(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 1604006 B
(45)授权公告日 2010.09.01

(21)申请号 200410083445.7

(22)申请日 2004.09.30

(30)优先权数据
10/676,967 2003.10.01 US

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 A·M·钱德利

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 谢喜堂

(51)Int.Cl.
*G06F 1/00*(2006.01)
*G06F 9/445*(2006.01)
*H04L 12/00*(2006.01)

(56)对比文件
US 5966081 A,1999.10.12, 说明书第2栏第27行-第3栏第47行, 第4栏第49-60行.
US 5406261 A,1995.04.11, 全文.
US 6577239 B2,2003.06.10, 说明书第4栏第30-56行.
US 6433685 B1,2002.08.13, 说明书第2栏第24-28行, 第10栏第33-52行.
US 6087937 A,2000.07.11, 全文.

审查员 齐慧峰

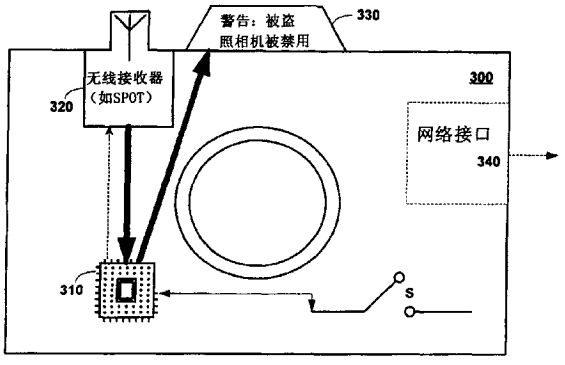
权利要求书 3 页 说明书 13 页 附图 8 页

(54)发明名称

阻止电子设备的盗窃行为的系统和方法

(57)摘要

提供了用于通过无线网络远程地关闭或防止设备的操作的系统和方法。可以使用该设备在广域网,如SPOT网络或无线载波网络上接收的一定义的命令来禁用该设备。在各种实施例中,该设备响应于预定义的命令,并本地地禁用操作。可使用覆盖代码来本地地重新启用该设备。在“保持活动”实施例中,只要该设备继续从预期的环境接收“保持活动”消息,它就操作。




CN 1604006 B

1. 一种用于阻止对电子设备的盗窃的方法，其特征在于，它包括：

响应于所述电子设备丢失的指示，由所述电子设备的接收器远程地通过网络接收一以所述电子设备为目标的禁用信号，其中所述禁用信号以一频度进行发送，该频度在从所述电子设备被报告丢失起到到期日的一时间期限内逐渐衰减；

响应于接收所述禁用信号，通过不破坏所述电子设备就无法移除的所述电子设备的组件电子地禁用所述电子设备；以及

响应于接收所述禁用信号，从所述电子设备传输与该电子设备对应的 TCP/IP 路由信息；

其中，所述电子设备的一处理器是所述组件的一部分，并且所述处理器的存在对于保持所述电子设备的开关的启用是必需的，其中所述处理器通过打开所述开关来禁用所述电子设备。

2. 如权利要求 1 所述的方法，其特征在于，所述网络是无线网络、无线电广播网络和智能个人对象技术网络中的至少一种。

3. 如权利要求 1 所述的方法，其特征在于，它还包括：

响应于接收所述禁用信号，通过所述电子设备的显示屏显示一消息。

4. 如权利要求 1 所述的方法，其特征在于，所述禁用包括通过把所述电子设备中的至少一个连接的状态 (a) 从打开改成关闭，或 (b) 从关闭改成打开来电子地禁用所述电子设备。

5. 如权利要求 1 所述的方法，其特征在于，所述禁用包括电子地禁用所述电子设备的至少一个子组件。

6. 如权利要求 1 所述的方法，其特征在于，所述组件是一处理器，并且所述禁用包括通过禁用所述处理器的至少一部分的操作来电子地禁用所述电子设备。

7. 如权利要求 1 所述的方法，其特征在于，它还包括向所述电子设备本地地输入预定义代码来重新启用所述电子设备的操作。

8. 如权利要求 1 所述的方法，其特征在于，它还包括将所述禁用信号作为 (a) 明文、(b) 至少部分加密的形式、以及 (c) 依照预定义格式编码的形式其中之一发送。

9. 一种用于阻止对电子设备的盗窃的方法，其特征在于，它包括：

响应于接收所述电子设备丢失的指示，向列表添加与所述电子设备相关联的唯一的标识符；以及

依照至少一个预定义规则，周期性地通过网络的至少一个发射器广播一以所述电子设备为目标的禁用消息，其中所述禁用信号以一频度进行发送，该频度在从所述电子设备被报告丢失起到到期日的一时间期限内逐渐衰减；

使得响应于接收所述禁用消息，所述电子设备通过不破坏所述电子设备就无法移除的所述电子设备的组件来禁用，以及，响应于接收所述禁用消息，所述电子设备传输与该电子设备对应的 TCP/IP 路由信息；

其中，所述电子设备的一处理器是所述组件的一部分，并且所述处理器的存在对于保持所述电子设备的开关的启用是必需的，其中所述处理器通过打开所述开关来禁用所述电子设备。

10. 如权利要求 9 所述的方法，其特征在于，所述网络是无线网络、无线电广播网络和

智能个人对象技术网络的至少其中之一。

11. 如权利要求 9 所述的方法，其特征在于，它还包括：

通过 (a) 所述网络、以及 (b) 所述电子设备连接于其上的第二网络中的至少一个从所述电子设备接收附加信息，所述附加信息为解析所述电子设备的位置提供基础；以及

基于所述附加信息确定所述电子设备的位置。

12. 如权利要求 9 所述的方法，其特征在于，所述广播包括周期性地将所述禁用消息作为 (a) 明文、(b) 至少部分加密的形式、以及 (c) 依照一预定格式编码的形式至少其中之一来广播。

13. 一种电子设备，其特征在于，它包括：

能够通过至少一个本地禁用信号被禁用的至少一个组件；

耦合至所述至少一个组件的处理器；以及

通信上耦合至所述处理器、用于通过网络接收一以所述电子设备为目标的远程禁用信号的接收器，其中所述远程禁用信号以一频度进行发送，该频度从所述电子设备被报告丢失起到到期日的一时间期限内逐渐衰减，

其中，响应于所述接收器接收所述远程禁用信号，所述处理器通过所述至少一个组件电子地禁用所述电子设备，以及响应于所述接收器接收所述远程禁用信号，所述电子设备传输与该电子设备对应的 TCP/IP 路由信息；

其中，所述处理器的存在对于保持所述电子设备的开关的启用是必需的，其中所述处理器通过打开所述开关来禁用所述电子设备。

14. 如权利要求 13 所述的电子设备，其特征在于，所述网络是无线网络、无线电广播网络和智能个人对象技术网络的至少其中之一。

15. 如权利要求 13 所述的电子设备，其特征在于，它还包括：

用于响应于接收所述远程禁用信号，显示消息的显示屏。

16. 如权利要求 13 所述的电子设备，其特征在于，所述至少一个组件是至少一个连接，并且所述处理器通过使所述至少一个连接的状态 (a) 从打开改到关闭，或 (b) 从关闭改到打开来电子地禁用所述电子设备。

17. 如权利要求 13 所述的电子设备，其特征在于，所述至少一个组件是所述电子设备的至少一个子组件。

18. 如权利要求 13 所述的电子设备，其特征在于，所述至少一个组件是所述处理器的至少一部分，并且所述处理组件通过禁用所述处理器的至少一部分的操作来电子地禁用所述电子设备。

19. 如权利要求 13 所述的电子设备，其特征在于，所述 TCP/IP 路由信息包括因特网协议地址和媒体访问控制地址的至少其中之一。

20. 如权利要求 13 所述的电子设备，其特征在于，所述远程禁用信号被编码为 (a) 明文、(b) 至少部分加密的形式和 (c) 依照一预定格式编码的形式至少其中之一。

21. 一种用于阻止对电子设备的盗窃的系统，其特征在于，它包括：

用于由电子设备通过网络远程地接收一以所述电子设备为目标的禁用信号的装置，其中所述禁用信号以一频度进行发送，该频度从所述电子设备被报告丢失起到到期日的一时间期限内逐渐衰减；

用于响应于接收所述禁用信号，通过不破坏所述电子设备就无法移除的所述电子设备的组件电子地禁用所述电子设备的装置；以及

用于响应于接收所述禁用信号，从所述电子设备传输与该电子设备对应的 TCP/IP 路由信息的装置；

其中，所述电子设备的一处理器是所述组件的一部分，并且所述处理器的存在对于保持所述电子设备的开关的启用是必需的，其中所述处理器通过打开所述开关来禁用所述电子设备。

# 阻止电子设备的盗窃行为的系统和方法

[0001] 版权标示和许可

[0002] 本专利文档的揭示的一部分可包含服从版权保护的材料。版权所有人不反对本专利文档或专利揭示的任何人进行传真再现，如其出现在专利商标局的专利文件或记录中，但是保留所有版权权限。以下标示应当应用到该文档中：Copyright © 2003，Microsoft Corp.

