AIOps Challenge 智能运维挑战赛

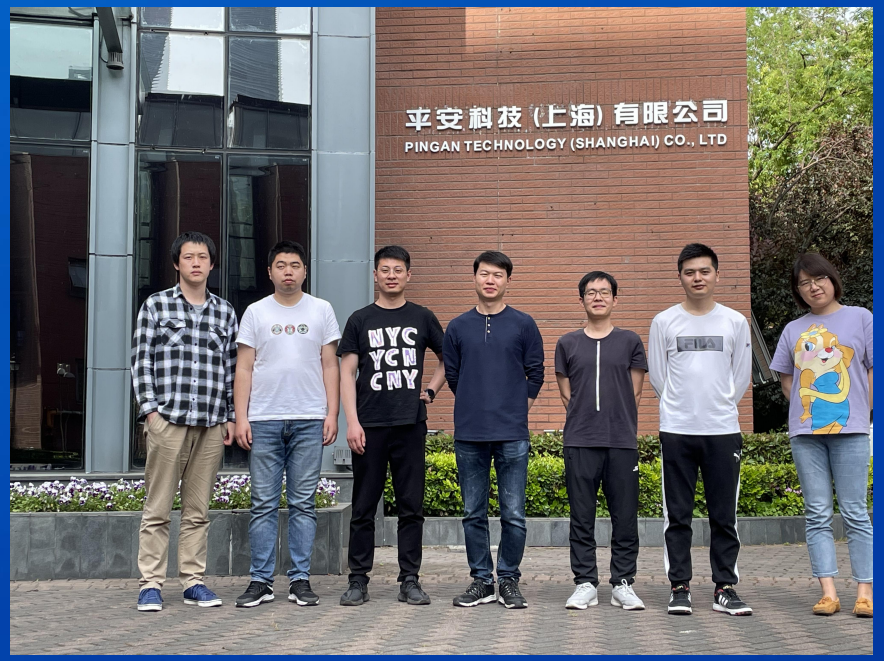
2021国际AIOps挑战赛决赛
暨AIOps创新高峰论坛

金融领域应用系统的故障检测与根因定位

参赛队伍：pa_tech(平安科技)

答辩选手：陈桢博

平安科技运营工具平台团队&平安科技混合增强算法团队介绍



团队简介

负责平安集团AIOPS建设，以全链路监控和业务数据为基础，大数据分析处理和机器学习等技术为支撑，为现有运维管理工具和管理体系赋予统一数据管控能力和智能化数据分析能力，全面提升运维管理效率。

