[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/00 (2006.01)
H04Q 7/24 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680001658.8

[43] 公开日 2008 年 1 月 2 日

[11] 公开号 CN 101099134A

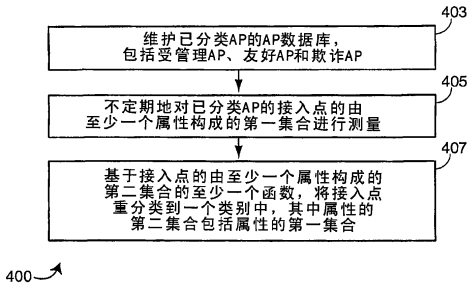
[22] 申请日 2006.2.6
[21] 申请号 200680001658.8
[30] 优先权
[32] 2005. 2.25 [33] US [31] 11/066,009
[32] 2005. 7.25 [33] US [31] 11/188,564
[86] 国际申请 PCT/US2006/004260 2006.2.6
[87] 国际公布 WO2006/093634 英 2006.9.8
[85] 进入国家阶段日期 2007.6.28
[71] 申请人 思科技术公司
地址 美国加利福尼亚州
[72] 发明人 杰里米·斯蒂格里兹
蒂莫西·S·欧尔森
佩曼·D·罗珊
[74] 专利代理机构 北京东方亿思知识产权代理有限责任公司
代理人 王 怡
权利要求书 6 页 说明书 25 页 附图 4 页

[54] 发明名称

对无线网络中的接入点进行动态测量和重分类

[57] 摘要

一种方法、装置和载波介质，该载波介质承载用于指示处理器执行该方法的计算机只读代码段。该方法用在包括至少一个接入点的无线网络中。 该方法包括不定期地对该无线网络中的至少一个已分类接入点的集合中的每个接入点(111 - 115)的至少一个属性的第一集合进行测量(405)。 该方法还包括基于接入点的至少一个属性的第二集合的至少一个函数对每个接入点进行重分类(407)，该属性的第二集合包括所述属性的第一集合。 至少一个接入点的集合根据一组 AP 类别被分类，并且其中所述重分类是分类到所述 AP 类别之一中。



1. 一种无线网络中的方法，该无线网络包括至少一个接入点（“AP”），该方法包括：

不定期地对所述无线网络中的至少一个已分类接入点的集合中的每个接入点的由至少一个属性构成的第一集合进行测量；以及

基于所述接入点的由至少一个属性构成的第二集合的至少一个函数对每个接入点进行重分类，属性的第二集合包括属性的第一集合，

其中，所述至少一个接入点的集合根据一组 AP 类别被分类，并且其中所述重分类是分类到所述 AP 类别之一中。

2. 如权利要求 1 所述的方法，其中，所述重分类是由指示所述接入点的属性的第二集合中的一个或多个属性的显著改变的至少一个函数触发的。

3. 如权利要求 2 所述的方法，其中，所述重分类是由指示所述接入点的属性的第二集合中的一个或多个属性被改变了至少一个相应的预设阈值的显著改变的至少一个函数触发的。

4. 如权利要求 3 所述的方法，其中，所述重分类是由所述接入点的属性的第二集合中的一个或多个属性中的任意一个被改变了一个相应的预设阈值的改变触发的。

5. 如权利要求 2 到 4 中任意一个所述的方法，其中，其显著改变触发了重分类的所述接入点的属性的第二集合包括：

检测到在特定 AP 处从其他邻近 AP 接收到的分组的 RSSI 改变；

在 AP 已被分类为受管理接入点的情形中，检测到新的或不同的配置设置；

检测 RF 参数的显著改变，所述 RF 参数包括以下一个或多个：

去往或来自其他 AP 的发送定时，以及

去往或来自其他 AP 的路径损耗；

检测 AP 的新的网络地址改变；

检测 AP 的数据成帧的显著改变；以及

在 AP 先前位于已知位置的情形中检测显著的位置改变。

6. 如前述权利要求中任意一个所述的方法，其中，所述接入点的至少一个属性的第二集合的至少一个函数是时间，使得所述重分类是根据预设的时间调度执行的。

7. 如前述权利要求中任意一个所述的方法，其中，所述接入点的一个或多个属性的第一集合包括以下至少一个：

线内无线台站检测；

所述台站的确定的位置；

在所述接入点处对来自其他 AP 的信号的无线电信号强度的测量值；以及

所述接入点的去往和/或来自所述无线网络的一个或多个其他无线台站的确定的发送定时。

8. 如前述权利要求中任意一个所述的方法，其中，所述无线网络是受管理的无线网络，并且其中所述 AP 类别的集合包括受管理 AP、友好 AP 和欺诈 AP。

9. 如权利要求 8 所述的方法，其中，所述无线网络的接入点的类别被存储在数据库中，并且该数据库在耦合到所述无线网络的每个受管理 AP 的无线管理器中被维护。

10. 如前述权利要求中任意一个所述的方法，

其中，所述无线网络遵循 801.11 标准或者其变体之一，

其中，所述对 AP 执行重分类是基于以下至少一个执行的：

- 该 AP 的 BSSID；
- 在其上接收到来自该 AP 的任意信标或探查响应的信道；
- 接收信标或探查响应的台站的 MAC 地址；
- 在接收台站的物理层处检测到的所述信标或探查响应的信号强度；
- 在接收台站的物理层处可获得的接收到的信标或探查响应的接收信号质量的任意其他测量值；和/或
- 从其他 AP 接收到的信标和探查响应，

并且，其中，从 AP 接收到的信标或探查响应包括以下一个或多个：

- 所述信标或探查响应中的 SSID；
- 信标时间（TSF 定时器）信息。在一个实施例中，这是以通过将所述信标/探查响应中的时间戳与接收该响应的受管理 AP 处的或者接收该响应的受管理客户端处的 TSF 定时器进行比较所确定的 TSF 偏移的形式发送的；和/或
- 接收到的信标/探查响应中包括的配置参数。

11. 如前述权利要求中任意一个所述的方法，还包括：

针对每个 AP 确定汇聚信任水平，这种信任水平是指示所述参数的第二集合中的一个或多个参数的改变的函数的加权和。

12. 如权利要求 11 所述的方法，其中，所述加权被用来根据所述接入点的最近类别来确定汇聚信任水平。

13. 一种承载一段或者多段计算机可读代码段的载波介质，所述计算机可读代码段指示处理系统的至少一个处理器执行一种无线网络中的方法，该无线网络包括至少一个接入点（“AP”），该方法包括：

不定期地对所述无线网络中的至少一个已分类接入点的集合中的每个接入点的由至少一个属性构成的第一集合进行测量；以及

基于所述接入点的由至少一个属性构成的第二集合的至少一个函数对每个接入点进行重分类，属性的第二集合包括属性的第一集合，

其中，所述至少一个接入点的集合根据一组 AP 类别被分类，并且其中所述重分类是分类到所述 AP 类别之一中。

14. 如权利要求 13 所述的载波介质，其中，所述重分类是由指示所述接入点的属性的第二集合中的一个或多个属性的显著改变的至少一个函数触发的。

15. 如权利要求 14 所述的载波介质，其中，所述重分类是由指示所述接入点的属性的第二集合中的一个或多个属性被改变了至少一个相应的预设阈值的显著改变的至少一个函数触发的。

16. 如权利要求 15 所述的载波介质，其中，所述重分类是由所述接入点的属性的第二集合中的一个或多个属性中的任意一个被改变了一个相应

的预设阈值的改变触发的。

17. 如权利要求 14 到 16 中任意一个所述的载波介质，其中，其显著改变触发了重分类的所述接入点的属性的第二集合包括：

检测到在特定 AP 处从其他邻近 AP 接收到的分组的 RSSI 改变；

在 AP 已被分类为受管理接入点的情形中，检测到新的或不同的配置设置；

检测 RF 参数的显著改变，所述 RF 参数包括以下一个或多个：

去往或来自其他 AP 的发送定时，以及

去往或来自其他 AP 的路径损耗；

检测 AP 的新的网络地址改变；

检测 AP 的数据成帧的显著改变；以及

在 AP 先前位于已知位置的情形中检测显著的位置改变。

18. 如权利要求 13 到 17 中任意一个所述的载波介质，其中，所述接入点的至少一个属性的第二集合的至少一个函数是时间，使得所述重分类是根据预设的时间调度执行的。

19. 如权利要求 13 到 18 中任意一个所述的载波介质，其中，所述接入点的一个或多个属性的第一集合包括以下至少一个：

线内无线台站检测；

所述台站的确定的位置；

在所述接入点处对来自其他 AP 的信号的无线电信号强度的测量值；以及

所述接入点的去往和/或来自所述无线网络的一个或多个其他无线台站的确定的发送定时。

20. 如权利要求 13 到 19 中任意一个所述的载波介质，其中，所述无线网络是受管理的无线网络，并且其中所述 AP 类别的集合包括受管理 AP、友好 AP 和欺诈 AP。

21. 如权利要求 20 所述的载波介质，其中，所述无线网络的接入点的类别被存储在数据库中，并且该数据库在耦合到所述无线网络的每个受管理 AP 的无线管理器中被维护。

22. 如权利要求 13 到 21 中任意一个所述载波介质，

其中，所述无线网络遵循 801.11 标准或者其变体之一，

其中，所述对 AP 执行重分类是基于以下至少一个执行的：

- 该 AP 的 BSSID；
- 在其上接收到来自该 AP 的任意信标或探查响应的信道；
- 接收信标或探查响应的台站的 MAC 地址；
- 在接收台站的物理层处检测到的所述信标或探查响应的信号强度；
- 在接收台站的物理层处可获得的接收到的信标或探查响应的接收信号质量的任意其他测量值；和/或
- 从其他 AP 接收到的信标和探查响应，

并且，其中，所述从其他 AP 接收到的信标和探查响应包括以下一个或多个：

- 所述信标或探查响应中的 SSID；
- 信标时间（TSF 定时器）信息。在一个实施例中，这是以通过将所述信标/探查响应中的时间戳与接收该响应的受管理 AP 处的或者接收该响应的受管理客户端处的 TSF 定时器进行比较所确定的 TSF 偏移的形式发送的；和/或
- 接收到的信标/探查响应中包括的配置参数。

