Certificate No.: 1712095

Patent Certificate for Invention

Title of the Invention: WIRELESS DEVICE MONITORING SYSTEMS AND MONITORING DEVICES, AND ASSOCIATED METHODS

Inventor(s): McCOWN, Steven, H./DERR, Kurt, W./ROHDE, Kenneth, W.

Patent No.: ZL 200980115611.8

Filing Date: February 26, 2009

Patentee: BATTELLE ENERGY ALLIANCE, LLC

The date of the announcement: July 1, 2015

The invention application has passed through the examination and has been issued the certificate by the State Intellectual Property Office. The invention patent is already recorded in the Patent Register. The patent right takes effect from the announcement date.

The duration of the patent right shall be twenty years counting from the filing date. The patentee shall pay annuity according to the Chinese Patent Law and its Implementing Regulations. The annuity of the above-mentioned patent should be paid within one month before **February 26** for each year. Otherwise, the patent right would be terminated from the expiration date of the last payment.

The certificate for patent right records the legal status while the patent is registered. Any information/legal action in relation with assignment, mortgage, invalidation, termination and comeback for the patent right and the change in the name, nationality or address of the patentee, occurred after the registration, will be recorded in the Patent Register.

The State Intellectual Property Office of
the People's Republic of China

Commission er: Changyu SHEN

July 1, 2015

证书号第1712095号

北京市海淀区地方税务局 印花税 代扣专用章 国家知识产权局

发明专利证书

发明名称：无线设备监测系统和监测设备以及关联的方法

发 明 人：斯蒂文·H·麦考恩;库尔特·W·德尔;肯尼思·W·罗德

专 利 号：ZL 2009 8 0115611.8

专利申请日：2009年02月26日

专利权人：巴特尔能源联合有限责任公司

授权公告日：2015年07月01日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年02月26日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

中华人民共和国国家知识产权局 2015年07月01日

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102016938 B
(45)授权公告日 2015.07.01

(21)申请号 200980115611.8

(22)申请日 2009.02.26

(30)优先权数据
12/188,284 2008.08.08 US

(85)PCT国际申请进入国家阶段日
2010.11.01

(86)PCT国际申请的申请数据
PCT/US2009/035205 2009.02.26

(87)PCT国际申请的公布数据
WO2010/016953 EN 2010.02.11

(73)专利权人 巴特尔能源联合有限责任公司
地址 美国爱达荷州

(72)发明人 斯蒂文·H·麦考恩
库尔特·W·德尔 肯尼思·W·罗德

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 徐金国 钟强

(51)Int.Cl.
G08B 1/08(2006.01)

(56)对比文件
US 2004/0166878 A1,2004.08.26,说明书第0006,0023-0024,0058-0059,0077段、附图1.
CN 1602611 A,2005.03.30,全文.
CN 1630994 A,2005.06.22,全文.
WO 2007/022811 A1,2007.03.01,全文.

审查员 刘豫川

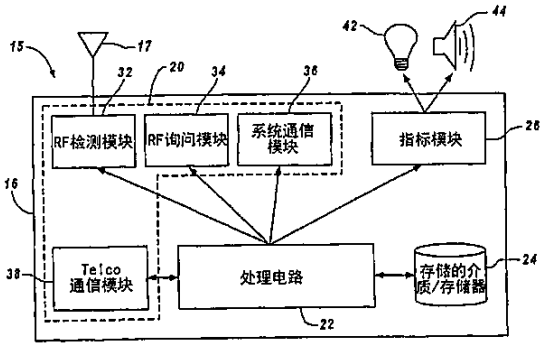
权利要求书4页 说明书13页 附图5页

(54)发明名称

无线设备监测系统和监测设备以及关联的方法

(57)摘要

无线设备监测系统和监测设备包括用于接收无线设备的无线通信的通信模块。处理电路与通信模块耦接并且经配置以处理无线通信，以基于所述无线设备的识别信息来确定授权或未授权所述无线设备在受监测区域中出现。还提供了用于监测无线设备的出现和身份的方法。



CN 102016938 B

1. 一种用于在指定区域中检测无线设备的出现和身份的监测设备，所述监测设备经配置以监测所述指定区域的入口和出口的多个点，所述监测设备包含：

通信模块，其经配置以当无线设备在接近所述监测设备的无线通信内时检测在指定和受监测区域内的所述无线设备的出现，响应在所述指定和受监测区域中检测所述无线设备的出现而向所述无线设备发送第一无线通信，所述第一无线通信包括对所述无线设备的认证数据的请求，和响应所述无线设备接收所述第一无线通信而从所述无线设备接收第二无线通信，所述第二无线通信包括所述监测设备使用的设备识别符以用以确定所述无线设备是经授权或未授权；

处理电路，其与所述通信模块耦接并且经配置以处理所述第二无线通信以确定授权或未授权所述无线设备在所述受监测区域中出现；和

指示电路，其经配置以在所述无线设备未经授权出现在所述受监测区域时，产生与所述无线设备的出现相关的指示，所述指示为无声警报、可视警报和声响警报中的至少一种；

其中所述通信模块经配置以向电信提供商转发所述无线通信；

其中如果向所述电信提供商转发的所述无线通信是加密的，那么所述通信模块经配置以从所述电信提供商接收包含所述无线通信中呈未加密格式的至少一部分的通信。

2. 根据权利要求 1 所述的监测设备，进一步包含存储介质，所述存储介质经配置以存储信息，并且其中所述处理电路经配置以使用所述存储的信息来确定授权或未授权所述无线设备在所述受监测区域中出现。

3. 根据权利要求 2 所述的监测设备，其中所述存储的信息包含一个或多个经授权无线设备的识别信息和认证数据中的至少一个。

4. 根据权利要求 1 所述的监测设备，其中所述通信模块经配置以向所述无线设备输出通信并且从所述无线设备接收响应的无线通信，并且其中所述处理电路经配置以使用所述响应的无线通信来确定所述无线设备为经授权或未经授权。

5. 根据权利要求 1 所述的监测设备，其中所述通信模块经配置以向至少一个其他监测设备传达所述无线通信，所述至少一个其他监测设备经配置以确定所述无线设备为经授权或未经授权。

6. 根据权利要求 1 所述的监测设备，其中所述通信模块经配置以从至少一个其他监测设备接收所述无线通信。

7. 根据权利要求 1 所述的监测设备，其中所述通信模块经配置以向外部设备转发所述无线通信，以确定所述无线设备为经授权或未经授权。

8. 一种无线设备监测系统，包含：

至少一个用于在指定区域中检测无线设备的出现和身份的监测设备，所述监测设备经配置以监测所述指定区域的入口和出口的多个点，所述监测设备包含：

通信模块，其经配置以当无线设备在接近所述监测设备的无线通信内时检测位于指定和受监测区域内的所述无线设备的出现，响应在所述指定和受监测区域中检测所述无线设备的出现而向所述无线设备发送第一无线通信，所述第一无线通信包括对所述无线设备的认证数据的请求，和响应所述无线设备接收所述第一无线通信而从所述无线设备接收第二无线通信，所述第二无线通信包括所述监测设备使用的设备识别符以用以确定所述无线设

备是经授权或未授权；

处理电路，其与所述通信模块耦接并且经配置以处理所述第二无线通信以确定授权或未授权所述无线设备在所述受监测区域中出现；和

指示电路，其经配置以在所述无线设备未经授权出现在所述受监测区域时，产生与所述无线设备的出现相关的指示，所述指示为无声警报、可视警报和声响警报中的至少一种；

其中所述通信模块经配置以向电信提供商转发所述无线通信；

其中如果向所述电信提供商转发的所述无线通信是加密的，那么所述通信模块经配置以从所述电信提供商接收包含所述无线通信中呈未加密格式的至少一部分的通信。

9. 根据权利要求 8 所述的系统，其中所述通信模块经配置以直接从所述无线设备接收所述无线通信。

10. 根据权利要求 8 所述的系统，其中所述通信模块经配置以从至少一个其他监测设备接收所述无线设备的所述无线通信。

11. 根据权利要求 10 所述的系统，其中所述至少一个其他监测设备包含至少另一个通信模块，所述至少另一个通信模块经配置以：

检测所述无线设备的所述无线通信；

向所述无线设备输出通信并且响应所述输出通信从所述无线设备接收无线通信；和

向在所述无线设备监测系统内的至少另一个监测设备传达所述无线通信。

12. 根据权利要求 10 所述的系统，其中所述至少一个其他监测设备包含经配置以向电信提供商转发所述无线通信的另一个通信模块。

13. 根据权利要求 8 所述的系统，其中所述至少一个监测设备的所述通信模块经配置以向电信提供商转发所述无线通信。

14. 根据权利要求 8 所述的系统，进一步包含经配置以存储信息的至少一个存储介质，并且其中所述处理电路经配置以使用所述存储的信息来确定授权或未授权所述无线设备在所述受监测区域中出现。

