(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112889242 B
(45)授权公告日 2024.11.26

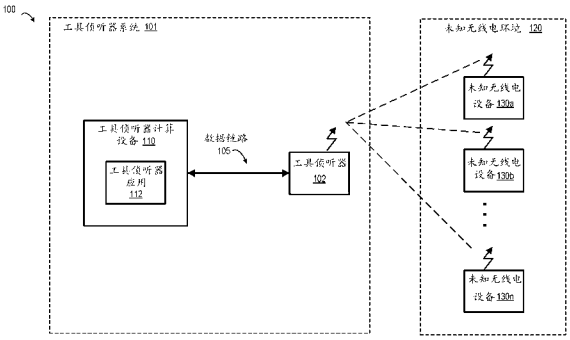
(21)申请号 201980071162.5
(22)申请日 2019.08.28
(65)同一申请的已公布的文献号
申请公布号 CN 112889242 A
(43)申请公布日 2021.06.01
(30)优先权数据
16/115837 2018.08.29 US
(85)PCT国际申请进入国家阶段日
2021.04.27
(86)PCT国际申请的申请数据
PCT/US2019/048515 2019.08.28
(87)PCT国际申请的公布数据
WO2020/047060 EN 2020.03.05
(73)专利权人 兰迪斯+盖尔科技股份有限公司
地址 美国佐治亚州
(72)发明人 A·B·洛厄尔
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 赵碧洋
(51)Int.Cl.
H04L 43/0817(2022.01)
H04L 12/46(2006.01)
H04L 41/22(2022.01)
H04L 41/0816(2022.01)
H04B 1/7156(2011.01)
(56)对比文件
US 2016337783 A1,2016.11.17
US 2018027054 A1,2018.01.25
US 5408506 A,1995.04.18
审查员 苏星晔
权利要求书5页 说明书7页 附图5页

(54)发明名称

用于检测来自无线电设备的通信的设备和方法

(57)摘要

一种包括收发器的工具侦听设备被配置成：在从发现信道跳跃序列中选择的无线电信道上进行侦听。工具侦听设备被配置成标识前导码，前导码指示分组的开始。工具侦听设备继续侦听，直到接收到分组报头。工具侦听器从分组报头中提取源地址、目的地址和帧类型。工具侦听设备将源地址、目的地址和帧类型添加到数据结构，并且将数据结构传输到外部设备，在所述外部设备中，数据可以被可视化。工具侦听设备进一步被配置成从发现信道跳跃序列中选择另一个无线电信道。



CN 112889242 B

1.一种用于检测来自无线电设备的通信的设备,所述设备包括收发器,所述收发器被配置成:

在从发现信道跳跃序列中选择的无线电信道上进行侦听,其中发现信道跳跃序列(i)使用与由所述无线电设备使用的信道跳跃序列所使用的序列不同的序列,并且(ii)包括由所述无线电设备的信道跳跃序列使用的多个无线电信道;

响应于标识分组的前导码,所述分组包括报头:

继续侦听,直到接收到报头,

从报头中提取源地址、目的地址和帧类型,

将源地址、目的地址和帧类型添加到数据结构,以及

将数据结构传输到外部设备,其中传输数据结构使得所述外部设备将数据结构可视化;以及

响应于或者(i)接收到附加分组或者(ii)确定预定时间量已经过去,从发现信道跳跃序列中选择下一个无线电信道。

2.根据权利要求1所述的设备,其中所述预定时间量与所述无线电设备所使用的时隙不同。

3.根据权利要求1所述的设备,其中所述收发器进一步被配置成:通过从前导码中标识对应于特定无线电设备的设备标识符来标识所述特定无线电设备。

4.根据权利要求1所述的设备,其中所述外部设备在可视化中显示包括源地址和目的地址的信息。

5.根据权利要求1所述的设备,其中所述分组进一步包括循环冗余校验,并且其中所述外部设备进一步被配置成基于循环冗余校验来确定所述分组是有效的。

6.根据权利要求1所述的设备,其中所述分组包括有效载荷,并且其中所述外部设备进一步被配置成丢弃所述有效载荷。

7.根据权利要求1所述的设备,其中所述分组是(i)确认分组、(ii)信标分组、(iii)信标请求分组、或(iv)数据分组。

8.根据权利要求1所述的设备,其中发现信道跳跃序列包括由所述无线电设备的信道跳跃序列使用的所有所述多个无线电信道。

9.根据权利要求1所述的设备,其中所述分组进一步包括(i)PAN ID或(ii)网络ID,并且其中所述外部设备进一步被配置成提取(i)PANID或(ii)来自所述分组的网络ID。

10.一种用于检测来自无线电设备的射频通信的系统,所述系统包括:

收发器,其被配置成:

在从发现信道跳跃序列中选择的无线电信道上进行侦听,其中发现信道跳跃序列(i)使用与由所述无线电设备使用的信道跳跃序列所使用的序列不同的序列,并且(ii)包括由所述无线电设备的信道跳跃序列使用的多个无线电信道;

响应于标识分组的前导码,所述分组包括报头:

继续侦听,直到接收到报头,

从报头中提取源地址、目的地址和帧类型,

将源地址、目的地址和帧类型添加到数据结构,以及

将数据结构传输到外部设备;以及

响应于或者(i)接收到附加分组或者(ii)确定预定时间量已经过去,从发现信道跳跃序列中选择下一个无线电信道,

其中所述外部设备被配置成:

从所述收发器接收数据结构;

从数据结构中提取源地址、目的地址和帧类型,其中帧类型包括确认、数据或信标;以及

在显示设备上将源地址、目的网络地址和帧类型可视化。

11.根据权利要求10所述的系统,其中所述收发器进一步被配置成:通过从前导码中标识对应于特定无线电设备的设备标识符来标识所述特定无线电设备。

12.根据权利要求10所述的系统,其中所述外部设备在可视化中显示来自数据结构的信息。

13.根据权利要求10所述的系统,其中所述分组进一步包括循环冗余校验,并且其中所述收发器进一步被配置成基于循环冗余校验来确定所述分组是有效的。

14.根据权利要求10所述的系统,其中所述分组包括有效载荷,并且其中所述收发器进一步被配置成丢弃所述分组的有效载荷。

15.根据权利要求10所述的系统,其中发现信道跳跃序列包括由所述无线电设备的信道跳跃序列使用的所有所述多个无线电信道。

16.一种存储计算机可执行程序指令的非暂时性计算机可读存储介质,其中在由处理设备执行时,所述计算机可执行程序指令使得处理设备执行包括以下步骤的操作:

在从发现信道跳跃序列中选择的无线电信道上进行侦听,其中发现信道跳跃序列(i)使用与由无线电设备使用的信道跳跃序列所使用的序列不同的序列,并且(ii)包括由所述无线电设备的信道跳跃序列使用的多个无线电信道;

