

(12) 发明专利

(10) 授权公告号 CN 1972520 B

(45) 授权公告日 2012.05.23

(21) 申请号 200610172875.5

[0019]-[0020], [0153] 段.

(22) 申请日 2006.10.08

WO 2005018162 A1, 2005.02.24, 说明书第
[0018], [0107]-[0108] 段.

(30) 优先权数据

11/242,884 2005.10.05 US

审查员 李燕

(73) 专利权人 阿尔卡特公司

地址 法国巴黎

(72) 发明人 J-M·罗伯特 M·巴尔博

(74) 专利代理机构 北京市中咨律师事务所

11247

代理人 杨晓光 李峰

(51) Int. Cl.

H04W 36/08 (2009.01)

H04B 7/26 (2006.01)

(56) 对比文件

US 2005171720 A1, 2005.08.04, 说明书第
[0003], [0070], [0082], [0019], [0091], [0095],
[0096], [0097], [0112], [0114]-[0115] 段、附图
7.

US 2005128989 A1, 2005.06.16, 说明书第

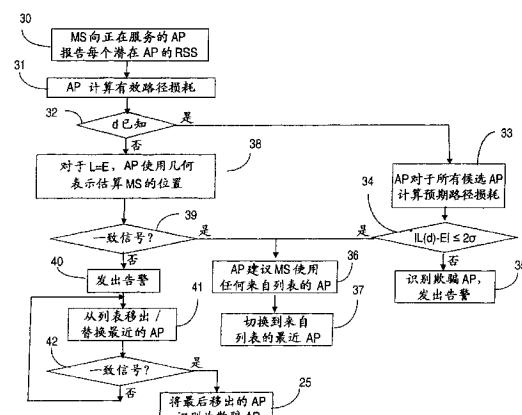
权利要求书 2 页 说明书 9 页 附图 5 页

(54) 发明名称

无线网络中的欺骗接入点检测

(57) 摘要

一种检测欺骗接入点 (AP) 的方法, 该方法防止到通信网所提供业务的未授权无线接入。移动台 (MS) 向正在服务的 AP 报告其移动区域内所有 AP 的信号强度 (RSS)。正在服务的 AP 基于该 RSS 报告中认识到的不一致性检测欺骗 AP, 该 RSS 报告是在切换阶段或者在通信进行的同时估算的。



1. 一种用于移动台 MS 在无线接入网中检测欺骗接入点 AP 的方法,包括:
在所述无线接入网的每个合法 AP 上保持服务区内所有合法 AP 的 AP 数据;
从所述服务区内漫游的所述 MS 请求从正在服务的 AP 切换到所述服务区内候选 AP 列表中的一个;在所述 MS 上,从所有候选 AP 收集 AP 存在信息,并向所述正在服务的 AP 报告所述 AP 存在信息;
计算每个候选 AP 的实际路径损耗值;
确定 MS 和特定候选 AP 之间的距离是否已知,
当距离已知时:计算所述特定候选 AP 的预期路径损耗值;比较所述特定候选 AP 的实际路径损耗值与预期路径损耗值;当实际路径损耗值与预期路径损耗值具有大于阈值的失配时,确定所述特定候选 AP 是欺骗 AP,
当距离不是已知时:在所述正在服务的 AP 上,确定所述 AP 存在信息是否与所述正在服务的 AP 上保持的所述 AP 数据一致;当所述 AP 存在信息和所述 AP 数据不一致时,从候选 AP 列表中随机移出一个候选 AP,并且重复移出步骤直到 AP 存在信息与所述正在服务的 AP 上保持的所述 AP 数据一致;并且将最后移出的候选 AP 识别为欺骗 AP。
2. 如权利要求 1 的方法,其中,对于每个候选 AP,所述 AP 存在信息包括接收信号强度 RSS 数据,该数据与相应 AP 标识 ID 相关。
3. 如权利要求 2 的方法,其中,对于所述服务区内每个候选 AP,所述 AP 数据包括相应 AP 的标识 ID,所述标识与 AP 位置数据和所述相应 AP 的有效各向同性辐射功率 EIRP 值相关。
4. 如权利要求 3 的方法,进一步包括:基于所述特定候选 AP 的相应 RSS 和 EIRP 值计算实际路径损耗。
5. 如权利要求 3 的方法,进一步包括:基于所述特定候选 AP 的相应 RSS 和 EIRP 值计算实际路径损耗;并且基于所述实际路径损耗估计所述 MS 和所述特定候选 AP 的距离。
6. 如权利要求 4 的方法,进一步包括:使用扫描器确定所述距离。
7. 如权利要求 4 的方法,进一步包括:如果所述特定候选 AP 的所述预期路径损耗与所述实际路径损耗一致,建议所述 MS 使用所述特定候选 AP。
8. 如权利要求 5 的方法,进一步包括:确定所述 MS 的假定的当前位置是否与所述 AP 数据一致。
9. 如权利要求 8 的方法,进一步包括:在最小距离和最大距离间估算所述 MS 的所述假定的当前位置。
10. 如权利要求 8 的方法,进一步包括:如果所述 MS 的所述假定的当前位置与所述 AP 数据一致,则建议所述 MS 使用所述候选 AP 的任何一个。
11. 如权利要求 8 的方法,进一步包括:
随机选择候选 AP,并从所述列表移出选择的候选 AP;
确定在不使用移出的候选 AP 的 RSS 值情况下重新计算的所述假定的当前位置是否与所述 AP 数据一致;及
如果所述 MS 的所述假定的当前位置与所述 AP 数据一致,则建议所述 MS 使用除移出的候选 AP 之外的任何候选 AP。
12. 如权利要求 9 的方法,进一步包括:

推选估计的距离等于所述移动台和所述候选 AP 间的实际当前距离的概率；根据所述概率和所述实际路径损耗计算所述最小和最大距离；及对于所有候选 AP，提供所述最小和最大距离的几何表示。

13. 如权利要求 11 的方法，进一步包括：使用所述候选 AP 列表中的另一 AP 替换所述移出的候选 AP。

14. 如权利要求 12 的方法，其中所述几何表示包括多个环面，其中每个候选 AP 位于相应环面的中心，该环面的半径分别等于所述最小和最大距离。

15. 如权利要求 12 的方法，其中所述几何表示包括多个圆盘，其中每个候选 AP 位于相应圆盘的中心，相应圆盘的半径等于所述最大距离。

16. 如权利要求 12 的方法，其中对于装配有扇区化天线的候选 AP，所述几何表示包括多个扇区。

17. 如权利要求 12 的方法，进一步包括：确定所述几何表示是否具有非空交集，所述非空交集表示所述移动台可能位于该交集区域内。

18. 一种用于移动台 MS 在包含合法接入点 AP 的无线接入网内检测欺骗 AP 的方法，包括：

在所述无线接入网的每个合法 AP 上保持邻居数据库，所述邻居数据库包含服务区内所有合法 AP 的 AP 数据；

在所述服务区内漫游的所述 MS 上收集数据集，该数据集包括所述服务区内候选 AP 列表中的 AP 的接收信号强度 RSS 值，并向正在服务的 AP 报告所述数据集；