15. 根据权利要求 14 所述的系统，其中所述存储的信息包含与至少一个经授权无线设备相关的识别信息和认证数据中的至少一个。

16. 一种用于监测无线设备的出现的方法，包含：

当无线设备在接近监测设备的无线通信内时检测在指定和受监测区域内的无线设备的出现；

响应在所述受监测区域中检测所述无线设备的出现而向所述无线设备发送第一无线通信，所述第一无线通信包括对所述无线设备的认证数据的请求，和

响应所述无线设备接收所述第一无线通信而从所述无线设备接收第二无线通信，所述第二无线通信包括所述无线设备使用的设备识别符以用以确定所述监测设备是经授权或未授权；

获得与所述无线设备相关的识别信息；

响应所述获得的识别信息来确定授权或未授权所述无线设备在所述受监测区域中出现，和

在所述无线设备未经授权出现在所述受监测区域时，产生与所述无线设备的出现相关

的指示，所述指示为无声警报、可视警报和声响警报中的至少一种；

其中获得与所述无线设备相关的识别信息包含：

从所述无线设备接收至少一个无法破译的通信；

向电信提供商转发所述至少一个无法破译的通信；和

从所述电信提供商接收与所述无线设备相关的识别信息。

17. 根据权利要求 16 所述的方法，其中检测所述无线设备包含扫描所述无线设备的使用频率。

18. 根据权利要求 16 所述的方法，其中获得与所述无线设备相关的识别信息包含：

产生去往所述无线设备的通信以请求所述识别信息；和

从所述无线设备接收至少一个响应的通信。

19. 根据权利要求 18 所述的方法，进一步包含：在所述无线设备提供所述至少一个响应的通信失败之后，确定所述无线设备为未经授权的。

20. 根据权利要求 16 所述的方法，其中获得与所述无线设备相关的识别信息包含获得与以下至少一个相关的信息：唯一的设备标识符、所述无线设备是否在公司 PED 服务器中登记的指示符以及用于所述无线设备的所述公司 PED 服务器的识别。

21. 根据权利要求 16 所述的方法，其中确定所述无线设备为经授权或未经授权包含将来自所述无线设备的所述获得的识别信息与所存储的信息进行比较。

22. 根据权利要求 16 所述的方法，其中确定所述无线设备为经授权或未经授权包含：

向外部设备传达所述识别信息中至少一些；和

将所述识别信息中所述至少一些与可由所述外部设备访问的存储的信息进行比较。

23. 根据权利要求 16 所述的方法，进一步包含指示所述无线设备为经授权或未经授权。

24. 根据权利要求 16 所述的方法，进一步包含：

获得涉及所述无线设备的设备认证数据；

将所述获得的设备认证数据与存储的认证数据中的至少一项进行比较；和

响应所述将所述获得的设备认证数据与存储的认证数据中的至少一项进行比较，确定所述设备为经授权或未经授权。

25. 一种用于检测无线设备的出现的方法，所述方法包含：

询问位于受监测区域中的无线设备；

响应所述询问所述无线设备，从所述无线设备接收至少一个应答，其中来自所述无线设备的所述至少一个应答包括监测设备使用的设备识别符以用以确定所述无线设备是经授权或未授权；

响应所述至少一个应答，确定授权或未授权所述无线设备在所述受监测区域中出现；

在所述无线设备未经授权出现在所述受监测区域时，产生与所述无线设备的出现相关的指示，所述指示为无声警报、可视警报和声响警报中的至少一种；和

向所述监测设备的用户而非所述无线设备的用户提供所述指示；

其中响应所述询问所述无线设备而从所述无线设备接收至少一个应答包含从所述无线设备接收至少一个无法破译的应答，并且进一步包含：

向电信提供商转发所述至少一个无法破译的应答；和

从所述电信提供商接收呈可破译格式的所述至少一个应答。

26. 根据权利要求 25 所述的方法，其中询问无线设备包含请求所述无线设备的识别信息和所述无线设备的认证数据中的至少一个。

27. 根据权利要求 25 所述的方法，其中确定授权或未授权所述无线设备在所述受监测区域中出现包含将所述至少一个接收的应答与存储的信息进行比较。

28. 根据权利要求 25 所述的方法，其中确定所述无线设备为经授权或未经授权包含：

向外部设备传达来自所述无线设备的所述至少一个接收的应答的至少一部分；和

将来自所述无线设备的所述至少一个接收的应答的所述至少一部分与可由所述外部设备访问的存储的信息进行比较。

29. 根据权利要求 25 所述的方法，进一步包含指示所述无线设备为经授权或未经授权。

无线设备监测系统和监测设备以及关联的方法

[0001] 相关申请

[0002] 本申请要求于 2008 年 8 月 8 日提交的标题为“无线设备监测系统和监测设备以及关联方法 (WIRELESS DEVICE MONITORING SYSTEMS ANDMONITORING DEVICES, AND ASSOCIATED METHODS)”的美国非临时专利申请 No. 12/188, 284 的权益和优先权，在此以引用方式将该申请全文并入本文。

[0003] 政府权利声明

[0004] 依据美国能源部与 Battelle Energy Alliance, LLC（巴特尔能源联合有限公司）之间的合约 No. DE-AC07-05ID14517，美国政府享有本发明的某些权利。

技术领域

[0005] 本发明涉及监测设备和方法。更具体来说，本发明的实施例涉及用于检测无线通信设备的出现和身份的监测设备和系统，以及涉及关联的方法。

背景技术

[0006] 诸如蜂窝电话、黑莓 (Blackberries)、双向 (two-way) 寻呼机、无线耳机、键盘等的无线设备和个人电子设备 (PEDs) 已成为当今生活方式的组成部分。在语音通信、电子邮件、即时消息传递、电子日历等已变成进行商业运作的标准方式的商业世界中，尤其如此。

[0007] 虽然无线设备是现代商业和组织的重要工具，但此类无线设备也引入潜在的安全性威胁。例如，已经认识到，可以将无线设备用作跟踪设备（通过集成 GPS 芯片），用于拒绝服务 (DoS) 和其他攻击的暂存区域以及其中攻击者远程开启设备麦克风以进行窃听的“漫游虫 (roving bugs)”。因此，已经开始关注将无线设备用于间谍活动。例如，在公司环境中，当公司执行官或其他公司成员会晤讨论内部策略和运作时，他们希望进行讨论而不用担心他们的整个会晤无意中泄密给竞争公司。为了减轻由将无线设备引入私人会晤而产生的威胁，一种可能的反应措施是完全禁止此类无线设备进入会议室和公司或政府活动的其他敏感区域。在许多情况下，这种解决方案是不可接受的，因为会议参加人员即使处于会议中也经常需要保持可联络，如 Research in Motion（行动研究公司）的黑莓®设备以及其他类似设备的快速增长所证明。

发明内容

[0008] 本发明的各个实施例包含用于在指定区域或地点中检测无线设备的出现和身份与用于在检测到未经授权无线设备时提供警告或一些其他指示的监测设备。在一个或多个实施例中，监测设备可包含通信模块和耦接到该通信模块的处理电路。该通信模块可经配置以在受监测区域内接收无线设备的无线通信。处理电路可经配置以处理该无线设备的无线通信，以基于该无线设备的识别信息来确定授权或未授权该无线设备在受监测区域中出现。

[0009] 本发明的其他实施例包含用于在指定区域中监测无线设备的出现和身份的监测

系统。此类系统的一个或多个实施例可以包括至少一个监测设备，该至少一个监测设备包括通信模块和耦接到该通信模块的处理电路。

[0010] 其他的实施例包含用于监测无线设备进入指定区域或地点或在指定区域或地点内监测无线设备的方法。此类方法的一个或多个实施例可以包括在受监测区域内检测无线设备。可获得与该无线设备相关的识别信息。例如，可询问该无线设备，并且可响应询问而从无线设备接收至少一个应答。基于所获得的识别信息，可将该无线设备确定为经授权或未经授权在所选区域中出现。

附图说明

[0011] 图 1 是图示具有关联无线设备监测系统的一个或多个受监测区域的方框图。

[0012] 图 2 图示根据一个实施例的用于无线设备监测系统的监测设备的配置的方框图。

[0013] 图 3 图示根据节点设备的一个实施例来配置的监测设备的实例。

[0014] 图 4 图示根据管理设备的一个实施例来配置的监测设备的实例。

[0015] 图 5 是图示根据一个实施例的经配置以监测多个受监测区域的监测系统的布置的方框图。

[0016] 图 6 是图示根据一个实施例的验证操作和组件的程序框图。

[0017] 图 7 是图示根据一个实施例的将无线设备识别为经授权或未经授权的方法的程序框图。

[0018] 图 8 是图示根据一个实施例的将无线设备识别为经授权或未经授权的方法的程序框图。

具体实施方式

[0019] 在以下详细说明中，可以用方框图形式示出电路和功能，从而避免以不必要的细节来使本发明难以理解。另外，如所绘示的方框定义和各个方框之间逻辑的划分是非限制性的，并且仅包含具体实施例的实例。对所属领域的技术人员将容易显而易见的是，本发明可以实践为实施许多其他划分解决方案的各个实施例。

[0020] 另外，应注意的是，这些实施例可以按照绘示成流程图、程序框图、结构图或方框图的过程来描述。虽然流程图可以将操作动作描述为连续的过程，但可以按另一次序、并行地或大体上同时地执行这些动作中的许多动作。另外，动作的顺序可以重新排列。当过程的动作完成时，该过程终止。过程可以对应于方法、功能、程序、子例程、子程序等。此外，本文公开的方法可以实施成硬件、软件或两者。

