5G 云化网络中的日志处理与故障诊断技术研究

李妙杏

（宜通世纪科技股份有限公司，广东　广州　510000）

摘要：随着 5G 技术的快速发展，云化网络架构在通信领域的引入迎来了前所未有的灵活性和智能性。然而，这种革命性的网络架构也带来了新的挑战，尤其是在网络运维和故障诊断方面。本文对 5G 云化网络架构进行了一定论述，在此基础上，分别从日志生成与采集、数据存储与管理以及数据分析与挖掘等方面探讨了日志处理技术，并结合 5G 云化网络的特点，分析了基于日志进行故障判断的方法，有助于实现故障的快速排除，进而为 5G 云化网络的安全高效运行提供技术支持。

关键词：5G；云化网络；日志处理；故障诊断

中图分类号：TN929　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2023.32.020

随着 5G 技术的快速发展，云化网络架构在通信行业中正迅速崭露头角。5G 云化网络将传统网络功能虚拟化，使网络变得更加灵活、可扩展和高效。然而，随着网络的复杂性和规模的增加，网络故障和问题的诊断与解决变得越来越复杂。为了确保 5G 网络的高可用性和稳定性，日志处理与故障诊断技术变得至关重要。

1 5G 云化网络架构概述

1.1 5G 云化网络定义

5G 云化网络是一种新兴的网络架构，旨在提供高度灵活和可编程的通信服务。它将传统的硬件网络设备虚拟化，并将网络功能以软件的形式部署在云端服务器上。这一架构的核心思想是将网络资源池化，以便根据需求动态分配，从而实现更高的资源利用率和网络灵活性。5G 云化网络允许运营商和企业在不断变化的市场环境中更快速地部署新服务，提供更高质量的用户体验，并降低运营成本。

1.2 云原生网络架构

云原生网络架构是 5G 云化网络的核心组成部分，它基于云计算和容器化技术，旨在实现网络的高度可扩展性和灵活性。在传统网络中，网络功能通常以专用硬件设备的形式存在，而云原生网络将这些功能以虚拟容器的形式部署在云端服务器上。这种容器化方法使得网络功能可以更快速地部署、伸缩和升级，而且更加灵活，能够适应不同的工作负载需求。云原生网络还支持微服务架构，允许网络功能以模块化方式组合，以适应不同应用场景。这种灵活性和可编程性为 5G 云化网络提供了强大的基础，但也带来了更复杂的网络管理和故障诊断挑战[1]。

2 日志处理技术

2.1 日志生成与采集

（1）网络设备与服务的日志生成

各种网络设备，包括路由器、交换机、防火墙和服务器，都会生成日志数据，记录其运行状态、事件和活动。这些日志数据包含了关键的信息，如性能指标、错误消息、安全事件等，对于监控网络健康和故障诊断至关重要。例如，路由器可能会记录路由表的变化，交换机可能会记录端口状态的变化，服务器可能会记录应用程序的日志信息。同时，5G 网络中的各种服务，如无线通信、边缘计算和虚拟化网络功能，也会产生大量的日志数据。因此，有效地识别、收集和存储这些日志数据对于后续的分析和故障诊断至关重要。

（2）日志采集方法

日志采集是从网络设备和服务中获取日志数据的关键步骤。在 5G 云化网络中，有多种方法可以用于采集日志数据，每种方法都有其适用的场景和优劣势。

首先是使用代理程序或代理设备。这些代理程序可以部署在网络设备或服务器上，负责定期收集和传输日志数据到集中式存储或分析平台。这种方法通常具有高度可控性和定制性，可以根据需求选择采集哪些日志数据，但需要在网络设备上额外部署代理，可能会增加管理复杂性。其次是使用网络协议，如 Syslog 或 SNMP（Simple Network Management Protocol），来实时传输日志数据。Syslog 允许设备将日志消息发送到指定的 Syslog 服务器，而 SNMP 可以用于监控设备的性能和状态。这些协议通常支持标准化的消息格式，以便于统一处理和分析。最后，还可以采用日志文件的方式，将日志数据保存在设备或服务器的本地文件中，然后定期将这些文件传输到中央存储或分析系统。这种方法适用于需要离线分析的场景，但可能会增加存储需求和数据传输成本[2]。

