MIDAS
An Impact Scale for DDoS attacks

Kobus Van der Merwe
with
Rangarajan Vasudevan, Morley Mao and Oliver Spatscheck

Motivation

DDoS attacks are an unfortunate fact of life on today's Internet

- Always active ongoing attacks
- Attacks typically against end-hosts
  - Protect end-hosts under attack
  - Networks have to deal with increased traffic demands
  - Can cause collateral damage

Needs to measure the severity of these attacks

- If we can't measure it we can't really understand/study it

Currently: packets/bits per second

- Misleading, 100Mbps attack against a multi-Gbps data center is quite different from a 2 Mbps attack against a T1 access link

Motivation

Well developed metrics for natural phenomena

- Richter Scale measures magnitude of an earthquake
  - Absolute measure of size, regardless of damage
- Fujita Scale measure actual damage of a tornado
  - Measure of impact rather than size
  - Same tornado, different impact different structures

Need something similar for DDoS attacks

- Lots of ongoing attacks, need to know which attacks to mitigate
- Use to study DDoS trends over time
- Use in modeling to understand the effectiveness of different architectures and mitigation strategies
- Potentially used to compare different networks

Requirements for a DDoS Metric

- Based on impact of an attack as opposed to the absolute magnitude
  - A more robust (better managed, engineered) network will be able to better withstand a DDoS attack of certain magnitude
  - Not all DDoS attacks impact network or customers
- Have to be driven by economic impact
  - Estimate economic impact based on network measurements
- Simple enough to calculate in real-time
  - Need to react to attacks in real time

MIDAS: Measure of Impact of DDoS AttackS

- Service provider viewpoint
- Relative metric
  - Same MIDAS metric = Same relative economic impact

Economic impact of DDoS attacks

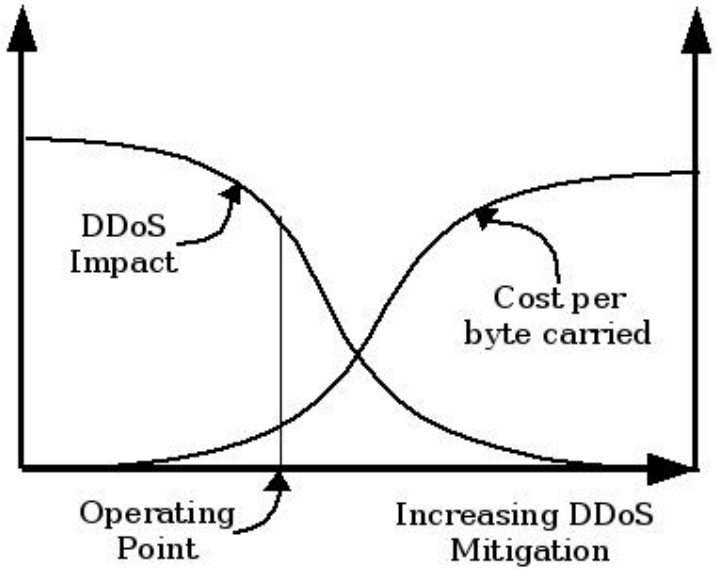
Increasing DDoS mitigation:

- Increase the cost-per-byte carried
- Decrease the impact of DDoS attacks

Represents a tension for service providers

Flat-rate billing: increased cost reduce operator income

Usage billing: increased traffic (good or bad) increase operator income



Main driver to convince providers to address provider impact of DDoS attacks:

- Potential loss of revenue:
  - Penalties when SLAs are violated (SLA cost)
  - Loss of revenue when customers leave or go out of business (Risk cost)

SLA cost

Providers have to pay penalties when service level agreements are violated

Penalties typically related to revenues provider would have received from customer

SLAs typically include:

- Network wide performance metrics (loss, delay etc)
- Reliability: site-to-site availability
- Packet delivery guarantees
- Outage reporting guarantees
- Power availability

SLA cost: sum of revenues of all impacted customers

Risk Cost

Cost associated with losing customer

= Future customer revenue * Risk customer leaving

- Future customer revenue
  - Proportional to current revenue
- Risk of customer leaving
  - Proportional to:
    - Attack scope: how much traffic impacted
    - Attack duration: how long impact was suffered
    - Attack frequency: how often impact was suffered
  - Increase in any of these leads to increase in risk
  - How much of what? Somewhat arbitrary choices:
    - 1% traffic impacted
      - Impacted means “application specific quality metrics not satisfied”
      - 1% becomes noticeable to application/protocols
    - Dissatisfaction grow non-linear with duration of attack
      - Capture as number of 10 minute bins attacks last
    - Dissatisfaction grow non-linear with frequency of attack
      - Number of attacks in 12 month period
  - Combine into risk expression

