(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 102089764 B
(45)授权公告日 2015.04.29

(21)申请号 200880002356.1
(22)申请日 2008.01.15
(30)优先权数据
60/880,800 2007.01.16 US
(85)PCT国际申请进入国家阶段日
2009.07.16
(86)PCT国际申请的申请数据
PCT/IB2008/000753 2008.01.15
(87)PCT国际申请的公布数据
WO2008/090470 EN 2008.07.31
(73)专利权人 绝对软件公司
地址 加拿大不列颠哥伦比亚
(72)发明人 威廉·D·戈登
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 于小宁
(51)Int.Cl.
G06F 21/00(2006.01)
(56)对比文件
US 5748084 A,1998.05.05, 全文.
CN 1799273 A,2006.07.05, 全文.
US 2006/0272020 A1,2006.11.30, 说明书第1-22段、第49-65段、第101-105段, 附图1-6.
审查员 吴卿

权利要求书2页 说明书16页 附图5页

(54)发明名称

具有与主代理配合的辅助代理的安全模块

(57)摘要

本发明旨在一种在主机装置中布置的安全模块,该安全模块提供了虽然与主机装置中的主代理配合进行操作、但是独立于主机装置的主机操作系统来进行操作、以独立地访问主机装置中的现有通信网络接口或单独的专用网络接口(如果可用的话)的辅助代理。在一方面中,本发明使能鲁棒性的盗窃赃物的找回和财物跟踪服务。该系统包括:监视中心;一个或多个受监视的装置;受监视的装置中的安全模块;以及一个或多个活动的通信网络。受监视装置可以是单独的装置,诸如计算机(例如,便携式或桌面计算机)、或是在一个系统中包括的装置或子系统。受监视的装置包括:安全模块、主代理和在受监视的装置的OS中运行的用于支持该主代理的软件。

CN 102089764 B

1. 一种用于对装置进行远程监视的系统，包括：

至少一个网络；

与所述至少一个网络相关联的该装置中的至少一个网络接口；

在该装置中提供的主机操作系统上运行的主代理，所述主代理能够经由所述至少一个网络接口来访问所述至少一个网络；

连接到所述至少一个网络的监视中心，被配置为经由所述至少一个网络接口来与主代理和辅助代理中的至少一个进行通信；以及

在该装置中提供的辅助代理，其中所述辅助代理能够独立于主机操作系统而经由所述至少一个网络接口来访问所述至少一个网络，并且其中辅助代理和主代理进行接口以配合来确定哪一个应该经由所述至少一个网络接口来访问所述至少一个网络，以向监视中心传达该装置和/或主机操作系统的属性，

其中所述配合导致所述主代理和所述辅助代理的呼叫行为的同步以及所述主代理优先于所述辅助代理进行与所述监视中心的通信。

2. 根据权利要求 1 的系统，其中所述至少一个网络包括第一和第二网络，其中所述至少一个网络接口包括用于访问所述第一网络的、主代理和辅助代理两者均可访问的主网络接口，以及专用于辅助代理访问的、经由第二网络与监视中心进行通信的辅助网络接口。

3. 根据权利要求 2 的系统，其中如果该主网络接口变为不可用，则所述辅助代理和监视中心经由该辅助网络接口来进行通信。

4. 根据权利要求 1 的系统，其中在该装置中的处理器上运行该主代理，而在相同处理器上的虚拟环境中运行该辅助代理。

5. 根据权利要求 1 的系统，其中在该装置中的处理器上运行该主代理，而对该辅助代理独立供电使得辅助代理能够独立于该处理器来起作用。

6. 根据权利要求 5 的系统，其中将该辅助代理配置为从禁用状态恢复主机操作系统的操作。

7. 根据权利要求 6 的系统，其中该辅助代理联系监视中心，并从监视中心接收用于恢复主机操作系统的操作和请求主代理联系监视中心的指令。

8. 根据权利要求 1 的系统，其中所述主代理和辅助代理以最小化网络费用的方式，来配合访问所述至少一个网络。

9. 根据权利要求 1 的系统，其中如果主代理不能起作用以访问所述至少一个网络，则该辅助代理经由所述至少一个网络接口来访问所述至少一个网络。

10. 根据权利要求 1 的系统，其中将该装置配置为当主机操作系统检测到存在辅助代理时，重新安装该主代理。

11. 根据权利要求 10 的系统，其中该主代理提供一个或多个装置跟踪和管理服务，并且其中在该装置中的永久存储位置中存储与所述服务相关联的许可。

12. 根据权利要求 11 的系统，其中一旦安装该操作系统，则自动地安装所述主代理和辅助代理，并且其中在不存在所述许可时，主代理和辅助代理卸载其自身。

13. 根据权利要求 1 的系统，其中所述至少一个网络包括蜂窝网络。

14. 根据权利要求 13 的系统，其中该监视中心通过向蜂窝网络传送 SMS 消息，来请求主代理或辅助代理联系该监视中心。

15. 根据权利要求 13 的系统，其中将该监视中心配置为在准许使用蜂窝网络服务之前、在需要供应蜂窝网络上的服务的情况下、发起该供应。

16. 根据权利要求 13 的系统，其中所述主代理或辅助代理经由与编号相关联的蜂窝调制解调器通过发送 SMS 来经由蜂窝网络联系监视中心，并且其中该监视中心能够根据在该 SMS 消息中包含的源信息来确定该编号。

17. 根据权利要求 1 的系统，其中供应所述至少一个网络上的网络服务，以响应于需要所述装置和监视中心之间的通信的预定事件、使能所述至少一个网络上的通信。

18. 根据权利要求 1 的系统，其中所述至少一个网络接口包括至少两个网络接口，其中之一独有地用于与该监视中心进行通信。

19. 根据权利要求 1 的系统，其中所述至少一个网络接口包括多个网络接口，其中所述主代理和辅助代理通过选择使用较小成本的网络来最小化网络费用。

20. 一种用于对装置进行跟踪的方法，包括 ：

提供与至少一个网络相关联的该装置中的至少一个网络接口 ；

提供在该装置中的主机操作系统上运行的主代理，所述主代理能够经由所述至少一个网络接口来访问所述至少一个网络 ；

将监视中心连接到所述至少一个网络，该监视中心被配置为经由所述至少一个网络接口与主代理和辅助代理中的至少一个进行通信 ；

在该装置中提供辅助代理，该辅助代理能够独立于主机操作系统而经由所述至少一个网络接口来访问所述至少一个网络 ；以及

在所述辅助代理和主代理之间进行接口，以配合来确定哪一个应该经由所述至少一个网络接口来访问所述至少一个网络，以向监视中心传达该装置和 / 或主机操作系统的属性，

其中所述配合导致所述主代理和所述辅助代理的呼叫行为的同步以及所述主代理优先于所述辅助代理进行与所述监视中心的通信。

具有与主代理配合的辅助代理的安全模块

[0001] 本申请要求于 2007 年 1 月 16 日提交的美国临时申请第 60 / 880,800 号的优先权。通过引用而完全合并该文献和在此引用的其他出版物，仿佛在此完全地阐述它们一样。

技术领域

[0002] 本发明涉及一种用于装置（例如，电子装置）的安全模块，具体地，涉及一种如下的安全模块，其用于与外部场所 (site) 进行通信，以用于为了诸如跟踪财物 (asset) 和协助找回 (recovery) 失窃或丢失的财物的目的来远程监视所述装置，且更具体地，涉及一种用于这种目的的无线安全模块。这种装置可以包括但不限于 :诸如，计算机之类的处理器控制的装置）和诸如影印机之类的、包括基于处理器的装置的系统。

背景技术

[0003] 转让给 Lo-Jack Corporation 的美国专利第 4,818,998 号描述了一种用于找回被盗窃汽车的方法，在该方法中，警察的跟踪车辆追踪 (home-in on) 车辆应答器 (transponder) 的周期性的无线电传送，该无线电传送被用于促使想要的车辆应答器进行回复、而在编码的车辆标识信息相同的载频上广播的命令激活信号所自动激活。

[0004] GM 的 OnStar 技术提供了一种用于向移动系统传递服务的通用无线平台。在 OnStar 的情况下，移动系统是汽车，而不是诸如膝上型计算机的用户便携式装置。OnStar 能够用于盗窃的赃物的找回，并且也可以用于传递其他服务。利用 OnStar，在用户发起事件时装置联系远程站。

[0005] 美国专利第 5,748,084 号涉及一种用于膝上型计算机或类似装置的物体的跟踪、通信、和管理系统，其中计算机中的信标 (beacon) 或收发机实现了诸如传送、破坏或编码敏感数据、并发射可跟踪的 RF 信号之类的文件完整性或装置的找回步骤。信标和主机 (host) 系统内的硬件和软件的组合发起并配合通信或安全特征的操作。例如，可以通过未能输入正确密码、篡改事件 (tampering)event 或通过对于该装置的广播信号来发起通信。在正常情况下，信标为该装置实现标准的通信功能，诸如电子邮件、语音或传真。以软件或硬件来实现对篡改的检测逻辑。进入的数据呼叫优选地包含由信标在向计算机报警或传送数据之前所解释的低级信标控制命令。优选地，在 BIOS 级别处进行低级代码的操作，以用于当较高级别的软件或插件组件已被撤销 (override) 或被移除时、执行紧急功能。

[0006] 美国专利第 6,362,736 号提供了一种用于自动定位个人电子物体的系统。该系统包括至少两个无线通信器。当通过篡改传感器或通过用户开始发觉对该系统的盗窃而确定危害了该系统的安全、并且对于计算机网络或无线网络的访问可用时，通过通信器传送由 GPS 装置确定的位置。

[0007] 美国专利第 6,636,175 号公开了一种允许用户定位位于个人或一件所有物上的远程寻呼 (paging) 装置、以确定该远程寻呼装置的物理位置的发明。通过 GPS 收发机来确定该远程装置的位置，并将其发送到位置服务提供商。然后，为用户在地图上显示该远程装置的位置。在一个实施例中，例如，在其中能够以有规律的间隔来设立蓝牙集线器 (hub) 的

