United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale

Daniel Wagner\textsuperscript{1,2}

Daniel Kopp\textsuperscript{1}, Matthias Wichtlhuber\textsuperscript{1}, Christoph Dietzel\textsuperscript{1,2}, Oliver Hohlfeld\textsuperscript{3},

Georgios Smaragdakis\textsuperscript{4} and Anja Feldmann\textsuperscript{2}
Distributed Denial of Service (DDoS)

- Network attack causing service downtime
- Targets: Financial services, health sector, ...
Amplification DDoS Attacks

Attacker

Requests with spoofed source IP address

Reflectors

Responses up to 51,200x larger

Target
Amplification DDoS Attacks

Attacker

Requests with spoofed source IP address

Reflectors

Local scrubbing service

Target
Amplification DDoS Attacks

Attacker

Requests with spoofed source IP address

Reflectors

IXPs in the core

Target
Contributions (1/3)

- Distance analysis
  - #hops from reflector?
  - #hops to target?
Contributions (2/3)

- Distance analysis
  - #hops from reflector?
  - #hops to target?
- Collaboration benefit
Contributions (3/3)

- Distance analysis
  - #hops from reflector?
  - #hops to target?
- Collaboration benefit
- Information exchange platform
Contributions (3/3)

- Distance analysis
  - #hops from reflector?
  - #hops to target?
- Collaboration benefit
- Information exchange platform
- Let’s leverage some data!
### Data Set

- **Flow data from 11 IXPs, April 2020 – October 2020**

<table>
<thead>
<tr>
<th>IXP Code</th>
<th>#Networks</th>
<th>Peak traffic</th>
<th>Region</th>
<th>#sampled Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE1</td>
<td>&gt;900</td>
<td>&gt;9000 Gb/s</td>
<td>Central Europe</td>
<td>1.08 Trillion</td>
</tr>
<tr>
<td>CE2</td>
<td>&gt;200</td>
<td>&gt;150 Gb/s</td>
<td>Central Europe</td>
<td>9.9 Billion</td>
</tr>
<tr>
<td>CE3</td>
<td>&gt;200</td>
<td>&gt;150 Gb/s</td>
<td>Central Europe</td>
<td>3.2 Billion</td>
</tr>
<tr>
<td>CE4</td>
<td>&gt;200</td>
<td>&gt;100 Gb/s</td>
<td>Central Europe</td>
<td>3.6 Billion</td>
</tr>
<tr>
<td>NA1</td>
<td>&gt;200</td>
<td>&gt;800 Gb/s</td>
<td>North America</td>
<td>78 Billion</td>
</tr>
<tr>
<td>NA2</td>
<td>&gt;75</td>
<td>&gt;150 Gb/s</td>
<td>North America</td>
<td>16.7 Billion</td>
</tr>
<tr>
<td>SE1</td>
<td>&gt;175</td>
<td>&gt;400 Gb/s</td>
<td>South Europe</td>
<td>30.5 Billion</td>
</tr>
<tr>
<td>SE2</td>
<td>&gt;75</td>
<td>&gt;100 Gb/s</td>
<td>South Europe</td>
<td>12.2 Billion</td>
</tr>
<tr>
<td>SE3</td>
<td>&gt;40</td>
<td>&gt;10 Gb/s</td>
<td>South Europe</td>
<td>2.2 Billion</td>
</tr>
<tr>
<td>SE4</td>
<td>&gt;30</td>
<td>&gt;100 Gb/s</td>
<td>South Europe</td>
<td>17.9 Billion</td>
</tr>
<tr>
<td>SE5</td>
<td>&gt;20</td>
<td>&gt;50 Gb/s</td>
<td>South Europe</td>
<td>2 Billion</td>
</tr>
</tbody>
</table>
Traffic Filtering

• UDP only
• Filtering for typical DDoS amplification protocols\(^2\)
• Packet size\(^2\)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Chargen</th>
<th>DNS</th>
<th>RPC</th>
<th>NTP</th>
<th>SNMP</th>
<th>CLDAP</th>
<th>OpenVPN</th>
<th>SSDP</th>
<th>ARMS</th>
<th>WS Discovery</th>
<th>Device Discovery</th>
<th>memcached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport port</td>
<td>19</td>
<td>53</td>
<td>111</td>
<td>123</td>
<td>161</td>
<td>389</td>
<td>1194</td>
<td>1900</td>
<td>3283</td>
<td>3702</td>
<td>10001</td>
<td>11211</td>
</tr>
</tbody>
</table>

