送给中央服务器之前，可以将该消息在本地存储某一段时间（例如，各种时间取决于该段的值）。替代地，可以将该消息或标识符、连同诸如时间戳和 GPS 坐标之类的任何相关联的数据，发送给多个位置。

[0169] 再举一个例子，邻近广播接收机可以基于类型和 / 或命令段，发起各种通信。邻近广播接收机可以向特定的 URL 进行报告，发送 SMS 消息，发起电话呼叫，或者建立新的网络连接。在各个实施例中，可以对这些动作中的一些动作进行选择性禁用，以保护用户隐私。

[0170] 在另外的实施例中，邻近广播接收机可以被配置为向另一个网络设备发送另外的段或者其它消息，以便其它网络设备采取某种动作。例如，邻近广播接收机可以将该消息连同相关联的数据转发给中央服务器。中央服务器可以基于该消息中的额外段来执行动作，例如，自动地向用户发送消息，而无需等待用户请求。

[0171] 图 10 描绘了基于与无线标识发射机的邻近性来提供内容的实施例方法 1000。在方框 1002 中，邻近广播接收机可以从无线标识发射机（其在图 10 中称为“WIT”）接收广播消息，其中该广播消息包含识别码和 / 或第二段。在判断框 1005 中，邻近广播接收机可以判断（例如，在邻近广播接收机的存储器中）是否在本地存储了与该识别码和 / 或第二段相关联的动作。如果在本地发现了相关联的动作（即，判断框 1005 ＝是），则在方框 1008 中，邻近广播接收机可以执行该动作。

[0172] 如果在本地没有发现相关联的动作（即，判断框 1005 ＝否），则在方框 1010 中，邻近广播接收机可以向中央服务器发送具有该标识符和 / 或第二段的目击消息。在一个实施例中，邻近广播接收机可以向另一个设备（例如，用户设备）发送消息。在方框 1012 中，邻近广播接收机可以接收指令消息。该指令可以是由中央服务器或者其它设备响应于具有该标识符和 / 或第二段的目击消息而发送的。在方框 1014 中，邻近广播接收机可以基于所接收的指令消息来执行动作，例如，通过进入网页或其它在线资源来访问内容。在替代的实施

例中，邻近广播接收机可以跳过判断框 1005，自动地转到方框 1010 中发送目击消息，或者尝试执行在本地存储的动作。

[0173] 基于邻近性的内容发布系统可以用于多种多样的活动。例如，十多岁的儿童可以随身携带无线标识发射机，这些无线标识发射机指向他们的社交网络网页（例如，Facebook®）。当他们与朋友邻近时，可以快速地在邻近广播接收机上访问这些网页（即，被配置为操作成移动的邻近广播接收机的移动电话）。房地产经纪人可以建立针对房屋的网页，并粘贴到该房屋的路标，无线标识发射机指向该网页，使得开车路过该房屋的任何人都可以访问该信息。商店可以包括具有产品的无线标识发射机，以便提供动态显示，例如，到优惠券的链接、消费者报告或者其它营养信息。如果丢失的狗在其项圈上具有无线标识发射机，则不用为了访问该项圈而尝试与该狗进行格斗，相反，邻近广播接收机可以简单地访问该无线标识发射机并发送消息或者呼叫其主人。

[0174] 各种特征和替代的动作可以使该系统具有灵活的和可扩展的功能。可以稍后添加该功能，这是由于所采取的动作是由可以随时间在邻近广播接收机中更新的应用来控制的。

[0175] 图 11 描绘了用于邻近广播接收机主动地搜索无线标识发射机的实施例方法 1100。在方框 1102 中，邻近广播接收机可以从中央服务器接收具有要搜索的无线标识发射机（其在图 11 中称为“WIT”）的目标标识符、以及一个或多个搜索扇区的警报（或者搜索激活消息）。在该警报中所指示的搜索扇区，可以对应于要搜索的一个或多个扇区。在判断框 1105 中，邻近广播接收机可以判断其是否位于这些搜索扇区中的一个搜索扇区之内。例如，邻近广播接收机可以将来自警报的搜索扇区与其当前 GPS 坐标或小区 ID 进行比较。

[0176] 如果本邻近广播接收机不位于这些搜索扇区中的一个之内（即，判断框 1105 ＝否），则在方框 1108 中，该邻近广播接收机可以继续记录标识符，例如，存储在所接收的广播消息中的、与相应的位置和时间有关的标识符。在一个实施例中，邻近广播接收机可以维持先前的无线标识发射机目击的日志。在该实施例中，不是将来自先前目击的所有数据存储在一个或多个远程服务器（例如，中央服务器）上，而是这些数据可以仍然分布在邻近广播接收机上，直到搜索或者警报变得活动为止。在各个实施例中，邻近广播接收机可以对来自先前目击的数据（例如，无线标识发射机的标识符和该目击的位置和时间（以及任何其它相关联的数据））进行存储。响应于警报，邻近广播接收机可以在数据库中搜索任何记录的目击，以查找存储的设备 ID 与该警报或者激活消息中所提供的目标设备 ID 相匹配的情况。如果存在匹配，则可以向中央服务器发送响应，其中该响应提供与目标设备 ID 相对应的数据，如下所述。

[0177] 如果邻近广播接收机位于这些搜索扇区中的一个之内（即，判断框 1105 ＝是），则在方框 1110 中，该邻近广播接收机可以对所述警报所指示的目标标识符进行监测，例如通过将目标标识符与来自附近的无线标识发射机的广播消息中接收的任何标识符进行比较。在判断框 1113 中，邻近广播接收机可以判断是否检测到目标标识符。如果没有检测到目标标识符（即，判断框 1113 ＝否），则邻近广播接收机可以转到下面所讨论的判断框 1119。

[0178] 如果检测到目标标识符（即，判断框 1113 ＝是），则在方框 706 中，邻近广播接收机可以立即向中央服务器发送目击消息，例如，通过发送包括该目标标识符、时间和位置信息（例如，GPS 坐标）的目击消息。在判断框 1119 中，邻近广播接收机可以判断是否接收

到具有与前一警报不同的扇区的新警报。如果接收到新警报（即，判断框 1119 ＝是），则邻近广播接收机可以通过执行判断框 1105 中的操作，来判断其是否位于这些新扇区中的一个之内。如果没有接收到新警报（即，判断框 1119 ＝否），则邻近广播接收机可以继续在方框 1110 中，对该目标标识符进行监测。

[0179] 在另外的实施例中，邻近广播接收机可以确定其所负责的搜索扇区。例如，已选择加入的蜂窝电话可以安装用于寻找无线标识发射机的跟踪应用。这种应用可以通过监测该蜂窝电话随时间变化的位置，来开发应当在其中进行搜索的扇区列表。随后，该应用可以基于列出搜索扇区的警报消息，来搜索无线标识发射机。因此，在该实施例中，中央服务器可以将标识出要进行搜索的扇区的这些警报（或搜索激活消息）广播或者多播给所有邻近广播接收机，接收机自身可以基于它们当前的位置来判断它们是否应当进入主动搜索模式。

[0180] 图 12 是描绘在各种实施例期间，与警报 1252 有关的通信的呼叫流程图 1250。通常，警报 1252 可以与如上所述的主动搜索有关。可以从诸如终端或移动设备之类的用户设备向中央服务器发送用户请求 806。用户请求 806 可以请求无线标识发射机的位置，并可以包括与该无线标识发射机相关联的代码或者标识符。中央服务器可以向一个或多个邻近广播接收机发送警报 1252（或者搜索激活消息）。警报 1252 可以包含所请求的无线标识发射机的标识符的表示。例如，警报 1252 可以包含安全的滚动标识符，而不提供该无线标识发射机或者其用户的标识。警报 1252 还可以包含能用于与请求的无线标识发射机进行配对的配对数据（例如，共享的密钥或者链接密钥）。

[0181] 如上所述，在一个实施例中，中央服务器可以将该警报发送给邻近广播接收机的某些子集（例如，位于特定的地理扇区之内的邻近广播接收机，其中，所请求的无线标识发射机很可能或者被怀疑位于该地理扇区中）。例如，用户请求 806 可以指示所请求的无线标识发射机的最后已知位置，中央服务器可以向位于该位置附近的扇区之内的邻近广播接收机发送警报 1252。

[0182] 接收到警报 1252 的邻近广播接收机，可以对具有所请求的无线标识发射机的标识符的广播消息 802（例如，广播通告）进行监测。替代地，邻近广播接收机可以尝试与目标无线标识发射机相配对，或者保持对于目标无线标识发射机的配对的接纳。如果邻近广播接收机进入该无线标识发射机的无线通信范围之内，则这些设备可以进行配对。作为该配对过程的一部分，无线标识发射机可以发送包括该设备的标识符信息的短距离无线消息 1254。随后，该邻近广播接收机可以向中央服务器发送目击消息 804。换言之，该邻近广播接收机可以上传相关联的数据，例如，时间戳、GPS 坐标、邻近广播接收机标识、和 / 或与该无线标识发射机或其标识符相关联的小区 ID。中央服务器可以向用户设备发送响应 808，该响应 808 通知用户 :相关联数据来自该邻近广播接收机与所搜索的无线标识发射机的联系。

[0183] 各个实施例可以将图 12 中所描绘的主动搜索方法与上面所讨论的被动搜索模式进行组合。例如，邻近广播接收机可以先前已从该无线标识发射机接收到短距离广播消息 802（例如，蓝牙 LE 无线信号）。该消息 802 和任何相关联的数据（例如，时间戳、GPS 坐标、小区 ID 等）可以本地存储在该邻近广播接收机上，或者被转发给执行跟踪服务的中央服务器。当接收到用户请求 806 时，除了通过发送警报 1252 来发起主动搜索，中央服务器或者邻近广播接收机还可以对与先前从无线标识发射机接收的广播消息 802（例如，广播消息、

包含配对报告的消息等等）和相关联的数据相对应的数据库进行搜索。响应 808 可以包括通过主动搜索得到的所有数据，以及与任何先前的消息 802 相关联的所有数据。

[0184] 在其它实施例中，邻近广播接收机可以被配置为：发送针对接收的所有广播消息的目击消息，而不管是否已经接收到警报消息。换言之，邻近广播接收机可以发送目击消息，以便中央服务器检测是否包括目标标识符，从而检测是否目击到主动搜索所寻找的无线标识发射机。

[0185] 图 13 描绘了中央服务器 120 中的各种模块的图 1300。下文在中央服务器 120 中的模块、组件和 / 或单元的背景下，描述这些各种模块和组件。但是，在各个实施例中，中央服务器 120 可以包括或连接到以下部件：各个计算设备、服务器刀片、或者可以执行与下面描述的各种模块和 / 或组件相关联的操作的其它单元。

[0186] 如上面参照图 1 所描述的，中央服务器 120 可以被配置为接收、存储和以其它方式处理与无线标识发射机相对应的数据。例如，中央服务器 120 可以被配置为：通过互联网 103 与各种设备（例如，邻近广播接收机 142、移动的邻近广播接收机 138、第三方系统 101 和其它支持系统和 / 或服务 102）交换通信。

[0187] 中央服务器 120 可以包括用于执行各种操作以处理数据（例如，从邻近广播接收机 142、138、第三方系统 101 或者其它支持系统和 / 或服务 102 接收的数据）的一些组件 104-109。具体而言，中央服务器 120 可以包括核心组件 108，所述核心组件 108 可以处理目击消息，执行警报或通知引擎模块，处理应用程序编程接口（API）命令，以及与中央服务器 120 中的其它组件交换数据。核心组件 108 可以包括数据层模块 1302，该数据层模块 1302 可以包括用于存储短期数据和第三方特定数据的单元。核心组件 108 还可以包括：用于生成警报消息，以便向邻近广播接收机传输并发起对各种目标无线标识发射机的搜索的警报引擎模块 1304。核心组件 108 还可以包括数据匿名器模块 1306，该数据匿名器模块 1306 可以基于隐私策略或者用户的简档偏好，来生成通用数据、匿名数据或者以其它方式处理的数据。例如，数据匿名器模块 1306 可以从发送给与商店相关联的邻近广播接收机的返回消息中剥离个人信息，从而不向该商店标识该无线标识发射机的消费用户，但仍然将用户位于该商店内的事实报告给该商店。核心组件 108 还可以包括隐私管理器模块 1308，隐私管理器模块 1308 可以维持各个用户的隐私许可信息。例如，隐私管理器模块 1308 可以包括：用户在注册时提供的隐私参数的数据库。

[0188] 核心组件 108 还可以包括：用于帮助组织和管理搜索的搜索管理器模块 1310 和授权系统模块 1312。核心组件 108 还可以包括目击解析器模块 1314，中央服务器 120 可以使用目击解析器模块 1314 来识别与从邻近广播接收机 142、138 接收的目击消息中报告的广播消息相关联的无线标识发射机。核心组件 108 可以包括 API 模块 1316、目击聚合器模块 1318，其中，所述 API 模块 1316 可以包括用于发起操作的功能和接口，所述目击聚合器模块 1318 用于对一段时间上的各种目击消息进行混合，以便以合并的形式向商家、第三方和其它服务进行传输。核心组件 108 还可以包括网络模块 1320，以用于通过互联网来发送和接收与诸如邻近广播接收机 142、138 和第三方系统 101 之类的设备的各种通信。

[0189] 此外，中央服务器 120 还可以包括可存储长期数据（例如，压缩的用户数据、过去的位置信息等等）的数据仓库组件 104。数据仓库组件 104 可以包括用于存储与无线标识发射机的用户有关的信息（例如，用户通过注册网站所提供的简档信息）的各种数据库。数

据仓库组件 104 可以被配置为与核心组件 108 的数据层模块 1302 交换数据。中央服务器 120 还可以包括操作、管理和维护（或 OA&M）组件 105，所述操作、管理和维护（或 OA&M）组件 105 可以处理和 / 或存储与用户门户接入相关联的软件、脚本、工具（例如，软件工具、例行程序等等）。OA&M 组件 105 可以被配置为与核心组件 108 交换数据。

[0190] 中央服务器 120 还可以包括开发者门户组件 106，所述开发者门户组件 106 可以存储开发者账户数据和执行注册、账户管理、以及与开发者（例如，注册以便与无线标识发射机 110 的用户进行交互的供应商或商家）相关联的警报（或通知）管理例行程序。中央服务器 120 还可以包括用户门户组件 109，所述用户门户组件 109 可以存储用户账户数据，执行注册、账户管理和与用户（例如，与无线标识发射机相关联的人员）相关联的搜索例行程序。用户门户组件 109 和开发者门户组件 106 可以被配置为与核心组件 108 的授权系统模块 1312 交换数据。中央服务器 120 还可以包括滚动标识符（或 ID）解析器组件 107，所述滚动标识符（或 ID）解析器组件 107 可以存储与无线标识发射机 110 相关联的出厂密钥，并且执行操作、软件或例行程序以便将所接收的目击消息中的加密、编码、滚动或以其它方式模糊的标识信息与附属的用户数据进行匹配。滚动标识符（或 ID）解析器组件 107 可以被配置为与核心组件 108 的目击解析器模块 1314 交换数据。

[0191] 在各个实施例中，参照图 13 所描述的模块和组件（例如，滚动 ID 解析器组件 107）可以由软件指令、应用、例行程序、线程、电路或硬件单元来执行或者以其它方式启用。

[0192] 图 14 描绘了在各种实施例中使用的无线标识发射机注册过程。通常，在中央服务器对广播消息进行处理之前，中央服务器可能需要无线标识发射机和它们的用户在该中央服务器中进行注册。例如，在可以发起与无线标识发射机有关的任何跟踪、搜索或者其它基于位置的活动之前，中央服务器必须能够确定与各个无线标识发射机相关联的用户分布在全世界。注册可以在无线标识发射机在广播消息中发送的标识符、这些无线标识发射机和它们的用户之间创建链接。例如，为了向丢失了孩子的家长发送已找到该孩子的通知，则必须将中继的模糊的（或者编码的）标识符与如与注册的用户账户有关的所存储的、指示该家长的蜂窝电话号码的账户信息进行匹配。

[0193] 具体而言，通过注册，可以在每一个无线标识发射机和中央服务器之间，对定时装置（即，计数器）进行同步。使用这种计数器，无线标识发射机和中央服务器可以分别对标识符进行编码（或滚动）和解码，保持与无线标识发射机（和其用户）相关联的标识被隐藏和私有。用于对这种定时装置或计数器进行同步的最恰当时间，可以是在如下所述的设备注册和 / 或账户创建过程期间。为了图 14，将移动设备（例如，智能电话）描述成 :被用户用于执行账户创建和注册操作（例如，该移动设备访问 web 门户以在中央服务器中进行注册等）。但是，连接到互联网并且能够通过注册 web 门户或网站与中央服务器交换通信的任何计算设备可以是相关的。

[0194] 在方框 1402 中，用户的移动设备（例如，iPhone、Android、平板设备等等）可以安装用于无线标识发射机的应用。这种应用（或者“app”）可以在移动设备的处理器上执行成后台服务，或者替代地可以被激活以便由用户进行选择性使用。如贯穿本说明书所描述的，这种应用可以使移动设备能处理来自附近的无线标识发射机的短距离广播消息，例如，通过将接收的信号识别成广播消息，并且在响应中，将具有位置信息的目击消息中继给中央服务器。在方框 1404 中，移动设备可以发送具有用户信息（例如，设备标识或者“设

备 ID”）的注册请求。可以通过与中央服务器控制或者以其它方式可访问的 web 门户、web 站点或者 web 服务器进行互联网通信，将该注册请求发送给中央服务器。换言之，移动设备可以调用该注册过程，或者通过提供设备 ID（设备 ID）和其它信息的已安装的 app 来提供用户信息（例如，设备 ID），中央服务器可以使用这些其它信息将注册请求绑定到帐户。例如，用户的移动设备可以访问注册网站，从用户接收输入，将该用户输入作为数据发送给注册网站，以便中央服务器使用，如上面参照图 13 所描述的。在一个实施例中，用户信息可以包括关于该用户的个人信息，例如，姓名、地址、联系信息（如，社交网络站点、手机号、电子邮件地址、电话号码等）、年龄和其它人口统计信息，以及关于无线标识发射机和与该用户的账户相关联的邻近广播接收机的识别信息。例如，发送给中央服务器的用户信息可以包括无线标识发射机上的序列号和 / 或移动设备响应于使用方框 1402 中的操作而安装的应用所产生的确认码。用户信息还可以包括偏好信息，例如，用户偏好的零售商店、产品线、以及吃饭或消费的区域。该用户信息还可以包括用于指示中央服务器如何分发或使用个人信息的隐私许可。在一个实施例中，用户可以注册成匿名用户，使得中央服务器不存储关于这些用户的任何识别信息。例如，可以注册账户，该账户链接到非标准 (non-descript) 邮政信箱、一次性使用的蜂窝电话号码或者不直接地标识该账户的用户或者持有者的其它联系信息。这对于可以选择使用中央服务器所提供的服务，但关注泄漏的隐私信息或识别信息的那些人来说可能是重要的。在方框 1412 中，用户的移动设备可以存储账户信息，例如，来自中央服务器的认证信息（例如，代码、消息）或者与拥有的无线标识发射机相关联的设备 ID。

[0195] 在方框 1406 中，中央服务器可以接收用户信息，以进行账户注册。在方框 1408 中，中央服务器可以为该用户注册一个账户。例如，中央服务器可以在所有注册用户的数据库中存储该用户的信息，其包括所提供的设备标识。在方框 1410 中，中央服务器可以向用户提供账户创建信息。该账户创建信息可以包括认证码，或者用户的移动设备可以存储以便未来使用的其它信息。例如，中央服务器可以在用户的移动设备可访问的网站上，显示账户创建的确认，或者替代地可以向用户的移动设备发送确认信号、文本消息、电子邮件或其它通信。

[0196] 在方框 402 中，无线标识发射机启动（例如，响应于用户插入电池）。当无线标识发射机启动时，可以对随机数或计数器值进行初始化。例如，无线标识发射机可以开始对表示时间流逝的值从零值开始进行递增。在方框 1413 中，无线标识发射机可以广播包括编码的（或者滚动的）标识符的消息（即，广播消息）。例如，无线标识发射机可以开始每几秒钟发送一次广播消息。无线标识发射机可以使用下面所描述的实施例方法来生成滚动标识符。通常，该广播消息可以包括 :具有通过执行伪随机函数所产生的数据的有效载荷。例如，无线标识发射机可以执行伪随机函数，以基于该无线标识发射机的设备 ID、随机数或计数器值和密钥、种子或者只有该无线标识发射机和中央服务器才知道的其它值的输入值，来生成编码数据。在一个实施例中，该伪随机函数可以是多项式时间可计算函数，所述多项式时间可计算函数可以使用只有无线标识发射机和中央服务器才知道的随机选择的种子值，使得该伪随机函数可以与在相同域上规定的随机函数无区别地计算，其中该随机函数与所述伪随机函数具有相同的输出范围。在一个实施例中，可以将键控的哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 用作伪随机函数。

[0197] 在一个实施例中，可能需要在移动设备使用方框 1404 中的操作来开始注册过程的时间之中的预先定义数量的秒之内，对无线标识发射机进行激活。换言之，一旦无线标识发射机开始对其随机数或计数器值进行递增，用户就必须在某个时段内向中央服务器进行注册。这使得当中央服务器尝试确定无线标识发射机在注册期间的随机数或者计数器值时，仅仅按照某个数量的值进行尝试。

[0198] 在一个实施例中，无线标识发射机可以通过调整广播消息的有效载荷之中的数据来指示初始广播。例如，无线标识发射机可以改变广播消息中的一个比特，中央服务器可以将该比特识别成指示该无线标识发射机的初始化时间段。如果在有效载荷中存在初始化指示符，则中央服务器可以通过避免与中央服务器查寻数据表中的已注册的（或者识别的）无线标识发射机相对应的有效载荷进行比较，来加快所接收的有效载荷和存储的有效载荷之间的比较。

[0199] 在方框 1414 中，用户的移动设备可以接收该广播消息。换言之，基于所安装的应用（或 app），移动设备可以充当成移动的邻近广播接收机。安装的应用（例如，使用方框 1402 中的操作所安装的 app）可以响应于通过注册请求而发起向中央服务器的注册操作，等待接收该广播消息。在方框 1416 中，移动设备可以发送该无线标识发射机的滚动标识符和其它信息（例如，存储的设备 ID 和认证信息）。在一个实施例中，移动设备可以从所接收的广播消息中提取编码的信息（例如，通过使用文本比较和 / 或解析操作）。例如，移动设备可以执行最高有效位操作。

[0200] 在方框 1418 中，中央服务器可以接收具有编码的信息、以及认证信息和设备 ID 的消息。在方框 1420 中，中央服务器可以对认证信息（例如，其位于从移动设备接收的消息之中）进行验证。具体而言，中央服务器可以将该认证信息与在方框 1408-1410 中的操作所生成的信息进行比较。在方框 1422 中，中央服务器可以使用该设备 ID 和可能的随机数或计数器值，生成一组滚动标识符。中央服务器可以将该集合中的编码的标识符与从移动设备接收的滚动标识符进行比较。在一个实施例中，中央服务器可以通过使用（例如，上面所描述的）伪随机函数、连同设备 ID 和多个随机数或计数器值，来计算一组编码的数据。例如，中央服务器可以使用与无线标识发射机共享的种子、该移动设备所指示的设备 ID、以及多个随机数或计数器值（其从 0 开始）来执行伪随机函数。在方框 1424 中，当中央服务器将所接收的滚动标识符与所生成的集合中的一个滚动标识符相匹配时，中央服务器可以存储有关的随机数或计数器值以及与该 WIT 有关的时间。中央服务器可以使用用于生成该匹配的滚动标识符的随机数或计数器值，以便与在该无线标识发射机上运行的随机数或计数器进行同步。在一个实施例中，中央服务器可以存储用于将该无线标识发射机描述成已成功注册和 / 或同步的指示符。在可选框 1426 中，中央服务器可以随后向用户发送注册结果消息（例如，通过向移动设备发送消息）。该注册结果消息可以指示中央服务器是否能够将所接收的编码标识符与生成的标识符进行匹配。在可选框 1428 中，移动设备可以接收该注册结果消息。在一个实施例中，该注册结果消息指示该注册过程失败（例如，该移动设备所接收的接收广播消息并不与该用户的无线标识发射机相对应），该移动设备可以通过接收和中继另一个广播消息，来重新尝试注册。

[0201] 上面所描述的操作（特别是在方框 1413-1424 之中），假定与无线标识发射机对随机数或计数器值进行递增（或更新）所需要的时间相比，各种设备执行的消息处理操作以

及任何传播延迟可以更小。这确保了无线标识发射机和中央服务器处的随机数或计数器值相差不超过 1。

[0202] 图 15A 描绘了用于中央服务器对从邻近广播接收机接收的目击消息进行处理的实施例方法 1500。如上所述，中央服务器可以被配置为使用各种模块、组件、电路和软件来处理目击消息。在判断框 1502 中，中央服务器可以判断是否接收到目击消息。中央服务器可以对接收电路、缓冲区、队列或其它指示符进行评估，以确定从各种设备（例如，邻近广播接收机）接收到消息的时间。在一个实施例中，中央服务器可以使用如上所述的网络模块来判断是否接收到目击消息。通常，可以通过远距离通信来接收目击消息，例如，在互联网上通过蜂窝网络来发送的分组。如果中央服务器没有接收到目击消息（即，判断框 1502 ＝“否”），则中央服务器可以继续执行判断框 1502 中的操作。

[0203] 如果中央服务器接收到目击消息（即，判断框 1502 ＝“是”），则在方框 1504 中，中央服务器可以基于该目击消息，来识别无线标识发射机信息、邻近广播接收机信息和相关联的数据。中央服务器可以对所接收的目击消息中的各种数据和信息段进行评估、解析、或者以其它方式使这些数据和信息段变得可访问。例如，中央服务器可以对该目击消息进行解析，以便识别所包括的来自无线标识发射机的广播消息。再举一个例子，中央服务器可以识别与无线标识发射机标识（即，滚动标识符）相对应的编码数据、邻近广播接收机标识信息（例如，接收机 ID)、位置信息、时间戳信息、传感器数据（例如，加速计传感器数据等等）、与邻近广播接收机相关联的应用（或 app) 的标识符（例如，安装的应用的列表、用于在该邻近广播接收机上执行的有关 app 的标识符等等）。在一个实施例中，中央服务器可以使用如上所述的目击解析器模块，来执行方框 1504 的操作。

[0204] 在方框 1506 中，中央服务器可以基于目击消息中的滚动标识符，来获得无线标识发射机标识。中央服务器可以执行操作，以便对该滚动标识符进行解码、解扰、解密、或者以其它方式使该滚动标识符变得可访问。例如，中央服务器可以执行操作，以应用密钥或解码算法，来获得该无线标识发射机的标识。在一个实施例中，方框 1506 的操作可以由中央服务器通过如上所述的滚动 ID 解析器组件的方式来执行。例如，中央服务器可以使目击解析器模块与滚动 ID 解析器组件交换数据，以获得解码的无线标识发射机标识符。下面将参照图 26 来描述用于基于包括滚动标识符的目击消息来识别无线标识发射机的实施例操作。

[0205] 在方框 1508 中，中央服务器可以基于所获得的无线标识发射机标识来获取无线标识发射机用户信息。例如，中央服务器可以获取与该无线标识发射机有关的用户账户信息，例如，人口统计信息、用于指示先前行为（例如，旅行路径、位置历史等等）的存储的数据。在一个实施例中，方框 1508 的操作可以由中央服务器通过如上所述的授权系统模块的方式来执行。例如，中央服务器可以使授权系统模块与用户门户组件交换无线标识发射机标识信息，以获得如保存在用户注册数据库中的用户信息。

[0206] 在方框 1510 中，中央服务器可以基于所识别的邻近广播接收机信息，来获取邻近广播接收机标识信息，例如，邻近广播接收机用户信息和有关的服务。例如，中央服务器可以获取与发送所接收的目击消息的邻近广播接收机相关联的商家标识、该邻近广播接收机注册参与的跟踪服务、以及与该邻近广播接收机有关的任何其它有关信息。中央服务器可以基于目击消息中的信息，获取与有关的邻近广播接收机的用户有关的电子邮件地址、MAC 地址、电话号码和其它联系信息。例如，中央服务器可以确定与邻近广播接收机相关联的用

户联系信息（其中该信息可以用于来自中央服务器的后续传输），例如，电子邮件或者指示与感兴趣物品的邻近性的 SMS 文本消息。在一个实施例中，中央服务器可以确定智能电话（其被配置为执行移动的邻近广播接收机的操作）的用户的标识。在一个实施例中，方框 1510 的操作可以由中央服务器通过如上所述的授权系统模块的方式来执行。例如，中央服务器可以使授权系统模块与开发者（或用户）门户组件交换邻近广播接收机信息，以获得关于有关的注册服务（例如，商家、商店、供应商、服务等等）的信息，如保存在开发者注册数据库中的信息。

[0207] 在可选框 1511 中，中央服务器可以对目击消息进行认证。基于所接收的目击消息中的认证信息，中央服务器可以执行认证操作，其中认证操作用于确认该目击消息来自于已知或者有效的邻近广播接收机的合法性。如上所述，目击消息可以包括 :能够对有效的邻近广播接收机的标识进行确认的数据（例如，密码、证书或哈希数据）。由于第三方可以尝试欺骗与注册的服务相关联的邻近广播接收机（例如，恶毒的垃圾邮件发送者可以通过发送欺诈的目击消息，尝试模仿商家的商店邻近广播接收机），中央服务器可以核查认证信息，确认目击消息中的信息是有用的，并且与注册的服务（例如，注册的商家、有效的开发者、或者部署合法的邻近广播接收机的其它方）有关。例如，中央服务器可以将目击消息中的模糊的报头信息（其与在中央服务器中建立的商家有关），检测成注册的开发者。当目击消息不包括中央服务器所预期的认证信息时（例如，位于某个建筑物中的所有邻近广播接收机都拥有的特殊编码）或者确实包括与中央服务器中存储的信息不匹配的认证信息时，中央服务器可以忽略该目击消息和其包括的所有信息。例如，中央服务器可以对具有过期或者不完整认证信息的目击消息进行忽略，或者替代地将其存储在针对潜在欺骗的邻近广播接收机的列表中。

[0208] 在可选框 1512 中，中央服务器可以基于所获得的和 / 或获取的数据，生成哈希的数据。在一个实施例中，可选框 1512 的操作可以由中央服务器通过如上所述的数据匿名器模块的方式来执行。在方框 1514 中，中央服务器可以基于目击消息，结合无线标识发射机标识来存储数据。例如，中央服务器可以将来自目击消息的识别的相关联数据存储在与该无线标识发射机的解码的标识有关的数据库中。在一个实施例中，方框 1514 的操作可以由中央服务器通过如上所述的数据层模块的方式来执行。

[0209] 图 15B 描绘了用于中央服务器对从邻近广播接收机接收的目击消息进行处理的实施例方法 1550。方法 1550 类似于上面所描述的方法 1500，除了中央服务器可以执行方法 1550 来发送消息，以便由在用户携带的移动设备上执行的第三方应用进行使用。如上所述，中央服务器可以向诸如与用户相关联的移动设备之类的各种接收者发送诸如返回消息、警报（或者搜索激活消息）之类的各种消息。例如，中央服务器可以向用户的平板计算机、智能电话、无线接收机设备或者其它计算设备发送消息。接收者还可以包括在移动设备上执行的应用或者 app。在一个实施例中，中央服务器还可以向其它第三方接收者或设备（例如，注册的服务，其可以包括 EMT、消防、当地警方、零售商店、商业计算设备和广告服务器）发送消息。

[0210] 可以将中央服务器响应于接收到目击消息而发送的消息进行发送，以便向诸如用户所携带的移动电话或者移动的邻近广播接收机之类的设备告知已知无线标识发射机的邻近的位置。例如，当诸如零售商店中的静止的邻近广播接收机之类的邻近广播接收机对

来自与用户相关联的无线标识发射机的广播消息进行中继时，中央服务器可以通过向该用户的移动设备发送回用于指示该用户位于该商店的接收机设备附近的消息，来进行响应。此外，在该用户的设备上运行的第三方应用，可以使用该消息中的信息。例如，在用户的智能电话上运行的零售商店 app，可以接收该用户已移动到位于零售商店建筑物的附近范围内的显示区域的附近范围之内。在各种其它实施例中，第三方应用可以用于跟踪所拥有的、与无线标识发射机相关联的物品。例如，当用户位于搜索丢失儿童的附近时，特定的第三方应用可以播放铃声。

[0211] 在判断框 1502 中，中央服务器可以判断是否接收到目击消息。如果中央服务器没有接收到目击消息（即，判断框 1502 ＝“否”），则中央服务器可以继续执行判断框 1502 中的操作。如果中央服务器接收到目击消息（即，判断框 1502 ＝“是”），则在方框 1504 中，中央服务器可以基于该目击消息，识别无线标识发射机信息、邻近广播接收机信息和相关联的数据。在方框 1506 中，中央服务器可以基于目击消息中的滚动标识符，来获得无线标识发射机标识。在方框 1508 中，中央服务器可以基于所获得的无线标识发射机标识来获取无线标识发射机用户信息。在方框 1510 中，中央服务器可以基于所识别的邻近广播接收机信息，来获取邻近广播接收机标识信息，例如，邻近广播接收机用户信息和有关的服务。在可选框 1512 中，中央服务器可以基于所获得的和 / 或获取的数据，生成哈希的数据。在方框 1514 中，中央服务器可以基于目击消息，结合无线标识发射机标识来存储数据。

[0212] 在判断框 1552 中，中央服务器可以判断是否允许第三方应用（或 app）获得邻近广播接收机信息。换言之，基于在中央服务器中存储的与该无线标识发射机的用户相关联的数据，中央服务器可以检测任何注册的服务或者与该用户的设备相关联的第三方应用。例如，中央服务器可以对数据库信息进行评估，以识别该用户已经在他 / 她的智能电话上安装了与零售商店相对应的第三方应用。该邻近广播接收机信息可以包括邻近广播接收机标识（例如，ID 代码或者标识符）和该邻近广播接收机的用户标识。在一个实施例中，中央服务器可以基于第三方的开发者权利（例如，当该第三方注册成开发者或者注册的服务时，所指示的权利），或者替代地基于在中央服务器中的该用户简档里存储的该用户的许可设置，来识别是否允许第三方应用使用该信息。在一个实施例中，中央服务器可以使用在所接收的目击消息中提供的应用标识信息，来判断用户的设备上的该第三方应用是否可以接收邻近广播接收机信息。例如，目击消息可以包含如下应用的指示符（例如，app ID）：该应用与该目击消息相对应从而允许从中央服务器接收任何邻近广播接收机信息。

[0213] 如果不允许第三方 app 获得邻近广播接收机信息（即，判断框 1552 ＝“否”），则在方框 1556 中，中央服务器可以向用户的设备发送只包括无线标识发射机标识信息和来自该目击消息的相关联的数据的消息。例如，中央服务器发送的消息可以包括：所获得的无线标识发射机标识、用户信息、时间戳数据、以及来自目击消息的位置信息。如果允许第三方 app 获得邻近广播接收机信息（即，判断框 1552 ＝“是”），则在方框 1554 中，中央服务器可以向用户的设备发送：包括无线标识发射机标识信息、邻近广播接收机信息和来自目击消息的相关联数据的消息。例如，中央服务器向用户的智能电话发送的消息可以包括：所获得的邻近广播接收机标识的指示符（例如，序列码、群组从属关系、商户类别等等）。随后，中央服务器可以继续执行判断框 1502 中的操作。在一个实施例中，中央服务器可以使用报警引擎模块（例如，上面参照图 13 所描述的），来发送和 / 或生成用于向各种设备传输的消

息。

[0214] 图 16 描绘了一种实施例呼叫流程图 1600，该图描绘了无线标识发射机、邻近广播接收机和中央服务器之间的通信。如上所述，无线标识发射机可以定期地通过短距离无线装置来发送短距离广播消息 802。当位于广播消息 802 的信号范围之内时，邻近广播接收机可以使用类似的短距离无线装置来接收广播消息 802。邻近广播接收机可以对广播消息 802 进行处理，并且有关数据可以作为目击消息 804 中继给中央服务器。在一个实施例中，目击消息 804 可以包括该广播消息、该邻近广播接收机和 / 或该无线标识发射机的标识信息、该邻近广播接收机不能解码的加密信息、以及与广播消息 802 的接收有关的其它信息。在一个实施例中，可以通过各种无线或有线网络来发送目击消息 804，其中这些无线或有线网络可以被配置为通过互联网协议进行通信。

[0215] 中央服务器可以对目击消息 804 进行接收和处理。当中央服务器基于目击消息中的信息（例如，请求响应的元数据、目击消息涉及需要接收升级的固件的无线标识发射机等等）来确定目击消息 804 需要响应时，中央服务器可以生成返回消息 1602，并向邻近广播接收机进行发送。在各个实施例中，返回消息 1602 可以包含配置信息、用于描述无线标识发射机的标识信息、或者如上所述的其它数据。邻近广播接收机可以对返回消息 1602 进行接收和处理。基于返回消息 1602 中的数据，邻近广播接收机可以可选地向无线标识发射机发送消息 1604，其中该消息 1604 可以包含配置信息和来自中央服务器的其它数据。无线标识发射机可以使用如上面参照图 4 所描述的操作，选择性地接受诸如消息 1604 之类的传输。

[0216] 作为另一种选项，邻近广播接收机可以基于返回消息 1602，向本地服务器发送消息 1606。消息 1606 可以包含无线标识发射机标识信息、配置信息、软件例行程序和来自返回消息 1602 的各种其它数据，以便由本地服务器进行存储、处理和以其它方式使用。基于消息 1606，本地服务器可以转而向邻近广播接收机发送可选的响应消息 1608，所述可选的响应消息 1608 可以包括软件指令、配置数据、或者响应于接收到消息 1606 而生成的其它数据。

[0217] 在一个实施例中，中央服务器还可以直接向本地服务器（没有示出）发送包括配置信息和其它数据的消息。例如，来自邻近广播接收机的目击消息 804，可以向本地服务器提供联系信息，其中中央服务器可以使用该联系信息进行后续通信。

[0218] 图 17 描绘了用于中央服务器通过向处于特定扇区中的邻近广播接收机发送激活消息，来激活搜索的实施例方法 1700。在方框 1702 中，中央服务器可以接收针对特定的无线标识发射机（即，目标无线标识发射机）的邻近性信息的请求（例如，上面所描述的用户请求）。换言之，请求者可能想要定位目标无线标识发射机。在方框 1704 中，中央服务器可以识别一个或多个初始扇区，以搜索该目标无线标识发射机。可以通过多种方式来识别这些初始扇区。例如，该请求可以包括位置（例如，目标无线标识发射机的上一次已知位置），中央服务器可以识别该位置周围的扇区。替代地，目标无线标识发射机可以具有与其相关联的扇区，这些扇区是基于先前跟踪尝试或根据先前的目击而从邻近广播接收机接收的数据（例如，GPS 坐标、小区 ID）。

[0219] 在方框 1706 中，中央服务器可以基于所识别的扇区来向邻近广播接收机发送警报。例如，中央服务器可以向当前位于所识别的扇区内的邻近广播接收机发送警报，其中这