## 技术领域

[0003] 本发明涉及在丢失或盗窃的情况下为防止对丢失的设备的进一步操作而禁用设备，尤其涉及用于通过无线网络基础结构远程地关闭或防止设备的完全操作的系统和方法。

## 背景技术

[0004] 当购买财物时，任何种类的财物的盗窃是消费者或保险公司所承担的风险。由于计算设备，如膝上计算机、蜂窝电话、智能设备、个人数字助理 (PDA)、MP3 播放器等等的继续增长，以一种简单且节省成本的方式阻止那些设备的盗窃行为吸引了所有类型的消费者的注意。当今，没有这类简单的手段存在，用于阻止所有品种和种类的计算设备的盗窃行为。随着这些设备在市场上的继续增长，包括用于阻止盗窃行为的这一简单且有效的手段的能力将在市场上有可预测的重大意义。

[0005] 有一些相关的系统尝试着眼于个人财物的盗窃行为阻止。例如，对于汽车盗窃—将被盗汽车的所有者置于表面上无助的情况的一种犯罪—已经投入了相当数量的注意力。问题是一旦汽车被盗，可以相当容易地隐藏该汽车，使得它不能被清楚地看到。搜索被盗汽车是耗时的，因为可以相对快速地将汽车移动很长的距离。

[0006] 在这一点上，汽车盗窃保护装置已经存在了约 30 年，这些装置的大多数着眼于阻止盗窃行为。然而，近来的趋势也针对被盗汽车的找回。现在有若干种协助被盗汽车找回的产品。这些装置包括汽车标识号、窗蚀刻、控制车轮锁、刹车和气动踏板锁、传动锁、汽车报警切断开关和警方跟踪系统。尽管许多这些装置降低了汽车被盗的机会，但是几乎没有装置提高重新找回被盗汽车的机率。许多这些装置中所缺乏的是自动联系所有者并报告汽车被盗的能力，这令汽车找回变为一种乏味的过程，因为被隐藏的汽车很难找到。此外，这些解决方案适合汽车的特定的组件，如气动踏板，并由此是自定义作业，不能被移植到汽车的其它组件。

[0007] 一些汽车跟踪系统在汽车内放置了全球定位系统 (GPS)，使得该装置能够向在地图上显示汽车的位置的计算机报告该汽车的位置。实现这一系统的一个这样的公司是 LoJack 公司，其产品名为 LoJack。LoJack 是安装在汽车内的一种装置，但是正常地是被关闭的。当汽车的所有者注意到他们的汽车被盗，他们呼叫 LoJack 公司（或警方），并且启用该装置用于跟踪汽车。

[0008] 如图 1A 所示，LoJack 系统包括在汽车 V 的隐藏部位安装小型、安静的发射器 T，允

许警方跟踪发射器 T。由此，如图 1B 所示，当用户怀疑汽车被盗，用户将呼叫打入到警察局 P（步骤 a）。然后，警方向发射器 T 发送一信号（步骤 b），它通过 GPS 技术检索其位置（步骤 c），并将其位置发送给警察局 P（步骤 d），使得警方能够跟踪该汽车的物理位置。由此，一旦涉及警方，LoJack 被激活。也可以采用触发步骤 b-d 的其它方式。例如，LoJack 可以结合具有定制的敏感度的震动传感器一起使用，使得当汽车报警时，对汽车的骤然震动触发发射器 T 的操作，类似地，可以采用通过运动检测技术检测到汽车的进入的周边传感器。

[0009] LoJack 系统的主要缺点包括：(1) 发射器 T 报告其位置的时间可以多达一小时，(2)LoJack 通常不自动激活其自身来报告它被盗，(3) 发射器 T 不能从一辆汽车被转移到另一辆汽车，(4) 仅当汽车在户外时 GPS 能够有效地起作用，(5) 如果被发现，聪明的盗窃犯会移除 LoJack 装置以及 (6) 它仅在几个州和主要城市中可用。

[0010] 其它 GPS 跟踪系统提议，通过令装置自动地报告其位置来减少定位被盗汽车所花费的时间。例如，Joseph Picone 博士的“GTS：GPS 跟踪系统 (GTS：GPS TrackingSystem)”(2003 年 3 月）中提出的系统与其它汽车跟踪解决方案不同，所有者能够跟踪他们的汽车。GTS 提出了一种系统 (A) 能够检测汽车被盗，(B) 发射器能够通过经度和纬度确定其位置，(C) 发射器可向汽车的所有者报告其位置，(D) 所有者可以从他或她的个人计算机禁用汽车，(E) 发射器足够小，从而能够小心地隐藏在汽车中，(F) 该装置在睡眠模式用足够低的功率消耗来操作，使得当停放汽车时，该装置不会快速地耗尽汽车电池，(G) 万一汽车电池被拆离，包括了一个备用电池以及 (H) 允许所有者轮询 GTS 查找其位置，汽车是否被盗。

[0011] 为检测汽车被盗，提出的 GTS 需要使用先前已安装的汽车报警系统。它监控汽车报警器的活动来确定它是否被盗，并在汽车报警系统被装备、解除或关闭之间区别。如果汽车开始移动，GTS 使用蜂窝调制解调器来向所有者报告其位置。可以通过打开用于从汽车的燃油泵移除动力的继电器来实现禁用汽车。

[0012] 如果没有可起作用的汽车报警系统，所有者仍能够从计算机联系 GTS 并禁用汽车，但是 GTS 不能自动检测汽车何时被盗。

[0013] 然而，仍存在问题，熟练的盗窃犯能够禁用或绕过几乎任何汽车报警系统。在这点上，不论 LoJack 还是 GTS（或在汽车中隐藏装置的任一其它系统）都不能不受这类手段的影响。因此，尽管装置保持隐藏，使得它能够不引人注意地操作，聪明的盗窃犯可以确定该装置的位置并禁用其操作。

[0014] 由此，如果试图将它们应用到无线计算装置，汽车跟踪系统将遭受许多缺点。具体地，如上所述，GPS 仅在户外工作良好。此外，作为汽车的物理可分组件，如果被发现，可以移除发射器装置。

[0015] 然而，对跟踪膝上计算机投入了一些努力。依照保险公司 Safeware 公司，2001 年在美国有 591,000 台膝上计算机被盗，大约 95％的被盗膝上计算机从未被找到。由此，开发了各种防盗跟踪软件和硬件来提供对膝上计算机和数据的永久丢失的防御的底线，丢失的数据在取走膝上计算机之后会被播放。

[0016] 示例性防盗跟踪系统工作如下。首先，购买软件并安装在膝上计算机上。一旦安装了该软件，激活一小型、隐藏跟踪程序。该程序在后台运行。该软件与监控点进行通信，取决于连接至因特网的膝上计算机。一种可能性是通过因特网，该程序偶尔将其位置发送

到监控服务器或电子邮件地址。另一种方法是仅当报告被盗并启动了找回努力时，它提供位置信息。

[0017] 如果膝上计算机被盗，则联系监控和找回中心。大多数软件连同一找回服务一起供应，当通过电话、电子邮件或在 web 上呼叫并报告膝上计算机被盗时，启动该找回服务。然后开始找回过程，监控公司试图联系被盗计算机。如果发现它连接至因特网，则该公司试图使用法律强制来工作，以通过从因特网服务供应商 (ISP) 获取关于 IP 地址的信息来找回该膝上计算机。

[0018] 不是所有的跟踪软件能够在硬盘驱动器被格式化之后还继续存在。同样，有时候，如果可以安装硬件的一部分，如附加版，或者如果移除了该硬件，PC 跟踪软件不再起作用。此外，盗窃犯应当无法移除或卸载该软件来关闭跟踪，或使用进程观察器来观察并杀死该程序。本质上，由于 PC 跟踪是软件，它很容易被久经世故的黑客欺骗。

[0019] 另一提出的系统，称为 Xilinx 解决方案，提供了抗击电话盗窃的工具。Xilinx 提出了由移动电话操作者使用 IRL（因特网可重配置逻辑）技术禁用蜂窝电话的小键盘。当返回至其所有者时，可通过 IRL 比特流对电话听筒重编程以再次启用小键盘。IRL 技术启用通过任一种类的网络，包括无线网络的 CPLD（复杂可编程逻辑器件）或 FPGA（现场可编程门阵列）硬件的远程升级或编程过程。使用 Xilinx 解决方案，盗窃犯或黑客实际上不可能重新激活蜂窝电话或从电话听筒检索数据。

[0020] Xilinx 的设计安全方面不仅埋放在设备的层中，而且也遍及芯片散布，令其检测变得不可能。因此，Xilinx 提供了以下设计安全组合：(1) 防止配置模式的意外 / 有目的的重写或读回，(2) 阻止配置模式的可视或电子检测，(3) 响应于电子或激光篡改的自动设备关闭锁定以及 (4) 实际上不可检测的保护模式的物理实现。

[0021] 通过使用 Xilinx 来远程地禁用被盗移动电话内的硬件，电话操作者和制造商能够帮助移除盗窃的诱因。尽管 Xilinx 解决方案向消费者和制造商提供了一些优点，然而 Xilinx 解决方案使用微控制器作为设计的功能性要求，如键盘接口，从而允许该功能的远程禁用。因此，为实现 Xilinx 解决方案，需要关于微控制器选择的特定设计选择，以将它们集成到现有设计中。另外，该设计是硬布线的，使得为将该技术应用到蜂窝电话的不同部分，如天线，需要从无到有地重新设计微控制器需求。此外，Xilinx 解决方案描述了仅禁用整个系统的一部分。

[0022] 此外，Xilinx 解决方案不具备内建的网络传输（无线或其它），因为它依赖于作为要保护的装置的一部分可用的某一形式的通信网络，Xilinx 也未预先考虑任一形式的网络基础结构。Xilinx 解决方案也揭示了禁用设备的指令通过因特网连接 (IRL) 来传输，突出了对该设备可用的高层因特网连接和对应的因特网服务供应商的需求。

[0023] 从消费者观点来看，降低对财物的盗窃或丢失的潜在关注可移除购买电子产品的阻碍。因此，本领域需要一种简单且成本节省的计算装置阻止盗窃的方法。此外，需要一种可应用到计算装置的多个部分的阻止盗窃的方法。另外，需要一种通过包括不能被容易地移除的无线组件来调节现有网络基础结构的现有网络传输的阻止盗窃的方法。