23. 如权利要求 13 到 22 所述的任意一个所述的载波介质，还包括：

针对每个 AP 确定汇聚信任水平，这种信任水平是指示所述参数的第二集合中的一个或多个参数的改变的函数的加权和。

24. 如权利要求 23 所述的载波介质，其中，所述加权被用来根据所述接入点的最近类别来确定汇聚信任水平。

25. 一种无线网络中的装置，该无线网络包括至少一个接入点（“AP”），该装置包括：

用于不定期地对所述无线网络中的至少一个已分类接入点的集合中的每个接入点的由至少一个属性构成的第一集合进行测量的装置；以及

用于基于所述接入点的由至少一个属性构成的第二集合的至少一个函

数对每个接入点进行重分类的装置，属性的第二集合包括属性的第一集合，

其中，所述至少一个接入点的集合根据一组 AP 类别被分类，并且其中所述重分类是分类到所述 AP 类别之一中。

26. 如权利要求 25 所述的装置，其中，所述用于重分类的装置是由指示所述接入点的属性的第二集合中的一个或多个属性的显著改变的至少一个函数触发来进行重分类的。

27. 如权利要求 25 到 26 所述的装置，还包括：

用于针对每个 AP 确定汇聚信任水平的装置，这种信任水平是指示所述参数的第二集合中的一个或多个参数的改变的函数的加权和。

28. 如权利要求 27 所述的装置，其中，所述加权被用来根据所述接入点的最近类别来确定汇聚信任水平。

对无线网络中的接入点进行动态测量和重分类

本发明要求 2005 年 7 月 25 日提交的美国专利申请 No. 11/188,564 的优先权，该申请的发明人为 Stieglitz 等，题为 DYNAMICALLY MEASURING AND RE-CLASSIFYING ACCESS POINTS IN A WIRELESS NETWORK，案卷号/文献号为 No. CISCO10744，该申请被转让给本发明的受让人。美国专利申请 No. 11/188,564 的内容通过引用被结合于此。

本发明是 2005 年 2 月 25 日提交的美国专利申请 No. 11/066,009 的继续申请，并且要求该申请的优先权，该申请的发明人为 Winget 等，题为 LOCATION BASED ENHANCEMENTS FOR WIRELESS INTRUSION DETECTION，案卷号/文献号为 No. CISCO-9838，该申请被转让给本发明的受让人。美国专利申请 No. 11/066,009 的内容通过引用被结合于此。

背景技术

本发明涉及无线网络，更具体地说，涉及对基础设施无线局域网系统（WLAN）中的接入点的属性进行测量并且对其重分类的方法。

WLAN 近来变得日益流行，尤其是遵循 IEEE 802.11 标准的 WLAN。这种标准提供了自组织网络，其中任意无线台站可以直接与任意其他无线台站通信，这种标准还提供了基础设施网络，其中被称作接入点（AP）的一个台站充当一组客户端台站的基站。因此，一个 AP 形成一个小区，在该小区中其任意客户端台站（或者转发器）可以与该 AP 通信。任意客户端台站都仅经由它到另一个客户端台站或者到网络的任意部分（例如，可以被连接到接入点之一的有线网络）的接入点通信。

WLAN 允许公司将网络的好处扩展到移动劳力，并且无线地派送新的联网服务和应用。公司在布署无线网络时面临的挑战之一是安全性，包括防止“外来”无线设备作为欺诈接入点连接到公司的网络。

WLAN 特有的一些安全性问题是由于无线客户端台站请求接入到各种

AP 而引起的。通常，在 WLAN 环境的布署中，AP 小区覆盖被重叠来实现最大的 RF 覆盖，以减小非服务点。无线客户端台站在 AP 之间移动，从而根据它们的位置改变 WLAN 的 RF 环境。另外，WLAN 通常被要求随着由于越来越多的客户端台站要求来自 WLAN 所服务而增长的需求而增大。扩充 WLAN 要求配置装备、添加 AP，以及将 AP 置于不与其他 AP 相冲突的位置中或者不以其他方式使管理 WLAN 复杂化的位置中。

因为无线是一种开放介质，所以任何人都可以争取接入并且通过无线信道发送信息。

无线网络一般使用 MAC 层的管理帧，这种帧被设计、发送和接收来用于管理目的。例如，在遵循 IEEE 802.1 标准的 WLAN 中，AP 定期发送声明该 AP 的存在的信标帧，即，向潜在的客户端通告该 AP 的服务，使得客户端可以与该 AP 相关联。类似地，客户端可以发送探查请求帧，该帧请求其无线电范围内的任何 AP 利用探查响应帧作出响应，该帧以与信标帧类似的方式，向请求客户端（以及在其无线电范围内并且能够接收其信道的任意其他频率器件）提供信息使得客户端足以判断是否与该 AP 相关联。

IEEE 802.11 管理帧一般在没有任何保护的情况下被发送，最近已提议了一些管理帧保护方法。利用不受保护的管理帧，攻击者从而可以容易地伪装合法的 AP，发送指示到客户端台站，如同其是服务于该客户端台站的 AP 一样。例如，几乎所有攻击都是开始于攻击者通过发送解关联或者去认证请求到客户端台站来伪装 AP。

因此，需要一种方法和装备，用来有效地保护 WLAN，并且向 WLAN 管理者提供进行管理和接入控制判决所需的信息。具体而言，因为 WLAN 的许多客户不控制哪种类型的设备可以连接到有线以太网和无线网络，这种客户正面临对是否、何时和如何在它们的环境中布署接入点进行控制的困难挑战。用户常常会插入未经批准的无线接入点，来递送未经企业批准和/或从企业信息技术部门不能获得的无线网络。较少发生但是值得关注的是，网络攻击者有时可能从不同的位置在不同的时刻将接入点置于企业网络内部，利用该未经批准的接入点来获得对企业网络的智能接入。

也被称作无线侵入检测系统（WIDS）的欺诈接入点检测系统（RAPDS）是公知的，并且用于管理无线 RF 安全性的某些方面。这种系统的多个方面包括检测、定位、报警，并且在理想情况下关闭它们的网络上的欺诈接入点的能力。这些系统一般利用对接入点进行分类的分层模型，接入点类别有已知且受管理的 AP（在这里称作*受管理 AP*）、在受管理网络附近的已知 AP、或者对受管理 AP 的客户端（即，受管理客户端）已知的 AP，已知不会给受管理无线网络带来问题（例如，干扰）的 AP。这样的 AP 被称作*友好 AP*。友好 AP 的一个示例是在咖啡店中的 AP，其中企业的雇员通常利用作为被管理客户端并且与该友好 AP 相关联的计算机来工作。最后，还存在未知的和/或已知“欺诈”的 AP（在这里总称为*欺诈 AP*）。

在下面的具体实施方式部分给出了对一些欺诈 AP 检测方法的概述。

这些欺诈 AP 检测系统所缺乏的是根据 AP 的行为改变将 AP 分类和重分类成分类方案中的类别之一的动态能力。

作为一个示例，比较聪明的攻击者可能利用已知的欺诈 AP 检测系统来将接入点放置到企业网络附近，期望随着时间流逝，该接入点会被标记为“友好 AP”。这种攻击者然后可以将该接入点移动到企业网络内部，然后利用该接入点作为 “特洛依木马”，从而避免利用一般的欺诈 AP 检测系统的检测。

因此，在本领域中需要一种方法，用来执行测量、无线电扫描、以及对已被分类到受管理无线网络中的接入点进行重分类。

发明内容

本发明的一个方面是利用全范围的主动空中检测、定位和测量系统，来主动、动态地对所有已知的已发现的受管理或者已被分类的接入点进行重分类。

具体而言，这里描述了方法、装置和携带计算机可读代码段的载波介质，所述计算机可读代码段指示处理系统中的至少一个处理器执行该方法。该方法用于包括至少一个接入点的无线网络中。该方法包括不定期地

对无线网络的至少一个已分类接入点的集合中的每个接入点的至少一个属性的第一集合进行测量。该方法还包括基于接入点的至少一个属性的第二集合的至少一个功能，对每个接入点进行重分类，该属性的第二集合包括属性的第一集合。至少一个接入点的集合根据一组 AP 类别被分类，并且被重分类到所述 AP 类别 之一中。

通过利用本发明，可以实现：

1. 提高的安全性。
2. 减少错误确定。
3. 对欺诈接入点的攻击自动自防护。

检测和将接入点分类成例如欺诈接入点的任何无线欺诈 AP 检测系统都可以使用本发明的实施例。

从下面的描述和附图中，将清楚其他方面和特征。

附图说明

图 1 示出了实现了本发明多个方面的包括 WLAN 管理器和 AP 的简化受管理网络；

图 2 示出了可以是 AP 或者客户端台站的实现了本发明一个或多个方面的无线台站的一个实施例的简化框图。

图 3 示出了用于利用在已知的例如受管理的 AP 处接收到的信号强度确定潜在的欺诈 AP 的位置的方法的一个实施例。

图 4 示出了确定是否对一个或多个接入点重分类的一个实施例。

具体实施方式

这里描述了方法、系统和载波介质中的软件程序，用来利用主动无线台站检测、台站定位和无线电测量，以对所有已知“友好”接入点、受管理接入点、新发现的接入点、欺诈接入点，或者以其他方式被分类的接入点重新分类。

受管理网络

将参考代表性无线网络来对本发明进行描述，所述代表性无线网络基本遵循 IEEE 802.11 标准，例如，802.11a、802.11b、802.11g 或者当前已预见到的标准，例如，802.11n。基本遵循的意思是与之兼容。假设本说明书的读者能够接触到定义这些标准的文档，并且定义这些标准的所有文档都为了一切目的通过引用被结合于此。在这里所讨论的示例中，要被无线网络覆盖的区域被划分成多个小区，每个小区具有一个接入点（AP）。客户端被与特定的接入点相关联，并且可以经由该接入点实现去往和来自该网络的通信。