些邻近广播接收机频繁地在这些扇区中移动（例如，已知进入这些扇区的移动邻近广播接收机），这些邻近广播接收机位于这些扇区附近或者先前曾位于这些扇区附近、和／或预测这些邻近广播接收机未来将处于这些扇区之内。在各个实施例中，该警报可以指示中央服务器已发起或者激活了一个搜索。在替代的实施例中，该警报消息可在单独的服务器或者其它网络位置上获得，邻近广播接收机可以对维持该警报的URL进行定期地查询。例如，蜂窝电话通常定期地对各种各样数据（例如，时钟和其它网络设置）进行核查，所以邻近广播接收机可以被配置为也用相同的方式或者用于这些其它数据核查的相同连接上，对警报进行核查。在一个实施例中，中央服务器可以发送这种警报消息，使得接收的邻近广播接收机可能不能够识别目标无线标识发射机。例如，该警报消息可以包括只有中央服务器才能够访问的、用于目标无线标识发射机的编码的、加密的或者以其它方式模糊的标识符，因此对于除了请求者之外的所有邻近广播接收机和其它设备保持匿名搜索。在另一个实施例中，当移动的邻近广播接收机被配置为不管该移动的邻近广播接收机是否已经接收到任何警报或者搜索激活消息，都对从目标无线标识发射机接收到的广播消息进行自动中继时，方框1706中的操作可以是可选的。例如，移动的邻近广播接收机可以向中央服务器发送目击消息，其中该目击消息包括从附近范围内的无线标识发射机接收的任何广播消息。

[0220] 在发送该警报之后，在判断框1710中，中央服务器可以判断是否通过目击消息接收到目标无线标识发射机的邻近度的报告。换言之，中央服务器可以旁观以接收用于指示该目标无线标识发射机位于邻近广播接收机的附近从而已定位该目标无线标识发射机的目击消息，或者搜索到该目击消息。中央服务器可以对接收的目击消息中的滚动标识符进行解码、解密或以其它方式访问，并判断其是否与目标无线标识发射机的标识相匹配。如果接收到目标无线标识发射机邻近度的报告（即，判断框1710＝“是”），则在方框1712中，中央服务器可以向请求者发送具有从邻近广播接收机接收到的任何数据的响应。只要警报仍然有效，就可以继续如下过程：在判断框1710中旁观并且从邻近广播接收机接收目击消息（或者其它位置报告），并在方框1712中向一个或多个请求者发送响应（例如，直到找到该儿童，并且请求机构取消了该警报为止），或者直到中央服务器停止接收该目标无线标识发射机的邻近报告为止（即，判断框1710＝否）。

[0221] 在判断框1714和1716中，中央服务器可以被配置为调整搜索扇区，以扩展该搜索区域，将搜索区域从一个扇区切换到另一个扇区，以跟踪移动的目标无线标识发射机，并响应于用于移动、扩展或者关注从请求者或机构接收的搜索的命令。用此方式，中央服务器可以通过向邻近广播接收机通知，来主动地调整搜索扇区，以便增加可以对设备进行定位和跟踪的可能性。在判断框1714中，中央服务器可以判断搜索持续时间是否超过时间门限，是否存在报告的位置（其指示该目标无线标识发射机正在离开该扇区），或者是否接收到搜索扇区命令。只要搜索持续时间或者自上一次报告以来的持续时间小于预先定义的时间门限，则目标无线标识发射机没有移出该搜索扇区和／或没有命令中央服务器调整该搜索区域（即，判断框1714＝否），中央服务器就可以在判断框1710中，继续旁观并且通过目击消息来接收邻近度报告。

[0222] 在一个实施例中，如果中央服务器通过目击消息（例如，请求的无线标识发射机已与邻近广播接收机配对，或者处于邻近广播接收机的附近范围之内的指示），未能接收到或停止接收关于目标无线标识发射机的邻近度报告（即，判断框1710＝否），则在判断框

1714 中，中央服务器可以判断自从搜索开始或者上一次接收的报告以来的时间是否超过预先定义的门限。请求者或者机构可以在对搜索进行激活的时刻对该预先定义的门限进行设置（例如，依据可疑的传输模式）。例如，可以在儿童的最后一次已知位置周围的扇区中对该搜索进行激活，但是，如果怀疑诱拐者是步行，则可以将该搜索配置为扩展到位于 15 分钟之内，或者如果怀疑诱拐者是乘车，则可以将该搜索配置为扩展到位于 5 分钟之内。以此方式，中央服务器可以对该搜索区域进行自动地扩展。如果中央服务器确定自从发起该搜索或者接收到上一次位置报告以来的预设置持续时间已经到期（即，判断框 1714 ＝是），则在方框 1716 中，中央服务器可以识别新的扇区，以搜索该目标无线标识发射机，在方框 1706 中，可以在这些新扇区中发送新的警报，或者以其它方式使该新警报可用于邻近广播接收机。以此方式，搜索可以扩展到涵盖更大的区域，以适应潜在的移动诱拐者。

[0223] 在另一个实施例中，可以基于目标无线标识发射机的移动，对搜索进行扩展。例如，在一个正在进行的搜索中，中央服务器可以从一个或多个邻近广播接收机接收目击消息。基于这些消息中的时间和位置，中央服务器可以假定目标无线标识发射机正在特定方向上移动，例如沿着公路向下移动，并且增加行进方向中的扇区以预期该目标无线标识发射机的未来位置。因此，在判断框 1714 中，中央服务器可以确定何时接收的报告位置（或者邻近性）指示目标无线标识发射机正在离开该扇区。这可以通过将在判断框 1710 中接收的位置或邻近性序列与数字地图进行比较，以估计行进的方向和速度来实现。当中央服务器确定已停止接收位置或者邻近报告，目标无线标识发射机正移出当前搜索扇区之外（即，判断框 1714 ＝是），则在方框 1716 中，中央服务器可以识别要搜索的新扇区，在方框 1706 中，可以在这些新扇区中发送新警报，或者以其它方式使该新警报可用于邻近广播接收机。在方框 1716 中，所识别的新扇区可以是沿着中央服务器所估计的运动方向的一个或多个扇区。以此方式，可以使搜索按照顺序地从一个扇区切换到另一个扇区，以便跟踪正在移动的无线标识发射机。

[0224] 在另一个实施例中，中央服务器可以被配置为：接收用于对搜索区域进行扩展、切换或者关注的命令，其中这些命令可以在判断框 1714 中进行接收。当中央服务器接收到用于对搜索进行扩展的命令时（即，判断框 1714 ＝是），则中央服务器可以在方框 1716 中识别与所接收的命令相符合的用于搜索目标无线标识发射机的新扇区，随后在方框 1706 中，可以发送与这些新扇区有关的新警报，或者以其它方式使该新警报可用于邻近广播接收机。用此方式，请求者或者搜索机构可以通过中央服务器来动态地调整该搜索，以便调查线索和目击者报告。

[0225] 替代地，可以对搜索进行逐渐地扩大。中央服务器初始时可以识别一个或者仅仅几个扇区，如果没有定位到目标无线标识发射机，则中央服务器可以识别要警报的额外扇区。例如，如果一个儿童在放学后失踪，则可以将该警报发送到该学校的扇区中的邻近广播接收机，随后发送到邻近扇区中的设备，随后发送到城镇的其余地区中的设备，随后甚至发送到邻近城镇中的设备以及之外的地方（如果需要的话）。

[0226] 按扇区进行搜索可以节省网络资源和允许更高效的响应。已经选择加入作为邻近广播接收机的蜂窝电话用户可以不需要担心其它城市或者州中的无成果的搜索（例如，加利福尼亚电话搜索在亚特兰大丢失的无线标识发射机）。在亚特兰大放学后失踪的儿童，不可能仅仅几个小时就在这个国家穿梭到加利福尼亚。但是，随着搜索过程和时间流逝，可以

根据需要对扇区进行增加，并且对搜索范围进行扩展。

[0227] 各种实施例可以包括用于保护所涉及的每一方的隐私的一个或多个特征。在各个实施例中，邻近广播接收机可以不向该邻近广播接收机的用户报告关于搜索的任何事情（例如，蜂窝电话可以不向用户暴露目标无线标识发射机的标识符、请求者的标识、是否已经找到目标无线标识发射机、或者甚至搜索正在进行）。在各个实施例中，可以通过将任何邻近广播接收机的个人信息排除在向中央服务器发送的任何数据之外，来对任何这种信息进行保护。

[0228] 图 18 描绘了用于中央服务器判断邻近广播接收机是否丢失无线标识发射机的实施例方法 1800。在中央服务器中，邻近广播接收机可以与该无线标识发射机相关联。例如，邻近广播接收机可以是用户的智能电话，其与某个资产（例如，钱包、皮包、箱包、医药包、衣服等等）中的无线标识发射机相关联。响应于未能从与特定的无线标识发射机相关联的邻近广播接收机接收到目击消息，则中央服务器可以被配置为发送消息（例如，警告），其中该消息指示该无线标识发射机（以及其连接到的对象）丢失、不存在、遗忘或者以其它方式与该邻近广播接收机不邻近。该实施例方法 1800 可以有利于联系若干资产（例如，财产、宠物和儿童）。例如，当一个孩子跑离家长时，家长的邻近广播接收机可能不再接收到来自该孩子的无线标识发射机的广播消息。结果，家长的邻近广播接收机可以不向中央服务器发送目击消息，并且中央服务器可以确定该孩子已丢失或者走远。

[0229] 在方框 1802 中，中央服务器可以注册邻近广播接收机和无线标识发射机之间的关系（例如，通过将信息存储在数据库中）。在各个实施例中，每一个邻近广播接收机和无线标识发射机可以涉及多个关系。另外，可以基于用户通过注册 web 门户向中央服务器的输入数据（例如，用户可以访问网站，指示他 / 她的全部无线标识发射机），来存储这种关系信息。在这种注册期间，中央服务器可以提示用户来提供中央服务器应当发送消息的状况（当无线标识发射机丢失时，或者以其它方式位于该邻近广播接收机的附近范围之外时）。例如，用户可以输入中央服务器所存储的配置数据，其中该配置数据指示如果在一天的某些小时之间，该邻近广播接收机没有从无线标识发射机接收到广播消息，则中央服务器应当发送警告消息。

[0230] 在判断框 1804 中，中央服务器可以判断是否从与该无线标识发射机有关的邻近广播接收机接收到目击消息。换言之，基于是否接收到这种目击消息，中央服务器可以检测该无线标识发射机是否靠近该邻近广播接收机。中央服务器还可以评估通过一个时段所接收的目击消息，以判断该无线标识发射机是否（或者最近已经）位于该邻近广播接收机的附近范围之内。在一个实施例中，中央服务器可以判断其是否接收到针对在所述关系中注册的每一个无线标识发射机的目击消息。例如，如果注册的关系包括多个无线标识发射机，则中央服务器可以期望从该邻近广播接收机接收关于所有无线标识发射机的目击消息。如果中央服务器接收到与该无线标识发射机有关的目击消息（即，判断框 1804 ＝“是”），则在可选框 1805 中，中央服务器可以等待一段时间，并可以继续执行判断框 1804 中的操作。在各个实施例中，中央服务器可以定期地（例如，每隔几秒、几分钟或者几小时）执行判断框 1804 中的操作。

[0231] 如果中央服务器没有接收到与该无线标识发射机有关的目击消息（即，判断框 1804 ＝“否”），则在方框 1806 中，中央服务器可以发送用于指示该无线标识发射机已丢失

的消息。在各个实施例中，中央服务器可以向该邻近广播接收机、与该邻近广播接收机的用户相关联的其它设备（例如，智能电话、平板计算机）和/或与该无线标识发射机有关的任何其它设备发送该消息。例如，当该无线标识发射机丢失并且与一个儿童相关联时，中央服务器可以向警察局服务器发送警告消息。

[0232] 图 19 描绘了可以在中央服务器中实现的实施例方法 1900。响应于从邻近广播接收机接收到目击消息（其中该目击消息包括无线标识发射机原始广播的编码的、滚动的或者以其它方式受保护的数据），中央服务器可以执行方法 1900。可以通过针对每一个无线标识发射机，使用滚动的或者随机变化的标识符（所以，该标识符随时间而改变），对无线标识发射机的用户的隐私进行保护。可以定期地或者基于某些事件（例如，当无线标识发射机将标识符广播某个数量的次数，或者广播了某个时间段（例如，一个小时）时，或者在一个或多个配对之后），来生成新标识符。可以与中央服务器协调这种滚动的标识符，使得可以仍然对无线标识发射机进行跟踪。例如，无线标识发射机和中央服务器可以各自具有密码安全伪随机数发生器算法，使用该算法在共同的时间尺度上生成标识符，使得在任何给定的时刻，中央服务器可以计算特定的无线标识发射机所发送的标识符。

[0233] 生成滚动标识符或者其它方法的混淆标识符是较为重要的，因为这样可以防止来自第三方的嗅探攻击。例如，如果标识符是静态的，则第三方可以对该标识符进行嗅探（例如，通过冒充邻近广播接收机），随后使用该标识符来跟踪该无线标识发射机。如果第三方缺乏伪随机数发生器或者生成最近的滚动标识符的其它方式，则滚动标识符可以使这种攻击变得不可能。

[0234] 在方框 1902 中，中央服务器可以在目击消息中从邻近广播接收机接收无线标识发射机的滚动标识符。在方框 1904 中，中央服务器可以将该滚动标识符与通过和无线标识发射机所共享的算法（例如，伪随机函数或者具有共享密钥的加密算法）所计算的代码进行比较。该算法可以是中央服务器用于计算代码的软件指令、例行程序、算法、电路或者模块，其中预期该代码与该无线标识发射机在一段时间上生成和广播的滚动标识符相对齐。在各个实施例中，中央服务器可以将所接收的标识符与接下来的几个代码进行比较（在遗漏一些标识符的情况下）。如果所接收的标识符与中央服务器所生成或者预期的任何代码相匹配，则在方框 1906 中，中央服务器可以与匹配的标识符、以及具有与该无线标识发射机相对应的序列码的任何相关数据进行关联。用此方式，如果中央服务器稍后接收到具有该无线标识发射机的序列码的用户请求（例如，来自家长的用于定位孩子所携带的无线标识发射机的请求），则中央服务器可以在无需搜索每一个先前的滚动标识符的情况下，寻找所有在先的匹配以及任何相关联的数据。

[0235] 在一个实施例中，当发起针对目标无线标识发射机的搜索时，中央服务器可以使用共享的算法和信息（例如，密钥）来生成在警报消息中发送的目标设备 ID。在该实施例中，每当目标无线标识发射机被调度以滚动其标识符，就可以重新发送具有更新的目标设备 ID 的警报消息。下面将讨论用于生成滚动标识符或其它编码的标识符的各种算法、以及其它解码算法。

[0236] 图 20-23B 描绘了用于在无线标识发射机和中央服务器之间同步随机数或计数器，以便能够发送和接收模糊信息的各种实施例方法。无线标识发射机可以执行用于对包括模糊的标识符和数据（即，有效载荷）的消息进行广播的各种方法，其中这些信息向中央

服务器标识该无线标识发射机，提供关于该无线标识发射机时钟的相对读数。同样，中央服务器可以执行用于对所接收的消息中的与该无线标识发射机相对应的模糊信息进行处理的各种方法。如上所述，可以直接或者通过中间设备，将来自无线标识发射机的广播消息发送给中央服务器，例如，邻近广播接收机发送目击消息。

[0237] 由于上面所描述的关于设备的非故意跟踪的隐私关注，因此无线标识发射机可以通过只有中央服务器和该无线标识发射机才知道的模糊化措施（例如，加密或者伪随机数据生成），对所发送的消息中的信息进行模糊。在一个实施例中，无线标识发射机可以维持通过随机数或计数器值来表示的时钟或定时器装置，并且一旦该设备进行操作，这些装置就开始运行（例如，通过电池的插入进行激活）。该时钟可以是相对较低质量，因此可能发生漂移，不像例如中央服务器中的更准确的时钟（例如，通过定期的原子时钟读数进行时钟校准）。该计数器或随机数可以是无线标识发射机所产生的非重复的数字，该计数器或随机数在每次无线标识发射机对其标识符进行编码以进行广播时都发生改变（例如，每一小时或者甚至每一个广播消息，变化一次）。在各个实施例中，可以使用伪随机函数或者其它加密算法（例如，AES），对随机数或计数器（或计数器值）进行加密或编码。例如，无线标识发射机可以使用 AES-CTR 块密码来对随机数或计数器值进行编码以生成随机数，以便用于生成包括广播消息的滚动标识符的有效载荷。再举一个例子，可以通过向随机数或计数器值应用线性反馈移位寄存器 (LFSR)，来生成随机数。

[0238] 如贯穿本说明书所描述的，无线标识发射机还可以存储唯一设备识别码或数字（即，设备标识符或“设备 ID”），并且预先设定有每一设备的共享密钥（或 K），其中该密钥与中央服务器处的唯一标识符相关联。例如，中央服务器可以将该唯一设备标识符和密钥存储在数据库中，并可以针对在该中央服务器中注册的所有无线标识发射机，维持设备 ID 和 K 个配对的表格。中央服务器可以使用该设备标识符和密钥，连同其它信息（例如，报告的随机数或计数器值），对来自该无线标识发射机的模糊消息进行识别、解密和以其它方式处理。在一个实施例中，可以顺序地或者随机地生成设备标识符（或设备 ID）。

[0239] 图 20 描绘了用于中央服务器识别通过无线标识发射机广播的消息中的加密数据所指示的该无线标识发射机的实施例方法 2000。在方框 2002 中，无线标识发射机可以接收共享的密钥（即，“K”）。换言之，例如在制造期间，可以向无线标识发射机预先设定每一设备的共享密钥 (K)。在另一个实施例中，无线标识发射机可以在来自附近的邻近广播接收机的消息广播中接收该密钥，例如，上面参照图 4A 所描述的。该密钥可以与中央服务器处的该无线标识发射机的唯一设备标识符（即，设备 ID）相关联。在一个实施例中，密钥可以是 128 比特密钥。

[0240] 在方框 2004 中，无线标识发射机可以通过流式的加密算法（例如，AES-CTR 加密），对设备标识符（设备 ID）、密钥 (K) 和随机数或计数器值进行编码，以生成滚动标识符。“AES-CTR”是国家标准与技术研究所为了实现高级加密标准 (AES) 所建议的保密模式之一。在一个实施例中，无线标识发射机可以包括：被配置为支持“CTR”模式的 AES 协处理器。在一个实施例中，可以通过下式来表示滚动标识符：

[0241] 滚动标识符＝（设备 ID||数据）XOR(MSB_N(AES_K(t)))

[0242] 其中，t 是无线标识发射机的随机数或计数器的值（例如，20 比特值），“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的 AES 块密码，“MSB_N()”意味着“N”个最高有

效位（例如，60 比特）。随后，可以将该滚动标识符包括在该无线标识发射机定期发送的广播消息中。下面参照图 28 来描述如何在蓝牙 LE 广播分组中包括滚动标识符的示例。如下面所更详细描述的，可以将其它设备数据（例如，电池水平、温度等）连同滚动标识符一起在广播分组中进行发送。

[0243] 在另外的实施例中，可以在滚动标识符中包括其它信息。因此，除了为无线标识发射机提供模糊的标识符之外，滚动标识符字段还可以包括只有中央服务器才能恢复的模糊数据。一种用于实现此目的的方法是对用于指示电池状态 (bat_stat) 的额外信息（例如，几比特）连接到设备标识符（设备 ID)，并向该连接串应用 XOR 函数。可以在滚动标识符（即，其在相同数据字段中模糊）中包括的额外信息的数量（即，信息的比特数），受到该滚动标识符字段中的有效位的长度 N 的限制。因此，如果在携带滚动标识符的数据部分中有更多的比特可用，则可以在加密的滚动标识符中包括更多这样的数据。由于在滚动标识符中包括的数据很可能随时间而变化，因此这种方法可以进一步对设备的标识进行模糊。

[0244] 如果期望在广播消息中发送更多的数据，则该数据中的一些可以用明文来携带，或者对数据进行加密。存在用于将数据（例如，电池状态、温度等）包括在广播消息中的多种方法。除了如上所述将数据包括在滚动标识符中，还可以通过将该数据连接到滚动标识符的末尾以作为制造商特定数据有效载荷的一部分（在滚动标识符之前或之后）、明文的传感器数据，来添加数据。因此，如果在制造商特定数据有效载荷中有更多比特可用，则可以使用它们来传送明文的数据。替代地，可以使用与用于生成滚动标识符相同的密钥、或者服务器已知与该无线标识发射机或者这些数据字段相关联的替代密钥，对数据进行编码。在这种替代情形下，滚动标识符中的信息使服务器能够既确定设备的真实标识符，又确定用于对该消息中包括的其它数据进行加密的加密密钥。在另外的实施例中，可以对用于携带其它数据的这些选项进行组合，使得其中一些被包括在滚动标识符中，一些用明文来携带，和 / 或可以对一些数据进行加密并包括在广播消息中。

[0245] 在方框 2006 中，无线标识发射机可以随后对包括随机数和滚动标识符的消息进行广播，或者简单地只包括滚动标识符（即，不具有随机数），如下面参照图 28 所描述的。在一个实施例中，广播消息可以是单个分组长度蓝牙 LE®线性调频消息。在各个实施例中，广播消息中包括的随机数可以是 20 比特，滚动标识符可以是 60 比特，所以整个广播消息是 80 比特。

[0246] 举例而言，在滚动标识符中包括电池状态的实施例中，可以通过下式来表示广播消息（或者广播消息的有效载荷）：

[0247] 有效载荷＝ t||（设备 ID||bat_stat)XOR(MSB_N(AES_K(t)))

[0248] 其中，t 是无线标识发射机的随机数的值，其可以仅仅是随机数或计数器（例如，20 比特值），“bat_stat”是该设备的电池状态信息（例如，4 比特代码），“||”意味着连接，“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的 AES 块密码，“MSB_N()”意味着“N”个最高有效位（例如，60 比特）。换言之，除了包括电池水平指示符的滚动标识符，该实施例广播消息还可以包括明文（即，没有被加密）的随机数。在另一个实施例中，可以不对电池水平指示符（即，bat_stat) 进行加密，电池水平指示符可以被包括在广播消息的另一个字段之中，例如，位于消息的服务通用唯一标识符 (UUID) 部分内，如下面参照图 28 所描述的。

[0249] 在另一个实施例中，有效载荷可以不包括随机数 t，在该情况下，可以通过下式来表示该有效载荷：

[0250] 有效载荷＝（设备 ID||bat_stat)XOR(MSB_N(AES_K(t)))。

[0251] 在方框 2010 中，中央服务器可以在例如上面参照图 14 所描述的账户创建操作期间，接收共享密钥 (K)。例如，中央服务器可以响应于从无线标识发射机的用户接收账户注册信息（例如，设备 ID 和注册请求信息），来生成密钥。在方框 2012 中，中央服务器可以将该共享密钥（即，K）与无线标识发射机的设备标识符（即，设备 ID）进行关联。例如，中央服务器可以将设备 ID 和 K 存储在注册设备的数据表中。

[0252] 在方框 2014 中，中央服务器可以接收包括随机数或计数器以及滚动标识符的消息。例如，所接收的消息可以是来自邻近广播接收机的目击消息，其中该目击消息包括无线标识发射机使用方框 2006 中的操作所广播的信息。在方框 2016 中，中央服务器可以从所接收的消息中提取该随机数或计数器，在方框 2018 中，可以提取滚动标识符。在方框 2019 中，中央服务器可以选择无线标识发射机（即，所选定的无线标识发射机）进行评估。换言之，中央服务器可以从例如用于存储所有注册的无线标识发射机的设备 ID、K 和随机数或计数器的数据库或数据表中，获得存储的中央服务器已知的、针对注册的无线标识发射机的设备 ID、K 和随机数或计数器。在方框 2020 中，中央服务器可以通过相同的流式的加密算法（例如，AES-CTR）与该随机数或计数器以及所选定的无线标识发射机的密钥 (K)，对滚动标识符进行解码，以生成解码后的设备标识符（或 M）。例如，中央服务器可以基于 AES-CTR 算法来执行解码操作，其使用滚动标识符连同所选定的无线标识发射机的密钥 (K) 和在所接收的消息中指示的随机数或计数器一起作为输入。

[0253] 在一个实施例中，可以通过下式来表示解码后的设备标识符 (M)：

[0254] M ＝（滚动标识符）XOR(MSB_{N-a}(AES_K(t)))，

[0255] 其中，t 是无线标识发射机的随机数或计数器的值（例如，20 比特值），“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的 AES 块密码，“MSB_{N-a}”意味着“N-a”个最高有效位（例如，当 a 是 4 比特且 N 是 60 比特时，N-a 是 56 比特）。

[0256] 在判断框 2022 中，中央服务器可以判断解码后的设备标识符 (M) 和设备 ID 是否匹配。换言之，中央服务器可以将解码后的设备标识符 (M) 与用于所选定的无线标识发射机的设备 ID 进行比较，其中 AES-CTR 算法操作使用该无线标识发射机的密钥 (K) 来获得解码后的设备标识符 (M)。如果 M 和设备 ID 确实匹配（即，判断框 2022 ＝“是”），则在方框 2024 中，中央服务器可以将该广播消息识别成来自所选定的无线标识发射机。如果 M 和设备 ID 不匹配（即，判断框 2022 ＝“否”），则在方框 2026 中，中央服务器可以使用与其它无线标识发射机相关联的密钥，对该滚动标识符进行解码。例如，中央服务器可以选择下一个注册的无线标识发射机，并使用相应存储的一对密钥 (K) 和相应的设备 ID。用此方式，中央服务器可以尝试针对所有注册的无线标识发射机和 / 或该系统的用户所存储的所有 K 和设备 ID，直到发现标识该广播消息的发起方的匹配为止。

[0257] 图 21A 描绘了用于无线标识发射机生成和广播加密消息（即，滚动标识符），以便由中央服务器进行接收 / 使用的实施例方法 2100。

[0258] 在方框 2102 中，无线标识发射机的用户可以在中央服务器中进行注册。无线标识发射机使用的服务可能需要对用户（例如，消费者、经营者等）所使用的所有活动设备进行

注册。该注册过程可以包括：无线标识发射机的用户与中央服务器的初始同步。例如，无线标识发射机的用户可以在能够接收无线标识发射机消息并由该用户操作的移动设备或PC中，通过Web应用来向中央服务器注册设备。可能需要在自该设备激活开始起的某个时间段之内，向中央服务器注册该无线标识发射机。例如，可能需要在发起该设备（例如，将电池放置在无线标识发射机中）之后的起初24小时内，对该无线标识发射机进行注册。上面参照图14进一步描述了注册操作。

[0259] 在方框2104中，无线标识发射机例如通过将随机数或计数器设置为零值，对内部随机数或计数器进行初始化。这种随机数或计数器初始化可以由于某种触发事件而发生（例如，电池或电源在该无线标识发射机中的放置）。例如，一旦无线标识发射机被激活或者加电，该随机数或计数器就可以开始递增。替代地，响应于如上所述的注册操作，可以发生初始化。该随机数或计数器可以从“0”（或者任何其它起始值，例如“1”）开始，并可以由无线标识发射机定期地递增。在一个实施例中，当更换无线标识发射机的电池时（例如，由于电池故障），或者当无线标识发射机以其它方式被重置／重新开始／重启时，该随机数或计数器可以返回到初始值（例如，“0”）。该随机数或计数器不会重复其表示的值，除非该无线标识发射机被重置／重新开始／重启。在一个替代的实施例中，在该随机数或计数器的初始化期间，无线标识发射机可以从闪存中读取预先定义的初始随机数或计数器值。例如，无线标识发射机可以使用在出厂时设置的值或者由安装的应用所更新的值，对该随机数或计数器进行初始化。

[0260] 在一个实施例中，可以使用本领域公知的方法，以随机或者伪随机方式，对该随机数或计数器进行初始化和调整。该随机数或计数器可以是伪随机产生的值，该值可以在无线标识发射机和中央服务器中复制。在另一个实施例中，无线标识发射机可以使用线性反馈移位寄存器（LFSR）来生成随机数或计数器，并且在适当的时段之内，其被配置为生成在该设备的寿命期间不会重复的随机数或计数器值。根据LFSR推导出的这些随机数或计数器也可以是伪随机的。

[0261] 在方框2106中，无线标识发射机可以使用中央服务器知道的密钥和加密算法，对连接后的数据进行加密。例如，无线标识发射机可以使用AES-CTR块密码，对随机数或计数器和／或设备标识符（即，设备ID）进行编码。加密算法可以将密钥用于加密和解密目的，这是由于该密钥是中央服务器和无线标识发射机都知道的。该加密算法可以导致某种大小的加密（或编码）数据。例如，使用AES-CTR密码，无线标识发射机可以生成128比特的编码数据。在一个实施例中，无线标识发射机可以生成通过下式所表示的加密数据：

[0262] （设备ID||bat_stat)XOR(MSB_N(AES_K(t))),

[0263] 其中，t是无线标识发射机的随机数或计数器的值（例如，20比特值），“bat_stat”是该无线标识发射机的电池状态信息（例如，4比特编码），“||”意味着连接，“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的AES块密码，“MSB_N()”意味着“N”个最高有效位（例如，60比特）。换言之，除了包括电池水平指示符的滚动标识符之外，该实施例广播消息还可以包括明文的随机数或计数器（即，没有被加密）。在另一个实施例中，可以通过下式来表示加密的数据：

[0264] （设备ID)XOR(AES_K(t)),

[0265] 其中，设备ID是唯一设备标识符，t是无线标识发射机的随机数或计数器的值（例

如，20 比特值），“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的 AES 块密码，“MSB_N()”意味着“N”个最高有效位（例如，60 比特）。

[0266] 由于无线标识发射机的有限的通信能力，因此广播消息的有效载荷（例如，蓝牙 LE 广播分组所支持的有效载荷）可能不能够包含完整的加密消息，而是仅包括一段加密数据的一部分。因此，在方框 2108 中，无线标识发射机可以对数据进行截短，以生成无法解密的滚动标识符。换言之，通过对加密数据进行截短，无线标识发射机可以创建被放置到广播消息（或有效载荷）中的标识符，使得所使用的通信格式（例如，蓝牙 LE）可以支持该标识符的大小。例如，无线标识发射机可以对加密数据进行截短，以适合于 80 比特有效载荷最大尺寸。当加密数据被截短时，在中央服务器中对该数据进行解密是不可能的。但是，中央服务器仍然可以使用这种不完整的加密数据，如下面参照图 21B 所描述的。在一个实施例中，可以使用诸如最高有效位操作之类的函数来实现截短。在另一个实施例中，可以通过下式来表示被截短的数据：

[0267] TRUNC（设备 ID XOR AES_K(t)），

[0268] 其中，t 是无线标识发射机的随机数或计数器的值（例如，20 比特值），“XOR”表示按位异或运算，“AES_K()”是具有密钥“K”的 AES 块密码，“TRUNC()”表示可以创建某个数量的比特或字节（例如，56 比特或 7 个字节）的截短操作。

[0269] 在方框 2110 中，无线标识发射机可以将当前随机数或计数器与截短的数据进行连接以生成消息有效载荷。例如，无线标识发射机可以将当前无线标识发射机系统时钟值（例如，长度为 20 比特）与该无线标识发射机的被截短为长度 60 比特的唯一识别码进行组合。在一个实施例中，有效载荷可以包括加密数据和未加密数据（或者“明文”数据）。例如，有效载荷可以包含用于表示加密数据和 / 或截短数据的多个比特、以及用于表示该无线标识发射机的电池状态或者随机数或计数器值的一些其它比特。

[0270] 在方框 2112 中，无线标识发射机可以例如通过使用如上所述的短距离无线通信技术进行广播，来定期地发送广播消息，其中该广播消息包括具有滚动标识符的有效载荷。依据系统配置、用户设置、或者与无线标识发射机通过无线信号进行通信有关的调度和定时的任何其它源，广播消息的传输频率可以发生变化。例如，无线标识发射机可以每隔几秒钟，对滚动标识符进行广播一次。

[0271] 在判断框 2114 中，无线标识发射机可以判断预先定义的随机数或计数器时间段是否到期。可以按照与如上所述的广播频率周期相类似的方式，来设置该随机数或计数器时间段。例如，制造商或许可以使用各种技术（例如，无线标识发射机的处理器电路中的硬编码变量），来建立随机数或计数器时间段。

[0272] 如果随机数或计数器时间段还没有到期（即，判断框 2114 =“否”），则无线标识发射机可以继续执行方框 2112 中的操作。例如，无线标识发射机可以在很多分钟的时间段中，按照几秒钟的频率，通过短距离无线传输来广播有效载荷。

[0273] 如果设备确定随机数或计数器时间段已到期（即，判断框 2114 =“是”），则在方框 2116 中，无线标识发射机可以对随机数或计数器值进行递增（例如，增加 1）。在方框 2117 中，无线标识发射机可以对随机数或计数器时间段进行重新设置。例如，在随机数或计数器时间段已到期之后，无线标识发射机可以将随机数或计数器增加值 1，并将随机数或计数器时间段重置为 0。无线标识发射机可以继续执行方框 2106 中的操作（例如，无线标识发射

机可以创建新的有效载荷，并在另一个随机数或计数器时间段内对其进行广播）。

[0274] 图 21B 描绘了用于中央服务器接收消息，并基于有效载荷信息对定时随机数和计数器进行同步的实施例方法 2150。在方框 2152 中，中央服务器可以建立具有设备标识符（即，设备 ID）、随机数或计数器、以及在该无线标识发射机在其注册时使用的密钥数据的数据库条目。中央服务器可以维持数据库，该数据库包含：针对与该中央服务器相关联的每个无线标识发射机和 / 或该中央服务器的附属服务的数据记录。该数据库可以被填充有通过上面所描述的注册操作所获得的信息。因此，可以存在针对与该中央服务器相关联的每个无线标识发射机的数据记录，每一条记录可以包含表示特定设备的标识、其当前随机数或计数器（例如，时钟值）、以及与该无线标识发射机相关联的密钥的信息。在一个实施例中，对于在中央服务器中注册的每个无线标识发射机来说，该密钥可以是唯一的。在一个实施例中，中央服务器还可以针对在该中央服务器中注册的每一个无线标识发射机，存储初始随机数或计数器值。

[0275] 在各个实施例中，当注册无线标识发射机时，中央服务器可以存储用于该无线标识发射机的初始随机数或计数器值。依据该无线标识发射机的激活（例如，当插入电池，并且该设备变为操作状态时）和该设备的注册之间的时间，针对该无线标识发射机的初始随机数或计数器可以是 0，也可以不是 0。例如，如果在用户将电池插入在无线标识发射机中几个小时之后，发生该无线标识发射机向中央服务器的注册，则初始随机数或计数器可以不是 0。在一个实施例中，中央服务器还可以通过设置注册标志或者其它指示符来指示该无线标识发射机的注册状态，并且可以存储用于描述已在数据库中注册的无线标识发射机的信息。在一个实施例中，中央服务器可以维持数据库，该数据库具有针对所有已知的无线标识发射机（无论它们是否注册）提供的初始值。例如，基于制造记录，中央服务器可以维持具有关于所创建的每个无线标识发射机的信息的数据库。

[0276] 中央服务器可以使用类似于上面参照方框 2106-2110 所描述的那些操作来生成和存储模型有效载荷。模型有效载荷可以是中央服务器基于存储的密钥、设备标识符（设备 ID）以及随机数或计数器信息，预期从该无线标识发射机接收的有效载荷。例如，针对每个注册的无线标识发射机，中央服务器可以通过将该设备的设备 ID 连接到随机数或计数器值，使用加密协议对连接的数据进行加密（其利用用于该无线标识发射机的密钥），对加密后的数据进行截短，来创建模型有效载荷。每一个模型有效载荷可以结合相应的设备 ID、以及用于生成各个模型有效载荷的随机数或计数器值，存储在中央服务器数据表（或查询表）中。例如，对应于用于每一个无线标识发射机的每一个模型有效载荷，中央服务器可以在数据表中存储该模型有效载荷、时间偏移值（例如，-2、-1、1、2 等）以及随机数或计数器，全部这些都与无线标识发射机的设备 ID 有关。

[0277] 在方框 2154 中，中央服务器可以在规定的初始化时段，生成和存储用于无线标识发射机的初始模型有效载荷。例如，以初始随机数或计数器值开始（例如，0 或者该设备和中央服务器知道的伪随机值），中央服务器可以使用与无线标识发射机的实际初始随机数或计数器相比相同、更低和 / 或更高的随机数或计数器值来生成模型有效载荷，使得这些模型随机数或计数器覆盖初始化时段。在一个实施例中，该初始化时段可以是一个小时、几个小时、几天等。中央服务器可以存储初始模型有效载荷，以便在无线标识发射机的注册 / 重置 / 重启的情况下使用。

[0278] 在方框 2155 中，中央服务器还可以生成和存储预期在规定的时间窗之内将接收的用于无线标识发射机的当前模型有效载荷。为了说明无线标识发射机中的可能的时钟漂移，中央服务器可以通过使用多个导出的随机数或计数器值（它们表示可能的随机数或计数器的范围），来生成和存储用于所规定的时间窗（或者时间段）的模型有效载荷。换言之，导出的随机数或计数器值可以与针对无线标识发射机所存储的当前随机数或计数器值有偏移。例如，中央服务器可以生成用于导出的随机数或计数器值的模型有效载荷，其中这些导出的随机数或计数器值与当前在数据库中存储的随机数或计数器值相比更低或者更高。导出的随机数或计数器值可以是向针对无线标识发射机所存储的随机数或计数器值增加偏移值（例如，-2、-1、1、2 等）的结果。中央服务器可以生成用于表示存储的随机数或计数器值以及导出的随机数或计数器值的模型有效载荷，所述导出的随机数或计数器值递增地表示窗时间段。例如，这些模型有效载荷可以表示按照较小的时间值（例如，一个小时）增加并且覆盖较大时间段（例如，多个小时）的随机数或计数器。再举一个例子，中央服务器可以存储与针对无线标识发射机所存储的当前随机数或计数器值相对应的有效载荷、与用于该设备的前一随机数或计数器值相对应的有效载荷、以及与用于该设备的下一个随机数或计数器值相对应的有效载荷。

[0279] 在一个实施例中，针对给定的无线标识发射机第一次生成的当前模型有效载荷，可以与针对该无线标识发射机的初始模型有效载荷相同，这是由于中央服务器可以基于相同的初始随机数或计数器值来生成这两组有效载荷。在一个实施例中，该初始化时段可以与所规定的时间窗相一致。例如，该初始化时段可以涉及与所规定的时间窗相类似数量的天数、小时、分钟等。

[0280] 在判断框 2156 中，中央服务器可以判断随机数或计数器时间段是否到期。中央服务器可以在任意的时间、或替代地在接收到无线标识发射机注册之后，初始化随机数或计数器时间段的评估。该随机数或计数器时间段可以是如上面参照判断框 2114 所描述的无线标识发射机使用的相同的时间段。

[0281] 如果该随机数或计数器时间段已到期（即，判断框 2156 ＝“是”），则在方框 2155’中，中央服务器可以针对注册的无线标识发射机，生成并存储更新的当前模型有效载荷。更新后的当前模型有效载荷可以替换先前的当前模型有效载荷，其可以是基于在每个相应的无线标识发射机的数据库记录中存储的随机数或计数器值。

[0282] 如果该随机数或计数器时间段还没有到期（即，判断框 2156 ＝“否”），或者如果该随机数或计数器时间段已到期并且中央服务器已生成更新的当前模型有效载荷，则在判断框 2160 中，中央服务器可以判断是否已经接收到任何有效载荷。在一个实施例中，可以直接从无线标识发射机传送有效载荷，或者替代地通过目击消息从邻近广播接收机来间接地向中央服务器传送有效载荷，其中该目击消息包括（或者中继）从附近的无线标识发射机到中央服务器的滚动标识符有效载荷。如果还没有接收到有效载荷（即，判断框 2160 ＝“否”），则中央服务器可以继续执行判断框 2156 中的操作。

[0283] 如果已接收到有效载荷（即，判断框 2160 ＝“是”），则在方框 2162 中，中央服务器可以被配置为使用存储的当前模型有效载荷（例如，针对每一个注册的无线标识发射机所存储的当前模型有效载荷），对接收的有效载荷进行评估。如上所述，中央服务器可以针对每个注册的无线标识发射机，维持两个存储的模型有效载荷的集合：初始模型有效载荷

