(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 103891202 B
(45)授权公告日 2017.07.28

(21)申请号 201280051143.4
(22)申请日 2012.10.24
(65)同一申请的已公布的文献号
申请公布号 CN 103891202 A
(43)申请公布日 2014.06.25
(30)优先权数据
61/552,158 2011.10.27 US
(85)PCT国际申请进入国家阶段日
2014.04.17
(86)PCT国际申请的申请数据
PCT/US2012/061645 2012.10.24
(87)PCT国际申请的公布数据
WO2013/063083 EN 2013.05.02
(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部
专利权人 中兴通讯(美国)公司
(72)发明人 布米普·哈斯纳比西
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 蒋黎丽 郑霞
(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101291293 A,2008.10.22,
US 2007086433 A1,2007.04.19,
CN 1859418 A,2006.11.08,
Marc Suñé.Deliverable 5.1 1st Version of the OFELIA Management Software.《OFELIA Deliverable 5.1》.2011,11-12,27,38-41,60.
Rob Sherwood等.FlowVisor: A Network Virtualization Layer.《OpenFlow》.2009,第3部分.
审查员 马兴婕

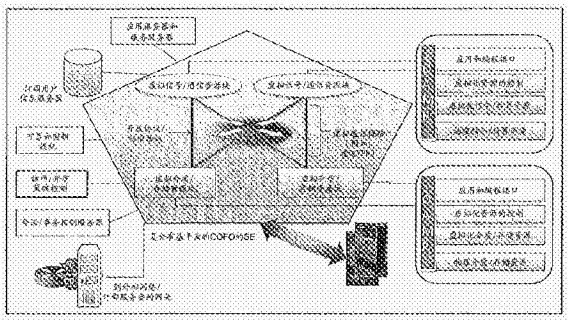
权利要求书2页 说明书4页 附图3页

(54)发明名称

用于经由显式(或虚拟化)机器到机器(M2M)网关元件的基于云的服务元件的集中过载控制(COFO-SE)的实现的系统和方法

(57)摘要

公开了一种用于基于云的服务元件的集中过载控制实现的系统和方法。从多种联网资源获得针对服务元件的信令部分的资源块。服务元件的信令部分经由指令通过虚拟专用网链路控制来自服务元件的介质部分的资源的分配。从多种联网资源获得针对服务元件的介质部分的资源块,其中,资源块被集成到池中并且统一视图被呈现给服务元件的信令部分。服务元件的介质部分在特定(例如,会话或事务长度)持续时间期间使用针对应用和服务的资源块,并且在成功使用之后释放额外的借入资源。



CN 103891202 B

1.一种用于经由显式或虚拟化机器到机器M2M网关元件的基于云的服务元件的集中过载控制COFO-SE的实现的方法，包括：

从多种联网资源获得针对服务元件的信令部分的资源块，其中，所述针对服务元件的信令部分的资源块被集成到池中并且统一视图被呈现给正在与服务元件的信令部分通信的应用和服务；

由所述服务元件的信令部分经由指令通过虚拟专有网链路来控制来自所述服务元件的介质部分的资源的分配；

从所述多种联网资源获得针对所述服务元件的介质部分的资源块，其中，所述针对所述服务元件的介质部分的资源块被集成到池中并且统一视图被呈现给所述服务元件的信令部分；

在持续时间期间针对应用和服务使用所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块；以及

在使用之后释放所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块；

其中，所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块是通过开放应用编程接口和资源编程接口从公共网络、专有网络或社区网络获得的。

2.根据权利要求1所述的方法，其中，所述服务元件是逻辑上/物理上分布式的且是非集成的。

3.根据权利要求1所述的方法，其中，所述虚拟专有网链路运行开放的标准协议。

4.一种用于经由显式或虚拟化机器到机器M2M网关元件的基于云的服务元件的集中过载控制COFO-SE的实现的装置，包括：

服务元件的信令部分，其包括来自多种联网资源的针对服务元件的信令部分的资源块，其中，所述针对服务元件的信令部分的资源块被集成到池中并且统一视图被呈现给正在与服务元件的信令部分通信的应用和服务；