图 1 示出了本发明的实施例可以被应用到的代表性无线通信网络 100。示出了五个接入点：AP1（111）、AP2（112）、AP3（113）、AP4（114）和 AP5（115）。每个 AP 可以具有若干个相关联的客户端（未示出）。在一个实施例中，每个 AP 是受管理无线网络的一部分，就每个 AP 与受管理无线网络的管理实体通信而言，该 AP 是受管理 AP。

取决于大小和复杂度，受管理网络是具有中央控制实体的一组 AP，或者具有最终被耦合到一组 AP 的一组层级控制域的层级结构。每个控制域被一个管理实体管理，该管理实体在这里称之为管理器。层级中的级别数目取决于网络的复杂度和/或大小，因此并非所有受管理的网络都具有所有控制级别。例如，简单的受管理网络可能仅具有一个控制级别，该控制级别具有对所有 AP 进行控制的单个管理实体。影响对控制域的选择的因素包括以下一个或多个：各种类型的 IP 子网配置；接入点的无线电邻近度；客户端台站漫游模式；实时漫游需求；以及网络的物理约束（例如，园区、建筑等等）。

在一个实施例中，受管理 AP 具有若干个性质，包括精确地测量其接收到的功率电平的能力，在这里被称作无线电信号强度指示（RSSI）。受管理的 AP 还具有接收来自 WLAN 管理器的指示，以便根据所接收到的指令以信道数的方式设置其发送功率和发送频率的能力。

IEEE 802.11 标准的一些方面稍稍被修改来适应受管理 AP 的一些管理方面。在一个实施例中，诸如受管理 AP 之类的网络的受管理的台站能够相对准确地测量所接收到的信号强度（在这里称作接收信号强度指示，或

者 RSSI）。受管理接入点还以已知的发送功率进行发送。

至于关于无线电管理的更多信息，参见 2004 年 1 月 28 日提交的美国专利申请 No. 10/766,174，该申请的发明人为 Olson 等，题为 A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK，该申请被转让给本发明的受让人，并且通过引用结合于此。

在本说明书中，假设存在被称作 *WLAN 管理器 103* 的单个管理实体。WLAN 管理器 103 对无线网络的若干个方面进行管理，在一个实施例中包括生成无线电计划，所述无线电计划包括分配每个 AP 的发送功率和发送信道。在其他实施例中，也可以包括被称作*子网上下文管理器*的管理实体，每个子网上下文管理器控制单个子网或者虚拟局域网（VLAN）的一些方面。子网上下文管理器例如可以将来自 WLAN 管理器 103 的指令中继到其子网或者 VLAN 中的所有受管理 AP。但是，在这里示出的实施例中，子网上下文管理器的功能由 WLAN 管理器实现。其他实施例在具有不同管理级别的层级中可以具有不同数目的级别。至于关于无线电管理的更多信息，参见 2004 年 1 月 28 日提交的美国专利申请 No. 10/766,174，该申请的发明人为 Olson 等，题为 A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK，该申请被转让给本发明的受让人，并且通过引用结合于此。

注意，在这里所述的实施例中位于 WLAN 管理器 103 内的被称作*无线电管理器*的控制器提供对给定 AP 集合内的无线电环境的各个方面的智能集中化控制。单个无线电管理器根据管理结构中的分层的数目（例如，是否存在本地控制域和/或园区控制域），处理给定 WLAN“本地控制域”或者 WLAN“园区控制域”中的所有 AP 的无线电方面。无线电管理器提供在最初网络布署和网络扩展期间确定网络范围内的无线电参数的能力，这给称作无线电计划。无线电管理器集中地协调所有客户端和 AP 测量，以便例如检测欺诈接入点。

在一个实施例中，WLAN 管理器 103 对网络中的受管理接入点的集合

授权，这包括维护被称作*配置数据库*的数据库，配置数据库包含诸如分配频率和发送功率的无线电计划之类的配置参数和诸如到其控制下的 AP 的信标间隔之类的其他配置参数。配置数据库还包括 *AP 数据库*，AP 数据库包括关于受管理 AP 的信息，例如，受管理 AP 的列表和关于这些 AP 的一些数据，例如，AP 的位置和 AP 能够以其发送的功率，以及对 AP 的任意分类。WLAN 管理器 103 提供对给定的 AP 集合内的无线电环境的各个方面的集中化控制，包括执行测量来获得路径损耗，以及利用这些路径损耗信息项来确定 AP 和/或客户端的位置，并且进一步确定无线电计划，所述无线电计划包括网络范围内的无线电参数，例如，在初始网络布署和网络扩展期间的发送功率和信道。

作为一个示例，在一个实施例中，路径损耗信息是通过一次或多次预排（walkthrough）获得的，而在另一个实施例中，路径损耗信息也是或者可替换地是通过在 AP 之间自动执行路径损耗测量获得的。例如，参见上述美国专利申请 10/766,174 和 2004 年 1 月 28 日提交的美国专利申请 No. 10/629,384，该申请题为“RADIOLOCATION USING A PATH LOSS DATA”，发明人为 Kaiser 等，案卷号/文献号 No. CISCO-7391，该申请被转让给本发明的受让人，并且通过引用结合于此。

注意，本发明并不要求存在单个 WLAN 管理器实体。这里所述的功能可以被结合到例如在本地层级的任何其他管理实体中，或者由被称作无线电管理器的对 WLAN 的无线电方面进行控制的分离的管理器所结合。此外，这些管理实体中的任意一个都可以被与其他功能组合，所述其他功能例如是交换、路由选择等等。

现在参考图 1，示出了一个简单的受管理网络。包括无线电计划生成之类的所有管理功能都假设被结合在能够访问 AP 数据库的单个管理实体中，即，WLAN 管理器 103。

在一个实施例中，WLAN 管理器 103 包括具有一个或多个处理器的处理系统 123 和存储器 121。存储器 121 被示为包括指令 127，指令 127 使处理系统 123 的一个或多个处理器实现本发明的 WLAN 管理方面，包括生成网络的无线电计划，包括以发送信道的形式分配频率、以及向每个接入

点分配发送功率。WLAN 管理指令 127 还包括这里所述的无线电测量方面，无线电测量方面用于无线电计划，还用于将 AP 分类成受管理 AP、其他类型的 AP，其他类型的 AP 包括可疑的欺诈 AP。存储器 121 也被示为包括指令 129，指令 129 使处理系统 123 的一个或多个处理器实现这里所述的本发明的欺诈 AP 检测和动态重分类方面。本领域技术人员应当清楚，并非所有如此实现这些方面的这些程序同时都在存储器中。但是，它们被示为在存储器中，以便保持描述的简单性。

WLAN 管理器 103 还维护配置数据库 131，以及配置数据库 131 中的 AP 数据库 133。

WLAN 管理器 103 包括用于耦合到网络的网络接口 125，这一般是通过有线或者其他方式连接的。在一个实施例中，WLAN 管理器 103 是网络交换机的一部分，并且在网络操作系统控制下操作，所述网络操作系统在这种情形中是 IOS 操作系统（Cisco Systems, Inc., San Jose, California）。

WLAN 管理器 103 经由其网络接口 125 和网络（一般是有线网络）被耦合到一组受管理 AP：分别具有标号 111，…，115 的 AP1，…，AP5。

图 2 示出了可以是 AP 或者客户端台站并且实现本发明的一个或多个无线电测量方面的无线台站 200 的一个实施例。尽管诸如台站 200 之类的无线台站一般属于现有技术，但是例如以软件形式包括本发明多个方面并且可以理解用来实现本发明多个方面的任何特定管理帧的无线台站不一定是现有技术。无线电部分 201 包括被耦合到无线电收发机 205 的一个或多个天线 203，无线电收发机 205 包括模拟 RF 部分和数字调制解调器。无线电部分从而实现物理层（PHY）。PHY 201 的数字调制解调器被耦合到实现该台站的 MAC 处理的 MAC 处理器 207。MAC 处理器 207 经由一条或多条总线（象征性地示作单总线子系统 211）被连接到主机处理器 213。主机处理器包括存储器子系统，例如被连接到主机总线的 RAM 和/或 ROM，存储器子系统在这里被示作总线子系统 211 的一部分。台站 200 包括到有线网络的接口 221。

在一个实施例中，MAC 处理（例如 IEEE 802.11 MAC 协议）完全在 MAC 处理器 207 处实现。处理器 207 包括存储器 209，存储器 209 存储用

于 MAC 处理器 207 实现 MAC 处理以及在一个实施例中由本发明使用的额外的处理中的一些或全部的指令。存储器一般是但是不一定是 ROM，软件一般处于固件形式。

MAC 处理器由主机处理器 213 控制。在一个实施例中，一些 MAC 处理在 MAC 处理器 207 处实现，而一些在主机处实现。在这种情形中，用于主机 213 实现由主机实现的 MAC 处理的指令（代码）被存储在存储器 215 中。在一个实施例中，由本发明使用的额外处理中的一些或全部也由主机实现。这些指令被示作存储器的一部分 217。

根据本发明的一个方面，诸如台站 200 之类的每个台站维护其接收到的信标和探查响应的数据库。信标和探查响应在一种或多种环境下（例如，在台站确定出是否与 AP 相关联时）被存储在数据库中。在本发明的多个方面的上下文中，在台站处接收到的信标和探查响应作为主动扫描或者被动扫描的结果而被存储在数据库中。这种数据库被称作信标表。如图 2 所示，在一个实施例中，信标表 219 在台站的存储器 215 中。其他实施例将信标表 219 存储在存储器 215 外部。台站将关于信标和探查响应的信息存储在其信标表 219 中，并且在其接收到信标时还存储关于该台站的状态的额外信息。

根据本发明的一个方面，诸如台站 200 之类的台站在实现 AP 时能够执行被动扫描。根据本发明的另一个方面，诸如台站 200 之类的台站在实现客户端台站时能够执行被动扫描。

