网络服务异常事件告警因果图构造方法

张蕾[1]，靖宇涵[2,3]，何波[2]，戚琦[2]，陈晨[3]，王敬宇[2]
（1. 中国联合网络通信集团有限公司，北京 100033；
2. 北京邮电大学网络与交换技术全国重点实验室，北京 100876；
3. 新讯数字科技有限公司，北京 100091）

摘　要：网络服务系统中，异常事件的发生经常导致系统中产生大量告警事件，形成告警风暴。运维人员需要花费大量的时间和精力从这些告警数据中寻找关键信息、确定异常事件的根源。为了减少运维人员所需处理的告警数量，智能化、自动化地提取告警风暴中的根源告警，基于网络服务告警的传播模式分析，提出了一种告警因果图构造方法，并将其应用于提取异常事件发生时的告警风暴关键信息。实验使用运营商现网管理系统的真实数据集，通过告警风暴摘要提取实验，验证了告警因果图生成的效果，并进行了相关案例的物理意义分析。结果表明，使用告警因果图生成的方式进行告警风暴摘要提取，达到了96%的召回率，保留了绝大部分关键信息。同时，使用该方法对系统产生的告警进行压缩，对较难压缩的告警码的压缩率能够达到66.5%。

关键词：告警压缩；异常事件；告警风暴摘要；因果图；智能运维
中图分类号：TN393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024091

A method of building alarm causality graph for anomaly events in network services

ZHANG Lei[1], JING Yuhan[2,3], HE Bo[2], QI Qi[2], CHEN Chen[3], WANG Jingyu[2]
1. China United Network Communications Group Co., Ltd., Beijing 100033, China
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
3. E-Byte Digital Technology Co., Ltd., Beijing 100191, China

Abstract: In network service systems, the occurrence of anomaly events often leads to a large number of alarm events in the system, forming alarm storms. Operators need to spend a lot of time and effort searching for key information and identifying the root cause of anomaly events from these alarm data. In order to reduce the number of alarms that operators needed to handle, as well as automatically extracted the root alarms in the alarm storm, a method for gener-

收稿日期：2023−12−30；**修回日期：**2024−03−10
通信作者：王敬宇，wangjingyu@bupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62171057，No.62101064，No.62071067，No.62001054）
Foundation Items: The National Natural Science Foundation of China (No.62171057, No.62101064, No.62071067, No.62001054)

ating an alarm causality graph based on the analysis of the propagation mode of network service alarms was proposed , and applied to extract key information of the alarm storm when anomaly events occurred. Real datasets of an operator's online network management system were used in experiments to verify the effect of building the alarm causal graph in extracting the alarm storm abstract. A real-world case was used to analyze the physical significance of this method. The results show that the recall rate of extracting alarm storm summary can reach 96% and the vast majority of key information is retained by using the method of alarm causality graph generation. In addition, the compression rate of alarms using this method can reach 66.5% for alarm codes that are difficult to compress.

Key words: alarm compression, anomaly event, alarm storm summary, causality graph, artificial intelligence for IT operations

0　引言

随着分布式系统架构的普遍应用，网络服务系统的规模愈发庞大，这为工程师的故障诊断带来了挑战，因为使用人工的方式进行系统故障的诊断和核查是费时和烦琐的。因此，运维人员对使用智能化的方式辅助和替代人进行故障诊断的需求愈发强烈。随着智能运维（artificial intelligence for IT operations，AIOps）技术的发展，异常检测[1-2]、告警诊断[3]、故障定位[4]等技术的提出，运维体系的改进和网络服务系统故障的智能化诊断都有了新的思路。

网络服务系统中，告警是监控系统状态的一种关键数据源。工程师收集各种监测数据，并通过指定的规则触发告警。然而，告警发生的数量远大于异常事件发生的次数。由于网络服务系统涉及多个组件，设备数量众多，当系统出现故障时，数分钟内就会汇聚成百上千条报警，形成告警风暴。为了降低告警风暴对系统异常排查的不利影响，相关领域的工程师和研究人员引入的网络服务系统告警诊断流程如图 1 所示，对网络服务系统产生的告警进行压缩和处理，从而为运维人员提供更有价值的故障信息。近年来，告警摘要提取成为热门的告警诊断策略，它通过从异常事件造成的告警风暴中筛选出一部分具有关键信息的告警数据，降低了告警风暴发生时运维人员需要关注的信息总量。告警聚类和告警优先级排序是常用的告警风暴摘要提取手段。告警聚类方法[5-6]能在频率或时间上产生模式相似的告警聚合成簇，但对于聚合后的一组相似告警，较难定位其中具体哪条或哪些告警更为重要。告警优先级排序[7-8]的方法通常需要使用其他方式（人工标注、系统故障记录等）导入训练所需的标签，而不是通过告警本身的产生模式来进行关键告警信息的提取。相对较为丰富的告警数据本身，标签数据通常数量有限且难以获取。

为了分析网络服务系统中的告警数据在系统各个组件上的传播模式，并进一步提取异常事件中具备关键价值的告警信息，本文基于真实系统的长期告警数据开展了研究和实验，以提取不同告警之间长期稳定的因果关系，从而对系统中异常事件导致的大量告警数据进行因果分析和根因诊断。在一套稳定运行的、多组件的网络服务系统中，不同类别的告警之间存在较为固定的因果关系，可以通过历史告警数据进行获取和分析。因此，本文针对如何为整个系统中所有类别告警建立完整的因果图展开研究。一张完整的告警因果图可以从全系统的视角展示异常事件发生时，告警数据在系统中的传播路径。其中，连通子图表示异常事件导致的具有固定模式的告警集合，不同告警之间存在上下游关系，上游告警的出现会导致下游告警的产生。使用告警因果图提取告警风暴中的关键信息，可以为网络服务系统异常事件发生的根本原因分析提供有效的渠道，同时

