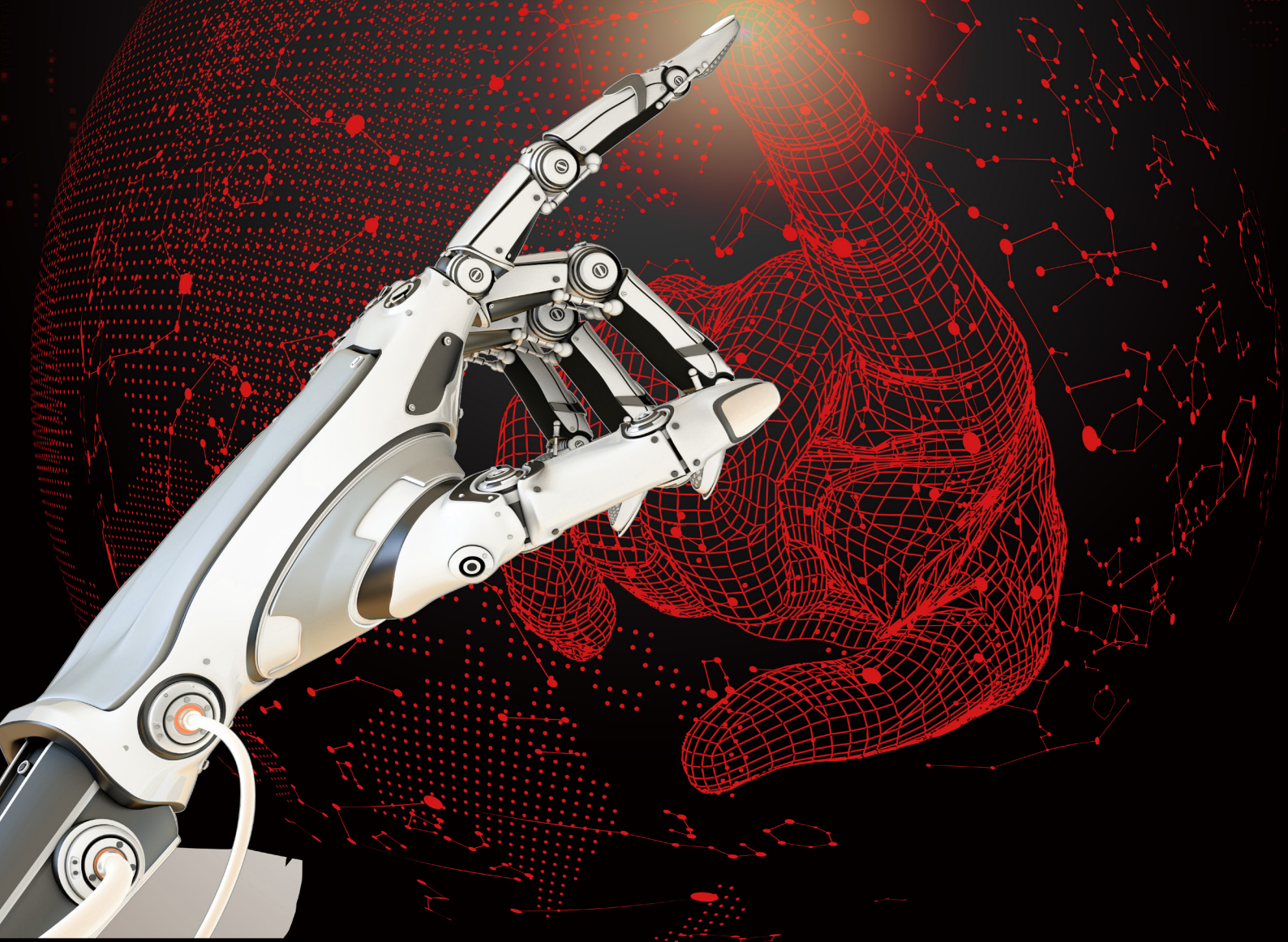
AI in Network智能自治网络在网络维护监控中的应用

——跨域智能告警根因分析



AI in Network智能自治网络在网络维护监控中的应用

跨域智能告警根因分析

【场景描述】

随着网络技术的不断发展，网络结构日趋复杂，网络运维排障的难度随之增大。发生故障后，传统的方式通常依靠人工根据经验及预设的检验规则对告警进行逐一排查和分析，费时费力，对于复杂情况，还需多部门协同处理，定位效率低、耗时长。在5G时代新型分层解耦网络架构下，这种处理方式的瓶颈就更加突出，既有规则或将不适应新型网络，监控告警的数量也将成倍增加，网络故障管理面临极大挑战。因此，亟需引入先进的技术方法，实现故障根因的快速定位和告警收敛，从而提升运维效率、保障运行质量、降低运营成本。

【技术方案概述】

本案例引入AI算法进行告警根因分析，基本思路是不依赖人工介入，通过分析大量的历史告警信息，并结合资源数据、拓扑数据进行分析建模，实现告警RCA规则动态挖掘，从而支撑故障快速定位，逐步积累运维知识库。相关流程如下：

