Anomaly Detection Framework for Cyber-Security Data

Marina Evangelou

Joint work with Niall Adams
Imperial College London

26 September 2017
As the number of cyber attacks, especially zero-day attacks and the emergence of advanced persistent threats (APT) is increasing, new approaches are required to complement the existing defence systems, for example signature based methods.

Such approaches include anomaly detection systems that seek to detect abnormal deviations from the “normal” behaviour of the network.
The aim of the proposed work is to model “normal” device behaviour and construct an anomaly detection framework based on the behaviour of each individual device.

The interest is on individual devices as a commonly observed pattern of a cyber-attack starts with the infection of an individual device.

Neil et al. (2013). *Scan Statistics for the Online Detection of Locally Anomalous Subgraphs*. Technometrics
Device behaviour is defined as the **network traffic** involving the device of interest observed within a pre-specified time period.

Network traffic data are obtained from NetFlow, a protocol operating at the router level which collects flow event logs and is widely used for **auditing** and **monitoring** a network.

```
time, duration, IP → IP, protocol, ports, packets, bytes
```

The data analysed and presented here are part of the anonymised "comprehensive, multi-source cyber-security events" dataset published by Los Alamos National Laboratory in 2015.
Device Behaviour

5 minutes time bin

2 events that start time within the time bin

NetFlow event start - end

Marina Evangelou
Anomaly Detection Framework for Cyber-Security Data
NetFlow Device Behaviour for 2 devices of the network
Regression models were built to model the relationship of the response variable $Y$ with a set of constructed features $X$ where:

- $Y$ is the number of events assigned to time bin $t + 1$
- $X$ represents the features constructed from the observed data of time bin $t$
Feature construction

<table>
<thead>
<tr>
<th>Time</th>
<th>Duration</th>
<th>Source Device</th>
<th>Source Port</th>
<th>Dest. Device</th>
<th>Dest. Port</th>
<th>Protocol</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>44369</td>
<td>13</td>
<td>C66</td>
<td>N23785</td>
<td>C585</td>
<td>445</td>
<td>6</td>
<td>14</td>
<td>3390</td>
</tr>
<tr>
<td>44370</td>
<td>0</td>
<td>C66</td>
<td>N978</td>
<td>C5721</td>
<td>445</td>
<td>6</td>
<td>8</td>
<td>3062</td>
</tr>
</tbody>
</table>

- Event related features:
  Number of events, Number of events with duration more than 5 minutes

- Nature related features:
  Number of events with specific protocol numbers

- Summary statistics of Duration, Bytes, Packets

- Time related features
  Working hours indicator, Working days indicator
Quantile Regression

- **Quantile Regression** aims to estimate the conditional quantiles from the data
- The $\tau^{th}$ conditional quantile minimizes the expected loss such that:
  \[ \min_{\beta} \sum_{i} \rho_{\tau}(y_i - X\beta) \]

  where:
  - $\rho_{\tau}(\cdot)$ is the quantile regression function


QRF in contrast to Random Forests keep the values of all observations in each node, not just their mean and assess the conditional distribution based on this information.
Prediction Intervals

- Let $Q_\alpha(x)$ be the $\alpha$-quantile such that
  $Q_\alpha(x) = \inf\{y : F(y|X = x) \geq \alpha\}$ where
  $F(y) = P(Y \leq y|X = x)$

- A $\eta\%$ prediction interval for the value of $Y$ is given by:
  $$I(x) = \{Q_{(1-\eta)/2}(x), Q_{(1+\eta)/2}(x)\}$$
  such that a 95% prediction interval is $\{Q_{0.025}(x), Q_{0.975}(x)\}$

- There is a high probability that a new observation of $Y$ given $X = x$ will lie in the prediction interval

- The width of the prediction interval depends on the observed feature vector
Predictions Intervals: 2.5% and 97.5% Conditional Quantiles
Observed device behaviour can be characterised as anomalous if it lies outside of the constructed prediction intervals of the QRF models, such that

\[
\begin{align*}
  y_{\text{observed}} &> Q(1+\eta)/2(x) \\
  y_{\text{observed}} &< Q(1-\eta)/2(x)
\end{align*}
\]

where \( y_{\text{observed}} \) is the recorded device behaviour.
The proposed anomaly detection framework was validated through a series of experiments.

The anomaly detector is compared to:

- **Benchmark Anomaly Detector**: any observed values outside of the 95% (unconditional) quantiles of device behaviour are classified as abnormal.

- Pruned Exact Linear Time (PELT): Change-point detection approach proposed by Killick et al. (2012).

Both the Benchmark anomaly detector and PELT do not rely on the feature vector.
The proposed anomaly detection framework was validated through a series of experiments.

The anomaly detector is compared to:

- **Benchmark Anomaly Detector**: any observed values outside of the 95% (unconditional) quantiles of device behaviour are classified as abnormal.

- **Pruned Exact Linear Time (PELT)**: Change-point detection approach proposed by Killick *et al.* (2012)
The proposed anomaly detection framework was validated through a series of experiments.

The anomaly detector is compared to:

- **Benchmark Anomaly Detector**: any observed values outside of the 95% (unconditional) quantiles of device behaviour are classified as abnormal.

- **Pruned Exact Linear Time (PELT)**: Change-point detection approach proposed by Killick et al. (2012)

The Benchmark anomaly detector intervals are the same across all time bins.

Both the Benchmark anomaly detector and PELT do not rely on the feature vector.
Validation Experiment

Normal Behaviour

Marina Evangelou

Anomaly Detection Framework for Cyber-Security Data
Validation Experiment

Contamination

Normal Behaviour
Validation Experiment

![Graphs showing normal and contaminated behavior]

Abnormal Deviations
Validation Experiment

<table>
<thead>
<tr>
<th>Detector</th>
<th>Accuracy</th>
<th>Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRF</td>
<td>0.959 (0.019)</td>
<td>0.934 (0.012)</td>
</tr>
<tr>
<td>PELT</td>
<td>0.544 (0.227)</td>
<td>0.349 (0.062)</td>
</tr>
<tr>
<td>Benchmark</td>
<td>0.930 (0.006)</td>
<td>0.935 (0.012)</td>
</tr>
</tbody>
</table>
NetFlow and Process device behaviour

NetFlow

Process

Number of events in a time bin

Time bin sequence
Process data: Feature construction

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Device</th>
<th>Process</th>
<th>Start/End</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>C66@DOM1</td>
<td>C66</td>
<td>N23785</td>
<td>Start</td>
</tr>
<tr>
<td>2</td>
<td>C66@DOM1</td>
<td>C66</td>
<td>N978</td>
<td>Start</td>
</tr>
</tbody>
</table>

- Event related features:
  Number of events, Number of events that only started in the time bin

- Nature related features:
  Entropy of processes

- Time related features
  Working hours indicator, Working days indicator
Process data: Predictions Intervals

Number of events in a time bin

Time bin sequence

Marina Evangelou
Anomaly Detection Framework for Cyber-Security Data
Conclusions

- Diverse device behaviours are observed across the network

- The QRF approach was found to have the best performance across a number of other tested regression models

- A data-driven anomaly detection framework is proposed that is based on prediction intervals of QRF models

- Through a number of validation experiments the proposed framework was found to outperform other detectors

- The anomaly detection framework can be extended for other data sources, e.g. process data
Thank you for listening! Any Questions?

- Data: https://csr.lanl.gov/data/cyber1/