## 发明内容

[0024] 考虑本领域的上述缺点，本发明提供了一种通过无线网络基础结构远程地关闭或

防止装置的操作的系统和方法。可使用装置在广域网上接收的定义的命令来禁用装置，如广域网如智能个人对象技术 (SPOT) 网络或无线载波网络。采用本发明的实施例，该装置响应于定义的命令，并且本地地禁用操作。可以使用覆盖代码来本地地重启用该装置。在本发明的“保持活动”实施例中，装置在连续地从预期的环境接收“保持活动”的消息时操作。在未接收“保持活动”消息的超时条件下，该装置类似于本发明的其它实施例被禁用。

[0025] 下文描述了本发明的其它优点和特征。

## 附图说明

[0026] 参考附图进一步描述了依照本发明的用于远程地禁用装置的系统和方法，附图中：

[0027] 图 1A 和 1B 示出了示例性现有技术汽车跟踪技术；

[0028] 图 2A 所示是具有可实现本发明的各种计算装置的示例性网络环境的框图；

[0029] 图 2B 所示是可实现本发明的示例性非限制计算装置的框图；

[0030] 图 3A 到 3D 示出了依照本发明的各种实施例具有接收器和处理能力的装置的示例性实现；

[0031] 图 4 示出了依照本发明警告装置它应当禁用的对被盗装置的示例性广播；

[0032] 图 5 描述了本发明的示例性实施例的示例性流程图；以及

[0033] 图 6 描述了使用 SPOT 网络实现的本发明的示例性实施例的示例性流程图。

## 具体实施方式

[0034] 综述

[0035] 本发明向 PC 和其它电子设备，如音频 / 视频播放器、数码相机、便携式摄像机、PDA 等提供了一种低成本盗窃 / 丢失预防解决方案。在一个实施例中，本发明使用了智能个人对象技术 (SPOT) 来提供与其它现有网络基础结构相关的有利结果。

[0036] 以下描述设备的丢失和由本发明启用的结果好处的情形应当被认为是示例性和非限制性的，但是尽管如此，本发明的实施例的优点的说明仍可容易地移植到市场上。

[0037] 在第一示例中，用户的图形输入板可能在机场被盗。通过仅访问 web 站点，并且用户标识其本身，该图形输入板被禁用，除向发现者提供信息并为其找回提供报酬的通知之外。

[0038] 在第二示例中，iPod 音乐播放器或数码相机被遗忘在沙滩上。在 web 站点上申请保险选项之后，申请人向保险公司报告丢失，保险公司禁用该物品并代表申请人采取适当的行动。

[0039] 在第三示例中，从一家小公司中偷走了几台膝上计算机。公司管理员在 web 站点上报告丢失。作为结果，下一次打开被盗系统时，它们显示系统被列为被盗的通知。被盗系统也尝试将警告路由到监控服务器。

[0040] 在第四示例中，从一家大企业中盗走了许多 PC。由于系统管理员使用了审查工具的“保持活动”功能，在被盗走的几个小时之内系统自动被禁用。

[0041] 在第五示例中，主要 OEM 作为分发渠道中的盗窃的结果丢失了大量的完成的系统。作为本发明应用到被盗（和将来）系统的结果，分发管理员能够显著地降低保险成本。

[0042] 如后文更详细地描述的，本发明着眼于所有上述情形以及更多情形所创建的需求。

[0043] 示例性网络化和分布式环境

[0044] 本领域的普通技术人员可以理解，本发明可以结合能够作为计算机网络的一部分展开的任一电子设备来实现，或者在分布式计算环境中实现。在这一点上，本发明涉及具有任意数量的存储器或存储单元以及跨任意数量的存储单元或卷宗出现的任意数量的应用程序和进程的任一计算机系统或环境，这些应用程序或进程可以结合用于依照本发明远程地禁用设备的过程来使用。本发明可应用到具有在具有远程或本地存储的网络环境或分布式计算环境中展开的服务器计算机和客户机计算机的环境。本发明也可应用到独立的计算装置，它们具有编程语言功能、用于结合远程或本地服务生成、接收、并发送信息的解释和执行能力。本发明尤其与在无线网络中操作的计算装置相关，尽管不限于此。

[0045] 分布式计算通过计算装置和系统之间的交换提供了计算机资源和服务的共享。这些资源和服务包括信息交换、文件的高速缓存存储和盘存储。分布式计算利用了网络连接，允许客户机发挥其集体能力来有益于整个企业。在这一点上，各种装置可具有对希望使用该装置潜逃的第三方具有重大价值的应用程序、对象或资源。

[0046] 图 2A 提供了示例性网络化或分布式计算环境的示意图。分布式计算环境包括计算对象 10a、10b 等等，以及计算对象或装置 110a、110b、110c 等等。这些对象可包括程序、模块、数据存储、可编程逻辑等等。对象可包括相同或不同设备的部分，设备如 PDA、音频 / 视频设备、MP3 播放器、个人计算机等等。每一对象可通过通信网络 14 与另一对象进行通信。该网络本身可包括向图 2A 的系统提供服务的其它计算对象和计算装置，并且其本身可代表多个互连的网络。依照本发明的一个方面，每一对象 10a、10b 等或 110a、110b、110c 等可包含可利用 API 或其它对象、软件、固件和 / 或硬件来实现用于依照本发明远程地禁用装置的过程的应用程序。计算对象或装置 10a、10b、110a、110b、110c 等的任一个也可结合使装置能够依照本发明远程地被禁用的组件，

[0047] 也可以理解，诸如 110c 等对象可被主存 (host) 在另一计算装置 10a、10b 等或 110a、110b 等上。由此，尽管所描述的物理环境可将连接的装置示为计算机，这一说明仅为示例性的，可选地可将物理装置描述为包括各种数字设备，如 PDA、电视机、MP3 播放器等，软件对象如接口、COM 对象等等。

[0048] 有支持分布式计算环境的的各种系统、组件和网络配置。例如，计算系统可以通过有线或无线系统、通过本地网络或广泛分布的网络连接在一起。当前，许多网络耦合至因特网，它为广泛分布的计算提供了基础结构，并包含许多不同的网络。任一基础结构可用于与依照本发明报告丢失或远程地禁用设备关联的示例性通信。

[0049] 服务器通常是可通过远程或本地网络，如因特网访问的远程计算机系统。客户机进程可在第一计算机系统中活动，并且服务器进程可在第二计算机系统中活动，它们通过通信媒质彼此通信，由此提供了分布式功能并允许多个客户机利用服务器的信息收集能力。例如，依据依照本发明的报告丢失所使用的任一软件对象可以跨多个计算装置或对象分布。

[0050] 客户机和服务器使用由协议层提供的功能彼此通信。例如，超文本传输协议 (HTTP) 是结合万维网 (WWW)，或“web”所使用的常见协议。通常，计算机网络地址，如因特网

协议 (IP) 地址或其它引用，如统一资源定位器 (URL) 可以用于相互标识服务器或客户机。网络地址可以被引用为 URL 地址。可通过通信媒质提供通信，如客户机和服务器可通过用于高容量通信的 TCP/IP 连接相互耦合。

[0051] 由此，图 2A 示出了一种可采用本发明的示例性网络化或分布式环境，它具有通过网络 / 总线与客户机计算机进行通信的服务器。更详细地，依照本发明，若干服务器 10a、10b 等通过通信网络 / 总线 14，可以是 LAN、WAN、内联网、因特网等，与诸如便携式计算机、手持式计算机、薄客户机、网络化设备等若干客户机或远程计算装置 110a、110b、110c、110d、110e，或诸如 VCR、TV、烤箱、灯、加热器等其它设备互连。

[0052] 例如，在通信网络 / 总线 14 是因特网的网络环境中，服务器 10a、10b 等可以是 web 服务器，客户机 110a、110b、110c、110d、110e 等可通过任一多种已知协议，如 HTTP 与其进行通信。服务器 10a、10b 等也可担当客户机 110a、110b、110c、110d、110e 等，作为分布式计算环境的特征。在适当时，通信可以是有线或无线的。客户机装置 110a、110b、110c、110d、110e 等可以是或不是通过通信网络 / 总线 14 进行通信，并可具有与其关联的独立通信。例如，在 TV 或 VCR 的情况下，可以有或没有网络化方面来控制它们。每一客户机计算机 110a、110b、110c、110d、110e 等和服务器计算机 10a、10b 等可以使用各种应用程序模块或对象 135 来装备，并使用对各种类型的存储元件或对象的连接或访问来装备，通过连接或访问可以储存数据流，或可以向连接或访问下载、发送或转移文件或数据流的各部分。计算机 10a、10b、110a、110b 等的任一个或多个可负责维护并更新数据库 20 或其它存储元件，如用于储存依照本发明处理的数据的数据库或存储器 20。由此，本发明可以在具有可访问计算机网络 / 总线 14 并与其交互的客户机 110a、110b 等，以及可与客户机 110a、110b 等和其它类似的装置交互的服务器计算机 10a、10b 等，以及数据库 20 的计算机网络环境中使用。

[0053] 示例性计算装置

[0054] 图 2B 和以下讨论旨在提供可结合其实现本发明的合适计算环境的简要一般描述。然而，应当理解，考虑手持式、便携式和其它计算装置一起所有种类的计算对象结合本发明一起使用，即，有价值的装置所处的任何地方是可从本发明的技术获益的装置。尽管下文描述了通用计算机，这仅是一个示例，本发明可以使用具有网络 / 总线互操作性和交互的薄客户机来实现。由此，本发明可以在网络化主存服务的环境中实现，其中，客户机装置仅担当到网络 / 总线的接口，如位于设备中的对象。本质上，可储存数据或可从其检索数据或向另一计算机发送数据的任何地方是用于依照本发明操作远程禁用技术的期望的或合适的环境。

