(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 101529795 B
(45)授权公告日 2013.03.13

(21)申请号 200780040384.8

(22)申请日 2007.10.31

(30)优先权数据
60/864,026 2006.11.02 US

(85)PCT申请进入国家阶段日
2009.04.29

(86)PCT申请的申请数据
PCT/US2007/083076 2007.10.31

(87)PCT申请的公布数据
WO2008/055191 EN 2008.05.08

(73)专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬

(72)发明人 O·加西亚 H·巴尔杜斯

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 赵腾飞 王英

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
CN 1753540 A,2006.03.29,
CN 1485737 A,2004.03.31,
Haowen Chan et al.On the Distribution and Revocation of Cryptographic Keys in Sensor Networks.《IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING》.2005,第2卷(第3期),

审查员 张玉洁

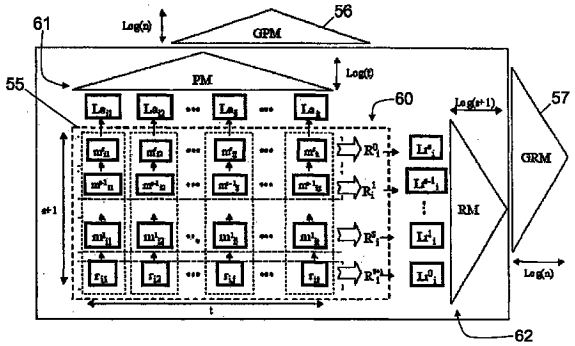
权利要求书 3 页 说明书 12 页 附图 5 页

(54)发明名称

分布式设备撤销

(57)摘要

在一种分布式撤销方法中,在分布式网络的多个自主设备节点中的每一个上单独决定是否应将分布式网络的一个可疑自主设备节点或可疑的所分配密钥从分布式网络中去除。实施投票期,在投票期中将多个自主设备节点的单独决定进行合并,用以决定是否应将可疑自主设备节点或可疑的所分配密钥从分布式网络中去除。响应于投票期决定支持去除,从分布式网络去除可疑自主设备节点或可疑的所分配密钥。



CN 101529795 B

1. 一种分布式撤销方法，包括：

在分布式网络的至少三个自主设备节点之间进行关于是否应将所述分布式网络的可疑自主设备节点从所述分布式网络中去除的投票；以及

响应于所述投票满足撤销标准，借助于以下操作来停止在所述可疑自主设备节点与所述分布式网络的其它自主设备节点之间的通信：(i) 通过合并用于撤销所述可疑自主设备节点的局部撤销信息来构成撤销消息，所述局部撤销信息分布在所述分布式网络上除了所述可疑自主设备节点之外的至少一些所述自主设备节点之间，以及 (ii) 在所述分布式网络的所述自主设备节点之间互相传送所述撤销消息，

其中，基于信任因子对所述投票进行加权，所述信任因子表示所述可疑自主设备节点在所述分布式网络中的可信度。

2. 如权利要求 1 所述的分布式撤销方法，还包括：

将所述撤销消息转发到其它分布式网络中的其它自主设备节点。

3. 如权利要求 1 所述的分布式撤销方法，还包括：

通过将由单向函数处理的所述撤销消息的第一部分与所述撤销消息的第二部分进行比较，来验证在自主设备节点上接收的所述撤销消息。

4. 如权利要求 1 所述的分布式撤销方法，还包括：

通过将由散列函数处理的所述撤销消息的第一部分与所述撤销消息的第二部分进行比较，来验证在自主设备节点上接收的所述撤销消息。

5. 如权利要求 1 所述的分布式撤销方法，还包括：

响应于将用于新的自主设备节点的局部撤销信息从所述新的自主设备节点传送到已经存在于所述分布式网络中的多个自主设备节点，将所述新的自主设备节点并入所述分布式网络中。

6. 如权利要求 1 所述的分布式撤销方法，其中，所述投票在时间上受限的撤销期间中重复进行，在先前撤销期间中的投票不计入随后的撤销期间中。

7. 如权利要求 1 所述的分布式撤销方法，还包括：

用所述分布式网络上的至少一些所述自主设备节点执行多个医学功能。

8. 一种分布式网络，包括：

至少三个自主设备节点，每一个自主设备节点都被配置为与其它自主设备节点安全地通信以便定义所述分布式网络，并和与该自主设备节点进行安全通信的其它自主设备节点协作以执行如权利要求 1 所述的分布式撤销方法。

9. 一种用于分布式撤销的设备，包括：用于在分布式网络的至少三个自主设备节点之间进行关于是否应将所述分布式网络的可疑自主设备节点从所述分布式网络中去除的投票的模块；以及

用于响应于所述投票满足撤销标准，借助于以下操作来停止在所述可疑自主设备节点与所述分布式网络的其它自主设备节点之间的通信的模块：(i) 通过合并用于撤销所述可疑自主设备节点的局部撤销信息来构成撤销消息，所述局部撤销信息分布在所述分布式网络上除了所述可疑自主设备节点之外的至少一些所述自主设备节点之间，以及 (ii) 在所述分布式网络的所述自主设备节点之间互相传送所述撤销消息，

其中，基于信任因子对所述投票进行加权，所述信任因子表示所述可疑自主设备节点

在所述分布式网络中的可信度。

10. 一种自主设备节点，其被配置为与分布式网络中的其它自主设备节点安全地通信，该自主设备节点包括：

用于在分布式网络的至少三个自主设备节点之间进行关于是否应将所述分布式网络的可疑自主设备节点从所述分布式网络中去除的投票的第一单元，以及

用于响应于所述投票满足撤销标准，停止与所述可疑自主设备节点的通信的第二单元，

其中，基于信任因子对所述投票进行加权，所述信任因子表示所述可疑自主设备节点在所述分布式网络中的可信度。

11. 如权利要求 10 所述的自主设备节点，还包括：

数据存储器，用于存储用于可疑自主设备节点的局部撤销信息，所述自主设备节点进一步被配置为响应于所述投票满足所述撤销标准，与其它自主设备节点协作以便将存储在所述数据存储器中的用于所述可疑自主设备节点的局部撤销信息与存储在其它自主设备节点上的用于所述可疑自主设备节点的局部撤销信息进行合并来构成撤销消息，将所述撤销消息在所述自主设备节点之间传送，以实现停止与所述可疑自主设备的通信。

12. 如权利要求 11 所述的自主设备节点，还包括：

数据存储器，用于存储完整的撤销信息，所述自主设备节点进一步被配置为执行一种分布式网络加入方法，该方法包括：将从所述完整撤销信息中得到的局部撤销信息传送到多个其它自主设备节点，被传送到其它每一个自主设备节点的所述局部撤销信息是：(i) 自身不足以重建所述完整撤销信息，但 (ii) 可以与传送到其它自主设备节点的所述局部撤销信息合并来重建所述完整撤销信息。