[0021] 本发明的各个实施例是针对用于在指定区域或地点中检测无线设备的出现和身份与用于在检测到未经授权无线设备时提供警告或一些其他指示的无线设备监测系统的实施例。图 1 图示与一个或多个受监测区域 10 相关联的用于监测无线设备 14 的出现的无线设备监测系统 12 的一个实施例。受监测区域 10，也可称为安全区域，可以包含其中可能期望或重要的是获得与所有出现的无线设备 14 和其使用相关的信息的任何区域。举例而言（但并非限制），受监测区域 10 可以包括其中可能讨论和 / 或展示敏感材料的（例如，公司、政府实体或其他组织的）会议室、办公室或制造车间。进一步举例而言（但并非限制），无线设备 14 可以包括诸如蜂窝电话、寻呼机、具有无线通信能力的个人音乐播放器（例如，

iPODS ®）、智能电话（例如，黑莓®）、计算机、无线耳机、键盘之类的个人电子设备 (PEDs) 或包含或配置有无线通信能力的任何其他设备。

[0022] 在一些实施例中，可以邻近于受监测区域 10 的入口和出口的各自点来放置监测系统 12 的一个或多个监测设备（下文论述），以提供无线设备监测功能。在其他实施例中，具有扩展范围的单个监测设备可以经配置以监测入口和出口的多个点以及一个或多个各自的受监测区域 10 的其他的占地空间或区域。也可以使用其他实施例和 / 或应用。

[0023] 根据各自的不同应用和将要监测的受监测区域 10 的配置，可以在不同的配置中实施监测系统 12。例如，对于其中将要监测单个受监测区域 10 的应用，监测系统 12 可以包括经配置以提供关于单个受监测区域 10 的无线设备监测和分析功能的单个监测设备（例如，节点设备 16（图 3））。对于额外的应用（包括其中将要监测多个受监测区域 10 的应用），监测系统 12 可以包括与集中监测设备（例如，管理设备 30（图 4））通信的一个或多个监测设备。该集中监测设备可以提供对多个监测设备所提供的信息的分析。在另一个实施例中，集中监测设备可以与在监测系统 12 外部的（例如与另一个公司或其他组织相关联的外部设备）并且实施本发明的一个或多个分析方面的设备通信。下文描述这些实施例的细节，并且在本文所述的实例之外的其他实施例中可以不同地实施监测系统 12。

[0024] 图 2 图示根据一个实施例的用于监测系统 12 的监测设备 15 的配置。如图所示，监测设备 15 可以包括通信模块 20（也可称为通信电路）、处理电路 22、存储介质 24（也可称为存储电路）以及指示模块 26（也可称为指示电路）。预期在本发明的范围内的其他布置，包括更多、更少和 / 或替代性的组件。

[0025] 通信模块 20 经配置以实施监测设备 15 的无线通信和 / 或有线通信。例如，在一些实施例中，通信模块 20 可以经配置以与无线设备 14 以及监测系统 12 的其他设备双向地传达信息。通信模块 20 可以与天线 17 耦接，并且可以包括用于与无线设备 14 无线通信的无线收发器电路，并且还可包括如网络接口卡 (NIC)、串行或并行连接、USB 端口、火线接口、闪速存储器接口、软盘驱动器或者用于与公用网络（例如，互联网）和 / 或专用网络或其他有线布置通信的任何其他适当的布置。

[0026] 在一些实施例中，通信模块 20 可以经配置以检测无线设备 14 的无线通信，发送和 / 或接收在受监测区域 10 内的无线设备 14 的无线通信，发送和 / 或接收去往 / 来自监测系统 12 的一个或多个其他监测设备以及外部设备的通信，和 / 或与一个或多个电信提供商 60（图 6）通信。举例而言（但并非限制），通信模块 20 可以包括 RF 检测模块，该 RF 检测模块经配置用于检测来自在受监测区域 10 内的无线设备 14 的 RF 信号。通信模块 20 还可包括 RF 询问模块，该 RF 询问模块经配置以通过向无线设备 14 输出无线通信和从无线设备 14 接收响应的无线通信来与无线设备 14 通信。此外，系统通信模块 36 或节点设备通信模块 46 可以被包括在内并且经配置以与监测系统 12 的其他设备通信，并且外部设备通信模块 48 可以经配置以与外部设备 40（图 5）通信。最终，通信模块 20 可以包括用于与一个或多个电信提供商 60 通信的电信 (Telco) 通信模块 38。

[0027] 在一个实施例中，Telco 通信模块 38 可以经配置以实施与电信提供商 60 的通信。通信模块 20 可以经配置以使用任何适当的通信来与电信提供商 60 通信。例如，通信模块 20 可以使用电信提供商 60 的网络来与电信提供商 60 通信。在另一个实施例中，通信模块 20 可以经由包交换网络、陆线或其他适当的通信通道来与电信提供商 60 通信。在一个实施

例中，通信模块 20 可以作为毫微微单元来操作，以便从无线设备 14 接收无线通信信号并且使用经由互联网的宽带连接来将从无线设备 14 接收到的通信转发到电信提供商 60。

[0028] 在一个实施例中，处理电路 22 经布置以获得、处理和 / 或发送数据，控制数据访问和存储，发出命令，以及控制其他期望的操作。在至少一个实施例中，处理电路 22 可以包含经配置以实施由恰当介质提供的期望程序设计的电路。例如，可以将处理电路 22 实施为经配置以执行包括例如软件和 / 或固件指令的可执行指令和 / 或硬件电路的处理器、控制器、多个处理器和 / 或其他结构中的一个或多个。处理电路 22 的实施例包括设计用于执行本文所述功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其他可编程逻辑组件、分立门或晶体管逻辑、分立硬件组件或其任何组合。通用处理器可以是微处理器，或者，处理器可以是任何传统的处理器、控制器、微控制器或状态机。还可将处理器实施为计算组件的组合，例如，DSP 和微处理器的组合、若干微处理器、与 DSP 核心协作的一个或多个微处理器或任何其他的此类配置。处理电路 22 的这些实例是用于举例说明，并且本发明的范围内的其他适当配置也受到涵盖。

[0029] 存储介质 24 经配置以存储程序设计，诸如可执行代码或指令（例如，软件和 / 或固件）、电子数据、数据库或其他数字信息，并且可以包括处理器可用的介质。数据库的非限制性实例可以包括与在一个或多个受监测区域 10 中可能出现的多个无线设备 14 相关的信息。存储介质可以是可由通用计算机或专用计算机访问的任何可用介质。举例而言（但并非限制），存储介质可以包含用于存储数据的一个或多个设备，包括只读存储器 (ROM)、随机访问存储器 (RAM)、磁盘存储介质、光存储介质、闪速存储设备和 / 或用于存储信息的其他计算机可读介质。

[0030] 处理器可用介质可以实施为任何计算机程序产品或制品，在示范性的实施例中，其可包含、存储或维持由包括处理电路的指令执行系统使用或与其有关的程序设计、数据和 / 或数字信息。例如，适当的处理器可用介质可以包括任何一种物理介质，诸如电子介质、磁性介质、光学介质、电磁介质、红外介质或半导体介质。处理器可用介质的一些更具体的实例包括（但不限于）便携式计算机磁盘，诸如软盘、压缩磁盘、硬盘驱动器、随机访问存储器、只读存储器、闪速存储器、高速缓冲存储器和 / 或能够存储程序设计、数据或其他数字信息的其他配置。

[0031] 使用上述恰当存储介质内存储的和 / 或通过网络或其他传输介质传达的并且经配置以控制恰当处理电路的程序设计，可以实施本文所述的至少一些实施例。例如，程序设计可以经由恰当的介质来提供，其包括（例如）实施在制品之内的程序设计、实施在经由恰当的传输介质来传达的数据信号（例如，已调制载波、数据包、数字表示等）之内的程序设计，该恰当的传输介质为（例如）经由通信接口提供的诸如通信网络（例如，互联网和 / 或专用网络）、有线电气连接、光学连接和 / 或电磁能之类，或者该程序设计可以通过使用其他恰当的通信结构或介质来提供。但在一个实例中，可以将包括处理器可用代码的程序设计作为实施为载波的数据信号来传达。

[0032] 指示模块 26 经配置以产生与在受监测区域 10 中无线设备 14 的出现和身份相关的指示。在一个实施例中，指示模块 26 在一个或多个位置上产生诸如无声警报、可视警报和 / 或声响警报的人类可察觉指示，以指示一个或多个无线设备 14 的出现和身份。指示模块 26 可以包括向操作者传送与无线设备 14 相关的信息的显示器。指示可以用于指示经授

权和 / 或未经授权无线设备 14 在受监测区域 10 中出现。

[0033] 如上所述，根据具体应用，可以各个方式来配置监测设备 15。图 3 图示根据节点设备 16 的一个实施例来配置的监测设备 15。在此实施例中，节点设备 16 包含通信模块 20，该通信模块 20 经配置以接收在受监测区域 10 内的无线设备 14 的无线通信。通信模块 20 耦接到处理电路 22，该处理电路 22 可以经配置以处理这些无线通信来确定该无线设备为经授权或未经授权。

[0034] 在一些实施例中，通信模块 20 包括 RF 检测模块 32、RF 询问模块 34、系统通信模块 36 和 Telco 通信模块 38。RF 检测模块 32 可以经配置用于检测一个或多个无线设备 14 的无线通信。RF 询问模块 34 可以经配置以输出无线通信（例如，询问信号）和从无线设备 14 接收响应的无线通信（例如，响应信号），处理电路 22 经配置以使用这些应答来确定无线设备 14 为经授权或未经授权。系统通信模块 36 可以经配置用于向系统 12 的至少一个其他的监测设备 14 传达无线通信以及其他信息，该监测设备 14 可以经配置以确定无线设备 14 为经授权或未经授权。此外，在一些实施例中，系统通信模块 36 可以经配置以与一个或多个外部设备 40 通信。Telco 通信模块 38 可以经配置用于与一个或多个电信提供商进行通信，该通信包括向一个或多个电信提供商转发无线通信。如果无线设备 14 的无线通信是加密的，那么 Telco 通信模块 38 还可经配置用于从电信提供商接收包括这些无线通信中呈未加密格式的至少一部分的通信。