游乐园或大型购物中心中使用蓝牙通信网络。

[0008] 美国专利第 6,950,946 号描述了一种用于发现和可选地找回失窃或丢失的可联网的计算机系统的方法。可联网的计算机系统生成包括安全标识符 ID 的身份信息，所述安全标识符 ID 使用加密密钥来保护。经由网络接口自动地向服务器模块发送该身份信息，在所述服务器模块中，所述身份信息被用于确定是否报告了相应计算机系统的丢失或失窃。优选地以硬件来实现该方案，这是因为操作系统 (OS) 或软件实现能够被可替换地进行修改以使该方案不激活 (deactivate)。

[0009] 美国专利申请公布第 2003 / 0117316 号公开了用于定位和跟踪无线装置的系统和方法，其包括用于存储该无线装置的位置信息的远程数据库。所述系统和方法可以包括该无线装置的安全模式并且与之协同工作，所述安全模式在装置不活动 (inactivity) 的时段期间，指导该无线装置进入低功率使用模式、睡眠模式、或关闭模式。优选地需要电子唤醒呼叫或密码来不使该安全模式激活或取消该安全模式。

[0010] 美国专利申请公布第 2006 / 0123307 号公开了一种计算机平台安全设备、系统和方法。可以操作该设备和系统、以及方法和制品 (articles) 以接收来自独立于 OS(OS-independent) 的模块的状态，所述独立于 OS 的模块能够在执行操作系统之前的某个时间处向网络提供与一装置相关联的独立于 OS 的地理位置信息。所述独立于 OS 的模块可以附着到该装置，与该装置共处一处 (co-located)，或与该装置分离。

[0011] 前述的所引用的系统都具有至少一个共有的缺点，即，假如现有通信接口变得不可用或不具备功能，则不能进行对外通信。

[0012] 作为本发明的受让人，Absolute Software Corporation（绝对软件公司）已经发展并且正在销售一种安全地跟踪财物并且找回丢失和失窃的财物的产品和服务 Computrace、以及一种通过 Computrace 技术平台来提供解决方案的安全财物跟踪、和库存 (inventory) 管理的 Absolute Track。Computrace 布置秘密行动代理 (stealth agent)，这是一种驻留在主机计算机的硬件驱动器 (hard drive) 上的软件客户端。一旦安装，该代理就在有规律地传送位置信息的基础上，联系监视中心和所有自动发现的财物数据点。在该代理和监视中心之间正在进行的通信不需要用户介入，并且经由因特网或电话连接进行维持。只要计算机被开启并且具有对于电话线的连接或者（通过 ISP 或通过公司网络的）对于因特网的访问 (access)，Computrace 代理就将能够向监视中心报告财物数据。该代理和监视中心之间的无需用户介入的通信确保了该代理的授权用户具有对于关于其整个计算机库存的最新的位置信息和综合财物数据的安全访问。无论是单独 (stand-alone) 使用、还是作为对于现有财物管理工具的补充，AbsoluteTrack 一直是一种费用低廉的应用服务，其用于帮助各种大小的企业监视远程、移动和桌面计算机，并且执行日常硬件和软件库存跟踪功能。Computrace 一直是一种用于跟踪盗窃的移动计算机、和用于找回失窃的移动计算机的有效工具。

[0013] 已经在美国和其他国家公开了作为各种 Computrace 产品和服务的基础的技术，并已取得了它们的专利权，这些专利已经共同转让给 Absolute Software Corporations。例如，参见美国专利第 5,715,174、5,764,892、5,802,280、6,244,758、6,269,392、6,300,863、和 6,507,914 号、以及相关外国专利。此外，Absolute Software Corporations 已经发表了有关 AbsoluteTrack 的信息（例如，AbsoluteTrack--Secure Computer Asset

Tracking Solution,a white paper,published Apr.25,2003(2003 年 4 月 25 日发表的白皮书“AbsoluteTrack——安全的计算机财物跟踪解决方案”))。

[0014] 可用于该代理的通信模式直接影响跟踪计算机的能力。尽管 Computrace 代理当前能够经由以太网、Wi-Fi、其他因特网或电话连接来进行通信,但是将期望开发一种这样的设备,该设备在例如由于不使用或不连接计算机持续一扩展的时段而导致的这些现有连接不可用或者变为不可用时,将准许该代理进行通信。与按日程的呼叫相反,将期望实时地发起通信。如果由于不存在主机 OS、存在不支持的 OS、存在防火墙或主机系统没有被供电而导致 Computrace 代理不能进行通信时,还将期望进行通信。即使 OS 不在运行,也将期望报告该 OS 的属性。还将期望有能力唤醒主机系统,并且执行数据保护措施或其他维护(servicing) 操作。通过下述的盗窃赃物的找回和财物跟踪系统来提供一个或多个这些所期望的特征。

发明内容

[0015] 本发明旨在一种在主机装置(例如,电子装置)中布置的安全模块,该安全模块提供了辅助代理 (secondary agent),该辅助代理与主机装置中的主代理 (host agent) 配合进行操作,但是独立于主机装置的主机操作系统来进行操作以独立地访问主机装置中的现有通信网络接口或分离的专用网络接口(如果可用的话)。可以连同可以包括财物跟踪、财物管理、财物找回、数据删除、软件布置等的服务一起布置该安全模块。

[0016] 在一方面中,本发明使能 (enable) 鲁棒性的盗窃赃物的找回和财物跟踪服务。该系统包括 :监视中心、一个或多个受监视的装置、受监视的装置中的安全模块、一个或多个活动 (active) 通信网络、(如果需要的话) 对于至少一个通信网络的预定。受监视的装置可以是单独的装置,诸如计算机 (例如,便携式或桌面计算机)、或在一个系统中包括的装置或子系统。受监视装置包括 :安全模块、主代理和在受监视的装置的 OS 中运行的用于支持该主代理的软件。

[0017] 在一个实施例中,该安全模块包括 :一个或多个网络接口、或对于该主机接口的共享访问 (access) ;应用处理器,用于与该网络进行接口 ;永久 (persistent) 存储器,从其中装载安全模块或子系统的操作环境或系统以及在该应用处理器上运行的应用 ;辅助、固件代理,用于在运行于该应用处理器上的操作环境或系统中运行 ;永久存储器,用于由固件代理使用 ;零个或多个位置确定技术,诸如 GPS。安全模块可以具有专用于安全相关通信的网络接口。所述网络接口中一个或多个可以是 WWAN 接口。安全模块包括 :可选的接口硬件和用于许可安全模块来促使主机 OS 引导或恢复 (resume) 的软件。该安全模块可以具有或可以不具有自己的电源。

[0018] 安全模块或子系统可以提供或可以不提供正常的蜂窝数据调制解调器的功能,所述功能包括 :(1) 准许受监视的计算机建立 IP 连接 ;以及 (2) 在安全模块具有蜂窝数据接口模块的情况下,准许受监视的计算机发送并接收 SMS 消息。

[0019] 优选地,安全模块的存在和操作对于计算机的用户是秘密或不显而易见的。在其中安全模块不具有其自己的电源的情况下,可以将或可以不将该系统作为整体设计为向安全模块提供独立的电源。

[0020] 如果需要,则为对于安全模块或子系统可用的网络建立数据预定。可替换地,刚刚

及时（just-in-time）地经过监视中心和通信网络之间的接口来供应该服务。

[0021] 根据本发明的安全模块利用某些行为方面来使能鲁棒性的盗窃赃物的找回和财物跟踪服务，可以将所述某些行为方面中的一个或多个合并到该系统的各实施例中。例如，主代理在预定日程或在受监视的计算机的属性的感兴趣的改变时（例如，其 IP 地址的改变）来呼叫监视中心，并且其优选在所建立的网络连接上呼叫监视中心。主代理使用典型地具有零成本或低成本的网络连接，所述网络连接包括以太网或 WiFi 网络上的 IP 连接。主代理和固件代理进行接口使得如果主代理正在正常呼叫，则仅仅是主代理呼叫。在该方面，固件代理如同故障保险（fail-safe）或“备用”通信系统。

[0022] 主代理和 / 或主代理支持软件传输典型地对于嵌入式模块不可用的受监视的计算机和 OS 的属性，所述属性包括：计算机的序列号、主机操作系统的类型、在主机操作系统中安装的应用等。该传输可以周期性地、或作为一个或多个属性的改变的结果而发生。

[0023] 如果主代理由于任何原因而没有呼叫，或被禁用，则固件代理将呼叫。因为从主代理向安全模块传输属性，所以固件代理能够向监视中心报告与主代理向监视中心报告的准许计算机被标识和要被上载的属性相同的属性。

[0024] 与其常规呼叫能力分离，主代理能够向监视中心发送信息并且从监视中心接收消息。术自监视中心的消息例如可以指示主代理应当呼叫监视中心以调用数据保护措施。这些消息可以是在 SMS 上的。

[0025] 与其常规呼叫能力分离，固件代理也能够独立地向监视中心发送信息并且从监视中心接收消息。来自监视中心的消息例如可以指示固件代理应当呼叫唤醒主机使得能够调用数据保护措施。

[0026] 如果位置确定技术在安全模块或另一子系统上可用，则主代理和 / 或固件代理可以向监视中心报告该位置。

[0027] 如果重新安装主机 OS，则经由即插即用或其他硬件检测和驱动器选择处理来检测安全模块，并且能够从 Windows 或其他 OS 安装媒体并且经由诸如 Windows 更新之类的用于驱动器的在线资源，来重新安装用于安全模块的驱动器、代理和支持软件。

[0028] 根据本发明的另一实施例，要保护的财物（例如，诸如膝上型计算机的电子装置）包括：从膝上型计算机的 OS 执行的代理和附加地能够传送并且接收的无线安全模块，并且该无线安全模块可以类似于常规的嵌入式蜂窝无线模块。该无线模块包括能够指令该模块独立于主代理来呼叫监视中心的固件。该固件可以在常规蜂窝预定用户信道上或在专用安全信道上进行呼叫。

[0029] 监视中心能够发起用于预定休眠（dormant）通信信道的请求。该特征的优点在于如果对于所述用户正常使用膝上型计算机不需要蜂窝通信预定、则用户不必维持它。在失窃的情况下，用户可以向监视中心通知该失窃，使得能够进行无线通信信道的刚刚及时的供应（provisioning），以便采取找回或数据保护步骤。

[0030] 公开技术的首要商业使用可以包括：失窃计算机的被盗窃的找回和计算机的财物跟踪管理。由于该技术的基础特性在于永久并且难以意外地移除（即使由授权用户），并且具有可靠的通信管道，其是休眠的并且能够使其苏醒、或是可修复的，该技术可以用于许多目的，所述目的包括保证任何类型的应用的安装。从这些特征中最为受益的应用是系统管理应用。

