FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Scalable Supervisory Control Approach for Dynamic Cybersecurity

Mohammad Rasouli, Erik Miehling, Demosthenis Teneketzis
Dept. of Electrical Engineering & Computer Sciences,
University of Michigan, MI, USA

NSF FORCES Grant: CNS-1238962

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Outline

- Introduction/Contribution
- Model
- Problem formulation
- **Scalability of the approach**
- Results
- Summary/conclusion

[Preliminary version has shown up in GameSec2014 and FORCES Nov14 Annual Review]

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

Motivation

- Key issues in cyber-security systems
  - **Progressive attacks**
  - **Dynamic/adaptive defense**
  - **Imperfect information** (for attacker and/or defender) of system status
  - **Non-strategic** vs. strategic attacker (**control** vs. game theory)
  - **Complexity** of security problems growing in **time** and in **scale of the network**.

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

Contribution

A **supervisory control** approach for cyber-security from the point of view of the defender with

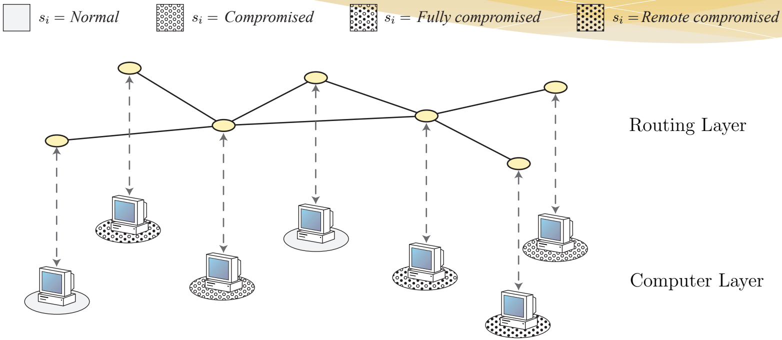
- progressive attacks,
- defender's imperfect information,
- dynamic defense,
- conservative approach to security,
- quantification of defender cost of state and action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal policy (within a restricted set) for a min-max performance criterion
- scalabe in time and size of the security environments

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

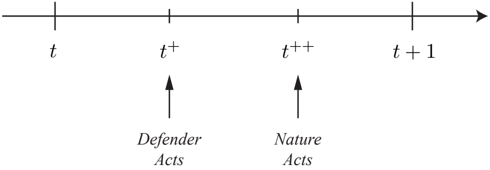
Model: Network Structure



- Possible states of each computer : Normal ($L1$), Compromised ($L2$), Fully Compromised ($L3$), Remote Compromised ($L4$).

Model: Timing

- Interaction rules between controller and nature



- Time horizon ⇒ finite or infinite

Model: Decision maker and its costs

Decision Maker

- One decision-maker
  - Defender ⇒ controller/decision maker
  - Attacker ⇒ nature
- Imperfect observation for defender

Costs

- Cost of state $Z \Rightarrow C(Z)$
- Cost of controllable event $d \Rightarrow \hat{C}(d), d \in \mathcal{D}$

Model: Decision maker and its costs

Decision Maker

- One decision-maker
  - Defender ⇒ controller/decision maker
  - Attacker ⇒ nature
- Imperfect observation for defender

Costs

- Cost of state $Z \Rightarrow C(Z)$
- Cost of controllable event $d \Rightarrow \hat{C}(d), d \in \mathcal{D}$

Model: Decision maker and its costs

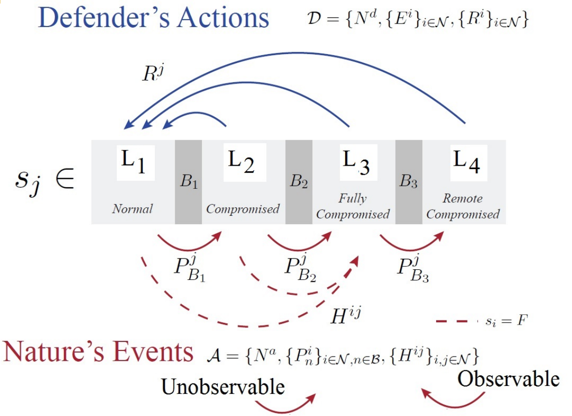
Decision Maker

- One decision-maker
  - Defender $\Rightarrow$ controller/decision maker
  - Attacker $\Rightarrow$ nature
- Imperfect observation for defender