所述服务元件的介质部分，其包括来自所述多种联网资源的针对所述服务元件的介质部分的资源块，其中，所述针对所述服务元件的介质部分的资源块被集成到池中并且统一视图被呈现给所述服务元件的信令部分，

其中，所述服务元件的信令部分还被配置为经由指令通过虚拟专有网链路来控制来自所述服务元件的介质部分的资源的分配；

其中，用于应用和服务的所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块被配置为在持续时间期间使用；以及

在使用之后被释放；

其中，所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块通过开放应用编程接口和资源编程接口来自公共网络、专有网络或社区网络。

5.根据权利要求4所述的装置，其中，所述服务元件是分布式的且是非集成的。

6.根据权利要求4所述的装置，其中，所述虚拟专有网链路运行开放的标准协议。

7.一种用于经由显式或虚拟化机器到机器M2M网关元件的基于云的服务元件的集中过载控制COFO-SE的实现的系统，包括：

用于从多种联网资源获得针对服务元件的信令部分的资源块的工具，其中，所述针对

服务元件的信令部分的资源块被集成到池中并且统一视图被呈现给正在与服务元件的信令部分通信的应用和服务；

用于控制来自所述服务元件的介质部分的资源的分配的工具；

用于从所述多种联网资源获得针对所述服务元件的介质部分的资源块的工具，其中，所述针对所述服务元件的介质部分的资源块被集成到池中并且统一视图被呈现给所述服务元件的信令部分；以及

用于在持续时间期间针对应用和服务使用所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块的工具；

其中，所述针对服务元件的信令部分的资源块和针对所述服务元件的介质部分的资源块是通过开放应用编程接口和资源编程接口从公共网络、专有网络或社区网络获得的。

8.根据权利要求7所述的系统，其中，所述服务元件是分布式的且是非集成的。

9.根据权利要求7所述的系统，其中，虚拟专有网链路运行开放的标准协议。

用于经由显式(或虚拟化)机器到机器(M2M)网关元件的基于云的服务元件的集中过载控制(COFO-SE)的实现的系统和方法

技术领域

[0001] 本发明的领域涉及基于云的系统,更具体地,涉及使用分布式虚拟资源的服务元件的集中过载控制。

背景技术

[0002] 在通信网络中,当联网服务元件不具有足够的资源(例如,CPU处理能力、存储器、网络带宽、输入/输出、磁盘资源等)来成功地处理它所接收的所有请求时会发生过载。一些联网服务元件可能由于高速率的输入服务请求和/或部分网络不可用而经历持久的过载,从而导致故障。服务元件包括但不限于语音邮件服务器、即时消息传送(IM)服务器、呈现服务器、位置服务器、地址簿服务器、订阅用户简档服务器、自助服务亭、监视触发/输入聚集器、移动设备发起的业务聚集器或网关、策略服务器、保护和安全性服务管理器等。集中过载是网络过载的特殊情况,在该情况下,过载集中在服务元件上。该子集的范围可以从网络目的地(例如,电话号码或IP地址)到一组交换和网络服务器。

[0003] 在不存在过载控制的情况下,这种过载可能威胁到通信网络的稳定性,并且可能引起服务请求的成功完成的显著下降。最终,服务元件可能由于丢失的请求而不能提供服务,这导致客户不能得到服务。通常,过载问题可能自我混合,这可能对服务元件造成甚至更持久的负载。此外,在过载期间,服务器的总能力可能显著下降,这是因为其大部分资源花费在拒绝和/或处理它们实际上不能处理的负载上。在严重的过载情况下,吞吐量可能下降至最初处理能力的一小部分。这通常被称作拥塞崩溃。此外,过载条件往往造成服务请求延迟和/或丢失,这可能触发更高速率的客户放弃和/或重试。