集合和当前模型有效载荷集合，其中，所述初始模型有效载荷集合可以包括基于初始随机数或计数器以及导出的随机数或计数器值（它们占据初始化时段）的模型有效载荷，所述当前模型有效载荷集合是基于在数据库记录中针对每个无线标识发射机所存储的当前随机数或计数器值。在一个实施例中，中央服务器可以设置系统变量，其中该系统变量指示中央服务器应当将所接收的有效载荷与存储的当前模型有效载荷进行比较。可以将该系统变量设置为指示中央服务器对用于无线标识发射机的当前或初始模型有效载荷进行评估。

[0284] 在方框 2164-2172 中，中央服务器可以执行下面的操作循环：中央服务器对所接收的有效载荷（即，无线标识发射机广播的数据）与针对所有注册的无线标识发射机的存储的模型有效载荷进行比较，直到找到匹配为止。在方框 2164 中，中央服务器可以选择下一个注册的无线标识发射机。中央服务器可以基于注册的无线标识发射机的数据库来确定下一个注册的设备，并且可以在方框 2164-2172 中的操作期间，依次迭代每个设备。在方框 2166 中，中央服务器可以基于系统配置（例如，方框 2162 中的操作里设置的配置），将所接收的有效载荷与针对所选定的无线标识发射机所存储的模型有效载荷进行比较。例如，基于使用方框 2162 中的操作而被设置为“当前”的系统变量，中央服务器可以将所接收的有效载荷与针对所选定的无线标识发射机所存储的当前模型有效载荷进行比较。基于所接收的有效载荷的加密数据的形式，这种比较可以是模式匹配例行程序，其中在该例行程序中，中央服务器将模型有效载荷的数据与所接收的有效载荷进行比较。例如，中央服务器可以将所存储的有效载荷和所接收的有效载荷的比特值进行比较。

[0285] 在判断框 2168 中，中央服务器可以判断存储的模型有效载荷中的任一模型有效载荷是否与所接收的有效载荷相匹配。如果没有任何存储的模型有效载荷与所接收的有效载荷相匹配（即，判断框 2168 ＝“否”），则在判断框 2170 中，中央服务器可以判断是否存在另一个注册的无线标识发射机要进行评估。换言之，中央服务器可以判断是否已经对所有注册的无线标识发射机的存储的模型有效载荷进行了评估。如果存在另一个注册的无线标识发射机要进行评估（即，判断框 2170 ＝“是”），则中央服务器可以通过使用方框 2164 中的操作来选择下一个注册的无线标识发射机来继续操作。

[0286] 如果中央服务器已经对所有注册的无线标识发射机的存储的模型有效载荷进行了评估（即，判断框 2170 ＝“否”），则在方框 2172 中，中央服务器可以被配置为使用存储的、初始模型有效载荷（例如，在每一个注册的无线标识发射机注册时，针对该设备所存储的初始模型有效载荷），对所接收的有效载荷进行评估。例如，中央服务器可以设置系统变量，其中该系统变量指示中央服务器应当将所接收的有效载荷与用于评估的注册的无线标识发射机的存储的初始模型有效载荷进行比较（例如，该系统变量可以被设置为“初始”）。随后，该操作循环可以继续执行方框 2164-2168 中的操作，在这些操作中，中央服务器可以选择每个注册的无线标识发射机，将所选定的设备的初始模型有效载荷与所接收的有效载荷进行比较。

[0287] 如果中央服务器确实在所接收的有效载荷和注册的无线标识发射机的存储的模型有效载荷（当前或初始）中的任一模型有效载荷之间找到匹配（即，判断框 2168 ＝“是”），则在方框 2174 中，中央服务器可以基于该匹配来确定无线标识发射机标识。换言之，中央服务器可以基于与匹配的存储的模型有效载荷所关联存储的标识信息（例如，设备 ID），来识别与所接收的有效载荷相对应的无线标识发射机。在方框 2176 中，中央服务器

可以使用基于所接收的有效载荷所识别的无线标识发射机的随机数或计数器，对数据库进行更新。基于与匹配的存储的模型有效载荷相对应的数据库记录，中央服务器可以确定与所接收的有效载荷相对应的导出的随机数或计数器值，并且可以对所存储的随机数或计数器值进行更新，以表示该导出的随机数或计数器值，因此对所识别的无线标识发射机的随机数或计数器和中央服务器随机数或计数器进行同步。在一个实施例中，中央服务器还可以在数据库中存储该中央服务器接收到所接收的有效载荷时的中央服务器随机数或计数器（或时间）。

[0288] 在一个实施例中，中央服务器可以维持最近接收的消息和相应的无线标识发射机标识的列表。例如，中央服务器可以在数据表中记录在某个时间段内接收到的消息的设备ID和有效载荷信息。中央服务器可以将任何后续接收的有效载荷与数据表进行比较，以便基于最近从相同的无线标识发射机接收的有效载荷来判断后续接收的有效载荷是否是冗余的。例如，后续接收的有效载荷可以表示：来自特定无线标识发射机的某个随机数或计数器值在几分钟之前已经被中央服务器接收并处理。这样可以加快方法2150处理，并减少方框2164-2172中的操作的搜索时间。在一个实施例中，中央服务器可以删去（或清除）最近识别的有效载荷和无线标识发射机的数据表，并且可以与方框2176中所述的类似方式来调度该清除操作（例如，可以在确定随机数或计数器时间段将到期的每一次，对最近的数据表进行清除）。

[0289] 图22描绘了用于中央服务器识别在由无线标识发射机广播的消息中的加密数据所指示的该无线标识发射机的另一种实施例方法2200。在方法2200的操作中，为了提高无线标识发射机发送其标识的安全性，可以从不将随机数或计数器值包括在广播消息中。例如，由于随机数或计数器值在不同的无线标识发射机之间可能有所不同，因此具有捕获广播消息能力的攻击者也许能够容易地预测来自该无线标识发射机的未来广播消息中的值。但是，在不具有以明文发送的随机数或计数器数据的情况下，可以更好地阻挠邪恶的窥探者跟踪来自特定的无线标识发射机的广播。

[0290] 在方框2002中，无线标识发射机可以接收共享的密钥（即，“K”）。例如，可以向每个无线标识发射机预先设定每一设备共享的密钥，其中该密钥与中央服务器处的无线标识发射机的唯一设备标识符（即，设备ID）相关联。在方框2204中，无线标识发射机可以对随机数或计数器进行同步。当无线标识发射机在中央服务器处注册了时，该随机数或计数器可以与中央服务器进行同步。同步后的随机数或计数器值还可以与中央服务器中存储的数据表（例如，具有存储的成对的ID和K值的表格）中的设备ID和K相关联。

[0291] 在方框2206中，无线标识发射机可以将随机数或计数器递增到该无线标识发射机的当前设备时间。例如，在预先定义数量的秒数（例如，一秒、一小时等等）之后，可以对该随机数或计数器进行递增。再举一个例子，无线标识发射机可以每3600秒，对随机数或计数器递增1。用此方式，该随机数或计数器值可以变为如无线标识发射机上的振荡器所计数的当前值。在方框2208中，无线标识发射机可以通过伪随机函数，对设备标识符（即，设备ID）、共享的密钥（即，K）、以及用于生成滚动标识符的随机数或计数器进行编码，以生成滚动标识符。用此方式，可以随着该随机数或计数器值改变，而生成滚动标识符。在一个实施例中，伪随机函数可以是具有种子（“s”）和输入变量（“x”）的多项式时间可计算函数，使得当该种子是随机选择的并且观察者不知道时，与在相同域上规定的、具有输出到相

同范围的随机函数相比，伪随机函数（例如，PRF(s,x)）可能在计算上是难以区分的。例如，可以将密钥哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 用作伪随机函数。

[0292] 在方框 2210 中，无线标识发射机可以广播包括滚动标识符的消息（例如，长度为 1 个分组的蓝牙 LE chrp 消息）。在一个实施例中，可以通过下式来表示广播消息（或者该广播消息的有效载荷）：

[0293] 有效载荷＝ MSB_N(PRF(K,（设备 ID||t)))

[0294] 其中，t 是无线标识发射机的随机数或计数器的值，“||”意味着连接，“PRF()”是伪随机函数，“MSB_N()”意味着“N”个最高有效位（例如，80 比特）。换言之，无线标识发射机可以对设备标识符以及随机数或计数器信息进行故意地模糊（或者偏斜），因此广播消息的有效载荷可以既不包括明文的设备标识符，也不包括明文的随机数或计数器信息。

[0295] 在方框 2010 中，中央服务器可以接收共享密钥 (K)。在方框 2212 中，中央服务器可以对随机数或计数器进行同步。例如，可以将该随机数或计数器进行设置，以表示与该无线标识发射机有关的前一消息（例如，注册消息）中所包括的值。在方框 2214 中，中央服务器可以将该共享密钥（即，K) 以及随机数或计数器，与该无线标识发射机的设备标识符（即，设备 ID) 进行关联。例如，中央服务器可以将该设备 ID、K 和随机数或计数器，存储在注册设备的数据表中（例如，存储在数据库的元组记录中）。在一个实施例中，中央服务器还可以存储用于指示是否已注册或激活各无线标识发射机的指示符或标志。

[0296] 在方框 2216 中，中央服务器可以接收包括滚动标识符的消息。例如，所接收的消息可以是来自邻近广播接收机的目击消息，其包括无线标识发射机使用方框 2210 中的操作所广播的滚动标识符。在方框 2018 中，中央服务器可以提取该滚动标识符，例如，通过对所接收的消息进行解析以识别滚动标识符的有效载荷。

[0297] 在方框 2019 中，中央服务器可以选择无线标识发射机（即，所选定的无线标识发射机）进行评估。换言之，中央服务器可以例如从用于存储所有注册的无线标识发射机的设备 ID、K 和随机数或计数器的数据库或数据表中，获得所存储的针对中央服务器已知的注册的无线标识发射机的这些设备 ID、K 和随机数或计数器。在方框 2218 中，中央服务器可以将所选定的无线标识发射机的随机数或计数器，递增到该服务器的当前时间。在一个实施例中，中央服务器可以随后对所存储的随机数或计数器值进行递增，以说明自从对存储的随机数或计数器值进行同步以来流逝的时间。举例而言，中央服务器可以将使用方框 2216 中的操作来接收该消息的时间，与中央服务器的当前时间进行比较（例如，通过中央服务器时钟或时间装置）。基于无线标识发射机对它们各自的随机数或计数器进行递增的已知周期（例如，每一小时一次），中央服务器可以对所选定的随机数或计数器值进行递增，以说明时间差。

[0298] 在一个实施例中，中央服务器可以对所选定的随机数或计数器仅递增用于表示无线标识发射机的广播之间的时间的量。换言之，中央服务器可以不对所选定的随机数或计数器进行递增，以便包括在方框 2216 中的操作中接收该消息之间的时间、和邻近广播接收机接收到该广播消息的时间。例如，邻近广播接收机可以在将目击消息中继给中央服务器之前，已对广播消息进行了缓冲。中央服务器可以基于使用方框 2216 中的操作所接收的消息里的元数据，来计算该时间差。例如，来自邻近广播接收机的目击消息可以指示何时接收到了广播消息。因此，所选定的随机数或计数器递增的量，可以是基于邻近广播接收机实

际接收到该广播消息的时间，而不是基于中央服务器从邻近广播接收机接收到该消息的时间。

[0299] 在方框 2220 中，中央服务器可以通过伪随机函数，对所选定的无线标识发射机的设备标识符、密钥、以及随机数或计数器进行编码，以生成服务器加密的数据（即，C'）。该伪随机函数可以与方框 2208 中的操作里所使用的伪随机函数相同。在一个实施例中，可以通过下式来表示所生成的服务器加密的数据：

[0300] C' = MSB_N(PRF(sel_K,(sel_ 设备 ID||sel_t)))，

[0301] 其中，sel_K 是所选定的无线标识发射机的密钥的值，sel_ 设备 ID 是所选定的无线标识发射机的唯一设备标识符的值，sel_t 是所选定的无线标识发射机的随机数或计数器的值，"||"意味着连接，"PRF()"是伪随机函数，"MSB_N()"意味着"N"个最高有效位（例如，60 比特、74 比特、80 比特等等）。

[0302] 在判断框 2222 中，中央服务器可以判断所生成的服务器加密数据（C'）是否与所接收的滚动标识符相同。换言之，中央服务器可以将所接收的滚动标识符与所生成的服务器加密数据进行比较，以判断它们是否匹配。如果该滚动标识符和所生成的服务器加密数据相匹配（即，判断框 2222 ="是"），则在方框 2024 中，中央服务器可以将所接收的消息识别成来自所选定的无线标识发射机（例如，与所选定的无线标识发射机的唯一标识符相对应）。

[0303] 如果该滚动标识符和所生成的数据不匹配（即，判断框 2222 ="否"），则在方框 2224 中，中央服务器可以对用于其它无线标识发射机的设备标识符、密钥以及随机数或计数器进行编码，以识别所接收的消息的发起方。换言之，中央服务器可以从数据库中选择下一个存储的设备 ID、随机数或计数器以及 K 群组，对所选定的随机数或计数器值进行递增，对所选定的设备 ID、随机数或计数器以及 K 进行编码，将所生成的编码数据与所接收的滚动标识符进行比较，直到找到匹配为止，并且所接收的消息中的滚动标识符的发起方的标识是已知的。

[0304] 在一个实施例中，当无线标识发射机的电池已经被移除和重新安装时，可以将最新的随机数或计数器值保持在该无线标识发射机的非易失性存储器中，使得当电池被去除并随后放回时，可以从该无线标识发射机的非易失性存储器中读回该随机数或计数器值。替代地，如果非易失性存储器是不可获得的或者没有被使用，则在电池重新安装之后，无线标识发射机可以回退到初始的随机数或计数器值。可能需要对中央服务器进行稍微修改，以适应这种"计数器同步"。更具体地，除了尝试与预先计算的计数器或随机数列表中的最大随机数或计数器值相比更大的值，当执行"计数器同步"时，中央服务器还可以尝试诸如 (counter+i) 之类的值，其中 i = 0,…,n。在该情况下，当"计数器同步"失败多次时，可能需要通知无线标识发射机用户：需要对电池进行重新安装。

[0305] 图 23A 描绘了用于无线标识发射机使用伪随机函数来生成滚动标识符以进行广播的实施例方法 2300。方法 2300 中的操作可以类似于上面所描述的实施例方法 2100。但是，不使用 AES-CTR 加密算法对诸如随机数或计数器值之类的数据进行加密，而是，方法 2300 可以基于伪随机函数的应用来生成有效载荷。如上所述，该伪随机函数和用于各无线标识发射机的密钥可以是相应的无线标识发射机和中央服务器二者均知道的，使得二者都可以基于类似数据来生成类似的有效载荷。

[0306] 在方框 2102 中，无线标识发射机的用户可以在中央服务器中注册设备。在方框 2104 中，无线标识发射机例如通过将随机数或计数器设置为零值，对内部随机数或计数器进行初始化。在方框 2302 中，无线标识发射机可以将当前随机数或计数器与该无线标识发射机的唯一设备标识符（即，设备 ID）进行连接。在方框 2304 中，无线标识发射机可以使用伪随机函数与连接的数据和密钥，来生成具有滚动标识符的有效载荷。例如，该伪随机函数可以将连接的数据（即，设备 ID+ 随机数 / 计数器）用作输入，并且可以使用用于该无线标识发射机的密钥作为随机种子变量。具有滚动标识符的有效载荷可以包括来自伪随机函数的输出数据。在一个实施例中，具有滚动标识符的有效载荷还可以包括关于该无线标识发射机的其它方面的明文信息。例如，无线标识发射机可以向有效载荷添加几个比特（例如，4 比特）的信息，其中该信息用于描述该无线标识发射机的电池状态。在一个实施例中，与在相同域上定义的、并且输出到相同范围的随机函数相比，伪随机函数可以是在计算上是难以区分的多项式时间可计算函数。例如，可以将密钥哈希消息认证码 (HMAC) 或者基于密码的消息认证码 (CMAC) 用作伪随机函数。在一个实施例中，无线标识发射机可以对所生成的滚动标识符有效载荷执行截短操作，也可以不执行截短操作。例如，具有滚动标识符的有效载荷可以是对于伪随机函数的结果执行最高有效位操作的结果。

[0307] 在方框 2112 中，无线标识发射机可以例如通过使用如上所述的短距离无线通信技术进行广播，来定期地发送广播消息，其中该广播消息包括具有滚动标识符的有效载荷。在判断框 2114 中，无线标识发射机可以判断预先定义的随机数或计数器时间段是否到期。如果随机数或计数器时间段还没有到期（即，判断框 2114 ＝“否”），则无线标识发射机可以继续执行方框 2112 中的操作。如果设备确定随机数或计数器时间段已到期（即，判断框 2114 ＝“是”），则在方框 2116 中，无线标识发射机可以对该随机数或计数器值进行递增（例如，加 1）。在方框 2117 中，无线标识发射机可以对随机数或计数器时间段进行重新设置，并可以继续执行方框 2302 中的操作。

[0308] 图 23B 描绘了用于中央服务器响应于接收到包含伪随机函数滚动标识符的消息的实施例方法 2350。实施例方法 2350 操作可以类似于上面参照图 21B 所描述的操作，除了中央服务器可以将伪随机函数的输出与中央服务器中存储的时间同步信息进行比较，以匹配从无线标识发射机接收的消息中的有效载荷之外。

[0309] 在方框 2352 中，中央服务器可以针对系统中的每一个无线标识发射机，建立数据库记录，所述数据库记录具有设备标识符（即，设备 ID）、随机数或计数器、时间、注册状态（即，“reg_stat”）和密钥（即，“K”）信息。该时间可以指示中央服务器接收到与特定的无线标识发射机相对应的消息（例如，中继广播消息的目击消息）的上一次时间，或者换言之，当接收 / 在数据库中记录了针对一个无线标识发射机的随机数或计数器值的时刻的中央服务器时钟值。可以假定，在无线标识发射机广播具有滚动标识符（或滚动标识符有效载荷）的消息的时刻与中央服务器接收到该滚动标识符的时刻之间的时间段非常短。因此，可以假定所存储的随机数或计数器和时间值创建无线标识发射机的大致精确的时钟状态。

[0310] 另外，一旦无线标识发射机发送了注册信息，中央服务器就可以通过在数据库中针对该无线标识发射机设置注册标志（例如，“reg_stat”），来指示有效的注册。中央服务器可以查询针对所有无线标识发射机记录的数据库，其中 reg_stat 指示已进行了有效的

注册，并且可以基于 reg_stat 值来创建仅包括注册的无线标识发射机的数据表。

[0311] 在方框 2354 中，中央服务器可以通过来自邻近广播接收机的目击消息，接收滚动标识符有效载荷。目击消息可以具有添加到该有效载荷的时间信息，该时间信息描述了邻近广播接收机通过来自响应的无线标识发射机的广播消息而遇到该有效载荷的时间。例如，智能电话邻近广播接收机可以接收有效载荷，转而将其自己的系统时钟读数添加到有效载荷信息，并将该数据作为目击消息发送给中央服务器。邻近广播接收机所提供的时间测量值可以与中央服务器系统时间近似地同步。在一个实施例中，邻近广播接收机可以将其它另外的信息（例如，该邻近广播接收机的位置信息（如，GPS 坐标））添加到目击消息中。在方框 2356 中，中央服务器可以从该目击消息中获得邻近广播接收机时间（即，“ir_time”），例如在该目击消息中所指示的。例如，中央服务器可以对目击消息进行解析，并且提取用于指示该邻近广播接收机何时接收到与滚动标识符有效载荷相对应的广播消息的时间值。

[0312] 在方框 2164-2374 中，中央服务器可以执行下面的操作循环：中央服务器可以对该中央服务器的数据库中所存储的所有注册的无线标识发射机进行评估，以发现与所接收的滚动标识符有效载荷相匹配的设备记录。在方框 2164 中，中央服务器可以选择下一个注册的无线标识发射机。例如，中央服务器可以迭代地选择所有无线标识发射机的数据表中所表示的下一个无线标识发射机，其中该无线标识发射机使得 reg_stat 变量被设置为指示发生了注册。在方框 2164-2374 中的操作期间，中央服务器可以针对每一个设备，对整个该数据表或者列表继续顺序地迭代。在一个实施例中，中央服务器可以访问与所选定的注册的无线标识发射机相对应的存储的数据库记录，其中该数据库记录包含使用方框 2352 中的注册操作所建立的信息的当前值。

[0313] 在方框 2360 中，中央服务器可以计算目击消息中指示的时间（ir_time）与所选定的注册的无线标识发射机的数据库记录中存储的时间（即，“sel_time”）之间的时间差（即，“t_diff”）。例如，t_diff 值可以是非零值或者零值。该时间差可以是中央服务器从所选定的无线标识发射机接收到有效载荷的实例之间的预期的流逝时间的测量值。

[0314] 在方框 2362 中，中央服务器可以将时钟漂移偏移（即，“offset”）设置为下一个值。通常，中央服务器可以通过设置时钟漂移偏移值，考虑可能的无线标识发射机时钟漂移（例如，不准确的设备系统时钟读数）。这些时钟漂移偏移值可以表示偏移量，当其应用于随机数或计数器值时，可以表示与预期的随机数或计数器值相比更低、相同或者更高的随机数或计数器。换言之，这些时钟漂移偏移可以表示在针对所选定的注册设备的当前随机数或计数器所表示的时间之前、期间或者之后的时间。该时钟漂移偏移值可以是时钟漂移偏移值序列中的一个。在一个实施例中，该时钟漂移偏移值可以是 0。在一个实施例中，可能的时钟漂移偏移值可以包括集合 {-N、…、-1、0、1、…、N} 中的数字，其中 N 是任意数。

[0315] 在方框 2364 中，中央服务器可以使用所选定的无线标识发射机的存储的随机数或计数器值、所计算的时间差值（即，t_diff）和集合偏移值（即，offset），来计算预期的随机数或计数器值（即，“new_ctr”）。如上所述，可以将该随机数或计数器存储在所选定的注册的无线标识发射机数据库记录之中。例如，中央服务器可以通过将时钟漂移偏移值加上 t_diff 值与存储的随机数或计数器值之和，来计算 new_ctr。

[0316] 在判断框 2366 中，中央服务器可以通过伪随机函数，对所选定的无线标识发射机

的设备标识符、密钥和计算的随机数或计数器（即，new_ctr）进行编码，以生成服务器加密的数据（即，C'）。该伪随机函数可以是与无线标识发射机使用的相同的伪随机函数，如上面参照图 23A 所描述的。

[0317] 在判断框 2222 中，中央服务器可以判断所生成的服务器加密的数据（C'）是否与所接收的滚动标识符相同。换言之，中央服务器可以将所接收的滚动标识符与所生成的服务器加密数据进行比较，以判断它们是否匹配。如果该滚动标识符和所生成的服务器加密数据相匹配（即，判断框 2222 ＝“是”），则中央服务器可以将所接收的消息识别成源自于所选定的无线标识发射机（例如，与所选定的无线标识发射机的唯一标识符相对应）。在一个实施例中，密钥（K）可以是伪随机函数的种子值。在一个实施例中，中央服务器可以将所选定的无线标识发射机的设备 ID 和计算的 new_ctr 值进行连接，并将连接后的数据提供给伪随机函数。该伪随机函数可以返回（或者输出）与接收的滚动标识符有效载荷具有类似结构的加密数据。

[0318] 如果该滚动标识符（例如，在目击消息中所接收的）和所生成的服务器加密数据（即，C'）相匹配（即，判断框 2222 ＝“是”），则在方框 1276 中，中央服务器可以使用该随机数或计数器和时间信息（例如，new_ctr 和 ir_time），来对所选定的无线标识发射机的数据库记录进行更新。例如，中央服务器可以对该数据库记录的时间值进行更新，以表示在邻近广播接收机中接收到有效载荷的时间（例如，ir_time），还可以更新所存储的随机数或计数器值以表示 new_ctr 值。中央服务器可以继续执行方框 2354 中的操作。

[0319] 如果该滚动标识符（例如，在目击消息中所接收的）和所生成的服务器加密的数据（即，C'）不匹配（即，判断框 2222 ＝“否”），则在判断框 2370 中，中央服务器可以判断是否存在下一个时钟漂移偏移值。换言之，中央服务器可以判断是否使用所有可能的时钟漂移偏移值（例如，-1、0、1 等），计算出了 new_ctr 值。如果存在下一个时钟漂移偏移值（即，判断框 2370 ＝“是”），则中央服务器可以继续执行方框 2362 中的操作。但是，如果不存在下一个时钟漂移偏移值（即，判断框 2370 ＝“否”），则在判断框 2170，中央服务器可以判断是否存在另一个注册的无线标识发射机要进行评估。如果存在另一个注册的无线标识发射机要进行评估（即，判断框 2170 ＝“是”），则中央服务器可以继续执行方框 2164 中的操作。但是，如果不存在其它注册的无线标识发射机（即，判断框 2170 ＝“否”），则在方框 2374 中，中央服务器可以对系统进行配置，以评估针对每一个注册的无线标识发射机所存储的初始随机数或计数器值。在一个实施例中，上面所描述的注册数据库还可以包括：用于表示与每一个注册的无线标识发射机相对应的初始随机数或计数器值的数据。如果 / 当各个无线标识发射机被重启或者以其它方式对它们的计数器进行重置时，可以使用该初始的随机数或计数器值。例如，无线标识发射机可以在对其内部随机数或计数器进行重置（由于电池更换）之前的一段时间中，操作并传输用于描述非初始的随机数或计数器的有效载荷。在该场景中，无线标识发射机可以广播消息，其中该消息包括基于重置的随机数或计数器信息的滚动标识符。

[0320] 在另一个实施例中，可以在方框 2362-2370 中的操作循环期间，针对各个注册的选定设备，执行方框 2374 中的操作，其中可以使用初始的存储的随机数或计数器值，来替代方框 2364 中的存储的随机数或计数器值。例如，一旦中央服务器确定所选定的注册的无线标识发射机的存储的随机数或计数器值与各种时钟漂移偏移值，不能够用于生成与所

接收的滚动标识符有效载荷相匹配的加密数据，则中央服务器可以在选择下一个注册的无线标识发射机之前，对所选定的无线标识发射机的初始的存储的随机数或计数器值进行评估。

[0321] 图 24A 描绘了用于无线标识发射机生成和广播具有滚动标识符和编码的随机数或计数器的消息的实施例方法 2400。方法 2400 可以具有由无线标识发射机进行执行的操作，其类似于上面参照图 20、21A、22 和 23A 所描述的那些操作。但是，方法 2400 可以涉及对包括滚动标识符（即，编码的设备标识符）以及编码的随机数或计数器的消息进行广播，其中中央服务器可以使用下面参照图 24B 所描述的操作来单独地评估该随机数或计数器。用此方式，可以在广播消息的有效载荷中不使用明文来发送无线标识发射机的随机数或计数器值（或随机数）。

[0322] 在方框 2102 中，无线标识发射机的用户可以在中央服务器中注册该设备。例如，无线标识发射机可以向中央服务器提供该唯一设备标识符（即，设备 ID），以便存储在注册的无线标识发射机的数据库中。在方框 2402 中，无线标识发射机可以存储中央服务器知道的第一密钥 (K) 和第二密钥 (K') 以及初始的随机数或计数器。例如，可以在本申请中所描述的注册操作期间，在中央服务器与该无线标识发射机之间共享这些值。在方框 2404 中，无线标识发射机可以通过将当前的随机数或计数器设置为初始的随机数或计数器值，来对这些随机数或计数器进行初始化。

[0323] 类似于上面参照图 20 所描述的，在方框 2406 中，无线标识发射机可以通过流式的加密算法（例如，AES-CTR），对设备标识符（设备 ID）、第一密钥 (K) 和当前的随机数或计数器进行编码，以生成滚动标识符。在方框 2408 中，无线标识发射机可以通过伪随机函数对当前的随机数或计数器和第二密钥 (K') 进行编码，以生成编码的计数器或随机数。在一个实施例中，可以通过下式来表示该编码的随机数或计数器：

[0324] 编码的随机数 / 计数器 = MSB_M(PRF(K', t))，

[0325] 其中，“K'”是每一设备的第二密钥（其通常与第一每一设备的密钥 K 不相同），“t”是当前的随机数或计数器，PRF()' 是伪随机函数，“MSB_M()”意味着“M”个最高有效位（例如，20 比特）。

[0326] 在方框 2410 中，无线标识发射机可以定期地发送广播消息，所述广播消息包括具有滚动标识符和编码的随机数或计数器的有效载荷。在判断框 2114 中，无线标识发射机可以判断预先定义的随机数或计数器时间段是否已到期。如果该随机数或计数器时间段还没有到期（即，判断框 2114 =“否”），则无线标识发射机可以继续执行方框 2410 中的操作。如果该设备确定该随机数或计数器时间周期已到期（即，判断框 2114 =“是”），则在方框 2412 中，无线标识发射机可以对当前的随机数或计数器值进行递增（例如，加 1）。在方框 2117 中，无线标识发射机可以对随机数或计数器时间段进行重置，并且可以继续执行方框 2406 中的操作。

[0327] 图 24B 描绘了用于中央服务器接收和处理包括滚动标识符和编码的随机数或计数器的消息的实施例方法 2450。中央服务器可以结合或者响应于无线标识发射机执行上面所描述的方法 2400，来执行方法 2450 的操作。该方法可以包括两路：第一路，其中，中央服务器尝试基于所接收的消息（例如，目击消息）中的编码的随机数或计数器，来识别无线标识发射机，以及第二路，其中，中央服务器基于所接收的消息中的滚动标识符，尝试该识别。

[0328] 在方框 2452 中，中央服务器可以针对该系统中的所有无线标识发射机，建立具有设备标识符（即，设备 ID）、初始随机数或计数器、当前随机数或计数器、以及密钥（K 和 K'）的数据库条目。在无线标识发射机的注册时刻，所述当前的随机数或计数器值可以与初始的随机数或计数器相同。在方框 2454 中，中央服务器可以针对所有无线标识发射机，使用伪随机函数、第二密钥（K'）和当前的随机数或计数器值，对编码的随机数或计数器进行预先计算。例如，中央服务器可以针对每一个注册的无线标识发射机，生成多个编码的随机数或计数器值，例如，一个基于当前的随机数或计数器值，另一个基于与当前的计数器值相比更大的一个值等。在一个实施例中，中央服务器可以针对每一个注册的无线标识发射机，预先计算 24 个编码的随机数或计数器。在一个实施例中，中央服务器可以针对所有注册的无线标识发射机，都存储预先计算的编码的随机数或计数器的单独列表（或数据表），其还包括与每一个存储的预先计算的编码的随机数或计数器相关联的设备标识符。

[0329] 在方框 2456 中，中央服务器可以接收包括编码的随机数或计数器和滚动标识符的消息，例如，在邻近广播接收机发送的目击消息之中。在方框 2458 中，中央服务器可以从所接收的消息中提取编码的随机数或计数器，在方框 2018 中，可以从所接收的消息中提取滚动标识符。在判断框 2460 中，中央服务器可以判断所提取的随机数或计数器（或“ctr”）是否与预先计算的随机数或计数器中的任一随机数或计数器相匹配。例如，中央服务器可以将从所接收的消息中提取的编码的随机数或计数器值，与用于每一个注册的无线标识发射机的多个中央服务器编码的随机数或计数器值进行比较，以识别任何匹配。如果所提取的随机数或计数器与预先计算的随机数或计数器相匹配（即，判断框 2460 ＝“是”），则在方框 2462 中，中央服务器可以基于匹配的预先计算的随机数或计数器来识别候选的无线标识发射机。换言之，中央服务器可以将该候选者识别成结合预先计算的随机数或计数器在中央服务器中的数据表里存储的设备 ID。在方框 2464 中，中央服务器可以使用所存储的候选无线标识发射机的信息（例如，设备 ID、密钥等），通过流式加密算法（例如，相同的 AES-CTR 无线标识发射机在执行图 24A 中的操作时使用的算法）对滚动标识符进行解码，以发现解码设备标识符（或 M）。在判断框 2466 中，中央服务器可以判断解码后的设备标识符 (M) 是否与该候选无线标识发射机的设备 ID 相匹配。这种匹配可以使中央服务器能够识别与所接收的滚动标识符相关联的无线标识发射机，而无需对该滚动标识符或者编码的随机数或计数器值进行解码。如果该设备 ID 和解码的标识符 (M) 相匹配（即，判断框 2466 ＝“是”），则在方框 2470 中，中央服务器可以将所接收的消息识别成源自于该候选无线标识发射机。在方框 2472 中，中央服务器可以对当前随机数或计数器和预先计算的编码的随机数或计数器进行更新。例如，可以使用新的当前随机数或者计数器信息，以及新的预先计算的编码的随机数或计数器，对用于被识别成所接收的消息的发起方的无线标识发射机的数据库条目进行更新。另外，任何存储的预先计算的编码的随机数或计数器列表，可以在将与所识别的无线标识发射机相对应的新计算出编码的随机数或计数器添加到该列表的同时，删除更旧的预先计算的编码的随机数或计数器。在另一个实施例中，如果被识别成所接收的消息的发起方的无线标识发射机，在中央服务器的数据库中指示成“没有被激活”（即，没有设置标志），则中央服务器还可以对该数据库进行调整，以便反映现在激活了所识别的无线标识发射机（例如，设置一个标志）。随后，中央服务器可以继续执行方框 2456 中的操作。

[0330] 如果该设备 ID 和解码的标识符 (M) 不匹配（即，判断框 2466 ＝“否”），则在判断

框 2468 中，中央服务器可以判断是否存在其它候选者，例如，中央服务器还没有评估的其它已注册的无线标识发射机。如果存在其它候选者（即，判断框 2468 ＝“是”），则中央服务器可以继续执行方框 2462 中的操作，例如通过识别下一个无线标识发射机以便关于滚动标识符进行评估。

[0331] 如果不存在其它候选者（即，判断框 2468 ＝“否”），或者如果所提取的随机数或计数器与预先计算的随机数或计数器不匹配（即，判断框 2460 ＝“否”），则中央服务器可以通过将所提取的滚动标识符与和系统中的所有注册的无线标识发射机相关联的信息进行比较，来尝试识别所接收的消息的发起方。因此，在判断框 2170 中，中央服务器可以判断是否存在另一个注册的无线标识发射机要进行评估。例如，中央服务器可以迭代地使用所有注册的无线标识发射机的信息。如果不存在另一个注册的无线标识发射机（即，判断框 2170 ＝“否”），则中央服务器可以继续执行方框 2456 中的操作。

[0332] 如果存在另一个注册的无线标识发射机（即，判断框 2170 ＝“是”），则在方框 2164 中，中央服务器可以选择下一个注册的无线标识发射机。在方框 2474 中，中央服务器可以通过流式加密算法（例如，AES-CTR），与所使用的无线标识发射机的初始随机数或计数器和第一密钥 (K)，对滚动标识符进行解码，以发现解码后的设备标识符 (M’)，其类似于上面参照图 20 所描述的。在判断框 2476 中，中央服务器可以判断解码后的设备标识符 (M’) 是否与所选定的无线标识发射机的设备 ID 相匹配。如果这些标识符不匹配（即，判断框 2476 ＝“否”），则中央服务器可以继续执行判断框 2170 中的操作。但是，如果这些标识符相匹配（即，判断框 2476 ＝“是”），则在方框 2478 中，中央服务器可以将所接收的消息识别成源自于所选定的无线标识发射机，并可以继续执行方框 2472 中的操作。

[0333] 图 24C 描绘了用于中央服务器接收和处理包括滚动标识符和编码的随机数或计数器的消息的实施例方法 2480。方法 2480 的操作类似于方法 2450 的操作，除了不是执行上面在图 24B 中所讨论的两路处理，而是中央服务器可以将方法 2480 执行成一路处理。具体而言，中央服务器可以生成针对每一个注册的无线标识发射机的多个中央服务器加密的随机数或计数器值、以及多个中央服务器加密的设备标识符（即，设备 ID）。中央服务器可以使用数据库中针对每一个无线标识发射机所存储的数据（例如，设备 ID、K、K’、初始的随机数或计数器、以及当前的随机数或计数器）、以及用于每个设备的多个预先计算的随机数或计数器值，来对多个中央服务器加密的随机数或计数器值以及多个服务器加密的设备 ID 进行编码。当中央服务器接收到包括滚动标识符和编码的随机数或计数器的目击消息时，中央服务器可以将所述多个中央服务器加密的随机数或计数器值以及所述多个中央服务器编码的设备 ID，与从所接收的目击消息获得的滚动标识符以及编码的随机数或计数器进行比较。随后，可以完全基于对预先计算的随机数或计数器值以及设备标识符进行比较，而无需对该滚动标识符自身进行实际解码，来识别发起该滚动标识符的无线标识发射机的设备标识符。

[0334] 在方框 2452 中，中央服务器可以针对该系统中的所有无线标识发射机，建立具有设备标识符（即，设备 ID）、初始的随机数或计数器、当前的随机数或计数器、以及密钥 (K 和 K’）的数据库条目。在方框 2454 中，中央服务器可以针对所有无线标识发射机，使用伪随机函数、第二密钥 (K’）以及当前的随机数或计数器值，对编码的随机数或计数器进行预先计算。在方框 2482 中，中央服务器可以针对所有无线标识发射机，使用流式加密算法（例

如，AES-CTR 块密码）、设备标识符、当前的随机数或计数器、以及第一密钥 (K)，对编码的设备标识符进行预先计算。换言之，中央服务器可以针对每一个注册的无线标识发射机，生成多个编码的设备标识符，例如通过使用当前的随机数或计数器以及预先定义的偏移随机数或计数器值，或者替代地，仅仅单个编码的设备标识符是基于中央服务器中存储的当前的随机数或计数器。

[0335] 在方框 2456 中，中央服务器可以接收包括编码的随机数或计数器以及滚动标识符的消息，例如，在由邻近广播接收机发送的目击消息中。在方框 2458 中，中央服务器可以从所接收的消息中提取编码后的随机数或计数器，在方框 2018 中，可以从所接收的消息中提取滚动标识符。在判断框 2460 中，中央服务器可以判断所提取的随机数或计数器（或“ctr”）是否与预先计算的随机数或计数器中的任一个相匹配。如果所提取的随机数或计数器与预先计算的随机数或计数器相匹配（即，判断框 2460 =“是”），则在方框 2462 中，中央服务器可以基于匹配的预先计算的随机数或计数器，来识别候选的无线标识发射机。在判断框 2484 中，中央服务器可以判断所提取的滚动标识符是否与预先计算的标识符（例如，针对候选的无线标识发射机的预先计算的设备标识符）中的任一个相匹配。

[0336] 如果所提取的滚动标识符与针对候选的无线标识发射机所预先计算的标识符中的任一个相匹配（即，判断框 2484 =“是”），则在方框 2470 中，中央服务器可以将所接收的消息识别成源自于该候选无线标识发射机。在方框 2472’ 中，中央服务器可以对当前的随机数或计数器和预先计算的编码的随机数或计数器，以及预先计算的编码的设备标识符进行更新。例如，可以使用新的当前随机数或者计数器信息、以及新的预先计算的编码的随机数或计数器和预先计算的编码的设备标识符，对用于被识别成所接收的消息的发起方的无线标识发射机的数据库条目进行更新。另外，预先计算的编码的随机数或计数器的任何存储的列表，可以在将与所识别的无线标识发射机相对应的新计算出的编码的随机数或计数器或者设备标识符添加到该列表的同时，删除更旧的预先计算的编码的随机数或计数器或者编码的设备标识符。在另一个实施例中，如果被识别成所接收的消息的发起方的无线标识发射机，在中央服务器的数据库中指示成“没有被激活”（即，没有设置标志），则中央服务器还可以对数据库进行调整，以便反映现在对所识别的无线标识发射机进行激活（例如，设置一个标志）。随后，中央服务器可以继续执行方框 2456 中的操作。

