(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 101283539 B
(45)授权公告日 2012.10.24

(21)申请号 200680036993.1

(22)申请日 2006.10.05

(30)优先权数据
60/723,902 2005.10.05 US

(85)PCT申请进入国家阶段日
2008.04.03

(86)PCT申请的申请数据
PCT/CA2006/001639 2006.10.05

(87)PCT申请的公布数据
WO2007/038872 EN 2007.04.12

(73)专利权人 拜尔斯安全公司
地址 加拿大不列颠哥伦比亚省

(72)发明人 埃里克·拜尔斯 达雷恩·利斯摩尔
约翰·卡尔施 凯·李

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 陈源 张天舒

(51)Int.Cl.
H04L 9/00(2006.01)
G05B 23/02(2006.01)
G05B 9/02(2006.01)
H04L 12/24(2006.01)

(56)对比文件
US 20050005093 A1,2005.01.06,
US 20020099958 A1,2002.08.25,
CN 1549493 A,2004.11.24,
US 6970068 B1,2005.11.29,

审查员 廖然

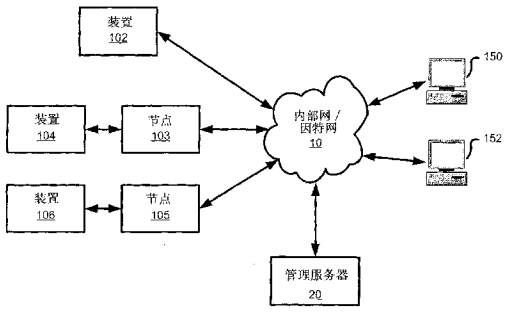
权利要求书 2 页 说明书 11 页 附图 13 页

(54)发明名称

网络安全设备

(57)摘要

一种网络安全设备，该设备通过将业务透明地桥接至终端装置来给工业环境中的装置提供安全。安全设备与管理服务器进行安全地通信，以通过加密的通信为安全设备中的安全模块的操作接收配置数据。当与管理服务器进行通信时，安全设备利用工业装置的网络地址，管理服务器通过采用与该安全设备相关联的被保护装置中的一个的地址对该安全设备进行寻址。安全设备将获知的装置特征提供给管理服务器，管理服务器使软件和安全规则适合装置和控制协议的特定网络漏洞。安全设备采用装置的网络地址将周期性的心跳消息发送给管理服务器。心跳消息还可以报告异常事件，这种异常事件要求管理服务器将另外的软件提供给该节点。



CN 101283539 B

1. 一种在安全设备中保护网络工业装置的方法，该安全设备将网络工业装置耦接至数据网络，该方法包括以下步骤：

在所述安全设备中，对源于所述网络工业装置而到达其它通过所述数据网络可以访问的装置的数据业务进行监视，来确定与所述网络工业装置相关联的属性；

在所述安全设备中，从被寻址到所述网络工业装置的包中接收加密管理连接数据，所述加密管理连接数据源于被连接至所述数据网络的管理服务器；

将传递所确定的装置属性的包发送给所述管理服务器，所述包利用所述网络工业装置的地址作为所述包的起始地址；

在所述安全设备中，从被寻址到所述网络工业装置的包中接收来自于连接至所述数据网络的管理服务器的加密配置数据，其中所述配置数据提供安全描述档，所述安全描述档由管理服务器基于所传递的装置属性进行选择；

在所述安全设备中，基于所述配置数据来对所述网络工业装置和通过所述数据网络可以访问的其他装置之间的包进行管理；以及

利用所述网络工业装置的地址作为所述包的起始地址，从所述安全设备将加密心跳消息周期性地发送到所述管理服务器。

2. 根据权利要求 1 的方法，其中所述包的地址还包括没有被所述网络工业装置利用的 TCP 或者 UDP 端口号。

3. 根据权利要求 1 的方法，其中当将数据发送到所述管理服务器时，所述安全设备既利用所述网络工业装置的层 2 的地址和又利用了所述网络工业装置的层 3 的地址。

4. 根据权利要求 1 的方法，其中基于对所述包进行的管理针对异常事件生成所述心跳。

5. 根据权利要求 1 的方法，其中从包括防火墙模块、装置识别模块、虚拟专用网络模块、侵入检测模块、网络统计收集模块以及带宽监视和业务调整模块的组中选择配置软件。

6. 根据权利要求 1 的方法，其中异常事件使所述管理服务器将重新配置数据发送到所述安全设备。

7. 根据权利要求 1 的方法，其中通信模块接收来自管理服务器的管理连接请求，用于建立与所述管理服务器的加密连接。

8. 根据权利要求 1 的方法，其中通过安全套接链路或 IPSec 安全连接对数据进行加密。

9. 根据权利要求 1 的方法，其中从所述管理服务器提供给所述安全设备的配置数据包括适用于所述网络工业装置所利用的特殊控制协议的安全规则和软件模块。

10. 根据权利要求 1 的方法，其中所述心跳消息和所述加密管理连接数据利用无连接包类型。

11. 一种用于保护处在数据网络内的安全设备下游的一个或多个网络工业装置的安全设备，该安全设备包括：

心跳模块，其利用与所述装置中的一个装置相关联的地址作为包的起始地址，来产生加密心跳消息到所述数据网络中的管理服务器；

通信模块，其用于处理从所述管理服务器传输的并且寻址到所述安全设备下游的一个网络工业装置的包，所述通信模块对嵌入所述包内数据进行解密；以及

可由所述管理服务器配置的一个或多个安全模块，所述安全模块基于与每个或多个网

络工业装置相关联的安全描述档对经过所述安全设备的数据提供安全管理，其中所述安全设备处于所述网络上的装置和所述安全设备下游的一个或多个网络工业装置之间，所述安全描述档由根据经过的数据而确定的装置属性来确定。

12. 根据权利要求 11 的安全设备，其中从包括防火墙模块、装置识别模块、虚拟专用网络模块、侵入检测模块、网络统计收集模块以及带宽监视和业务调整模块的组中选择所述一个或多个安全模块。

13. 根据权利要求 11 的安全设备，其中所述心跳模块产生异常心跳和定时心跳，当所述一个或多个安全模块识别出异常事件时产生所述异常心跳。

14. 根据权利要求 11 的安全设备，其中所述通信模块还包括用于对所述安全设备和所述管理服务器之间的数据进行认证的认证模块。

15. 根据权利要求 11 的安全设备，其中所述管理服务器基于所述一个或多个网络工业装置的属性来配置所述一个或多个安全模块。

16. 根据权利要求 11 的安全设备，其中所述通信模块处理加密包，该加密包是以所述安全设备下游的一个装置的 IP 地址和预定义端口号来寻址的。

17. 根据权利要求 11 的安全设备，其中所述通信模块建立与所述管理服务器的安全加密连接以利用 SSL 或 IPSec 加密技术交换配置数据。

18. 一种数据网络，其包括 ：

多个安全设备，每个安全设备均与多个网络工业装置的一个或多个相关联，所述安全设备透明地将所述网络工业装置桥接到所述数据网络，并且基于与相关网络工业装置的属性相关联的安全描述档，对流入所述相关网络工业装置和从所述相关网络工业装置流到与数据网络耦接的其他装置的数据通信提供管理 ；

管理服务器，其用于管理所述多个安全设备并且给与安全描述档的相关网络工业装置相关的安全设备提供安全描述档以对经过所述安全设备的数据进行管理 ；并且

其中所述管理服务器通过利用相关联的网络工业装置之一的地址与多个安全设备进行通信，并且所述多个安全设备利用相关网络工业装置的地址信息作为心跳消息源来将加密心跳消息周期性地发送到所述管理服务器。

19. 根据权利要求 18 的数据网络，其中所述多个安全设备和所述管理服务器能够建立用于交换配置数据的加密数据连接。

20. 根据权利要求 18 的数据网络，其中所述管理服务器基于所述网络工业装置的属性将配置数据提供给所述多个安全设备中的每一个，其中所述配置数据适合于网络工业装置所用的控制协议及其相关的安全漏洞。

网络安全设备

技术领域

[0001] 本发明涉及工业网络安全，尤其涉及网络安全设备以及部署和管理这些设备以保护工业装置的方法。

背景技术

[0002] 在对诸如发电和配电、石油生产、运输、制造和健康服务之类的关键工业系统进行管理时使用的监视控制和数据采集 (SCADA) 和自动控制设备通过使用诸如 Ethernet、TCP/IP 和 web 服务之类的流行通信技术日益互连起来。虽然 SCADA 和自动控制设备的联网以改进的信息流和效率的形式带来相当多的优点，但是一旦从世界各地都可以访问分离的装置和网络时，这些系统也有可能受到病毒、黑客和恐怖分子的威胁。当前，存在大量的保护不充分的控制装置遍布世界各地。这些控制装置负责诸如电力传输变电所、气体管线、制造工厂等等的关键系统和基础设施的安全操作，然而同时很大程度上未对它们进行保护以避免它们成为恶意攻击的目标。

[0003] 传统的安全解决方案是基于用来保护不安全的内部装置或计算机不受外界攻击的中心防火墙，这种设计不能满足工业控制领域的要求。现存的控制器不提供验证、完整 (integrity) 或加密机制，并且可以被任何能够发现或“ping”该网络和相关装置的个人完全地控制。另外，他们不易于被修补或者添加安全特性。一旦病毒或黑客设法冲破（或已经进入）传统防火墙，由防火墙保护的诸如典型的可编程逻辑控制器 (PLC) 或分布控制系统 (DCS) 之类的装置就成为易于攻击的目标。

[0004] 在很多诸如输油管线或配电系统的工业环境中，在包括偏远区域的宽广地域上可以分布着数以百计的控制器装置。在这些偏远区域通常没有具备管理传统安全装置技能的人员，因此即使装置只需要进行少量本地配置也是无法接受的。例如，提供“透明的”操作的当前防火墙产品仍然需要网络属性（诸如 IP 地址、网关和网络掩码）的本地配置，否则它们就无法被远程控制，这是 SCADA 领域的一个严重的缺点。同样地，由于在这些分布控制系统中存在大量的分离区域（每个都需要防火墙），所以需要从中心区域同时管理数以百计的防火墙的技术，这就排除了采用基于“逐个”管理的流行小型办公室防火墙解决方案。

[0005] 使该问题复杂化的是市场上存在数以千计不同的工业控制装置的零部件，其中每一个零部件采用了 350 种以上的已知 SCADA 通信协议中的一种或多种进行通信。每种控制装置都需要非常特殊的安全规则以被正确保护，例如一种流行的 PLC 对于包含超过 125 个字符的 URL 的 web 请求具有不常见但是众所周知的安全问题。在传统防火墙中人工地为每个被保护装置的各个漏洞创建不同的规则会使整个防火墙配置极度地复杂并且有很可能导致配置错误。

[0006] 最后，操作和维护这些 SCADA 系统的工作人员必然是进行了高度培训的控制系统专家，而不是信息技术或安全专家。因此，这些安全系统的管理需要基于控制技术人员能够理解的新范例，而不是传统的关注于网络系统的管理和配置的网络技术。如果没有针对控制技术人员和控制产品的解决方案，则可能在任何安全解决方案的建立和管理中出现严重