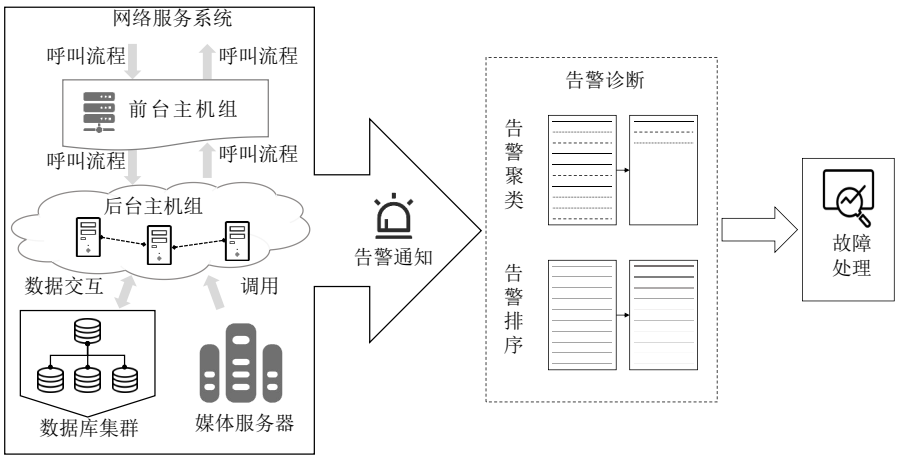


图1　网络服务系统告警诊断流程

不需要依赖大量的人工标注的根因标签。

本文提出了一种基于关联规则的PC算法（Peter-Clark algorithm based on association rules，PC-association）用于网络服务告警因果图的生成。该方法能够从大量长期历史告警数据中抽取数量趋势特征，有效地提取告警之间长期稳定的因果关系，生成表示异常事件发生时告警在系统中传播特征的告警因果图。本文使用PC算法在从中国联通的现网管理系统所收集的数据集上开展实验，生成了系统的告警因果图，并分析了其在告警风暴摘要提取方面的应用和效果。在两套数据集的109次告警风暴中，与运维人员手动标注的告警摘要标签进行比对，PC-association在达到96%的召回率的前提下，将告警码的压缩率降低至66.5%（人工标签的压缩率为52.7%）。

1　相关工作

1.1　网络服务告警诊断

为了减少告警推送数量，降低运维人员维护网络服务系统的资源开销和时间成本，相关研究人员和工程师在诊断服务系统告警方面做出了各种探索。

告警压缩一般指对同类告警的推送数量的压缩，通常是将在一定时间范围的同一类型的告警数据进行压缩。在自动化运维领域，工程师开发了各种告警管理软件和工具处理这类问题，如阿里云服务的CloudMonitor系统、百度智能云监控BCM（Baidu cloud monitor）系统等，都配置了告警合并的相关功能。本文研究的运营商现网管理系统（见第4.1节）中，具备完善的告警码体系，对相同来源和类型的告警作出了唯一标识，使得运维人员不必在内容相同而重复出现的告警上花费额外的精力。

对于不同类型，甚至来源于系统不同组件的告警数据，自动化运维系统仍然没有较好的应对手段，当系统发生较大范围的异常事件时，大量组件同时产生告警，运维人员仍然需要较多时间检查问题的根源，这显然不利于系统异常的快速诊断和恢复。为了进一步降低运维人员所需要检验的告警种类，使用智能化的手段自动对异常事件发生时的告警数据进行分析，以提取其中的关键信息（告警摘要）成为了一种新型的解决方案。随着智能运维技术的发展，研究人员提出了多种不同类型的告警摘要提取方法。文献[5]采用了基于极值理论的异常检测算法检测告警风暴的产生，依据告警产生的频率等特征对告警进行聚类，并使用每一聚类的质心代表此类告警，最终生成告警风暴的摘要信息。

AlertRank 方法[7]使用工单数据为告警记录生成重要性标签，并使用 XGBoost 算法[9]对告警记录进行排序学习，当告警风暴发生时，AlertRank 将重要性排序在前列的告警推荐为告警风暴摘要信息。这种有监督的排序学习可以有效地判断异常事件中更为关键的告警条目，但需要使用关联告警系统的工单数据或者人工标签数据。

CoFlux 方法[10]通过计算系统指标的互相关特性，聚类引发告警的原始关键绩效指标，使得同一聚类中的指标只生成一次告警，从而降低告警生成量。这种方法主要用于指标聚类，并不完全适用于告警关键信息的提取，因为系统中常常还包含大量由指标以外的因素触发的告警。

1.2　关联关系计算

为了有效地度量异常事件发生时网络服务不同的告警之间的关联关系，可以通过计算告警之间的相似性进行分析，这也是告警聚类中常用的手段。文献[11]使用了基于告警属性的形态相似聚类方法。文献[12]使用了告警集合的杰卡德距离（Jaccard distance）衡量告警集合的相似性并进行聚类。但用于计算告警相似度的属性或相关系数[13-14]是对称（无向）的，不能实现对告警间因果（有向）关系的度量。因此本文参考了基于频繁项集挖掘的关联关系[15-16]来建立告警间因果关系的度量。基于频繁项集挖掘的关联关系是数据挖掘的重要基础，经常被用于文本分析等问题。它能够利用项集的产生模式，从数据结构角度给出有关生成条件概率的结论[17]。本文以此作为不同类型告警之间因果关系度量计算的基础，并基于工程实践经验和告警摘要提取实验效果做出了适用于服务告警诊断系统的应用改进。

1.3　因果图的生成

由于网络服务系统中不同组件之间的交互，异常事件会传播到系统中的多个组件，从而产生多种不同类型告警。为了描述告警在整个系统中的传播模式，需要将告警间关联关系的计算扩展到全系统的告警数据。因果图生成技术可以根据一组变量间条件相关性的描述，生成表示变量间整体因果关系的完全有向无环图（complete partially directed acyclic graph，CPDAG）。PC 算法[18]是一种典型的因果分析算法，最早由 Peter 和 Clark 等提出，用于建立表示随机变量间因果关系的因果图。文献[19]描述了典型 PC 算法用于高维有向无环图估计的方案，并提出了将图的骨架扩展到等价类的方法，其前置条件是已知所有随机变量间的条件独立关系。而 rPC 算法[20]则利用长路径对协方差的贡献衰减实现了对 PC 算法的减量，降低了计算复杂度。

2　问题说明

大型网络服务系统通常由多台物理主机或虚拟主机组成分布式结构，其附属的告警系统监控网络服务系统中各个主机的运行状态并收集告警信息。其中，告警码（alarm code）是一种常见的标识告警类型编码。当主机产生告警时，每条告警记录包含告警码信息，相同来源和触发原因的告警具有相同的告警码，因此，本文使用告警码作为研究告警关联关系的基本单位，告警之间关联关系的生成可以转化为告警码之间关联关系的生成。

当网络服务系统出现异常时，出现的告警通常不是独立存在的，而是在所有相关模块上的同一时刻或相近时刻发生。例如，当数据库主机产生告警时，会引发连接该服务器主机的多部后台主机同时产生相关告警。

