[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04B 1/58
H04M 1/00

[12] 发明专利申请公开说明书

[21] 申请号 03811426.7

[43] 公开日 2005 年 8 月 17 日

[11] 公开号 CN 1656703A

[22] 申请日 2003.4.21 [21] 申请号 03811426.7

[30] 优先权

[32] 2002. 4.19 [33] US [31] 60/373,787

[86] 国际申请 PCT/US2003/012321 2003.4.21

[87] 国际公布 WO2003/090371 英 2003.10.30

[85] 进入国家阶段日期 2004.11.19

[71] 申请人 计算机联合思想公司

地址 美国纽约

[72] 发明人 乔翰·冯 德 格罗恩南戴尔
迈克尔·弗莱 桑迪普·杰恩
安德尔泽吉·赞流斯基
拉尔夫·萨波罗斯基
达万纽·斯林尼瓦斯

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

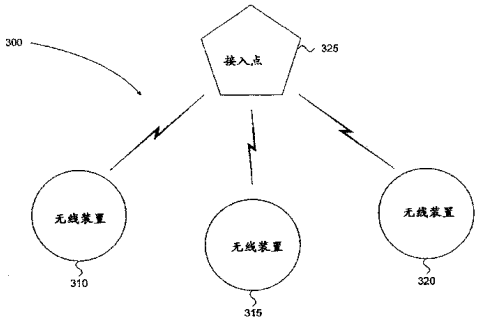
代理人 郭思宇

权利要求书 3 页 说明书 12 页 附图 7 页

[54] 发明名称 管理企业中的无线装置的系统和方法

[57] 摘要

公开一种管理企业中的无线装置(310、315、320)的方法和系统。 第一例证方法管理企业中的无线网络的物理接入点(325)。 第二例证方法管理企业中的无线装置(310、315、320)的资产。 第三例证方法能够在无线装置(310、315、320)内实现病毒扫描。 第四例证方法管理无线装置数据备份。



ISSN1008-4274

1、一种管理网络中的无线装置的方法，所述方法包括:

识别网络内的多个经授权的逻辑无线接入点;

检测网络内的多个物理无线接入点;

对于多个物理无线接入点中的每个接入点，确定该物理无线接入点是否与多个经授权的逻辑无线接入点之一相关联; 和

报告与经授权的逻辑无线接入点无关的每个物理无线接入点。

2、按照权利要求 1 所述的方法，还包括:

检测多个无线装置，包括确定相关的物理无线接入点; 和

建立反映所述多个无线装置中的每个无线装置与相应的相关物理无线接入点之间的关系的网络布局图。

3、按照权利要求 1 所述的方法，还包括:

定义与无线装置相关的优选量度值;

检测无线装置，包括确定实际量度值; 和

比较确定的量度值和优选量度值，以便确定该无线装置是否正在不正常工作; 和

报告该无线装置是否正在不正常工作。

4、按照权利要求 3 所述的方法，其中优选量度是发射功率的量度。

5、按照权利要求 3 所述的方法，其中优选量度是可接受的干扰的量度。

6、按照权利要求 3 所述的方法，其中优选量度是碎片计数。

7、按照权利要求 3 所述的方法，其中优选量度是传输速度。

8、按照权利要求 3 所述的方法，其中优选量度是故障计数。

9、按照权利要求 1 所述的方法，还包括:

确定与无线装置相关的安全策略;

检测该无线装置，包括获得与该无线装置相关的安全信息;

确定所述安全信息违反安全策略; 和

报告违反安全策略。

10、按照权利要求 9 所述的方法，其中安全策略定义经授权的用户 ID/口令组合，其中安全信息是未经授权的用户 ID/口令组合。

11、按照权利要求 9 所述的方法，其中安全策略定义经授权的无线装置标识符，安全信息是未经授权的无线装置标识符。

12、一种管理网络中的无线装置的方法，所述方法包括:

定义与网络上的某一无线装置相关的一组经授权的资产;

检测网络上的该无线装置;

确定与该无线装置相关的实际资产;

分析所述一组经授权的资产和实际资产，识别至少一个标记资产;

报告所述至少一个标记资产。

13、按照权利要求 12 所述的方法，其中分析包括确定每个实际资产是否是所述一组经授权资产的一部分; 和

其中每个标记资产是一种实际资产，它不是所述一组经授权资产的一部分。

14、按照权利要求 12 所述的方法，其中分析包括确定每个经授权资产是否是实际资产; 和

其中每个标记资产是一种不是实际资产的经授权资产。

15、按照权利要求 12 所述的方法，其中经授权资产是具有版本标识符的应用软件。

16、按照权利要求 12 所述的方法，其中经授权资产是具有标识符的硬件装置。

17、按照权利要求 12 所述的方法，其中标记资产是应用软件，所述方法还包括:

把所述应用软件传送给无线装置。

18、一种管理网络中的无线装置的方法，所述方法包括:

检测网络上的装置;

确定该装置是无线装置;

确定该装置已从一计算机接收数据；和

执行与该无线装置相关的病毒扫描例程。

19、一种管理网络中的无线装置的方法，所述方法包括：

定义与网络中的一无线装置相关的数据备份策略；

检测网络中的该无线装置；

分析数据备份策略，确定驻留在该无线装置上的数据应被备份；和

备份驻留在该无线装置上的数据。

管理企业中的无线装置的系统和方法

相关申请的交叉参考

本申请要求美国临时申请“无线企业管理系统和方法”，No. 60/373,787，申请日为2002年4月19日，的优先权，在此结合作为参考。

技术领域

本发明的系统和方法涉及企业信息处理环境。更具体地说，本发明的系统和方法与管理企业信息处理环境中的无线装置有关。

背景技术

近年来，企业和个人用户对移动技术的使用稳定增长。移动电话机被普遍使用，许多人采用个人信息管理（“PIM”）装置或掌上型电脑管理他们的时间表、通信录、金融信息和其它数据。这种装置特别适合于其工作职责要求他们旅行的雇员。一些企业鼓励这样的雇员通过无线装置，定期与他们的企业信息处理环境联系，以便提高响应和生产力。移动定期连接促进了雇员之间的通信，并通过移动装置和企业之间的同步进程，提高了收集的数据的及时性。

具有无线能力的个人数字助手（“PDA”）移动电子邮件装置和笔记本PC的日益激增鼓励无线电信公司不仅提供语音的传输，而且还提供相对于移动无线装置的数据信号的收发。虽然把无线装置集成到企业信息处理环境中促进了生产率和效率的提高，这样的集成也会导致对保存在这种移动装置内，以及相对于这种移动装置收发的信息的安全性和保密性的威胁不断增大。

