(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 103430183 B
(45)授权公告日 2016.04.20

(21)申请号 201180059505.X
(22)申请日 2011.10.11
(30)优先权数据
12/939,702 2010.11.04 US
(85)PCT国际申请进入国家阶段日
2013.06.09
(86)PCT国际申请的申请数据
PCT/US2011/055705 2011.10.11
(87)PCT国际申请的公布数据
WO2012/060979 EN 2012.05.10
(73)专利权人 思飞信智能电网公司
地址 美国加利福尼亚
(72)发明人 R·瓦斯瓦尼 W·C·Y·尤恩格
C·赛伯特 N·B·波尔亚德
B·N·达姆 M·C·圣约翰斯
(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 11038
代理人 鲍进
(51)Int.Cl.
*G06F 21/57*(2013.01)
*G06F 21/71*(2013.01)
*H04L 9/32*(2006.01)
(56)对比文件
CN 101467131 A,2009.06.24,
CN 1318161 A,2001.10.17,
CN 1405944 A,2003.03.26,
WO 2006065917 A1,2006.06.22,
CN 201118607 Y,2008.09.17,
审查员 彭明明

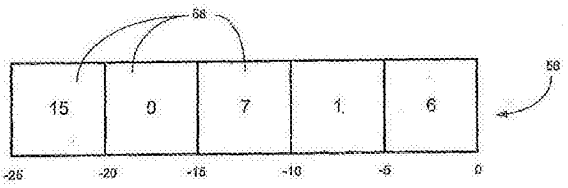
权利要求书4页 说明书8页 附图4页

(54)发明名称

用于公用事业应用的物理安全授权

(57)摘要

为了对公用事业管理系统提供整体安全性，要发布到该系统的部件的关键命令和控制消息是由安全授权机构明确批准的。明确批准认证所请求的动作并授权消息中所指示的具体动作的执行。公用事业管理与控制系统中与访问控制关联的关键部件放在物理掩体中。利用这种方法，变成只需要把负责批准网络动作的那些子系统放在掩体中。其它管理模块可以仍然留在掩体外面，由此避免把它们分割成放在掩体中的和不放在掩体中的部件的需求。对每个不放在掩体中的子系统的关键部件的访问是通过放在掩体中的批准系统来控制的。




CN 103430183 B

1. 一种用于公用事业应用的数据中心，包括：

物理上安全的环境，所述物理上安全的环境限制对其的访问；

在所述物理上安全的环境之外的至少一台服务器，所述至少一台服务器配置成执行与公用事业的操作关联的一个或多个应用程序，所述应用程序中的至少一些具有用于从位于数据中心之外的位置接收远程请求以执行和公用事业的操作有关的功能的接口；

硬件安全模块，位于所述物理上安全的环境中并且存储秘密密钥；

位于所述物理上安全的环境中的授权引擎，配置成接收指向所述应用程序的远程请求并且提供授权请求，所述授权请求是根据所述秘密密钥签名的；及

位于所述物理上安全的环境中的策略模块，配置成根据与所述应用程序关联的业务逻辑处理远程请求并且选择性地使请求能够基于定义要求授权的请求被所述授权引擎签名以便能够被执行的远程请求的类型的业务逻辑被所述授权引擎授权。

2. 如权利要求 1 所述的数据中心，还包括：

用于所述接口的代理服务器，位于所述物理上安全的环境中，所述代理服务器操作以接收在所述数据中心接收到的并且要针对所述应用程序的远程请求，并且把所述接收到的请求转发到所述策略模块。

3. 如权利要求 1 所述的数据中心，其中所述应用程序配置成把由所述应用程序接收到的远程请求重定向到所述策略模块。

4. 如权利要求 1 所述的数据中心，其中策略模块配置成确定包含断开和重新连接电力的命令的远程请求序列是否与同一个消费者关联，并且，如果它们满足这一条件，就阻止命令的执行。

5. 如权利要求 1 所述的数据中心，其中策略模块配置成确定包含断开或重新连接电力的命令的远程请求是否与消费者的当前状态不一致，并且，如果不一致，就阻止命令的执行。

6. 如权利要求 1 所述的数据中心，其中策略模块配置成确定远程请求是否是从经认证的来源接收到的，并且，如果所述来源未通过认证，就阻止请求被处理。

7. 如权利要求 1 所述的数据中心，其中策略模块配置成确定执行操作的远程请求是否是从具有对请求这种操作的许可的应用接收到的，并且如果发出请求的应用不具有这种许可，就阻止请求被处理。

8. 如权利要求 1 所述的数据中心，其中策略模块能够由从物理上安全的环境中输入的命令重新配置。

9. 一种用于公用事业应用的数据中心，包括：

物理上安全的环境；

在所述物理上安全的环境之外的至少一台服务器，配置成执行与公用事业的操作关联的一个或多个应用程序，所述应用程序中的至少一些具有用于从位于数据中心之外的位置接收远程请求以执行和公用事业的操作有关的功能的接口；

硬件安全模块，位于所述物理上安全的环境中并且存储秘密密钥；

位于所述物理上安全的环境中的授权引擎，配置成接收指向所述应用程序的远程请求并且提供授权请求，所述授权请求是根据所述秘密密钥签名的；及

位于所述物理上安全的环境中的策略模块，配置成根据与所述应用程序关联的业务逻

辑处理远程请求并且选择性地使请求能够被所述授权引擎授权，

其中策略模块配置成确定在预定时间段内发布的、包含断开电力的命令的远程请求的次数是否超过限制值，并且，如果请求的次数超过限制值，就阻止命令的执行。

10. 一种公用事业控制与通信网络，包括：

多个终端节点；

数据中心，包括：

物理上安全的环境，具有关联的认证证书；

至少一台服务器，配置成执行与公用事业的操作关联的一个或多个应用程序，所述应用程序中的至少一些具有用于从位于数据中心之外的位置接收远程请求以执行与公用事业的操作有关的功能的接口；

硬件安全模块，位于所述物理上安全的环境中并且存储密码密钥；及

位于所述物理上安全的环境中的授权引擎，配置成接收指向所述应用程序的远程请求并且提供根据所述密码密钥签名的授权请求；

至少一个接入点，所述终端节点经过所述接入点与位于所述数据中心中的应用程序通信；及

服务器，响应于数据中心处的物理上安全的环境的安全性已经受损的指示，向接入点发布配置证书撤销列表的命令，所述命令指示与其安全性受损的物理上安全的环境关联的证书无效，并且向所述终端节点发布从接入点加载证书撤销列表的命令。

11. 如权利要求 10 所述的网络，其中，响应于在数据中心处的物理上安全的环境的安全性已经受损的指示，所述服务器还向接入点发布忽略源自其物理上安全的环境已经受损的数据中心的通信的命令。