[0004] 通常以两种不同的方式来控制集中过载。一种方式是通过拒绝服务来减小输入负载。例如,只允许较高优先级的会话或事务,并且可以拒绝所有其他会话或事务。不幸的是,该方法可能引起客户失望并且最终流失,从而导致收入损失。

[0005] 另一种控制集中过载的方式是将输入的会话或事务请求路由到本地备用服务元件,该本地备用服务元件通常是由拥有需要控制其过载的服务元件的相同组织拥有和运营的。然而,这可能需要大幅提高的资金和运营开销,这是因为不能准确地预测过载事件的发生和持续时间。此外,利用基于本地基础设施元件的服务元件过载控制实现的某些缺点包括:

[0006] a)成本;

[0007] b)用于测试过载服务元件并且将过载服务元件与网络集成在一起所需的时间;

[0008] c)静态资源分配;

[0009] d)重新布置资源的灵活性变低;计算和通信资源的耦合更严格,这些计算和通信资源具有包括服务(通常由正受保护以避免过载的服务元件提供)的预先设计的特征和功能;以及

[0010] e)系统升级和改进的机会减少。

[0011] 处于动态和不断发展的联网和服务开发环境中的服务提供商需要：

[0012] a)投资保护，即，对可以快速地重新布置或重新目的化以用于不同的创收应用和服务的资源的投资；和/或

[0013] b)机动性和灵活性，即，利用网络中已经存在的计算和通信资源来部署即将出现的特征和功能。

[0014] 因此，需要使网络运营商和服务提供商能够基于预期的设计限制来分配其用于计算、通信和控制基础设施开发的预算的系统。因此，将不需要创建和安装计算和联网设备库以控制服务元件的集中过载。

发明内容

[0015] 本发明的各个方面解决了这些问题，并且例如使服务提供商能够分配其用于计算、通信和控制基础设施开发而不是用于创建和安装这些计算和联网设备库的预算，其中，所述计算和联网设备库通常未充分使用或者在达到充分发挥(或者给投资提供充分回报)之前已经过时。

[0016] 在一个方面，提供了一种方法，包括：从多种联网资源获得针对服务元件的信令部分的资源块，其中，所述资源块被集成到池中并且统一视图被呈现给正在与服务元件的信令部分通信的应用和服务。所述服务元件的信令部分经由指令通过虚拟专有网链路来控制来自所述服务元件的介质部分的资源的分配。从多种联网资源获得针对所述服务元件的介质部分的资源块，其中，所述资源块被集成到池中并且统一视图被呈现给所述服务元件的信令部分。所述服务元件的介质部分在持续时间期间针对应用和服务使用所述资源块。所述持续时间的范围可以从几秒到几十或者几百小时。可以通过开放应用编程接口和资源编程接口(API和RPI)从公共网络、专有网络或社区网络获得资源块。

附图说明

[0017] 图1示出了服务元件的集中过载的控制(“COFO-SE”)实现(服务元件的集中过载的控制(COFO-SE)的传统实现——使用一对一的备用元件——[未示出一对多的备用元件])的当前模型的框图

[0018] 图2给出了基于云的COFO-SE的高层实现模型。

[0019] 图3示出了基于云的COFO-SE实现的详细框图。

[0020] 图4示出了用于COFO-SE聚集来自内部和/或外部资源(例如，专有云、公共云)的资源的步骤的流程图。

具体实施方式

[0021] 在传统的单独的或基于基础设施元件的COFO-SE的保护实现中，可能需要专用计算资源、存储资源和通信资源。这些资源需要与服务和网络基础设施集成在一起并且根据业务管理和隐私/认证/安全性管理两个方面需要以协调的方式操作。

[0022] 因此，为了使这些额外的元件服务准备好以支持灾害管理和过载控制特征/功能所需的时间，以及用于成功地实现期望的结果的成本变得相当高。例如，需要分配和集成额

