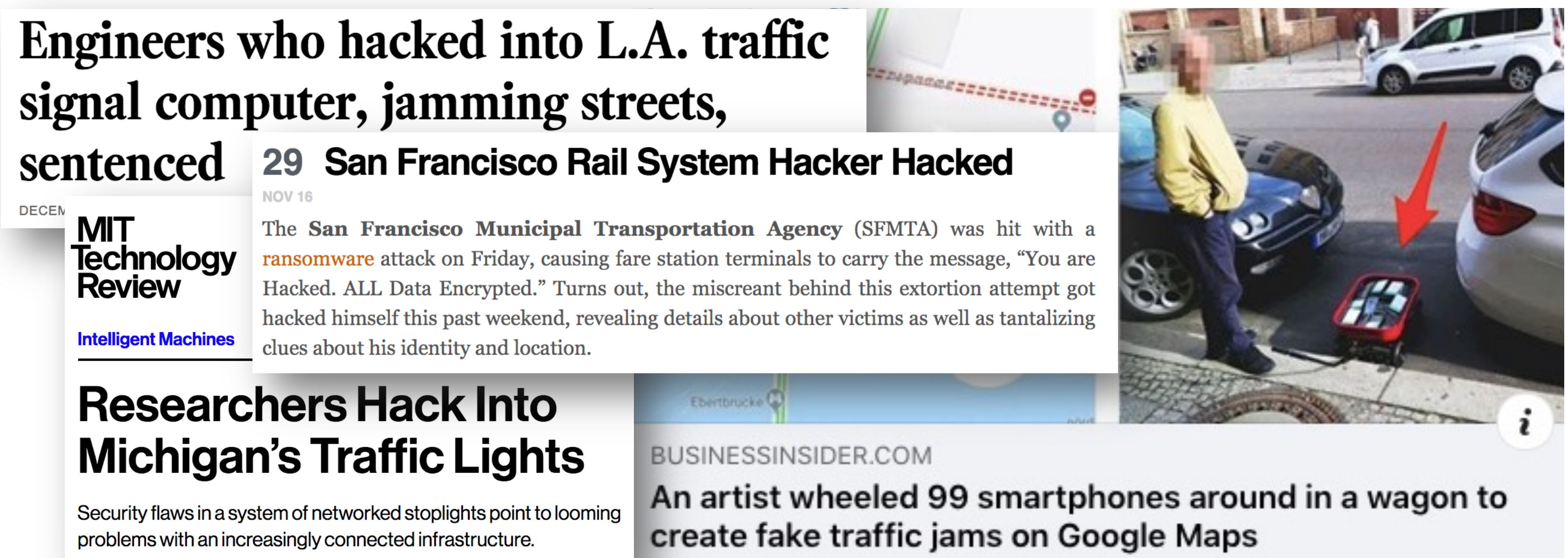
Cost-aware Defense for Parallel Server Systems against Reliability and Security Failures