12. 如权利要求 10 所述的网络，其中终端节点配置成确定接收到的命令是否是通过使用与密码密钥关联的公钥授权的。

13. 一种用于控制公用事业网络中的设备的方法，包括：

生成对于要由公用事业网络中的设备执行的操作的命令；

把命令转发到硬件安全模块；

在硬件安全模块中，执行以下功能：

对命令执行密码服务，使得对其执行了该服务的命令的接收方能够认证所述命令是允许接收方执行的命令，

计数在规定时间段内硬件安全模块执行密码服务的次数，及

如果在规定时间段内执行密码服务的所计数的次数超过阈值限制，就终止对接收到的命令执行进一步密码服务；及

把对其执行了密码服务的命令发送到公用事业网络中的设备，以便执行该操作。

14. 如权利要求 13 所述的方法，其中密码服务次数的计数是在规定时段的滑动时间窗口上执行的。

15. 如权利要求 14 所述的方法，其中密码服务次数的计数是针对多个滑动时间窗口执行的，每个窗口都与不同的相应时间长度和阈值限制关联。

16. 如权利要求 13 所述的方法，其中密码服务是命令的加密。

17. 如权利要求 13 所述的方法，其中密码服务是对命令进行签名。

18. 如权利要求 13 所述的方法，还包括步骤：

当密码服务的所计数的次数达到小于所述阈值限制的预定值时生成报警。

19. 如权利要求 13 所述的方法，其中硬件安全模块包括多个槽，而且其中所述功能是在所述槽中的一个中执行的。

20. 如权利要求 19 所述的方法，其中所述功能还利用不同的相应阈值限制在第二个槽中执行。

21. 如权利要求 13 所述的方法，其中设备配置成确定接收到的命令是否是通过使用与密码服务关联的公钥授权的。

22. 一种用于控制公用事业网络中的设备的方法，包括：

生成对于要由公用事业网络中的设备执行的操作的命令；

确定所生成的命令是否需要许可；

如果所生成的命令需要许可，就把命令转发到许可服务器；

在许可服务器中，生成许可，所述许可规定 (i) 许可有效的时段，(ii) 要执行的操作，及 (iii) 要执行所述操作的设备；

把包含许可的数据包发送到公用事业网络中的设备；

当在设备处接收到数据包时，确定所规定的操作是否需要许可，而且，如果需要的话就确定许可当前是否有效；及

如果许可当前有效，就执行所规定的操作。

23. 如权利要求 22 所述的方法，其中许可包含指示许可何时变得有效的开始值，及指示从开始值开始许可保持有效的时间长度的持续时间值。

24. 如权利要求 22 所述的方法，其中许可包括第一字段和第二字段，所述第一字段包含要执行操作的设备的标识，而所述第二字段指示第一字段的格式。

25. 如权利要求 24 所述的方法，其中第一字段中所包含的标识包括设备的 MAC 地址。

26. 如权利要求 24 所述的方法，其中格式是 DER 八位字节串。

27. 如权利要求 22 所述的方法，其中许可是利用与许可服务器关联的密钥签名的，而且设备验证许可的签名。

28. 如权利要求 22 所述的方法，其中许可服务器是在硬件安全模块中实现的。

29. 如权利要求 28 所述的方法，其中硬件安全模块执行以下功能：

计数在规定时间段内由硬件安全模块生成许可的次数，及

如果在规定时间段内生成许可的所计数的次数超过阈值限制，对于接收到的命令就终止进一步许可的生成。

30. 如权利要求 29 所述的方法，其中生成许可的次数的计数是在规定时段的滑动时间窗口上执行的。

31. 如权利要求 30 所述的方法，其中生成许可的次数的计数是针对多个滑动时间窗口执行的，每个窗口都与不同的相应时间长度和阈值限制关联。

32. 一种用于公用事业网络的认证系统，包括：

许可服务器，配置成接收对于要由公用事业网络中的设备执行的操作的命令，并且生成许可，所述许可规定 (i) 许可有效的时段，(ii) 要执行的操作，及 (iii) 要执行所述操作的设备；及

通信接口，配置成把包含许可的数据包发送到公用事业网络中的设备。

33. 如权利要求 32 所述的认证系统，其中许可包含指示许可何时变得有效的开始值，及指示从开始值开始许可保持有效的时间长度的持续时间值。

34. 如权利要求 32 所述的认证系统，其中许可服务器是在硬件安全模块中实现的。

35. 如权利要求 34 所述的认证系统，其中硬件安全模块配置成执行以下功能：

计数在规定时间段内由硬件安全模块生成许可的次数，及

如果在规定时间段内生成许可的所计数的次数超过阈值限制，对于接收到的命令就终止进一步许可的生成。

36. 如权利要求 35 所述的认证系统，其中生成许可的次数的计数是在规定时段的滑动时间窗口上执行的。

37. 如权利要求 36 所述的认证系统，其中生成许可的次数的计数是针对多个滑动时间窗口执行的，每个窗口都与不同的相应时间长度和阈值限制关联。

38. 如权利要求 32 所述的认证系统，还包括其中放置了许可服务器的物理上安全的环境。

39. 一种公用事业网络，包括：

许可服务器，配置成接收对于要由公用事业网络中的设备执行的操作的命令，并且生成许可，所述许可规定 (i) 许可有效的时段，(ii) 要执行的操作，及 (iii) 要执行所述操作的设备；

通信接口，配置成经公用事业网络发送包含许可的数据包；及

连接到公用事业网络的多个设备，用于接收数据包，每个所述设备都配置成：

确定在接收到的数据包中所规定的操作是否需要许可，

如果需要，就确定许可当前是否有效，及

如果许可当前有效，就执行所规定的操作。

40. 如权利要求 39 所述的公用事业网络，其中许可包含指示许可何时变得有效的开始值，及指示从开始值开始许可保持有效的时间长度的持续时间值。

41. 如权利要求 39 所述的公用事业网络，其中许可服务器配置成利用密钥对许可进行签名，并且设备配置成验证许可的签名。

42. 如权利要求 39 所述的公用事业网络，其中许可服务器是在硬件安全模块中实现的。

43. 如权利要求 42 所述的公用事业网络，其中硬件安全模块配置成执行以下功能：

计数在规定时间段内由硬件安全模块生成许可的次数，及

如果在规定时间段内生成许可的所计数的次数超过阈值限制，对于接收到的命令就终止进一步许可的生成。

44. 如权利要求 43 所述的公用事业网络，其中生成许可的次数的计数是在规定时段的滑动时间窗口上执行的。

45. 如权利要求 44 所述的公用事业网络，其中生成许可的次数的计数是针对多个滑动时间窗口执行的，每个窗口都与不同的相应时间长度和阈值限制关联。

# 用于公用事业应用的物理安全授权

## 技术领域

[0001] 本公开涉及与公用事业公司关联的操作的管理与控制，尤其涉及管理和控制这种操作的系统的安全性。

## 背景技术

[0002] 公用事业公司具有复杂的、高度互连的系统，这种系统在运行大量关联软件模块的物理服务器上执行，用于管理和控制公用事业公司的操作。图 1 是可以在用于为消费者提供电力而且还有可能提供诸如气、水等的其它商品的公用事业公司的典型管理与控制系统中找到的部件中的一些的通用框图。系统的后端支援部门 10 包括与公用事业的各种操作关联的多个单独的子系统，例如消费者信息系统（CIS）12、消费者关系模块（CRM）14、停电管理系统（OMS）16、GPS 信息系统 18、计费系统 20、电网稳定模块 22 与用户接口 24。尽管在图 1 中没有说明，但是在后端支援部门 10 中还可以存在附加的功能性模块。这些子系统中的一些可以具有与分配网络中的设备通信的能力以便给其提供商品，并且远程控制与那些设备关联的操作。例如，后端支援部门服务器可以与位于消费者住所的单独的仪表 26 通信，以便为了计费而获得消费数据，并且命令仪表选择性地断开消费者与由公用事业公司提供的一种或多种商品的供给或者重新连接到由公用事业公司提供的一种或多种商品的供给。从后端支援部门服务器到单独仪表的其它命令可以包括从消费者接受外送 (outbound) 能量流的命令。

