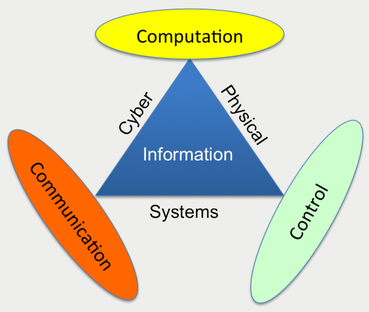
Opacity and Structural Resilience in Cyberphysical Systems

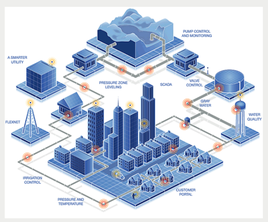
Bhaskar Ramasubramanian[1], Rance Cleaveland[2], Steven I. Marcus[1]

[1]Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park
[2]Department 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

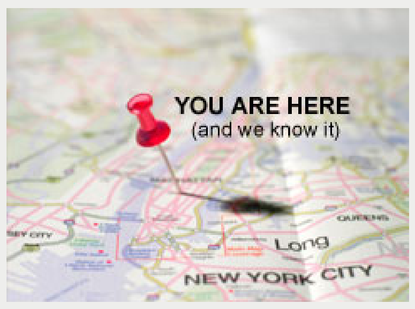


Attack Impact

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

Opacity: 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

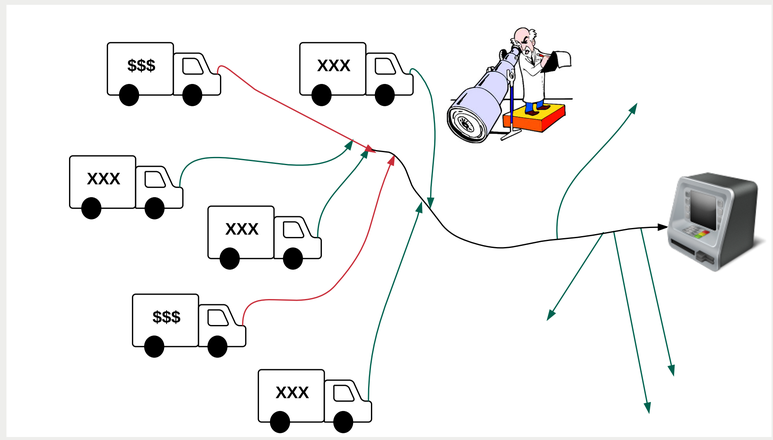
- Square matrix: $A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{bmatrix}$; $rank(A) = 3$
- $A_{ij} \neq 0 \rightarrow *$; Structured matrix: $[A] = \begin{bmatrix} * & 0 & * \\ * & * & 0 \\ * & * & * \end{bmatrix}$
- Arbitrarily assign 'numbers' to $*$
- RANK (almost) ALWAYS REMAINS THE SAME!
- Extends to several system properties

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 system
  - 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

Opacity for Continuous State Systems



- Discrete-time linear time-invariant system:

$$x(t+1) = Ax(t) + Bu(t)$$
$$x(0) = x_0 \in X_0$$
$$y_i(t) = C_i x(t);\ i = 1, 2, \ldots, l$$

- $\mathcal{K} \subset \mathbb{Z}_+$: times at which adversaries observe the system.
- $X_s, X_{ns} \subset X_0$: sets of initial secret, nonsecret states.
- **Q.** When is X_s **opaque** with respect to X_{ns}, given observations at $k \in \mathcal{K}$?

Opacity: The Single Adversary Case

Definition (Strong k- Initial State Opacity): Given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathcal{K}$, X_s is **strongly k-ISO** with respect to X_{ns} if :
$\forall\ (x_s(0) \in X_s$, and admissible controls $u_s(0), \ldots, u_s(k-1))$,
$\exists\ (x_{ns}(0) \in X_{ns}$, and admissible controls $u_{ns}(0), \ldots, u_{ns}(k-1))$,
such that $\mathbf{y_s(k)} = \mathbf{y_{ns}(k)}$.

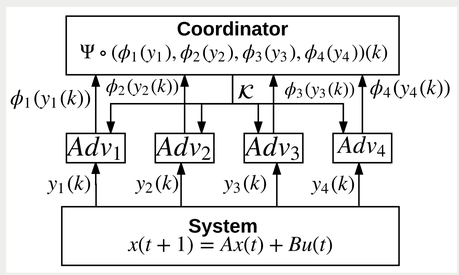
- Adversary must determine $x(0)$ from snapshots of output.
  - will not want to reveal its presence.
  - might not have resources to observe for all time.