[0031] 当在具有蜂窝无线电接口的主机系统（诸如，膝上型计算机）中实现该系统时，该系统的优点在于其可以在任何时间和其中存在网络覆盖的地点处连接到监视中心。它不必等待建立有线或 WiFi 因特网连接。在独立供电的模块的情况下，由于不必等待直到膝上型计算机加电就能够进行通信，所以该优点甚至更清楚。甚至在主机系统上没有安装 OS 或安装了的不支持的 OS，也可以进行与膝上型计算机的通信。其能够经受对于主代理的完整性的攻击。其能够绕过可能屏蔽主代理的防火墙。

[0032] 根据本发明的另一实施例，该安全模块可以支持仅仅专用于安全目的的无线通信信道，所述无线通信信道允许向盗窃赃物的找回服务提供商对数据和广播 (air) 费用进行计费 (bill)。即使预定用户尚未获取个人无线服务或即使由于无论什么原因而终止了预定用户的个人服务（包括该系统的被盗窃），这也准许了通信。专用安全信道和预定用户信道两者的可用性准许开发用以基于预定用户和安全监视提供商两者的成本最优化来选择合适的通信信道的逻辑。例如，可以使用预定用户的信道并且对该预定用户计费直到所述信道由于无论什么原因而不可用为止。

[0033] 盗窃赃物的找回和财物跟踪系统可以包括已经在美国和其他国家公开并已取得了专利权的并且已经共同转让给 Absolute Software Corporation 的一个或多个各组件、特征和服务，或者与其进行交互。例如，参见美国专利第 5,715,174、5,764,892、5,802,280、6,244,758、6,269,392、6,300,863、和 6,507,914 号，通过引用而完全合并这些专利，仿佛在此完全地阐述它们一样。

附图说明

[0034] 为了更全面地理解本发明的本质和优点、以及优选的使用模式，应该对结合附图阅读的以下详细描述做出参考。在附图中，同样的附图标记指定贯穿附图中的同样或类似的部分。

[0035] 图 1 是图示了根据本发明一个实施例的、具有安全模块的受保护装置及其交互的示意功能框图。

[0036] 图 2 是示意性地表示了根据本发明一个实施例的、正常操作期间的流程处理的功能流程图。

[0037] 图 3 是示意性地表示了根据本发明一个实施例的、当主代理不活动时的流程处理的功能流程图。

[0038] 图 4 是示意性地表示了根据本发明一个实施例的、用于监视中心发起的呼叫的流程处理的功能流程图。

[0039] 图 5 是描绘了根据本发明一个实施例的、包括网络的表示性通信链路的示意图，可以通过所述表示性通信链路来实现本发明的安全模块。

具体实施方式

[0040] 本描述是用于实现本发明的目前预期的最佳模式。为了阐明本发明的一般原理的目的而做出本描述，并且不以限制性意义来理解本描述。通过参考所附权利要求来最佳地确定本发明的范围。如根据对作为本发明的基础的原理的理解将明显的，本发明可以在各种实现中找到效用，而不脱离本发明的范围和精神。为了阐明本发明的安全模块的特征和

功能的目的，可以将对跟踪和找回财物所做出的参考布置作为本发明所结合的服务的一个示例。要理解，本发明的安全模块可以用于其他服务，诸如计算机管理、备份和复原应用、远程数据删除操作等，而不脱离本发明的范围和精神。

[0041] 主要在方法或处理、操作的符号表示、本发明的功能和特征方面呈现以下详细描述。这些方法描述和表示是由本领域技术人员使用、以有效地向本领域其他技术人员告知他们工作的主旨的手段。这里并且一般地，将软件实现的方法或处理构想为导致期望结果的自身一致的 (self-consistent) 步骤序列。这些步骤需要物理量的物理操纵。经常但非必须地，这些量采用能够被存储、传输、组合、比较、和其他方式操纵的电或磁信号的形式。还将意识到，硬件和软件之间的分界线不总是分明的，本领域技术人员要理解，软件实现的处理可以以诸如以微代码和 / 或以所存储的编程指令这类的编码指令的形式以硬件、固件、或软件进行实施。

[0042] 安全模块和布置的综述

[0043] 可以在主机装置（例如，电子装置）中布置本发明的安全模块，该安全模块提供了辅助代理，该辅助代理虽然与主机装置中的主代理配合进行操作、但是独立于主机装置的主机 OS 来进行操作、以独立地访问主机装置中的现有通信网络接口或单独的专用网络接口（如果可用的话）。全部系统包括 :监视中心、一个或多个受监视主机装置、受监视主机装置中的安全模块、一个或多个通信网络、对于至少一个通信网络的预定。受监视主机装置可以是单独的装置，诸如计算机（例如，便携式或桌面计算机）、或是在系统中包括的装置或子系统。受监视装置包括 :安全模块、主代理和在受监视装置的 OS 中运行的用于支持该主代理的软件。

[0044] 本发明的安全模块可以布置为补充现有财物跟踪应用的组件、或子系统。例如，安全模块可以布置为由作为本发明受让人的 Absolute Software Corporation 开发的 AbsoluteTrack 和 / 或 Computrace 的组件。Computrace 是一种安全地跟踪财物并且找回丢失和失窃的财物的产品和服务，而 AbsoluteTrack 是通过 Computrace 技术平台来提供解决方案的一种安全财物跟踪、和财物管理、财物找回、数据删除、软件布置等。Computrace 布置秘密行动代理，这是一种驻留在客户端计算机的硬件驱动器上的软件客户端。Absolute Software Corporation 还通过提供一种用于使能、支持和 / 或提供与财物的管理和保护相关的各种服务的改进的反篡改 (tamper resistant) 维护代理（包括但不限于 :硬件、固件、软件、数据等），来改进原始的代理平台，所述各种服务包括诸如数据删除、防火墙保护、数据加密、位置跟踪、消息通知、和软件布置及更新的服务。远程服务器能够控制所述维护功能。已经在美国和其他国家公开了作为各种 Computrace 产品和服务的基础的技术，并已取得了它们的专利权，这些专利已经共同转让给 Absolute SoftwareCorporation。例如，参见美国专利第 5,715,174、5,764,892、5,802,280、6,244,758、6,269,392、6,300,863、和 6,507,914 号以及相关外国专利。在于 2005 年 3 月 28 日提交的共同待审的 (co-pending) 美国专利申请第 11 / 093,180 号（现在为公布后的美国专利公布第 US2005-0216757 号，其与 PCT 申请公布第 WO2006 / 102399 号对应）;于 2006 年 3 月 20 日提交的美国专利申请第 11 / 386,040 号（现在为公布后美国专利公布第 US2006-0272020 号）、以及于 2007 年 3 月 20 日提交的 ;美国专利申请第 11 / 726,352 号（现在为美国专利公布第 US2007-0234427A1 号 ;其与 PCT 申请公布第 WO2007 / 109366 号对应）中公开了永久代理和各种相关服务的

细节。

[0045] 此外，Absolute Software Corporation 已经发表了有关 AbsoluteTrack 的信息（例如，AbsoluteTrack--Secure Computer Asset Tracking Solution，a white paper，published Apr.25，2003(2003 年 4 月 25 日发表的白皮书“AbsoluteTrack——安全计算机财物跟踪解决方案”)）。通过引用而完全合并这些文献，仿佛在此完全地阐述它们一样。

[0046] 盗窃赃物的找回和财物跟踪系统综述

[0047] 财物跟踪和盗窃赃物的找回是可以利用本发明的装置标识应用来使能、支持、和 / 或提供服务的示例。要通过在此公开的盗窃赃物的找回和财物跟踪系统保护的装置或财物被称为主机 (host)。主机可以是膝上型计算机、手机、Blackberry、便携式电子游戏控制台 (console)、个人数字助理、音频或可视娱乐装置、医疗器械、任何包括计算机、用于保证电子或非电子财物（诸如，机动车辆、船只、和运输中的货物）的安全的任何其他电子装置或专用电子跟踪器的系统或装置。

[0048] 参考图 5，根据本发明一个实施例的财物跟踪系统含有可以包括以下主要组件的客户端 / 服务器架构 :(a) 主机装置 A 例如由所示的电子装置中的任何一个组成，所述电子装置已经被植入有可选的永久主代理和根据本发明的安全模块。为了报告布置应用（例如，包括向远程服务器报告信息和从远程服务器接收指令，以对主代理进行编程，从而支持和执行期望功能）的目的，主代理和安全模块中的辅助代理以配合的方式在主机装置 A 上运行。(b) 通信链路 B，诸如信息交换网络，其可以包括 :交换通信网络、因特网、专用和公用内部网、无线电网络、卫星网络、和线缆网络 ;以及 (c) 主机监视系统 C，其包括监视主机装置 A 和主机监视系统 C 之间的通信的主机监视服务器 3，通过来自主机装置的主机装置记录信息在有规律的或按日程的基础上来联系该主机监视服务器 3。监视服务器还向主机提供关于要执行什么动作的指令，包括了主机要执行什么动作、要收集什么数据和主机下次按日程的呼叫时间。

[0049] 根据本发明，将主机监视系统 C 配置为与主机装置 A 中的主代理和主机装置 A 中的安全模块中的辅助代理进行通信，该主机监视系统 C（例如，通过评估使用驻留在该主机装置中的装置属性收集应用所收集的数据点）远程地确定正被监视的主机装置的身份，如于 2007 年 3 月 20 日提交的美国专利申请第 11 / 726,352 号（现在为美国专利申请公布第 US2007-0234427A1 号，其与 PCT 申请公布第 WO2007 / 109366 号对应）中公开的那样。主机装置 A 经由通信链路 B 联系监视服务器。主机监视系统 C 可以包括报告和管辖端口 (reporting and administration portal)，其用于向顾客、管理员和财物跟踪服务提供商提供用于观看数据和管理监视服务器和主机装置的功能的能力。

[0050] 除了本发明的安全模块和将其集成到主机装置中之外，在于 2006 年 3 月 20 日提交的共同待审的美国专利申请第 11 / 386,040 号（现在为美国专利申请公布第 US2006-0272020 号 ;其与 PCT 申请公布第 WO2006 / 102399 对应）中已经完全公开了图 5 所示的每个组件。