Qian Xie
qx66@cornell.edu

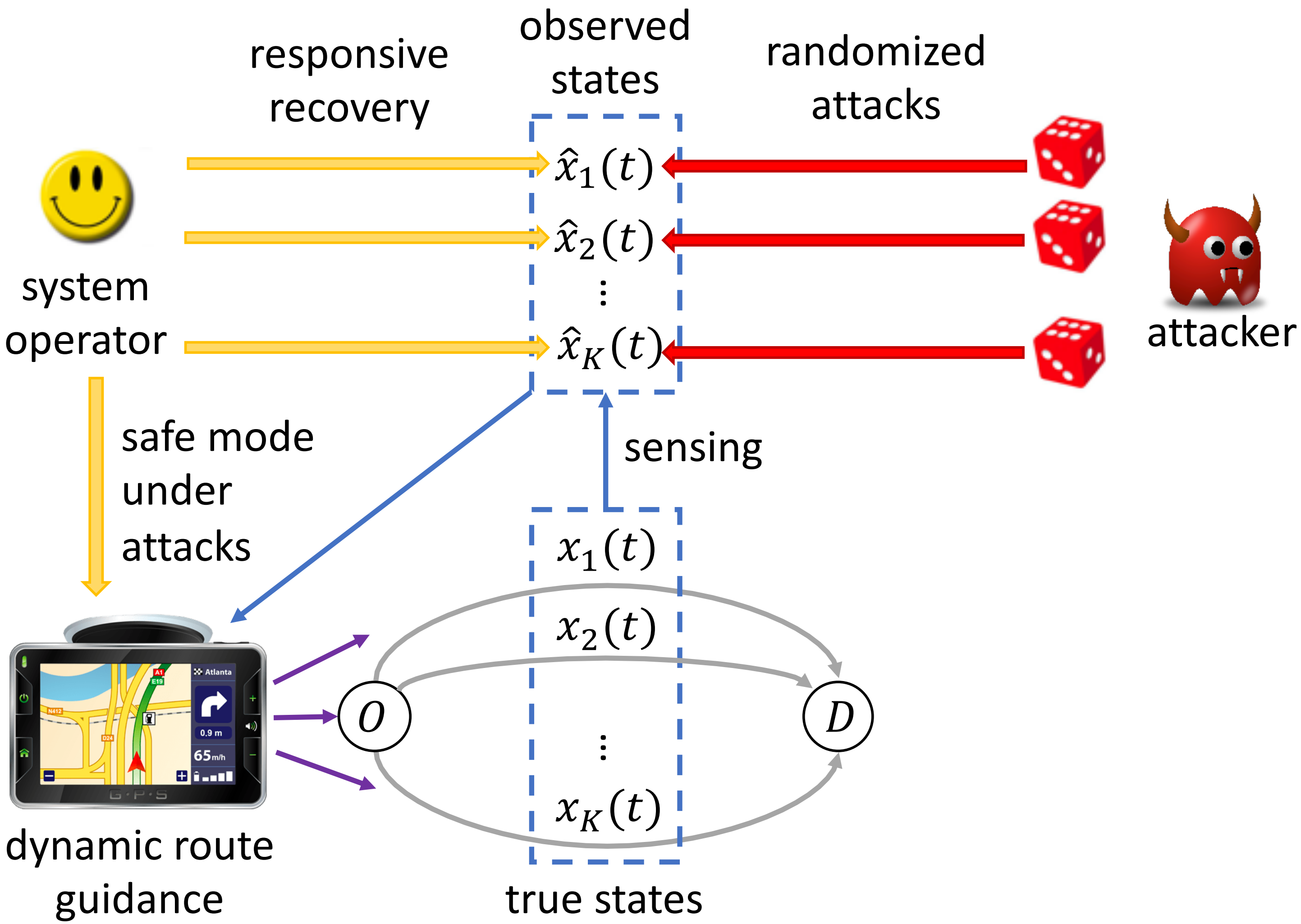
Joint work with Jiayi Wang and Li Jin

Security risks in network systems

- Network systems rely on data collection and transmission
  - Intelligent transportation systems (ITSs)
  - Manufacturing systems (production lines)
  - Communication networks
- Cyber components susceptible to data loss and data errors
  - E.g., traffic sensors and traffic lights can be intruded and manipulated
  - Need secure-by-design features



Example: dynamic routing in ITSs



Research questions

Modeling & analysis

- How to model stochastic & recurrent faults/attacks?
- How to quantify attacker's incentive?
- How to quantify the impact due to faults/attacks?
- How to evaluate various security risks?

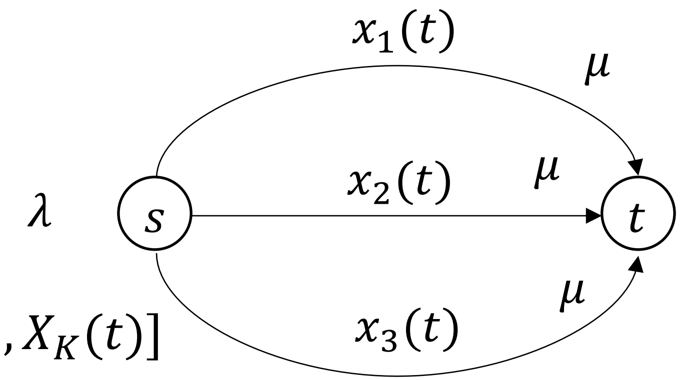
Resource allocation

- How to allocate limited/costly security resources, including redundant components, diagnosis mechanisms, etc.?

Decision making

- How to make protecting (resp. defending) decisions in the face of random faults (resp. malicious attacks)?

