A Framework for Opacity in Linear Systems

Bhaskar Ramasubramanian\textsuperscript{1}, Rance Cleaveland\textsuperscript{2}, Steven I. Marcus \textsuperscript{1}

\textsuperscript{1}Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA.

\textsuperscript{2}Department of Computer Science, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA.
Opacity: Motivation

Opacity as a Notion of Security

- Can a passive intruder infer a "secret" of the system based on its observation of the system behavior?
- Current state of the art: opacity for DESs.
- States in a DES are discrete.
Opacity as a Notion of Security

- Can a passive intruder infer a "secret" of the system based on its observation of the system behavior?
- Current state of the art: opacity for DESs.
- States in a DES are discrete.

Prior Work

- Supervisory control of DESs [Ramadge, Wonham(1987, 1989)].
- Opacity for cryptographic protocols [Mazaré(2004)].
- Opacity for DESs [Badouel(2007), Saboori(2007)].
Goal: every ‘secret’ should ‘look’ like something ‘nonsecret’.

(a) $\Sigma_o = \{a, b, c\}$
LBO: $L_s = \{abd\}, L_{ns} = \{abcc^*d, adb\}$
not LBO: $L_s = \{abcd\}, L_{ns} = \{adb\}$

(b) $\Sigma_o = \{a, b\}$
ISO: $X_s = \{x_3\}$, $X_{ns} = X \setminus X_s$
not ISO: $X_s = \{x_1\}$, $X_{ns} = X \setminus X_s$

Figure: DES Opacity [Wu, Lafortune(2013)]
Consider the discrete time linear time invariant system:

\[ x(t + 1) = Ax(t) + Bu(t) \]
\[ x(0) = x_0 \in X_0 \]
\[ y(t) = Cx(t) \]

\( K \subset \mathbb{Z}_+ \): times at which adversary observes the system.
\( X_s \subset X_0 \): set of initial secret states.
\( X_{ns} \subset X_0 \): set of initial nonsecret states.
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 w.r.t. $X_{ns}$ if
\[ \forall (x_s(0) \in X_s \text{ and admissible controls } u_s(0), \ldots, u_s(k)), \]
\[ \exists (x_{ns}(0) \in X_{ns} \text{ and admissible controls } u_{ns}(0), \ldots, u_{ns}(k)) \]
such that $y_s(k) = y_{ns}(k)$.

Definition: Strong $\mathcal{K}$- Initial State Opacity

$X_s$ is strongly $\mathcal{K}$–ISO w.r.t. $X_{ns}$ if $X_s$ is strongly $k$–ISO w.r.t. $X_{ns}$ for all $k \in \mathcal{K}$. 
Motivation for Definition

- **Standard Observability/ Estimation**: determine $x(0)$, given entire output and control sequences $\{y(\cdot)\}$ and $\{u(\cdot)\}$.

- **DES Opacity**:  
  - observation of the entire secret trajectory must coincide with that of an entire nonsecret trajectory.  
  - opacity enforcing supervisory control treated separately from the verification of opacity.
Motivation for Definition

- **Standard Observability/ Estimation**: determine $x(0)$, given entire output and control sequences $\{y(\cdot)\}$ and $\{u(\cdot)\}$.

- **DES Opacity**:  
  - observation of the entire secret trajectory must coincide with that of an entire nonsecret trajectory.
  - opacity enforcing supervisory control treated separately from the verification of opacity.

Our Framework

- Adversary must determine $x(0)$ from only snapshots of the system output. Only outputs at $k \in \mathcal{K}$ need to coincide.

- **Reasons**: Adversary will not want to reveal its presence. Might not have resources to make continuous observations.

- Controls form an integral part of the definition of $\mathcal{K}$–ISO.
Opacity and Reachable Sets

- Let $U^k_s := \{u_s(0), \ldots, u_s(k-1)\}$, $U^k_{ns} := \{u_{ns}(0), \ldots, u_{ns}(k-1)\}$
- Sets of reachable states starting from $X_s$ and $X_{ns}$:

$X_s(k) = \bigcup x_0 \in X_s \bigcup u(i) \in U^k_s \{x : x(i+1) = Ax(i) + Bu(i), \forall i < k\}$

$X_{ns}(k) = \bigcup x_0 \in X_{ns} \bigcup u(i) \in U^k_{ns} \{x : x(i+1) = Ax(i) + Bu(i), \forall i < k\}$
Opacity and Reachable Sets

- Let $U^k_s := \{u_s(0), \ldots, u_s(k - 1)\}$, $U^k_{ns} := \{u_{ns}(0), \ldots, u_{ns}(k - 1)\}$
- Sets of reachable states starting from $X_s$ and $X_{ns}$:

$$
X_s(k) = \bigcup_{x_0 \in X_s} \bigcup_{u(i) \in U^k_s} \{x : x(i + 1) = Ax(i) + Bu(i), \forall i < k\}
$$

$$
X_{ns}(k) = \bigcup_{x_0 \in X_{ns}} \bigcup_{u(i) \in U^k_{ns}} \{x : x(i + 1) = Ax(i) + Bu(i), \forall i < k\}
$$

- Sufficient condition for $k$–ISO: $X_s(k) \subseteq X_{ns}(k)$.