[0051] 除了驻留在利用根据本发明的本发明安全模块实现的主机装置 A 中的基本主机操作系统之外，所述装置包括可以由在所述装置中存储的程序、应用、例程、和 / 或指令和 / 或逻辑的序列来选择性地进行操作、激活或配置。简言之，在此所描述和建议的方法的

使用不限于具体处理配置。依靠示例而非限制的方式，参考将膝上型或笔记本计算机参照为主机装置 A 的布置和实现的示例来描述本发明（虽然计算机 A1 被示意性地表示为桌面装置，但是可取代的可以包括便携式计算装置）。

[0052] 通信链路 B 包括任何形式的信息交换网络，在所述信息交换网络中，可以布置本发明以进行财物跟踪。由包括根据本发明的安全模块的主机装置访问的信息交换网络可以含有但不限于：分布式信息交换网络、诸如公用和专用计算机网络（例如，因特网、内部网、WWAN、WAN、LAN 等）、增值网络、通信网络（例如，有线或无线网络）、广播网络、线缆网络、蜂窝网络、无线电网络、以及这些网络的同构或异构组合。如本领域技术人员将意识到的，所述网络包括硬件和软件两者，并且可以被视为其一或两者，据此描述对于具体目的最有帮助。例如，能够将该网络描述为能够通过通信设施来互连的一组硬件节点，或可替换地将该网络描述为该通信设施，或可替换地将该网络描述为具有或不具有所述节点的该通信设施本身。还将意识到，硬件、固件和软件之间的分界线不总是分明的，本领域技术人员要理解，这些网络和通信设施、以及永久代理技术平台的组件含有软件、固件和硬件方面。

[0053] 采用安全模块的财物跟踪和盗窃赃物的找回

[0054] 现在，将更详细地描述采用安全模块（且具体地为无线安全模块）的盗窃赃物的找回和财物跟踪系统的各部分、包括安全模块的装置和操作模式。作为描述性示例，将膝上型计算机用作要保护的装置，并且在本发明中，将该膝上型计算机定义为成为无线安全模块和在安全系统中包括的各软件和固。件代理的主机。该系统的各部分包括：主机、安全模块、永久主代理、固件代理、支持软件、和监视中心。

[0055] 在该主机中存储了以计算机可读介质中或上的计算机可读指令形式的支持软件。支持软件包括：驱动器和用于将无线模块与主机进行接口的应用编程接口 (API) 层。虽然驱动器和 API 两者均基于用于蜂窝无线模块的标准驱动器，但是可按照以下方式进行扩展。扩展 API 以支持用于与固件代理进行接口所需的附加 API。扩展 API 以支持对于安全模块上的属性存储器的访问。扩展 API 以仅准许所信任的应用来调用包括上面每个 API 扩展的、安全模块的敏感功能。如果安全模块支持专用 (OTA) 安全通信信道的使用，则扩展所述 API 和驱动器以允许所信任的应用创建、管理和使用该专用的安全通信信道。

[0056] 组件之中的交互

[0057] 包括安全模块、首要主代理和监视中心的三个主要组件进行交互，以促进财物跟踪和盗窃赃物的找回功能。

[0058] A. 安全模块或子系统

[0059] 安全模块或子系统的一般属性是例如从永久应用存储器、网络接口和用于固件代理从其中读取或写入其中的数据存储器中装载的、以固件代理形式、或以其他形式的辅助代理。利用专用于与主代理进行配合以对外通信的特定功能、以及在此进一步描述的相关功能来使能辅助代理。虽然安全模块或安全子系统中的固件代理可以在蜂窝无线模块的应用处理器上运行，但是可取代的它可以驻留在受监视计算机中的其他地方。其他合适的位置包括主板上的分离的处理器或与主板分离的插件板 (board) 上的分离的处理器。固件代理具有对永久数据存储器可以读写的访问。

[0060] 可以扩展或可以不扩展位于无线模块中或者其他地方的固件，以支持专用 OTA 安全通信信道。该固件包括能够独立于在 OS 中实现的主代理、来触发对监视中心的无线呼叫

的固件代理。使用该固件代理访问的永久数据存储器中的所存储的属性，它可以担当主代理的替代者 (surrogate)。

[0061] 主机接口固件支持以下机制，用于配置和使用安全通信信道，与固件安全代理进行接口和控制固件安全代理，以及在安全模块上存储主机计算机的属性。在每种情况下，利用安全措施来保护这些机制本身，以确保仅通过授权应用能够可以使用安全通信信道。

[0062] 安全模块包括一个或多个网络接口或对于主机接口的共享访问。安全模块可以具有专用于与安全相关通信的网络接口。所述网络接口中一个或多个可以是 WWAN 接口。

[0063] 安全模块包括准许安全模块来促使主机 OS 进行引导或恢复的可选接口硬件和软件。

[0064] 根据本发明，存在无线安全模块可以采取的多个不同的物理形式，所述物理形式如下：

[0065] (i) 无线广域网 (WWAN) 数据模块：

[0066] 该模块是能够并入诸如高度便携式计算机的主机中的硬件模块。它实现与常规嵌入式蜂窝无线模块类似的功能。事实上，除非使能了本发明的安全特征，否则该模块如同常规嵌入式蜂窝无线模块唯一地地操作。

[0067] 无线安全模块可以支持一个或两个可独立计费的通信信道。用于实现两个可独立计费的信道的一种方式是让该模块表示为好像是具有分离器械标识符的两个独立的蜂窝装置。为了在信道之间进行切换，该模块从它所预定的当前网络注销，并且然后利用不同的器械 ID 随后在该网络或不同网络上注册。可替换地，该模块可以简单地支持两个完全分离的基带，每个基带报告不同的器械标识符。可替换地，可以使用完全不同的机制来准许所述通信的独立计费。

[0068] 在另一替换方案中，可以将该模块配置为、或能够配置为支持未来的 OTA 协议，该协议用于准许具有一个器械标识符的一个蜂窝无线模块来支持多个、独立计费的数据信道。

[0069] 各种膝上型计算机可以从 OEM 得到，并且包括蜂窝调制解调器（同样已知为移动宽带模块等）。例如，www.dell.com、www.hp.com、www.lenovo.com 等。这些模块通常具有（现在最普通地，一个管芯 (die) 上的）两个处理器。（同样参见，Broadcom Corporation published Product BriefEDGE / GPRS / GSM Single—Chip Multimedia Baseband Processor ;Publication No.BCM2133-PB07-D1(Broadcom 公司发表的产品简介“EDGE / GPRS / GSM 单芯片多媒体基带处理器”，出版物第 BCM2133-PB07-D1 号）;11 / 30 / 06 ; http : / / www.broadcom.com / coUateral / pb / 2133-PB07-R.pdf)。固件代理将典型地在该模块上的“应用处理器”上运行。

[0070] (ii)WWAN 子系统

[0071] 除了硬件芯片或芯片组位于主板上而不是模块中之外，这与 (i) 具有相同的功能。

[0072] (iii) 安全子系统

[0073] 在此情况下，在与膝上型计算机的主处理器分离的处理器中合并安全模块或子系统的功能。例如，可以在能够注入 (inject) 和过滤 (filter) 往返于主机的网络控制器中的分组 (packet) 的分离的处理器中合并该功能。这样的实施例的示例可以

包括作为英特尔(Intel)AMT架构内的管理引擎固件框架中的服务而运行的辅助代理:(参 见,Architecture Guide:Intel Active Management Technology,published September19,2007(2007年9月19日发表的“架构指南:Intel活动管理技术”).http://softwarecommunity.intel.com / articles / eng/1032.htm)。在AMT中,第二处理器以辅助电源(auxiliary power)运行。

[0074] (iv)虚拟化实现

[0075] 在此情况下,功能在该计算机的主处理器上的虚拟环境中运行安全模块或子系统的功能。主机OS正常运行,并且完全不知道安全环境和固件代理。(对于有关虚拟化的进一步信息,参见An overview of Virtualization:Introduction to Virtualization-Overview of Virtualization and the Most Common Types of Virtualization(“虚拟化综述:对于虚拟化的介绍——虚拟化综述和虚拟化的最常见类型”);http: / / www.virtualization.org / Virtualization / Introduction to Virtuaization.html)。“固件代理”可以作为管理程序(hypervisor)的部分或者以完全分离的OS实例运行。

[0076] B. 主代理

[0077] 根据一个实施例,主代理是在主机内部中实施的反篡改客户端模块。在本申请中,它是指从主机OS运行的代理。主机OS支持用于该装置(例如,运行MicrosoftOS的计算机、运行塞班(Symbian)OS的手机等)的用户应用的运行。在现有技术中,主代理或其组件可以是指代理、智能代理、透明代理、区段(segmented)代理、永久代理、维护代理、反篡改维护代理、应用代理、跟踪代理、秘密行动代理、可扩展代理、呼叫代理、全功能驱动器代理、部分驱动器代理、Computrace代理或其他类似项目。

[0078] 主代理周期性地或当在受监视计算机上发生感兴趣的改变时,呼叫监视中心。在呼叫期间,它可以报告受监视计算机的属性,并且如果必要,可以包括用于建立蜂窝数据连接的属性。

[0079] 主代理检测安全模块或子系统的存在,安装所需的接口和支持软件,与安全模块或子系统进行接口,并且控制安全模块或子系统。这包括同步呼叫行为,使得正常地仅仅是主代理呼叫监视中心、而固件代理不进行呼叫。但是,在用于校验该系统的正确操作的情形下,可能期望准许固件代理来呼叫监视中心。它还包括向主代理传输属性。

[0080] 如果安全模块包括蜂窝接口,则主代理可以使用该接口来发送和接收SMS消息。监视中心可以经由SMS消息来要求主代理提起蜂窝数据连接。

[0081] 如果并且当安全通信信道变为必要时,则主代理还向监视中心提供足够的信息,以便让监视中心激活对于安全通信信道的预定。例如,这包括提供无线模块的唯一的器械标识符。

[0082] 在本发明的另一实施例中,该代理只有必要时才使用安全通信信道,以用于报告主机的位置或者用于执行紧急或重要的维护任务。在一个模式中,如果预定用户信道因为不管什么原因而不可用时,才采用安全通信信道,使得由监视中心招致的服务和开销代价保持为最小。在一个实施例中,将该代理配置为在特殊情况下(例如,如果在超过预定时段中,对于经由因特网连接的尝试仍未成功,则)建立蜂窝数据连接。还可以设想其他操作模式。