因为台站在其信标表中存储其已接收到的信标和探查响应，所以一种形式的被动扫描包括仅报告该台站的信标表的累积内容。注意，一种备选实施例可能包括该台站在特定时段中进行侦听，并且在该特定时段中报告递增的信标表信息。

根据又一个实施例，诸如台站 200 之类的台站在实现 AP 时能够主动扫描，尤其是递增主动扫描。为了执行递增主动扫描，AP 腾空其服务信道，并且通过在一条或多条信道上发送探查请求帧来探查一条或多条信道。AP 通过对竞争自由周期（CFP）进行调度来防止客户端发送。或者，AP 可以通过发送未被请求的 CTS 帧，该帧持续足够长的时间来覆盖主动

扫描时间，从而防止客户端发送。根据又一个实施例，台站 200 在实现客户端时能够主动扫描，尤其是递增主动扫描。为了实现递增主动扫描，客户端台站腾空其服务信道，通过在一条或多条信道上发送探查请求帧来探查一条或多条信道。在客户端的情况下，主动扫描包括报告探察其他（一条或多条）信道的结果。为了防止客户端从服务 AP 发送，客户端必须指示其正处于省电模式。或者，客户端可以使用诸如应用操作之类的具体的本地知识，来确保 AP 将不发送任何在客户端处指示的发送。

扫描包括在信标表中存储来自通过被动或主动扫描而在台站处接收到的信标和探查响应的信息。

欺诈 AP 检测系统

如上面的背景技术部分所述，欺诈接入点检测系统（RAPDS）是已知的，用于管理无线 RF 安全性的一些方面。取决于具体系统，RAPDS 利用一种或多种空中（over-the-air）和/或通过以太网局域网（LAN）技术来检测接入点的存在，并且区分所检测到的接入点是否是欺诈接入点。这些系统包括用来例如：利用 MAC 地址、利用配置、利用 RSSI、利用位置、利用 IP 地址属性等等，将接入点分类成一组类别之一的方法，所述类别例如是受管理 AP、友好 AP 或者（类似）欺诈 AP。

用于检测欺诈接入点的已知方法包括使客户端报告其他 AP 上的失败的认证尝试，或者由 AP 自身检测失败的认证尝试。例如，认证泄密方法是已知用于报告欺诈接入点的方法。参见 2001 年 7 月 27 日提交的 Halasz 等人的美国专利申请 S/N 09/917,122，该申请题为“ROGUE AP DETECTION”，被转让给本申请的受让人，并且通过引用结合于此。这种现有方法一般包括利用适当的 WLAN 标识符（服务集标识符（SSID））对台站进行配置，来进行认证尝试。仅在到客户端的合适的位置中（即，在尝试认证时具有无线电接触）的欺诈可以被检测出。这可能导致延迟的检测或者根本检测不出。

其他已知的欺诈检测方法包括利用可以在 WLAN 覆盖区域中携带的某些类型的嗅探设备。携带嗅探设备的操作员周期性地在 WLAN 覆盖区域中行走，进行测量来搜索欺诈 AP。例如参见，来自 WildPackets, Inc.,

Walnut Greek, CA 的“AiroPeek and Wireless Security: Identifying and Locating Rogue Access Points”（2002年9月11日的版本）。

另一种已知的嗅探技术是利用 AP 作为嗅探设备。例如参见，来自 AirWave Wireless, Inc., San Mateo, California （www.airwave.com）的文档“AirWave Rogue Access Point Detection”。这种 AP 由管理实体从中央位置管理。大多时候，这种受管理的 AP 充当常规接入点。在正执行欺诈扫描时，管理实体发出命令（例如 SNMP 命令）到该受管理 AP，将其转换成无线嗅探设备。受管理 AP 对其覆盖半径内的无线电波进行扫描，寻找所有信道上的流量。AP 然后将所有数据报告回管理实体作为跟踪数据，然后返回到正常工作模式。管理实体对来自受管理 AP 和岗哨设备的跟踪数据进行分析，将检测到的 AP 与其可信的受管理 AP 的数据库进行比较。但是，这种方法要求 AP 暂停正常操作。

另一种已知的欺诈 AP 检测技术要求到欺诈 AP 的连接，例如有线连接。但是，因为欺诈 AP 可能是安装在邻近位置处的设备，所以要求有线连接的检测方法可能不会总是成功。

用于检测甚至定位欺诈接入点的方法和装置的一种示例在 2004 年 1 月 28 日提交的发明人为 Olson 等的共同未决美国专利申请 No.:10/766,174 中有所描述，该申请题为“A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK”，案卷号/文献号 No. CISCO-6592，该申请被转让给本发明的受让人。美国专利申请 No. 10/766,174 的内容通过引用被结合于此。这里的这些发明在这里单独或者总地被称作“我们的欺诈检测发明”。

我们的欺诈检测发明美国专利申请 No. 10/766,174 描述了由 AP 进行的被动和/或主动扫描如何在 WLAN 管理器 103 指示下使 AP 接收信标和探查响应，而其又使 WLAN 管理器 103 利用被动或主动扫描检测到的并且被报告回 WLAN 管理器 103 的信标和/或探查响应来识别潜在的欺诈 AP。被动扫描的意思是在不首先发送探查请求的情况下侦听信标和探查响应。利用被动扫描是本发明的一个重要方面，这是因为其提供了在台站处（例如，在 AP 处）与正常处理并发的欺诈检测。主动扫描的意思是在侦

听信标和探查响应之前发送探查请求。主动扫描和被动扫描二者都可以在用于无线通信的同一信道（“服务”信道）或者其他信道（“非服务”信道）上发生。对于非服务信道，一般使用主动扫描。

根据欺诈检测发明的一个变体，WLAN 管理器 103 接收来自受管理 AP 的关于在该受管理 AP 处接收到的信标或探查响应的任何发送的报告，包括潜在的欺诈 AP 发送的那些。根据欺诈检测发明的另一个变体，WLAN 管理器 103 接收来自受管理 AP 的关于在该受管理 AP 的一个或多个客户端处接收到的信标或探查响应的任何发送的报告，包括潜在的欺诈 AP 发送的那些。WLAN 管理器 103 接收来自其受管理 AP 的报告，并且利用这些报告例如通过查找 WLAN 数据库来确定该潜在的欺诈台站是否可能是欺诈台站。在一个版本中，该分析包括确认发送了信标或探查响应的 AP 的 MAC 地址是否与 AP 数据库中的 AP 的 MAC 地址匹配，来确认该 AP 是潜在的欺诈 AP、或者受管理 AP、或者友好 AP。欺诈 AP 的近似位置（例如，精确到在例如建筑的楼层之类的感兴趣区域内或者甚至更精细）是根据关于接收信标或探查响应的受管理 AP 的位置的知识确定的，或者是根据关于接收信标或者探查响应的受管理客户端的位置的推测知识确定的。

在一个实施例中，报告给 AP 管理器（或者对 AP 进行分类的其他实体）的信息对于每个检测到的 AP 包括关于该检测的信息、关于信标/探查响应的内容的信息或者从信标/探查响应的内容获得的信息。检测信息包括以下之一或者多种：

- 例如 MAC 地址形式的被检测到的 AP 的 BSSID。
- 在其上接收到来自 AP 的任何信标或探查响应的信道。
- 接收台站的 MAC 地址。
- 在接收方的 PHY 处检测到的信标/探查响应的信号强度，例如 RSSI。
- 在接收台站的 PHY 处可获得的接收到的信标/探查响应的接收信号质量的任何其他测量。
- 从其他 AP 接收到的信标和探查响应。这可能有助于定位检测台

站。

所发送的信标/探查响应信息包括以下之一或多种：

- 信标或探查响应中的 SSID。
- 信标时间（TSF 时间）信息。在一个实施例中，这是以通过将信标/探查响应中的时间戳与接收该响应的受管理 AP 处的或者接收该响应的受管理客户端处的 TSF 定时器进行比较所确定的 TSF 偏移的形式发送的。
- 在接收到的信标/探查响应中包括的配置参数。

注意，这种信息中的一些超出了 IEEE 802.11h 2003 年 6 月所建议的。还要注意，尽管 IEEE 802.11 标准指定在物理层（PHY）处确定相对 RSSI 的值，但是本发明的一个方面利用了下述事实：许多调制解调器频率器件包括提供相对准确的绝对 RSSI 测量的 PHY。因此，这些报告包括在接收方的 PHY 处检测到的接收到的信标/探查响应的 RSSI。在一个实施例中，在 PHY 处检测到的 RSSI 被用来根据路径损耗确定位置信息。

在 WLAN 管理器 103 处接收到的信息的一部分是在接收来自潜在的欺诈 AP 的信标或探查响应的台站处的 RSSI。这些接收到的信号强度或者更具体地说 AP 之间的路径损耗根据我们的欺诈检测发明的一个方面被用来提供路径损耗图，然后进一步定位潜在的欺诈 AP。

用于确定其发送功率未知的潜在的欺诈 AP 的位置的方法的一个实施例通过显示一组发送功率的可能性轮廓来确定可能的位置，例如，作为位置的函数的可能性。该组发送功率包括可能的发送功率。

图 3 示出了该方法的基本步骤。在步骤 303 中，WLAN 管理器 103 对包括关于其管理的 AP 的信息的 AP 数据库进行维护。AP 数据库还包括关于受管理 AP 的信息，以及关于在受管理网络附近的已知 AP 或受管理 AP 的客户端（或受管理客户端）已知的 AP 的信息，和已知不会对受管理无线网络带来问题（例如，干扰）的 AP 的信息。这些 AP 被称作友好 AP。友好 AP 的一个示例是咖啡店里的 AP，在咖啡店中，企业雇员通常利用作为受管理客户端并且被与友好 AP 相关联的计算机进行工作。AP 数据库还包括关于欺诈 AP 的信息。在一个实施例中，AP 数据库在配置数据库中，

