Fifty-fourth Annual Allerton Conference
Allerton House, UIUC, Illinois, USA
September 27 - 30, 2016

A Framework for Decentralized Opacity in Linear Systems*

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

***Abstract*— We formulate several notions of decentralized opacity for cyberphysical systems in the presence of multiple adversarial observers. Broadly speaking, we study the following cases: i) the presence or lack of a centralized coordinator, and ii) the presence or absence of collusion among the adversaries. In the case of colluding adversaries, we derive a condition for non-opacity that depends on the structure of the directed graph representing the communication between adversaries. Finally, we define a notion of opacity where the condition that the outputs be indistinguishable is relaxed.**

I. Introduction

Cyberphysical systems (CPSs) integrate communication, control, and computation with physical processes. Examples of CPSs include power systems, water distribution networks, and medical devices. A consequence of this interaction between computers and the physical system is that significant material damage can be caused by an attacker who is able to gain access to the system remotely. There have been several instances of remote attacks on CPSs. Examples include [1], [2], while techniques to alleviate threats are suggested in [3].

To gain illicit access to a CPS (or any other system), a prospective attacker must be able to extract useful information pertaining to the system, which can then be used by him or her to subvert the operation of the system. Thus, information critical to nominal operation should be safeguarded in a well-designed system; this motivation has led researchers to develop approaches for analyzing how *opaque* the system behavior is to an adversary. Opacity was initially formulated as a technique to study cryptographic protocols in [4], and is a property that captures whether a passive adversarial observer can infer a "secret" of the system based on its observations of the system behavior. It has been defined for discrete event systems (DESs) described by regular languages in [5], [6]. Language based ([7], [8]) and state based ([6], [9], [10]) notions of opacity were shown to be equivalent in [11], where algorithms to transform one form of opacity to the other were given. Opacity was compared to properties of DESs like detectability and diagnosability, and privacy properties like secrecy and anonymity in [12]. A subsequent paper [13] defined opacity for DESs in a decentralized framework with multiple adversaries, each carrying out its own observation of the system. Two cases were studied: first, in the absence of a centralized coordinator, and second, when the agents reported their observations to a coordinator. We cast both these cases within our framework, and study a third case when the agents communicate among themselves in the absence of a coordinator.

Although this theory is quite rich, it suffers from the drawback that states in a DES are discrete. In CPSs like power systems and water networks, it is common for the states to take values in a continuous domain. A notion of opacity for continuous state systems with a single adversary was first defined in [14]. The CPS was modeled as a discrete-time linear time invariant (DT-LTI) system, and tools from control theory were used to study opacity for such systems. A

*This work was supported by the NSF under Grants $CNS-1446665$ and $CMMI-1362303$, and by the AFOSR under Grant $FA9550-15-10050$.

[1]Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA.
{rbhaskar, marcus}@umd.edu

[2]Department of Computer Science, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. rance@cs.umd.edu

set of secret states was defined to be strongly $k-$ISO ($k-$initial state opaque) with respect to a set of nonsecret states if the outputs at time k of every trajectory starting from the set of secret states could not be distinguished from the output of some trajectory starting from the set of nonsecret states. Necessary and sufficient conditions for $k-$ISO were established in terms of sets of reachable states of the system. Further, under certain conditions, $k-$ISO was shown to be equivalent to output controllability of a system obeying the same dynamics, but with different initial conditions. In this paper, we extend this work by studying opacity for the case when there is more than one adversarial observer.

A. Outline of Paper

We briefly review the definition of opacity for LTI systems with a single adversarial observer in Section (II). Section (III) presents the main results of this paper. We formulate several notions of decentralized opacity for LTI systems with multiple observers, depending on whether or not there is a centralized coordinator, and the presence or absence of communication among the adversaries. Conditions to ensure decentralized opacity are formulated in terms of reachable sets of states. In the case of collusion amongst the adversaries, we derive a condition to ensure non-opacity in terms of the structure of the communication graph. The necessity of the indistinguishability of outputs in the existing definition of $k-$ISO is relaxed in Section (IV), where we define a notion of $\epsilon-$opacity. We conclude in Section (V) by presenting possible future directions of research.