目前已实现异常检测、根因分析、智能预测等三大场景的数据平台和AI模型建设和落地。

第一章节

赛题分析

赛题分析-典型运维场景根因分析，包含两大挑战

AIOps Challenge 智能运维挑战赛 | 科创会 NIICON

赛题解析

- Kafka实时推送监控数据
- 算法实时分析数据
- 发现故障则预测根因报出

图1. 根因定位流程

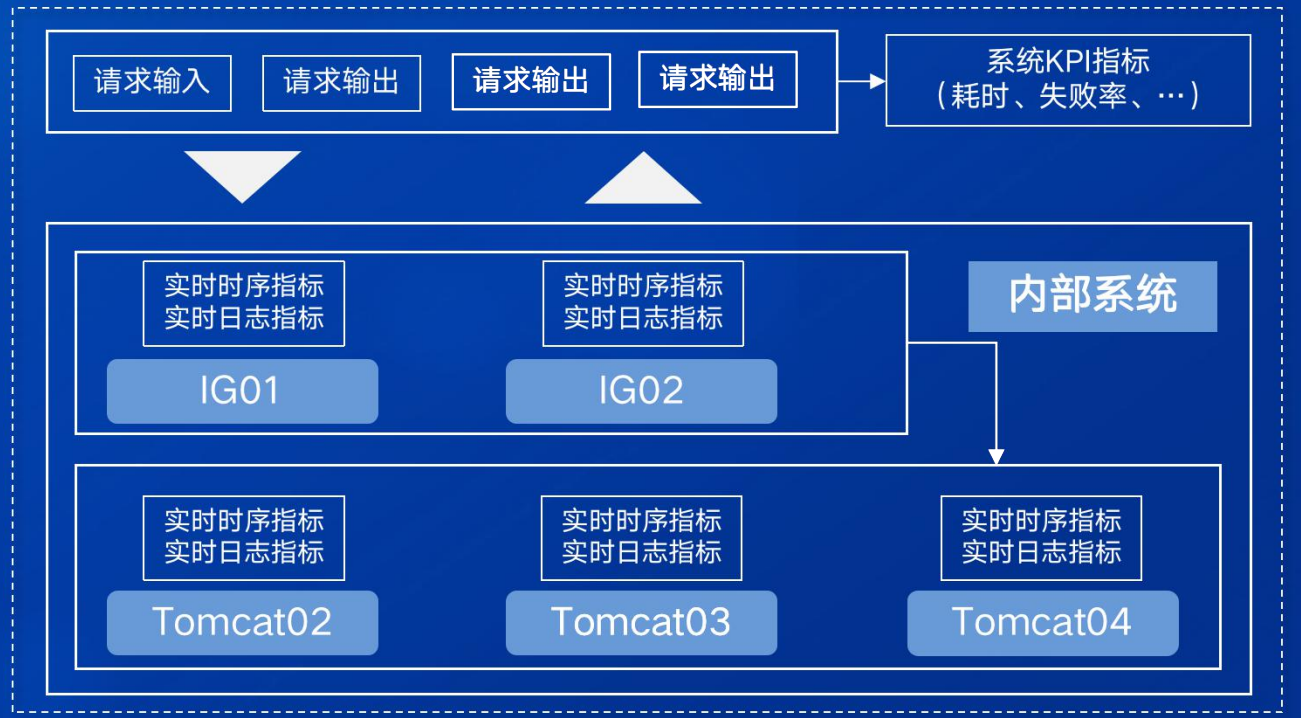


图2. 调用链路简化示意图

挑战1：Trace数据差异

- 系统A、B的trace数据存在差异，需研发通用化方法；

挑战2：历史数据不足

- 历史数据不足，需针对性改进异常检测与根因分析方法

第二章节

方案阐述

01 异常检测

02 故障触发

03 根因分析

异常检测-创新性：通过Bayes方法为各种业务属性的指标动态估计阈值

痛点分析

- 痛点： 固定超参+标准化异常检测模型方案（各指标用的模型和超参数相同），**无法适配各种指标特性。**

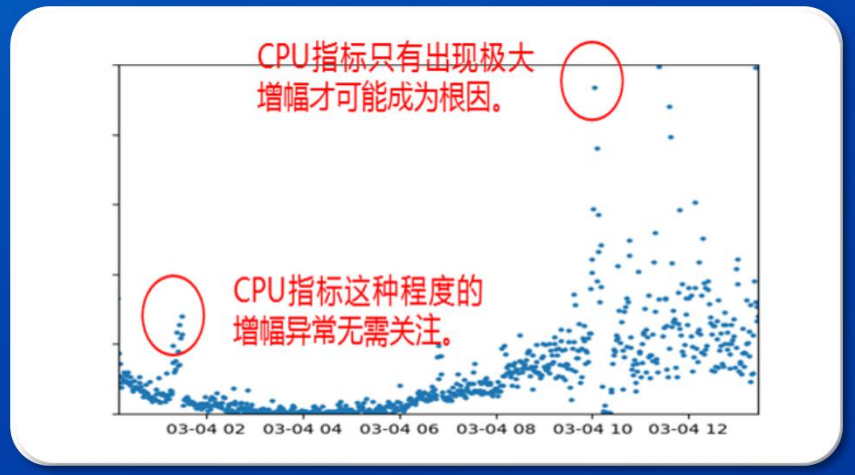


图3. 异常检测痛点图示

解决方案

- ✓ 解决方案：用Bayes方法，结合历史标注动态估计各类指标异常性。

$$P(Y = \text{abnormal} \mid X, \sigma, W)$$

$$P(W = \text{magnitude} \mid X, \sigma, Y)$$

构建观测值X，涨幅W，与异常性Y的概率估计关系，以此计算阈值的边界，从而将指标特性加入模型的阈值估计中。

优势阐述

- ◆ 相比N-Sigma等传统异常检测算法具备以下优势：

1. 在传统时间序列的基础上，**引入故障标注结果**，使其对理论上的正常波形的估计更加准确；
2. **新方法确定临界值可自适应指标异常敏感性**，减少误告、漏告概率。

• 参考文献：时间序列异常值探测的 Bayes 方法及其 GNSS 数据质量控制中的应用、Bayesian methods for outliers detection in GNSS time series