[0003] 在图 1 的例子中，仪表构成通过局域网 30 与后端支援部门通信的终端节点，其中局域网 30 具有把能量提供到网络中或者网络外面的接入点 32。在一种实施例中，局域网可以是无线网状网络。接入点 32 通过广域网 34 或者专用通信链路与位于后端支援部门 10 的服务器通信。

[0004] 在这种类型的系统中，所关心的一个问题是远程断开与重新连接的安全管理，断开和重新连接分别会在消费者腾出住所或拖欠费用时或者当新消费者占有该住所时发生。恶意和 / 或错误发出的远程断开和 / 或重新连接住所的命令有可能使配电网络不稳定。未授权的重新连接也会导致所分配电力的窃取。为了限制这种可能性，必须努力确保命令和控制操作都以安全的方式发生，而且只能由被授权采取这种操作的实体进行。但是，由于典型公用事业的后端支援部门包括许多互联的系统，因此安全访问的实施变得很困难。公用事业中许多不同的组需要访问软件系统的全部或者部分，这使得限制对单个子系统的逻辑和 / 或物理访问的能力复杂化。

[0005] 对这个问题的一种可能的解决办法是把某些系统，或者这些系统的部分，放到物理上安全的环境中，在下文中称之为掩体 (bunker)。掩体的例子包括访问受限的房间或容器，例如上锁的房间，及被保护系统周围的防篡改外壳或封装。掩体严格地限制对在其上执行所述系统或者所述系统的被保护部分的硬件设备的物理访问。此外，掩体中的系统输出非常有限的逻辑访问。但是，这种解决办法仍然存在具有挑战性的问题，因为很难重构公用事业软件系统来确定哪些部分需要放在掩体中，哪些部分可以保留在其外面，以便为需要

它的人提供更灵活的访问。

## 发明内容

[0006] 为了对公用事业公司管理系统提供整体安全性，发布到该系统的部件的关键命令与控制消息需要被安全授权机构明确批准。明确批准认证所请求的动作并且授权消息中所指示的具体动作的执行。公用事业管理与控制系统中与访问控制关联的关键部件放在物理上安全的环境中。利用这种方法，变成只需要物理上保护负责批准网络动作的那些子系统，例如通过掩体。换句话说，大部分的管理模块，诸如 CIS、CRM、OMS、计费等，可以留在掩体的外面，由此避免把这些子系统分割成放到掩体中和不放到掩体中的部件的需求。对每个不放到掩体中的子系统的关键部件的访问是通过放到掩体中的批准系统来控制的。

## 附图说明

[0007] 图 1 是公用事业管理与控制系统的通用框图；

[0008] 图 2 是具有放到掩体中的部件的公用事业后端支援部门系统的框图；

[0009] 图 3 是示意性地绘出当消息发送到仪表时的数据流的框图；

[0010] 图 4 是硬件安全模块的配置的框图；

[0011] 图 5 是经滑动窗口计数密码操作的多级缓冲区的框图；

[0012] 图 6 说明了用于发布对于命令的许可的系统与过程的例子；

[0013] 图 7 是许可的有效载荷的示例性格式的框图；及

[0014] 图 8 是在多个数据中心中实现的公用事业控制与管理系统的框图。

## 具体实施例

[0015] 为了方便对本发明所基于的原理的理解，下文参考电力配送系统中远程连接与断开命令的安全控制来描述。但是，应当认识到，这个例子不是这些原理的仅有的实践应用。相反，它们可以联系任何类型的关键命令采用，这些关键命令如果被不正确地或者错误地发布的话，有可能严重干扰或损害系统。同样，它们可以结合发送到系统的关键部件的所有命令与控制消息一起使用，这些关键部件的正确操作在任何时候都是必需的。

[0016] 图 2 说明了其中实现本发明概念的数据中心 40 的例子。就像常规的那样，数据中心包含多个物理服务器，各种应用 12、14、16 在所述物理服务器上执行。尽管图中只说明了几个代表性的应用，但是应当认识到，大量的此类应用可以在数据中心中实现。相反，由任意两个或多个这种应用执行的功能可以集成到单个全面的程序中。

[0017] 位于数据中心中的还有具有受限物理访问的物理掩体 42，诸如具有加固的墙壁的上锁房间。作为另一个例子，除了上锁之外或者代替上锁，掩体可以是利用安全摄像机、运动检测器等密切观察或保护的区域。作为还有另一个例子，掩体可以是物理上分布的，在分布的部分之间建立了安全关系。作为还有另一个例子，掩体可以是诸如通过使用安全执行软件和 / 或固件从逻辑上保护的，其中所述软件和 / 或固件的功能性被保护不受物理篡改，诸如自毁灭包装。掩体不需要是房间，还可以是例如物理上安全的盒子。

[0018] 具有关联的硬件安全模块 44 的一个或多个附加服务器设备位于掩体中，用于授权引擎 46 的实现，其中授权引擎 46 具有执行与安全性相关的操作，诸如授权、认证和记账，

的软件模块。硬件安全模块 44 包含以安全方式的私有和其它秘密密钥。它还可以包含链接到私钥的公共证书。硬件安全模块优选地使用健壮的安全算法，诸如椭圆曲线密码或者另一种高度安全的密码方法，来执行密码操作。适于在此所述的应用的硬件安全模块的一个例子是来自 Utimaco Safeware AG 的硬件安全模块的 SafeGuard CryptoServer 产品线。

[0019] 对掩体及位于其中的服务器设备的安全访问可以利用生物传感器技术，例如指纹检测、物理密钥或令牌和 / 或口令保护，来加强。在一种实现中，可以采用有层次结构的分层的安全系统来最大化保护。如果安全性中的一层失败，例如口令意外泄漏或被窃，那么更高级的安全机制可以被激活，诸如密钥或令牌启动死锁，来维护整个系统的物理安全性。

[0020] 来自不放在掩体中的后端支援部门应用 12-16 等中的某些类型的命令是受约束的，使得它们除非被单独认证否则将被不执行。例如，远程断开和重新连接命令是这些受限命令中的一类，由于它们会严重干扰电力配电网络稳定性的可能性。为了加强与这些类型的操作有关的安全性，执行它们的应用可以只在命令源自掩体 42 中的控制台或者以别的方式被从掩体 42 中发布的许可认证的时候才接受命令这么进行。因而，只有有权利发布这些命令和拥有访问掩体的必要手段，例如口令、密钥、指纹等，的人员才能够对应用发布受限的命令。

[0021] 当启动生成命令的操作时，它可以被授权引擎 46 签名或者以别的方式认证，然后转发到与在掩体 42 外面的适当应用关联的应用编程接口（API）。例如，命令可以由存储在硬件安全模块 44 中的私钥来签名。当在外部应用，例如应用 12-16 中的一个或者运行在仪表 26 之一中的应用处接收到经签名的命令时，通过该应用可以访问的公钥来验证该命令。一旦得到验证该命令是源自掩体内，该命令就由所述外部应用执行。