为了研究网络服务系统告警之间的关系，本节将告警数据和告警之间的关联关系进行了如下描述。

（1）告警码：代表网络服务系统中的告警码，或该告警码对应的全部告警，单个告警码用小写字母表示，如告警码 i，j。告警码集合用大写字母表示，如告警码集 I，J。

（2）告警码的时间序列：按照一定的时间间隔（如每分钟）采集系统中每一个告警码在此间隔内出现的告警频次。将告警码 i 在时间范围 T 内的数量-时间序列记为 $\boldsymbol{X_i}=\{x_1^{(i)}, x_2^{(i)},\cdots, x_t^{(i)}\}$，其中，$t\in T$。

（3）关联规则：表示两个告警码（集）之间的关联关系。关联规则分为“因果”和“相关”，$i\rightarrow j$ 表示告警码 i 是告警码 j 的原因，及告警码 j 是告警码 i 所导致的结果。i-j 表示告警码 i 和告警码 j 之间存在相关关系，相关关系表明告警码 i 与告警码 j 之间的因果关系不能确定方向。

（4）置信度：表示某个关联规则的概率，用 $P(i\rightarrow j)$ 表示。这里特指有向关联关系的置信度，无向的关联关系 i-j 则能够拆解为两个反向的有向关联关系 $i\rightarrow j$ 和 $j\rightarrow i$。

基于告警码之间的关联关系，可以定义告警因果图。告警因果图是一张完全部分有向无环图 $G=(V, E)$，其中，顶点与告警码一一对应，即顶点 $v_i\in V$ 对应告警码 i。告警因果图中的边对应告警码之间的关联关系，即边 $e=(v_i, v_j)\in E$ 对应关联关系 $i\rightarrow j$。

本文研究的重点为从大量历史告警数据中生成告警因果图的方案。结合第 1 节对现有相关工作的总结，告警因果图的生成主要有如下难点。

（1）告警之间的关联关系计算。告警关联规则是生成告警因果图的基础，如何准确计算告警之间的关联关系，使其能够有效地表达告警数据的因果特征，是告警关联关系计算的重要挑战。

（2）从关联规则生成告警因果图。完成任意告警码（集）之间的关联规则计算后，据此生成完整的告警因果图，使告警因果图能够准确表达整个网络服务系统中不同告警码之间的相互关系，是告警因果图生成方法的主要研究目标和挑战。

为了应对这些挑战，本文提出了一种 PC-association 算法，基于告警码的数量-时间曲线，计算不同告警码之间的关联规则，对因果图进行初始化，并使用关联规则的提升度计算因果关系，作为 PC 算法分离集的度量，生成告警因果图，最后对因果图进行定向，消减无向边。在实验部分，本文将告警因果图生成算法用于告警摘要的提取，并与使用聚类方式进行的告警摘要提取进行对比，在真实网络服务系统的数据集上验证效果。

3 模型设计

3.1 基于关联规则的 PC 算法整体结构

PC-association 算法使用历史告警生成告警因果图，PC-association 整体结构及其在告警风暴摘要提取中的应用如图 2 所示。整体结构主要包括 3 个部分：初始化因果图、基于提升度的因果图剪枝、对因果图中无向边的定向。模型需要输入告警码的数量-时间序列，并在初始化因果图部分使用告警码之间关联规则的置信度进行有向边的赋权。其后，在初始化的因果图上基于关联规则的提升度进行因果图的剪枝，去掉冗余的边，生成部分有向的因果图骨架。最后，对因果图中仍存在的无向边进行定向。最终生成一张关于网络服务系统中所有告警码的完全部分有向无环图作为告警因果图。

将因果图生成模型应用于网络服务系统告警风暴的摘要提取，可以将传统的运维人员手动检查异常事件发生时全部系统告警的过程，简化为运维人员检查少量告警风暴摘要的过程。首先，使用历史告警数据生成一张网络服务系统的告警因果图。当系统中出现异常时，使用告警风暴检测算法检出告警风暴，并使用已经生成的告警因果图数据提取告警风暴中的摘要告警。最后，运维人员检查摘要告警数据进行故障排查。使用告警因果图提取告警风暴摘要的细节将在第 4.2 节中描述。

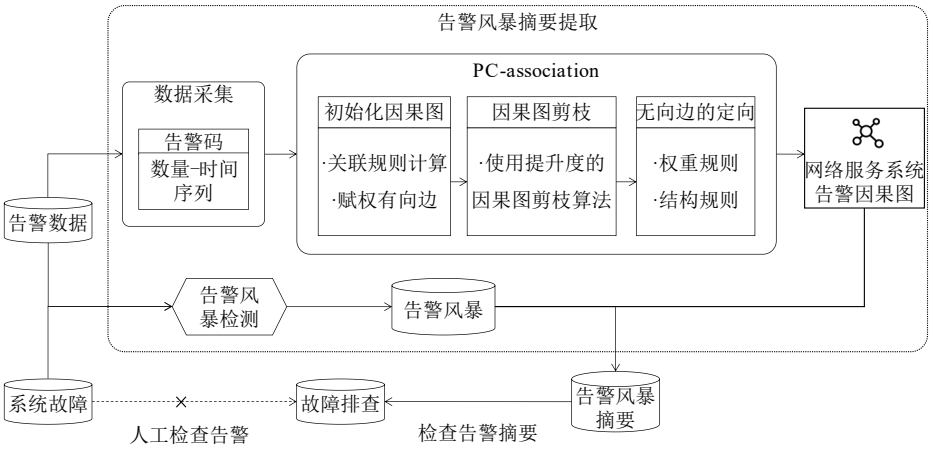


图2　PC-association整体结构及其在告警风暴摘要提取中的应用

3.2　初始化有向因果图

根据第2节的描述，初始化有向因果图的关键是计算告警之间关联规则的置信度。首先根据网络服务系统中告警的特征，参考运维的领域知识和数据实验结论，提出对告警关联和传播的经验性观点。本节以告警码i、j两者之间的关联关系为例，描述告警码之间的传播模式。