[0083] 在一个实施例中，该代理支持由监视中心发起的呼叫，而不是使监视中心等待来自主机的按日程的呼叫。监视中心可以发起数据呼叫，以允许该代理在蜂窝网络上、而不是经由因特网来进行通信。为了优化成本，监视中心可以传送用于触发固件代理发起主机创建的呼叫的短消息服务 (SMS) 呼叫。这种 SMS 呼叫、或本质上类似的呼叫的类型可以促使固件代理唤醒主机，并且允许主代理进行呼叫。

[0084] 该代理可以处于不活动模式、活动模式或报警模式。在不活动模式中，该代理虽然存在，但是不做任何事情，直到通过用户建立对于安全监视或财物跟踪的预定所激活为止。在活动模式中，该代理以有规律的、预定的或随机的间隔向监视中心呼出。在报警模式中，该主机已经失窃，并且通过监视中心已经向该代理给出指令，以更频繁地呼入或执行诸如数据加密的保护任务。

[0085] C. 监视中心

[0086] 根据本发明，监视中心被配置为与主机装置网络接口进行通信，由与安全模块中的辅助代理配合的主代理来管理该访问。有时也使用其他术语来指代监视中心，所述其他术语包括 :远程站、远程服务器、服务器、主机监视系统、主机系统、远程主机系统和监视服务器。

[0087] 根据本发明的实施例，典型的监视中心可以包括 :呼叫服务器和软件、网站服务器和网站应用、数据库服务器和数据库、验证系统、管辖系统和后端处理系统。监视中心能够在诸如 IP 或 PSTN 之类的的各承运 (bearer) 服务上从主代理接受呼叫，并且能够标识计算机，确定它们的许可级别并记录它们的属性和位置，安装并更新受监视计算机上的软件，并且设立数据删除服务和盗窃赃物的找回工具。监视中心能够为用户提供网页 (web) 接口，以生成他们所监视的财物和它们的位置的报告。

[0088] 此外，本盗窃赃物的找回和财物跟踪系统的监视中心包括一个或多个新特征。例如，这些特征包括与用于 SMS 消息传送的网关的接口，其允许比在如果监视中心等待要被保护的装置根据它们的日程来进行呼入更早地发起盗窃赃物的找回操作。附加好处在于监视中心能够潜在地与离线的计算机进行通信。进一步的附加好处在于监视中心能够经由唤醒呼叫来潜在地与虽然关断但是具有分开供电的安全模块的计算机进行通信。

[0089] 监视中心可以是被安置的 (staffed) 监视服务站。可以跨越通信网络来 (例如，在不同地理区域中) 分布多个监视系统。

[0090] 与根据本发明的安全模块相关地，监视中心服务器包括 :处理器、硬盘、硬盘控制器、或其他数据存储部件，并且被配置为执行下述的附加功能中的一个或多个。可以将键盘和屏幕操作地连接到该服务器，以允许输入数据到该服务器和从该服务器读出数据，并且准许操作员与监视服务器进行交互。

[0091] 监视中心的第一附加功能是在主代理呼叫期间检测安全模块的存在，并且配置该安全模块、以及主代理的呼叫行为和固件代理的呼叫行为的同步。

[0092] 监视中心的第二附加功能是收集并存储从具有安全模块的客户端所收集的新属性。例如，这些新属性包括用于安全模块的器械标识符。

[0093] 监视中心的第三附加功能是如果需要、在适当的时间处激活对于安全通信信道的预定。该激活处理需要与承载 (carrier) 系统进行接口。可替换地，关于来自已失窃的受跟踪装置的所有者的通知，监视中心处的工作人员可以经由电话、电子邮件、传真或其他方法

来联系电信公司，以建立对于已失窃的受跟踪装置中的无线模块的预定（subscription）。

[0094] 监视中心的第四附加功能是发起对于受跟踪的计算机的呼叫。该功能在已将受跟踪装置通知为失窃时尤其有用。代替了等待受跟踪的装置在其下一按日程的时间向监视中心呼入，可以立即呼叫该受跟踪的装置，并且将主代理置入报警模式。可以在 SMS 或具有用于准许对于受监视的计算机的实时入站（inbound）通信的类似能力的另一服务上实现该技术。

[0095] 监视中心的第五功能是记录与受跟踪的装置的位置相关的附加位置信息或记录能够用于推断受跟踪的装置的位置的信息。该信息可以包括从内置于安全模块中的 GPS 收发机或与该安全模块分离的 GPS 单元所收集的坐标、可见的单元塔（cell tower）的 ID 及其相应信号强度、可见 WiFi 路由器的 MAC 地址和信号强度。在其中直接提供该装置的位置的情况下，例如在 GPS 的情况下，直接在数据库中存储该位置。在其中根据所收集的属性（例如，可见 WiFi 路由器的 MAC 地址和信号强度）来推断位置的情况下，监视中心与用于推断受监视的计算机的位置的系统进行接口。

[0096] 示范实施例

[0097] 图 1-4 图示了应用于跟踪财物（即，要保护的装置）的本发明的示例，其是通过用户在该财物上安装代理、并且该财物呼入监视中心来跟踪的。

[0098] 要保护的装置（或主机）是膝上型计算机 10。示出该膝上型计算机的一些组件和模块来帮助理解本发明，并且为了清楚已省略了其他组件和模块。，与诸如网络堆栈 / OS 服务 15 和其他驱动器 18 的其他特征一起，将主代理 14 示出为驻留在 OS13 中。主代理具有驻留在 BIOS12 中的永久模块 11。如果需要，则该永久模块恢复 51 主代理预引导（pre-boot）。可以经由计算机可读分布介质 40 在主机中安装主代理 14，在该计算机可读分布介质 40 上，承载了用于形成 MSI 文件安装器的计算机可读指令 41、连同承载了用于安装主代理的必要的代码和文件。可以使用其他类型的计算机可读介质。在 OS 内还安装了用于允许主代理与蜂窝无线安全模块 19 进行交互并控制该蜂窝无线安全模块 19 的模块驱动器 16。模块驱动器 16 可以包括压缩的代理 17，并且可以配置为如果需要、则恢复 52 主代理，从而这提供了该代理的自我修复的额外级别。主代理使能 34 基于驱动器的永久性。可以从计算机可读介质 42 将包括压缩的代理 17 的模块驱动器 16 安装到 OS 中，该计算机可读介质 42 承载了用于形成模块驱动器的安装器的计算机可读指令 43 以及必要的驱动器代码和文件，以及主代理 44 的压缩的版本。还可以经由包括了必要的驱动器代码 46 和压缩的代理 47 的 Microsoft 更新 45 来安装无线模块驱动器和压缩的代理。可替换地，还可以在操作系统安装期间或通过 Windows 更新来直接安装主代理。膝上型计算机 10 还包括：以太网接口 24、WLAN 接口 23 和 Wi-Fi 或其他调制解调器 22。

[0099] 蜂窝无线安全模块 19 包括：固件代理 21 和非易失性数据存储装置 20。尽管已经将固件代理 21 和非易失性数据存储装置 20 示为位于无线模块 19 中，但是可替换地可以将它们一起或者彼此分离地安装在膝上型计算机中的其他地方。固件代理促使计算机属性（诸如所安装的软件的细节）被电子地存储在数据存储装置 20 中。将可选电源 25 操作地连接到无线安全模块，以使得当关断主机或该主机没有连接到电源时、固件代理和无线安全模块能够进行操作。

[0100] 将主代理 14 配置为与安全模块 19 和 / 或固件代理 21 进行接口并且对它们进行

控制。将主代理 14 和固件代理 21 配置为如果在该系统中包括位置确定技术、则检索位置信息。只有主代理不呼叫时，固件代理才将呼叫。例如，如果主代理在可配置超时时段中没有对固件代理进行“ping”，则固件代理将呼叫。

[0101] 当该膝上型计算机的用户或所有者 73 开始发觉该膝上型计算机已经失窃时，该用户 73 经由电话、传真、电子邮件或任何其他可用方法来联系监视中心 71。通过监视中心的工作人员手动地、或者如果经由因特网连接或自动电话应答系统来发出该通知、则自动地在监视中心中的服务器 71 中的数据库中记录该膝上型计算机已经失窃的事实。

[0102] 如果不期望等待来自主代理的下一按日程的呼叫，则监视中心可以尝试经由 SMS 消息的传送来与主代理和 / 或固件代理进行通信。该消息指令主代理和固件代理进行呼叫。由于主代理和固件代理在几乎相同的时间处接收该消息，所以固件代理等待可配置的超时，以查看主代理是否将呼叫。如果主代理不呼叫，则固件代理将提起蜂窝数据连接并且呼叫。

[0103] 如果不存在用于受监视的计算机的蜂窝数据预定，则可以通过监视工作人员联系蜂窝网络运营商提供商公司 72 并且向他们提供用于无线模块的器械标识符来设立预定，或者这可以经由与一个或多个蜂窝网络运营商的编程接口来自动进行。很有可能在膝上型计算机已失窃或已提交数据删除请求之后，对预定进行设立。

[0104] 图 2 是示意性地表示了以下通常处理的流程图，利用该通常处理、连同主代理 14 和固件代理 21 与监视中心 70 的交互，主代理 14 和固件代理 21 进行操作。一旦主代理正在运行，在检查到已完成之后，它进入能够被设置为任何预定值的短的时段等待 200。仅用于阐明性示例，可以将该值设置为 15 分钟。在该等待时段之后，其与固件代理进行接口 210，该固件代理在其访问的非易失性存储器中存储 211 属性和下一固件代理呼叫时间 212。将下一固件代理呼叫时间典型地设置为超过该代理将与固件代理进行接口的下一时间的、将来的某些值。但是，如果该代理尚未在扩展的时段中成功地呼叫监视中心，则其可以向固件代理指示其将立即尝试呼叫。所存储的属性可以包括 OS 的属性和在计算机上安装的程序的细节。