[0022] 在有些情况下，让发布远程断开命令的实体物理地位于掩体中可能是不实际的。但是，如果支持这种命令的远程生成，那么这种命令可能是由假扮被授权实体的用户恶意发布的。为了限制这种事件的可能性，根据本发明，在掩体中实现策略模块 48。策略模块可以是单独的软件或固件部件，如图 2 中所绘出的，或者逻辑地结合到硬件安全模块中，如下文将描述的。策略模块 48 可以以安全的方式——诸如通过从掩体内部输入的命令——被重新配置或者重新编程。这个模块包含检查所请求的动作并且确定是否允许其执行的业务逻辑。例如，如果重新连接命令是在可能干扰配电网络稳定性的序列中或者具有利用定时发布的，它们就可以通过策略被阻塞而且不传递到授权引擎进行签名。此外，策略标记可以出现并且执行适当的动作，诸如在检测到某些条件的时候断开与发布命令的实体。这些条件可以包括，例如 ：

[0023] 1. 例如在预定的时间间隔内，同时发布了大量的远程断开命令，这指示把用户从配电网络恶意断开的可能意图 ；

[0024] 2. 命令是以可疑的次序发布的，诸如与同一消费者关联的重复的连接与断开命令序列，或者与消费者的当前状态不一致的命令，例如向还没有连接到电网的用户发布断开命令 ；

[0025] 3. 发出请求的应用未能提供必要的凭证，或者以别的方式被认证 ；

[0026] 4. 发出请求的应用不在具有发布某些操作的许可的一组被批准的应用之内 ；及

[0027] 5. 基于实际的电力负荷和计划的电力需求，配送网络的状态。

[0028] 为了实现这种功能性，掩体可以包含代理服务器 50，用于在掩体外面的应用的应

用编程接口(API)。在操作中,当对用于这些“外部”应用中的一个的 API 进行调用时,该调用被指向掩体中的代理服务器 50。代理服务器咨询策略模块 48 中的授权所述请求可能需要的公用事业业务逻辑,并且让适当的业务逻辑对请求进行签名。然后,请求被传递到授权引擎 46 进行签名。一旦被授权,代理服务器就可以为在掩体外面的被调用应用启用正常的 API,并且与被授权的调用一起传递。

[0029] 在一种可供选择的实现中,掩体 42 可以不包括代理服务器。在这种情况下,请求可以直接对外部应用的 API 进行。反过来,如果确定所请求的操作需要签名的话,外部应用就调用掩体中的授权引擎。缺省地,所有请求都可以为了授权而传递到掩体中,以避免需要由外部应用作出任何决定。提交给掩体的请求首先被检查并且由策略模块签名,然后传递到授权引擎 46。一旦请求得到授权,被调用的应用就可以对该请求起作用。

[0030] 掩体 42 中所包括的硬件安全模块 44 可以在两个层次上操作。下文联系在仪表 26 执行的操作来描述例子。在操作的第一层,公用事业公司可以制定位于后端支援部门 10 和仪表 26 处的应用或者网络 30 的任何其它部件之间的所有通信都必须被加密和签名的策略。这种策略的实现在图 3 的例子中绘出。在这个例子中,仪表管理应用 52 具有要发送到一个或多个仪表 26 的消息,例如命令。这种消息是在所述应用的仪表命令与接口模块 54 中构造的,并且转发到掩体 42 中的硬件安全模块 44,具有执行该消息的适当加密与签署的请求。策略模块 48 可以首先做检查,以确认请求是否是源自被授权的来源。如果是,请求就一路传递到硬件安全模块。利用与应用关联的适当密钥,硬件安全模块 44 对消息执行所请求的操作,并且返回加密和签名后的数据。然后,仪表管理应用的命令与接口模块 54 创建结合了加密和签名后的消息的数据包,并且经网络 30 把它发送到仪表。

[0031] 对于由应用 52 从网络 30 中的节点接收到的消息,它们首先转发到硬件安全模块,以被解密。模块 48 还可以对接收到的消息的发送方的可靠性和数据的完整性执行适当的验证。然后,经过验证和解密的消息返回到应用 52。

[0032] 对于关键操作,诸如远程连接与断开,硬件安全模块可以在第二层操作,以便加强对这种操作的速率限制。图 4 绘出了硬件安全模块的内部配置的一个例子。该模块配置成具有多个槽。每个槽都包含私钥、证书、秘密密钥和访问特权的集合,来执行诸如签名、加密、解密等的密码服务。不同的槽与不同的安全上下文关联,而且包含与其对应上下文有关的密钥、证书和其它信息。利用硬件安全模块对命令执行密码服务,诸如用私钥对其签名,使得命令的接收方,例如节点 26,能够利用关联的公钥来认证命令的来源。策略模块 48 作出对于所请求的命令是否被允许提供给硬件安全模块以获得一个或多个密码服务的初始决定。

[0033] 为了加强期望的业务逻辑,例如通过命令行管理工具,每个槽可以选择性地配置成具有一个或多个速率限制。配置槽的命令的一个例子如下 :

[0034] HSM_configure slot=2rate-name=”rate1”window=24h count=10000

[0035] 这个命令把槽 2 配置成具有每个 24 小时的滑动窗口有 10,000 次密码操作的最大速率限制。如果在前面的 24 小时内出现了多于这个分配次数的密码操作,那么该槽将暂停全部进一步的密码操作。其后,管理员有必要通过发送复位命令来复位该槽。

[0036] 槽可以配置成具有多于一个速率,如下 :

[0037] HSM_configure slot=2rate-name=”rate1”window=24h count=40000

[0038] HSM_configure slot=2rate-name=”rate2”window=60m count=2000

[0039] 这两个命令把槽 2 配置成具有两个速率限制窗口，一个是 24 小时的滑动窗口有 40,000 次密码操作，另一个是 60 分钟的滑动窗口有 2000 次密码操作。

[0040] 如果槽配置成具有速率限制，那么在滑动窗口上针对所分配的限制对在该槽中执行的所有密码操作计数。在以上给出的例子中，如果在过去的 24 小时内有多于 40,000 次密码操作，或者在过去的 60 分钟内有多于 2000 次密码操作，那么该槽就暂停任何进一步的密码操作。

[0041] 在一种实施例中，对违反阈值的记账可以 5 分钟的增量执行。图 5 说明了一个例子，其中槽配置成在 25 分钟的滑动窗口内有 800 次密码操作的限制。滑动窗口可以实现为多级缓冲区 56。所说明的缓冲区包括五个级 58，每个级代表 5 分钟的时间间隔。每个级包含在其对应时间间隔内槽所执行的密码操作的次数的计数。下表提供了给定时间点缓冲区中所包含的数据的快照。

[0042]

| 级 | 时间帧 | 计数 |
|---|---|---|
| 1 | -25 至 -20 分钟 | 15 |
| 2 | -20 至 -15 分钟 | 0 |
| 3 | -15 至 -10 分钟 | 7 |
| 4 | -10 至 -5 分钟 | 1 |
| 5 | -5 至 0 分钟 | 6 |

[0043] 如果所有计数之和，在这个例子中是 15+0+7+1+6=29，超过阈值，槽就暂停所有进一步的密码操作，直到它被管理员复位。为了在暂停操作之前通知管理人员，可以实现报警机制。例如，当总的计数超过速率限制的 80% 时生成第一报警，并且在其到达限制的 90% 时生成第二报警。

