



GOPS2018  
Shenzhen

# GOPS

## 全球运维大会 2018

2018.4.13-4.14

中国·广东·深圳·南山区 圣淘沙大酒店（翡翠店）





GOPS2018  
Shenzhen

# 腾讯运维的 AI 实践

张戎 机器学习研究员

腾讯科技（深圳）有限公司  
社交网络运营部



GOPS2018  
Shenzhen

# 目录



1

时间序列异常检测

2

智能多维下钻分析

3

告警收敛根源分析

4

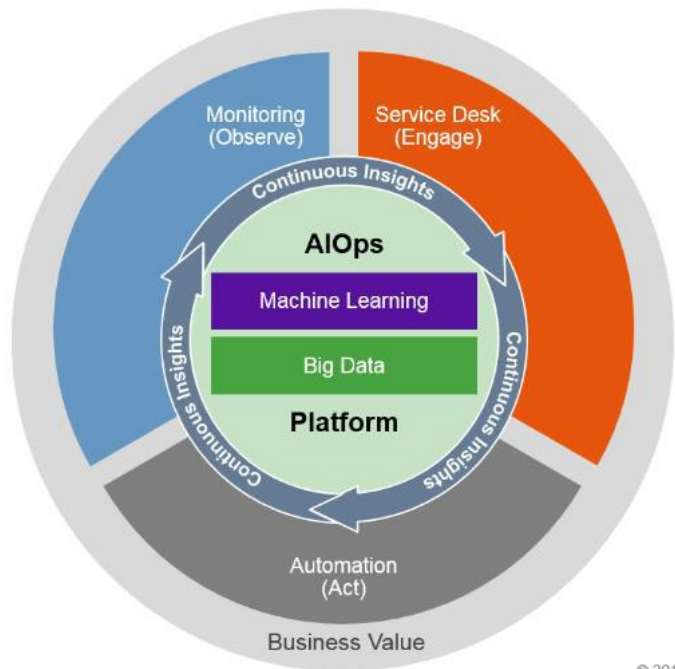
AIOPS的未来规划





GOPS2018  
Shenzhen

# 基于机器学习的智能运维



© 2017

发现问题

- 时间序列异常
- 日志分析异常
- 设备性能异常

分析问题

- 多维下钻分析
- 关联事件分析
- 容量预估分析

解决问题

- 扩容
- 决策
- 调度
- 优化



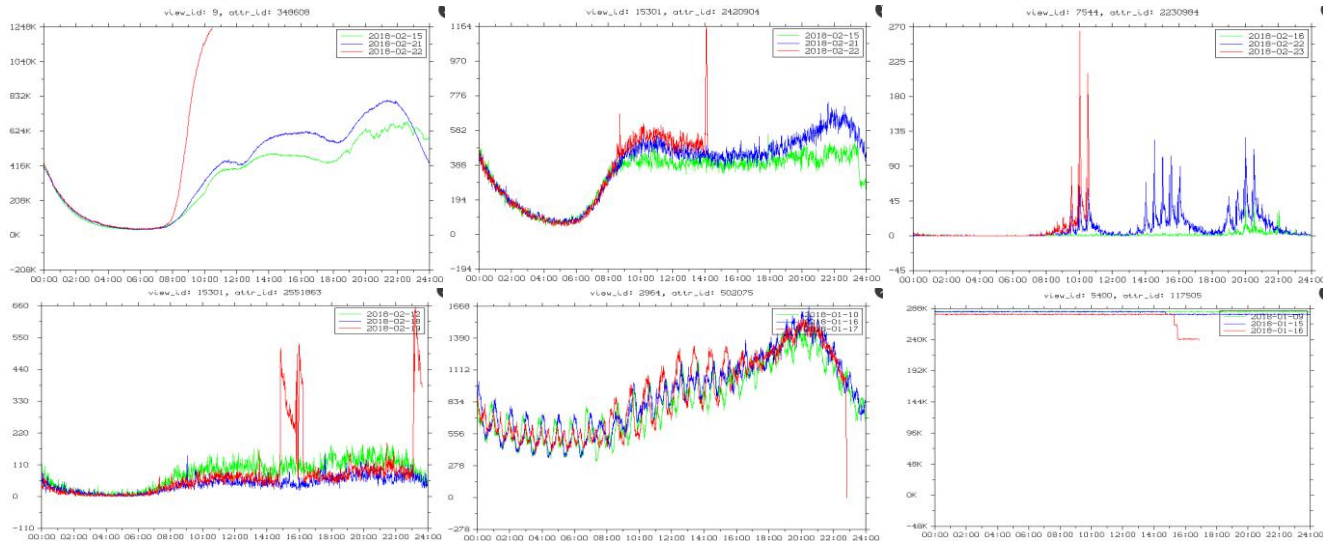
GOPS2018  
Shenzhen

# 发现问题：时间序列异常检测

● 织云 Monitor 智能监控项目的目标 --- 发现问题

实时寻找时间序列中的异常点

● 织云 Monitor 智能监控项目典型案例





GOPS2018  
Shenzhen

# 发现问题：时间序列异常检测

## ● 织云 Monitor 智能监控项目的难点和挑战

### 1. 历史包袱沉重

- 误告邮件多
- 告警电话多

### 2. 海量的时间序列

- 200万条时间序列
- 时间序列的种类多

### 3. 传统的规则处理

- 最大值，最小值，均值等
- 波动率等



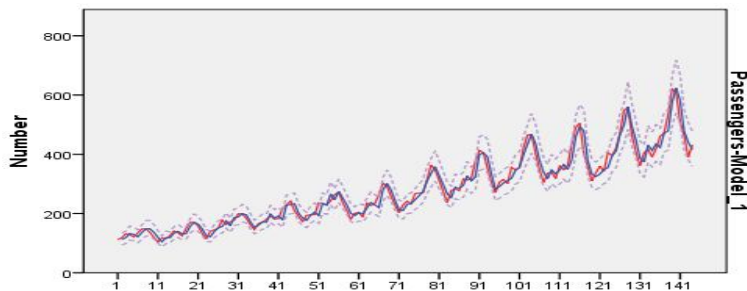
## Question

如何找到通用的算法  
同时监控百万条曲线？

# 经典算法的使用场景

## AR/MA/ARMA/ARIMA

- 需要定阶，确定合适的参数
- 时间序列具有自相关性
- 时间序列具有自相似性



- 自回归 **AR(p)** 模型

$$X_t = c + \sum_{i=1}^p \varphi_i X_{t-i} + \varepsilon_t.$$

- 移动平均 **MA(q)** 模型

$$X_t = \mu + \varepsilon_t + \sum_{i=1}^q \theta_i \varepsilon_{t-i}$$

- **ARMA(p,q)** 模型

$$X_t = c + \varepsilon_t + \sum_{i=1}^p \varphi_i X_{t-i} + \sum_{j=1}^q \theta_j \varepsilon_{t-j}$$

- **ARIMA(p,d,q)** 模型

$$\left(1 - \sum_{i=1}^p \phi_i L^i\right) (1 - L)^d X_t = \left(1 + \sum_{i=1}^q \theta_i L^i\right) \varepsilon_t$$

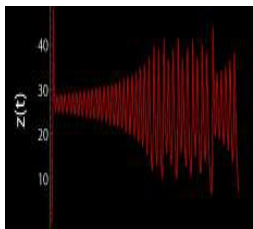


GOPS2018  
Shenzhen

# 经典算法的使用场景

## 相空间重构算法

- 针对混沌序列
- 属于预测和异常检测场景
- 将一维时间序列嵌入高维空间



## ● 原始的时间序列

$$\{x(i) : i = 1, \dots, n\},$$

## ● 高维的时间序列

$$y(i) = (x(i), \dots, x(i + (d - 1)\tau)), \text{ where } 1 \leq i \leq n - (d - 1)\tau.$$