13. 一种分布式撤销方法，包括：

实施时间上受限的撤销期间，在所述撤销期间中，将多个自主设备节点的个别决定进行合并，以决定是否应将可疑自主设备节点从分布式网络中去除；以及

响应于所述撤销期间决定支持去除，将所述可疑自主设备节点从所述分布式网络中去除，

其中，所述撤销期间的所述实施包括：

基于表示所述可疑自主设备节点的可信度的信任因子，偏移所述决定。

14. 如权利要求 13 所述的分布式撤销方法，还包括：

对在时间上交叠的后续撤销期间重复所述撤销期间的所述实施。

15. 如权利要求 13 所述的分布式撤销方法，还包括：

对后续撤销期间重复所述撤销期间的所述实施。

16. 如权利要求 15 所述的分布式撤销方法，还包括：

当一个撤销期间期满时，丢弃在该撤销期间中做出的所述个别决定。

17. 如权利要求 13 所述的分布式撤销方法，其中，将所述可疑自主设备节点从所述分布式网络中去除的步骤包括：

根据以前在所述分布式网络的至少一些所述自主设备节点之间分发的撤销信息，构成撤销消息；以及

在所述分布式网络中除了所述可疑自主设备节点之外的其它所述自主设备节点之间

相互传送所述撤销消息。

18. 如权利要求 17 所述的分布式撤销方法，其中，将所述可疑自主设备节点从所述分布式网络中去除的步骤还包括：

在除了所述可疑自主设备节点之外的接收到所述撤销消息的每一个自主设备节点上验证所述撤销消息；以及

响应于对接收到的所述撤销消息的成功验证，停止在所述可疑自主设备节点与接收到所述撤销消息的自主设备节点之间的通信。

19. 如权利要求 17 所述的分布式撤销方法，还包括：

响应于将用于新的自主设备节点的撤销信息在已经存在于所述分布式网络中的至少一些所述自主设备节点之间的分发，将所述新的自主设备节点并入所述分布式网络中。

20. 一种自主设备节点，其被配置为与分布式网络中的其它自主设备节点安全地通信，该自主设备节点包括：

用于实施时间上受限的撤销期间的第一单元，在所述撤销期间中，将多个自主设备节点的个别决定进行合并，以决定是否应将可疑自主设备节点从分布式网络中去除；以及

用于响应于所述撤销期间决定支持去除，将所述可疑自主设备节点从所述分布式网络中去除的第二单元，

其中，所述撤销期间的所述实施包括：

基于表示所述可疑自主设备节点的可信度的信任因子，偏移所述决定。

分布式设备撤销

技术领域

[0001] 以下涉及分布式数据采集、处理及相关技术。尤其涉及相互无线通信的医学设备的分布式网络的安全性，其被配置为监控病人的生命特征或其它在诊断上有重大意义的生理参数，给病人提供受控制的药物传送，给病人提供流量受控的静脉注射液传送等，并借助对此的具体参考来加以描述。以下总体上更多地涉及任何种类的自主设备节点的分布式网络的安全性，不论自主设备节点是以无线方式连接还是以有线方式连接，所述自主设备节点被配置为执行医学应用、控制应用（例如分布式建筑物灯光的控制或气候控制通风调节装置 (climate control register)）等。在另一个普遍方案中，以下总体上涉及分布式网络的安全性，在该分布式网络中能够以 ad hoc 方式增加或移除自主设备节点，例如电子设备的蓝牙网络、膝上型电脑或其它具备 WiFi 性能的设备可以以 ad hoc 方式连接及断开连接的 WiFi 热点、分布式对等文件共享网络等。

背景技术

[0002] 自主无线互联医疗设备正越来越多的在医院及其它医疗机构使用。这种设备消除了有线通信连接，例如电缆和导线，否则它们会妨碍医务人员和病人的行动。这种无线自主医疗设备可以互相连接以构成ad hoc分布式网络，其有助于根据病人变化的医疗位置来增加和去除医疗设备。互联为分布式网络的无线自主设备的使用还可以提供了计算资源的有效分布，提高了在发生设备故障时的冗余性，提高了数据存储的冗余性，这在一个设备丢失了其存储内容的情况下会是有优势的，等等。

[0003] 分布式网络暗示了大量的安全性问题。每一个自主设备都代表可能危及分布式网络安全性的点。该设备的自主本质的结果是原则上任何单个设备都可能被恶意软件接管（例如病毒、木马、蠕虫等）。一旦入侵者接管了其中一个自主设备，入侵者就可以使用受危害的设备中断分布式网络或窃取医学数据。例如在 1996 年美国医疗保险携带（流通）和责任法案 (HIPAA) 通过了给予医疗数据的法律保护证明了保持病人医疗数据的完整性和隐私权的重要性。如果分布式网络包括为病人提供治疗的设备（例如静脉注射液流量计、药物传送系统等），分布式网络的这个危害甚至会直接伤害病人。

[0004] 确保网络安全性的两个方式是：(1) 避免任何节点受到危害，或者 (2) 检测受危害的节点，并将其从网络中去除。本文是针对第二个选择，在后一方案中，检测受危害的节点，撤销其网络特权，从而将这个受危害的节点与网络隔离。这个方案将受危害的节点可以造成的损害限制在受危害节点直接控制下的区域中。

[0005] 在集中式网络中，中央服务器节点控制通信，并具有针对网络的其它节点的权限。因此，在集中式网络中，任何指定节点的撤销（除了中央服务器节点以外）都是直接的并且仅仅涉及使支配性的中央服务器节点撤销受危害的节点的网络特权。然而，在分布式网络中，撤销困难得多，因为不存在可配置为授权进行撤销的中央节点。同时，分布式网络的设备的自主本质提高了在单一节点受到危害时所涉及的风险，因为受危害的节点不受集中控制，并且相对更自由地执行恶意的或破坏性的操作。

发明内容

[0006] 根据一个方案，公开了一种分布式撤销方法，包括：在分布式网络的至少三个自主设备节点之间，进行对于是否应将分布式网络的可疑自主设备节点从分布式网络中去除的投票，并且响应于所述投票满足撤销标准，通过以下操作来停止在可疑自主设备节点与分布式网络的其它自主设备节点之间的通信：通过分布在分布式网络中除了该可疑自主设备节点之外的至少一些自主设备节点中的、用于撤销该可疑自主设备节点的局部撤销信息进行合并来构成撤销消息，在所涉及的分布式网络的自主设备节点之间互相传送该撤销消息，并可任选地，将该撤销消息转发到其它分布式网络中的其它自主设备节点。

[0007] 根据另一个方案，公开了一种分布式网络，其包括多个自主设备节点，每一个自主设备节点都被配置为：与其它自主设备节点安全地通信以便定义分布式网络；以及和与该自主设备节点进行安全通信的其它自主设备节点协作以执行在前段落中的分布式撤销方法。

[0008] 根据另一个方案，公开了一种自主设备节点，其被配置为与分布式网络中的其它自主设备节点安全地通信，并和与该自主设备节点进行安全通信的其它自主设备节点协作以执行分布式撤销方法，该方法包括：(i) 在分布式网络的至少三个自主设备节点之间进行关于是否应将分布式网络的可疑自主设备节点从分布式网络中去除的投票，并基于表示分布式网络中该可疑自主设备节点的可信度的信任因子对所述投票进行加权，以及 (ii) 响应于所述投票满足撤销标准，停止与可疑自主设备节点的通信。

[0009] 根据另一个方案，公开了一种分布式撤销方法，包括：实施时间上受限制的撤销期间 (session)，在该撤销期间中对多个自主设备节点各自的决定进行合并以便决定是否应将可疑自主设备节点从分布式网络中去除；并且响应于赞同去除的撤销期间决定，将可疑自主设备节点从分布式网络中去除。

[0010] 根据另一个方案，公开了一种自主设备节点，其被配置为与分布式网络中其它自主设备节点安全地通信，并和与该自主设备节点进行安全通信的其它自主设备节点协作以执行在前段落中阐述的分布式撤销方法。

[0011] 根据另一个方案，公开了分布式医学监控网络中的多个节点。对每一个节点进行编程以便与该网络的其它节点协商并民主地决定是否撤销与被检测到参与一个或多个可疑活动的节点之间的网络通信。

[0012] 根据另一个方案，公开了一种包括多个节点的分布式网络。每一个节点都被配置为：(i) 随机产生并向其它节点分发局部撤销投票，所述局部撤销投票可以被合并以构成针对该节点的撤销消息，以便被分发到一个其它节点的所述局部撤销投票不能由另一个节点进行复制或伪造；以及 (ii) 存储从其它节点接收的局部撤销投票。

[0013] 一个优点在于，通过提供对可疑自主设备节点的网络特权的撤销来提高分布式网络的安全性。

[0014] 另一个优点在于，禁止分布式网络的受危害的自主设备节点妨碍将该自主设备节点从网络撤销。

[0015] 另一个优点在于，减小了将正确运行的自主设备节点或分布式网络的所分配密钥 (distributed key) 从分布式网络不正确去除的可能性。

[0016] 本领域普通技术人员在阅读并理解了以下详细说明后会意识到本发明更进一步的优点。

附图说明

[0017] 本发明会采取多种组件和组件布置以及多个步骤及步骤安排的形式。附图仅是用于示出优选实施例的目的，而不应解释为限制本发明。

[0018] 图 1 以图解方式显示了用于监控并治疗病人的医学设备的分布式网络，其中将所述设备配置为执行分布式设备撤销方法。

[0019] 图 2 以图解方式显示了适于由图 1 的分布式网络或由另一个分布式网络执行的分布式设备撤销方法。

[0020] 图 3 以图解方式显示了二叉树。

[0021] 图 4 以图解方式显示了 Merkle 树。

[0022] 图 5 以图解方式显示了示例性的分布式设备撤销系统数据结构。

[0023] 图 6 以图解方式显示了用于两个相邻撤销期间的相对时序。

具体实施方式

[0024] 参考图 1，在分布式网络 8 的实例应用中，监控及可任选地治疗病人 10。分布式网络 10 包括多个自主设备节点，例如实例示出的设置在胸部的传感器 12、14、16，设置在手腕的传感器 18，静脉 (IV) 注射液滴注流量计 20，和安装在天花板上的显示监视器 22。自主设备节点 12、14、16、18、20、22 执行多种医疗功能，例如：由设置在胸部的和设置在手腕的传感器 12、14、16、18 执行的对监控病人 10 的生命特征或其它在诊断上有重大意义的生理参数的监控；执行治疗功能，例如由流量计 20 控制从 IV 包 24 向病人 10 传送静脉注射液流体；执行辅助任务，例如由显示监视器 22 显示由传感器 12、14、16、18 采集的生命特征数据；等等。监视器 22 的实例显示是显示适合于由设置在胸部的传感器 12、14、16 之一采集的脉搏信息 26 以及由设置在手腕的传感器 18 采集的血液氧合 (SpO_2) 数据 28。