缺陷。

[0007] 因此，需要用于 SCADA 和自动控制设备的网络安全设备，该网络安全设备易于配置并且可被远程可控，并且有助于保护广泛分布工业环境中的具备网络功能的控制设备。

发明内容

[0008] 提供了一种用于保护网络环境中的工业装置的方法、设备和系统。在工业装置的通信路径上配置安全设备或节点，所述安全设备或节点在装置和网络之间透明地桥接业务。当与管理服务器通信时，安全设备利用工业装置的网址，并且管理服务器使用该装置的地址访问该安全设备。安全设备没有唯一的地址，并且通过利用装置地址而不是唯一的地并利用数据加密来提供隐身能力。

[0009] 安全设备通过监视经过的业务来获知正在被保护的装置的特征。该特征然后被提供给管理服务器，该管理服务器能使软件和安全规则适合于装置的特殊网络漏洞和装置所使用的控制协议。配置数据通过安全连接被传送给装置，然后被用于配置安全设备的安全模块。安全设备拦截数据包并且确定该包是来自于管理服务器还是网络上的其它装置，以及是否应该被发送到终端装置或从终端装置发送。如果业务指向终端装置，则安全模块管理业务以保证装置安全。安全设备利用装置网址将周期心跳消息发送给管理服务器。心跳消息还可以描述需要从管理服务器向节点提供附加软件的异常事件。

[0010] 因此，本发明的一方面提供一种采用安全设备保护网络工业装置的方法，该安全设备将网络工业装置耦接到数据网络，该方法包括以下步骤：在安全设备中，监视从工业装置到其它通过数据网络可访问的装置的数据业务，用于确定与该工业装置相关联的属性；在安装设备中，从被寻址到所述装置的包中接收源自于与数据网络相连接的管理服务器的加密管理连接数据；利用与该装置相关联的地址作为包的始发地址来将确定的装置属性发送给管理服务器；在安全设备中，从被寻址到所述装置的包中接收源自于与数据网络相连接的管理服务器的加密配置数据，其中配置数据是由管理服务器基于所提供的装置属性选择的；基于配置后的数据管理工业装置和网络之间的包；以及利用与该装置相关联的地址作为包的始发地址将加密心跳数据周期地发送给管理服务器。

[0011] 本发明的另一方面提供一种用于保护处在数据网络中安全设备的下游的一个或多个工业装置的安全设备，该安全设备包括心跳模块，心跳模块用于产生加密心跳消息，并且利用与该装置中的一个相关联的地址作为该包地始发地址；通信模块，用于处理从管理服务器传输的并且发给安全设备下游的一个装置的包，该通信模块对嵌入包内的数据进行解密；以及一个或多个可由管理服务器配置的安全模块，该模块基于与工业装置的每个或多个相关联的安全描述档对经过安全模块的数据进行安全管理，安全模块处于网络上的装置和安全设备下游的一个或多个工业设备之间。

[0012] 本发明的另一方面提供一种数据网络，该数据网络包括多个网络工业装置；多个安全设备，每个设备与多个工业设备中的一个或多个相关联，安全设备透明地将工业装置桥接到数据网络，并且基于相关联的工业装置的识别特征来对传送到工业装置的和来自工业装置的数据提供管理；管理服务器，用于管理多个安全设备；其中管理服务器通过利用相关联的工业装置中的一个工业装置的地址与多个安全设备进行通信，多个安全设备利用相关联的装置的地址信息作为心跳消息源将加密心跳信息周期地发送给管理服务器。

[0013] 在参考附图对本发明的特定实施例进行如下描述后，本发明的其它方面和特点对于本领域的普通技术人员来说是显见的。

附图说明

[0014] 结合附图，通过接下来的详细描述，本发明的其它特点和优点将变得显见，其中：

[0015] 图 1 图示了与装置串联的安全设备的部署拓扑；

[0016] 图 2 图示了集成在网络交换机中的多个安全设备的部署拓扑；

[0017] 图 3 图示了与装置集成在一起的安全设备的部署拓扑；

[0018] 图 4a 图示了保护多个装置的安全设备的部署拓扑；

[0019] 图 4b 是图 4a 所示的部署拓扑的逻辑图；

[0020] 图 5 以框图形式图示了安全设备；

[0021] 图 6 以框图形式图示了管理服务器；

[0022] 图 7 图示了预初始化阶段消息流；

[0023] 图 8 图示了在装置侧的安全设备中的获知模式的方法；

[0024] 图 9 图示了在网络侧的安全设备中的获知模式的方法；

[0025] 图 10 图示了初始化阶段的消息流；

[0026] 图 11 图示了安全设备中的初始化阶段的方法；

[0027] 图 12 图示了操作阶段的消息流；

[0028] 图 13 图示了在操作阶段中安全节点处理业务的方法；

[0029] 图 14 图示了安全节点更新过程的方法；

[0030] 图 15 图示了管理服务器建立与安全设备连接的方法；以及

[0031] 图 16 图示了管理服务器监视接收到的心跳数据包的业务的方法。

[0032] 注意，在附图中，相同的标号表示相同的特征。

具体实施方式

[0033] 参考图 1 至 16，下面仅通过示例的方式描述本发明实施例。保证工业装置的网络安全已经变得越来越重要。终端装置包括任何具备网络功能的装置，诸如计算装置、工业处理设备（诸如智能测量装置）、工业控制装置（诸如 PLC- 可编程逻辑控制器、RTU- 远程遥测 / 终端单元、IED- 智能电子装置和 DCS- 分布控制系统）、医疗装置等等。例如，在 SCADA（监视控制和数据采集）系统中，RTU（远程终端单元）是安装在偏远地区的装置，该装置收集数据，将数据编码为可以传输的格式，并且将该数据传输返回到中心站或主站。RTU 还从主站收集信息，并且执行由主站指示的处理。RTU 可以配备用于感测或测量的输入信道，用于控制、指示或报警的输出信道以及通信端口。

[0034] SCADA 和自动控制系统通常是用于收集和分析实时数据以及控制工业处理的计算机系统。SCADA 系统可以被用于监视和控制诸如电信、自来水和废水控制、能源、石油和天然气提炼和运输等工业中的工厂或设备。SCADA 系统收集诸如沿管线的压力描述信息，将信息传递回中心站点以警告主站压力可能高于或低于安全界限，执行必要的分析和控制诸如确定情况是否紧急，并且以逻辑和组织的形式显示该信息。

[0035] 为了保护终端装置，网络安全设备或安全节点可以被连续地部署在终端装置的上

游路径中，该终端装置需要诸如防火墙、侵入检测、抗病毒扫描等等的保护。安全节点没有IP地址，因此简化了配置并且很难直接攻击该节点。当安全节点取得被保护的装置中的一个装置的IP地址时，由安全节点产生的业务看起来来自该装置。当安全节点利用层2和层3级别的现有装置地址与管理服务器进行通信时，不需要通过传统防火墙中采用的诸如通过经由动态主机配置协议(DHCP)分配动态寻址或通过手动配置静态寻址的公共IP寻址方法来进行装置地址的重新映射。

[0036] 假如管理服务器能将报文传送到要被保护的终端装置中的任何一个，则可以在控制或SCADA网络中的任何位置，或通过互连的网络来管理安全节点。通过安全管理连接协议对安全节点进行管理。在管理服务器与安全节点连接的过程中，只有流向或来自管理服务器的加密业务被允许进入或流出节点。所有离开节点的业务被警报为好像来自该节点所保护的终端装置。尤其，如果攻击者没有获得需要建立连接的所有信息，则他们甚至不知道节点就在那里。

[0037] 安全节点可适用能运行在因特网协议(IP)之上的任何协议。具体的应用协议可以包括：超文本传输协议(HTTP)(用于通过web浏览器查看要被保护的装置)；文件传输协议(FTP)(用于发送装置数据文件)；Ethernet/IP、MODBUS、DNP3、ICCP、OPC(所有公共SCADA和PLC协议)和IEEE P1073医疗信息总线。当末端装置和网络中的其它装置或计算机之间的业务通过时，安全节点被动地收集信息并且可以将该信息提供给管理服务器。

[0038] 安全节点提供用于在节点(网络安全设备)和管理服务器之间检测、建立和维护安全通信链路的装置，同时又保持节点本身在网络中无法被检测到。这种安全链路可以利用诸如SSL或IPSec的各种已证实的安全协议。安全节点允许有效地部署，而无需本地操作者或节点安装者进行任何配置。如上所述，无需重新配置各种节点和/或终端装置的IP地址。管理服务器以安全的方式远程配置网络安全设备的功能。

[0039] 为了启动远程配置，负责管理节点的策略和设置的管理服务器系统能够通过网络与至少一个该节点将要保护的装置进行通信。安全节点装置策略可以于节点部署之前在管理服务器上进行设置，并且将由节点在其连接到网络并接通电源时下载。这种策略下载使装置在通过或获取状态中花费的时间能够最小化。然而，还可以在管理服务器被配置前保护和部署节点。初始部署安全设置针对安全设备所处网络的位置和设置是特有的。可选地，安全节点可以独立地确定被保护装置的特性，并且在与管理服务器连接前自动地实施一些基本的安全功能。

[0040] 加密心跳机制允许大量(例如数千个)节点报告返回单个管理服务器。心跳机制在SCADA环境内共有的带宽限制系统中是有用的。心跳机制将足够的信息发送返回到管理服务器，用以向安装在节点上的每个安全应用报告当前的状态和条件。通过调节安全节点的心跳设置还可以远程控制报告信息的数量。这种心跳机制还通过使用将异常事件报告给管理服务器的异常报告而避免了基于轮询管理系统比如简单网络管理协议(SNMP)所共有的网络业务负荷问题。这些类型的事件可以包括攻击报告、到达临界系统设置以及其它管理服务器应该立刻知道已经出现了某事的问题。每个安全节点的心跳模块可以用它自己的一套密钥来进行设置。在接收到心跳数据后，确定源并且在管理服务器监视站上完成适当的解密。为了提高可量测性，可以使用多组监视站。

[0041] 图1至4描述了多个网络安全设备的部署拓扑。如图1所示，各种终端装置102、

104 和 106 与网络 10 连接。计算机 150 和 152 或其它管理或监控装置通过网络 10 从终端装置发送和接收数据。网络 10 可以是利用诸如 Internet 协议 (IP) 的各种网络路由协议的控制网络、内部网络或 Internet。如在图中和描述中所示，安全节点 103 和 105 代表网络安全设备，网络安全设备为与网络连接的终端装置提供安全和防火墙类型的功能。如图 1 所示，装置 102 是一个暴露于潜在攻击的未被保护装置，而装置 104 和 106 具有在通信路径上与它们分别串联的安全节点 103 和 105。因此所有到达装置和来自装置的通信必须经过相关联的安全节点，的安全节点在基础水平上用作从装置到网络的桥接器。

[0042] 管理服务器 20 可以与安全节点 103 和 105 连接到相同网络，也可以通过网络 10 被一个或多个网络互连。管理服务器 20 将管理和控制功能提供给网络中的安全节点。

[0043] 图 2 示出一个示例，其中装置 102、104 被网络交换机 200 互连，网络交换机 200 主控各个安全节点 103、105 到 107。网络交换机实质上代表主控多个装置的子网络。

