Cross-Organizational Continual Learning of Cyber Threat Models

Chanel Cheng, Shanchieh Jay Yang

**Introduction**

- Intrusion detection systems are developed to help detect cyber threats across networks.
- Yet, cyber threats evolve over time and follow different patterns across various organizations.
  - Continuous detection of changing data is difficult by traditional means\(^1\)

**Consider:**

An incoming stream of network traffic from two different organizations.

- Similar attack types have different patterns across organizations
- New attack types are also present in each organization

Stream encounters both gradual and sudden changes in attack patterns

**Related Works**

PNNs / EWC / SI / iCaRL / GEM

- PNNs\(^6\) - constructs new networks as novel tasks occur, resulting in linearly increasing memory requirement.
- EWC & SI\(^5,6\) - extends loss function with a term that consolidates selective network weights, but requires explicit task boundaries.
- iCaRL\(^3\) - combined use of replay and distillation but still requires explicit task boundaries.
- GEM\(^3\) - builds optimization constraints using old data but less effective across shifting domains.

**Methodology**

**Table 1.** Side-by-side comparison of continual learning strategies\(^3\)

<table>
<thead>
<tr>
<th>Methods</th>
<th>PNN</th>
<th>P2Net</th>
<th>BIL</th>
<th>ER</th>
<th>GS5</th>
<th>GEM</th>
<th>HAL</th>
<th>Cali</th>
<th>FDR</th>
<th>Gd</th>
<th>Sl</th>
<th>iCaRL</th>
<th>GEM</th>
<th>DERR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant memory</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>No task boundaries</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>No task oracle</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Experiment & Results**

**Figure 1.** Example data stream for task-agnostic continual learning on network traffic flow from CIC-IDS-2018\(^8\) and USB-IDS-2021\(^9\)

- Two datasets were converted into a single data stream for continual learning without task boundaries.
  - Regular benign traffic and malicious traffic are present together in stream (with benign as the majority of traffic)
  - Order and source of data does not matter for our continual model in learning the attack types

**Observations & Future Works**

- By the 10th iteration, no more samples are required to be labeled, while most of the F1-scores reach above 0.9 except DoS-GoldenEye (~0.88) and DoS-Slowloris (~0.8), both of which have a much smaller sample size.
- This learning strategy largely reduces the number of labeled data needed and can quickly reach good prediction performance.

**Future Works:**

1) Expand the experiment to include more attack types, 2) further investigate class imbalance issue, and 3) optimize the sampling strategy for replay buffer.

**References**


---

**Table 2.** Aggregate port mapping and one-hot encoding maps the most commonly used port numbers to their corresponding port services and one-hot encodes them as features for the model to learn from.

<table>
<thead>
<tr>
<th>Port Service</th>
<th>Port #</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>HTTP</td>
<td>80, 8080</td>
</tr>
<tr>
<td>https</td>
<td>443, 8443</td>
</tr>
<tr>
<td>smb</td>
<td>139, 137</td>
</tr>
<tr>
<td>Rtp</td>
<td>20, 21</td>
</tr>
<tr>
<td>ssh</td>
<td>22</td>
</tr>
<tr>
<td>ltm</td>
<td>5555</td>
</tr>
<tr>
<td>other</td>
<td>(unassigned port #s)</td>
</tr>
</tbody>
</table>