外的交换/路由、控制/处理和保护资源以支持期望的过载控制特征/功能。

[0023] 根据本发明的某些方面，COFO-SE实现克服了传统的单独过载控制实现的上述缺点，这是因为无需预先分配单独的或者在基础设施服务元件中的本地计算资源、存储资源和通信资源以用于控制过载的目的。相反，通过例如资源代理或交换公司经由开放应用编程接口和资源编程接口(API和RPI)从公共网络、专有网络或社区网络获得资源。

[0024] API/RPI可以使用以下各项中的任意一项或多项：SOAP、XML、WSDL、Parlay/Parlay-X、HTTP、CORBA等。API/RPI设计和分析的细节超出了本专利申请的范围。应当注意的是，这些API/RPI不仅简化了对期望的资源的访问，而且还确保与现有网络/基础设施和安全性、可用性、服务连续性机制等的快速集成和互操作性。这是由于这样的事实，即，通过经由开放API/RPI浏览可用联网资源并且获取这些可用联网资源来获得期望的过载控制特征/功能，使得可以在会话/服务的持续时间期间按照应用和服务的需求使用这些资源。例如，防火墙和加密密钥资源的实时可用性对于在语音通信会话的持续时间期间通过公共互联网进行的实时企业安全语音通信服务是有用的。可以使用本发明的实施例来处理该FAAS(防火墙即服务)的合法过载。

[0025] 总的来说，需要利用过载控制特征/功能的任何应用或服务可以通过开放API/RPI从网络(例外，互联网)获得这些资源，然后可以在具有保证的可用性、安全性和可靠性的情况下在会话的持续时间期间使用这些资源。在其他方面，本发明提供了具有与上文所讨论的内容相对应的特征和优点的系统和计算机程序。

[0026] 图1示出了当前COFO-SE实现的框图。正在保护的服务元件直接连接到应用服务器、会话控制元件、服务网关等。服务元件接收到针对订阅用户和用户的身份验证的请求以认证对基于事务或会话的服务(例如，ID验证、语音邮件、IM、位置、呈现等)的访问。该服务元件可以使用预定的多个属性(例如，服务名称和位置)、凭证(例如，密码或生物识别信息)、以及标识符(名字、userId、MACId、IP地址、地理位置等)。一旦用户/订阅用户已经被认证，服务元件就可能控制或可能不能控制针对会话和介质的资源。策略、服务质量和安全性需求也可能指示这些分配。SE的信令元件与SE的介质控制元件之间的接口可以是开放协议(标准协议)或者专有协议，并且接口可以是点对点的或点对多点的，以通过分发资源请求来支持可靠性。

[0027] 可以在通过引用的方式完整地并入的http://tools.ietf.org/id/draft-khasnabish-cloud-reference-framework-01.txt处找到云框架参考模型的细节。

[0028] 图2示出了根据本发明的方面的COFO-SE实现模型。在该实现中，从一组联网资源获得构成服务元件的信令部分和介质控制部分的额外资源(用于防止过载保护或用于灾害管理)，并且这些额外资源在它们被需要的持续时间期间被使用，然后被释放回资源池。该持续时间可以从几秒至很多小时不等。

[0029] 可以从多种联网资源获得用于管理信令过载控制的资源块，并且这些块可以集成到服务元件资源池中，使得统一视图可以呈现给正在与受保护的防止过载/灾害的服务元件的信令部分进行通信的应用和服务——订阅用户信息/简档服务器、可靠和密钥授权、访问/介质策略控制、会话/事务控制服务器。服务元件的信令部分使用指令通过运行具有标准化配置的开放协议的虚拟专用网链路来控制来自服务元件的会话和介质控制部分的资源的分配。

[0030] 用于控制服务元件的介质部分的资源是从一组联网资源获得的并且在要求的持续时间期间被使用。该持续时间可以从几分钟至很多小时不等。针对服务元件的介质部分的资源块可以从多种联网资源获得并且这些块可以集成到介质控制部分的资源池中，使得统一视图可以被呈现给服务元件的信令部分。