[0044] 图 3 描述了集成的装置和安全节点 300。在该示例中，安全节点 103 可以与装置 102 集成在相同的封装中。依据整个装置 300 的结构，实际的装置功能和安全节点功能可以共享软件和硬件。出于操作考虑，安全节点仍然可以以独立于装置 102 的方式操作。

[0045] 图 4a 和 4b 描述了由单个安全节点 103 保护的多个装置 102、104 和 106。在图 4a 中，安全节点 103 完全地保护和互连多个装置。安全节点 103 可以具有集成的集线器、交换机或路由器，或者它可以与实际的安全节点 103 分离，它的作用是将数据业务分配给相关联的装置。如图 4b 所示，安全节点 103 通过提供单独例子的安全节点 105、107 和 109 看起来像分别给每个装置 102、104 和 106 提供单独的保护。安全节点 103 可以为每个下游装置提供唯一的保护。如果需要，管理服务器 20 可以独立地实施对装置的管理。

[0046] 图 5 示出安全节点 103 的模块。装置接口 502 连接安全节点和被保护的终端装置 104。网络接口 504 连接安全节点和网络侧。这些接口可以执行诸如 Ethernet PHY 管理的标准协议和物理层处理。利用处理器 506 来处理流经装置接口 502 和网络接口 504 的业务。根据安全节点 103 的操作状态，处理器可以通过与该节点的其它模块交互来执行一些功能。在建立与管理服务器 20 的安全管理连接的过程中利用通信模块 508。认证模块 510 保存安全节点和管理服务器之间交换的资格的认证过程中所利用的信息。利用数据库模块 511 来保存安全节点所保护装置的装置描述档和已知对话者的数据库，所述对话者即与正被保护的装置进行通信的外部装置。心跳模块 509 将周期性的心跳发送给管理服务器 20。在诸如企图侵入或发现新装置的异常事件的情况下，可以发送异常心跳来通知管理服务器 20 并且保证执行适当的行动。

[0047] 当安全节点 103 处于操作状态时，可以利用各种网络模块来管理网络业务。例如侵入检测模块 512 监视业务以确定是否存在恶意访问装置 104 的企图，并且执行适当程序以记录和拒绝访问。类似地，防火墙模块 514 提供能与特殊装置 104 的漏洞适合的防火墙功能。其它模块诸如模块 516 可以被部署在安全节点 103 中，这些模块可以提供各种功能：诸如装置识别、虚拟专用网 (VPN)、网络统计收集、带宽检测和业务调整等。

[0048] 在与管理服务器进行安全通信的过程中，通信模块提供由安全节点 103 观察到的关于业务的细节，并且能请求对模块 512、514 和 516 进行软件更新。远程可部署的软件模块以及这些模块的配置和命令可以经由从管理服务器 20 通过网络 10 到达通信模块 508 的安全连接被安全地发送到安全节点 103。可以通过安全通信链路来部署新的或更新的模块

512、514 和 516。

[0049] 为了使安全节点不具有确定的网络地址，每个节点可以使用隐身 IP 寻址方案，其中不将任何的 Internet 协议 (IP) 地址分配给节点（甚至不分配诸如 0.0.0.0 或 192.168.1.1 的泛用地址）。节点从其所保护的终端装置中的一个装置借用 IP 地址，并且使用这个地址来配置和管理通信，以达到上述要求。因此，所有由该节点产生的业务看起来好像来自于下游终端装置中的一个或多个，并且不能被追溯到该节点，这使它不能被看到并且易于配置。另外，安全节点可以采取诸如装置的媒介访问控制 (MAC) 的第二层身份识别以保证隐身能力。

[0050] 图 6 示出管理服务器 20 的模块。管理服务器具有网络接口 602，网络接口 602 用于在管理控制下接收业务并且将业务传输给安全节点。管理服务器通过多个网络可以操纵任何数量的安全节点。处理器 604 通过网络接口 602 接收并且发送业务。处理器 604 与通信模块 606 和远程应用程序接口 608 交互，用于建立与网络中的安全节点的连接。利用数据库子系统 610 存储网络中节点上的信息和特殊类型装置的描述档。然后该描述档可以被下载到适当节点和该安全节点的相关联安全模块上。心跳记录器模块 612 记录来自于网络上的安全设备的周期性心跳消息。与心跳记录器模块 612 串接的是心跳监视模块 614，心跳监视模块 614 用于检查记录的心跳数据，判断其中是否存在需要服务器进行自动操作或引起管理服务器操作者注意的错误或警告条件。

[0051] 与管理服务器 20 的接口被概括为管理 API 616，以便各种用户接口系统 618 可以被用于各种交互功能。用户接口系统 618 可以包括本地图形用户接口 (GUI) 客户端、命令行接口 (CLI) 客户端或安全 web 服务器接口，它们可以在管理系统中被直接访问或者通过直接连接的或通过网络 10 连接的计算机终端 620 远程访问。

[0052] 图 7 示出在预初始化阶段中终端装置 102 和管理服务器 20 之间的消息流。在部署和初始化节点 103 之前，在装置 102 和网络 10 上的其它设备之间可以具有或不具有未被保护的双向网络业务。如果节点 103 物理上就位（但是未被初始化），则它将允许业务 702 通过。然而，节点 103 将记录该业务，用于确定它将保护的装置的类型。在这个预初始化阶段中，管理服务器 20 将在网络 10 上周期性地发送管理连接请求 (MCR) 包 704，发送地址是最终将被节点 103 保护的装置 102，但是将如图 11 所示地被节点 103 拦截。

[0053] 图 8 是安全节点基于来自装置侧的业务的获知过程的方法图。当节点被初始安装并引导启动，并且处于获知模式时，节点确定它将保护的下游终端装置的网络信息。在获知阶段过程中和在管理服务器进行配置前，所有装置业务被透明桥接。可以通过被设置在安全节点上的缺省防火墙规则对包进行过滤（在很多情况下，在这个阶段没有任何防火墙规则，因此将不完成任何过滤）。以被动方式完成装置信息收集并且不产生任何的网络业务。在启动状态中，在步骤 802，安全节点监视源于装置侧的业务。如果该包源于新的源 MAC、IP 地址或端口号（在步骤 804 中为是），则将装置描述记录在位于安全节点内的装置描述数据库 806 中。然后在步骤 808 将该包转发到网络。如果已知该包的源（在步骤 804 中为否），则将没有任何修改的包转发到装置描述数据库中。当安全节点已被配置并且处于检测其它新装置的操作阶段时，获知模式也可以操作。获知模式可以在较低执行优先级操作或者可以在安全节点完全操作的周期间隔中操作。

[0054] 与监视装置侧的业务类似，安全节点也监视网络侧的业务。图 9 是安全节点在网

络侧的获知过程的方法图。在步骤902，监视进入的业务。如果目标地址不在装置描述数据库内（在步骤904中为否），则在步骤910将该包转发到装置接口。如果目标装置处于装置描述数据库内（在步骤904中为是），则在步骤906确定业务的源。如果源处于存储在安全节点数据库模块511内的已知的对话者数据库中（在步骤906中为是），则在步骤910转发该包。如果该装置不在已知的对话者数据库内（在步骤906中为否），则在步骤908记录源信息，然后在步骤910转发该包。

[0055] 在图8的步骤808和在图9的步骤910中的转发包的步骤可以是将包直接转发到对侧的网络接口（可以是装置接口502或网络接口504），或者可以在将包从节点转发出去之前将包转发到安全模块512、514和516进行进一步的处理。如果该包未能通过某个安全模块所进行的检查，则该包可以被丢弃。

[0056] 图10示出在初始化阶段的安全节点103和管理服务器20之间的消息流。当节点103处于适当位置，被接通电源并且已经拦截管理连接请求(MCR)包1002时，初始化阶段开始。带着收集的基本装置信息，节点等待来自管理服务器20的MCR触发。MCR是诸如用户数据报协议(UDP)包的无连接包类型，其包括关于管理服务器20的加密信息、理想管理服务器设置和连接时序。将MCR包寻址到节点后的一个终端装置，但是该包具有该终端装置不使用的端口号。当在步骤1002被安全节点接收时，MCR被捕获，被从网络10移除并且被进行密码检查。该密码针对该节点被部署的位置和终端装置被部署进的网络设置是特定的。节点103将试图对MCR包进行解密并且确认MCR包（详细内容参考图11和12）。MCR包含可以被用来建立管理服务器连接的IP地址、端口号、加密类型和时序。一旦有效的MCR被接收并且被认证，则节点进入管理服务器连接设置模式1004并且以连接肯定应答1006来对服务器作出响应。然后在节点103和管理服务器20之间建立了安全双向连接1008。然后，安全节点103和管理服务器20以安全方式交换信息。

[0057] 设置诸如TCP（传输控制协议）的面向连接协议连接拦截机制，以仅接收来自管理服务器IP地址和在MCR中规定的源端口的业务，以及将业务引导至目标IP地址和在MCR中规定的目的地端口。这种连接拦截系统将连接业务传递给一个在安全节点上运行的控制软件，并且与管理服务器20建立诸如安全套接层(SSL)连接的加密连接。

[0058] 图11是安全节点103的初始化阶段的流程图。图12示出在操作阶段中的安全节点103和管理服务器20之间的消息流。在步骤1102，安全节点103拦截可能是网络10上的包而不管其目的地地址。在步骤1104，对该包进行分析以确定它是否是MCR包。如果该包不包含MCR信息（在步骤1104中为否），则在步骤1122将其转发。如果该包包含MCR信息（在步骤1104中为是），则在步骤1106检查该包的密码以确定该包是否可以被解密。如果MCR可以被解密（在步骤1106中为是），然后在步骤1108对管理通信链路捕获进行准备。如果解密失败（在步骤1106为否），则在步骤1122释放该包以将其转发。

[0059] 在步骤1110，将连接请求中的加密目的地IP地址与安全节点的数据库511中的桥接列表进行对比检查，以确定它是否属于安全节点的下游装置。如果IP地址验证正确（在步骤1110中为是），则安全节点开始侦听安全管理连接(MCE)1112。如果IP地址证明无效（在步骤1110中为否），则在步骤1120丢弃（在步骤1108中确立的）连接捕获并复位，在步骤1122将该包转发。节点仅在一段时间内侦听安全管理服务器连接，这有效地限制了管理服务器20能与节点103连接的时间（即超时管理）。如果安全管理连接在这段时

间内没有开始，而在步骤 1112 节点 103 正在侦听时，连接捕获被丢弃和复位（在步骤 1114 中为否）。如果在超时前接收到连接请求（在步骤 1114 中为是），则在步骤 1116 检查连接安全并且完成连接。如果成功完成连接（在步骤 1118 中为是），然后安全设备 103 进入操作阶段。如果连接不成功（在步骤 1118 中为否），则将该包转发。应该注意，依照 MCR 和 MCE 包的结构，如果包不含有有效载荷信息或任何与终端装置相关联的信息，则可以丢弃该包而不是将该包转发。如果 MCR 和 MCE 信息被嵌入包内并且该过程失败或成功，则在将其转发至终端装置前将该信息从包中剥离。已确立的 MCE 连接是安全加密链路。通过设置数字证书的重新生效水平来完成连接的安全维护。

