[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/20 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200480031433.8

[43] 公开日 2008 年 8 月 13 日

[11] 公开号 CN 101243697A

[22] 申请日 2004.10.28
[21] 申请号 200480031433.8
[30] 优先权
[32] 2003.10.31 [33] US [31] 10/699,257
[86] 国际申请 PCT/US2004/035714 2004.10.28
[87] 国际公布 WO2005/046254 英 2005.5.19
[85] 进入国家阶段日期 2006.4.24
[71] 申请人 讯宝科技公司
地址 美国纽约州
[72] 发明人 J·莎洛尼

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 钱慰民

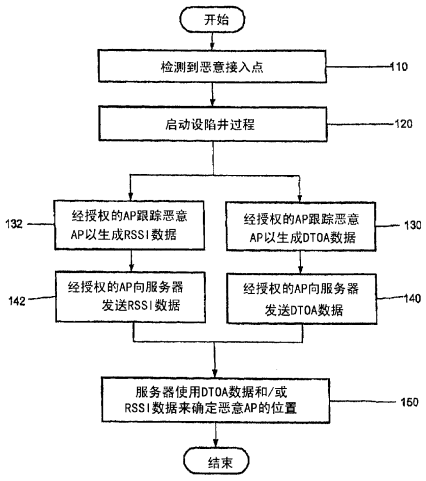
权利要求书 4 页 说明书 6 页 附图 2 页

[54] 发明名称

确定恶意无线接入点的位置的系统和方法

[57] 摘要

一种使用第一无线频带和第二无线频带的无线通信的系统。该系统包括第一双频带无线收发机和智能天线，该第一设备使用智能天线在第一频带上排它地单向发射负荷数据，而无须在发射前就保留第一频带，该系统还包括至少一个包括第二双频带无线收发机的第二无线设备，该第二设备使用第一和第二频带中的至少一个，通过全向地发射确认数据来确认负荷数据的接收。



1．一种确定访问通信网络的未经授权的无线接入点（“AP”）的位置的方法，包括：

一经通知所述未经授权的 AP 的存在，就使用所述通信网络的至少三个经授权的 AP 来跟踪所述未经授权的 AP 的信标；

部分地基于在所述跟踪步骤中所获得的信息来生成跟踪数据记录，所述跟踪记录包括每个所述经授权的 AP 的位置、以及以下各项中的至少一个：(i)对应于由每个所述经授权的 AP 测量的所述跟踪信标的强度的第一强度数据，以及(ii)对应于所述跟踪信标到达每个所述经授权的 AP 所花的时间周期的第一时间数据；以及

根据以下各项中的至少一个来确定所述未经授权的 AP 的位置：(i)所述跟踪记录，以及(2)校准记录，所述校准记录包括：(a)对应于从所述通信网络内的预定位置发送、并由每个所述经授权的 AP 接收的校准信标的强度的第二强度数据，和对应于所述校准信标从所述预定位置到达每个所述经授权的AP所花的时间周期的第二时间数据中的至少一个，(b)所述预定位置，以及(c)每个所述经授权的 AP 的位置。

2．如权利要求 1 所述的方法，其特征在于，当所述跟踪记录包括所述第一强度数据时，所述确定步骤包括根据所述第一和第二强度数据来计算所述未经授权的 AP 的位置的子步骤。

3．如权利要求 1 所述的方法，其特征在于，当所述跟踪记录包括所述第一时间数据时，所述确定步骤包括以下各项中的至少一个：(i)使用所述第一时间数据对所述未经授权的 AP 的精确位置进行三角测量的子步骤，以及(ii)根据所述第一和第二时间数据来计算所述未经授权的 AP 的位置的子步骤。

