Robust KPI Anomaly Detection for Large-Scale Software Services with Partial Labels

Shenglin Zhang¹, Chenyu Zhao¹, Yicheng Sui¹, Ya Su²,
Yongqian Sun¹, Yuzhi Zhang¹, Dan Pei², Yizhe Wang
Software services

Online Shopping: Amazon.com, Taobao.com

Social Networks: WeChat, Facebook

Search Engines: Baidu, Google
Millions of KPIs are constantly monitored and collected

Key Performance Indicator (KPI):

- User perceived metrics: response delay, queries per second, failure ratio...

- System-level metrics: CPU utilization, memory utilization, network throughput...

The metric of CPU utilization

The metric of average response delay
## Existing KPI anomaly detection algorithms

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Labeling effort</th>
<th>Shortcoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervised</td>
<td>Opprentice</td>
<td>Full labels</td>
<td>Time-consuming and labor-intensive labeling work</td>
</tr>
<tr>
<td></td>
<td>EGADS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unsupervised</td>
<td>Donut</td>
<td>No labels</td>
<td>Low accuracy or require large amounts of training data</td>
</tr>
<tr>
<td></td>
<td>iForest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semi-supervised</td>
<td>ADS</td>
<td>Full labels of cluster centroids</td>
<td>Need a large number of KPI streams with high-quality ground truth</td>
</tr>
<tr>
<td>Transfer learning</td>
<td>ATAD</td>
<td>For a KPI dataset with 10 million data points, about 500,000 labels are needed</td>
<td></td>
</tr>
</tbody>
</table>
Comparison between PU learning and Semi-supervised learning

For a KPI stream in the training set:

- PU learning only requires labeling part of anomalous segments.
- Semi-supervised learning need to label all the anomalous segments.
- PU learning greatly reduces the labeling effort.
Challenge 1: Large-scale and diverse KPI streams

KPI streams are large in number and diverse in pattern.

- Train a PU learning model for each KPI stream?
Challenge 1: Large-scale and diverse KPI streams

KPI streams are large in number and diverse in pattern.

• Train a PU learning model for each KPI stream?
  
  Too many manual labels are needed.
Challenge 1: Large-scale and diverse KPI streams

KPI streams are large in number and diverse in pattern.

- Train a PU learning model for each KPI stream?
  Too many manual labels are needed.
- Train a universal PU learning model for all KPI streams?
Challenge 1: Large-scale and diverse KPI streams

KPI streams are large in number and diverse in pattern.

- Train a PU learning model for each KPI stream?
  Too many manual labels are needed.

- Train a universal PU learning model for all KPI streams?
  The model will suffer from low accuracy and is difficult.
Challenge 2: Active learning strategy

Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.
Challenge 2: Active learning strategy

Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.

Step 2
Challenge 2: Active learning strategy

Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.
Challenge 2: Active learning strategy

Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.
KPI streams are large in number and diverse in pattern.
Contribution

KPI streams are large in number and diverse in pattern.

Utilize clustering, PU learning, and semi-supervised learning together to complete anomaly detection.
KPI streams are large in number and diverse in pattern.

Utilize clustering, PU learning, and semi-supervised learning together to complete anomaly detection.

Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.
## Contribution

- **KPI streams are large in number and diverse in pattern.**
- **Utilize clustering, PU learning, and semi-supervised learning together to complete anomaly detection.**
- **Active learning-assisted PU learning can improve its performance. However, it will produce many false positives.**
- **Select samples that are most likely to be positive in each iteration to label.**
Outline

Introduction  Challenges  Contribution  Framework  Evaluation
The framework of PUAD
Clustering in the offline training process

We can train an anomaly detection model for each cluster using a few manual labels, and “transfer” the trained model within each cluster.
Feature extraction in the offline training process

We extract and categorize the features into two groups: temporal features and forecasting error features.
The training set consisting of positive samples and unlabeled samples will be input together into the PU learning component.
The detailed framework of PU learning

- **Pre-training:** Initialize $\Omega(N)$.
- **Active learning-based self-training:** Extend $\Omega(P)$ and $\Omega(N)$.
For a newly emerging KPI stream A, assign it into an existing cluster and then extract its features. Train a model for it through semi-supervised learning.
For a newly arrived data point of the KPI stream A, its features would be firstly extracted. Then the features would be fed into the trained model to get an anomaly score.
## Dataset