[0025] 自主设备节点 12、14、16、18、20、22 是借助于适合的无线协议，例如蓝牙、Zigbee、WiFi 等，相互通信的无线设备。可替换地，可以使用经由有线网络相互通信的有线设备，例如可以使用有线以太网网络，尽管电缆走线存在电缆连接会妨碍医务人员和病人的行动的缺陷。自主设备节点 12、14、16、18、20、22 是自主的，因为每一个设备都可以独立于集中控制而运行。然而，在一些情况下，当从某些其它设备断开连接时，自主设备会丧失一些功能。例如，传感器 12、14、16、18 会具有有限的数据存储，很少的或没有显示能力。通常，这些传感器 12、14、16、18 与显示监控器 22 一起操作，显示监控器 22 提供了大面积显示以便示出趋势数据等，并且还会具有更大的数据存储器。如果病人 10 移出或被移出房间以致于传感器 12、14、16、18 脱离了与安装在天花板上的监视器 22 的无线接触，那么显示监视器 22 就暂时退出分布式网络 8，并且传感器 12、14、16、18 就丧失了它们的一些功能。然而，自主传感器 12、14、16、18 继续在分布式网络 8 中以降低后的功能级别操作，以采集并存储数据，至少直到板载存储器耗尽为止。可任选地，在这种情况下可以改变数据采集速率、分辨率或其它参数，以便减小存储器使用的速率。类似地，IV 流量计 20 通常可以与医院网络相连接，以便为护士站提供与 IV 输送状态有关的信息。如果病人移出或被移出医院网络的范围，那

么就丧失了这个与护士站通信的功能。然而，在这个功能降低的状态，自主流量计 20 继续操作，以控制到病人 10 的 IV 流体的流动。分布式网络 8 是 ad hoc 网络，在该网络中，设备节点随时可以加入或退出。然而，如本文所述的，与分布式设备撤销系统有关的特定协议对于新加入分布式网络 8 的设备节点而言是必不可少的。

[0026] 每一个自主设备节点通常都对应于一个自主设备，尽管并不总是这样的情况。例如，在一些情况下，单个自主设备会定义两个或更多个设备节点，例如在同时实现两个或更多个虚拟机的单个计算机的情况下。

[0027] 分布式网络 8 是 ad hoc 网络，在该网络中，按照病人状况、病人位置、病人的治疗进程、设备的可用性等所指示的，可以增加或去除设备。例如，在图 1 中，安装在天花板上的显示监视器 22 是分布式网络 8 的一部分；然而，如果病人移出或被移出房间并脱离显示计时器 22 的范围，那么显示监视器 22 就会退出分布式网络 8，至少直到病人 10 回到或被移回无线通信范围中为止。

[0028] 为了保持分布式网络 8 的安全性和完整性，使用了适合的安全性协议。这个协议包括使用密钥保护的通信协议，在该协议中，分布式网络 8 的自主设备仅从分布式网络 8 中包含适当验证密钥或其它适当验证信息的其它自主设备接受数据。这种验证可以基于安全性密钥，例如分级确定性对偶密钥预分配方案 (HDPKPS) 中的密钥，或者共 / 私密钥对等等，或者基本上任何其它类型的安全通信。

[0029] 分布式网络 8 的自主设备节点 12、14、16、18、20、22 的自主本质提出了额外的安全性问题。例如，其中一个自主设备节点会由于被恶意病毒或其它恶意软件代码感染，或者由未授权的人登入等等而受到危害。这个受危害的自主设备节点会继续被配置为与分布式网络 8 的其它自主设备节点进行授权的通信，因为它会继续用识别的共 / 私密钥对协议或其它安全通信协议进行通信。因此，这个受危害的设备造成了显著的安全性威胁。

[0030] 因此，分布式网络 8 的自主设备节点 12、14、16、18、20、22 还可操作地执行分布式撤销方法，其能够实现将受危害的自主设备从自主网络 8 排除。为了确保受危害的设备不能针对未受危害的设备使用该分布式撤销方法，该撤销方法包括在设备节点之间的民主交互。如果针对可疑设备的投票满足撤销标准，那么未受危害的设备就停止与可疑的并被撤销的自主设备进行通信。假定大多数自主设备没有受到危害，这个分布式撤销方案确保了受危害的自主设备不能撤销未受危害的设备，并且不能阻挠对其本身的撤销，因为在未受危害的设备在得票数上会胜过它。

[0031] 参考图 2，描述了分布式撤销过程。在设置操作 40，将能够实现安全的相互通信的安全性信息配置给每一个自主节点 12、14、16、18、20、22。例如，可以使用密钥管理方案，其提供并管理加密密钥以便能够实现安全性服务，例如验证、保密性和完整性。结合实例撤销系统而操作的密钥管理方案包括两个组件：密钥分配和密钥撤销。密钥分配描述如何在自主节点之间分发安全信息，以便引导安全通信。分布式撤销方法能够实现对已经受危害的可疑自主节点的撤销，或者以可信的方式表明对可能的危害的指示。

[0032] 本文公开的分布式撤销方案的特点展现了一些或全部以下特点。首先，撤销方案是分布式撤销方案。分布式网络 8 是不具有集中服务器或控制器节点的 ad hoc 网络，从而使得分布式撤销方案是有优势的。其次，分布式撤销方案利用了分布式网络 8 的自主节点的协作。自主节点 12、14、16、18、20、22 协作，以民主的方式发现受危害或明显受危害的自

主节点，并从分布式网络 8 将其驱除。第三，撤销是受到验证的。该分布式设备撤销方法使自主设备节点的任何足够大的子集在对任何可疑自主设备节点的撤销发生之前，在在该撤销上取得一致意见。为了避免撤销系统排除正确运行的自主设备节点的误用情况，至少借助于那些投票驱除可疑自主设备节点的设备来构成撤销消息，这个撤销消息被配置为在分布式网络 8 的任何自主设备节点受到验证，以便设备节点能够验证针对可疑自主设备节点的撤销消息的真实性。

[0033] 第四，该撤销方法可任选地使用基于可疑设备的可信度的加权。在自主设备节点之间的信任可以不同。作为医学领域中的实例，考虑监控病人生命特征的一组自主传感器设备。如果一个明显不同的（例如不是传感器设备）新的传感器请求允许加入该网络，则传感器设备节点就可以不信任它。如果已经在该网络中的设备节点不信任该新的候选节点，那么撤销就用选择的信任度因子加权该新节点，从而提高了撤销可能性。因此，在一些实施例中，设备撤销方案包括对于不同节点的不同信任度因子，其表示在节点之间的信任的不同程度，以便构建灵活的加权撤销方案。

[0034] 第五个可任选的特点涉及分布式撤销方案的鲁棒性。任何一个给定的自主节点都会表现出偶然的行为，它会被另一个节点视为可疑的。例如，自主传感器设备节点由于假信号 (glitch) 而传送错误的测量值，或者传送在该测量的预期范围之外的真实测量值。这种行为会使得接收方自主节点断定发送节点受到危害，使得接收方节点投票赞成撤销该发送节点。随着时间过去，会认识到这种偶然的不常见的行为会累积到用于撤销的足够票数的点，使得撤销系统排除正确运行的设备节点，该设备节点没有受到危害但表现出偶然的异常行为。为了应付这个可能性，分布式撤销系统可任选地使用时间上受限的撤销期间，每一个投票都基于在该时间上受限的撤销期间中观察到的行为。这个方案避免了在较长的时间段上的偶然异常行为的累积导致不准确撤销的情况。撤销期间是限制了针对一个设备的撤销信息的有效性的时间段。

[0035] 图 2 的分布式撤销方案可以分为两个阶段，即由设置操作 40 体现的部署前阶段，和部署后阶段。在部署前阶段或设置操作 40 中，服务器或其它设置控制器（未示出）产生安全性密码资料 (keying material) 或其它安全性资料，并分发给要并入分布式网络中的每一个自主设备节点。分发的安全性资料包括用于每一个节点的撤销信息，其能够在部署后阶段期间实现设备撤销。

[0036] 在网络建立操作 42 中，设法加入分布式网络的每一个自主设备节点通过向其它节点分发撤销信息来与至少一些其它设备节点进行交互。这种撤销信息的成功分发是与分布式网络建立通信的先决条件。因此，每一个自主设备节点都向分布式网络的其它设备节点散布撤销信息。网络建立操作 42 可以还包括其它操作，例如交换公钥以便能够实现安全通信，确定相互兼容的通信协议等等。在建立操作 42 结束时，建立了分布式网络 8，并且每一个自主节点都在该分布式网络的至少一些其它自主节点之间分发了其撤销信息。