[0055] 尽管并非所需，本发明可以通过操作系统部分地实现，由服务的开发者用于装置或对象，并且 / 或者本发明可以包括在结合本发明的组件操作的应用软件中。软件可以在计算机可执行指令的一般上下文环境中描述，如由一个或多个计算机，如客户机工作站、服务器或其它装置执行的程序模块。一般而言，程序模块包括例程、程序、对象、组件、数据结构等，执行特定的任务或实现特定的抽象数据类型。通常，如各种实施例所期望的，程序模块的功能可组合或分布。此外，本领域的技术人员可以理解，本发明可使用其它计算系统配置和协议来实践。适合使用本发明的其它众所周知的计算系统、环境和 / 或配置包括但不限于，个人计算机 (PC)、自动化播音机器人、服务器计算机、手持式或膝上设备、多处理器系统、基于微处理器的系统、可编程消费者电子设备、网络 PC、电器设备、灯、环境控制元件、小

型机、大型机等等。本发明也可以在分布式计算环境中实践，其中，任务由通过通信网络/总线或其它传输媒质连接的远程处理设备来执行。在分布式计算环境中，程序模块可以位于本地和远程计算机存储媒质中，包括存储器存储设备，并且客户机节点可进而担当服务器节点。

[0056] 图2B示出了适合在其中实现本发明的计算系统环境100的一个示例，尽管如上文清晰所述，计算系统环境100仅为合适的计算环境的一个示例，并非建议对本发明的使用或功能的范围的局限。也不应将计算环境100解释为对示例性操作环境100中示出的任一组件或其组合具有依赖或需求。

[0057] 参考图2，用于实现本发明的示例系统包括以常规计算机110形式的通用计算装置。计算机110的组件可包括但不限于，处理单元120、系统存储器130以及将包括系统存储器的各类系统组件耦合至处理单元120的系统总线121。系统总线121可以是若干种总线结构类型的任一种，包括存储器总线或存储器控制器、外围总线以及使用各类总线结构的局部总线。作为示例而非局限，这类结构包括工业标准体系结构(ISA)总线、微通道体系结构(MCA)总线、增强ISA(EISA)总线、视频电子技术标准协会(VESA)局部总线以及外围部件互连(PCI)总线(也称为Mezzanine总线)。

[0058] 计算机110通常包括各种计算机可读媒质。计算机可读媒质可以是可由计算机110访问的任一可用媒质，包括易失和非易失媒质、可移动和不可移动媒质。作为示例而非局限，计算机可读媒质包括计算机存储媒质和通信媒质。计算机存储媒质包括以用于储存信息的任一方法或技术实现的易失和非易失，可移动和不可移动媒质，信息如计算机可读指令、数据结构、程序模块或其它数据。计算机存储媒质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CDROM、数字多功能盘(DVD)或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存所期望的信息并可由计算机110访问的任一其它媒质。通信媒质通常在诸如载波或其它传输机制的已调制数据信号中包含计算机可读指令、数据结构、程序模块或其它数据，并包括任一信息传送媒质。术语“已调制数据信号”指以对信号中的信息进行编码的方式设置或改变其一个或多个特征的信号。作为示例而非局限，通信媒质包括有线媒质，如有线网络或直接连线连接，以及无线媒质，如声学、RF、红外和其它无线媒质。上述任一的组合也应当包括在计算机可读媒质的范围之内。

[0059] 系统存储器130包括以易失和/或非易失存储器形式的计算机存储媒质，如只读存储器(ROM)和随机存取存储器(RAM)。基本输入/输出系统(BIOS)包括如在启动时帮助在计算机110内的元件之间传输信息的基本例程，通常储存在存储器130中。存储器130通常包含处理单元120立即可访问或者当前正在操作的数据和/或程序模块。作为示例而非局限，存储器130也可包括操作系统、应用程序、其它程序模块和程序数据。

[0060] 计算机110也可包括其它可移动/不可移动、易失/非易失计算机存储媒质。例如，计算机110可包括对不可移动、非易失磁媒质进行读写的硬盘驱动器141、对可移动、非易失磁盘进行读写的磁盘驱动器以及对可移动、非易失光盘，如CD-ROM或其它光媒质进行读写的光盘驱动器。可以在示例性操作环境中使用的其它可移动/不可移动、易失/非易失计算机存储媒质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字视频带、固态RAM、固态ROM等等。硬盘驱动器通常通过不可移动存储器接口，如接口连接到系统总线121，磁盘驱动器和光盘驱动器通常通过可移动存储器接口，如接口连接到系统总线121。

[0061] 用户可以通过输入设备，如键盘和定位设备，通常指鼠标、轨迹球或触摸板向计算机 110 输入命令和信息。其它输入设备可包括麦克风、操纵杆、游戏垫、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通常通过耦合至系统总线 121 的用户输入接口 140 和关联的接口连接至处理单元 120，但是也可以通过其它接口和总线结构连接，如并行端口、游戏端口或通用串行总线 (USB)。图形子系统可也连接至系统总线 121。监视器或其它类型的显示设备也通过接口，如输出接口 150 连接至系统总线 121，可进而与视频存储器进行通信。除监视器之外，计算机也包括其它外围输出设备，如扬声器和打印机，通过输出接口 150 或其类似物连接。

[0062] 计算机 110 可以在使用到一个或多个远程计算机，如远程计算机 170 的逻辑连接的网络化环境中操作。远程计算机 170 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它公用网络节点，并通常包括许多或所有上述与计算机 110 相关的元件。图 2B 描述的逻辑连接包括网络 171，如局域网 (LAN) 和广域网 (WAN)，但也可包括其它网络 / 总线。这类网络环境常见于家庭、办公室、企业范围计算机网络、内联网以及因特网。

[0063] 当在 LAN 网络环境中使用时，计算机 110 通过网络接口或适配器连接至 LAN171。当在 WAN 网络环境中使用时，计算机 110 可包括调制解调器或其它装置，用于通过 WAN，如因特网建立通信。调制解调器可以是内置或外置的，通过用户输入接口 140 或其它合适的机制连接至系统总线 121。在网络化环境中，描述的与计算机 110 相关的程序模块或其部分可储存在远程存储器存储设备中。可以理解，示出的网络连接是示例性的，也可以使用在计算机之间建立通信链路的其它装置。

[0064] 示例性分布式计算框架或体系结构

[0065] 鉴于个人计算活动与因特网的交汇，已经发展并且正在发展各种分布式计算框架。个人和商业用户同样地拥有用于应用程序和计算设备的无缝的互操作和启用 web 的接口，使得计算活动越来越面向 web 浏览器和网络。

[0066] 例如，MICROSOFT ®的管理代码平台，即 .NET 包括服务器、构件块服务，如基于 web 的数据存储、以及可下载设备软件。一般而言，.NET 平台提供 (1) 令整个范围的计算设备共同工作并在所有设备上自动更新并同步化用户信息的能力，(2) 提高的 web 站点交互能力，通过大量使用 XML 而不是 HTML 来实现，(3) 具有定制访问和从中央起点到用户的产品和服务传送的特点，用于各种应用，如电子邮件，或软件，如 Office.NET 的管理的在线服务，(4) 中央化数据存储，将增加对信息访问以及用户和设备间的信息同步的效率和简易性，(5) 集成各种通信媒质，如电子邮件、传真和电话的能力，(6) 对开发员来说，创建可重复使用模块的能力，借此提高生产力并降低编程错误数，以及 (7) 还有其它跨平台综合特性。

[0067] 尽管这里的某些示例性实施例是结合驻留在计算设备上的软件描述的，也可以通过操作系统、应用程序接口 (API) 或“中间人”对象、控制对象、硬件、固件、中间语言指令或对象等来实现本发明的一个或多个部分，使得该方法可以在由管理代码，如 .NET 代码启用的所有语言和服务中包括、支持或通过其访问，并也包括在其它分布式计算框架中。

[0068] 用于阻止电子设备的盗窃的系统和方法

[0069] 如上文在背景技术中所描述的，电子设备，如 PC、笔记本计算机、个人音频播放器、照相机等，易受盗窃或丢失的攻击。用于跟踪汽车可有多种选择；然而，鉴于各种所描述的原因，这些选则较昂贵并且对一般的电子产品不实用。因此，本发明为 PC 和其它电子设备

提供了一种无线激活的盗窃阻止方法和系统，它更适合便携式电子产品。在各种实施例中，本发明提供了允许当发现丢失时禁用设备的被盗部分的低成本技术。由此，本发明能使企业顾客和消费者同样可以避免遭受财物的重大损失。通过创建可负担的安全系统，本发明减少了损失，并使用本发明的功能创建了对设备的增加的需求。

[0070] 本发明使组件能够被包括在设备中，用于关闭设备或防止设备的操作，由接收远程信号启用。可以使用设备在广域网，如 SPOT 网络或无线载波网络上接收的定义的命令来禁用该设备。采用本发明的实施例，设备本身响应于定义的命令，并且本地地禁用操作。可使用覆盖代码来本地地重新启用该设备。这与蜂窝电话禁用不同，设备本身响应于定义的命令，并且本地地禁用操作。相反，诸如蜂窝电话等网络化设备在被盗时并未真正地被禁用，仅服务了其对适当的网络的访问。

[0071] 使用广域无线接收组件，如微软的 SPOT 或诸如使用广播或定向消息通信的无线寻呼机等其它技术，电子设备，如，但不限于，PC、笔记本计算机、个人音频播放器、照相机等等，可周期性地倾听消息，这些消息可指示设备停止操作，并由显示屏上的消息或简单的指示灯指示盗窃锁已被激活。