计算每个候选 AP 的实际路径损耗值；

确定 MS 和特定候选 AP 之间的距离是否已知，

并且当距离已知时：计算所述特定候选 AP 的预期路径损耗值；比较所述特定候选 AP 的实际路径损耗值与预期路径损耗值；当实际路径损耗值与预期路径损耗值具有大于阈值的失配时，确定所述特定候选 AP 是欺骗 AP，

当距离不是已知时：在所述正在服务的 AP 上，确定所述数据集内的 RSS 值是否与所述正在服务的 AP 上保持的所述 AP 数据一致；当所述 RSS 值和所述 AP 数据不一致，从候选 AP 列表中随机移出一个候选 AP，并且重复移出步骤直到 RSS 值与所述正在服务的 AP 上保持的所述 AP 数据一致；并且将最后移出的候选 AP 识别为欺骗 AP。

19. 如权利要求 18 的方法，其中，对于所述服务区内的每个 AP，所述 AP 数据包括相应 AP 的标识 ID，所述标识与 AP 位置数据和相应 AP 的有效各向同性辐射功率 EIRP 相关。

20. 如权利要求 18 的方法，其中，对于所述服务区内的所有 AP，所述数据集包括每个所述 AP 的 ID 和 RSS 值。

21. 如权利要求 18 的方法，进一步包括：如果对于所有路径，所述预期路径损耗值与所述实际路径损耗值一致，则建议所述 MS 使用所述数据集中的候选 AP。

22. 如权利要求 19 的方法，进一步包括：基于特定候选 AP 的相应 EIRP 和 RSS 值计算实际路径损耗；基于所述实际路径损耗估算所述 MS 的假定的当前位置和特定候选 AP 之间的距离；确定所述 MS 的所述假定的当前位置是否与所述 AP 数据一致；以及，如果所述 MS 的所述假定的当前位置与所述 AP 数据一致，则建议所述 MS 使用所述特定候选 AP。

无线网络中的欺骗接入点检测

技术领域

[0001] 本发明涉及通信网络,特别涉及无线网络中的欺骗接入点检测。

背景技术

[0002] 无线网是全球电信市场中正快速增长的一个部分。在典型的无线(无线电)系统中,由一系列互相连接的无线电台或基站为移动用户提供服务,这些无线电台或基站每一个覆盖特定的地理区域。基站被连接到并受控于移动交换中心(MSC),移动交换中心又依次连接到有线(陆地线路)公共交换电话网(PSTN)。移动用户配备有便携式或移动(车载)电话单元,其总体上被称为移动台。基站代表进入点或网络接入点(AP)。

[0003] 困扰无线通信系统的严重问题是欺骗,这导致了对于相应网络和业务提供商的大量资金流失。为了解决这一问题,无线网络使用加密用于维护基于空中链路交换的信息的机密性。但是加密不能完全解决非授权移动台接入网络窃取业务(例如欺骗性的使用移动标识号码、“漫游者”欺骗、移动台“克隆”)。开发并安装了多种验证和识别系统以避免这些欺骗类型。因此,大多数用于保证无线系统中通信安全的工具在登记、呼叫发起和呼叫接收时执行认证来识别移动台的身份。由于认证和加密都需要远程(访问)网络和归属网络(其中MS具有永久性注册)间的通信,从而获取特定移动信息,因而MS的认证是一个复杂和精密的任务。

[0004] 除移动欺骗外,如今最有挑战性的一个IT安全问题是非法(欺骗)无线AP的检测和清除,这些通常称为“欺骗接入点(AP)”。欺骗AP由怀有恶意的攻击者建立,目的是简单地拒绝到网络的接入,或者向它们吸引业务量并从用户获取敏感信息。这可以使公司的有用资源对于临时的窥探者或犯罪的黑客在攻击范围内开放。

[0005] 现有的无线协议没有提供用于确定AP是否是合法AP或欺骗AP的认证机制,攻击者利用了这一弱点。例如,当802.11MS试图连接到给定网络时,其对环境进行扫描并寻找位于附近的AP,自动选择最好的可用AP并与之连接,例如Windows XP自动连接到可能在邻近范围内的最好连接。在这一点上,无线协议包括认证移动台的方式,而不是AP。由于这一行为,一个组织的授权客户机可连接到来自邻近组织的AP。尽管邻近AP并没有有意地吸引该客户机,但这些联系会暴露敏感数据。该问题的存在已经由Niemi和Nyberg对GSM网络进行了证明(UMTS Security,Wiley,2003),并由Johnston和Walker对IEEE 802.16网络进行了证明(IEEE Security and Privacy Magazine,2004第2卷第40~48页的Overview of IEEE 802.16Security)。

[0006] 欺骗AP检测是包含两个步骤的过程,该过程开始于发现网络中AP的存在,然后识别其是否为欺骗AP。现有的发现AP存在的方法可分为无线电频率(RF)扫描、AP扫描或者使用有线输入。RF扫描适用于WLAN,通过在有线网范围内设置RF传感器实现。这些传感器主要由重复使用的(repurposed)AP构成,这些AP仅执行分组捕获和分析、检测工作在该区域内的任何无线设备、并向WLAN管理员告警。但是,欺骗AP可设置在死区,其没有被传感器覆盖,因而除非加入更多的传感器,否则不会被发现。同时,这些固定的传感器不能

检测定向的欺骗 AP。

[0007] AP 扫描意味着部署能够具有扫描设备的 AP 以发现在附近区域内工作的所有 AP。尽管这是非常有用的特征,但很少有 AP 厂商在他们的产品中实施该功能。此外,能够具有 AP 扫描的 AP 的能力被限制在非常短的范围,工作在该覆盖区域之外的欺骗 AP 将不会被注意到。

[0008] 通常,网络管理软件使用有线侧输入技术来发现 AP,其可检测连接到 LAN(例如 SNMP、Telnet、Cisco 发现协议 CDP 等)的设备。该方法是可靠的,并且已经证明其可检测到 LAN 内任何位置的 AP 而不考虑其物理位置无关。此外,无线网络管理系统(NMS)可另外长期监控这些 AP 的状态和可用性。该方法的局限是:不支持各自网络管理软件的任何 AP 将不会被网络管理软件注意到。