[0037] 用于验证投票和撤销消息的一些适合的验证方案使用单向函数。例如，可以使用散列函数 h，其至少具有以下两个特性：(i) 压缩特性，其中，散列函数 h 将任意有限比特长度的输入 x 映射到固定比特长度 n 的输出 h(x)；以及 (ii) 易于计算的特性，在于指定 h 和输入 x，易于计算出 h(x)。单向散列函数是这样的散列函数：对它难以找到散列到预先指定的散列值的输入。通常单向散列函数具有预映射和第二预映射抵抗性

(pre-imageresistance)。

[0038] 简要参考图3,二叉树也可以用于验证。高度H的完整的二叉树T具有2^H个叶子和2^H-1个内部节点。如在图3的图解实例中(其中在该实例中H=3),每一个内部节点都具有两个孩子,标记为“0”(左)和“1”(右),由三个比特标记每一个叶子节点,例如“000”、“001”等。依据这个命名约定,自然地排序叶子并按照从根到该叶子的路径的二进制表示进行索引,如图3所示。

[0039] 简要参考图4,高度H的Merkle树是对每一个内部节点和叶子分配了1个比特的位串的二叉树。如下确定位串:(i)叶子值(L_j, j=1, …,2^H-1)是一些叶子预映射(m_j)的单向散列函数,以使得$La = h(m_a)$;以及(ii)内部节点是孩子节点或叶子的单向散列函数,以使得$N_{ad} = h(N_{ab}||N_{cd})$或者$N_{ad} = h(L_a||L_d)$。Merkle树可用于以有效的方式验证预映射值-只需要H个值和散列计算来验证2^H个预映射。例如,为了验证图4所示的Merkle树的个别的m_0,可以计算$h(h(h(h(m_0)||L_1)||N_{23})||N_{47})$并将结果与树根$N_{07}$进行比较。

[0040] 改进验证Merkle树(MAMT)适用于识别Merkle树的路径。为此,如下确定位串:(i)由$N_{ad} = h(a||N_{ab}||N_{cd}||d)$或$N_{ad} = h(a||L_a||L_d||d)$给出内部节点(对应于图3中标记为$N_{xy}$的节点);以及(ii)由$L_a = h(a||m_a)$给出叶子节点(对应于图3中标记为“$L_i$”,i=0…7的节点)。MAMT的使用还避免了生日攻击(birthday attack)。

[0041] 依据这些定义,定义了散列链形式(m^1, …,m^s),它是多个值的集合,以便每一个值m^k(除了最后一个值m^s以外)都是下一个值的单向散列函数。就是说,$m^{k+1} = h(m^k)$,其中h()是单向散列函数。在一些实施例中,将给定的散列链第(k+1)个元素,即元素m^(k+1),计算为m^(k+1)=h(k||m^k)。以这个方式构建散列链有利地避免了生日攻击。

[0042] 回来参考图2,节点设置操作40产生分布式设备撤销系统密码资料。在实例实施例中,这个资料包括撤销信息,本文有时也称为局部撤销值或投票。这个信息是向相邻自主设备节点公开的信息,它是网络设置的一部分。相邻自主设备节点可以协作利用该局部撤销投票信息来撤销可疑的自主设备节点。通常每一个自主设备节点都拥有t(s+1)个局部撤销投票,其中t指代每一个撤销期间的局部撤销投票的数量,(s+1)指代撤销期间的数量。在该实例实施例中,每一个自主设备节点的局部撤销值由t个随机撤销值以及从每一个随机撤销值中产生的长度为s的t个散列链的集合组成。

[0043] 在撤销期间中,如果进行投票并决定赞成撤销一个可疑自主设备节点,那么就产生撤销投票或撤销消息,其明确地指示要撤销该可疑自主设备节点。这个撤销投票或消息明确地确定要在撤销期间k中撤销该可疑自主设备节点,并且其只能通过利用该可疑设备节点的第k个撤销期间的局部撤销投票或信息来产生,该局部撤销投票或信息已经在先前在网络设置42期间分发给其它设备节点。

[0044] 在实例实施例中,分布式设备撤销系统密码资料还包括用于验证局部撤销投票或信息的局部撤销投票MAMT,以及用于验证撤销投票或信息的撤销投票MAM。该局部撤销MAMT包括用于验证局部撤销投票的两个MAMT:(i)第一MAMT是撤销验证树(RAT,本文有时也表示为用于设备i的局部撤销投票验证树PM_i),其用于验证一个设备节点的局部撤销投票,以及(ii)第二MAMT是全局撤销验证树(GRAT,本文有时也表示为全局局部撤销投票验证树GPM),其用于验证全部网络设备的RAT。撤销投票MAMT由两个另外的MAMT组成,其功能是验证设备节点的撤销投票或信息。

[0045] 继续参考图 2，并进一步参考图 5，在实例实施例中，在节点设置 40 期间如下产生分布式设备撤销系统密码资料。密码资料的产生具有两个主要阶段：(i) 用于每一个设备的密码资料产生；以及 (ii) 全局 MAMT 产生。图 5 描绘了为自主设备节点 55 产生的分布式设备撤销系统密码资料，以及两个全局 MAMT 56、57。

[0046] 在第一阶段，为每一个设备节点产生密码资料。局部撤销投票信息的产生如下。产生一组随机撤销投票。每一个随机撤销投票都具有长度 1 个比特，并由 $r_{i,j}$ 来表示，其中 i 表示设备，j 表示设备节点中的第 j 个随机撤销投票。在图 5 中，用于设备 i 的随机撤销投票位于用于自主设备节点 55 的分布式设备撤销系统信息的最后一行。对于每一个随机撤销投票 $r_{i,j}$，设置服务器（未示出）都产生长度 s 的散列链。本文将散列元素称为散列撤销投票，并由 $m_{i,j}^{k}$ 表示，其中 i 表示设备节点，k 和 j 表示用于撤销期间 k 的设备节点中的第 j 个散列撤销投票。按如下从随机撤销投票中产生散列撤销投票：$m_{i,j}^{1} = h(r_{i,j})$，$m_{i,j}^{2} = h(m_{i,j}^{1})$，并推广到第 s 个值，$m_{i,j}^{s} = h(m_{i,j}^{s-1})$。在图 5 中，散列撤销投票 $m_{i,j}^{k}$ 由用于自主设备节点 55 的分布式设备撤销系统密码资料内的 t 个 s 个元素的列来进行符号表示。

[0047] 如下产生撤销值或信息。该设置包括产生表示为 R_i^k 的 s+1 个撤销值，其中 i 标识设备节点，k 表示第 k 个撤销期间。这些值由以下给出：对于 k = 0 的值，$R_i^0 = h(r_{i,1} \| r_{i,2} \| .. \| r_{i,i})$，对于 k = 1，…，s，$R_i^{s-k} = h(m_{i,1}^{k} \| m_{i,2}^{k} \| .. \| m_{i,i}^{k})$来给出这些值。在图 5 中，撤销值 60 显示在用于自主设备节点 55 的分布式设备撤销系统密码资料的右侧。

[0048] 局部撤销投票 MAMT 的计算如下。这个 MAMT 验证一个设备节点所具有的局部撤销投票。设备 i 的局部撤销投票 MAMT 具有表示为 $La_{i,j}$，j = 1，…，t 的 t 个叶子。将每一个叶子计算为 $La_{i,j} = h(j \| m_{i,j}^{s})$。本文将用于设备 i 的局部撤销投票 MAMT 的根表示为 PM_i。在图 5 中局部撤销投票 MAMT 61 显示在用于自主设备节点 55 的分布式设备撤销系统密码资料上方，并称为 PM。

[0049] 撤销投票 MAMT 的计算如下。这个 MAMT 验证一个设备所具有的撤销投票或信息。用于设备 i 的撤销投票 MAMT 具有 s+1 个叶子 Lr_i^k，k = 0，…，s。将每一个叶子计算为 $Lr_i^k = h(k \| R_i^K)$。用于设备 i 的撤销投票 MAMT 的根称为 RM_i。撤销投票 MAMT 62 在图 5 中显示在撤销值 60 的右侧。

[0050] 密码资料产生的第二个主要阶段是全局 MAMT 56、57 的产生。表示为 GPM 56 的全局局部撤销投票 MAMT 验证网络设备节点的局部撤销投票。GPM 具有 n 个叶子，其值为 $Lga_i = h(i||RAT_i)$，i = 1，…，n。表示为 GRM 57 的全局撤销投票 MAMT（有时也称为全局撤销投票验证树 (GRCT)）验证全部网络设备节点的撤销投票。GRM 具有 n 个叶子，其值为 $Lgc_i = h(i||RCT_i)$，i = 1，…，n，其中 RCT_i 表示用于设备 i 的撤销投票验证树。