[0072] 低成本广域无线系统，如 SPOT 的可用性使本发明不仅可以灵活地用于高价值、高智能设备，如 PC，也可以灵活地用于其它设备，如音频播放器或照相机。

[0073] 在第一实施例中，由于本发明的系统需要最小的处理容量，本发明的“标签”包括现有的基于 SPOT 处理的完全或降低成本的版本。较低成本的 CPU 有利地降低了标签组件成本和功率消耗、本发明对设备的应用被集成到现有设计中，并由此可以容易地从一种类型的设备移植到另一种类型的设备，而不会干扰现有设计。尽管有利，本发明的标签技术可以被实现为独立的解决方案，用于另外的安全层，本发明也可以被实现为现有产品的主电路内的功能，或甚至是组件芯片组或应用专用集成电路 (ASIC) 之一内的功能，而几乎没有设计的变化。

[0074] 由此，例如，依照本发明，图 3A 示出了将标签包括在典型的设备 300，如照相机内。如上所述，设备 300 包括最小处理器 310，它能够从无线接收器 320，如 SPOT 接收器接收禁用信号。处理器 310 的功能也可以被容易地包括在如示例性设备 110 的处理单元 120 内，而在处理单元 120（或使用处理单元 120 工作的软件）的设计内有最小的变化。在示例性情形中，照相机 300 的所有者注意到照相机 300 丢失，并向本发明系统通知该丢失。例如，用户可以被注册为 web 站点的用户，用于报告设备丢失，或者用户可通过电子邮件或其它常规手段，如电话、传真等联系本发明的管理员。

[0075] 一旦报告了丢失，从网络广播一禁用信号，包括与接收器 320 和 / 或处理装置 310 关联的唯一的标识符，当接收器 320 接收该信号时，促使设备 300 变为禁用。例如，禁用设备的一个示例性方法是在设备的电子器件中任何必需的地方断开开关 S。不论它是被呈现为不可操作的模拟继电器、晶体管开关等，在不知道设备中禁用了什么，或者它如何被禁用的情况下，本发明的禁用操作都不能容易地被绕过。除禁用设备之外，处理装置 310 可任选地促使显示屏 330 指示该设备被禁用，和 / 或该设备假定被丢失或盗窃。显示屏 330 也可向重新找到该设备的人指示如何返回该设备，以某一利益，如报酬来交换。发送的禁用信号的编码可以是 (a) 明文 (b) 至少部分地被加密和 / 或 (c) 其它编码。

[0076] 也可以向本发明的系统添加位置报告增强。在替换实施例中，一旦被禁用，设备

300 可进入试图通过网络接口 350（设备独立地连接到替换网络之处）连接到网络，如诸如因特网等广域网的状态，企图帮助设备的找回。设备 300 也可通过包括在无线接收器 320 中的无线发射器向本发明的系统发送回信号，即，组件 320 可以是无线收发器。一旦已知设备丢失，传统上已知的三角测量方法也可以用于补充本发明以发现该设备的位置。然而，应当理解，发射器不是必需的，它仅是本发明的一个可任选增加。该选项的一个示例性使用是，例如，如果设备 300 已具有到因特网的连接。在这一情况下，设备 300 将向本发明的系统的适当的授权机构或管理员发送出其因特网协议 (IP) 地址和媒体访问控制 (MAC) 地址，授权机构或管理员将使第三方能够跟踪该设备物理位置。更详细地，如果被盗设备在锁定模式中具有到因特网的连接，它可以向安全监控服务发送任一已知的位置信息（如 TCP/IP 路由）。令被盗物品使用短范围 SPOT 网络无线电发射器无线电来发送能够由相邻的现场装备的 PC 拾获的报警代码也是可行的，这些 PC 进而能够向安全监控服务发送回位置信息。

[0077] 如上所述，一旦设备 300 的所有者发现设备丢失，所有者通过任一各种手段报告该丢失。图 4 示出了一个示例性情形，其中，一旦已知丢失了哪一设备，依照预定义的规则使用网络来向远程设备广播禁用信号。由此，对于具备处理器 310 和无线接收器 320 的功能的每一设备，本发明分配一个唯一的标识符。因此，对于报告被盗或丢失的每一设备，编译具有丢失的设备的唯一标识符的列表。然后，周期性地，或依照当设备发现被盗时启动的一组调度，可使用现有网络基础结构，如 SPOT 网络广播信号，以传送被盗设备的列表。设备 300 将该列表与其号码进行比较，并且如果其号码在该列表中，处理器 310 如通过打开开关 S 来禁用该设备。如上所述，开关 S 可以是物理开关、晶体管开关、继电器等等，或响应于由处理器 310 启动的禁用信号禁用该电子设备的任一开关。例如，处理器 310 本身可禁用对设备的功能所必需的处理器 310 的一部分，或者开关 S 可包括在处理器 310 内。通过令处理器 310 的存在对保持设备 300 的开关 S 或其它部分启用是必需的，本发明有利地防止了移除处理器 310 作为绕过本发明的一种方法。

[0078] 由于设备可包括值得盗窃的组件的多个可分组，图 3B 到 3D 示出了本发明可应用到设备 300 的多个部分。例如，如图 3B 所示，作为启用整个设备 300 的替代，处理器禁用设备 300 的一个子组件 300a。如图 3C 所示，作为禁用单个子组件 300a 的替代，该实施例示出了禁用多个子组件 300a、300b 等的能力。图 3D 示出了一个替换实施例，其中，对要禁用的每一子组件（或组件）提供了单独的处理器。例如，处理器 310a 结合禁用子组件 300a 使用，处理器 310b 结合禁用子组件 300b 使用。

[0079] 在图 4 中，设备 D1、D2、D3、D4 和 D5 在更大的现有网络基础结构，如 SPOT 网络的塔 T 的附近。塔 T 依照包括在设备中的接收器 / 处理器组合所理解的预定义协议广播被盗 ID，并且具有包括在广播信号中的被盗 ID 的设备变为被禁用。在图 4 的示例中，设备 D3 和 D5 被禁用，作为被盗 ID987654321 和 231765789 的广播的结果。

[0080] 图 5 通过流程图示出了本发明。在 500，报告设备 300 被盗。在 510，设备通过接收器 310 接收消息，并由处理器 320 处理，将该设备标识为丢失设备。在 520，由处理器 320 禁用设备。

[0081] 依照本发明，可以为额外的安全对上述本发明的通信的任一个进行加密，以防止网络上的探听和所使用的通信协议的发现。

[0082] 在更多的实施例中，对于管理网络中的基于 PC 的解决方案，可以向本发明添加安

全的额外模式。在这一情况下，默认设置是系统被禁用，企业管理员可向使用本发明的标签配置的 PC 指引特殊的网络“保持活动”分组，以保持到企业网络的连接。由此，万一系统被从企业网络中移除，在保持活动超时之后，系统将进入锁定模式，直到它接收到新的分组。可选地，如果系统被授权离开网络，则系统管理员可以登录到 web 站点，并将系统的模式改变为默认启用，或发送另一保持活动消息。一旦标签，即接收器 / 处理器组合接收到该消息，它将解锁该系统。保持活动状态也允许管理员跟踪 PC 资产。

[0083] 示例性非限制 SPOT 网络实现

[0084] 由此，本发明可应用到数以万计的情形，用于禁用被盗货物以向设备的所有者和保险公司提供优点。在一个实施例中，本发明使用 SPOT 网络基础结构。通过初始的估计，向超过十亿个设备提供设计基于该 SPOT 网络规模，每一设备具有每一 SPOT 位置上的覆盖（每年有大约一千万个物品被盗或丢失），而使用少于 6％的可用 SPOT 带宽。可以使用简单的压缩技术来改进这些数字，且不考虑从对找回的物品取消警告中所获得的带宽，并也假定每一丢失的设备具有全球范围的覆盖。

[0085] 图 6 示出了使用 SPOT 接收器 320/ 处理器 310 组合的设备 300 的示例性信令。在 600，设备 300 在多个预标识的射频上扫描消息。当在 610 接收到消息，在步骤 620，处理该消息来确定向其调谐的站。在一个实施例中，为进一步细分带宽，在无线电站信道中划分 ID。由此，例如，如果设备具有包括 5 作为第一位的 ID，则设备知道调谐到可用站的第五个无线电站。在 630，监控该站的消息帧。读取帧的内容。在 640，如果内容包括通过其唯一的 ID 标识该设备的消息，并且该消息是禁用消息，则在 650，设备如上所述地禁用。如果该消息不是禁用消息，或者不是供给该设备使用，则忽略该消息并且在 610 重复该过程。在一个非限制实施例中，帧包括 112 字节数据。

[0086] 在一个示例性非限制实现中，对于给定的报告设备，在丢失的位置处以在一个月时间内从一天 30 次衰减到一天一次的速率（平均值是一天 6 次发送）发送主要锁定分组（如，具有被盗 ID 的禁用信号），并在 12 个月后衰减到零。在任一时刻，用户可选择刷新设备。

[0087] 在所给出的 SPOT 网络是由本发明使用的网络的示例中，约一年 100 次在全球范围的每一 SPOT 覆盖范围内发送锁定分组。也可使用在国家范围或全球范围发送的增加的频率。

[0088] 如上所述，本发明的规模是可伸缩的，即，诸如图 3 所示的接收器 / 处理器组合等标签可以被包括在任一设备中。但是某些网络是地理上受限制、带宽上受限制或两者都受限制的。采用 SPOT 网络，FM 无线电塔的网络用于向 SPOT 设备提供数据覆盖。每一塔可支持多达 20,000 个唯一的 SPOT 标识符，并每天发送总共约 125MB 的数据（或在完全加载的忙碌人口中每一设备约 5KB 的目标数据），这使本发明能方便地够容纳另外的设备，而不创建新的塔或覆盖区域。由于使用 SPOT 网络的标签不需要接收大量的数据，带宽并未超载，并适合于规模可伸缩的系统。

