FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

A Supervisory Control Approach to Dynamic Cyber-Security

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

Berkeley University of California · Massachusetts Institute of Technology · NSF · Michigan · Vanderbilt University

Outline

- Introduction/Motivation
  - Literature review
  - Contribution
- Model
- Problem formulation
- Results
- Summary/conclusion

Outline

Introduction/Motivation

Model

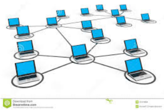
The Defender's Problem (P_D)

Defender Optimal Policy

Conclusion

Motivation

- Increasing importance of safety of many modern technological systems
  - computer networks
  - the internet
  - mobile networks
  - power grids
  - implantable medical devices
  - ...

- Strengthen resiliency of systems against attacks, intentional and unintentional misuses, and inadvertent failures.

Motivation

- Key issues in cyber-security systems
  - Progressive attacks
  - Dynamic/adaptive defense
  - Imperfect knowledge (for attacker and/or defender) of system status
  - Non-strategic vs. strategic attacker (control vs. game theory)

Literature Review

- Static models: perfect vs. imperfect information
  - One-agent-model: resource allocation for infrastructure protection [Bier et al 2007, Bohme-Felegyhazi 2010, Chen-Jamil 2006, Bloem et al 2007, Bloem et al 2009, Chen-Jamil 2006, Mastroleon 2009 and many others]
  - Based on game theory: [Bier et al 2007, Chen-Jamil 2006, Roy et al. 2010, Schwartz 2013 and many others].
- Dynamic models: perfect vs. imperfect information
  - Based on control theory: [Khouzani et al. 2012, Ligatti et al. 2005, Ligatti 2009, Rowe et al. 2012, Schneider 2000 and many others]
  - Based on game theory: [Khouzani 2012, Roy et al. 2010, Van Dijk et al. 2013, Yin et al. 2010 and many others].

Literature Review

- Static models: perfect vs. imperfect information
  - One-agent-model: resource allocation for infrastructure protection [Bier et al 2007, Bohme-Felegyhazi 2010, Chen-Jamil 2006, Bloem et al 2007, Bloem et al 2009, Chen-Jamil 2006, Mastroleon 2009 and many others]
  - Based on game theory: [Bier et al 2007, Chen-Jamil 2006, Roy et al. 2010, Schwartz 2013 and many others].
- **Dynamic models**: perfect vs. **imperfect information**
  - **Based on control theory**: [Khouzani et al. 2012, Ligatti et al. 2005, Ligatti 2009, Rowe et al. 2012, Schneider 2000 and many others]
  - Based on game theory: [Khouzani 2012, Roy et al. 2010, Van Dijk et al. 2013, Yin et al. 2010 and many others].

Contribution

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

- progressive attacks,
- defender's imperfect knowledge of the state of the system,
- dynamic defense,
- conservative approach to security,
- quantification of the cost incurred at every possible state of the system and every possible defender action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal control policy (within a restricted set of policies) for a min-max performance criterion.

Contribution

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

- progressive attacks,
- defender's imperfect knowledge of the state of the system,
- dynamic defense,
- conservative approach to security,
- quantification of the cost incurred at every possible state of the system and every possible defender action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal control policy (within a restricted set of policies) for a min-max performance criterion.

Contribution

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

- progressive attacks,
- defender's imperfect knowledge of the state of the system,
- dynamic defense,
- conservative approach to security,
- quantification of the cost incurred at every possible state of the system and every possible defender action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal control policy (within a restricted set of policies) for a min-max performance criterion.

Contribution

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

- progressive attacks,
- defender's imperfect knowledge of the state of the system,
- dynamic defense,
- conservative approach to security,
- quantification of the cost incurred at every possible state of the system and every possible defender action,

that achieves

- quantification of the performance of various defender policies,
- determination of the defender's optimal control policy (within a restricted set of policies) for a min-max performance criterion.