采用可与企业连接的移动无线装置的企业期待来自使用这种装置的一些优点。例如，这样的优点可包括无线连接膝上型计算机，使得能够从任意地方虚拟地完成工作的能力。无线连接的另一优点在于

对商业过程的灵活接入。无线连接的另一优点在于在移动装置上接收恰当的报警和消息，以便在效率提高的情况下执行所需的工作职责。

除了无线连接的优点之外，采用可连接的无线装置的企业面临一些挑战。例如，挑战之一是充分保护无线装置上的信息，以确保机密企业和个人信息不会丢失或被盗的挑战。另一挑战是信息的实时同步，以确保准确性和一致性。

为了限制与移动装置和企业的连接相关的安全性和保密性威胁，一些企业运行两个独立的信息处理环境：一个用于有线装置，一个用于无线装置。维持两个不同环境的企业失去了运行组合环境的那些企业可能享有的集成和同步优点。

对把无线装置集成到企业信息处理环境中的第二种现有解决方案是按照其中保持用于有线装置和无线装置的独立专用资源的混合模式运行。在组合环境中采用这样的独立资源常常导致装置之间不兼容和/或削弱安全性。

因此，需要一种管理企业信息处理环境中的无线装置的系统和方法，所述系统和方法能够在保护不论有线或无线连接的装置上的数据的安全性和保密性的同时，实现无线装置的集成和同步。

发明内容

下面给出与在企业处理环境中管理无线装置相关的系统和方法的简要概述。该概述不是详尽的综述，并不打算识别方法和/或系统的关键或紧要部件，或者详细记述方法和系统媒体的范围。该概述概念地简要说明所述方法和系统，作为后面给出的更详细说明的前序。

根据本申请的一个方面，公开一种管理网络中的无线装置的例证方法。所述方法包括识别网络内的多个经授权的逻辑无线接入点。该方法还包括检测网络内的多个物理无线接入点，并关于多个物理无线接入点中的每个接入点，确定该物理无线接入点是否与多个经授权的逻辑无线接入点之一相联系。该方法还包括报告与经授权的逻辑无线接入点无关的每个物理无线接入点。

根据本申请的第二方面，公开一种管理网络中的无线装置的例证方法。所述方法包括定义与网络上的某一无线装置相关的一组经授权的资产。该方法还包括检测网络上的该无线装置，确定与该无线装置相关的实际资产。该方法还包括分析该组经授权的资产和实际资产，从而识别至少一个标记资产。该方法还包括报告所述至少一个标记资产。

根据本申请的第三方面，公开一种管理网络中的无线装置的例证方法。所述方法包括检测网络上的装置，确定该装置是无线装置。该方法还包括确定该装置已从一计算机接收数据。该方法还包括执行与该无线装置相关的病毒扫描例程。

根据本申请的第四方面，公开一种管理网络中的无线装置的例证方法。所述方法包括定义与网络中的一无线装置相关的数据备份策略。该方法还包括检测网络中的该无线装置，并分析数据备份策略，确定驻留在该无线装置上的数据应被备份。该方法还包括备份驻留在该无线装置上的数据。

这里结合下面的说明和附图，描述了本发明的方法和系统的某些例证方面。但是，这些方面只表示可采用本发明的方法、系统和媒体的原理的各种方式中的一些方式，从而所述例子意图包括这些方面和等同物。结合附图，根据下面的详细说明，其它优点和新颖特征会变得显而易见。

附图说明

结合附图，参考下面的说明，能够更完整地理解本发明的方法和系统，其中相同的附图标记表示相同的特征：

图 1 是根据本申请中描述的系统和方法，图解说明例证的企业信息处理环境的方框图；

图 2 是图解说明对等无线网络的方框图；

图 3 是图解说明具有基础设施体系结构的无线 LAN 的方框图；

图 4是图解说明自动发现网络中的无线接入点的例证方法的流程

图；

图5是图解说明管理网络中的无线装置的资产的例证方法的流程图；

图6是图解说明维护网络中的无线装置的安全性的例证方法的流程图；

图7是图解说明备份网络中的无线装置的数据的例证方法的流程图。

具体实施方式

下面参考附图说明例证方法和系统，其中相同的附图标记表示相同的部件。在下面的描述中，为了便于说明，陈述了许多具体细节，以便彻底地理解本发明的方法和系统。但是，显然可在没有这些具体细节的情况下实践本发明的方法和系统。在其它情况下，以方框图的形式表示了公知结构和装置，以便简化描述。

图1图解说明了例证的企业信息处理环境100。企业环境包括企业环境的一部分110，它包括管理并提供对数据120和应用程序125的访问的企业内部网115。构成无线局域网（“LAN”）135的一个或多个装置通过网关130可接入企业内部网115。无线LAN 135可以是本领域的技术人员已知的任意类型的无线LAN，并且可以遵守许多已建立的无线LAN标准中的任意一种标准。

目前，关于电子商务环境的标准主体集中于和硬件或基础设施相关的问题。这样的标准主体的例子包括无线以太网兼容性联盟（“WECA”），电气与电子工程师学会（IEEE），蓝牙特别利益小组（“SIG”）和无线应用协议（“WAP”）论坛。

WECA寻找证明基于802.11b规范的产品的互用性。WECA证明这样的产品兼容无线相容性认证（Wi-Fi）。WECA还赞成Wi-Fi作为跨越所有市场细分的全球无线LAN标准。

IEEE在横跨宽广频谱的技术方面进行大量的研究。IEEE创建用于无线网络的802.11标准，并且还正在帮助创建诸如有线等效保密

（WEP）之类的保密协议。IEEE 不为他们的规范提供任意类型的认证。

SIG 是由来自会员公司的雇员管理的志愿者组织。会员支持关注于特殊领域，例如工程、鉴定和市场行销的许多工作组。会员公司按照严格的鉴定程序建立并证明产品合格，同时定期在蓝牙发起的活动测试产品。

WAP 论坛提供覆盖装置测试、内容核实和一组创作准则的全面的认证和互用性测试程序，以帮助开发人员提供可互用的 WAP 应用和服务。

无线 LAN 135 可采用任意已知的网络体系结构，例如对等体系结构或基础设施体系结构。如图 2 中所示，对等无线网络 200 中的每个无线装置或客户机（210、215 和 220）与网络中指定传输范围或小区内的其它装置通信。如果无线客户机不得不与指定小区外的某一装置通信，那么该小区内的某一客户机必须起网关的作用，并实现必需的路由选择。