[0044] 与最近间隔关联的级，在这个例子中是级 5，保持对每个新密码操作的运行计数。在每个 5 分钟间隔结束时，所存储的计数移到下一个最旧的级中。最后一个级复位成零，并且开始为下一个 5 分钟间隔重新开始对密码操作进行计数。

[0045] 由于每个槽可以选择性地配置成具有其自己的速率限制，因此在业务逻辑的实现中提供了灵活性。例如，如下文中所描述的，某些关键命令可以在执行之前需要显式类型的认证，下文中称为“许可”。这些命令可以映射到与执行许可过程的槽关联的安全上下文，并且具有特别严格的速率限制。其它类型的命令可以映射到不同的安全上下文并且可以经具有不太严格的速率限制的不同槽加密和 / 或签名。

[0046] 对于关键命令，诸如远程断开和重新连接命令，更高级的安全性可能是合适的，诸如由多方批准，每一方都必须在接收节点通过认证。但是，从网络效率的角度看，如果为了执行命令只需要接触该命令所指向的节点一次，这将是期望的。在本发明的一方面，这些目标可以通过允许提供所有所需信息的系统使节点能够认证命令来实现。本质上，发送到应

用的每个关键命令，诸如发送到仪表的断开命令，可能需要附带许可。如上面所指出的，不同类型的命令可以映射到不同的安全上下文。当要发布一个命令时，该命令或者是应用自动发布的或者是通过用户接口发布的，发布命令的应用都检查该命令的安全上下文。如果需要加密，命令就转发到硬件安全模块适当的槽，以进行这种操作。如果确定安全上下文需要许可，命令就转发到掩体中发布该许可的许可服务器。在一种实施例中，许可服务器的功能可以由硬件安全模块中的槽实现。

[0047] 参考从配电网络断开住所的命令，用于发布许可的布置与过程的一个例子在图 6 中说明。在这个例子中，后端支援部门 10 中的一个业务模块，例如记账系统，向仪表管理应用 52 发布断开与一个账户关联的住所的命令。当接收到这种命令时，仪表管理应用可以调度在特定的时间内的断开操作，然后经安全链路向负荷管理模块 59 发送消息，以请求发布这种命令的许可。负荷管理器是位于掩体 42 中的业务逻辑的部件并且确定负荷改变对配电网络是否有害。在这个例子中，负荷管理器充当允许服务器的一种实现。如果确定所请求的改变可能是有害的，负荷管理器就可以拒绝该请求，例如，如果当前有太多未完成的请求，就推迟该请求一段时间，或者批准该请求。到负荷管理器的请求可以包括诸如目标节点、调度操作时间、完成命令执行所需的时间窗口大小之类的信息。

[0048] 如果请求被批准，负荷管理器就创建可以被命令所指向的节点识别的许可。在许可返回到仪表管理应用 52 之前，利用与负荷管理器关联的密钥进行签名。在所说明的例子中，许可服务器，即，负荷管理器 59，与硬件安全模块 44 是分离的。因此，在这种情况下，许可发送到硬件安全模块，以利用负荷管理器的私钥进行签名。然后，签名后的许可返回到负荷管理器，以转发到仪表管理应用 52。

[0049] 当接收到签名后的许可时，仪表管理应用把授权的命令连同签名后的许可一起发送到与要断开的住所关联的节点 26。然后，该节点可以验证许可，例如通过遵循从许可、通过负荷管理器的凭证到与配电网络的系统操作员关联的根授权的一连串证书。节点还验证许可内的时间值与当前时间一致。如果所有信息都是正确的并且通过验证，该节点就执行命令并且向仪表管理应用 52 发送签名后的收据，用于指示命令完成。收据的拷贝可以发送到负荷管理器 59，使得它可以跟踪未完成的请求。

[0050] 仪表管理应用 52 还可以对发送到节点的数据包的有效载荷进行签名，以便为由不同控制实体，即，仪表管理应用和负荷管理器，发布的命令提供两种单独的授权。这两种形式的授权都需要在执行命令之前由节点进行验证。在这个例子中，许可服务器，例如负荷管理器，不拥有直接与节点 26 通信所需的凭证。相反，它把凭证提供给另一个控制实体，在这种情况下是仪表管理应用 52，以便执行授权命令。

[0051] 用于确定是否批准命令的业务逻辑可以是相对简单的，例如漏桶算法，其中允许预定数量的断开操作的初始突发序列 (burst)，然后每单位时间较少量的操作。在这种情况下，利用前面描述过的速率控制，负荷管理器的功能可以在硬件安全模块的槽中实现。另一种更复杂的算法可以基于电力配电网络的状态，例如，跟踪实际的电力负荷并基于电力需求的计划作出决定。这后一种实施例可以在硬件安全模块的外面执行，如图 6 中所绘出的，例如在专用的物理系统、虚拟服务器或共享系统上的应用中执行。

[0052] 除了远程断开与重新连接，其它类型的命令也可以需要具有许可，诸如为了降低规定时间段内的消耗而针对消费者的住所的负荷限制命令。此外，如果系统中特定类型设

备的安全操作对于系统稳定性是关键的，诸如分配自动部件，那么发布到那个设备的所有命令可能都需要具有许可。无论什么时候后端支援部门模块向这种设备发布命令，它都把命令转发到许可服务器，以获得必需的许可。

[0053] 用于包含在消息有效载荷中的许可的示例性格式在图 7 中绘出。许可有效载荷的第一个字段 60 指示开始时间，即，许可变得有效的时间。当在一个节点接收到包含许可有效载荷的消息时，该节点比较所述开始时间与其当前时间。如果所述开始时间比当前时间加上预定增量——例如五分钟——晚，该节点就拒绝该许可，认为其是无效的。

[0054] 许可有效载荷的第二个字段 62 指示许可保持有效的持续时间窗口。这个字段包含一值，该值指示超过许可有效的开始时间的预定时间间隔——例如五分钟的块——的数目。如果节点的当前时间大于许可开始时间加上预定间隔与窗口值之积，该许可就作为无效被拒绝。例如，如果开始时间是 1:00:00，窗口值是 2，当前时间是 1:12:38，那么许可将被拒绝，因为已经过期了。

[0055] 许可有效载荷的下一个字段 64 指示被允许执行的操作。例如，这个字段可以包含指示电力断开操作或者电力重新连接操作的值。多个操作可以与单个许可关联。目标类型字段 66 指示接下来的目标字段 68 的格式。目标字段 68 指定要执行被允许的操作的节点或设备。例如，目标可以是节点的 MAC 地址。目标类型字段 66 指示其中表达这个地址的格式，例如 DER 八位字节串。

[0056] 为了进一步增加安全性，可以强加断开或重新连接命令一次只能发布到一个仪表的约束。在发布许可之前，负荷管理器可以做检查，以确保用于设备的目标地址与单个设备关联，而不是一个组或者广播地址。

[0057] 许可有效载荷可以通过与具有用于所指示操作的特权的证书关联的私钥签名。当接收到包含许可有效载荷的数据包时，节点首先做检查，看所指示的操作是否需要许可。如果需要许可，节点就确认用于给许可签名的证书和私钥是否具有执行所请求操作的必需特权。如果确认是肯定的，节点就验证签名后的许可的真实性，如已经通过所指示证书的对应私钥签名的。然后，节点验证 :目标指定识别节点本身。最后，节点相对于其当前时间检查开始时间与窗口值，以便确认许可还没有到期。