[0060] 图 12 是安全节点 103 的操作阶段的流程图。一旦确立管理连接，节点 103 就进入操作阶段。管理服务器 20 将在 1202 把基本节点配置上载给节点 103，这将定义将被节点 103 所使用的软件模块、基本配置和心跳设置（参考图 5）。当节点 103 确定新的终端装置的类型时，它将通过安全管理服务器连接来发送针对装置 102 的装置安全描述档请求 1204，装置类型描述档是基于用于获知模式的被保护装置的已知属性。当管理服务器 20 接收到装置安全描述档请求，则它在管理服务器的装置数据库中查询装置类型。装置的安全描述档被产生并且如在管理服务器上所记录地被添加到安全节点的现存安全描述档中。然后在 1206 新节点安全描述档可以被优化并且被下载到节点。如果节点 103（或软件模块 512、514 和 516）需要被关注或在心跳模块中出现周期性请求报告，则节点 103 可以被触发以将心跳消息 1208 发送到管理服务器 20。心跳消息 1208 包含管理服务器关注的请求和请求的原因。当管理服务器 20 接收到这些心跳请求包中的一个时（通过心跳记录器 612 和监视器 614），依照请求的原因和在管理服务器 20 上的当前用户优选设置，它选择服务请求或延迟服务。请求的服务包括建立管理服务器与节点 103（如果节点没有被激活）的连接，以及以命令和响应 1210 的形式来采取适当的命令动作。命令和响应通信还可以被用于重新配置在节点 103 上的可部署软件模块 512、514 和 516 或者部署新的模块。可以通过持续连接进行安全节点和管理服务器之间的通信或基于消息问答的方式启动该通信。

[0061] 在管理服务器连接确立前的等待时间中，连同图 8 所述的获知程序，节点 103 可以使用已确立的被动采指纹技术（诸如“xprobe”和“p0f”开源软件产品中所使用的技术）来识别什么装置将可能需要被保护。甚至在管理服务器配置后，仍可继续使用指纹技术以便对被添加到被保护网络中的新装置进行检测。

[0062] 图 13 是安全节点在操作阶段处理业务的流程图。从初始化阶段（图 11）开始，安全节点现在进入了操作阶段。在步骤 1302，在安全节点的装置接口 502 或网络接口 504 接收业务。在步骤 1304 检查该业务，以将 CMP 相关业务从非 CMP 相关业务分离出来。采用标准 TCP 业务跟踪技术以及对解密的 CMP 包进行排序的包来识别来自 CMP 通信业务的包。CMP 消息是被引导到安全节点的嵌入包，其需要安全节点执行更新。如果识别结果是 CMP 业务（在步骤 1304 中为是），则如在 CMP 消息中所定义地更新节点或执行命令。如果识别结果不是 CMP 业务（在步骤 1304 中为否），则在步骤 1306 利用安全模块 512、514 和 516 来管理包。如果安全模块中的一个识别出该包存在异常条件（在步骤 1308 中为是），例如包被寻址到对特别装置关闭的端口，或该包包含恶意命令，则在步骤 1310 基于各个安全模块所定义的管理规则来处理业务。在此阶段还可以记录关于该包的细节，用于进一步的分析。然后，在步骤 1312，心跳模块将异常心跳发送给管理服务器 20，管理服务器 20 识别出事件发

生。每次事件，心跳消息都发生，或者在一定数量事件发生后被触发。

[0063] 安全节点（网络安全设备）和管理服务器之间的通信操作基于“心跳”信令和“异常报告”的原则。采用心跳信令以将节点的当前状态条件发送给管理服务器。异常报告通信用于将发生在节点上的异常条件发送信号到管理服务器。采用加密可以保护从节点到管理服务器通信的这两个原则。

[0064] 如果业务经过安全模块，而且没有检测到异常业务（在步骤1308中为否），则在步骤1314出现用以确定周期心跳是否被发送到管理服务器的检查。如果需要心跳（在步骤1314中为是），则在步骤1316发送心跳，并且在步骤1318将该包转发到适当接口。如果不需要心跳（在步骤1314中为否），则包被转发到适当接口并且安全节点继续检测到来的业务1302。

[0065] 图14是安全节点更新过程的流程图。如果安全节点在图13的步骤1304接收到CMP消息，则在步骤1402对包进行解密。包的有效载荷可以包含诸如安全描述档或软件更新的配置信息。在步骤1404实施适当配置改变，在步骤1406执行软件模块512、514和516的更新。依照安全节点的操作，如果需要，可以执行诸如节点本身的热重启或冷重启等其它步骤以实施软件或硬件更新。

[0066] 图15是管理服务器20确立与安全节点的MCE连接的流程图。在步骤1502，使用属于特定安全节点所保护的装置的地址，管理服务器将MCR消息发送到该节点。在一段预定义时间后，在步骤1504发送MCE包。如果连接不成功（在步骤1506中为否），在与理想节点的连接被确立或预定义时间期满前，管理服务器20继续1502的发送。如果MCE成功，并且适当的数字证书和密码短语正确，连接已被接受并且与安全节点确立了安全通信（在步骤1506为是），则在步骤1508接收节点信息。然后，在步骤1510，节点将其通过监视业务所确定的装置信息传输给终端装置。然后，在步骤1512，管理服务器20可以为装置确定适当的安全描述档。如果可以获得安全描述档信息（在1512中为是），则在步骤1514从管理服务器20数据库取回适当的规则和软件。如果在数据库中不存在装置描述档（在步骤1512中为否），则在步骤1520取回一般描述档，并且可以在步骤1522基于对安全节点在步骤1510所提供的装置信息的分析创建定制描述档。然后，在步骤1516，将该描述档作为CMP业务发送给安全节点，并且在步骤1518将其激活。

[0067] 当启动安全节点时发生描述档上载，但是当在管理服务器20接收到表示终端装置发生了某些变化或已经检测到新的安全威胁的异常心跳时，也可以发生描述档上载。

[0068] 市场上存在成千上万种不同的工业控制装置的零部件，每个零部件采用350种以上的已知的SCADA通信协议中的一个或多个进行通信。每种控制装置需要非常特殊的安全规则以被正确保护，例如，一种流行的PLC（终端装置的示例）对于包含超过125个字符的URL的web请求具有不常见但是已知的安全问题。当另一个PLC接收到具有选择码为4的MODBUS对话消息并且需要电源复位以恢复时，它会停止所有通信。在传统的防火墙中，手动创建规则以满足这些问题则要求具有关于控制产品缺点和怎样创建用户防火墙的规则集的广泛知识。这也可能使整个防火墙设置过度复杂，也增加了在设置中产生严重错误的可能性。

[0069] 在管理服务器上的数据库子系统610内提供了为公共控制产品开发的特殊装置规则模板。针对上面提到的第二PLC的这种模板示例可以是特殊漏洞保护规则，诸如：

[0070] ●拒绝来自所有地址的选择码为 4 的 MODBUS 对话消息

[0071] ●拒绝来自所有地址的 HTTP 消息

[0072] ●拒绝来自所有地址的 VxWorks™ 生产商开发者端口消息可以提供装置特殊业务控制规则，诸如：

[0073] ●允许来自 PLC 编程站的 MODBUS 固件加载消息

[0074] ●拒绝来自所有其它地址的 MODBUS 固件加载信息

[0075] ●允许来自操作站的 MODBUS 读消息

[0076] ●拒绝来自所有其它地址的 MODBUS 读消息

[0077] ●拒绝来自所有地址的所有其它 MODBUS 消息

[0078] 基于前述的装置发现过程，规则集可以被自动加载到安全节点。在本发明中，采用软件语言编译器中共用的已知技术来组合和优化多个规则集，但是这些技术在安全设备领域是未知的。可以采用文本形式或图形形式来进行用户确认（如果需要），其中用户在模板中的推荐规则上进行点击并且拖曳允许装置的图标以调整针对特殊地址的规则。

[0079] 如上所述，代替由安全管理器 20 为安全节点创建规则集并且上载它们，根据要被保护的终端装置可以自动创建规则集。注意，规则集是依据要被保护的终端装置的需要而设计，而不是依据节点的需要。例如，节点获知需要被保护的 PLC 或 RTU（终端装置的示例）的构造，并且通知管理站。然后，管理站进行数据库查询，并且推荐用于保护该装置的适当的防火墙或 IDS（侵入检测系统）模板。然后，安全管理器判断这些规则是否满足它们的需要，并对它们进行相应地修改以及将他们部署到现场（这同样适用于当节点保护多个不同终端装置时的情况）。对于操作者，看起来好像这些规则被直接发送给装置，并且看起来好像其中不包括节点 / 防火墙。这降低了规则的复杂性，并且将焦点集中在保护装置（例如 PLC、RTU 等）不受不必要业务的干扰。在将节点部署在现场前，也可以创建规则集，以便该装置在加电时自动获得它的配置。

[0080] 图 16 是管理服务器 20 监视接收到的心跳数据包的业务的流程图。在步骤 1602，心跳记录器 612 监视进入管理服务器 20 的业务。如果在步骤 1604 接收到心跳包，则在步骤 1606 执行节点查询并且对该包进行解密。如果该包不能被解密（在步骤 1608 中为否），则丢弃它。如果该包可以被解密（在步骤 1608 中为是），则对心跳有效载荷进行处理以确定安全节点的状态并且在步骤 1612 确定是否有反常条件被报告。如果存在表示需要改变安全策略的条件，则利用现存的 MCE 或建立一个新的 MCE 以将更新的描述档发送给安全节点。

[0081] 适合的计算系统环境或可以适合实施各种实施例的配置的示例包括：一般用途个人计算机 (PC)；掌上或手提式计算机；基于多处理器的系统；基于微处理器的系统；可编程消费电子装置；网络计算机、小型计算机、大型计算机；分布计算环境；工业处理设备；工业控制设备（诸如 PLC、RTU、IED、DCS）和医疗设备等等。

[0082] 典型计算装置的组件包括，但是不限于，处理单元、输入 / 输出接口、系统内存和系统总线。系统总线与上面提到的组件和许多其它协同交互组件可通信地连接。输入 / 输出接口通过输入 / 输出单元（可以包括键盘、鼠标类型的控制器、监视器、媒体读取器 / 写入器等等）与外部组件交互。系统内存例示了根据本发明实施例的网络安全设备的各种组件和操作。

[0083] 详细描述并不将本发明实施例的实施局限于任何特定的计算机编程语言。只要OS(操作系统)提供了可以支持计算机程序产品要求的设备,则计算机程序产品可以用很多计算机编程语言实现。本发明的示范性实施例可以用C或C++计算机编程语言实现,或可以用其它受支持的编程语言混合实现。所提出的任何限制可能是特定类型的操作系统、计算机编程语言或数据库管理系统所导致的结果,而不是对本文所述的本发明的实施例的限制。