4．如权利要求 1 所述的方法，其特征在于，还包括：

在所述跟踪步骤之前，执行包括以下各子步骤的校准过程：

将校准设备放在所述通信网络内的多个预定位置，

使用每个所述经授权的 AP 来跟踪来自所述校准设备的所述校准信标，以及

基于在所述跟踪子步骤中生成的数据来生成所述校准记录。

5．如权利要求 1 所述的方法，其特征在于，还包括：

用每个所述经授权的 AP 的位置、以及所述确定步骤的结果覆盖所述通信网络的地理地图。

6．如权利要求 1 所述的方法，其特征在于，所述跟踪记录包括所述未经授权的 AP 的 MAC 地址。

7．如权利要求 1 所述的方法，其特征在于，所述跟踪步骤包括根据所述经授权的 AP 的地理位置，从所述通信网络的多个可用的经授权的 AP 中选择所述至少三个经授权的 AP 的子步骤。

8．如权利要求 1 所述的方法，其特征在于，还包括：

在所述生成步骤之后，将所述跟踪记录存储在每个所述经授权的 AP 的存储器装置中；以及

向所述通信网络的计算机提供所述跟踪记录，

其中所述确定步骤是由所述计算机执行的。

9．一种用于确定访问通信网络的未经授权的无线接入点（“AP”）的位置的系统，包括：

多个经授权的 AP；以及

计算装置，

其中一经通知所述未经授权的 AP 的存在，所述多个经授权的 AP 中的至少三个经授权的 AP 即跟踪所述未经授权的 AP 的信标，所述至少三个经授权的 AP 生成包括每个所述经授权的 AP 的位置、以及以下各项中的至少一个的跟踪数据记录：(i)对应于每个所述经授权的 AP 所测量的所述跟踪信标的强度的第一强度数据，以及(ii)对应于所述跟踪信标到达每个所述经授权的 AP 所花的时间周期的第一时间数据，以及

其中所述计算机根据所述跟踪记录、以及校准数据记录来确定所述未经授权的 AP 的精确位置，所述校准记录包括：(a)以下各项中的至少一个；(i)对应于从所述通信网络内的预定位置发送、并由每个所述经授权的 AP 接收的校准信标的强度的第二强度数据，以及(ii)对应于所述校准信标从所述预定位置到达每个所述经授权的 AP 所花的时间周期的第二时间数据，(b)所述预定位置，以及(c)每个所述经授权的 AP 的位置。

10．如权利要求 9 所述的系统，其特征在于，还包括：

发送所述校准信标的校准设备，所述校准设备包括无线发射器。

11．如权利要求 10 所述的系统，其特征在于，所述校准设备是无线移动设备

和 AP 中的一种。

12. 如权利要求 9 所述的系统，其特征在于，当所述跟踪记录包括所述第一强度数据时，所述计算装置根据所述第一和第二强度数据来计算所述未经授权的 AP 的位置。

13. 如权利要求 9 所述的系统，其特征在于，当所述跟踪记录包括所述第一时间数据时，所述计算装置包括以下各项中的至少一个(i)使用所述第一时间数据来对所述未经授权的 AP 的精确位置进行三角测量，以及(ii)根据所述第一和第二时间数据来计算所述未经授权的 AP 的位置。

14. 如权利要求 9 所述的系统，其特征在于，所述计算装置用每一个所述经授权的 AP 和未经授权的 AP 的位置来覆盖所述通信网络的地理地图。

15. 如权利要求 9 所述的系统，其特征在于，所述跟踪记录包括所述未经授权的 AP 的 MAC 地址。

16. 如权利要求 9 所述的系统，其特征在于，所述计算装置从所述多个经授权的 AP 中选择所述至少三个经授权的 AP，以根据每个所述经授权的 AP 的位置来跟踪所述未经授权的 AP。

17. 如权利要求 9 所述的系统，其特征在于，所述跟踪记录位于每个所述经授权的 AP 的存储器装置中，所述跟踪记录在以下各种情况中的一种发生时被提供给所述计算装置，(i)预定时间周期到期，以及(ii)有来自所述计算装置的请求。

18. 如权利要求 9 所述的系统，其特征在于，当所述计算装置确定所述未经授权的 AP 的存在时，所述计算装置指令所述至少三个经授权的 AP 启动对所述未经授权的 AP 的信标的跟踪。