响应于标识分组的前导码,所述分组包括报头:

继续侦听,直到接收到报头,

从报头中提取源地址、目的地址和帧类型,

将源地址、目的地址和帧类型添加到数据结构,以及

将数据结构传输到外部设备,其中所述传输使得所述外部设备将数据结构可视化;以及响应于或者(i)接收到附加分组或者(ii)确定预定时间量已经过去,从发现信道跳跃序列中选择下一个无线电信道。

17.根据权利要求16所述的非暂时性计算机可读存储介质,所述操作进一步包括:通过从前导码中标识对应于特定无线电设备的设备标识符来标识所述特定无线电设备。

18.根掘权利要求16所述的非暂时性计算机可读存储介质,其中所述传输使得所述外部设备在可视化中显示包括源地址和目的地址的信息。

19.根据权利要求16所述的非暂时性计算机可读存储介质,其中所述分组包括有效载荷,并且其中所述操作进一步包括丢弃所述分组的有效载荷。

20.根据权利要求16所述的非暂时性计算机可读存储介质,其中发现信道跳跃序列包括由所述无线电设备的信道跳跃序列使用的所有所述多个无线电信道。

21.一种用于检测来自无线电设备的通信的方法,包括:

在不加入第一网状网络的情况下,在从发现信道跳跃序列中选择的第一无线电信道上

进行侦听,其中发现信道跳跃序列(i)使用与由在第一网状网络上操作的第一无线电设备使用的信道跳跃序列和/或由在第二网状网络上操作的第二无线电设备使用的信道跳跃序列所使用的序列不同的序列,并且(ii)包括由所述第一无线电设备的信道跳跃序列使用的多个无线电信道;

当在所述第一无线电信道上接收到第一分组的前导码时:

继续在所述第一无线电信道上进行侦听,直到接收到第一报头;

使用数据链路向外部设备传输所述第一报头;其中所述第一报头包括与所述第一网状网络相关联的至少一个标识符;

在接收到所述第一分组后,从所述发现信道跳跃序列选择后续无线电信道;以及

在不加入所述第二网状网络的情况下,在所述后续无线电信道上进行侦听:以及

当在所述后续无线电信道上接收到第二分组的前导码时:

继续侦听所述后续无线电信道,直到接收到第二报头;以及

使用所述数据链路将所述第二报头传输到所述外部设备,其中所述第二报头包括至少一个与所述第二网状网络相关联的标识符。

22.根据权利要求21所述的方法,其中所述第一分组包括有效载荷,所述方法进一步包括:当接收到第一分组的前导码时,丢弃所述有效载荷。

23.根据权利要求21所述的方法,其中所述第一分组是(i)确认分组、(ii)信标分组、(iii)信标请求分组、或(iv)数据分组。

24.根据权利要求21所述的方法,其中发现信道跳跃序列包括由所述第一无线电设备的信道跳跃序列使用的所有所述多个无线电信道。

25.根据权利要求21所述的方法,其中所述第一分组进一步包括(i)PANID或(ii)网络ID,所述方法进一步包括:提取(i)PANID或(ii)网络ID,并且将(i)PANID或(ii)网络ID提供给所述外部设备。

26.根据权利要求21所述的方法,其中当没有在所述第一无线电信道上接收到第一分组的前导码时,等待预定时间量过去,以及

所述预定时间量与所述第一无线电设备在所述第一网状网络上操作时所使用的时隙不同。

27.根据权利要求21所述的方法,进一步包括:

从所述第一报头中标识对应于在第一网状网络上操作的所述第一无线电设备的源地址;以及

使得所述第一无线电设备加入诊断网络。

28.一种用于检测来自无线电设备的通信的方法,包括:

在不加入第一网状网络或与该第一网状网络同步的情况下,在从用于来自加入第一网状网络的第一设备的通信的发现信道跳跃序列中选择的无线电信道上进行侦听,其中发现信道跳跃序列包括与用于第一网状网络上的通信的信道跳跃序列不同的无线电信道序列;

响应于标识第一分组的前导码,所述第一分组包括报头:

继续侦听,直到接收到所述第一分组;

分析所述第一分组,以标识来自所述第一分组的报头的信息;以及

将来自所述第一分组的报头的信息存储在数据结构中;

在接收到所述第一分组之后,从发现信道跳跃序列中选择下一个无线电信道;以及

在不加入第二网状网络或与之同步的情况下,在从用于来自加入所述第二网状网络的第二设备的通信的发现信道跳跃序列中选择的下一个无线电信道上进行侦听;响应于标识第二分组的前导码,其中所述第二分组包括报头;

继续侦听,直到接收到所述第二分组;

分析所述第二分组,以标识来自所述第二分组的所述报头的信息;以及

将来自所述第二分组的报头的信息存储在所述数据结构中。

29.根据权利要求28所述的方法,进一步包括:从所述第一分组中提取网络地址和帧类型,其中帧类型包括确认、数据或信标。

30.根据权利要求28所述的方法,进一步包括:从所述第一分组的所述报头中标识对应于所述第一设备的设备标识符。

31.根据权利要求30所述的方法,进一步包括:将来自所述第一分组的报头的信息与数据结构中的来自具有相同标识符的另一分组的另一报头的信息相关联。

32.根据权利要求28所述的方法,其中发现信道跳跃序列包括由所述第一网状网络的信道跳跃序列使用的所有多个无线电信道。

33.根据权利要求28所述的方法,其中所述第一分组的所述报头进一步包括(i)PAN ID或(ii)网络ID,所述方法进一步包括提取(i)PANID或(ii)网络ID。

34.一种用于检测来自无线电设备的通信的方法,包括:

标识发现信道跳跃序列中的第一无线电信道,其中发现信道跳跃序列(i)使用与由第一网状网络使用的信道跳跃序列所使用的序列不同的序列,并且(ii)包括由第一网状网络的信道跳跃序列使用的多个无线电信道;

在不加入第一网状网络的情况下,在第一无线电信道上进行侦听;

当在预定时间量内没有在第一无线电信道上检测到通信时,切换到发现信道跳跃序列中的第二无线电信道,其中所述预定时间量与第一网状网络所使用的时隙不同;

在不加入第一网状网络的情况下,在第二无线电信道上进行侦听;

当在第二无线电信道上进行侦听时,检测包括报头的第一分组的前导码,并且继续在第二无线电信道上进行侦听,直到接收到报头;

从所述第一分组的所述报头中标识对应于与所述第一分组和所述第一网状网络相关联的第一设备的源地址;以及

切换到发现信道跳跃序列中的第三无线电信道;

在不加入第二网状网络的情况下侦听所述第三无线电信道;