II. Opacity for Linear Systems

Consider the system:

$$\begin{aligned} x(t+1) &= Ax(t)+Bu(t) \\ x(0) &= x_0 \in X_0 \\ y(t) &= Cx(t) \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n, u \in \mathbb{R}^m, y \in \mathbb{R}^p$, and A,B,C are matrices of appropriate dimensions containing real entries.

Let $\mathscr{K}$ be the instants of time the adversary makes an observation of the system. The subscript s (ns), when appended to the states, inputs, and outputs, will correspond to trajectories that start from the set of initial secret (nonsecret) states. The adversary is assumed to have knowledge of the initial sets of secret and nonsecret states, X_s and X_{ns}, the system model (A,B), and its own observation map C. Further, we assume that it has unlimited computing power, in that it will be able to compute the sets of reachable states at time k. Its goal is to deduce, on the basis of observing the system at times $k \in \mathscr{K}$, whether the system started from a state in X_s or not. We recall the definition of strong $k-$ISO from [14].

Definition 2.1: For system (1), given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathscr{K}$, X_s is **strongly $k-$ISO** with respect to X_{ns} if for all $x_s(0) \in X_s$ and for every sequence of admissible controls $u_s(0),\ldots,u_s(k)$, there exist an $x_{ns}(0) \in X_{ns}$, and a sequence of admissible controls $u_{ns}(0),\ldots,u_{ns}(k)$ such that $y_s(k) = y_{ns}(k)$.

X_s is **strongly $\mathscr{K}-$ISO** with respect to X_{ns} if it is strongly $k-$ISO for all $k \in \mathscr{K}$.

This means that starting from any secret state and applying any sequence of k admissible controls corresponding to the instants the adversary makes an observation, the system will reach a state that is indistinguishable from a state reached by the application of some admissible control sequence of length k, starting from some nonsecret state. A weaker notion of $k-$ISO has been defined in [14], but we will not need it in this paper.

That the adversary does not continuously observe the system in the above definition is motivated by the following reasons: first, it might not want to reveal its presence to the system, and second, it might not have the resources to continuously monitor the system. In this paper, the set $\mathscr{K}$ is arbitrary. Formulating observation strategies for the adversary is an interesting direction of future research.

Let $U_s^k := \{u_s(0),\ldots,u_s(k-1)\}$ and $U_{ns}^k := \{u_{ns}(0),\ldots,u_{ns}(k-1)\}$. Let $X_s(k)$ and $X_{ns}(k)$ denote the sets of reachable states in k steps,

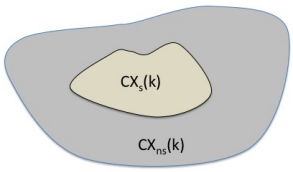

Fig. 1: Representation of strong $k-$ISO

starting from nonempty sets X_s and X_{ns} respectively. That is,

$$X_s(k) = \bigcup_{x_0 \in X_s} \bigcup_{U_s^k} \{x : x(i+1) = Ax(i) + Bu(i), \forall i < k\},$$
$$X_{ns}(k) = \bigcup_{x_0 \in X_{ns}} \bigcup_{U_{ns}^k} \{x : x(i+1) = Ax(i) + Bu(i), \forall i < k\}.$$

Theorem 2.2: The following hold:

1) X_s is strongly $k-$ISO with respect to X_{ns} if and only if $CX_s(k) \subseteq CX_{ns}(k)$.
2) X_s is strongly $\mathcal{K}-$ISO with respect to X_{ns} if and only if $CX_s(k) \subseteq CX_{ns}(k)$ for all $k \in \mathcal{K}$.