## ● 相空间重构算法的步骤

### 1. 延迟时间的确定

- 自相关系数法
- 交互信息法

### 2. 嵌入维度的确定

- 几何不变量法
- 虚假最邻近法



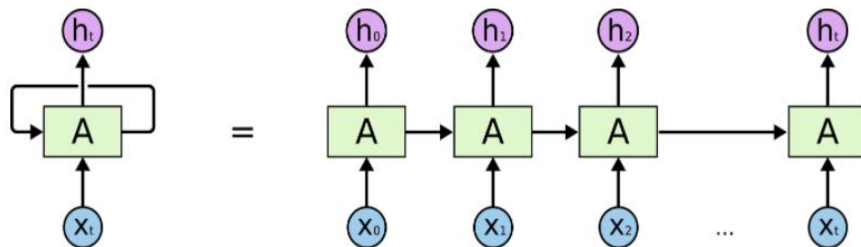
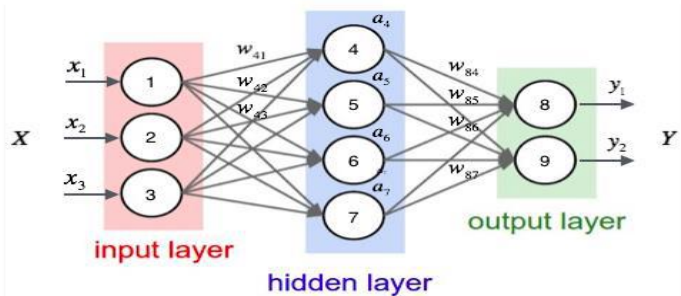
# 经典算法的使用场景



