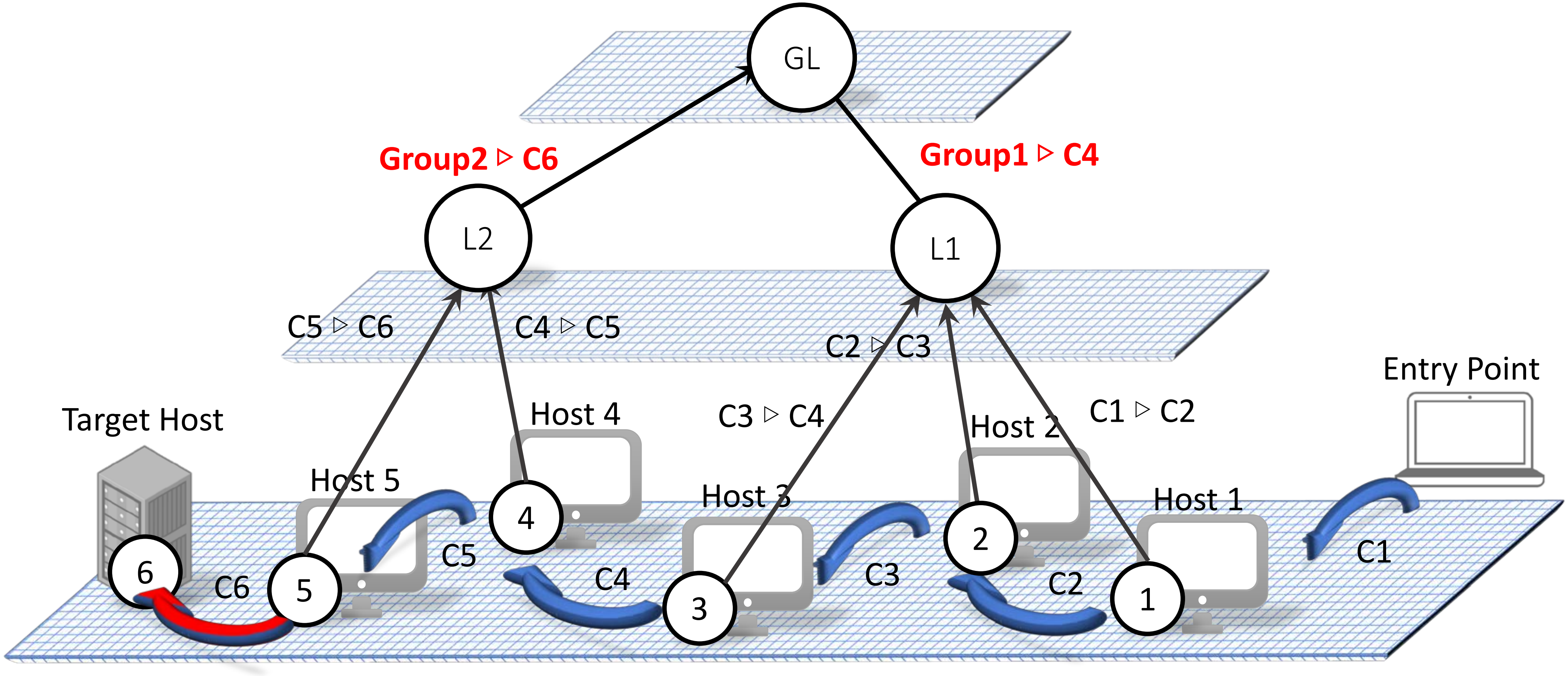
Lateral Movement Detection and Response

Ahmed Fawaz

June 15, 2017

Lateral Movement Detection

A critical step during APT to move from the entry point to target host



Response to Lateral Movement

- Achieve resiliency against lateral movement
- Resilience by stopping virus spread while maintaining acceptable service availability, as opposed to disconnecting the whole network