2.2 数据存储与管理

（1）数据库与大数据平台

数据库系统是一种常见的数据存储方式，它具有结构化数据存储和高效查询的优势。在数据库中，日志数据可以以表格形式组织，每个表格包含特定类型的日志信息。这使得查询和检索特定事件或信息变得更加容易，同时数据库系统还提供了数据备份和恢复的机制，以确保数据的可靠性。在 5G 云

化网络中，常用的数据库系统包括关系型数据库（如 MySQL、PostgreSQL）和 NoSQL 数据库（如 MongoDB、Cassandra）。这些数据库系统可以根据具体需求进行选择和配置，以满足日志数据的存储和检索需求。另一方面，大数据平台在处理大规模、非结构化或半结构化数据方面表现出色。大数据平台通常采用分布式架构，可以轻松处理日志数据的实时收集和批处理。这些平台包括 Hadoop、Spark、Kafka 等，它们提供了丰富的数据处理工具和框架，可用于数据清洗、转换、分析和可视化。对于 5G 云化网络中的海量日志数据，大数据平台可以提供更好的处理性能和灵活性，支持实时监控和分析。

（2）数据归档与保留策略

在 5G 云化网络中，数据归档与保留策略决定了日志数据的长期保存和管理方式。不同类型的日志数据可能需要不同的保留周期，以满足合规性要求和故障诊断的需要。

一方面，数据归档是将历史日志数据从主要存储中迁移到长期存储中的过程。这样做可以释放主要存储的空间，同时保留历史数据以供后续查询和分析。归档数据通常存储在较便宜的存储介质上，如磁带或冷存储云服务。归档策略应考虑数据的重要性和访问频率，以确定何时、何种类型的数据应该被归档。

另一方面，数据保留策略涉及确定数据在系统中的保留时间。这可以由法规性要求、合规性要求或组织内部政策来指导。不同类型的数据，如安全日志、性能日志和用户活动日志，可能具有不同的保留要求。例如，合规性法规可能要求某些类型的日志数据保留一定的时间以供审计目的，而其他类型的数据则可以根据需要进行较短时间的保留。

2.3 数据分析与挖掘

（1）日志分析工具和技术

首先是 SIEM（安全信息与事件管理）系统。SIEM 系统可以收集、存储和分析多种来源的日志数据，包括网络设备、操作系统、应用程序等。它们通常具有强大的检测和报警功能，可以及时识别潜在的安全威胁和异常活动。SIEM 系统提供了可视化的仪表板和报告，帮助管理人员更好地理解日志数据中的趋势和模式。其次是日志挖掘，它使用机器学习和数据挖掘算法来发现隐藏在日志数据中的有价值信息。通过分析日志数据中的模式和异常，可以帮助识别潜在的故障和性能问题。日志挖掘技术还可以用于建立预测性模型，以提前预测可能的故障和问题。这种方法对于提高网络的可靠性和效率非常有价值。最后，日志分析工具还包括开源工具和商业工具，如 Elasticsearch、Logstash、Kibana（ELK Stack）、Splunk 等。这些工具提供了丰富的查询和分析功能，可以帮助管理人员快速定位问题并采取相应的措施。

（2）异常检测与模式识别

异常检测旨在识别与正常行为不符的事件或数据点。它可以通过监视日志数据的实时流来识别突发的异常情况，或者通过历史数据分析来发现长期的异常趋势。常用的异常检测方法包括统计方法、机器学习算法和深度学习技术。例如，基于统计的方法可以使用均值和标准差来识别偏离正常范围的数据点，而机器学习算法可以根据历史数据的模式来检测异常。