[0031] 图3示出了如何使用固定(内部)资源和借入或租用(外部)资源的组合来以成本有效的方式控制服务元件上的集中过载的另外的细节。

[0032] 图4示出了用于COFO-SE聚集来自内部资源和/或外部资源(例如，专有云、公共云)的资源的步骤的流程图。通过考虑历史趋势并且监控当前资源和需求，规划在接下来几个时间段期间的需求。接下来，确定内部资源的可用性。如果有足够的内部资源可用，则已经实现了针对额外资源的请求。如果内部资源不可用，则针对来自专有云或公共云的资源发出请求。

[0033] 应当理解的是，采用包括简单和复杂计算机的机器和装置来实现本发明的方法和系统。此外，上文所描述的架构和方法可以部分地或完全地存储在各种形式的机器可读介质上。例如，本发明的操作可以存储在可以经由磁盘驱动器(或机器可读介质驱动器)访问的机器可读介质(例如，磁盘或光盘)上。可选择地，执行如上文所讨论的操作的逻辑可以实现在额外计算机和/或机器可读介质(例如，诸如大规模集成电路(LSI)、专用集成电路(ASIC)等的分立硬件组件、诸如电可擦除可编程只读存储器(EEPROM)等的固件)等中。特定实施例的实现还可以采用机器实现的(包括网络实现的)计算机软件的形式。

[0034] 虽然已经示出和描述了本发明的各个方面，但是本领域技术人员将清楚的是，可以在不偏离本文所描述的发明构思的情况下进行更多的修改。因此，除了在所附权利要求的精神内的内容之外，本发明不受限制。

