

网络虚拟化环境中的故障管理现状 调查：面临的挑战与相应的解决方案

Sihem Ch^D
索菲安·伊马达利、埃里克·法布尔、格雷戈尔·格斯勒以及伊门·格里达·本·亚希亚



摘要——5G技术的出现，以及对带宽、延迟和服务质量日益严格的要求，正在挑战传统移动网络运营商现有技术所能实现的极限。网络功能虚拟化技术为解决这些挑战提供了有效途径，该技术已被业界广泛采纳，并得到了标准化组织的规范支持。本质上，网络功能虚拟化意味着将网络功能作为虚拟化 workload 在普通硬件上运行。这一技术有助于降低部署成本并简化网络功能的生命周期管理，但同时也带来了新的故障管理难题。在本文中，我们系统总结了现有的故障管理技术成果，分析了虚拟化技术对故障管理的影响，并对网络虚拟化环境下最新的故障管理研究成果进行了分类，同时指出了这些成果的主要贡献与不足之处。

索引术语——故障管理、网络功能虚拟化、软件定义网络、机器学习。

一、引言

随着5G技术的出现，移动网络运营商开始使用越来越多的专用硬件设备，以及复杂的传统通信协议和架构。这些系统需要逐步过渡到基于软件的架构[1]。新的网络服务需要部署新的硬件服务器，同时还需要对这些服务器进行维护，并在出现故障时及时更换，以确保服务能够正常运行。这一与网络设备生命周期相关的流程成本高昂，且能源利用效率低下。此外，移动网络运营商在ITU-T、ETSI、IETF或NGMN等标准化组织中所花费的时间也被忽视了——这些时间其实用于确保各类专用硬件设备及通信协议符合相关标准。

Manuscript received April 23, 2019; revised August 12, 2019 and October 7, 2019; accepted October 13, 2019. Date of publication October 21, 2019; date of current version December 10, 2019. The associate editor coordinating the review of this article and approving it for publication was S. Schmid. (Corresponding author: Sihem Cherrared.)

S. Cherrared is with the Cloud Infrastructure Solutions and Services, Orange Lab Networks, 92320 Châtillon, France, and also with the Supervision of Large Modular and Distributed Systems, INRIA (Campus de Beaulieu), 35042 Rennes, France (e-mail: sihem.cherrared@gmail.com).

S. Imadali and I. Grida Ben Yahia are with the Cloud Infrastructure Solutions and Services, Orange Lab Networks, 92320 Châtillon, France.

E. Fabre is with the Supervision of Large Modular and Distributed Systems, INRIA (Campus de Beaulieu), 35042 Rennes, France.

G. Gössler is with Univ. Grenoble Alpes, INRIA, CNRS, Grenoble INP, LIG, 38000 Grenoble, France.

Digital Object Identifier 10.1109/TNSM.2019.2948420

然而，作为一个快速发展的行业，电信产业正面临日益激烈 的竞争，因为新的竞争者正凭借新兴的软件技术和开源项目 进入这一领域。其中一个典型的例子是Facebook发起的“电 信基础设施项目”[2]，该项目旨在为新一代移动网络运营商 开发一款开源的通用硬件设备。这种基础设施建设方式与 电信行业传统的做法截然不同，促使移动网络运营商投资并采 用一系列新技术，包括软件定义网络、网络功能虚拟化、云 计算技术以及实时监控系统。

基于软件的创新技术有助于设计未来的5G网络[3]。5GPP旗 下的相关项目，如“新型无线电服务自适应网络架 构”(NORMA) [4]，倡导采用基于API的架构开放性，通过 颠覆性的创新推动经济增长。这些项目提出了对移动网络功 能进行灵活分解与重新分配的方案，即将这些功能部署在最 合适的位置。归根结底，这意味着需要为5G网络设计一种以 服务为导向的架构，而这种架构与长期演进(LTE) 网络的 设计与实现方式相比具有颠覆性。

随着5G技术的软件化发展，移动网络运营商正在寻求新的收 入来源与商业模式。下一代移动通信网络技术提出了打破传 统单一网络基础设施所有权的商业模式，转而采用网络共享 或多租户模式。这种模式有望将无线接入网的相关成本降低 多达35%[6]。

网络虚拟化环境使得多租户SDN与NFV架构能够在同一基础 设施中共存，且不会影响生产服务的正常运行[7]。然而，为 确保这些服务的高可用性与可靠性，移动网络运营商绝对不 能忽视对网络虚拟化环境的管理。相关管理措施可归纳为五 个方面：故障管理、配置管理、计费管理、性能管理以及 安全管理。网络虚拟化环境的出现带来了新的挑战，这要求 人们重新审视现有的管理方法，并使其适应这种新的环境。故 障管理是其中最重要的管理环节之一，因为故障可能导致重 大损失，进而影响企业的形象与信誉。2013年，IBM就发生 过一起典型的云服务故障事件，造成的经济损失估计达3100 万澳大利亚元。

在圣诞节期间，IBM服务器发生故障，导致一家澳大利亚大型零售商的网站整整一周都无法正常访问[8]。NVE的灵活性为网络监控带来了全新的方法。在构建5G网络架构之前，应通过增强网络的弹性及自愈能力来进行相关监管工作，同时充分利用NVE的动态性与可重复性来实现这些功能。然而，尽管网络监控是一个早已被广泛研究的领域，且已有许多成熟的技术被应用，其中通常涉及简单网络管理协议(SNMP)以及Nagios等软件工具[9]，但虚拟网络的出现带来了新的挑战与问题，这些挑战与问题改变了故障管理的实施方式。

在本文中，我们探讨了虚拟化对传统故障管理技术的影响。我们的工作主要旨在补充现有研究中提到的各种调查结果。简而言之，我们的主要贡献可归纳如下：

- 我们全面总结了现有的先进故障管理技术，以及网络故障管理虚拟化技术所带来的影响。同时，我们展示了在NVE故障管理领域取得的最新研究成果及实际应用案例。
- 我们提出了一种新的分类方法，用于梳理当前各类解决故障定位问题的技术手段，并对比了这些技术的主要优势与不足之处。

本文的其余部分安排如下：第二节探讨了现有关于NVE管理的调研文献，并明确了本次调研的范围；第三节介绍了NVE的相关概念以及故障管理的相关步骤与方法；第四节分析了NVE领域存在的问题；第五节提出了针对NVE故障管理的新方法与创新举措；第六节对各种管理方法进行了分类，并阐述了在不同应用场景下如何最佳地运用这些方法；第七节对全文进行了总结。

二、相关研究工作

最近的调查论文探讨了虚拟网络中的故障管理技术，但在研究的虚拟环境类型及管理方面存在差异。Esteves等人[7]全面总结了当前在虚拟网络管理领域取得的进展。该论文首先提出了一个用于描述虚拟网络中各类实体、它们之间的关系以及相关管理操作的概念性管理模型，随后回顾了若干代表性项目，指出了这些项目的主要特点、优势与局限性，并从管理目标、管理功能和管理方法三个不同角度对它们进行了分类。而论文[10]–[14]则聚焦于软件定义网络的管理技术。Fonseca与Mota[10]研究了软件定义网络各层（即基础设施层、控制层和应用层）中可能出现的故障问题，分析了这些故障的潜在来源，包括来自各层本身的问题，以及层与层之间的交互所带来的故障。Da Silva等人[11]的调研则着重于提升软件定义网络的抗故障能力。

作者得出的结论与Fonseca和Mota[10]的研究结果相似，他们都指出了各韧性研究领域所面临的主要挑战。不同之处在于，Fonseca和Mota[10]是从应用层面、控制层面以及数据层面来分析这些挑战的。

陈等人首先探讨了传统网络中服务器与链路层面的容错能力。随后，他们研究了基于OpenFlow协议的SDN数据平面与控制平面的故障检测与恢复机制。霍尔费尔德等人[14]讨论了SDN三大层中的可扩展性问题，以及相关研究领域的进展。冈萨雷斯等人[15]调查了传统网络与SDN中实现快速、一致的网络更新所需的机制与协议。福斯特等人[13]则重点研究了NFV编排器的可靠性问题，包括其抗故障能力。

近期，多篇调研论文[16]–[19]探讨了人工智能与机器学习在网络环境中的应用。Boutaba等人在[16]中全面总结了机器学习在网络技术中的应用。这些调研论文涵盖了多种类型的网络，如蜂窝网络与无线传感器网络，并涉及了流量分类、故障管理等网络管理相关议题。其中，故障管理相关的研究根据网络类型、所使用的机器学习技术、数据集、特征提取方法、输出结果以及评估方式进行了分类。论文[17]–[19]分别对用于解决无线传感器网络、自组织网络以及软件定义网络中常见问题的机器学习方法进行了文献综述，每篇论文中也简要介绍了相关的故障管理技术。

我们的工作旨在补充现有的调查成果，并介绍一些新的方法，包括在故障定位与修复方面的最新进展。我们探讨了在多租户环境中整合SDN/NFV技术所带来的新特性与挑战。随后，我们根据故障管理的相关步骤、所采用的方法及其在解决NVE相关问题中所发挥的积极作用，对NVE领域中的故障管理相关举措及开源项目进行了分类与比较。最后，我们分析了这些举措的贡献与不足之处。

三、背景情况

NVE技术使得多种架构能够在同一基础设施上共存。图1展示了这种架构环境的高层概览，它从纵向和横向两个角度展示了租户专属5G服务中各相关组件的构成。本节将介绍SDN与NFV的基本概念、这两种架构的共存机制，以及支撑NFV技术的基础设施构成。同时，我们还会对故障管理流程进行定义，并阐述相关机器学习与人工智能技术在这些流程中的应用方式。

A. 网络虚拟化环境

我们介绍了SDN与NFV技术，并强调了它们之间的关联。
1) 软件定义网络：SDN是一种新兴的网络架构，它将网络的控制、管理及数据转发功能分离开来，从而使网络控制功能能够被直接编程实现，并使底层基础设施变得可被抽象出来，以便为各种应用和服务提供支持[20]。在SDN架构中，外部控制器负责决定与控制平面相关的功能，这些功能包括系统配置、管理以及路由表信息的交换。正是由于这种功能分离，网络才能具备更高的灵活性和可编程性。

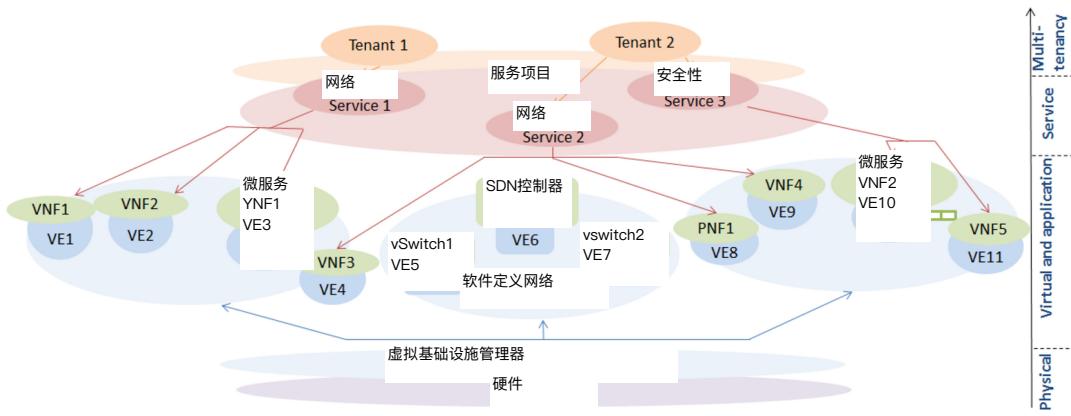


图1. 网络虚拟化环境。

交换机变成了简单的转发设备，而控制逻辑则由控制器来实现。这样一来，使用OpenFlow协议进行策略执行及网络重新配置的工作变得更加简单。这种架构使得控制器能够直接与网络设备（如交换机、路由器）的转发层进行交互。SDN分为三层：基础设施层、控制层和应用层。基础设施层也被称为数据层，它包含所有的转发设备，即物理交换机和虚拟交换机。应用层则托管着网络功能实体，并通过北向应用程序编程接口与SDN控制层进行通信，用于传递网络状态信息及特定需求。位于控制层的控制器则通过南向接口向数据转发设备发出指令。近期，开源社区推出了多种SDN控制器，这些控制器的成熟度及功能各不相同：POX、Beacon、Ryu、Trema、OpenContrail和ONOS都是著名的例子[21]。