在所述第三无线电信道上侦听时,检测包含报头的第二分组的前导码,并继续在所述第三无线电信道上侦听,直到接收到所述第二分组的所述报头;以及

从所述第二分组的所述报头中标识与所述第二分组和所述第二网状网络相关联的第二设备对应的源地址。

35.根据权利要求34所述的方法,进一步包括:从所述第一分组中提取网络地址和帧类型,其中帧类型包括确认、数据或信标。

36.根据权利要求34所述的方法,进一步包括:通过从所述第一分组的所述报头中标识对应于特定无线电设备的特定网络地址来标识所述特定无线电设备。

37.根据权利要求34所述的方法,进一步包括:标识所述第一分组和后续分组,其中所述第一分组和所述后续分组源自于特定无线电设备;以及使得外部设备在可视化中显示来自所述第一分组和所述后续分组的信息。

38.根据权利要求34所述的方法,其中所述第一分组进一步包括循环冗余校验,所述方法进一步包括基于循环冗余校验来确定所述第一分组是有效的。

39.根据权利要求34所述的方法,其中所述第一分组包括有效载荷,所述方法进一步包括丢弃所述第一分组的有效载荷。

40.根据权利要求34所述的方法,其中所述第一网状网络的发现信道跳跃序列包括由所述信道跳跃序列使用的所有所述多个无线电信道。

用于检测来自无线电设备的通信的设备和方法

技术领域

[0001] 本文中描述的方面总体上涉及射频网络诊断工具,并且更具体地涉及标识可配置成在无线网状网络上操作的网络设备。

背景技术

[0002] 资源分配网络(诸如,电力、天然气或水分配网络)可以使用智能计量表来收集并聚集资源消耗数据。智能计量表可以帮助自动计费,降低成本,并且为公用事业公司提供高级分析工具。智能计量表可以被配置成在网状网络上操作。网状网络可以是具有或不具有中心节点的短距离无线网络。

[0003] 在智能计量表被添加到现有网络之前,将智能计量表配置成用于正常操作,例如通过配置一组网络参数。当被配置和放置在现场之后,智能计量表然后可以自动与网状网络建立连接。

[0004] 各种诊断工具可以用于标识智能计量表的故障。有缺陷的智能计量表从现场被带回到计量表维修设施,技术人员在那里执行诊断、维修或重新配置。技术人员可以使用诊断工具来确定智能计量表是针对特定网络配置的、正在尝试连接到网络、还是不可操作的。此外,技术人员可以使用诊断工具以将智能计量表配置成与测试网络通信,从而实现进一步的分析或网络重新配置。

[0005] 但是现有的诊断工具存在缺陷。具体地,现有的诊断工具要么被限于一次检测一个设备,从而需要标识符(诸如,网络或设备地址)以便针对计量表进行搜索,要么不必要地存储整个分组(packet),从而利用不必要的信息使诊断工具的视觉界面过载。

[0006] 因此,需要新的解决方案。

发明内容

[0007] 某些方面和特征包括用于检测射频设备的系统和方法。在一示例中,包括收发器的工具侦听设备被配置成:在从发现信道跳跃序列(hopping sequence)中选择的无线电信道上进行侦听。发现信道跳跃序列使用与所述射频设备所使用的信道跳跃序列不同的序列,并且包括由所述射频设备的信道跳跃序列使用的无线电信道。工具侦听设备标识分组的前导码。分组包括报头。工具侦听设备继续侦听,直到接收到报头。工具侦听设备从报头中提取源地址、目的地址和帧类型,并且将源地址、目的地址和帧类型添加到数据结构。工具侦听设备将数据结构传输到外部设备,这可以使得外部设备将数据结构可视化。响应于或者接收到分组或者确定预定时间量已经过去,工具侦听设备被配置成从发现信道跳跃序列中选择下一个无线电信道,并且在该信道上进行侦听。

[0008] 提及这些说明性示例不是为了限制或限定本公开,而是为了提供示例以帮助理解本公开。具体实施方式中提供了附加示例和进一步描述。

附图说明

[0009] 当参考附图阅读以下具体实施方式时,可以更好地理解本公开的这些和其他特征、方面和优点,在附图中:

[0010] 图1图示了根据一方面的工具侦听器环境的示例。

[0011] 图2图示了根据一方面的工具侦听器系统的实现方式。

[0012] 图3是图示了根据一方面的由工具侦听设备用于检测另一个设备的存在的过程的流程图。

[0013] 图4是图示了根据一方面的与工具侦听设备检测到的无线电设备有关的数据的表。

[0014] 图5图示了根据一方面的用于实现工具侦听器的某些功能的计算设备。

具体实施方式

[0015] 本发明的方面涉及使用工具侦听设备来检测诸如智能计量表之类的无线设备。工具侦听设备或工具侦听器被配置成:侦听在无线网络(诸如,网状网络)上操作或尝试操作的设备。工具侦听器不需要加入网状网络来检测网络通信,并且也不需要使用具有与该网络相同的配置的参数。例如,工具侦听器可以使用与网状网络的信道跳跃序列不同的发现信道跳跃序列,并且可以进行侦听达预定时间量,该预定时间量与网状网络的时隙不同。

[0016] 网状网络(诸如,电气和电子工程师协会(IEEE)802.15.4网络)是作为典型地短距离、低比特率和自标识网络的无线个人区域网络。高级计量基础设施(AMI)或智能计量表可以使用网状网络来传送资源消耗或诊断信息。一旦连接到网络,网状网络上的设备就在指定时隙内并且根据特定的信道跳跃序列进行操作。

[0017] 信道跳跃序列包括有效信道、信道间隔、比特率和调制指数的列表。特定网络的信道跳跃序列可以是操作的地区或国家的可用信道的子集。例如,如果监管主体允许信道1-10用于操作,则特定网络以及因此被配置成在该网络上操作的无线电设备可能会使用包括信道1、5和8的信道跳跃序列。此外,网状网络上的设备利用各种通信特征,诸如同步(或sync)字、信标请求、以及不同的帧类型,诸如数据帧、信标帧、确认帧和媒体访问控制(MAC)命令帧。网状设备在它们通电或复位时可能会或可能不会发射信号,诸如出生啁啾信号(birth chirp)。

[0018] 工具侦听器可以在一组无线电信道上侦听网络活动,在不存储整个分组的情况下检测网络活动,将检测到的活动保存在数据结构中,并且将该数据提供给外部设备,诸如计算机或平板电脑。外部设备可以将该数据可视化。可视化的示例包括以表、图形、图表或作为原始文本来显示该数据。工具侦听器可以检测特定设备的存在,或者可以执行未知设备的清单(inventory)。未知设备可以包括加入网状网络或未加入网状网络的无线设备,例如正在尝试与网状网络通信的无线设备。