并且不定期地被自动更新。

AP 数据库中存储的关于 AP 的信息包括来自这样的 AP 的任何信标或者探查响应帧的信息，以及关于该 AP 的任何 802.11 信息。在一个实施例中，802.11 信息包括最大功率、频率和其他 802.11 参数。在一些实施例中，信息还可以包括位置信息。在一些实施例中，每个 AP 的信息可能还包括其他字段，例如，用于无线网络管理的其他方面的字段。例如，在受管理网络中，可能是 AP 的无线电设置被管理，并且从而 WLAN 管理器 103 了解该 AP 的无线电设置。也可以知道 AP 的位置。

本发明的一个方面将从信标或探查响应的扫描获得的信息与 AP 数据库中的信息相比较。该比较是关于来自受管理 AP 的信息的，并且在一个实施例中，是关于来自受管理的 AP 的客户端的信息的。该信息是关于从潜在的欺诈 AP 接收到的信标或探查响应的，同时 AP 数据库中存储的信息是关于受管理 AP、友好 AP、以及已知或可疑的欺诈 AP 的。

在一个实施例中，对 AP 数据库进行维护包括不定期地更新 AP 数据库中的信息。该更新是例如无论何时只要获得了关于潜在的欺诈 AP 的新信息或者无论何时只要 AP 配置被改变就自动执行。

因此，在步骤 305 中，WLAN 管理器 103 将一个或多个请求发送到一个或多个受管理 AP 来实现扫描。在一个实施例中，由 AP 执行的扫描是被动扫描。在另一个实施例中，由 AP 执行的扫描是对其中潜在的欺诈 AP 可能正进行发送的一条或多条信道的主动扫描。因为欺诈 AP 可能在任何受管理 AP 的无线电范围之外，但是仍在受管理 AP 的一个或多个客户端的范围中，因此在一个实施例中，对受管理 AP 的请求包括请求这种 AP 客户端执行扫描的指示。在一个实施例中，由受管理客户端执行的扫描是被动扫描。在另一个实施例中，由受管理客户端执行的扫描是对其中潜在的欺诈 AP 可能正在进行发送的一条或多条信道的主动扫描。

作为这种请求的结果，在步骤 307 中，WLAN 管理器 103 接收来自 AP 和它们的客户端的关于在 AP 和/或客户端的扫描中接收到的任何信标和探查响应的报告。

在步骤 309 中，WLAN 管理器 103 对在接收到的报告中获得的关于发

送了这些接收到的信标或探查响应的 AP 的信息进行分析，这种分析包括与 AP 数据库中的信息相比较。步骤 309 用于确定发送 AP 是否在 AP 数据库中。发送了响应的 AP 的 MAC 地址（BSSID）被用来在 AP 数据库中搜索匹配。在一个实施例中，该分析包括将信标/探查响应中的配置信息与 AP 数据库中存储的关于受管理 AP 的配置的信息相比较。在一个实施例中，该分析还包括利用定时信息。在一个实施例中，该分析还包括使用受管理 AP 的已知位置信息和定时信息来确定潜在的欺诈 AP 的大约位置，以便进一步确认该 AP 是否可能是欺诈 AP。步骤 309 中的分析的结果包括将每个 AP 分类成友好 AP 或者潜在的欺诈 AP。

一个实施例还包括步骤 311，该步骤试图定位接收信标和/或探查响应的接收台站，以便尝试定位（一个或多个）潜在的欺诈 AP 来进一步确认该 AP 是否可能是欺诈 AP。一种定位方法利用在接收信标/探查响应的台站处的 RSSI，以及向/从在已知位置处的受管理台站提供各个位置处的路径损耗的环境的经校准路径损耗模型。一种这样的方法在题为“RADIOLOCATION USING PATH LOSS DATA”的美国专利申请 No. 10/629,384 中有所描述，该申请的发明人为 Kaiser 等，案卷号/文献号为 CISCO-7391，该申请被转让给本发明的受让人，并且通过引用被结合于此。

一个实施例还包括步骤 313，该步骤将分析结果与一种或多种补充欺诈 AP 检测技术的结果组合。一种这样的补充技术包括客户端向服务 AP 报告失败的与 AP 的先前的认证尝试，例如，包括利用其 MAC 地址标识出可疑的 AP。一种实现方式利用基于 IEEE 802.11 安全性系统的 IEEE 802.1X，客户端和 AP 根据 IEEE 802.1X 被置于认证服务器数据库中。在客户端认证时，会话密钥被分别递送到客户端和接入点。客户端在其已利用认证服务器认证之后不能使用该会话密钥时检测到失败的认证。客户端最终与另一个当前的受管理 AP 相关联，并且经由该受管理 AP 向 WLAN 管理器 103 报告潜在的欺诈 AP。这种补充方法在 2001 年 7 月 27 日提交的题为“ROGUE AP DETECTIONI”的未决美国专利申请 S/N 09/917,122 中有所描述，该申请的发明人为 Halasz 等，该申请被转让给本发明的受让

人，并且通过引用被结合于此。

利用无线电定位，无线网络管理员（负责 WLAN 管理的 IT 人员；WLAN 管理器 103 的用户）可以尝试物理定位 AP。在定位了该 AP 之后，管理员可以将该 AP 分类成欺诈的、受管理的或者友好的，然后利用关于该 AP 的信息更新 WLAN 数据库，所述信息包括其被分类成欺诈的、受管理的或友好的。如果是欺诈 AP，则网络管理员可以发出报警。

在一个实施例中，用来确定 AP 是友好的还是欺诈的的标准的集合由无线网络管理员设置，并且被存储在配置数据库中。

在分类时也可以使用补充技术，来进一步评估检测出的潜在的欺诈 AP 实际上是欺诈 AP 的概率。

作为用于定位可疑欺诈 AP 的补充技术的一个示例，该方法可以包括确定可疑 AP 被连接到的交换机端口。定位可疑欺诈 AP 被连接到的交换机端口的方法是已知的。例如，基于相关的方案是已知的，该方案包括将（潜在的）欺诈 AP 的有线侧的 MAC 地址与 IEEE 802.11 MAC 地址相关。一旦这些 MAC 地址被相关，则然后可以搜索边沿交换机来定位 MAC 地址。MAC 地址也可以从与潜在的欺诈 AP 相关联的客户端台站捕获，并且这种捕获地址也可以被用来搜索边沿交换机以定位 AP。

基于相关的方法和类似的方法存在一些缺点，并且在不包括网络地址翻译（NAT）功能时通常不能工作。

2005 年 3 月 3 日提交的发明人为 Olson 等人的美国专利申请 No. 11/073,317 描述了可以被用于成功地定位交换机端口的技术，该申请题为 METHOD AND APPARATUS FOR LOCATING ROGUE ACCESS POINT SWITCH PORTS IN A WIRELESS NETWORK RELATED PATENT APPLICATINOS，案卷号/文献号为 No. CISCO-9772，该申请被转让给本发明的受让人，并且通过引用结合于此。一个版本包括与潜在的欺诈 AP 相关联的专门的客户端作为客户端，并且通过该（潜在的）欺诈 AP 向 WLAN 管理器 103 发送发现分组。如果接收到发现分组，则欺诈 AP 然后被连接到网络，并且其交换机端口然后可以被定位。美国专利申请 No. 11/073,317 还包括用于如果必要的化禁用欺诈 AP 的交换机端口的方法。

图 4 示出了本发明一个方面的方法实施例 400 的流程图。该方法包括，在 403 中，维护被分类成例如包括受管理 AP、友好 AP 和（潜在的）欺诈 AP 的一组分类的 AP 的数据库。该方法包括，在 405 中，不定期地对无线网络的由至少一个已分类的接入点构成的集合中的每个接入点的至少一种属性的第一集合进行测量。该方法还包括，在 407 中，基于由接入点的至少一种属性构成的第二集合的至少一个函数，对每个接入点重新分类，该属性的第二集合包括属性的第一集合。

具体而言，重分类由指示接入点的属性的第二集合中的改变的至少一个函数触发。

因此，本发明的一个方面对已分类的 AP 动态地重分类，例如，分类成受管理 WLAN 系统中的所有接入点（例如，AP 数据库中的 AP）中的受管理 AP、友好 AP、或者欺诈 AP 之一。具体而言，本发明的一个方面基于检测到接入点的一种或多种属性的函数的改变，实时地对接入点动态重分类。

在一个版本中，重分类是根据作为 WLAN 管理器 103 中的参数的时间调度设置的。在另一版本中，重分类是由检测到接入点的以下属性中的至少一种的显著改变而被触发的。在特定版本中，当以下属性中的多于一种改变时，触发重分类的这种改变的量被设置为比在仅以下设置中的一种属性改变时触发所需的小。此外，在又一个版本中，重分类根据可设置的时间调度发生，并且进一步由于检测到接入点的以下属性中的至少一种的显著改变而发生。

在一个实施例中，对于特定 AP，触发重分类的属性如下：

1．检测到在特定 AP 处从其他邻近 AP 接收到的分组的 RSSI 的改变。在一个实施例中，AP 数据库存储到该 AP 数据库中的其他 AP 的 RSSI。假设在 AP 数据库中存在 N 个已知的 AP，并且假设特定 AP 是第 k 个 AP，$1 \le k \le N$。用 $RSSI_{k,j}(t)$表示在由 t 表示的当前时刻处在第 k 个 AP 处从第 i 个 AP 接收到的 RSSI，其中 $k \neq i$，$1 \le k,i \le N$。在一个实施例中，检测到 RSSI 的表示为 $f_{k,RSSI}(RSSI_{k,1}(t),\ldots,RSSI_{k,N}(t))$ 的函数的比表示为 $Thresh_{k,RSSI}$ 的量大的改变。即，如果，

对于任意的 k ，$1 \leqslant k \leqslant N$，$\Delta f_{k,RSSI}(RSSI_{k,1},..., RSSI_{k,N}) \geqslant Thresh_{k,RSSI}$，其中 $\Delta f_{k,RSSI}= f_{k,RSSI}(RSSI_{k,1}(t),...,RSSI_{k,N}(t))-f_{k,RSSI}(RSSI_{k,l}(t-\Delta t),... ,RSSI_{k,N}(t-\Delta t))$，则事件被触发。