[0089] 有多种实现本发明的方法，如适当的 API、工具箱、驱动器代码、操作系统、控制、独立或可下载软件对象等等，它们使应用程序和服务能够使用本发明的远程禁用方法。除在可能丢失的设备内供应组件之外，本发明考虑从 API（或其它软件对象）的观点使用本发明，以及从接收禁用请求或依照本发明发布禁用命令的软件或硬件对象使用本发明。由此，

此处描述的本发明的各种实现可具有完全以硬件、部分以硬件和部分以软件以及以软件的各个方面。

[0090] 如上所述，尽管结合各种计算装置和网络体系结构描述的本发明的示例性实施例，基本概念可应用到期望保护不受丢失或盗窃的任一计算装置和系统。例如，本发明的算法和硬件实现可以硬件或固件提供、应用到计算装置的操作系统、作为设备上的单独的对象提供、作为另一对象的的部分、作为可重复使用控制、作为可从服务器下载的对象、作为设备或对象和网络之间的“中间人”、作为分布式对象、作为硬件、在存储器中、上述的任一组合等等。尽管此处选择了示例性语言、名字和示例作为各种选择的代表，这些语言、名字和示例并不意味着局限。本领域的普通技术人员可以理解，有许多方法来提供达到本发明的各种实施例所达到的相同、类似或等效功能的对象代码和命名法。

[0091] 如上所述，此处描述的各种技术可以结合硬件或软件，或适当时两者的组合来实现。由此，本发明的方法和装置或其某些方面或部分可以采用包含在有形媒体中的程序代码（即指令）的形式，有形媒体如软盘、CD-ROM、硬盘驱动器或任一其它及其可读存储媒质，其中，当程序代码被加载到机器，如计算机并由其执行时，该机器变为用于实践本发明的装置。在程序代码在可编程计算机上执行的情况下，计算装置一般包括处理器、可由处理器读取的存储媒质（包括易失和非易失存储器和/或存储元件）、至少一个输入设备以及至少一个输出设备。如通过使用数据处理API、可重复使用控制等可实现或使用本发明的技术的一个或多个程序较佳地以高级程序语言或面向对象编程语言来实现，以域计算机系统进行通信。然而，如期望，程序可以汇编或机器语言实现。在任一情况下，语言可以是已编译或已解释语言，并与硬件实现相组合。

[0092] 本发明的方法和装置也可以通过以通过某一传输媒质，如通过电线或电缆、通过光纤或通过任一其它形式的传输发送的程序代码的形式实施的通信来实践，其中，当接收了程序代码并加载到机器，如 EPROM、门阵列、可编程逻辑器件 (PLD)、客户机计算机等，并由其执行时，该机器变为用于实践本发明的装置。当在通用处理器上实现时，程序代码与处理器组合来提供一种独特的装置，它操作来调用本发明的功能。另外，结合本发明使用的任一存储技术可以不变地为硬件和软件的组合。

[0093] 尽管结合各种示图的较佳实施例描述了本发明，可以理解，可以使用其它类似的实施例，并可以向所描述的实施例作出修改和添加，以在不脱离本发明的情况下执行其相同的功能。例如，尽管在网络化环境，如对等网络化环境的上下文中描述了本发明的示例性网络环境，本领域的技术人员将认识到，本发明不限于此，并且本申请中所描述的方法可应用到任一计算装置或环境，如游戏控制台、手持式计算机、便携式计算机等，无论它们是有线还是无线的，并且可以应用到通过通信网络连接并通过网络进行交互的任意数量的这类计算装置。此外，应当强调，考虑了各种计算机平台，包括手持式设备操作系统和其它应用专用操作系统，尤其当无线网络化设备的数量持续增长时。

[0094] 尽管示例性实施例涉及在 SPOT 网络的上下文环境中使用本发明，本发明不限于此，而是可以被实现来结合任意无线网络提供盗窃阻止。例如，如此处所使用的，术语破坏旨在描述如果依照本发明设备 300 的处理器 310 被移除时设备的状态。万一处理器 310 被移除，可以理解，本发明的意图是设备 300 不再对其一般预期的电子目的可操作。此外，本发明也可以在多个处理芯片或设备中或跨这些芯片或设备来实现，并且可类似地跨多个设