[0019] 引入以下非限制性示例用于说明性目的。在第一示例中,工具侦听设备被部署在计量表维修设施中,以诊断有缺陷或需要重新配置的特定智能计量表。工具侦听器根据发现信道跳跃序列来选择初始信道,并且侦听通信达预定时间量。该预定时间量可以不同于网状网络上的时隙的长度。在接收到通信后,工具侦听器过滤出来自该特定智能计量表的通信(或来自该智能计量表的通信尝试),将这些通信存储在数据结构中,并且然后可选地

将该数据提供给外部设备。在一方面,工具侦听器可以使得该特定设备加入临时或诊断网络,以便接收重新编程命令。

[0020] 在第二示例中,工具侦听器被提供有发现信道跳跃配置,该发现信道跳跃配置包括由计量表的特定网络使用的信道跳跃序列的信道。工具侦听器从信道跳跃序列中选择在其上进行侦听的初始信道,并且进行侦听达特定时间量。如果工具侦听器检测到该信道上的活动,则工具侦听器尝试接收分组。分组包括前导码、同步字、报头和有效载荷。工具侦听器丢弃分组的有效负载并且分析报头。

[0021] 工具侦听器存储报头的内容,具体地是源地址、目的地址和帧类型,并且将该信息提供给工具侦听应用,工具侦听应用可以将该信息可视化。工具侦听器然后在发现信道跳跃序列中选择不同的信道,并且继续侦听。随时间的推移,工具侦听器收集到关于先前未知的设备和网络的信息,并且积聚(amass)一定范围内的设备的数量和类型的清单。附加地,通过查询外部数据库,工具侦听器可以确定是否有任何设备被移除或不再尝试加入网络。

[0022] 现在转到附图,图1图示了根据一方面的工具侦听器环境的示例。工具侦听器环境100包括工具侦听器系统101和未知无线电环境120。工具侦听器系统101包括工具侦听器102、工具侦听器计算设备110、工具侦听器应用112和数据链路105中的一个或多个。未知无线电环境120包括一个或多个未知无线电设备130a-n。未知无线电设备130a-n可以位于智能计量表或其他电网设备内。

[0023] 通过侦听不同信道上的业务,工具侦听器102可以确定无线环境中是否存在任何未知无线电设备130a-n。工具侦听器102可以在无线网络上操作,该无线网络诸如网状网络、IEEE 802.15.4网络、WiFi网络、蓝牙网络或其他无线网络。

[0024] 在一示例中,工具侦听器102在特定信道上进行侦听达预定时间量,以检测任何未知无线电设备130a-n的存在。未知无线电设备130a-n可以在可能特定于特定网络的信道跳跃序列内操作。工具侦听器102可以与工具侦听器计算设备110和工具侦听器应用112相结合地操作,以检测一个或多个未知无线电设备130a-n的存在。例如,工具侦听器102可以跨数据链路105向工具侦听器计算设备110传输通过侦听获得的数据(诸如,分组、报头、源地址或目的地址、或帧类型),以用于进一步分析和可视化。

[0025] 数据链路105可以是通用串行总线(USB)连接、蓝牙连接、以太网连接、无线连接、串行或并行连接、或任何合适的数据链路。工具侦听器计算设备110可以是膝上型、台式、平板计算机、移动电话或任何其他计算设备。工具侦听器应用112在工具侦听器计算设备110上执行,并且可以执行本文中描述的一些或所有功能。

[0026] 图2图示了根据一方面的工具侦听器系统的实现方式。图2描绘了工具侦听器系统200,工具侦听器系统200包括工具侦听器201和工具侦听器计算设备110。工具侦听器201是工具侦听器102的实现方式的示例。工具侦听器201包括无线电设备220、处理器230、天线240和数据收发器250中的一个或多个。

[0027] 无线电设备220是被配置成根据特定协议(诸如,IEEE802.15.4)操作的无线电接收器、或发射器/接收器组合。无线电设备220连接到天线240。天线240可以是任何种类的天线。合适天线的示例包括定向天线或全向天线。定向天线允许工具侦听器201从智能计量表被预期将位于其中的特定区域收集更强的信号。如果未知设备的大致位置未知,则全向天线可能是有用的。无线电设备220可以从处理器230接收命令,诸如何时进行侦听、移动到不

同的信道、通电或断电,并且可以将接收到的分组数据发送回处理器230。

[0028] 处理器230可以是任何合适的微控制器、微处理器、信号处理器或嵌入式处理器,诸如基于Intel®的处理器、基于ARM®的处理器等。处理器230可以执行固件或软件,这些固件或软件执行本文中描述的功能,诸如处理分组以及向无线电设备220发出命令。数据收发器250是通信设备,该通信设备可以通过数据链路105向工具侦听器计算设备110发送数据和命令,并且通过数据链路105从工具侦听器计算设备110接收数据和命令。

[0029] 处理器230执行与无线网络的诊断有关的各种功能。例如,处理器230可以访问特定的发现信道跳跃序列,将无线电设备220配置成在特定信道处操作达特定时间量,从无线电设备220接收数据或者从无线电设备220发送数据。

[0030] 图3是图示了根据一方面的由工具侦听设备用于检测另一个设备的存在的过程的流程图。过程300可以由工具侦听器102、工具侦听器201或另一个设备来实现。过程300可用于检测一个或多个未知无线电设备(诸如,智能计量表)的存在。

[0031] 在框301处,过程300涉及:在从发现信道跳跃序列中选择的无线电信道上进行侦听。网状网络上的智能计量表与议定的(agreed-upon)时隙同步,并且根据信道跳跃序列进行操作。网状网络设备所使用的信道跳跃序列包括有效信道、信道间隔、比特率和调制指数的列表。相比之下,工具侦听器102所使用的发现信道序列可以是与由该射频设备使用的信道跳跃序列所使用的序列不同的序列,并且可以包括由该射频设备的信道跳跃序列使用的无线电信道。

[0032] 此外,工具侦听器102与来自未知无线电设备130a-n和任何其他网状网络的广播异步地操作。工具侦听器102不需要与网状网络同步或加入网状网络。相反,工具侦听器102保持在信道上达预定时间量,除非检测到分组。该预定时间量不需要等于网络时隙的时间量,并且可以通过配置该工具侦听器来调整。

[0033] 在一示例中,处理器230访问特定发现信道跳跃序列。处理器230使得无线电设备220在该序列中的第一信道处操作。进而,无线电设备220在第一信道处操作,并且经由天线240来侦听无线电传输。如果在预定持续时间期间没有检测到前导码,则处理器230控制被传递到框306。替代地,如果检测到前导码,则控制被传递到框302。

[0034] 在框302处,过程300涉及继续侦听,直到接收到报头。分组可以包括前导码、同步字、分组报头和有效载荷。工具侦听器102侦听来自所选信道上的未知无线电设备130a-n之一的分组的前导码、同步字和报头。报头由无线电设备220来接收,并且被发送到处理器230。