GOPS2018  
Shenzhen

## RNN/LSTM

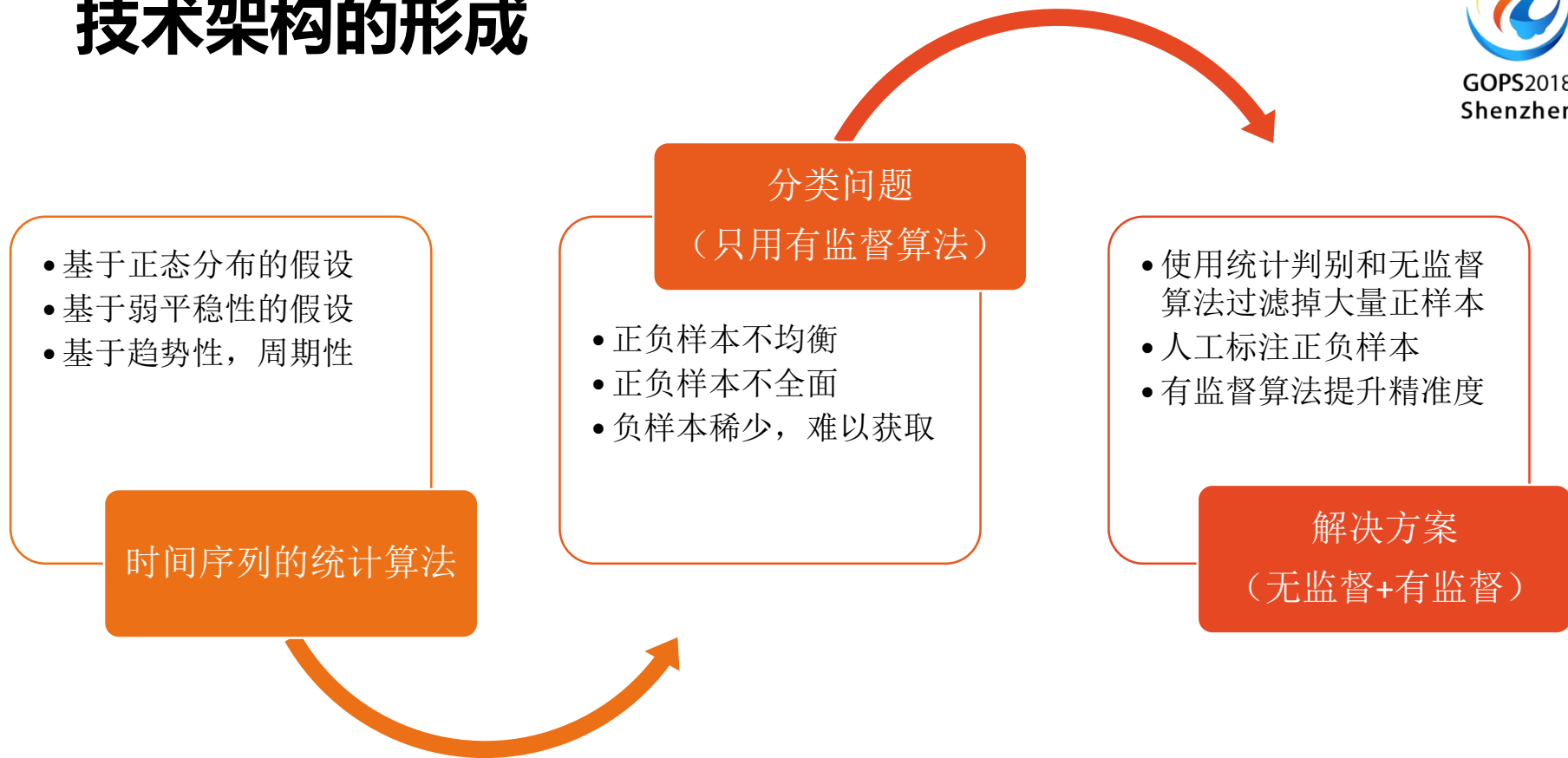
- 属于预测和异常检测场景
- 适用于文本，语音类场景
- 梯度爆炸/消失





GOPS2018  
Shenzhen

# 技术架构的形成

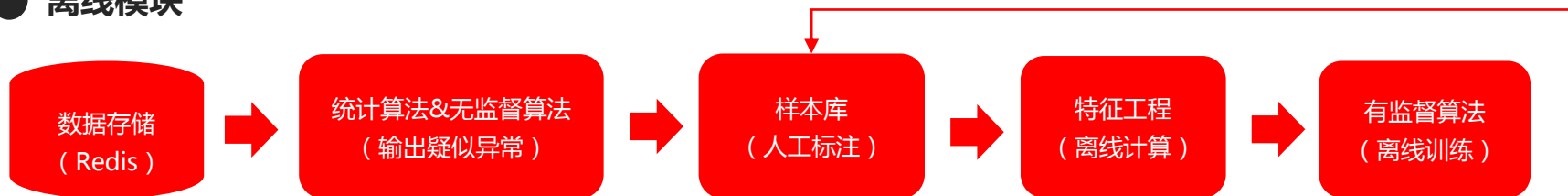




GOPS2018  
Shenzhen

# 织云 Monitor 时间序列异常检测的技术框架

## ● 离线模块



## ● 在线模块



## ● ABTest 模块

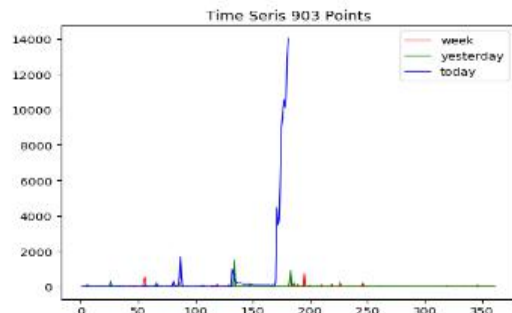
# 第一层：统计判别算法

## 3-Sigma算法和控制图算法的优缺点

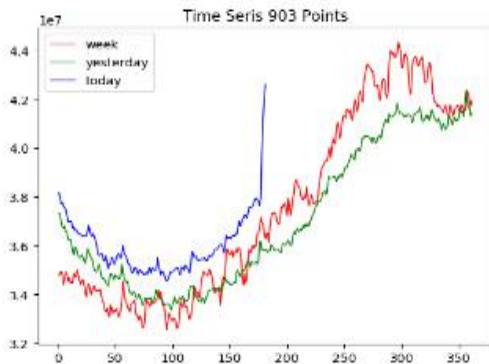


GOPS2018  
Shenzhen

√



×



数据获取

- 以当前时刻为标准
- 七天前后三小时 + 昨天前后三小时 + 今天前三小时

3-sigma

- 3-sigma原理

控制图

- 移动平均算法
- 指数移动平均算法

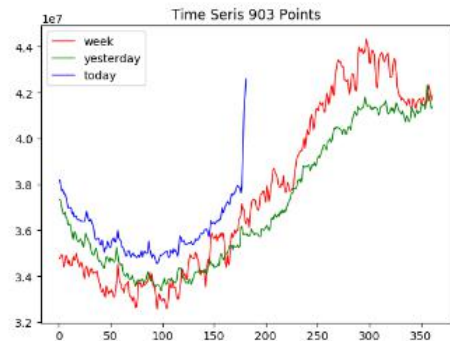
# 第一层：无监督算法



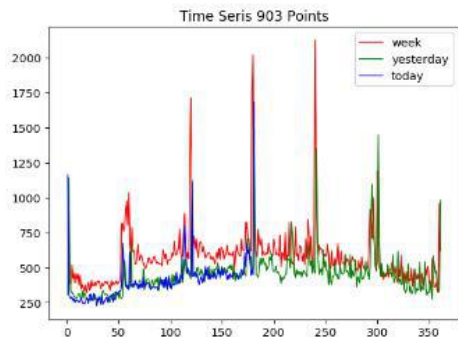
GOPS2018  
Shenzhen

## 无监督学习算法的优缺点

√



×



数据获取

- 以当前时刻为标准
- 七天前后三小时 + 昨天前后三小时 + 今天前三小时

孤立森林

- 可以从多维特征中寻找异常点

SVM

- 使用超平面的思想来进行异常/正常的区分

RNN

- 使用神经网络的误差来进行异常判断

## Isolation Forest

- 属于无监督算法
- 集成学习的思想
- 适用于连续数据的异常检测
- 通过多颗 iTree 形成森林来判断是否异常

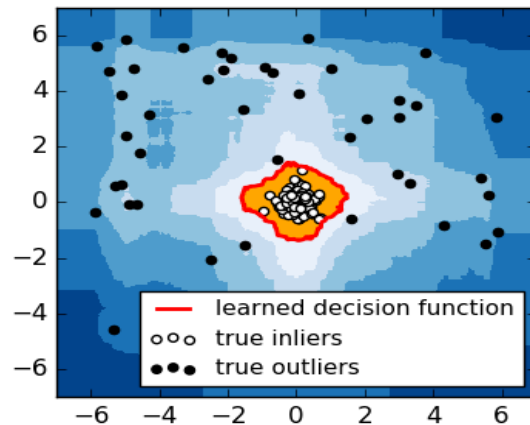
### Algorithm 1 $iTree(X, e, h)$

Input:  $X$  - input data;  $e$  - current height;  $h$  - height limit.

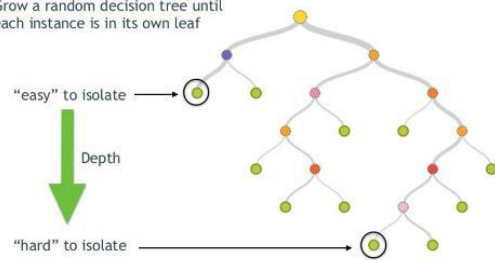
Output: an  $iTree$ .

- 1: if  $e \geq h$  OR  $|X| \leq 1$  then
- 2:   return  $exNode\{Size \leftarrow |X|\}$ ;
- 3: else
- 4:   Randomly select an attribute  $q$ ;
- 5:   Randomly select a split point  $p$  between  $min$  and  $max$  values of attribute  $q$  in  $X$ ;
- 6:    $X_l \leftarrow filter(X, q < p)$ ,  $X_r \leftarrow filter(X, q \geq p)$ ;
- 7:   return  $inNode\{ Left \leftarrow iTree(X_l, e + 1, h),$   
                     $Right \leftarrow iTree(X_r, e + 1, h),$   
                     $SplitAttr \leftarrow q, SplitValue \leftarrow p\}$ ;

8: end if

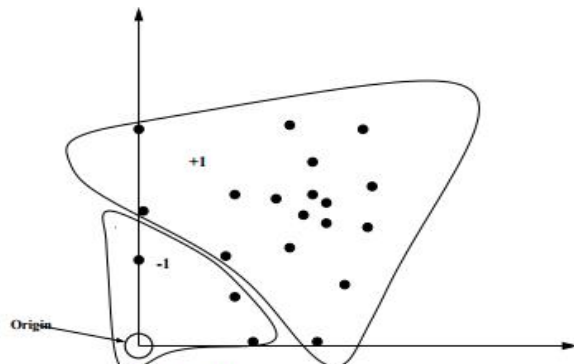


Grow a random decision tree until  
each instance is in its own leaf



## One Class SVM

- 属于无监督算法
- 使用了超平面的思想
- 适用于连续数据的异常检测
- 适用于对样本进行一定比例的筛选
- 寻找高维平面区分正常点与异常点

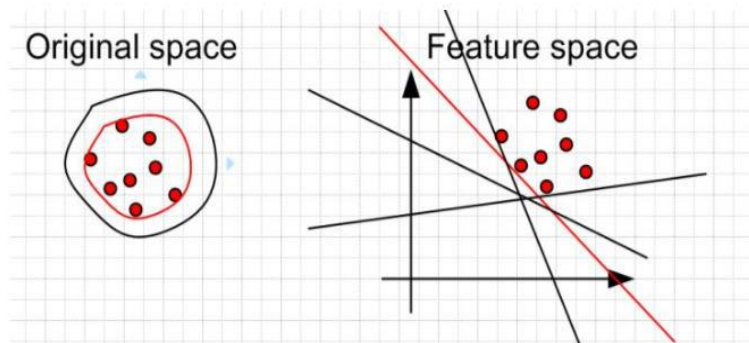


One-Class SVM Classifier. The origin is the only original member of the second class.

subject to

$$\min \frac{1}{2} \|w\|^2 + \frac{1}{vl} \sum_{i=1}^l \xi_i - \rho$$

$$(w \cdot \Phi(x_i)) \geq \rho - \xi_i \quad i = 1, 2, \dots, l \quad \xi_i \geq 0$$