19. 一种用于确定访问通信网络的未经授权的无线接入点（“AP”）的位置的计算设备，包括：

存储校准数据记录的存储器装置；

与所述经授权的 AP 通信的通信装置；以及

根据跟踪数据记录和所述校准数据记录中的至少一个来确定所述未经授权的 AP 的精确位置的处理器，

其中所述跟踪记录是由多个经授权的 AP 中的至少三个经授权的 AP 在对所述未经授权的 AP 的跟踪期间生成的，所述数据记录包括每个经授权的 AP 的位置、以及以下各项中的至少一个：(i)对应于每个所述经授权的 AP 所测量的跟踪信标的强度的第一强度数据，以及(ii)对应于所述跟踪信标到达每个所述经授权的 AP 所花

的时间周期的第一时间数据，并且

其中所述校准记录包括：(a)以下各项中的至少一个：(i)对应于从所述通信网络内的预定位置发送、并由每个所述经授权的 AP 接收的校准信标的强度的第二强度数据，以及(ii)对应于所述校准信标从所述预定位置到达每个所述经授权的 AP 所花的时间周期的第二时间数据，(b)所述预定位置，以及(c)每个所述经授权的 AP 的位置。

确定恶意无线接入点的位置的系统和方法

技术领域

背景技术

随着无线网络的激增，许多组织（例如，企业、大学、医院等等）在有线网络以外，或作为其替换而安装了或准备安装无线网络。此类无线网络据信将提高效率和生产率。但是，无线网络的缺点之一是此类网络的安全性。与通常被包含在组织安全的和受保护的建筑物内的有线网络不同，无线网络的单元（例如，无线接入点[“AP”]）可能分散遍及组织的建筑物。

对无线网络安全的一个主要威胁是恶意 AP。恶意 AP 是允许第三方在没有组织许可的情况下访问组织的网络的未经授权的 AP。例如，恶意 AP 可能是出于恶意目的（例如，获得对存储在网络上的组织的数据的访问）而安装的。利用恶意 AP 的另一个示例是威胁较小的情形：组织的成员（例如，雇员）可能在没有正确授权的情况下将恶意 AP 连接到组织的网络。换言之，该雇员可能被授权使用组织的网络，但该特定 AP 的使用可能是未经授权的。例如，如果雇员决定使用他个人的 AP 以便更方便地访问组织的网络，就可能会发生这种情况。如果 AP 没有被正确配置成向未经授权的用户提供安全访问，则使用兼容硬件的未经授权的用户也可获得对网络的访问。这在 AP 覆盖组织建筑物以外的物理区域时可能尤其需要考虑。由此，未经授权的用户无需物理地进入组织的建筑物即可访问网络。

为解决恶意 AP 的威胁，网络管理员监视网络上的通信。但是，一旦检测到恶意 AP，问题就是要定位此恶意 AP 以便将其移除。寻找恶意 AP 可能是困难的任务，因为 AP 可能被隐藏在组织建筑物里的任何地方。例如，恶意 AP 可能被隐藏在天花板下或者墙壁后。因此，需要一种在组织的建筑物内以高精度（例如，在两英尺内）确定恶意 AP 的特定位置的系统和方法。

发明概述

本文描述一种确定正在访问通信网络的未经授权的无线接入点（“AP”）的位置的方法和系统。一经通知未经授权的 AP 的存在，该通信网络的至少三个经授

权的 AP 即启动对未经授权的 AP 的信标的跟踪。

部分地基于在跟踪信标的跟踪期间所获得的信息来生成跟踪数据记录。跟踪记录可包括每个经授权的 AP 的位置，以及以下各项中的至少一个，(i)对应于由每个经授权的 AP 测量的跟踪信标的强度的第一强度数据，以及(ii)对应于跟踪信标到达每个经授权的 AP 所花的时间周期的第一时间数据。根据以下各项中的至少一个来确定未经授权的 AP 的位置，(i)跟踪记录，以及(ii)校准记录。校准记录可包括(a)对应于从通信网络内的预定位置发射、并由每个经授权的 AP 接收的校准信标的强度的第二强度数据、以及对应于校准信标从预定位置到达每个经授权的 AP 所花的时间周期的第二时间数据这两者中的至少一个，(b)预定位置，以及(c)每个经授权的 AP 的位置。