Proof: The proof can be found in [14]. Figure 1 illustrates strong $k-$ISO in terms of these sets of states. ■

The above result indicates that it suffices for the adversary to check membership of the output at time k in the sets $CX_s(k)$ and $CX_{ns}(k)$ to determine opacity of the set of secret states.

III. Decentralized Opacity for Linear Systems

In this section, we define several notions of decentralized opacity in the presence of multiple adversaries. The presence or absence of collusion among the adversaries, and the presence or absence of a coordinator that aggregates information based on the adversaries' observations, is the distinguishing feature, and a definition of decentralized opacity is proposed in each case. The system model is identical to (1) except that there are multiple adversaries, each seeing an output corresponding to its observation map C_i. As in the single adversary case, every adversary is assumed to have knowledge of the initial sets of secret and nonsecret states, X_s and X_{ns}, the system model (A,B), and its own observation map C_i, and is assumed to have unlimited computing power.

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ x(0) &= x_0 \in X_0 \\ y_i(t) &= C_i x(t);\ i = 1,2,\ldots,l \end{aligned} \tag{2}$$

where $x \in \mathbb{R}^n, u \in \mathbb{R}^m, y_i \in \mathbb{R}^{p_i}$, and A, B, C_i are matrices of appropriate dimensions containing real entries. Throughout the paper, we will assume that all of the adversaries observe the system at the same time instants in the set $\mathcal{K}$.

A. No Coordinator, No Collusion

In this case, the agents do not communicate with each other, and there is no coordinator. Opacity of the secret is achieved when it is simultaneously opaque with respect to every adversary.

Definition 3.1: For system (2), given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathcal{K}$, X_s is **strongly decentralized $k-$ISO** with respect to X_{ns} if for all $x_s(0) \in X_s$ and for every sequence of admissible controls $u_s(0),\ldots,u_s(k)$, there exist an $x_{ns}(0) \in X_{ns}$, and a sequence of admissible controls $u_{ns}(0),\ldots,u_{ns}(k)$ such that $y_{s_i}(k) = y_{ns_i}(k)$ for all $i \in \{1,2,\ldots,l\}$.

X_s is **strongly decentralized $\mathcal{K}-$ISO** with respect to X_{ns} if it is strongly decentralized $k-$ISO for all $k \in \mathcal{K}$.

As in the single adversary case, we have a necesary and sufficient condition for for decentralized opacity in terms of sets of reachable states in k steps.

Theorem 3.2: The following hold:

1) X_s is strongly decentralized $k-$ISO with respect to X_{ns} if and only if $C_i X_s(k) \subseteq C_i X_{ns}(k)$ for all $i \in \{1,2,\ldots,l\}$.
2) X_s is strongly decentralized $\mathcal{K}-$ISO with respect to X_{ns} if and only if $C_i X_s(k) \subseteq C_i X_{ns}(k)$ for all $k \in \mathcal{K}$, and for all $i \in \{1,2,\ldots,l\}$.

Proof: The proof follows from extending the proof of Theorem 2.2 to multiple adversaries with observation maps $C_1,\ldots,C_l$. ■

The following result explores the relationship between decentralized $k-$ISO for a set of adversaries and $k-$ISO for a single adversary with an aggregated observation map.

Proposition 3.3: X_s is strongly decentralized $k-$ISO with respect to X_{ns} and adversaries with observation maps $C_1,\ldots,C_l$ if X_s is strongly $k-$ISO with respect to X_{ns} for the single adversary with the aggregated observation map $\bar{C} := \begin{pmatrix} C_1^T & C_2^T & \ldots & C_l^T \end{pmatrix}^T$.