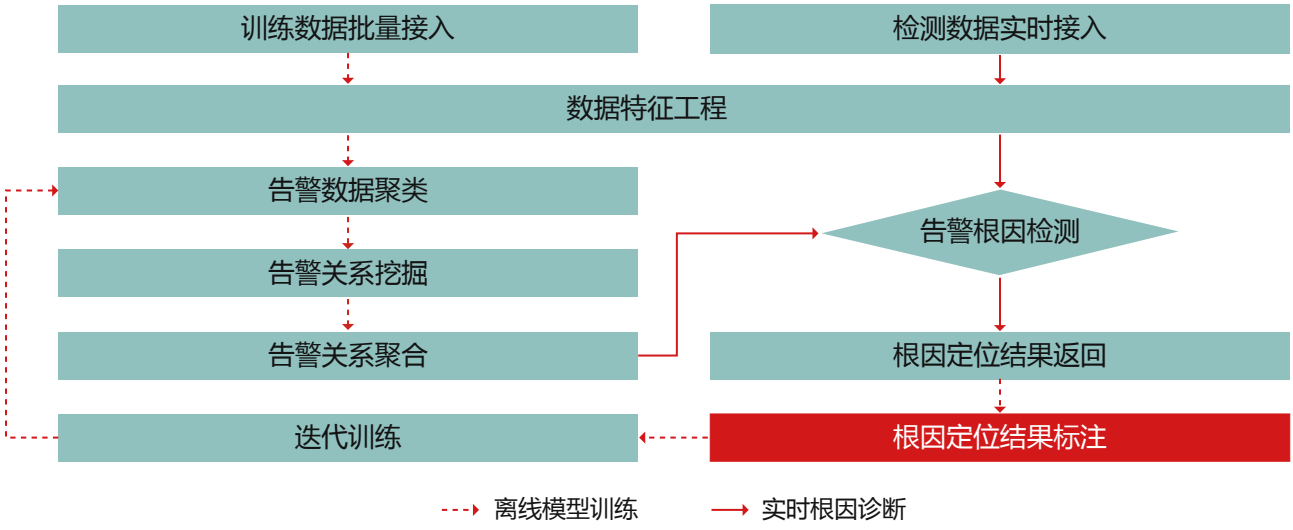


图1　智能告警根因分析流程

数据接入

告警根因分析模型训练过程中，以文件方式批量接入数据集，主要包括两类，一类是告警数据，一类是资源、拓扑信息。前者通常包括告警明细和相关信息维表，关联后参与训练的数据集至少包括告警主体及对应告警类型、告警发生时间等。后者类型较多，可包括网络拓扑、系统部署关系、服务调用关系等，旨在通过解析和处理，构建告警主体之间的空间联系。

告警根因实时诊断流程，则基于实时告警信息，以消息、API等方式发起根因诊断请求。

数据特征工程

对于智能告警根因分析方案来讲，特征工程除了数据解析、缺失值处理等常规动作外，需重点处理：1）过滤恢复告警和手工清除告警等不需参与训练的数据；2）各类拓扑信息解析后，基于主键进行串接，构建告警主体间拓扑关系图，并根据是否存在连接关系进行子图划分。

告警数据聚类

告警数据聚类是告警关联关系挖掘的基础。聚类算法方面，从聚类效果、调参难度、运行速度等维度综合比较，DBSCAN, HDBSCAN, OPTICS, Birch, Agglomerative, GMM等算法中优选。

聚类维度方面，将综合考虑时间维度和空间维度；其中，时间维度指根据告警数据的首次发生时间进行聚类；空间维度指根据告警主体在拓扑关系子图划分后的空间距离大小进行聚类。

告警关系挖掘

基于聚类划分结果，进一步采用关联挖掘算法寻找告警之间的关联关系。本方案将每个聚类结果划为一个项目集，根据大量的项目集，进行二元告警数据之间的关联关系挖掘，并根据支持度和提升度等指标进行结果过滤，根据置信度进一步判断告警数据对之间的主次关系。

告警关系聚合

在关联关系挖掘得到的二元主次告警依赖表基础上，需对告警数据关系进一步聚合，生成告警关系网，以支持实时告警根因检测等场景需求。

告警根因检测

告警根因检测时，基于告警关系网，在一定的时间窗口内，从实时告警信息中诊断定位根因告警并及时干预处置。

结果标注及迭代训练

为了保障模型的定位效果，生产中，需要周期性发起增量训练任务。同时，运维人员也可根据经验和实际情况对定位的根因告警进行异常标注并反馈，系统自动将标注数据纳入下一次迭代训练。

【应用效果】

针对上述跨域智能告警根因分析方案，结合某省运营商云管平台的告警数据进行了主次告警依赖分析测试，并进行了算法的验证和调优，挖掘网络设备、主机、数据库、中间件、大数据组件、DCOS的告警潜在关系，情况如下：