# 第一层：无监督算法

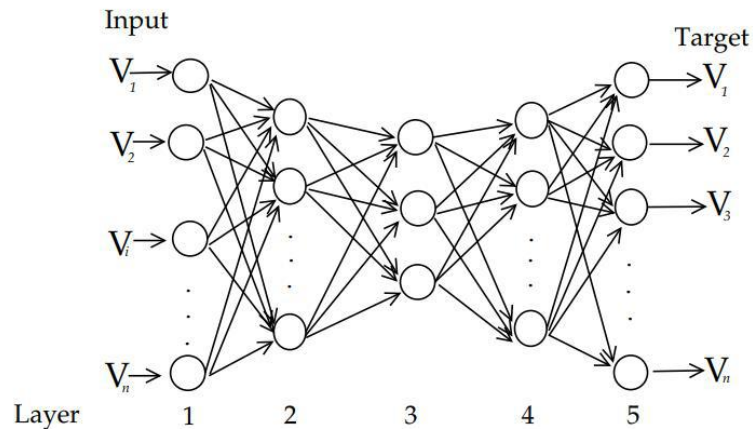


GOPS2018  
Shenzhen

## Replicator Neural Network

- 属于无监督算法
- 需要构造必要的特征
- 使用了神经网络的思想
- 适用于连续数据的异常检测
- 寻找神经网络的误差来区分正常点与异常点

$$OF_i = \frac{1}{n} \sum_{j=1}^n (x_{ij} - o_{ij})^2$$





# 第二层：有监督算法

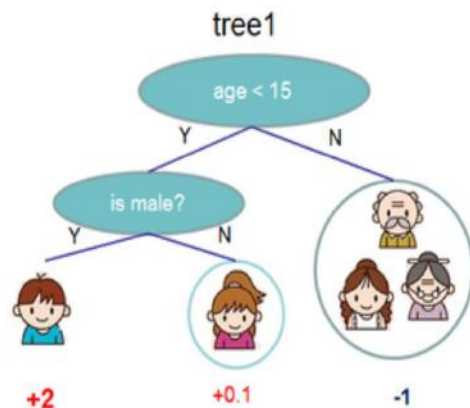
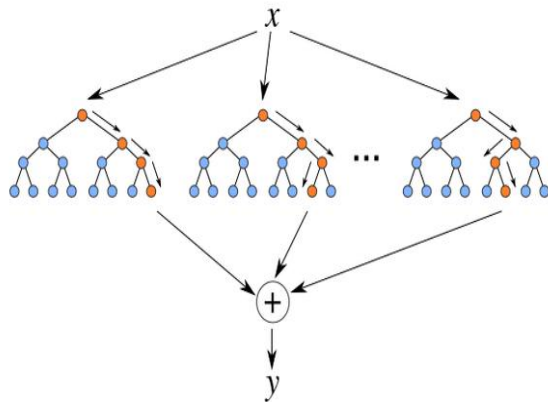


GOPS2018  
Shenzhen

## 有监督算法能解决的问题

有监督算法

- Linear Regression/Logistic Regression
- Decision Tree/Naïve Bayes
- Random Forest/GBDT





GOPS2018  
Shenzhen

## 第二层：时间序列的特征工程

### 时间序列的统计特征

- 最大值，最小值，值域
- 均值，中位数
- 方差，偏度，峰度
- 同比，环比，周期性
- 自相关系数，变异系数

### 时间序列的拟合特征

- 移动平均算法
- 带权重的移动平均算法
- 指数移动平均算法
- 二次指数移动平均算法
- 三次指数移动平均算法
- 奇异值分解算法
- 自回归算法
- 深度学习算法

### 时间序列的分类特征

- 熵特征
- 值分布特征
- 小波分析特征

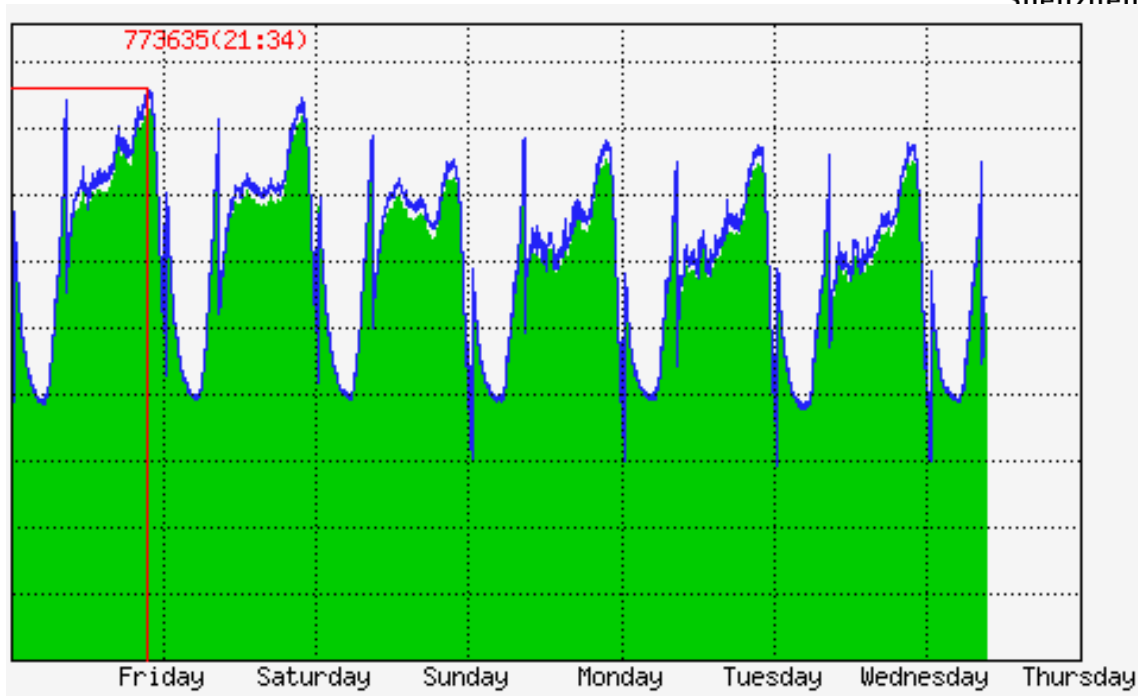
# 第二层：时间序列的特征工程



GOPS2018  
Shenzhen

## 时间序列的统计特征

- 最大值，最小值，值域
- 均值，中位数
- 方差，偏度，峰度
- 同比，环比，周期性
- 自相关系数，变异系数

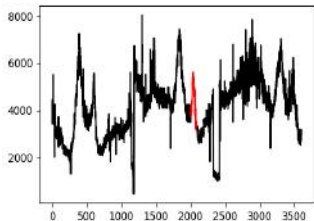




GOPS2018  
Shenzhen

# 时间序列的拟合特征

## ● 集成学习的思想



移动平均, 窗口长度 5

移动平均, 窗口长度 25

EWMA,  $\alpha = 0.2$

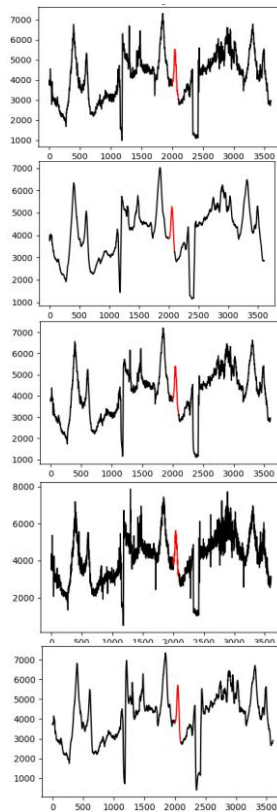
EWMA,  $\alpha = 0.9$

Double EWMA,  
 $\alpha = 0.1, \beta = 0.1$

MA  
•  $w$  in {5, 10, 20, 30, 50, 100}

EWMA  
•  $\alpha$  in {0.2, 0.4, 0.6, 0.8}

Double EWMA  
•  $\alpha$  in {0.2, 0.4, 0.6, 0.8}  
•  $\beta$  in {0.2, 0.4, 0.6, 0.8}