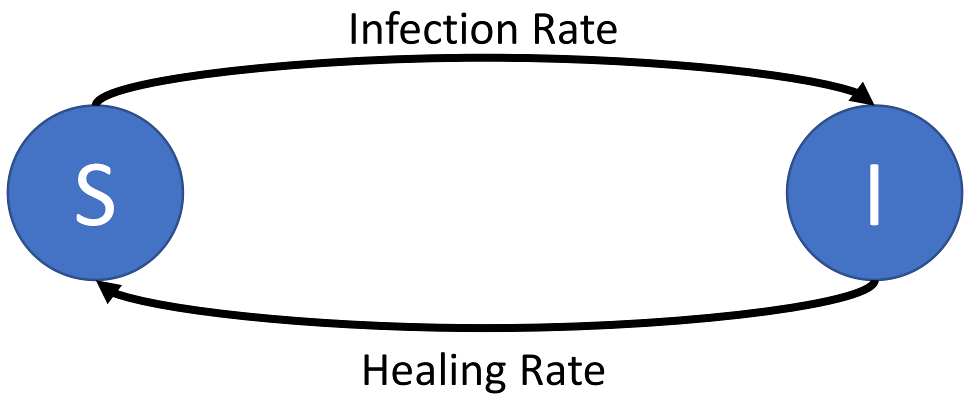
Strategy:

1. Learn attacker movement
2. Respond by limiting connectivity to stop spread
3. Recover the system

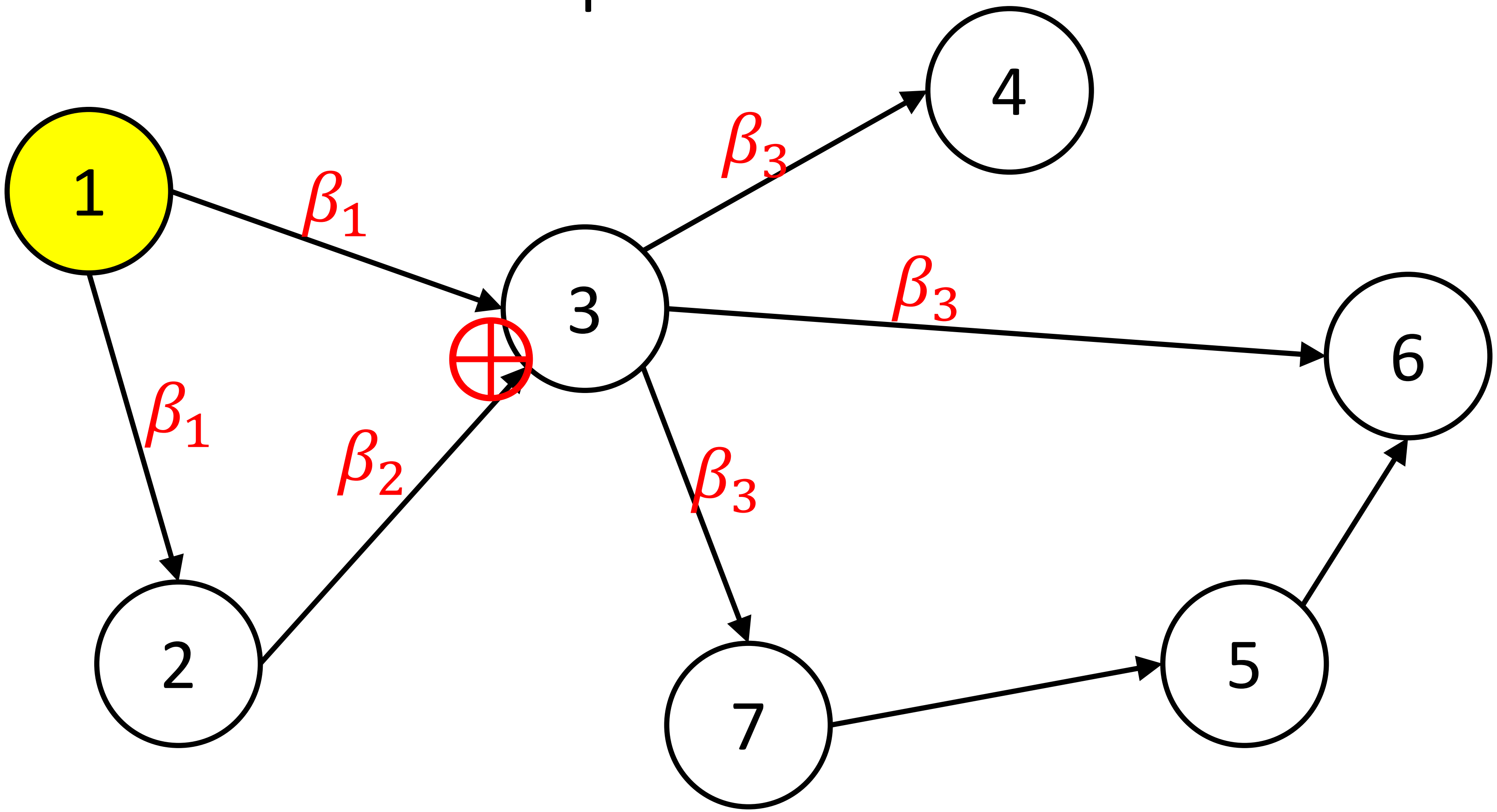
Lateral Movement Model

- Susceptible-infected-susceptible (SIS) CTMC virus spread model

- A node can be in two states: {**Susceptible**, **Infected**}
- Nodes are not cured



