Opacity vs. Security in Linear Dynamical Systems

Varkey M. John, *Member, IEEE* and Vaibhav Katewa, *Member, IEEE*

***Abstract*— Opacity is a notion of privacy that is well-studied in computer science and discrete-event systems. It describes an eavesdropper's inability to infer a system's "secret" states by observing the system's outputs. In this paper, we consider opacity in linear dynamical systems and study four opacity classes - initial-state, current-state, K-step and infinite-step opacity, and show that they are fundamentally connected to two subspaces of the linear system - the weakly unobservable subspace and the weakly unconstructible subspace. With these subspaces, we derive conditions for opacity of secret states under constrained and unconstrained state and input sets. Further, we establish that a trade-off exists between opacity and security in the system. We show this in two ways – (i) we prove that an opaque system always permits undetectable attacks, (ii) we show that expanding the set of opaque states in the system expands the set of undetectable attacks. Our work provides the necessary mathematical foundation for system designers to build opaque systems, while ensuring adequate security.**

I. Introduction

PRIVACY breaches in Cyber-Physical Systems (CPS) have been used by malicious actors to inflict major damage to the system components as seen in real-world examples in the recent Stuxnet attack (2010) and the Ukraine power grid attack (2015), among others [1], [2]. To prevent such attacks, extensive research has been performed both on privacy and security.

On the privacy side, tools such as opacity, differential privacy, and homomorphic encryption were developed in recent years to keep the transmitted data private [3]. Opacity, in particular, was first introduced by the computer science community in the study of discrete event systems [4], [5]. This property has recently been applied in linear dynamical systems with continuous state space [6]–[9]. In essence, a system is said to be opaque if its secret states cannot be distinguished from its non-secret states with the knowledge of just the output sequences. Hence, opaque systems keep the secret states undisclosed to potential eavesdroppers. This prevents the eavesdropper from obtaining the state information and performing more focused attacks. For example, consider the application of a household smart grid system. The power utilization data (high vs. low) can reveal to an eavesdropper whether individuals are present in the household. With this information, the eavesdropper can plan the right time to rob the house by knowing when it is vacant. Other real-world applications, such as to keep web services private, also use opacity [10]. In the literature, mainly four types of opacity are considered - initial state, current state, K-step and infinite-step. All these types are important, as they ensure the privacy of secret states at different time instants.

On the security side, attack detection, prevention, and resilience have been the main focus areas of research [11]. Among these, real-time attack detection has been studied extensively [12]. Pure cyber-security solutions are ineffective against physics-based attacks, thereby necessitating such attack detection mechanisms. In these mechanisms, the detection is performed by comparing the system model's output estimate with the actual outputs using statistical tests such as CUSUM, chi-squared, etc. An attack is detected if the test measure crosses a given threshold set by the operator. Attack detection mechanisms have been developed for various domains such as power grid, remote aircraft system, etc. [13]. Though such attack detection mechanisms are useful, there may exists a set of attacks for a certain class of systems that cannot be detected by any attack detector. For improving security, it is essential that this set is minimized.

Though a large spectrum of results have emerged from independent studies on security and privacy, research on the impact of security on privacy, and vice-versa, is fairly limited. Since the attacker's goals, information availability, and mechanisms are different from that of the eavesdropper, at first thought it may seem that the security and privacy of a system are unrelated. In contrast, we demonstrate that a fundamental connection and trade-off exists between these two properties.

A. Literature Review

1) Opacity: Previous works have considered various frameworks and approaches to characterize opacity in CPS. In [6], the authors developed the notion of initial-state opacity for linear dynamical systems and established its relation to other system properties like output controllability. In contrast to [6], we consider in our work the definition of opacity that is more widely used in discrete event systems literature [5], [9], [14]. This definition has a broad spectrum of real-world applications, as shown in previous works [10], [15]. Also, while only sufficient conditions that connect system properties could be established for a single class of opacity in [6], in our work, we establish necessary and sufficient conditions for four classes of opacity (initial-state, current-state, K-step and infinite-step opacity). Further, we show in our work that exact verification of system opacity can be performed efficiently. This is, in general, not possible with the opacity definition in [6] that requires computation of reachable sets.

V. M. John is with the School of ECE at the Georgia Institute of Technology. V. Katewa is with the Robert Bosch Center for Cyber-Physical Systems and the Department of ECE at the Indian Institute of Science, Bangalore. Email IDs: {vjohn8@gatech.edu, vkatewa@iisc.ac.in} This work is supported in part by SERB grants SRG/2021/000292 and MTR/2022/000522, and the Cisco Center for Networked Intelligence at IISc.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3426549

A relaxed notion of "approximate opacity" was developed in [9], where the outputs from secret and non-secret initial states were allowed to be "close" to each other. Algorithms to enforce opacity for robust control and distributed state estimation in linear CPS are proposed in [7] and [8], respectively. In [15]–[17], algorithms for verification of opacity are developed. While these algorithms are useful in verifying opacity for a broad class of systems, they provide only sufficient conditions for verification. In contrast, in our work we propose necessary and sufficient conditions for opacity verification in linear systems. Further, the conditions in our work are simpler and more efficient than those in [15]–[17]. Particularly, in our work, opacity verification involves simple matrix manipulations which are much easier to both implement and compute than the approaches in [15]–[17] that require searching for and constructing control barrier functions.

In our work, we characterize opacity in linear dynamical systems using the general definitions of opacity (e.g. [5], [9], [14]). Further, we connect opacity with the system using the system's weakly unobservable and weakly unconstructible subspaces. These subspaces were developed in connection with the study of unknown input observability, constructibility, etc. [18]–[21]. In contrast to these studies, in our work we establish results specific to the notion of opacity, such as formulating the conditions for the existence of opaque states (for four notions of opacity), constructing the set of opaque states that a non-secret state makes opaque, developing the conditions required for the set of opaque states to expand when the system matrices are changed, etc. Further, different from previous works, we consider constraints on the state and input sets in our work.