● 移动平均算法

● 带权重的移动平均算法

● EWMA 算法

● Double EWMA 算法

● Holt Winters 算法

● SVD 算法

● AR/MA/ARMA/ARIMA 算法

● RNN/LSTM 算法

# 时间序列的分类特征



GOPS2018  
Shenzhen

## 时间序列的分类特征

- 熵特征
- 值分布特征
- 小波分析特征

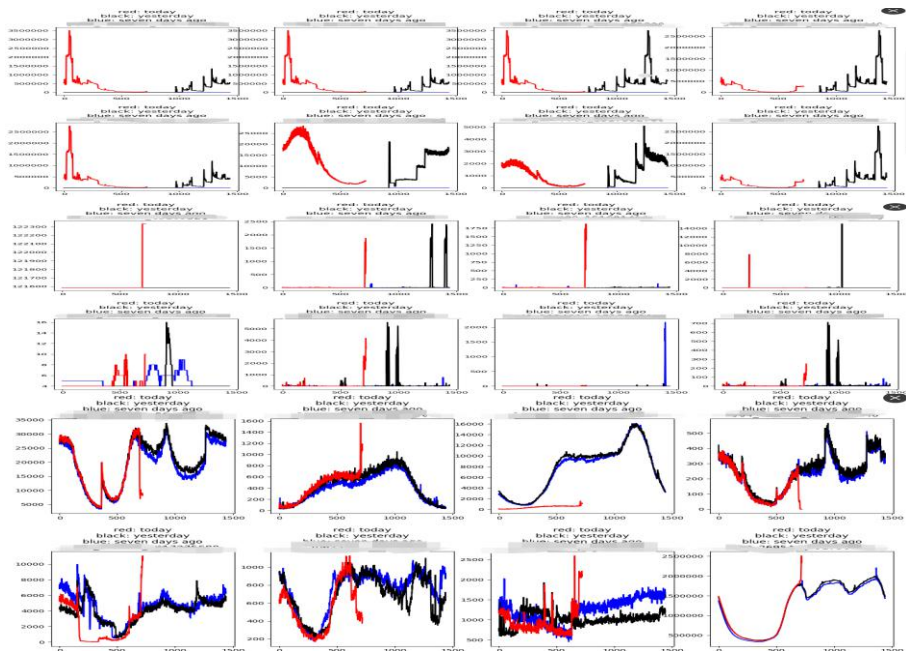
聚类算法

Kmeans等



查看效果

● 时间序列的典型类别：昨日放量型，毛刺型，平稳型等





GOPS2018  
Shenzhen

# 织云 Monitor 智能监控的业务效果

## 目前效果

用少量模型覆盖所有曲线  
时间序列异常只是 AIOPS 的第一步

# 90%

**准确率**

计算方法：人工抽查，查看告警出来的时间序列和相应的时间点是否准确。

# 70%

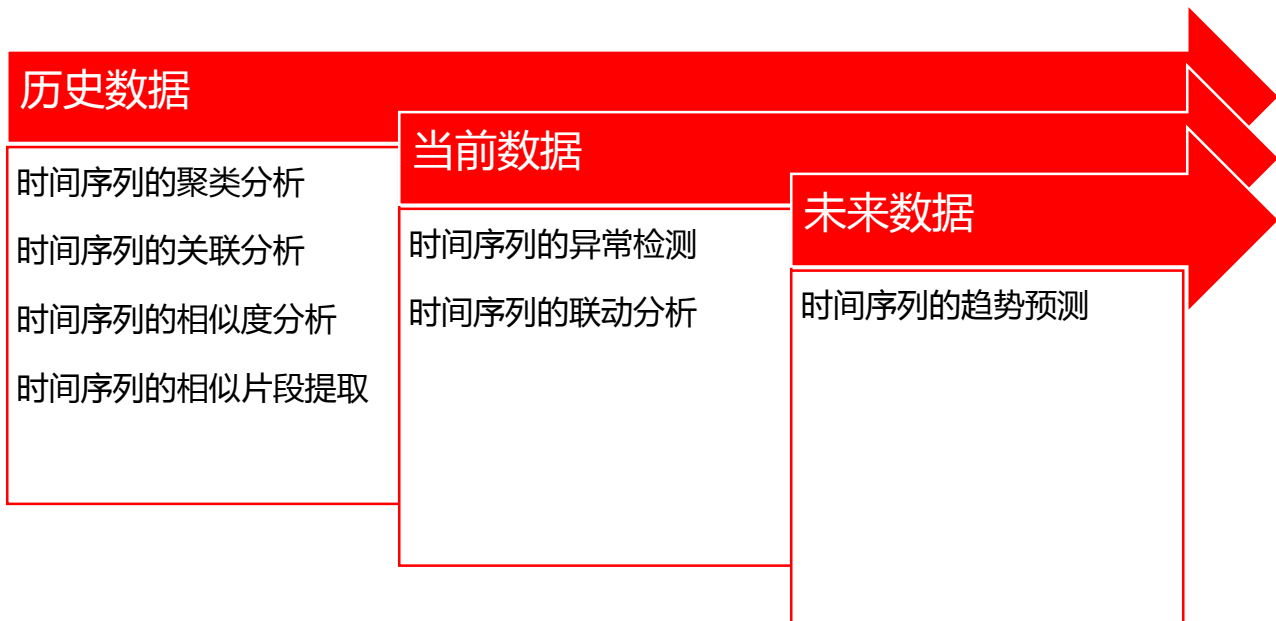
**召回率**

计算方法：人工从Monitor视图里面选择一批异常的时间序列和相应的时间点，然后让这批序列通过现有模型，看看是否被召回。



GOPS2018  
Shenzhen

# 时间序列相关技术的发展规划





GOPPS2018  
Shenzhen

# 目录

**1** 时间序列异常检测



**2** 智能多维下钻分析

**3** 告警收敛根源分析

**4** AIOPS的发展规划

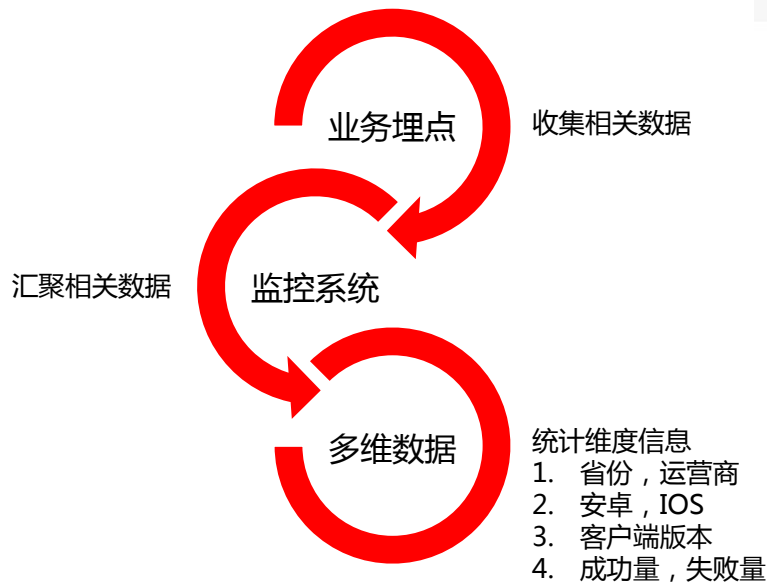




GOPS2018  
Shenzhen

# 分析问题：多维下钻分析的背景描述

## 背景描述





GOPS2018  
Shenzhen

# 传统的人工分析的弊端

## 第一步：判断成功率是否下跌

- 人工设定阈值
- 业务随着时间会变化

## 第二步：人工查找可疑维度

- 查看成功数
- 查看成功率

## 第三步：可疑维度的汇总

- 收集第二步的结果
- 输出维度的组合



时间	请求数	成功请求数	失败请求数	成功率	平均响应	平均请求时长	平均返回时长
2018-02-27 04:32:00	2032	1840	212	89.06%	140.352	6854.581	6231.441
2018-02-27 04:33:00	2421	2230	211	91.28%	83.724	4712.038	2949.915
2018-02-27 04:34:00	2662	2450	212	92.03%	122.914	5860.292	5231.745
2018-02-27 04:40:00	1825	1713	112	93.86%	94.982	9326.77	4444.673
2018-02-27 04:42:00	2220	2094	126	94.32%	487.822	11511.16	5833.552
2018-02-27 04:43:00	1510	1421	89	94.08%	426.885	7821.574	4739.169
2018-02-27 04:44:00	1836	1723	103	94.38%	513.357	9825.73	4775.227