[0058] 如果所有的验证检查都成功，就执行操作，并且返回响应，以确认成功的执行。如果有任何一个验证步骤失败，许可就被拒绝，而且返回错误消息。只要数据包中的所有操作都已经完成，或者返回错误，许可就被丢弃并且不进一步保留。

[0059] 在对掩体的访问已经受损 (compromise) 的情况下，可以实现合适形式的补救动作。一种这样的解决办法是提供与掩体关联的逻辑或物理应急按钮。这种应急按钮可以被激活(诸如，通过有人按下物理按钮或者激活用户接口元素，或者通过自动作出适当决定的逻辑)，以便通知管理系统与该应急按钮关联的掩体已经受损，并且不应当再被信任。例如，对由已经受损的掩体签名的对于远程断开服务的任何请求都应当被忽略。

[0060] 应急按钮可以多种方式实现。合适的例子包括经无线或有线通信系统、位于合适位置(例如员工桌子上)的连接到局域网或广域网的物理按钮，和 / 或具有音频命令能力和无线连接性的可戴式设备发送的控制信号。

[0061] 图 8 说明了其中可以实现应急按钮功能性的一种系统的例子。在这个例子中，公用事业管理与控制系统位于两个数据中心 70 和 72 中。例如，为了冗余，每个数据中心都可

以包含各种管理与控制子系统的完整实例。每个数据中心都包含关联的掩体，分别标记为“掩体 1”和“掩体 2”。每个掩体都具有其根在已知授权机构中的证书链中的证书。用于两个掩体的证书是彼此不同的。

[0062] 控制网络中的每个节点，例如接入点 32 和终端节点 26，具有存储并安装证书撤销列表的能力。接入点 32 还具有过滤来源地址的能力。

[0063] 将对其中对掩体 1 的访问已经受损的情况描述一种示例性操作。与掩体 1 关联的应急按钮被激活，而且结果产生的应急信号发送到掩体 2 中实现应急按钮功能的服务器。这个应急信号包括从其发送该信号的设备的认证的适当指示。例如，它可能包括与设备关联的签名，或者附带根据预定算法生成的哈希值。当接收到通过认证的应急信号时，掩体 2 中的服务器发布配置用于所有接入点 32 的防火墙规则的命令，该命令指示它们丢弃源自数据中心 70 的包。掩体 2 中的服务器还发布配置所有接入点上证书撤销列表的命令，该命令指示与掩体 1 关联的证书不再有效。掩体 2 中的服务器还向每个终端节点发送消息，该消息指示从一个接入点重新加载其证书撤销列表。

[0064] 通过在接入点上配置丢弃来自数据中心 70 的数据包的防火墙过滤器，想成为攻击者的人可以被放慢一段时间，这段时间足以使证书撤销列表传播到所有的终端节点。为了在发生可能的破坏之后恢复掩体 1，必须安装新的证书，而且必须进行与那个证书的新的关联并且将其传播到控制网络中的所有节点。

[0065] 总而言之，所公开的发明提供了各种安全特征，以便减少与由公用事业提供的商品交付关联的恶意或以其它方式不适当的动作的风险。有可能干扰公用事业配送网络稳定性的关键命令是通过限制对后端支援部门管理系统的敏感部件的访问的物理掩体机制并结合使用用于认证、签名和加密这种命令的硬件安全模块来保护的。对于特别关键的命令，基于许可的授权框架提供了更细粒度的安全性。硬件安全模块还可以配置成限制命令执行的速率，从而进一步阻止发布不适当的命令序列的尝试。

[0066] 本领域普通技术人员将认识到，在不背离本发明主旨或本质特性的情况下，所公开的概念可以以其它具体形式中体现。目前所公开的实施例在其所有方面都被认为是说明性而不是限制性的。本发明的范围是由所附权利要求，而不是以上描述，来指示的，而且属于其等同的含义和范围内的所有改变都要包含在本发明的范围中。

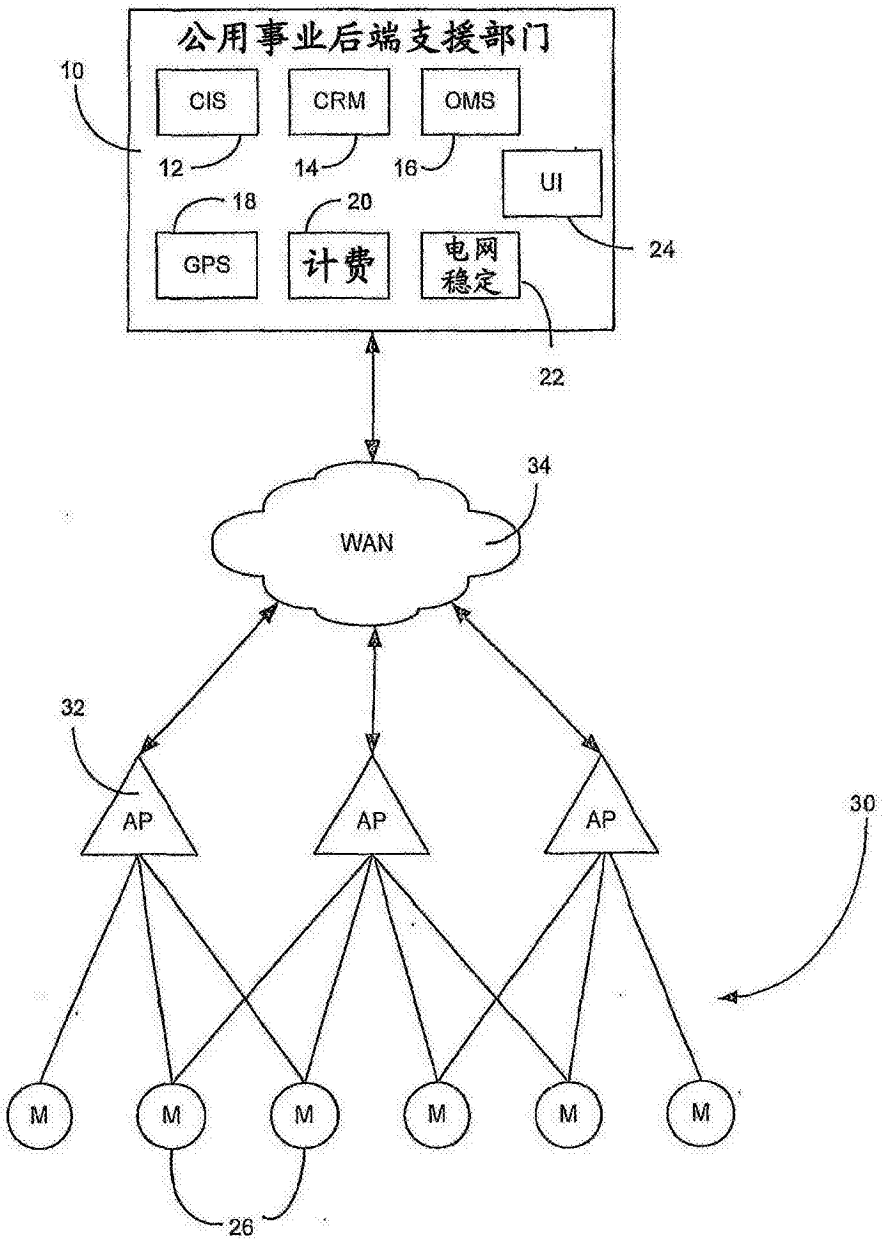

公用事业后端支援部门
10
CIS
CRM
OMS
12
14
16
UI
18
20
GPS
计费
电网
稳定
24
22
34
WAN
32
AP
AP
AP
30
M
M
M
M
M
M
26