异常检测-通用性：能够泛化至各种数据场景下的通用方案

AIOps Challenge 智能运维挑战赛 | 科创会 NIICON

当前短时数据

指标关联分析 → Bayes异常探测方法 → 阈值=分位数Q*F(涨幅/降幅)

$$\frac{\sum (X_t - \bar{X}_t)(Y_{t+n} - \bar{Y}_{t+n})}{\sum (X_t - \bar{X}_t)^2 (Y_{t+n} - \bar{Y}_{t+n})^2}$$

$$w_j = \xi_j^2$$

$$\{\delta_j [(x_j - \sum_{i=1}^{p} \varphi_i z_{j-i}) + \sum_{t=j+1}^{T} \varphi_{i-j} (\sum_{i=1}^{p} \varphi_i x^*_{t-i} - x^*_t)] + \mu\}$$

历史长期数据（如果可用）

时序预处理 → 异常检测算法 → 确定数据分布阈值边界

时序预处理，例如去除outlier处理，或者对周期性指标进行STL时序分解。

采用S-H-ESD等算法，为历史数据分布范围、统计特性计算相应阈值。

若当前值同时不满足两种阈值

连续k次异常的metric记录异常

故障时Metirc异常数量的下5%分位数，作为连续异常数量阈值

- 算法整体泛化性能较高，可适应不同粒度、长度、特点的观测数据，从而延伸至各种业务场景；
- Bayes方案不仅能保证精度，而且在线上过程中仅需输入较少数据即可快速完成预测。

