Intelligent Anomaly Detection in Heterogeneous Internet Services

Dong Wang
Principal Architect, wangdong13@baidu.com
Baidu Inc.
Agenda

• Brief introduction to Baidu
• Heterogenous services and their challenges to our SREs
• Anomaly detection in typical services
• ARK: A generalized intelligent operation platform for Baidu services
Introduction to Baidu

• One the largest search engines in the world
  ✓ Web/Image/Video/News/…

• Besides search, we also have
  ✓ Location Based Service - Maps
  ✓ Social/Knowledge - Tieba/Zhidao
  ✓ Online to Offline - Nuomi/Waimai
  ✓ Finance/Payment - Wallet
  ✓ Cloud computing - Cloud

• Covers more than 1 Billion users in total
Anomaly Detection in Heterogenous Services

- Anomaly Detection in theory

- However, here are some realities
Divide and Conquer

• Several typical categories we manually touch on
  ✓ Holiday sensitive
  ✓ Very unstable
  ✓ Requiring fully automatic configuration
Holiday Sensitive Curves

• Holidays in Chinese Calendar have no fixed dates
  ✓ 2016 - Spring Festival (Feb., 8th) - Dragon Boat festival (Jun., 9th)
  ✓ 2017 - Spring Festival (Jan., 28th) - Dragon Boat festival (May, 30th)

• There is no common pattern among different holidays

• It’s hard to know the baselines!
  ✓ The training data are pretty sparse
Basic idea and the result

- Clustering on daily CDF of curves
- Classification on dates (features include weekend, holiday, etc.)
- LR based estimated algorithm
Very Unstable Curves

- Very unstable but not anomaly, caused by
  - Revenue with significantly different price goods
  - Revenue under some promotions

- The curve’s variance is huge, traditional method cannot guarantee the precision/recall
Basic Idea and Result

• A compound solution, including
  ✓ smoothing by sliding window
  ✓ Reduce the impact from huge absolute values by using logarithm
  ✓ Considering the increasing/decreasing rate

• The results
Curves requiring automatic configuration

• Two many curves to monitor, but
  ✓ No enough bandwidth to do manual configuration from SRE side
  ✓ Hard to select algorithms
  ✓ Even harder to setup/adjust parameters

• The examples of such metrics
  ✓ RPC numbers between two modules
  ✓ Network transmission amount on some switch devices
Basic Idea and Results

• Using machine learning to select algorithm
  ✓ Whether or not the curve is periodical
  ✓ How the curve’s stability look like
  ✓ The difference between maximum and minimum

• The default parameters configuration, plus auto-adjustment based on user feedback (marked by on-call)

• The sampling results so far
  ✓ Precision is about 84%
More Pain Points

• Other SREs have needs to customize the existed algorithms

• Codes are hard to reuse
  ✓ Different execution environments (programming languages)
  ✓ Different data sources with different formats
  ✓ Different teams/projects
ARK - A Generalized OP Platform

User Code Management

Operation Abstraction Layer
- Interface
- Driver
- Runtime Environment
- Cloud/PaaS
- Scheduler

Develop Tool-Chain
- IDE
- Build
- Debug
- Test
- Simulation
- Prof
Unified Algorithms and deployment

- Offline Data
- Detector Training
- Case DB
- Realtime Data
- 3-sigma
- LR
- BP Neural Net
- ... ...
- Auto/Manual Config
- Anomal detection
- Alarm
Unified Monitoring DB and Platform

Collectors → Data Processing → Anomaly Detection → Alarm Filter → Alarm

TSDB
EventDB
MetaDB

Message Bus

Auto Remediation
Root Cause Analysis
On call Platform
Thanks Very Much
&
Welcome Questions!