Parallel-queueing system



Basic model

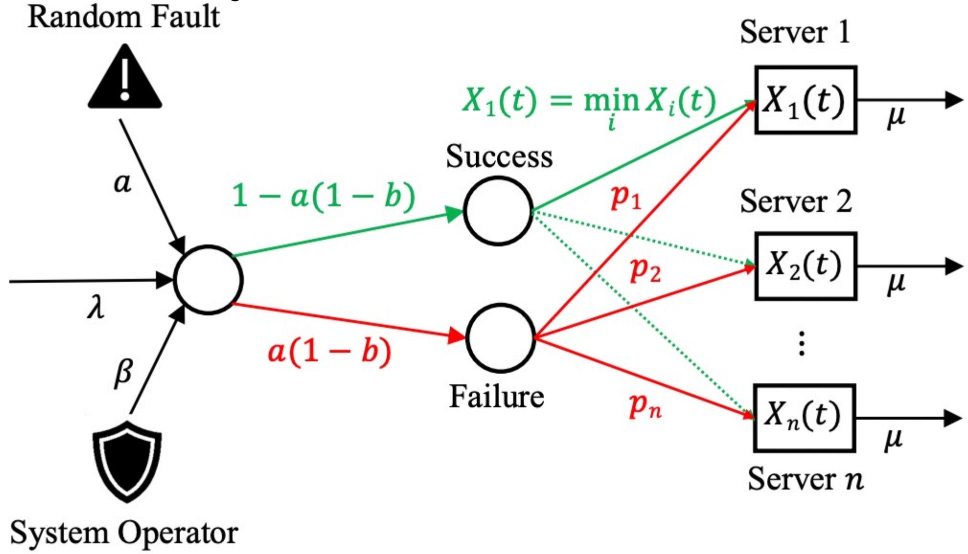
- Poisson arrivals of rate λ
- Parallel servers with service rate μ
- State: vector of queue lengths
$$X(t) = [X_1(t), X_2(t), \dots, X_K(t)]$$
- Dynamic routing: dynamically allocate jobs (e.g., customers, vehicles, components, data packets) to servers
- Provably optimal routing policy: join-the-shortest-queue (JSQ)[1]
- Existing works based on perfect observation of system state $X(t)$ and perfect implementation of dynamic routing
- Faulty/failed closed-loop can be worse than open-loop (e.g., round robin or Bernoulli routing)
- Research gap: designing fault-tolerant dynamic routing

[1] Ephremides, Anthony, P. Varaiya, and Jean Walrand. "A simple dynamic routing problem." *IEEE transactions on Automatic Control* 25.4 (1980): 690-693.

Protection against reliability failures

- Reliability failures
  - Random malfunction: operator fails to send routing instructions
  - With constant probability a, a job joins a random queue
- Markov decision process
  - Operator protects the routing with state-dependent probability $\beta(x)$
  - Minimize expected cumulative discounted queuing cost + tech cost

$$J^*(x) = \min_\beta \mathbb{E}[\int_0^\infty e^{-\rho t}(|X(t)| + c_b \beta(X(t)))dt | X(0) = x]$$

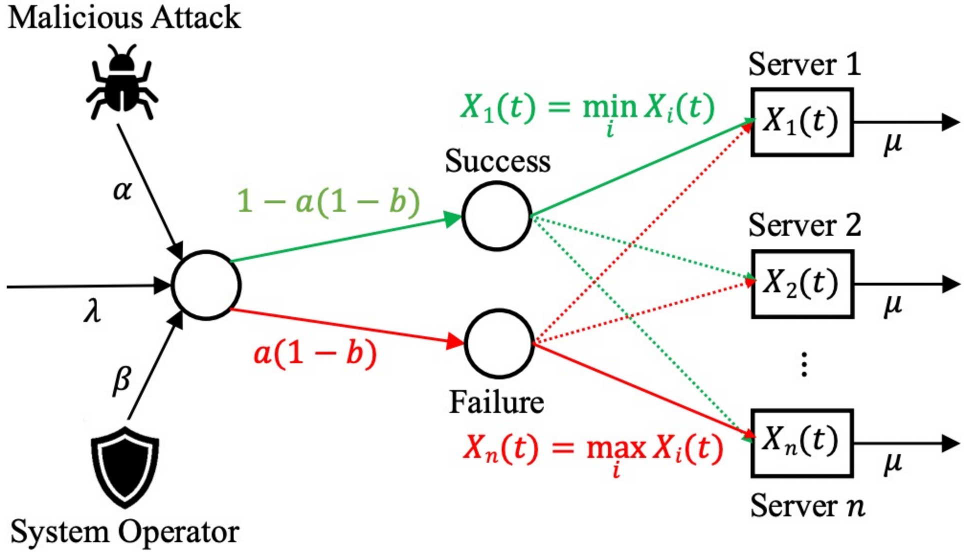


Defense against security failures

- Security failures
  - Spoofing: attacker manipulates routing (e.g., send-to-longest-queue)
- Stochastic attacker-defender game (attacker side)
  - Attacker attacks with state-dependent probability $\alpha(x)$
  - Maximize expected cumulative discounted reward