图 1

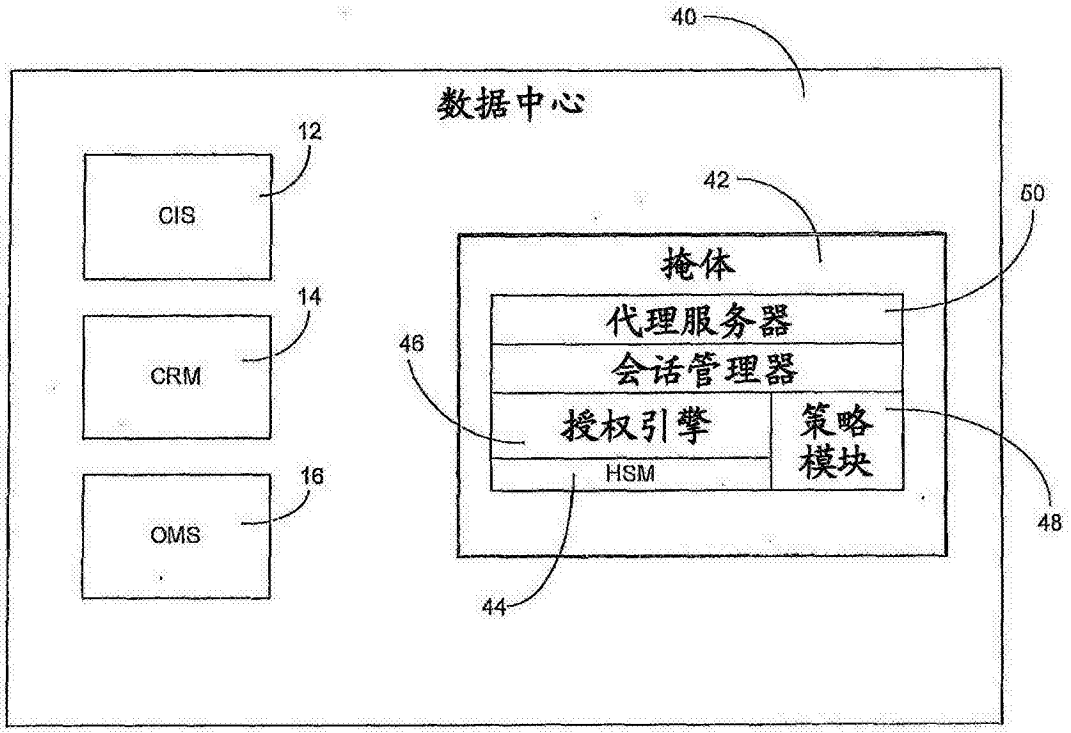

40
数据中心
12
CIS
14
CRM
16
OMS
42
掩体
50
代理服务器
会话管理器
46
授权引擎
策略
模块
HSM
48
44

图 2

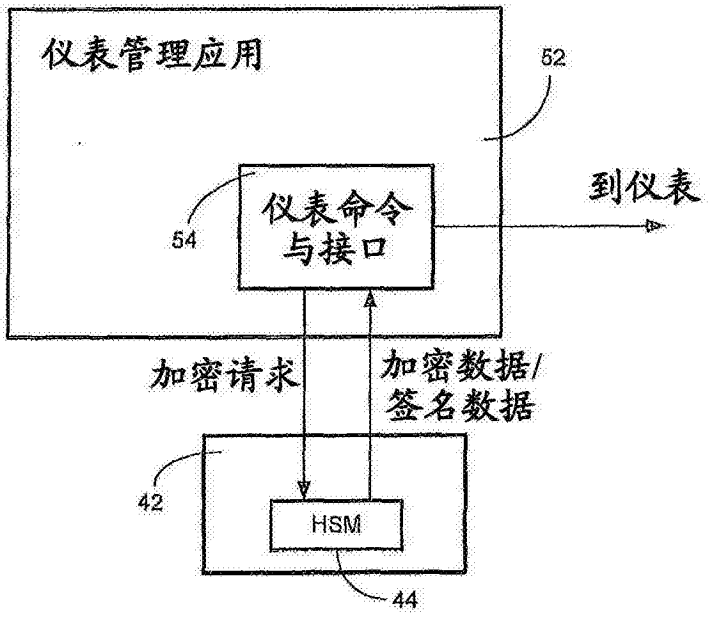

仪表管理应用
52
仪表命令
与接口
54
到仪表
加密请求
加密数据/
签名数据
42
HSM
44

图 3

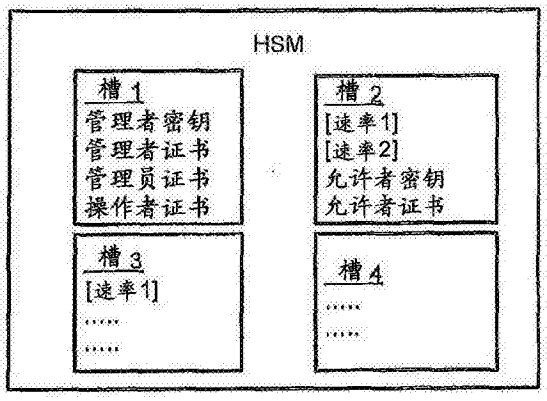

HSM
槽 1
管理者密钥
管理者证书
管理员证书
操作者证书
槽 2
[速率1]
[速率2]
允许者密钥
允许者证书
槽 3
[速率1]
.....
.....
槽 4
.....
.....