[0084] 上述的本发明实施例仅仅是为了说明目的。本发明的范围仅被附加的权利要求唯一地限制。

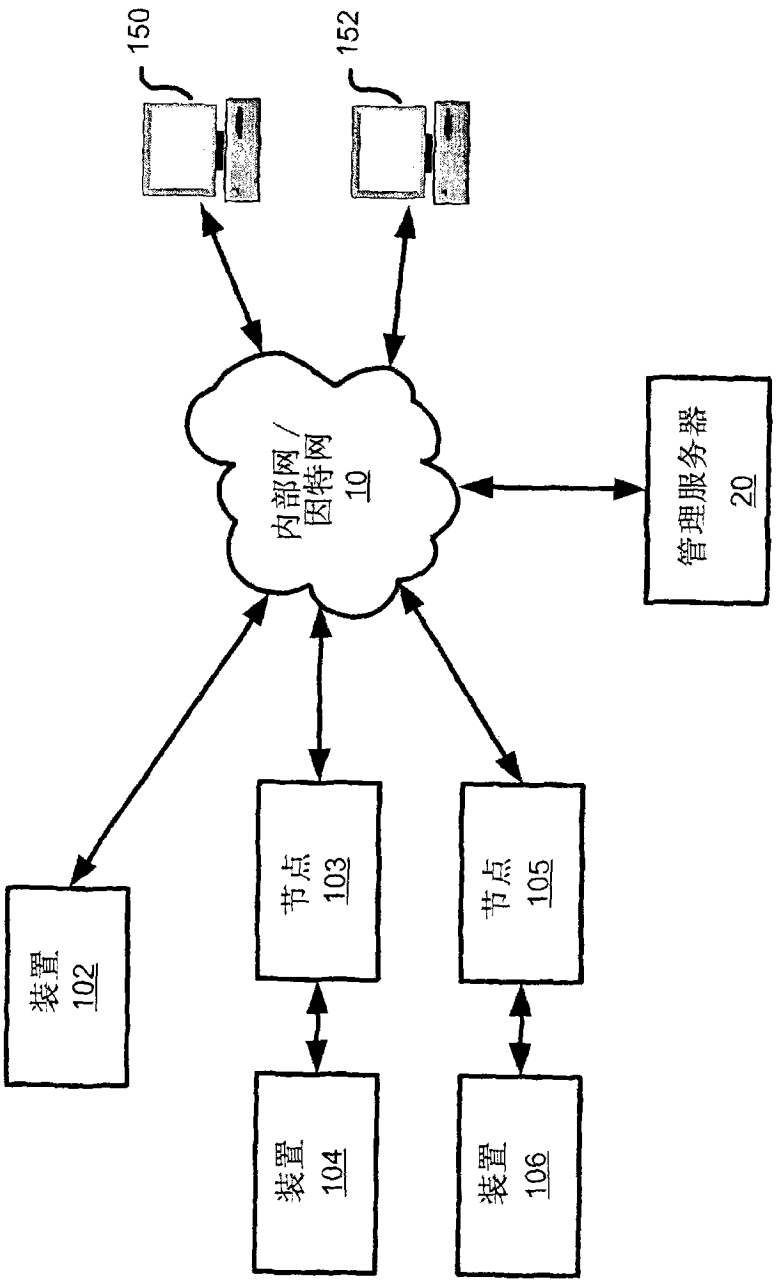


图 1

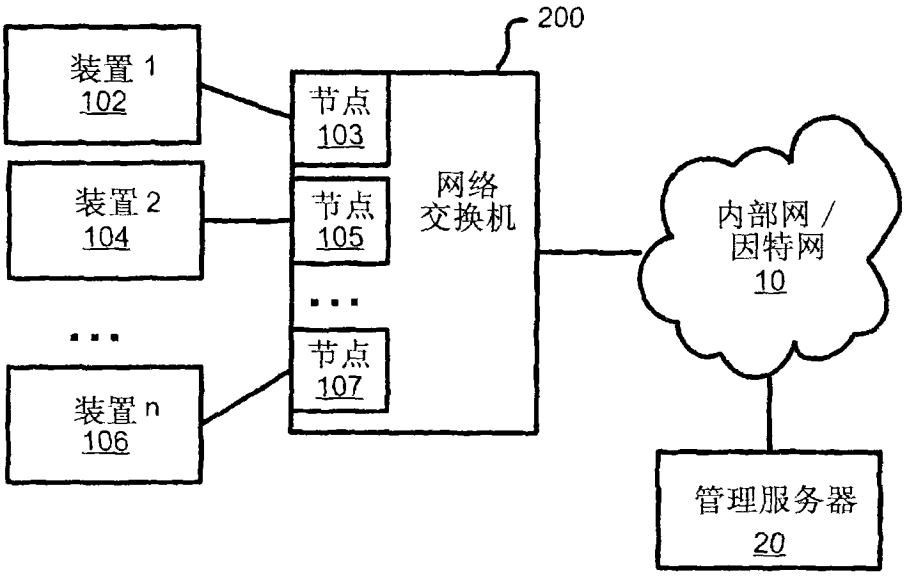

200
装置 1
102
装置 2
104
装置 n
106
节点
103
节点
105
节点
107
网络
交换机
内部网 /
因特网
10
管理服务器
20

图 2

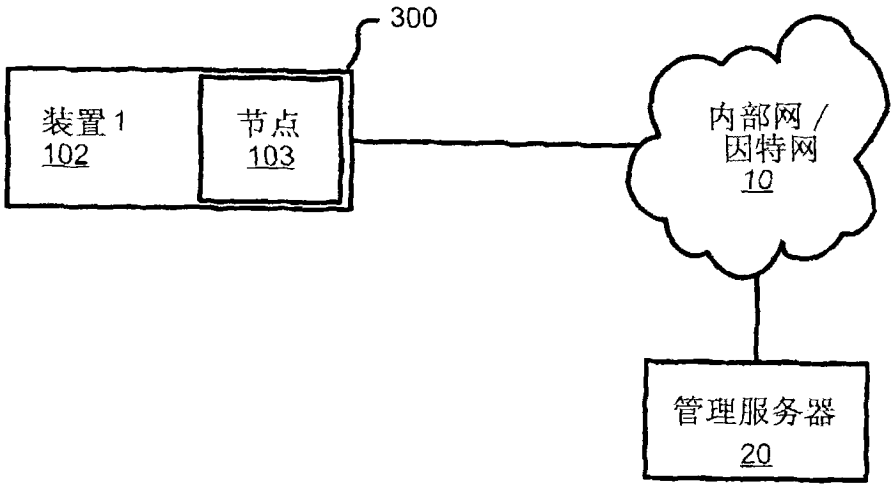

300
装置 1
102
节点
103
内部网 /
因特网
10
管理服务器
20

图 3

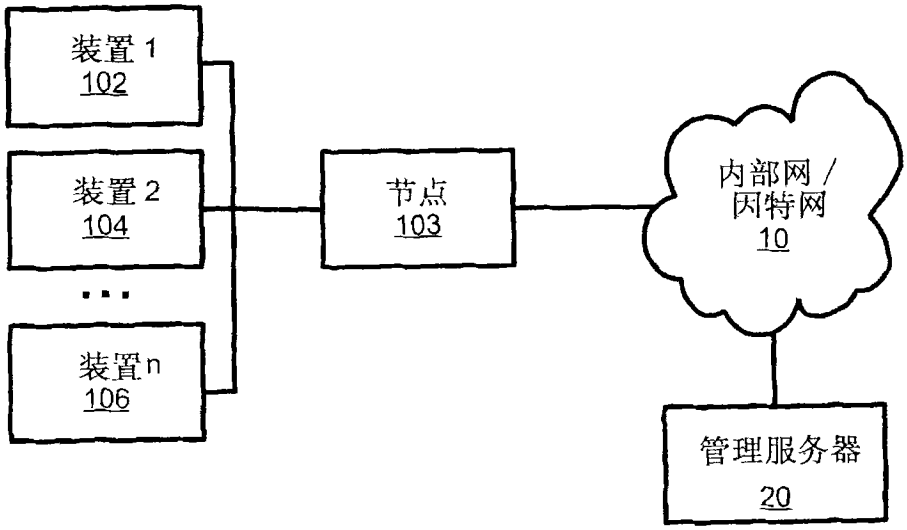

装置 1
102
装置 2
104
装置n
106
节点
103
内部网 / 因特网
10
管理服务器
20

图 4a

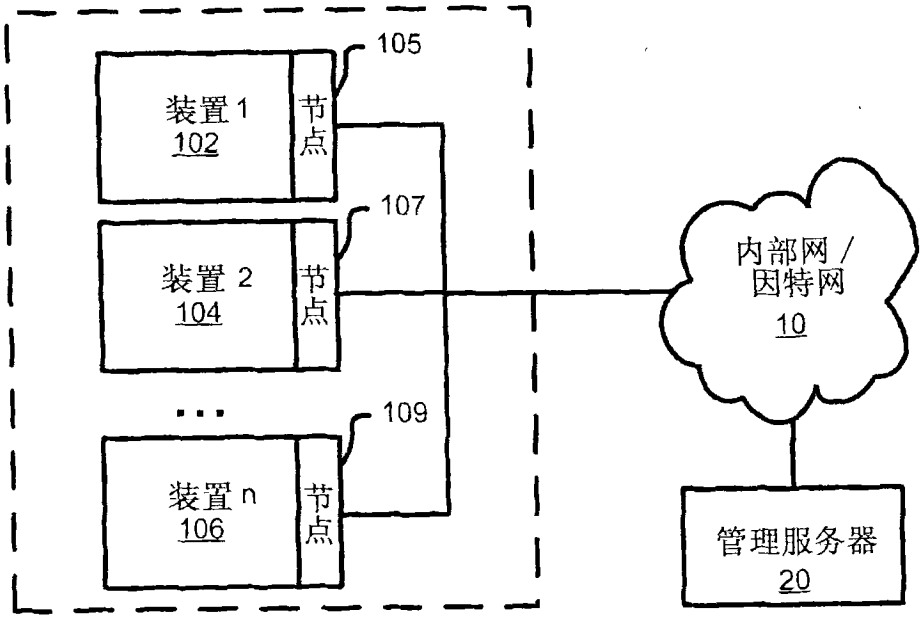

105
装置 1
102
节点
107
装置 2
104
节点
109
装置 n
106
节点
内部网 / 因特网
10
管理服务器
20

图 4b

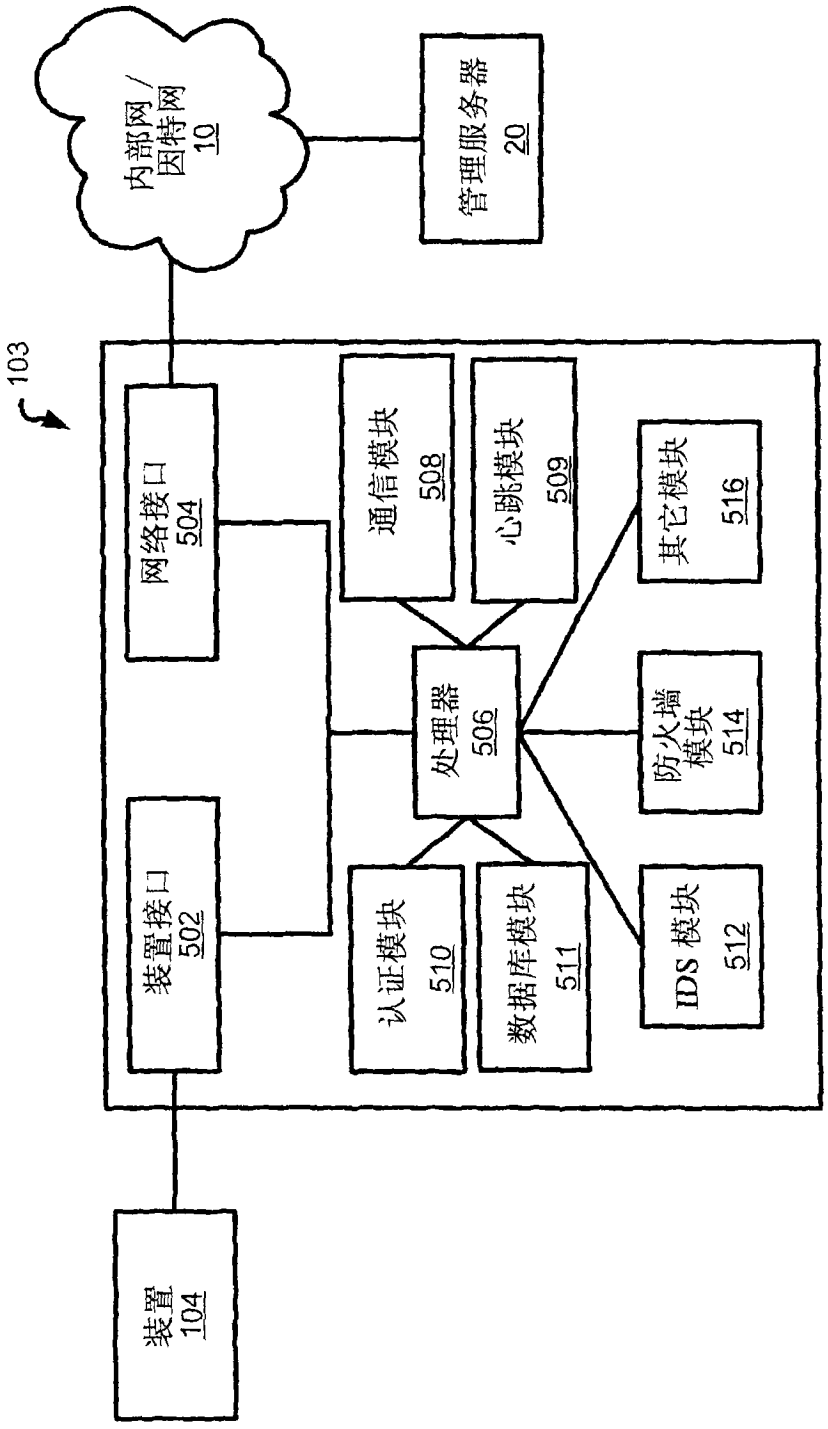

内部网/因特网 10
管理服务器 20
103
网络接口 504
通信模块 508