[0035] 节点设备 16 可以进一步包含一个或多个存储介质 24，该存储介质 24 经配置以存储与一个或多个经授权无线设备 14 相关的信息。存储介质 24 可以包含用于存储（尤其是）用户数据的数据库或其他数据的存储器。一个或多个存储介质 24 耦接到处理电路 22，以使得处理电路 22 可以使用存储的信息来确定授权或未授权无线设备 14 在受监测区域 10 中出现。还可包括指示模块 26，该指示模块 26 经配置以产生与无线设备 14 的出现相关的指示。指示模块 26 可以可操作地耦接至视觉指示器 42（例如，灯）和音频传感器 44（例如，扬声器）中的至少一个。

[0036] 图 4 图示根据管理设备 30 的一个实施例来配置的监测设备 15。管理设备 30 包含上文关于图 2 来描述的每个组件。管理设备 30 的通信模块 20 经配置以接收在受监测区域 10 内的无线设备 14 的无线通信。在此实施例中，通信模块 20 从至少一个其他的监测设备 15（诸如节点设备 16）接收无线通信。通信模块 20 可以包括用于与至少一个其他的监测设备 15 通信的节点设备通信模块 46。通信模块 20 耦接到处理电路 22，该处理电路 22 可以经配置以处理这些无线通信来确定该无线设备 14 为经授权或未经授权。通信模块 20 还包括用于与至少一个外部设备 40 通信的外部设备通信模块 48。此外，通信模块 20 包括用于与一个或多个电信提供商通信的 Telco 通信模块 38。Telco 通信模块 38 可以向电信提供商转发无线设备 14 的无线通信，并且如果来自无线设备 14 的无线通信是加密的，那么 Telco 通信模块 38 还可从电信提供商接收包括这些无线通信中呈未加密格式的至少一部分的通信。

[0037] 管理设备 30 可以包含一个或多个存储介质 24，该存储介质 24 经配置以存储与一个或多个经授权无线设备 14 相关的信息。存储介质 24 可以包含用于存储（尤其是）用户数据的数据库或其他数据的存储器。一个或多个存储介质 24 耦接到处理电路 22，以使得处理电路 22 可以使用存储的信息来确定是否授权该无线设备 14。还可包括指示模块 26，且

该指示模块 26 经配置以产生与无线设备 14 的出现相关的指示。指示模块 26 可以可操作地耦接至视觉指示器 42（例如，灯）和音频传感器 44（例如，扬声器）中的至少一个。

[0038] 参见图 5，根据一个实施例展示了经配置以监测多个受监测区域 10 的监测系统 12a 的布置。监测系统 12a 的布置包括多个节点设备 16，多个节点设备 16 与多个各自的受监测区域 10 相关联并且经配置以监测多个各自的受监测区域 10。节点设备 16 经配置以与管理设备 30 通信，在一些实施例中，可以将管理设备 30 实施为服务器。在一些实施例中，可以分别根据图 3 所图示的节点设备 16 和图 4 所图示的管理设备 30 来单独配置节点设备 16 和管理设备 30。

[0039] 如图 5 中图示和下文进一步详细描述，在一些实施例中，节点设备 16 可以与无线设备 14 通信并且向管理设备 30 输出通信以用于分析。在一个实施例（例如，单个组织应用）中，管理设备 30 执行该分析。在另一个实施例（例如，多个组织应用）中，管理设备 30 可以与执行该分析的外部设备 40 通信。在一些布置中，在一个组织或实体（例如，公司）内实施监测系统 12a，并且外部设备 40 与不同的组织或实体相关联。其他实施例是可能的。

[0040] 参见图 6，根据一个实施例展示和描述对受监测区域监测无线设备 14 的出现。最初，节点设备 16 经配置以监测在各自的受监测区域 10，例如邻近于受监测区域 10 的入口点，无线设备 14 的出现。如上所述，节点设备 16 可以包括 RF 检测模块 32，该 RF 检测模块 32 经配置以检测来自无线设备 14 的无线通信。在一个实施例中，节点设备 16 经配置以扫描无线设备 14 的使用频率，并且可以通过由其发射（例如当无线设备 14 与其他设备或服务器通信时）和由通信模块 20（图 2）接收的 RF 信号来检测无线设备 14。在 2006 年 7 月 28 日提交的标题为“Radio Frequency Detection Assembly andMethod for Detecting Radio Frequencies”的共同待审美国专利申请No. 11/460,662 中描述了根据一个实施例的检测无线设备 14 的额外细节，其公开内容全文以引用方式并入本文。

[0041] 在检测无线设备 14 之后，节点设备 16 可以产生通信以询问该无线设备。到无线设备 14 的通信可以包括识别节点设备 16 的无线设备 14 的标识符（例如，认证 ID）。该通信可以请求无线设备 14 的识别信息。该通信可以包括一个或多个质询，诸如“你的唯一设备标识符 (ID) 是什么？”、“你是否在公司 PED 服务器中登记？”和“谁是你的公司 PED 服务器？”。在一个实施例中，该通信可以包括对设备认证数据的请求，该设备认证数据诸如对应于无线设备 14 的当前配置（例如，所有系统文件和设置）的来自无线设备 14 的配置信息。

[0042] 在一些实施例中，无线设备 14 可以单独地经配置以与来自节点设备 16 的通信协作实施操作。例如，无线设备 14 可以包括先前加载的认证软件，该认证软件配置无线设备 14 以接收和处理来自节点设备 16 的通信，收集恰当的信息和向节点设备 16 返回恰当的应答。认证软件可以包括嵌入的数字签名和 / 或加密密钥以执行签名和 / 或加密功能。响应来自节点设备 16 的通信，无线设备 14 可以形成应答通信，诸如数字签名的响应。该响应可以包括设备标识符、与无线设备 14 相关联的公司 PED 服务器的标识符、设备认证数据和 / 或额外信息。设备认证数据可以包括呈加密数字散列形式的配置信息。在一个实施例中，由无线设备 14 自身来确定加密数字散列。例如，无线设备 14 可以使用由公司 PED 服务器指定的签名密钥来计算其配置信息（例如，内部操作系统文件 / 数据，用户和 / 或 CPS 安装的应用程序 / 数据等）的数字散列。

[0043] 在一些实施例中，节点设备 16 可以在检测到无线设备 14 之后向无线设备 14 传达对话令牌。可以产生多个对话令牌，以作为用于所检测无线设备 14 的各自询问对话的唯一标识符。无线设备 14 可以将各自对话令牌包括在数字签名响应的计算中。对话令牌可以用于确保无线设备 14 的先前数字签名响应不会被存档以供将来使用，并且可以排除间谍软件 (spyware) 或恶意软件 (malware) 冒充合法的无线设备 14。当认证无线设备 14 时，节点设备 16 可以在分析无线设备 14 的当前响应时考虑来自各自无线设备 14 的先前存储的响应和各自的对话令牌。

[0044] 此外，根据一些实施例，可以从节点设备 16 向无线设备 14 传达插入点，指示无线设备 14 在何处将对话令牌插入散列函数（例如，在第 5 个文件之后、在第 25 个文件之后等）。根据一个实施例来指定对话令牌在某个索引上的位置可以有助于排除针对数字签名算法的过载攻击。在一个实施例中，节点设备 16 可以存档个别文件的数字散列或者与所有信息的单个散列相反地设置分组。在一些实例中，当无线设备 14 注册服务时和在已知的系统更新次数上，可以实施存档。

[0045] 在另一个实施例中，在检测到无线设备 14 的出现之后，节点设备 16 可以启动包括节点识别值 (NIV) 的到无线设备 14 的通信。在一个实施例中，NIV 可以提供该通信节点设备 16 的参考而不直接予以识别。例如，可以取节点设备 16 的实际节点 ID 的散列并将其与该请求的时间戳组合来形成 NIV。无线设备 14 可以解码该 NIV 并且确定其是否希望应答（如果设备 14 不应答那么可以发出警报）。在该所述实施例中，一些无线设备 14 可以被编程以避免泄露设备标识符、与公司或服务的关联等。

[0046] 具体地讲，公司政策或其他政策可以确定无线设备 14 是否响应所接收节点询问请求的部分、所有或者全部不响应，并且可以由无线设备 14 的所有者、节点管理员或两者进行配置。与诸如 RFID 或蓝牙的标签设备相比，根据一个实施例的这种应答与否的能力可以减低无线设备 14 对不期望跟踪的脆弱性。

[0047] 无线设备 14 可以响应来自节点设备 16 的通信或询问而提供一个或多个通信。如上文所提及，该响应可以包括设备 ID 以及设备认证数据。然后，监测系统可以确定授权或未授权无线设备 14 在受监测区域 10 中出现。在仅使用单个节点设备 16 的一些实施例中，该节点设备 16 可以经配置以执行图 6 的管理设备 30 和外部设备 40 的操作，如在下文中更详细描述。在此实施例中，没有使用管理设备 30 或外部设备 40。另外，在单个组织或系统内执行监测和分析的实施例中，可以在管理设备 30 内实施外部设备 40 的操作。因此，取决于实施例，节点设备 16 其自身可以分析响应通信的信息，以确定无线设备 14 是经授权或未经授权，或者节点设备 16 可以向远程设备（例如，管理设备 30 或外部设备 40（如果存在））传达响应通信以用于分析。