Proof: X_s strongly $k-$ISO with respect to X_{ns} is equivalent to $\bar{C}X_s(k) \subseteq \bar{C}X_{ns}(k)$. This means that for every $x_s(k) \in X_s(k)$, there exists an $x_{ns}(k) \in X_{ns}(k)$ such that $C_1x_s(k) = C_1x_{ns}(k)$, $\ldots$, $C_lx_s(k) = C_lx_{ns}(k)$. Thus, we have $C_iX_s(k) \subseteq C_iX_{ns}(k)$ for all $i \in \{1,\ldots,l\}$, which is equivalent to X_s being strongly decentralized $k-$ISO with respect to X_{ns}. ■

It is to be noted that strong decentralized $k-$ISO need not necessarily ensure strong $k-$ISO with respect to an adversary with the aggregated observation map since, the nonsecret states in $X_{ns}(k)$ and the corresponding control sequence for each adversary may be different.

B. With Coordinator, No Collusion

Here, we assume that there is a coordinator, whose role is to poll the observations of each adversary, and decide on *co-opacity* according to some (predefined) rule. The coordinator does not have knowledge of the system model or the adversaries' observation maps. In fact, our model is such that the coordinator cannot do any better even if it knows the system model or the observation maps. It can be viewed as an agent whose role is to ensure that the whole is greater than the sum of its parts.

Formally, the coordinator communicates to the adversaries the time instants $\mathcal{K}$, at which the system needs to be observed. At each $k \in \mathcal{K}$, agent i observes $y_i(k) = C_ix(k)$. The agents communicate $\phi_i(y_i(k))$ to the coordinator, where $\phi_i : \mathbb{R}^{p_i} \to 2^{\mathbb{R}^n \times \mathbb{R}^n}$, and $\phi_i(y_i(k)) := \{(x^1,x^2) \in X_s(k) \times X_{ns}(k) : C_ix^1 = C_ix^2 = y_i(k)\}$ at time k. Let $\phi(CX(k)) := \bigcup\{\phi(y(k)) : [y(k) =$

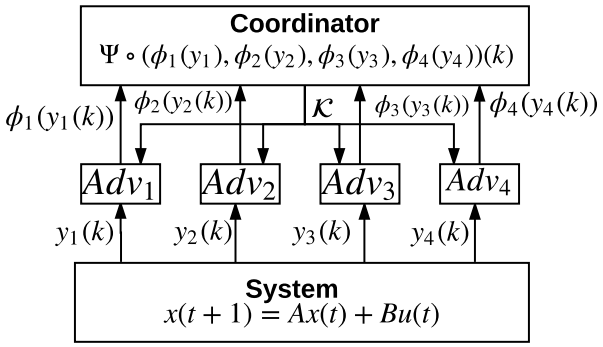

Fig. 2: Coordinated Decentralized Opacity

Thus, $\phi_i(\cdot)$ returns secret-nonsecret state pairs that give the same output $y_i(k)$ at time k.

The coordinator then computes a function $\Psi(k) := \Psi(\phi_1(y_1(k)),\ldots,\phi_l(y_l(k)))$, where $\Psi : (2^{\mathbb{R}^n \times \mathbb{R}^n})^l \to 2^{\mathbb{R}^n \times \mathbb{R}^n}$. Thus, the coordinator plays the role of gathering the outputs of the observations of each adversary, and composing them to then decide on opacity. An example of a valid coordinator function is $\Psi(k) = \bigcup_i(\phi_i(C_ix(k)))$.

The scheme is shown in figure 2 for the case of four adversaries.

Definition 3.4: For system (2), given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathcal{K}$, X_s is **strongly co-$k-$ISO** with respect to X_{ns} and Ψ if for all $x_s(0) \in X_s$ and for every sequence of admissible controls $u_s(0),\ldots,u_s(k)$, there exist an $x_{ns}(0) \in X_{ns}$, and a sequence of admissible controls $u_{ns}(0),\ldots,u_{ns}(k)$ such that $\Psi(k)$ is nonempty.

X_s is **strongly co-$\mathcal{K}-$ISO** with respect to X_{ns} and Ψ if it is strongly co-$k-$ISO for all $k \in \mathcal{K}$.

