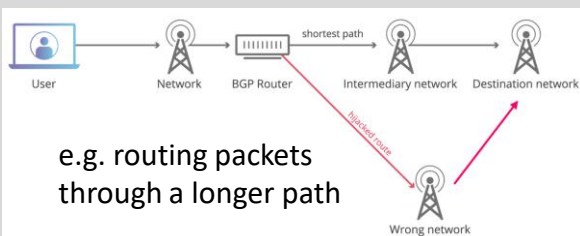# Fundamental Limits of Routing Attack on Network Overload

Motivation

Routing Attack can cause **Network Overload** thus causing traffic loss
- Most works on routing attack focuses on privacy and security issues
- Unlike DDoS & removal attack, the capability of routing attack on causing loss is unexplored


e.g. routing packets through a longer path

Q: What is the routing attack policy that maximizes network overload?

Contributions

1) Propose exact, approximation, and distributed algorithms, for **no-loss throughput minimization** & **loss maximization**
2) Propose algorithms for **optimal node selection** to conduct routing attack
3) Near-optimal performance shows the algorithms serve as **benchmarks** for overload risk evaluation and critical node protection

Example

Node 3 is attacked
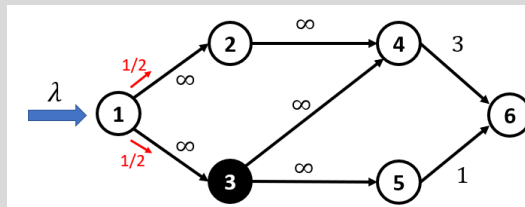
- **No-loss throughput minimization**: routes all packets to 5 (then loss occurs when $\lambda > 2$)
- **Loss maximization**: routes all packets to 4 when for example $\lambda = 6$

Main Results

No-loss throughput minimization
- Exact algorithm: (based on max-flow)
- 2-Approximation algorithm:
    - With partial network information
- Distributed algorithm:
    - >50% tested cases with 2-approx.

Loss maximization
- NP-hardness
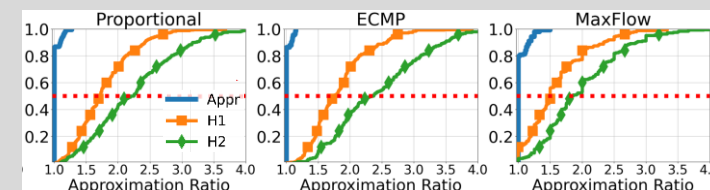- Approximation algorithms with multiplicative & additive guarantee

Optimal Node Selection
- NP-hardness
- Exact algorithm for min no-loss throughput
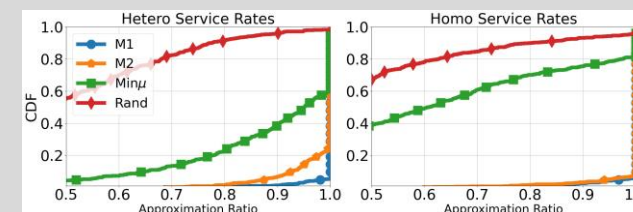
Simulation

No-loss throughput minimization

Approx. alg is **near-optimal** under different density, size of attacked nodes, and routing policies (Proportional, ECMP, Max-Flow)

Loss maximization

Proposed algorithms (M1, M2) achieve **>95%** of maximum loss in **>90%** tested networks

Optimal Node Selection

Proposed algorithms achieve **>80%** of maximum loss in **>90%** tested networks