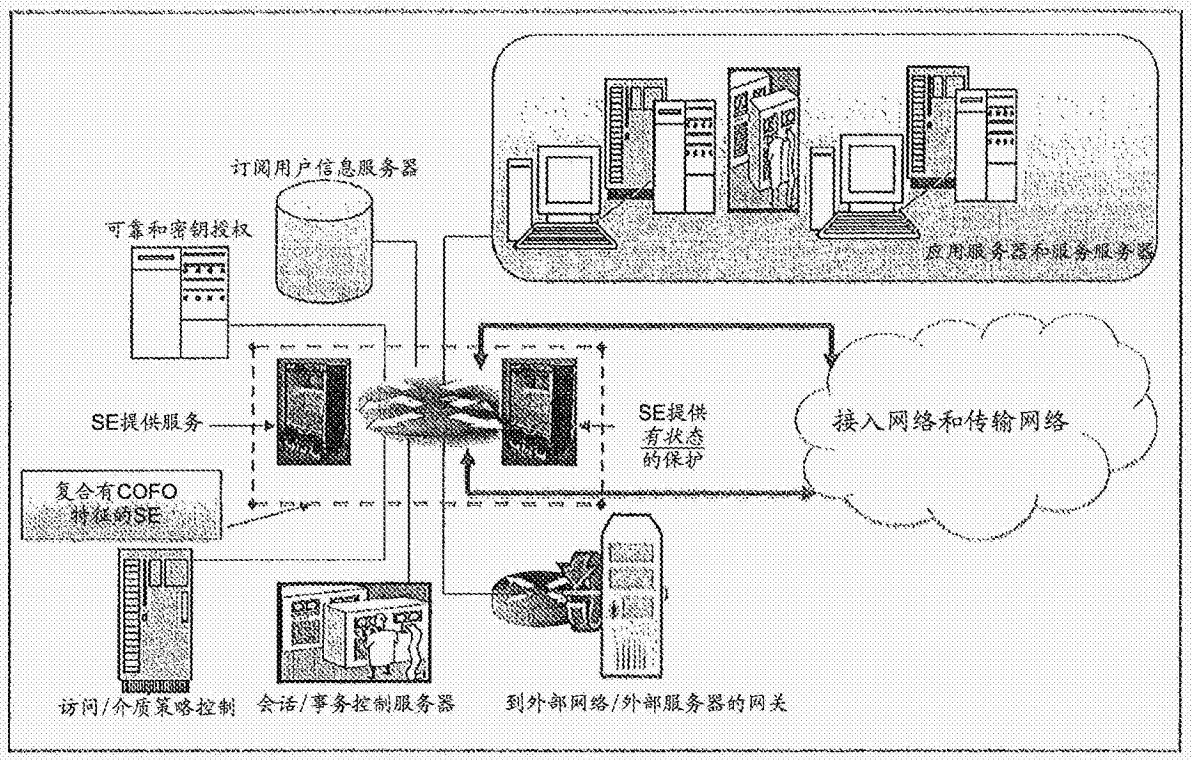

订阅用户信息服务器
可靠和密钥授权
应用服务器和服务服务器
SE提供服务
SE提供
有状态
的保护
接入网络和传输网络
复合有COFO
特征的SE
访问/介质策略控制
会话/事务控制服务器
到外部网络/外部服务器的网关

图1

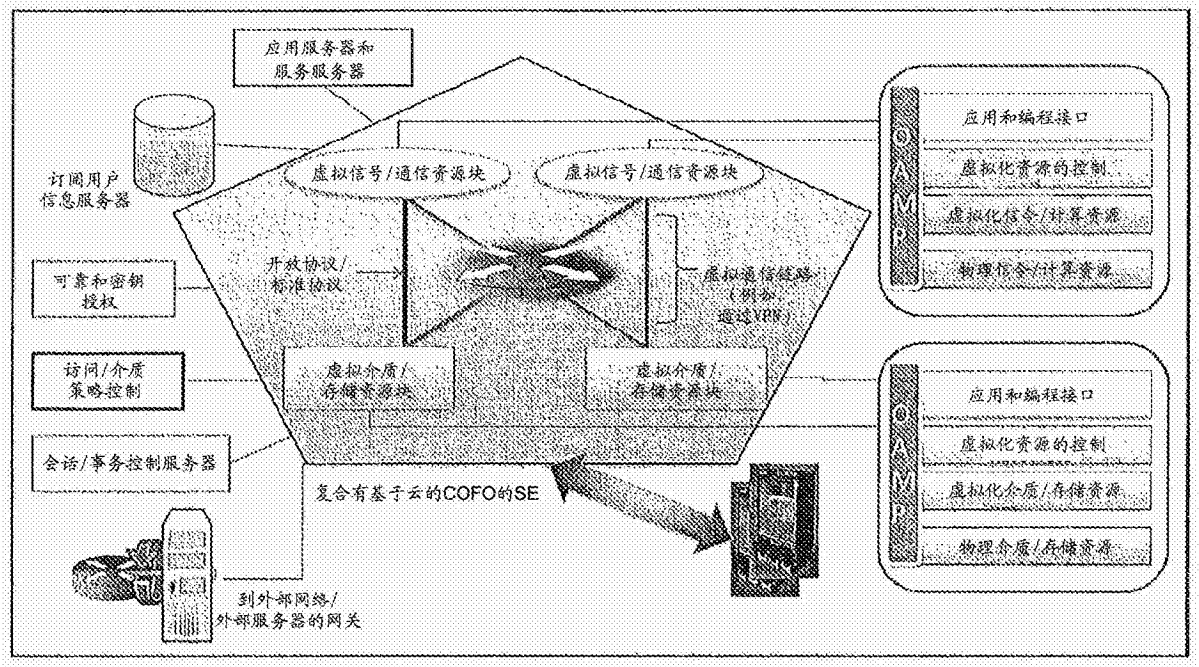

应用服务器和
服务服务器
订阅用户
信息服务器
虚拟信号/通信资源块
虚拟信号/通信资源块
可靠和密钥
授权
开放协议/
标准协议
虚拟通信链路
(例如
通过VPN)
访问/介质
策略控制
虚拟介质/
存储资源块
虚拟介质/
存储资源块
会话/事务控制服务器
复合有基于云的COFO的SE
到外部网络/
外部服务器的网关
OAM&P
应用和编程接口
虚拟化资源的控制
虚拟化信令/计算资源
物理信令/计算资源
OAM&P
应用和编程接口
虚拟化资源的控制
虚拟化介质/存储资源
物理介质/存储资源