[0051] 继续参考图 2 和 5，作为节点设置 40 的一部分，设置服务器向每一个自主设备节点分发以下分布式设备撤销系统密码资料：(i) 用于自主设备节点的分布式设备撤销系统密码资料 55，其包括 t 个随机撤销投票构成的组 $\{r_{i,j}\}$，j = 1，…，t 以及从所述随机撤销投票中产生的 t 个散列撤销投票或者散列链 $\{m_{i,j}^{k}\}$，j = 1，…，t，k = 1，…，s 构成的组；(ii) 与该随机撤销投票和散列链的组相关联的局部撤销投票 MAMT 61；(iii) 与从随机撤销投票和散列撤销投票中产生的撤销投票或信息相关联的撤销投票 MAMT 62；(iv)GPM 56

的路径，其使设备节点 i 能够验证随机撤销投票和散列撤销投票；以及 (v)GRM 57 的路径，其能够实现对撤销投票的验证。

[0052] 参考图 2，在网络建立操作 42 中，每一个设备节点都向其相邻设备节点公开了足够的撤销信息，以允许相邻设备节点能够协作实现对该设备节点的撤销。这个公开是加入该分布式网络的先决条件。每一个相邻设备节点都接收用于当前撤销期间的局部撤销信息，它是在用于期间 k 的 t 个可能的局部撤销投票中选择的，即 $\{m_{i,j}{}^{s-k}\}$ $j = 1 \ldots t$。所公开的信息对于每一个相邻设备节点都是不同的。例如，如果 $t = 8$，$x = 2$，当前期间是 5，设备节点 #7 具有四个邻居，那么设备节点 #7 会分别向第一、第二、第三和第四相邻设备节点公开 $\{m_{7,0}{}^{s-5}, m_{7,1}{}^{s-5}\}$，$\{m_{7,2}{}^{s-5}, m_{7,3}{}^{s-5}\}$，$\{m_{7,4}{}^{s-5}, m_{7,5}{}^{s-5}\}$，$\{m_{7,6}{}^{s-5}, m_{7,7}{}^{s-5}\}$。每一个相邻设备节点还接收局部撤销投票 MAMT 和 GPM 56 的值，其验证一个设备节点向相邻设备节点公开的局部撤销投票。每一个相邻设备节点还接收撤销投票 MAMT 62 和全局撤销投票 MAMT(GRM)57 的值，其验证当前撤销期间 k 的撤销投票。注意，这些值对于任何单个相邻设备节点撤销可疑的设备节点而言是不够的，因为没有公开对于该节点的撤销投票。撤销投票只能通过共享所公开的局部撤销投票信息而借助于在相邻设备节点之间的合作来产生。

[0053] 继续参考图 2，一旦由操作 40、42 建立了网络，它就运行以执行其预期的功能，例如图 1 以图解方式描绘的实例医学分布式网络 8 的医学监控和治疗功能。在这种操作期间，多个自主设备节点通过彼此发送安全的消息来进行相互通信。在撤销期间 70 期间，每一个自主设备节点都监控它与其它设备节点的通信，其目的在于检测在另一个设备节点上的可疑性质或行为，其可能暗示另一个设备节点是某种方式受到危害的可疑的自主设备节点。可疑性质或行为的一些实例可以包括例如：发送明显不正确的数据值；请求未授权的服务或操作；拒绝对授权请求的响应；对授权请求的不正确或非预期的响应；用无效安全性信息进行通信；等等。从而每一个设备节点都在撤销期间 70 期间对是否投票撤销可疑节点作出各自的决定。为了针对撤销进行投票，设备节点向其它设备节点公开其针对可疑节点的局部撤销信息。

[0054] 继续参考图 2，在撤销期间 70 中的任意时间，设备节点能够进行关于是否排除可疑设备节点的投票。通常，当公开了针对可疑设备的所有局部撤销投票投票时，发生关于撤销的投票。在决定 74，决定投票是否满足撤销标准，例如针对可疑设备的所有局部撤销投票的公开。如果不是，那么撤销期间 70 就继续，直到其时间间隔终止为止。在该撤销期间终止时，丢弃 76 任何公开的局部撤销投票，且新的撤销期间开始。撤销标准例如可以是根据赞成去除可疑自主设备节点的投票数的阈值标准。例如，如果对于可疑设备存在 T 个分布式局部撤销投票，那么 T 个设备节点就必然投票赞成撤销，以便使决定 74 赞成撤销。在其它实施例中，使用了多数决定原则标准，它基于赞成撤销的投票与自主设备节点的总数的比值。在多数决定原则方案中，随着增加的节点的增多，用于撤销的阈值 T 增大。也可以使用其它撤销标准。

[0055] 在一些实施例中，将节点可信度加权 78 并入到撤销标准中。体现在节点可信度加权 78 中的节点可信度与可疑设备节点是否表现出可疑的行为无关，而是与设备节点的使得它具有或多或少的可信度的内在方面有关。这些内在方面可以包括，例如，可疑设备节点与分布式网络的其它设备节点的共同性或区别，假定极为不同的设备节点更有可能是受危害的节点，有可能是由恶意第三方引入来获得对分布式网络的访问。例如，如果将用于执行

非医学功能的设备节点引入图 1 的医学分布式网络 8 中，则为这个非医学设备节点分配表示该设备节点不应轻易认为是可信的节点可信度加权 78 的值，就会是合理的。

[0056] 会影响分配的节点可信度加权 78 的设备节点的另一个内在方面是可疑设备节点是否被配置为与分布式网络以外的设备通信，假定这种外部通信提供了危害可疑设备节点的机会。针对图 1 的医学分布式网络 8 进行考虑，如果安装在天花板上的显示监视器 22 与医院外的网络或与互联网连接，那么为这个显示监视器 22 分配表示该设备节点不应轻易认为是可信的节点可信度加权 78 的值，就会是合理的。相反，如果设置在胸部的传感器节点 12、14、16 仅与分布式网络 8 的其它设备节点通信，那么为这些传感器节点 12、14、16 分配表示这些设备节点更易于认为是可信的节点可信度加权 78 的值，就会是合理的。

[0057] 会影响分配的节点可信度加权 78 的设备节点的另一个内在方面是可疑自主设备节点运行的独立控制或操作系统的类型。如果操作系统是不太安全且更易于受到危害的类型，那么为这个设备节点分配表示该设备节点不应轻易认为是可信的节点可信度加权 78 的值，就会是合理的。相反，如果操作系统是被认为是更安全且难以受到危害的类型，那么为这个内在上更安全的设备节点分配表示该设备更易于认为是可信的节点可信度加权 78 的值，就会是合理的。

[0058] 影响节点可信度加权 78 的各种因素对总节点可信度加权 78 会具有不同的影响。例如，对信息不适当的请求对节点可信度会具有较重的权重，而超出范围的测量值输出会对节点可信度具有较轻的权重。在一些实施例中，将各种因素的每一个对节点可信度的影响存储在每一个节点上的或中央服务器中的数据库中。

[0059] 图 6 以图解方式显示了一个实例，其示出了使用所述撤销期间方案的优势。在图 6 中，以黑点 80 来表示可疑节点的可疑异常行为的每一次出现。在第一撤销期间 70_1 中，两个这种可疑事件 80 出现，使得两个相邻设备节点分别决定撤销该可疑设备节点（假定由两个不同相邻设备节点观察到这两个可疑事件）。这两个设备节点分别投票赞成撤销，但没有观察到可疑行为的剩余设备节点投票多于它们。作为集体，投票反对撤销。在第一撤销期间 70_1 结束时，丢弃这两个赞成撤销的个别决定。大约在第一撤销期间 70_1 的终点，第二撤销期间 70_2 开始。

[0060] 在图 6 中，第二撤销期间 70_2 在时间上与第一撤销期间 70_1 交叠一个较小的时间间隔 $T_{overlap}$（就是说，相对于撤销期间 70_1、70_2 的持续时间来说较小）。如果下一个撤销期间精确地在上一个撤销期间结束时开始，这会导致协议故障，例如如果一个撤销过程在一个撤销期间的终点开始，但撤销消息（它只对该撤销期间有效）在下一个撤销期间的某个时间才会到达网络的其余部分。通过提供相邻撤销期间的时间交叠 $T_{overlap}$，消除了撤销过程的这个可能的异常终止，或者降低了其可能性。在交叠时间间隔 $T_{overlap}$ 期间，撤销过程根据以下规则进行：(i) 分布式网络的成员使用来自最新撤销期间（就是说，用于图 6 的交叠时间间隔 $T_{overlap}$ 的撤销期间 70_2）的局部撤销投票针对要被撤销的节点投局部票；但 (ii) 节点可能会接收并验证来自最新撤销期间（图 6 的期间 70_2）或来自前一个撤销期间（图 6 中的期间 70_1）的合并撤销投票—在任一情况下验证了的时候就撤销可疑节点。尽管交叠时间间隔 $T_{overlap}$ 具有某些优点，但预期是没有交叠，即 $T_{overlap} = 0$。