Attack Detection

- Global attack traffic with $n \geq 10$ reflectors, $t > 1\text{Gbps}$ attack traffic
- We identified $>120k$ DDoS attacks
- Including confirmed attacks
• Thousands of attacks every day!
Case study: Attack to Akamai

Case study: Attack to Akamai

Local detection feasible

Case study: Attack to Akamai

1.44 Tbps and 385 Mpps DDoS Attack Mitigated by Akamai

How accurate are we? (1/2)

• Compare found events to benign data
  • Traffic to IP addresses that was
    • Caught by the filter
    • Not caught by the detection mechanism
  • Compare traffic characteristics
  • Geographical distribution and port combinations
Benign Traffic vs. Attacks: Sites / Ports

![Graph showing the comparison between benign traffic and attacks in terms of sites and ports.](image)

- **X-axis:** Diversity [Sites/Ports/SitePortCombinations]
- **Y-axis:** eCDF(Diversity)
- **Legend:**
  - Attack Sites
  - Attack Ports
  - Attack SitesPorts
  - Benign Sites
  - Benign Ports
  - Benign SitesPorts

The graph illustrates the distribution of sites and ports across benign traffic and attacks, highlighting differences in diversity metrics.
Self-Attacks: Features and Clustering

Sample features to the rotation of the first 4 PCAs

3 most explaining PCs (25% of the variance)
How accurate are we? (2/2)

• Compare found events to benign data
  • Traffic to IP addresses that was
    • Caught by the filter
    • Not caught by the detection mechanism
  • Compare traffic characteristics
  • Geographical distribution and port combinations

• Fire up self-attacks to get ground truth
  • Derive and compare features
  • Compare packet sizes
Packet Sizes

![Graph showing packet sizes for different protocols and traffic types (Attacks, Self Attacks, Benign traffic).]
Contributions (1/3)

- Distance analysis
  - #hops from reflector?
  - #hops to target?
- Collaboration benefit
- Information exchange platform

Reflectors

Target

Dist = ?
Distance analysis

- Hops counted from IXP’s RS
- About 45% of attack traffic originates from a direct neighbor
- About 70% of attack traffic’s destination is just two hops away
Contributions (2/3)

- Distance analysis
- #hops from reflector?
- #hops to target?
- Collaboration benefit
- Information exchange platform
Attack Events

- Ground truth of combined data
Attack Events

- Ground truth of combined data
- Versus local detectable attack traffic
Collaboration benefit

![Collaboration benefit graph](image)

- **Collaboration benefit**

  - **Location**:
    - SE5
    - SE3
    - CE3
    - CE4
    - SE2
    - CE2
    - SE4
    - NA2
    - SE1
    - NA1
    - CE1

- **Missed % of traffic**
  - **Global: Threshold 100 Mbps**
  - **Local: Threshold 100 Mbps**
Collaboration benefit

- Up to ~80% of attacks locally undetected („missed“)
Collaboration benefit

- Up to ~80% of attacks locally missed (100mb/s)
- Up to ~90% of attacks locally missed (1Gb/s)
Contributions (3/3)

- Distance analysis
- #hops from reflector?
- #hops to target?
- Collaboration benefit
- Information exchange platform
DDoS Information Exchange Point (DXP)
DDoS Information Exchange Point (DXP)

- Governance body
- Defines filters and thresholds
- Builds community
- Handles SLAs
- Processes abuse cases
DDoS Information Exchange Point (DXP)

- Members pull and push rules from / to the DXB
- Apply filters
- Choose a trust scenario
DDoS Information Exchange Point (DXP)

- **Low trust:**
  - Reflector’s IP shared
  - Semi-sensitive
- **High trust:**
  - All information shared
  - Scr/dst IP & port
  - Traffic volume
  - Duration
  - ....
DXP Evaluation: Low Trust - High Trust

Location

Low trust

High trust

- Attacks with traffic
- Detectable attacks — Boosted (threshold: 50 Mbps)
- Detectable attacks — Boosted (threshold: 100 Mbps)
- Detectable attacks — Boosted (threshold: 1000 Mbps)
- Detectable attacks — Boosted (threshold: 5000 Mbps)
- Detectable attacks — Boosted (threshold: 10000 Mbps)