MIDAS Scale

Cost of a DDoS attack = Cost of SLA violations + Cost/Risk of customers leaving

MIDAS_factor = (Cost of DDoS attack) /(Total provider revenue)

Calculating this in real time is difficult

Estimate using the MIDAS_network_factor

- Provisioned bandwidth proportional to used capacity proportional to revenue

Specifics:

- Total provider revenue proportional to total provider capacity
- Customer revenue proportional to customer access capacity
- Risk of customer leaving proportional to capacity of links impacted by the attack
- Impacted customer:
  - 1% of traffic in last 10 minutes traversed a link with at least 5% packe

Can be calculated in real time

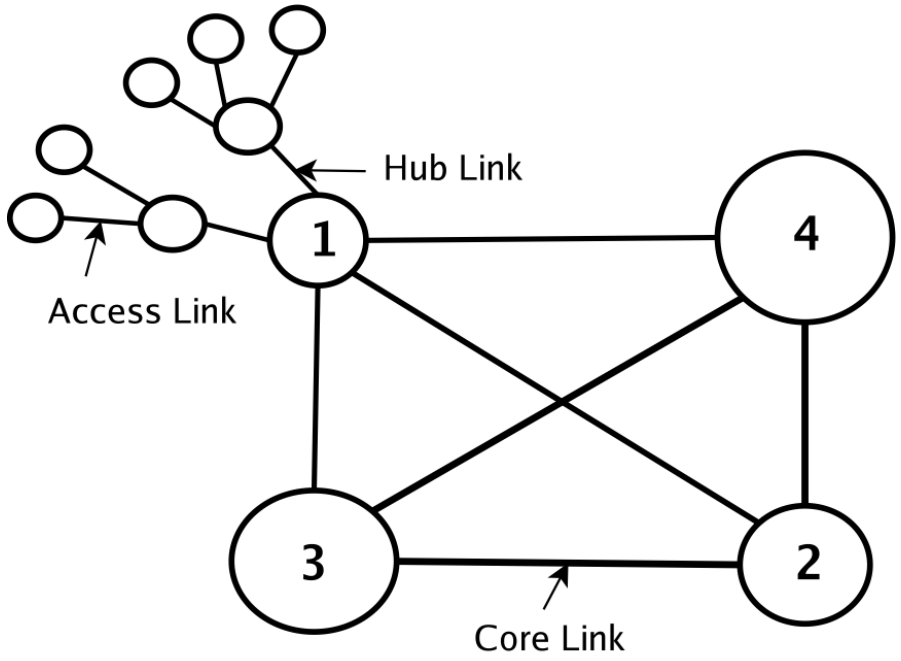
Validation

Hypothetical topology, synthetic attacks

- Capacities/Nodes based on population density of US
- Assume three tiered PoP architecture
- Show that MIDAS scale value reflect intuitive network impact of different attacks

Simulator:

- Scale attacks up/down
- Determine when links are impacted
- Calculate MIDAS value



Validation

DDoS attacks “types”:

- Strong and concentrated (s&c): large volume, originates from small number of sources, targets small number destinations
- Weak and concentrated (w&c): as above but lower attack volume
- Strong and distributed (s&d): large volume, multiple sources, several destinations
- Weak and distributed (w&d): as above but lower attack volume

Validation results: attack types

Concentrated attacks:

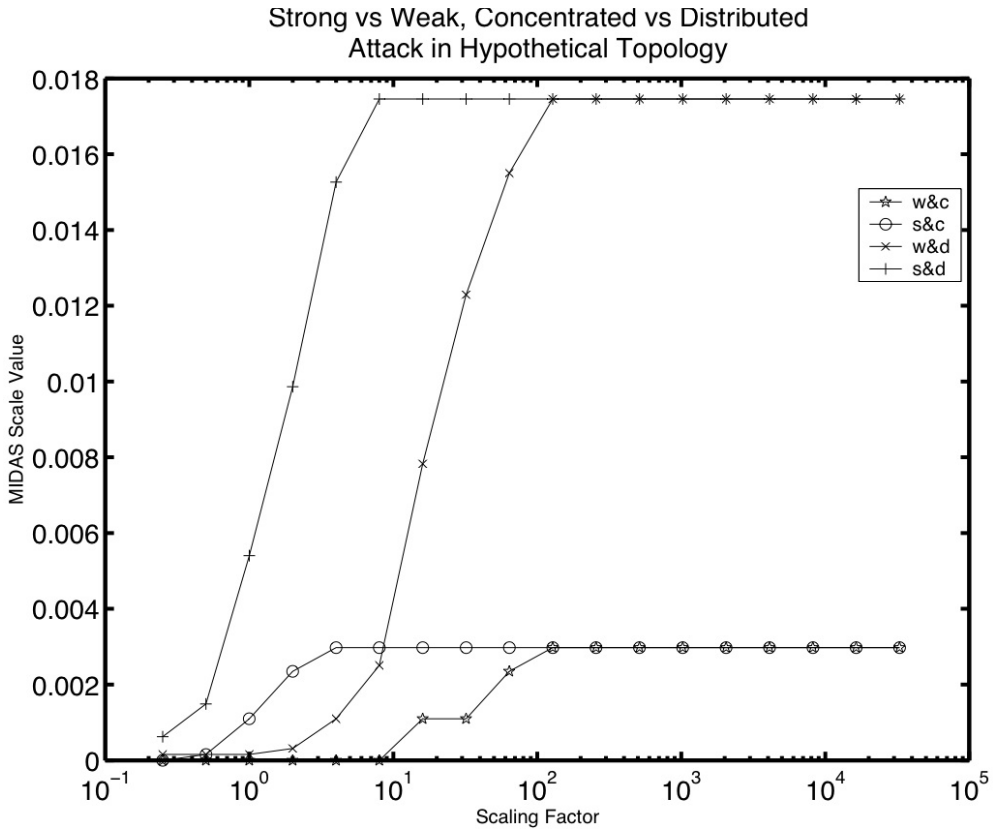
- Impact access links and limited number of core links
- Max impact when these links are overloaded