图 3 图解说明了具有基础设施体系结构的无线 LAN 300。在无线 LAN 300 中，多个无线客户机 310、315 和 320 之间的通信由称为接入点 325 的中央站路由。接入点 325 起桥接器的作用，并把所有通信转发给网络中的恰当客户机（不论是有线的还是无线的）。除了具有路由机构之外，接入点 325 还包括简化小型或大型商业环境中的无线通信的 DHCP 服务器和其它特征。住宅网关类似于接入点，但是不具有公司网络或高通信量环境所需的先进管理特征。在无线客户机实现任意通信之前，首先验证该无线客户机，随后使其与接入点相联系。

参见图 1，企业环境 100 包括无线广域网（“WAN”）140。无线 WAN 140 包括位于无线 LAN 的覆盖范围之外，并且由无线操作员支持的无线装置。WAN 140 可以是本领域的技术人员已知的任意类型的无线 WAN，并且可以遵守许多无线协议中的任意一种无线协议。

WAN 140 可使用的 WAN 协议的例子包括码分多址访问（“CDMA”）和全球移动通信系统（“GSM”）。在 CDMA 网络中，

大量的用户能够应请求访问无线通道。CDMA 一般由数字移动电话公司使用，性能几乎比传统的模拟蜂窝电话系统好 8-10 倍。最新一代的这种技术被称为 3G，并且受到许多移动用户的高度期盼。

GSM 是向全语音和数据支持提供全球漫游能力的无线平台。GSM 家族包括在移动装置上传送因特网内容的通用无线电分组服务（"GPRS"）平台，传送移动多媒体的增强数据速率 GSM 演进（"EDGE"）平台。一些无线电信公司以上述平台为基础提供其业务，大大影响了所实现协议的强度。

无线操作者 115 可以是提供硬件和通信基础设施从而在无线 LAN 和/或无线 WAN 环境中实现无线传输的任意机构或系统。一般来说，无线操作者 145 提供基本无线电话服务，并且可提供传送各种形式的数据的服务。

在该例证实施例中，通过无线网关 150、因特网 155 和防火墙 160，在无线操作者 145 和所述一部分企业环境 110 之间传送数据。

对实现包括无线装置的网络的企业的重要挑战涉及无线网络管理和移动装置管理。构成无线基础设施的组件包括诸如服务器、桌上型计算机和接入点之类的有线组件。这些组件应被有效监控和管理，从而维持有生产效能的工作环境。随着各种移动装置在整个企业内激增，重要的是保护、管理和监控这些装置的使用。诸如 PDA、蜂窝电话机和膝上型计算机之类的移动装置，以及保存在它们上面的资产应得到保护和管理。重要的是考虑到大部分的无线基础设施实际上是有线连接的。可通过有线企业内部网连接现有基础设施内的所有企业资产，所述有线企业内部网与提供对移动装置的无线接入的接入点连接。

无线网络管理考虑事项

根据本申请，管理无线网络的一些系统和方法提高性能，并允许管理团队快速对问题做出反应。除了提供无线网络的实时观察之外，管理解决方案还应提供未来展望，从而能够在问题发生之前，抢先采取措施防止问题。无线网络管理中需要考虑的重要事项包括：

·接入点的发现和安全。应知道、控制和计及无线网络的接入点。

由于接入点低廉并且易于安装，因此各个雇员或部门可购买一个接入点，并建立他们自己的未经授权的无线网络。由于在其默认配置方面存在缺陷，因此未经授权的接入点常常造成网络中的安全缺口。在目前的网络中，未经授权的接入点可被增加到网络中，但是许多仍然未被发现，从而导致安全措施被忽视。

·接入点布局：现有接入点同时支持的移动装置的数目因型号而异。企业应知道为了支持他们的无线用户，需要多少个接入点，并且接入点应被布置在恰当的地理位置，以使覆盖范围达到最大。良好的接入点还取决于接入点的布置的物理视线，在某些环境中，例如在具有内部办公室的建筑物内，这会是一个问题。

·故障和性能管理：类似于多数硬件组件，接入点具有发生故障的可能。另外，由于对同时存在的用户的数目的某些限制，重要的是监视容量和利用率，从而能够采取措施，以便根据需要提供另外的接入点。当策略被违背，或者如果某一组件发生故障时，应通知管理人员。管理解决方案应支持不同的标准，例如 RMON、MIB-II 和专有 MIB，以便有效地监视这些装置的状态。

·保密性和安全性：黑客最易于侵入无线网络，现有的安全措施不足以防止这种入侵。在 802.11b 标准中提供的 WEP 安全特征中，存在数个弱点。WEP 的目的是以和在有线网络中相同的水平提供无线网络中的数据机密性。但是，尽管具有众所周知的加密机制，即 RC4 密码，WEP 容易受到被动和主动攻击。这种弱点为偷听和损害无线传输的恶意方开启了无线网络。

·病毒防护：现有的企业防病毒解决方案可保护服务器、桌上型计算机和膝上型计算机，但是现有技术没有提供保护企业服务器免受通过利用移动装置作为载体感染企业的病毒的侵害的解决方案。病毒甚至能够把它们附到接入点上，偷听机密传输。

·移动管理人员的企业管理：网络管理人员应具有通过移动装置管理企业的能力。管理人员应能够通过他们的移动装置，获得所有恰当的管理工具，从而在移动过程中他们的效率能够更高。

本申请认识到最好按照统一的或者集成的方式管理有线和无线基础设施。这样，机构能够更容易地隔离会对服务质量产生不利影响的故障和性能问题。具有有线和无线支持的管理解决方案能够传送复杂的根本原因分析和端对端服务级管理。

移动装置管理考虑事项

作为无线企业的可移动部分，应在有效控制而不限制用户的自由以便通过杠杆作用充分发挥移动的优点的情况下，管理和保护类似于膝上型计算机、PDA 的装置，以及其它无线装置。关于移动装置管理的重要考虑事项包括:

·装置发现：企业管理人员应了解哪些移动装置正在网络上使用。根据本申请，跟踪并保持所有被批准装置的详细目录能够避免未经许可访问无线网络。

·软件传送：管理工具应保证所有移动装置运行正确版本的公司应用程序。例如，应在移动装置上更新最新的病毒定义码，以便保持安全性。当某一装置被更换或复制时，管理人员应能够容易地把批准的公司软件传送到用户的移动装置上，以便保持商业连续性。

