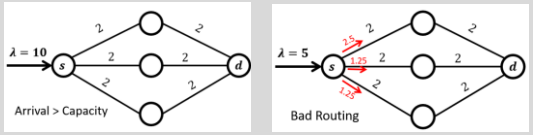
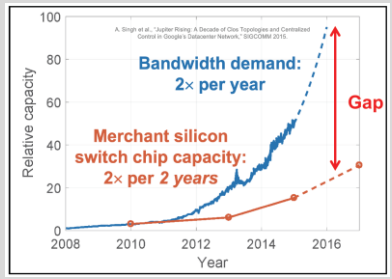
Ph.D. Research Poster: Analysis & Optimization for Networks in Overload

Motivation

Overload: Demand > Capacity



Network Overload is more frequent with unsystematic study
- **Rate control** to guarantee QoS
- **Risk** evaluation & protection

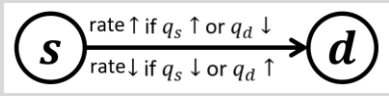


Series 1: Rate Control

Core: Fluid-queue model facilitates optimal rate control in overload

Stability

Prove explicit conditions to avoid queue overload in networks with bounded buffer



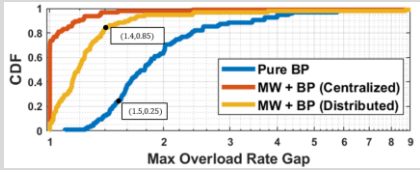
$$\frac{\partial g_{ij}(q_i,q_j)}{\partial q_i} > 0 \qquad \frac{\partial g_{ij}(q_i,q_j)}{\partial q_j} < 0$$

Highlights:
- Generalizing a set of policies that stabilize the networks, including backpressure
- Extendable to multi-commodity systems, and arbitrary buffer settings
- Explicit conditions for the guidance of policy design

Fairness

PaperLink

Prove policies to achieve most balanced overload in networks with bounded buffers

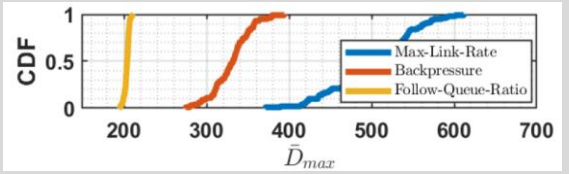


Highlights:
- Applicable to arbitrary buffer size and capacity, and agnostic of arrival rate
- Both centralized and distributed implementation
- Extendable to multi-layer networks (Fat-tree, Clos)

Delay

PaperLink

Prove a *follow-queue-ratio* policy to minimize queueing delay in overloaded networks



Highlights:
- Reveal counterintuition that serving in maximum rate is **NOT** necessarily delay-optimal
- Show we can optimize the delay with fewer transmission resources than link capacity
- Reduces >**10%** of average delay and >**50%** of max delay compared with backpressure & max-rate serving

Contribution

1. **Rate Control**
- Policy design for network stability, fairness & delay to mitigate overload effect by fluid-queue model

2. **Risk Analysis**
- Quantification of node attack impact on overload & Identification of critical nodes to shield

Series 2: Risk Analysis

Core: Fundamental limit analysis for node attackers to cause overload

Problem Setting: Given $G = (V, E)$, where each link l has capacity c_l. Suppose an adversary controls a subset of nodes V_A. The adversary can modify the routing policy of nodes in V_A. Given a flow (s, d, r) with default routing policy P.

Questions:
- Optimal routing of nodes in the given V_A controlled by adversary that maximizes overload?
- Optimal choice of V_A for the adversary to maximize overload?

Related attacks: BGP Hijacking; SQL Injection; Routing Table Poisoning, etc.

Motivation & Significance: (1) Evaluate the influence and limits of node attack on overload (2) Identify critical nodes that should be shielded to prevent from severe overload due to node attack

Primary results: NP-hardness, algorithms with promising results

Plans: Prove performance guarantee & Solve different variants
- Single flow -> Multiple flows
- Throughput -> Loss; Fairness; Delay
- Fixed routing of normal nodes -> Dynamic routing of normal nodes
- Deterministic flow model -> Stochastic queueing model