Distributed attacks:

- Can have larger overall network impact (more links to overload)

Strong attacks have impact sooner

Max impact (for these attacks) same for concentrated and distributed respectively

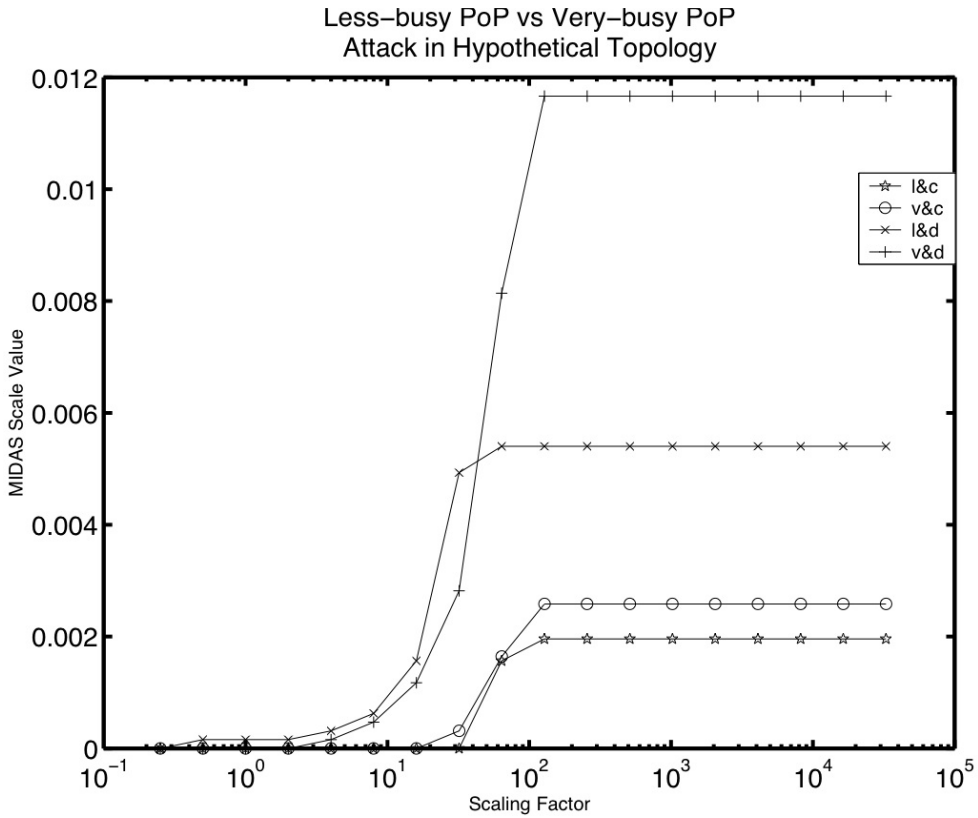


at&t

Validation results: collateral damage

Same attacks, attack targets in “very busy” or “less busy” PoP

- Expect more collateral damage in very busy PoP
  - For same attack MIDAS scale value should be higher



at&t

Summary

DDoS attacks real problem

Need means to measure, MIDAS:

- Service provider centric view
- Relative measure based on (potential) economic impact

Shown that MIDAS values changes according to our intuition of the impact of different types of attacks

Stake in the ground… more work needs to be done

- Extend to non Tier-1 ISP (e.g., uplink costs)
- More sophisticated attacks