·资产管理：应保护打算供公司使用的移动装置免受未经批准的应用程序和数据的影响。管理人员应保持每个移动装置的软件和硬件详细目录，并强制实施正确的策略。

·装置安全性：移动装置应包括复杂的安全特征，从而如果它们被丢失、放错地方或者被盗，在机密信息流失之前，能够容易地查找它们的位置，和使之无效。

·装置识别和跟踪：许多移动装置不具有唯一的名称或标识符，使得管理人员难以跟踪和计及所有使用中的无线装置。许多雇员可能正在使用不被企业支持的装置，并且可能成为安全漏洞。于是，批准的移动装置应被扩展到包括支持唯一标识符的能力。

·病毒防护：膝上型计算机和一些基于 Windows 的移动装置易受在 PC 上运行的病毒的影响，需要防病毒保护。虽然目前关于多数移动装置还未报道任何主要病毒，不过可能传播专门感染并破坏移动装

置上的文件和信息的新病毒。不仅应保护这些装置免受病毒攻击，而且这些装置还不应变成潜伏在无线装置上并同步感染配对 PC 或 LAN 上的其它机器的病毒的载体。

·数据保存：无线膝上型计算机和其它移动装置上的信息应被定期备份。在丢失数据的情况下，数据恢复不应复杂。

本申请认识到无线系统并不与有线基础设施无关地独立工作，无线系统被集成到 IT 基础设施中。于是，应在整个企业基础设施的环境中管理无线基础设施。专门用于并局限于无线网络的现有解决方案不能有效地把无线装置管理功能和监控企业的其它部分结合起来，从而迅速识别和解决问题。无线管理解决方案应是集成的，全面的和可靠的。这种全面的解决方案允许网络管理人员管理和保护他们的无线网络基础设施，并使他们能够改进管理效率，并保持无线应用的高水平服务。

根据本申请的一个方面，无线网络中诸如接入点和移动装置之类的装置被自动检测和识别。这种自动检测和识别确保计及无线网络中的所有组件，包括服务器、桌上型计算机、无线接入点和移动装置。产生它们的物理和逻辑连接的布局图。利用该布局图，网络管理人员能够容易地发现网络中未经批准的组件的增加，并采取恰当的行动改正特定的情形。

在一个例证的实施例中，集成的网络管理解决方案能够自动检测和识别网络中的无线装置。图 4 是图解说明自动发现诸如网络 100 之类网络中的无线接入点，例如无线接入点 325 的例证方法的方框图。

在方框 405，识别网络内的多个经授权的逻辑无线接入点。每个物理接入点可提供对网络的一个或多个无线装置接入。在方框 410，网络检测网络内的多个物理无线接入点。在方框 415，比较每个物理无线接入点和多个经授权的逻辑无线接入点，从而确定物理无线接入点是否是网络的经授权的接入点。在方框 420，如果该物理接入点未被授权，那么在方框 425，向网络管理人员或另一负责方报告未经授权的接入点，从而可采取纠正动作。

利用方法 400 收集的信息，连同和包括利用物理接入点的无线装置的其它装置相关的信息一起，可被用于建立网络的布局图。一旦发现了无线基础设施中的组件，所得到的布局图可被用于构成更有效的布局，以便提高无线网络的性能。

无线网络具有分级布局，每个移动装置与它用于连接网络的接入点相联系。当用户从一个接入点漫游到另一接入点时，布局会发生变化，以反映这种移动。按照这种方式，无线网络上的移动装置可被跟踪，据此可映射它们的位置。

无线媒体的动态本质对管理无线网络上的装置的故障和性能带来一定的挑战。除了所有有线网络共有的一组标准量度之外，无线网络具有可被监视的与无线媒体本身相关的另外一组量度。这些量度中的一些包括发射功率、干扰、重发、碎片计数、故障计数和传输速度的变化。本申请的解决方案为目前的许多接入点采用的 RMON-I、RMON-II 和 MIB-II 装置配置提供广泛的监视能力。也可收集来自厂家专有 MIB 的量度。

当接入点关闭，或者当正常操作被中断时，可提醒管理人员。利用根源分析，网络管理应用程序可确定某一网络组件是否发生故障，或者装置本身是否存在问题。也可产生定制策略，以确保无线网络组件正在有效工作。

除了管理故障和性能之外，重要的是管理对无线装置和对网络的访问。在一个实施例中，试图登录无线网络的用户可被验证，并且可检测任意异常活动。因此，能够防止入侵者获得敏感信息。可定义并强制实施安全策略，当违反某一策略时，可通知恰当的管理机构。

无线装置资产管理是无线网络管理的另一重要中心区。在一个例证实施例中，集成的网络管理解决方案可管理网络中的无线装置的资产。图 5 是图解说明管理无线网络装置的资产的例证方法的方框图。

在方框 505，定义一组经授权的资产。该组资产与网络上的一个无线装置相关。该组资产可包括硬件或软件，资产定义可足够明确，足以识别特定版本的软件或者特定修正级别的硬件。移动装置上的任

意硬件和软件资产可被管理。在方框 510 和 515，网络管理应用程序检测网络上的无线装置，并确定与检测到的无线装置实际相关或者实际驻留在检测到的无线装置上的资产。

在方框 520，分析该组经授权的资产和实际驻留在无线装置上的资产，从而识别至少一个标记资产。例如，标记资产可以是缺少的或者过时的软件组件、未经授权的硬件组件或者受损的硬件或软件组件。

在方框 525，向网络管理人员报告任意标记资产。方法 500 使得能够保持资产的详细目录，并检测和报告对政策的任意违背，从而能够自动地或者手动地对其进行改正。这可防止无线装置不遵守网络政策或者以其它方式被错误使用。

利用方法 500，通过插座（cradled）单元或者直接通过无线网络，企业软件可被传送给移动装置。这可确保统一性，并且所有移动用户在他们的装置上具有最新版本的软件，以便提高生产率，并简化支持。

图 6 是图解说明保持网络中的无线装置的安全性的例证方法 600 的流程图。在方框 605 和 610，网络检测某一装置，并确定该装置是无线装置。在方框 615，网络确定该装置最近已从可能感染计算机病毒的计算机接收数据。在方框 620，网络开始执行与该无线装置相关的病毒扫描例程。

特别为移动装置创立的 light footprint 反病毒程序可被用于保留网络免受病毒攻击。每当无线装置与配对 PC 同步，或者从配对 PC 下载信息时，可进行病毒扫描。当然，任意时候可应请求进行扫描。还可检测不会影响移动装置的 PC 病毒，从而防止移动装置成为病毒载体。