2) 网络功能虚拟化：网络功能虚拟化是一种将原本运行在专用硬件设备上的网络功能（如NAT、防火墙、入侵检测系统及DNS服务器）转变为运行在普通硬件服务器上的软件功能的技术。这类与底层硬件解耦的软件功能被称为虚拟网络功能。ETSI-NFV在相关白皮书中提出了多种网络功能虚拟化在移动网络中的应用场景[22]。其中一个有趣的应用场景是“虚拟网络功能转发图”技术，该技术可实现端到端的5G

服务部署。“虚拟网络功能转发图”被定义为一系列相互连接的虚拟网络功能，它们共同提供具有特定功能的网络服务[23]。文献[24]的作者总结了当前市场上常见的虚拟网络功能相关产品与解决方案。例如，Metaswitch公司的Clearwater项目就是一个虚拟IP多媒体子系统[25]。

3) NFV与SDN的共存：SDN与NFV是两种独立的技术概念，但它们实际上可以互补共存。从本质上讲，网络功能单元完全可以不借助SDN技术即可被虚拟化并部署；同时，那些未经过虚拟化的网络功能仍可以通过SDN技术进行管理。这两种技术互为补充，能够实现共赢——NFV可以通过提供运行SDN软件所需的基础设施来支持SDN的发展。例如，SDN的软件系统就可以依托NFV所提供的基础设施来运行。

控制器可作为虚拟网络功能实体使用。此外，SDN基础设施可用于实现虚拟网络功能实体之间的数据转发。从开放网络基金会(ONF)的角度来看，SDN控制器所对应的虚拟网络功能实体只不过是网络图中的另一个资源节点——该节点具备已知的连接关系以及可被控制的传输功能[26]。从网络运营商的角度来看，将NFV与SDN结合应用于同一基础设施中是明智之举，此举有助于降低NFV的部署及管理成本。此外，SDN所具备的可扩展性与灵活性使得NFV能够动态部署，从而满足虚拟网络与物理网络基础设施的各种需求，实现按需配置NFV服务以及满足相应的通信要求[26]。

4) 多租户架构：为更充分地利用虚拟化技术，运营商可将未使用的资源共享给客户，这些客户便成为同一基础设施的租户。不同供应商及机构对多租户架构的定义略有差异。一般来说，多租户架构意味着多个租户或客户共享相同的虚拟计算、存储及网络资源[27]。例如，在图1中，两个租户正在同一基础设施上共享资源。多租户架构的实现依赖于“资源切片”技术——该技术能够将多个租户的流量分隔开来，通过专门建立的隧道在相应的资源切片内传输数据[28]。

B. 基础设施与运行环境

ETSI-NFV产业规范组将NFV架构分解为若干主要组成部分，包括虚拟网络功能模块（VNFs）、NFV管理与编排系统（MANO），以及基于传统网络组件（如运营与业务支持系统OSS/BSS）构建的网络功能虚拟化基础设施（NFVI）[29]。

虚拟基础设施管理器（VIMs）是NFV-MANO架构中的关键组成部分，对于实现NFV架构所带来的商业价值至关重要。VIM负责协调物理资源，以提供网络服务。在NFV市场中，众多供应商提供了相应的VIM解决方案，例如Kubernetes、VMware、OpenStack和OpenVIM等。虚拟机、容器及单内核技术则为虚拟网络功能模块提供了必要的虚拟计算与存储资源。



图2. 故障管理流程。

容器作为一种更灵活、更敏捷的应用程序运行方式应运而生。与传统虚拟机需要运行独立的操作系统不同，容器能够让轻量级应用程序直接在Linux操作系统上运行。而单内核技术则是一种更为轻量级的解决方案——它将虚拟网络功能与所需的库打包在一起，而不像虚拟机那样需要提供完整的客户机操作系统。单内核使用一种“基于库的操作系统”，其内核功能与单内核镜像代码一起被编译进去。因此，单内核镜像的大小与容器相当。不过，这一限制使得无法将诸如ICMP Ping之类的系统诊断工具嵌入到单内核系统中。虚拟机与容器为虚拟化技术带来了新的应用方式，相关内容可见[24]文献。其中一种方法是在虚拟机中运行容器；另一种被称为“清晰容器”的技术，则是在运行基于Clear Linux的轻量级操作系统的虚拟机中运行容器，这种虚拟机的启动时间更接近容器的启动时间。

C. 故障管理

故障管理是指定位、分析、修复并报告各类网络问题（如链路故障及网络过载）的整个流程。图2展示了从问题发现到问题解决的整个故障管理流程。故障诊断的核心目标是完成三项相互通补的任务：故障检测、故障定位以及故障类型识别[30]。在接下来的内容中，将详细阐述故障管理的各个环节，以及针对传统电信网络所采取的相应措施。

1) 故障检测：故障检测既是一项基础性任务，同时也是一项具有挑战性的任务。这一环节用于判断系统是处于正常工作状态，还是发生了故障。故障是导致系统进入错误状态的根本原因。当错误引发网络设备或软件出现故障时，就会出现相应的问题或警报。系统的正常运行状态与故障状态可能取决于服务级别协议以及各网络服务提供商的性能要求。根据故障的表现形式和成因，可将故障分为不同类型。故障可能是永久性的，也可能是短暂出现的，还可能反复发生。其产生原因可能包括维护操作失误、配置错误或恶意入侵[15]。此外，故障可能导致系统完全崩溃，也可能仅导致系统性能下降。表II列出了NVE中可能出现的一些故障类型，这些内容将在第IV-B节和第V-B节中进一步讨论。网络管理员利用两种类型的数据来判断网络的状态：警报信息与各项性能指标。

a) 警报：警报其实是系统故障的外在表现形式。这些警报信息可能来自诸如SNMP陷阱之类的管理工具[31]，也可能以系统日志文件的形式出现，而这些日志文件是由syslog协议（或其他协议）生成的[32]。Syslog协议允许设备通过网络将事件通知信息发送到任何预先设定的接收端[32]。Syslog日志中包含的信息可能包括：

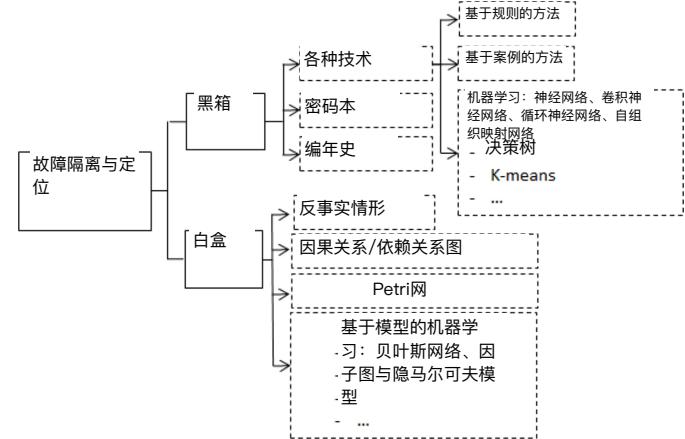


图3. 故障定位方法。

生成警报的对象的IP地址、时间戳、警报标识符、故障严重程度的等级，以及关于该故障的附加文字描述。Syslog消息通常会被存储在日志文件中。这些消息包含了关于系统运行状态的重要信息，其中一些消息仅用于提供信息，而另一些则用于发送紧急通知。然而，尽管警报能提供关于故障根本原因及类型的重要线索，但某些故障可能只能部分被观察到，或者根本无法被察觉。在复杂网络环境中进行日志管理时会遇到一些问题：

- 由于设备的连接方式及相互依赖关系，一次故障可能会引发多起警报；
- 在重新配置、维护操作期间，或由于网络设备状态需要较长时间才能稳定下来时，可能会出现误报现象；
- 警报信息的丢失、延迟，或时间格式不符合ISO8601标准[33]；
- 分布式系统中的时钟同步问题会导致接收到的警报顺序混乱。

由于大多数故障无法直接被观察到，因此管理系统必须根据接收到的报警信息来推断这些故障的存在。这就凸显了故障关联分析与推理技术的重要性。

b) 指标：另一种检测异常行为的方法是收集网络性能指标。这些指标既能从定量角度也能从定性角度验证系统是否具备所需的功能，同时还能衡量系统性能的下降程度。网络性能指标包括延迟、抖动、吞吐量以及网络利用率等。例如，抖动指的是数据包传输过程中的延迟变化；而网络利用率则反映了当前网络容量被实际使用的程度。在故障检测过程中，需要持续监测系统层面的各项指标。

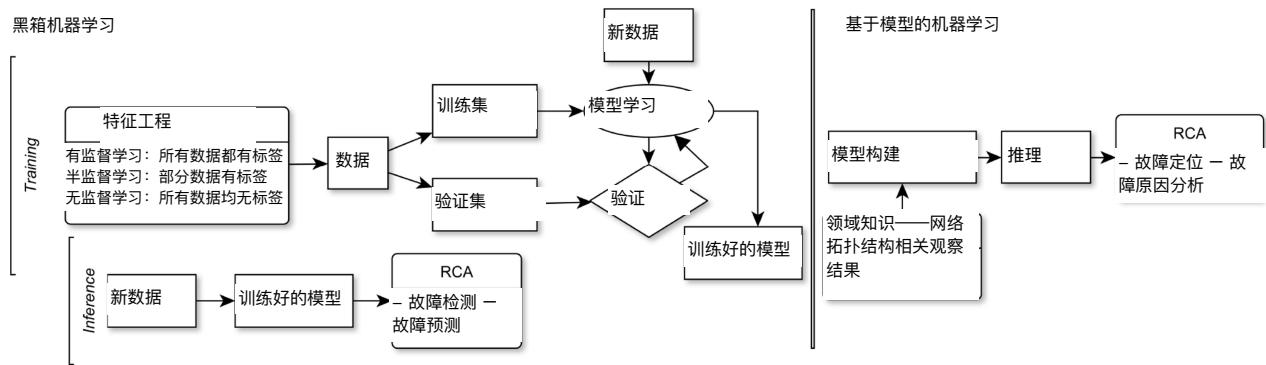


图4. 黑箱方法与基于模型的机器学习方法。

当出现指标显示服务水平协议被违反或未得到满足的情况时，系统会发出通知。

2) 故障定位与识别：当系统出现故障或性能下降时，虽然会通过警报通知发现故障现象，但仍有许多疑点需要解决。由于检测过程提供的信息有限，因此故障证据往往具有不确定性、矛盾性或不完整性[34]。故障定位（也称为故障隔离或根本原因分析）是指从各种警报、通知及相关数据中推断出故障确切根本原因的过程。这一过程需要解决由于警报信息模糊不清以及错误信息传播方式不一致所带来的各种问题[34]。此外，故障定位结果应为操作人员提供关于故障根本原因及类型的明确解释，并且必须考虑网络拓扑结构、正在运行的服务以及系统的配置与维护情况。