[0105] 该代理随后检查，以查看是否到了呼叫监视中心的时间。例如，可以将用于呼叫监视中心的时间设置为每 24 个小时。如果还没有到呼叫的时间，则主代理返回等待模式 200。如果经过了用于呼叫的时间，则主代理检查因特网连接是否可用，并且如果可用，则经由因特网向监视中心进行呼叫 203。在呼叫以前，监视中心处于其正在等待要进行的进入呼叫的等待状态 206 中。一接收到呼叫 203，监视中心就处理该呼叫 207，其后，它返回到等待随后呼叫的状态。如果不存在可用的因特网连接，则主代理检查是否允许蜂窝连接 204，如果允许，则主代理提起用来呼叫 203 监视中心的蜂窝数据连接 205。

[0106] 如果该呼叫不成功 208，则主代理回到短等待 200 的状态，并且重复所述处理。如果呼叫成功，则主代理保存 209 该时间以用于其下一呼叫。

[0107] 在成功呼叫期间，监视中心可以记录呼入计算机的位置和身份，并且向主代理提供进一步指令。对于主代理的进一步指令可以用于发起时间删除处理、程序更新或加密密钥改变，并且可以包括要在终止该呼叫之后要执行的指令。

[0108] 如果存在用户蜂窝信道和专用无线安全信道这两者，则可以将主代理设置为在专用安全信道上尝试连接之前，在用户信道上进行呼叫。可取代的，可以将主代理设置为在用

户信道上尝试连接之前，在安全信道上进行呼叫。可替换地，可以通过成本最小化算法来控制信道的选择。

[0109] 图 3 是示意性地表示在其中主代理 14 不活动的情况下的固件代理 21 的处理的流程图。这可能是因为关断了计算机、不存在因特网连接或因为不知何故主代理已被禁用。在关断了计算机的情况下，安全模式必须自我供电。

[0110] 在主代理不活动的情况下，固件代理处于等待 300 短的时段中。在该等待时段之后，固件代理检查 301 是否经过了用于呼叫监视中心 70 的时间。如果没有经过该时间，则固件代理返回到等待状态 300。如果经过了用于呼叫的时间，则固件代理提起用来呼叫 303 监视中心的蜂窝数据连接 302。在该呼叫以前，监视中心处于其中正在等待要进行的进入呼叫的等待 304 的状态。一接收到呼叫 303，监视中心就处理 305 该呼叫，其后，它返回到等待随后呼叫的状态。

[0111] 如果该呼叫不成功 306，则固件代理回到 300 短等待状态，并且重复所述处理。如果该呼叫成功 307，则固件代理在其访问的非易失性存储器中存储所述属性和下一呼叫时间 308。所存储的属性可以包括 OS 的属性和在计算机上安装的程序的细节。

[0112] 图 4 是示意性地表示以下处理的流程图，其中因为不是用于呼叫的按日程的时间、所以主代理 14 和固件代理 21 处于等待时段中、但是期望向计算机进行呼叫。例如，这可能是处于其中计算机已失窃的情况下。最初，主代理、固件代理和监视中心 70 处于等待的状态中。如果向监视中心通知计算机已经失窃 400，则它将检查 401 是否存在无线数据预定，并且如果存在，则向主代理和 / 或固件代理进行呼叫 404。如果不存在该计算机对无线通信提供商的预定，则它将使用所存储或以其他方式提供的、与该计算机内的无线模块的唯一器械标识符相关的 ID 信息 402，来建立预定 403，并且然后进行无线呼叫 404。为了建立预定，监视中心可以自动或手动地联系电信提供商公司。

[0113] 由监视中心进行的无线呼叫 404 可以是 SMS 呼叫。如果主代理不活动 408（例如，如果已关闭了计算机、或如果主代理损坏），则固件代理接受呼叫，并处理 SMS 消息 409。然后，如果主代理是活动的，则其自身处理 SMS 呼叫 410。

[0114] 在其中主代理活动的情况下，SMS 呼叫 410 指令主代理回叫监视中心。SMS 呼叫结束 411、405，监视中心进入等待 406 来自受保护装置的进入呼叫的状态，并且主代理检查 412 是否存在因特网连接。如果存在，则它向监视中心进行基于因特网的呼叫 414，但是如果不存在，则它提起在其上呼叫 414 监视中心的蜂窝连接 413。监视中心处理该呼叫 407，并且然后返回到等待 406 的状态。在成功呼叫以后，主呼叫存储需要呼叫监视中心的下一时间，该时间在失窃计算机的情况下可能比在没有失窃时短得多。仅用于示例，可以将下一呼叫时间设置为在 15 分钟中的时间。主代理与固件代理进行接口 419，该固件代理在其访问的非易失性存储器中存储 422 所述属性和下一固件代理呼叫时间 421。示例呼叫时间可以在 25 分钟中的时间。此后，主代理进入等待 200 的状态，其后，主代理遵循图 2 所示的过程。

[0115] 在其中主代理不活动的情况下，固件代理将 SMS 呼叫 409 解释为用于回叫监视中心的指令。SMS 呼叫结束 415，并且然后固件代理提起在其上呼叫 417 监视中心的蜂窝数据连接 416。监视中心处理呼叫 407，并且然后返回到等待 406 的状态。例如该呼叫可以含有用于让固件代理接通计算机和 / 或唤醒主代理的指令。

[0116] 在成功呼叫以后或在成功呼叫期间，固件代理在其访问的非易失性存储器中存储所述属性和下一固件代理呼叫时间 421。固件代理然后前进到等待 300 的状态，并且继续图 3 所述的处理。

[0117] 替换实施例

[0118] 所设想的替换实施例是将无线安全模块完全集成到主机系统的主板中。这将有效地消除经由物理地移除该模块来禁用该安全模块的可能性。

[0119] 所公开的技术不限于蜂窝无线通信，而是可以采用包括个人区域网络 (PAN)、无线局域网 (WLAN) 和基于卫星的技术的其他无线或移动技术。

[0120] 在另一实施例中，无线模块可以能够进行 Wi-Fi 和 / 或 WIMAX 两者、和 / 或蜂窝无线通信。

[0121] 可以使用其中在计算机的主处理器上的虚拟环境中运行固件代理并且以计算机的主 OS 完全未知的 (unbeknownst) 方式来共享系统的网络接口的可视化技术，来实现安全模块。

[0122] 可以由独立电源来为无线安全模块供电。这可以是以专用电池或对于膝上型计算机的主电源的简单独立连接的形式。这种配置的优点在于即使当主机计算机系统关闭时，固件代理也能够通信。

[0123] 在模块独立供电的情况下，无线安全模块可以能够唤醒主机系统。如果是这种情况，则监视中心能够与固件代理进行通信，并且唤醒主机计算机例如以执行数据保护操作。

[0124] 系统管理员也能够确定受跟踪的系统的物理位置。他们还可以加强基于地理的策略，例如，计算机 X 不能被移动到所定义的地理边界之外。该代理可以在每当检测到膝上型计算机的位置改变时向监视中心呼入，以及根据预定日程进行呼入。可替换地，它可以在每当检测到处于新的位置而不是改变的位置时，进行呼入。可以通过蜂窝三角测量、WiFi 信号强度三角测量、RFID 标签技术、IP 查找或 GPS 装置来提供位置信息。

[0125] 上述实施例提供了能够有效地集成到主机装置中的安全模块，该模块与主代理配合以与外部场进行通信。能够扩展上述安全模块实施例以保护不限于上述结构和处理实施例的各种类型的装置、系统、和子系统，而不脱离本发明的范围和精神。因此，不应该通过特定实现算法来界定本发明的安全模块。

[0126] ***

[0127] 上面，已经在以框图格式和流程处理的功能模块的方面描述了本发明的处理和系统。要理解，除非在此相反地陈述，否则可以将一个或多个功能集成到单一物理装置或软件产品中的软件模块中，或者可以在单一位置处或在网络上分布的分离的物理装置或软件模块中实现一个或多个功能，而不脱离本发明的范围和精神。

[0128] 要意识到，每个模块的实际实现的详细讨论对于使得能够理解本发明不是必需的。给定在此对于系统属性、系统的功能和各功能模块的相互关系的公开，实际的实现彻底处于程序员和系统工程师的日常技术内。本领域的普通技术人员应用普通的技术可以实践本发明，而无需过度实验。

[0129] 尽管已经针对所描述的根据本发明的实施例而对本发明进行了描述，但是对本领域技术人员明显的是，可以做出各种修改和改进，而不脱离本发明的范围和精神。例如，能够容易地修改信息提取应用，来容纳不同的或附加的处理，以便向用户提供用于网页浏览