故障触发：将相关数据缓存以便实时触发根因分析

01 时序异常检测结果

时间序列异常检测的告警记录，即若干告警的cmdb组件及其metric。

02 日志异常检测结果

日志分析异常检测的告警记录，包含异常cmdb组件与指标。

03 系统KPI时序值

系统服务KPI时序值，用于触发根因分析条件（后续弃用）。

04 链路数据

Kafka推送的trace数据按id进行整合，当trace完整且trace耗时高于预设值（低于该值则没有分析的必要）则将其缓存。

- 数据将缓存在Detector类中，准备随时触发根因分析，并定时将无用的历史数据删除。

故障触发-实用性：分析缓存数据，避免以KPI作为触发条件导致漏告

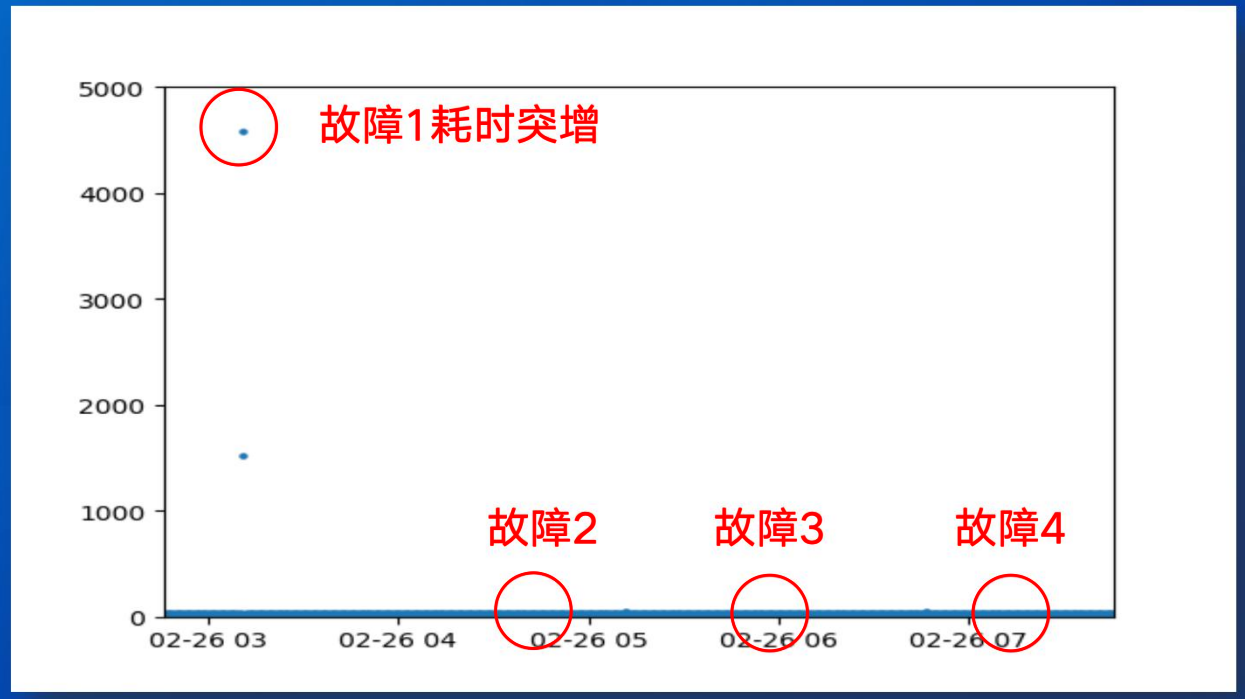


图4. 故障触发数据分析图示

以A系统2月26日KPI响应耗时为例，标注故障时段KPI未必伴随发生异常。若通过KPI异常检测判定是否触发根因分析，会造成故障遗漏。

01 取0:00至0:05的异常检测告警记录与trace数据，进行分析。

02 取0:02:30至0:07:30的异常检测告警记录与trace数据，进行分析。

... ...

n 按5min滑窗，取切片时段内的异常检测记录与trace数据触发一次根因分析。

以2.5min为步长，5min为窗口滑窗选取缓存数据进行分析。

根因分析-前期思路：通过特征工程+监督学习实现根因预测

cmdb组件
Tomcat01
Tomcat02
Tomcat03
MG01
MG02
IG01
IG02
...

特征工程

cmdb组件	异常频次	被调次数	…
Tomcat01	10	30	…
Tomcat02	7	56	…
Tomcat03	8	20	…
MG01	0	12	…
MG02	1	17	…
IG01	4	45	…
IG02	3	62	…
...	…	…	…

机器学习

cmdb组件	预测概率
Tomcat01	0.32
Tomcat02	0.21
Tomcat03	0.14
MG01	0.05
MG02	0.06
IG01	0.09
IG02	0.11
...	…

步骤1：数据获取

从前文所述的数据缓存之中，获取各类数据在某一时段下的切片。

为切片数据下的cmdb组件计算相应特征工程（异常频次、被调次数、执行耗时等）。

建立随机森林监督学习模型，根据特征工程预测各cmdb作为根因的概率。

根因分析-创新性：迁移项目训练模型特征信息，解决新场景下标注少的问题

AIOps Challenge 智能运维挑战赛 | 科创会 NICON

难点1：标注样本少

- 用户标注样本少，难以训练得到较优模型

难点2：数据偶然性

- 标注数据集中在一两天或某种类型，存在偶然性

✓ **解决方案：**

参考项目建模特征重要性作为权重，将各特征归一化后进行加权，得到根因得分score从而定位根因。

$$score = feature_1 \times w_1 + feature_2 \times w_2 + \cdots + feature_n \times w_n$$