[0035] 处理器230可以丢弃通常不需要的有效载荷信息,以节省存储器空间。即使工具侦听器102可以不被配置成分析分组的有效载荷,但是工具侦听器102也可以接收并检验整个分组,以便针对错误进行检查。处理器230可以使得无线电设备220:即使预定持续时间已经过去也继续侦听,直到接收到分组并且可以针对错误来检查该分组。

[0036] 在框303处,过程300涉及从报头中提取源地址、目的地址和帧类型。更具体地,处理器230提取分组报头,并且提取源地址、目的地址和帧类型。如果存在IEEE802.15.4个人区域网络(PAN)ID,还可以捕获网络ID。如果IEEE802.15.4报头信息元素(IE)包含网络ID,也可以捕获网络ID。网络ID用于在不同公用事业所运营的网络之间进行区分,例如当公用事业网络相邻时。

[0037] 在框304处,过程300涉及将源地址、目的地址、帧类型、以及可选的PANID和网络ID添加到数据结构。工具侦听器102将所捕获的信息添加到数据结构。

[0038] 在一方面,处理器230可以针对特定未知无线电设备130a-n随时间的推移在数据结构中聚集如下标识符或标志:该标识符或标志指示帧类型是确认、数据、信标还是MAC命令等。数据结构可以被本地存储,即存储在连接到处理器230的存储器中,或者存储在工具侦听计算设备110上。

[0039] 处理器230可以使用错误检测来针对接收到的分组中的错误进行检查。如果检测到无法恢复的错误,则处理器230可以丢弃有错误的分组,或者使得数据收发器250向工具侦听器计算设备110发送具有任何其余有用信息的消息。

[0040] 在一方面,工具侦听器接收计量表的特定网络地址(例如,LAN标识符)或特定媒体访问控制(MAC)地址,并且过滤掉或忽略其他通信。例如,在指定网络地址的情况下,处理器230对照与该特定设备相对应的网络地址来检查分组报头中的源地址。如果网络地址不匹配,则丢弃整个分组。以这种方式,工具侦听器可以聚焦于感兴趣的特定网络或设备,诸如来自维修店中的特定有缺陷的计量表的通信,并且忽略可能在维修店中的其他计量表。

[0041] 在另一方面,工具侦听器102可以从全球定位系统(GPS)或其他定位设备获取位置信号。工具侦听器102可以访问预期在该位置处的智能设备的数据库,并且对照来自该数据库的预期设备来验证检测到的网络地址,以确定新的或有错误的设备的存在。

[0042] 在框305处,过程300涉及将数据结构传输到外部设备,从而使得外部设备将数据结构可视化。处理器230将数据结构发送到数据收发器250,并且使得数据收发器250跨数据链路105将该信息发送到工具侦听器计算设备110。工具侦听器102可以在本地维护数据结构,并且周期性地将数据结构传输到工具侦听器计算设备110,工具侦听器计算设备110可以执行进一步的可视化和分析。可选地,工具侦听器计算设备110周期性地向无线电设备查询该信息表,并且相应地更新可视化。在一方面,工具侦听器计算设备110可以针对特定未知无线电设备130a-n随时间的推移来聚集、显示或可视化如下数据:该数据指示帧类型是确认、数据、信标还是MAC命令等。

[0043] 工具侦听器计算设备110可以实时显示数据。随时间的推移,工具侦听器102可以捕获从特定未知无线电设备130a-n接收到的多个分组。以这种方式,工具侦听器102随时间的推移向该表中添加新的数据和帧类型,以构建来自相邻无线电设备的业务的聚集图像。为了将大量分组可视化,可以按MAC地址和/或网络ID对数据进行索引。图4中示出了示例表,该示例表示出了由工具侦听计算设备110呈现的数据的示例。

[0044] 在框306处,过程300涉及从发现信道跳跃序列中选择下一个无线电信道。过程300使用下一个信道在框301处继续。如果在预定时间量期间没有检测到网络活动,则处理器230循环通过发现信道跳跃序列,从而保持在每个信道上达预定时间量。处理器230不需要以信道跳跃序列所定义的相同次序循环通过发现信道跳跃序列的信道;不同的信道次序是可能的。

[0045] 图4是图示了根据一方面的与工具侦听设备检测到的无线电设备有关的数据的表。图4描绘了表400。表400可以由工具侦听器系统101、工具侦听器系统200、或者由执行过程300或类似过程的另一个合适的系统或设备来填充。

[0046] 表400包括条目401a-n。每个条目可以对应于从无线网络检测到的分组。例如,每

个条目401a-n包括LAN地址(特定设备的地址)、PAN ID(或网络地址)、ACK(确认)、MAC命令、数据和信标。

[0047] “ACK”字段指代该分组是否是确认分组。“数据”字段指代该分组是否包括数据字段。分组中的“信标”字段指示该分组包含信标请求。“MAC命令”信标请求分组可以指示特定无线电设备没有成功建立与网络的连接,并且正在尝试通信。其他字段是可能的。技术人员可以使用从工具侦听器收集的信息来确定无线电设备未被正确配置或有缺陷。

[0048] 如所描绘的,条目401a包括LAN地址ab:cd:ef:01:02:03、PAN ID 10:01、ACK 0、数据1、信标0、MAC命令1。条目401b包括LAN地址ab:cd:ef:10:20:30、PAN ID 10:01、ACK 0、数据0、信标1和MAC命令0。条目401c包括LAN地址ac:99:88:77:11:22、PAN ID 20:21、ACK 1、数据0、信标0和MAC命令1。条目401d包括LAN地址ac:99:88:66:22:33、PAN ID 20:11、ACK 0、数据0、信标0和MAC命令1。

[0049] 如可以看出的,条目401a和401b具有相同的PAN ID,并且可能在相同网络上通信。在一方面,源自于或去往相同地址的条目可以被聚集以实现更容易的查看。

[0050] 示例性计算环境

[0051] 图5图示了根据一方面的用于实现工具侦听器的某些功能的计算环境500。任何合适的计算系统或设备都可以用于执行本文中描述的操作,诸如实现工具侦听器102、工具侦听器外部计算设备110或过程300的功能。所描绘的计算设备501包括通信地耦合到一个或多个存储器设备504的处理器502。处理器502执行存储在存储器设备504中的计算机可执行程序代码530,访问存储在存储器设备504中的数据520,或者其两者。处理器502的示例包括微处理器、专用集成电路(“ASIC”)、现场可编程门阵列(“FPGA”)、或任何其他合适的处理设备。处理器502可以包括任何数量的处理设备或核,包括单个处理设备。计算设备的功能可以用硬件、软件、固件或其组合来实现。