### Dataset 1

<table>
<thead>
<tr>
<th>Process</th>
<th>Number of KPI streams</th>
<th>Interval (minute)</th>
<th>Total points</th>
<th>Anomaly points</th>
<th>Anomaly ratio (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustering</td>
<td>128</td>
<td>5</td>
<td>1024664</td>
<td>8318</td>
<td>0.81%</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>80</td>
<td>5</td>
<td>643593</td>
<td>6839</td>
<td>1.06%</td>
</tr>
</tbody>
</table>

### Dataset 2

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Interval (minute)</th>
<th>Total points</th>
<th>Anomaly points</th>
<th>Anomaly ratio (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>5</td>
<td>67740</td>
<td>3097</td>
<td>4.57%</td>
</tr>
<tr>
<td>Artificial</td>
<td>5</td>
<td>16128</td>
<td>624</td>
<td>3.87%</td>
</tr>
<tr>
<td>Twitter</td>
<td>5</td>
<td>142765</td>
<td>217</td>
<td>0.15%</td>
</tr>
</tbody>
</table>
Evaluation Metrics

\[
\text{precision} = \frac{TP}{TP + FP}
\]

\[
\text{recall} = \frac{TP}{TP + FN}
\]

\[
F1\text{- score} = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}
\]

\[
\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}
\]
## Baseline

<table>
<thead>
<tr>
<th>Type</th>
<th>Baseline method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervised</td>
<td>Apprentice</td>
</tr>
<tr>
<td>Unsupervised</td>
<td>Donut</td>
</tr>
<tr>
<td>Semi-supervised</td>
<td></td>
</tr>
<tr>
<td>Transfer learning</td>
<td></td>
</tr>
</tbody>
</table>
The effectiveness of different methods on dataset 1
The effectiveness of different methods on dataset 1
The effectiveness of different methods on dataset 2
The effectiveness of different methods on dataset 2
Ablation Study

The effectiveness of clustering and semi-supervised learning components

<table>
<thead>
<tr>
<th>Clusters</th>
<th>W/o active learning</th>
<th>With random labels</th>
<th>Label boundary</th>
<th>PUAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.612</td>
<td>0.697</td>
<td>0.812</td>
<td>0.920</td>
</tr>
<tr>
<td>2</td>
<td>0.545</td>
<td>0.576</td>
<td>0.667</td>
<td>0.967</td>
</tr>
<tr>
<td>3</td>
<td>0.819</td>
<td>0.850</td>
<td>0.860</td>
<td>0.851</td>
</tr>
<tr>
<td>4</td>
<td>0.745</td>
<td>0.720</td>
<td>0.860</td>
<td>0.872</td>
</tr>
<tr>
<td>5</td>
<td>0.596</td>
<td>0.714</td>
<td>0.785</td>
<td>0.839</td>
</tr>
<tr>
<td>6</td>
<td>0.458</td>
<td>0.664</td>
<td>0.638</td>
<td>0.737</td>
</tr>
<tr>
<td>7</td>
<td>0.871</td>
<td>0.900</td>
<td>0.872</td>
<td>0.921</td>
</tr>
<tr>
<td>8</td>
<td>0.714</td>
<td>0.762</td>
<td>0.793</td>
<td>0.812</td>
</tr>
<tr>
<td>9</td>
<td>0.587</td>
<td>0.589</td>
<td>0.673</td>
<td>0.675</td>
</tr>
<tr>
<td>Average</td>
<td>0.636</td>
<td>0.719</td>
<td>0.772</td>
<td>0.833</td>
</tr>
<tr>
<td>Increase ratio</td>
<td>31.0%</td>
<td>15.9%</td>
<td>7.9%</td>
<td>--</td>
</tr>
</tbody>
</table>

The effectiveness of active learning
Conclusion

- We propose PUAD, a PU learning-based method to accurately detect anomalies with a small number of partial labels for large-scale KPI streams.

- Clustering, PU learning, active learning, and semi-supervised learning are combined to achieve accurate anomaly detection and small labeling effort at the same time.

- PUAD applies a novel active learning strategy to avoid false alarms.

- Extensive evaluation experiments demonstrate that PUAD achieves close accuracy to supervised methods, and significantly outperforms existing semi-supervised learning-based, transfer learning-based, and unsupervised learning-based methods.
Thank you!

Q&A