备实现存储。因此，本发明不应局限于任一单个实施例，而应当依照所附权利要求书的宽度和范围来解释。

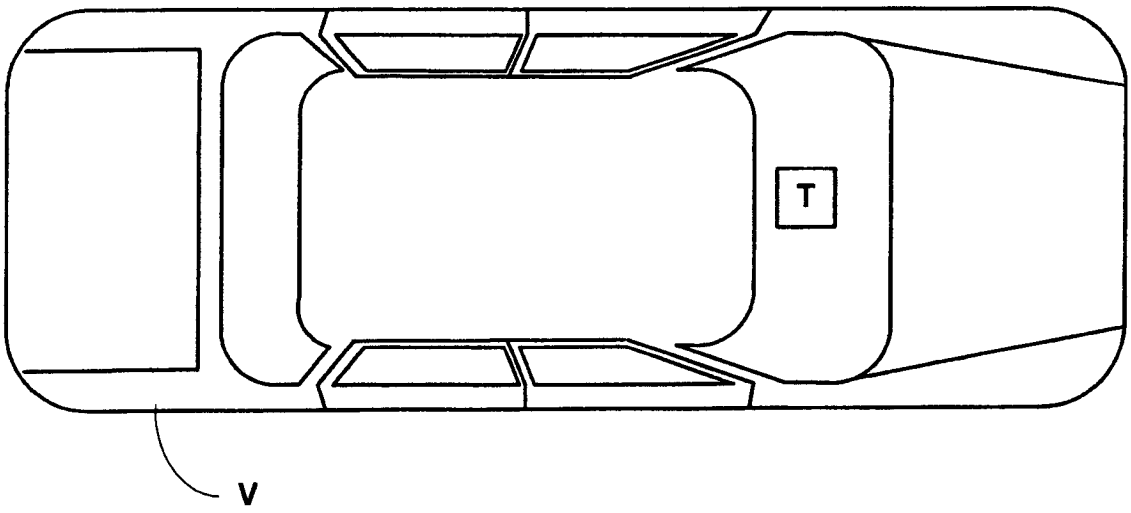



图 1A 现有技术

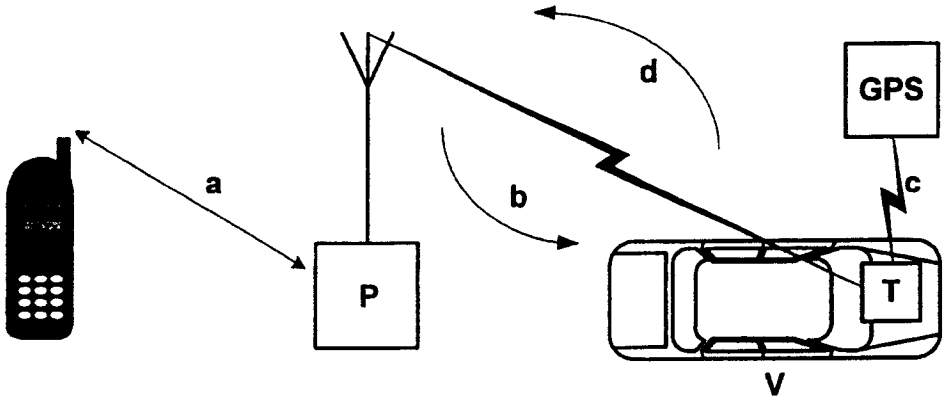



图 1B 现有技术

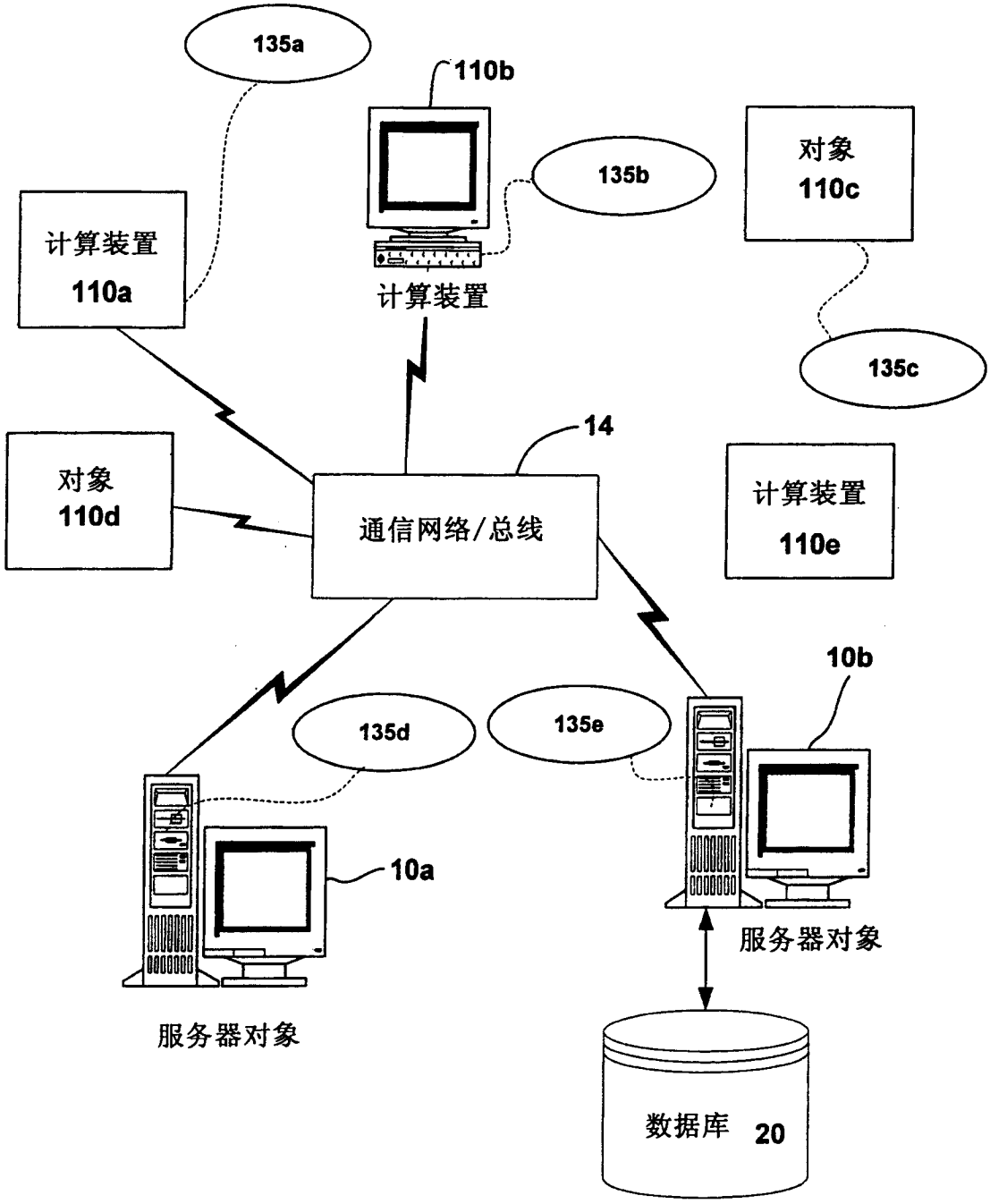

135a
110b
135b
对象
110c
计算装置
110a
计算装置
135c
14
对象
110d
通信网络/总线
计算装置
110e
10b
135d
135e
10a
服务器对象
服务器对象
数据库 20

图 2A

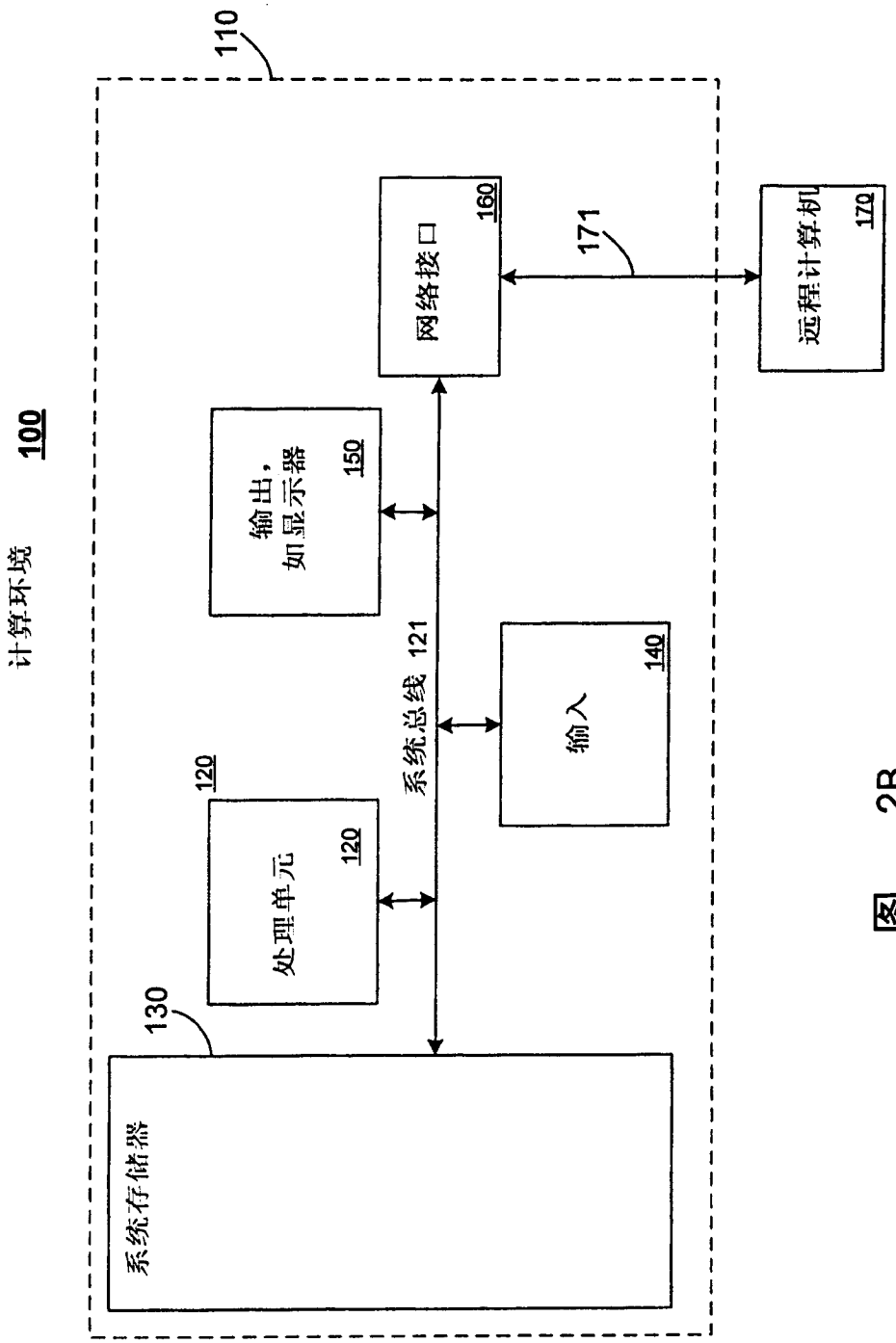

计算环境 100
110
网络接口 160
171
远程计算机 170
输出，如显示器 150
系统总线 121
输入 140
120
处理单元 120
130
系统存储器