的附加灵活性。相应地，要理解，不是通过特定阐明的实施例、而是仅通过所附权利要求的范围来限定本发明。

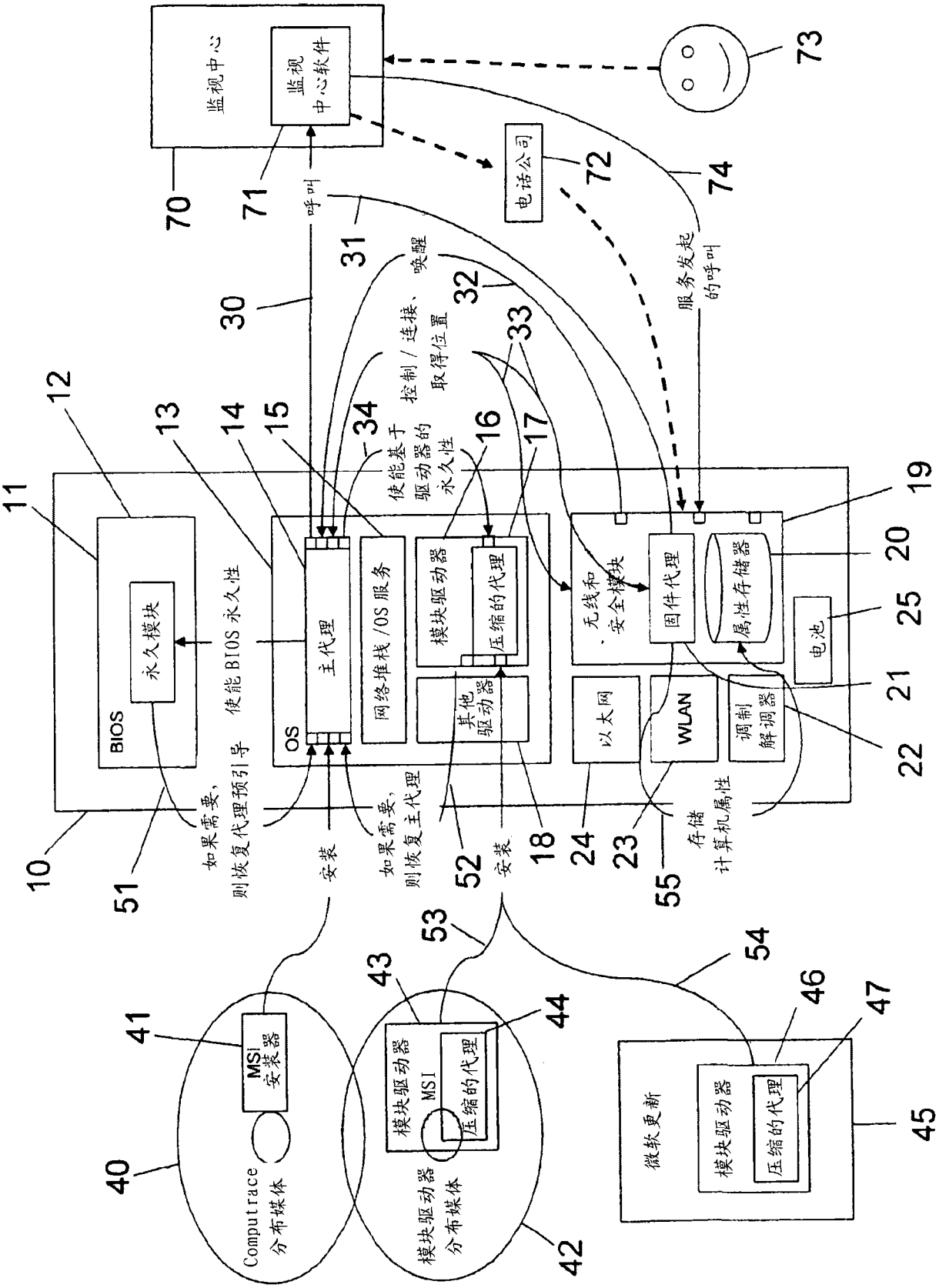
监视中心
监视中心软件
70
71
呼叫
73
电话公司
72
74
服务发起的呼叫
31
30
32
33
唤醒
控制 / 连接、取得位置
使能基于驱动器的永久性
34
16
17
12
13
14
15
11
19
20
25
21
22
BIOS
永久模块
使能 BIOS 永久性
OS
主代理
网络堆栈 /OS 服务
模块驱动器
压缩的代理
其他驱动器
无线和安全模块
固件代理
属性存储器
电池
以太网
WLAN
调制解调器
如果需要，则恢复代理预引导
如果需要，则恢复主代理
安装
存储计算机属性
10
51
52
18
24
23
55
53
54
43
41
44
46
47
45
40
42
MSI 安装器
Computrace 分布媒体
模块驱动器 MSI
压缩的代理
模块驱动器分布媒体
微软更新
模块驱动器
压缩的代理

图 1

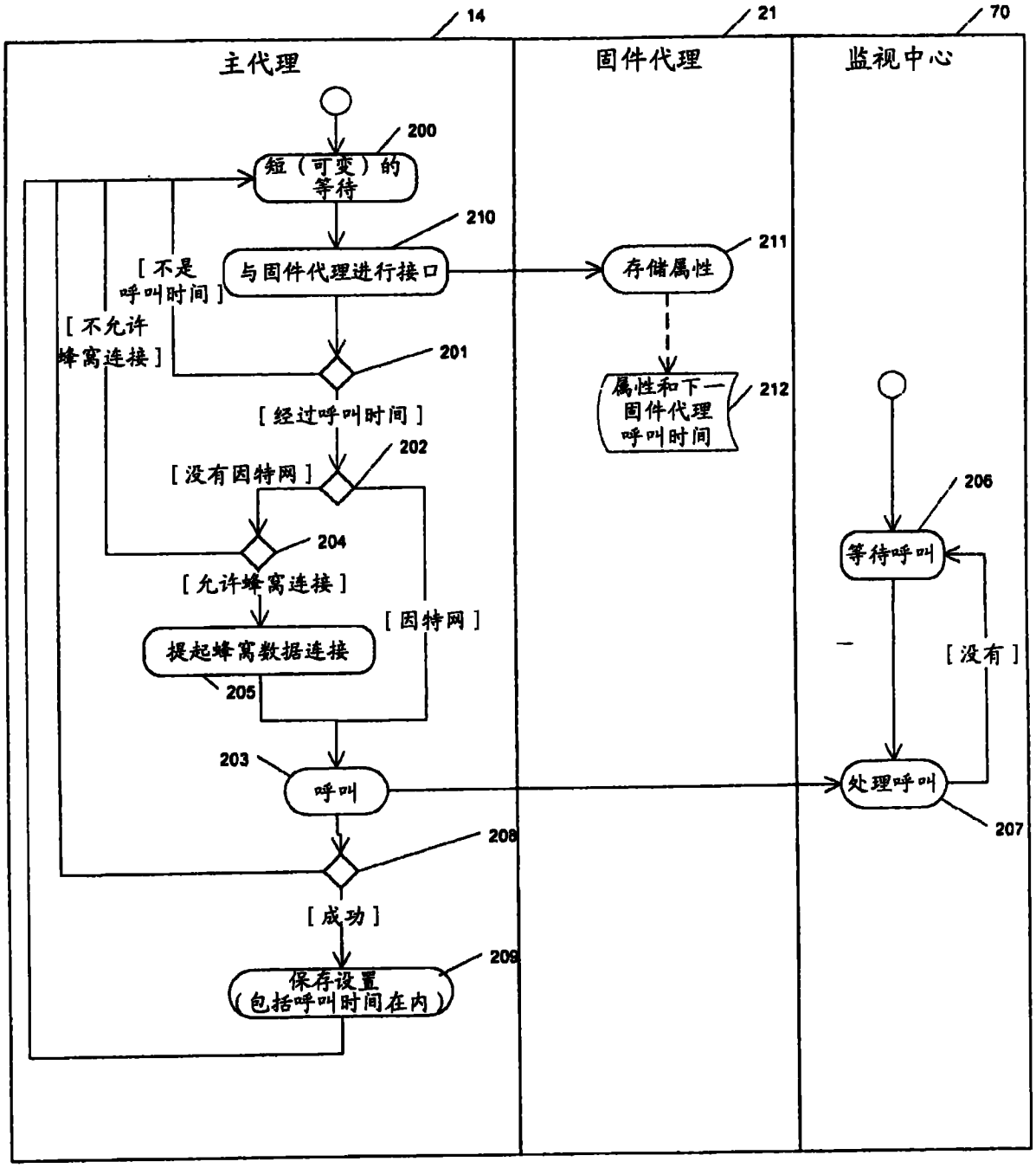
14
21
70
主代理
固件代理
监视中心
200
短（可变）的等待
210
与固件代理进行接口
211
存储属性
[不是呼叫时间]
[不允许蜂窝连接]
201
属性和下一固件代理呼叫时间
212
[经过呼叫时间]
202
[没有因特网]
206
等待呼叫
204
[允许蜂窝连接]
[因特网]
提起蜂窝数据连接
205
[没有]
203
呼叫
处理呼叫
207
208
[成功]
209
保存设置（包括呼叫时间在内）

图 2

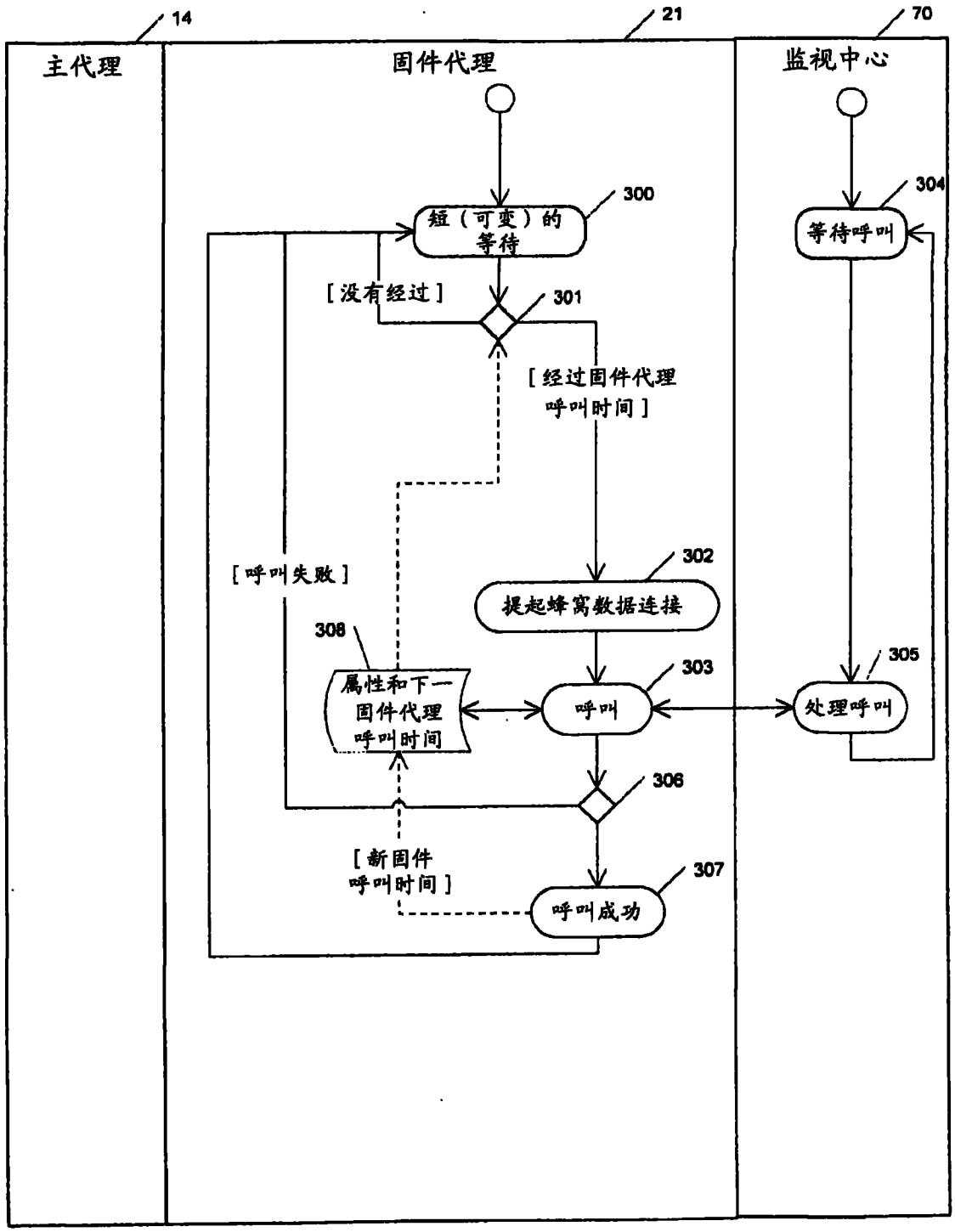
14
21
70
主代理
固件代理
监视中心
300
短（可变）的等待
304
等待呼叫
[没有经过]
301
[经过固件代理呼叫时间]
[呼叫失败]
302
提起蜂窝数据连接
308
属性和下一固件代理呼叫时间
303
呼叫
305
处理呼叫
306
[新固件呼叫时间]
307
呼叫成功