- 样本接入：3个月告警数据，DCN网段表以及各类主体拓扑关系表
- 算法选型：DBSCAN，Birch，Apriori，FP-growth等
- 告警关系挖掘：在限制告警数据依赖关系置信度阈值的情况下，共计挖掘出200条关系，经专家组验证，准确率在60%以上。根据主次关系表，在实验室生成的告警关系网局部示意如下，其中圈起的四个点为可能的根因节点，可据此进行在线告警根因实时检测。

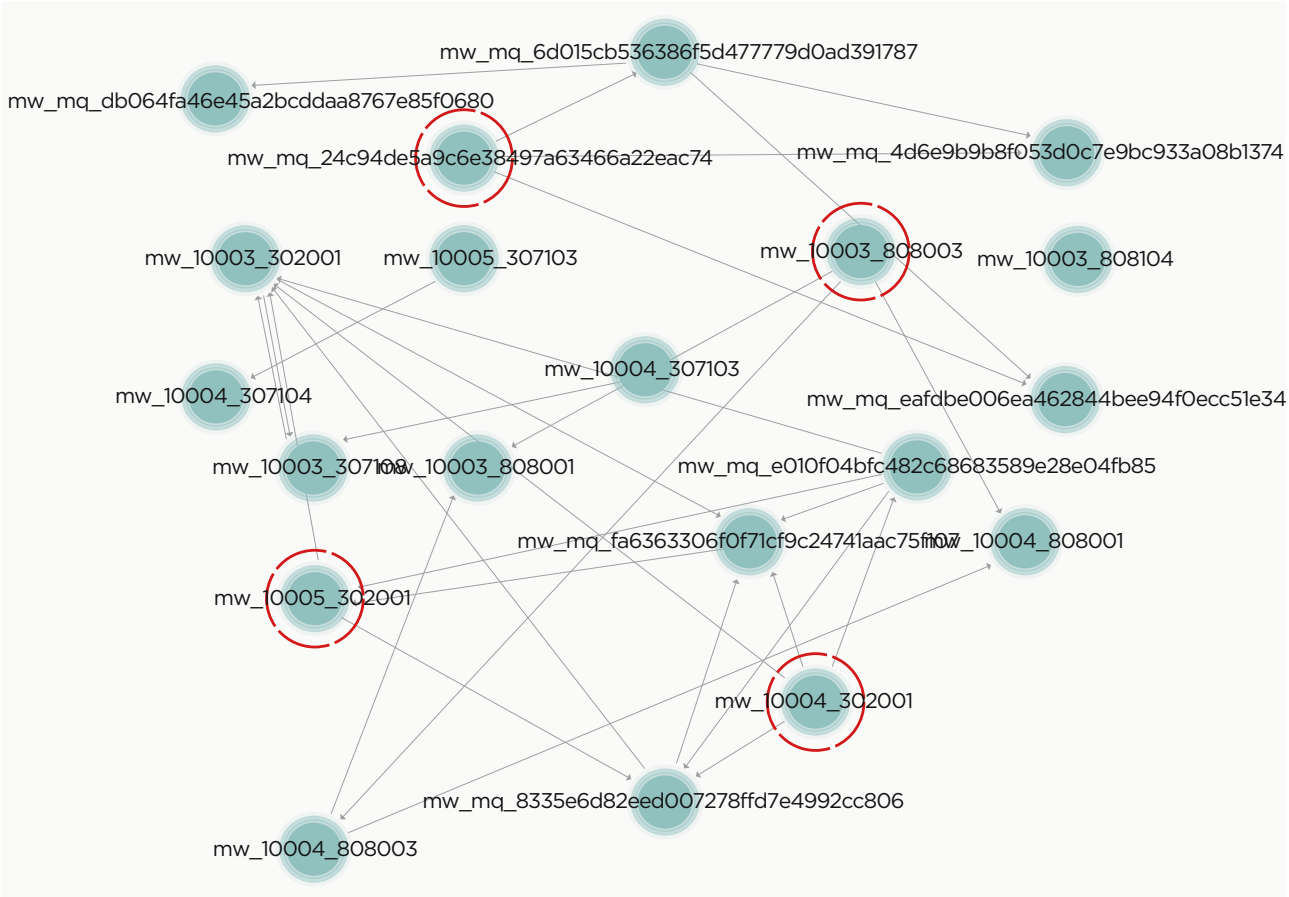


图2　告警关系示意图

【下一步工作建议】

为了更准确进行空间维度聚类，避免不相关数据的相互干扰，建议进一步加强资源数据的标准化工作，即督促各系统进一步完善告警相关主体的网络拓扑、部署信息和调用关系等资源数据，同时，规范告警主体拓扑关系的数据接口标准，以进一步提高方案落地时对不同场景的适配性，降低定制开发改造工作量。

同时，上述方案尚未在5G场景下进行测试，后续需结合切片运维等实际数据优化和调整特征工程的处理逻辑和步骤，以期本方案能够切实支撑面向切片的跨层跨域告警分析和故障诊断等5G网络运维需求。