图 7 是图解说明启动网络中的无线装置的数据备份的例证方法 700 的流程图。在方框 705，为无线装置定义备份策略。在方框 710，网络检测无线装置，分析数据备份策略，确定驻留在无线装置上的数据应被备份（715）。在方框 720，执行数据备份例程。

上面描述了几个例子。当然，不可能描述用于说明与管理企业中的无线装置相关的系统、方法和计算机可读媒体的组件或方法的每种

可能组合。但是，本领域的普通技术人员会认识到其它组合和改变也是可能的。因此，本申请意图包括落入附加权利要求的范围内的所有这些变更、修改和改变。此外，就详细说明或权利要求中采用的术语“包括”来说，按照和当把术语“包含”用作权利要求中的过渡语时，解释该术语类似的方式，术语“包括”意指包括一切。

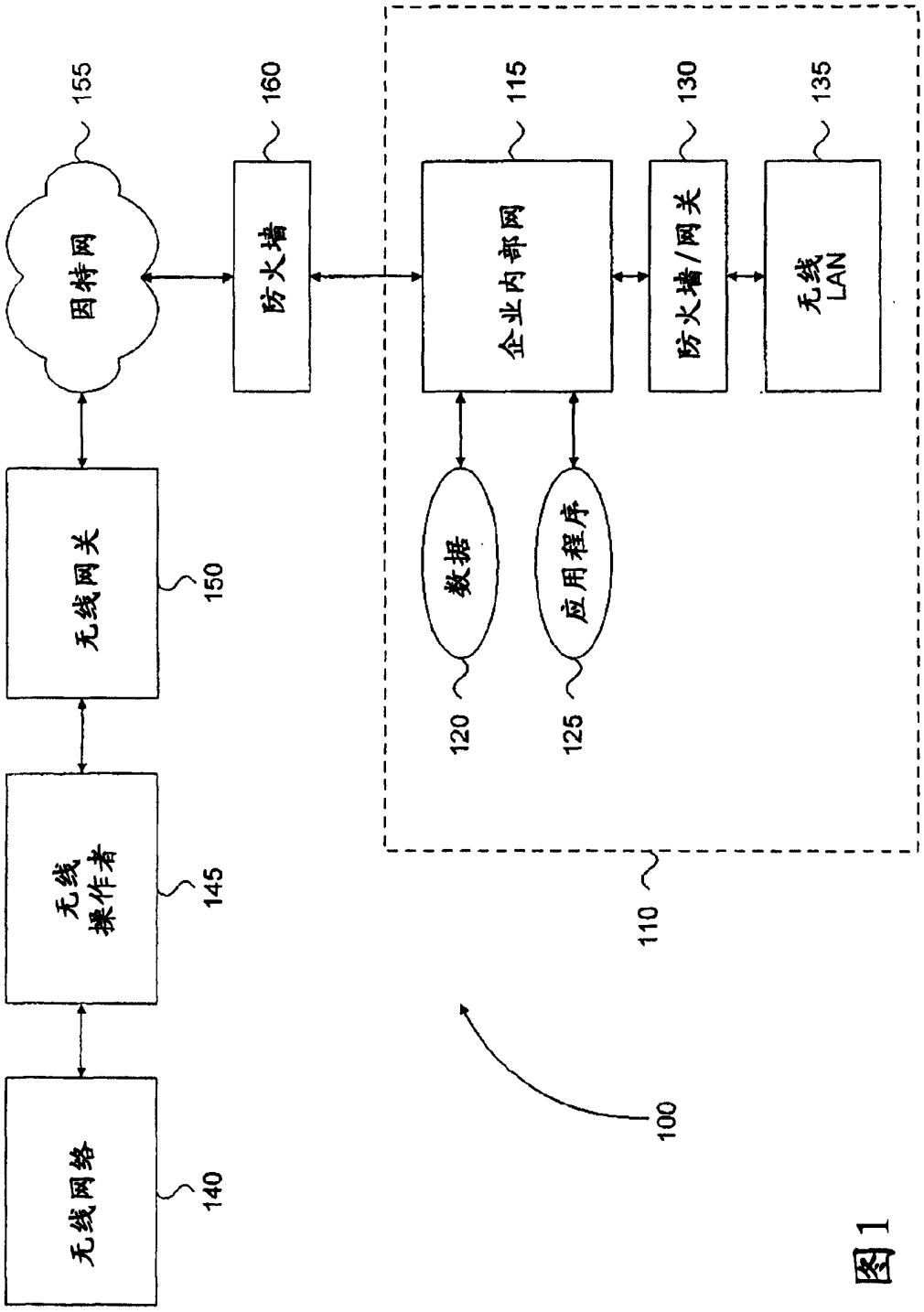

因特网
155
防火墙
160
企业内部网
115
防火墙/网关
130
无线 LAN
135
无线网关
150
数据
120
应用程序
125
无线操作者
145
无线网络
140
110
100