图 3

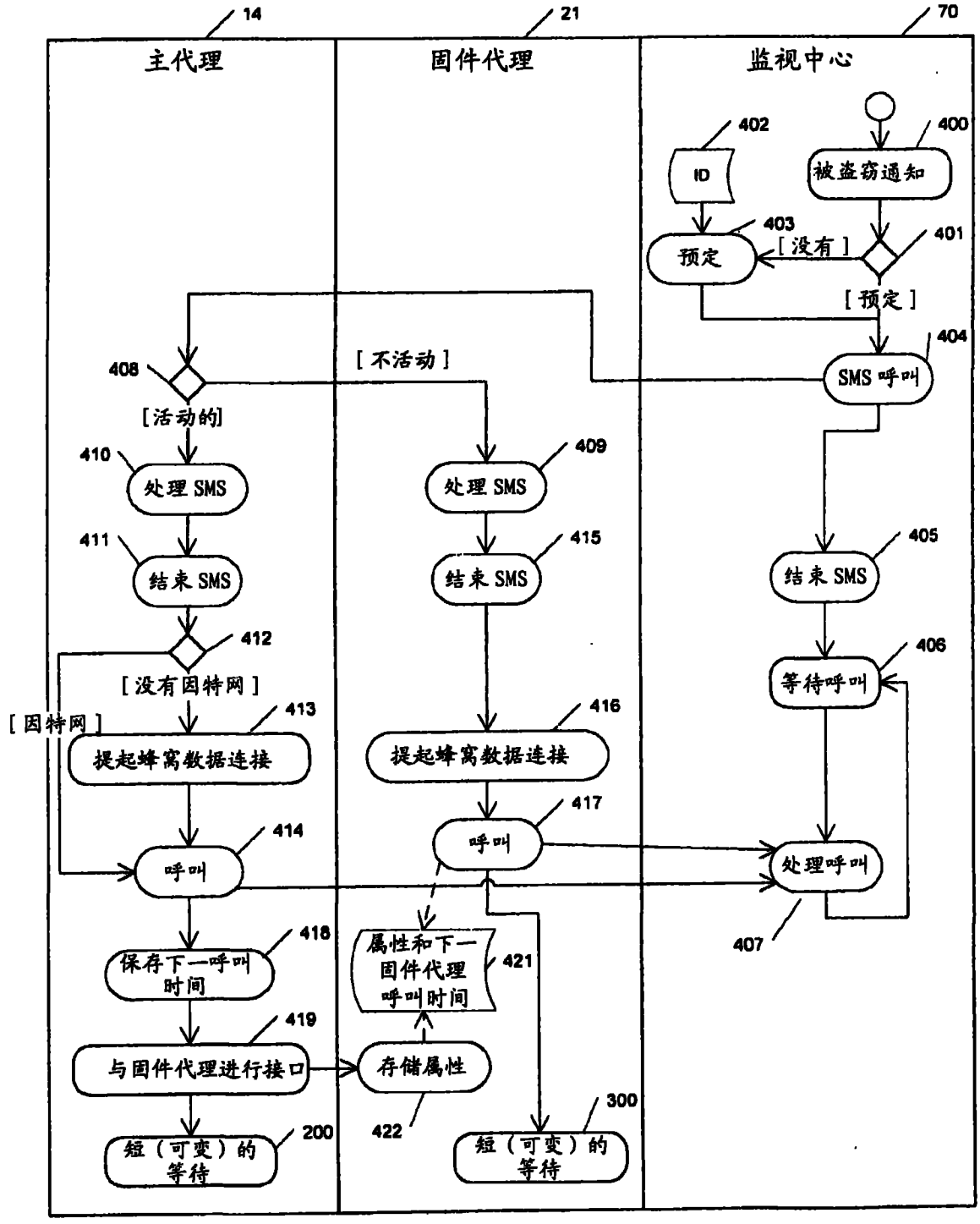
14
21
70
主代理
固件代理
监视中心
402
400
ID
被盗窃通知
403
401
预定
[没有]
[预定]
404
408
[不活动]
SMS 呼叫
[活动的]
410
409
处理 SMS
处理 SMS
411
415
405
结束 SMS
结束 SMS
结束 SMS
412
406
[没有因特网]
等待呼叫
[因特网]
413
416
提起蜂窝数据连接
提起蜂窝数据连接
417
414
呼叫
呼叫
处理呼叫
418
属性和下一
固件代理
呼叫时间
421
407
保存下一呼叫
时间
419
与固件代理进行接口
存储属性
422
300
200
短（可变）的
等待
短（可变）的
等待

图 4

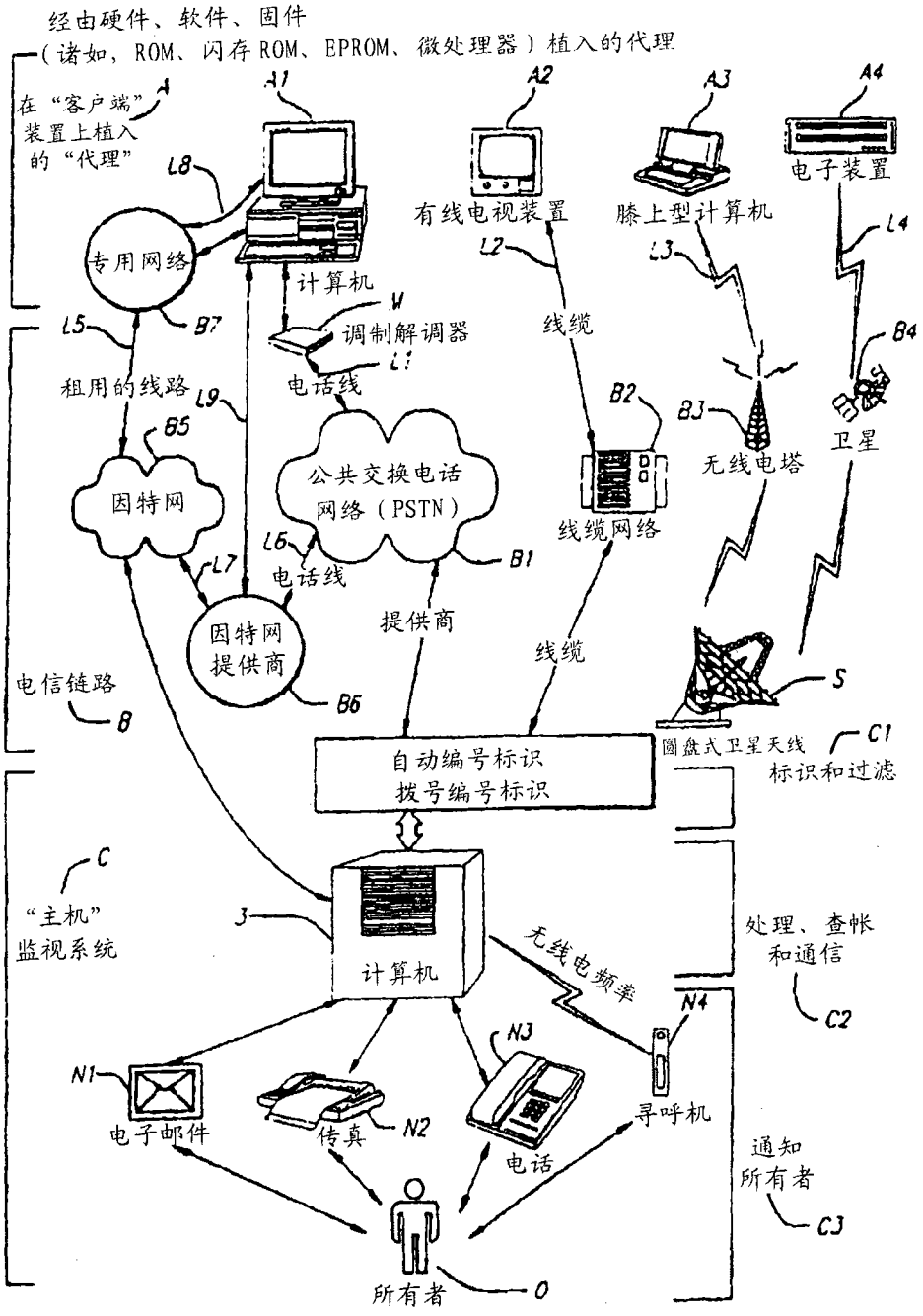
经由硬件、软件、固件
（诸如，ROM、闪存 ROM、EPROM、微处理器）植入的代理
在“客户端”装置上植入的“代理”
A
A1
A2
A3
A4
L8
专用网络
计算机
有线电视装置
膝上型计算机
电子装置
L4
L2
L3
B4
L5
B7
W
调制解调器
线缆
租用的线路
L9
L1
电话线
B2
B3
B5
公共交换电话网络（PSTN）
因特网
线缆网络
无线电塔
卫星
L6
电话线
B1
L7
因特网提供商
提供商
B6
线缆
电信链路
B
S
圆盘式卫星天线
C1
标识和过滤
自动编号标识
拨号编号标识
C
“主机”监视系统
J
计算机
无线电频率
处理、查帐和通信
C2
N4
N3
N1
电子邮件
传真
N2
电话
寻呼机
通知所有者
C3
所有者
O

图 5