Before presenting the main result of this section, we provide an alternative characterization of strong $k-$ISO in terms of the map ϕ (the subscript on ϕ_i is dropped since we consider only a single adversary in this case). Further, it is important to note that the functions ϕ_i and Ψ return a set of pairs of states at time k. This information needs to be used to determine opacity of the initial set of secret states with respect to the initial set of nonsecret states.

We extend the definition of ϕ to sets of outputs

$Cx(k)] \wedge [x(k) \in X(k)]\}$. For $(x_i^1, x_j^2) \in X_s(k) \times X_{ns}(k)$, in a slight abuse of notation, we treat each x_i^1 and x_j^2 as a set. This will allow us to define $\bigcup_{i,j}(x_i^1, x_j^2) := (\bigcup_i x_i^1, \bigcup_j x_j^2)$, where $\bigcup_i x_i^1 \subseteq X_s(k)$, and $\bigcup_j x_j^2 \subseteq X_{ns}(k)$.

Proposition 3.5: X_s is strongly $k-$ISO with respect to X_{ns} if and only if $\phi(CX_s(k)) = (X_s(k), X'_{ns}(k))$, where $X'_{ns}(k) := \{x \in X_{ns}(k) : Cx \in CX_s(k)\}$.

Proof: Let strong $k-$ISO hold. Then, $CX_s(k) \subseteq CX_{ns}(k)$ (Theorem 2.2), and $\phi(CX_s(k)) = (X_s(k), X'_{ns}(k))$, where $X'_{ns}(k)$ is as defined above.

If $\phi(CX_s(k)) = (X_s(k), X'_{ns}(k))$, then $\forall x^1 \in X_s(k)$, $\exists x^2 \in X'_{ns}(k) \subseteq X_{ns}(k)$ such that $Cx^1(k) = Cx^2(k)$. This gives $CX_s(k) \subseteq CX_{ns}(k)$, which implies strong $k-$ISO (Theorem 2.2). ■

The above result says that strong $k-$ISO holds if and only if the first component of $\phi(\cdot)$ when acting on the set of secret outputs at time k is the entire set of reachable states at time k, starting from X_s. Further, it also determines the states in $X_{ns}(k)$ that ensure strong $k-$ISO.

Theorem 3.6: X_s is strongly co-$k-$ISO with respect to X_{ns} and Ψ if and only if $\Psi(\phi_1(C_1X_s(k)), \ldots, \phi_l(C_lX_s(k))) = (X_s(k), X'_{ns}(k))$, where $X'_{ns}(k) \subseteq X_{ns}(k)$.

Proof: The proof of this result follows from the previous result, and the definition of co$-k-$ISO. The major difference is that in this case, the first component of $\phi_i(C_iX_s(k))$ can be a subset of $X_s(k)$. However, the coordinator function Ψ must be such that its first component is $X_s(k)$. ■

Thus, X_s can be strongly co$-k-$ISO with respect to X_{ns} though strong $k-$ISO might not hold for any single adversary.

C. No Coordinator, With Collusion

In this case, there is no coordinator, but the adversaries are assumed to communicate among themselves. This is a new approach, and has not been studied for DESs. The communication structure is represented by a directed graph $\mathcal{G}$, whose vertices are the adversaries, and $\mathcal{G}$ has an edge directed from i to j if adversary j can receive information from adversary i. The goal of the adversaries is to ensure, using the coordination structure, that X_s is not $k-$ISO with respect to X_{ns} for each of them. To this end, we introduce the following definitions:

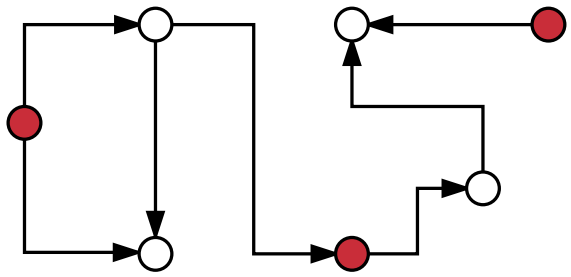

Fig. 3: Vertices in red form a directed dominating set

Definition 3.7: For the system (2), given $X_s, X_{ns} \subseteq X_0$ and $k \in \mathcal{K}$, X_s is **strongly not $k-$ISO** with respect to X_{ns} if X_s is not strongly $k-$ISO with respect to X_{ns} for every adversary.