[0337] 如果所提取的滚动标识符与针对候选的无线标识发射机所预先计算的标识符中的任何一个都不匹配（即，判断框 2484 =“否”），则在判断框 2468 中，中央服务器可以判断是否存在其它候选者，例如，中央服务器还没有评估的其它注册的无线标识发射机。如果存在其它候选者（即，判断框 2468 =“是”），则中央服务器可以继续执行方框 2462 中的操作，例如通过识别下一个无线标识发射机以便关于滚动标识符进行评估。

[0338] 如果不存在其它候选者（即，判断框 2468 =“否”），或者如果所提取的随机数或计数器与预先计算的随机数或计数器不匹配（即，判断框 2460 =“否”），则中央服务器可以通过将所提取的滚动标识符与和系统中的所有注册的无线标识发射机相关联的信息进行比较，来尝试识别所接收的消息的发起方。因此，在判断框 2170 中，中央服务器可以判断是否存在另一个注册的无线标识发射机要进行评估。例如，中央服务器可以迭代地使用所有注册的无线标识发射机的信息。如果不存在另一个注册的无线标识发射机（即，判断框 2170 =“否”），则中央服务器可以继续执行方框 2456 中的操作。

[0339] 如果存在另一个注册的无线标识发射机（即，判断框 2170 =“是”），则在方框 2164 中，中央服务器可以选择下一个注册的无线标识发射机。在方框 2474 中，中央服务器可以通过流式加密算法（例如，AES-CTR），与所选定的无线标识发射机的初始随机数或计数器和第一密钥 (K)，对滚动标识符进行解码，以找到解码后的设备标识符 (M')。在判断框 2476 中，中央服务器可以判断解码后的设备标识符 (M') 是否与所选定的无线标识发射机的设备 ID 相匹配。如果这些标识符不匹配（即，判断框 2476 =“否”），则中央服务器可以继续执行判断框 2170 中的操作。但是，如果这些标识符相匹配（即，判断框 2476 =“是”），则在方框 2478 中，中央服务器可以将所接收的消息识别成源自于所选定的无线标识发射机，并继续执行方框 2472' 中的操作。

[0340] 图 25A 描绘了用于无线标识发射机通过协商的通信链路，与邻近广播接收机执行双向无线通信的实施例方法 2500。如上所述，无线标识发射机可以从邻近广播接收机接收并处理短距离无线传输（例如，蓝牙 LE 分组等）。但是，无线标识发射机还可以使用协商的、一对一通信链路，从特定的邻近广播接收机接收数据。这种链路的示例可以通过蓝牙®配对和 / 或结合 (bond) 来实现。

[0341] 在方框 552 中，无线标识发射机可以对随机数或计数器（例如，随机数或计数器变量）进行重置，以指示该无线标识发射机可能不接收消息的时段的起点（或初始化）。在方法 554 中，无线标识发射机可以生成包括标识信息、随机数或计数器、以及可用于接收消息的时间的消息。在方框 556 中，发射机可以通过短距离无线传输来广播所生成的消息（例如，蓝牙 LE 分组）。在判断框 558 中，无线标识发射机可以判断预先定义的随机数或计数器时间段是否已经到期。如果该随机数或计数器时间段还没有到期（即，判断框 558 =“否”），则在方框 556 中，无线标识发射机可以继续定期地广播所生成的消息。

[0342] 如果该随机数或计数器时间周期已到期（即，判断框 558 =“是”），则在方框 560 中，无线标识发射机可以对该随机数或计数器进行递增，在判断框 562 中，基于该随机数或计数器值，判断该无线标识发射机是否变得可用。如果其不可用于接收消息（即，判断框 562 =“否”），则无线标识发射机可以继续执行方框 554 中的操作，以生成要广播的新消息。如果该无线标识发射机可用于接收消息（即，判断框 562 =“是”），则在可选框 2526 中，无线标识发射机可以发送用于指示其可用于接收消息的消息。在一个实施例中，该消息可以包括在方框 556 中发送的各种生成的广播消息内已发送的信息。

[0343] 在方框 2528 中，无线标识发射机可以对链路通告消息进行监听，其中该链路通告消息可以是邻近广播接收机发送的用于指示建立通信链路所需要的信息的消息。例如，链路通告消息可以包括邻近广播接收机为了与无线标识发射机进行配对所需要的蓝牙 MAC 地址或者其它信息。在判断框 2530 中，无线标识发射机可以判断是否已经从例如邻近广播接收机接收到链路通告消息。如果没有接收到链路通告消息（即，判断框 2530 =“否”），则在判断框 568 中，无线标识发射机可以判断该接收时间段是否已到期。该接收时间段可以是可用于接收链路通告消息的时段。

[0344] 如果已接收到链路通告消息（即，判断框 2530 =“是”），则在方框 2532 中，无线标识发射机可以与邻近广播接收机协商（或建立）通信链路。例如，无线标识发射机可以建立蓝牙绑定，并且基于所接收的链路通告消息中的信息与邻近广播接收机进行配对。在可选框 2534 中，无线标识发射机可以对链路进行认证。这种认证可以确保在该链路通告消

息中所指示的邻近广播接收机的标识与参与所协商 / 建立的通信链路的设备相同。在一个实施例中，这种认证可以涉及：发送用于请求确认标识的数据分组，并执行对通过所建立的链路而接收的数据和在链路通告消息中接收的数据进行比较。在一个实施例中，这种认证可以涉及：将接收由配对的邻近广播接收机所发送的 PIN 信息，与该无线标识发射机中存储的已知或可接受 PIN 值的列表进行比较。一旦建立（并认证）了通信链路，则在方框 564 中，无线标识发射机可以监听输入的消息（例如，通过协商链路的来自邻近广播接收机的数据），在方框 566 中，可以对所接收的输入消息进行处理。在判断框 568 中，无线标识发射机可以判断该接收时间段是否到期。如果是（即，判断框 568 ＝“是”），则无线标识发射机可以继续执行方框 552 中的操作。但是，如果该接收时间段还没有到期（即，判断框 568 ＝“否”），则无线标识发射机仍然可用于接收消息，并且可以在方框 2528 中，继续对链路通告消息进行监听。

[0345] 图 25B 描绘了用于邻近广播接收机向可用的无线标识发射机发送消息的实施例方法 2550。方法 2550 的操作可以与上面参照图 25A 所描述的操作相对应。在方框 902 中，邻近广播接收机可以从无线标识发射机接收广播消息（例如，蓝牙 LE 广播）。在方框 2552 中，邻近广播接收机可以对所接收的广播消息进行分析。邻近广播接收机可以对所接收的广播消息中的报头或元数据进行分析，并解析和评估该消息中的各种数据。在一个实施例中，该广播消息可以包含加密数据和非加密数据，其中接收机可以被配置为或者可以不被配置为解密或以其它方式访问。在一个实施例中，邻近广播接收机可以向中央服务器发送所接收的广播消息，以便进行解密、处理，在返回消息中提供用于指示邻近广播接收机可以如何对所接收的广播消息进行响应的指令。例如，返回消息可以指示邻近广播接收机发送链路通告消息，或者开始与该无线标识发射机的配对操作。

[0346] 另外，如上所述，所接收的广播消息可以包含定时、随机数或计数器、递减计数、或者用于指示该无线标识发射机接收消息的可用性的调度信息。例如，所接收的广播消息可以指示该无线标识发射机将在规定的时间窗内接受输入消息。再举另一个例子，当接收的广播消息包含特定信息（例如，指示可用性的符号）时，邻近广播接收机可以确定其可以向无线标识发射机发送消息。

[0347] 基于所接收的广播消息的分析，在判断框 2554 中，邻近广播接收机可以判断该无线标识发射机是否可用于接收输入消息。换言之，邻近广播接收机可以判断所接收的广播消息是否包括：用于指示该无线标识发射机何时可用于从该邻近广播接收机接收消息的信息。如果该无线标识发射机可用于接收输入消息（即，判断框 2554 ＝“是”），则在判断框 2556 中，邻近广播接收机可以判断是否存在要向该无线标识发射机传输的存储消息（例如，存储在存储器中）。在一个实施例中，无线标识发射机可以从中央服务器接收用于传输的消息。替代地，用于向无线标识发射机传输的消息，可以替代地由邻近广播接收机产生。例如，智能电话邻近广播接收机（或者移动的邻近广播接收机）可以在软件应用（或“app”）中接收用于指示该无线标识发射机修改其行为（例如，信令调度、强度等）的用户输入。要传输的消息可以包括软件或固件升级、用于执行的指令、配置信息、调试命令、以及该无线标识发射机要使用的其它数据。例如，用于传输的消息可以指示无线标识发射机激活诸如加速计之类的传感器单元，开始收集传感器数据，以便并入到后续的广播消息中。用于传输的消息还可以指示无线标识发射机对广播的信号强度进行调制，减少或增加广播的

频率，改变在广播消息中表示的数据，并且以其它方式调整后续传输的特性和 / 或改变该无线标识发射机的行为。例如，可以指示无线标识发射机缩短其广播信号传输范围，以模拟近场通信 (NFC)。

[0348] 如果邻近广播接收机具有要向该无线标识发射机传输的消息（即，判断框 2556 =“是”），则在方框 2558 中，邻近广播接收机可以发送链路通告消息，该链路通告消息包括用于建立链路的信息。该链路通告消息可以包括 :无线标识发射机用于建立蓝牙®配对 / 结合所需要的信息。在方框 2560 中，邻近广播接收机可以与无线标识发射机协商（或建立）链路。例如，无线标识发射机和邻近广播接收机可以建立安全的蓝牙®链路。一旦建立了链路，则在方框 2562 中，邻近广播接收机可以通过所建立的与无线标识发射机的链路，来发送用于传输的消息。

[0349] 如果该无线标识发射机不可用于接收输入消息（即，判断框 2554 =“否”），或者如果邻近广播接收机没有要向该无线标识发射机传输的消息（即，判断框 2556 =“否”），或者如果邻近广播接收机已使用在方框 2562 中的操作，通过建立的链路发送了用于传输的消息，则在方框 706 中，邻近广播接收机可以向中央服务器发送目击消息，并继续执行方框 902 中的操作。

[0350] 图 25C 描绘了用于无线标识发射机使用滚动蓝牙 MAC 地址（同时与移动设备相配对），来发送安全性增加的消息的实施例方法 2570。如上所述，当通过蓝牙协议来发送分组时，无线标识发射机可以被配置为 :定期地改变每个蓝牙消息中表示的蓝牙 MAC 地址（其在图 25C 中被称为“BT MAC 地址”），以维持隐私。这是重要的，因为 :甚至在使用加密算法（如上所述）来生成用于在传输中进行广播的滚动标识符时，也可以基于其传输中的静态信息来追踪或跟踪无线标识发射机。例如，恶意的数据包嗅探器可以基于无线标识发射机的广播消息内的静态蓝牙 MAC 地址来跟踪该无线标识发射机，其中该广播消息包括滚动标识符（例如，具有加密的设备 ID 的有效载荷）。在各个实施例中，无线标识发射机可以使用上面所描述的加密方案对蓝牙 MAC 地址进行模糊，以便通过与对设备标识符进行模糊相类似的方式，来创建滚动蓝牙 MAC 地址。在各个实施例中，被配置为通过蓝牙传输进行通信和 / 或与其它无线设备进行配对的任何通信设备，在发送短距离无线传输时，可以执行方法 2570 以提高私密性。例如，无线耳机（或者耳麦）在与智能电话配对时，可以执行方法 2570。

[0351] 在方框 2572 中，无线标识发射机可以与移动设备建立链路。例如，无线标识发射机可以与已知的移动设备（例如，用户的电话）执行标准蓝牙配对。在方框 2104 中，无线标识发射机可以例如通过将初始的随机数或计数器设置为 0 或某个随机数，对该随机数或计数器进行初始化。在判断框 452 中，无线标识发射机可以判断其是否需要新的蓝牙 MAC 地址。这种判断可以是基于定时器的到期、所接收的用于指示新 MAC 地址的信号、或者用于定期地产生新的蓝牙 MAC 地址的任何其它机制。例如，定时器可以每几分钟、几小时等到期，其指示该无线标识发射机应当生成新的蓝牙 MAC 地址。如果需要新的蓝牙 MAC 地址（即，判断框 452 =“是”），则在方框 2116 中，无线标识发射机可以对所述随机数或计数器值进行递增，例如，将该值增加设置的值（例如，“1”）。

[0352] 如果不需要新的蓝牙 MAC 地址（即，判断框 452 =“否”），或者如果对所述随机数或计数器进行了递增，则在方框 2574 中，无线标识发射机可以使用该随机数或计数器、以及与移动设备共享的加密算法，来生成滚动蓝牙 MAC 地址。这种算法可以启用上面所描述

的加密算法或技术中的任何一种（例如，伪随机函数、AES-CTR 等）。在方框 2578 中，无线标识发射机可以使用该滚动蓝牙 MAC 地址，向配对的移动设备发送消息。例如，该分组可以包括用于指示该分组是由与滚动蓝牙 MAC 地址相关联的设备进行发送的或者通过滚动蓝牙 MAC 地址进行标识的数据。在可选框中，无线标识发射机可以对来自配对的移动设备的任何输入消息进行处理。例如，无线标识发射机可以接收和使用移动设备发送的固件、软件指令、配置数据和其它信息。在可选框 2576 中，无线标识发射机可以休眠一段时间（例如，几毫秒、几秒、或者几分钟），随后可以继续执行判断框 452 中的操作。

[0353] 图 25D 描绘了用于移动设备（例如，智能电话）对于从使用滚动蓝牙 MAC 地址的无线标识发射机接收的消息进行处理的实施例方法 2580。在各个实施例中，该移动设备可以使用上面所描述的加密（和 / 或解密）方案，对所接收的传输中的滚动蓝牙 MAC 地址进行解码和 / 或重复，以便维持与无线标识发射机的链路。在方框 2560 中，该移动设备可以与无线标识发射机协商和 / 或建立链路（例如，蓝牙配对链路）。该移动设备可以维持可与移动设备进行配对的所有设备的列表、以及建立该链路所需要的任何初始信息。在方框 2581 中，移动设备可以存储与配对的无线标识发射机共享的随机数或计数器。可以在该链路的建立期间接收该随机数或计数器，或者可以（例如，在该移动设备与无线标识发射机之间的结合或注册过程期间）预先设定该随机数或计数器。在各个实施例中，该移动设备可以是使用蓝牙无线装置和 / 或蓝牙通信协议的任何通信设备。

[0354] 在方框 2582 中，移动设备可以对失败计数进行初始化。换言之，移动设备可以存储失败的次数（例如，存储在整数系统变量中）。在方框 2584 中，移动设备可以从配对的无线标识发射机接收消息。在方框 2585 中，移动设备可以使用随机数或计数器以及与无线标识发射机共享的加密算法，来生成期望的蓝牙 MAC 地址。该算法可以类似于上面所描述的算法，并可以被执行成软件或其它操作，以便生成可以与从所配对的无线标识发射机接收的传输中的地址进行比较的滚动蓝牙 MAC 地址。

[0355] 在判断框 2586 中，移动设备可以判断所接收的地址是否与预期的地址相匹配。换言之，移动设备可以将所生成的预期的蓝牙 MAC 地址与从所配对的无线标识发射机接收的消息中指示的地址相匹配。

[0356] 如果这些地址相匹配（即，判断框 2586 ＝“是”），则在方框 2587 中，该移动设备可以例如通过以下方式来处理所接收的消息：对所接收的消息中的信息进行解密，向中央服务器发送用于报告所接收的消息的接收的消息（例如，目击消息），或者使用所接收的消息中的数据来执行软件操作（例如，配置智能电话上的应用）。在方框 2588 中，该移动设备可以对失败计数进行重置，在判断框 2589 中，判断是否要对所述随机数或计数器进行更新。判断框 2589 中的操作可以类似于上面参照图 25C 所描述的无线标识发射机在判断框 452 中所执行的那些操作。例如，该移动设备可能需要每几个时钟周期，或者响应于从配对的设备接收到某个数量的消息，对所述随机数或计数器进行更新。如果确实需要对该随机数或计数器进行更新（即，判断框 2589 ＝“是”），则在方框 2590 中，该移动设备可以对该随机数或计数器进行递增（例如，加“1”）。如果不需要对该随机数或计数器进行更新（即，判断框 2589 ＝“否”），或者如果该随机数或计数器已递增，则该移动设备可以继续执行方框 2584 中的操作。

[0357] 如果这些地址不匹配（即，判断框 2586 ＝“否”），则在判断框 2591 中，该移动设

备可以判断失败计数是否超过门限。换言之，在丢弃与该无线标识发射机的链路之前，可以将失败计数的值（例如，系统变量），与允许该移动设备对所接收的地址和期望的地址未能匹配的预定次数进行比较。如果失败计数超过了门限（即，判断框 2591 ＝“是”），则在方框 2592 中，该移动设备可以忽略该消息和 / 或不参与该配对链路。

[0358] 如果失败计数没有超过门限（即，判断框 2591 ＝“否”），则在方框 2593 中，移动设备可以对所述随机数或计数器改变一个失败偏移值。该移动设备可以被配置为 :对所述随机数或计数器修改各种偏移值，以便说明在配对的设备之间的随机数或计数器漂移，例如如上所述。例如，当期望的地址与所接收的地址不匹配时，该移动设备可以对所述随机数或计数器增加偏移值“1”，并且生成另一个预期的蓝牙 MAC 地址，以便与所接收的消息的蓝牙 MAC 地址进行比较。在方框 2594 中，该移动设备可以对失败计数进行递增（例如，将该值增加一），以便指示生成的期望的蓝牙 MAC 地址与所接收的消息的地址不匹配。随后，该移动设备可以继续执行方框 2585 中的操作，以生成用于与所接收的消息地址进行比较的新的期望地址。

[0359] 图 26A 描绘了示例性无线标识发射机 110 的组件。无线标识发射机 110 可以包括微控制器 2602、耦接到天线 2606 的短距离无线装置 2604（例如，蓝牙®无线装置或收发机）、存储器 2608 和电池 2610。虽然将这些组件示出为通过共同连接进行链接，但可以用各种方式对它们进行互连和配置。例如，无线标识发射机 110 可以被配置为使得微控制器 2602 可以基于存储器 2608 的内容，确定何时发送消息。在一个实施例中，微控制器 2602 可以是蓝牙片上系统单元。存储器 2608 还可以包括由短距离无线装置 2604 基于来自微控制器 2602 的命令，通过天线 2606 来发送的一个或多个消息或者消息的一部分。电池 2610 可以根据其它组件的需要来供电。此外，在一些实现中，可以将微控制器 2602、短距离无线装置 2604 和 / 或存储器 2608 一起集成为单个集成电路。由于这些组件可以是标准或现成配置的微芯片，因此在图 26A 中将它们表示成符合示例性实施例的结构的框图。

[0360] 无线标识发射机 110 可以与各种物品（例如，手镯）相耦合，或者内建到各种物品中。例如，示例性无线标识发射机 110 可以具有容易连接到带子（例如，表带或狗项圈）的形式。替代的实施例可以将无线标识发射机 110 并入到可能需要跟踪的任何其它移动对象中。

[0361] 无线标识发射机 110 可以通过定期地进入省电模式或者进入休眠（例如，在休眠和广播具有无线标识发射机 110 的识别码的分组之间定期地交替）来省电。各个实施例可以包括广播和休眠的不同循环，例如，一些实施例更频繁或者更不频繁地进行广播，例如，在休眠周期之间，每隔几秒或几分钟进行苏醒和广播。

[0362] 在一个实施例中，电池 2610 可以是可更换的纽扣电池。在另一个实施例中，无线标识发射机 110 可以使用天线 2606 来接收更新软件、指令或者用于存储并在配置操作中使用的其它数据，例如配置传输时间间隔和 / 或发射功率。无线标识发射机 110 还可以存储并执行软件、算法、指令、代码、或者用于生成滚动码或标识符的其它例行程序，如上面参照图 3 所描述的。在一个实施例中，无线标识发射机可以不维持时间（例如，UTC）信息，而是可以使用 30ppm 16kHz 晶振作为时钟。这种将晶振用作时钟，可能每年产生大约 40 秒的定时漂移。

[0363] 图 26B 描绘了实施例无线标识发射机 110 的组件。类似于上面参照图 26A 所描

述的实施例，无线标识发射机 110 可以包括微控制器 2602、连接到天线 2606 并耦接到微控制器 2602 的短距离无线装置 2604（例如，蓝牙 ®、BTLE、Zigbee®、Peanut®等）、存储器 2608 和电池单元 2610。替代地，存储器 2608 可以被包含在微控制器 2602 中，其中该微控制器 2602 还可以包括单独的处理单元。短距离无线装置 2604 可以是能够广播包括设备 ID 的消息或信号的发射机，或者替代地，可以是被配置为发送和接收 RF 信号的收发机，从而实现使用通信协议与其它设备进行通信。例如，无线标识发射机 110 可以被配置为与其它启用短距离无线的设备（例如，智能电话）进行通信。在一个实施例中，短距离无线装置 2604 可以被配置为通过诸如 LTE-D、对等 LTE-D 和 WiFi-Direct 之类的各种低功耗的无线通信协议进行通信。

[0364] 在一个实施例中，无线标识发射机 110 可以包括扬声器（没有示出），该扬声器被配置为发出能够由邻近广播接收机进行接收和 / 或能够由用户听到的声音。例如，无线标识发射机 110 可以发出用于向监听的邻近广播接收机指示其存在性的音频通信。在另一个实施例中，无线标识发射机 110 可以被配置为按照可变的信号强度来发送信号，从而改变邻近广播接收机能够对来自无线标识发射机 110 的广播进行接收的范围。

[0365] 另外，无线标识发射机 110 可以包括用于对各种状况和变量进行测量的一个或多个传感器。在一个实施例中，无线标识发射机 110 可以包括加速计 2615（或者诸如陀螺仪或重力计之类的任何其它运动传感器），该加速计 2615 可以收集用于指示与无线标识发射机 110 相关联的资产的运动的数据。例如，加速计 2615 可以生成用于描述携带无线标识发射机 110 的儿童的移动的运动数据。无线标识发射机 110 中可以包含的其它传感器包括：温度传感器 2616（例如，热敏电阻）、辐射传感器 2617、湿度传感器 2618、以及二氧化碳 ($CO_2$) 传感器 2619。在各个实施例中，无线标识发射机 110 可以包括这些和其它传感器的任意组合。这些潜在传感器只是可以集成到无线标识发射机 110 的传感器类型的示例，还可以包括其它类型的传感器。例如，无线标识发射机 110 还可以包括在各个附图中没有示出的传感器，例如，麦克风、相机、热传感器、压力传感器和光传感器。

[0366] 图 27A 描绘了示例性邻近广播接收机实施例的主要组件。该邻近广播接收机 142 可以包括能够与耦接到天线 2706 的短距离无线装置（例如，无线标识发射机中的蓝牙无线装置）进行通信的短距离无线装置 2704（例如，蓝牙无线装置或收发机）、以及能够通过诸如互联网之类的网络，直接或间接向中央服务器 120 通信的第二网络设备 2708。在一些实施例中，第二网络设备 2708 可以是蜂窝或无线装置或调制解调器或者其它有线网络设备。邻近广播接收机 142 还可以包括处理器 2702、存储器 2712 和电池 2710，该电池 2710 用作主电源或者用作备用电源（在邻近广播接收机 142 耦接到公用电源的情况下）。邻近广播接收机 142 可以包括 GPS 接收机 2714、或者用于确定当前位置的其它类型的位置确定机制，以便与从无线标识发射机接收到的任何消息进行关联。如果该邻近广播接收机不是移动的，则在一些实施例中，其可能不包括 GPS 接收机 2714，这是由于该位置可能是已知并且不变的。虽然将这些组件示出为通过共同的连接进行链接，但可以通过各种方式对它们进行互连和配置。由于这些组件可以是标准或者现成配置的微芯片，因此在图 27A 中将它们表示成与示例性实施例的结构相一致的方框。

[0367] 图 27B 描绘了可以插入到电源插座的实施例邻近广播接收机 2775。类似于上面参照图 27A 所描述的实施例，邻近广播接收机 2775 可以包括处理器 2702、存储器单元 2712

和连接到天线 2706 的短距离无线装置 2704（例如，蓝牙®、蓝牙 LE、LTE-D、对等 LTE-D、Zigbee®、Peanut®等等）。邻近广播接收机 2775 还可以包括耦接到第二天线 2776 的 WiFi 片上系统 2778（其在图 27C 中称为“SOC”）。在另一个实施例中，片上系统 2778 可以是蓝牙低功耗片上系统。邻近广播接收机 2775 可以使用片上系统 2778 来通过无线局域网来交换数据（例如，通过与 WiFi 路由器进行通信）。另外，邻近广播接收机 2775 可以包括用于与电源或以其它方式接收供电（例如，交流电源（或“AC”））进行对接的插头 2782。在各个实施例中，插头 2782 可以被配置为与不同的电源插座标准（例如，英国标准、美国国家电气制造商协会等）相连接，并且可以包括接地元件（没有示出）。插头 2782 可以耦接到 USB 电源 2780，该 USB 电源 2780 向邻近广播接收机 2775 的各个组件（例如，处理器 2702）提供电源。在一个替代的实施例中，邻近广播接收机 2775 可以使用从插头 2782 和 / 或 USB 电源 2780 所接收的供电，对内部电池（没有示出）进行充电。

[0368] 在一个实施例中，邻近广播接收机 2775 可以在存储器 2712 或者其它电路中存储软件指令，其中处理器 2702 和 / 或片上系统 2778 可以使用这些软件指令来执行分别发送和 / 或接收短距离和远距离信号的操作。在一个实施例中，邻近广播接收机 2775 可以使用天线 2706、2776 来接收更新软件、指令或用于存储的其它数据，并用于更新固件、修改操作参数和其它配置修改。

[0369] 如上所述，可以在标准蓝牙 LE 消息格式的有效载荷中传输滚动标识符和其它信息。图 28 描绘了实现实施例滚动标识符的示例性蓝牙 LE 消息结构。根据一种实施例，广播消息 2800 可以包括普通蓝牙 LE 消息的地址和报头、数据字段 2802 到 2808，并可以在该蓝牙消息的有效载荷部分 2810 中包括设备信息和滚动标识符。例如，广播消息 2800 可以包括标准访问地址块 2802，该标准访问地址块 2802 可以是用于标识正在发送的蓝牙消息的类型的 4 字节信息（在本例中，其是不可连接的通告事件）。广播消息 2800 中的下一个数据块可以是通告的分组数据单元类型 2804（例如，一个字节数据），后面可以跟着通告的分组数据单元报头 2806，该通告的分组数据单元报头 2806 后面转而跟着通告的分组数据单元地址 2808（其可以是 6 字节的数据）。标准蓝牙数据字段 2802 到 2808 基本上将该消息标识成不可连接的通告事件，该不可连接的通告事件后面跟着通告的数据分组 2810，该通告的数据分组 2810 包括要发送的任何数据以及唯一滚动标识符。

[0370] 广播蓝牙消息 2800 的通告数据部分 2810 可以将广播信息和滚动标识符并入成两个部分 2820 和 2822。在通告类型蓝牙 LE 分组中，可以包括任何类型的通告数据，其提供灵活性以便在广播消息 2800 中包括滚动标识符和其它数据。在图 28 中所描绘的示例性实施例中，服务通用唯一用户标识符 (UUID) 部分 2820 可以用于传送来自无线标识发射机的传感器或其它数据，例如，如图 28 中所描绘的电池状态和温度。例如，数据部分 2820 可以包括用于指示该数据字段的长度（例如，图 28 中所示出的 11HEX，其指示该消息的这部分长度是 17 个字节）的标准蓝牙数据字段 2830，后面可以跟着数据类型字段 2832，该数据类型字段 2832 提供用于指示在后续信息字节中跟着的信息的类型的代码。跟在这些报头字段 2830、2832 之后的可以是数据部分 2834。该数据部分 2834 可以包括具有通用唯一值形式的代码，该代码可以用作表格查询关键词以获得该代码的意图含义。例如，可以根据用于创建 UUID 的过程，来生成全球唯一标识符号码（即，UUID），随后可以将该 UUID 链接到相应数据

库中的特定含义、值、警报和/或命令，并可以由中央服务器进行维持。因此，可以在符合蓝牙协议但标识特定的消息或状况而不是用作该设备的普通地址或标识符的服务 UUID 字段 2834 中，包括有效的 UUID。例如，可以在数据库中将 UUID 链接到特定的电池水平以及温度值或范围。用此方式，可以使用广播消息 2800 的标准 UUID 部分来传送多种含义、值、警报或者命令，而无需对标准蓝牙协议进行改变。还可以在服务 UUID 部分 2834 中包括原始数据或传感器数据，但这些原始数据可以不符合蓝牙协议，其中该数据表示通用唯一标识符。

[0371] 不以随机方式将 UUID 链接到数据表，而是使用 UUID 的标准格式来在所生成的 UUID 的范围内提供数据字段。例如，图 28 描绘了其中服务 UUID 数据字段 2834 包括 22 比特 UUID 前缀 2840 和 12 字节后缀 2846 的实施例，其中在该前缀和后缀之间包括要发送的三个字节数据（例如，电池水平值字段 2842 和温度值字段 2844）。在该示例中，可以生成 1024 个不同的 UUID，它们包括相同的 UUID 前缀值 2840（例如，960c4）和相同的 UUID 后缀值（例如，244c-11e2-b29-00a0c60077ad）。随后，这种数据结构在前缀和后缀之间提供三个字节数据，以便携带数据，例如两个字节用于指示该无线标识发射机的电池水平（方块 2842），一个字节用于指示测量的温度（方块 2844）。这种数据结构只是提供成一个例子，并且可以使用多种其它数据结构，并可以用此方式来传输不同类型的信息（或者不传输信息）。

[0372] 跟在服务 UUID 部分 2820 之后是数据字段 2822，在数据字段 2822 中可以包括滚动标识符。例如，该标识符数据部分 2822 可以包括分组字节长度 2835，该分组字节长度 2835 标识了该分组中的数据的字节数量。该数据字段后面跟着是分组类型字段 2836，该分组类型字段 2836 包括用于指示跟着的信息类型（在该情况下，该数据字段是特定于制造商的）的代码。在这些报头数据字段后面可以跟着具有例如 2 字节数据的制造商 ID 字段 2837，其可以用于标识制造商或者无线标识发射机的类型、该系统的服务提供商等。可以在消息 2800 的最后部分 2838 中包括滚动标识符。上面描述了用于生成在最后部分 2838 中包括的滚动标识符的各种实施例方法。例如，该数据字段 2838 可以包括：随机数（例如，定时器、随机数或计数器）和使用该随机数生成的模糊“blob”、只有该无线标识发射机和中央服务器才知道的密钥、该无线标识发射机的唯一（例如，MAC）标识符。再举一个上面讨论的例子，该数据字段 2838 可以包括：使用计数器/时钟/随机数所生成的单个“blob”、只有该无线标识发射机和中央服务器知道的密钥、以及该无线标识发射机的唯一（例如，MAC）标识符。

[0373] 在各个实施例中，可以通过减少用于传输数据的服务 UUID 部分 2820 中所包括的数据（即，数据字段 2834）的字节数，来增加在最后数据部分 2822 中所包括的滚动标识符的长度。

[0374] 图 29 是适合用于各种实施例的智能电话类型移动设备的系统框图。智能电话 2900 可以包括耦接到内部存储器 2902、显示器 2903，并且耦接到扬声器 2954 的处理器 2901。此外，智能电话 2900 可以包括用于发送和接收电磁辐射的天线 2904，该天线 2904 可以连接到无线数据链路和/或蜂窝电话收发机 2905，该蜂窝电话收发机 2905 耦接到处理器 2901 并能够通过广域无线通信网络进行通信。智能电话可以包括能够与无线标识发射机进行通信或者与无线标识发射机进行配对的单独的短距离无线收发机 2924。智能电话 2900 通常还可以包括菜单选择按键或者用于接收用户输入的摇臂开关 2908。

[0375] 图30是适合于实现本申请的各种实施例的服务器3000的系统框图。服务器3000可以是市售的服务器设备。这种服务器3000通常包括耦接到易失性存储器3002和大容量非易失性存储器（例如，硬盘驱动器3003）的处理器3001。服务器3000还可以包括耦接到处理器3001的软盘驱动器、压缩光碟（CD）或DCD光碟驱动器3006。服务器3000还可以包括耦接到处理器3001的网络接入端口3004，以便与网络3005（例如，耦接到其它广播系统计算机和服务器的局域网）建立数据连接。

[0376] 处理器2901、3001可以是能通过软件指令（应用）进行配置，以执行多种功能（其包括下面所描述的各种实施例的功能）的任何可编程的微处理器、微计算机或多个处理器芯片或芯片集。在一些移动的邻近广播接收机中，可以提供多个处理器2901，例如，一个处理器专用于无线通信功能，一个处理器专用于运行其它应用。通常，在访问软件应用并将它们装载到处理器2901、3001之前，可以将这些软件应用存储在内部存储器2902、3002、3003中。处理器2901、3001可以包括足够用于存储这些应用软件指令的内部存储器。

[0377] 上述方法描述和处理流程图仅仅作为示意性示例提供，而并不旨在要求或暗示各个实施例的步骤必须按照所给出的顺序来执行。如本领域的技术人员应该了解的是，上述实施例中的步骤顺序可以按照任何顺序来执行。诸如“之后”、“然后”、“接下来”等词语并不旨在限制步骤的顺序；这些词语仅仅用于引导读者通读对这些方法的描述。此外，任何对权利要求元素的单数引用（例如，使用冠词“a”、“an”或者“the”），不应被解释为将该元素限制为单数形式。

[0378] 结合本文所公开的实施例所描述的各种示例性的逻辑框、模块、电路和算法步骤均可以实现成电子硬件、计算机软件、或者二者的组合。为了清楚地描绘硬件和软件之间的这种可交换性，上面已经对各种示例性的部件、框、模块、电路以及步骤围绕其功能进行了总体描述。至于这种功能是实现成硬件还是实现成软件，取决于具体应用和向整个系统施加的设计约束。熟练的技术人员可以针对每个特定应用，以变通的方式实现所描述的功能，但是，这种实现决策不应解释为导致背离本发明的保护范围。

[0379] 可以利用通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或其它可编程逻辑器件、分立门或晶体管逻辑、分立硬件部件、或者被设计为执行本文所述功能的它们的任何组合来实现或执行结合本文公开的各方面所述的各种示意性的逻辑、逻辑块、模块、以及电路。通用处理器可以是微处理器，但在可选方案中，处理器可以是任何常规的处理器、控制器、微控制器或状态机。还可以将处理器实现为计算设备的组合，例如，DSP和微处理器的组合、多个微处理器、结合有DSP内核的一个或多个微处理器、或者任何其它这类配置。替代地，一些步骤或方法可以由特定于给定功能的电路来执行。

[0380] 在一个或多个示例性方面，所述功能可以用硬件、软件、固件或它们任意组合的方式来实现。当用软件来实现时，可以将这些功能作为一个或多个指令或代码存储在计算机可读介质上或者通过计算机可读介质进行传输。本申请所公开的方法或算法的步骤可以在处理器可执行软件模块中具体实现，所述处理器可执行软件模块可以位于有形的非临时性计算机可读存储介质上。有形的非临时性计算机可读存储介质可以是计算机可访问的任何可用介质。举例说明，而非限制，这种非临时性计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储器、磁盘存储器或其它磁存储设备、或者可以用于存储具有指令或

数据结构形式的期望的程序代码并能够由计算机访问的任何其它介质。如本申请所使用的，盘 (disk) 和碟 (disc) 包括压缩光碟 (CD)、激光光碟、光碟、数字多功能光碟 (DVD)、软盘和蓝光光碟，其中盘通常磁性地复制数据，而碟则用激光来光学地复制数据。上述的组合也应当被包括在非临时性计算机可读介质的范围之内。另外，一种方法或算法的操作可以作为位于有形的、非临时性机器可读介质和 / 或计算机可读介质上的一个代码和 / 或指令的任意组合或集合，其中所述有形的、非临时性机器可读介质和 / 或计算机可读介质可以并入到计算机程序产品中。

[0381] 为使本领域任何技术人员能够实施或使用本发明，上面围绕所公开的实施例进行了描述。对于本领域技术人员来说，对这些实施例的各种修改是显而易见的，并且，本申请定义的总体原理也可以在不脱离本发明的精神或范围的前提下应用于其它实施例。因此，本发明并不限于本申请所示出的实施例，而是与所附权利要求书和本文公开的原理和新颖特征的最宽范围相一致。

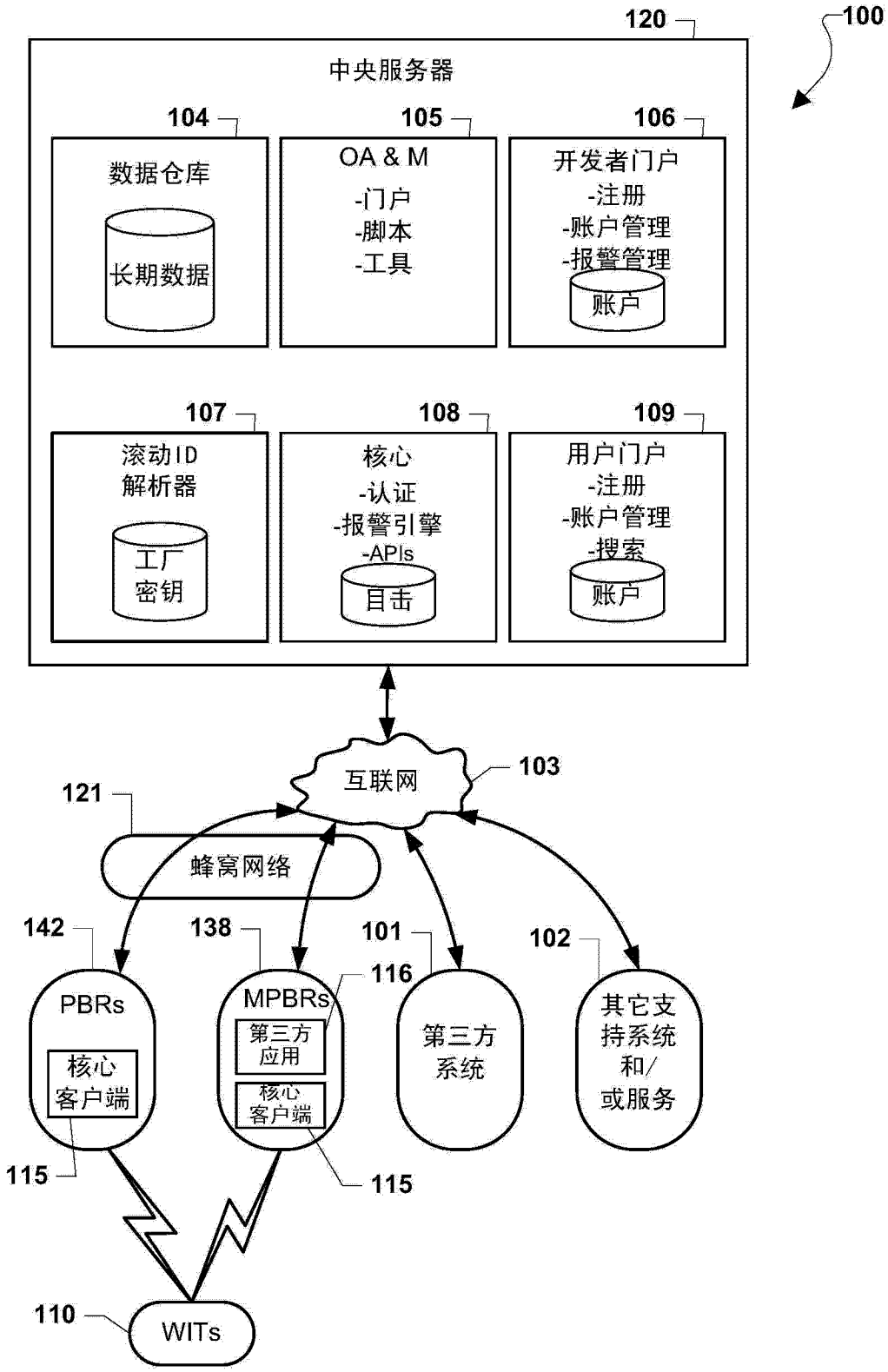

100
120
中央服务器
104
数据仓库
长期数据
105
OA & M
-门户
-脚本
-工具
106
开发者门户
-注册
-账户管理
-报警管理
账户
107
滚动ID
解析器
工厂
密钥
108
核心
-认证
-报警引擎
-APIs
目击
109
用户门户
-注册
-账户管理
-搜索
账户
103
互联网
121
蜂窝网络
142
PBRs
核心
客户端
138
MPBRs
116
第三方
应用
核心
客户端
101
第三方
系统
102
其它支
持系统
和/
或服务
115
115
110
WITs