心跳模块 509
其它模块 516
处理器 506
防火墙模块 514
装置接口 502
认证模块 510
数据库模块 511
IDS 模块 512
装置 104

图 5

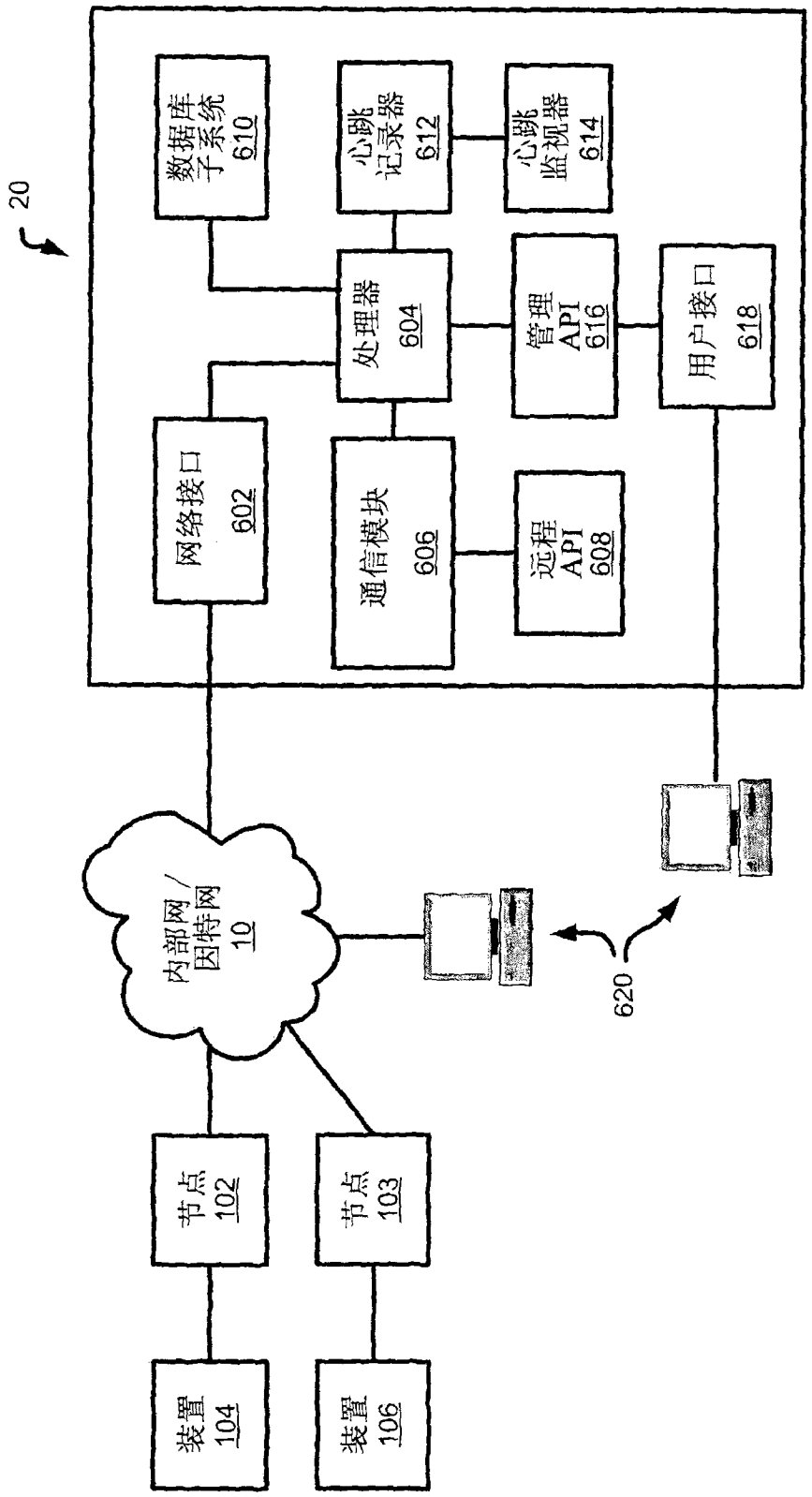

20
数据库子系统 610
心跳记录器 612
心跳监视器 614
处理器 604
管理 API 616
用户接口 618
网络接口 602
通信模块 606
远程 API 608
内部网 / 因特网 10
620
节点 102
节点 103
装置 104
装置 106

图 6

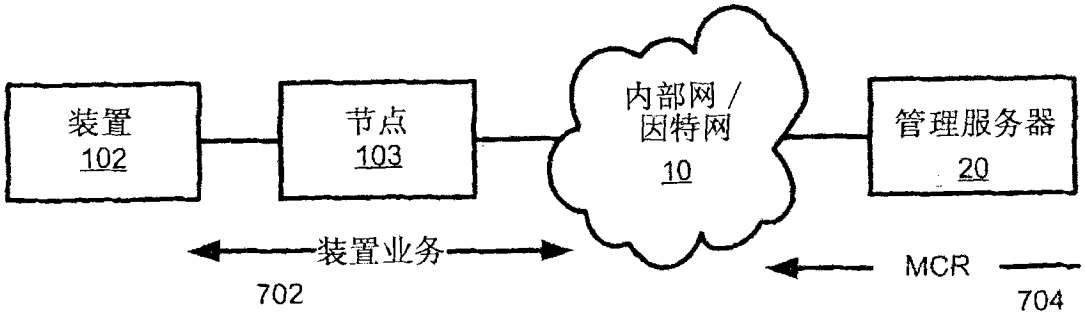

装置
102
节点
103
内部网 /
因特网
10
管理服务器
20
装置业务
702
MCR
704

图 7

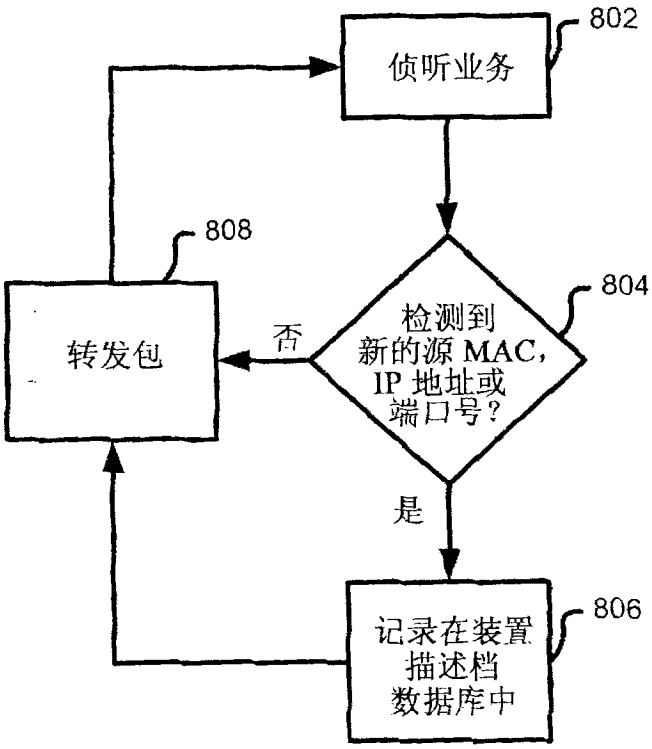

侦听业务
802
检测到
新的源 MAC,
IP 地址或
端口号?
804
否
是
转发包
808
记录在装置
描述档
数据库中
806

图 8

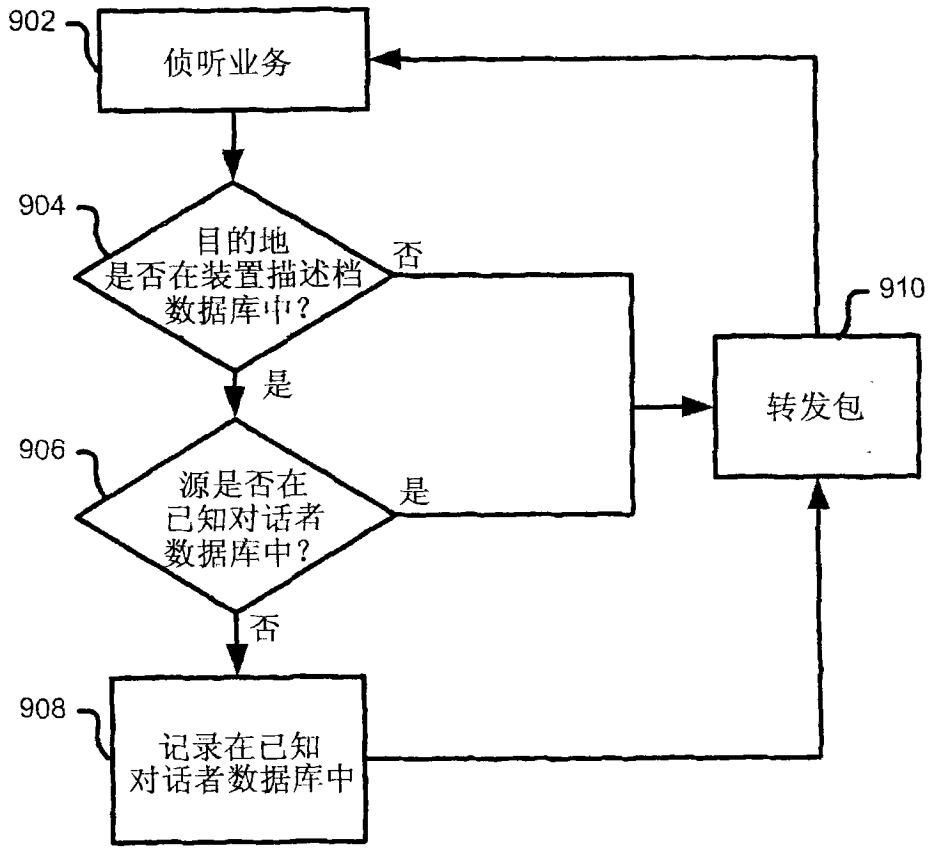

902
侦听业务
904
目的地
是否在装置描述档
数据库中?
否
是
906
源是否在
已知对话者
数据库中?
是
否
908
记录在已知
对话者数据库中
910
转发包