[0061] 继续参考图 6，在第二撤销期间 70_2 期间观察到单个可疑事件，使得单一相邻设备节点单独决定撤销该可疑设备节点。因此在撤销期间 70_2 的投票中，集合的投票再一次反

对撤销。在不使用撤销期间的情况下，其结果会是赞成撤销的投票会随时间累积，最终导致该可疑设备节点的撤销。这个结果不是所希望的，因为没有受到危害的正常运行的设备节点仍会偶尔表现出被相邻节点认为是可疑的行为，例如偶然的假信号，其导致了明显无效的数据输出等等。

[0062] 尽管撤销期间的使用通常是有利的，但在一些实施例中可以省略撤销期间并允许在延长的时间上累积撤销投票。在另一个变化例中，不是简单地在撤销期间的终点丢弃所公开的局部撤销投票，而是可以将那些局部撤销投票用于调整节点可信度加权 78。例如，如果几个节点通过公开其局部撤销投票来投票撤销可疑节点，但没有足够的未受危害的节点投票赞成撤销以启动撤销操作，针对该可疑设备节点的几个所公开的局部撤销投票的存在可以用于调整该可疑设备节点的节点可信度加权 78。这个方案反映了这些局部撤销投票公开表示了该可疑节点存在某些问题，即使在撤销期间中累积的投票不足以撤销该可疑节点。

[0063] 回来参考图 2，如果在决定 74 中确定投票满足撤销标准，那么设备节点在操作 84 中协作来合并与被撤销的可疑设备节点有关的所公开的局部撤销信息，以构成撤销消息（例如重建存储在被撤销的可疑设备节点上的撤销投票）。构成的撤销消息随后在操作 86 中通过分布式网络相互传送，并接收到该撤销消息的每一个设备节点停止与被撤销的可疑设备节点的通信。这个相互通信 86 的结果是将被撤销的可疑设备节点从分布式网络中排除。可任选地，撤销消息可以包括超出验证该撤销消息所必需的内容之外的额外信息，例如观察到的异常行为的列表或标识，用于帮助技术人员进行随后的诊断。

[0064] 可任选地，响应于分布式网络中接收到并验证了该撤销消息的至少一个自主设备节点（通常除了该可疑自主设备节点之外）与中央控制节点的连接，将该撤销消息传送到中央控制节点。中央控制节点可任选地采取进一步的操作，例如向人员通知与被撤销的可疑设备节点有关的可能的安全性问题，或者采取措施以确保被撤销的可疑设备节点不会加入其它分布式网络，撤销相关密钥，等等。在一些实施例中，预期中央控制器可任选地重新配置并重新接纳可疑节点回到网络中。这种重新接纳是可任选地，以对可疑节点的后续行为的观察为条件，并可以包括向重新接纳的节点分配较低的信任因子。

[0065] 操作 84、86 组成设备节点撤销阶段，只在由投票决定 74 确定要撤销一个可疑设备节点时才会发生。在此情况下，可疑设备节点的相邻节点启动针对它的撤销过程 84、86。为此，相邻设备节点交换它们在网络建立阶段 42 期间从可疑设备节点接收到的、并且它们用 RAT 和 GRAT 值验证过的局部撤销投票。此刻已经公开了用于撤销期间 k 的全部 t 个局部撤销投票 ($m_{i,1}^{s-k}$, $m_{i,2}^{s-k}$, ..., $m_{i,t}^{s-k}$)，被撤销的可疑设备节点的任何相邻设备节点都能够通过计算用于当前期间 k 的 t 个良好排列的局部撤销投票的散列值 ($R_i^k = h(m_{i,1}^{s-k} \| m_{i,2}^{s-k} \| ... \| m_{i,t}^{s-k})$)，来计算针对可疑设备节点的撤销投票。为了验证计算的撤销投票或信息以便核对撤销可疑设备节点的授权，相邻设备节点将计算的撤销投票与验证该撤销投票的撤销投票验证树 (RCT) 和全局撤销投票验证树 (GRCT) 的值一起广播。

[0066] 所述分布式设备撤销系统在与当前密钥分配系统结合时，还可以用于提供密钥撤销。用于撤销受危害的密钥的方案适合取决于所用的密钥预分配方案 (KPS) 的类型。对于随机 KPS，可以通过删除受危害的密钥来实现密钥撤销。例如，一旦一组设备节点投票撤销

可疑设备节点，并启动了针对它的撤销过程 84、86，分布式网络中的所有设备节点都可以删除与被撤销的设备节点的共用密钥。然而，这个方案导致安全链路数量的减少，并减小了网络的连接性。为了避免这个问题，可任选地更新受危害的密钥而不是删除它。在基于 Blundo 多项式的确定性 KPS 中，例如 HDPKPS 方案，不能删除密码资料，因为这种删除会引起网络连接性的显著降低。一旦一个设备受到危害，在此类密钥分配方案中的密钥撤销可任选地更新受危害的密码资料。这个方案包括安全设置服务器或中央控制节点的协作。

[0067] 可以基于表示可疑的所分配密钥的可信度的信任因子，以类似于使用节点信任度加权 78 的方式，来偏移在密钥撤销系统中的投票。这里，由个别自主设备节点进行的投票赞成撤销的个别决定适合基于可疑的所分配密钥的可疑使用。关于是否撤销所分配密钥的集合投票可以基于信任因子，其值与可疑的所分配密钥的长度或密钥的表示其它安全性级别的特性有关，或者其值与发出该所分配密钥的设备节点的可信度有关，等等。

[0068] 现有 KPS 方案可觉察到借助于节点复制、女巫攻击等造成的危害。在基于密钥的随机分配或 Blundo 多项式的密钥预分配方案中可以找到多个实例。在随机 KPS 中，攻击者可以使用来自几个设备节点的密码资料来得到新的密码资料，攻击者从而可以伪造新的身份。在基于 Blundo 多项式的 KPS 中，攻击者通过捕获大于用以成功进行危害的阈值数量的多个设备，可以伪造许多身份，随后读出密码资料，并重建密码资料。本文公开的分布式设备撤销方案可以用于避免这种复制攻击。这个避免的实现原因在于不能复制或伪造分布式设备撤销系统密码资料，因为局部撤销投票是随机产生的，并且只由每一个接收设备节点获知。而且，可以通过使用 MAMT 来验证局部撤销投票。因此，因为不能重建分布式设备撤销系统的密码信息，本文公开的分布式设备撤销方案避免了身份伪造。

[0069] 在医学分布式网络 8 中，检测可疑性质或行为，依据适合的投票结果，能够导致可疑设备节点的撤销。医学分布式网络 8 中的这个可疑性质或行为通常涉及觉察到的或实际的安全性威胁，其中可疑设备节点被觉察到或实际上已经受到入侵者的危害，例如通过数字病毒、木马、蠕虫，或其它恶意软件或可执行数字代码的媒介。然而更普遍的，将可疑自主设备节点的“可疑”性质或行为广泛地解释为被认为是与分布式网络的福利或目的相反的任何特性或行为。

[0070] 例如，本文公开的分布式设备撤销方案的另一个预期的应用是对等文件共享网络，例如基于互联网的对等音乐共享网络、对等电影共享网络等。在这个应用中，可疑行为可以包括违反适用的版权法或道德方面的考虑，试图共享（即发送、企图发送或请求）有版权的资料。例如，每一个合法的自主节点（例如个人计算机、便携式音乐播放器、有互联网连接能力的立体声或娱乐系统，或其它消费者音乐设备）可以保留有版权的歌曲的列表。如果合法的自主设备节点被另一个自主节点连接，该另一个自主节点请求或企图发送在该合法的自主节点的有版权的歌曲的列表上的歌曲，那么该合法的自主节点就适当地做出个别决定：所述另一个自主节点是可疑自主节点，应撤销其在对等共享网络上的接入特权。

[0071] 注意该个别决定不必包括人为干预 - 相反，该合法的自主节点可以检测所述请求或企图发送，识别到它涉及有版权的歌曲，并且拒绝所述企图并记录该个别决定以便在无需任何人为干预的情况下进行撤销。可替换地，可以请求人为干预，例如通过显示该请求并向用户请求关于是否贯彻用以撤销的投票的决定。