图2

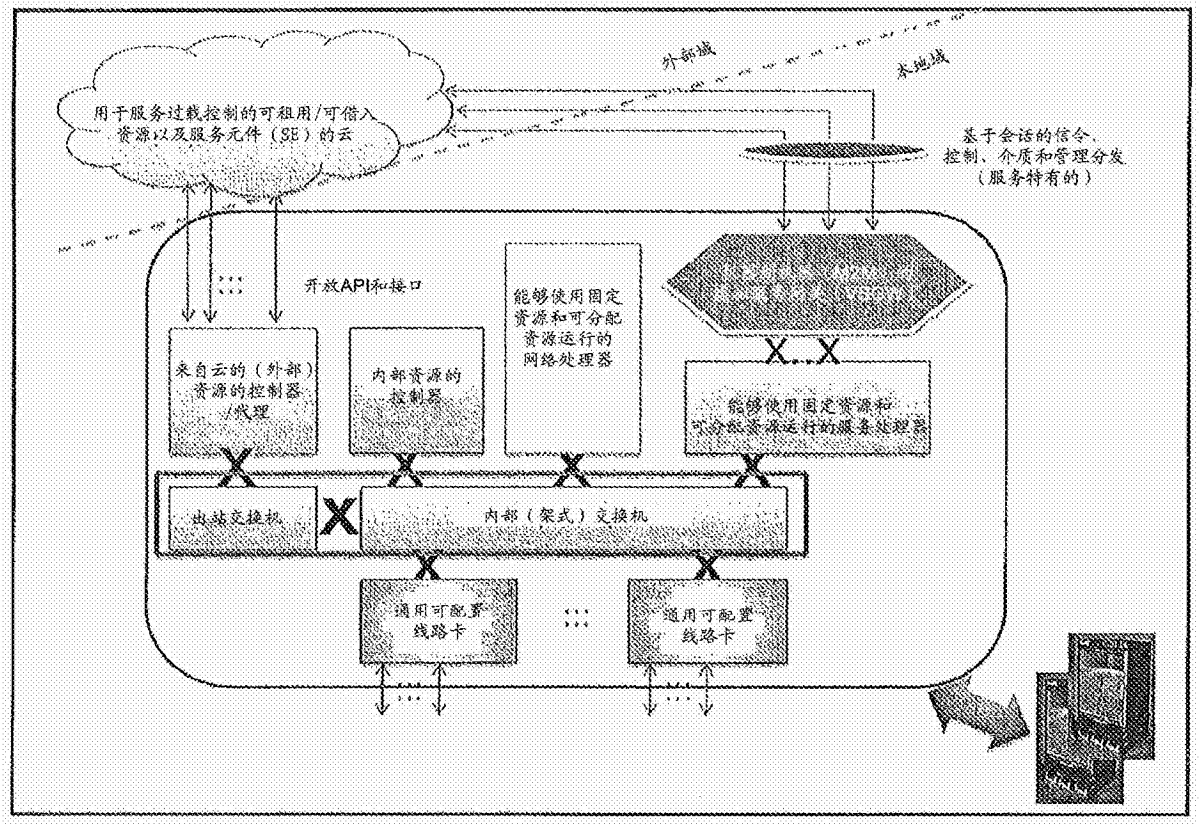

外部域
本地域
用于服务过载控制的可租用/可借入资源以及服务元件（SE）的云
基于会话的信令、控制、介质和管理分发（服务特有的）
开放API和接口
来自云的（外部）资源的控制器/代理
内部资源的控制器
能够使用固定资源和可分配资源运行的网络处理器
能够使用固定资源和可分配资源运行的服务处理器
出站交换机
内部（架式）交换机
通用可配置线路卡
通用可配置线路卡