图1

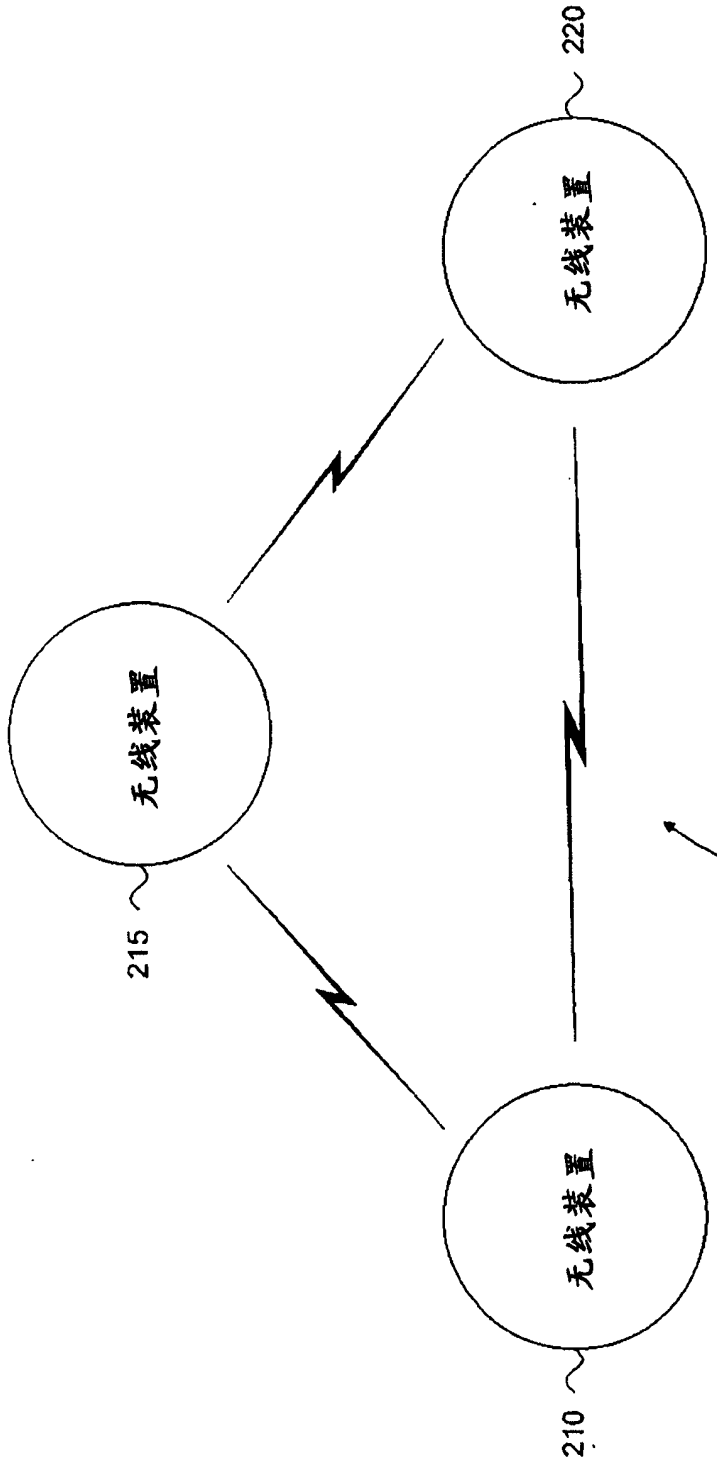


图2

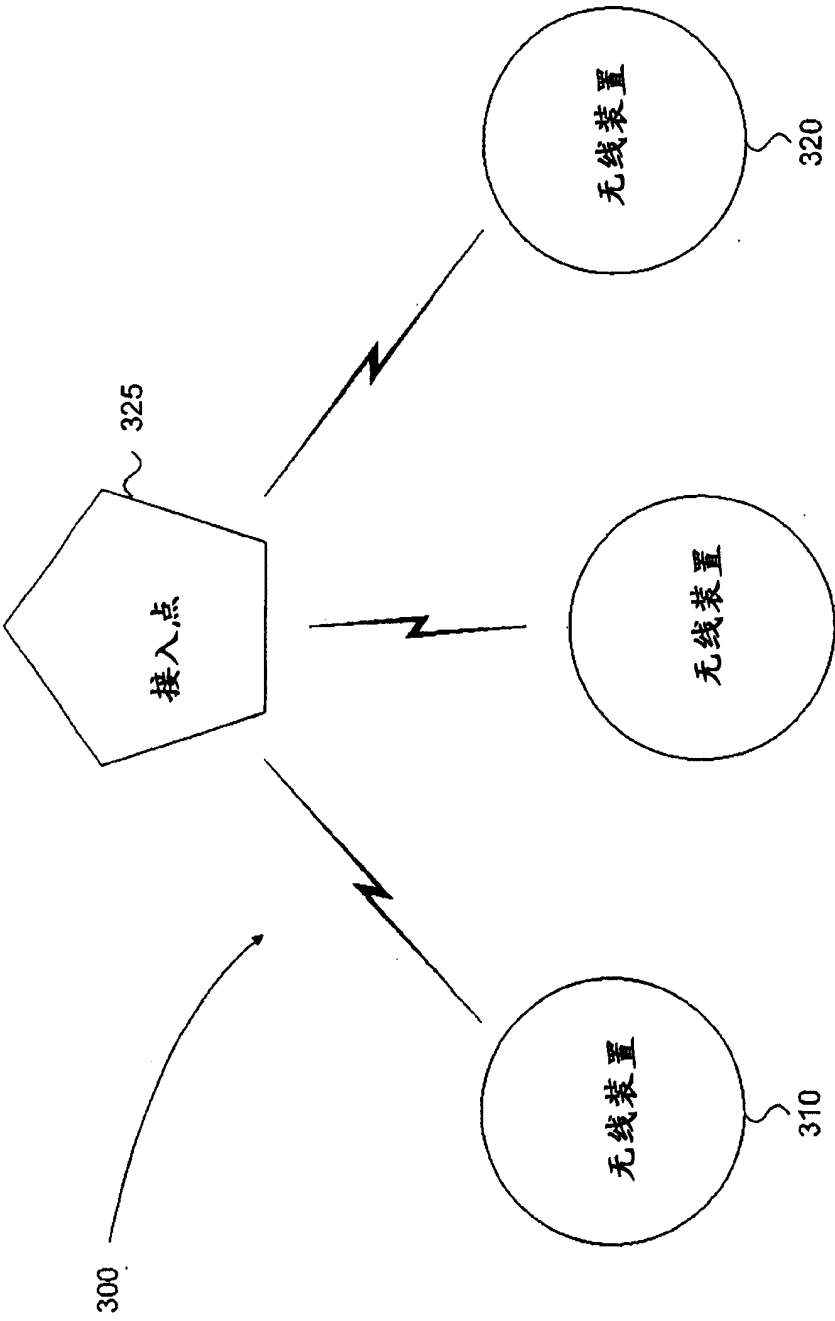


图3

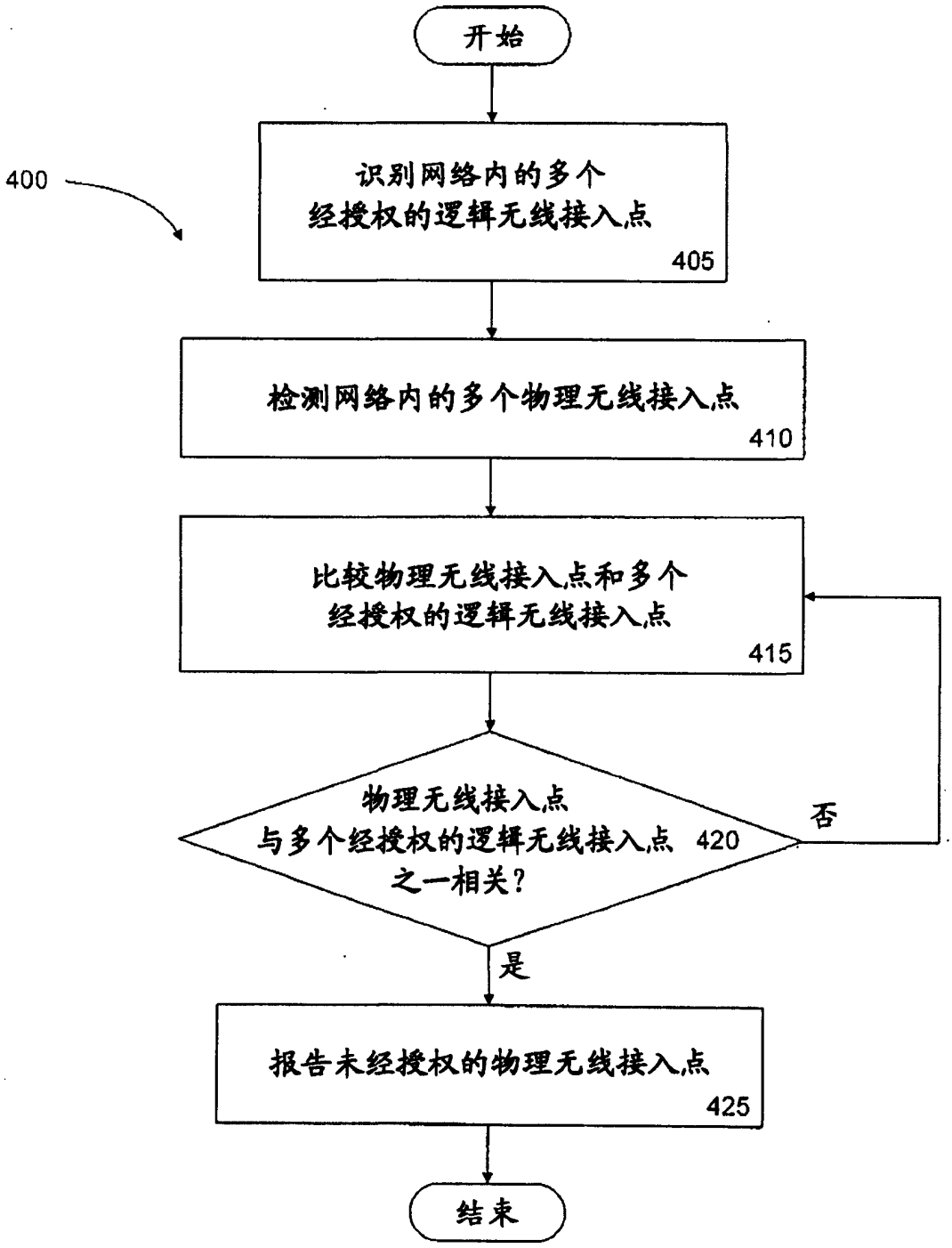

开始
400
识别网络内的多个
经授权的逻辑无线接入点
405
检测网络内的多个物理无线接入点
410
比较物理无线接入点和多个
经授权的逻辑无线接入点
415
物理无线接入点