# of attacks (in K)

0 50 100 150

0 50 100 150
Conclusion

• Quantification of DDoS origin distribution
  • About 50% of attacks in >=3 locations, about 25% in >=5 locations
Conclusion

• Quantification of DDoS origin distribution
  • About 50% of attacks in >=3 locations, about 25% in >=5 locations

• Quantification of collaboration benefit
  • >80% of the globally detectable attacks are not detected locally
Conclusion

• Quantification of DDoS origin distribution
  • About 50% of attacks in >=3 locations, about 25% in >=5 locations

• Quantification of collaboration benefit
  • >80% of the globally detectable attacks are not detected locally

• Emphasis on IXP’s critical role for DDoS mitigation
  • About 45% of the reflectors and about 30% of the targets are an IXP member
Conclusion

• Quantification of DDoS origin distribution
  • About 50% of attacks in >=3 locations, about 25% in >=5 locations

• Quantification of collaboration benefit
  • >80% of the globally detectable attacks are not detected locally

• Emphasis on IXP’s critical role for DDoS mitigation
  • About 45% of the reflectors and about 30% of the targets are an IXP member

• Collaboration platform proposal and evaluation
  • DXP
  • Up to 90% more attack traffic detectable at a site due to collaboration
(Backup Slides)
Distance / geographical distribution analysis

![Graph showing distance/geographical distribution analysis](image)

- **75th percentile Mbps (log)**

- **Locations**: CE1, CE2, CE3, CE4, NA1, SE1, SE2, SE3, SE4, SE5

- **Colors**:
  - Blue: announcement at CE1 only
  - Orange: announcement at all locations
# Features

