Opacity and Structural Resilience in Cyberphysical Systems
Bhaskar Ramasubramanian1, Rance Cleaveland2, Steven I. Marcus3
1Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park
2Department of Computer Science, and Institute for Systems Research, University of Maryland, College Park

Cyberphysical Systems are Ubiquitous
- Found across scales/sizes
- Controlled over a n/w
- Remote attacks

Attack Impact
- Compromised CPS: repercussions
- Information critical to nominal operation must be safeguarded
- Several instances in last 15–20 years

Opacity for Continuous State Systems
- Square matrix: A
- Computed CPS: repercussions
- Controlled over a n/w
- Remote attacks

Opacity: Motivation
- Can an intruder infer a ‘secret’ of the system based on its observation of the system behavior?
- ‘Secret’ = location, electricity consumption, ...
- Current state of the art: opacity for DESs.

Structural Resilience: Motivation
- Square matrix: A
- Computed CPS: repercussions
- Controlled over a n/w
- Remote attacks

Research Outline
CPS Security is Important!
- New notion of opacity for CPSs:
  - Single adversary: k-ISO
  - Multiple adversaries: > 1 notion of decentralized opacity
  - Switched Linear Systems: DES opacity + k-ISO
  -Opacity in terms of reachable states
  - Structural resilience of CPSs to attacks:
    - Method independent of numerical values
    - Resilience depends on properties of directed and bipartite graph representations of systems
    - Establish conditions for resilience to DoS attacks
    - Future directions:
      - Computing reachable sets efficiently
      - Controls incurring costs
      - Structural resilience of switched systems
      - Extension to nonlinear systems

The Structural Approach
- Large scale CPS: many states, variables’ values fluctuate ⇒ computational analysis costly.
- Use knowledge of positions of zero/ nonzero entries of system matrices.
- Properties will hold for almost all valid numerical realizations.
- Linear structured system:
  \[ x(t+1) = Ax(t) + Bu(t) \]
  \[ y(t) = Cx(t); i=1,2,\ldots,l \]
  \[ A \in \mathbb{R}^{n \times n} \]
- Every entry in \( A \) and \( B \) is either a fixed zero (0) or a free parameter (\( \ast \)).
- \( (A, B) \) is structurally controllable if there exists an admissible \( (A, B) \) that is controllable.
- \( (A, B) \) structurally controllable ⇒ almost every \( (A, B) \) is controllable

Structured as a Graph
- \( A_{ij} \neq 0 \Rightarrow \text{edge } (i \rightarrow j) \)
- \( (i \rightarrow j) \Rightarrow y_{ij} = y_{ij} \)
- \( n \in \text{ right unm. vertices} \)
- \( \beta \) = # non top-linked SCCs

Denial of Service: Structural Resilience
- Inputs in \( v_{ij} \) can only be connected to state vertices in \( X_{\text{diff}}(X_{\text{sys}}) \)
- Attacker blocks \( u_{ij} \Rightarrow u_{ij} = 0 \)
- STRUCTURALLY, \( |B| = 0 \)
- Ensure resilience to attack by controlling states in \( X_{\text{diff}} \) via \( |B| \)
- Structural resilience: system post-attack is structurally controllable
- Assume \( x_{1}, \ldots, x_{n} \in X_{\text{diff}} \) \( x_{7}, \ldots, x_{10} \in X_{\text{safe}} \)

Opacity: The Single Adversary Case
Definition (Strong k- Initial State Opacity): Given \( X, X_{\text{sys}} \subseteq X_{0} \) and \( k \in K \), \( X_{i} \) is strongly k-ISO with respect to \( X_{\text{sys}} \) if:
- \( \exists! \ x_{i}(0) \in X_{i} \) and admissible controls \( u_{i}(0), \ldots, u_{i}(k-1) \), \( \exists! x_{\text{sys}}(0) \in X_{\text{sys}} \) and admissible controls \( u_{\text{sys}}(0), \ldots, u_{\text{sys}}(k-1) \), such that \( y_{i}(k) = y_{\text{sys}}(k) \).
- Adversary\ must determine \( x(0) \) from snapshots of output.
- Will not want to reveal its presence.
- Might not have resources to observe for all time.
- Theorem:
  - Verifying k-ISO is equivalent to checking membership of \( y(k) \) in a set of states reachable at time \( k \), starting from \( X \) and \( X_{\text{sys}} \).
  - k-ISO (under mild additional assumptions) is equivalent to output controllability.

Opacity: The Multiple Adversary Case
- Notions of decentralized opacity based on:
  - Presence/absence of centralized coordinator
  - Presence/absence of collusion among adversaries

Opacity for Switched Linear Systems
- Discrete-time Switched Linear System:
  \[ x(t+1) = A_{M_{t}}(t)x(t) + B(t)u(t) \]
  \[ y(t) = C_{t}x(t) \]
  \[ A_{M_{t}} \in \{1, \ldots, z\} \]
  \[ M_{t} = \text{mode at time } t \]
  \[ k = \text{time at which adversary makes observation} \]
  \[ q = \text{number of mode changes} \]

Adversary Goal
- Q: Observes \( M_{t-1} \), is initial mode a secret mode?
  \( A, (k, q) \)
  (Initial Mode Opacity (k, q)-IMO)
- Q: Observes \( y(t) \), \( M_{t-1} \), did system start from a secret state and mode?
  \( A, (k, q) \)
  (Initial Mode and State Opacity (k, q)-IMSO)

References

Work supported by NSF Grant CNS-1446665
rRhaskar@umd.edu, rance@cs.umd.edu, marcus@umd.edu