图 1

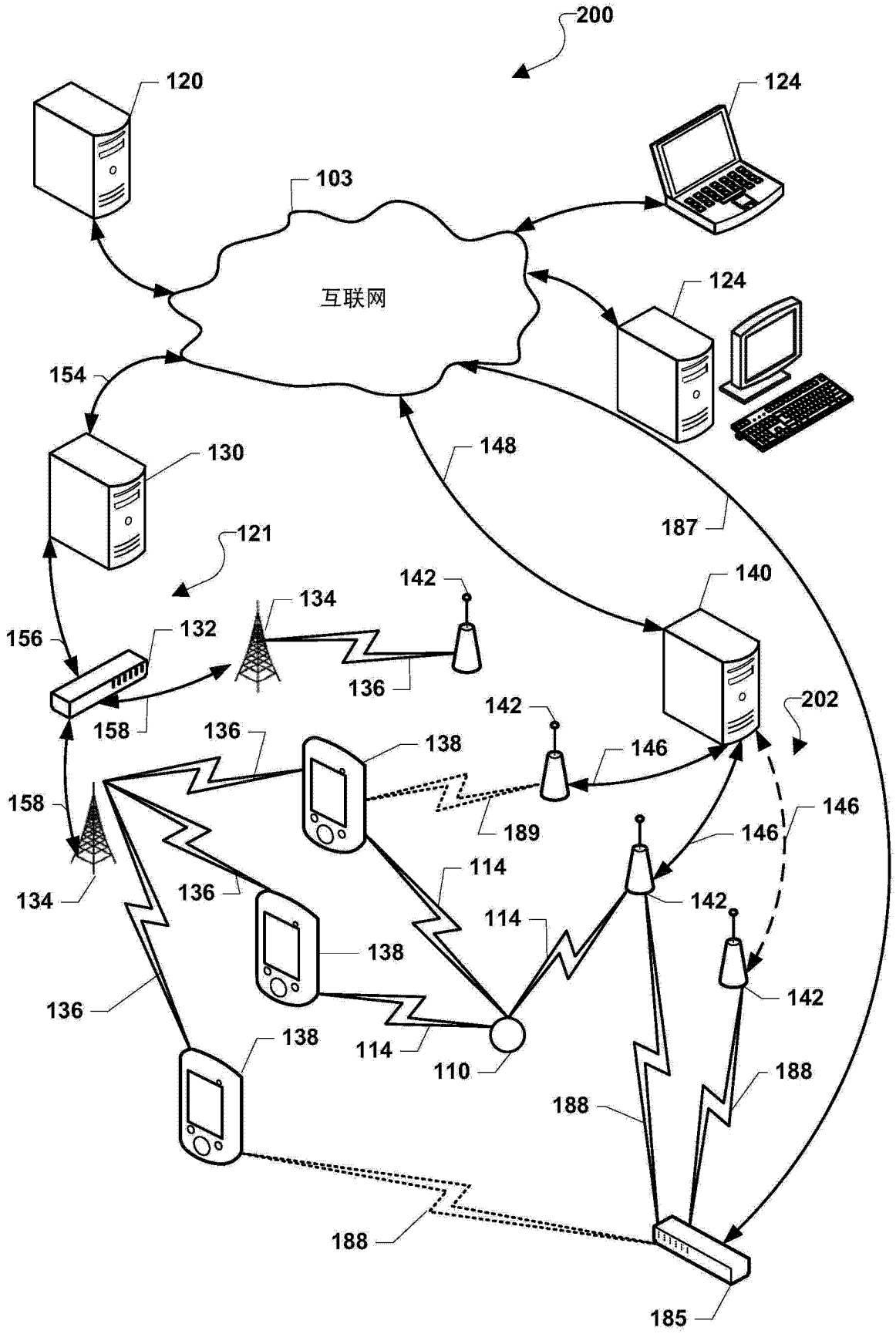

200
120
124
103
互联网
124
154
130
148
187
121
142
140
134
156
132
136
142
202
158
136
138
146
158
189
146
146
114
134
136
142
114
138
142
136
138
114
110
188
188
188
185

图 2

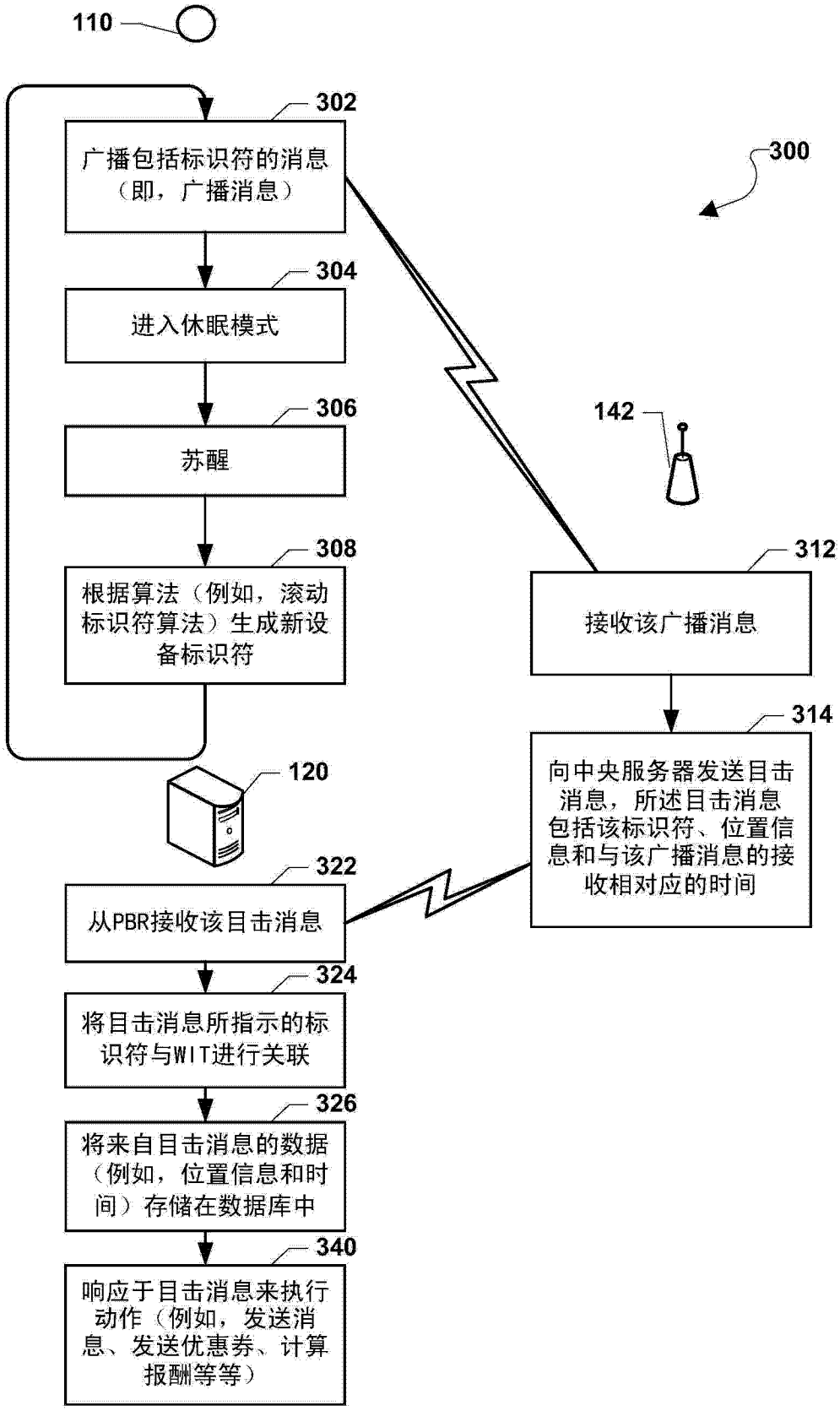

110
302
广播包括标识符的消息（即，广播消息）
300
304
进入休眠模式
306
苏醒
142
308
根据算法（例如，滚动标识符算法）生成新设备标识符
312
接收该广播消息
314
向中央服务器发送目击消息，所述目击消息包括该标识符、位置信息和与该广播消息的接收相对应的时间
120
322
从PBR接收该目击消息
324
将目击消息所指示的标识符与WIT进行关联
326
将来自目击消息的数据（例如，位置信息和时间）存储在数据库中
340
响应于目击消息来执行动作（例如，发送消息、发送优惠券、计算报酬等等）

图 3

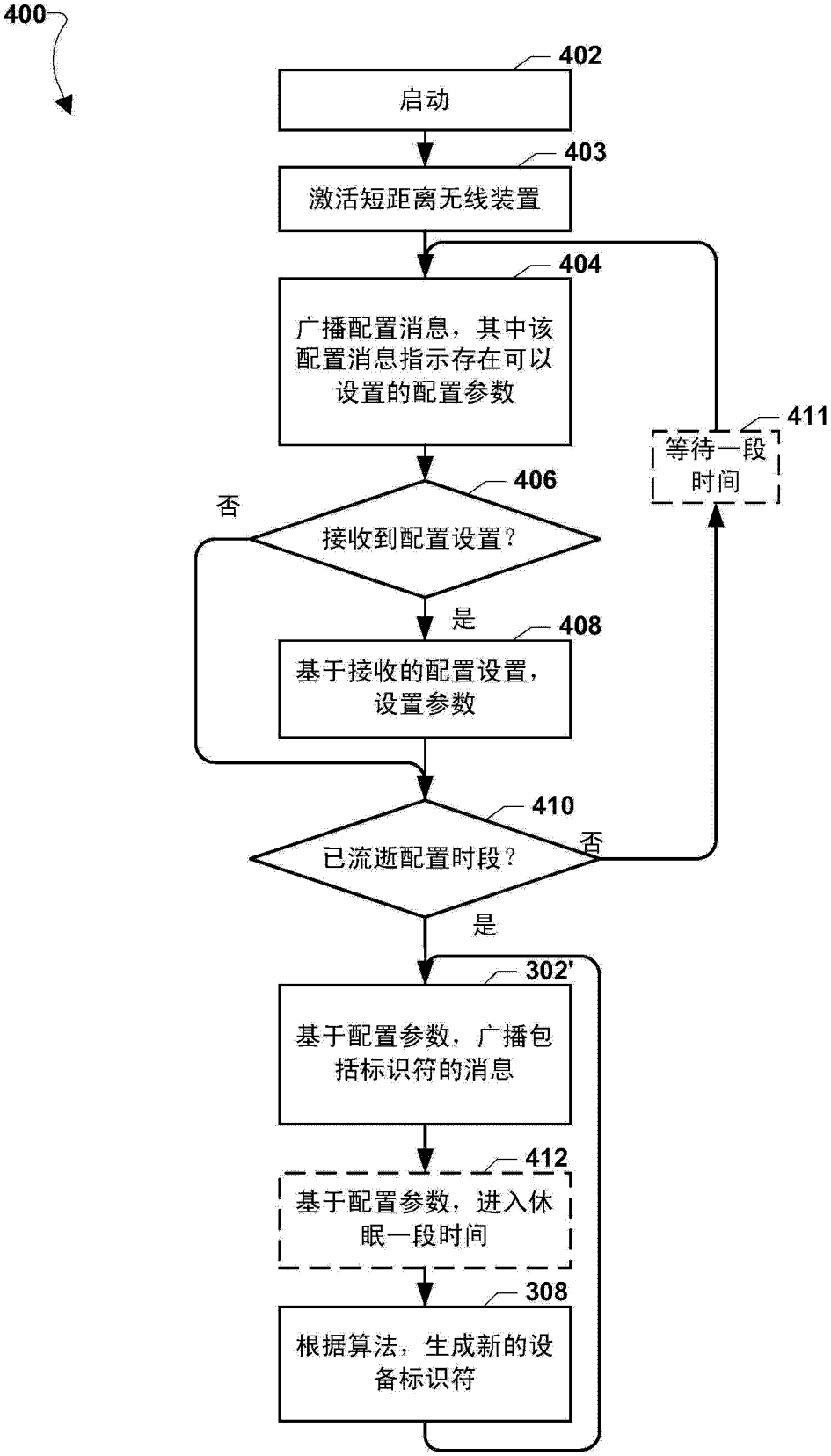

400
402
启动
403
激活短距离无线装置
404
广播配置消息，其中该配置消息指示存在可以设置的配置参数
406
接收到配置设置？
否
是
408
基于接收的配置设置，设置参数
410
已流逝配置时段？
否
是
411
等待一段时间
302'
基于配置参数，广播包括标识符的消息
412
基于配置参数，进入休眠一段时间
308
根据算法，生成新的设备标识符

图 4A

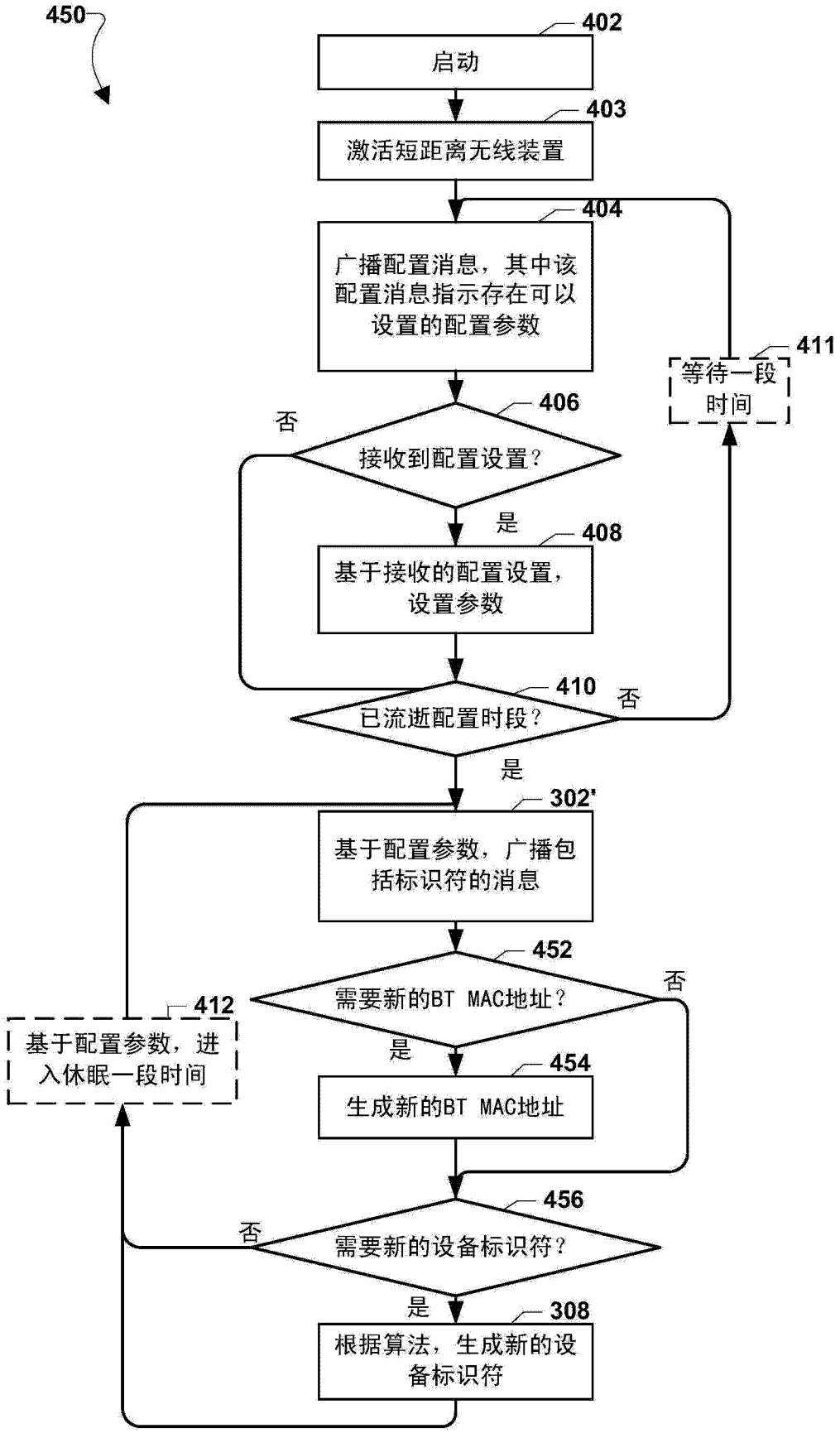

450
402
启动
403
激活短距离无线装置
404
广播配置消息，其中该配置消息指示存在可以设置的配置参数
406
否
接收到配置设置？
是
408
基于接收的配置设置，设置参数
410
否
已流逝配置时段？
是
411
等待一段时间
302'
基于配置参数，广播包括标识符的消息
452
否
需要新的BT MAC地址？
是
454
生成新的BT MAC地址
456
否
需要新的设备标识符？
是
308
根据算法，生成新的设备标识符
412
基于配置参数，进入休眠一段时间

图 4B

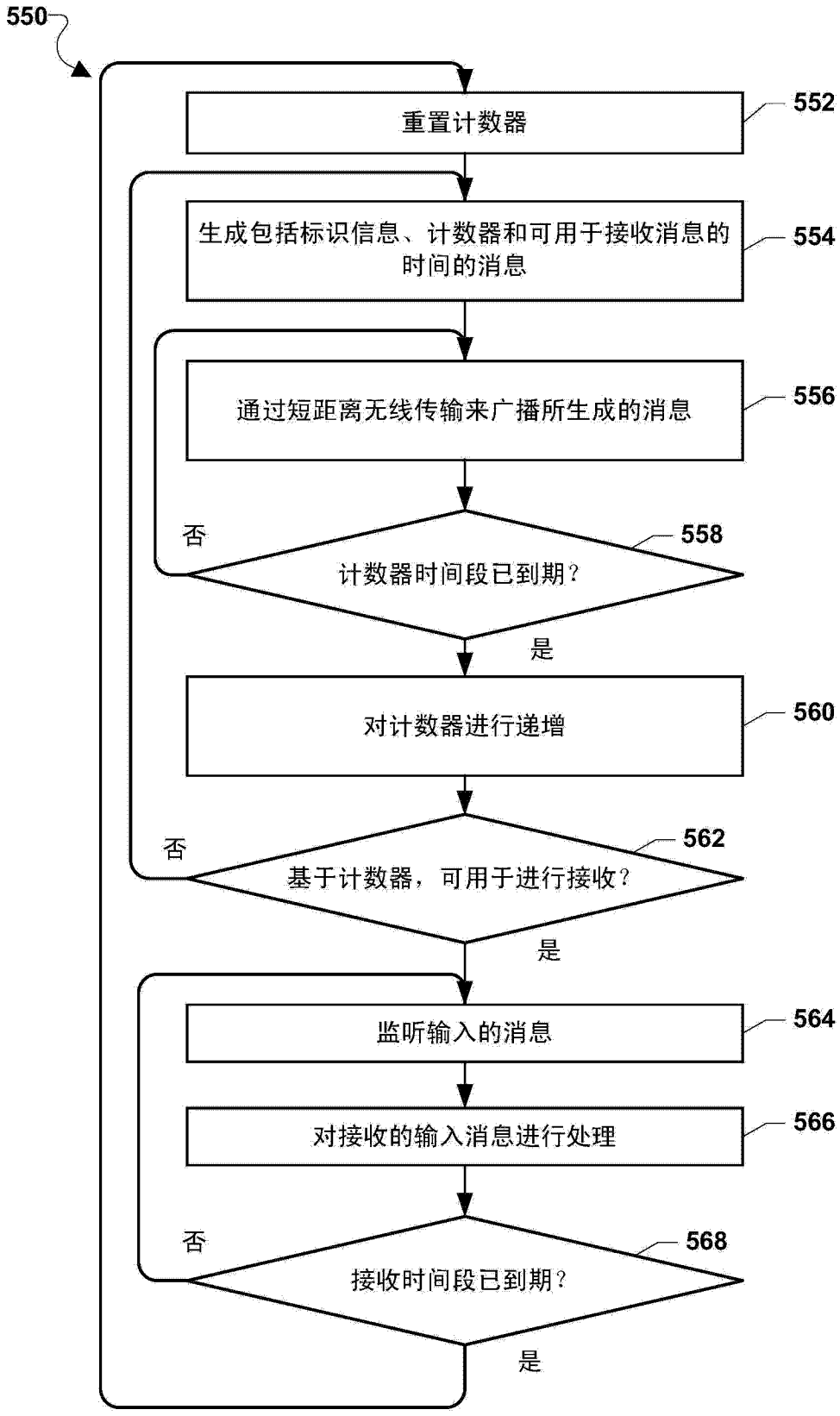

550
重置计数器
552
生成包括标识信息、计数器和可用于接收消息的时间的消息
554
通过短距离无线传输来广播所生成的消息
556
否
计数器时间段已到期？
558
是
对计数器进行递增
560
否
基于计数器，可用于进行接收？
562
是
监听输入的消息
564
对接收的输入消息进行处理
566
否
接收时间段已到期？
568
是

图 5

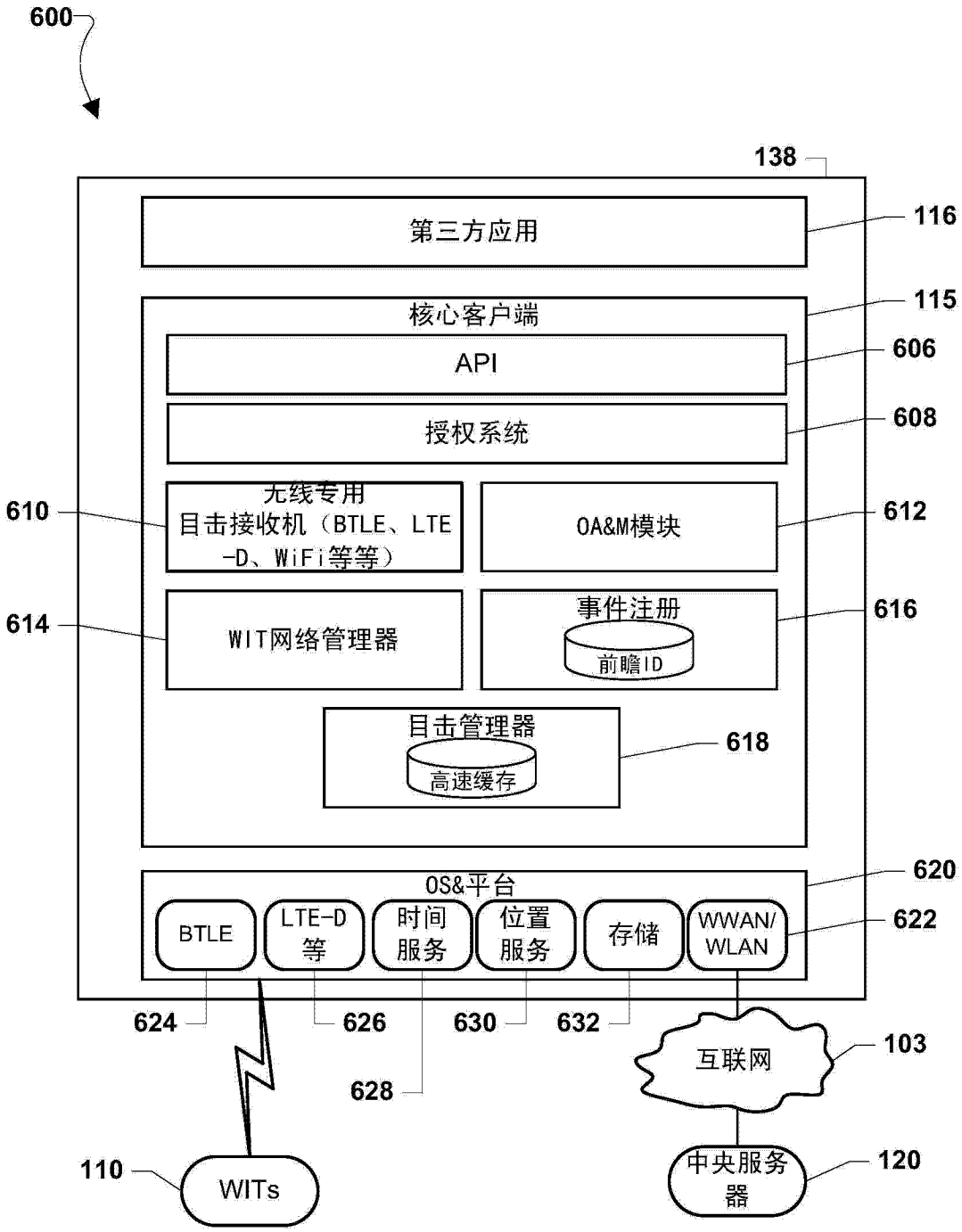

600
138
第三方应用
116
核心客户端
115
API
606
授权系统
608
610
无线专用
目击接收机（BTLE、LTE-D、WiFi等等）
OA&M模块
612
614
WIT网络管理器
事件注册
前瞻ID
616
目击管理器
高速缓存
618
OS&平台
620
BTLE
LTE-D等
时间服务
位置服务
存储
WWAN/WLAN
622
624
626
628
630
632
互联网
103
110
WITs
中央服务器
120

图 6

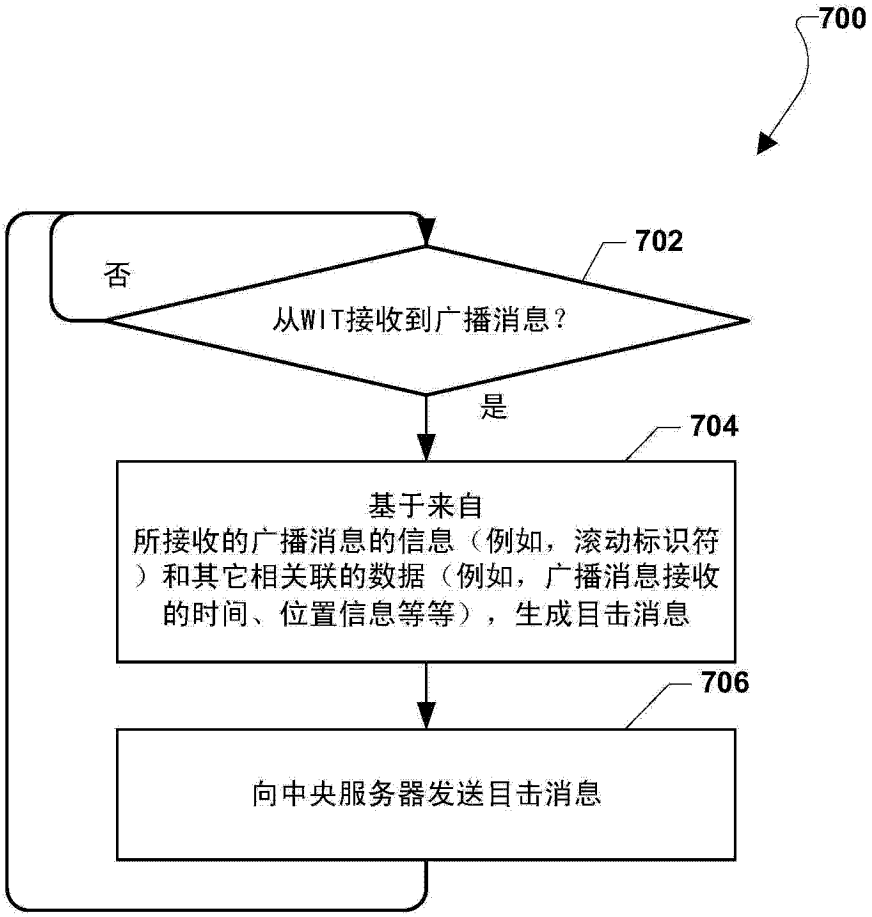

700
702
否
从WIT接收到广播消息？
是
704
基于来自
所接收的广播消息的信息（例如，滚动标识符）和其它相关联的数据（例如，广播消息接收的时间、位置信息等等），生成目击消息
706
向中央服务器发送目击消息

图 7A

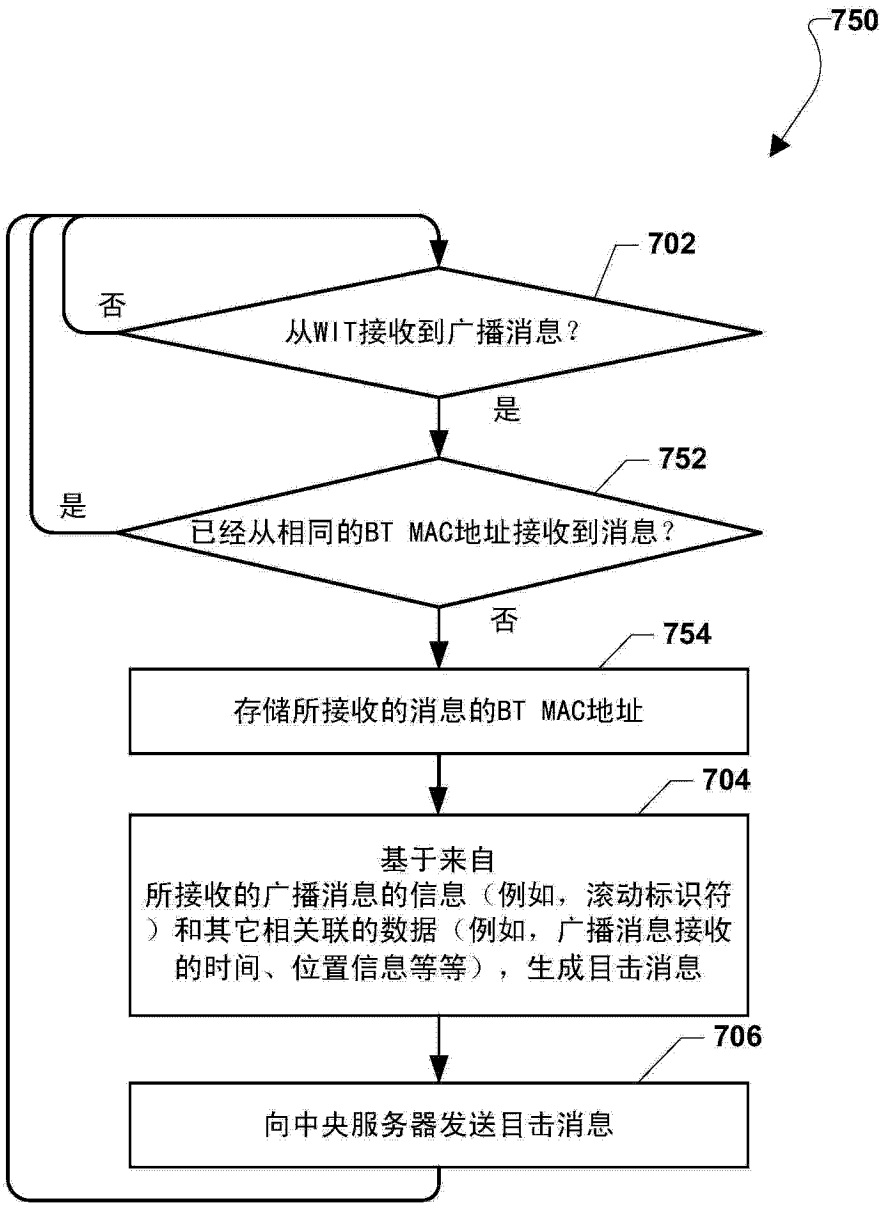

750
702
否
从WIT接收到广播消息？
是
752
是
已经从相同的BT MAC地址接收到消息？
否
754
存储所接收的消息的BT MAC地址
704
基于来自
所接收的广播消息的信息（例如，滚动标识符）和其它相关联的数据（例如，广播消息接收的时间、位置信息等等），生成目击消息
706
向中央服务器发送目击消息

图 7B

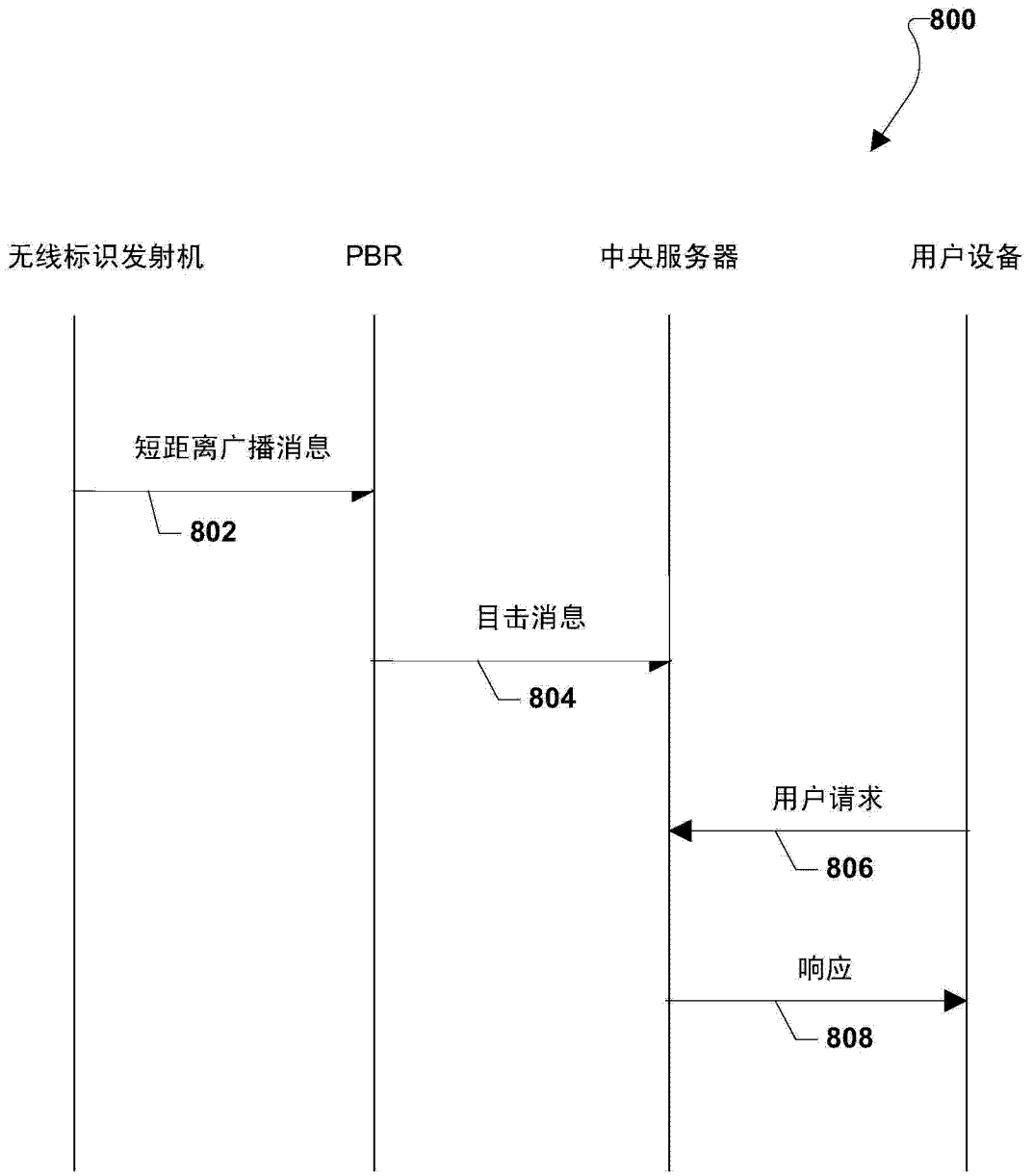

800
无线标识发射机
PBR
中央服务器
用户设备
短距离广播消息
802
目击消息
804
用户请求
806
响应
808

图 8

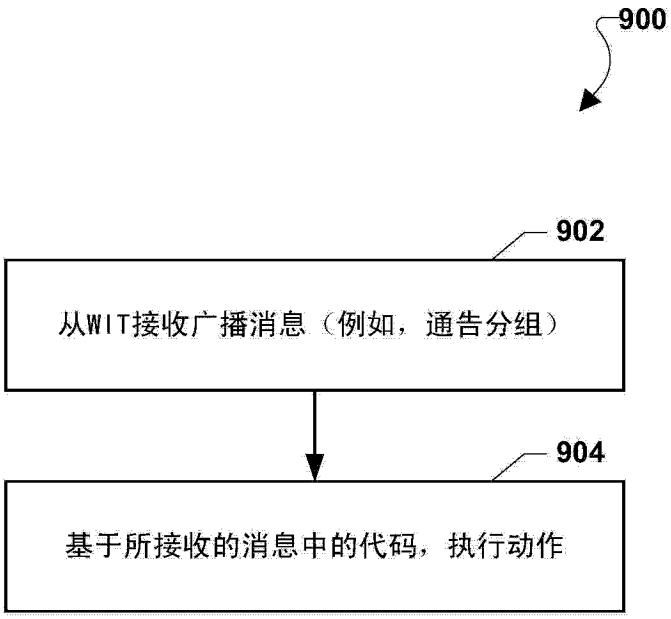



图 9

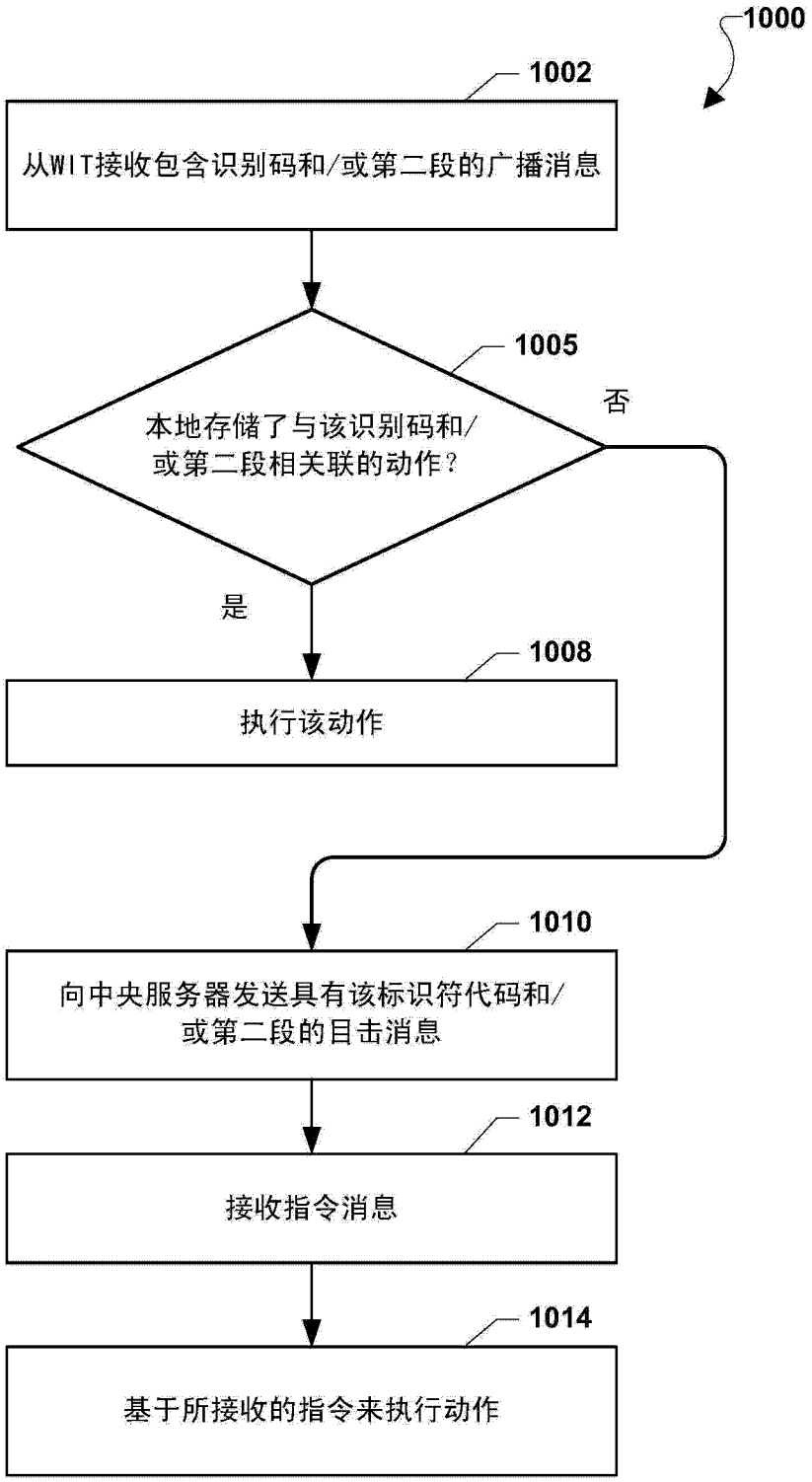

1000
1002
从WIT接收包含识别码和/或第二段的广播消息
1005
本地存储了与该识别码和/或第二段相关联的动作？
否
是
1008
执行该动作
1010
向中央服务器发送具有该标识符代码和/或第二段的目击消息
1012
接收指令消息
1014
基于所接收的指令来执行动作