[0009] 一旦发现了 AP,下一个步骤是识别其是否为欺骗 AP,这不是简单的任务。一个主要的难点由攻击方法取决于网络类型的事实提出。在 WiFi/802.11 网络中,其使用载波监听多路访问,攻击者必须捕获合法 AP 的身份从而使用合法 AP 的身份建立消息。一旦其捕获到了这样的授权身份,欺骗 AP 等待直到介质空闲,然后向 MS 发送消息。

[0010] 在本地平面上,通过某些管理员解决这一问题,其使用具有用于授权 AP 的授权 MAC 地址、厂商、媒体类型或信道的预配置列表,并提供工具,该工具可对任何最新检测到的属于授权 AP 范围外的 AP 进行自动告警。例如, M. K Chirumamilla 等在 2003 年 IEEE 有关通信的国际会议(ICC)第 492-496 页题为“Agent Based Intrusion Detection and Response Systemfor Wireless LAN”的论文中描述了这样的技术。该论文建议对于在注册 AP 的列表中的成员,检查从 AP 的信标中提取的 MAC 地址。不能分辨 MAC 地址就解释为欺骗 AP 攻击。但是该方法容易受到 MAC 地址欺骗的攻击。此外,列表必须被更新并且有时会过期,因而是不可靠的。

[0011] 此外,在 WiMax/802.16 接入网背景下似乎没有解决欺骗 AP 检测。WiMax/802.16 是下一代无线接入网技术,其更加快速(速度达到每秒 70M 比特),提供了约超过 50km 距离内的网络覆盖,提供了更好的业务质量并比以前的无线技术更加安全。未来的 WiMax 产品将支持移动无线连接,例如,Intel 计划到 2006 年在笔记本电脑中,和到 2007 年在移动电话中加入 WiMax。考虑到未来 WiMax 市场潜在的市场大小,以及当前在网络安全上攻击增长的趋势,欺骗 AP 检测的问题成为了安全 WiMax 通信的重要方面。

[0012] 然而,欺骗 AP 攻击对于这些网络是重要的威胁。为了成功,攻击者必须首先装备从合法 AP 获取到的身份,并与合法 AP 在同一时间发送。攻击者也必须发送到达目标 MS 的信号,即经由比从该区域内任何合法 AP 接收到的信号更强的接收信号强度(RSS)。在这种情况下,MS 接收器在该强大的非法信号出现时自动地减小了其增益,减小到合法信号表现为背景噪声这样的一个点。两个信号间实际的强度差别取决于接收器灵敏度。

[0013] 此外,使用该技术,移动台和 AP 的相互认证是可选的,并且发生在网络接入处理之后。同样,物理层上不存在安全。这样,在 WiMax/802.16 接入网的 MS 和 AP 间的对话过程中,欺骗 AP 攻击可发生在多个点上。

[0014] 其它建立 AP 合法性的方法包括由 Beyah 等人在题为“Rogue AccessPoint Detection using Temporal Traffic Characteristics”中提出的方法,该文章公开在 2004 年 IEEE 全球电信会议(GLOBECOM)会议录的第 2271-2275 页。该文章提出了一种基于网络

业务量时间特性分析的方法。其基于这样的假设：无线业务量比有线业务量更加随机。但是，在 Beyah 等文章中描述的方法提出了通过业务量图的可视检查来发现欺骗 AP，并且不是自动的。此外，对业务量特性的假设在实际网络中很难识别。

[0015] 大体上，现有的检测欺骗 AP 的方案是昂贵的、初布的并容易避开。因此，无线网络需要有效的方法来检测欺骗 AP，从而避免恶意攻击。

发明内容

[0016] 本发明的目的是提供一种用于在无线接入网中检测欺骗 AP 的系统，全部或部分减轻现有欺骗 AP 检测系统的缺点。

[0017] 因此，本发明提供了一种用于在无线接入网中检测欺骗接入点 (AP) 的方法，包括：a) 在所述无线接入网的所述每个 AP 上为服务区域内的所有 AP 保持 AP 数据；b) 从在所述服务区域内漫游的移动台 (MS) 请求从服务中的 AP 切换到所述服务区域内多个候选 AP 中的一个；c) 在 MS 上收集来自所有所述候选 AP 的 AP 存在信息，并向所述正在服务的 AP 报告所述 AP 存在信息；d) 在所述正在服务的 AP 上确定所述 AP 存在信息是否与所述正在服务的 AP 上保持的所述 AP 数据一致；以及 e) 只要所述 AP 存在信息与所述 AP 数据不一致，则识别所述欺骗 AP。

[0018] 根据本发明的另一个方面，提供了一种用于在无线接入网中检测欺骗接入点 (AP) 的方法，包括 i) 准备 Voronoi 图，其可将对应于服务区域的平面分为多个凸多边形，每个多边形包括代表所述服务区域内的 AP 位置的生成点，并且给定多边形内的每个点到其生成点比到任何其它点更近；及 ii) 为每个多边形计算所述相应凸区域的任何点和 Voronoi 图内每个其它生成点之间的最小距离和最大距离，并存储所述最小和最大距离。

[0019] 进一步地，本发明旨在提供一种用于在无线接入网中检测欺骗接入点 (AP) 的方法，包括：p) 在所述无线接入网的每个 AP 上为服务区域内的所有 AP 保持 AP 数据；r) 在所述服务区域内漫游的移动台 (MS) 上收集数据集，该数据集包括所述服务区域内的所有 AP 的接收信号强度 (RSS) 数据，并向所述正在服务的 AP 报告所述数据集；s) 在所述正在服务的 AP 上确定所述数据集内的所述 RSS 数据是否与在所述正在服务的 AP 上保持的所述 AP 数据一致；及 t) 当所述数据集内的所述 RSS 数据与所述 AP 数据不一致时，识别所述欺骗 AP。

[0020] 本发明的方法有利地解决了现有无线系统安全中的弱点，并可用于任何无线技术，与欺骗 AP 的信号范围无关。特别地，根据本发明的系统可结合有新的 WiMax 设备。同时，根据本发明的系统和方法使 AP 在切换阶段内检测部署在邻近区域内的欺骗 AP，而不使用定向天线及大范围的传感器。

[0021] 本发明的另一个优点是其使得 MS 作为移动传感器操作来检测欺骗 AP。移动设备可在连接装置上检测并报告 AP 信号。因此，由于它们的移动性会消除检测范围上的死区。使用本发明甚至能够检测定向的欺骗 AP。

附图说明

[0022] 通过以下优选实施例更具体的说明，本发明前述及其它目的、特征及优点将更加明显，如附图中所示，这里：

[0023] 图 1 例示了简单的无线网，其包括根据本发明实施例的移动台；

[0024] 图 2 表示了在切换阶段期间欺骗接入点检测方法的流程图, 该方法是精确的解决方案;