观点1　如果告警码i是导致告警码j的原因（之一），则在对应的时间间隔内，在告警码i存在的条件下，告警码j存在的概率较高。

为了便于计算观点1中对应时间间隔内的告警码的存在性，记告警码i、j的时间序列分别为$\boldsymbol{X}_i$、$\boldsymbol{X}_j$。设$\boldsymbol{X}_{i,\,\mathrm{exist}}$为告警码$i$的存在变量，表示告警码在对应的时刻是否存在告警。其中，存在变量取值为1的时刻表示该时刻存在至少1条该告警码对应的告警数据；存在变量取值为0的时刻表示该时刻不存在该告警码对应的告警数据。类似的，$\boldsymbol{X}_{i,\,j,\,\mathrm{exist}}$取值为1的点表示该时刻告警码$i$和$j$同时存在。如式（1）和式（2）所示。

$$\boldsymbol{X}_{i,\mathrm{exist}}=\min\left(X_i,1\right) \tag{1}$$

$$\boldsymbol{X}_{i,j,\mathrm{exist}}=\min\left(\boldsymbol{X}_i,\boldsymbol{X}_j,1\right)\boldsymbol{X}_{i,j,\mathrm{exist}}=\min\left(\boldsymbol{X}_i,\boldsymbol{X}_j,1\right) \tag{2}$$

使用两种或以上告警码的存在变量与其中每种告警码的数量-时间变量进行逐元素相乘，可以方便地过滤出多个告警码在共同出现的时刻的数量关系。式（3）和式（4）中给出了$\boldsymbol{X}_{i,\,\mathrm{masked}}$和$\boldsymbol{X}_{j,\,\mathrm{masked}}$的计算方式，$\boldsymbol{X}_{i,\,\mathrm{masked}}$和$\boldsymbol{X}_{j,\,\mathrm{masked}}$称为告警码$i$和$j$的掩蔽变量，表示在告警码$i$和$j$共同存在的时刻，每个告警码的告警数量。

$$\boldsymbol{X}_{i,\mathrm{masked}}=\min\left(\boldsymbol{X}_i,\boldsymbol{X}_{i,j,\mathrm{exist}}\cdot\max\left(X_i\right)\right) \tag{3}$$

$$\boldsymbol{X}_{j,\mathrm{masked}}=\min\left(\boldsymbol{X}_j,\boldsymbol{X}_{i,j,\mathrm{exist}}\cdot\max\left(X_j\right)\right) \tag{4}$$

由于网络服务系统通常由多台或多组主机组成系统，因此告警在传递的过程中通常不是等量传播。其中，告警码i、j之间的数量关系见观点2。

观点2　如果告警码i导致告警码j，则在对应的时间间隔内，告警码i与i导致的告警码j的数量比值大致是固定的不变量。该不变量对于不同的(i,j)告警码对具有独立的取值，且在系统中维持较长时间的恒定。

根据观点2，按照共同存在的时刻的告警总数规模一致，对告警码i、j进行放缩，如式（5）和式（6）所示，得到放缩后的数量向量$\boldsymbol{X}_{i,\,\mathrm{scaled}}$和$\boldsymbol{X}_{j,\,\mathrm{scaled}}$。

$$\boldsymbol{X}_{i,\mathrm{scaled}}=\frac{\boldsymbol{X}_i\cdot\mathrm{sum}(\boldsymbol{X}_{j,\mathrm{masked}})}{\sqrt{\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{masked}})\cdot\mathrm{sum}(\boldsymbol{X}_{j,\mathrm{masked}})}} \tag{5}$$

$$\boldsymbol{X}_{j,\mathrm{scaled}}=\frac{\boldsymbol{X}_{\boldsymbol{i}}\cdot\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{masked}})}{\sqrt{\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{masked}})\cdot\mathrm{sum}(\boldsymbol{X}_{j,\mathrm{masked}})}} \tag{6}$$

式（7）中的$\mathrm{Freq}(\boldsymbol{X}_i,\boldsymbol{X}_j)$计算告警码$i$、$j$的放

缩后向量在共同存在的时刻的最小值之和，作为告警码i、j共同存在的频次。关联规则$i\rightarrow j$的置信度$P(i\rightarrow j)$以及$j\rightarrow i$的置信度$P(j\rightarrow i)$使用式（8）和式（9）表示。

$$\mathrm{Freq}(\boldsymbol{X}_i,\boldsymbol{X}_j)=\mathrm{sum}(\min(\boldsymbol{X}_{i,\mathrm{scaled}},\boldsymbol{X}_{j,\mathrm{scaled}}))$$

$$\mathrm{Freq}\left(\boldsymbol{X}_i,\boldsymbol{X}_j\right)=\mathrm{sum}(\min(\boldsymbol{X}_{i,\mathrm{scaled}},\boldsymbol{X}_{j,\mathrm{scaled}})) \quad (7)$$

$$P\left(i\rightarrow j\right)=\frac{\mathrm{Freq}(\boldsymbol{X}_i,\boldsymbol{X}_j)}{\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{scaled}})} \quad (8)$$

$$P\left(j\rightarrow i\right)=\frac{\mathrm{Freq}(\boldsymbol{X}_i,\boldsymbol{X}_j)}{\mathrm{sum}(\boldsymbol{X}_{j,\mathrm{scaled}})} \quad (9)$$

如果式（5）中，$\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{masked}})=0$或$\mathrm{sum}(\boldsymbol{X}_{j,\mathrm{masked}})=0$，则应有$P(i\rightarrow j)=0$，$P(j\rightarrow i)=0$。如果$\mathrm{sum}(\boldsymbol{X}_{i,\mathrm{exist}})$低于支持事件阈值$\mathrm{th}_{\mathrm{support_events}}$，则表示数据集中支持关联规则$i\rightarrow j$的样本过少，因此该关联规则在初始化因果图的过程中不应使用。

根据上述任意两个告警码之间关联规则置信度计算方法，PC-association计算全部告警码的两两置信度，并采用大于置信度阈值$\mathrm{th}_{\mathrm{confidence}}$的关联规则初始化因果图。

至此，根据告警关联规则生成了一张初始化的因果图$G_{\mathrm{init}}\leftarrow(V,E)$。

3.3 基于提升度的因果图剪枝

根据第3.2节中描述的方法，使用告警码间的两两因果关系初始化有向的因果图之后，本节主要描述计算告警码之间因果传递关系的方法。初始化的告警因果图可能存在若干组形，如(i,j)、(j,k)和(i,k)形式，可以构成三角形的3条边。如果在排除了告警码j的影响的条件下，告警码i和k没有明显的因果关系，则应从因果图中去除边(i,k)，从而去除因果关系中的三角形。

本节提出了一种改进的PC（Peter-Clark）算法来解决上述问题，该算法在PCpop算法[19]的基础上进行改进，使用关联规则的提升度计算图顶点间的条件因果关系，并对因果图进行剪枝。