**Example**

Consider $C = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$, and $X_s(k) = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T$ and $X_{ns}(k) = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}^T$. Then, $y_s(k) = y_{ns}(k)$, establishing $k$–ISO, though $X_s(k) \not\subseteq X_{ns}(k)$. 
Theorem

\( X_s \) is strongly \( k \)-ISO w.r.t. \( X_{ns} \) \( \iff \) \( CX_s(k) \subseteq CX_{ns}(k) \).

\( X_s \) is strongly \( \mathcal{K} \)-ISO w.r.t. \( X_{ns} \) \( \iff \) \( CX_s(k) \subseteq CX_{ns}(k) \ \forall k \in \mathcal{K} \).
Theorem

\(X_s\) is strongly \(k\)-ISO w.r.t. \(X_{ns}\) \(\iff CX_s(k) \subseteq CX_{ns}(k)\).

\(X_s\) is strongly \(\mathcal{K}\)-ISO w.r.t. \(X_{ns}\) \(\iff CX_s(k) \subseteq CX_{ns}(k) \forall k \in \mathcal{K}\).

Proposition

1. \(X_{s_i} k\)-ISO w.r.t. \(X_{ns} \forall i \Rightarrow \bigcup_i X_{s_i} k\)-ISO w.r.t. \(X_{ns}\).
2. \(X_s k\)-ISO w.r.t. \(X_{ns_i} \forall i \Rightarrow X_s k\)-ISO w.r.t. \(\bigcup_i X_{ns_i}\).
3. \(X_{s_i} k\)-ISO w.r.t. \(X_{ns} \forall i \Rightarrow \bigcap_i X_{s_i} k\)-ISO w.r.t. \(X_{ns}\).
4. \(X_s k\)-ISO w.r.t. \(X_{ns_i} \forall i \neq X_s k\)-ISO w.r.t. \(\bigcap_i X_{ns_i}\).
A state $x$ is *output controllable* on $[0, k_f]$ if there exists a control sequence $\{u(\cdot)\}$ that transfers the system from $x(0) = x$ to $y(k_f) = 0$.

The output solution trajectory is given by:

$$y(k) = CA^k x(0) + \sum_{j=0}^{k-1} CA^{k-j-1} Bu(j)$$
Let $X_s$ be $k$–ISO with respect to $X_{ns}$.

Then, there exists a state that is output controllable on $[0, k]$.

Further, if $k$–ISO is established for $(x_s(0), x_{ns}(0)) \in X_s \times X_{ns}$ (and appropriate control sequences $\{u_s(\cdot)\}$ and $\{u_{ns}(\cdot)\}$), then the controls $u(i) = u_s(i) - u_{ns}(i), i = 0, \ldots, k - 1$, will ensure output controllability for the initial state $x(0) = x_s(0) - x_{ns}(0)$. 
Theorem

Let the system be output controllable in $k$ steps for a set of states $X_{oc}(0) \setminus \{0\}$ and controls $\{U(\cdot)\}$.

Let $X_1$ and $X_2$ be sets such that every $x_1 \in X_1$ can be written as $x + x_2$, where $x \in X_{oc}(0) \setminus \{0\}$ and $x_2 \in X_2$.

Then, $X_1$ is strongly $k$–ISO with respect to $X_2$. 
Proposed a new framework for opacity in linear systems.

Conditions derived to ensure opacity in terms of sets of reachable states.

Opacity shown to be equivalent to output controllability.

Other topics in paper:
- Weak \( k-\text{ISO} \).
- Algorithm to find \( X_s \) and \( X_{ns} \), given candidate initial secret and nonsecret states.
Future Work

- Decentralized, Weaker Notions of Opacity:
  - with/ without coordinator.
  - $k-$ISO holds only for a subset of adversaries.
  - $\epsilon$ $k-$ISO: Relax $y_s(k) = y_{ns}(k)$.

- Opacity for nonlinear and hybrid systems:
  - discrete time nonlinear systems.
  - (DES Opacity + $k-$ISO) for hybrid systems.
  - extension to continuous time systems and switched systems.

- Quantifying opacity and resilience:
  - differential privacy to model $\epsilon$ $k-$ISO.
Thank You.
Questions?