图3

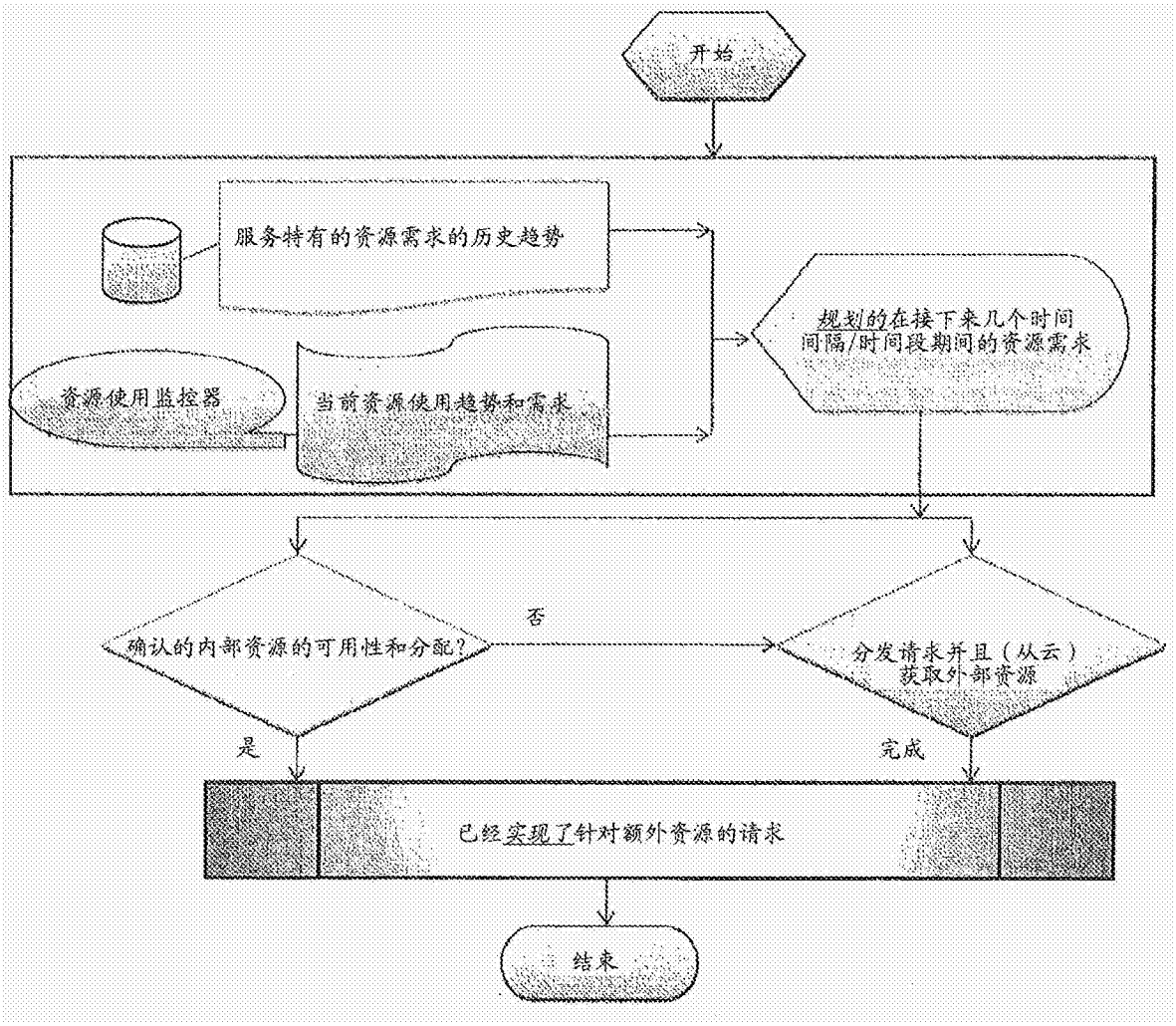

开始
服务特有的资源需求的历史趋势
规划的在接下来几个时间间隔/时间段期间的资源需求
资源使用监控器
当前资源使用趋势和需求
确认的内部资源的可用性和分配?
否
分发请求并且（从云）获取外部资源
是
完成
已经实现了针对额外资源的请求
结束

图4