附图简述

图 1 示出根据本发明的系统的示例性实施例；以及

图 2 示出根据本发明的方法的示例性实施例。

详细描述

图 1 示出无线网络的示例性实施例，特别地，示出根据本发明的无线局域网（“WLAN”）100。WLAN 100 可包括多个经授权的接入点（“AP”）10、20 和 30。WLAN 100 还可包括多个经授权的移动单元 MU（例如，MU 1 – 5），以及至少一个服务器（例如，服务器 70）。AP 10 – 30 可被直接连接到服务器 70。WLAN 100 包括数据库 82，它存储关于经授权的设备、经授权的用户、该 WLAN 的器材的位置等数据。数据库 82 还可包括关于被明确禁止访问 WLAN 100 的设备的标识信息。

MU 1 经由 AP 10 – 30 来访问 WLAN 100 的各个器材。根据 MU 1 在特定时间位于何处，MU 1 可经由最靠近的 AP 来访问 WLAN 100。每个 AP 周期性地发送信标信号，它们可被用来确定最靠近的 AP。例如，MU 1 可确定 AP 20 是最靠近的 AP。因此，MU 1 经由 AP 20 建立与 WLAN 100 的无线通信，而不是经由 AP 10 或 AP 30。

如果 MU 1 的用户试图访问服务器 70，则 MU 1 首先等待到 AP 20 的通信信道可用。一旦该通信信道可用，MU 1 即向 AP 20 发送认证消息，以请求访问 WLAN 100。认证消息可包含用户的标识数据（例如，登录名称和密码）。当 AP 20 接收

到来自 MU 1 的认证消息时，它启动认证过程。认证过程可包括将从用户接收的标识数据针对存储在数据库 82 中的数据的验证。如果标识数据未能通过验证，则 MU 1 将被拒绝访问 WLAN 100。但是，如果标识数据通过验证，则 AP 20 发送对应的响应，以授权 MU 1 访问 WLAN 100。一旦 MU 1 接收到授权，MU 1 即可经由 AP 20 访问 WLAN 100。例如，MU 1 的用户随即可访问服务器 70。

未经授权的用户可能想要获得 WLAN 100 的访问，尤其是利用未经授权的、或恶意的 AP 60 来访问服务器 70。恶意 AP 60 可被配置成在批准访问 WLAN 100 之前检查其驻留数据库。由未经授权的用户配置的 AP 60 的驻留数据库可包含例如该未经授权的用户的登录名称和/或密码。或者，恶意 AP 60 可被配置成不对来自认证消息的标识数据进行验证即批准访问。恶意 AP 60 由此可提供恶意 MU 6 对 WLAN 100 的访问。

未经授权的用户可使用 MU 6 经由恶意 AP 60 来访问服务器 70。MU 6 向恶意 AP 60 发送认证消息，恶意 AP 60 被未经授权的用户配置成允许 MU 6 访问 WLAN 100。未经授权的用户可通过以和经授权的用户相同的方式登录来获得对服务器 70 的访问。

图 2 示出根据本发明的示例性实施例的一种方法，该方法用来以高精度（例如，在两英尺内）确定恶意 AP 60 的位置。该位置，或可在其内定位恶意 AP 60 的特定区域，可关于另一个已知对象或位置（例如，在 Smith Alex 办公室中的打印机的三英尺半径内；在接待区 – 靠近门等）来确定。参考图 1 来描述该方法。本领域技术人员将会理解，具有不同配置，例如不同个数的 AP、WLAN 或 MU 的其它系统可被用来实现该示例性方法。