Costs

- Cost of state $Z \Rightarrow C(Z)$
- Cost of controllable event $d \Rightarrow \hat{C}(d), d \in \mathcal{D}$

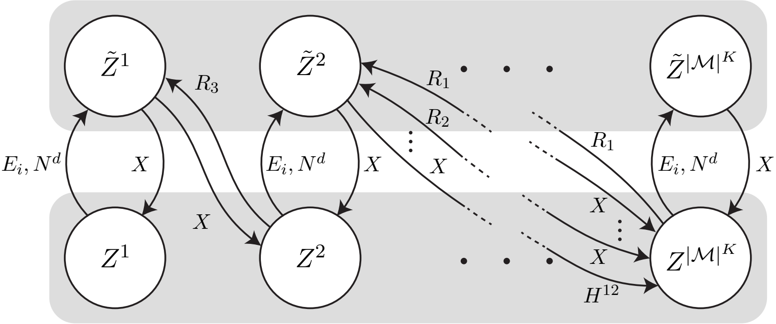
Model: Defender and Nature Actions



- Non-probabilistic dynamics

Model: System Automaton

System state before nature's event



System state before defender's action

Defender's Optimal Policy

choose best defense policy

compute worst case state trajectory under policy, g

$$\min_{g\in\mathcal{G}} \max_{\{Z_t^g\in\mathcal{Z},t\in\mathcal{T}\}} \left\{\sum_{t\in\mathcal{T}} \beta^t \left[C_{Z_t^g} + \hat{C}(d_t)\right]\right\}$$

$$\text{subject to} \qquad \text{System dynamics}$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

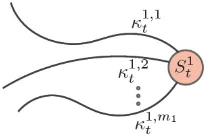
Problem: Growing in time/Countably infinite

Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite
Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$

$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

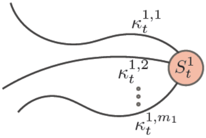
Problem: Growing in time/Countably infinite

Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite
Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$
$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

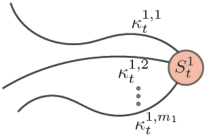
Problem: Growing in time/Countably infinite

Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite
Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$
$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

Problem: Growing in time/Countably infinite

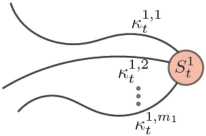
Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite

Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$

$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

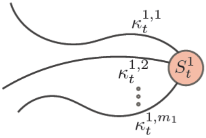
Problem: Growing in time/Countably infinite

Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite
Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$

$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

Problem: Growing in time/Countably infinite

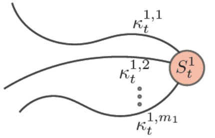
Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite

Solution: We propose the first approximation

$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$

$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

Time Complexity: Information State

Defender problem has complex information structure

- History of observations and actions

For MinMax objective function can be translated to

- All system trajectories consistent with the history

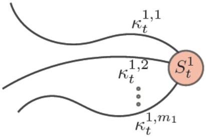
Problem: Growing in time/Countably infinite

Due to Markovian and non-probabilistic dynamics can be translated to

- All possible system states and maximum cost of reaching each

Problem: Bounded but countably infinite
Solution: We propose the first approximation

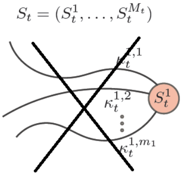
$$S_t = (S_t^1, \ldots, S_t^{M_t})$$



$$\kappa_t^1 = \max\{\kappa_t^{1,1}, \ldots, \kappa_t^{1,m_1}\}$$

$$\kappa_t = (\kappa_t^1, \ldots, \kappa_t^{M_t})$$

First Approximation: Observer States



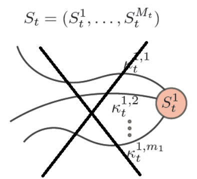
$$S_{t+1} = f(S_t, d_t, a_t)$$

observer state

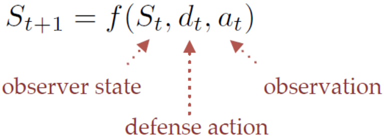
defense action

observation

First Approximation: Observer States



Defender's observer: the possible states that the network can be in at time *t* from the defender's perspective (defender has imperfect information).