Outline

Introduction/Motivation

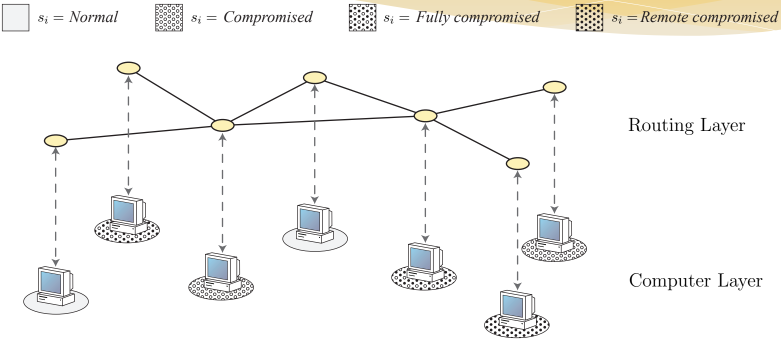
Model

The Defender's Problem (P_D)

Defender Optimal Policy

Conclusion

Model: Network Structure



- Possible states of each computer i : Normal (N), Compromised (R), Fully Compromised (W), Remote Compromised (F).

Model: System State

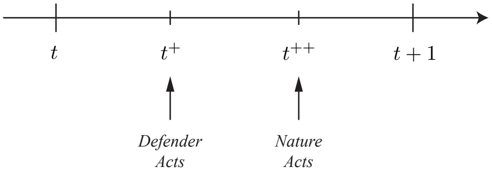
- System of K computers, $\mathcal{N} = \{1, 2, \ldots, K\}$
  - state of the system $Z = \{s_1, s_2, ..., s_K\}$
  - s_i state of computer i
  - $s_i \in \{N, R, W, F\}$
    - N = Normal
    - R = compromised
    - W = Fully compromised
    - F = Remote compromised

Model

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

Model: Timing

- Interaction rules between controller and nature



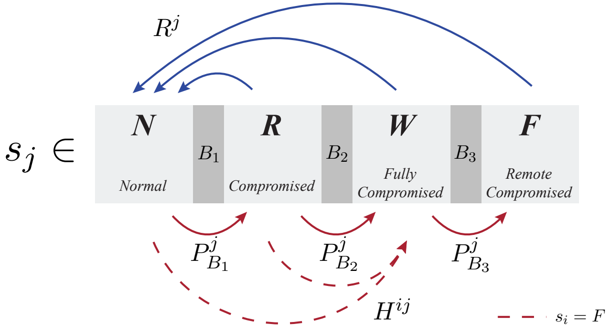
Model: Defender Costs

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

Model: Defender and Nature Actions

Defender's Actions

$\mathcal{D} = \{N^d, \{E^i\}_{i\in\mathcal{N}}, \{R^i\}_{i\in\mathcal{N}}\}$



Nature's Events

$\mathcal{A} = \{N^a, \{P^i_n\}_{i\in\mathcal{N}, n\in\mathcal{B}}, \{H^{ij}\}_{i,j\in\mathcal{N}}\}$

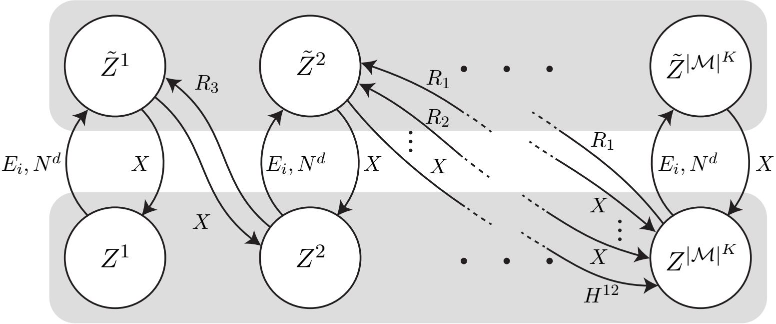
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Model: Discrete Event Systems

- All events/transitions $\mathcal{E} = \mathcal{A} \cup \mathcal{D}$.
- Controllable (by the defender) events: $\mathcal{D}$
- Observable (by the defender) events: $\mathcal{D} \cup \left\{\{H^{ij}\}_{i,j\in\mathcal{N}}\right\}$
  - Defender's observation of nature's events: $\mathcal{A}' = \{X, \{H^{ij}\}_{i,j\in\mathcal{N}}\}$ where $X = \{N^a, \{P_n^i\}_{i\in\mathcal{N}, n=B_1,B_2,B_3}\}$
- Events admissible/allowable at each state
  - $\mathcal{D} \cup \{N^a\}$ are admissible from every state
  - Event $\{H^{ij}\}_{i,j\in\mathcal{N}}$ is only admissible when $s_i = F$ and $s_j = \{N, R, W\}$
  - Probe $P_{B_1}^i$, $P_{B_2}^i$, and $P_{B_3}^i$ only admissible from $s_i = N$, $s_i = R$, and $s_i = W$, respectively.