在图3中，我们提出了一种新的网络故障定位技术分类方法。这一分类体系是对现有研究[34]中提出的方法的补充。故障定位技术被划分为白盒技术与黑盒技术两大类。图3展示了那些被证明对网络故障排查具有实用价值的技术方法。所谓白盒技术，是指那些利用网络及其拓扑结构的显式模型来进行故障定位的技术；而黑盒技术则基于隐式模型来实现故障定位。白盒方法通过模拟节点、事件、警报与故障之间的相互关系，帮助人们理解故障的发生机制及其传播过程。黑盒方法则从数据中学习模型，但这种模型往往难以被理解和解释。人工智能，尤其是机器学习技术，在电信领域受到了越来越多的关注，因为它能够实现自动化管理。机器学习利用基于数据训练得到的数学模型来做出决策，而无需预先编写具体的程序来执行这些任务[35]。机器学习方法主要应用于四种类型的问题：聚类、分类、回归以及规则提取[16]。分类任务的目的是将新的输入数据与预先设定的离散输出结果进行匹配；回归任务的输出结果是连续型的；聚类任务的目的是将具有相似特征的数据归为一类；而规则提取则是从数据中提取出具有符号意义的规则。

在定位技术中，这些方法被划分为黑盒模型与白盒模型两类（见图3）。基于模型的机器学习方法（如贝叶斯网络）旨在为推理过程构建一个明确的诊断模型；而黑盒机器学习方法（例如神经网络）则通过训练数据和验证数据来学习模型。根据数据是否被标注，这些方法可分别应用于有监督学习、半监督学习及无监督学习场景。其中，数据可能被完全标注、部分标注，或者根本不标注。

a) 白盒技术：白盒方法主要包含两种结构：领域模型与问题解决算法[36]。领域模型描述了系统中的各个组成部分及其报警信息传播的机制，而问题解决算法则是用于识别模型中根本原因的事件管理工具。然而，基于模型的方法存在两个缺陷：一是模型本身的定义问题，二是其处理大规模网络的能力有限。基于模型的因果关系或依赖关系图（见图3）展示了故障、报警、中间故障以及由此引发的后续故障之间的相互关系。节点之间的连线代表因果关系，这种关系可以是“必然导致”的，也可以是“可能导致”的[37]。网络拓扑结构及故障传播规律是基于管理员对硬件和软件规格的了解而总结出来的。许多研究[38]–[40]利用依赖关系图来实现故障定位。Petri网是一种描述并发与分布式系统状态变化的基本模型，它通过“转换”与“状态节点”来表示系统的状态变迁，而这些转换的发生取决于输入数据的可用性。Petri网被用来描述网络中的故障传播过程：其中状态节点代表设备生成的报警信息，而转换则代表导致网络状态变化的事件。这种方法曾在同步数据层次结构网络中得到应用[41]；另有研究[42]利用Petri网来检测网络服务级别协议的违规行为。在[42]中，每个报警事件都对应一个Petri网模型，这些模型被用作查找根本原因的行动计划。

较新的RCA方法[37]、[43]采用了贝叶斯网络。贝叶斯网络是对因果关系图及依赖关系图的概率化扩展。它是一种有向无环图，用于表示可观测事件与不可观测事件之间的因果关系；通过观察一系列症状，便可确定最可能的原因[44]。该有向无环图中的节点代表随机变量。

元素、事件以及错误关系分别用节点表示；而边则象征着相连变量之间存在直接的因果关系。这种因果关系的强度通过条件概率来体现。要构建一个贝叶斯网络模型，就需要人类专家对该领域中各种因果关系有深入的了解。这样一来，就能生成人类能够理解的因果关系解释，而不同于那些属于“黑箱”性质的技术[37]。

[37]和[43]的作者提出了基于贝叶斯网络的电信网络自诊断方法。[37]的作者设计了一种基于通用贝叶斯网络框架的自建模与诊断系统，用于IP多媒体子系统中的故障定位。IP多媒体子系统属于具有多层结构的大型网络系统，该模型能够描述IMS服务中各组件之间的依赖关系。当IMS服务出现故障时，该算法会从给定的网络拓扑结构中找出与该服务相关的贝叶斯网络实例，并生成相应的贝叶斯网络模型。[43]的作者则提出了一种适用于光纤到户网络的三层自重构概率模型，用于故障诊断。该模型结合了决策机制与人工智能学习技术：决策部分基于贝叶斯推理原理，而人工智能学习功能则实现了系统的自重构能力。

多变量逻辑模型的另一个有趣应用实例是乘法因子图或约束图。约束图由一组变量、每个变量的取值范围以及一组约束条件构成[45]。这类图可以被表示为一个包含两种类型节点的簇图：变量节点和函数节点，后者用于表示变量之间的约束关系。一个节点实际上是由多个通过约束条件连接起来的变量组成的。当两个节点包含相同的变量时，它们就被视为相互连接。在因子图中应用的RCA算法被称为“簇树消除算法”。该算法整合了多种现有的算法机制，包括前向-后向算法、求和-乘积算法、Viterbi算法以及信念传播算法[46]。作者们提出利用基于因子图的算法来监测无线传感器网络中的链路丢失率。其核心思想是借鉴无线传感器网络中的数据聚合通信机制，通过观察传入的数据包来推断链路丢失率。

在故障诊断中，另一种推理方法是反事实推理[47]–[50]，其形式如下：

“如果A为真，那么B也必然为真吗？”

其中A和B分别代表事件或现象。A是导致结果B出现的反事实前提条件——也就是说，A是一种与实际观察结果相悖的事件；而B则是在该反事实前提条件下才会出现的预期结果[47]。近期关于实际因果关系[48]以及过错归属[50]的定义中，都运用了反事实推理的方法，旨在确定那些导致安全规范被违反的具体事件或因素；这些安全规范通常由VN要求来界定。

b) 黑箱技术：这类方法仅公开输入数据及输出结果，其学习过程往往难以被解释。文献[51]提出了一种属于黑箱技术的解决方案，用于过滤警报或日志，并寻找已知模式。所有被记录的事件都会被标注上时间戳。

事件被分类到相应的事件流中。当记录中的事件与接收到的事件流相匹配时，专家会对故障原因进行解释。这种技术能够实现从日志中自动学习故障信息。另一方面，代码本方法[52]通过一个包含二进制值的矩阵将故障症状与相应问题关联起来，每个问题都由一组症状向量来表示。基于规则的方法[53][54]则通过一系列条件形式化的规则来描述故障现象与根本原因之间的对应关系，即“如果出现<症状>，则故障的根本原因是<原因>”。而基于案例的方法[55][56]则通过学习过去的经验及类似情况来识别故障原因。

近年来，机器学习这一术语被用来指代那些能够适应新环境、识别并推断出规律性的技术。神经网络通过分析示例数据来实现逐步学习。这种学习系统由相互连接的神经元构成，这些神经元共同构成了一个或复杂或简单的神经网络结构。人工神经元是一种自主处理单元，它能接收一个或多个输入信号；这些输入信号会经过加权处理，再通过激活函数或传递函数进行运算，最终产生输出结果。在训练阶段，神经元会利用示例数据（即输入与输出数据）进行训练，直到达到预定的精确度为止；训练完成后，这些神经元便可被用来对实际数据进行处理并生成输出结果（见图4）。凭借从原始数据中提取信息的能力，神经网络能够有效识别数据中的规律模式，并检测出系统故障——而对于管理员或其他计算机技术而言，这类任务通常颇具挑战性。在各种类型的神经网络中，出现了多种用于故障管理的算法，包括卷积神经网络、深度神经网络、概率神经网络、循环神经网络以及自组织映射网络。除了神经网络之外，机器学习还包括许多其他应用于网络管理的方法，例如决策树（如随机森林）、支持向量机、长期记忆网络、K均值聚类算法以及K近邻算法[16]。

论文[57]–[60]采用了黑盒机器学习方法进行故障定位。论文[57]的作者使用了包含系统日志信息的神经网络。系统日志信息被分解为“时间”和“IP地址”等字段，并被转换为数值形式，作为机器学习过程中的输入数据。随后，这些输出结果会通过决策规则进行解读。

[58]中的作者使用RNN来检测无线传感器网络中的故障节点。RNN属于神经网络的一种，其神经元之间的连接构成一个或多个循环结构，从而实现神经元对自身输入的反馈。RNN模型中的节点对应于无线传感器网络中的节点。此外，RNN的输出是对无线传感器网络运行状态的估计值，该估计值会与实际网络行为进行对比，以此实现故障检测。[59]和[60]中的研究分别提出了基于K均值聚类的方法，用于检测IP网络和无线传感器网络中的故障。K均值聚类的目的在于将n个观测值划分为k个簇，使得每个观测值都属于距离其最近的簇中心。

3) 影响分析与恢复措施：影响分析常被误认为是故障隔离。然而，仅仅找出根本原因并不足以采取恢复措施；了解受影响的组件以及网络受损的程度同样至关重要。运维人员需要根据问题的严重程度来确定恢复工作的优先级。

表一：SDN与NFV多租户环境中的故障管理问题及其后果

	ISSUES	SDN?	NFV?	Multi-tenant?	CONSEQUENCES
拓扑结构	向SDN控制器发出的大量请求	✓			SDN控制器的处理能力有限
	- 出现了大量故障与警报现象。	✓	✓	✓	警报相关性分析与故障检测
	- 越来越多的资源			✓	资源分配的最优化
	- 动态拓扑结构		✓		对网络拓扑进行建模的难度
	- 虚拟网络多层架构		✓		多层、多分辨率的故障关联关系
	- Multi-tenants			✓	缺乏对网络状况的清晰了解
	- 复杂的金融实体	✓	✓	✓	选择适合频率测量精度的合适粒度。
	- 单个SDN控制器的故障	✓			网络通信功能失效
	- 链接故障	✓	✓		网络连接中断
	- 端到端服务链崩溃		✓		快速检测并恢复客户的服务。
容错能力	物理故障与虚拟故障	✓	✓		物理故障可能会影响多个虚拟实体。
	- 多租户故障			✓	租户的故障隔离与通知机制
	- SDN控制器与vSwitch的性能表现	✓			SDN的性能取决于网络拓扑结构。
	- 运行环境		✓		VNF的性能取决于虚拟主机。
绩效	租户应用程序或VNF的迁移		✓		在迁移VNF的同时保持其原有的性能水平
		✓	✓	✓	

根据故障对最终用户服务的影响来进行故障排除[61]。影响分析旨在确定故障的具体性质，例如故障的严重程度、传播范围、重要性以及造成的损害等。此外，影响分析还能帮助管理员了解潜在流程或产品故障所带来的风险。目前已开发出多种方法来量化故障的影响：基于图的方法[54]；因果分析[62]；故障模式与效应分析(FMEA)；故障模式、效应及临界性分析(FMECA)[63]。在传统网络中，大多数恢复操作都是由网络专家完成的，因为大多数故障都是由于硬件服务器崩溃引起的，这时就需要管理员来修复或更换相关设备。不过，网络链接的恢复过程中也支持一些自动恢复机制。网络路径恢复过程主要采用两种故障恢复方法：保护机制与恢复机制[64]。在保护机制中，故障发生之前就会预先规划并确定路由路径；而在恢复机制中，则是在故障发生后才进行新的链接分配。恢复机制可能会延长恢复时间，因为它属于被动响应方式；而保护机制则可能因链接被预先占用而导致网络拥塞。