$$V_A^*(x,\beta) = \max_\alpha \mathbb{E}[\int_0^\infty e^{-\rho t} R\big(X(t)\big) dt | X(0) = x]$$

where $R(\xi) = |\xi| + c_b\beta(\xi) - c_a\alpha(\xi)$

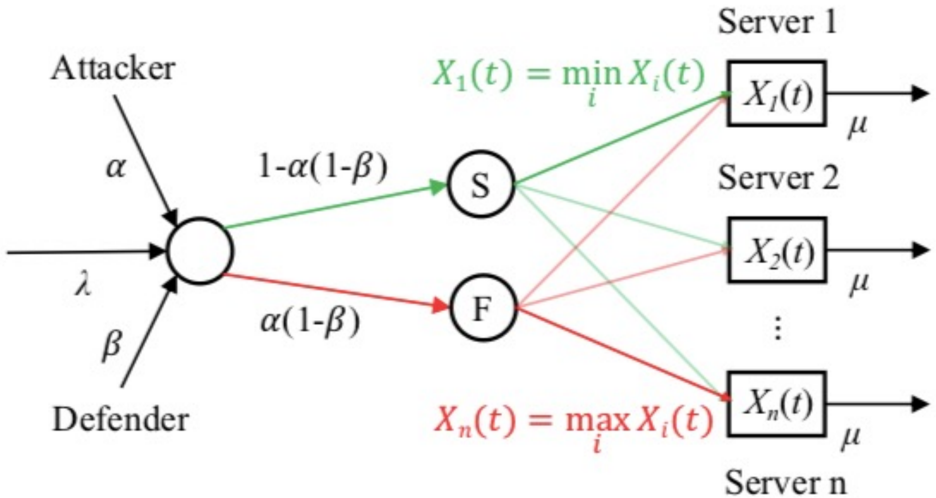


Defense against strategic attacks (cont'd)

- Security failures
  - Routing fails iff attacked and not defended (i.e., $\alpha(x) = 1$ & $\beta(x) = 0$)
- Stochastic attacker-defender game (operator side)
  - Defend the routing with state-dependent probability $\beta(x)$
  - Minimize expected cumulative discounted loss

$$V_B^*(x, \alpha) = \min_\beta \mathbb{E}[\int_0^\infty e^{-\rho t} C\big(X(t)\big) dt | X(0) = x]$$

where $C(\xi) = |\xi| + c_b \beta(\xi) - c_a \alpha(\xi)$



Stability criteria

Theorem 1. The parallel n-queue system with reliability failures is stable if for any non-diagonal vector x,

$$\beta(x) > 1 - \frac{\mu|x| - \lambda x_{min}}{a\lambda(\sum_{i=1}^{n} p_i x_i - x_{min})}.$$

Theorem 2. The parallel n-queue system with security failures is stable if for any non-diagonal vector x,

$$\alpha(x)\big(1 - \beta(x)\big) < \frac{\mu|x| - \lambda x_{min}}{\lambda(x_{max} - x_{min})}.$$