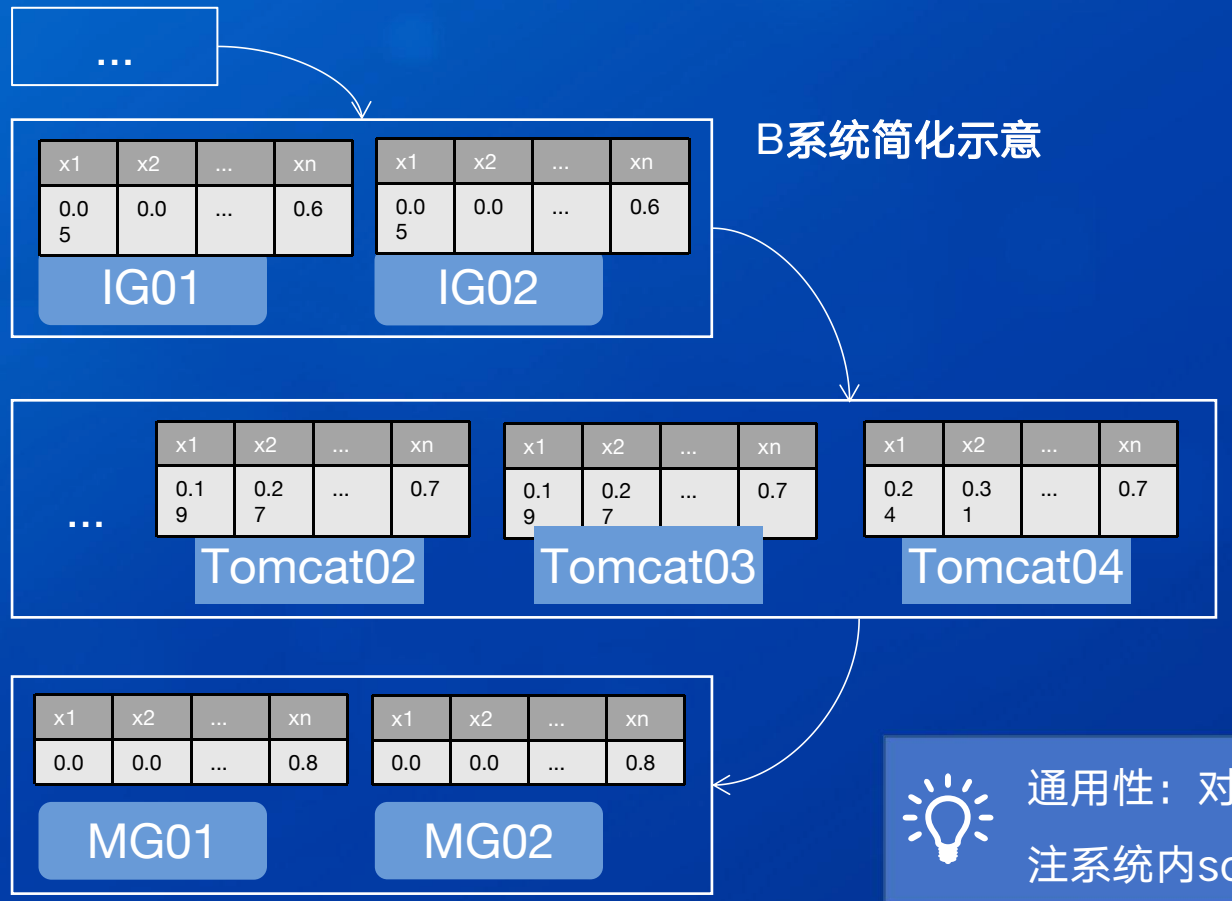
特征	权重（特征重要性）
trace层级	0.305
duration超时频次	0.174
异常metric数	0.122
...	...
异常关键metric数	0.069
异常频次	0.042
被调用次数	0.027

- 较小的启动成本，新场景提供少量标注样本即可适配；
- 商业场景中可更早完成上线部署，不断积累数据并迭代优化。

根因分析-通用性：适配各种应用系统，具备较高泛化性

A 为trace切片中的各cmdb组件，结合相关数据计算特征工程。

B 为每一cmdb组件计算加权分数score，并输出分数最高者作为预测结果。



B系统简化示意

cmdb	异常metric数	duration超时频次	...	trace层级	加权得分
Tomcat04	0.24	0.31	...	0.7	0.34
Tomcat03	0.19	0.27	...	0.7	0.31
Tomcat02	0.19	0.27	...	0.7	0.31
MG01	0.0	0.0	...	0.8	0.02
MG02	0.0	0.0	...	0.8	0.02
IG01	0.05	0.0	...	0.6	0.11
IG02	0.05	0.0	...	0.6	0.11

通用性：对于A系统（无法重组trace）部分特征无法计算，但是仅需关注系统内score的相对大小，因此同样可以沿用这一模式。

第三章节

拓展空间

拓展空间：结合现实场景，推进迭代优化

AIOps Challenge 智能运维挑战赛 | 科创会 NIICON

A 联合模型方案

- 摒弃现有“异常检测-根因分析”两步流程，从而避免误差在该流程中传播。
- 联合时间序列分析与链路trace分析特征工程共同建模训练，直接定位得到根因。

B 异常检测拓展空间

- 尝试采用VAE（包括我们之前发表的T2IVAE）、LSTM等深度学习模型进行更精确的异常检测。
- 在数据支持的前提下，可取历史数据作为补充，计算同比等特征加入模型以提高精度。

C 根因分析拓展空间

- 根据项目经验，如果标注样本量能够达到80，采用监督学习建模就能达到较理想精度。

T2IVAE论文：NVAE-GAN Based Approach for Unsupervised Time Series Anomaly Detection
arXiv：https://arxiv.org/abs/2101.02908v1

2021国际AIOps挑战赛决赛暨AIOps创新高峰论坛

THANKS

谢 谢 观 看

第一届国际互联网产业科技创新大会暨互联网创新产品展览会

The First International Internet Industry Science And Technology Innovation Conference & Internet Innovation Product Exhibition