四、NVE故障管理面临的挑战与问题

本节阐述了NVE相关问题，并探讨了在运用现有故障管理技术时所面临的局限性。

A. 问题

表一列出了SDN、NFV以及多租户架构所带来的挑战。表一中所总结的问题是从故障管理的角度出发，针对不同领域而提出的相应解决方案。下文将对这些问题进行详细说明。

1) 可扩展性：网络的可扩展性指的是其在流量增加时仍能保持性能的能力。在软件定义网络中，控制功能的集中化会引发可扩展性问题。事实上，连接到软件定义网络控制器的交换机数量不断增加，相应的请求量也随之上升，这可能导致控制链路出现拥塞现象。为了解决这一问题，通常需要采用控制器集群的方式来实现冗余设计[65]。控制器架构可以通过多种方式进行设计，以降低拥塞程度。此外，负载均衡技术也能有效提升网络的可扩展性。

需要采用相关技术来在集群中的控制器之间分配过重的负载[66]。随着NFV中服务数量的增加，需要管理的实体也随之增多，同时故障和警报的数量也在增加。这些警报可能来自不同的网络层和资源类型；例如，它们可以是传统的操作系统日志消息，也可能是为每种NFV服务专门定义的警报信息。将VNF分布在不同的站点上有助于提升服务运行的稳定性。然而，这也带来了一个新的管理问题：究竟应该将日志数据及管理系统分散部署还是集中管理。此外，在NFV环境中，故障可能会在各个网络层及不同站点之间传播，从而导致警报数量急剧增加。要有效应对这类情况，就需要采用先进的存储与过滤技术，并能及时通知严重的故障事件[15]。

2) 拓扑结构：NFV的灵活性使得网络中的拓扑结构能够进行灵活调整，同时各组件也能重新部署。在故障发生时，考虑实际的网络拓扑结构对于避免误判至关重要——即准确识别出那些已不再处于运行状态的故障组件。此外，在NVE架构中，物理实体与虚拟实体共存，这带来了新的依赖关系，在构建故障诊断模型时必须将这些依赖关系纳入考量。如图1所示，该拓扑结构是多层次的。因此，在构建故障管理机制时，需要兼顾不同的管理层次，并充分考虑各层次之间的依赖关系。例如，基础设施所有者可能仅负责处理物理层与虚拟层中的故障，并向租户收取服务管理相关费用。当存在多个租户时，便会出现一些棘手的问题，比如如何区分不同客户的警报信息、如何向租户发送通知、由于客户对所有者基础设施的访问权限受限而导致的信息可见性问题，以及如何在基础设施所有者与租户之间分配管理任务。

3) 颗粒度：如图5所示，NVE实体可分为两类：虚拟实体与物理实体。被管理的对象可以是节点、链接、网络或服务。节点可代表物理网络功能实体、虚拟网络功能实体、虚拟主机（例如容器、虚拟机或单内核系统），或是站点。虚拟网络功能实体通过虚拟链接相互连接，而站点则通过物理链接进行连接。网络管理的具体定义可见于[7]文献。

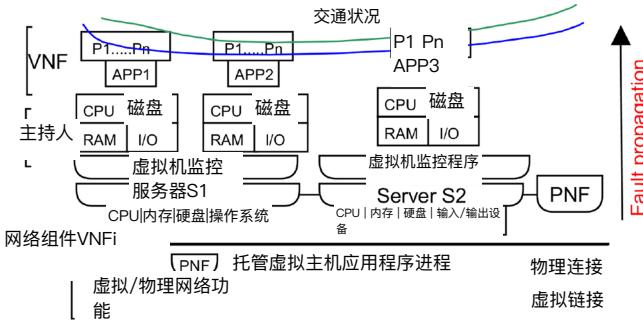


图5. 虚拟网络组件。

用于监控一组相互连接的虚拟节点与物理节点。服务实际上是由多个虚拟网络功能实体及物理网络功能实体组成的有序组合，其存在目的在于支持特定的应用场景，例如基于IP的语音通话服务。为确保故障定位的准确性，应采用更细粒度的划分方式，例如将系统划分为具体的应用进程，以及CPU、网络接口等子组件。

4) 容错能力：SDN的容错问题主要与传统网络中已存在的问题相关，即链路故障与节点故障。然而，SDN计算逻辑的集中化带来了新的挑战——单一的SDN控制器会成为故障的单一点，进而影响网络节点的数据转发能力，最终波及整个网络。在NVE架构中，一台物理服务器可能承载大量应用程序；一旦服务器发生故障，将导致大量服务受到影响，而这种情况在传统专用硬件架构中是不会出现的。

5) 性能：性能指的是提供所需服务质量的能力。性能是通过多种网络指标（如延迟、抖动和吞吐量）以及运行环境、协议与节点的可靠性、网络拓扑结构等因素来评估的。某些配置选择，例如网络设备被查询信息的最大频率，或是否保持足够的冗余机制，都可能影响系统的整体性能。另一个需要考虑的因素是具有相同配置参数的租户解决方案的迁移问题。迁移既需要时间，又会产生网络流量，而这些因素对于确保所需的服务质量至关重要。

6) 其他问题：解决上述问题时可能会引发其他新的问题。在软件定义网络中，为避免可扩展性难题并提升性能，人们提出了多种控制器集群方案。然而，这些方案会带来同步机制及控制器部署相关的问题[14]。此外，尽管在传统网络中路由更新的机制已被广泛研究，但在软件定义网络中，动态变化的网络拓扑结构以及需要持续进行的网络更新带来了额外的挑战。另外，控制器向网络节点发送的规则更新信息可能会出现延迟或异步传输的情况[13]。防止虚拟网络功能出现故障的一种方法是部署冗余节点，并保持足够的冗余能力以确保更好的性能。关于冗余机制及部署技术的内容将在第V-B节中进一步讨论。

B. 讨论

显然，网络虚拟化所带来的好处远超.....

NVE本质上比当前的网络系统具有更低的容错能力。故障管理方面虽然面临新的挑战，但同时也受益于虚拟化技术。事实上，得益于NFV的灵活性与可编程性，虚拟机的生命周期管理及相关修复操作实现了自动化。NFV的另一个优点在于其分布式架构能够提升网络的整体稳定性。例如，由于各服务分布在不同位置，NVE能够有效防止故障在服务之间传播[67]。然而，故障管理的需求正在发生显著变化，管理系统必须考虑各种细节，包括逻辑资源、虚拟资源，以及动态变化的网络拓扑结构、租户资源在不同地点的分布情况，还有硬件与软件之间的依赖关系。此外，在NVE环境中，自动化已成为不可避免的趋势。因此，有必要定义一系列自我管理功能，尤其是网络的自我修复与自我建模能力。第三-C节中介绍的传统故障管理技术，在面对NVE的特性时存在诸多局限性。

- 基于规则与基于案例的方法需要根据网络功能虚拟化技术的可扩展性及动态特性进行调整。在存在专家知识的静态网络环境中，模板与规则能够发挥重要作用；然而在像网络功能虚拟化这样的动态网络环境中，获取此类专家知识却十分困难。

代码本与日志记录属于快速且灵活的模式识别技术，能够根据症状及警报信息识别出存在的问题。不过它们的缺点在于无法充分解释网络中实际发生了什么，同时对于警报信息的丢失情况较为敏感，也不太擅长处理大量警报同时出现的状况。

Petri网与反事实推理仅能用于此类推理。

事件是按特定顺序发生的，且不具备良好的扩展性。

- BN模型与因子图能为诊断提供辅助依据。
然而，NVE的多层动态拓扑结构增强了系统的灵活性与性能。确定合适的诊断模型的难度。
- 尽管机器学习方法因其诸多优势而极具吸引力.....
为高效地解读数据，在非线性向量机中，训练数据起着关键作用。应适应虚拟数据的特性及相关要求。

NVE的动态性。

为展示NVE管理的相关问题与功能，我们提出了两种故障场景，如图6所示。图6(a)中的OPNFV DOCTOR用例展示了为快速检测故障并通知受影响的租户所需执行的各项步骤[68]。在此场景中，用于托管Openstack虚拟机的服务器出现故障。该故障会通过虚拟化层传播，进而影响正在运行的虚拟机。一旦VIM识别出哪些虚拟机受到了影响，相关客户端便会收到恢复指导信息。此时，客户端1会切换到备用虚拟机1。在第二个场景中（见图6(b)），vIMS注册服务出现故障，错误代码为408。这种情况下，代理Bono应用程序中的某个关键进程会停止运行。为完成注册操作，客户端会向代理发送认证请求，代理会将请求转发给Sprout路由器，并尝试通过Homestead（即家庭用户服务器HSS）对客户端进行认证。但由于代理出现故障，客户端无法完成注册，此时路由器会发出警报以提示相关问题。

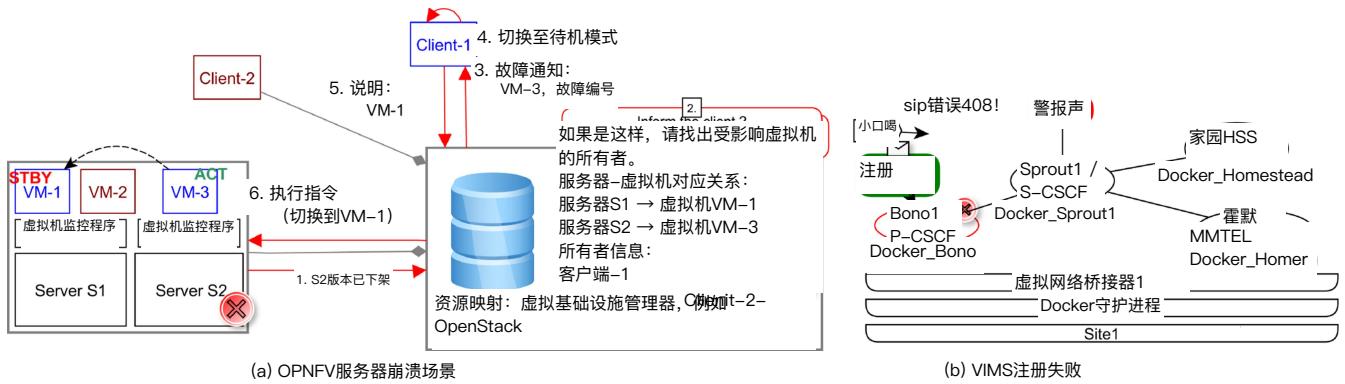


图6. 虚拟网络故障场景。

表二
NVE中断层的分类

层次结构		故障类型	SDN/NFV faults	自我修复功能
物质形态	维护费用	服务器的维护工作	1. 向客户发送维护通知; 2. 将服务器状态设置为维护状态。	
	物理碰撞	· 交换机物理端口的故障。 · SDN控制器发生故障。 · 提供链接 · 物理机器发生故障。	将逻辑接口迁移到另一个物理端口上。 切换至备用控制器进行操作。 寻找其他途径。	
	Crash/ Saturation	· 虚拟机崩溃，或虚拟机的CPU负载过高。 · vSwitch端口的饱和状态。 · Switch忽略了如何与客户端建立连接的问题。 · 桥接配置错误。 · SFC配置错误。 · 对VNF服务的请求数量过多。 · 端到端服务的崩溃。 · VNF应用程序崩溃。	1. 更改该相机的状态；2. 将运行在该相机上的虚拟网络功能模块迁移出去；3. 清空该相机的内存，以便进行维护。 创建其他虚拟机，或扩展现有虚拟机的内存与CPU资源。 创建另一个端口或虚拟交换机。 控制器或交换机的重新配置 桥接器重新配置。 SFC重新配置。 1. 复制VNF；2. 增加VNF主机的内存和CPU资源。 1. 重新启动相关虚拟网络功能；2. 重启端到端服务。 重新启动或创建VNF主机。	
虚拟的	配置设置			
	Crash/ Saturation			
应用程序/服务				