[0048] 可以由节点设备 16、管理设备 30 和 / 或外部设备 40（取决于监测系统 12 的实施例）来分析所接收的设备 ID 和设备认证数据，以确定是否要产生警报或其他指示。在一个实施例中，恰当的节点设备 16、管理设备 30 或外部设备 40 可以包括数据库，该数据库包括经授权以在各自的受监测区域 10 中出现的无线设备 14 的列表。如果未将无线设备 14 识别为经授权设备，那么可以产生警报。可以由节点设备 16、管理设备 30、外部设备 40 和 / 或其他模块或电路来产生该警报或其他指示。

[0049] 在一些实施例中，分析包含无线设备 14 的配置信息的设备认证数据，以确定是否

已对另外经授权无线设备 14 的配置进行了任何未经授权的改变。例如，恰当的设备 16、设备 30、设备 40 可以使用无线设备 14 的设备 ID，以从数据库访问所存储的各自无线设备 14 的配置信息。所存储的配置信息可以包含与在初始时刻的无线设备 14 的配置相关的信息（例如，在无线设备 14 发放给雇员时的配置信息的散列）。在一个实施例中，监测系统 12 在随后的时刻执行操作（例如，当在受监测区域 10 的位置上检测到无线设备 14 时），以验证从初始时刻以来尚未修改无线设备 14 的配置。

[0050] 如果无线设备 14 的配置已改变，那么设备 16、设备 30、设备 40 中的一个或多个设备可以发出警报或其他指示。所存储的配置信息可以呈散列形式，并且执行设备配置分析的各自的设备 16、设备 30、设备 40 可以将存储的散列与无线设备 14 所提供的散列进行比较以确定该配置是否已改变。如果各自的设备 16、设备 30、设备 40 确定该配置已改变，那么各自的设备 16、设备 30、设备 40 可以发出恰当的警报或指示。例如，如果已修改操作系统文件、公司 PED 服务器所安装的文件或受控制的设置或者如果已安装了应用程序，那么所接收的设备配置信息的散列将以不同于所存储散列的方式进行计算，从而指示无线设备 14 可能已由恶意攻击者修改或者以其他方式已遭泄密。

[0051] 在一些使用情况中，一些无线设备 14 可以实施无线通信，其中一些传达信息未被加密并可由监测系统 12 接收和直接读取以确定无线设备 14 是否经授权在正受监测的位置上出现。例如，GSM 无线通信的至少一些内容未被加密，并且可以由监测系统 12 容易地接收和读取。在其他无线设备中，监测系统 12 可能无法破译正在通过无线通信传达的信息的部分或全部。例如，无线通信的数据内容、报头和 / 或其他信息（例如，设备 ID、无线设备 14 的配置信息）可以受到加密或者以其他方式不可由监测系统 12 读取或访问。举例而言，UMTS 和 WCDMA 使用加密，其中诸如通信设备的识别信息之类的通话详情对监测系统 12 来说可能无法破译。即使由监测系统 12 接收的无线设备 14 的无线通信可以被加密或者以其他方式对监测系统 12 来说无法破译，但下文描述的实施例中的至少一些实施例允许执行本文所述的认证操作。

[0052] 在一些地理位置上，破解加密和对正通过无线通信传达的信息进行解码可能被认为是线路窃听，从而可能是违法的。在一些实施例中，节点设备 16 和 / 或管理设备 30（取决于监测系统 12 的配置）可以经配置以实施与外部设备的通信，该外部设备诸如试图破译来自无线设备 14 的加密识别信息的电信提供商或运营商 60 的通信设备。此类配置可以避免潜在线路窃听的法律纠缠。在一个实施例中，电信提供商 60 可以是无线通信提供商，诸如经配置以使用电信提供商 60 的无线网络来在包括无线设备 14 的多个设备之间实施蜂窝通信的蜂窝电信提供商。

[0053] 如果因为接收的无线通信是无法破译的（例如，无线通信的报头信息是加密的），所以无线设备 14 的身份不可由监测系统 12 根据接收的无线通信直接确定，那么监测系统 12 可以经配置以实施与电信提供商 60 的通信以确定无线设备 14 的身份。在一些实施例中，监测系统 12 经配置以向电信提供商 60 转发由监测系统 12 接收的无法破译的无线通信，以用于认证和确定无线设备 14 的身份。在一个实施例中，即使从无线设备 14 接收的无线通信的部分（例如，无线设备 14 的识别信息）对于监测系统 12 来说无法破译，监测系统 12 仍可经配置以解码这些无线通信的其他部分，该无线设备 14 识别这些无线通信将转发到的恰当电信提供商 60。转发到电信提供商 60 的无线通信可以或不可以由监测系统 12 修

改。

[0054] 电信提供商 60 可以经配置以解码和处理（例如，解密）所接收的无线通信并且以可破译格式向监测系统 12 提供包括无法破译的通信的至少一部分（可以包括识别信息）的应答信息。然后，监测系统 12 可以唯一地识别该无线设备 14。在一些实施例中，监测系统 12 可以不包括管理设备 30，并且节点设备 16 经配置以与电信提供商 60 通信。在监测系统 12 内存在管理设备 30 的实施例中，节点设备 16 可以向管理设备 30 转发由节点设备 16 接收的无线通信，并且管理设备 30 可以经配置以向电信提供商 60 转发这些无线通信。在其他实施例中，节点设备 16 可以经配置以向电信提供商 60 转发无线通信并且向管理设备 30 转发来自电信提供商 60 的任何应答信息。在其他实施例中，节点设备 16 可以向电信提供商 60 转发无线通信，且然后，电信提供商 60 可以向管理设备 30 传达应答信息。

[0055] 在一个实施例中，节点设备 16（或管理设备 30）的通信模块 20（图 2）经配置以实施与电信提供商 60 的通信，以确定无线设备 14 的身份。例如，节点设备 16（或管理设备 30）可以按照上文参考图 3 和图 4 所述来配置，其中通信模块 20 包括 Telco 通信模块 38。在一个可能的配置中，通信模块 20 可以从无线设备 14 接收无线通信，并且将所接收的无线通信转发到经配置以接收这些通信的电信提供商 60 的恰当通信设备。在一些示范性实施例中，监测系统 12 的操作者与电信提供商 60 为不同的实体，并且存在这样的布置，其中监测系统 12 要将无法破译的无线通信转发到试图获悉无线设备 14 的身份的电信提供商 60。在其他实施例中，监测系统 12 可以是电信提供商 60 的一部分，并且电信提供商 60 可以具有专门的部门来应付来自监测系统 12 的询问。其他布置也涵盖在本发明的范围内。

[0056] 在一个实施例中，由监测系统 12 检测的来自无线设备 14 的无线通信和监测系统 12 与电信提供商 60 的通信经由各自的独立通信链路来发生（例如，在一个实施例中，这些无线通信可以包含由监测系统 12 接收的 RF 信号，并且监测系统 12 和电信提供商 60 的通信可以经由互联网来发生）。也可能存在用于与电信提供商 60 通信的其他实施例和配置，包括向电信提供商 60 转发所接收的通信。

[0057] 电信提供商 60 经授权并且能够破译从无线设备 14 发射、由监测系统 12 接收并且经转发到电信提供商 60 的无线通信。具体地讲，电信提供商 60 可以解密无线通信的报头信息，以获得无线设备 14 的识别信息。在一个实施例中，电信提供商 60 向监测系统 12 的通信模块 20（图 2）传达识别信息（例如，设备 ID、设备配置信息）。

[0058] 根据一个实施例，在操作中，个别节点设备 16 可以监测和检测在一个或多个受监测区域 10 中一个或多个无线设备 14 的出现。节点设备 16 可以获得与无线设备 14 相关的识别信息。具体地讲，节点设备 16 可以通过产生到无线设备 14 的通信以请求识别信息来询问检测到的无线设备 14，并且节点设备 16 可以接收一个或多个响应的通信或其应答。如果无线设备 14 的身份不能由监测系统 12 根据接收的无线通信直接确定（例如，无线通信的报头信息是加密的），那么监测系统 12 可以实施与电信提供商 60 的通信，以确定无线设备 14 的识别信息的内容。无线设备 14 的识别信息可以从电信提供商 60 传达到节点设备 16 和 / 或管理设备 30。节点设备 16 可以将应答从无线设备 14 或者电信提供商 60（取决于实施例）传达到管理设备 30。在一些实施例中，从节点设备 16 到管理设备 30 的通信可以被加密并且经由安全通信通道（例如，使用内部网络、内联网或互联网）来传达。

[0059] 管理设备 30 的存储介质可以包括存储的数据库，该存储的数据库包含与经授权

无线设备 14 相关的识别信息。管理设备 30 的处理电路 22 可以通过将所获得的识别信息与关于一个或多个经授权无线设备 14 的所存储的识别信息进行比较，来确定由节点设备 16 接收的识别信息是否指示恰当的无线设备 14。如果识别信息未指示恰当的无线设备 14，那么管理设备 30 可以提供警报或其他指示和 / 或向各自的节点设备 16 传达应答，各自的节点设备 16 可以提供无线设备 14 未经授权的警报或其他指示。在一个实施例中，如果无线设备 14 未经授权，那么节点设备 16 还可控制对禁止访问受监测区域 10 的锁定。

[0060] 如果管理设备 30 使用识别信息将无线设备 14 识别为经授权的，那么管理设备 30 可以提取用于各自无线设备 14 的认证数据（例如，所存储的配置信息）。管理设备 30 的处理电路 22 可以将所存储的认证数据的至少一部分或至少一项与从无线设备 14 接收的设备认证数据进行比较。如果所存储的认证数据与设备认证数据不同，那么管理设备 30 和 / 或各自的节点设备 16 可以产生警报或其他指示。