[0052] 存储器设备504包括用于存储数据、程序代码或其两者的任何合适的非暂时性计算机可读介质。计算机可读介质可以包括能够向处理器提供计算机可读指令或其他程序代码的任何电子、光学、磁性或其他存储设备。计算机可读介质的非限制性示例包括闪速存储器、ROM、RAM、ASIC、或处理设备可以从中读取指令的任何其他介质。指令可以包括由编译器或解译器从代码所生成的处理器特定的指令,该代码是以任何合适的计算机编程语言(包括例如,C、C++、C#、Visual Basic、Java或脚本语言)编写的。

[0053] 计算设备501还可以包括多个外部或内部设备,诸如输入或输出设备。例如,计算设备501被示出具有一个或多个输入/输出(“I/O”)接口508。输入/输出接口508可以从输入设备接收输入,或者向输出设备提供输出。计算设备501中还包括一个或多个总线506。总线506通信地耦合了计算设备501中的相应计算设备的一个或多个组件。

[0054] 计算设备501执行程序代码530,该程序代码530将处理器502配置成执行本文中描述的一个或多个操作。例如,程序代码530使得处理器执行图3中描述的操作。

[0055] 计算设备501还包括网络接口设备510。网络接口设备510包括适合于建立去往一个或多个数据网络的有线或无线数据连接的任何设备或设备组。网络接口设备510可以是无线设备并且具有天线514。计算设备501可以使用网络接口设备510经由数据网络与实现该计算设备或其他功能的一个或多个其他计算设备进行通信。

[0056] 计算设备501还可以包括显示设备512。显示设备512可以是LCD、LED、触摸屏、或可

操作以显示关于计算设备501的信息的其他设备。例如,信息可以包括计算设备的操作状态、网络状态等。

[0057] 虽然本主题已经关于其特定方面而被详细描述,但是应当领会的是,本领域技术人员在获得对前述内容的理解后,可以容易地得出对这种方面的更改、这些方面的变化和等同物。因此,应当理解的是,本公开是出于示例而非限制的目的而呈现的,并且不排除包括对本领域普通技术人员来说将显而易见的对本主题的这种修改、变化和/或添加。

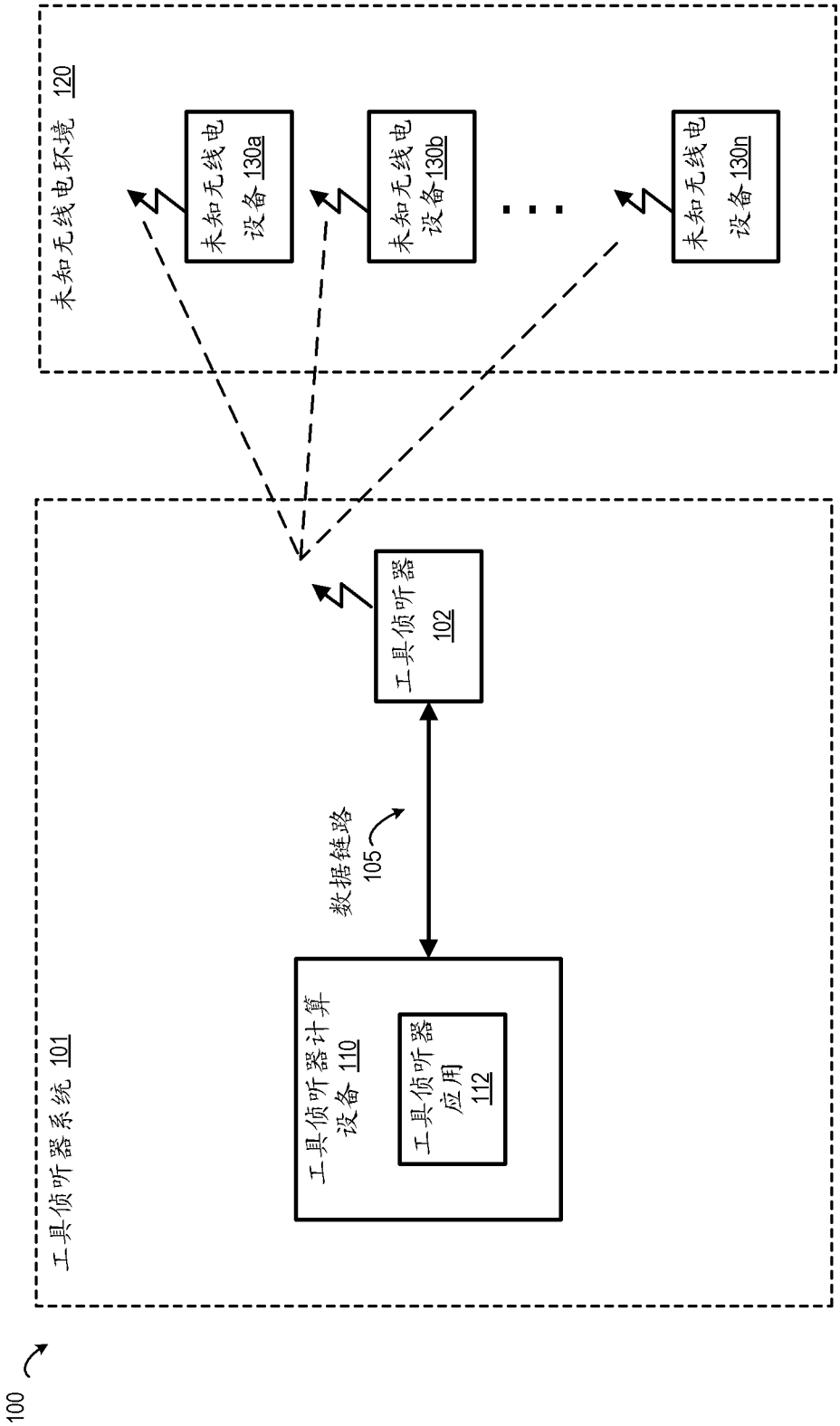

未知无线电环境 120
未知无线电设备 130a
未知无线电设备130b
未知无线电设备 130n
工具侦听器 102
数据链路 105
工具侦听器计算设备 110
工具侦听器应用 112
工具侦听器系统 101
100

