Leveraging interdomain stability for squeezed and juicy BGP dynamics

Authors

Thomas GREEN (PhD Student)
Anthony LAMBERT (PhD Advisor)
Dario ROSSI (PhD Director)
Cristel PELSSER (Researcher)

Research objectives

Context
- Border Gateway Protocol: path vector protocol
- Internet (Autonomous Systems) relationships based on trust
- Robustness/integrity is questionable: more and more incidents, attacks

Goals (long term)
- Detection of abnormal routing events
- Mitigation

Challenges

Complexity
- High verbosity and number of networks
- "Path Selection" is made hop-by-hop
- Routing policies are not known
- Opaque and complex environment

Requirements
- Online methodology
- Real-time detection and mitigation

Approach

Leverage interdomain stability

- Construct a referential: « Primary Paths »
  - For each <router, prefix> pairs, one path is preferred (most used) for a given time-window
  - Updates are compared to this nominal value and interpreted as deviations (abnormal behavior) if they don’t match

Interpreted deviations: « Pseudo-events »
- Primary path unavailabilities, defined by:
  - Starting time (fall of the PP): t_s
  - End time (recovery of the PP): t_e
  - Sequence of paths explored: X
- Two types:
  - Transient (spontaneous change)
  - Structural (planned change)

Squeezed: dimension reduction

<table>
<thead>
<tr>
<th></th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of events</td>
<td>487,104,558</td>
<td>157,249,182</td>
</tr>
<tr>
<td>Number of pseudo-events</td>
<td>57,066,053</td>
<td>17,687,525</td>
</tr>
<tr>
<td>Structural pseudo-events</td>
<td>1,406,392</td>
<td>78,995</td>
</tr>
<tr>
<td>Transient pseudo-events</td>
<td>55,659,661</td>
<td>17,608,530</td>
</tr>
<tr>
<td>Gain (events/pseudo-events)</td>
<td>8.5</td>
<td>8.9</td>
</tr>
</tbody>
</table>

Comparative table of dimension gain using pseudo-events

Juicy: increased semantic

<table>
<thead>
<tr>
<th></th>
<th>Reported</th>
<th>Outages</th>
<th>Reported</th>
<th>Hijacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source: BGP raw data taken from RIPE RIS RRC01 collector from January 1st to March 31st 2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td><a href="mailto:thomas.green@telecom-paristech.fr">thomas.green@telecom-paristech.fr</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site web</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>