[0072] 在预期的分布式对等文件共享应用中，对等网络偶尔会保持撤销期间，在其中，正

在线的自主设备节点（假定为大部分是合法的自主节点，就是说，由守法的用户操作的）对可疑自主节点（在此适合定义为至少一个个别投票赞成对其撤销特权的任何自主节点）的撤销进行投票。再一次，这个投票通常是自动的，尽管可任选地首先请求用户授权参与，或者请求用户授权用以撤销的特定投票，或者请求用户进行干预。

[0073] 通过当前在对等网络上在线的那些自主设备节点的投票表决，确保了不能任意由单个在线的自主节点撤销合法的节点；相反，这个撤销只能是投票的结果，其中足够数量的当前在线的自主节点投票赞成撤销，其表示该可疑自主节点有可能是复制版权触犯者。而且，可以任选地使用本文阐述的其它可选的规定。例如，可以通过将使得用于撤销的个别决定在特定时间段之后结束来引入撤销期间的概念，以便避免起因于几个无意的不适当歌曲请求在几年中累积而造成的对合法用户的特权的撤销。然而，由于在对等网络中在投票时实际在线的可用的设备节点的比例会较低，因此在两个或更多个撤销期间中保留用以撤销的个别投票以增加这种个别投票的持续性是有利的。类似的，可以使用基于可信度的加权，其基于适合的标准，例如适于分配给以前的触犯者的试用状态，该触犯者在试用的基础上被重新接纳到对等网络中。撤销消息可任选地包括超出足以验证该撤销消息的内容之外的额外信息，例如观察到的断定的或明显的版权侵犯的详细列表，其构成了撤销的基础，以便允许断定的版权侵犯者回顾证据，并且如果想要的话，对撤销进行申诉（例如在审查者面前）。

[0074] 在这个对等文件共享网络应用中，“可疑”性质或行为的概念可以超出版权侵犯行为而扩展到其它方面，例如共享或试图共享被检测为包含病毒的文件，或者文件共享网络的过度使用等。而且，尽管描述了可疑设备节点的撤销，但该方案还可以用于撤销与特定设备节点不相关的可疑的所分配密钥。例如，可疑的所分配密钥可以是与歌曲相关联的数字签名。

[0075] 已经参考优选实施例描述了本发明。其他人在阅读并理解了在前详细描述后会想到修改和变更。其旨在将本发明构造为包括所有这种修改和变更，只要它们在所附权利要求或其等价物的范围内。

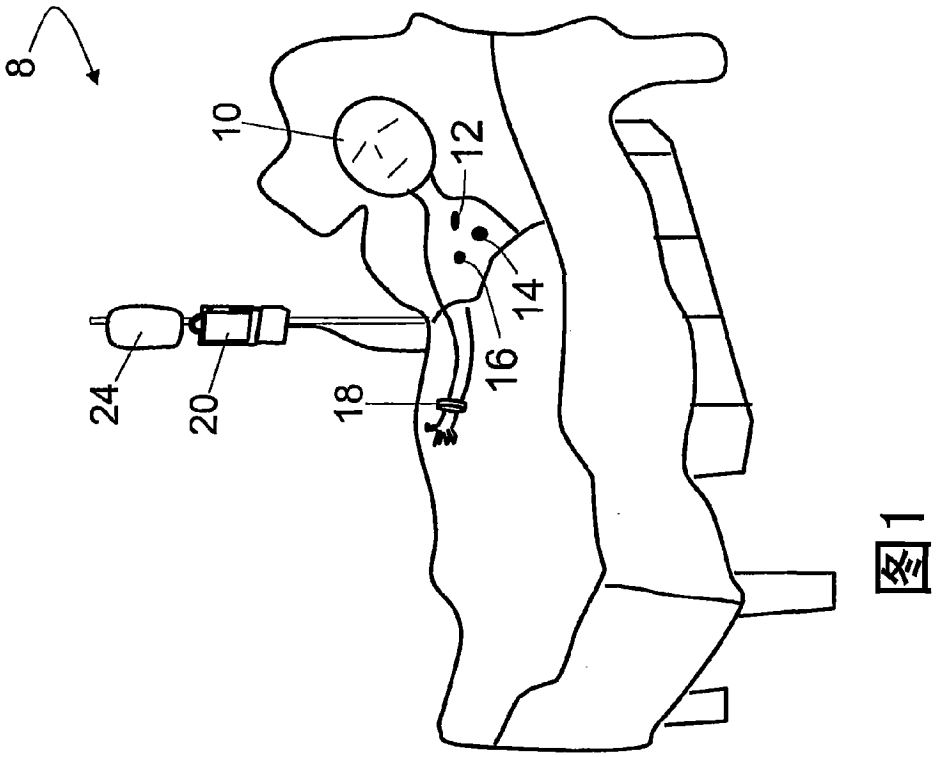
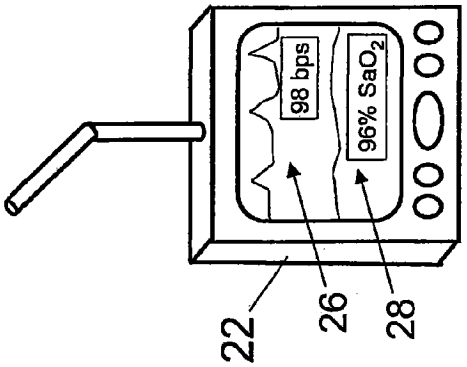


图1



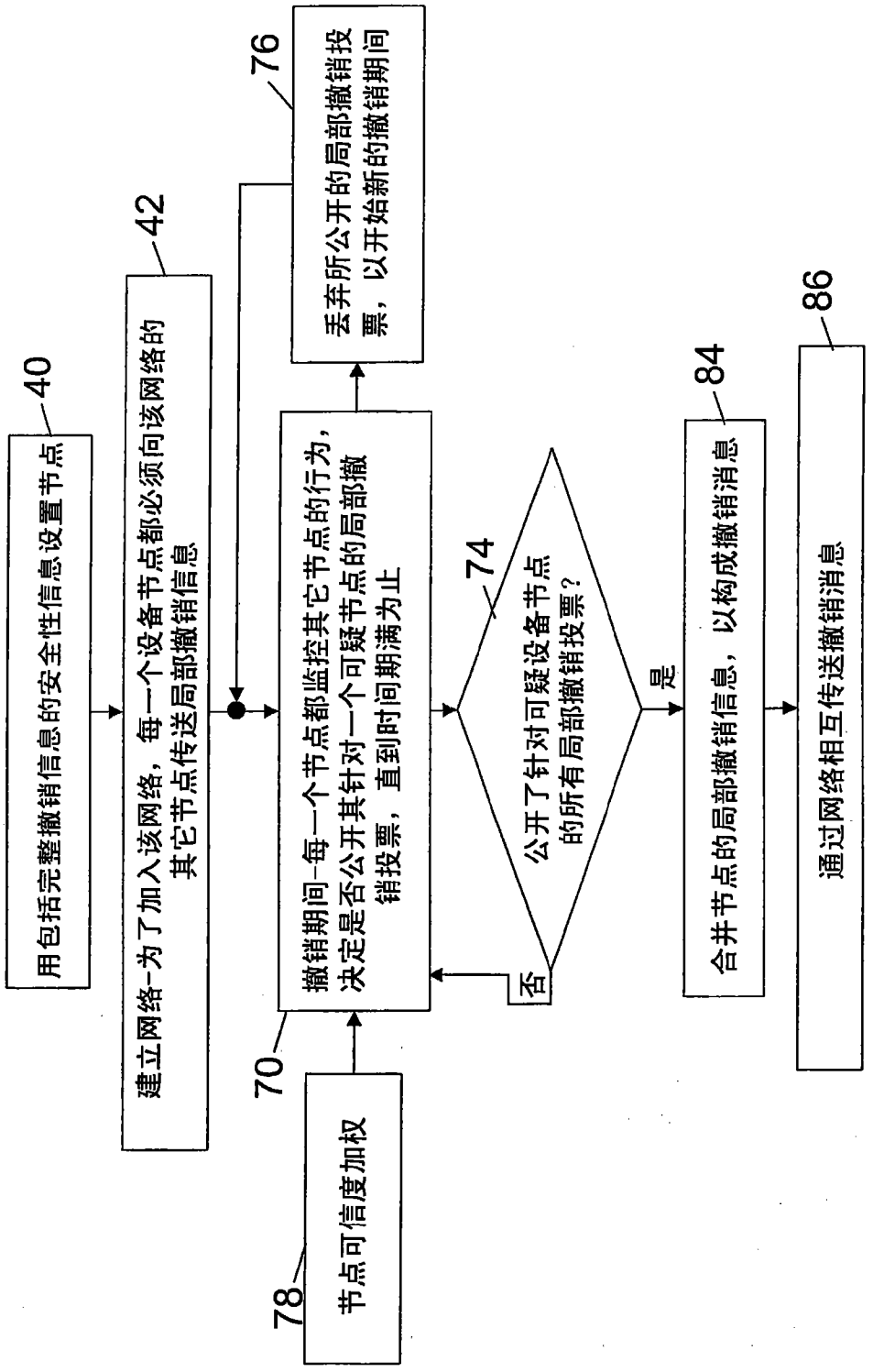

用包括完整撤销信息的安全性信息设置节点
40
建立网络-为了加入该网络，每一个设备节点都必须向该网络的其它节点传送局部撤销信息
42
撤销期间-每一个节点都监控其它节点的行为，决定是否公开其针对一个可疑节点的局部撤销投票，直到时间期满为止
70
节点可信度加权
78
丢弃所公开的局部撤销投票，以开始新的撤销期间
76
公开了针对可疑设备节点的所有局部撤销投票？
74
否
是
合并节点的局部撤销信息，以构成撤销消息
84
通过网络相互传送撤销消息
86