图 1

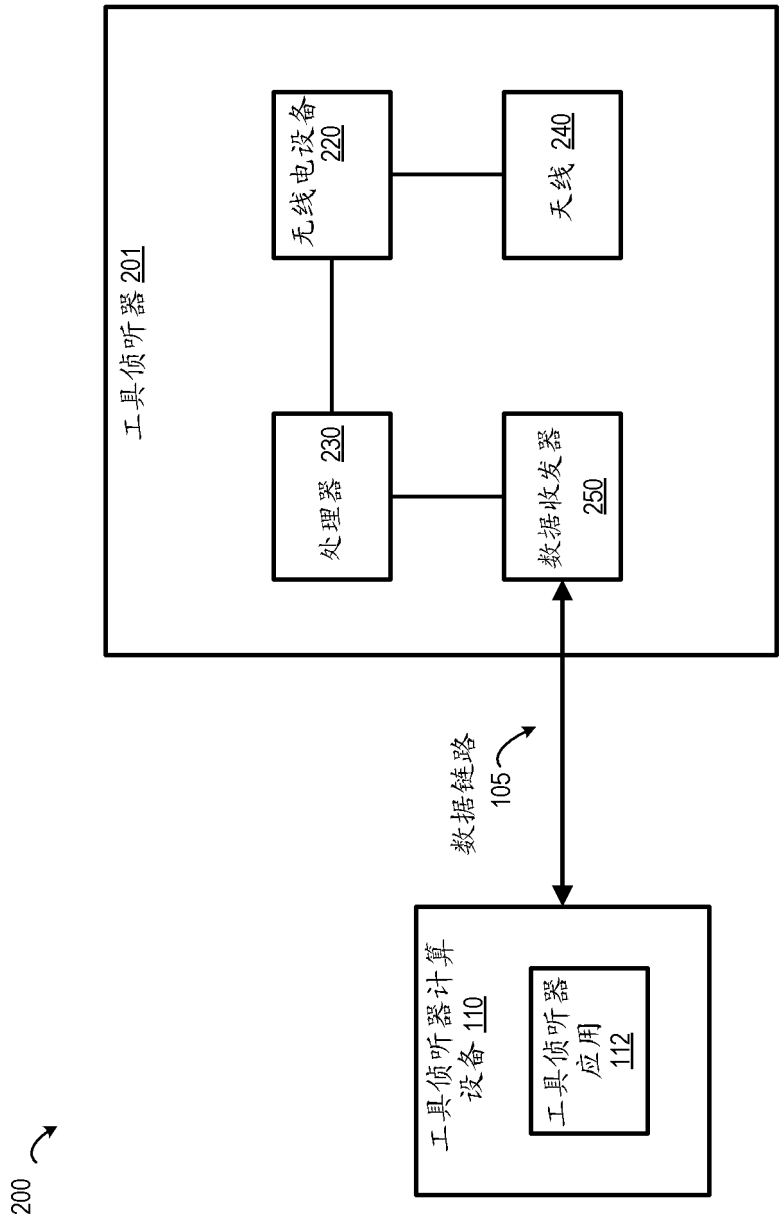

工具侦听器 201
无线电设备 220
天线 240
处理器 230
数据收发器 250
数据链路 105
工具侦听器计算设备 110
工具侦听器应用 112
200

图 2

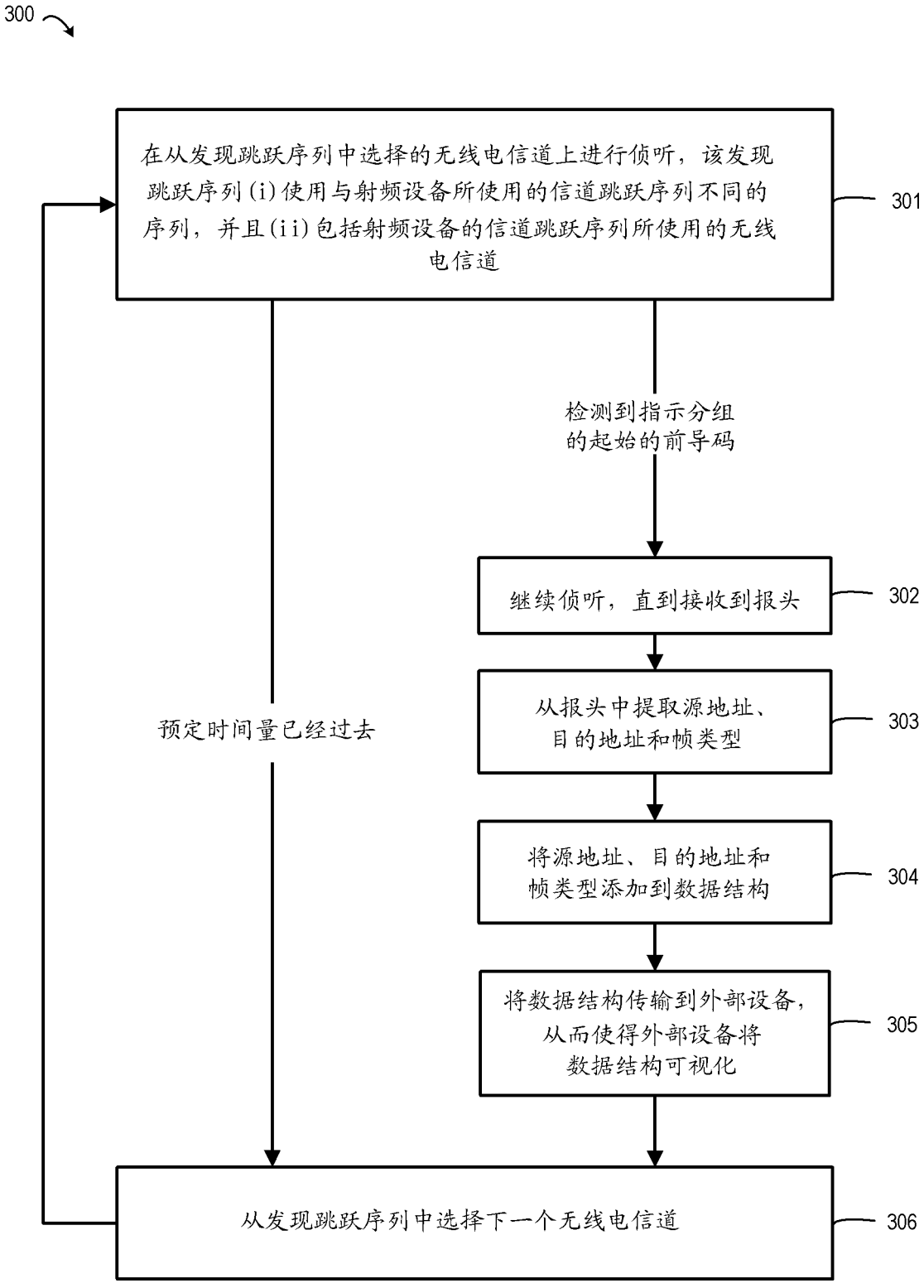

300
在从发现跳跃序列中选择的无线电信道上进行侦听，该发现跳跃序列(i)使用与射频设备所使用的信道跳跃序列不同的序列，并且(ii)包括射频设备的信道跳跃序列所使用的无线电信道
301
检测到指示分组的起始的前导码
预定时间量已经过去
继续侦听，直到接收到报头
302
从报头中提取源地址、目的地址和帧类型
303
将源地址、目的地址和帧类型添加到数据结构
304
将数据结构传输到外部设备，从而使得外部设备将数据结构可视化
305
从发现跳跃序列中选择下一个无线电信道
306