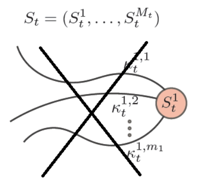
$$S_{t+1} = f(S_t, d_t, a_t)$$

observer state

defense action

observation

First Approximation: Observer States



Defender's observer: the possible states that the network can be in at time *t* from the defender's perspective (defender has imperfect information).

$$S_{t+1} = f(\underset{\text{observer state}}{S_t}, \underset{\text{defense action}}{d_t}, \underset{\text{observation}}{a_t})$$

Observer Automaton: Dynamics of observer states

The Defender's Problem (P'_D)

Problem (P'_D)

$$\min_{g \in \mathcal{G}'} \max_{Z_t^g \in S_t} \left\{ \sum_{t \in \mathcal{T}} \beta^t \left[C_{Z_t^g} + \hat{C}(d_t) \right] \right\} \qquad (P'_D)$$

$$\begin{aligned} \text{subject to} \quad & \text{model dynamics} \\ & d_t = g_t(S_t),\ t \in \mathcal{T}, \\ & S_{t+1} = f(S_t, d_t, a'_t),\ t \in \mathcal{T}. \end{aligned}$$

$$\mathcal{G}' := \{g \,|\, g := \{g_t, t \in \mathcal{T}\}, g_t : \mathcal{S} \to \mathcal{D}, d_t = g_t(S_t) \quad \text{for all} \quad t \in \mathcal{T}\}.$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Numerical Sensitivity Analysis for Two Computers

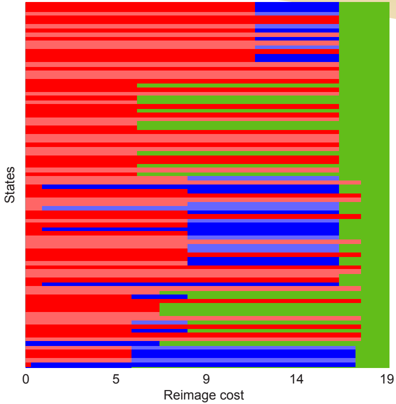


Figure: Optimal defender policy (Reimage, Sense, Null) with increasing cost of Reimage.

- **Threshold in Costs** - If $d^*(S1) = Reimgae$, by decreasing the cost of Reimage, it remains optimal action.
- **Duality of Control and Estimation** - There is no Sensing action in the optimal policy when there is no Reimage.

Numerical Sensitivity Analysis for Two Computers

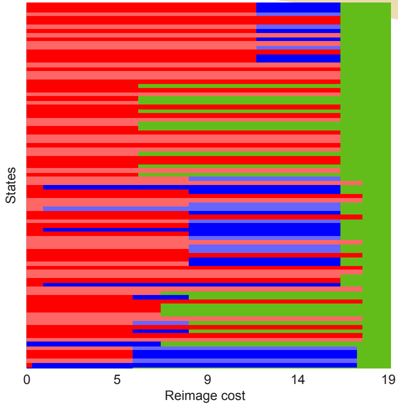


Figure: Optimal defender policy (Reimage, Sense, Null) with increasing cost of Reimage.

- **Threshold in Costs** - If $d^*(S1) = Reimgae$, by decreasing the cost of Reimage, it remains optimal action.
- **Duality of Control and Estimation** - There is no Sensing action in the optimal policy when there is no Reimage.