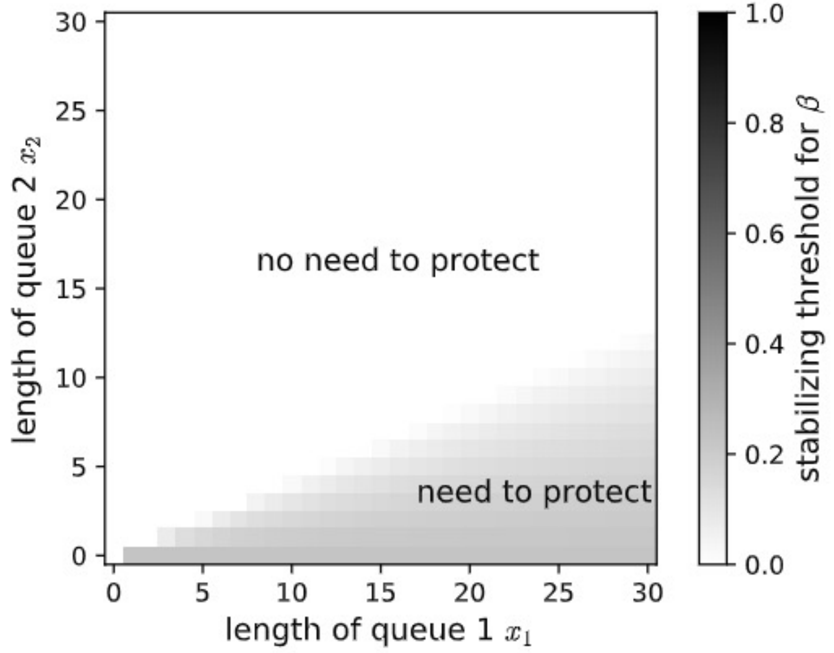
Proof sketch. Consider the quadratic Lyapunov function $V(x) = \frac{1}{2}\sum_{i=1}^{n} x_i^2$ and apply the infinitesimal generator.

Stability criteria (cont'd)

Theorem 1. The parallel n-queue system with reliability failures is stable if for any non-diagonal vector x,

$$\beta(x) > 1 - \frac{\mu|x| - \lambda x_{min}}{a\lambda(\sum_{i=1}^{n} p_i x_i - x_{min})}.$$

Characterization of the stabilizing threshold:



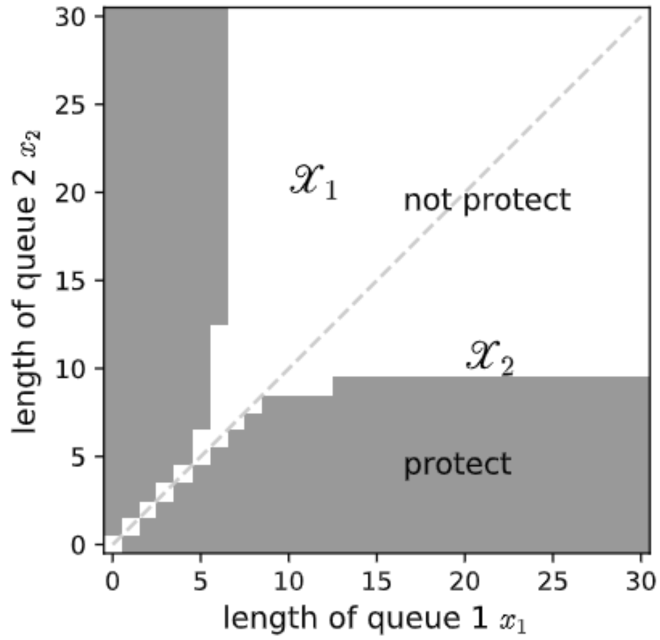
$p_1 = 0.1, p_2 = 0.9, \lambda = 1.6, \mu = 1, a = 0.9$

Optimal protecting policy

Theorem 3. Consider a parallel n-queue system with reliability failures. The optimal protecting policy $\beta^*(x)$ is threshold-based.

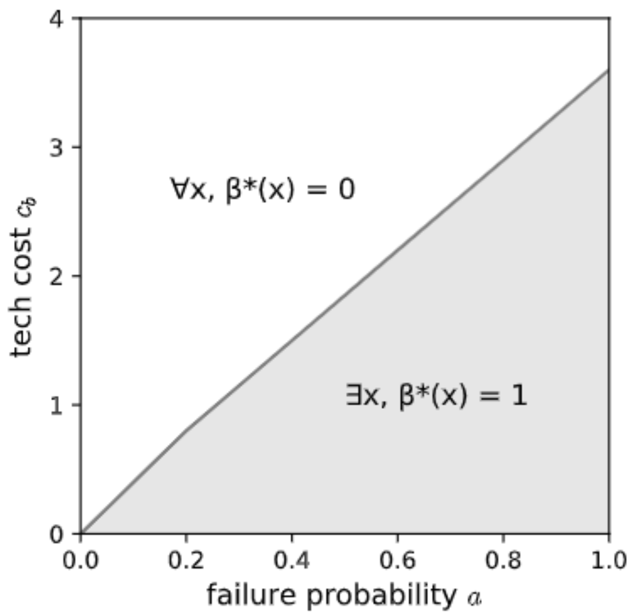
- Bang-bang control: operator either protects or does not protect (no probabilistic protection), i.e., $\beta^*(x) \in \{0,1\}$
- Operator needs to protect when 1) the queue lengths are less ‘‘balanced’’; (2) the queues are close to empty

Proof idea: HJB equation and induction on value iteration.