图 3

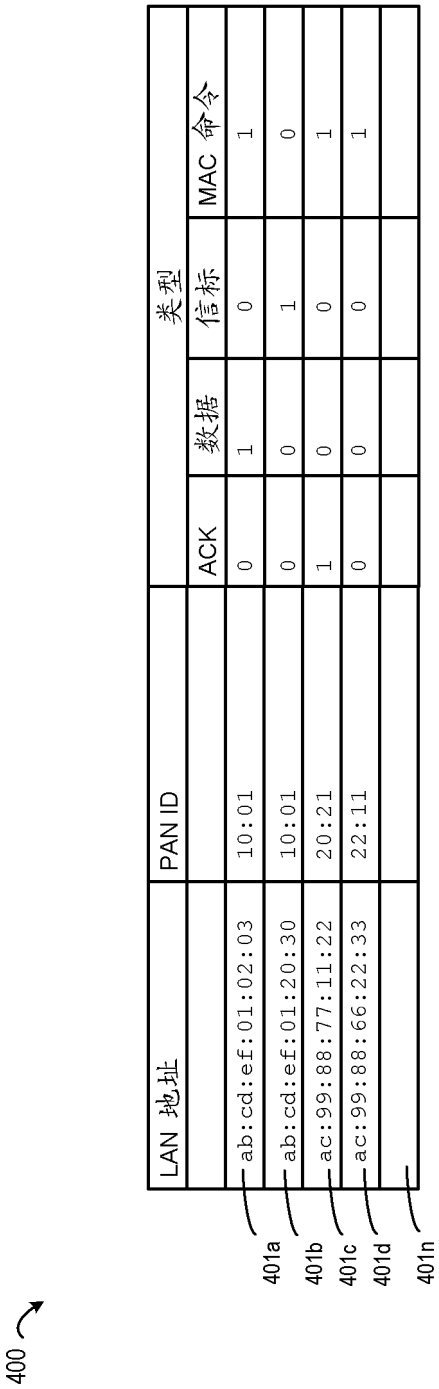

LAN 地址
PAN ID
类型
ACK
数据
信标
MAC 命令
ab:cd:ef:01:02:03
10:01
0
1
0
1
ab:cd:ef:01:20:30
10:01
0
0
1
0
ac:99:88:77:11:22
20:21
1
0
0
1
ac:99:88:66:22:33
22:11
0
0
0
1
401a
401b
401c
401d
401n
400

图 4

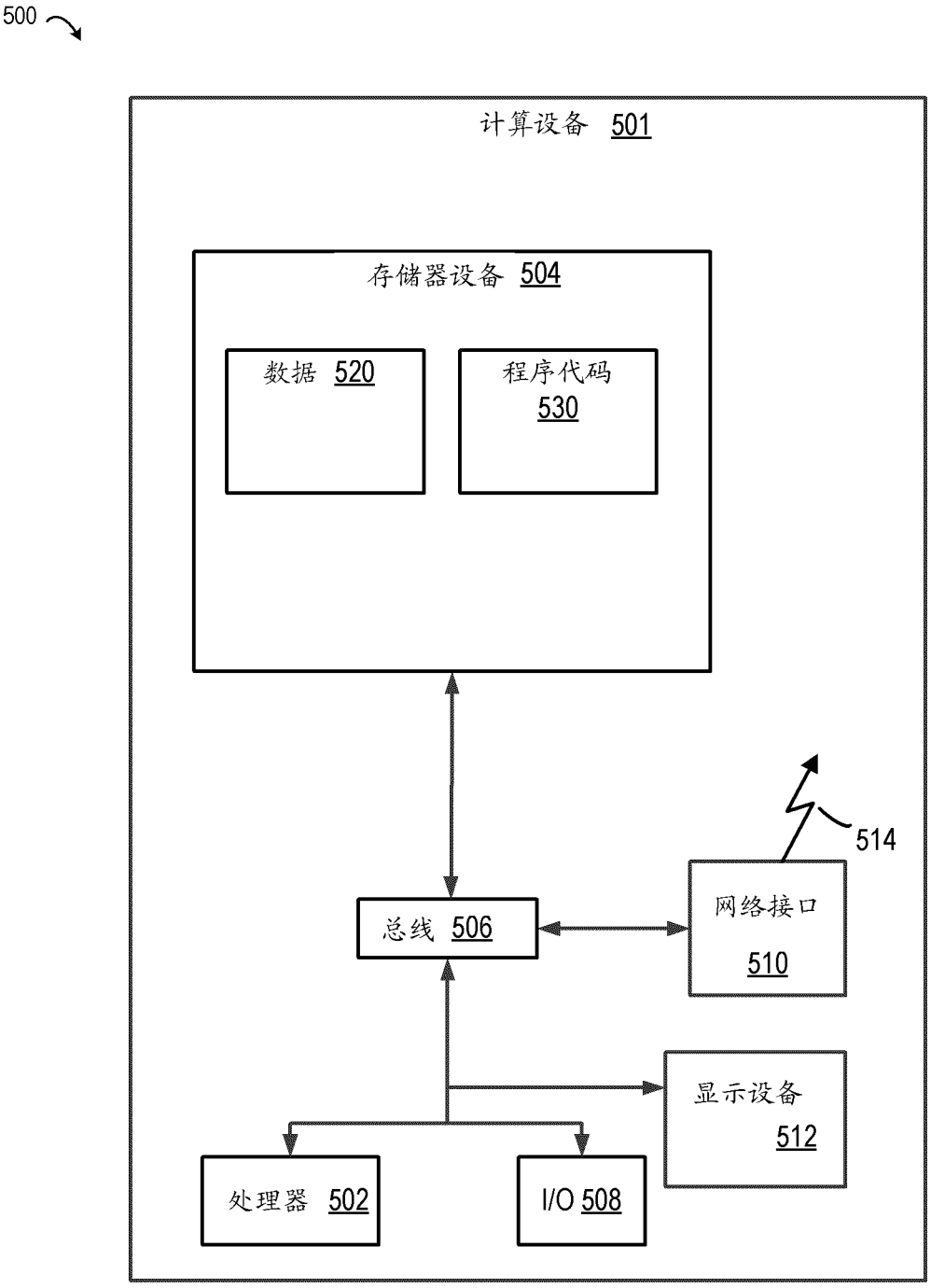

500
计算设备 501
存储器设备 504
数据 520
程序代码 530
514
网络接口 510
总线 506
显示设备 512
处理器 502
I/O 508

图 5