在步骤 110，恶意 AP 60 被检测到，并被标识为未经授权的 AP。本领域技术人员将会理解，恶意 AP 60 的检测能以各种方式来实现。例如，网络管理员可使用嗅闻程序来监视 WLAN 100 上的通信以检测任何恶意 AP。

检测恶意 AP 60 的另一种方法可涉及信标信号。这些信标由每个 AP 周期性地发送。信标信号可包含包括发送 AP 的 MAC 地址、服务集标识（“SSID”）、所支持的数据率等的信息。MAC 地址是由制造商分配的标识符，因此它被用作该 AP 的制造商标识。SSID 标识由特定 WLAN 服务的虚拟局域网（“VLAN”）。VLAN 可包括单个 WLAN（例如，WLAN 100）或多个 WLAN。反之，WLAN 100 可服务多个 VLAN，并且来自与 WLAN 100 相关联的 AP 的特定 AP 信标包含 SSID 的列表。

基于存储在信标信号中的信息，即可确定该信标信号是从经授权的还是未经授权的 AP 接收。这可基于两个示例性准则来确定。这些准则可被替换地或联合地使用，以确定特定 AP 是否未经授权。本领域技术人员将会理解，可能有被用来进行此类确定的多个其它准则。

第一示例性准则是基于发送 AP 的 MAC 地址的制造商标识的验证。将存储在信标信号中的数据与存储在数据库 82 上的数据相比较，数据库 82 包含经授权 AP 的数据。

第二示例性准则是基于使用存储在信标信号中的 SSID 来对照存储在数据库 82 中的经授权的 SSID 的验证。如果使用这一准则，则网络管理员或其它经授权的用户可生成有效 SSID 的列表。因此，如果恶意 AP 60 是由经授权的制造商制造，但该信标中的 SSID 无效，则可检测到恶意 AP 60 的存在。本领域技术人员将会理解，网络管理员还可在经授权 AP 的信标中插入其它代码，这些代码被用来标识经授权/未经授权的 AP。

在步骤 120，一旦确定信标是从未经授权的恶意 AP 60 接收的，即启动“设陷阱”过程。“设陷阱陷阱”过程创建对跟踪恶意 AP 60 可能有用的信息的数据记录。这一数据记录可包括例如，AP 10 的 MAC 和 SSID 地址，以及恶意 AP 60 的 MAC 和 SSID 地址。该数据记录还可包括该数据记录被创建的时间和日期，以及用来检测恶意 AP 60 的准则（例如，未经验证的制造商 MAC 地址、不匹配的 SSID 等）。

在“设陷阱”过程以被启动之后，位于恶意 AP 60 预定的附近范围内的 AP（即，检测到该恶意 AP 的那些 AP）被指令跟踪从恶意 AP 60 发射的信标信号。例如，假定所有 AP 10 – 30 检测到恶意 AP 60，所有 AP 10 – 30 还跟踪被检测到的恶意 AP 60 的信号。

恶意 AP 60 的物理位置可通过使用以下将更加详细讨论的接收信号强度指示（以 dBm 为单位测量的“RSSI”）数据和/或到达时间差（以 ns 为单位测量的“DTOA”）数据来确定。尽管 DTOA 数据或 RSSI 数据单独可能就足以计算恶意 AP 60 的位置。优选的是，同时使用这两个数据集，以提供对恶意 AP 60 的位置最精确的计算。

如果要使用 RSSI 过程，则在设陷阱过程之前，需要执行校准过程。校准过程对于 DTOA 是可选的。校准过程可通过将计算设备（例如，MU 4 或任何 AP）放置在 WLAN 100 内的若干特定位置（即，地标）处来实现。地标可以是接待区、出版室、存储室、服务器室等。在校准过程期间，将生成诸如以下所示的校准数据。