在联合高斯分布[19]或带噪声线性结构方程模型[20]建立的因果图中，代表图顶点的变量是来自随机变量的一系列抽样点。与此不同，告警因果图中代表图顶点的告警码的数量-时间曲线只在特定的部分时刻存在非零值，且告警码之间的因果关系更多是通过关联规则而非随机变量的互相关系数进行判断的（见观点1、观点2），这使得告警码之间的条件独立性判断变得困难，因为很难在进行条件因果关系判断时排除中间告警码的影响。因此，本节提出一种使用提升度近似度量条件因果关系的计算方案。

（1）提升度：在本文中，提升度具体指两个关联规则置信度的比值。例如，告警码集S导致告警码集J的置信度，除以告警码集I导致告警码集J的置信度，称为S对I在导致J作用的提升度，记为$\mathrm{Lift}((S\rightarrow J)/(I\rightarrow J))$，提升度的计算式为：

$$\mathrm{Lift}\left(\frac{S\rightarrow J}{I\rightarrow J}\right)=\frac{P(S\rightarrow J)}{P(I\rightarrow J)} \quad (10)$$

$$P\left(I\rightarrow J\right)=P(\sum_{i\in I}^{i}i\rightarrow\sum_{j\in J}^{j}j) \quad (11)$$

式（11）中，$\sum_{i\in I}i$表示求所有$i\in I$的告警码的数量-时间序列之和，得到告警码集I的数量-时间序列。

提升度是一种对条件因果关系基于实验基础上的近似。在已知I与S关联的条件下，如有$\mathrm{Lift}((S\rightarrow J)/(I\rightarrow J))>1$，则认为告警码集$I$导致$J$的因果关系更大概率是通过告警码集$S$传递的。

基于这种理念，本文提出了使用提升度的度量剪去初始化因果图中不直接相关的边，以排除告警因果图中因果传递关系，基于提升度的因果图剪枝过程如算法1所示。

算法1 基于提升度的因果图剪枝

输入 初始化的告警因果图G_{init}，所有告警码的数量-时间序列$\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_i,\cdots,i\in\mathbf{R}$

输出 剪枝后的告警因果图G

初始化$l=-1$，$G=G_{\mathrm{init}}$；

do $l=l+1$；

do 选择一个 G 中（新的）有向边 (v_i,v_j)，其中，$\mathrm{adj}(G,v_i)\setminus\{v_j\}\geqslant l$；

do 选择（新的）$S\subset\mathrm{adj}(G,v_i)\setminus\{v_j\}$，其中，$|S|=l$；

if $\mathrm{Lift}((S\rightarrow\{j\})/(\{i\}\rightarrow\{j\}))>1$ 或（$\mathrm{Lift}((\{j\}\rightarrow S)/(\{i\}\rightarrow\{j\}))>1$ 且 $\mathrm{Lift}((S\rightarrow\{i\})/(\{i\}\rightarrow\{j\}))>1$）**then**；

从 G 中删除边 (v_i, v_j)；

将 S 中的所有顶点存入使边 (v_i, v_j) 分离的分离集 $\mathrm{Sep}(v_i, v_j)$；

end if

until 边 (v_i, v_j) 被删除，或所有的 $S\subset\mathrm{adj}(G,v_i)\setminus\{v_j\}$，其中，$|S|=l$ 已经被选择过；

until 所有的有向边 (v_i, v_j) 被检查过；

until 对于每个有向边 (v_i, v_j)，$\mathrm{adj}(G,v_i)\setminus\{v_j\}<l$。

该算法中，有向边 (v_i, v_j) 的分离（算法 1 第 8 行）独立于有向边 (v_j, v_i) 的分离。有向边 (v_i, v_j) 的分离考虑以下两种结构。

（1）G 中包含边 (v_i, v_j)，且 G 中包含另一条从 v_i 到 v_j 的路径，记为 $v_i\rightarrow V_S\rightarrow v_j$，其中，$V_S$ 表示路径上不包括起点和终点的其他顶点组成的集合。如有 $\mathrm{Lift}((S\rightarrow\{j\})/(\{i\}\rightarrow\{j\}))>1$，则告警码集合 $\{i\}-S\rightarrow\{j\}$ 的间接联系比 $\{i\}\rightarrow\{j\}$ 的直接联系更为紧密，因此分离 (v_i, v_j)。

（2）G 中包含边 (v_i, v_j)，且 G 中包含另一条从 v_j 到 v_i 的路径，记为 $v_j\rightarrow V_S\rightarrow v_i$。如有 $\mathrm{Lift}((\{j\}\rightarrow S)/(\{i\}\rightarrow\{j\}))>1$ 且 $\mathrm{Lift}((S\rightarrow\{i\})/(\{i\}\rightarrow\{j\}))>1$，则告警码集合 $\{j\}-S\rightarrow\{i\}$ 的间接联系比 $\{i\}\rightarrow\{j\}$ 的直接联系更为紧密，因此分离 (v_i, v_j)。

3.4　无向边的定向

基于提升度对因果图进行剪枝后，因果图中仍然存在无向边，为了对这些无向边进行定向，本文参考了文献[21]中用于构建因果图的 4 条结构定向规则。文献[19]中给出了结构定向规则在 PC 算法中的应用方案。使用类似的方式，能够对第 3.3 节中生成的因果图仍然存在的无向边进行定向，将其扩展到完全部分有向无环图。

除了使用文献[21]所提的 4 条结构性定向规则外，本文还使用了关联关系的权重对因果图中的无向边进行定向，并将其定义为权重规则。

规则 1（权重规则）　如果 $P(i\rightarrow j)>P(j\rightarrow i)$，则将 v_i-v_j 定向为 $v_i\rightarrow v_j$。

由于权重规则直接来自对原始告警数据关联关系的有向计算，因此将其置于结构性定向规则之前执行。

4　实验评估

4.1　实验设计

为网络服务系统中的告警码标注完整的因果图对于运维人员来说是相对困难和复杂的，为了验证告警因果图生成的效果及其在异常事件的关键信息提取方面的作用，本文设计了告警风暴摘要推荐实验，以验证因果图生成方法的效果。具体实验设计如下。

（1）采用从通信运营商的在线管理系统（online management system，OMS）中收集的告警数据作为数据源，该网络管理系统主要服务于中国联通的业务控制节点应用服务（service control point application server，SCP_AS）等网络服务系统，能够监控和收集不同网络服务系统的告警，本文从两个使用该 OMS 的服务中收集告警数据。

（2）使用全部原始告警数据，应用本文提出的 PC-association 算法，为每个网络服务系统生成告警因果图。

（3）从原始告警数据中，使用时间序列异常检测模型，如 OneShotSTL[22]、TimesNet[23] 等，检测出若干告警风暴。其中，每个告警风暴至少包含 100 条告警。