有必要采用更细粒度的划分方式，以便识别那些可能影响服务运行的子组件故障。在网络虚拟化环境中，还可能出现其他类型的故障，例如SDN控制器故障、控制器与交换机之间的连接故障，或是由于负载过重导致的系统饱和现象（详见表1）。此外，编排系统和监控子系统的故障也可能对各种网络组件产生负面影响[13]。

五、新颖的故障管理方案

本节探讨了当前为解决NVE相关问题而采取的各项措施。这些措施包括在解决方案中运用自动化技术，引入新的概念，以及重新启用那些在NVE环境中变得可行且实用的旧方法。

A. 自我建模

在大多数基于模型的故障检测技术中，构建模型是实现故障诊断与修复的重要步骤。系统模型是对其结构与功能特性的抽象表示，其中包含了网络拓扑结构、故障类型及其所带来的后果。该模型可通过运用专家知识、相关标准、收集到的数据、网络节点之间的依赖关系以及统计分析方法来构建。在早期网络部署阶段，构建模型要容易得多——那时网络规模较小且拓扑结构固定，只需依赖标准规范和专家知识即可完成模型的建立。

然而，借助虚拟化技术，网络拓扑结构变得动态化，这使得提取通用模型变得复杂。因此，Sánchez-Vilchez等人[69]以及Cherrared等人[70]分别提出了如下方法：在SDN环境中利用从控制器中提取的拓扑信息；在NFV环境中则利用从VIM及监控工具中获取的拓扑数据。为了对SDN组件进行建模，Sánchez-Vilchez等人[69]定义了两种模板：网络节点模板和链路模板。这些模板用于描述每个网络元素内部虚拟组件与物理组件之间的关联关系。随后，他们利用模板实例化算法，根据控制器提供的拓扑信息对网络进行建模。Cherrared等人[70]则提出了一个监控框架，用于提供NVE环境中的实时拓扑数据。这些数据有助于构建与实际网络拓扑结构相匹配的诊断模型。该方法充分利用了开源监控工具所提供的实时网络基础设施视图功能；同时，OpenStack工具如Ceilometer、AODH[71]和Monasca[72]也能提供相应的指标监测与报警功能。其他开源工具Nagios[9]和Zabbix[73]同样能够在虚拟云环境中实现高效的报警通知功能。

B. 自我修复能力

自我修复能力指的是系统具备自动从故障中恢复过来的能力。在网络虚拟化环境中，这种自我恢复功能能够显著缩短故障修复所需的时间，因为可以在保持服务正常运行的同时进行故障排查。为实现网络虚拟化环境中的自我恢复功能，人们已经开发出了多种相关机制，并对这些机制进行了持续优化。详见表二。

如第IV-B节所述, 第一种情况是硬件故障。此时, 首要措施是将受影响的虚拟机从服务器上迁移出去。第二种情况是应用程序出现故障, 解决办法是重新创建代理Docker实例或重启相关进程。下文将介绍一些重要的自修复机制及其相应的处理方法。

开源恢复工具: OpenStack VIM通过Heat模块提供了在虚拟机发生故障时的基本恢复功能, 该模块能够尝试重新启动无法正常运行的虚拟机。然而, 它并不支持任何故障转移或冗余机制。为填补这一空白, 出现了多种解决方案, 例如添加Pacemaker等OpenStack故障转移插件[99]。不过, 即便采用了冗余机制, 仍存在风险——即当用于故障转移的虚拟机本身也发生故障时, 系统将无法正常运行。为解决这一问题, Moghaddam等人[84]提出了使用多代理系统或HAstack插件来监控OpenStack中的计算节点及虚拟机实例的方案。该方案的思路是结合Pacemaker与OpenStack模块的功能。当某虚拟机发生故障时, 系统会立即启动一台配置与服务完全相同的新虚拟机来替代它; 同时, HAstack插件会负责修复出现故障的虚拟机。这一机制显著缩短了系统在发生故障时的恢复时间。
SDN控制器故障转移: 冗余机制也是提升控制器容错能力的一种方式。事实上, OpenFlow标准本身并不支持控制平面的自动恢复功能。在较新的OpenFlow版本中, 可以为控制器分配主从角色——主控制器负责执行核心控制功能, 而从控制器则仅能读取交换机的状态信息。然而, 要实现有效的故障转移机制, 就必须解决一些关键问题, 例如: 哪个控制器最适合替代发生故障的控制器? 需要多少次更新才能让冗余控制器及时了解当前的网络拓扑结构? 究竟需要配置多少个冗余控制器才能满足需求? 为了解决这些问题, 一些研究[85][86]提出了更为复杂的控制器故障转移方案。例如, Pashkov等人[85]提出了一种高可用性控制器架构, 通过在控制器核心与网络服务及应用程序之间添加集群中间件来优化故障转移流程。不过, 采用多控制器架构意味着需要处理控制器之间的同步问题以及网络更新数据的一致性保障问题[13]。Guo等人[100]则建议仅在某台服务器的负载超过预设阈值时才进行控制器间的状态同步, 从而降低同步带来的开销。

通道或链路故障切换: OpenFlow交换机能够检测到链路故障, 但必须等待控制器建立备用路径。一些研究[87]—[89]探讨了在SDN环境中利用第II-C3节中提到的恢复与保护机制来实现链路故障恢复的方法。Hwang与Tang[87]提出了一种针对控制通道与数据通道的故障切换解决方案: 对于数据通道, 同时采用了恢复机制与保护机制。在恢复过程中, SDN控制器会根据网络拓扑的完整二分图来计算备用路径; 而在保护机制中, 控制器会配置SDN交换机的流表项。至于控制通道的恢复, Hwang与Tang[87]采用了恢复机制来实现这一目标。

为了解决恢复与保护机制所带来的问题——即随着交换机数量增加导致故障转移时间延长, 以及如何应对网络状态的动态变化——Ko等人[89]将这两种方法结合到一个基于动态网络管理器的框架中。所提出的方法包括在更短的时间间隔内(例如5秒)计算备份路径, 并且只有当实际发生物理网络故障时, 才会配置相应的恢复流程规则。Giatsios等人[88]提出了一种针对租户数据流的主动故障转移机制, 这些数据流通常通过隧道进行传输。一旦主路径中的某个链路发生故障, 使用隧道的数据流就会被重新路由到备份子路径上, 同时这一过程对使用相同隧道的租户来说是透明的。链路故障还可能影响到NFV架构。Soualah等人[90]提出了一种方法, 旨在通过合理布置和连接NFV组件来最小化因链路故障而导致的服务中断所带来的影响。他们采用了决策树算法来选择可靠的路径, 以防止链路故障的发生; 而在发生故障后, 则能及时将受影响的虚拟链路重新导向到更安全的物理路径上。

NFV链式服务故障转移: 在服务功能链中, 网络服务的性能取决于各个服务功能的性能。Lee与Shin在[91]中研究了在等待服务功能链控制平面提供备用服务功能路径时可能出现的服务恢复延迟问题。他们提出的方案能够在某个服务功能发生故障时, 通过将流量重定向到服务功能转发节点列表中存储的另一个功能上来临时恢复服务功能链的正常运行, 且整个过程仅需使用数据平面信号进行控制。Sauvanaud等人在[75]中提出了一种检测服务水平协议违规行为的方法, 并能识别出导致违规现象的异常虚拟机。该方案采用了随机森林算法及故障注入工具; 其核心目标是从每15秒收集一次的监控数据中识别出异常行为, 这些数据来自两个来源: 托管虚拟机的管理程序以及虚拟机自身的操作系统。故障注入工具的运用确保了在训练阶段能够精确模拟故障的发生情况。实验测试平台基于Clearwater开源项目开发的vIMS平台进行搭建[25]。

回滚: 这是一种广为人知的实现容错性的技术。回滚机制能够以低成本、透明地恢复系统状态[92]。所谓“快照”实际上代表了虚拟网络功能的正确运行状态, 这种状态会定期被保存到稳定的存储介质中, 以便在系统发生故障时立即恢复系统运行, 从而最大限度地减少数据丢失。然而, 与常规的系统重启方式相比, 回滚机制会导致更长的服务中断时间, 其主要原因在于快照文件的大小通常相当可观, 且其大小与虚拟机的规模成正比。崔等人[92]与施等人[93]均致力于解决回滚过程中的延迟问题。例如, 崔等人提出了一种基于虚拟机间相似性特征的回滚系统, 该系统利用组播技术将相同的数据页传输到多个虚拟机上, 从而让所有主机只需保存一份副本即可, 而无需各自独立地存储这些数据。

C. 故障预测与主动恢复机制

5G网络的架构、运行机制及管理方式仍处于设计阶段。因此，对于网络运营商而言，此刻正是采取主动措施的关键时机——通过这些措施能够迅速发现潜在的严重故障迹象，并预防未来可能出现的缺陷。为实现故障预测，众多研究[74][75][78][96]提出了基于机器学习的解决方案，这些方案通常需要处理海量数据或日志信息。Sauvanaud等人[75]采用了随机森林算法来识别异常运行的虚拟机。论文[74][78]则提出了离线分析方法，用于挖掘网络数据中的规律性趋势，帮助运营商提前发现并解决类似故障。Gonzalez等人[78]利用结合了数据摘要处理技术的随机森林算法，自动识别系统事件之间的关联关系，从而帮助网络运营商找出故障的根本原因。此外，Cotroneo等人[74]提出了一个可靠性评估基准，旨在帮助NFV服务提供商判断哪种管理方案能带来最佳的可靠性效果。为此，他们设计了一套评估指标，既能用来衡量人为引入的故障对服务水平协议的影响，也能量化故障管理机制的覆盖范围及响应速度。Zhang等人[96]则应用RNN/LSTM模型来预测NVE中的故障。在实验中，他们在OPNET仿真环境中对多个VNF实例注入了6种不同类型的故障。实验结果表明，故障的严重程度越高，预测结果的准确性也就越高。预测所需的时间约为800秒。

D. 故障注入

故障注入过程包括向网络中注入多种类型的缺陷。根据注入目标及缺陷类型的不同，可能会出现不同的故障场景。注入目标可以是网络中的各类组件；注入的粒度也可以有所不同，例如可以针对CPU使用率、特定进程或网络链接进行故障注入。这些故障的设置目的可能是为了对网络造成压力（例如导致CPU过载），或是为了使被注入的目标失效（例如让物理服务器停止运行）。通常，故障注入技术被用来测试网络的稳定性，比如Netflix采用的“混沌猴子”测试方法。其目的是在网络出现故障的情况下收集相关性能数据，进而评估网络维持良好服务水平的能力。Cotroneo等人[74]提出了一种可靠性评估方法，该方法能够根据作者定义的故障类型来评估网络的服务质量。

