Robust Heuristics: Packet job size estimation with provable guarantees against DoS attacks

Erica Chiang (eschiang@andrew.cmu.edu), Nirav Atre, Hugo Sadok, Weina Wang, Justine Sherry

Carnegie Mellon University

Background

Algorithmic complexity attacks: class of DoS attack that targets a system's worst-case behavior to induce significant harm with little resource investment

Packet scheduling policies affect **which packets are dropped** in overload (implications for network performance, security, robustness to attacks)

Weighted Shortest Job First (WSJF)

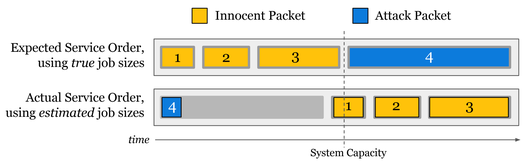
- Serves packets in increasing job size $c(p)$ to packet size $s(p)$ ratio
- Leads to **powerful bounds on displaced traffic** relative to resource investment [1]

$$\text{Displacement Factor (DF)} = \frac{\text{Innocent traffic displaced (Gbps)}}{\text{Attack bandwidth used (Gbps)}} \leq 1$$

(# of innocent bits dropped per bit of attack data transmitted)

- Relies on job size heuristics – often not perfect in practice

Can we **maintain theoretical guarantees** in the presence of imperfect heuristics?



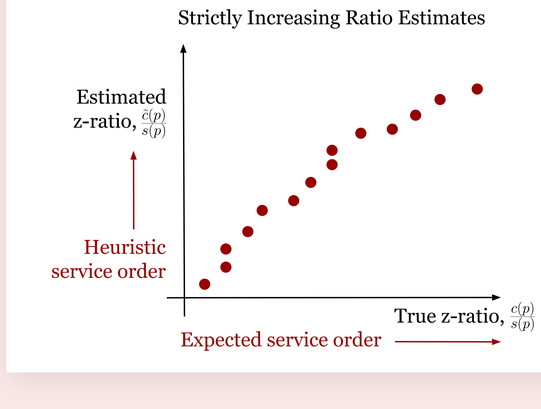
[1] Atre et al. 2022. SurgeProtector. *(SIGCOMM '22).*

Methods

- Design heuristics $\tilde{c}(p)$ that map packets of certain job size to same estimate
  - Assumptions: static time, adversary knows innocent packet distribution
  - Analysis: consider optimal adversarial attack, analyze heuristic for DF bounds, generalize to robust heuristic properties
- Analyze DF bounds in system preempts jobs when they exceed estimated runtime

Results

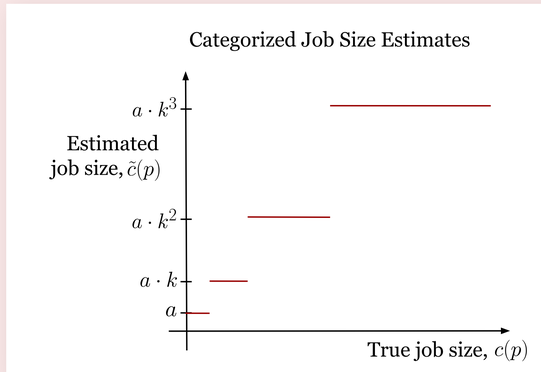
1. Strictly Increasing Heuristics Maintain Perfect Scheduling



It is possible to **maintain protection guarantees** with heuristics that estimate ratios monotonically increasing with true ratios

Perfect scheduling $\Longrightarrow$ DF ≤ 1

2. Step Functions Preserve a Constant Bound

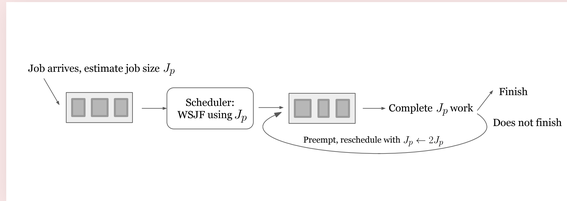


We can **preserve weaker guarantees** with heuristics that classify packets into job size categories

$$\tilde{c}(p) = a \cdot k^{\lfloor \log_k c(p) \rfloor}$$

Adversarial packet cannot displace innocent packets with ratio more than a factor of k smaller $\Longrightarrow$ DF $\leq k$

3. Preemption Cannot Maintain Bounds (Negative Result)



Preempting incorrectly estimated jobs **introduces new vulnerabilities**

Weaponize innocent traffic $\Longrightarrow$ unbounded DF

Discussion

Novel theoretical findings on provable protection against DoS attacks:

THEOREM 1 (**DF OF MONOTONIC HEURISTIC**). *Under WSJF, a heuristic $\tilde{c}$ is perfect if and only if $\frac{\tilde{c}(p)}{s(p)}$ is strictly monotonically increasing relative to $\frac{c(p)}{s(p)}$; such heuristics result in the DF being upper-bounded by* 1.

THEOREM 2 (**DF OF STEP FUNCTION HEURISTIC**). *A heuristic of the form $\tilde{c}(p) = a \cdot k^{\lfloor \log_k c(p) \rfloor}$, where a is some arbitrary constant, results in the DF being upper-bounded by k.*

THEOREM 3 (**DF OF PREEMPTIVE MODEL**). *Under WSJF with preemption but without heuristics, there exist regimes of system parameters for which the DF is lower bounded by $\frac{\rho}{1-\rho}$, where $\rho \leq 1$ is the load on the system due to innocent traffic.*

Next Steps

- Design data structures and corresponding heuristics that possess these properties, examine performance in practice
- Examine preemption performance when paired with stronger heuristics

Conclusion

- Certain heuristic properties provably maintain generalizable robustness against DoS attacks in WSJF systems
- Other methods of protection (i.e. preemption) can introduce new system weaknesses

Scan for abstract and proofs