<table>
<thead>
<tr>
<th>Feature Class</th>
<th>Feature Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>1</td>
<td>Number of sites involved in the attack</td>
</tr>
<tr>
<td>Ports</td>
<td>1</td>
<td>Number of source transport ports involved in the attack</td>
</tr>
<tr>
<td>SitesPorts</td>
<td>1</td>
<td>Sum of source transport ports seen at the sites, where the attack is visible</td>
</tr>
<tr>
<td>DOR</td>
<td>1</td>
<td>Total duration of the attack in minutes</td>
</tr>
<tr>
<td>DurAttack</td>
<td>1</td>
<td>Duration in minutes where the attack volume is greater than ( t ) (in our study: 1 Gbps)</td>
</tr>
<tr>
<td>TotalMBps</td>
<td>1</td>
<td>Volume of the attack in Mbps, summed across all sites and all source transport ports</td>
</tr>
<tr>
<td>TotalMBpsAttack</td>
<td>1</td>
<td>Volume of the attack in Mbps, summed across all sites and all source transport ports, while the volume is greater than ( t )</td>
</tr>
<tr>
<td>TotalPeakMBps</td>
<td>1</td>
<td>Peak of the attack volume in Mbps, summed across all sites and all source transport ports</td>
</tr>
<tr>
<td>PeakMBps</td>
<td>1</td>
<td>Peak of the attack volume in Mbps, single site, single source transport port</td>
</tr>
<tr>
<td>TotalMBpsCE1</td>
<td>1</td>
<td>Sum of the attack traffic across all source transport ports in Mbps, seen at site CE1</td>
</tr>
<tr>
<td>TotalMBpsAttackCE1</td>
<td>1</td>
<td>Sum of the attack volume across all source transport ports in Mbps, seen at site CE1 while exceeding ( t )</td>
</tr>
<tr>
<td>TotalPeakMBpsCE1</td>
<td>1</td>
<td>Peak attack volume across all source transport ports, seen at site CE1, in Mbps</td>
</tr>
<tr>
<td>PeakMBpsCE1</td>
<td>1</td>
<td>Peak attack volume of a single source transport port, seen at site CE1, in Mbps</td>
</tr>
<tr>
<td>TotalMBpsNoCE1</td>
<td>1</td>
<td>Volume of the attack in Mbps, seen at all sites but CE1, all source transport ports</td>
</tr>
<tr>
<td>TotalMBpsAttackNoCE1</td>
<td>1</td>
<td>Volume of the attack in Mbps, seen at all sites but CE1, all source transport ports while exceeding ( t )</td>
</tr>
<tr>
<td>TotalPeakMBpsNoCE1</td>
<td>1</td>
<td>Peak volume of the attack in Mbps, seen at all sites but CE1, across all source transport ports</td>
</tr>
<tr>
<td>PeakMBpsNoCE1</td>
<td>1</td>
<td>Peak volume of the attack in Mbps, seen at all sites but CE1, across a single transport port</td>
</tr>
<tr>
<td>Cor [SitePort]</td>
<td>6</td>
<td>Counter for correlation of the attack between sites and source transport ports, respectively, being greater than ( 7, 8, 9 ), respectively per minute</td>
</tr>
<tr>
<td>TotalMBps[XP*]</td>
<td>11</td>
<td>Volume of the attack in Mbps, as seen at the 11 sites, all source transport ports, respectively</td>
</tr>
<tr>
<td>TotalMBps[PORT*]</td>
<td>12</td>
<td>Volume of the attack in Mbps, summed across all sites, for each of the 12 source transport ports in our study</td>
</tr>
<tr>
<td>PeakMBps[XP*]</td>
<td>11</td>
<td>Peak volume of the attack in Mbps, as seen at the 11 sites, respectively, single source transport port</td>
</tr>
<tr>
<td>PeakMBps[PORT*]</td>
<td>12</td>
<td>Peak volume of the attack in Mbps, summed across all sites, for each of the 12 source transport ports in our study</td>
</tr>
<tr>
<td>TotalMBps</td>
<td>1</td>
<td>Sum of packets transmitted for the attack across all sites, all source transport protocols, in Mpps</td>
</tr>
<tr>
<td>TotalMBpsAttack</td>
<td>1</td>
<td>Sum of packets transmitted for the attack across all, all source transport ports, sites while exceeding ( t ), in Mpps</td>
</tr>
<tr>
<td>TotalPeakMBps</td>
<td>1</td>
<td>Peak of packets transmitted for the attack, summed across all sites, all source transport protocols, in Mpps</td>
</tr>
<tr>
<td>PeakMBps</td>
<td>1</td>
<td>Peak of packets transmitted for the attack at any site, single transport port, in Mpps</td>
</tr>
<tr>
<td>TotalMBps[XP*]</td>
<td>11</td>
<td>Sum of packets transmitted across all source transport ports, at the 11 sites, respectively</td>
</tr>
<tr>
<td>TotalMBps[PORT*]</td>
<td>12</td>
<td>Sum of packets transmitted at all sites, for each of the 12 source transport protocols in our study</td>
</tr>
<tr>
<td>TotalMBpsNorm</td>
<td>1</td>
<td>Volume of the attack, summed across all source transport ports and all sites, normalized by their size</td>
</tr>
<tr>
<td>Feature Class</td>
<td>Feature Count</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TotalMByteAttNetNorm</td>
<td>1</td>
<td>Volume of the attack in Mbytes, summed across all source transport ports, all sites, normalized by its size, while exceeding 1</td>
</tr>
<tr>
<td>TotalPkMByteAttNorm</td>
<td>1</td>
<td>Peak of the attack volume in Mbytes, summed across all source transport ports, all sites, normalized by its size, while exceeding 1</td>
</tr>
<tr>
<td>PeakMByteAttNorm</td>
<td>1</td>
<td>Peak of the attack volume in Mbytes, single source transport port, any site, single site, normalized by its size</td>
</tr>
<tr>
<td>TotalMByteAttNetC1</td>
<td>1</td>
<td>Volume of the attack in Mbytes, all source transport ports, seen at all sites but C1, normalized by their size</td>
</tr>
<tr>
<td>TotalMByteAttNetNormC1</td>
<td>1</td>
<td>Volume of the attack in Mbytes, all source transport ports, seen at all sites but C1, normalized by their size, while exceeding 1</td>