图 2B

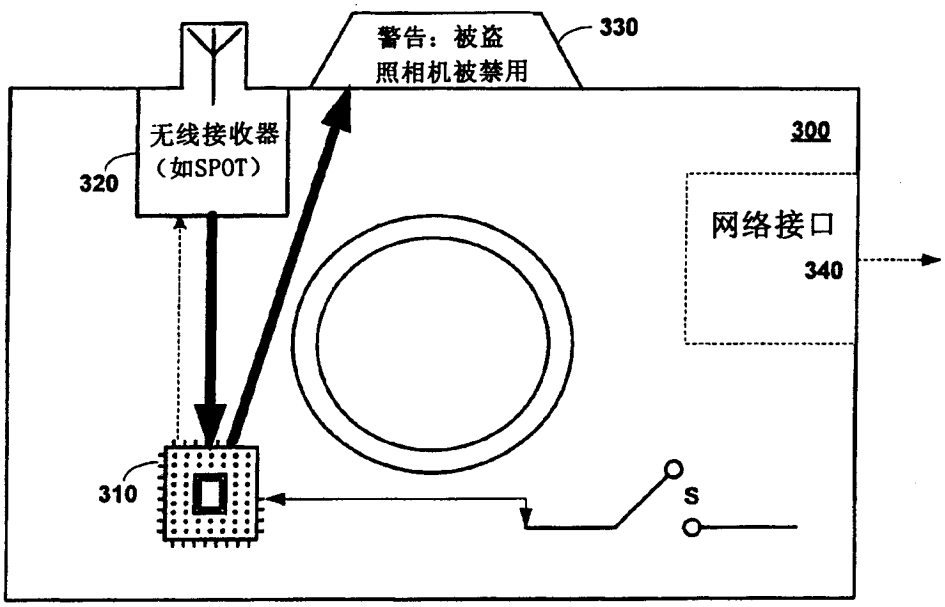

警告：被盗
照相机被禁用
330
无线接收器
（如SPOT）
320
300
网络接口
340
310
S

图 3A

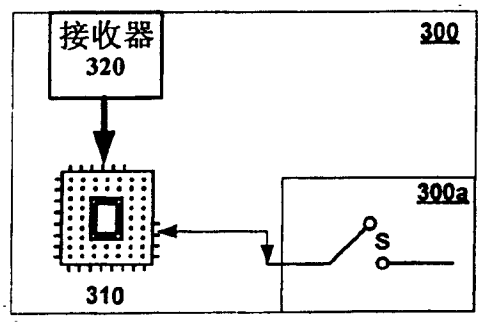

接收器
320
300
300a
S
310

图 3B

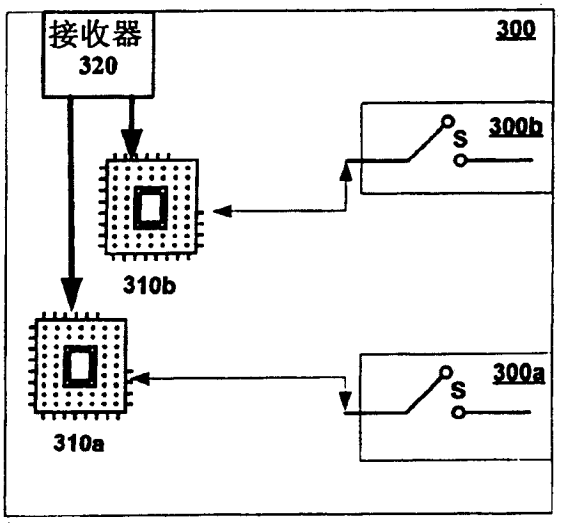

接收器
320
300
300b
S
310b
300a
S
310a

图 3D

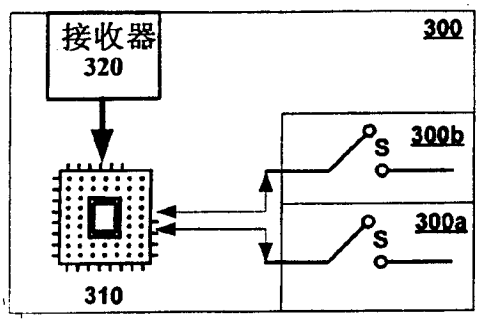



图 3C

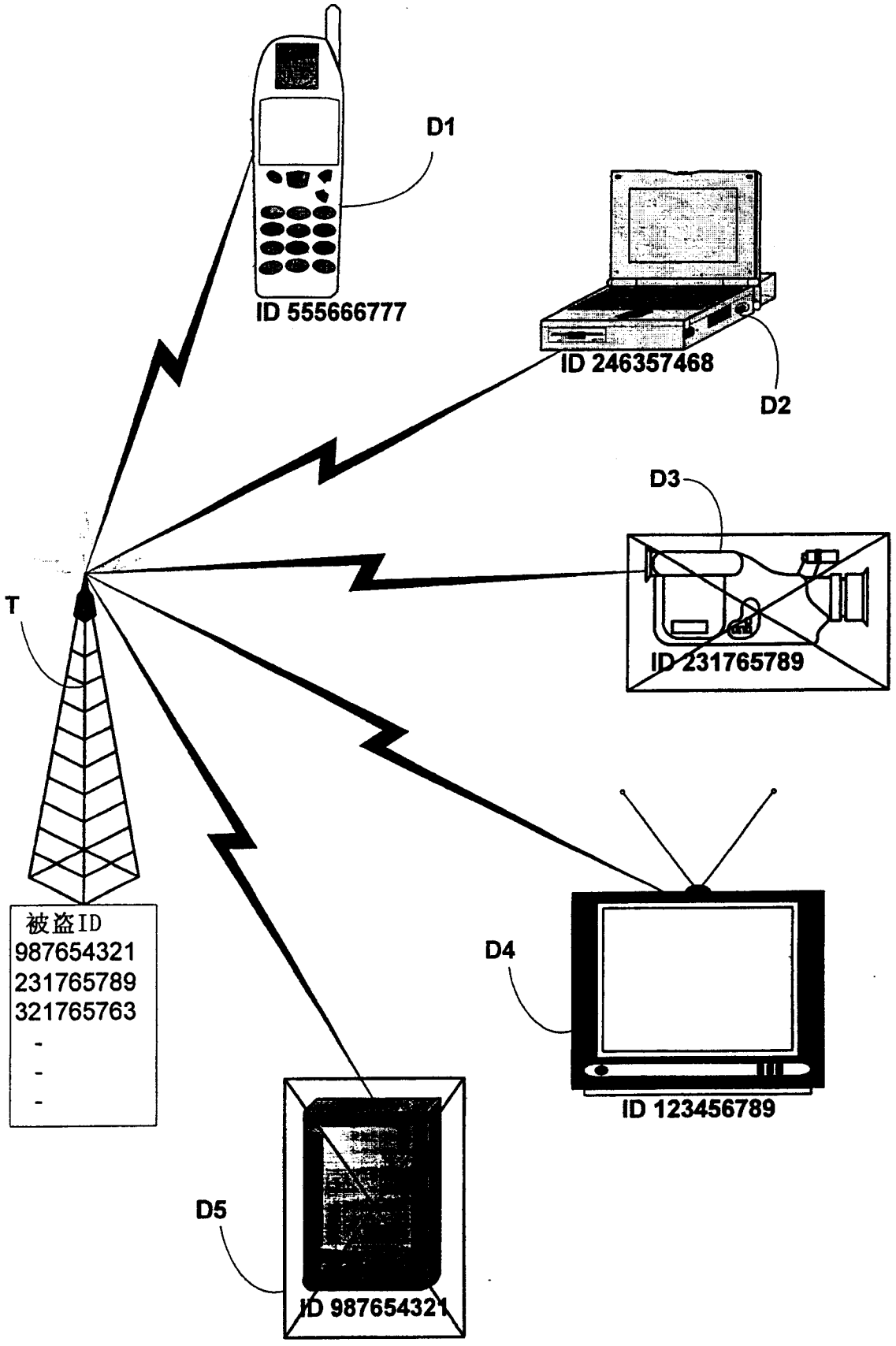

D1
ID 555666777
ID 246357468
D2
D3
ID 231765789
T
被盗ID
987654321
231765789
321765763
-
-
-
D4
ID 123456789
D5
ID 987654321

图 4

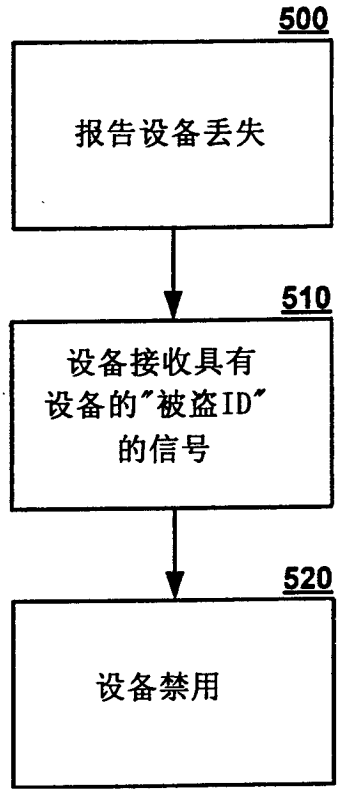



图 5

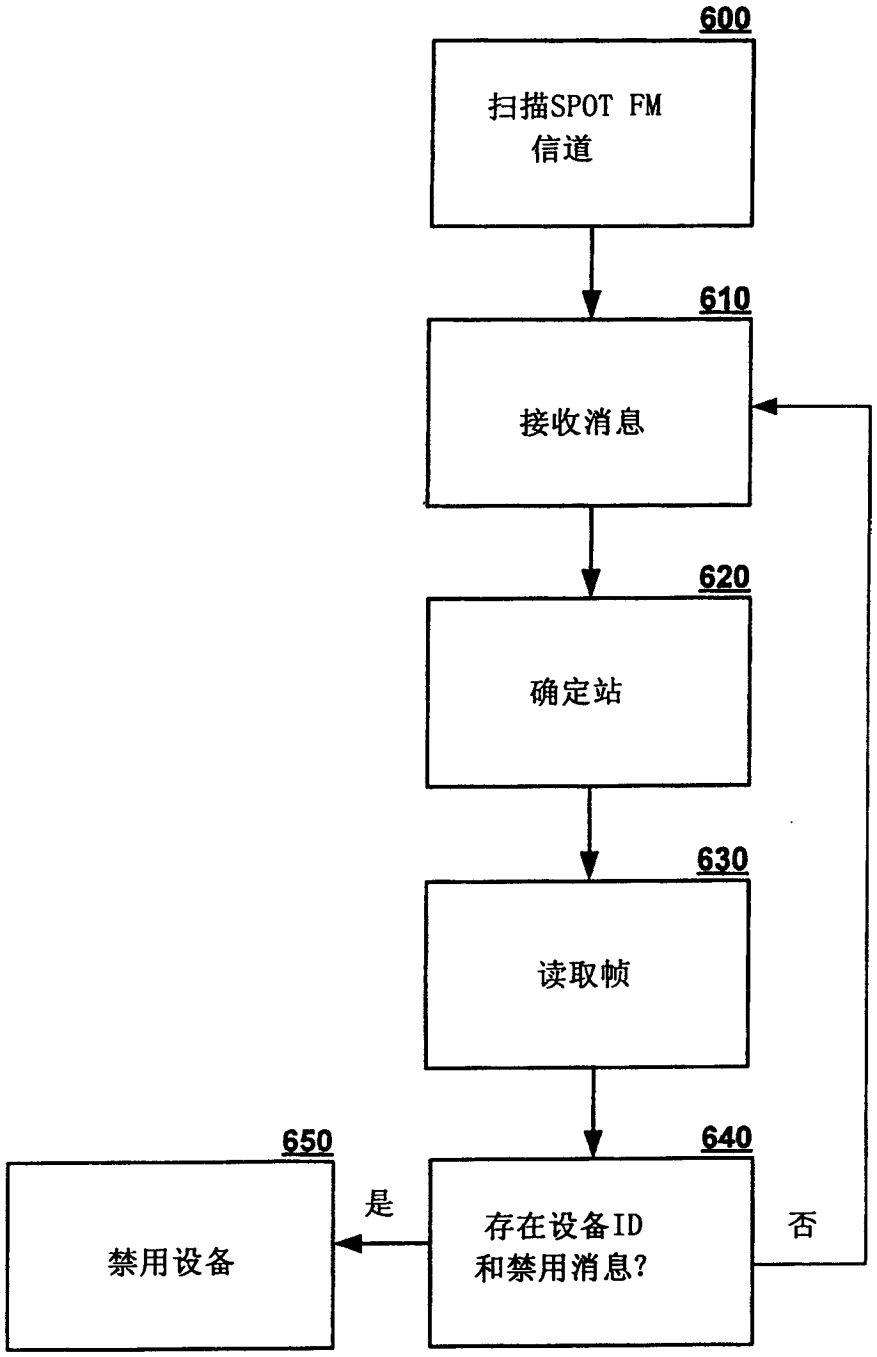

600
扫描SPOT FM
信道
610
接收消息
620
确定站
630
读取帧
640
存在设备ID
和禁用消息?
是
否
650
禁用设备

图 6