在一个实施例中，$t-\Delta t$ 是最近一次利用 RSSI 进行评估的时间。

在另一个实施例中，AP 数据库存储从已知 AP 到特定 AP 的路径损耗。在此情况下，再次假设在 AP 数据库中存在 N 个已知的 AP，并且假设特定 AP 是第 k 个 AP，$1 \leq k \leq N$。用 $PL_{k,i}(t)$表示从第 i 个 AP 到第 k 个 AP 的路径损耗，其中 $k \neq i$，$1 \leq k,i \leq N$。在一个实施例中，检测到从表示为 $t-\Delta t$ 的前一时间起到表示为 t 的当前时刻处，路径损耗的表示为 $f_{k,PL}(PL_{k,1}(t),\ldots,PL_{k,N}(t))$的函数的比表示为 $Thresh_{k,PL}$ 量大的改变。即，如果，

对于任意的 k ，$1 \leqslant k \leqslant N$，$\Delta f_{k,PL}(PL_{k,1},...,PL_{k,N}) \geq Thresh_{k,PL}$，其中 $\Delta f_{k,PL}= f_{k,PL}(PL_{k,1}(t),...,PL_{k,N}(t))-f_{k,PL}(PL_{k,1}(t-\Delta t),...,PL_{k,N}(t-\Delta t))$，则事件被触发。

在一个实施例中，$t-\Delta t$ 是最近一次利用路径损耗进行评估的时间。

2．在受管理接入点的情形中，可以使用对新的或不同的配置设置（例如在计划参数的值中表示的）的检测。在受管理网络中，WLAN 管理器 103 针对每个受管理接入点确定一组无线电计划参数，包括作为 RF 计划的一部分的 AP 的工作信道和发送功率设置。还可以包括其他参数，例如，天线增益设置，数据速率等。例如，在 WLAN 管理器运行 IOS（Cisco Systems，Inc.，San Jose，CA）的实施例中，特定受管理 AP 的 IOS 行命令 show running-config 提供了该 AP 的当前配置设置的列表。

假设对于特定 AP 存在 n_p 个计划参数，并且还假设该特定 AP 是第 k 个 AP， $1 \leq k \leq N$。用 $P_{k,i}(t)$表示在时刻 t 处的第 i 个参数，$1 \leq i \leq n_p$。在一个实施例中，表示为 $Thresh_{P,k}$ 的阈值被与从较早的 Δt 之前的时刻的值到时刻 t 的参数的表示为 $f_{k,P}(P_{k,1}(t),\ldots,P_{k,}n_p(t))$的函数的改变相比较。即，如果，

对于任意的 k ，$1 \leqslant k \leqslant N$，$\Delta f_{k,P}(P_{k,1},..., P_{k,}n_{p)} \geq Thresh_{k,P}$，其中 $\Delta f_{k,P}= f_{k,P}(P_{k,1}(t), ... ,P_{k,}n_p(t))-f_{k,p}(P_{k,l}(t-\Delta t),\ldots,P_{k,}n_p(t-\Delta t))$，则事件被触发。

在一个实施例中， $t-\Delta t$ 是最近一次利用参数进行评估的时间。

参见上面针对这里所用的一些参数的欺诈接入点确定的讨论。

3．诸如发送定时或者数据路径损耗之类的 RF 参数/行为可以被用来触发事件。参见上面针对路径损耗改变的讨论。类似地，函数和阈值改变可以被设计来触发作为来自邻近 AP 的发送定时的函数的重分类。例如，参见 2004 年 3 月 18 日提交的共同转让美国专利申请 No. 10/803,367，该申请发明人为 Crawford 等，题为 RADIOLOCATION IN A WIRELESS NETWORK USING TIME DIFFERENCE OF ARRIVAL，该发明描述了一种接入点，该接入点包括用于确定从邻近接入点到达该接入点的时间的方法。美国专利申请 No. 10/803,367 的内容通过引用结合于此。

再次假设在 AP 数据库中存在 N 个已知的 AP，并且假设特定 AP 是第 k 个 AP，$1 \le k \le N$。用 $T_{k,i}(t)$表示在表示为 t 的某一时刻从第 i 个 AP 到第 k 个 AP 的发送时刻，$k \ne i$，$1 \le k,i \le N$，并且考虑从较早时刻（$t-\Delta t$）的改变。在一个实施例中，检测出发送时间的表示为 $f_{k,T}(T_{k,1}(t),\ldots,T_{k,N}(t))$的函数的比表示为 $Thresh_{k,T}$ 的量大的改变。注意，如果，

对于任意的 k，$1 \leqslant k \leqslant N$，$\Delta f_{k,T}(T_{k,1},\ldots, T_{k,N}) \ge Thresh_{k,T}$，其中 $\Delta f_{k,T}(T_{k,1},\ldots,T_{k,N})=f_{k,T}(T_{k,1}(t),\ldots,T_{k,N}(t))-f_{k,T}(T_{k,1}(t-\Delta t),\ldots,T_{k,N}(t-\Delta t))$，则事件被触发。

在一种实施例中，$t-\Delta t$ 是最近一次利用发送时间进行评估的时间。

4．检测新的网络地址改变或者 AP 的数据帧的改变可以触发事件。

5．已知诸如 WLAN 管理器 103 之类的 WLAN 管理器中的网络管理软件包括用于发现接入点的有线发现方法。例如，已知利用 Cisco 发现协议（来自 Cisco Systems，Inc.，San Jose，California 的“CDP”）的“线内（in the wire）”检测和其他有线侧发现方法。一般而言，一种或多种协议被用来检测 LAN 中连接的设备，包括 SNMP、Telnet、Cisco 发现协议（Cisco Systems，Inc.，San Jose，California），等等。有线侧发现方法的组合非常可靠，并且证明其可以检测出 WLAN 中任何位置处的 AP，而不管其物理位置。重分类可以在新 AO 这样被发现时发生。

6．在 AP 先前位于已知位置的情形中检测显著位置改变可以触发重分类。许多 WLAN 管理器，例如，WLAN 管理器 103 包括基于一种或多种

方法的位置确定方法。例如，参见上述题为“RADIOLOCATION USING A PATH LOSS DATA”的美国专利申请 No. 10/629,384，该申请公开了一种利用路径损耗的方法。还参见上述题为 RADIOLOCATION IN A WIRELESS NETWORK USING TIME DIFFERENCE OF ARRIVAL 的美国专利申请 No. 10/803,367。

再次假设在 AP 数据库中存在 N 个已知的 AP，并且假设特定 AP 是第 k 个 AP，$1 \le k \le N$。用 $X_k(t)$表示在时刻 t 处所确定的第 k（$1 \le k \le N$）个 AP 的位置，并且考虑从较早时间（$t-\Delta t$）的改变，在一个实施例中，检测出表示为 $f_{k,X}(X_k)$的（一个或多个）位置的函数比表示为 $Thresh_{k,X}$ 的量大的改变。即，如果，

对于任意的 k，$1 \leqslant k \leqslant N$，$\Delta f_{k,X}(X_k) \geq Thresh_{k,X}$，其中 $\Delta f_{k,X}(X_k) = f_{k,X}(X_k(t))-f_{k,X}(X_k(t-\Delta t))$，则事件被触发。

在替换实施例中，位置改变被结合到包括这种设施的那些 AP 中的路径损耗和/或发送时间的函数中。

在替换实施例中，不是函数改变被检测到，而是特定值的改变的函数被检测到。例如，在位置的情形中，再次用 $X_k(t)$表示在时刻 t 处所确定的第 k 个 AP 的位置，$1 \leqslant k \leqslant N$，并且考虑从较早的时间（$t-\Delta t$）的改变。在一个实施例中，位置改变的函数被估计。由 $\Delta X_k(t)$表示从时刻 $t-\Delta t$ 到 ti 的改变，例如，$\Delta X_k(t)=X_k(t)-X_k(t-\Delta t)$。考虑函数 $F_{k,X}(\Delta X_k(t))$，并且令 $Thr_{k,X}$ 为阈值。则，如果，

对于任意的 k，$1 \leqslant k \leqslant N$，$F_{k,X}(\Delta X_k) \geq Thr_{k,X}$，则事件被触发。

注意，一些检测标准是可以被配置来实时发生的测量值，例如，在一些配置中是位置改变，而其他可以在调度的时间发生，例如，AP 有线网络位置和地址的“线内”重发现。在一种实施例中，重分类既利用实时变化参数实时发生也可以按照调度时间在调度估计之后发生。

为了有助于减少这种方法可能存在的错误确定的程度，本发明还利用 AP 分类的汇聚“信任水平”。因此，对于 N_C 个标准（其中每一个都是根据对于标准 C_j（$1 \leqslant j \leqslant Nc$）表示为 $f_{k,j}(\ )$的各个函数的改变（该改变表示为 $\Delta f_{k,j}(\ )$）所确定的），对于一组 N 个 AP 中的第 k 个 AP（$1 \leqslant k \leqslant N$）的汇

聚信任水平 Q_k，该汇聚信任水平是函数：

$$Q_k = \sum_{j=1}^{N_c} \alpha_{k,j} \Delta f_{k,j}(.), 1 \le k \le N$$

其中，$\alpha_{k,j}$，$1 \le j \le N_C$ 表示对于对重分类触发作出贡献的第 k 个接入点，用于每个独立的基于参数的函数的加权值。$\alpha_{k,j}$，$1 \le j \le N_C$，$1 \le k \le N$ 包括使 fk,j( )函数具有相同比例和单位所要求的任何缩放。表示为 $Thresh_{k,Q}$ 的阈值是针对第 k 个 AP 定义的，并且因此在一个实施例中，对于一组 N 个 AP 中的第 k 个 AP，$1 \le k \le N$，如果，

对于任意的 k，$1 \leqslant k \leqslant N$，$Q_k = \sum_{j=1}^{N_c} \alpha_{k,j} \Delta f_{k,j}(.) \ge Thresh_{k,Q}$，则重分类被触发。