然而，在NVE中，为了加速故障的发生，从而为机器学习方法提供学习和验证数据集，人们采用了故障注入技术。实际上，获取这些数据可能需要数天的时间。例如，Gonzalez等人[78]花费了206天时间才收集到约21,442起网络故障事件。论文[75]和[96]提出了使用故障注入模型来缩短这一时间。

Sauvanaud等人[75]采用了两种故障注入方法：一种是在单个虚拟机中实施局部故障注入；另一种则是通过提交大量计算任务来引发全局性故障。张等人[96]在OPNET仿真环境中模拟了六种不同严重程度的故障类型，其发生频率遵循泊松分布规律。

E. 日志分析与数据挖掘

日志分析最初是由专家们进行的，但后来……

在监控信息及日志分析自动化方面，相关技术变得至关重要。随着服务器存储容量的增加以及数据在云端的分布式存储，存储海量数据成为可能，这些数据被称作“大数据湖”。数据挖掘是指从大数据集中提取有用信息的过程。在虚拟网络环境中，利用日志分析或数据挖掘技术进行异常检测依然是一种高效的方法，因为数据始终是宝贵信息的来源。在数据挖掘过程中，前三个步骤（即数据整合、清洗与筛选）用于对数据进行处理，以便后续应用数据挖掘技术[101]。最后，通过聚类分析、关联分析等数据挖掘方法来发现有趣的数据模式，并对这些模式进行评估，从而做出最终决策。一些研究[77][95]采用了这种方法来提取有助于异常检测的有用数据模式。Baseman等人[77]提出了一种基于从虚拟机中收集的系统日志数据进行异常检测的方法：他们首先从文本数据中提取Infomap聚类结果，从数值数据中提取关联特征，并将这两种特征与关键词统计结果结合，形成一个统一的数据集。每条日志会根据其文本内容所属Infomap聚类的占比被分配到相应的聚类中。

F. 故障管理框架

关于故障管理的自动化以及故障管理架构的设计，已有多种方法[42][76][83][98]提出了相应的故障管理框架。这些框架大多基于自动化管理理念以及相关标准化组织的定义，例如ITU-T的M30xx系列建议书，该系列建议书为电信网络管理提供了通用框架[102]。故障管理框架通常由多个相互协作的组件构成，每个组件都具有特定的功能，如故障建模、故障检测或故障根源分析等。在最新的研究中，这些框架中的组件越来越多地被开源工具所取代，这些工具能够提供所需的功能。近期的一些研究[70][76][83][97][98]提出了针对网络功能虚拟化的故障管理框架。例如，Luchian等人[98]使用了OpenStack作为NFV的虚拟化基础设施，同时利用Nagios收集云环境中各链路的传输速率及单向延迟数据，从而帮助优化网络功能虚拟化服务。Song等人[76]则采用了SNMP和Syslog协议作为事件检测工具，同时使用Openflow与SDN控制器进行通信。Vilchez等人[83]提出了一种用于提升5G网络弹性的自愈框架，该框架能够在SDN的应用层、控制层、数据层以及服务层发挥作用，通过对网络状况的监测并启动相应的恢复措施来实现网络的自愈。OPNFV项目中的Doctor团队提出了Vitrage[97]这一OpenStack故障根源分析工具，该工具能够针对虚拟实体和物理实体生成快速报警通知，并利用推导出的报警规则来提升故障处理的效率。Vitrage的数据来源包括OpenStack模块以及Nagios、Zabbix等外部开源工具，同时它还能提供实时的网络拓扑映射功能。其故障诊断过程基于预先定义的模板，这些模板包含了用于故障根源分析的各种规则。Cherrared等人[70]……

表三 错误管理措施的分类

Papers Ref.	故障检测 指标	警报声	故障定位	影响分析	故障预测	Self-modeling	日志分析数据挖掘	Self-healing	FM Framework
[37], [69]		✓	✓			✓			
[46], [71], [72], [74]–[76]	✓								
[57], [70], [77]–[80]		广							
[9], [73], [81], [82]									
[43], [75], [82]			✓						
[54], [62], [63]				✓					
[83]–[93]								✓	
[77], [94], [95]							✓		
[74], [75], [78], [96]					✓				
[42], [70], [76]									
[83], [97], [98]									✓

表四：NVE公司针对各类故障所采取的管理措施

Papers Ref.	环境	附加价值	调频步进
[75]	vIMS VMs	随机森林	故障预测与包含故障注入的训练数据集
[70]	NFV	网络数据过滤	多租户故障隔离技术及NFV数据过滤功能
[97]	OpenStack虚拟机	Rule-based	快速故障检测与恢复，以及向客户发送通知
[78]	VMs	随机森林	积极主动的财务经理
[69]	SDN	BN	Self-modeling
[84]	OpenStack虚拟机	故障转移机制	Self-healing
[85]	SDN控制器	故障转移机制	Self-healing
[87]、[89]和[88]	SDN通道或链接	故障转移机制	Self-healing
[90]	NFV link	故障转移机制	Self-healing
[91]	SFC	故障转移切换机制	Self-healing
[74]	NFV、VIMS、VMware ESXi/vSphere以及Linux/Docker	可靠性基准	在注入故障的情况下测试产品的可靠性、性能及评估其各项指标
[96]	NFV	RNN LSTM	带有故障注入功能的故障预测系统及训练数据集
[92] and [93]	VMs	回滚	Self-healing

在决策过程中，用于网络数据监控的前三层功能可通过开源的Elastic技术栈来实现[94]。

六、讨论

表二和表四总结了包括开源项目在内的各种故障管理相关工作。表三按照不同的故障管理步骤对传统网络与虚拟网络的相关工作进行了分类。可以看出，大多数相关工作仅针对一两个故障管理步骤进行探讨，因为要同时解决所有故障管理问题实在颇具挑战性。最新的研究[69][90][91]倾向于采用自动诊断与自修复技术，同时也使用了开源工具[70][84][98]。此外，一些传统网络中已存在的解决方案，如日志分析、自建模及故障预测技术[37][43][57]，在虚拟网络环境中依然具有重要的应用价值[69][77]。表四列出了针对虚拟网络环境问题的相关研究。可以看出，当前的大多数研究[84][85][87][93]都在提出故障转移机制，而这要归功于虚拟化技术——与物理网络的情况截然不同。在电信网络中，物理功能与虚拟功能很可能会共存，这一现象应当被予以充分考虑。一些关于故障定位的研究[75][78][97]主要关注虚拟层的管理问题；而那些在应用层或进程层发生的、会导致服务警报的故障，则未被纳入研究范围。在虚拟网络环境中，运用机器学习技术并非易事，因为我们必须先将复杂的网络数据转化为适合机器学习算法处理的形式。

例如，如果我们希望检测网络中的故障状态，就需要将日志数据转化为适合机器学习算法处理的格式。在K均值聚类算法中，日志数据需要被转换成具有实际意义的数值。在故障定位相关研究中[75][78]，基于决策树的随机森林算法被广泛使用——因为决策树能够模拟决策及其可能带来的后果，这种建模方式非常直观。此外，由于日志文件属于文本格式，因此也有研究[96]尝试应用更适合处理文本数据的机器学习技术，如LSTM模型。

近期的一些研究采用了自建模与数据过滤技术，旨在克服第IV-B节中提到的故障定位技术的局限性。然而，针对非虚拟化环境中的故障管理相关研究仍在进行中。目前仍存在一些亟待解决的问题，同时也有一些问题尚未得到充分探讨。黑盒机器学习技术在从数据中提取特征以及预测网络状态的后续行为方面表现优异[16]。不过，这些技术所学到的特征应包含那些无法通过现有方法直接获取的知识，同时应避免学习那些能轻易从数据中提取出的信息，例如由网络拓扑结构所决定的各种依赖关系[78]。例如，虚拟机与宿主服务器之间的依赖关系就是显而易见的。此外，在需要实现高精度、细粒度的故障定位时，白盒方法（如贝叶斯网络）能提供更准确的故障解释机制，因为这类方法能够在模型中考虑进程等子组件。

为降低诊断的不确定性，实时自我诊断至关重要。第五节中提出的方法考虑了数据收集或警报关联的时间窗口问题（例如，[75]中提到的15秒时间窗口）。在动态网络环境中，时间窗口的选择可能会影响诊断的准确性，从而导致错误或过时的诊断结果。

七、结论

5G技术的实现依赖于多种架构的共存，其中包括NFV与SDN技术。这两种截然不同却又相互补充的技术共存，带来了诸多新的故障管理问题，而传统方法很难解决这些问题。本文回顾了传统电信网络中常用的故障管理方法与措施，并指出了在NFV网络故障管理中需要重点关注的问题。同时，本文还总结了近期相关研究的成果以及未来的研究方向。

致谢

作者们想要感谢审稿人提出的宝贵意见，以及他们为改进这项调查所付出的努力。同时，他们也要感谢Christian JACQUENET和Ian HAY仔细阅读了调查报告，并提出了建设性的建议。