校准表

	AP 10		AP 20		AP 30	
接待区	-10 dBm	4 ns	-20 dBm	3 ns	-30 dBm	2 ns
出版室	-40 dBm	1 ns	-20 dBm	3 ns	-20 dBm	3 ns
存储室	-30 dBm	2 ns	-10 dBm	4 ns	-20 dBm	3 ns
服务器室	-20 dBm	3 ns	-30 dBm	2 ns	-10 dBm	4 ns

校准表示出示例性校正数据，包括由每个 AP10-30 为 WLAN 100 内四个不同的地标记录的 RSSI 数据和 DTOA 数据。特别地，每个 AP 10 – 30 因为每个 AP 10 – 30 与 MU 4 之间不同的距离而获得不同的数据读数。优选重复该校准过程若干次，以获得精确的校准数据。

在步骤 132，AP 10 – 30 可记录并分析信标信号以生成 RSSI 数据。然后该 RSSI 数据可被发送到服务器 70 以进行进一步的分析（步骤 140）。或者，该 RSSI 数据可由对应的 AP 存储，并由服务器 70 周期性地检索，或被周期性地自动转发到服务器 70。用于处理此 RSSI 数据的通信的系统可用常用的简单网络管理协议（“SNMP”）或类似的协议来实现。

为了使用 RSSI 数据来确定恶意 AP 60 的位置，优选的是使用至少三个参考点（即，AP 10 – 30）。三个参考点（例如，AP 10 – 30）标识计算第四个点（即，恶意 AP 60）的位置所需的三维空间（即，WLAN 100 所位于的建筑物）内最少个数的位置。因为恶意 AP 60 不断地发送信标信号，所以 AP 10 – 30 可不断地接收并汇编对应的 RSSI 数据。这一三维空间中仅有一个点与由 AP 10 – 30 从恶意 AP 60 收集的所有三个 RSSI 数据点相关。

还可能用 DTOA 数据，通过对恶意 AP 60 与三个参考点：AP 10 – 30 之间的距离进行三角测量来确定恶意 AP 60 的位置。此外，或替换地，可将 DTOA 数据与校准数据一起使用来确定该位置。在步骤 130，AP 10 – 30 或单独、或与 RSSI 数据结合来生成 DTOA 数据。DTOA 数据可通过处理从恶意 AP 60 接收的信标信号，并测量那些信标信号到达对应 AP 10 – 30 所花的时间来生成。为使用 DTOA 数据来确定恶意 AP 60 的位置，需要至少三个参考点（例如，AP 10 – 30）。

在步骤 150，服务器 70 分析从 AP 10 – 30 接收的 RSSI 和/或 DTOA 数据，并将其与在校准过程期间所生成的 RSSI 数据和/或 DTOA 数据相比较。RSSI 数据和/或 DTOA 数据允许服务器 70 确定恶意 AP 60 与对应的 AP 10 – 30 之间的距离。例如，如果 AP 20 比 AP 30 记录到更强的信号强度，则可能 AP 60 的位置更靠近 AP 20。如果 AP 20 和 AP 30 中的任何一个或两者都使用定向天线，则能以额外的精确性来作出此确定。

RSSI 数据和/或 DTOA 数据为服务器 70 提供充分的距离数据来确定恶意 AP 60 在 WLAN 100 内的位置。换言之，因为服务器 70 有从 RSSI 和/或 DTOA 数据获得的每个 AP 10 – 30 与恶意 AP 60 之间的距离数据，所以它能够计算恶意 AP 60 相对于那些 AP 10 – 30 的位置。确定恶意 AP 60 的位置一种示例性方法如下。首先，使用 RSSI 数据和校准数据来确定恶意 AP 60 的位置。然后，通过用 DTOA 数据进行三角测量来进一步精确定位恶意 AP 60 的位置。

服务器 70 随即可在 WLAN 100 的地图（例如，图 1）上显示计算的结果，并将 AP 10 – 30 覆盖在该地图上，因为 AP 10 – 30 的位置是已知的。可结合该组织建筑物的物理地图（例如，建筑蓝图）来使用 WLAN 100 的地图。