图2

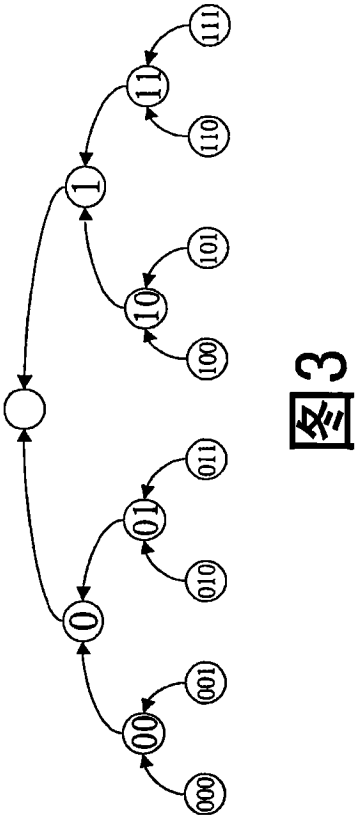

0
1
00
01
10
11
000
001
010
011
100
101
110
111

图3

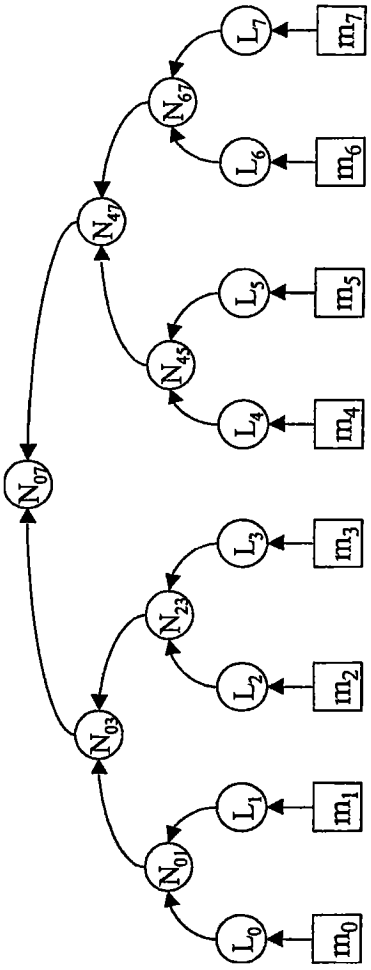

N_{07}
N_{03}
N_{47}
N_{01}
N_{23}
N_{45}
N_{67}
L_0
L_1
L_2
L_3
L_4
L_5
L_6
L_7
m_0
m_1
m_2
m_3
m_4
m_5
m_6
m_7

图4

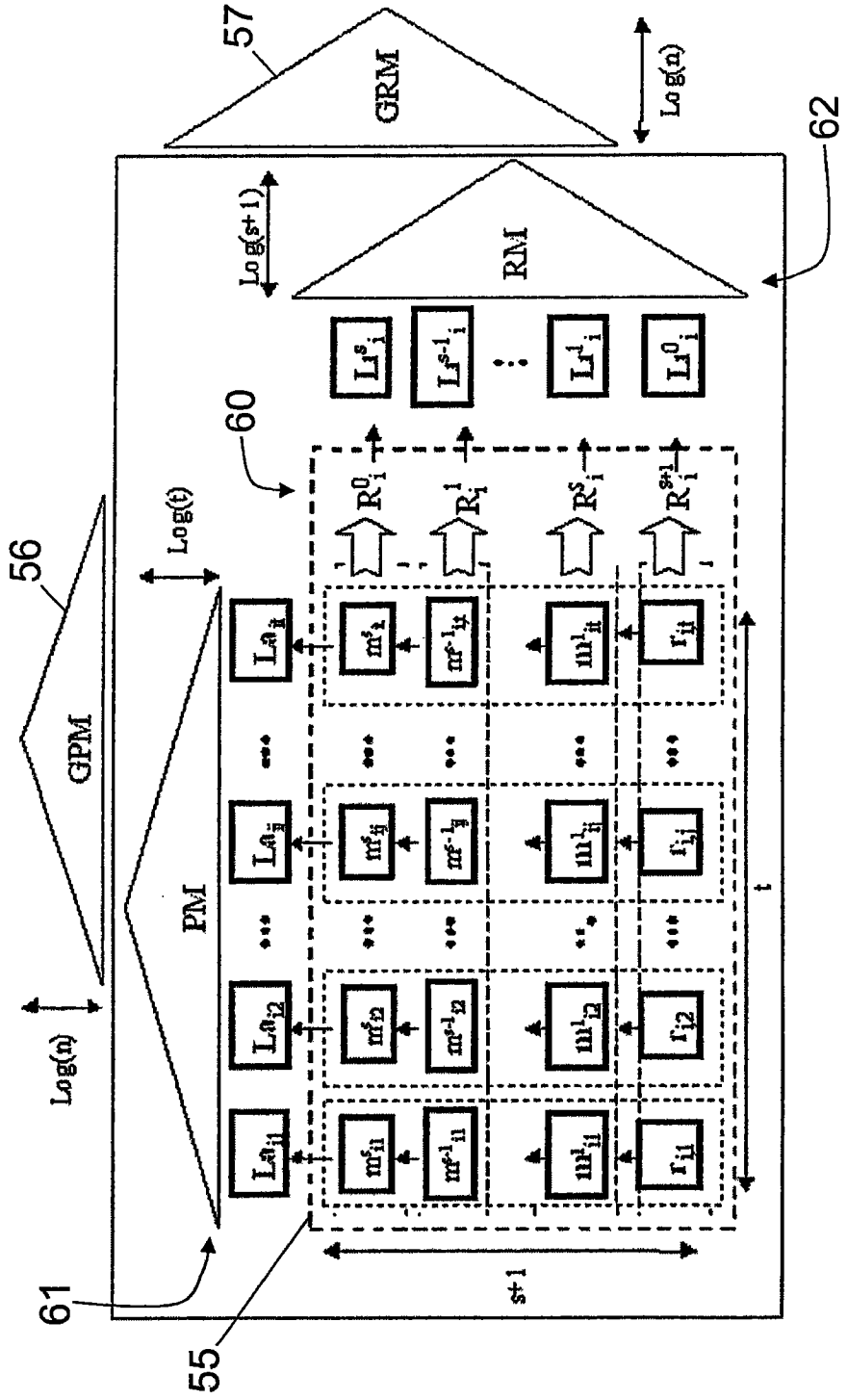


图5

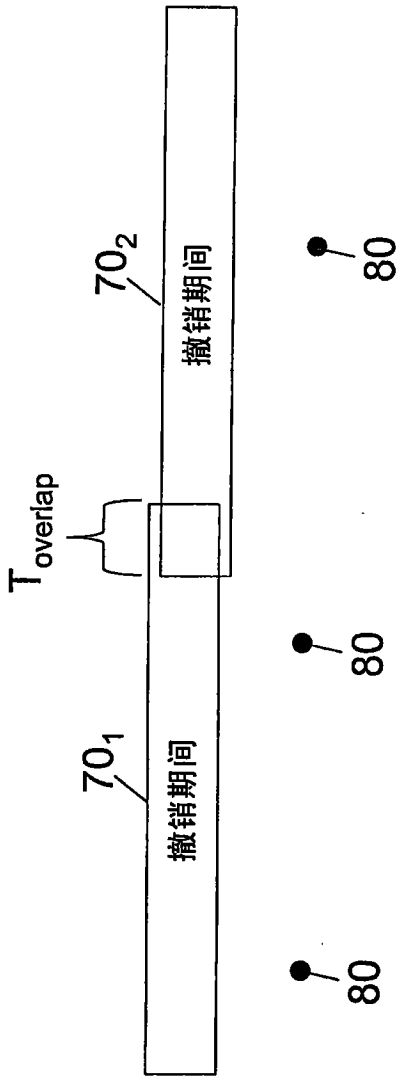


图6