与多个经授权的逻辑无线接入点
之一相关？
420
否
是
报告未经授权的物理无线接入点
425
结束

图4

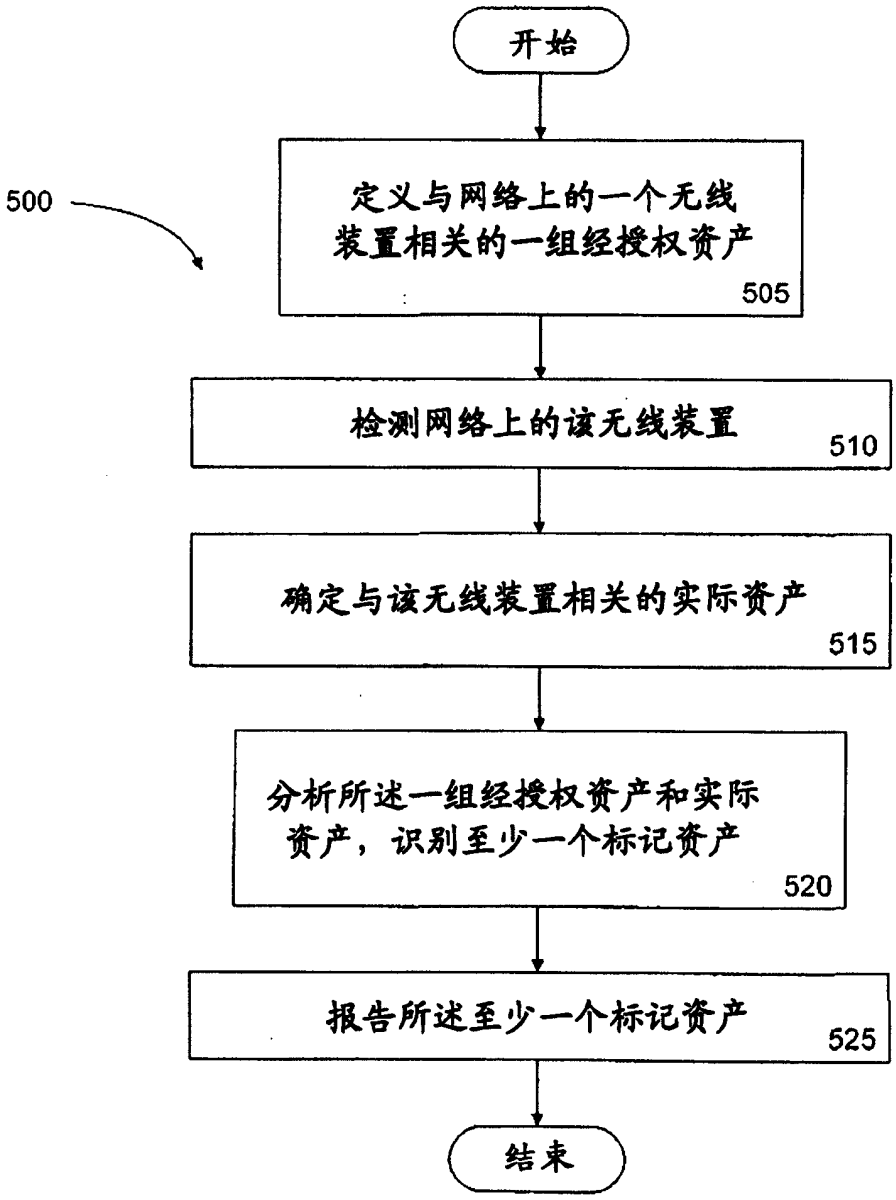

开始
500
定义与网络上的一个无线装置相关的一组经授权资产
505
检测网络上的该无线装置
510
确定与该无线装置相关的实际资产
515
分析所述一组经授权资产和实际资产，识别至少一个标记资产
520
报告所述至少一个标记资产
525
结束