（4）请相关运维人员根据对应的异常事件情况标注告警风暴中的摘要告警码集合，用于评估告警风暴摘要推荐的准确性。

（5）在上述告警风暴中，使用（2）中获得的告警因果图，为每个告警风暴映射一个告警因果图的子图，按照第4.2节中描述的方法推荐告警风暴摘要。

（6）将应用PC-association算法推荐的告警摘要与运维人员标注的告警摘要标签进行对比，得到准确性评估结果，并与其他告警风暴摘要算法进行对比实验，从而评估告警因果图生成方法的应用效果。

实验数据集信息见表1。

表1 实验数据集信息

数据集	时间范围	告警数	告警码数	告警风暴数
A	2021年1月15日—2021年3月29日	31 068	63	74
B	2019年6月1日—2020年1月16日	4 503	54	35

4.2 使用告警因果图推荐告警风暴摘要

为每个告警风暴映射一个告警因果图的子图的方式为：选择告警风暴中存在的告警码集R'，使用其对应的顶点集合$V_{R'}$截取告警因果图G_{oriented}的子图G_{storm}。

其后，采用子图G_{storm}中所有入度为0的顶点以及所有只有无向入边的顶点，取对应的告警码集合作为告警风暴摘要。

4.3 算法表现效果的度量

对于数据集中每一次告警风暴，将运维人员标注的摘要告警码集合作为真实标签，设集合RSet使用算法得出的摘要告警码集合为RSet*，RSet*中每包含一个RSet中的告警码，则记为一次真阳性（true positive，TP）；RSet*中每包含一个不在RSet中的告警码，则记为一次假阳性（false positive，FP）；每一个RSet*中的告警码，如果RSet中未包括，则记为一次FN（false negative）。告警风暴摘要的F1-Score（F1分数）采用式（14）计算，F1-Score越高，表示提取出的摘要信息越准确。

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{12}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{13}$$

$$\text{F1-Score}=\frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{14}$$

其中，Precision为精确率，Recall为召回率。

另外，告警码的压缩率也是一个衡量告警摘要提取效果的重要度量。告警摘要算法对告警码的压缩率越低，表示提取出的摘要信息越精简，越有效。本文实验的告警码压缩率定义为：

$$\text{告警码压缩率}=\frac{\text{告警摘要中的告警码数量}}{\text{原始告警码的数量}} \tag{15}$$

4.4 实验设置

本文使用第3节提出的PC-association算法和DBSCAN（density-based spatial clustering of applications with noise）聚类算法、层次聚类算法进行告警风暴的摘要提取，并对比F1-Score和告警码压缩率。

（1）DBSCAN聚类算法。将告警码的数量-时间曲线使用DBSCAN算法进行聚类，将告警码聚类为多个聚类簇，并选择每个聚类簇的质心代表该聚类簇，提取所有簇质心作为告警摘要。

（2）层次聚类算法。将告警码的数量-时间曲线使用层次聚类算法进行聚类，聚类簇的提取和聚类质心的提取与使用DBSCAN聚类的方案相同。

实验参数设置见表2。

表2 实验参数设置

算法	参数	取值
数据采集	采样间隔	1 min
PC-association	支持事件阈值$\text{th}_{\text{support_events}}$	2
	置信度阈值$\text{th}_{\text{confidence}}$	0.6
DBSCAN聚类	距离度量metric	互相关系数
	样本点为邻居的距离上限eps	0.3
层次聚类	距离度量metirc	皮尔森相关系数
	聚类数量n_clusters	45

4.5 实验结果

4.5.1 对比实验结果

本节将PC-association、DBSCAN聚类和层次

聚类算法分别用于数据集A、B的告警风暴摘要提取实验，全数据集实验结果见表3，PC-association、DBSCAN聚类和层次聚类算法在数据集A上的实验结果如图3所示，PC-association、DBSCAN聚类和层次聚类算法在数据集B上的实验结果如图4所示。

本文使用的数据集中，人工标注的告警摘要，告警码压缩率约为52.7%，使用PC-association算法进行告警摘要提取，能够达到66.5%的压缩率，相比于DBSCAN聚类的81.6%和层次聚类的80.6%明显降低。

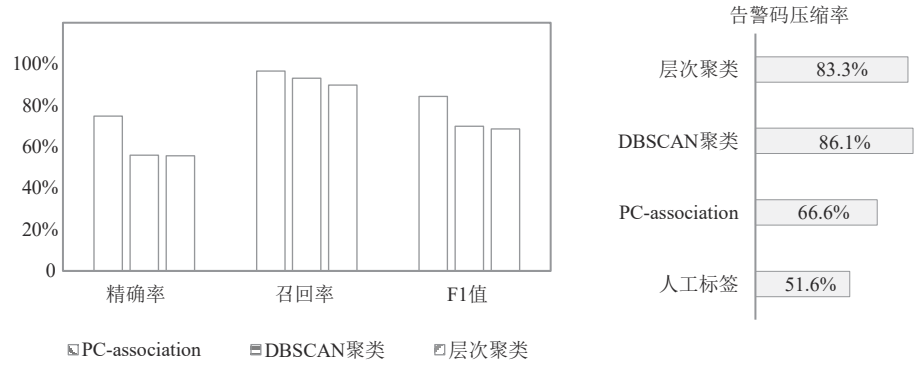
表3　全数据集实验结果

算法	F1值	精确率	召回率	告警码压缩率
PC-association	85.0%	76.2%	96.1%	66.5%
DBSCAN聚类	67.8%	55.8%	86.4%	81.6%
层次聚类	67.6%	55.9%	85.4%	80.6%
人工标签	—	—	—	52.7%

实际生产中，运维人员更关注召回率，PC-association的召回率能够达到96.1%，使用PC-association进行告警摘要提取，对于运维人员所关注的关键信息损失较小，同时能够满足压缩告警码的需求。