# 基于机器学习的根因分析

发现问题 → 分析问题





GOPS2018  
Shenzhen

# 根因分析的机器学习模型（一）

决策树

模型的性质：

1. 解释性好
2. 规则模型
3. 离线分析

模型种类：

1. ID3
2. C4.5
3. CART

决策树：

1. 形成分支：信息增益/信息增益率/Gini系数
2. 去掉分支：前剪枝/后剪枝

● 信息熵

$$H(X) = \sum_i P(x_i) I(x_i) = - \sum_i P(x_i) \log_b P(x_i),$$

● Gini 系数

$$\text{Gini}(p) = \sum_{k=1}^K p_k (1 - p_k) = 1 - \sum_{k=1}^K p_k^2$$

# 根因分析的机器学习模型（一）

## 根因分析的样本和特征工程

成功率	运营商	操作系统	客户端版本	网络类型	图片数量
99.9%	移动	安卓	XXX1	4G	3
90.1%	联通	IOS	YYY2	WIFI	20



根据成功率获得标签

1. 抽样比例
2. 抽样数量



特征类型：连续特征与离散特征

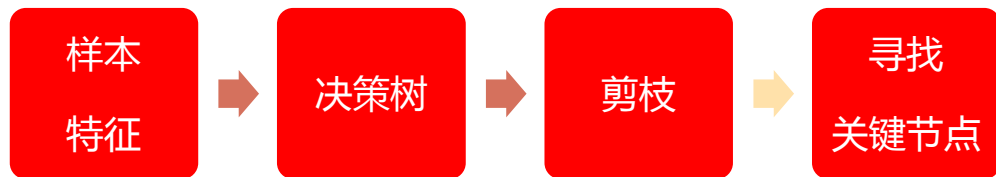
1. 连续特征直接使用
2. 离散特征使用 one-hot 编码：几个原始特征变成上千个特征