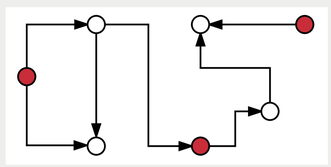
Theorem:

- Verifying k-ISO is equivalent to checking membership of $y(k)$ in a set of states reachable at time k, starting from X_s and X_{ns}.
- 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:

$$x(t+1) = A(\mathcal{M}_t)x(t) + B(\mathcal{M}_t)u(t)$$
$$x(0) = x_0 \in X_0$$
$$y(t) = Cx(t)$$

- $\mathcal{M}_t \in \{1, \ldots, z\}$: mode at time t
- $k :=$ time at which adversary makes observation
- $q :=$ number of mode changes

Adversary Goal

- **Q.** Observes $\mathcal{M}_{k-1}$, is initial mode a secret mode?
  A. (k, q)-Initial Mode Opacity ((k, q)-IMO)
- **Q.** Observes $y(k), \mathcal{M}_{k-1}$, did system start from a secret state and mode?
  A. (k, q)-Initial Mode and State Opacity ((k, q)-IMSO)

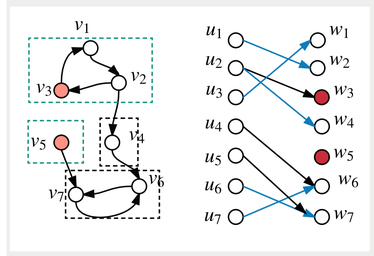
The Structural Approach

- 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:

$$\dot{x}(t) = [A]x(t) + [B]u(t)$$
$$= [A]x(t) + [B_{def}]u_{def}(t) + [B_{att}]u_{att}(t)$$

- Every entry in $[A]$ and $[B]$ is either a *fixed* zero (0) or a *free* parameter ($*$).
- $([A], [B])$ is *structurally controllable* if there exists an admissible (A, B) that is controllable.
- $([A], [B])$ *structurally controllable* ⇒ *almost* every (A, B) is controllable

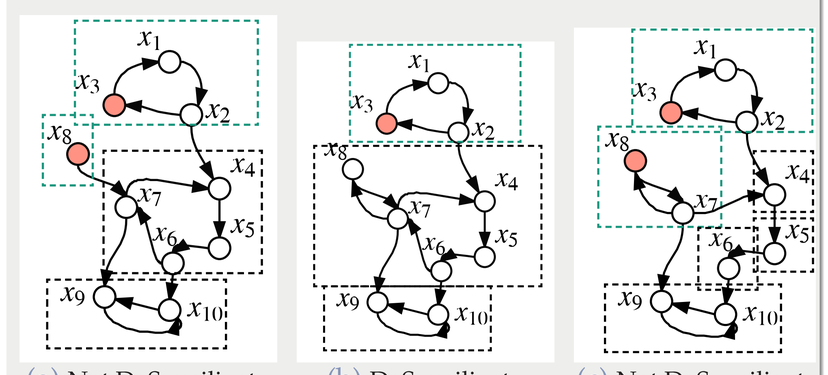
Structured System as a Graph



- $[A]_{ji} \neq 0 \Rightarrow$ edge $(v_i \Rightarrow v_j)$
- $(v_i \rightarrow v_j)_{\mathcal{D}([A])} \Rightarrow (u_i \rightarrow w_j)_{\mathcal{B}([A])}$
- m : # right unm. vertices in a max. matching
- β : # non top-linked SCCs

Denial of Service: Structural Resilience

- Inputs in $u_{def}(u_{att})$ can only be connected to state vertices in $\mathcal{X}_{def}(\mathcal{X}_{att}) \subset \mathcal{X}$
- Attacker blocks $u_{att} \Rightarrow u_{att} = 0$
- *STRUCTURALLY*, $[B_{att}] = 0$
- Ensure resilience to attack by controlling states in $\mathcal{X}_{def}$ via $[B_{def}]$
- **Structural resilience**: system *post-attack* is structurally controllable
- Assume $x_1, \ldots, x_6 \in \mathcal{X}_{def}$, $x_7, \ldots, x_{10} \in \mathcal{X}_{att}$



(a) Not DoS-resilient (b) DoS-resilient (c) Not DoS-resilient

Figure: Structural Resilience to DoS Attack

References

1. B. Ramasubramanian, R. Cleaveland, S. I. Marcus, *Opacity for Switched Linear Systems: Notions and Characterization*, Proc. of the IEEE Conference on Decision and Control, 2017.
2. B. Ramasubramanian, R. Cleaveland, S. I. Marcus, *A Framework for Decentralized Opacity in Linear Systems*, Proc. Annual Allerton Conference in Communication, Control, and Computing, 2016.
3. B. Ramasubramanian, R. Cleaveland, S. I. Marcus, *A Framework for Opacity in Linear Systems*, Proc. IEEE American Control Conference, 2016.
4. B. Ramasubramanian, M. A. Rajan, M. G. Chandra, *Structural Resilience of Cyberphysical Systems Under Attack*, Proc. IEEE American Control Conference, 2016.
5. B. Ramasubramanian, M. A. Rajan, M. G. Chandra, R. Cleaveland, S. I. Marcus, *Denial of Service Resilience in Cyberphysical Systems: A Structured Systems Approach*, In Submission.

Work supported by NSF Grant CNS-1446665

rbhaskar@umd.edu, rance@cs.umd.edu, marcus@umd.edu