已参考具有 WLAN 100 的实施例描述了本发明，其中 WLAN 100 中有 AP 10 – 30、单个恶意 AP 60、一个经授权的 MU 1 以及服务器 70。本领域技术人员将会理解，对于 WLAN 中的多个恶意 AP、多个 AP 等也可成功地实现本发明。由此，可对这些实施例进行各种修改和改变，而不会偏离如所附权利要求书中所述的本发明最宽泛的精神和范围。由此，应将本说明书和附图视为是示例性而非限制性的。

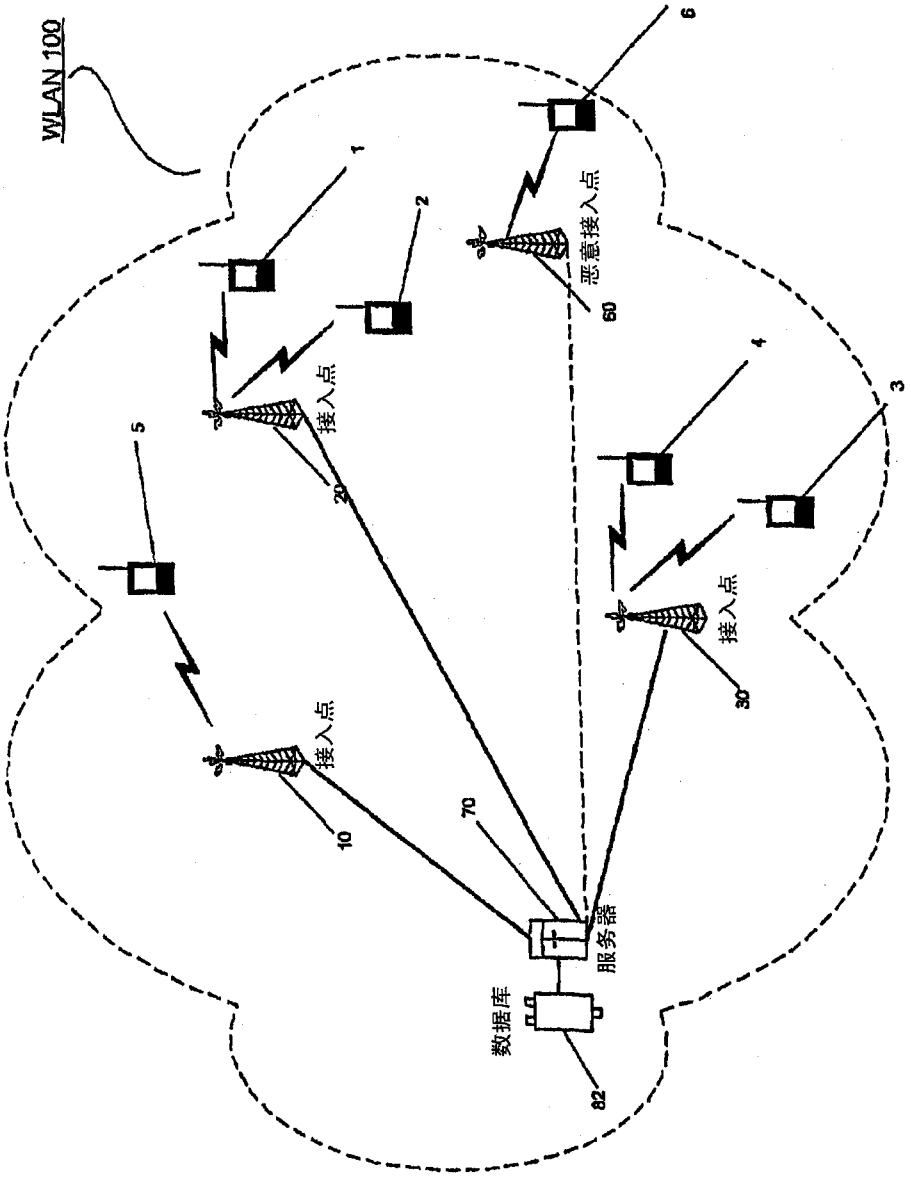