图 10

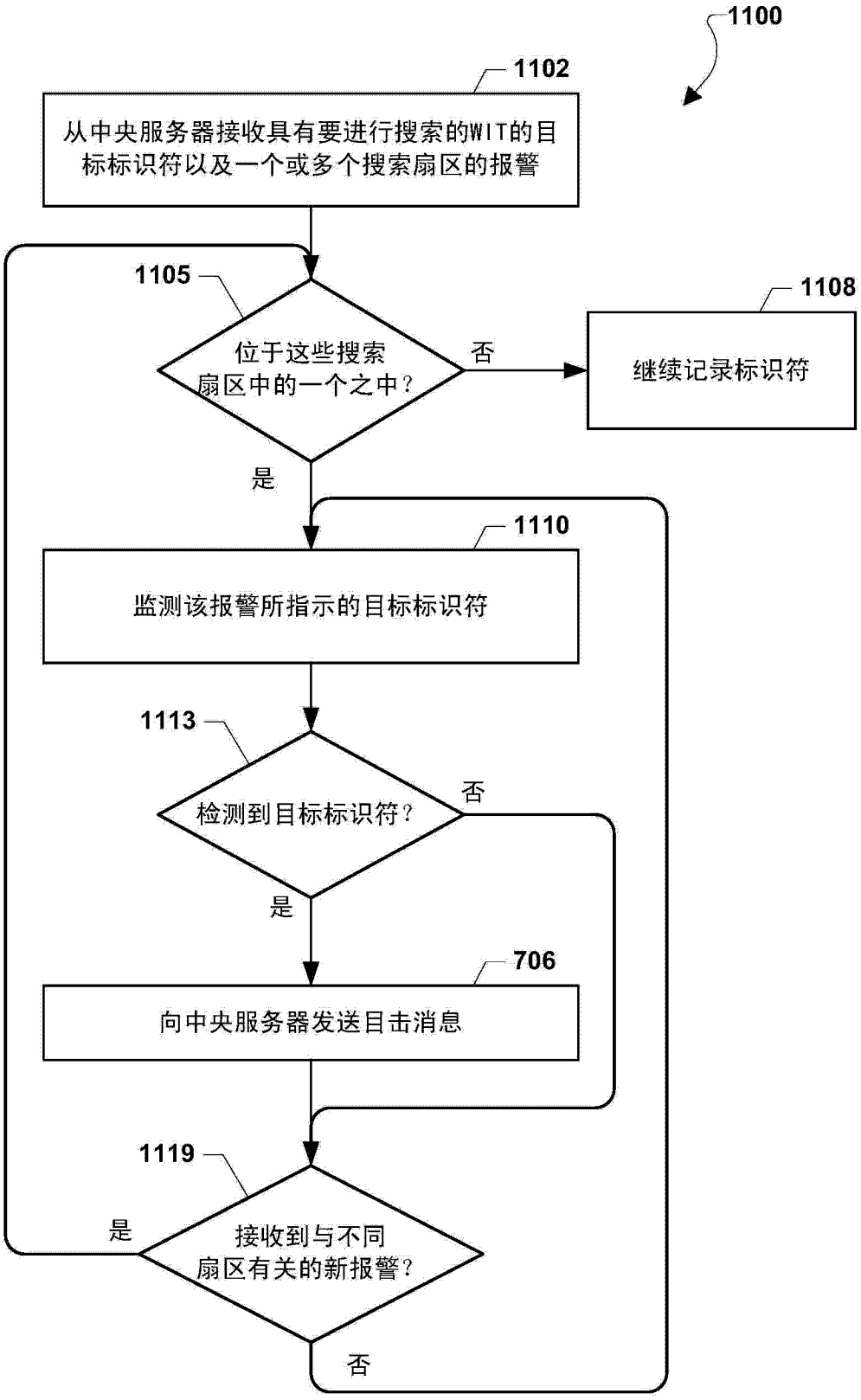

1100
1102
从中央服务器接收具有要进行搜索的WIT的目标标识符以及一个或多个搜索扇区的报警
1105
位于这些搜索扇区中的一个之中？
否
1108
继续记录标识符
是
1110
监测该报警所指示的目标标识符
1113
检测到目标标识符？
否
是
706
向中央服务器发送目击消息
1119
是
接收到与不同扇区有关的新报警？
否

图 11

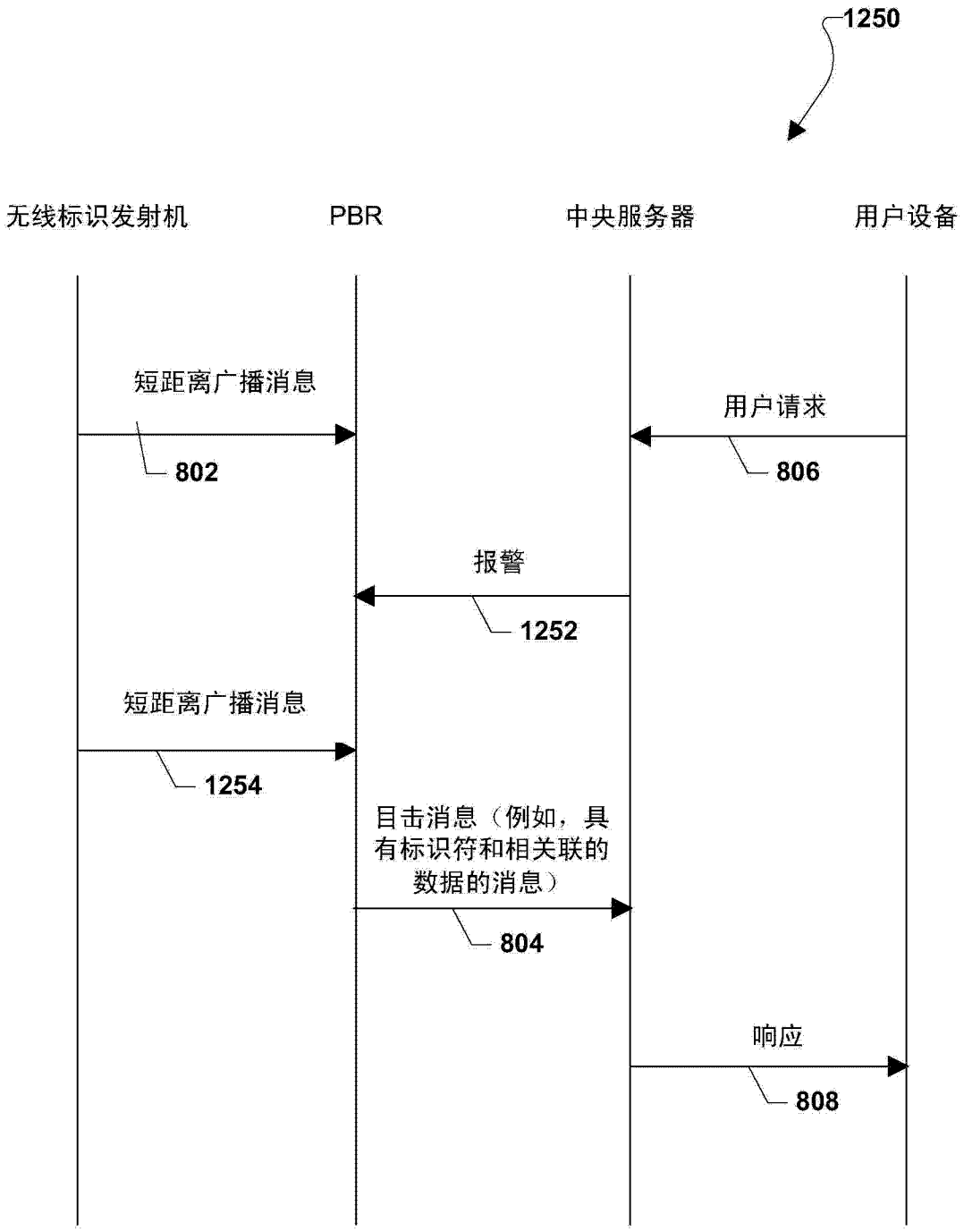

1250
无线标识发射机
PBR
中央服务器
用户设备
短距离广播消息
802
用户请求
806
报警
1252
短距离广播消息
1254
目击消息（例如，具有标识符和相关联的数据的消息）
804
响应
808

图 12

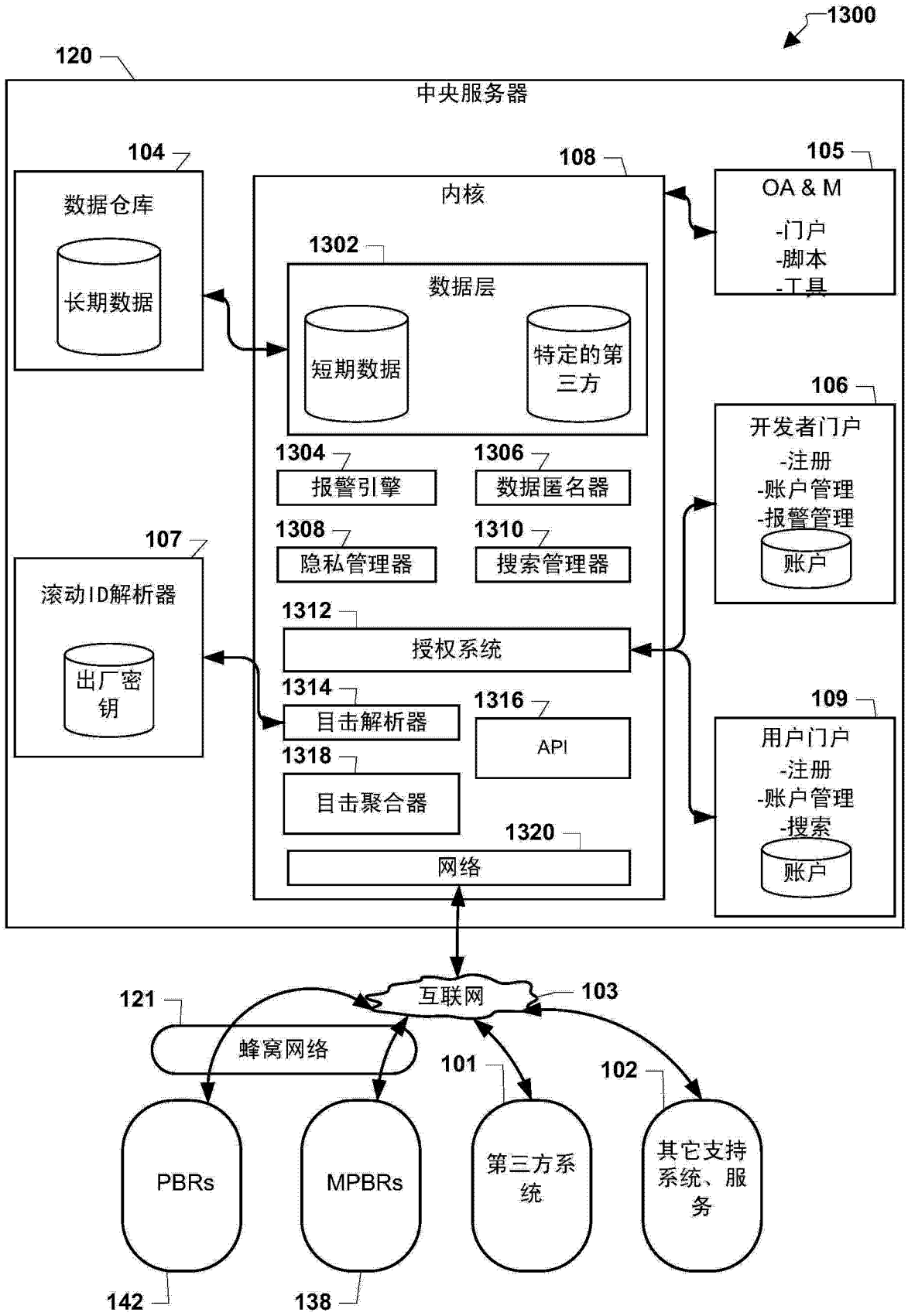

1300
120
中央服务器
104
数据仓库
长期数据
108
内核
1302
数据层
短期数据
特定的第三方
105
OA & M
-门户
-脚本
-工具
106
开发者门户
-注册
-账户管理
-报警管理
账户
1304
报警引擎
1306
数据匿名器
1308
隐私管理器
1310
搜索管理器
107
滚动ID解析器
出厂密钥
1312
授权系统
1314
目击解析器
1316
API
1318
目击聚合器
1320
网络
109
用户门户
-注册
-账户管理
-搜索
账户
互联网
103
121
蜂窝网络
101
102
PBRs
MPBRs
第三方系统
其它支持系统、服务
142
138

图 13

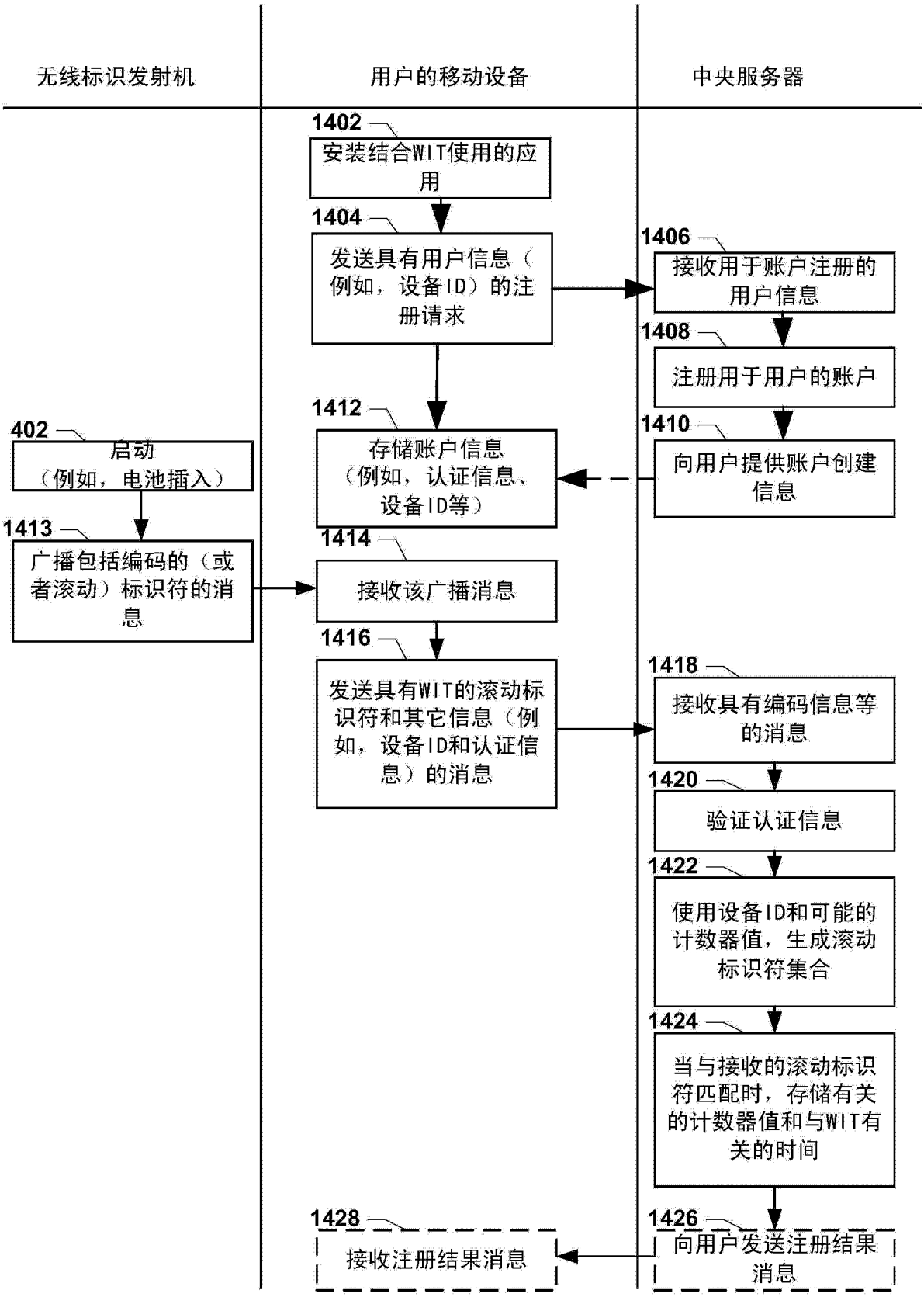

无线标识发射机
用户的移动设备
中央服务器
1402
安装结合WIT使用的应用
1404
发送具有用户信息（例如，设备ID）的注册请求
1406
接收用于账户注册的用户信息
1408
注册用于用户的账户
1410
向用户提供账户创建信息
1412
存储账户信息（例如，认证信息、设备ID等）
402
启动（例如，电池插入）
1413
广播包括编码的（或者滚动）标识符的消息
1414
接收该广播消息
1416
发送具有WIT的滚动标识符和其它信息（例如，设备ID和认证信息）的消息
1418
接收具有编码信息等的消息
1420
验证认证信息
1422
使用设备ID和可能的计数器值，生成滚动标识符集合
1424
当与接收的滚动标识符匹配时，存储有关的计数器值和与WIT有关的时间
1426
向用户发送注册结果消息
1428
接收注册结果消息

图 14

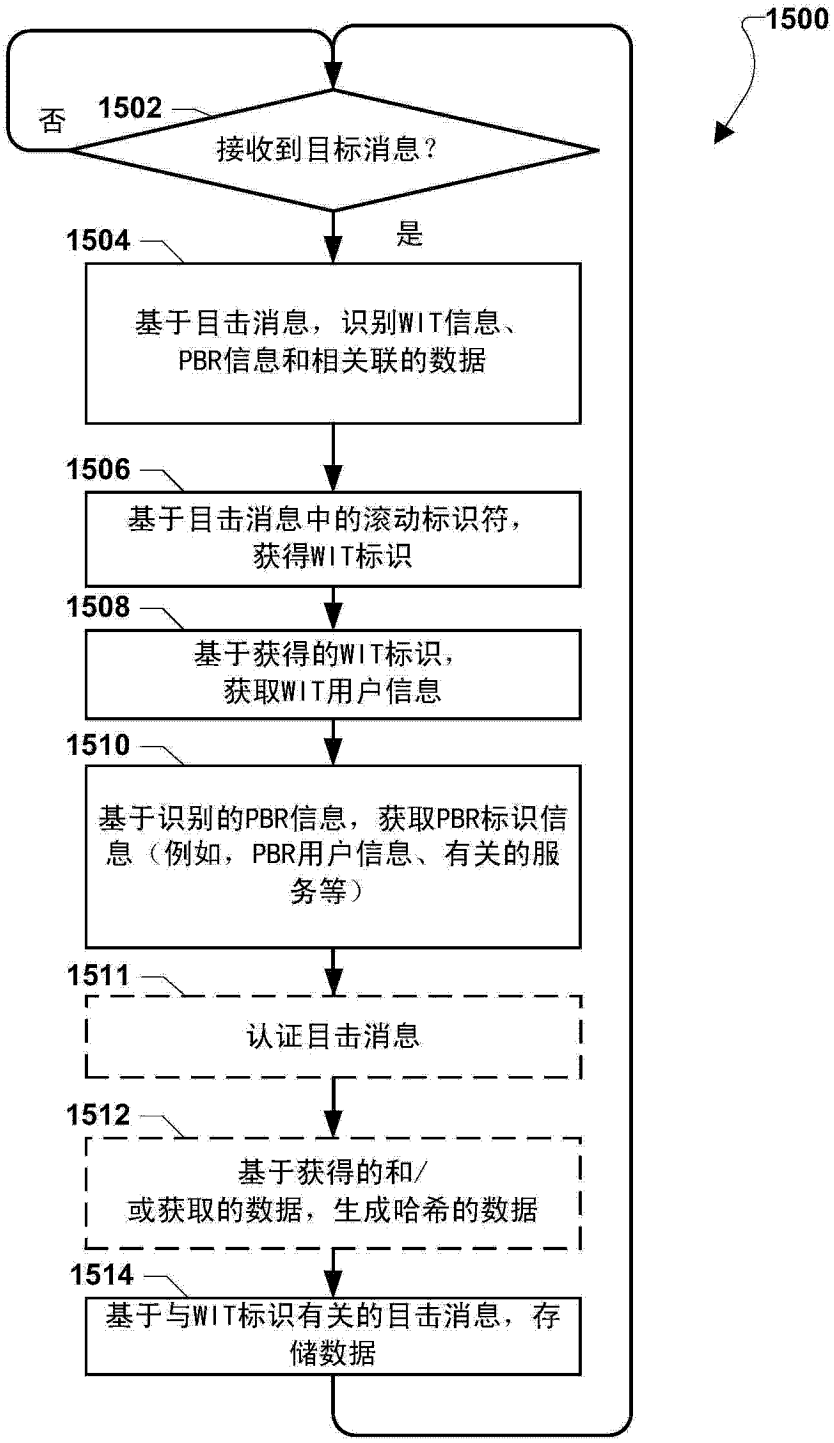

1500
1502
否
接收到目标消息？
是
1504
基于目击消息，识别WIT信息、PBR信息和相关联的数据
1506
基于目击消息中的滚动标识符，获得WIT标识
1508
基于获得的WIT标识，获取WIT用户信息
1510
基于识别的PBR信息，获取PBR标识信息（例如，PBR用户信息、有关的服务等）
1511
认证目击消息
1512
基于获得的和/或获取的数据，生成哈希的数据
1514
基于与WIT标识有关的目击消息，存储数据

图 15A

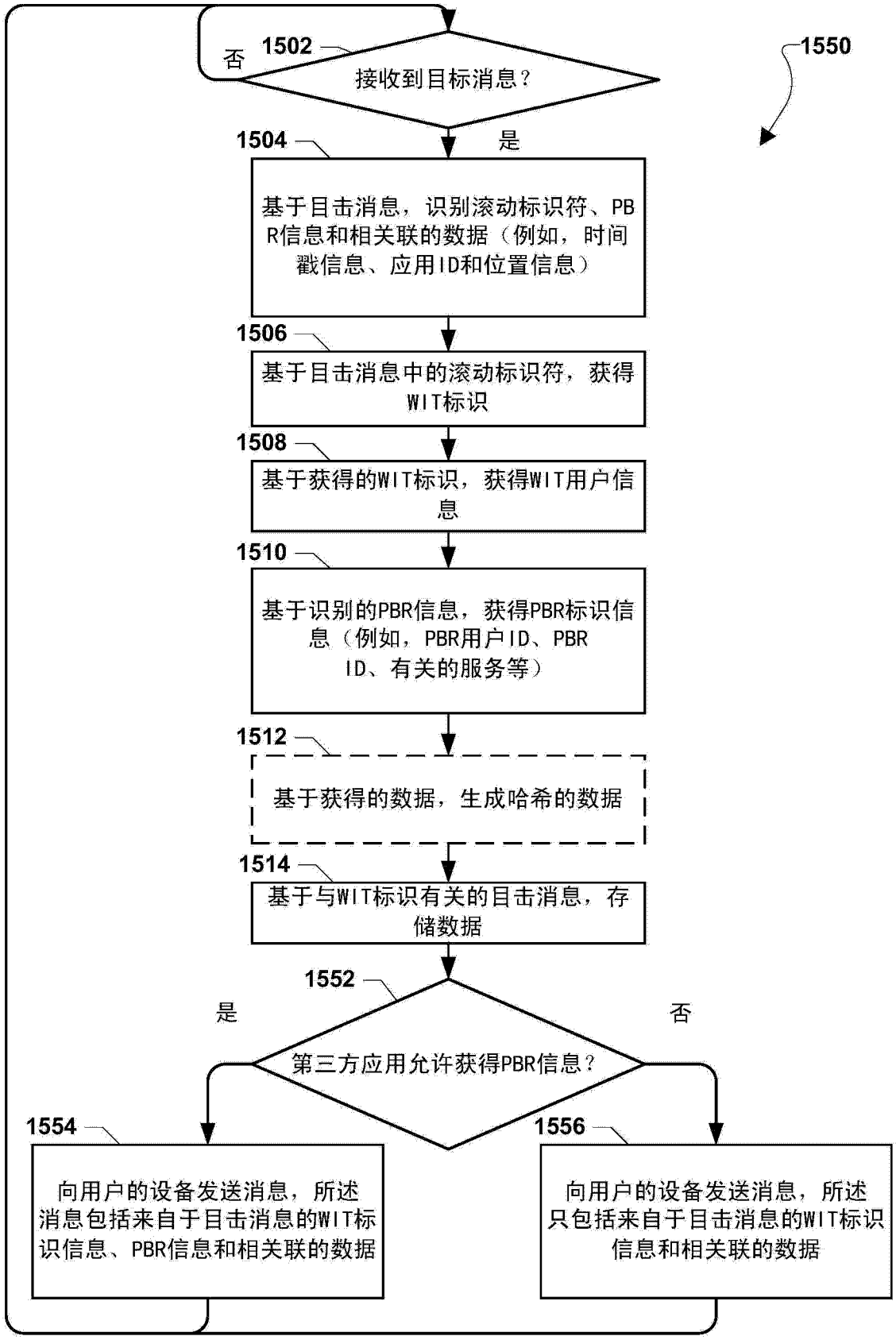

1550
1502
否
接收到目标消息？
是
1504
基于目击消息，识别滚动标识符、PBR信息和相关联的数据（例如，时间戳信息、应用ID和位置信息）
1506
基于目击消息中的滚动标识符，获得WIT标识
1508
基于获得的WIT标识，获得WIT用户信息
1510
基于识别的PBR信息，获得PBR标识信息（例如，PBR用户ID、PBR ID、有关的服务等）
1512
基于获得的数据，生成哈希的数据
1514
基于与WIT标识有关的目击消息，存储数据
1552
是
否
第三方应用允许获得PBR信息？
1554
向用户的设备发送消息，所述消息包括来自于目击消息的WIT标识信息、PBR信息和相关联的数据
1556
向用户的设备发送消息，所述只包括来自于目击消息的WIT标识信息和相关联的数据

图 15B

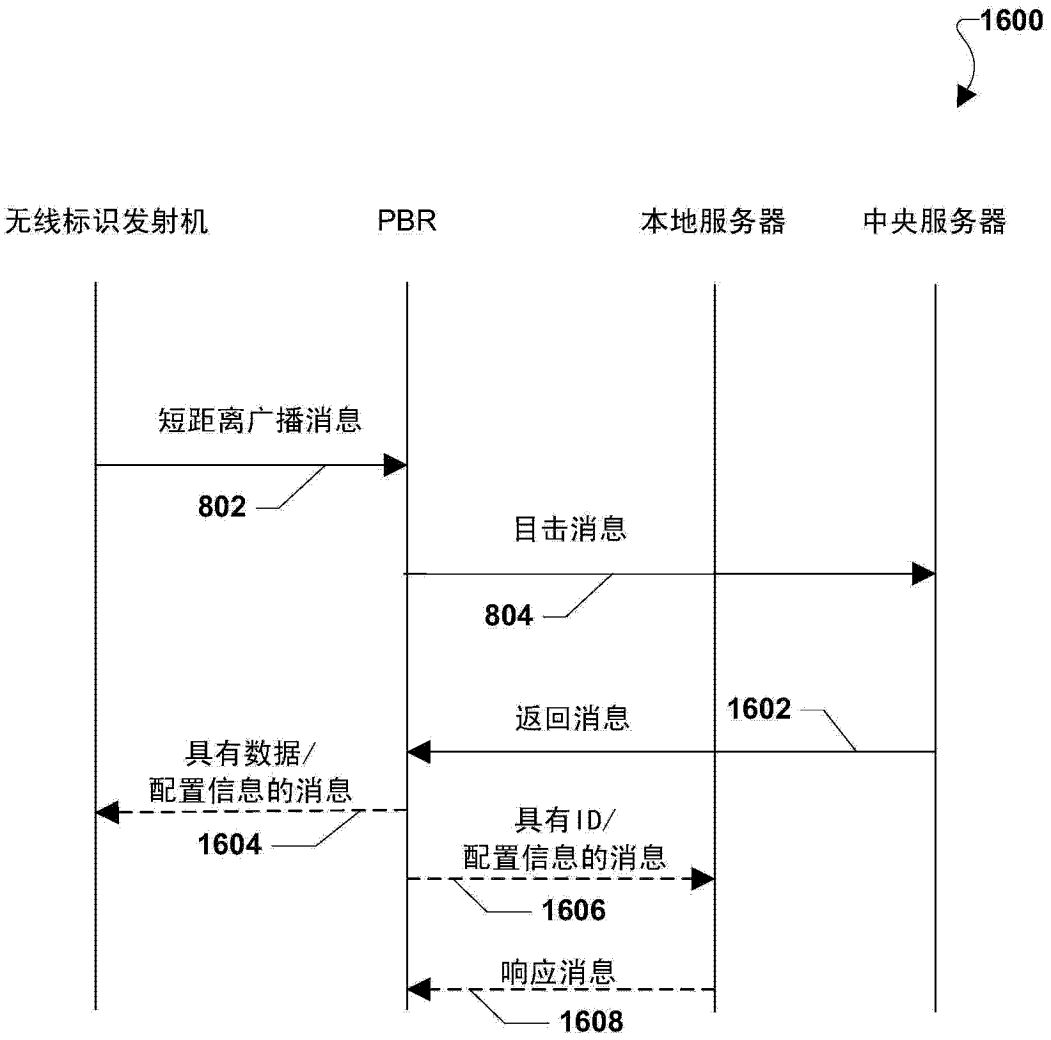

1600
无线标识发射机
PBR
本地服务器
中央服务器
短距离广播消息
802
目击消息
804
返回消息
1602
具有数据/
配置信息的消息
1604
具有ID/
配置信息的消息
1606
响应消息
1608

图 16

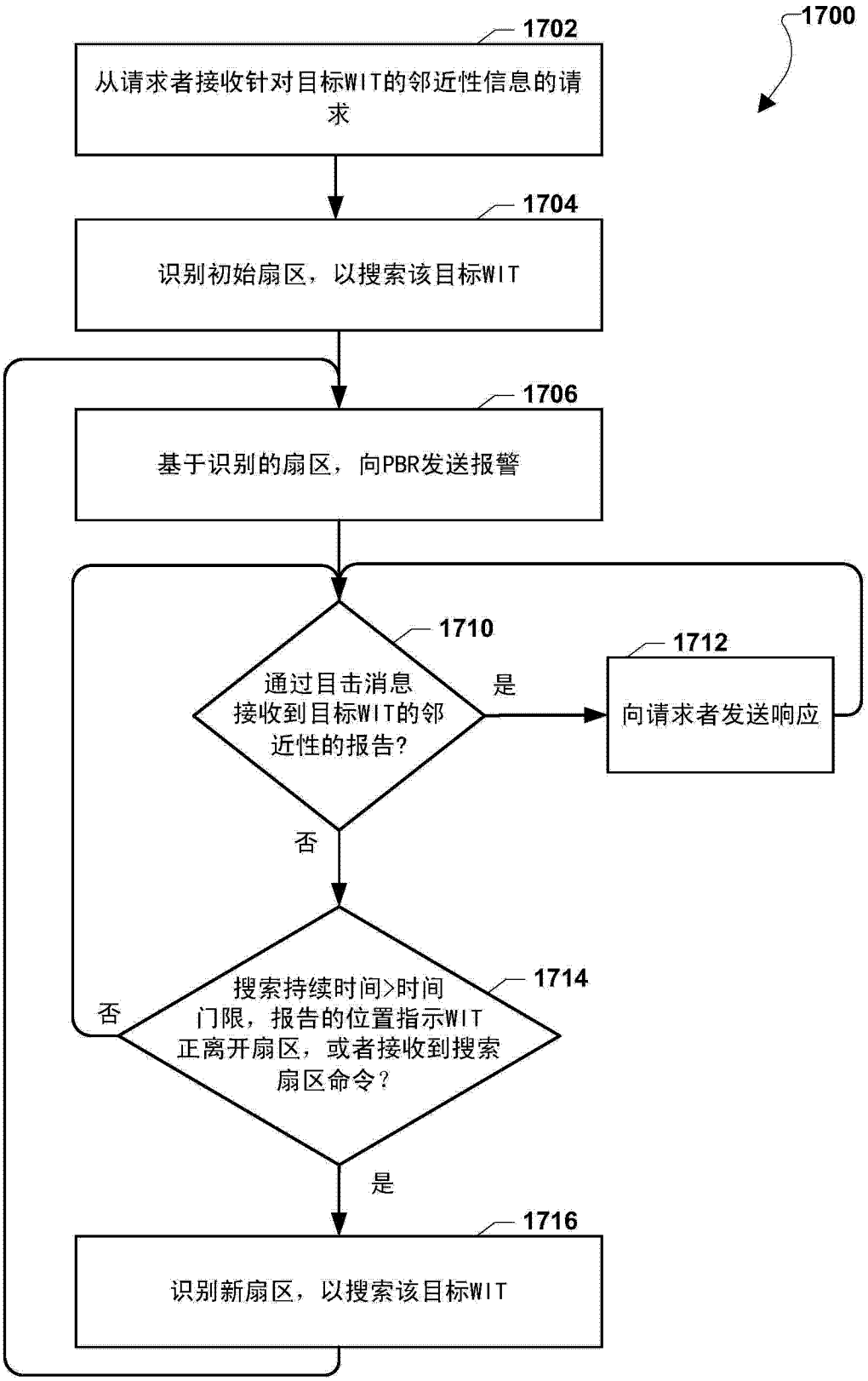

1700
1702
从请求者接收针对目标WIT的邻近性信息的请求
1704
识别初始扇区，以搜索该目标WIT
1706
基于识别的扇区，向PBR发送报警
1710
通过目击消息接收到目标WIT的邻近性的报告?
是
1712
向请求者发送响应
否
1714
搜索持续时间>时间门限，报告的位置指示WIT正离开扇区，或者接收到搜索扇区命令?
否
是
1716
识别新扇区，以搜索该目标WIT

图 17

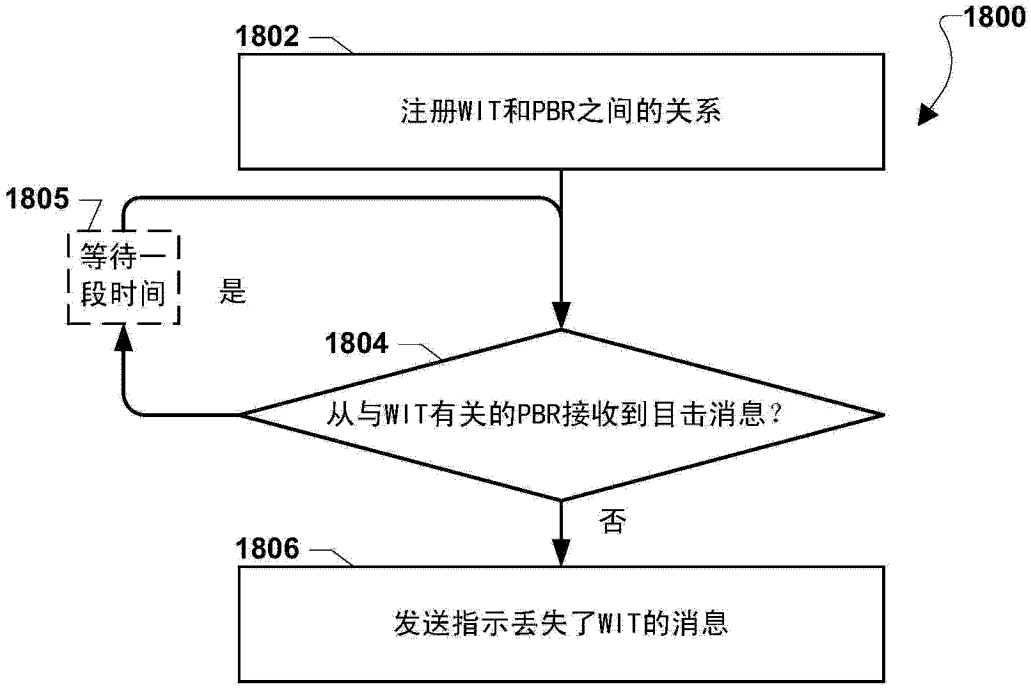

1800
1802
注册WIT和PBR之间的关系
1805
等待一段时间
是
1804
从与WIT有关的PBR接收到目击消息？
否
1806
发送指示丢失了WIT的消息