[0025] 图 3 表示了在图 2 的流程图上如何确定信号的一致性, (a) 上表示了一致的信号, (b) 上表示了不一致的信号;

[0026] 图 4 表示了在切换阶段期间欺骗接入点检测方法的流程图, 该方法是快速测试解决方案; 及

[0027] 图 5 表示了在通信进行的同时欺骗接入点检测方法的流程图。

具体实施方式

[0028] 本发明基于来自移动台 (MS) 的接收信号强度 (RSS) 报告中的一致性确定接入点 (AP) 对于无线网络的合法性。特别地, 其使得 MS 在合法 AP 的帮助下在切换阶段和 / 或在通信进行的同时识别欺骗 AP。一旦 MS 与合法 AP 通信, 本发明也涉及使用 MS 作为移动传感器。

[0029] 术语“切换”在这里指从一个 AP 到另一个的处理中普遍公认的交换呼叫而不会中断通信的操作。该过程用于用户向 / 从相应覆盖区域移动时为 MS 提供无缝业务。在切换期间, 欺骗 AP 可伪装为合法 AP, 从而移动用户会失去与接入网的连接。术语“通信”在这里用于指 MS 通过所选的 AP 接入到网络后, MS 和远程实体间的信息交换。

[0030] 无线接入网包括多个 AP, 提供到漫游无线 MS 的连接。这些 AP 在单独的主干网络上连接在一起, 该主干网络用于交换通信信息。通过设计, 每个 MS 尽力通过具有最强 RSS 的 AP 得到连接。由于同一 AP 和两个 MS 间的距离非常可能不同, 并且由于 MS 具有最大可能不同的灵敏度, 该由 MS 对特定 AP 测量的 RSS 值与每个 MS 相关。

[0031] 图 1 概略地表示了无线接入网 150, 其包括根据本发明实施例的 MS。该例子中的网络包括合法 AP10 和 10'、欺骗 AP100 和在这些站的覆盖区域之间移动的 MS5。合法 AP 基于可信物理网络 150 互相连接, 并可同时接入到如 200 所示的有线网络。应当注意, 在 MS5 和 AP10 的结构图上仅例示了与本发明有关的单元。

[0032] 已知的, AP 和移动台配置有收发器 13 和 13', 其具有接收器 16 和发射器 20 (仅对于 MS5 进行了表示), 用于在 MS 和 AP 间基于接口 11 和 11' 实现双向通信, 以及单独的处理器 15 和 17。处理器 15 和 17 一般性地例示了相应 MS5 和 AP10 的全部功能, 即在网络 200 上实现移动台和 AP 间的数据通信及信令, 包括建立连接、切换、数据传递 (通信) 及其它不同样与本发明相关的功能。

[0033] 此外, 接入网中的全部合法 AP10 和 10' 还装配有邻居数据库 12, 其存储有用于接入网 150 中所有 AP 的位置数据, 或者至少最近的邻居的位置。AP 位置数据可以用任何已知的方式确定, 例如通过骨干网协议或通过配置。所述位置信息以例如表格的形式保存在邻居数据库 12 中, 其中每一行提供 AP 标识符 (MAC 地址、AP 下标)、相应 AP 的位置, 及有效各向同性辐射功率 (EIRP); 其它关于各个邻居的控制信息也可以保存在该表中。我们假设这些信息是可信的。

[0034] 根据本发明, AP 还装配有 AP 位置估算单元 14, 其基于从移动台接收到的信息计算当前 AP 位置数据, 该移动台例如在 AP10 的覆盖区域内漫游的 MS5。可以不同方式及在过程中的不同呼叫阶段 (切换或 / 和通信) 确定 AP 位置, 如结合图 2-5 所描述的。然后将当

前的 AP 位置数据与存储器 12 中存储的位置数据进行比较。如果数据一致，则认为该 AP 合法。如果不一致，则在附近存在欺骗 AP。

[0035] MS5 装配有 AP 扫描器 19，用于检测从相应区域内的 AP 接收到的信号的信号强度（接收信号强度 RSS）。扫描器 19 表示为独立的单元，当然，其可以是接收器 16 的一部分。在如下面讨论的移动传感器的操作中，移动台维持数据库 22，其收集与扫描器 19 检测到的 AP 有关的 RSS 和方向信息。除执行的建立 / 终止连接、对连接进行切换及随之发出信令的一般任务外，处理器 15 还从扫描器 19 收集 AP 信息，并将其存储在数据库 22 中。在发射器 20 上取出该信息以向 AP 报告移动台当前用于接入（正在服务的 AP）。由于站点是移动的，这些能力使得 MS 在接入网中作为移动传感器工作。结果，攻击者不能通过使用定向天线简单地对抗该检测方法。

[0036] 根据本发明，MS 在这样的时间间隔内对正向其提供服务的 AP 做出命令，其中在该时间间隔内 MS 扫描频率并评估该区域内可用 AP 的 RSS，这被称为扫描时间间隔。正在服务的 AP 基于 MS 的当前位置使用从数据库 12 中取出的推荐的 AP 标识符回复这一扫描间隔命令。在扫描间隔期间，MS 测量推荐的 AP 的 RSS。例如，通过对在帧前同步信号期间获得的信号强度进行平均获得 RSS。当扫描器 18 收集到所有的测量时，MS 向正在服务的 AP 发送报告，该报告包括与该测量的 RSS 配对的相应 AP 的身份。

[0037] 根据本发明，欺骗 AP 检测可发生在移动台呼叫的切换阶段和 / 或发生在通信进行的同时。对于切换阶段期间的欺骗 AP 检测，目标是保证切换期间从候选 AP 接收到的信号与那些候选 AP 的实际位置一致。当通信进行时，目标是检测并报告该区域内所有 AP 的存在，在该方式中，MS 在接入网中作为移动传感器工作。

[0038] 应当理解，本发明不限于用于检测欺骗 AP 的 RSS 的处理。可以使用任何提供在 MS 的漫游区域内操作的 AP 的指示的其它存在信息，以及移动台能够收集并向正在服务的 AP 报告的存在信息。

[0039] 在切换阶段的欺骗 AP 检测

[0040] 图 2 表示了在切换阶段内欺骗 AP 检测方法的流程图，该方法是“精确的解决方案”。假设，图 1 的 MS5 连接到无线 150 以通过网络 200 与固定台通信。同时，我们假设 MS5 使用 AP10 作为当前 AP，并且当其离开 AP10 的覆盖区域时，其搜索单元能够从 AP10 无缝接管该连接的预期 AP。如步骤 30 所见到的，MS5 向 AP10 报告所有指示能够接管当前由正在服务的 AP10 执行的接入功能的 AP。