Definition 3.8: Given a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ are the vertices of the graph and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ are edges, $D \subset \mathcal{V}$ is a **dominating set** if every vertex not in D has a neighbor in D.

Given a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, $D \subset \mathcal{V}$ is a **directed dominating set**(red vertices in figure (3)) if every vertex not in D has an incoming edge from some vertex in D, that is, $[\forall u \in \mathcal{V} \setminus D$, $\exists v \in D$ such that $(v \to u) \in \mathcal{E}]$.

At each $k \in \mathcal{K}$, each adversary observes $y(k)$, determines if $k-$ISO holds or not, and communicates $(C_i, <k-\text{ISO status}>_i)$ to its neighbors in $\mathcal{G}$. If $<k-\text{ISO status}>_i = 0$, i.e. $k-$ISO does not hold for adversary i, then a neighbor j of i in $\mathcal{G}$ adopts C_i as its observation map if $<k-\text{ISO status}>_j \neq 0$. This scheme can be interpreted as a dynamic version of $k-$ISO, in which the adversaries change their observation maps at times $k \in \mathcal{K}$ depending on the $k-$ISO status of their neighbors in $\mathcal{G}$. A key assumption here is that the time required for the adversaries to communicate amongst themselves is much less than the time scale of the system. The following result provides a means to achieve strong non-opacity without requiring non-opacity with

respect to every adversary using the communication scheme described above.

Theorem 3.9: For the system (2), X_s is strongly not $k-$ISO with respect to X_{ns} if the set of adversaries for which X_s is not strongly $k-$ISO with respect to X_{ns} is a directed dominating set of $\mathcal{G}$.

Proof: Each adversary communicates (C_i,< $k-$ISO status>$_i$) to its neighbors in $\mathcal{G}$. Thus, if $k-$ISO does not hold for some adversary i, then its neighbors will also adopt the same C_i matrix at time k. The result then follows from the definition of a directed dominating set. ■

IV. $\epsilon-$Opacity

The condition that the output at times $k \in \mathcal{K}$ starting from every state in X_s be equal to the output obtained by starting from some state in X_{ns} is quite strong. In this section, we postulate that (a form of) opacity will still hold if the outputs differ by a predefined amount. We only consider the single adversary case; the material can be easily extended to the decentralized notions of opacity in Sections (III-A) and (III-C). Defining $\epsilon-$opacity for the case in Section (III-B) will require more careful consideration.

Definition 4.1: For system (1), given $X_s, X_{ns} \subseteq X_0$, $k \in \mathcal{K}$, and $\epsilon \geq 0$, X_s is **strongly $\epsilon-k-$ISO** with respect to X_{ns} if for all $x_s(0) \in X_s$ and for every sequence of admissible controls $u_s(0),\ldots,u_s(k)$, there exist an $x_{ns}(0) \in X_{ns}$, and a sequence of admissible controls $u_{ns}(0),\ldots,u_{ns}(k)$ such that $\|y_s(k) - y_{ns}(k)\|_2 \leq \epsilon$.

X_s is **strongly $\epsilon - \mathcal{K} -$ISO** with respect to X_{ns} if it is strongly $\epsilon-k-$ISO for all $k \in \mathcal{K}$.