标签	特征1	特征2	特征3	.....	特征n
0（异常）	1	1	0		3
1（正常）	0	1	0		20



GOPS2018  
Shenzhen

# 根因分析的机器学习模型（一）

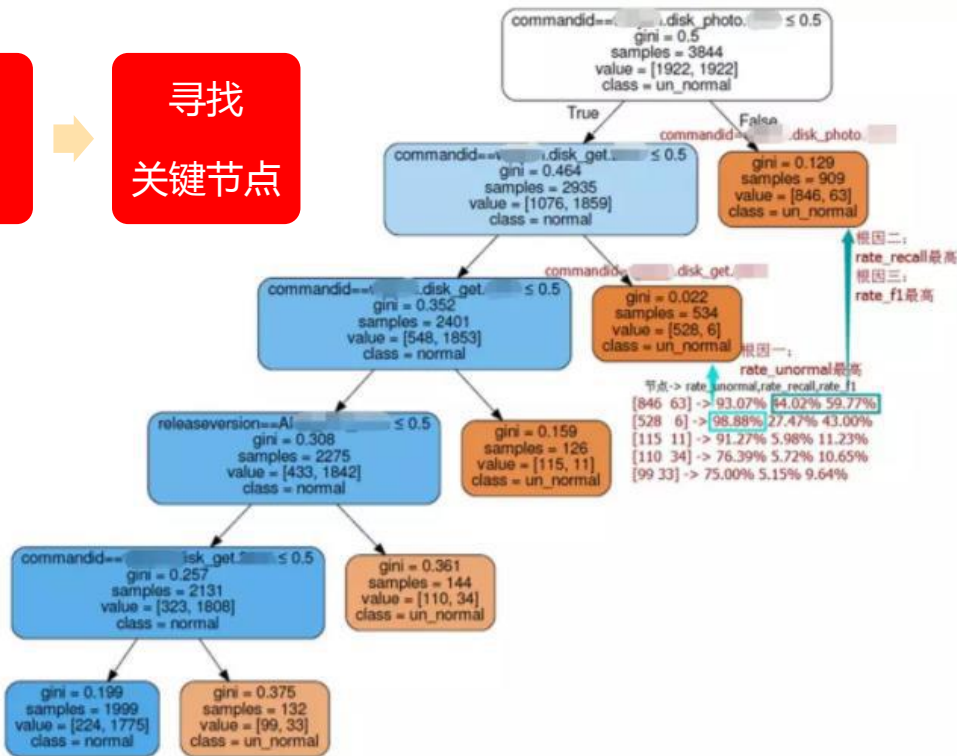


关键节点

异常聚集率：节点负样本数量/节点样本总量

异常检出率：节点负样本数量/树的样本总量

二者的加权平均：F1 Score等





GOPS2018  
Shenzhen

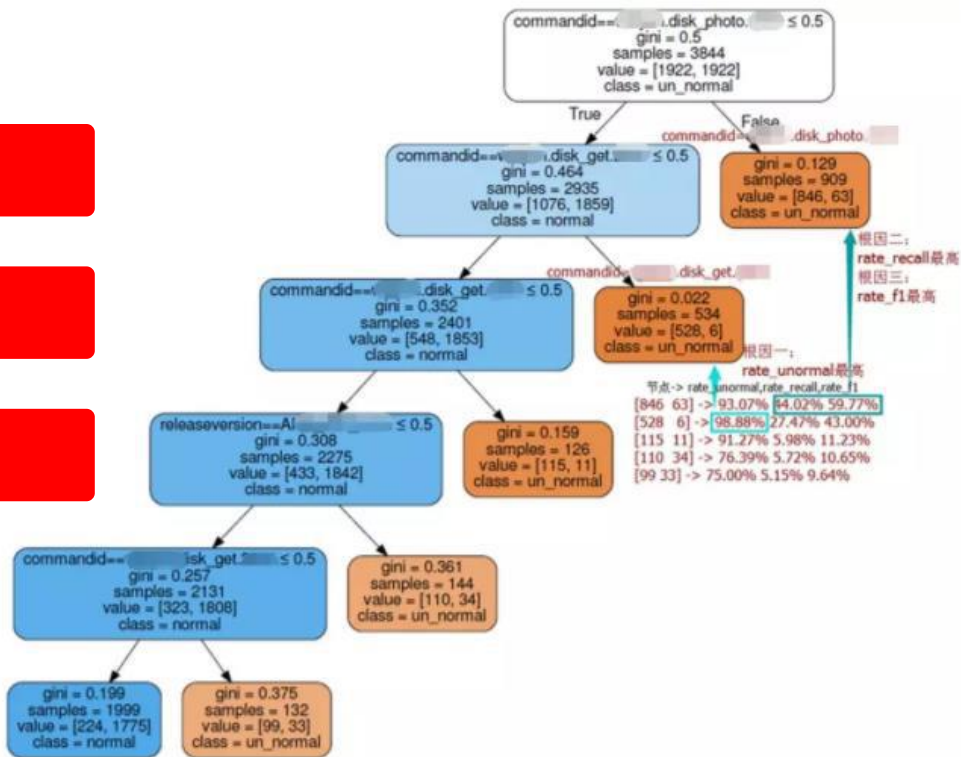
# 根因分析的机器学习模型（一）

找到三个关键节点

沿着树图，寻找路径

路径上的规则就是根因

冗余规则的合并

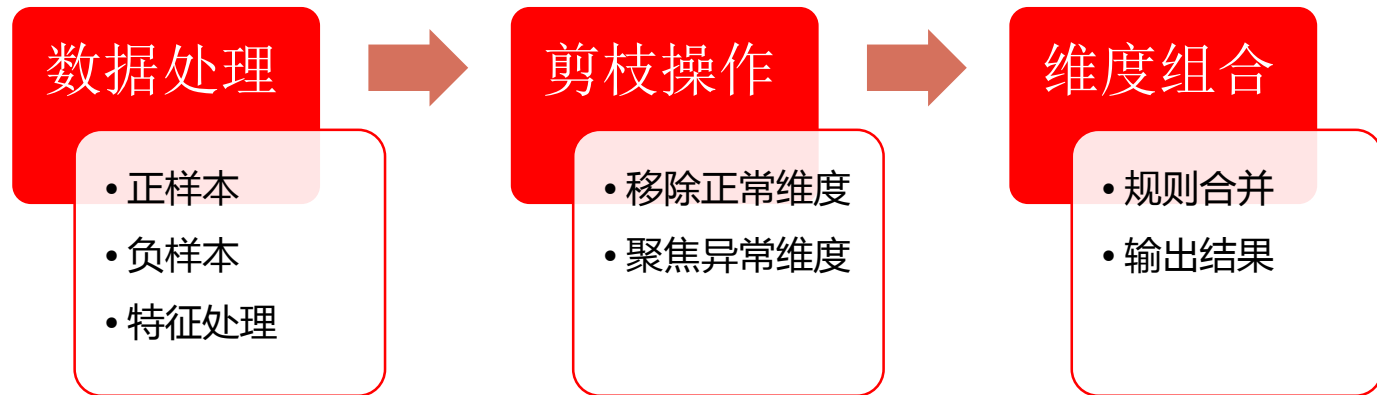




GOPS2018  
Shenzhen

# 根因分析的机器学习模型（二）

## ● 根因分析算法的一般流程



## ● 提炼决策树的核心步骤



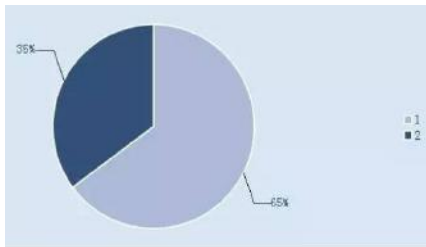
## ● 信息熵 / Gini 系数



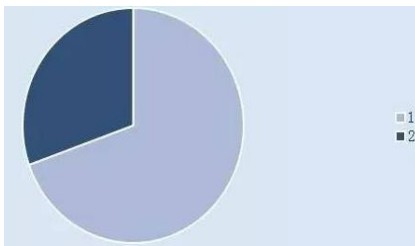
# 根因分析的机器学习模型（二）

## ● 如何描述两个概率分布的“距离”

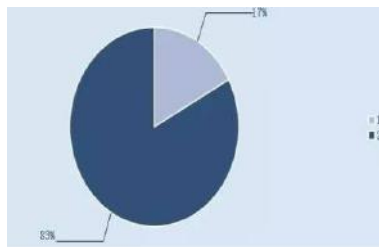
男女分布情况



App1的下载量



App2的下载量



## ● KL 散度（不对称）

$$D_{\text{KL}}(P \parallel Q) = \sum_i P(i) \ln \frac{P(i)}{Q(i)}.$$

## ● Jensen Shannon Entropy（对称）

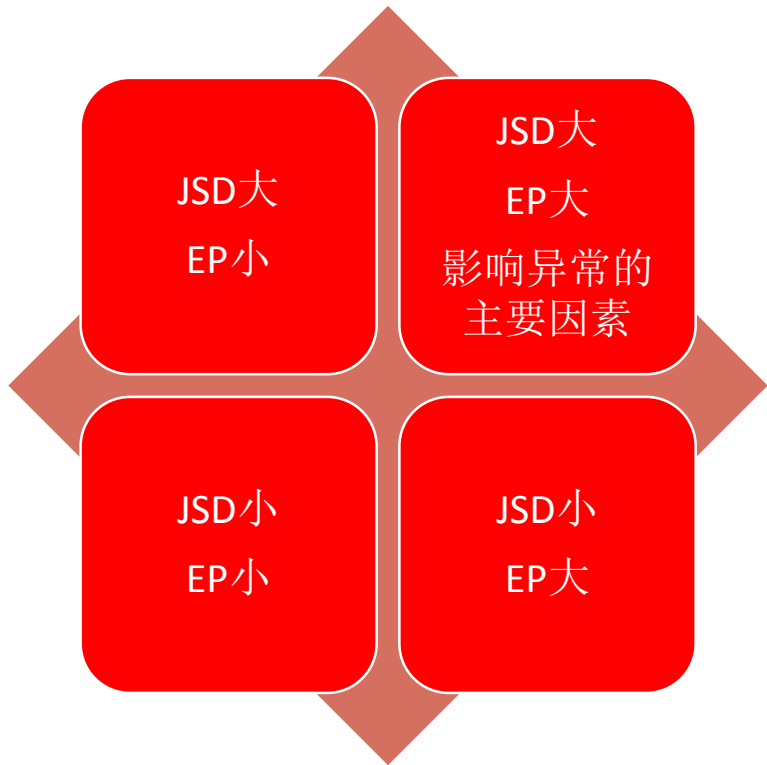
$$\text{JSD}(P \parallel Q) = \frac{1}{2} D(P \parallel M) + \frac{1}{2} D(Q \parallel M)$$

$$\text{where } M = \frac{1}{2}(P + Q)$$



GOPS2018  
Shenzhen

# 根因分析的机器学习模型（二）



## ● Jensen Shannon Entropy

$$\text{JSD}(P \parallel Q) = \frac{1}{2}D(P \parallel M) + \frac{1}{2}D(Q \parallel M)$$