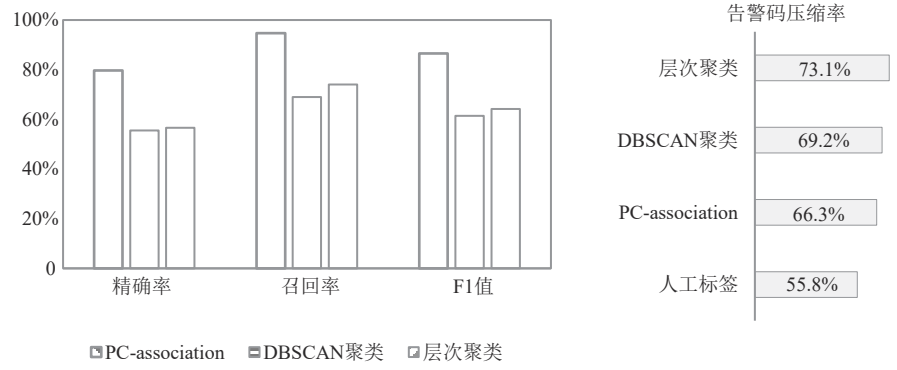
4.5.2　可视化案例

与聚类算法相比，将告警因果图用于告警摘要提取，能够可视化地表达告警码之间的因果关系，给出更加丰富的信息，使运维人员能够参考生成的因果图，更加便捷地判断产生告警的故障在系统中的传播过程。本节使用数据集B中的部分数据，展示PC-association算法的运行结果和在告警风暴摘要提取中的作用。



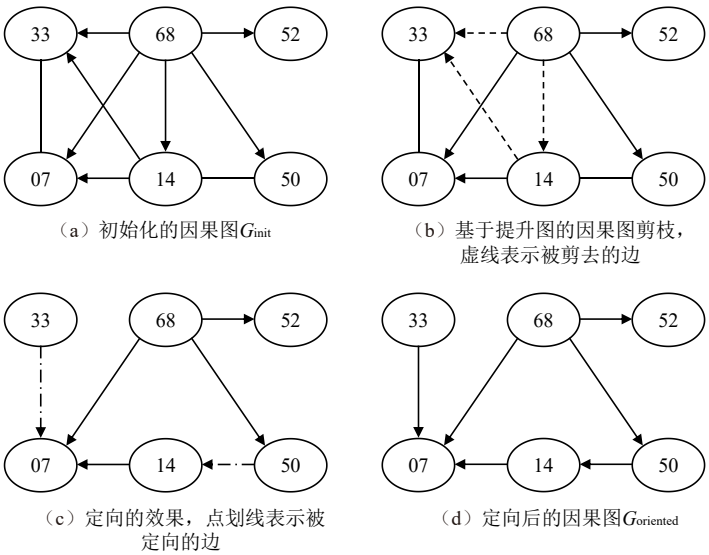
（a）准确性对比　　（b）告警码压缩率对比

图3　PC-association、DBSCAN聚类和层次聚类算法在数据集A上的实验结果



（a）准确性对比　　（b）告警码压缩率对比

图4　PC-association、DBSCAN聚类和层次聚类算法在数据集B上的实验结果



（a）初始化的因果图G_{init}　（b）基于提升图的因果图剪枝，虚线表示被剪去的边

（c）定向的效果，点划线表示被定向的边　（d）定向后的因果图$G_{oriented}$

图5　PC-association应用案例

PC-association应用案例如图5所示，图5为本文在数据集B上建立的告警因果图的一个子图。图5中顶点的数字表示告警码，告警码和告警内容对应关系见表4（告警码和告警内容进行了脱敏）。其中，图5（a）表示按照第3.2节中的方法初始化的因果图，可以看到，在部分起点和终点间存在复数条传递路径，如路径68→07和路径68→14→07等。按照第3.3节所述的方法进行剪枝，得到图5（b）的结果，消除了冗余的路径，因果关系变得更加简洁。图5（c）中，根据第3.4节中描述的定向方法，定向了边33→07和边50→14。最后得到定向后的因果图$G_{oriented}$，如图5（d）所示。

表4　告警码和告警内容对应关系

告警码	告警内容
14	scf（service control function）脱离主循环
33	scf发生重启
68	前台主用socket连接中断
50	同外部网关的链路断开
52	外部网关向平台非法登录
07	日志增长过快

选取2019年6月12日14:34:00—14:36:00的一次告警风暴，告警风暴内包含的告警码集合为{68, 50, 52, 14}，按照第4.2节中的方式，进行告警风暴摘要提取，获得的告警风暴摘要为{68}，这与运维人员标记的告警风暴摘要集合是一致的。结合表4的内容分析，告警风暴发生的主要原因是前台主用socket连接中断，并由此引发了scf脱离主循环的情况，以及同外部网关链路的断开和外部网关向平台非法登录的告警信息，与系统实际的运行状态基本符合。

在网络服务系统的原始告警数据中，每个告警风暴发生时，运维人员平均收到271条告警信息。使用本文提出的PC-association算法后，每个告警风暴发生时，运维人员平均仅收到2.58条压缩后的摘要告警信息，降噪率达到了99%。同时，使用告警因果图进行告警摘要的提取，告警诊断程序可以根据实际需求，为每次告警风暴输出告警因果图的子图，或按需展示网络服务系统中完整的告警因果图，帮助运维人员观测告警风暴发生时系统各个组件告警的传递路径，起到辅助分析系统故障的作用。

5　结束语

网络服务系统中，各个组件产生的告警通常

不是独立的。当系统异常事件发生时，与之相关的多个组件均产生告警，这些告警之间存在着一定的因果关联关系，且在一套稳定运行的系统中，告警之间存在的因果关联保持一定的稳定模式。本文从网络服务系统告警发生和传播的经验规律着手，以在线运行系统中获取的真实告警数据为基础，对告警之间的因果关系进行了实证研究，并提出了一种网络服务系统中异常事件告警因果图的生成方法。使用运营商现网管理系统的告警数据进行了告警风暴摘要提取实验，并与其他告警诊断方法进行了对比，实验证明该方法提取的告警风暴摘要更加准确和简洁。

参考文献：

[1] 戚琦, 申润业, 王敬宇. GAD:基于拓扑感知的时间序列异常检测[J]. 通信学报, 2020, 41(6): 152-160.
QI Q, SHEN R Y, WANG J Y. GAD: topology-aware time series anomaly detection[J]. Journal on Communications, 2020, 41(6): 152-160.

[2] 周雪峰, 徐强, 谭艳婷, 等. 基于改进灰色聚类算法的云架构数据中心网络异常流量过滤算法[J]. 电信科学, 2023, 39(7): 90-98.
ZHOU X F, XU Q, TAN Y T, et al. Cloud architecture data center network abnormal traffic filtering algorithm based on improved grey clustering algorithm[J]. Telecommunications Science, 2023, 39(7): 90-98.