Numerical Sensitivity Analysis for Two Computers

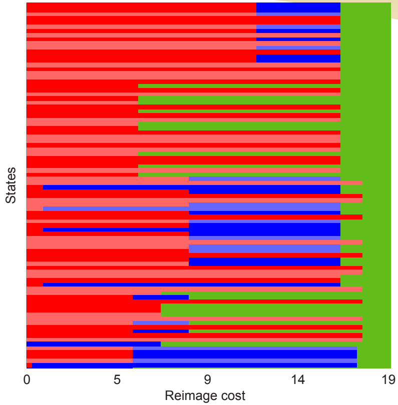


Figure: Optimal defender policy (Reimage, Sense, Null) with increasing cost of Reimage.

- **Threshold in Costs** - If $d^*(S1) = Reimgae$, by decreasing the cost of Reimage, it remains optimal action.
- **Duality of Control and Estimation** - There is no Sensing action in the optimal policy when there is no Reimage.

Network Scale Complexity

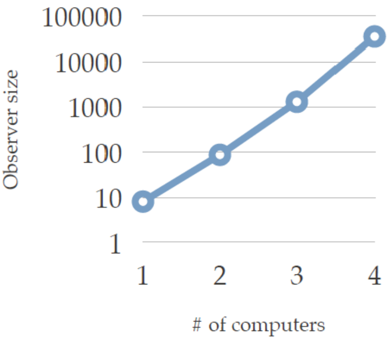


Figure: Number of observer states

Solution: We propose the second approximation

Network Scale Complexity

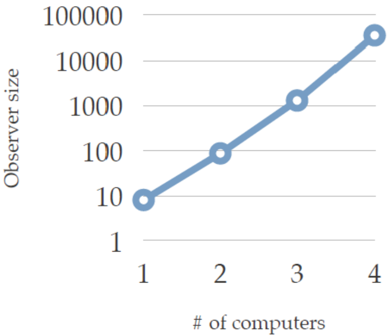
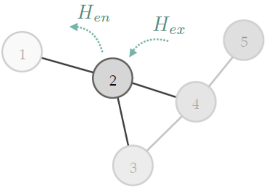


Figure: Number of observer states

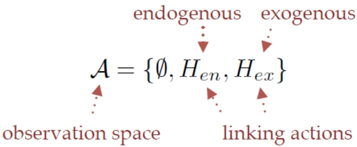
Solution: We propose the second approximation

Second Approximation: Decomposition and Parallel Computation

1. Consider **individual computers** coupled to other computers by **endogenous** and **exogenous** events.
2. Assume **exogenous** events are always possible.



For node 2: $S_t = \{\{L_1\}, \{L_1, L_2\}, \{L_2, L_3\}, \{L_3, L_4\}\}$



endogenous exogenous

$$\mathcal{A} = \{\emptyset, H_{en}, H_{ex}\}$$

observation space linking actions

Numerical Results: Sets of policies for each computer

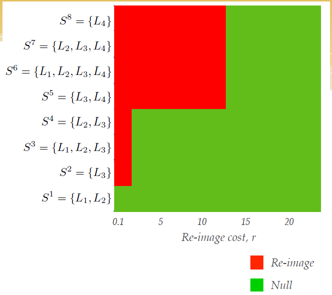


Figure: Computation based on local information

- **Threshold in Observer States** - If most costly state is more expensive in S_1 than S_2, and $d^*(S2) = Reimage$ then $d^*(S1) = Reimage$.
- **Grouping** - If S_1 and S_2 have same most costly state, then $d^*(S1) = d^*(S2)$.
- No sense action

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Numerical Results: Sets of policies for each computer

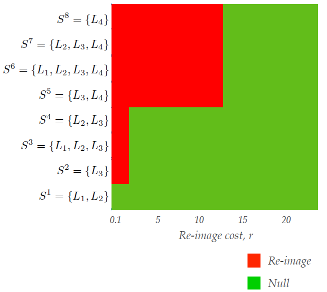


Figure: Computation based on local information

- **Threshold in Observer States** - If most costly state is more expensive in S_1 than S_2, and $d^*(S2) = \mathit{Reimage}$ then $d^*(S1) = \mathit{Reimage}$.
- **Grouping** - If S_1 and S_2 have same most costly state, then $d^*(S1) = d^*(S2)$.
- No sense action