[0061] 否则，如果所存储的认证数据与设备认证数据匹配，那么管理设备 30 可以向各自的节点设备 16 传达经授权的信号。节点设备 16 可以产生无线设备 14 已被授权的指示或不进行操作，并且允许无线设备 14 在受监测区域 10 中出现。在一些实施例中，可以认证或验证在节点设备 16 与管理设备 30 之间的通信，并且认证或验证的失败可能导致将无线设备 14 识别为未经授权。

[0062] 在另一个实施例中，可能存在外部设备 40。如先前所提及，在一些实施例中，监测系统 12 和外部设备 40 可以对应于不同的组织。在一个可能的实施方式中，可以将外部设备 40 实施为公司 PED 服务器，并且先前可以将外部设备 40 登记 / 批准为监测系统 12 的覆盖网络的参与成员。使用在管理设备 30 与外部设备 40 之间共享的安全密钥和认证数据，可以建立一种可能的登记过程。

[0063] 如上所述，个别节点设备 16 可以监测和检测无线设备 14 在一个或多个受监测区域 10 的出现。节点设备 16 可以询问所检测到的无线设备 14 并且从无线设备 14 接收应答。在一些实施例中，节点设备 16 可以向电信提供商 60 转发这些应答以用于解码。节点设备 16 或电信提供商 60 可以向管理设备 30 传达应答。在一个实施例中，可以加密从节点设备 16 到管理设备 30 的通信和 / 或从电信提供商 60 到节点设备 16 或管理设备 30 的通信。在一个实施例中，例如，使用各自的无线网络 50 和无线服务供应商 52，管理设备 30 可以使用公司 PED 服务器标识符将该通信路由至与恰当的公司 PED 服务器对应的各自的外部设备 40。在一个实施例中，管理设备 30 可以验证该外部设备 40 是预订成员。如果不是，那么管理设备 30 和 / 或各自的节点设备 16 可以产生该无线设备 14 未经授权的警报或其他恰当指示。在一个实施例中，可以加密并且经由安全通信通道传达从节点设备 16 到管理设备 30 和到外部设备 40 的通信。例如，管理设备 30 可以在通信传达到外部设备 40 之前对其进行签名。在一个实施例中，管理设备 30 还可将其自身的标识符包括在到外部设备 40 的通信中。

[0064] 在一个布置中，外部设备 40 可以位于外部设备 40 的各自组织的防火墙内部的公司内部网络上。在一个实施例中，使用与各自无线设备 14 相关联的无线网络 50 和无线服务供应商 52 以及互联网 54 来提供到外部设备 40（例如，实施为公司 PED 服务器）的连接，可以传输去往外部设备 40 的通信。

[0065] 在收到之后，外部设备 40 可以验证无线设备 14、节点设备 16 和 / 或管理设备 30

的签名。可由外部设备 40 访问的存储介质 24 可以包括数据库，该数据库包含与和 CPS 的组织相关联并且寻求获得进入与监测系统 12 相关联的组织的受监测区域 10 之一的经授权无线设备 14 相关的信息。外部设备 40 的处理电路 22 可以确定该识别信息是否指示恰当的无线设备 14。在至少一些实施例中，外部设备 40 的处理电路 22 可以通过将设备识别信息与所存储的信息进行比较来确定该识别信息是否指示恰当的无线设备。如果识别信息未指示恰当的无线设备 14，那么外部设备 40 可以提供警报或其他指示和 / 或向管理设备 30 和各自的节点设备 16 传达应答，管理设备 30 和各自的节点设备 16 中的每一个都可以提供无线设备 14 未经授权的警报或其他指示。

[0066] 如果外部设备 40 将无线设备 14 识别为经授权的，那么外部设备 40 可以提取用于各自无线设备 14 的所存储的认证数据（例如，配置信息）。外部设备 40 的处理电路 22 可以将所存储的认证数据与从无线设备 14 接收的设备认证数据进行比较。如果所存储的认证数据和设备认证数据不同，那么外部设备 40 可以产生警报或其他指示和 / 或向监测系统 12 传达应答。管理设备 30 和 / 或各自的节点设备 16 还可响应来自外部设备 40 的应答来产生警报或其他恰当的指示。

[0067] 否则，如果无线设备 14 是经授权的（例如，所存储的认证数据与设备认证数据匹配）并且所有认证都经验证，那么外部设备 40 可以向各自的监测系统 12 的管理设备 30 传达经授权的信号。管理设备 30 可以验证或认证从外部设备 40 接收的经授权的信号并且向节点设备 16 提供经授权的响应。在一个实施例中，将在设备 30 与设备 40 和 / 或设备 16 与设备 30 之间的安全数据通道（例如，加密的数据包、数字签名、公共密钥基础设施等）用于通信，并且将进入包解密并且检查其签名以验证在设备 30 与设备 40 和 / 或设备 16 与设备 20 之间的通信。在一个实施例中，可以认证或验证在设备 16 与设备 30 和设备 30 和设备 40 之间的通信，并且认证或验证失败可能导致将无线设备 14 识别为未经授权。响应来自设备 30 和设备 40 的授权，管理设备 30 和 / 或节点设备 16 可以产生无线设备 14 经授权的指示或者不进行操作，并且允许无线设备 14 在受监测区域 10 中出现。

[0068] 根据监测系统 12 的额外实施例，管理设备 30 或外部设备 40 可以维持其中授权给定无线设备 14 出现的（例如，组织的）受监测区域 10 的列表。去往管理设备 30 和外部设备 40 的通信可以包括检测无线设备 14 出现的各自节点设备 16 的标识符。设备 30 和 / 或设备 40 的处理电路可以认证节点设备 16 的标识符和 / 或将节点设备 16 的标识符与用于各自无线设备 14 的经授权受监测区域 10 的列表进行比较，并且如果无线设备 14 在其出现的各自的受监测区域 10 中为未经授权，那么可以如本文所述那样启动警报或其他指示。

[0069] 在另一个实施例中，外部设备 40 可以启动从监测系统 12 到无线设备 14 的通信（例如，使用无线网络 50）。该通信可以请求在询问期间从节点设备 16 传达到无线设备 14 的节点设备 16 和 / 或管理设备 30 的标识符。无线设备 14 将节点设备 16 和 / 或管理设备 30 的标识符传达到外部设备 40，该外部设备 40 可以使用该标识符来认证监测系统 12 的组件。如果由外部设备 40 处理的监测系统 12 的标识符并不匹配，那么可以由节点设备 16、管理设备 30 和 / 或外部设备 40 产生警报或其他指示。

[0070] 如本文论述和根据一些实施例，本发明的装置和方法可以用于验证携带进入或试图携带进入受监测区域的无线设备 14 经允许在受监测区域中出现。在一个实施例中，可以使用这些装置和方法来验证无线设备 14 尚未被更改（例如）而包括恶意软件或其他系统

修改。在一个实施例中，如果未经批准的或经暗中修改的无线设备 14 出现在受监测区域 10 中，那么可以使用这些装置和方法来发出警报或其他指示。根据本发明的各个实施例，提供无线设备 14 的配置是否已改变和 / 或是否允许无线设备 14 进入一个或多个受监测区域 10 的信息。根据本发明的一些实施例，可以将批准的无线设备 14 带入受监测区域 10 中并且在受监测区域 10 内对其进行操作，同时提供与无线设备 14 是否已被修改（可能是恶意地）有关的信息。

[0071] 如上文所论述，在一个实施例中，监测系统 12 可以与无线设备 14 通信以实施一个或多个认证功能（例如，在一个实施例中，通过询问信号和响应信号）。在一些实施例中，监测系统 12 可以建立与无线设备 14 的额外通信。举例而言（但并非限制），监测系统 12 可以使用电信提供商 60 的 SMS 消息或 OTA 消息来实施这些额外通信。在一个实施例中，这些额外通信独立于最初由无线设备 14 发送并且由监测系统 12 检测到的无线通信（例如，独立于无线设备 14 和电信提供商 60 的蜂窝网络通信）。例如，在一些实施例中，监测系统 12 的节点设备 16 可以通过蓝牙连接或使用近场通信来建立与无线设备 14 的通信。可能存在用于实施这些额外通信的其他实施例。在一个实施例中，监测系统 12 与无线设备 14 之间的通信可以包括上文论述的询问信号和响应信号。在一个实施例中，使用各自的独立通信链路，可以传达由监测系统 12 检测到的来自无线设备 14 的初始无线通信和在无线设备 14 与监测系统 12 之间的其他无线通信。

[0072] 图 7 是图示根据一个实施例的将无线设备识别为经授权或未经授权的方法的程序框图。可能存在包括更多、更少和替代性动作的其他方法。在 710，由邻近于受监测区域的节点设备来检测被带入该受监测区域的无线设备。在 712，该节点设备可以问询或询问所检测到的无线设备以获得信息。在 714，该节点设备获得包括识别信息的来自该无线设备的响应。该响应可以包括识别信息，该识别信息包含（例如）唯一设备标识符、设备 14 是否在公司服务器中登记的指示符和公司 PED 服务器的识别（如果恰当的话）等。另外，该节点设备可以获得认证数据（例如，设备配置信息）。如果没有接收到响应，那么可以将该设备识别为未经授权。基于所获得的识别信息和 / 或所获得的认证数据，可以将该无线设备确定为经授权或未经授权在该受监测区域中。例如，在 716，分析设备识别信息和 / 或设备认证数据。该分析可以包含将该设备识别信息和 / 或设备认证数据与所存储的识别信息和 / 或所存储的认证数据进行比较。如果在该分析期间设备识别信息或设备认证数据中任何一个不能得到验证或认证，那么可以将设备识别为未经授权。在 718，响应该分析，可以将该无线设备识别为经授权和未经授权之一以及允许或禁止其进入受监测区域。