图 18

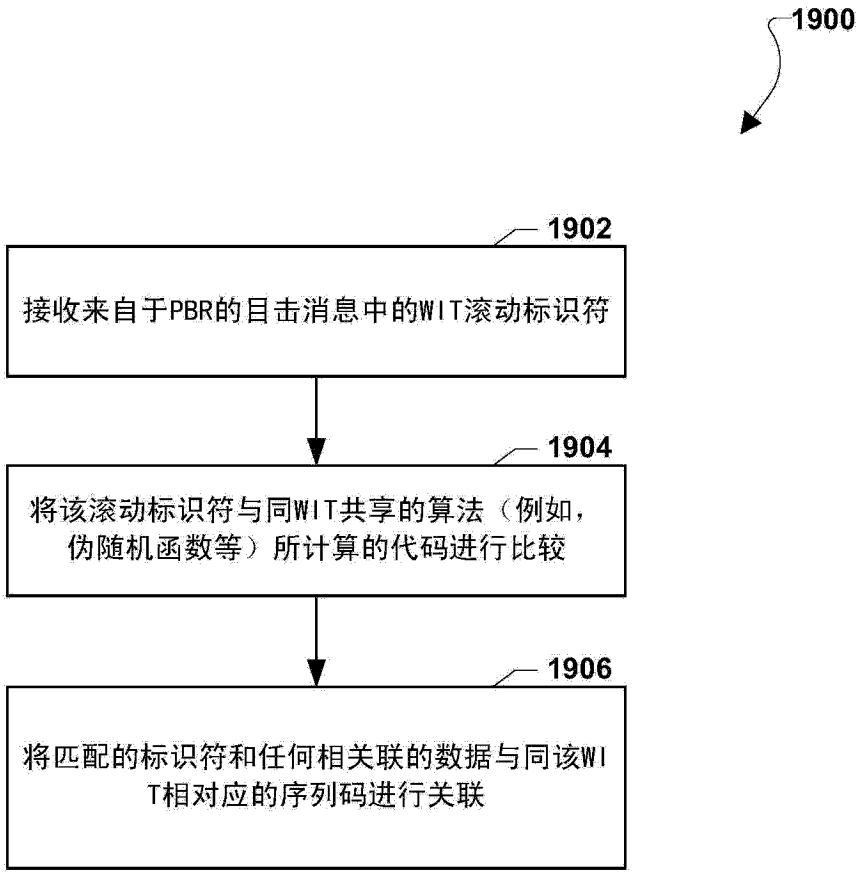

1900
1902
接收来自于PBR的目击消息中的WIT滚动标识符
1904
将该滚动标识符与同WIT共享的算法（例如，伪随机函数等）所计算的代码进行比较
1906
将匹配的标识符和任何相关联的数据与同该WIT相对应的序列码进行关联

图 19

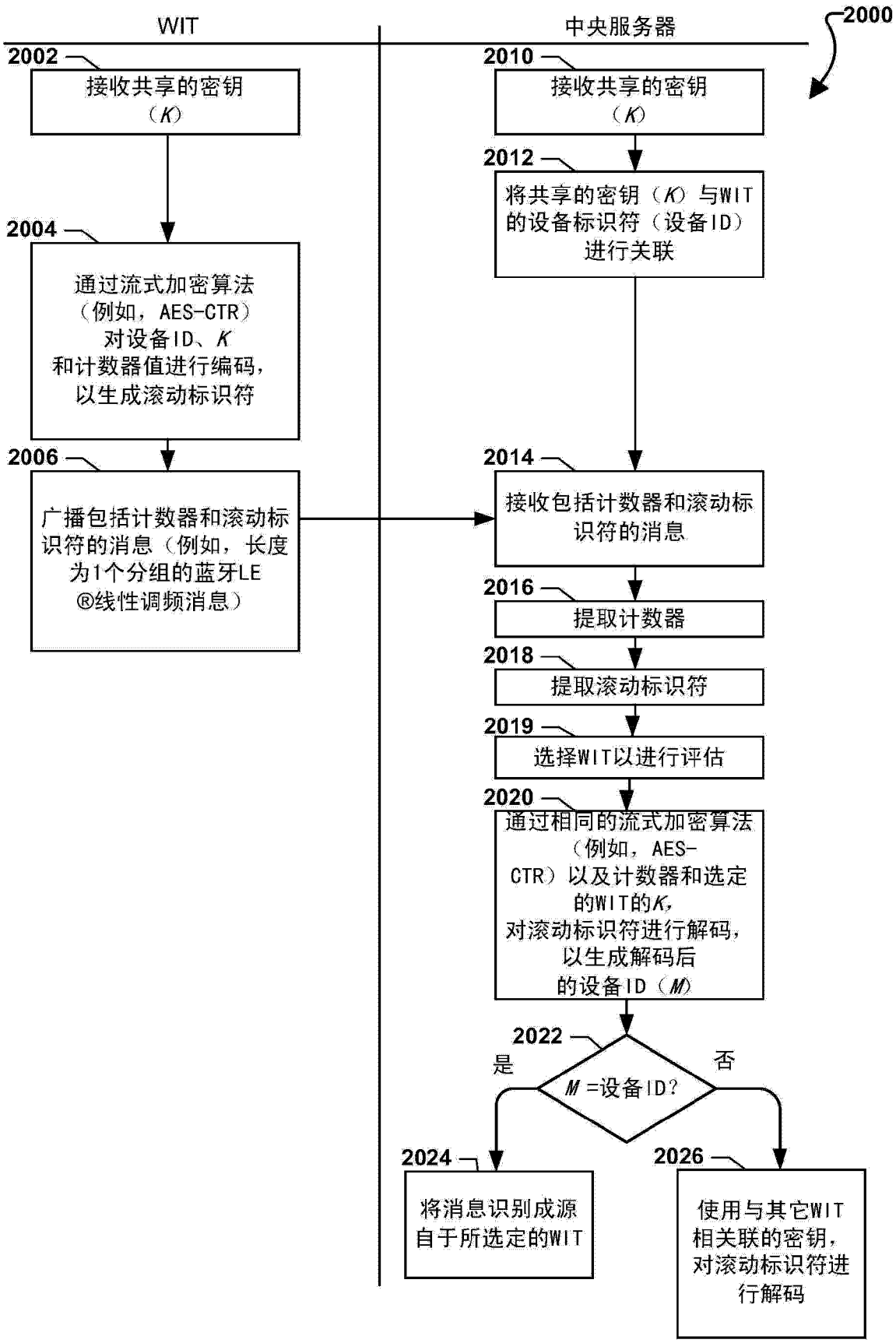

WIT
中央服务器
2000
2002
接收共享的密钥（K）
2004
通过流式加密算法（例如，AES-CTR）对设备ID、K和计数器值进行编码，以生成滚动标识符
2006
广播包括计数器和滚动标识符的消息（例如，长度为1个分组的蓝牙LE®线性调频消息）
2010
接收共享的密钥（K）
2012
将共享的密钥（K）与WIT的设备标识符（设备ID）进行关联
2014
接收包括计数器和滚动标识符的消息
2016
提取计数器
2018
提取滚动标识符
2019
选择WIT以进行评估
2020
通过相同的流式加密算法（例如，AES-CTR）以及计数器和选定的WIT的K，对滚动标识符进行解码，以生成解码后的设备ID（M）
2022
M =设备ID?
是
否
2024
将消息识别成源自于所选定的WIT
2026
使用与其它WIT相关联的密钥，对滚动标识符进行解码

图 20

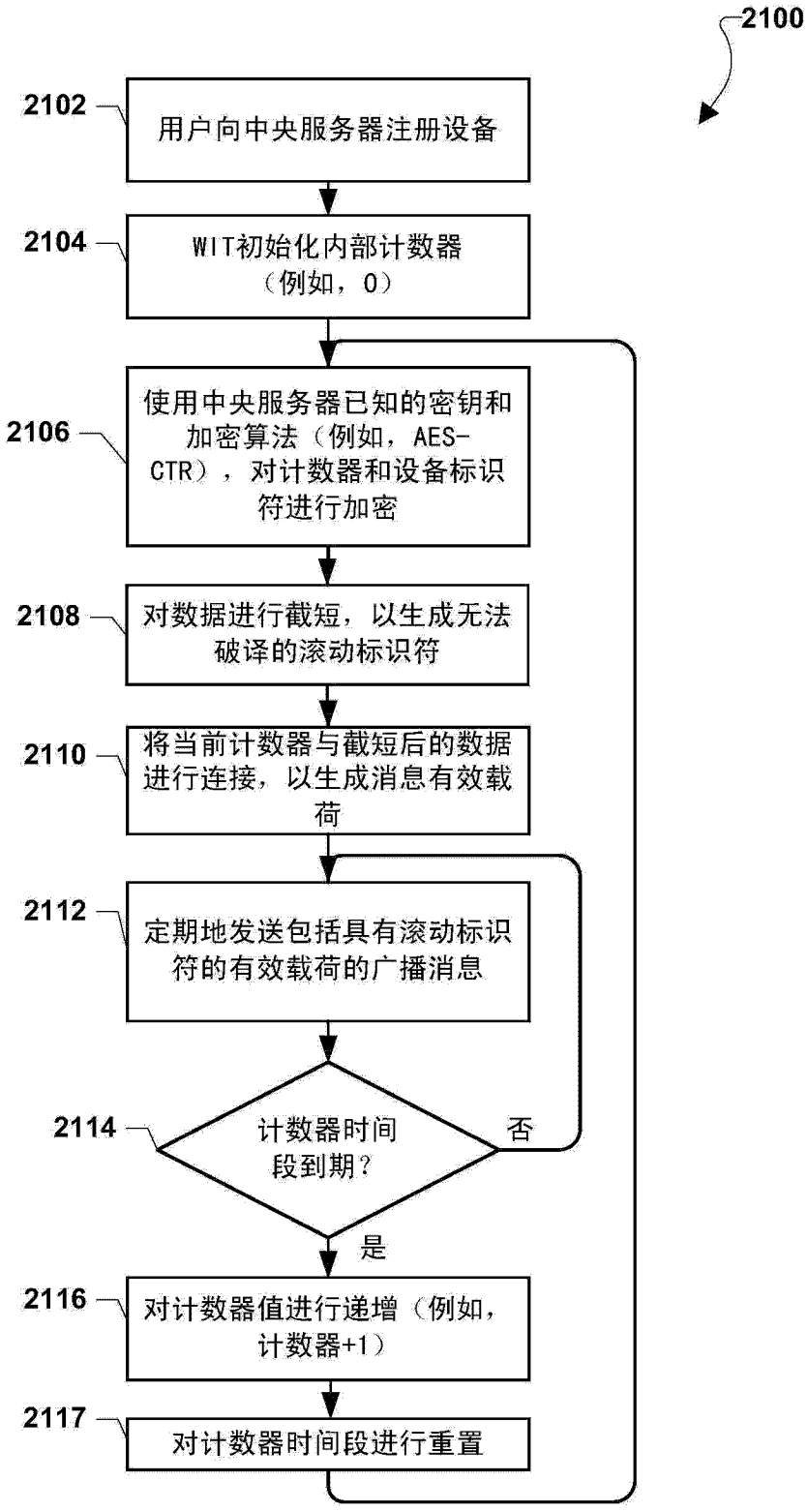

2100
2102
用户向中央服务器注册设备
2104
WIT初始化内部计数器（例如，0）
2106
使用中央服务器已知的密钥和加密算法（例如，AES-CTR），对计数器和设备标识符进行加密
2108
对数据进行截短，以生成无法破译的滚动标识符
2110
将当前计数器与截短后的数据进行连接，以生成消息有效载荷
2112
定期地发送包括具有滚动标识符的有效载荷的广播消息
2114
计数器时间段到期？
否
是
2116
对计数器值进行递增（例如，计数器+1）
2117
对计数器时间段进行重置

图 21A

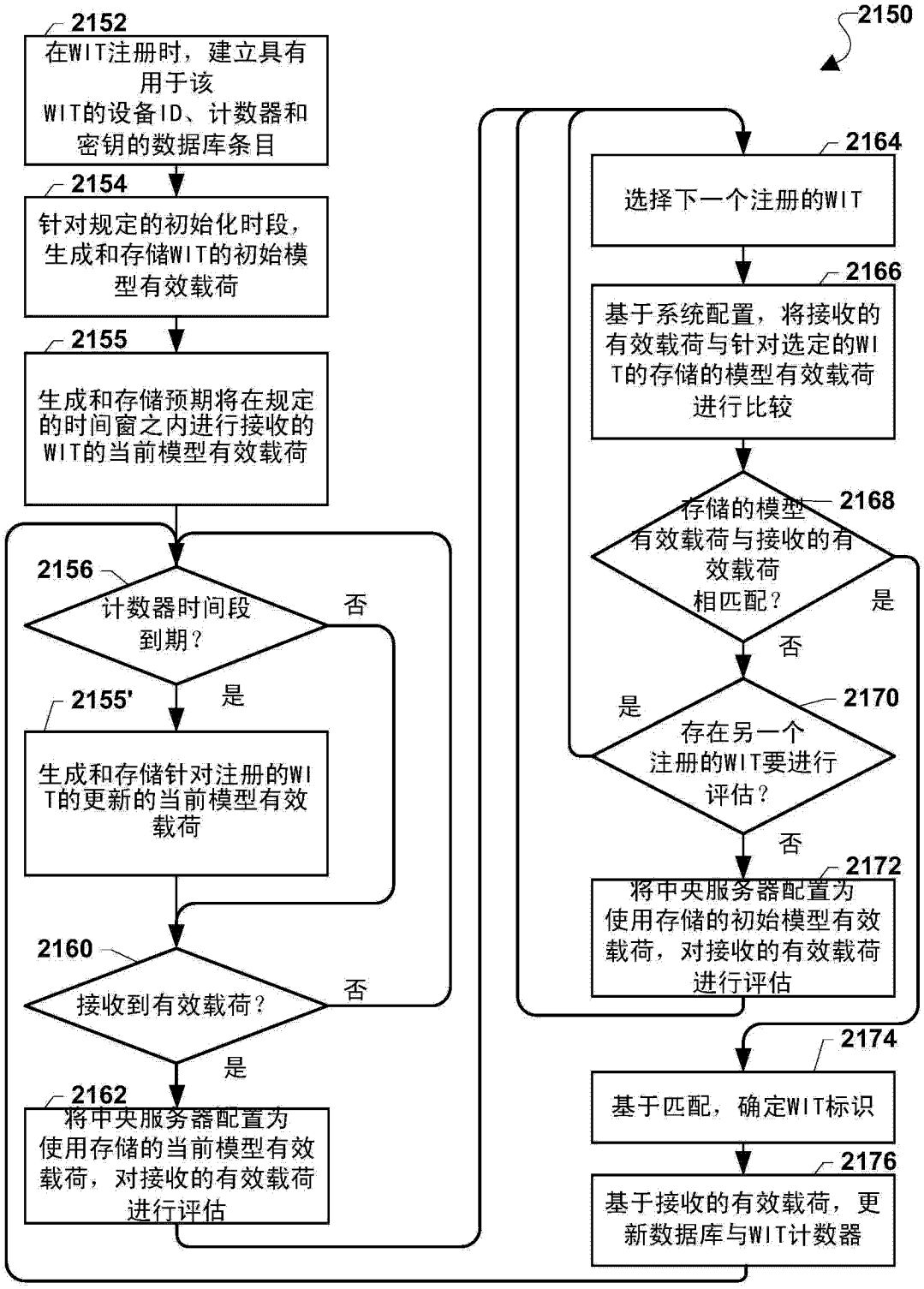

2150
2152
在WIT注册时，建立具有用于该WIT的设备ID、计数器和密钥的数据库条目
2154
针对规定的初始化时段，生成和存储WIT的初始模型有效载荷
2155
生成和存储预期将在规定的时间窗之内进行接收的WIT的当前模型有效载荷
2156
计数器时间段到期？
否
是
2155'
生成和存储针对注册的WIT的更新的当前模型有效载荷
2160
接收到有效载荷？
否
是
2162
将中央服务器配置为使用存储的当前模型有效载荷，对接收的有效载荷进行评估
2164
选择下一个注册的WIT
2166
基于系统配置，将接收的有效载荷与针对选定的WIT的存储的模型有效载荷进行比较
2168
存储的模型有效载荷与接收的有效载荷相匹配？
是
否
2170
是
存在另一个注册的WIT要进行评估？
否
2172
将中央服务器配置为使用存储的初始模型有效载荷，对接收的有效载荷进行评估
2174
基于匹配，确定WIT标识
2176
基于接收的有效载荷，更新数据库与WIT计数器

图 21B

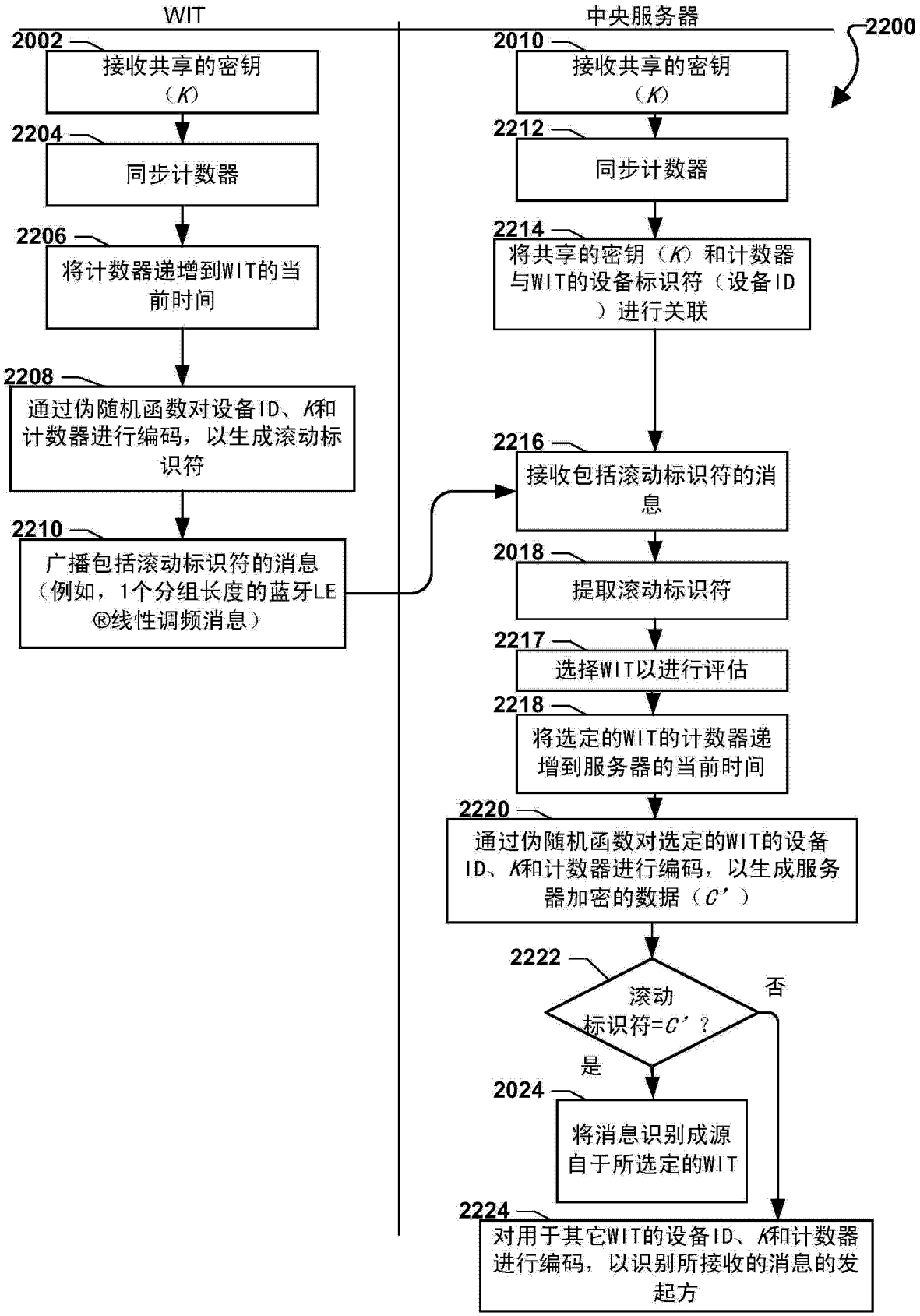

WIT
中央服务器
2200
2002
接收共享的密钥（K）
2204
同步计数器
2206
将计数器递增到WIT的当前时间
2208
通过伪随机函数对设备ID、K和计数器进行编码，以生成滚动标识符
2210
广播包括滚动标识符的消息（例如，1个分组长度的蓝牙LE®线性调频消息）
2010
接收共享的密钥（K）
2212
同步计数器
2214
将共享的密钥（K）和计数器与WIT的设备标识符（设备ID）进行关联
2216
接收包括滚动标识符的消息
2018
提取滚动标识符
2217
选择WIT以进行评估
2218
将选定的WIT的计数器递增到服务器的当前时间
2220
通过伪随机函数对选定的WIT的设备ID、K和计数器进行编码，以生成服务器加密的数据（C'）
2222
滚动标识符=C'？
否
是
2024
将消息识别成源自于所选定的WIT
2224
对用于其它WIT的设备ID、K和计数器进行编码，以识别所接收的消息的发起方

图 22

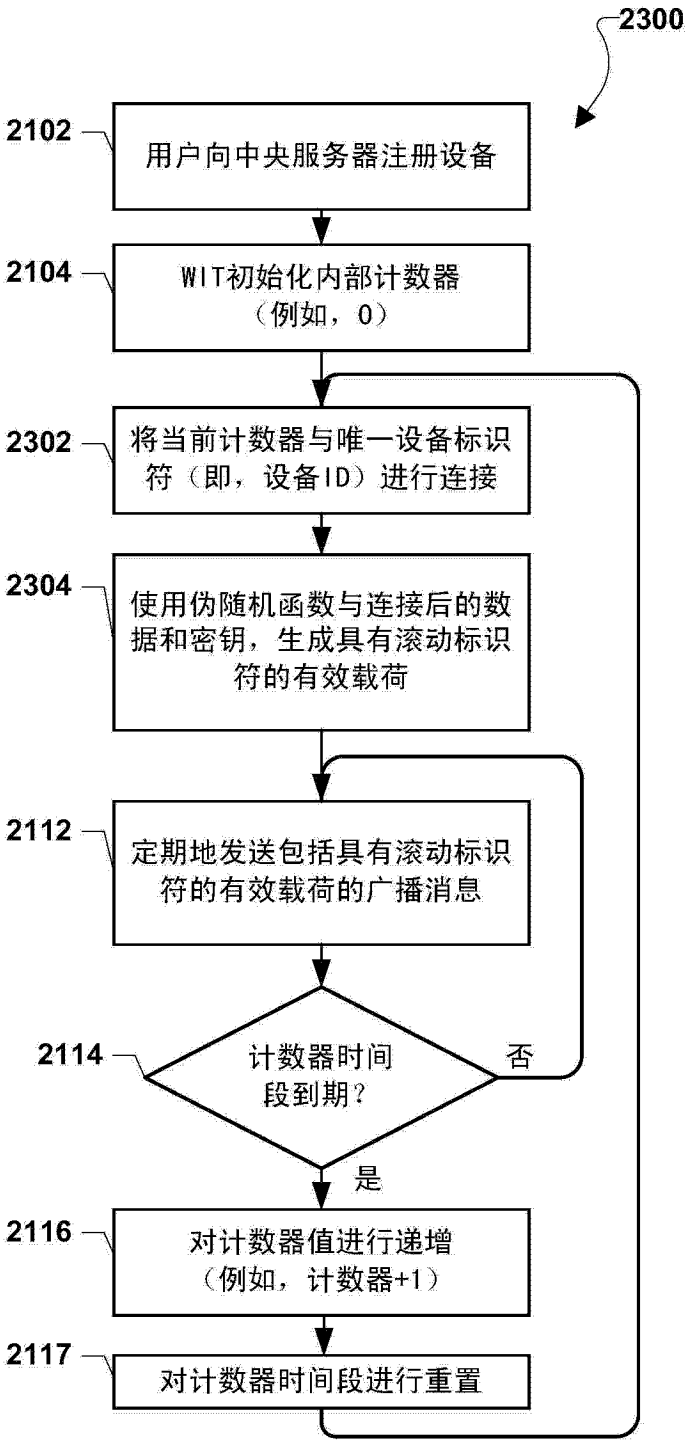

2300
2102
用户向中央服务器注册设备
2104
WIT初始化内部计数器
（例如，0）
2302
将当前计数器与唯一设备标识符（即，设备ID）进行连接
2304
使用伪随机函数与连接后的数据和密钥，生成具有滚动标识符的有效载荷
2112
定期地发送包括具有滚动标识符的有效载荷的广播消息
2114
计数器时间段到期？
否
是
2116
对计数器值进行递增
（例如，计数器+1）
2117
对计数器时间段进行重置

图 23A

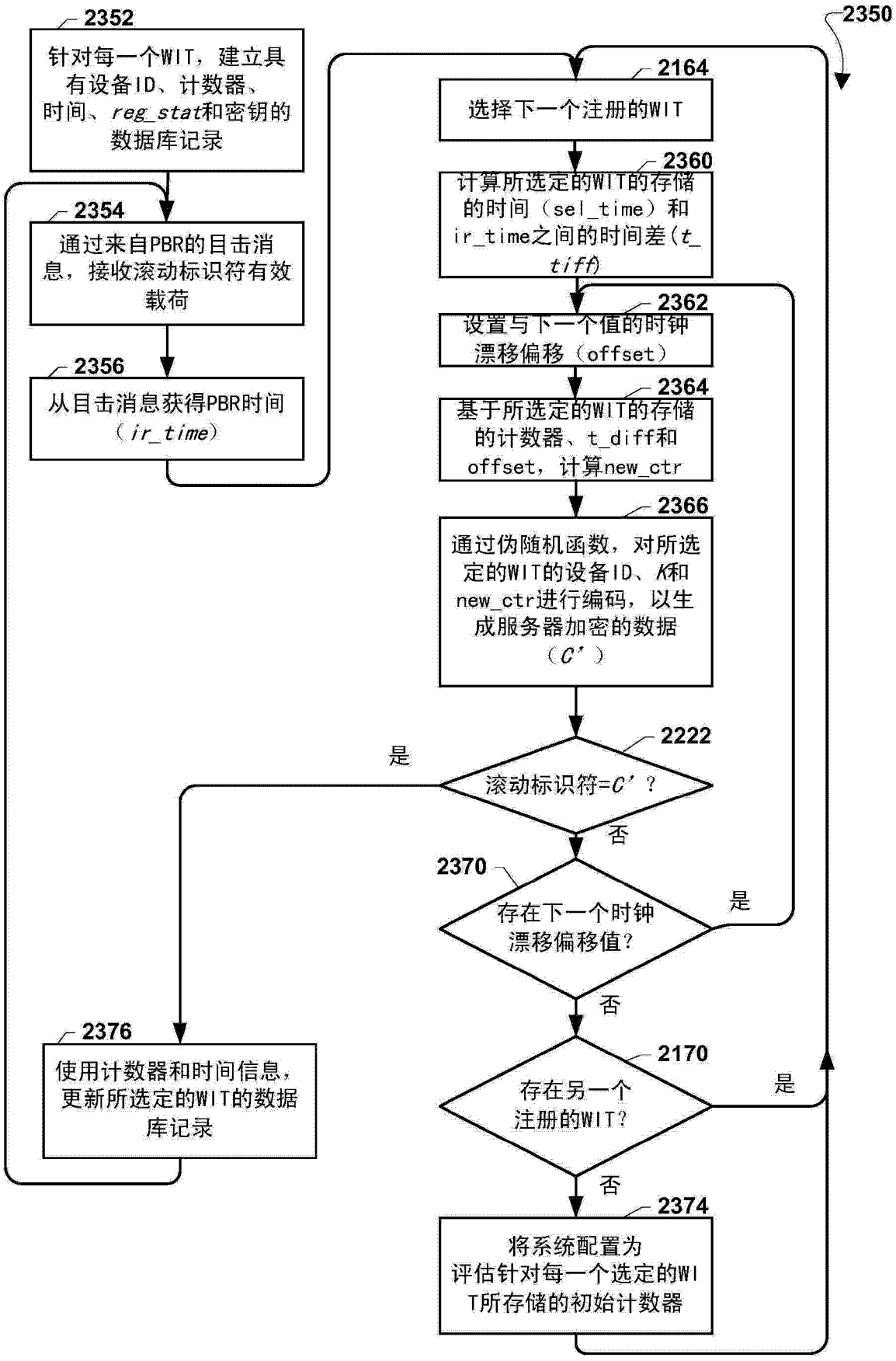

2352
针对每一个WIT，建立具有设备ID、计数器、时间、reg_stat和密钥的数据库记录
2354
通过来自PBR的目击消息，接收滚动标识符有效载荷
2356
从目击消息获得PBR时间（ir_time）
2350
2164
选择下一个注册的WIT
2360
计算所选定的WIT的存储的时间（sel_time）和ir_time之间的时间差（t_tiff）
2362
设置与下一个值的时钟漂移偏移（offset）
2364
基于所选定的WIT的存储的计数器、t_diff和offset，计算new_ctr
2366
通过伪随机函数，对所选定的WIT的设备ID、K和new_ctr进行编码，以生成服务器加密的数据（C'）
2222
滚动标识符=C'？
是
否
2370
存在下一个时钟漂移偏移值？
是
否
2376
使用计数器和时间信息，更新所选定的WIT的数据库记录
2170
存在另一个注册的WIT？
是
否
2374
将系统配置为评估针对每一个选定的WIT所存储的初始计数器

图 23B

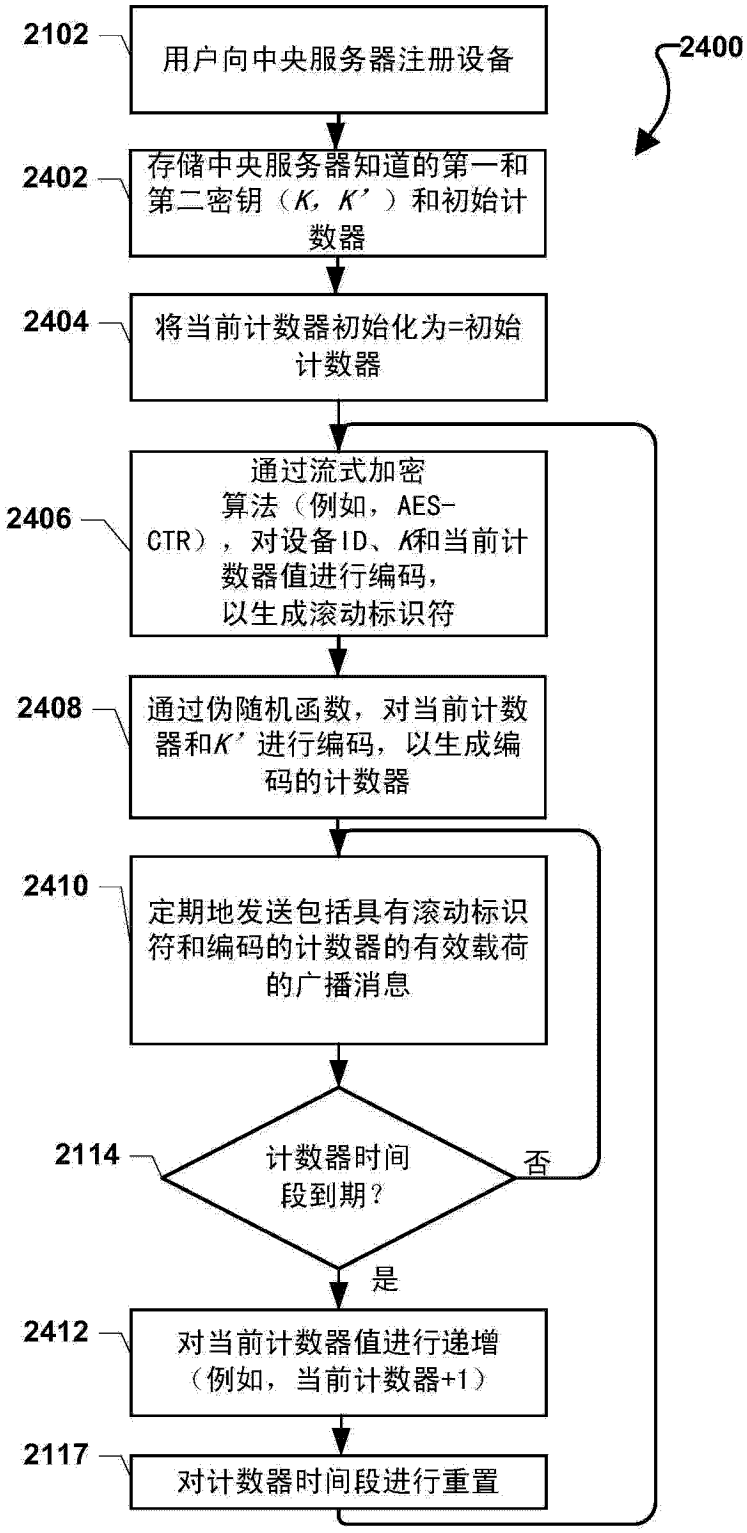

2102
用户向中央服务器注册设备
2400
2402
存储中央服务器知道的第一和第二密钥（K，K’）和初始计数器
2404
将当前计数器初始化为=初始计数器
2406
通过流式加密算法（例如，AES-CTR），对设备ID、K和当前计数器值进行编码，以生成滚动标识符
2408
通过伪随机函数，对当前计数器和K’进行编码，以生成编码的计数器
2410
定期地发送包括具有滚动标识符和编码的计数器的有效载荷的广播消息
2114
计数器时间段到期？
否
是
2412
对当前计数器值进行递增（例如，当前计数器+1）
2117
对计数器时间段进行重置

图 24A

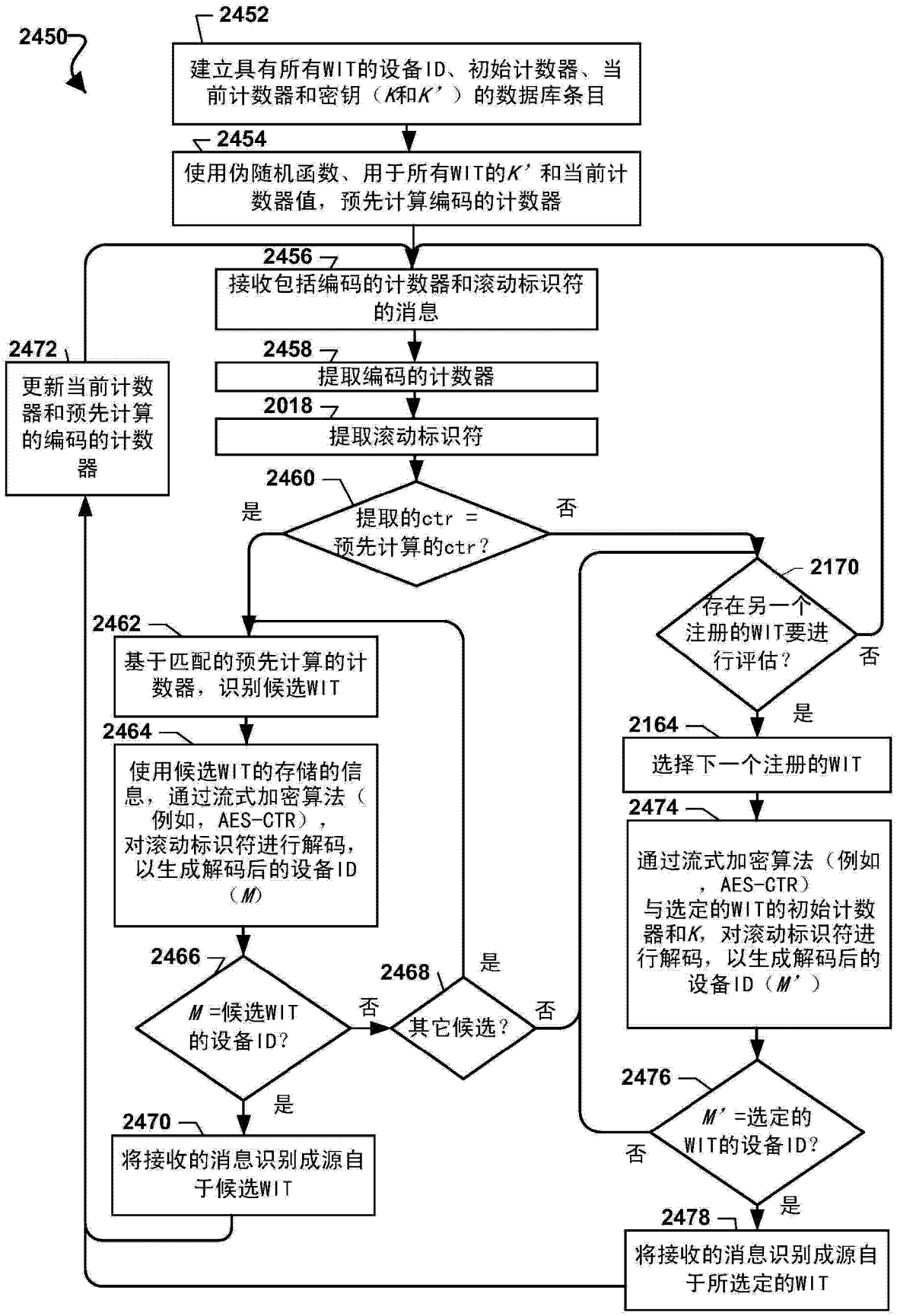

2450
2452
建立具有所有WIT的设备ID、初始计数器、当前计数器和密钥（K和K'）的数据库条目
2454
使用伪随机函数、用于所有WIT的K'和当前计数器值，预先计算编码的计数器
2456
接收包括编码的计数器和滚动标识符的消息
2458
提取编码的计数器
2018
提取滚动标识符
2460
提取的ctr = 预先计算的ctr？
是
否
2472
更新当前计数器和预先计算的编码的计数器
2462
基于匹配的预先计算的计数器，识别候选WIT
2464
使用候选WIT的存储的信息，通过流式加密算法（例如，AES-CTR），对滚动标识符进行解码，以生成解码后的设备ID（M）
2466
M =候选WIT的设备ID？
否
是
2468
其它候选？
是
否
2470
将接收的消息识别成源自于候选WIT
2170
存在另一个注册的WIT要进行评估？
否
是
2164
选择下一个注册的WIT
2474
通过流式加密算法（例如，AES-CTR）与选定的WIT的初始计数器和K，对滚动标识符进行解码，以生成解码后的设备ID（M'）
2476
M' =选定的WIT的设备ID？
否
是
2478
将接收的消息识别成源自于所选定的WIT