[0041] 然后在步骤 31，在正在服务的 AP 上使用 RSS 测量以对于 MS 和相应 AP 间的信号计算实际路径损耗。使用来自数据库 12 的候选 AP 的 EIRP、由 MS 在步骤 30 报告的用于该 AP 的 RSS 以及 EQ1 确定该实际路径损耗：

$$[0042] E = EIRP - RSS - Gr \quad EQ1$$

[0043] 这里 Gr 是 MS 的接收天线增益。

[0044] 如上面所指出的，正在服务的 AP 得知预先存储在数据库 12 中的合法 AP 的位置。在某些情况下，AP 也可以得知 MS 的当前位置。例如，如果 MS 配备有 GPS，则 MS 可向正在服务的 AP 提供其位置。在这种情况下，MS 和候选 AP_i 之间的距离 d_i 可用于估算预期路径的损耗。这种情况沿着图 2 的判定框 32 的“是”分支表示。

[0045] 根据 2001 年 Prentice Hall 出版社，S. Rappaport 和 T. Rappaport 的著作

“Wireless Communications :Principles and Practice”第二版,以 dB 表示的路径损耗 $L(d)$ 作为以米表示的距离 d 的函数,该路径损耗是遵循正态分布的随机变量,由 EQ2 给出:

$$[0046] \quad L(d) = \bar{L}(d_0) + 10\nu \log\left(\frac{d}{d_0}\right) + X_\sigma \quad \text{EQ2}$$

[0047] d_0 表示到候选 AP 的发射器的参考距离。在该距离上计算的平均损耗是 $\bar{L}(d_0)$ 。值 ν 表示路径损耗指数,其范围从 1.5 到 6。该路径损耗指数捕获这样的速率,信号强度按该速率衰减,并使用抽样来确定。 X_σ 为高斯分布随机变量,以 dB 表示,具有零平均值和标准偏移 σ 。该距离然后用于计算 $L(d)$,如步骤 33 所示。

[0048] 已知 $L(d)$ 和 E 间的差异小于或等于具有 95% 可能性的 2σ 。这一事实是根据正态分布的标准表得出的。因此,认为处于攻击时,计算的有效 AP 到 MS 的路径损耗大大小于平均的理论上的 AP 到 MS 的路径损耗,是合理的。因此,用于确定候选 AP 是否合法的测试变为:

$$[0049] \quad |L(d) - E| \leq 2\sigma \quad \text{EQ3}$$

[0050] 使用该技术,错误否定的比率大约为 2.5%。错误肯定的比率依赖于攻击者成功所需要的附加 RSS。此外,如果 AP 使用扇区化天线,则 MS 的方位角必须在 AP 的扇区之内。如果这些测试失败(如果 AP 合法这很不可能),则应认为对于该 AP 报告的信号是反常的。

[0051] 如果 EQ3 的测试没有被满足,即判定框 34 的“否”分支,其意味着相应 AP 是一个欺骗 AP,正在服务的基站在步骤 35 向 NMS 警告该欺骗 AP 的存在。如果 EQ3 中的测试指示 AP 合法,即,判定框 34 的“是”分支,这意味着从 MS 接收到的 RSS 数据是一致的,切换阶段可选择任何新报告的 AP,如步骤 36 所示。正在服务的 AP 然后在步骤 37 执行到步骤 36 中选择的相应候选 AP 的切换。

[0052] 如果不知道 MS 的位置,即仅知道候选 AP 的位置,则路径损耗的估算变得更加复杂,如判定框 32 的“否”分支所示。在这种情况下,如步骤 38 所示,优选地使用信号强度的几何表示来进行计算。取决于相应预期 AP 的测量数,MS 的近似位置可表示为圆盘、环面、圆盘的扇区、环面的扇区、线段等。给出损耗 L ,对数正态阴影模型可用于计算距离估计 d :

[0053]

$$d = d_0 10^{\frac{L(d_0) - L}{10\nu}} \quad \text{EQ4}$$

[0054] 损耗 L 和距离 d 都是随机变量。从 MS 到候选 AP 的实际距离在最小值 d_{\min} 和最大值 d_{\max} 之间的间隔之内的可能性大于或等于 95%。使用 EQ5 计算最小和最大距离:

$$[0055] \quad d_{\min} = d_0 10^{\frac{L(d_0) - L - 2\sigma}{10\nu}}$$

[0056]

$$d_{\max} = d_0 10^{\frac{L(d_0) - L + 2\sigma}{10\nu}} \quad \text{EQ5}$$

[0057] 以上 EQ5 遵循这一事实,即 95% 的时间内测量到的路径损耗和平均路径损耗的最大差别是 2σ dB。因此可假设 MS 95% 的可能性位于由候选 AP 的位置 (s, y) 为中心,半径为 d_{\min} 和 d_{\max} 的环面所定义的区域内。在这种情况下,需要校准阶段来确定平均短距离损耗 $\bar{L}(d_0)$ 、路径损耗指数 ν 及标准偏移 σ 。

[0058] 回到图 2,随着在步骤 30 对于每个候选 AP 的 RSS 的接收,正在服务的 AP 在步骤

31 使用 EQ1 确定有效损耗。使用 EQ4 估算 MS 到 AP_i 的距离 d_i , 该 EQ4 具有用作预期损耗 ($L = E$) 的有效损耗值。每个 AP_i 定义以相应位置 (x_i, y_i) 为中心, 半径为 $d_{i,\min}$ 和 $d_{i,\max}$ 的环面 A_i 。

[0059] 也如图 3 的例子所示, 在步骤 39 基于环面的交集评估信号一致性。如果对于所有候选 AP 的环面具有非空的交集, 如图 3(a) 所示, 就表示存在这样的区域 (交集), 其中 MS 看起来可位于该区域, 因为对于临近区域内的 AP 接收到的 RSS 是一致的。

[0060] 在步骤 38 可仅使用 $d_{i,\max}$ 值进一步简化检测。每个 AP 同时定义半径为 $d_{i,\max}$, 中心为位置 (x_i, y_i) 的圆盘 D_i 。图 3 例示了一般情况和非一般情况的例子。在一般情况下, 圆盘具有非空交集, 以及与 MS 应位于的共同区域一致的信号报告。在反常情况下, 攻击者使用充分强的 RSS 模仿 AP_2 。这导致了错误的解释, 即接收器更接近实际上的 AP_2 。信号报告与 MS 应位于的共同区域不一致。

[0061] 如果 AP 使用扇区化天线, 则应证实扇区的交集代替环面和圆盘。

[0062] 如以上所指出的, 为了揭露欺骗 AP, AP_{10} 的 AP 位置估算单元 14 对于相应候选 AP 执行在步骤 38 计算出的所有几何表示 (环面、环或扇区等) 的交集, 如步骤 39 所示。可通过求解一系列等式来得到用于每个 AP 的位置的解 (x_i, y_i) 来实现圆盘、环面和扇区交集的验证。