Virus Spread over Graph



-A node's infection rate depends on the state of neighboring nodes.

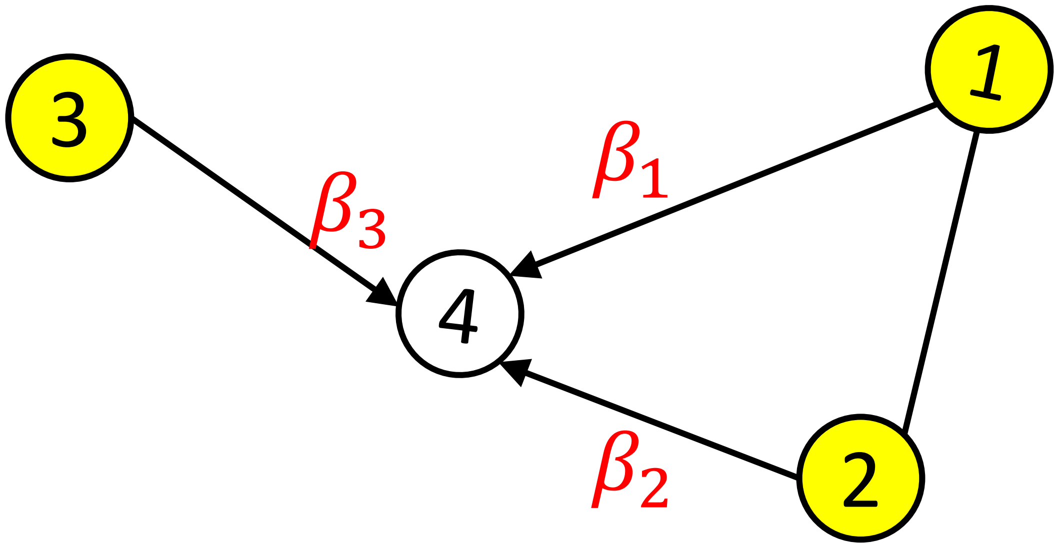
  -Each node infects its neighbors with rate β_i.

    -Each node is healed independently with rate δ_i.

Spread Dynamics

The total system dynamics as N-intertwined CTMCs:

$$\dot{p} = (AB - P(t)AB - D)p$$



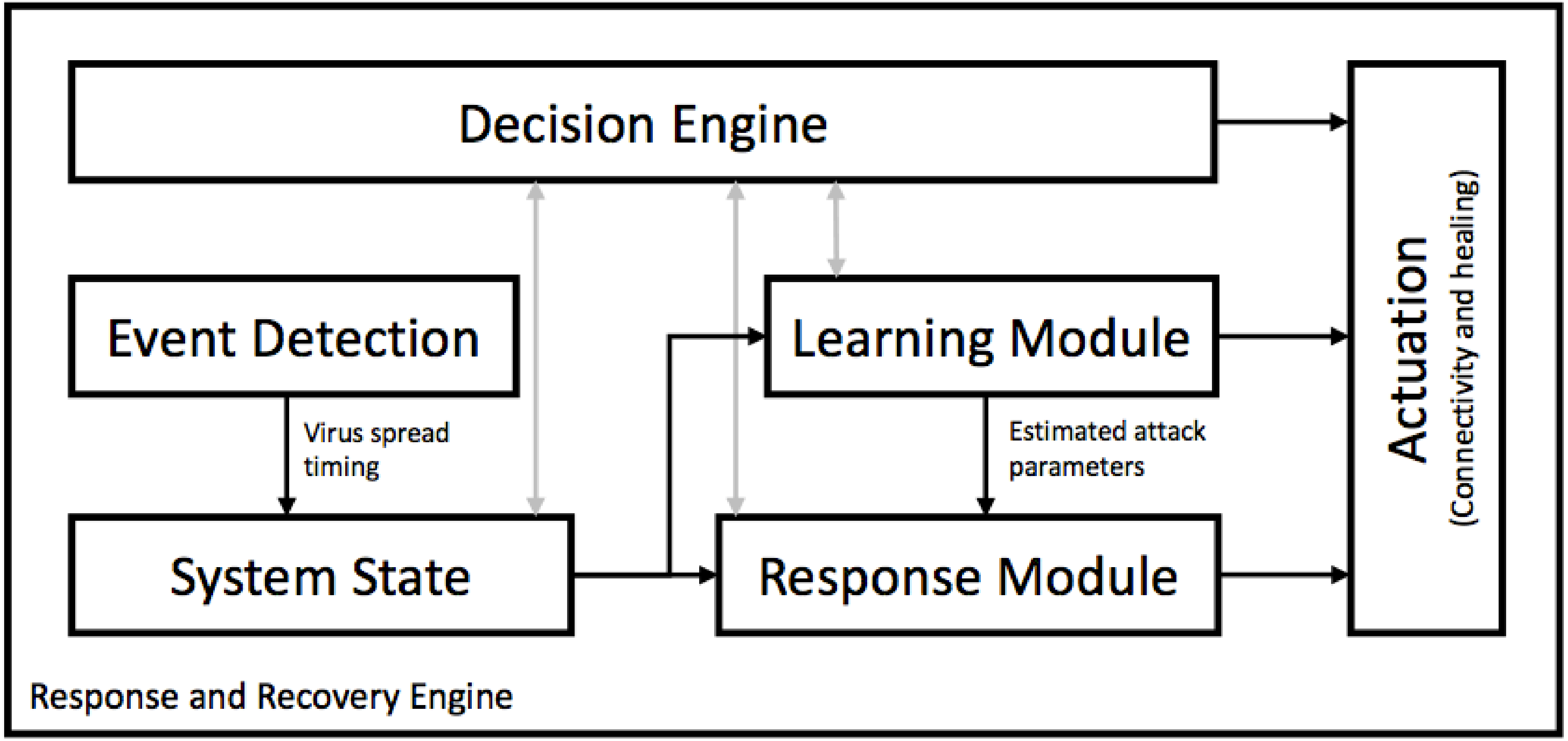
Controllable parameters:

- The connectivity graph **A**
- The healing rate **D = diag($\boldsymbol{\delta_1, \dots, \delta_n}$)**

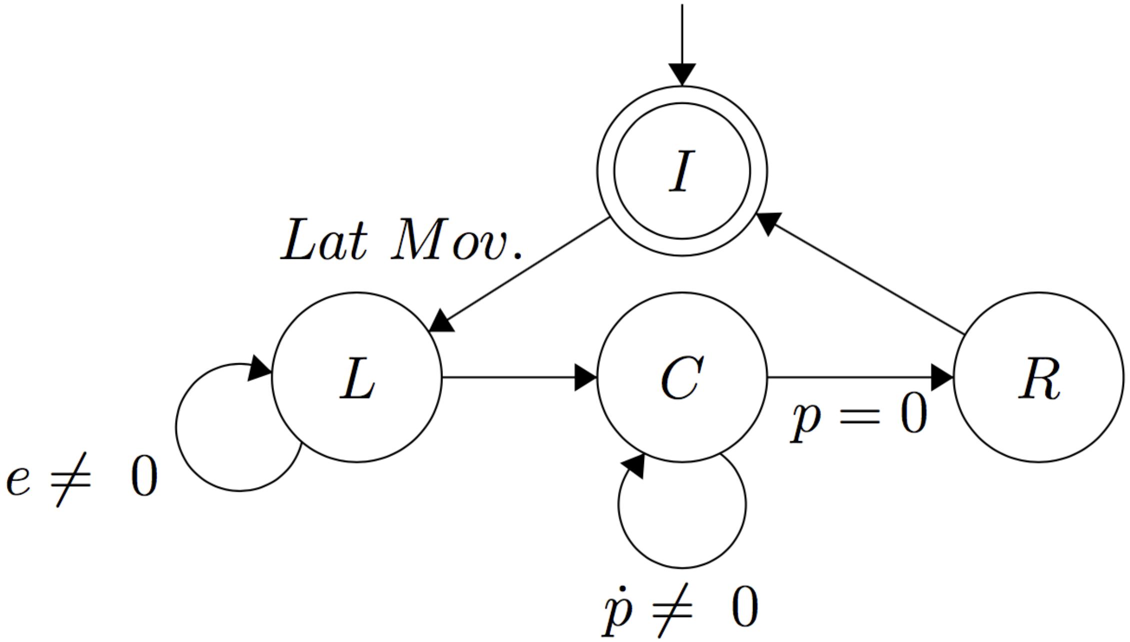
Unknown:

- The infection rate **B = diag($\boldsymbol{\beta_1, \dots, \beta_n}$)**

Response and Recovery Engine



RRE Decision Modes



Initial: no infection

Learn: estimate attacker parameters

Containment: stop attacker spread

Recovery: return system to secure state

Learning Phase

- Estimate the infection rate of each node when it's neighbors are infected.

- Measure the duration to infect a node using lateral movement chains

$$\mathcal{S}_i = (s_1, s_2, \ldots, s_m) \quad \text{where} \quad s_i = t - t_{\text{healed}}$$

- Use the ML estimator: $\widehat{\lambda}_i = \dfrac{m}{\sum_j s_i}$

Learning Strategy

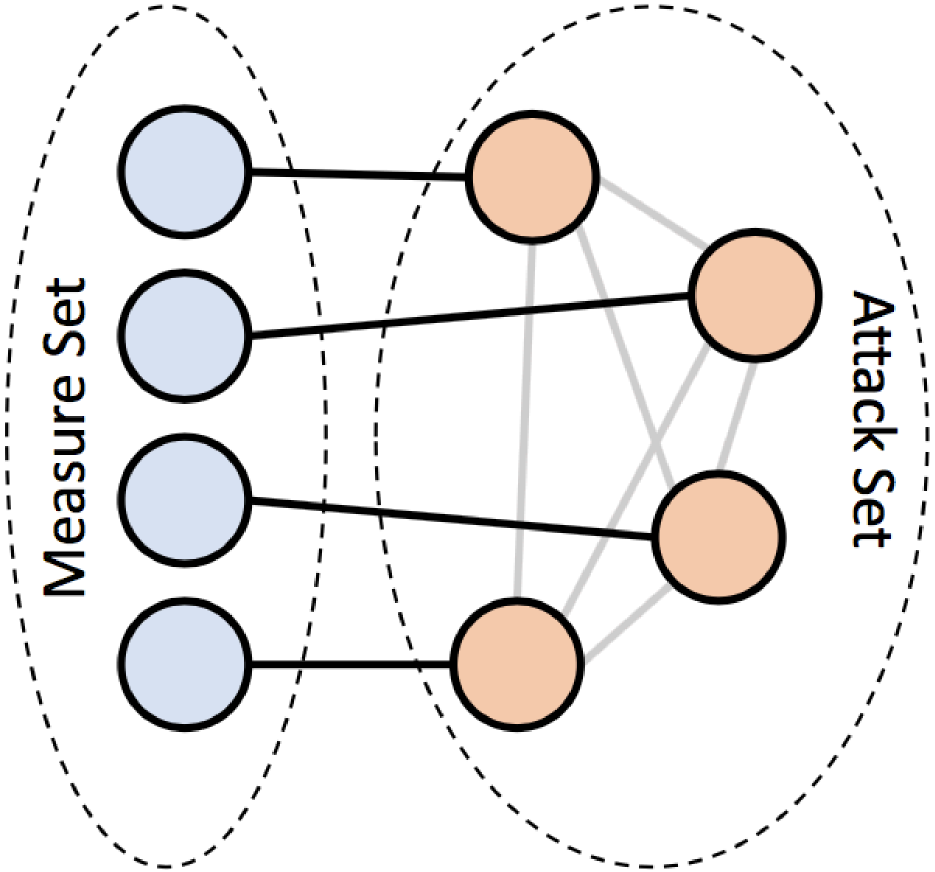
- Naïve approach: all nodes infected, heal one node at a time for sample collection
  - Slow learning
  - Highest availability

- Optimal approach: find independent sets as the minimal coloring of a graph
  - Finding coloring is NP-hard