图 4

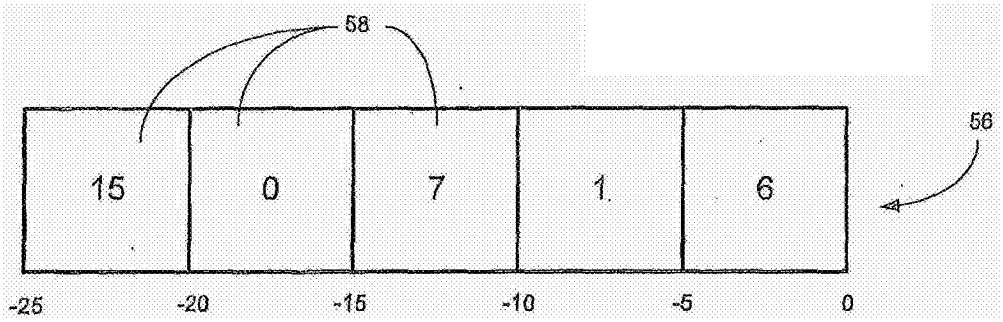

58
15
0
7
1
6
56
-25
-20
-15
-10
-5
0

图 5

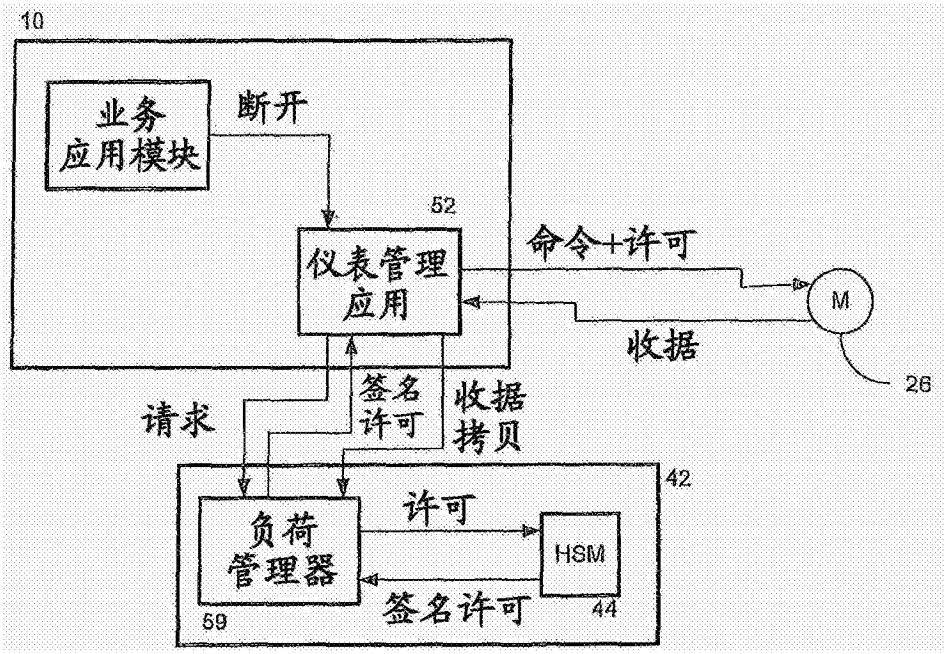

10
业务
应用模块
断开
52
仪表管理
应用
命令+许可
M
收据
26
请求
签名
许可
收据
拷贝
42
负荷
管理器
许可
HSM
签名许可
59
44

图 6

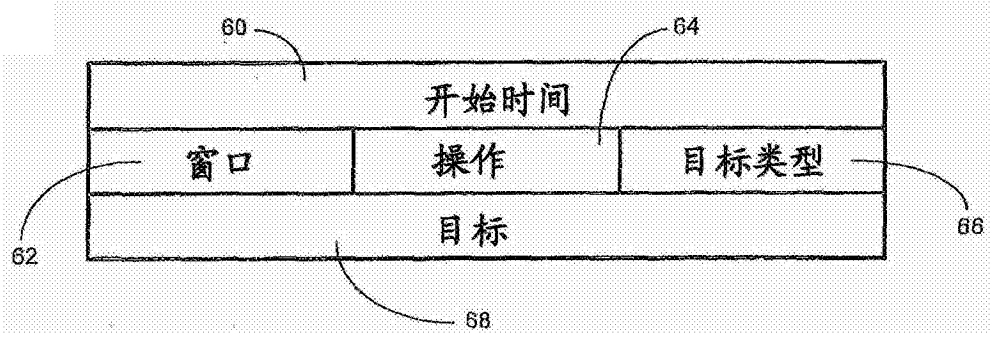

60
64
开始时间
窗口
操作
目标类型
目标
62
66
68

图 7

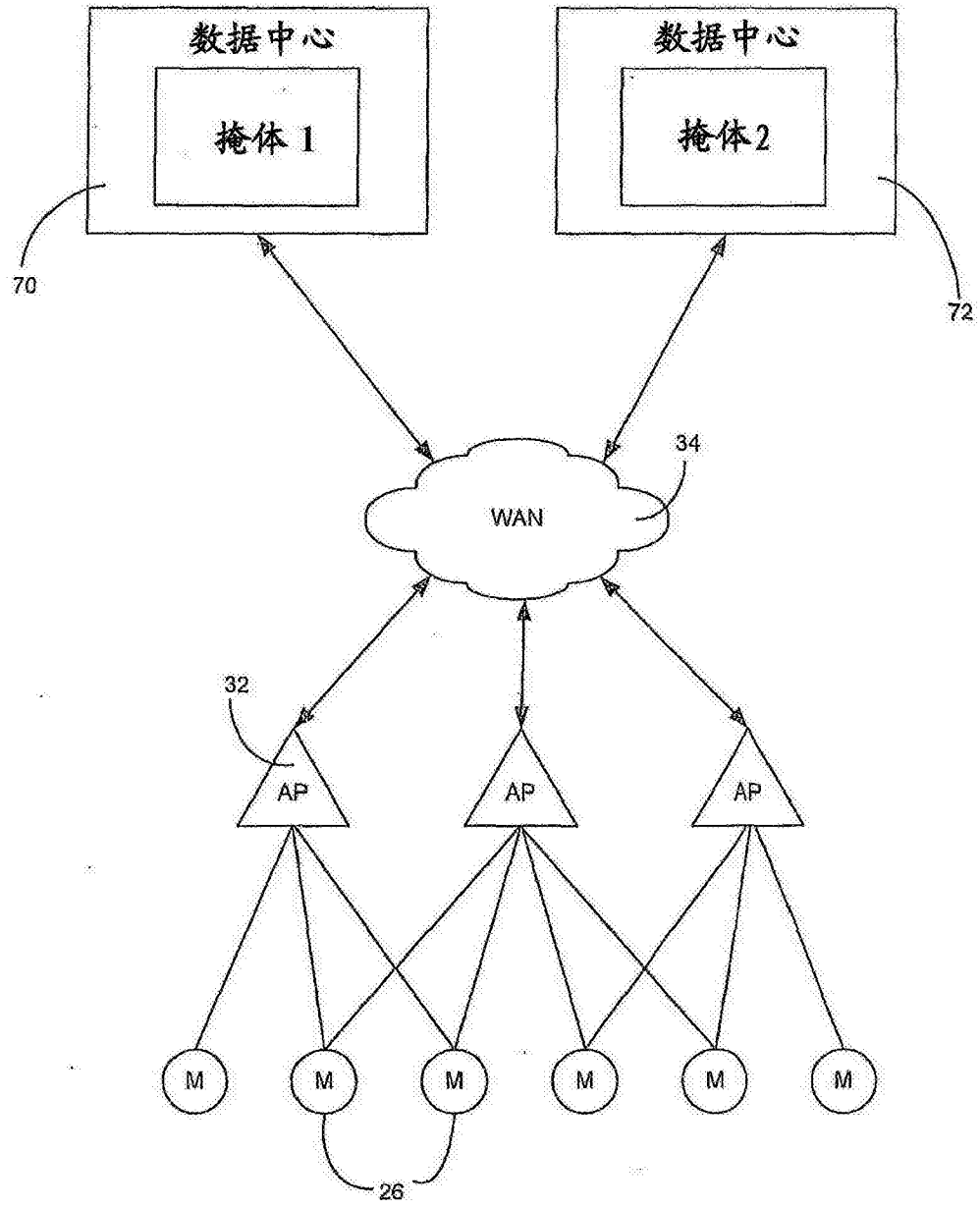

数据中心
掩体 1
数据中心
掩体2
70
72
34
WAN
32
AP
AP
AP
M
M
M
M
M
M
26

图 8