[0063] 如果几何表示的交集不是空的, 即判定框 39 的“是”分支, 这表示从 MS 接收到的 RSS 数据是一致的, 并且切换阶段可选择任何新报告的 AP, 如步骤 36 所示。现在, 可处理切换, 并且最近的候选 AP 是新的正在服务的 AP。图 3(a) 表示了当信号一致时的例子。

[0064] 另一方面, 如果信号不一致, 如图 3(b) 所示, 即判定框 39 的“否”分支, AP 将向网络管理系统 (未示) 发出告警信号, 如步骤 40 所示。为了确定哪一个预期 AP 是欺骗 AP, 正在服务的 AP 试图确定具有非空交集的几何表示的最大基数子集。假设列表中仅有一个欺骗 AP, 则从该列表简单选择一个 AP 并移出, 如步骤 41 所示, 在步骤 42 再次计算剩余几何表示的公共交集。如果该公共交集仍为空, 替换该列表中的相关 AP, 并从初始列表移出另一 AP。重复步骤 41-42 直到信号一致, 在这种情况下, 最后移出的 AP 是欺骗 AP, 如步骤 25 所示。如果距离不一致, 则可在任何时间完全拒绝切换。

[0065] 应当注意确定哪个 AP 引入了距离上的差异的其它方式。例如可以从该列表同时移出两个或多个 AP, 而不是一个, 或者正在服务的 AP 可以使用某些选择标准来选择从列表移出 AP 的顺序等。这些测量可以例如试图加速欺骗 AP 检测处理, 或者更精确地识别欺骗 AP 等。

[0066] 由于必须在通信切换期内完成欺骗 AP 的检测, 可以使用更快速的方案。虽然这种快速方案不是十分精确, 但可以结合精确方案来使用以消除某些最坏的欺骗。该快速方案依赖于使用 Voronoi 图的预处理步骤。该图将具有 n 个生成点的平面划分成凸多边形, 这样每个多边形精确地包含一个生成点, 给定多边形内的每个点到其自己的生成点比到任何其它生成点更近。使用可信 AP 的已知位置作为生成点。当网络拓扑固定时, 相应 Voronoi 图是不变的, 并且能够以时间复杂性 $O(n \log n)$ 预先计算。

[0067] 图 4 表示了在切换阶段欺骗 AP 检测方法的流程图, 这是一种快速检测方案。在步骤 43, 正在服务的 AP 计算代表预存储在存储器 12 中的 AP 位置的点的 Voronoi 图。如循环 44-47 所示, 对于 Voronoi 图的凸区域, AP 计算该凸区域的任何点和每个其它生成点之间的

最小和最大距离。该距离存储在每个凸区域的数据库 12 中。

[0068] 如图 2 所示的实施例中, MS 在步骤 47 向正在服务的 AP 报告每个候选 AP 的 RSS。在步骤 48, 基于这些 AP 的特征和测量到的 RSS, AP 计算 MS 的当前位置和候选 AP 间的近似距离。这些近似值定义了距离范围。在步骤 49, 正在服务的 AP 识别被认为与 MS 的当前位置最接近的候选 AP_i。最短距离 d_i 使得正在服务的 AP 确定相应的 Voronoi 图上的凸区域, 其中该 MS 应该在该区域内。接下来, 在步骤 51, AP 确定在步骤 45 对于 AP_i 确定的距离范围是否与在步骤 49 计算出的距离一致。如果距离相符, 则执行判定框 51 的“是”分支, 然后在步骤 61 执行切换。否则, 为了更精确的确定当前仍执行精确方案。

[0069] 如果不相符, 即判定框 51 的“否”分支, 如步骤 53 所示, AP 向接入网的网络管理系统发出告警。然后, 正在服务的 AP 试图确定具有一致距离的 AP 的最大候选子集。假设该区域内仅有一个欺骗 AP, 在步骤 55 随机选择并移出一个 AP。例如, 其可以是在步骤 49 识别出的最接近的候选 AP。在步骤 57, 像以前一样确定当前与 MS 最接近的候选基站, 并识别用于该新的最接近候选 AP 的相应凸多边形。如果在判定框 59 距离不一致, 则再次替换选择的 AP 并移出另一个 AP; 重复步骤 55、57 和 59, 直到距离一致。在这种情况下, 在步骤 25, 将最后移出的 AP 识别为欺骗 AP。总之, 如果距离不一致, 可以在任何时候拒绝切换。

[0070] 应当注意, 可以使用确定哪个 AP 引入了距离差异的其它方法。例如可以从列表中同时移出两个或多个 AP, 而不是一个, 或者正在服务的 AP 可以使用某些选择标准来选择从列表中移出 AP 的顺序等等。这些策略可试图例如加速欺骗 AP 检测的进程, 或者更精确的识别欺骗 AP 等等。

[0071] 在通信进行的同时检测欺骗 AP

[0072] 图 5 表示了在通信进行的同时欺骗 AP 检测方法的流程图。一旦移动用户已经与合法 AP 建立了通信, 该 AP 可希望检测任何由移动用户报告的潜在的欺骗 AP。在这种情况下, MS 成为了尽力检测接入网中的欺骗 AP 的移动传感器。显然, 在连接阶段不存在快速检测的实际需要, 因而, 检测过程可以离线于 AP- 移动用户的通信建立进行。

[0073] 在步骤 50, 移动台从该区域内的所有 AP 收集 RSS, 并向正在服务的 AP 报告该信息。应当注意, 如图 5 的流程图上的虚线所示, 当移动台在 AP 的服务区内漫游时, 继续执行步骤 50。该报告包括由 MS 对于相应区域内的所有 AP 收集到的信息, 并可周期性的产生, 或者当正在服务的 AP 请求时产生; 可以同样想象其它安排。这些信息包括至少具有相应 AP 的标识和相应的 RSS(例如 AP1-RSS1 ;AP2-RSS2. APn-RSSn) 的数据集。也可以记录收集相应数据集的时间。

[0074] 在步骤 52, 对于移动用户报告的每个数据集, 正在服务的 AP 计算移动用户的近似位置。基于相应候选 AP 的特征和移动用户接收到的信号强度执行确定。可以如前使用几何表示来代表与 AP 相关的 MS 的近似位置, 如圆盘、环面、圆盘扇区、环面扇区、线段。

[0075] 接下来, 正在服务的 AP 对于给定的数据集确定从 MS 接收到的 RSS 是否与其在相应区域内合法 AP 的消息一致。在步骤 52, 通过计算所有几何表示的交集来执行这一点。如果交集不为空, 这表示从 MS 接收到的给定数据集的信号一致, 没有报告的 AP 认为是欺骗 AP。如判定框 56 的“是”分支所示, 对于 MS 报告的每个数据集重复步骤 50 和 56。