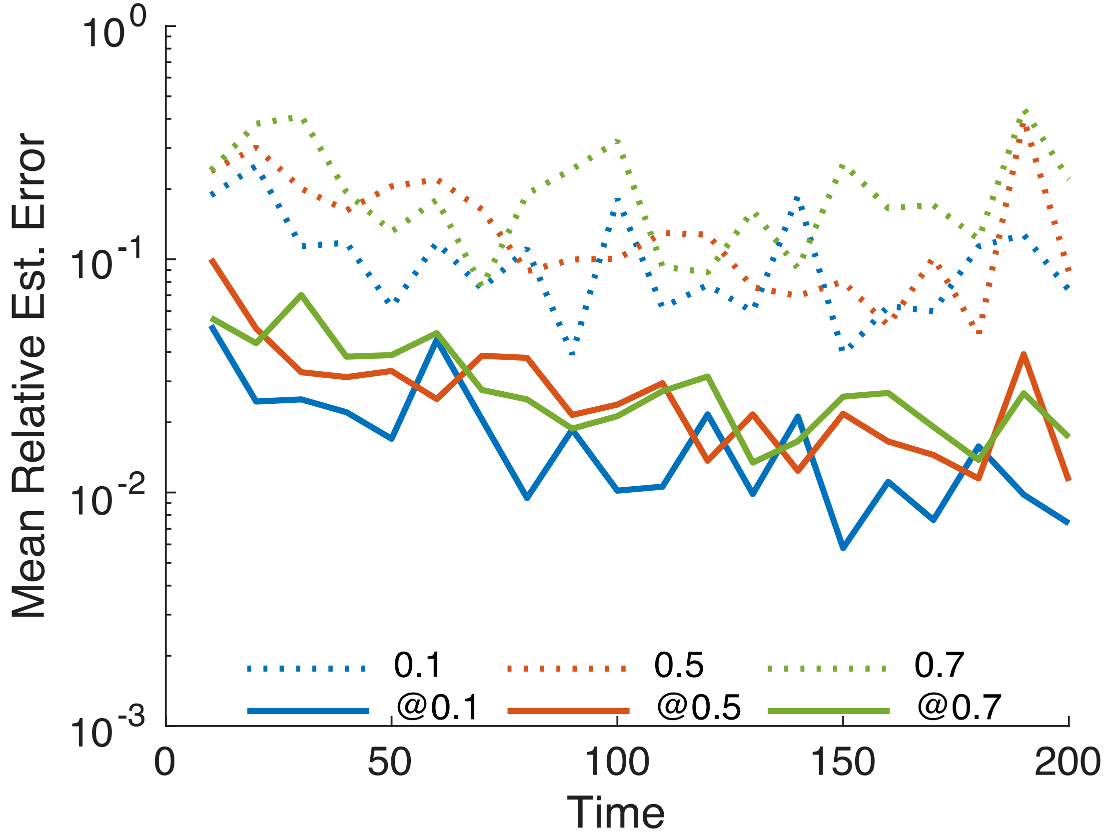
Dynamic Strategy

- Divide nodes to attack set and measure set.
- Attack set is fully connected.
- Measure set has limited connectivity to the attack set.

- Switch the roles after data is collected.
- Solve: $$A\beta = \widehat{L}$$



Estimation Error



- Error decreases as more data is collected
- A sparse connectivity matrix performs better overall

Containment Phase

- After learning the parameters; we find the connectivity and healing rates to stop the spread

- **Goal:** achieve a globally asymptotic stable (GAS) disease-free equilibrium (DFE)
  - Starting from an initial state
  - Consequence: p → 0 with an exponential decay

- Pick *A*,*D* such that (AB-D) is Hurwitz

Resiliency during Containment

- Maximize availability such that *A* and *D* result in a stable DFE.
- Encoded as a Mixed-Integer Nonlinear Optimization Problem