Model: System Automaton

System state before nature's event



System state before defender's action

Outline

Introduction/Motivation

Model

The Defender's Problem (P_D)

Defender Optimal Policy

Conclusion

Defender's Optimal Policy

- Optimization problem

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

$$\text{subject to} \quad \text{model dynamics}$$

- Information state at $t^+ \Rightarrow$ All system trajectories up to $(t-1)^{++}$ consistent with the history of observations and actions
- Using this information state one can in principle write the dynamic program for P_D.
- Computationally intractable dynamic program
- Restricting attention to defense policies with specific structure

The Defender's Problem (P'_D)

- Defender's observer: the possible states that the network can be in at time t from the defender's perspective (defender has imperfect information).
- Observer dynamics
  - S_t: observer's state at t
  - d_t: defender's action at t^+
  - a'_t: nature's move at t^{++}

$$S_{t+1} = f(S_t, d_t, a'_t)$$

- Problem (P'_D)

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

subject to model dynamics

$$d_t = g_t(S_t),\ t \in \mathcal{T},$$

$$S_{t+1} = f(S_t, d_t, a'_t),\ t \in \mathcal{T}.$$

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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Solution to (P'_D)

- Defender's dynamic program

$$V(S) = \min_{d \in \mathcal{D}} \max_{Z \in S} \left[C_Z + \hat{C}(d) + \max_{S' \in \mathcal{Q}(S,d,Z)} \beta V(S') \right]. \tag{1}$$

- $\mathcal{Q}(S, d, Z)$ is the set of observer states that can be reached by S when the defender's action is d and the true system state is Z
- Right-hand side of Eq. 1 is a contraction mapping.
- Use value iteration to solve P'_D.

Outline

Introduction/Motivation

Model

The Defender's Problem (P_D)

Defender Optimal Policy

Conclusion

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Numerical Solution to P'_D

- Build observer automaton from the system automaton (details in appendix)
- Number of observer states grows exponentially with number of computers
  - Two computer network: 87 states and 1207 transitions
    - Example: $\{RF, WF, FF\}, \{RN, WN, RR, WR, RW, WW, RF\}$.
  - Three computer network: 1423 states and 65602 transitions
    - Example: $\{RFW, WFW, FFN\}, \{RNW, WNN, RRW\}$.

Numerical Sensitivity Analysis for Two Computers

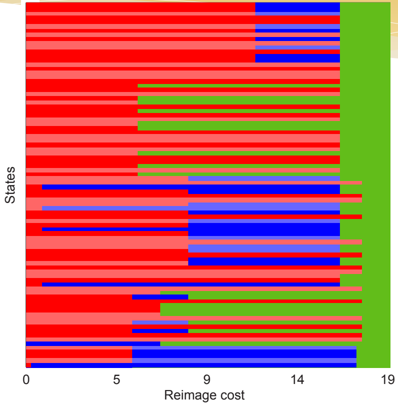


Figure: Optimal defender policy (Reimage, Sense, Null) with increasing cost of Reimage.

Numerical Sensitivity Analysis for Two Computers

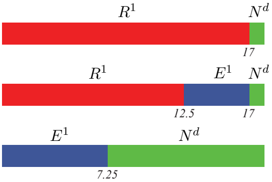
$S' = \{FN, FW, FR\}$

$\vdots$

$S'' = \{WN, FN, WR, FW, FR, WW, WF, FF\}$

$\vdots$

$S''' = \{NN, RN, NR, WN, RR, FN, WR, NW, RW, NF\}$



Results: Threshold property switching from Reimage to other defense actions

- Switching from Reimage to Sense or Null actions happens at different costs
- Duality of control (Reimage) and estimation (Sense)
- No Sense when there is no Reimage in the policy

Outline

Introduction/Motivation

Model

The Defender's Problem (P_D)

Defender Optimal Policy

Conclusion

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
- Dynamic programming with numerical results for determining defender's optimal min-max actions at each instant of time
- Threshold behavior with varying cost of actions/states

Future Research

- Address exponentially growing number of states and transitions with the number of computers
  - qualitative properties of optimal defender strategies to accommodate large networks
  - hierarchical decomposition
  - approximate dynamic programming methods
- Game theoretic formulation
  - dynamic game with asymmetric information

Thank you!!

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.