[0076] 另一方面, 如果给定数据集中的信号不一致, 如判定框 56 的“否”分支所示, 在步骤 58, 正在服务的 AP 向网络管理系统发出告警。然后, 如以上所描述地, 正在服务的 AP 试

图通过确定具有非空交集的几何表示的最大候选子集来确定欺骗 AP 的身份。

[0077] 每个合法 AP 使用该方法来监控接入网。如果给定 AP 被报告的太过频繁，并最终由太多的 AP 被报告，中央网络管理从而执行并要求接入网中的所有合法 AP 将相应的 AP 标识为处于危险。此外，网络管理系统通过合法 AP 可下载 MS 中处于危险 AP 标识的黑名单。然后，AP 和 MS 可执行某些安全策略，例如仅在没有其它可能时使用处于危险的 AP。

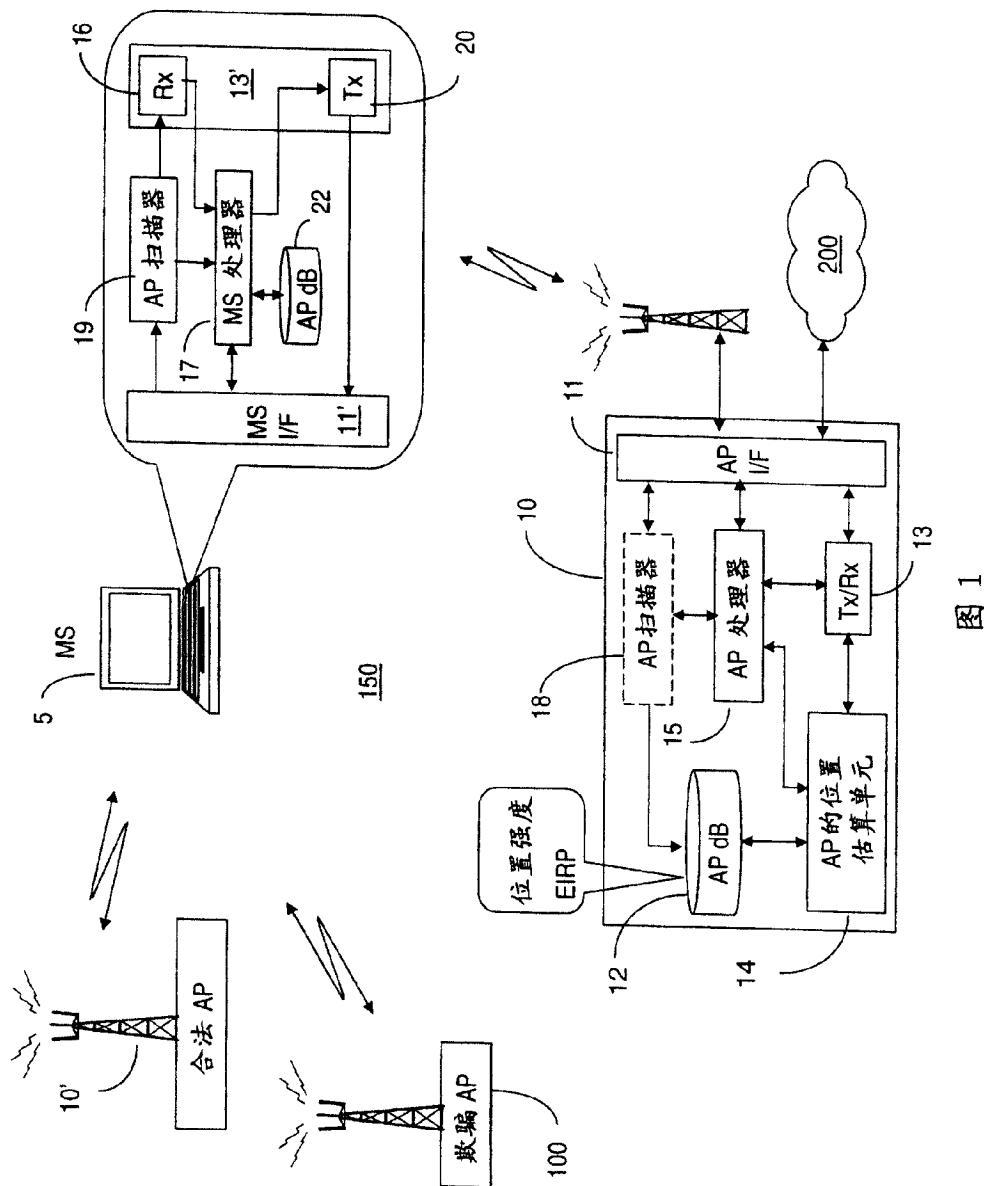


图 1

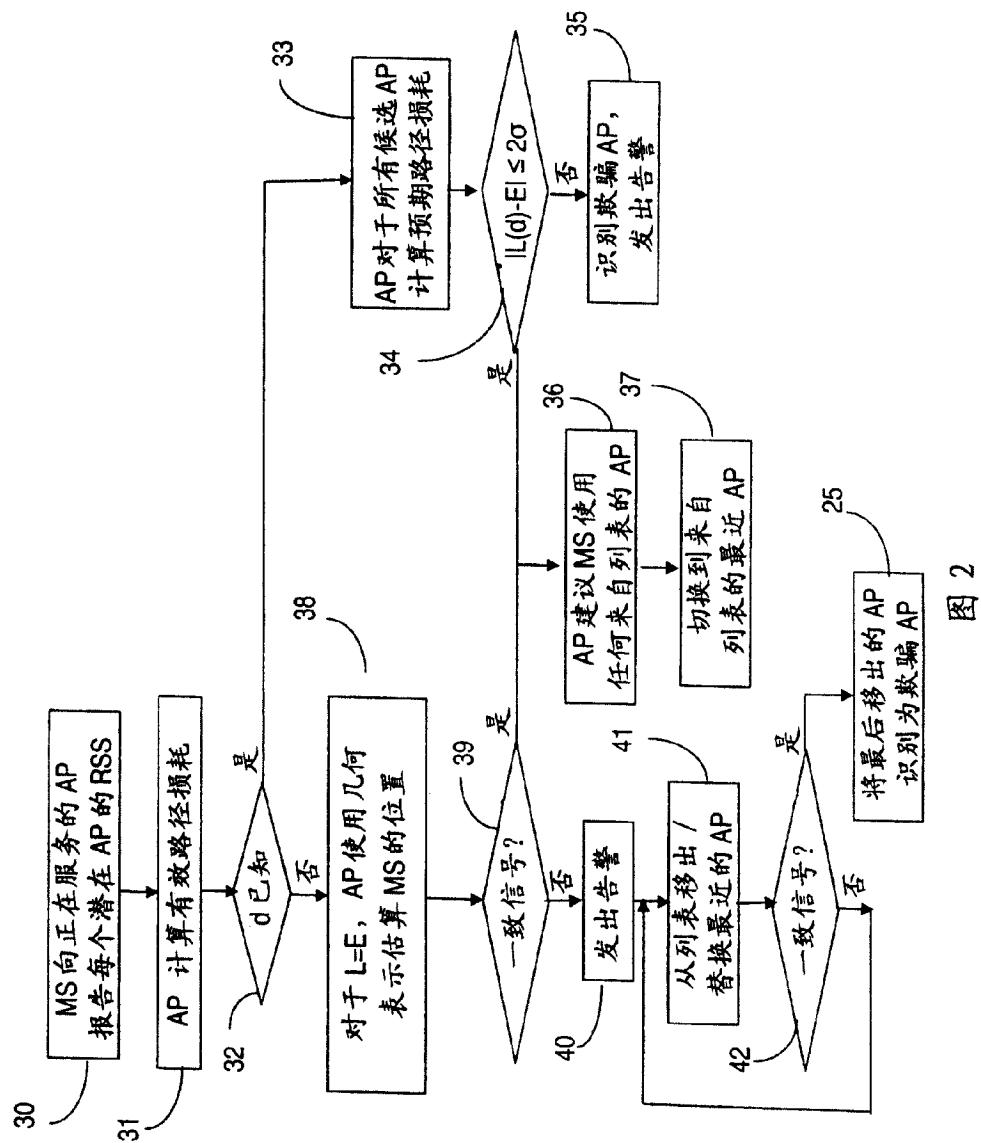


图 2

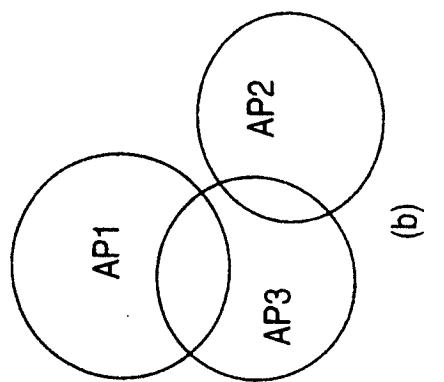
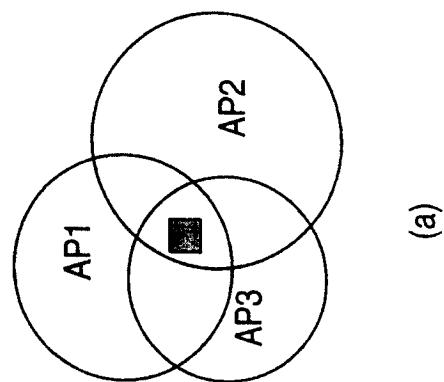


图 3
(b)



(a)

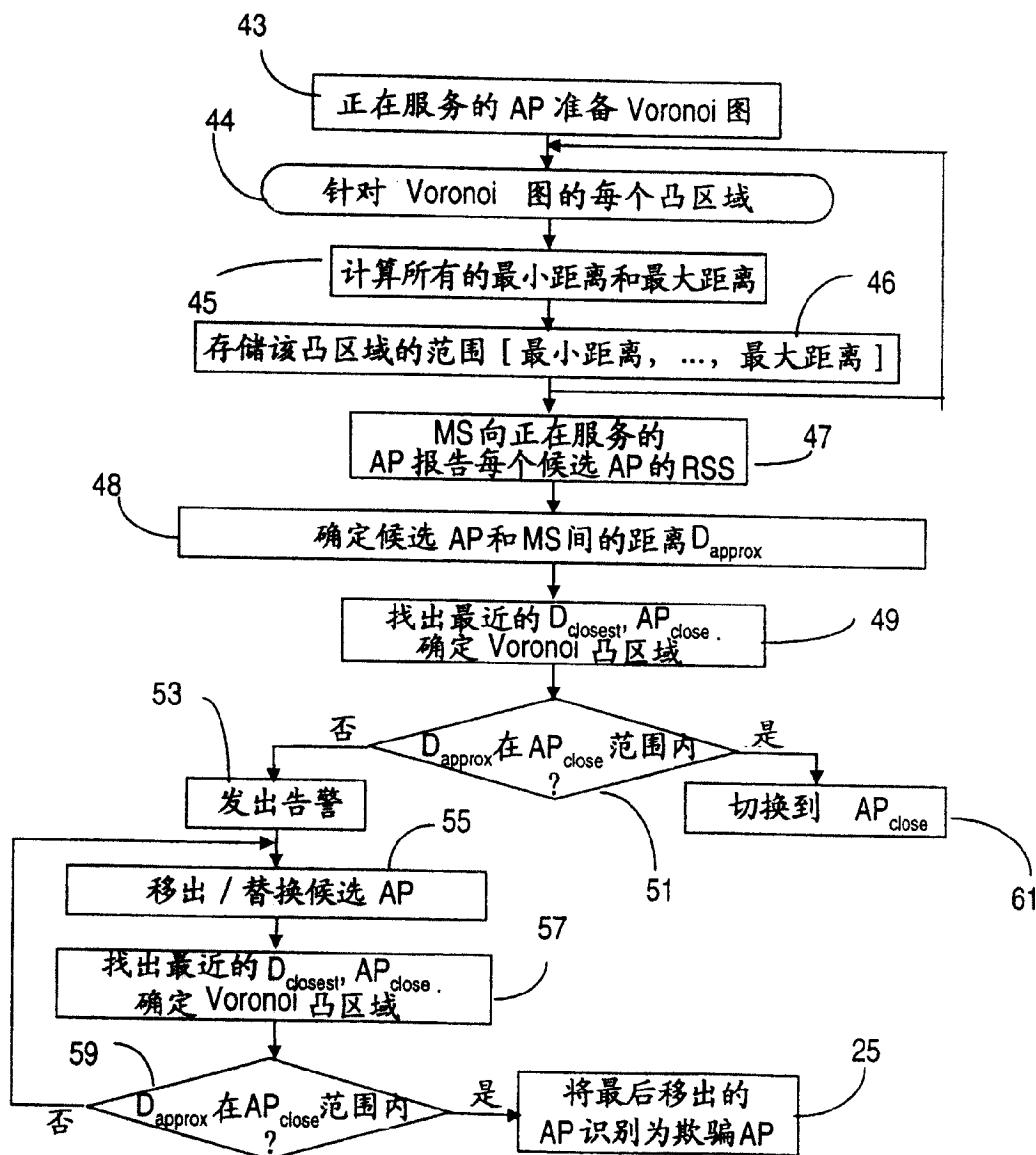


图 4