[3] 曹祺. 基于开关量信息的电网故障诊断及保护告警方法研究[D]. 北京:华北电力大学(北京), 2023.
CAO Q. Research on fault diagnosis and protection alarm method based on switch quantity information in power grid[D]. Beijing: North China Electric Power University (Beijing), 2023.

[4] 杨敏. 5G 支撑网告警数据的故障定位方法[J]. 移动通信, 2022, 46(12): 120-128.
YANG M. Fault location method for alarm data of 5G supporting network[J]. Mobile Communications, 2022, 46(12): 120-128.

[5] ZHAO N, CHEN J, PENG X, et al. Understanding and handling alert storm for online service systems [C]//Proceedings of the 42nd International Conference on Software Engineering, Software Engineering in Practice. New York: ACM Press, 2020: 162-171.

[6] 刘波, 万维威, 邹大均, 等. 基于聚类算法的电网告警数据分析与处理模型[J]. 通信技术, 2023, 56(7): 915-922.
LIU B, WAN W W, ZOU D J, et al. Analysis and processing model of power grid alarm data based on clustering algorithm[J]. Communications Technology, 2023, 56(7): 915-922.

[7] ZHAO N W, JIN P S, WANG L X, et al. Automatically and adaptively identifying severe alerts for online service systems [C]//Proceedings of the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 2420-2429.

[8] GARCIA A J, TORIL M, OLIVER P, et al. Automatic alarm prioritization by data mining for fault management in cellular networks[J]. Expert Systems with Applications, 2020, 158:113526.

[9] CHEN T Q, GUESTRIN C. XGBoost: a scalable tree boosting system[C]//Proceedings of the Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2016: 785-794.

[10] SU Y, ZHAO Y J, XIA W T, et al. CoFlux: robustly correlating KPIs by fluctuations for service troubleshooting[C]//Proceedings of the 2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS). Piscataway: IEEE Press, 2019: 1-10.

[11] LIU S G, XIE J, ZHAO Z C, et al. Extraction method of alarm transaction based on morphology similarity clustering[C]//Proceedings of the 2019 IEEE 15th International Conference on Control and Automation (ICCA). Piscataway: IEEE Press, 2019: 917-921.

[12] FAHIMIPIREHGALIN M, WEISS I, VOGEL-HEUSER B. Causal inference in industrial alarm data by timely clustered alarms and transfer entropy[C]//Proceedings of the 2020 European Control Conference (ECC). Piscataway: IEEE Press, 2020: 2056-2061.

[13] MELNYCHUK O, BEKHTA I, TKACHIVSKA M. Pearson correlation coefficient in studying the meaning of a literary[C]// Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems. Kharkiv, Ukraine: CEUR-WS.org, 2023: 460-477.

[14] SALLER D, KUMOVA B I, HENNEBOLD C. Detecting Causalities in Production Environments Using Time Lag Identification with Cross-Correlation in Production State Time Series [C]///Proceedings of the Artificial Intelligence and Soft Computing-19th International Conference. Zakopane, Poland: Springer, 2020: 243-252.

[15] 丁宏, 周宏林. 基于机器学习的通信网告警关联分析综述[J]. 东方电气评论, 2021, 35(1): 77-84, 88.
DING H, ZHOU H L. Survey of alarm correlation analysis for communication networks based on machine learning[J]. Dongfang Electric Review, 2021, 35(1): 77-84, 88.

[16] 毛伊敏,邓千虎,陈志刚. 基于信息熵与遗传算法的并行关联规则增量挖掘算法[J]. 通信学报, 2021, 42(5): 122-136.
MAO Y M, DENG Q H, CHEN Z G. Parallel association rules incremental mining algorithm based on information entropy

and genetic algorithm[J]. Journal on Communications, 2021, 42(5): 122-136.

[17] 闫利霞, 凌兴宏, 尼洪涛. 基于Apriori算法的混合型数据频繁项集挖掘算法[J]. 计算机仿真, 2023, 40(12): 538-542.
YAN L X, LING X H, NI H T. Hybrid data frequent itemset mining algorithm based on Apriori algorithm[J]. Computer Simulation, 2023, 40(12): 538-542.

[18] SPIRTES P, GLYMOUR C. An algorithm for fast recovery of sparse causal graphs[J]. Social Science Computer Review, 1991, 9(1): 62-72.

[19] KALISCH M, BÜHLMANN P. Estimating high-dimensional directed acyclic graphs with the PC-algorithm[J]. Journal of Machine Learning Research, 2007, 8: 613-636.

[20] SONDHI A, SHOJAIE A. The reduced PC-algorithm: improved causal structure learning in large random networks[J]. Journal of Machine Learning Research, 2019, 20(164): 1-31.

[21] MEEK C. Causal inference and causal explanation with background knowledge[C]// Proceedings of the Eleventh Annual Conference on Uncertainty in Artificial Intelligence. New York: ACM Press, 1995: 403-410.

[22] HE X, LI Y, TAN J, et al. OneShotSTL: one-shot seasonal-trend decomposition for online time series anomaly detection and forecasting[J]. Proceedings of the VLDB Endowment, 2023, 16(6): 1399-1412.

[23] WU H, HU T, LIU Y, et al. TimesNet: temporal 2D-variation modeling for general time series analysis[C]// Proceedings of the Eleventh International Conference on Learning Representations (ICLR), Kigali, Rwanda: OpenReview.net, 2023: 1-5.

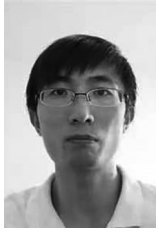
[作者简介]

张蕾（1978– ），女，中国联合网络通信集团有限公司高级工程师，主要研究方向为通信网络、云网融合、人工智能等。

靖宇涵（1995– ），女，北京邮电大学网络与交换技术全国重点实验室博士生，新讯数字科技有限公司技术专家，主要研究方向为AIOps、时间序列分析、异常检测和故障定位。

何波（1995– ），男，博士，北京邮电大学网络与交换技术全国重点实验室博士后研究员，主要研究方向为5G/6G网络、多路径网络、集体通信、传输控制和深度强化学习。

戚琦（1982– ），女，博士，北京邮电大学网络与交换技术全国重点实验室教授、博士生导师，主要研究方向为智能边缘计算、轻量级神经网络、业务网络智能化等。



陈晨（1986– ），男，新讯数字科技有限公司架构师，主要研究方向为智能运维、大语言模型、数字人关键技术的应用。

王敬宇（1978– ），男，博士，北京邮电大学网络与交换技术全国重点实验室教授、博士生导师，主要研究方向为智能网络、人工智能、多媒体通信。