图5

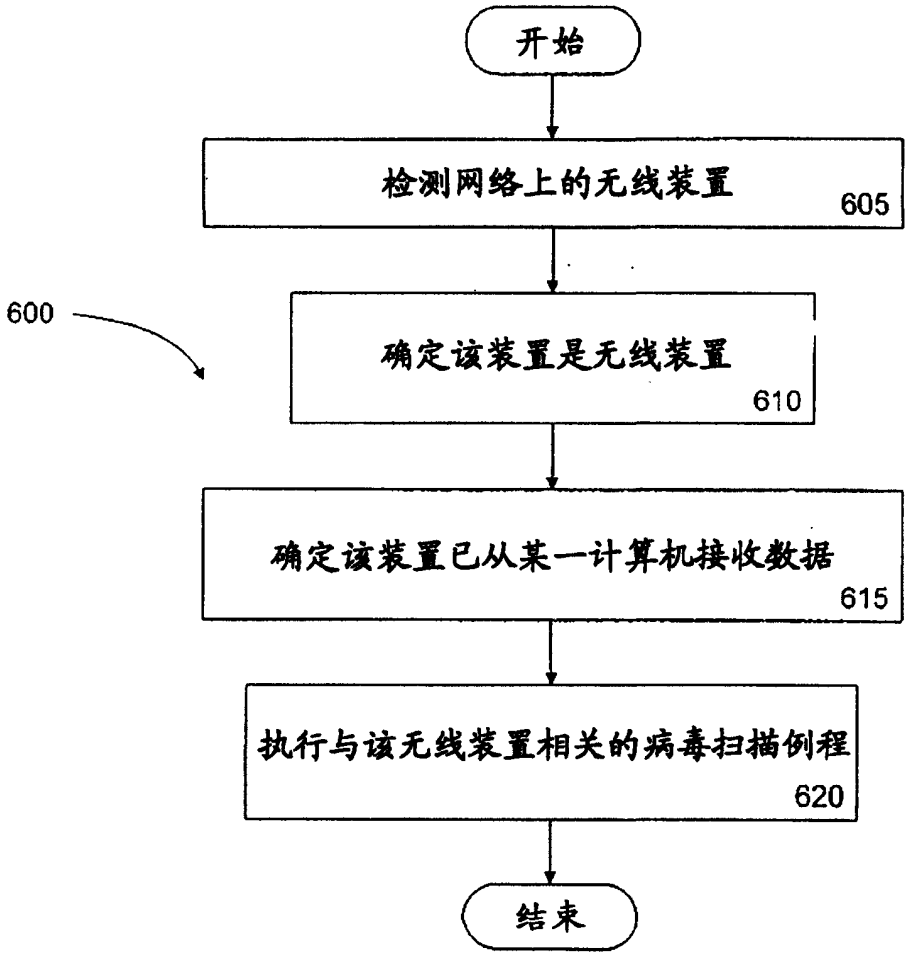

开始
检测网络上的无线装置
605
600
确定该装置是无线装置
610
确定该装置已从某一计算机接收数据
615
执行与该无线装置相关的病毒扫描例程
620
结束

图6

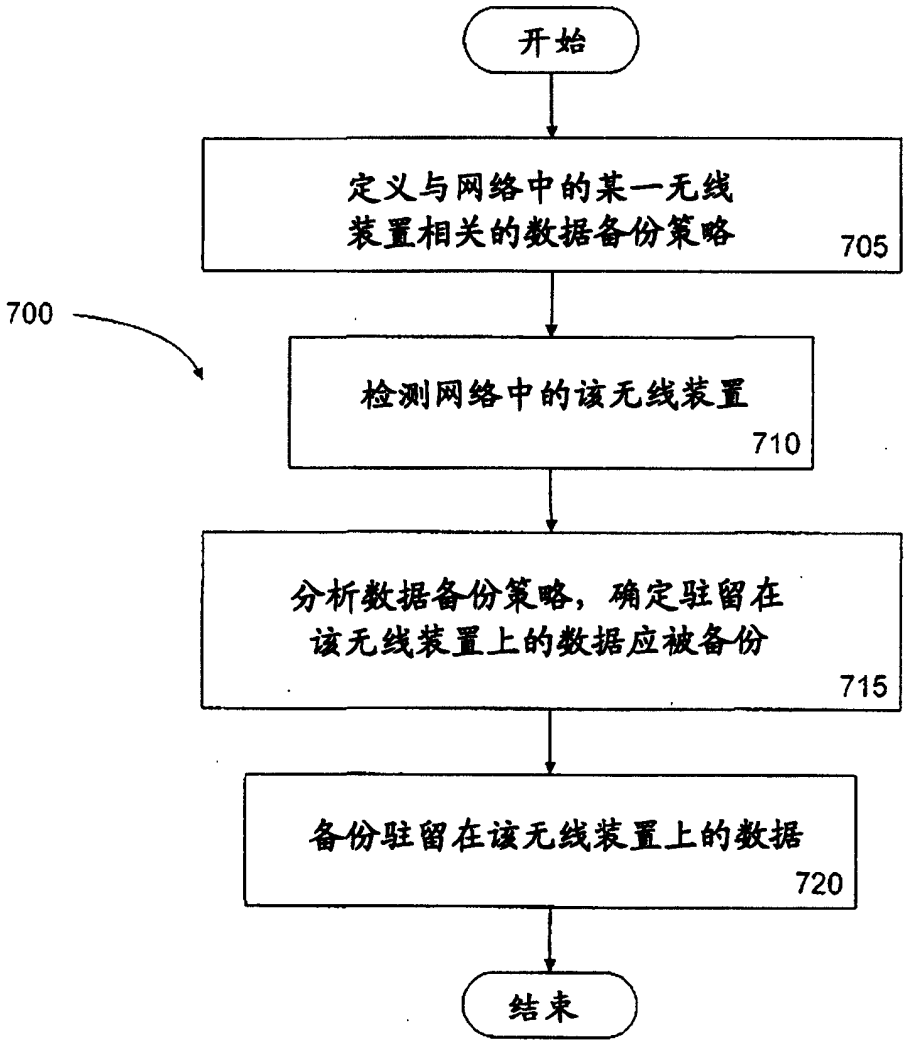

开始
定义与网络中的某一无线装置相关的数据备份策略
705
700
检测网络中的该无线装置
710
分析数据备份策略，确定驻留在该无线装置上的数据应被备份
715
备份驻留在该无线装置上的数据
720
结束

图7