图 9

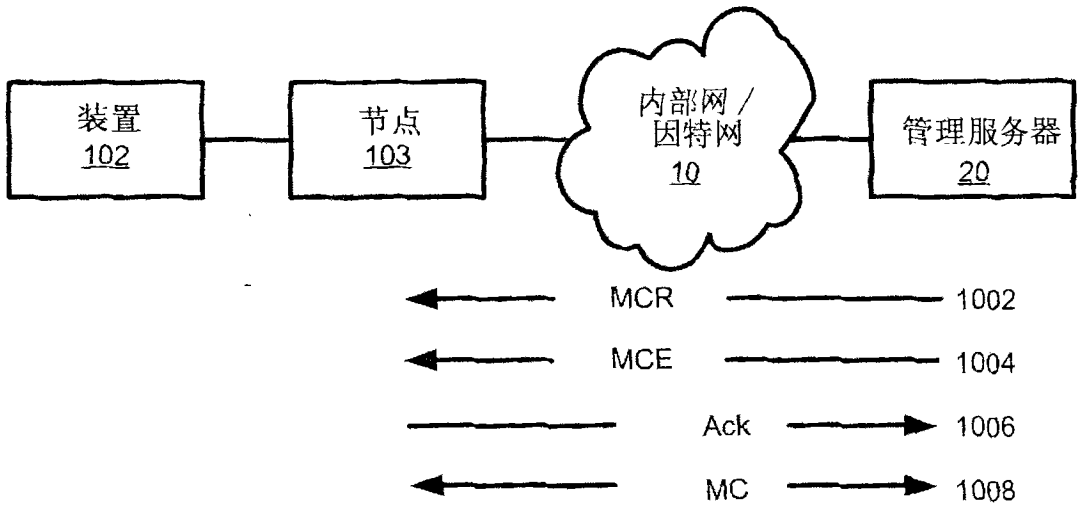

装置
102
节点
103
内部网 /
因特网
10
管理服务器
20
MCR
1002
MCE
1004
Ack
1006
MC
1008

图 10

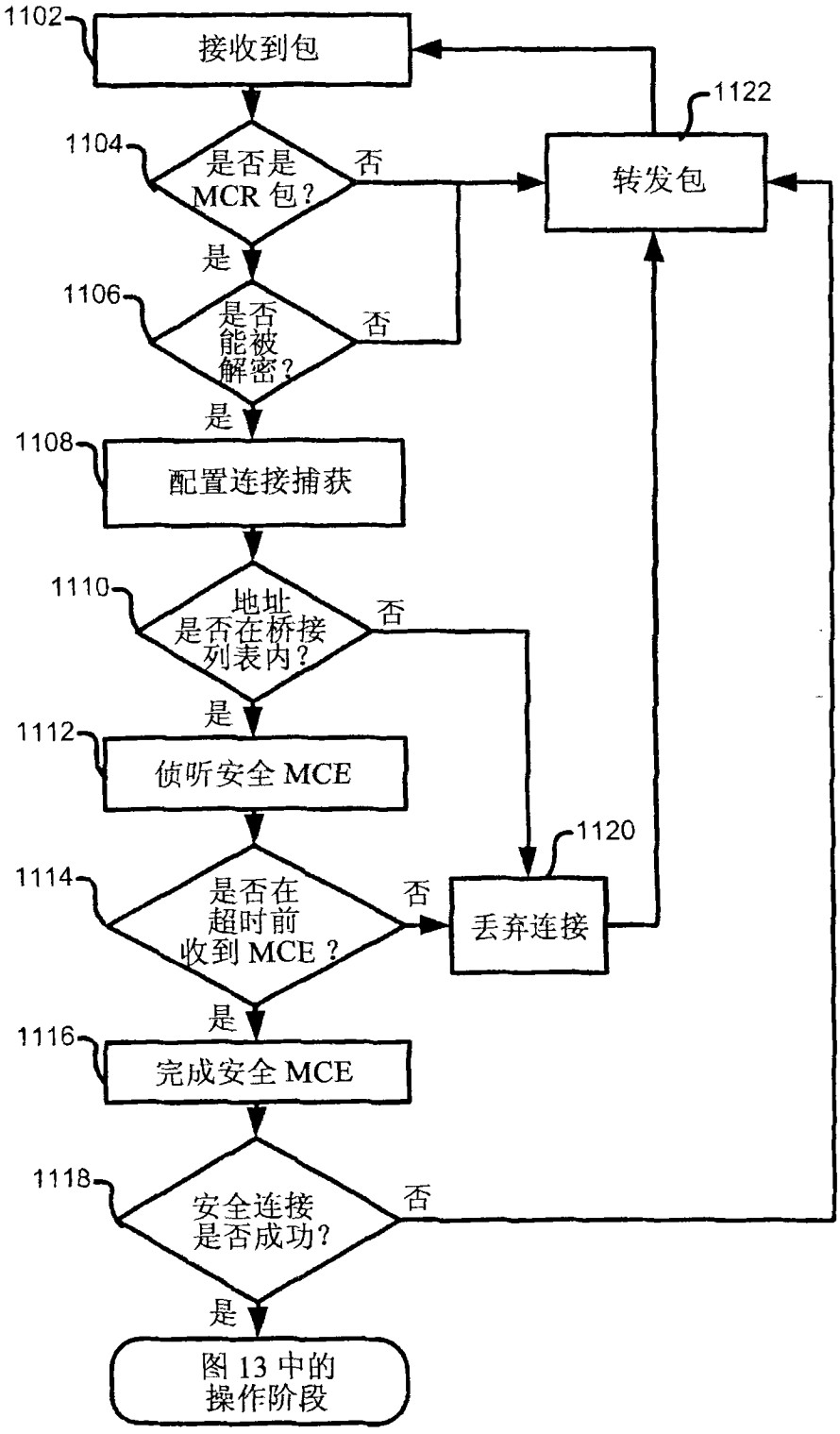

1102
接收到包
1104
是否是 MCR 包?
否
是
1106
是否能被解密?
否
是
1108
配置连接捕获
1110
地址是否在桥接列表内?
否
是
1112
侦听安全 MCE
1114
是否在超时前收到 MCE ?
否
是
1116
完成安全 MCE
1118
安全连接是否成功?
否
是
图 13 中的操作阶段
1120
丢弃连接
1122
转发包

图 11

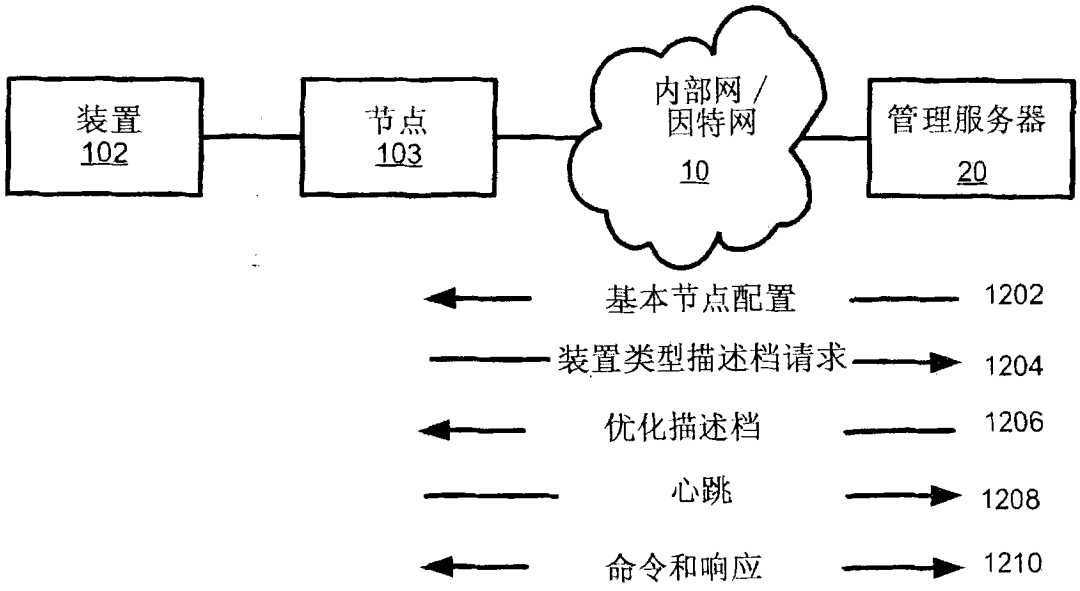

装置
102
节点
103
内部网 /
因特网
10
管理服务器
20
基本节点配置
1202
装置类型描述档请求
1204
优化描述档
1206
心跳
1208
命令和响应
1210