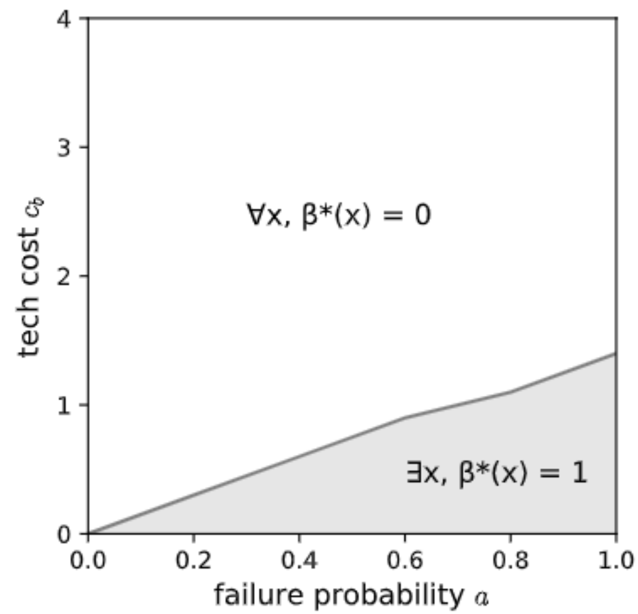


Numerical study

The incentive to protect is non-decreasing in the failure probability a, non-increasing in the tech cost c_b, and non-decreasing in the throughput λ (estimation of the optimal protecting policy is based on the truncated policy iteration).