图 24B

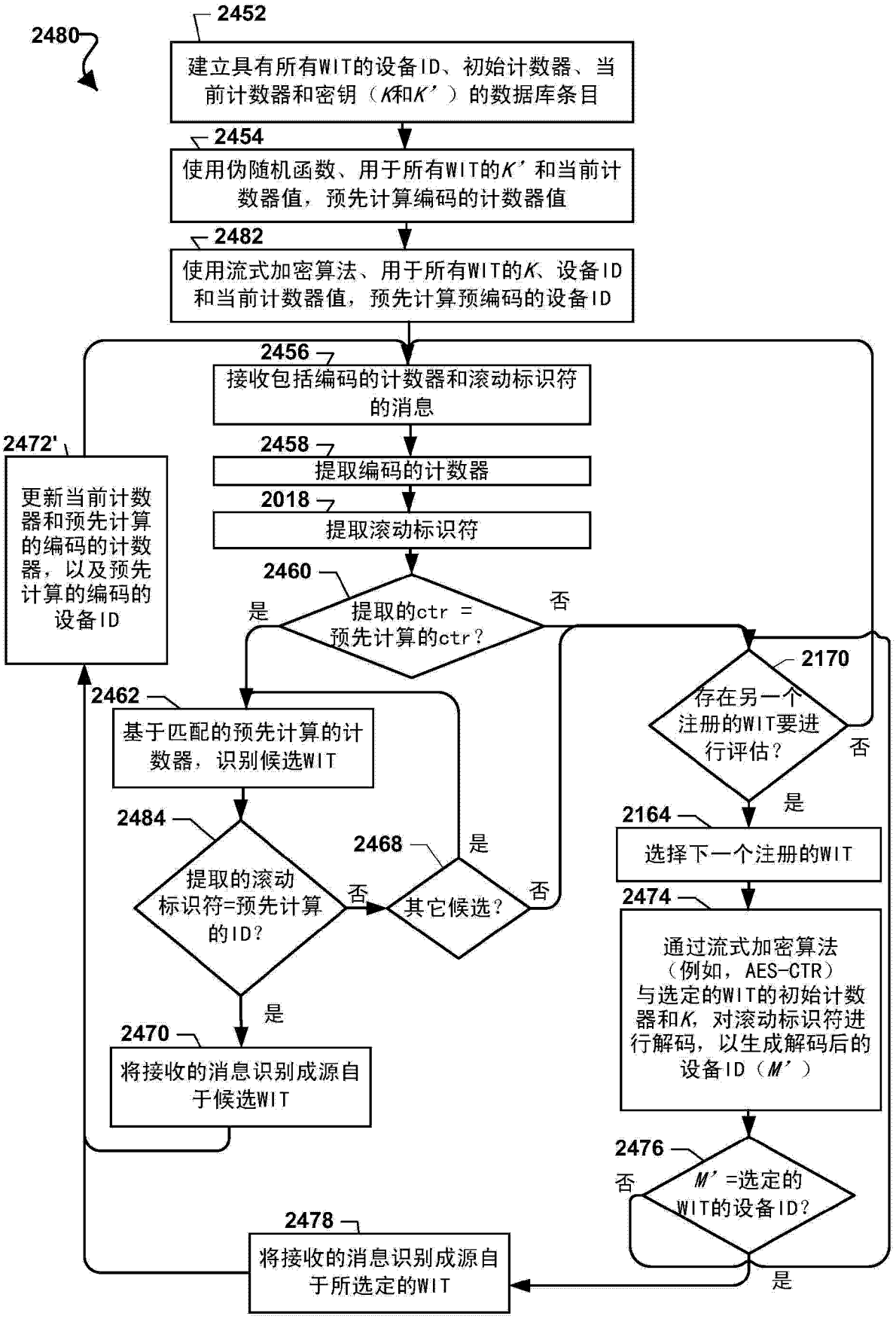

2480
2452
建立具有所有WIT的设备ID、初始计数器、当前计数器和密钥（K和K'）的数据库条目
2454
使用伪随机函数、用于所有WIT的K'和当前计数器值，预先计算编码的计数器值
2482
使用流式加密算法、用于所有WIT的K、设备ID和当前计数器值，预先计算预编码的设备ID
2456
接收包括编码的计数器和滚动标识符的消息
2458
提取编码的计数器
2018
提取滚动标识符
2460
提取的ctr = 预先计算的ctr？
是
否
2472'
更新当前计数器和预先计算的编码的计数器，以及预先计算的编码的设备ID
2462
基于匹配的预先计算的计数器，识别候选WIT
2484
提取的滚动标识符=预先计算的ID？
否
2468
其它候选？
是
否
是
2470
将接收的消息识别成源自于候选WIT
2170
存在另一个注册的WIT要进行评估？
否
是
2164
选择下一个注册的WIT
2474
通过流式加密算法（例如，AES-CTR）与选定的WIT的初始计数器和K，对滚动标识符进行解码，以生成解码后的设备ID（M'）
2476
M'=选定的WIT的设备ID？
否
是
2478
将接收的消息识别成源自于所选定的WIT

图 24C

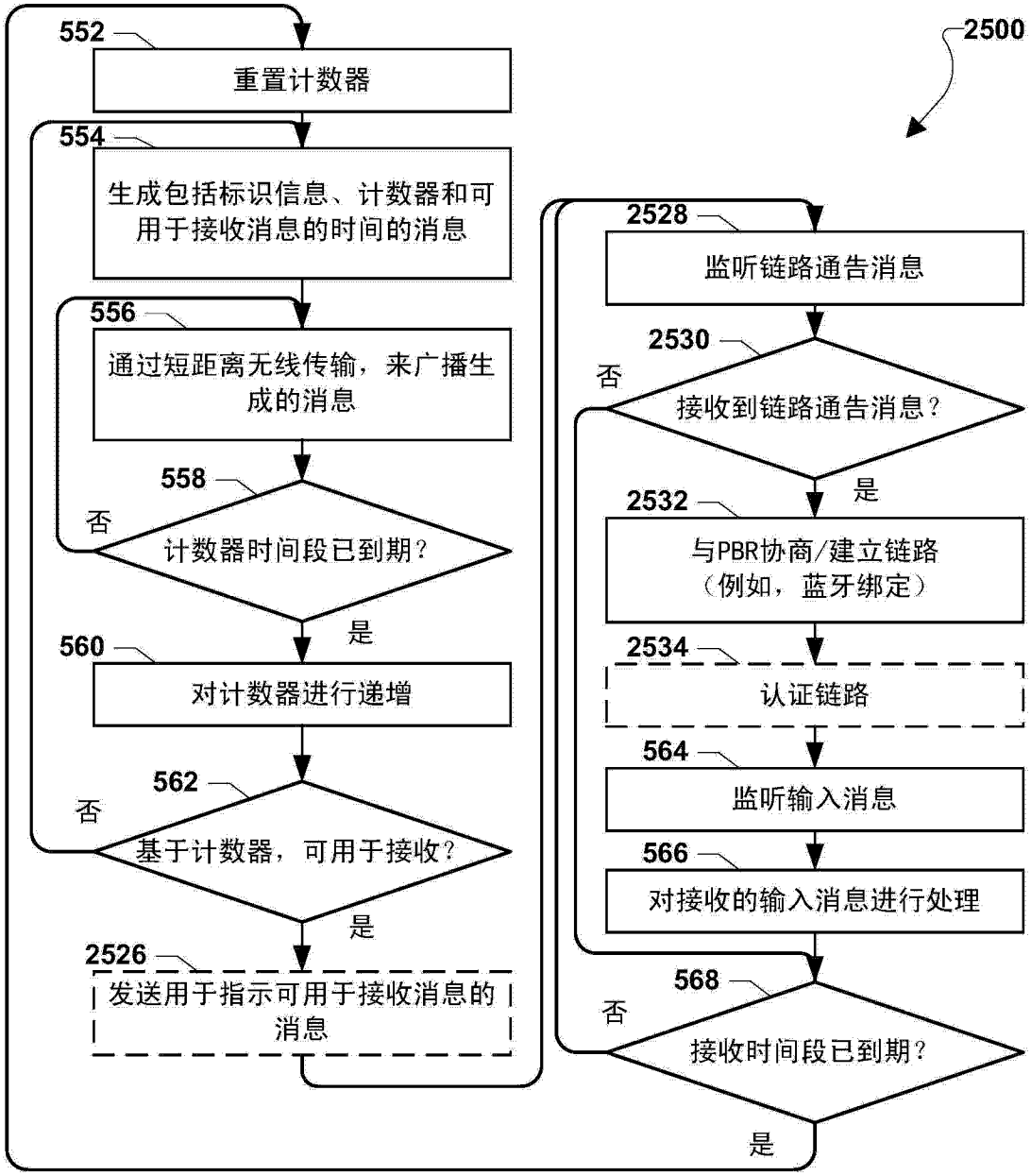

2500
552
重置计数器
554
生成包括标识信息、计数器和可用于接收消息的时间的消息
556
通过短距离无线传输，来广播生成的消息
558
计数器时间段已到期？
否
是
560
对计数器进行递增
562
基于计数器，可用于接收？
否
是
2526
发送用于指示可用于接收消息的消息
2528
监听链路通告消息
2530
接收到链路通告消息？
否
是
2532
与PBR协商/建立链路（例如，蓝牙绑定）
2534
认证链路
564
监听输入消息
566
对接收的输入消息进行处理
568
接收时间段已到期？
否
是

图 25A

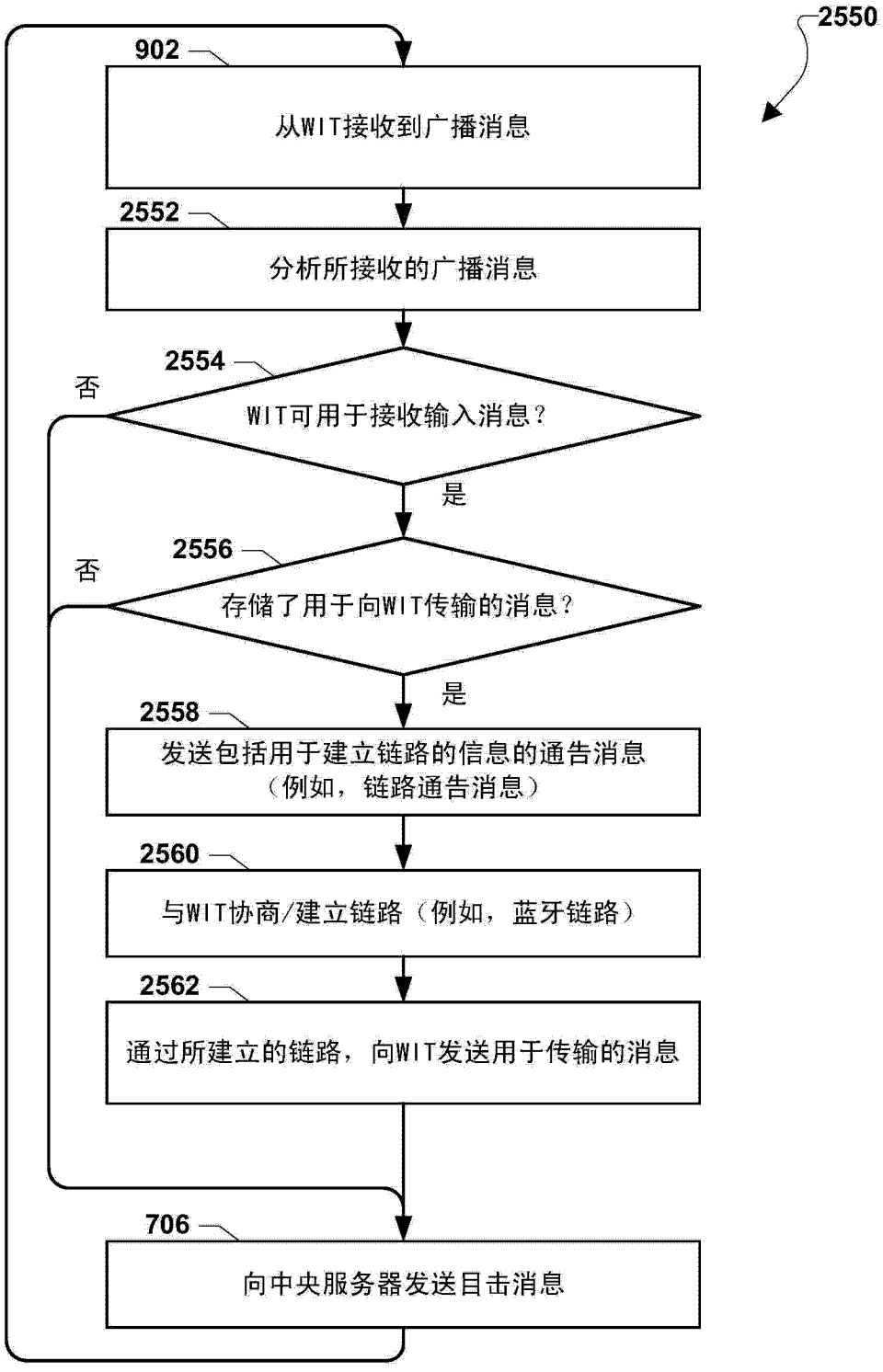

2550
902
从WIT接收到广播消息
2552
分析所接收的广播消息
2554
WIT可用于接收输入消息？
否
是
2556
存储了用于向WIT传输的消息？
否
是
2558
发送包括用于建立链路的信息的通告消息
（例如，链路通告消息）
2560
与WIT协商/建立链路（例如，蓝牙链路）
2562
通过所建立的链路，向WIT发送用于传输的消息
706
向中央服务器发送目击消息

图 25B

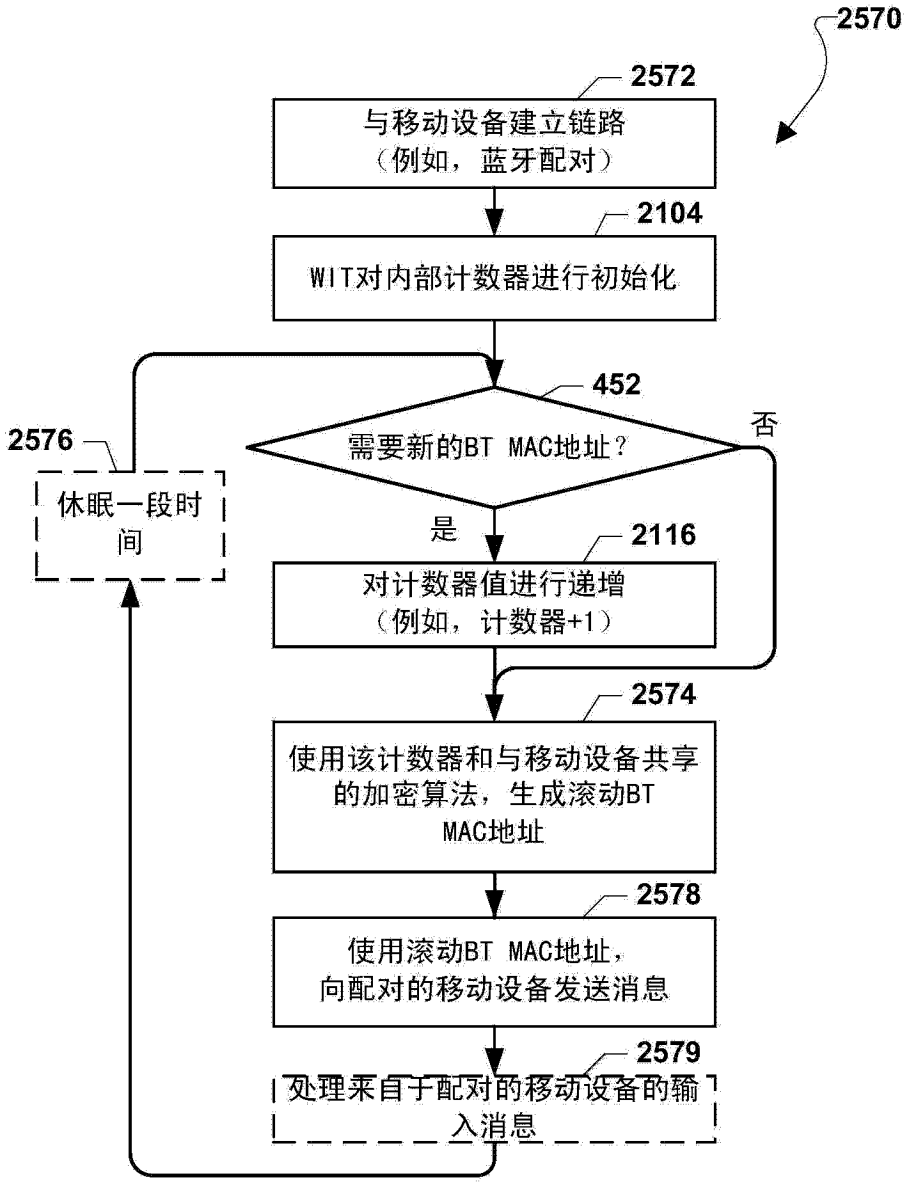

2570
2572
与移动设备建立链路
（例如，蓝牙配对）
2104
WIT对内部计数器进行初始化
452
需要新的BT MAC地址？
否
是
2576
休眠一段时间
2116
对计数器值进行递增
（例如，计数器+1）
2574
使用该计数器和与移动设备共享的加密算法，生成滚动BT MAC地址
2578
使用滚动BT MAC地址，向配对的移动设备发送消息
2579
处理来自于配对的移动设备的输入消息

图 25C

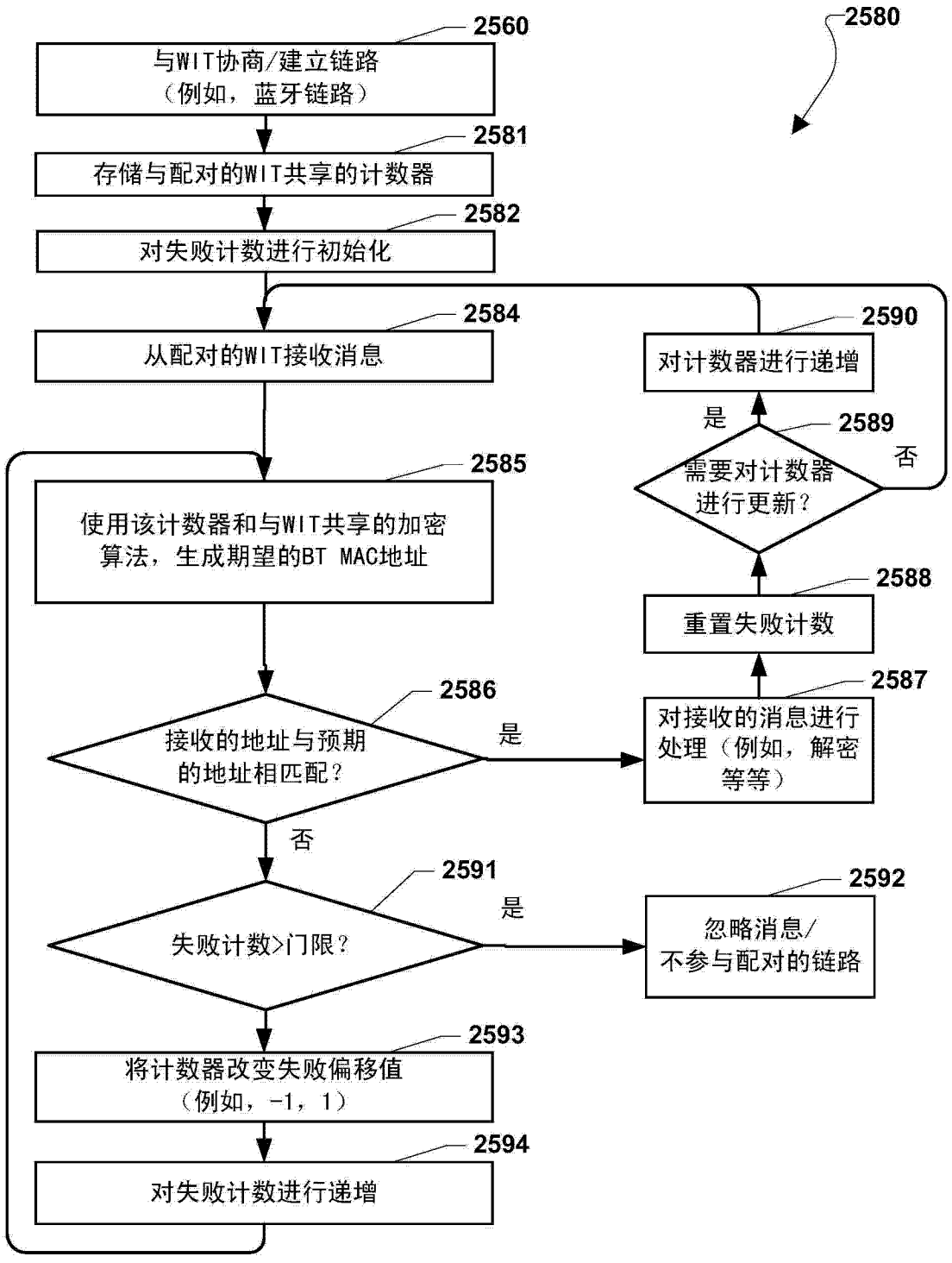

2580
2560
与WIT协商/建立链路
（例如，蓝牙链路）
2581
存储与配对的WIT共享的计数器
2582
对失败计数进行初始化
2584
从配对的WIT接收消息
2585
使用该计数器和与WIT共享的加密
算法，生成期望的BT MAC地址
2586
接收的地址与预期
的地址相匹配？
是
否
2591
失败计数>门限？
是
2592
忽略消息/
不参与配对的链路
2593
将计数器改变失败偏移值
（例如，-1，1）
2594
对失败计数进行递增
2590
对计数器进行递增
是
2589
需要对计数器
进行更新？
否
2588
重置失败计数
2587
对接收的消息进行
处理（例如，解密
等等）

图 25D

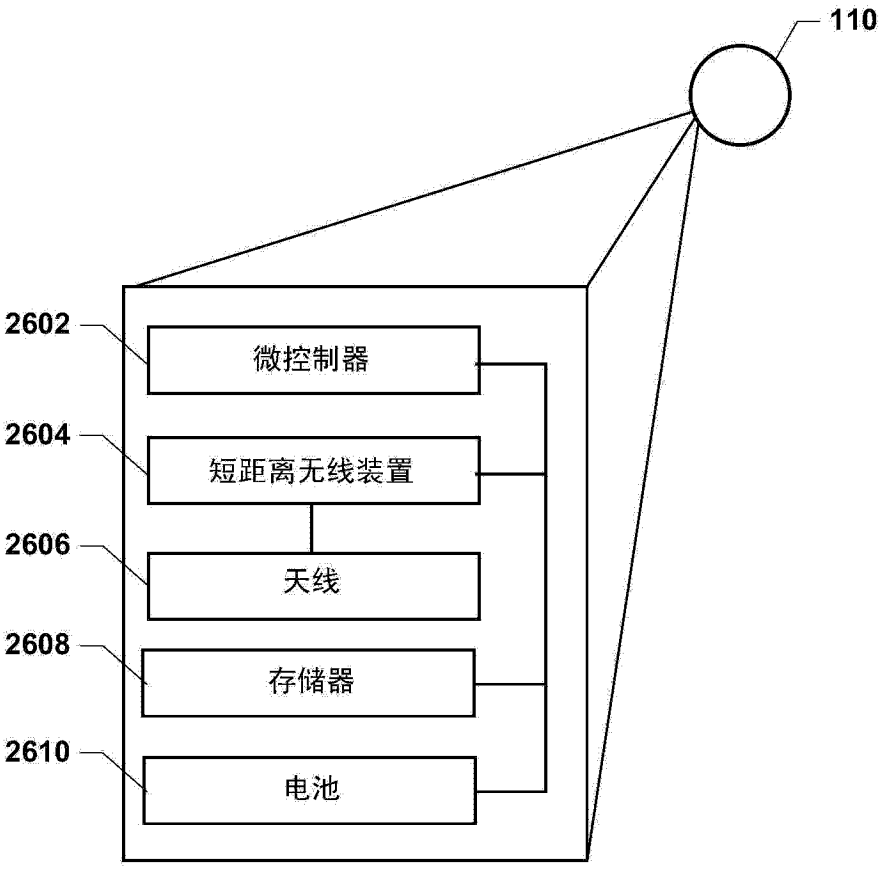



图 26A

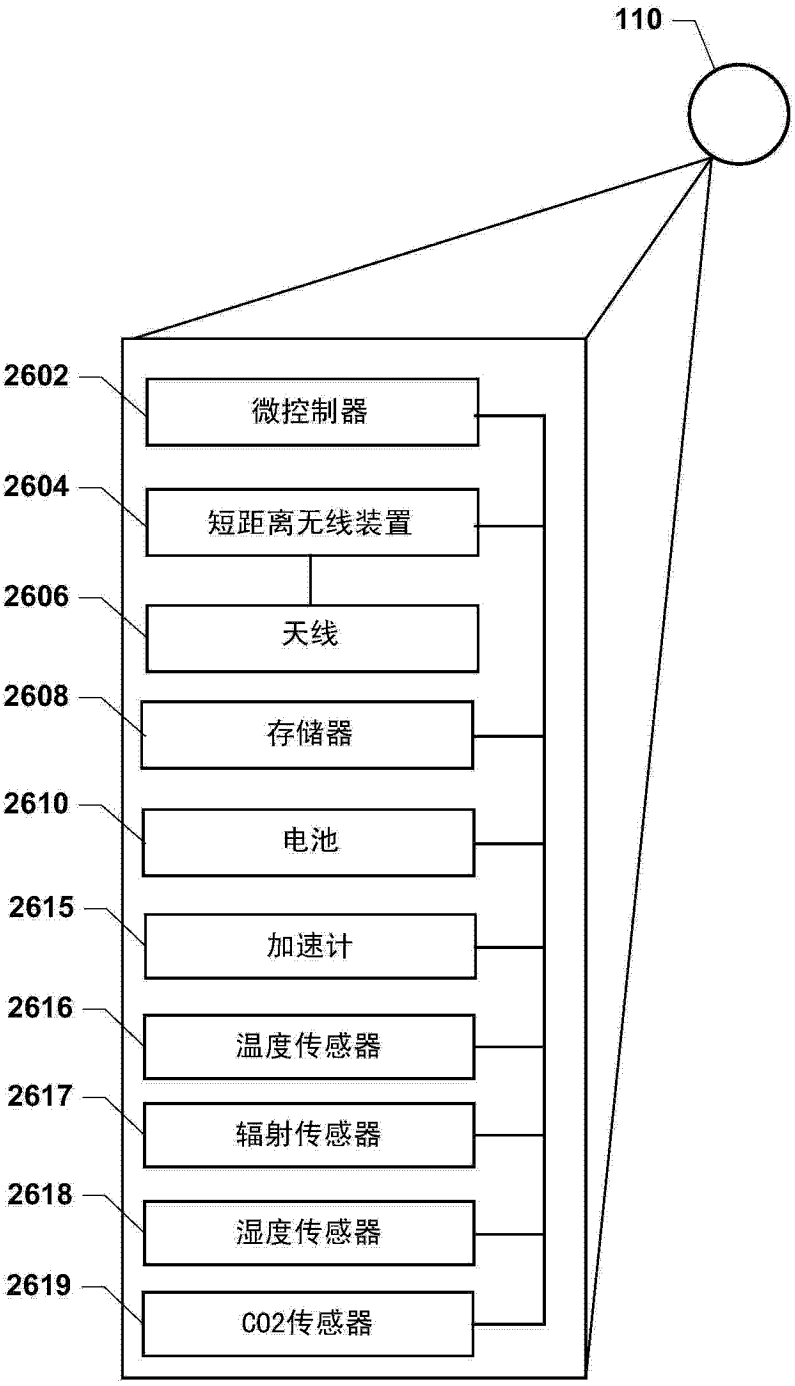

110
2602
微控制器
2604
短距离无线装置
2606
天线
2608
存储器
2610
电池
2615
加速计
2616
温度传感器
2617
辐射传感器
2618
湿度传感器
2619
CO2传感器

图 26B

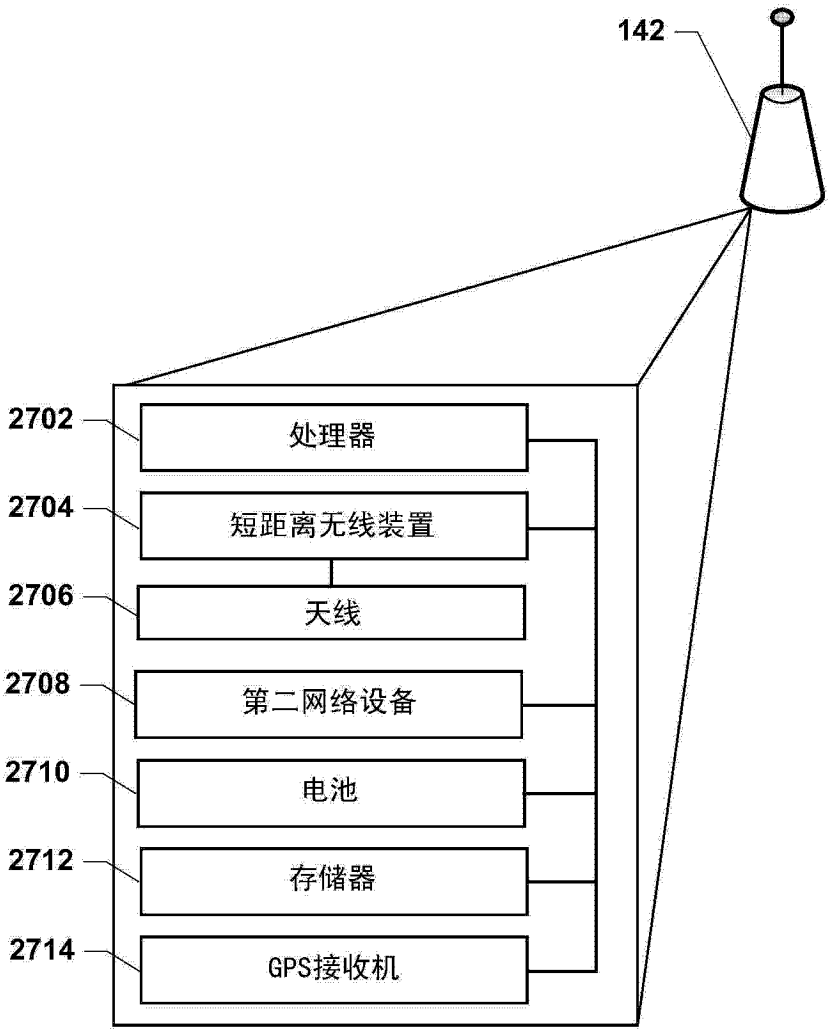

142
2702
处理器
2704
短距离无线装置
2706
天线
2708
第二网络设备
2710
电池
2712
存储器
2714
GPS接收机

图 27A

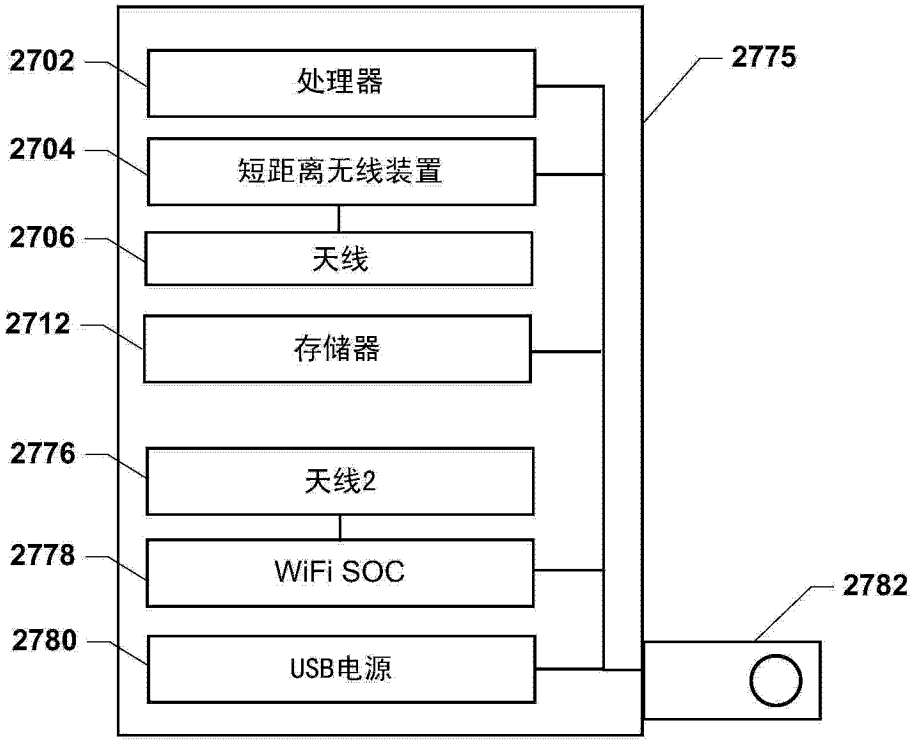

2702
处理器
2704
短距离无线装置
2706
天线
2712
存储器
2776
天线2
2778
WiFi SOC
2780
USB电源
2775
2782

图 27B

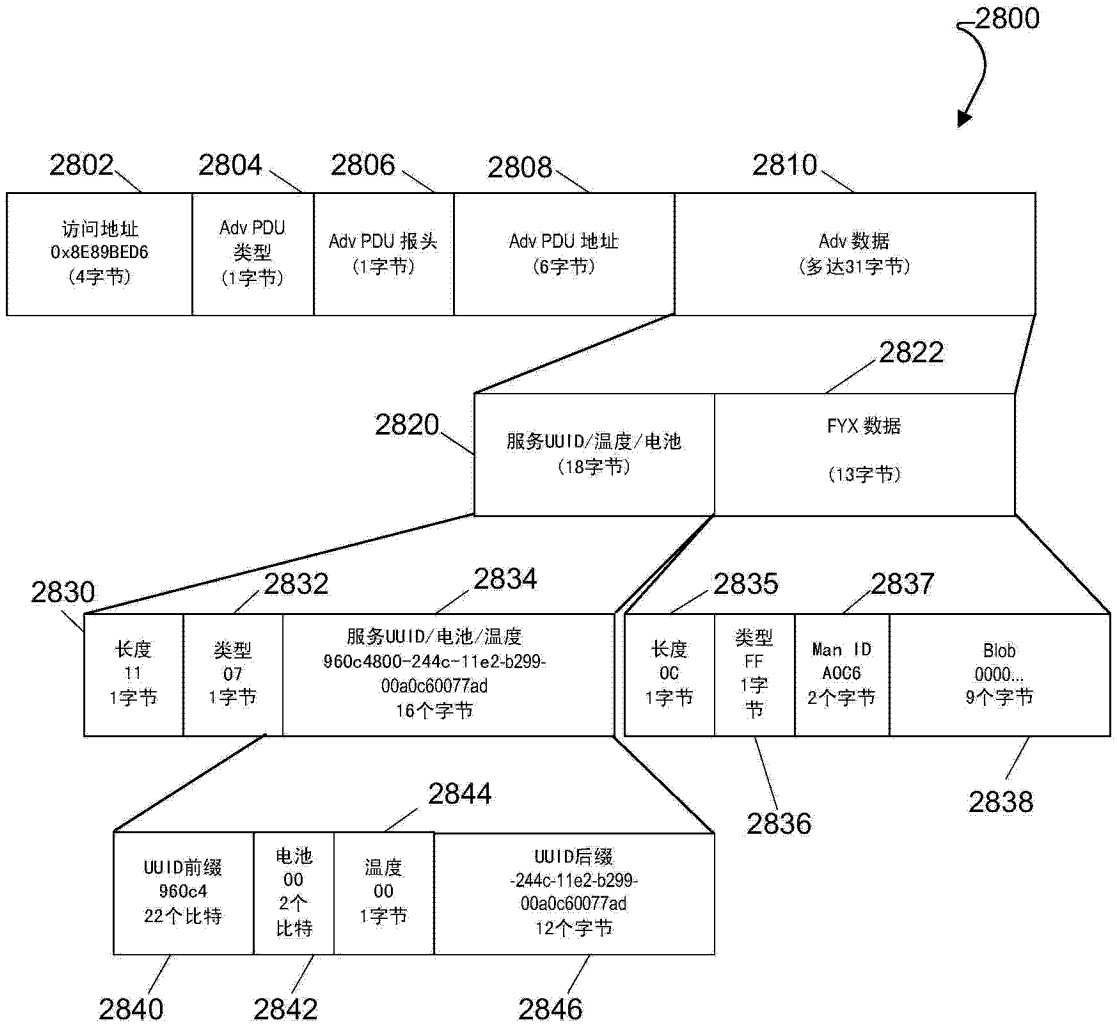

2800
2802
2804
2806
2808
2810
访问地址
0x8E89BED6
(4字节)
Adv PDU
类型
(1字节)
Adv PDU 报头
(1字节)
Adv PDU 地址
(6字节)
Adv 数据
(多达31字节)
2822
2820
服务UUID/温度/电池
(18字节)
FYX 数据
(13字节)
2830
2832
2834
2835
2837
长度
11
1字节
类型
07
1字节
服务UUID/电池/温度
960c4800-244c-11e2-b299-
00a0c60077ad
16个字节
长度
0C
1字节
类型
FF
1字
节
Man ID
A0C6
2个字节
Blob
0000...
9个字节
2836
2838
2844
UUID前缀
960c4
22个比特
电池
00
2个
比特
温度
00
1字节
UUID后缀
-244c-11e2-b299-
00a0c60077ad
12个字节
2840
2842
2846

图 28

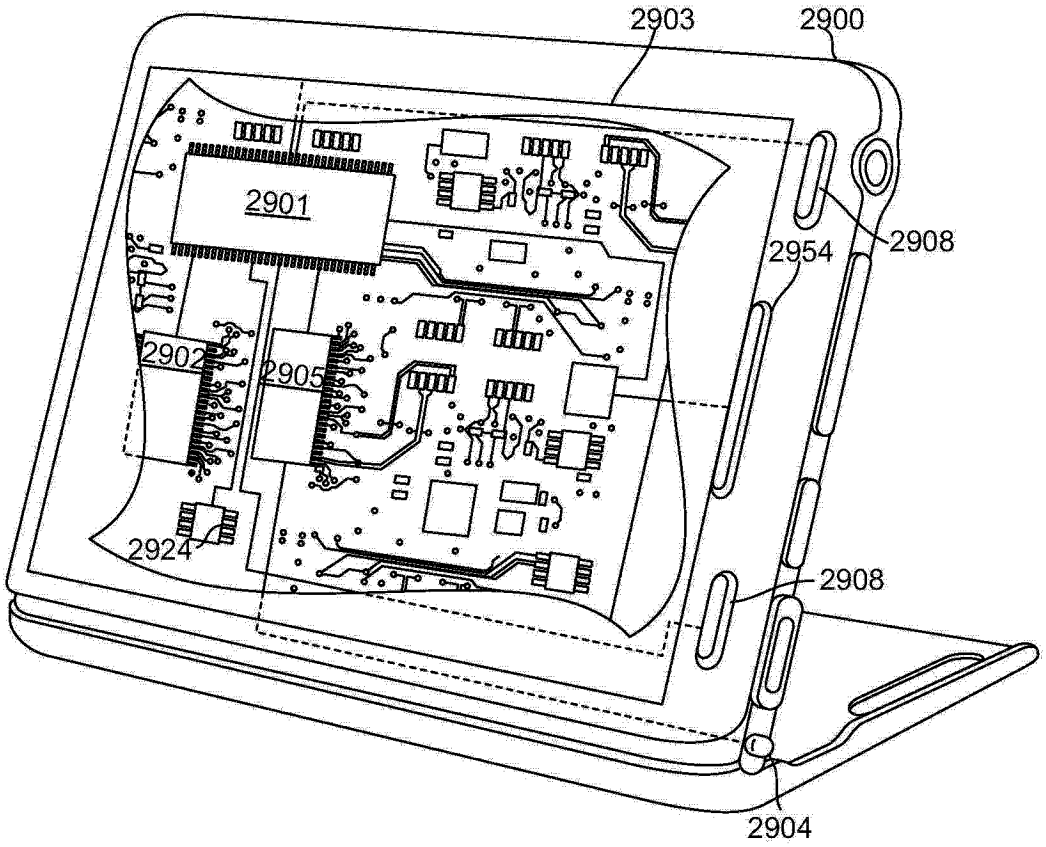

2903
2900
2901
2908
2954
2902
2905
2924
2908
2904

图 29

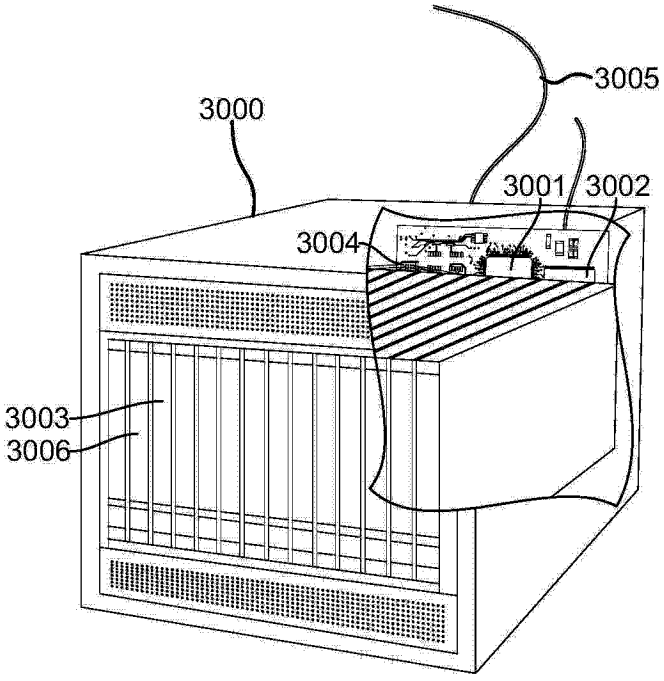

3005
3000
3001
3002
3004
3003
3006

图 30