模式识别则旨在寻找数据中的重复模式或规律。在 5G 云化网络中，这可以用于发现网络性能的周期性波动或规律性事件。模式识别方法通常包括时间序列分析、聚类分析和关联规则挖掘等技术。例如，时间序列分析可以帮助识别网络负载的周期性变化，而关联规则挖掘可以发现不同事件之间的相关性[3]。

3 基于日志进行故障判断的方法

3.1 规则引擎

（1）制定规则来检测特定的日志事件和模式

规则引擎旨在制定一系列规则来检测特定的日志事件和模式。规则引擎的核心思想是事先定义一组规则，这些规则基于经验和专业知识，描述了在正常运行状态下所期望的日志事件和行为。每个规则通常由两部分组成：条件和操作。条件部分定义了触发规则的条件，也就是在哪些情况下规则应该被激活。这些条件可以基于特定的关键词、事件发生的时间、日志的来源等。操作部分则规定了当规则被触发时应该采取的措施，例如生成警报、触发自动化修复操作或记录事件。规则引擎可以根据日志数据应用这些规则，当某个日志事件与规则的条件匹配时，引擎会触发相关操作。

举例来说，考虑一个 5G 云化网络中的规则：如果某个服务器的日志中连续出现三次以上的内存利用率超过 90% 的事件，那么生成一条警报并记录该事件。在这个规则中，条件部分指定了触发条件（内存利用率超过 90% 且连续出现三次以上），操作部分规定了触发操作（生成警报和记录事件）。这样的规则可以帮助及时发现潜在的性能问题或内存泄漏，并采取必要的措施来应对故障。

规则引擎的优势在于它们可以用于实时监测和诊断常见故障，而且配置相对简单。然而，规则引擎也有局限性，即需要人工定义规则，对于复杂、不断变化的网络环境可能需要频繁更新规则。同时，规则引擎难以应对一些新型的、不明显的故障模式，因为它们需要预先定义的规则来进行检测[4]。

3.2 机器学习算法

（1）使用监督学习和无监督学习算法

机器学习算法在基于日志的故障判断中发挥着重要作用，它们能够使用监督学习和无监督学习算法来识别和诊断各种故障模式。

首先，在监督学习中，算法依赖于已标记的训练数据，这些数据包含了历史日志事件以及与这些事件相关的故障或问题的信息。通过分析这些数据，监督学习算法能够学习模式和关联，从而在未来的日志事件中识别类似的故障情况。例如，如果过去的数据显示某个特定的日志模式与服务器崩溃有关，监

督学习算法可以在新的日志数据中检测到相同的模式，并警示管理员或采取自动化措施。

其次，无监督学习算法则不需要预先标记的数据，它们可以自动发现数据中的模式和异常。这对于探测新型故障或不断变化的网络环境非常有用，因为它们可以识别不明显的模式和异常情况。机器学习算法的优势在于它们能够处理大规模的非结构化日志数据，自动学习特征和模式，以及适应不同的故障场景。它们可以在实时或离线模式下运行，具有更高的灵活性和自适应性。

最后，机器学习算法也面临一些挑战，包括数据质量问题、需要大量的训练数据、算法选择和调整等方面的问题。在 5G 云化网络中，选择合适的机器学习算法以及优化其参数配置是至关重要的，以确保故障判断的准确性和性能。

（2）通过历史日志数据训练模型来检测异常和预测故障

机器学习算法在基于日志的故障判断中具有重要的功能，通过历史日志数据的训练，它们可以检测异常并预测潜在的故障。

首先，收集和准备历史日志数据。这些数据可以包括来自各种网络设备和服务的日志事件，例如路由器、交换机、服务器、应用程序等产生的日志信息。这些数据需要经过预处理，包括清洗、去噪声、去重和格式化，以确保数据的质量和一致性。其次，选择适当的机器学习算法。监督学习算法可以用于已知故障模式的检测，而无监督学习算法可以用于探测未知的异常情况。根据具体的问题和数据特点，可以选择合适的算法，如决策树、支持向量机、随机森林、聚类分析、神经网络等。最后，一旦模型训练完成，它可以应用于实时的日志数据流中。当新的日志事件进入系统时，机器学习模型会分析这些事件并进行分类，判断它们是否与已知的故障模式或异常情况相匹配。如果匹配到异常，系统可以触发警报，通知管理员或采取自动化的故障修复措施。