A couple of remarks are in order before we present the main result of this section. Notice that $\epsilon = 0$ corresponds to the definition of strong $k-$ISO seen earlier. Moreover, we can derive conditions that establish $\epsilon-$opacity in terms of sets of reachable states.

Let z be a point, and S be a set. Then, the distance of z from S is defined as $dist(z,S) := inf\{dist(z,s) | s \in S\}$.

Theorem 4.2: The following hold:

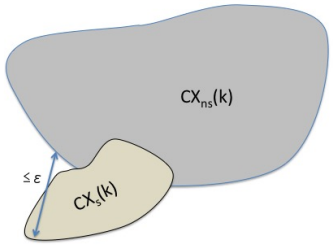

Fig. 4: Representation of $\epsilon-k-$ISO

1) X_s is strongly $\epsilon-k-$ISO with respect to X_{ns} if and only if :

$$\max_{z \in CX_s(k)} dist(z, CX_{ns}(k)) \leq \epsilon \qquad (3)$$

That is, the farthest a point in $CX_s(k)$ can be from $CX_{ns}(k)$ is ϵ.

2) X_s is strongly $\epsilon - \mathcal{K} -$ISO with respect to X_{ns} if and only if (3) holds for all $k \in \mathcal{K}$.

Proof: The proof of this result is similar to Theorem 2.2. Figure 4 illustrates $\epsilon-k-$ISO in terms of sets of reachable states at time k. ■

V. Conclusion

We defined notions of decentralized opacity for linear systems and considered scenarios in the presence and the absence of a centralized coordinator. The case when the adversaries could possibly communicate among each other was also studied. We also defined a weaker notion of opacity, where the condition that the outputs at time k be equal was relaxed.

We propose to extend this study by formulating a theory of opacity for nonlinear systems, and further, to switched systems and networked systems. We also intend to investigate a possible connection between $\epsilon-k-$ISO and the notion of differential privacy. It is our belief that this would enable the development of a comprehensive framework for opacity for general cyber-physical systems.

REFERENCES

[1] J. Slay and M. Miller, *Lessons learned from the Maroochy water breach*. Springer, 2008.

[2] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[3] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems.," in *HotSec*, 2008.

[4] L. Mazaré, "Using unification for opacity properties," *Proceedings of the 4th IFIP WG1*, vol. 7, 2004.

[5] E. Badouel *et al.*, "Concurrent secrets," *Discrete Event Dynamic Systems*, vol. 17, no. 4, pp. 425–446, 2007.

[6] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *46th IEEE Conference on Decision and Control*, 2007.

[7] J. Dubreil, P. Darondeau, and H. Marchand, "Supervisory control for opacity," *IEEE Trans. on Automatic Control*, vol. 55, no. 5, pp. 1089–1100, 2010.

[8] F. Cassez, J. Dubreil, and H. Marchand, "Synthesis of opaque systems with static and dynamic masks," *Formal Methods in System Design*, vol. 40, no. 1, pp. 88–115, 2012.

[9] A. Saboori and C. N. Hadjicostis, "Verification of initial-state opacity in security applications of DES," in *9th International Workshop on Discrete Event Systems*, pp. 328–333, IEEE, 2008.

[10] A. Saboori and C. N. Hadjicostis, "Verification of infinite-step opacity and complexity considerations," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1265–1269, 2012.

[11] Y.-C. Wu and S. Lafortune, "Comparative analysis of related notions of opacity in centralized and coordinated architectures," *Discrete Event Dynamic Systems*, vol. 23, no. 3, pp. 307–339, 2013.

[12] F. Lin, "Opacity of DES and its applications," *Automatica*, vol. 47, no. 3, pp. 496–503, 2011.

[13] A. Paoli and F. Lin, "Decentralized opacity of discrete event systems," in *American Control Conference (ACC), 2012*, pp. 6083–6088, IEEE, 2012.

[14] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus, "A framework for opacity in linear systems," *Proceedings of the American Control Conference*, 2016.