[0073] 图 8 是图示识别使用加密的无线通信的无线设备是否经授权以在受监测位置上出现的方法的一个实施例的程序框图。可能存在包括更多、更少和 / 或不同动作的其他方法。在 810，监测系统检测在受监测区域内无线设备的出现。例如，在一个实施例中，在该无线设备与关联的无线网络（例如，蜂窝网络）进行通信期间，该监测系统从该无线设备接收无线通信。可以由该监测系统在受监测区域内定位该无线设备。在一个实例中，该监测系统经配置以监测进入房间的入口，并且该监测系统经配置以检测在该入口内出现的无线设备的无线通信。

[0074] 该监测系统可以从该无线设备接收识别信息。响应请求该识别信息的询问或通信，可以接收该识别信息。该监测系统可以确定这些无线通信的至少一些内容对该监测系

统来说是无法破译的。例如，该无线设备的识别信息不能根据由该监测系统接收的无线通信来确定。在 812，在一个实施例中，该监测系统进行操作以将这些无线通信向监测系统外部转发到该无线设备使用的无线网络的提供商或转发到电信提供商。

[0075] 在 814，该监测系统从唯一地识别该无线设备的提供商（或其他源）接收识别信息，并且在 816，该监测系统使用该识别信息来确定授权或未授权该无线设备在正由该监测系统监测的位置上出现。例如，该监测系统可以将所接收的识别信息与存储在该监测系统内的识别信息进行比较，该监测系统识别经授权以在受监测位置上出现的一个或多个设备。如上所述，该监测系统可以实施关于该无线设备的询问操作，并且可以响应这些询问操作来指示该无线设备是否经授权。在一个实施例中，该监测系统可以指示关于正在受监测的位置来说该无线设备的授权的被确定状态。

[0076] 虽然已描述了某些实施例并且将其展示附图中，但这些实施例仅为说明性的且并不限制本发明的范围，并且本发明并不限于这些所展示和所描述的具体构造和布置，因为存在各个其他的添加和修改以及删除，所述实施例对所属领域的技术人员将是显而易见。从而，本发明的范围仅由以下权利要求书的字面语言和法律等效物限制。

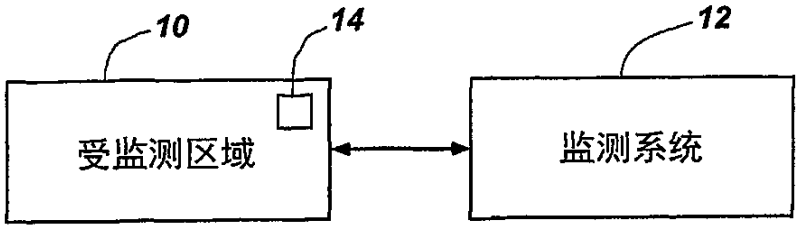


图 1

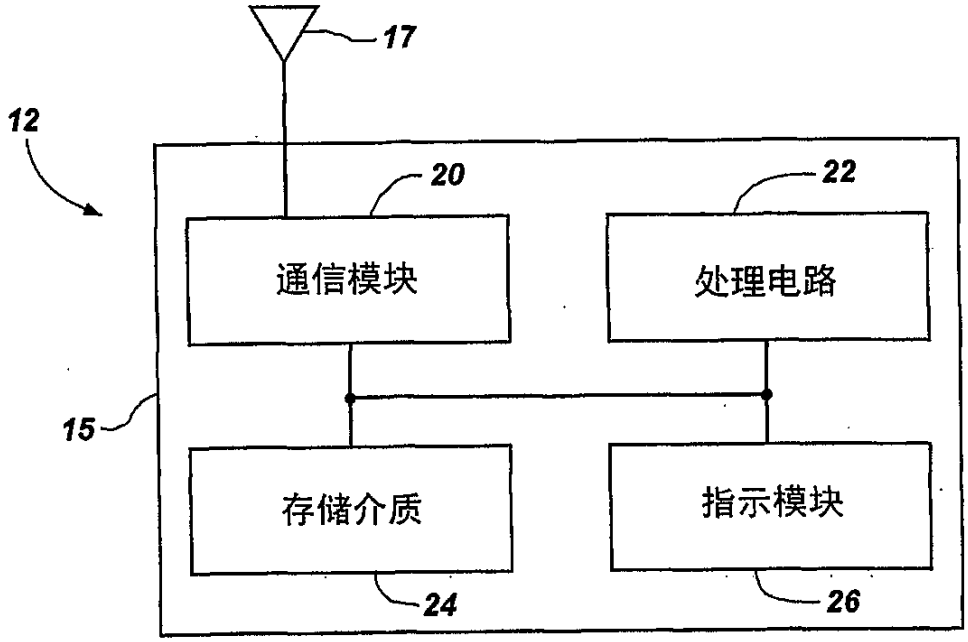


图 2

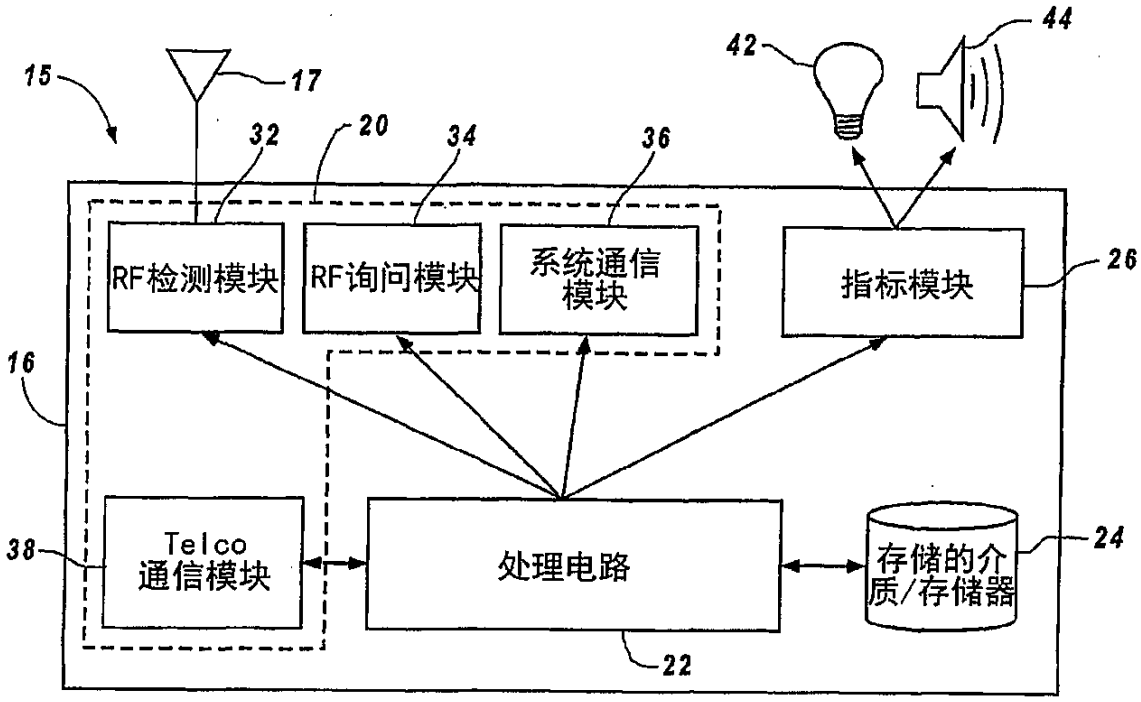

15
17
32
20
34
36
42
44
RF检测模块
RF询问模块
系统通信模块
指标模块
26
16
38
Telco通信模块
处理电路
存储的介质/存储器
24
22

图 3

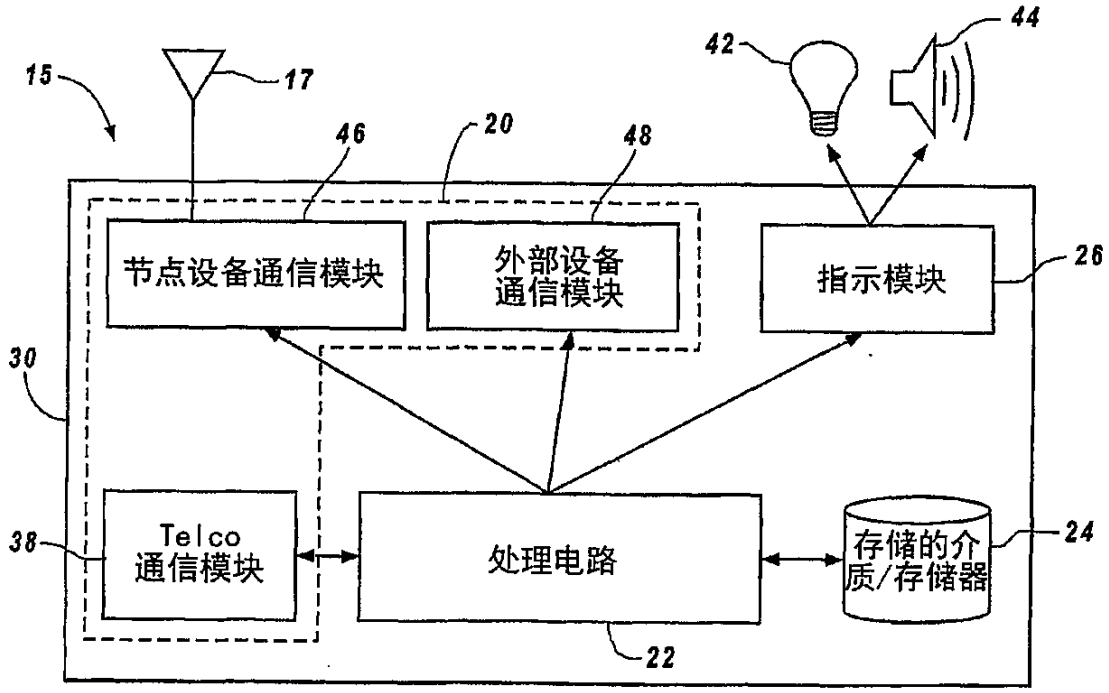

15
17
46
20
48
42
44
节点设备通信模块
外部设备通信模块
指示模块
26
30
38
Telco通信模块
处理电路
存储的介质/存储器
24
22