$$\text{where } M = \frac{1}{2}(P + Q)$$

## ● EP值

$$EP_{ij}(m) = \frac{A_{ij}(m) - F_{ij}(m)}{A(m) - F(m)},$$

## ● 效果

准确率大于 95%



GOPPS2018  
Shenzhen

# 目录

**1** 时间序列异常检测

**2** 智能多维下钻分析



**3** 告警收敛根源分析

**4** AIOPS的未来发展



GOPS2018  
Shenzhen

# 解决问题：告警收敛

1. 海量告警怎么办？
2. 如何寻找海量告警的根因？
  - 网络抖动
  - 机房故障
  - 程序异常
  - 日志变更





GOPS2018  
Shenzhen

# ROOT根源分析要解决的问题

## ● ROOT 项目的难点和挑战

历史包袱沉重

- 误告邮件多
- 误告消息多
- 告警电话多



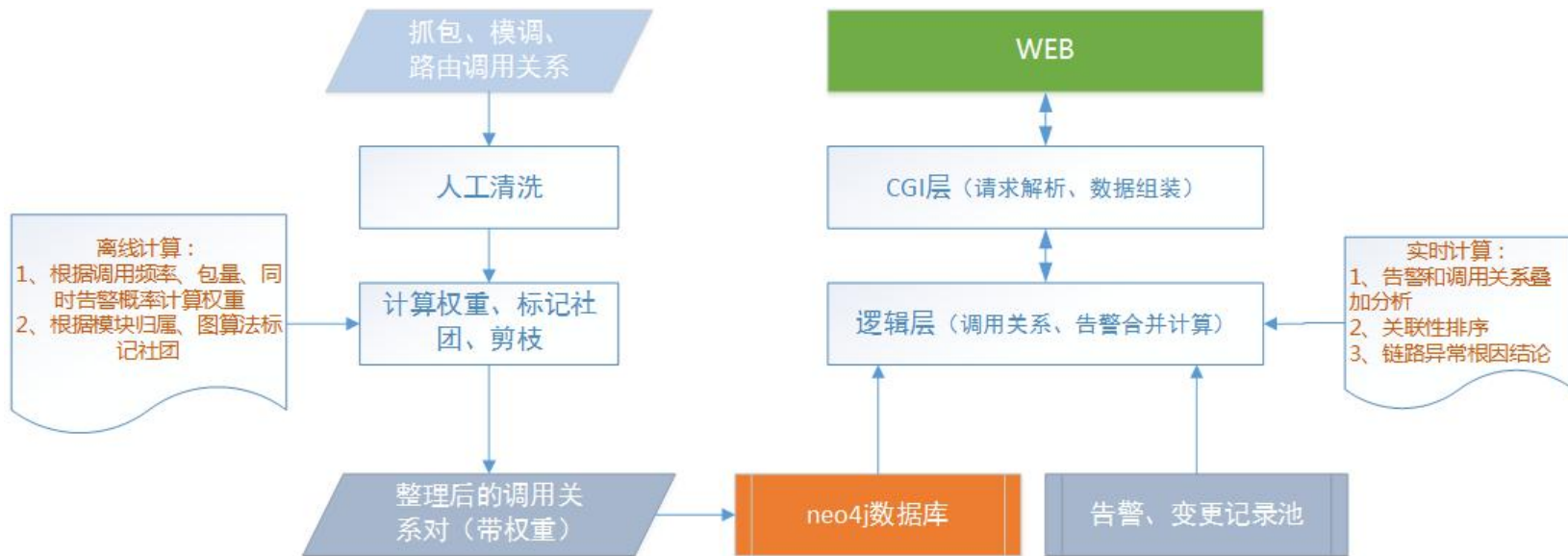
- 如何才能找到造成告警的根源故障
- 如何发现有价值的告警

# 织云 ROOT 根源分析



GOPS2018  
Shenzhen

## ● 织云 ROOT 项目整体架构

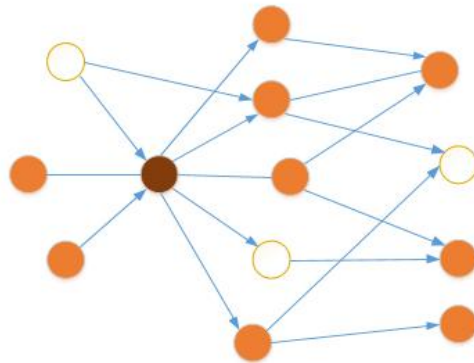
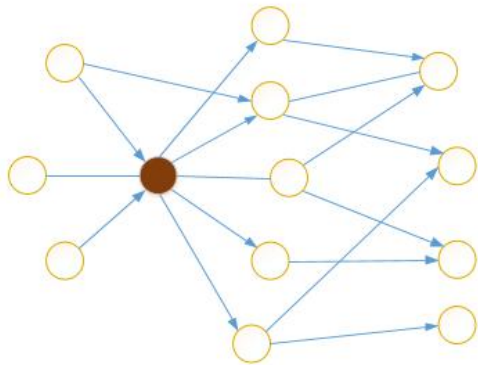


# 织云 ROOT 根源分析的机器学习方案



GOPS2018  
Shenzhen

- 对于要分析的模块，  
考察它所在的子网构成的链路中其他模块节点在邻近时间范围内的告警情况

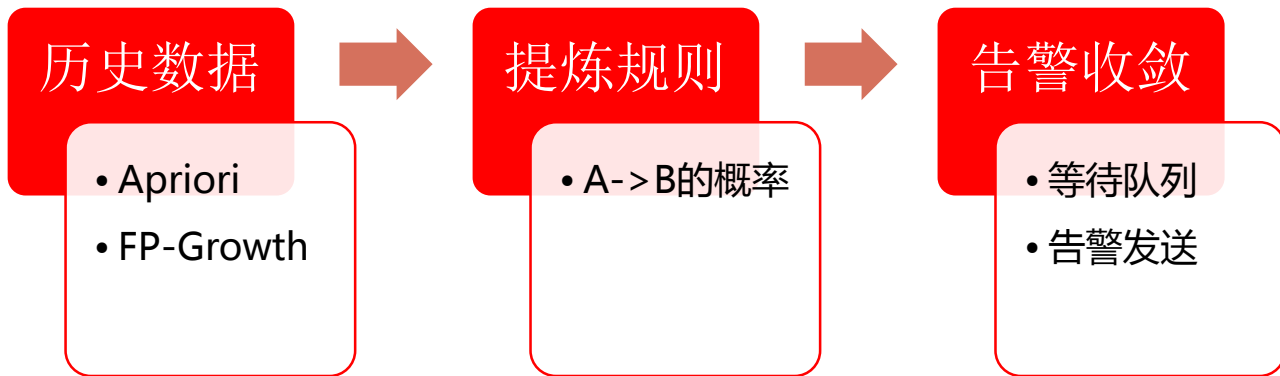


调用关系拓扑



GOPS2018  
Shenzhen

# 告警收敛的机器学习方案







GOPS2018  
Shenzhen

# 时间序列的关联分析



相关联的模块KPI曲线在发生异常时，往往会呈现相似的异常特征

对两个KPI曲线的告警按时间切片进行统计，时间切片内有告警为1，无告警为0

0	0	0	1	0	0	0	0	0	1	1	1	1	1	1	0	1	0	0
0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	1	0	1	0

必要时对序列进行位移操作，计算出皮尔逊相关系数

0	0	0	1	0	0	0	0	0	1	1	1	1	1	1	0	1	0	0
0	0	0	1	0	0	0	0	0	1	1	1	1	1	1	0	1	0	0

$$Pearson = \frac{Cov(\tilde{E}_1, \tilde{E}_2)}{\sqrt{Var(\tilde{E}_1)Var(\tilde{E}_2)}}$$



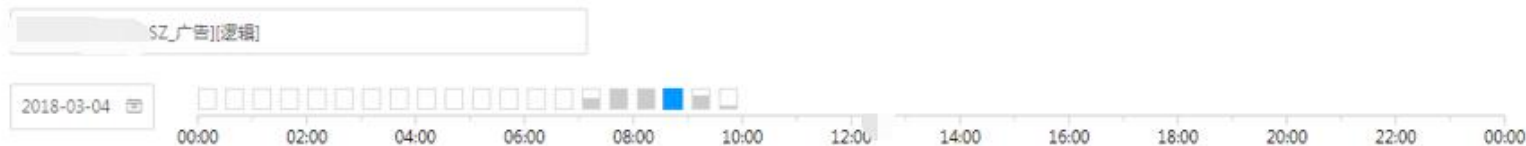
# 织云 ROOT 根源分析的效果展示

织云

首页

ROOT

018  
hen



推荐访问的模块







GOPPS2018  
Shenzhen

# 目录

**1** 时间序列异常检测

**2** 智能多维下钻分析

**3** 告警收敛根源分析



**4** AIOPS的未来发展



GOPS2018  
Shenzhen

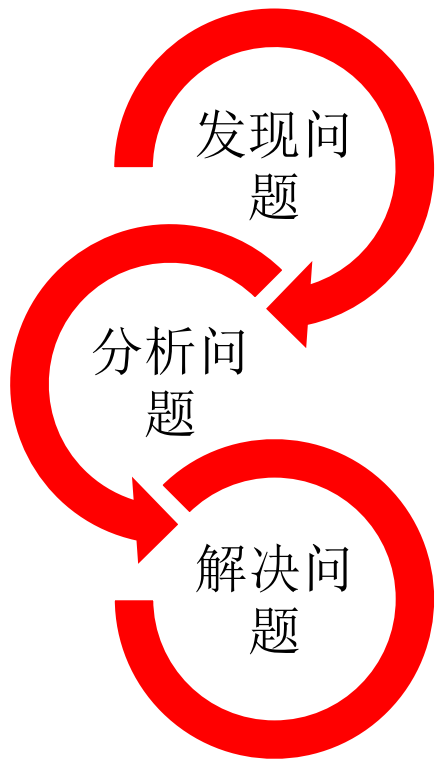
# 织云 AIOPS 的未来规划

## 根因分析

### ● 多维下钻分析

### ● 故障传播链分析

1. 事件与事件的关联分析
2. 时序与事件的关联分析
3. 时序与时序的关联分析



## 时间序列

### ● 异常检测

1. 时间序列聚类
2. 时间序列分类
3. 时间序列的局部相似度
4. 时间序列的整体相似度
5. 时间序列的关键部分提取

### ● 趋势预测

## 智能决策

### ● 扩容

### ● 决策

### ● 调度

### ● 优化



GOPS2018  
Shenzhen



高效运维社区  
开放运维联盟

# Thanks

腾讯运维体系专场  
荣誉出品



GOPS2018  
Shenzhen

想第一时间看到高效运维社区的  
最新动态吗？