(a) $\rho = 1.6$

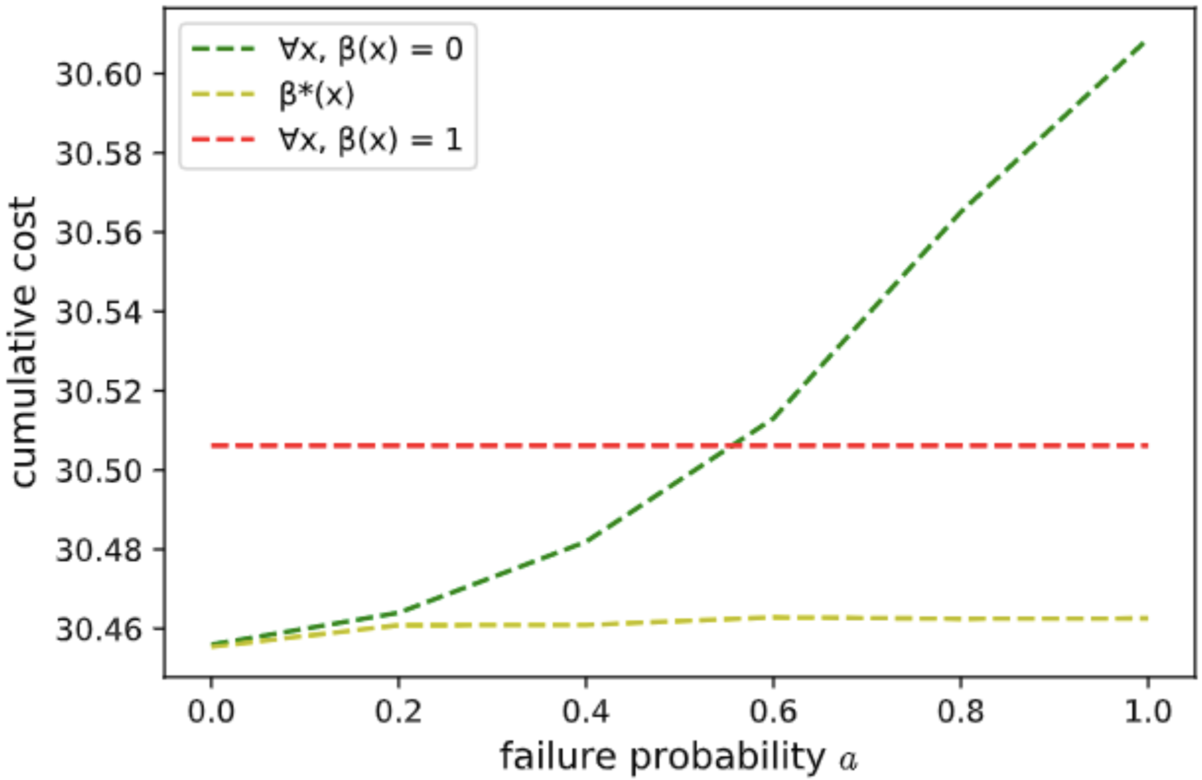


(b) $\rho = 0.4$

Tipping points when the operator starts to protect “riskier states”

Numerical study (cont'd)

Simulation result: the optimal closed-loop protecting policy β^* performs better in terms of the cumulative cost, compared to the open-loop policies (benchmark) never defend and always defend.



Attacker-defender game

Definition. The equilibrium Markovian attacking (resp. defending) strategy α^* (resp. β^*) satisfies that for any state $x \in \mathbb{Z}^n_{\geq 0}$,

$$\alpha^*(x) = \mathrm{argmax}_\alpha\, V_A^*(x, \beta^*),$$
$$\beta^*(x) = \mathrm{argmin}_\beta\, V_B^*(x, \alpha^*).$$

Attacker's (resp. defender's) is $V_A^*(x, \beta^*)$ (resp. $V_B^*(x, \alpha^*)$). In particular, (α^*, β^*) is a Markovian perfect equilibrium (MPE).

Remark. According to Shapley's extension on minimax theorem,

$$V_A^*(x, \beta^*) = V_B^*(x, \alpha^*) = V^*(x)$$

Proof idea. Induction on value iteration.

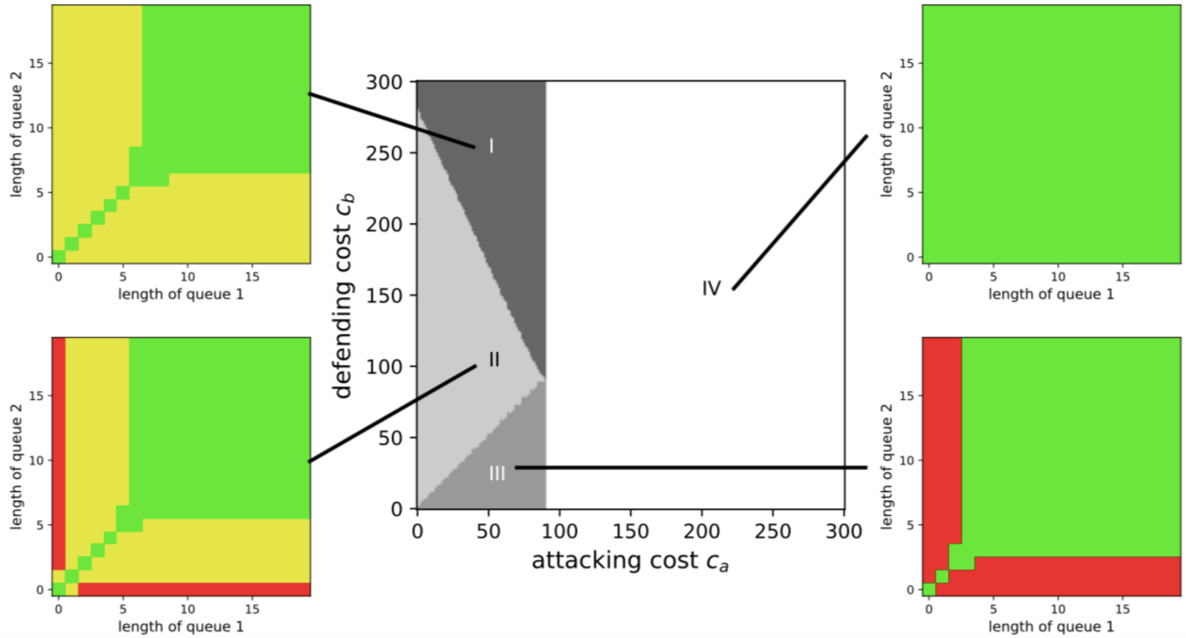
Question. Existence of MPE? - Countable infinite state space!

Question. Estimation of MPE? - Adapted Shapley's algorithm.