图 1

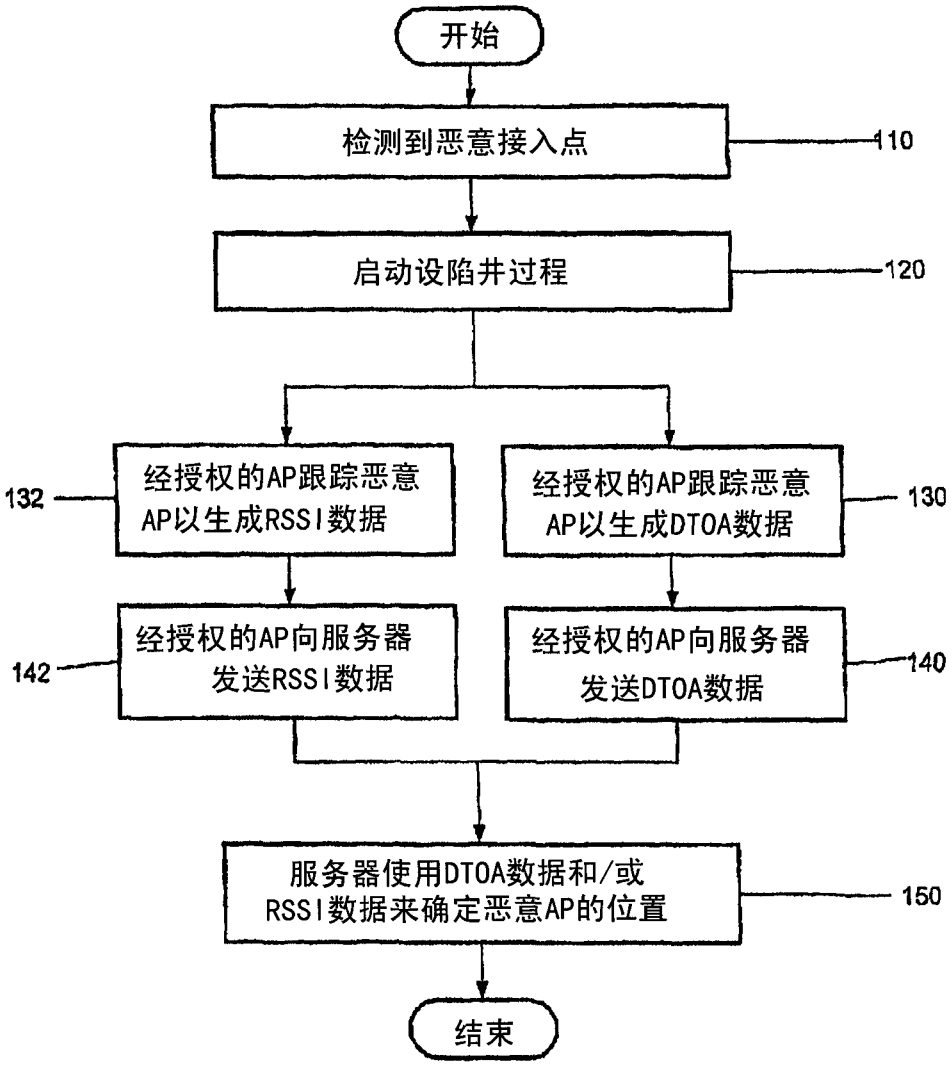

开始
检测到恶意接入点
110
启动设陷井过程
120
经授权的AP跟踪恶意AP以生成RSSI数据
132
经授权的AP跟踪恶意AP以生成DTOA数据
130
经授权的AP向服务器发送RSSI数据
142
经授权的AP向服务器发送DTOA数据
140
服务器使用DTOA数据和/或RSSI数据来确定恶意AP的位置
150
结束

图 2