Numerical Results: Sets of policies for each computer

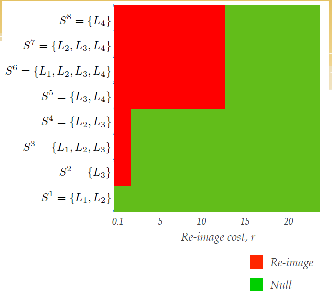


Figure: Computation based on local information

- **Threshold in Observer States** - If most costly state is more expensive in S_1 than S_2, and $d^*(S2) = Reimage$ then $d^*(S1) = Reimage$.
- **Grouping** - If S_1 and S_2 have same most costly state, then $d^*(S1) = d^*(S2)$.
- No sense action

Numerical Results: Sets of policies for each computer

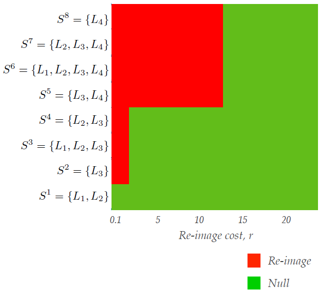


Figure: Computation based on local information

- **Threshold in Observer States** - If most costly state is more expensive in S_1 than S_2, and $d^*(S2) = \mathit{Reimage}$ then $d^*(S1) = \mathit{Reimage}$.
- **Grouping** - If S_1 and S_2 have same most costly state, then $d^*(S1) = d^*(S2)$.
- No sense action

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Summary

- **Supervisory control approach** to **dynamic cyber-security** from defender's perspective with **imperfect information**, progressive attacks, and min-max performance criterion by use of **system automaton**
- Capturing **complexity** in **time** and **scale of the network**
- Dynamic programming with numerical results for determining defender's optimal min-max actions at each instant of time
- Structural properties
  - Threshold behavior: costs of actions/states, observer states
  - Grouping: Observer states with same optimal policies

Summary

- **Supervisory control approach** to **dynamic cyber-security** from defender's perspective with **imperfect information**, progressive attacks, and min-max performance criterion by use of **system automaton**
- Capturing **complexity** in **time** and **scale of the network**
- Dynamic programming with numerical results for determining defender's optimal min-max actions at each instant of time
- Structural properties
    - Threshold behavior: costs of actions/states, observer states
    - Grouping: Observer states with same optimal policies

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Summary

- **Supervisory control approach** to **dynamic cyber-security** from defender's perspective with **imperfect information**, progressive attacks, and min-max performance criterion by use of **system automaton**
- Capturing **complexity** in **time** and **scale of the network**
- Dynamic programming with numerical results for determining defender's optimal min-max actions at each instant of time
- Structural properties
    - Threshold behavior: costs of actions/states, observer states
    - Grouping: Observer states with same optimal policies

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Summary

- **Supervisory control approach** to **dynamic cyber-security** from defender's perspective with **imperfect information**, progressive attacks, and min-max performance criterion by use of **system automaton**
- Capturing **complexity** in **time** and **scale of the network**
- Dynamic programming with numerical results for determining defender's optimal min-max actions at each instant of time
- Structural properties
  - Threshold behavior: costs of actions/states, observer states
  - Grouping: Observer states with same optimal policies

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Future Research

- Extending approximations and using structural results for scalability
- Extending to probabilistic events (Bayesian framework)
- Game formulation: dynamic game with asymmetric information

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Future Research

- Extending approximations and using structural results for scalability
- Extending to probabilistic events (Bayesian framework)
- Game formulation: dynamic game with asymmetric information

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Future Research

- Extending approximations and using structural results for scalability
- Extending to probabilistic events (Bayesian framework)
- Game formulation: dynamic game with asymmetric information

Thank you

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Appendix: observer automaton

Construction of observer automaton based on system automaton using UMDES-LIB software library available on https://www.eecs.umich.edu/umdes/toolboxes.html.