参考文献

- [1] B. Han, V. Gopalakrishnan, L. Ji, S. Lee, 《网络功能虚拟化：创新面临的挑战与机遇》，《IEEE通信杂志》，第53卷，第2期，第90–97页，2015年2月。
- [2] 电信基础设施项目。访问日期：2019年8月9日。[在线资源]。网址：<https://telecominfraproject.com>
- [3] K. Katsalis, N. Nikaein, E. Schiller, R. Favraud, T. I. Braun, 《5G架构设计模式》，载于2016年IEEE国际通信研讨会论文集，第32–37页。
- [4] NORMA。访问日期：2019年11月8日。[在线资源]。网址：<https://5g-ppp.eu/5g-norma/>
- [5] E. H. Rachid等人（2015年2月）。NGMN联盟5G白皮书：可靠性部分——关于端到端可靠性相关模型与功能的报告V1.0版。访问日期：2019年10月23日。[在线资源]。网址：https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0_01.pdf
- [6] BEREC关于基础设施共享的报告。访问日期：2019年9月8日。[在线资源]。网址：https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8164-berec-report-on-infrastructure-sharing
- [7] R. P. Esteves, L. Z. Granville, R. Boutaba, 《虚拟网络的管理》，《IEEE通信杂志》，第51卷，第7期，第80–88页，2013年7月。
- [8] C. Cérin等人，《当前云解决方案的停机时间统计》，国际云计算弹性工作组报告，2013年。访问日期：2019年10月23日。[在线资源]。网址：<http://iwgcr.org/wp-content/uploads/2013/06/IWGCR-Paris.Ranking-003.2-en.pdf>
- [9] Nagios。访问日期：2019年9月8日。[在线资源]。网址：<https://www.nagios.com/>
- [10] P. C. D. R. Fonseca, E. S. Mota, 《软件定义网络中的故障管理研究》，《IEEE通信调查与教程》，第19卷，第4期，第2284–2321页，2017年第四季度。
- [11] A. S. da Silva, P. Smith, A. Mauthe, A. Schaeffer-Filho, 《软件定义网络中的弹性支持研究》，《计算机网络》，第92卷，第189–207页，2015年12月。
- [12] J. Chen, F. Xu, M. Yin, W. Zhang, 《软件定义网络与容错技术的结合研究》，瑞士尚姆：施普林格国际出版社，2015年，第351–368页。
- [13] K.-T. Foerster, S. Schmid, S. Vissicchio, 《关于软件定义网络持续更新的研究》，《IEEE通信调查与教程》，第21卷，第2期，第1435–1461页，2019年第二季度。
- [14] O. Hohlfeld, J. Kempf, M. Reisslein, S. Schmid, N. Shah, 《软件定义网络的可扩展性问题与解决方案》，《IEEE选择领域通信杂志》，第36卷，第12期，第2595–2602页，2018年12月。
- [15] A. J. Gonzalez, G. Nencioni, A. Kamisinski, B. E. Helvik, 和 P. E. Heegaard, “NFV编排器的可靠性：现状与研究挑战”，IEEE通信调查与教程，第20卷，第4期，页3307–3329，2018年第四季度。
- [16] R. Boutaba等人，“关于网络领域机器学习的全面调查：发展历程、应用场景及研究机遇”，互联网服务应用杂志，第9卷，页16，2018年12月。
- [17] M. A. Alsheikh, S. Lin, D. Niyato, 和 H.-P. Tan, “无线传感器网络中的机器学习：算法、策略与应用”，IEEE通信调查与教程，第16卷，第4期，页1996–2018，2014年第四季度。
- [18] P. V. Klaine, M. A. Imran, O. Onireti, 和 R. D. Souza, “应用于自组织蜂窝网络的机器学习技术调查”，IEEE通信调查与教程，第19卷，第4期，页2392–2431，2017年第四季度。
- [19] J. Xie等人，“应用于软件定义网络(SDN)的机器学习技术调查：研究问题与挑战”，IEEE通信调查与教程，第21卷，第1期，页393–430，2019年第一季度。
- [20] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, 和 S. Uhlig, “软件定义网络：全面调查”，IEEE会议记录，第103卷，第1期，页14–76，2015年1月。
- [21] L. Cui, F. R. Yu, 和 Q. Yan, “当大数据遇上软件定义网络：大数据与SDN的结合”，IEEE网络杂志，第30卷，第1期，页58–65，2016年1/2月。
- [22] 网络功能虚拟化(NFV)；用例，ETSI标准GS NFV 001，2013年。
- [23] M. Mechtri, C. Ghribi, 和 D. Zeghlache, “一种用于服务功能链部署的可扩展算法”，IEEE网络服务管理传输，第13卷，第3期，页533–546，2016年9月。
- [24] B. Yi, X. Wang, K. Li, S. K. Das, 和 M. Huang, “网络功能虚拟化的全面调查”，计算机网络，第133卷，页212–262，2018年3月。
- [25] Clearwater. 访问日期：2019年7月8日。[在线] 可访问地址：<http://www.projectclearwater.org/>
- [26] M. Zimmerman等人. 支持OpenFlow的SDN与网络功能虚拟化，ONF，美国加利福尼亚州门洛帕克，2014年。
- [27] K. Samdanis, X. Costa-Perez, 和 V. Sciancalepore, “从网络共享到多租户服务：5G网络切片代理”，IEEE通信杂志，第54卷，第7期，页32–39，2016年7月。
- [28] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, 和 H. Flinck, “网络切片与软件化：原理、实现技术及解决方案调查”，IEEE通信调查与教程，第20卷，第3期，页2429–2453，2018年第三季度。
- [29] 网络功能虚拟化(NFV)；管理与编排，第1卷，ETSI标准GS NFV-MAN 001，2014年。
- [30] J. Zaytoon 和 S. Lafourche, “离散事件系统故障诊断方法概述”，控制年度评论，第37卷，第2期，页308–320，2013年。
- [31] M. Schoffstall 和 C. Davin, “简单网络管理协议(SNMP)”，IETF, RFC 1157，1990年4月。
- [32] R. Gerhards, 《Syslog协议》，IETF, RFC 5424，2009年3月。
- [33] 《数据元素与交换格式——信息交换中的日期和时间表示方法》，ISO标准8601:2000，2000年。
- [34] M. I. Steinder与A. S. Sethi, 《计算机网络中故障定位技术综述》，《科学计算程序》，第53卷，第2期，第165–194页，2004年。
- [35] S. Russell与P. Norvig, 《一种现代方法》，载于《人工智能》，第25卷。美国新泽西州恩格尔伍德克利夫斯：Prentice-Hall出版社，第27页，1995年。
- [36] L. N. De Barros, M. Lemos, V. Bernal与J. Wainer, 《基于模型的网络通信故障诊断方法》，载于《国际人工智能与分布式信息网络研讨会论文集》，1999年，第57–62页。
- [37] C. Hounkonnou与E. Fabre, 《利用自建模实现自我诊断功能》，载于《第八届国际网络服务管理会议论文集》，2012年，第364–370页。
- [38] I. Ben-Gal, 《贝叶斯网络》。美国新泽西州霍博肯：Wiley出版社，2008年。
- [39] J. Lu、C. Dousson与F. Krief, 《基于因果图的自诊断算法》，载于《第七届国际自主系统会议论文集》，2011年，第146–151页。
- [40] M. Hasan、B. Sugla与R. Viswanathan, 《网络管理事件关联与过滤系统的概念框架》，载于《第六届IFIP/IEEE国际综合网络管理与分布式管理研讨会论文集》。

- [41] R. Boubour, C. Jard, A. Aghasaryan, E. Fabre, 和 A. Benveniste, “基于Petri网的分布式系统故障检测与诊断方法。I. 在电信网络中的应用、研究动机及建模方法,” 收录于《第36届IEEE决策与控制会议论文集》, 第1卷, 1997年12月, 第720–725页。
- [42] P. Varga 和 I. Moldovan, “将服务级监控与故障管理集成, 用于端到端的多供应商以太网服务,” 《IEEE网络服务管理汇刊》, 第4卷, 第1期, 第28–38页, 2007年6月。
- [43] S. R. Tembo, J.-L. Courant, 和 S. Vaton, “一种三层自重构通用模型, 用于电信网络的自我诊断,” 收录于《SAI智能系统会议论文集》, 英国伦敦, 2015年, 第25–34页。doi: 10.1109/IntelliSys.2015.7361080。
- [44] I. Ben-Gal, F. Ruggeri, F. Faltin, 和 R. Kenett, “贝叶斯网络,” 收录于《质量与可靠性统计百科全书》。英国奇切斯特: Wiley出版社, 2007年。
- [45] R. Dechter, 《约束处理》。美国加利福尼亚州旧金山: Morgan Kaufmann出版社, 2003年。
- [46] Y. Mao, F. R. Kschischang, B. Li, 和 S. Pasupathy, “基于因子图的方法, 用于无线传感器网络中的链路损耗监测,” 《IEEE选择领域通信杂志》, 第23卷, 第4期, 第820–829页, 2005年4月。
- [47] D. Lewis, “因果关系,” 《哲学杂志》, 第70卷, 第17期, 第556–567页, 1974年。
- [48] J. Y. Halpern, “对Halpern–Pearl因果关系定义的修改,” 收录于《第24届国际人工智能会议论文集》, 阿根廷布宜诺斯艾利斯, 2015年, 第3022–3033页。[在线] 可获取地址: <http://dl.acm.org/citation.cfm?id=2832581.2832671>
- [49] J. Y. Halpern 和 J. Pearl, “原因与解释: 一种结构化模型方法。第一部分: 原因,” 《英国哲学科学杂志》, 第56卷, 第4期, 第843–887页, 2005年。
- [50] G. Gössler 和 J.-B. Stefani, “并发系统中的故障归因,” 收录于《国际可信全球计算研讨会论文集》, 2015年, 第79–94页。
- [51] P. Laborie 和 J.-P. Krivine, “自动生成事件记录及其在电力分配系统报警处理中的应用,” 收录于《国际诊断原理研讨会论文集》, 1997年, 第61–68页。
- [52] G. Reali 和 L. Monacelli, “NGN IMS网络中故障定位技术的定义与性能评估,” 《IEEE网络服务管理汇刊》, 第6卷, 第2期, 第122–136页, 2009年6月。
- [53] R. N. Cronk, P. H. Callahan, 和 L. Bernstein, “基于规则的专家系统在网络管理与运营中的应用: 简介,” 《IEEE网络杂志》, 第2卷, 第5期, 第7–21页, 1988年9月。
- [54] S. Shankar 和 O. Satyanarayanan, “一种自动分析IP电话网络中故障影响的系统,” 收录于《第10届IEEE/IFIP网络运营与管理研讨会论文集》, 2006年, 第1–4页。
- [55] L. Lewis, “基于案例推理的方法, 用于通信网络中的故障管理,” 收录于《第9届IEEE人工智能应用会议论文集》, 1993年, 第1422–1429页。
- [56] C. Melchior 和 L. M. R. Tarouco, “利用基于案例推理的方法进行计算机网络故障管理: DUMBO系统,” 收录于《国际案例推理会议论文集》, 1999年, 第510–524页。
- [57] G. 赵军与赵伟, “基于主机的系统日志的统计分析与处理”, 载于《第二届国际教育技术计算机科学研讨论文集》, 第2卷, 2010年3月, 第277–280页。
- [58] A. I. Moustapha与R. R. Selmic, “利用改进的循环神经网络对无线传感器网络进行建模: 在故障检测中的应用”, 载于《IEEE国际网络传感与控制会议论文集》, 2007年4月, 第313–318页。
- [59] M. Adda, K. Qader与M. Al-Kasassbeh, “网络流量故障分类中不同聚类技术的比较分析”, 《国际创新研究计算机通信工程杂志》, 第5卷, 第4期, 第6551–6563页, 2017年5月。
- [60] A. Akbari与N. Beikmahdavi, “基于聚类与蜂窝技术的无线传感器网络故障检测与恢复方法”, 载于《第三届ICACTE国际会议论文集》, 2010年, 第148–152页。
- [61] P. Gill, N. Jain与N. Nagappan, “理解数据中心中的网络故障: 测量、分析及其影响”, 《ACM SIGCOMM计算机通信评论》, 第41卷, 第4期, 第350–361页, 2011年。
- [62] A. S. Roque, D. Pohren, T. J. Michelin, C. E. Pereira与E. P. Freitas, “EFT故障对车内网络中关键任务性能的影响分析”, 《IEEE电磁兼容性传输杂志》, 第59卷, 第5期, 第1415–1423页, 2017年10月。
- [63] S. Huang, Z. Deng与S. Fu, “量化软件定义网络中各实体的关键性, 以便进行故障影响分析及提升系统可靠性”, 载于《IEEE第35届国际性能计算与通信会议论文集》, 2016年, 第1–8页。
- [64] J.-P. Vasseur, M. Pickavet与P. Demeester, 《网络恢复技术: 光网络、SONET–SDH网络、IP网络及MPLS网络的防护与恢复措施》。
- [65] T. Hu, Z. Guo, P. Yi, T. Baker, J. Lan, “基于多控制器的软件定义网络: 综述”, 《IEEE Access》, 第6卷, 第15980–15996页, 2018年。
- [66] A. A. Neghabi, N. J. Navimipour, M. Hosseinzadeh, A. Rezaee, “软件定义网络中的负载均衡机制: 系统性的文献综述”, 《IEEE Access》, 第6卷, 第14159–14178页, 2018年。
- [67] C. J. Bernardos等, “网络虚拟化研究面临的挑战”, 互联网工程任务组, 美国加利福尼亚州弗里蒙特市, 互联网草案draft-irrf-nfvrg-gaps-network-virtualization-06, 2017年7月。
- [68] OPNFV博士项目。访问日期: 2019年11月8日。[在线], 网址: <https://wiki.opnfv.org/display/doctor/Doctor+Home>
- [69] J. M. Sánchez-Vilchez, I. G. B. Yahia, N. Crespi, “基于自建模的软件定义网络故障诊断方法”, 载于《IEEE网络与软件会议论文集》, 2015年, 第1–6页。
- [70] S. Cherrared, S. Imadali, E. Fabre, G. Goessler, “LUMEN: 一种适用于网络虚拟化环境的全球性故障管理框架”, 载于《第21届创新云与互联网网络研讨会论文集》, 2018年2月, 第1–8页。
- [71] OpenStack遥测工具。访问日期: 2019年7月8日。[在线], 网址: <https://wiki.openstack.org/wiki/Telemetry>
- [72] OpenStack Monasca。访问日期: 2019年9月8日。[在线], 网址: <http://monasca.io/>
- [73] Zabbix。访问日期: 2019年2月8日。[在线], 网址: <https://www.zabbix.com/>
- [74] D. Cotroneo, L. De Simone, R. Natella, “NFV-bench: 一种用于网络功能虚拟化系统的性能测试工具”, 《IEEE网络服务管理汇刊》, 第14卷, 第4期, 第934–948页, 2017年12月。
- [75] C. Sauvanaud, K. Lazri, M. Kaaniche, K. Kanoun, “虚拟网络功能中的异常检测与根本原因定位方法”, 载于《第27届国际软件可靠性工程研讨会论文集》, 2016年, 第196–206页。
- [76] S. Song, S. Hong, X. Guan, B.-Y. Choi, C. Choi, “NEOD: 一种用于软件定义网络的嵌入式在线灾难管理框架”, 载于《IFIP/IEEE国际综合网络管理研讨会论文集》, 2013年, 第492–498页。
- [77] E. Baseman, S. Blanchard, Z. Li, S. Fu, “利用文本与数值数据的关系合成方法对计算机系统日志进行异常检测”, 载于《第15届IEEE国际机器学习与应用会议论文集》, 2016年12月, 第882–885页。
- [78] J. M. N. Gonzalez, J. A. Jimenez, J. C. D. Lopez, H. A. G. Parada, “利用机器学习与摘要技术对网络故障进行根本原因分析”, 《IEEE通信杂志》, 第55卷, 第9期, 第126–131页, 2017年9月。
- [79] K. Slávícek, J. Ledvinka, M. Javorník, O. Dostál, “对路由器和交换机产生的系统日志信息进行数学处理”, 载于《第4届国际信息自动化与可持续性会议论文集》, 2008年, 第463–468页。
- [80] H. Tsunoda, G. M. Keeni, “系统日志的管理方法”, 载于《第16届亚太地区网络运营与管理研讨会论文集》, 2014年, 第1–4页。
- [81] S. Shengyan, S. Xiaoliu, Z. Jianbao, M. 辛克: “利用多智能体技术研究网络与信息安全系统的系统日志收集与分析模型”, 载于2012年第四届国际多媒体信息网络安全会议论文集, 第23–26页。
- [82] 崔勇、施军、王志: “基于循环时间约束网络模型的计算机网络故障传播推理与诊断方法”, 《IEEE系统、人与控制论学报》, 第47卷第8期, 第1965–1978页, 2017年8月。
- [83] J. M. S. Vilchez, I. G. B. Yahia, N. Crespi, T. Rasheed, D. Siracusa: “具有自修复功能的软件化5G网络弹性机制”, 载于2014年第一届5G普适连接国际会议论文集, 芬兰莱维, 第229–233页。
- [84] F. F. Moghaddam, A. Gherbi, Y. Lemieux: “通过容错多智能体任务调度实现OpenStack应用的自我修复与冗余机制”, 载于2016年IEEE国际云计算技术科学会议论文集, 第572–577页。
- [85] V. Pashkov等: “SDN企业网络中的控制器故障转移技术”, 载于2014年IEEE现代网络技术会议论文集, 第69–74页。
- [86] M. Obadia, M. Bouet, J. Leguay, K. Phemius, L. Iannone: “分布式SDN控制器的故障转移机制”, 载于2014年IEEE网络未来会议论文集, 第1–6页。
- [87] 黄仁浩、唐永昌: “基于SDN的数据中心快速故障转移机制”, 载于2016年IEEE国际计算机研讨会论文集, 第171–176页。
- [88] D. Giatsios, K. Choumas, P. Flegkas, T. Korakis, D. Camps-Mur: “5G传输网络中基于SDN的分片技术及快速故障转移机制”, 载于2017年IEEE欧洲网络与通信会议论文集。