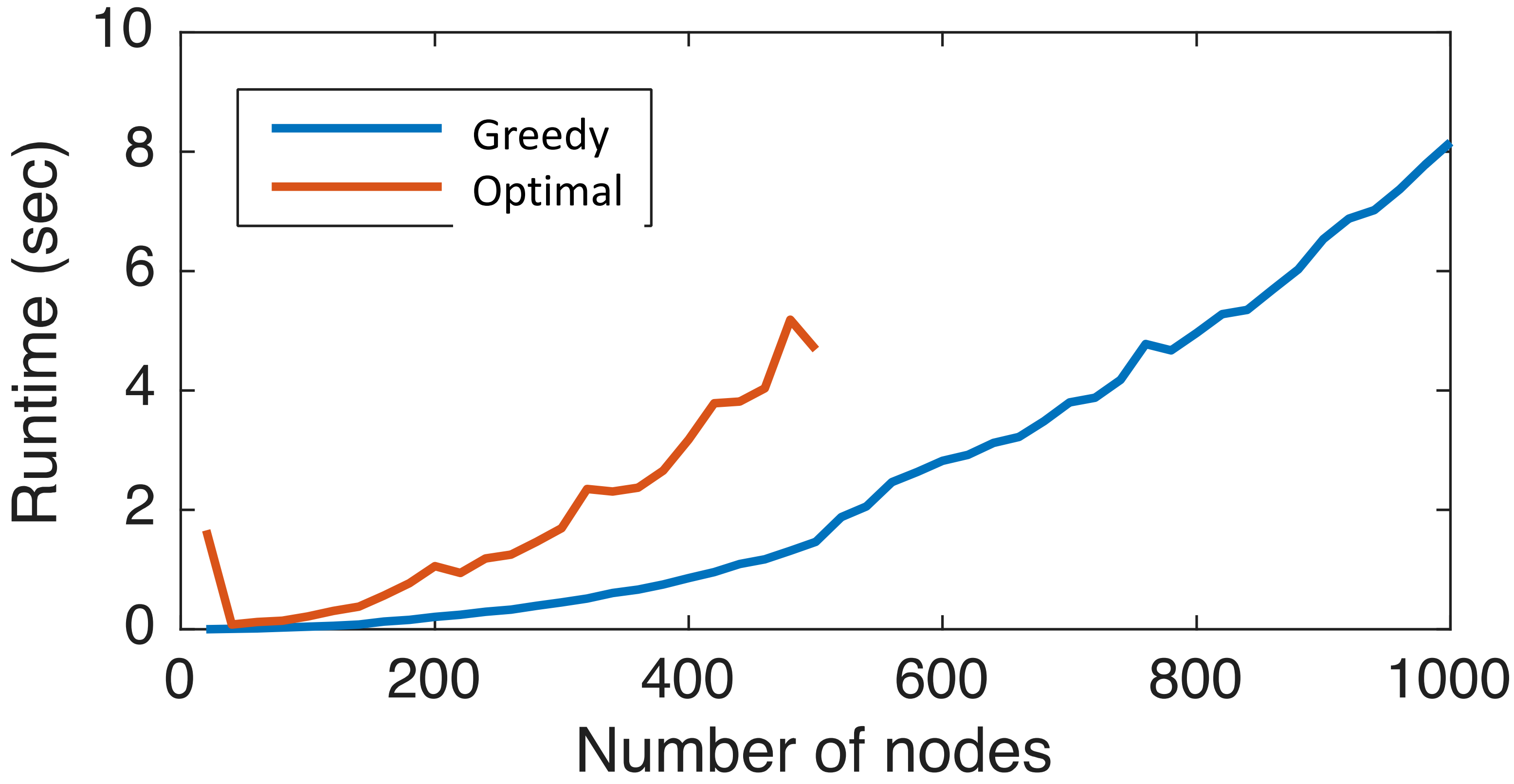
$$
\begin{array}{rrcl}
\min\limits_{A,d} & N^2 - \sum_i \sum_j a_{ij} & & \\
\text{s.t.} & \max \lambda(A\widehat{B} - diag(d)) & < & 0 \\
 & \sum_i d_i & \leq & c \\
 & A & \in & \{0,1\}^{n \times n} \\
 & d & \in & \mathbb{R}^n
\end{array}
$$

