MULTOPS

A data-structure for bandwidth attack detection

Thomer M. Gil
Vrije Universiteit, Amsterdam, Netherlands
MIT, Cambridge, MA, USA
thomer@lcs.mit.edu

Massimiliano Poletto
Mazu Networks, Inc., Cambridge, MA, USA
maxp@mazunetworks.com
Bandwidth attacks

• Maliciously generated traffic congests links

• Traffic is typically ICMP, UDP, or TCP

• IP spoofing: fake IP source addresses

• Distribution: multiple hosts pounding one victim
MULTOPS heuristic

Normal: proportional packet rates

Attack: disproportional packet rates

Drop packets from sources sending disproportionate flows
Feb 2000: ICMP flood

+ MULTOPS identifies attackers’ addresses
+ MULTOPS drops packets from those addresses
Implementation challenges

- Precise identification of malicious addresses
- Small memory footprint
- Minimal impact on forwarding performance
Naive data-structure

<table>
<thead>
<tr>
<th>from-rate</th>
<th>to-rate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>460</td>
<td>474</td>
<td>18.26.4.9</td>
</tr>
<tr>
<td>2,450</td>
<td>189</td>
<td>18.26.4.10</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

- Identifies individual attackers
- Requires too much memory
- Most entries are zero or insignificant
- Total packet rate per subnet expensive to calculate

$2^{32}$ entries
### Less naive data-structure

<table>
<thead>
<tr>
<th>from-rate</th>
<th>to-rate</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>0</td>
<td>0.0.0.0/8</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>18.0.0.0/8</td>
</tr>
<tr>
<td>528,238</td>
<td>518,234</td>
<td>19.0.0.0/8</td>
</tr>
<tr>
<td>309,988</td>
<td>20,876</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>255.0.0.0/8</td>
</tr>
</tbody>
</table>

- Requires little memory
- May not detect small attacks
- Prefixes very short; risky to use for dropping policy
- Impossible to collect finer grained data

256 entries
MULTOPS

+ Provides packet rates on different aggregation levels
+ Expands and contracts dynamically
+ Disregards insignificant subnets and addresses
+ Memory efficient
<table>
<thead>
<tr>
<th>from-rate</th>
<th>to-rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>2,986</td>
<td>2,746</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

source: 18.26.4.9
destination: 130.37.24.4

source: 130.37.24.4
destination: 18.26.4.9

Algorithm

18.0.0.0/8
Expansion

Nodes dynamically created to track finer grained packet rates

IP address

- 64
- 28
- 67
- 150

- Update rate for 64.0.0.0/8
- Update rate for 64.28.0.0/16; exceeds threshold: create child node
- Update rate for 64.28.67.0/24 in newly created node
Contraction

- MULTOPS could run out of memory
  - Attackers may cause this intentionally
- Impose absolute memory limit
- Contract stale parts of the tree periodically
+ MULTOPS drops packets with malicious address prefix
  • Collateral damage depends on length of address prefix
MULTOPS dropping decision

• Drop packet based on 2 criteria
  • Packet rate > 100 packets per second, and
  • Ratio > 1:3

• Values determined through experimentation
Randomized source addresses

• Impossible to identify attackers’ addresses

• Easy to identify victim’s address

• Drop packets based on victim’s address

• 2 MULTOPS to stop both attack types
  • Source-based MULTOPS: non-randomized attacks
  • Destination-based MULTOPS: randomized attacks
Reverse orientation

+ MULTOPS drops packets going to victim
+ Victim’s network relieved from malicious traffic
- MULTOPS drops benign packets going to victim
Performance

• MULTOPS implemented in Click, a modular router

• Forwarding speed inversely related to size of tree

• Forwards up to 825,000 packets per second
  • Pentium III, 833MHz PC
  • 256MB main memory, 256KB cache

• Better performance than reported in paper
  • Simpler mechanism to compute packet rates
Cycles per packet for different attacks

![Graph showing cycles per packet for different attacks with 16 MB, 8 MB, and 2 MB data sizes.](image)
Status

• Enhanced MULTOPS used by Mazu Networks

• Has detected TCP floods on commercial networks
  • Identified a single 8-bit malicious address prefix
Future work and problems

• Different ACK policies change ratio for valid traffic

• Not all Internet traffic is TCP

• Asymmetric routes
  • MULTOPS must see traffic in both directions
  • Requires distributed data collection
Related work

- Ingress/egress filtering (RFC2827)
- IP Traceback (Savage et al.)
- CenterTrack (Stone)
- Pushback (Bellovin et al.)
- RMON, Netflow (Cisco)

MULTOPS is complementary
Conclusion

- MULTOPS identifies attacker/victim addresses

- Effectiveness depends on
  - MULTOPS location on network
  - Randomized source address

- MULTOPS successfully detects and stops attacks