Inter-Arrival Curves for Multi-Mode and Online Anomaly Detection

Mahmoud Salem, Mark Crowley, and Sebastian Fischmeister
Inter-arrival Curves for Anomaly Detection [1]

- Inter-arrival curves make good features for reasoning about recurrent behavior using event traces

- Promising classification results from an offline anomaly detection framework, however some anomalies go undetected

- Current research interest in online anomaly detection approaches

Problem Statement & Approach (1)

“Given a set of event traces generated by a well-specified system that exhibits several modes of operations, check whether a new trace from the same system reflects any of these modes of operation.”
Preliminary Evaluation: Multi-Mode Model

Using a single model falsely flags a normal mode of operation as anomalous.
“Given a set of event traces generated by a well-specified system in a given execution scenario, check on-the-fly whether a stream of events from the same system originates from the same execution scenario.”
Preliminary Evaluation: Online Anomaly Detection

- Synthetically stream trace data files

- Using $|T|_{\text{testing}} \approx \Delta_{\text{max}}$ and $|T|_{\text{testing}} << |T|_{\text{training}}$

<table>
<thead>
<tr>
<th>Training Scenario</th>
<th>Normal Testing Scenario</th>
<th>Anomalous Testing Scenario</th>
<th>TPR</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 files</td>
<td>129 files</td>
<td>185 files</td>
<td>84%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Target Contribution

• Online anomaly detection technique for event traces using inter-arrival curves

• Multi-mode classification framework using inter-arrival curves for improved anomaly detection

• Empirically demonstrate the feasibility and viability of the proposed approaches using event traces from embedded real-time systems
Thank you!