Availability

Hurwitz Condition

Limit cost

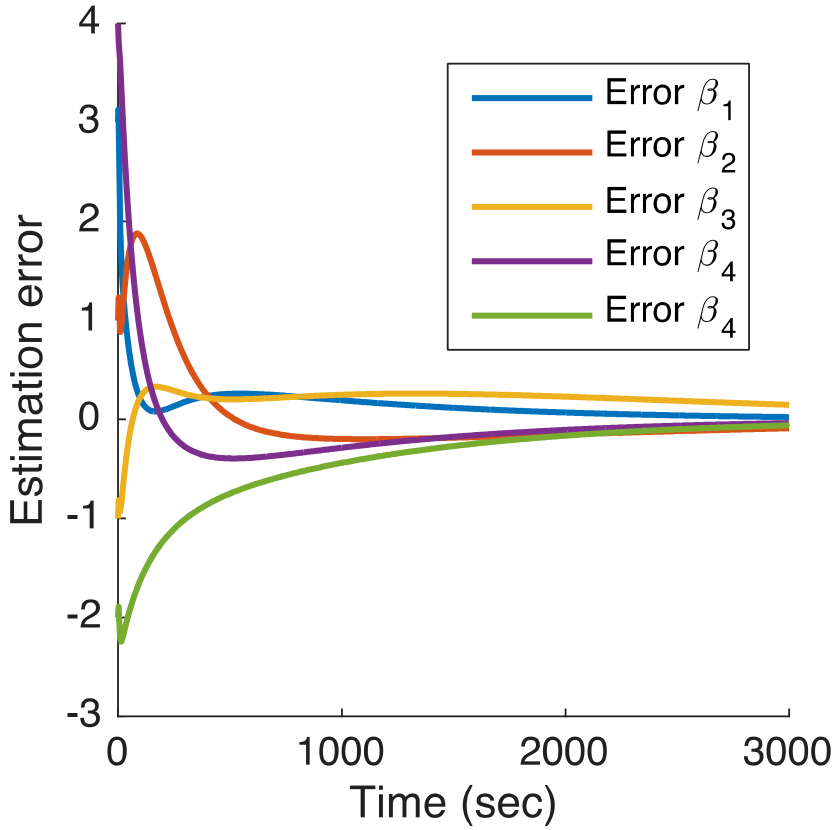
Connectivity matrix



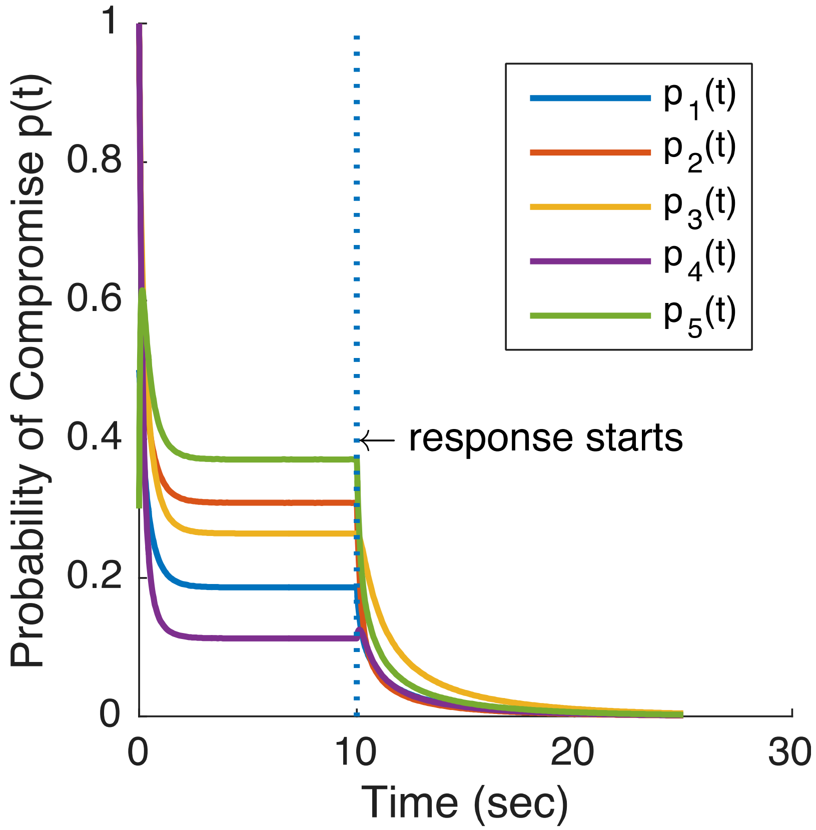
- The optimal solver cannot find matrices for N>500
- The greedy solver is faster but the solutions are suboptimal

Simulation of RRE

Error of parameter estimation error



State evolution over time during the response phase



Parameters: N=5, topology changes, infection randomly selected for the experiment run, healing constant

Conclusion

- RRE achieves resilience by limiting connectivity during healing and learning
- Method is robust against estimation error and clock drifts
- Containment is theoretically fast

Future Work

- Design a feedback controller that uses learned estimates
  - Improve estimate
  - Robustness to errors
  - Maximize connectivity

State estimation: $\hat{p} = f(\tilde{\beta}, A, D)$

Measurements: $p = \{0,1\}$

Feedback controller: $D = \gamma \cdot \hat{p}$ such that $\gamma > 0$