图 4

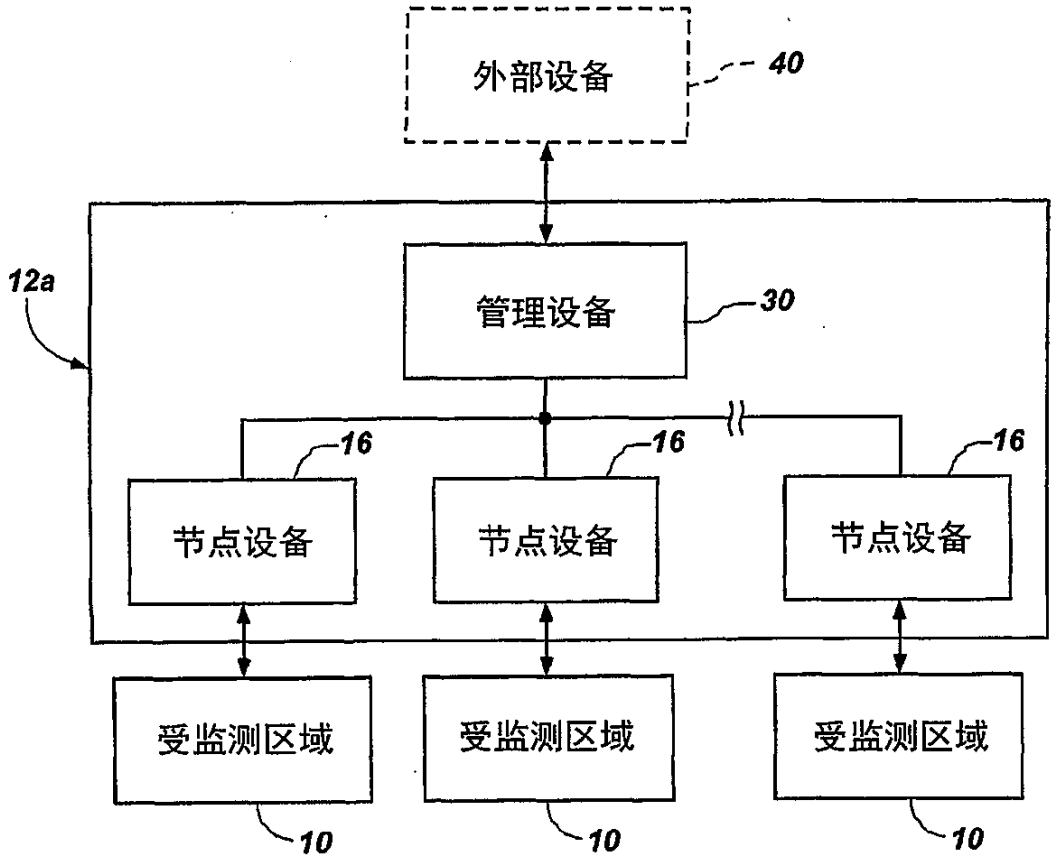

外部设备
40
12a
管理设备
30
16
16
16
节点设备
节点设备
节点设备
受监测区域
受监测区域
受监测区域
10
10
10

图 5

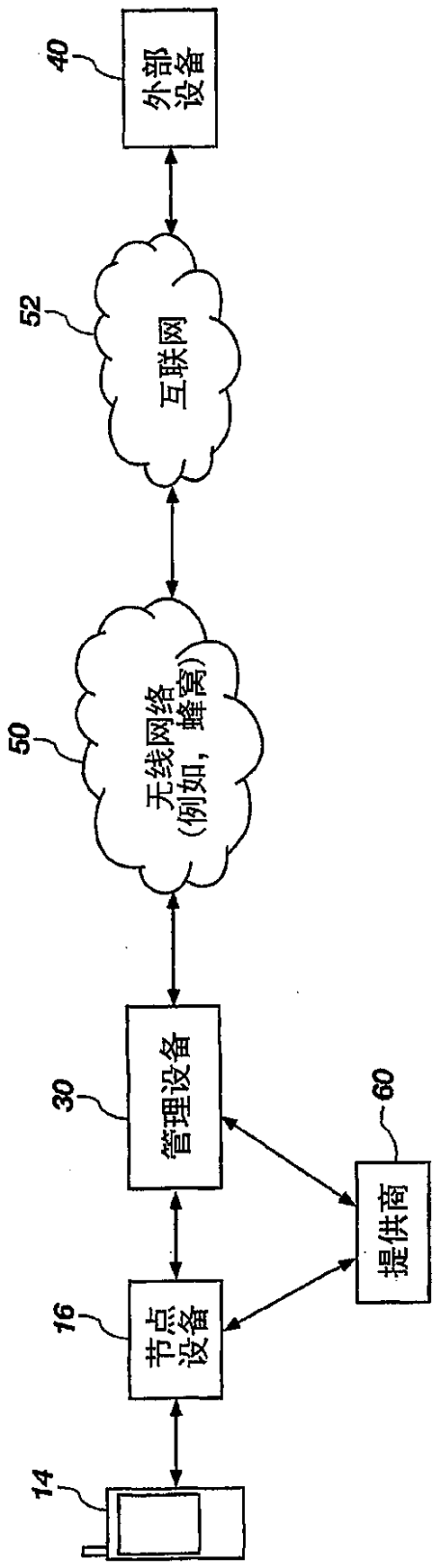

40
外部设备
52
互联网
50
无线网络（例如，蜂窝）
30
管理设备
60
提供商
16
节点设备
14

图 6

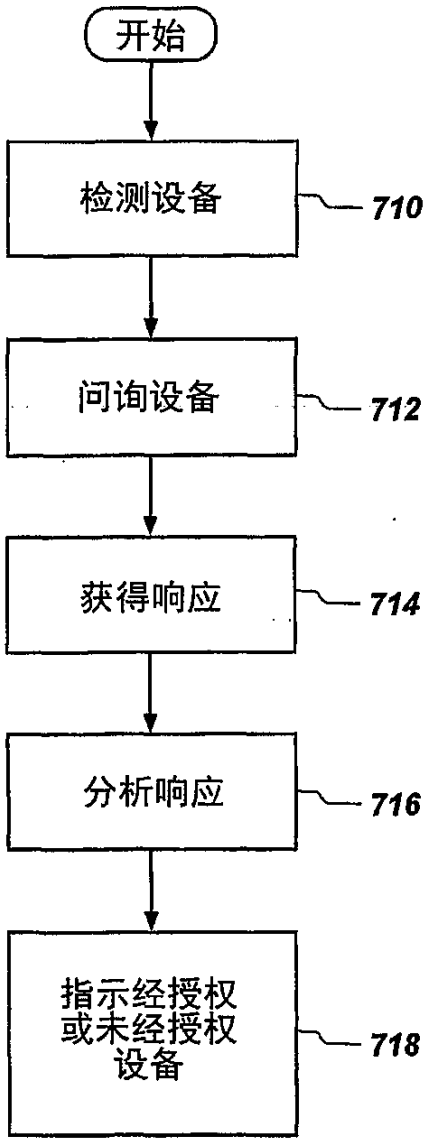

开始
检测设备
710
问询设备
712
获得响应
714
分析响应
716
指示经授权或未经授权设备
718

图 7

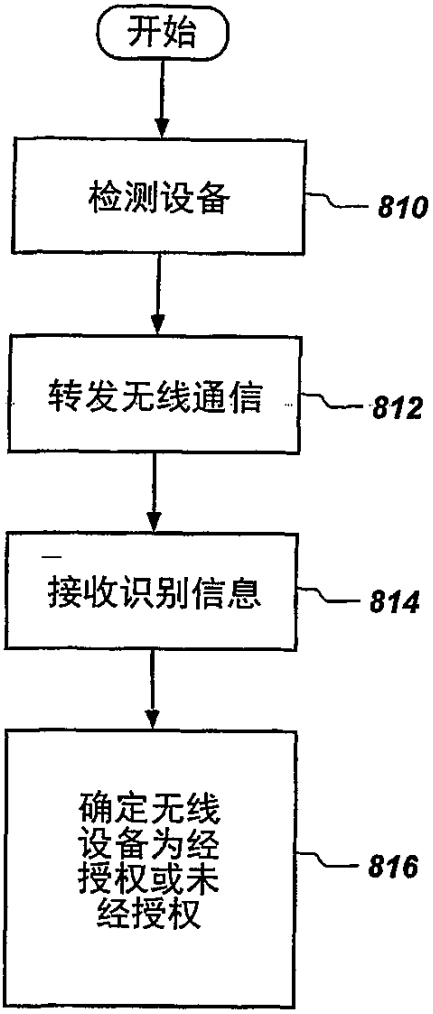


图 8