这种加权方法通过改变加权方案，例如，对于被分类/发现/重分类为可能的欺诈 AP 的 AP（即，对于 k 的多个值）随时间改变$\alpha_{k,j}$，$1 \le j \le N_C$，的值，从而可以降低“错误确定”的可能性。即，用来确定汇聚信任水平的加权值取决于接入点的最近分类。这种重分类被用户执行为友好的，即使在生成调整的新条件下也如此。即，一些自校正方面被内建到动态分类中，使得不同的测量值可以针对在 AP 分类中它们的预测的成功率而被加权。

应当理解，尽管在 IEEE 802.11 标准的上下文中描述了本发明，但是本发明不限于这种上下文，并且可以被用在各种其他应用和系统中，例如在遵循其他标准并且用于其他应用的其他无线网络中，包括例如其他 WLAN 标准和其他无线网络标准。可以包含的应用包括 IEEE 802.11 无线 LAN 和链路、无线以太网、HIPERLAN 2、欧洲技术标准协会（ETSI）宽带无线接入网（BRAN）、以及多媒体移动接入通信（MMAC）系统、无线局域网、本地多点分布式服务（LMDS）IF 带、无线数字视频、无线 USB 链路、无线 IEEE 1394 链路、TDMA 分组频率器件、低成本点对点链路、语音 IP 便携式“蜂窝电话”（无线因特网电话），等等。

这里所述的方法在一个实施例中可由包括一个或多个处理器的机器执行，所述处理器接受包含指令的代码段。对于这里所述的任意方法，在指令被该机器执行时，该机器执行该方法。能够执行指定要由机器执行的动作的一组指令（顺序的或者其他）的任何机器都被包括进来。因此，一种

典型的机器可由包括一个或多个处理器的典型的处理系统简化。每个处理器可以包括 CPU、图形处理单元和可编程 DSP 单元中的一个或多个。处理系统还可以包括存储器子系统，存储器子系统包括主 RAM 和/或静态 RAM 和/或 ROM。还可以包括用于在组件之间通信的总线子系统。如果处理系统要求显示器，则可以包括这种显示器，例如，液晶显示器（LCD）或阴极射线管（CRT）显示器。如果要求手工数据输入，则处理系统也可以包括输入设备，例如，诸如键盘之类的字母数字输入单元、诸如鼠标之类的点选控制设备等等中的一种或多种。这里所使用的术语存储器单元也包括诸如盘驱动单元之类的存储系统。在某些配置中，处理系统可以包括声音输出设备，以及网络接口设备。存储器子系统因此包括载波介质，载波介质承载包括用于在由处理系统执行时执行这里所述的方法中的一个或多个的指令的机器可读代码段（例如，软件）。软件可以存储在硬盘中，或者可以完全或至少部分存储在 RAM 中和/或在计算机系统对其进行执行时存储在处理器中。因此，存储器和处理器也组成承载机器可读代码的载波介质。

在替换实施例中，机器作为单独的设备工作，或者可以被连接（例如联网）到联网布署的其他机器，机器可以在服务器-客户端台站网络环境中作为服务器或者客户端台站工作，或者作为对等或分布式网络环境中的对等机器工作。机器可以是个人计算机（PC）、平板电脑、机顶盒（STB）、个人数字助理（PDA）、蜂窝电话、web 设备、网络路由器、交换机或网桥、或者能够执行一组指令（顺序的或者其他的）的任何机器，其中所述指令指定要由该机器执行的动作。

注意，尽管一些（个）图仅示出了单个处理器和存储代码的单个存储器，但是，本领域技术人员将理解上述许多组件被包括在其中，尽管为了避免模糊了创造性方面而未明确地示出或者描述。例如，尽管仅示出了单个机器，但是术语“机器”还应当被理解为包括独立或联合执行一组（或者多组）指令来实现这里所述的方法中的任意一种或多种的机器的任何集合。

因此，这里所述的方法中的每种的一个实施例处于在处理系统上执行

的计算机程序的形式，所述处理系统例如是作为接入点和/或 WLAN 管理器的一个或多个处理器。因此，本领域技术人员将理解，本发明的实施例可以被实现为方法、诸如专用装置之类的装置、诸如数据处理系统之类的装置，或者载波介质，例如，计算机程序产品。载波介质承载用于控制处理系统来实现方法的一段或多段计算机可读代码段。因此，本发明的多个方面可以采用以下形式：方法、完全硬件实施例、完全软件实施例，或者组合了软件和硬件方面的实施例。此外，本发明还可以采用承载在介质中实现的计算机可读程序代码段的载波介质（例如，计算机可读存储介质上的计算机程序产品）的形式。

软件还可以经由网络接口通过网络被发送或接收。尽管在示例性实施例中载波介质被示作单个介质，但是术语“载波介质”应当被理解为包括存储一组或多组指令的单个介质或多个介质（例如，集中式或分布式数据库，和/或关联缓存和服务器）。术语“载波介质”还应当被理解为包括能够存储、编码或承载由机器执行并且使该机器实现本发明的任意一种或多种方法的一组指令。载波介质可以采用多种形式，包括但不限于非易失性介质、易失性介质和传输介质。非易失性介质包括例如光、磁盘，以及磁光盘。易失性介质包括动态存储器，例如，主存储器。传输介质包括同轴线缆、铜缆和光纤，包括包含总线子系统在内的线路。传输介质也可以采用声波或光波的形式，例如，在无线电波和红外数据通信期间生成的那些。例如，术语“载波介质”因此应当被理解为包括但不限于固态存储器、光和磁介质，以及载波信号。

应当理解，这里所讨论的方法步骤在一个实施例中是由执行存储设备中存储的指令（代码段）的处理（即，计算机）系统的合适的处理器（或者多个处理器）执行的。还应当理解，本发明不限于任何具体的实现方式或者编程技术，并且本发明可以用实现这里所述的功能的任何合适的技术实现。本发明不限于任何具体的编程语言或操作系统。

在整个说明书中，提到“一个实施例”或“实施例”意思是结合在本发明的至少一个实施例中包括的实施例描述的特定特征、结构或特性。因此，在整个说明书中多个地方出现术语“在一个实施例中”或“在实施例

中”不一定全指同一个实施例。此外，特定特征、结构或特性在一个或多个实施例中可以以任何适当的方式被组合，本领域技术人员从本公开将清楚此点。

类似地，应当理解，在上面对本发明的示例性实施例的描述中，本发明的各种特征有时被一起分组到单个实施例、附图或者其描述中，以使公开流畅并且有助于对各个创造性方面中的一个或多个的理解。但是，本公开的该方法不应当被解释为反映出这样的意图：所要求的发明要求比在每项权利要求中明确引用的特征多的特征。相反，如下面的权利要求书所反映的，创造性方面在于比前面公开的单个实施例的全部特征少的特征。因此，具体实施方式之后的权利要求书因此而被明确地结合到具体实施方式中，其中每项权利要求自身作为本发明的一个独立的实施例。

此外，尽管这里所述的一些实施例包括其他实施例中包括的一些特征而不是其他特征，但是不同实施例的特征的组合也在本发明的范围内，并且形成不同的实施例，本领域技术人员将理解这一点。例如，在所附权利要求书中，所要求的实施例中的任意实施例可以以任何组合方式被使用。

此外，一些实施例在这里被描述为可由计算机系统的处理器或者由实现功能的其他装置实现的方法或者方法的元素的组合。因此，利用必要的指令用于实现这种方法或方法的元素的处理器形成用于实现该方法和方法的元素的装置。此外，这里所述的装置实施例的元素是用于实现由该元素实现的用于实现本发明的功能的装置的示例。

这里所使用的“IEEE 802.11 标准的变体”意思是 IEEE 802.11 标准的变体或提议的变体。变体是在标准的语句或者对标准的提议修改中定义的版本。

注意，接入点在不同的上下文中也被称作基站和小区台。

这里所引用的所有公开、专利和专利申请都通过引用从而被结合进来。

在所附权利要求书和这里的描述中，术语“包含”、“组成”或者“其包含”中的任意一个都是开放式术语，意思是至少包括所跟随的元素和/或特征中但是不排除其他。因此，术语“包含”在权利要求中被使用时

不应当被解释为对其后列出的装置或元素或步骤的限制。例如，语句“一种设备包含 A 和 B”的范围不应当被限制为仅由元件 A 和 B 组成的设备。这里所使用的术语 “包括”或者“其包括”也是开放式术语，意思是至少包括跟随该术语的元素/特征，但是不排除其他。因此，包括是具有的同义词，意思是包含。

类似地，应当注意到，术语“耦合”在被用在权利要求中时不应当被解释为仅限于直接连接。因此，语句“设备 A 耦合到设备 B”的范围不应当被限于其中设备 A 的输出被直接连接到设备 B 的输出的设备或系统。其意思是在 A 的输出和 B 的输入之间存在一条路径，该路径可以是包括其他设备或装置的路径。

因此，尽管描述了本发明的优选实施例，但是本领域技术人员将认识到在不脱离本发明的精神的情况下，可以对其作出其他和进一步的修改，并且是要要求落入本发明的范围内的所有这种改变和修改。例如，上面给出的任何公式都仅是可以使用的过程的代表。功能可以被添加到框图或者从框图删除，并且操作可以在功能块之间互换。步骤可以被添加到在本发明的范围内描述的方法，或者从这些方法删除。