图 12

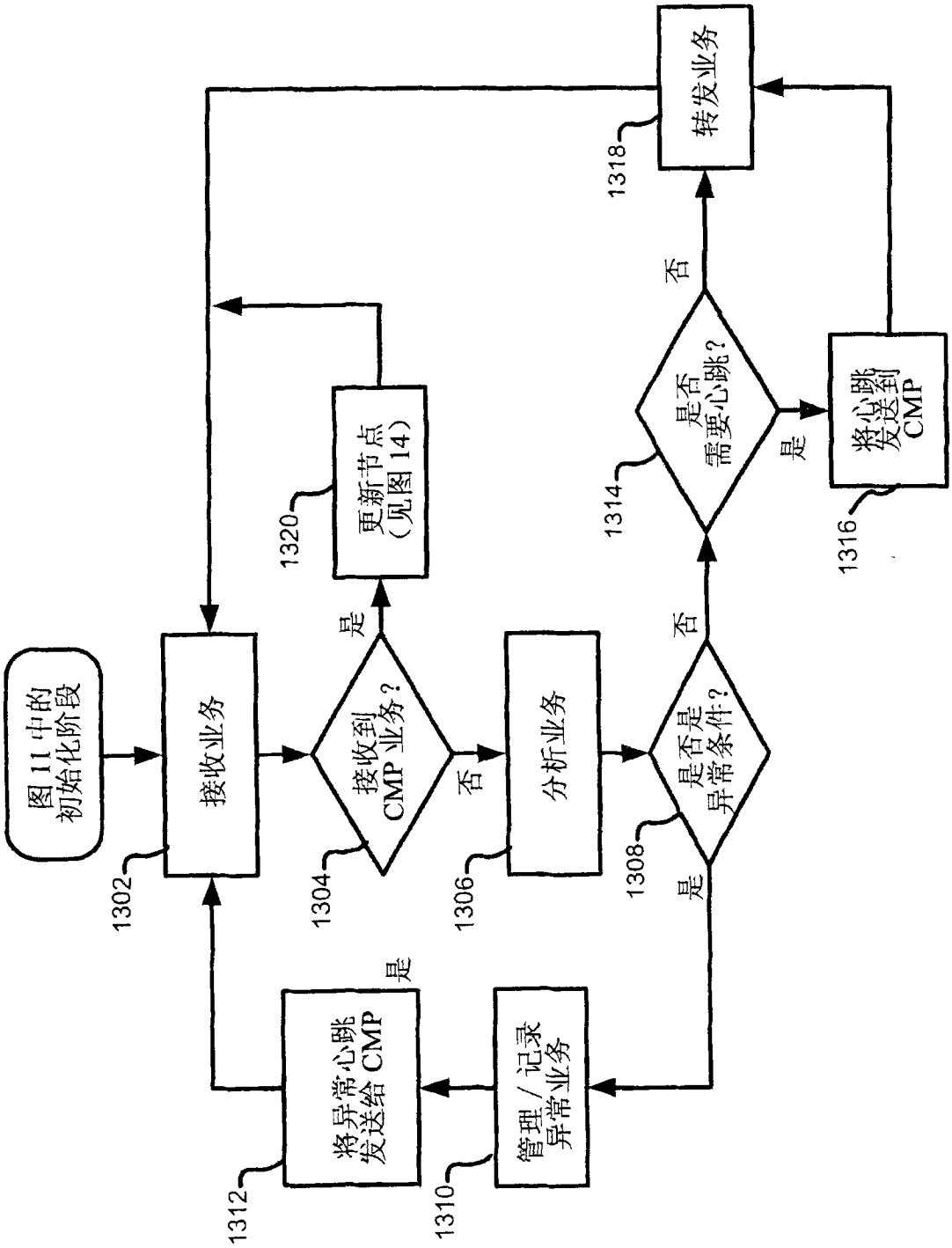


图 11 中的初始化阶段
接收业务
1302
接收到 CMP 业务？
1304
是
更新节点（见图 14）
1320
否
分析业务
1306
是否是异常条件？
1308
否
是否需要心跳？
1314
是
将心跳发送到 CMP
1316
否
转发业务
1318
是
管理 / 记录异常业务
1310
是
将异常心跳发送给 CMP
1312

图 13

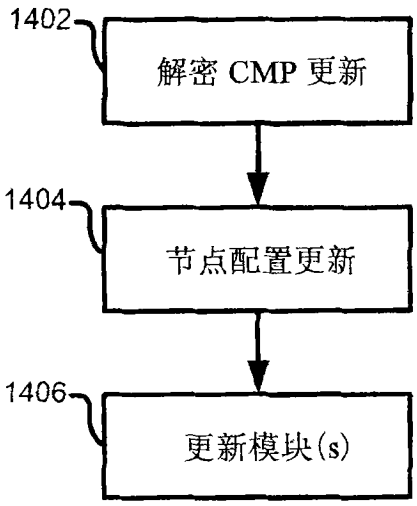


图 14

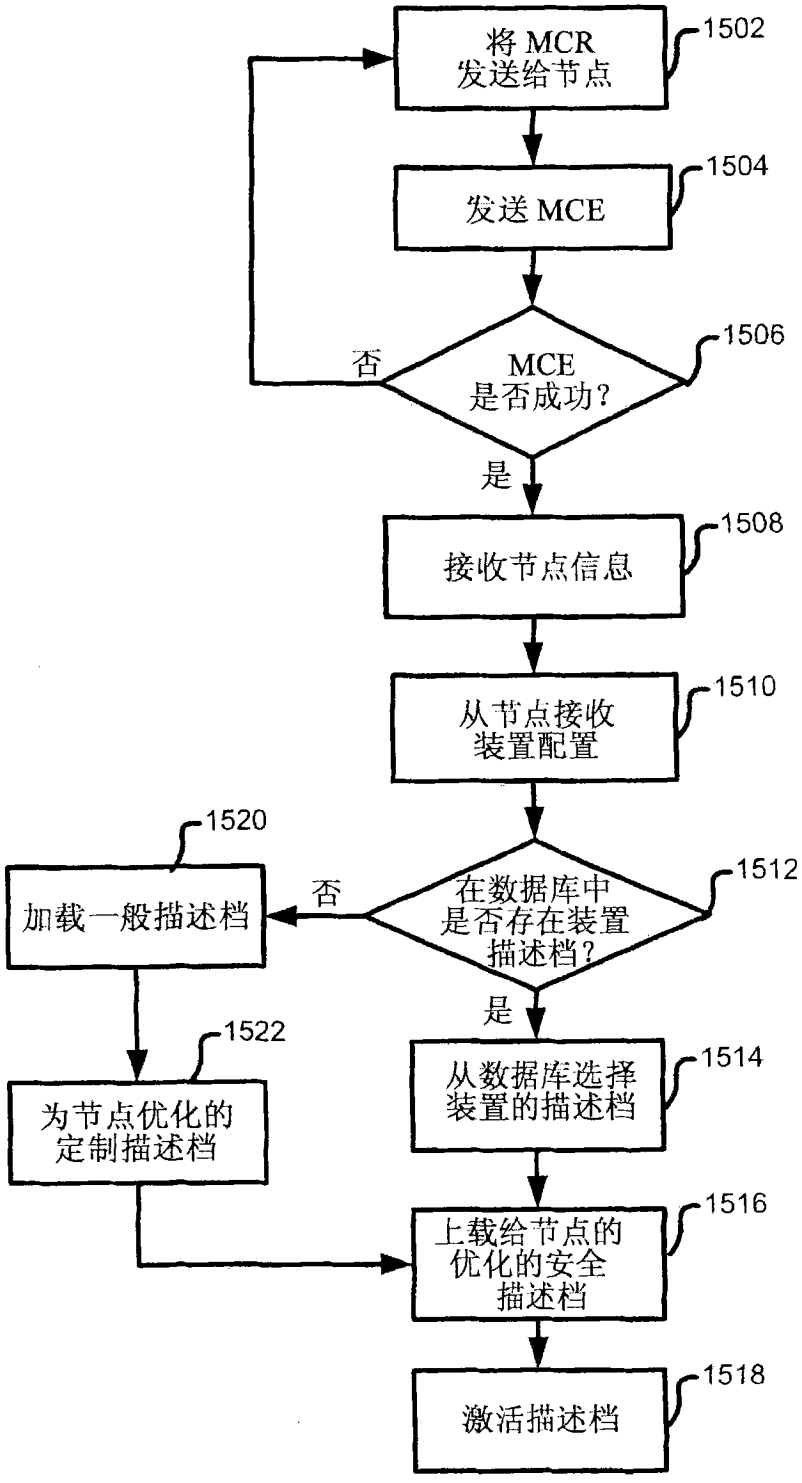

将 MCR 发送给节点
1502
发送 MCE
1504
MCE 是否成功?
1506
否
是
接收节点信息
1508
从节点接收装置配置
1510
在数据库中是否存在装置描述档?
1512
否
是
加载一般描述档
1520
为节点优化的定制描述档
1522
从数据库选择装置的描述档
1514
上载给节点的优化的安全描述档
1516
激活描述档
1518

图 15

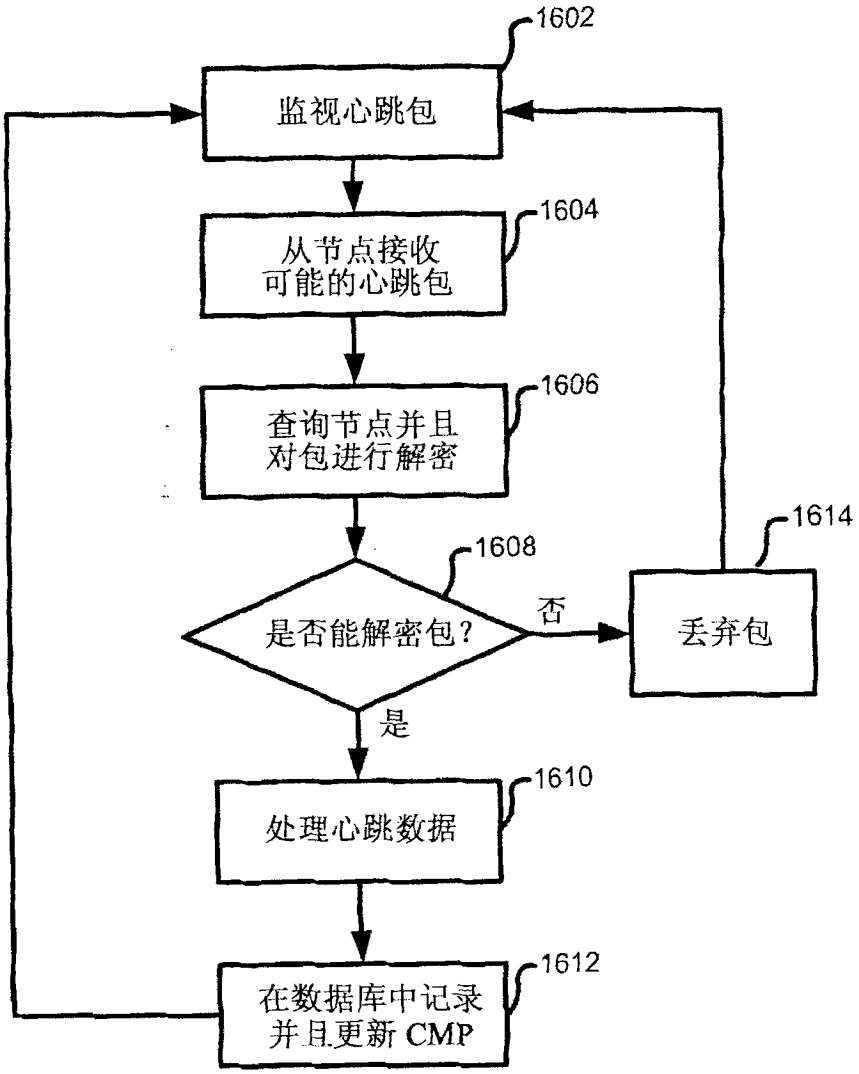

1602
监视心跳包
1604
从节点接收
可能的心跳包
1606
查询节点并且
对包进行解密
1608
是否能解密包?
否
1614
丢弃包
是
1610
处理心跳数据
1612
在数据库中记录
并且更新 CMP

图 16