MPE analysis

Theorem 4. The MPE has four regimes depending on $c_a,\ c_b$ and $\delta^*(x) = \lambda(\max_j V^*(x+e_j) - \min_j V^*(x+e_j))$. For each MPE, the state space is divided into subsets with different security risk levels:

- $S_1 = \{x|(\alpha^*(x), \beta^*(x)) = (0,0)\}$ (low risk)
- $S_2 = \{x|(\alpha^*(x), \beta^*(x)) = (1,0)\}$(medium risk)
- $S_3 = \{x|(\alpha^*(x), \beta^*(x)) = (\frac{c_b}{\delta^*(x)}, 1 - \frac{c_a}{\delta^*(x)})\}$ (high risk)

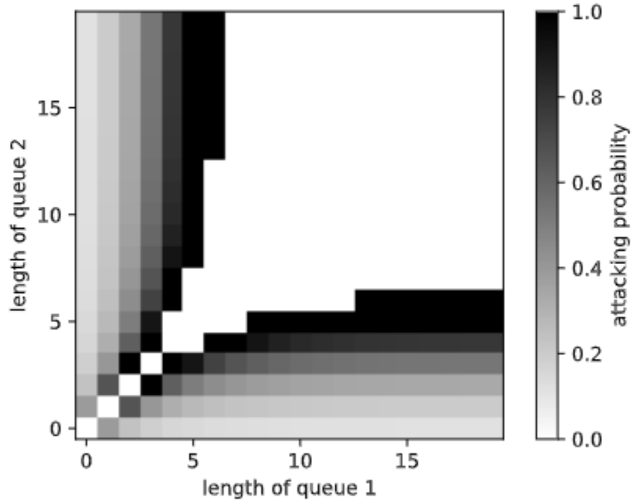


MPE analysis (cont'd)

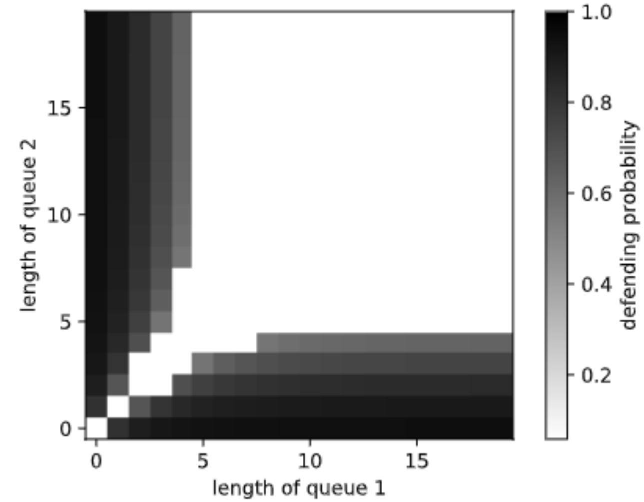
Theorem 4. The MPE has the following regimes depending on c_a, c_b and $\delta^*(x) = \lambda(\max_j V^*(x + e_j) - \min_j V^*(x + e_j))$

- $\delta^*(x) \leq c_a \Rightarrow S_1 = \{x | (\alpha^*(x), \beta^*(x)) = (0,0)\}$ (low risk)
- $c_a < \delta^*(x) \leq c_b \Rightarrow S_2 = \{x | (\alpha^*(x), \beta^*(x)) = (1,0)\}$(medium risk)
- $\delta^*(x) \geq \max(c_a, c_b) > 0 \Rightarrow S_3 = \{x | (\alpha^*(x), \beta^*(x)) = (\frac{c_b}{\delta^*(x)}, 1 - \frac{c_a}{\delta^*(x)})\}$ (high risk)

The equilibrium strategies α^* , β^* are both threshold-based.



α^*



β^*

Conclusion

- Without secure dynamic routing, random faults and malicious attacks can destabilize the queueing system
- The optimal protecting strategy and the equilibrium of attacker-defender game have threshold-properties
- The system operator has higher incentive to protect when
  - the failure probability is higher
  - the tech cost is lower
  - the throughput is higher
  - the queue lengths are less ‘‘balanced’’
  - the queues are close to empty
- Our proposed optimal protecting policy (closed-loop) performs better than the benchmark (open-loop)
- Optimal protecting strategy (resp. equilibrium) can be estimated by truncated policy iteration (resp. adapted Shapley’s algorithm)