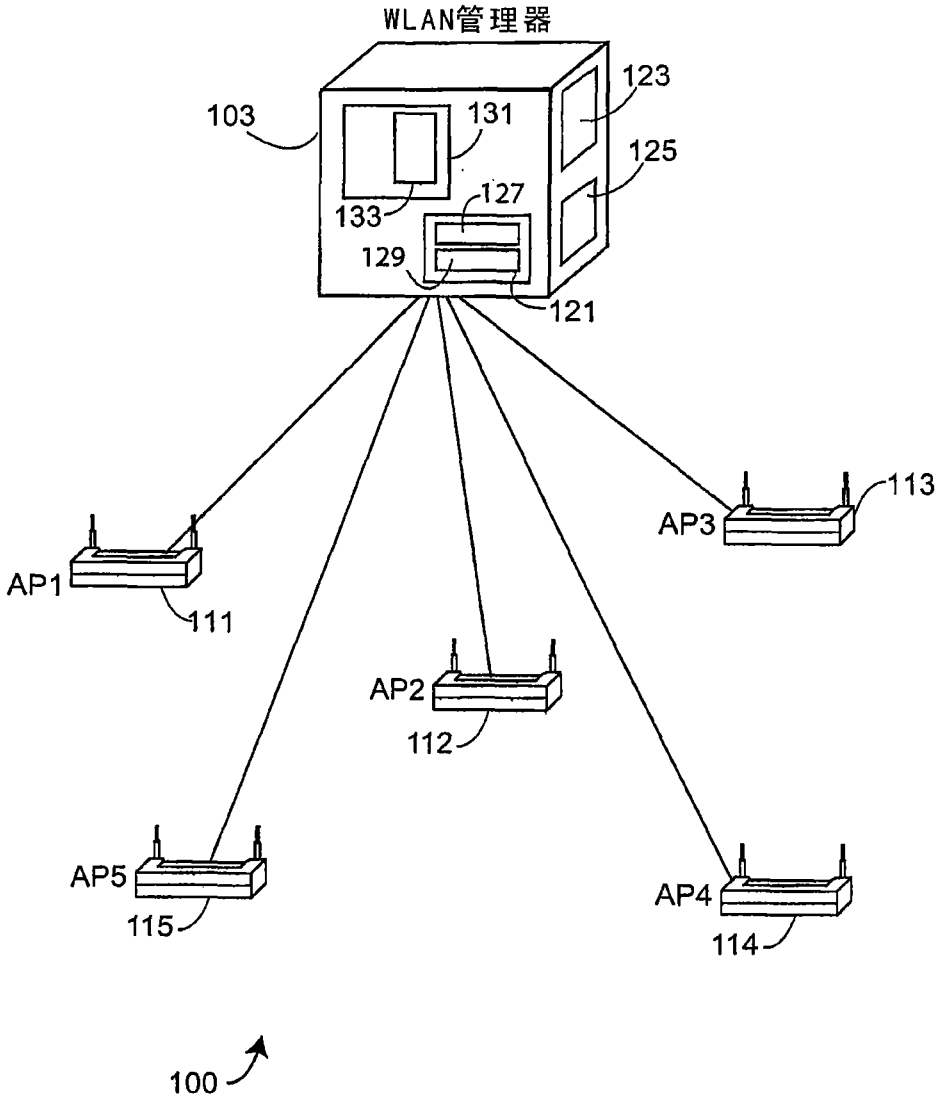

WLAN管理器
103
131
123
125
133
127
129
121
AP1
111
AP2
112
AP3
113
AP4
114
AP5
115
100

图1

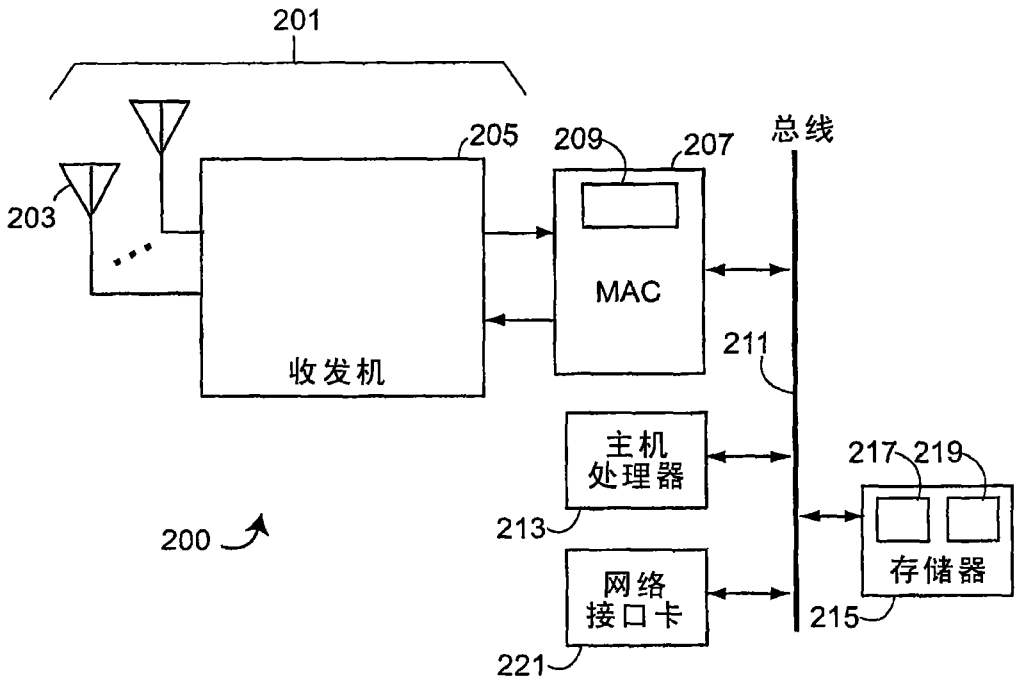

201
205
209
207
总线
203
MAC
收发机
211
主机
处理器
217
219
200
213
网络
接口卡
存储器
215
221

图2

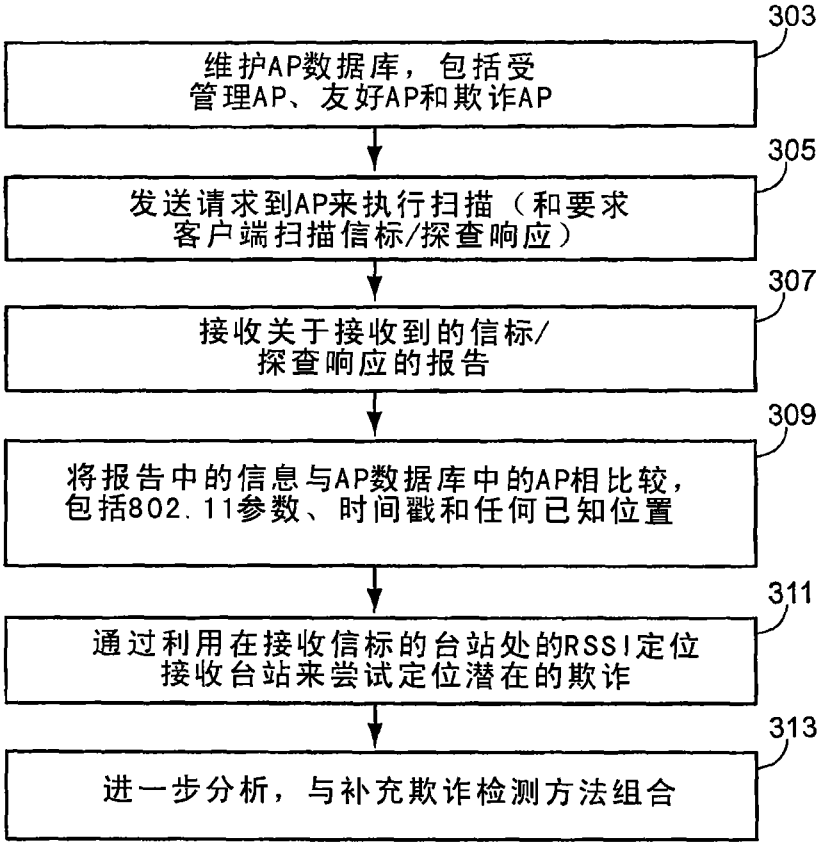

303
维护AP数据库，包括受管理AP、友好AP和欺诈AP
305
发送请求到AP来执行扫描（和要求客户端扫描信标/探查响应）
307
接收关于接收到的信标/探查响应的报告
309
将报告中的信息与AP数据库中的AP相比较，包括802.11参数、时间戳和任何已知位置
311
通过利用在接收信标的台站处的RSSI定位接收台站来尝试定位潜在的欺诈
313
进一步分析，与补充欺诈检测方法组合

图3

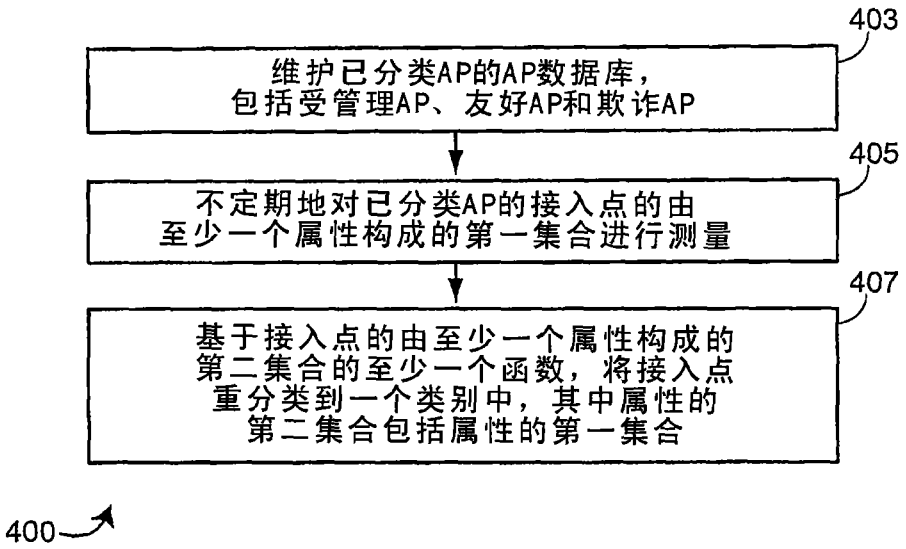

403
维护已分类AP的AP数据库，
包括受管理AP、友好AP和欺诈AP
405
不定期地对已分类AP的接入点的由
至少一个属性构成的第一集合进行测量
407
基于接入点的由至少一个属性构成的
第二集合的至少一个函数，将接入点
重分类到一个类别中，其中属性的
第二集合包括属性的第一集合
400

图4