- [89] K. Ko, D. Son, J. Hyun, J. Li, Y. Han, 和 J. W.-K. Hong, “基于SDN的虚拟网络的动态故障转移机制”, 载于2017年IEEE网络与软件会议论文集, 第1–5页。
- [90] O. Soualah, M. Mechtri, C. Ghribi, 和 D. Zeghlache, “虚拟网络功能链路的故障恢复算法”, 载于2017年IFIP/IEEE集成网络服务管理研讨会论文集, 第213–221页。
- [91] S.-I. Lee 和 M.-K. Shin, “服务功能链路的自恢复机制”, 载于2015年IEEE国际信息与通信技术融合会议论文集, 第108–112页。
- [92] L. Cui, Z. Hao, Y. Peng, 和 X. Yun, “Piccolo: 一种用于虚拟机集群的快速高效回滚系统”, 《IEEE并行与分布式系统汇刊》, 第28卷第8期, 第2328–2341页, 2017年8月。
- [93] B. Shi, D. Chen, L. Cui, J. Zheng, 和 B. Li, “Mercurial: 一种用于虚拟机集群的节能型回滚系统”, 载于2014年IEEE/ACM第七届实用云计算国际会议论文集, 美国华盛顿特区, 第877–882页。
- [94] Elastic Stack。访问日期: 2019年9月8日。[在线资源]: <https://www.elastic.co/products/elasticsearch>
- [95] U. S. Hashmi, A. Darbandi, 和 A. Imran, “利用数据挖掘技术分析网络故障日志以实现主动自愈功能”, 载于2017年国际计算机网络与通信会议论文集, 第511–517页。
- [96] L. Zhang, X. Zhu, S. Zhao, 和 D. Xu, “基于长短期记忆神经网络的虚拟网络故障诊断新方法”, 载于2017年IEEE第86届车辆技术会议论文集, 第1–5页。
- [97] Vitrage。访问日期: 2019年8月8日。[在线资源]: <https://wiki.openstack.org/wiki/Vitrage>
- [98] E. Luchian, P. Docolin, 和 V. Dobrota, “利用SNMP技术通过Nagios实现对OpenStack NFV基础设施的先进监控”, 载于2016年第12届IEEE IETC会议论文集, 第51–54页。
- [99] Pacemaker; Cluster Labs。访问日期: 2019年8月11日。[在线资源]: <http://clusterlabs.org/>
- [100] Z. Guo等人, “通过基于负载变化的同步机制提升软件定义网络中的负载均衡性能”, 《计算机网络》, 第68卷, 第95–109页, 2014年8月。
- [101] E. Rozaki, “利用数据挖掘分类器进行网络故障诊断”, 《国际数据挖掘、知识管理与过程杂志》, 第5卷第7期, 第29–40页, 2015年。doi: 10.5121/csit.2015.50703。
- [102] “电信管理网络原则”, 国际电信联盟, 瑞士日内瓦, ITU建议书M.3010, 2000年。



西赫姆·切拉雷德分别于2013年和2015年从阿尔及利亚科学技术大学获得电信与网络专业的学士学位, 以及网络与分布式系统专业的硕士学位(并获得优异成绩)。目前, 她正在法国雷恩第一大学与INRIA及ORANGE实验室联合成立的I/O实验室攻读博士学位。她的主要研究方向是可编程多租户网络的故障管理相关技术, 研究内容涵盖故障管理、网络功能等方面。

虚拟化技术、基于模型的机器学习方法以及根本原因分析技术。



索菲安·伊马达利于2010年从阿尔及利亚高等信息技术学院(前身为INI学院)获得计算机科学与工程学位, 并获得优异成绩; 2011年从法国巴黎第十一大学获得网络与电信领域硕士学位, 同样获得优异成绩; 2015年则从巴黎第十一大学/苏佩莱克大学的通信系统实验室获得计算机科学博士学位。他拥有在学术研究、电信行业以及法国顶尖学校和大学从事教学工作的经验。

在Orange公司, 他目前致力于构建下一代基于云的多租户基础设施, 该基础设施将用于承载5G虚拟网络功能实体。此外, 他还积极参与多项研究课题, 研究内容涵盖5G系统的故障管理机制、分布式系统中的数据一致性问题, 同时密切关注基于云的系统部署的最新趋势及相关技术进展。他近期发表了一些关于5G与云计算技术结合的相关论文, 同时也研究过IPv6协议以及未来互联网中的车联网通信技术。他的研究兴趣包括云计算、故障管理、分布式系统、移动性管理及相关架构、车联网技术, 以及5G技术。



埃里克·法布尔于1990年从巴黎电信理工学院获得信号处理与数字通信专业的学位; 1993年和1994年分别从雷恩第一大学获得数学硕士学位以及通信与信号处理专业的博士学位; 2007年又获得了法国国家信息与自动化研究院的教授资格。他于1996年加入法国国家信息与自动化研究院, 并于2010年被任命为高级研究科学家。他目前的研究方向主要包括大规模分布式/并发系统的管理相关课题。

自动系统建模、机器学习、故障诊断、最优控制以及规划技术。当前这些技术的主要应用领域包括网络管理、智能交通系统以及计算生物学。



格雷戈尔·格斯勒于1998年从格勒诺布尔大学和卡尔斯鲁厄大学获得计算机科学学位, 2001年又从格勒诺布尔大学获得计算机科学博士学位。他目前是INRIA的研究员, 同时担任“Spades”研究团队的负责人。他独自或与他人合作发表了40多篇学术论文, 并获得了2项专利。他的主要研究方向在于开发用于安全嵌入式系统及信息物理系统的形式化方法, 以及开展与故障管理及系统可解释性相关的因果分析研究。



伊门·格里达·本·亚希亚于2008年从居里夫妇大学获得了电信网络领域的博士学位。

她目前就职于法国的Orange Lab Network。作为Orange在未来网络与人工智能领域的专家, 她目前负责领导一系列与网络人工智能相关的研究与前瞻性项目。她工作的最终目标是通过人工智能技术革新网络运维方式, 提升网络的可靠性、灵活性及协同能力。与此同时, 她还与Orange的合作伙伴们紧密合作, 共同推进相关项目的进展。

她提出了多种网络维护解决方案, 包括日志分析、网络指标与关键性能指标的监测机制, 以及故障根源的识别技术。她在软件与可编程网络的自适应管理及认知管理技术领域开展积极的研究工作, 这些技术涵盖了利用人工智能实现服务水平协议管理与故障检测、运用知识管理系统优化管理流程、以及基于用户意图与策略的网络管理方法。目前, 她担任IEEE通信学会网络智能技术分会的主席。她参与了多项欧洲科研项目, 例如“Servery”项目、“FP7 UniverSelf”项目、“H2020 CogNet”项目, 以及当前的“5G SliceNet”项目。她在这些研究领域发表了多篇学术论文, 并在各类工业与学术会议上就网络智能技术及机器学习/深度学习的应用主题进行过演讲。