3.3 深度学习技术

（1）利用深度神经网络来处理大规模非结构化日志数据

深度学习技术在基于日志的故障判断中发挥着越来越重要的作用，它利用深度神经网络来处理大规模非结构化日志数据，以实现更高级别的故障诊断和异常检测。深度学习算法通过多层神经网络模拟人脑的学习过程，能够自动提取和学习日志数据中的特征和模式，而无需手动定义规则或特征。这种能力使深度学习算法非常适合处理复杂的、不断变化的网络环境。

深度学习技术的一个关键优势是它们能够处理非结构化数据，如文本日志、图像和时间序列数据。在 5G 云化网络中，日志数据通常包含大量的文本信息，以及时间戳、源地址、目的地址等信息，这些信息可能不易直接分析。深度学习模型能够自动学习文本中的关键词、短语和模式，并将它们与网络事件和故障情况关联起来。这使得深度学习能够发现潜在的、不明显的故障模式，甚至在新的故障类型出现时做出准确的判断。

（2）识别复杂的故障模式和异常情况

深度学习技术在基于日志的故障判断中的独特能力之一是其出色的复杂故障模式和异常情况识别能力。与传统的规则引擎或简单的机器学习方法相比，深度学习模型能够处理更复杂、多样化和不断演化的故障模式，因为它们可以自动学习和提取日志数据中的高级特征和模式。

深度学习中的深度神经网络（DNN）具有多层的隐藏层，可以模拟非常复杂的非线性关系。这使得它们能够识别那些难以用传统方法捕捉的故障模式。例如，在 5G 云化网络中，可能存在由多个因素交互引发的复杂故障，这些因素可能是不同设备之间的相互影响、大规模流量波动、网络拓扑的变化等。深度学习模型能够捕捉到这些复杂的关联性，从而更准确地识别和诊断故障。同时，深度学习技术也能够检测潜在的异常情况，即使这些异常情况不符合传统规则或常规模式。通过对大量历史数据的学习，深度学习模型可以建立对正常行为的复杂模型，从而更容易检测到与正常行为差异较大的异常情况。这对于发现新型故障或未知的威胁非常有用，因为它们不需要先验的规则或模式来检测异常，而是依赖于数据本身的统计分布和模式[5]。

4 结语

综上所述，在 5G 云化网络中，日志处理与故障诊断技术的研究和应用具有重要的实际意义。它们有助于降低维护成本、提高网络性能和用户满意度，从而推动了 5G 网络的快速发展。然而，仍然存在一些挑战，如大数据处理的复杂性、隐私和安全问题以及跨厂家设备的兼容性。因此，未来的研究需要继续探索新的方法和技术，以应对这些挑战，使 5G 云化网络能够更好地满足日益增长的通信需求，进而为云化网络的正常运行提供可靠保障。

参考文献：

[1]陈炜．5G 技术背景下的云化电信网络融合架构[J]．数字通信世界，2022，(10)：54-56.

[2]汪平．5G 技术下的云化电信网络融合架构[J]．电信快报，2021，(06)：8-9，13.

[3]关嘉辉，梁智成，李超然．5G 网络云化重构方案研究[J]．电信工程技术与标准化，2020，33(03)：59-64.

[4]唐路．面向 5G/B5G 的智能云化网络架构探讨[J]．通信电源技术，2020，37(04)：170-171.

[5]袁林，蔡超，黄庠奇．5G 时代云化网络运维转型探讨[J]．邮电设计技术，2019，(12)：12-16.

作者简介：李妙杏（1979-），女，广东四会人，大学本科，工程师，主要从事通信技术研究。