</tr>
<tr>
<td>TotalPkMByteAttNormC1</td>
<td>1</td>
<td>Peak volume of the attack, summed across all source transport ports, seen at all sites but C1, normalized by their size</td>
</tr>
<tr>
<td>PeakMByteAttNormC1</td>
<td>1</td>
<td>Peak volume of the attack, single source transport ports, seen at all sites but C1, normalized by their size</td>
</tr>
<tr>
<td>TotalMByteNet&lt;1626MB</td>
<td>1</td>
<td>Volume of the attack in Mbytes, all source transport ports, as seen at the 16 sites, normalized by their size, respectively</td>
</tr>
<tr>
<td>PeakMByteNet&lt;1626MB</td>
<td>1</td>
<td>Peak volume of the attack, single source transport port, as seen at the 16 sites, normalized by their size, respectively</td>
</tr>
<tr>
<td>AllBytesBefore [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source ports that belong to an attack, greatest volume of a single site, before the respective threshold was exceeded</td>
</tr>
<tr>
<td>AllBytesDetect [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source ports that belong to an attack, greatest volume of a single site, while the respective threshold is exceeded</td>
</tr>
<tr>
<td>AllBytesAfter [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source transport ports that belong to an attack, greatest volume of a single site, after the respective threshold is no longer exceeded</td>
</tr>
<tr>
<td>AllBytesTime [THRESHOLD]</td>
<td>7</td>
<td>Amount of time bins for which the attack volume across all source transport ports, greatest of all single sites, exceeded the respective threshold</td>
</tr>
<tr>
<td>AllBytesNeverBefore [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source ports that belong to an attack, greatest of a single site, normalized by its size, before the respective threshold was exceeded</td>
</tr>
<tr>
<td>AllBytesNeverDetect [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source ports that belong to an attack, greatest of a single site, normalized by its size, while the respective threshold is exceeded</td>
</tr>
<tr>
<td>AllBytesNeverAfter [THRESHOLD]</td>
<td>7</td>
<td>Volume of traffic across all source transport ports that belong to an attack, greatest of a single site, normalized by its size, after the respective threshold is no longer exceeded</td>
</tr>
<tr>
<td>AllBytesNeverTime [THRESHOLD]</td>
<td>7</td>
<td>Amount of time bins for which the attack volume across all source transport ports, greatest of all single sites, normalized by its size, exceeded the respective threshold</td>
</tr>
<tr>
<td>SiteBytes [4096MB] Before [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, for every site respectively, single source transport port, before exceeding the respective threshold</td>
</tr>
<tr>
<td>SiteBytes [4096MB] After [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, for every site respectively, single source transport port, after the respective threshold is no longer exceeded</td>
</tr>
<tr>
<td>SiteBytes [4096MB] Detect [THRESHOLD]</td>
<td>77</td>
<td>Amount of time bins for every site respectively, for every threshold, single source transport port, before exceeding the respective threshold</td>
</tr>
<tr>
<td>GlobalBytes [4096MB] Before [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, adding all site’s volume to every site respectively, all source transport ports, before exceeding the respective threshold</td>
</tr>
<tr>
<td>GlobalBytes [4096MB] After [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, adding all site’s volume to every site respectively, all source transport ports, after the respective threshold is no longer exceeded</td>
</tr>
<tr>
<td>GlobalBytes [4096MB] Detect [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, adding all site’s volume to every site respectively, all source transport ports, while exceeding the respective threshold</td>
</tr>
<tr>
<td>SiteBytesNever [4096MB] Before [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, for every site respectively, normalized by its size, single source transport port, before exceeding the respective threshold</td>
</tr>
<tr>
<td>SiteBytesNever [4096MB] After [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, for every site respectively, normalized by its size, single source transport port, after the respective threshold is no longer exceeded</td>
</tr>
<tr>
<td>SiteBytesNever [4096MB] Detect [THRESHOLD]</td>
<td>77</td>
<td>Volume of the attack, for every site respectively, normalized by its size, single source transport port, while exceeding the respective threshold</td>
</tr>
<tr>
<td>SiteBytesNever [4096MB] Time [THRESHOLD]</td>
<td>77</td>
<td>Amount of time bins, for every site respectively, normalized by its size, for every threshold, single source transport port, before exceeding the respective threshold</td>
</tr>
</tbody>
</table>

Total: 1106
Figure 21: Relative: Sensitivity of the detectable DDoS attacks in the low trust DXP setting for different boosting factors.
Boosting Factor evaluation (2)

Figure 22: Absolute: Sensitivity of the detectable DDoS attacks in the low trust DXP setting for different boosting factors.
Boosting Factor evaluation (3)

Figure 23: Sensitivity of the share of the attack traffic detected in the low trust DXP setting for different boosting factors.