2) Trade-off between Security and Privacy: Closely aligned to our work, the authors in [22] show that attack detection and differential privacy are linked to the system property called "input observability." In [23], the authors discuss how differential privacy mechanism can weaken system's security against integrity attacks. The trade-off between local mechanisms of security and privacy in interconnected dynamical systems is analyzed in [24]. The security-privacy trade-off has also been evaluated from an information-theoretic standpoint in [25], and the authors in [26] investigate the same using a game-theoretic approach with quantitative information flow theory. In contrast to these works which study noise-based privacy mechanisms (like differential privacy), we focus on a different notion of privacy in a noiseless setting, namely, opacity.

A preliminary version of this work was published in [27], where we considered just the notion of initial-state opacity with the limiting assumption that the state and input sets are unconstrained. In this paper, we consider four common notions of opacity in the literature and connect them with different system properties, wherein we also consider the state and input sets to be constrained. Further, we show that all these notions of opacity have a trade-off with security in linear systems.

B. Main Contributions

To the best of our knowledge, ours is the first work to investigate opacity in such generality for linear dynamical systems, and also to establish the fundamental trade-off with attack detectability.

The main contributions of this paper are three-fold:
1. We characterize the fundamental relation between the four notions of opacity - initial-state, current-state, K-step and infinite-step - and the weakly unobservable and the weakly unconstructible subspaces of the linear dynamical system.
2. We use the above subspaces to derive conditions for opacity of secret states for the case when the state and input sets are constrained and for the case when they are unconstrained. Further, we formulate largest possible opaque set in a system and characterize conditions under which the opaque sets expand with change of system matrices.
3. We show that there exists a trade-off between opacity and attack detectability. Specifically, if an opaque system is subjected to attacks, all attacks cannot be detected. Further, we show that expanding the opaque set also expands the set of undetectable attacks under certain conditions.

The results are discussed in a running example. We illustrate the practical application on a smart grid system.

C. Notation

We use the following notations in the paper (A, B are matrices, $\mathcal{S}, \mathcal{S}_1, \mathcal{S}_2$ are sets and $\mathcal{V}$ is a vector space):

Range(A)	:	Range space
Null(A)	:	Null space
$A \otimes B$	:	Kronecker product
A^T	:	Transpose
rank(A)	:	Rank
I_m	:	Identity matrix of size $m \times m$
$A\mathcal{S}$	:	$\{As : s \in \mathcal{S}\}$
$\mathcal{S}_1 \oplus \mathcal{S}_2$	:	Minkowski sum of sets $\mathcal{S}_1$ and $\mathcal{S}_2$
$\mathcal{S}_1 \backslash \mathcal{S}_2$	:	Set difference
$\lvert\mathcal{S}\rvert$	:	Cardinality of set $\mathcal{S}$
ϕ	:	Empty set
$\mathcal{V}^\perp$	:	Orthogonal complement of space $\mathcal{V}$
$\mathbb{C}$	:	Set of complex numbers
$\mathbb{R}$	:	Set of real numbers
$\mathbb{Z}$	:	Set of integers

II. System and Opacity Models

A. System Model

We consider a discrete-time linear time-invariant system (denoted by Γ):

$$\Gamma: \quad \begin{aligned} x(k+1) &= Ax(k) + Bu(k), \\ y(k) &= Cx(k) + Du(k), \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n, y \in \mathbb{R}^m, u \in \mathbb{R}^p, k \in \mathbb{Z}$ represent the state, output, normal input and time instant, respectively. Let $\mathcal{X}(0)$ denote the set of initial states in which the system is allowed to begin. Let $U(k) = \begin{bmatrix} u(0)^T & u(1)^T & \cdots & u(k)^T \end{bmatrix}^T$ denote the input sequence (represented as a vector) until time instant k, and let the vector $U(k_1, k_2) = \begin{bmatrix} u(k_1)^T & u(k_1+1)^T & \cdots & u(k_2)^T \end{bmatrix}^T$ denote the subsequence of the input sequence $U(k)$ from k_1 to k_2 (where $k \geq k_2 \geq k_1$). Further, for the input sequence $U(k)$, we define a truncation operator T_{k_0} as:

$$T_{k_0}[U(k)] = \begin{bmatrix} u(0)^T & u(1)^T & \cdots & u(k_0)^T \end{bmatrix}^T,$$

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3426549

that truncates $U(k)$ at $k_0 \leq k$. The input sequence $U(k)$ belongs to the set of input sequences $\mathcal{U}(k)$.

The state $x(k)$ for a system starting at initial state $x(0) \in \mathcal{X}(0)$ with the input sequence $U(k-1)$ is denoted by

$$x(k) \triangleq x_{x(0),U(k-1)} = A^k x(0) + N_k^\Gamma U(k-1), \tag{2}$$

where N_k^Γ is the extended controllability matrix given by:

$$N_k^\Gamma = \begin{bmatrix} A^{k-1}B & A^{k-2}B & \cdots & B \end{bmatrix} \qquad \text{for } k \geq 1, \tag{3}$$

and $N_0^\Gamma = 0$. Let $\mathcal{X}(k)$ denote the set of states that are reachable at time k, that is,

$$\mathcal{X}(k) = \left\{ x_{x(0),U(k-1)} : x(0) \in \mathcal{X}(0), U(k-1) \in \mathcal{U}(k-1) \right\}.$$

Further, let $Y_{x(0),U(k)}$ denote the output sequence (vector) produced by applying the input sequence $U(k)$ to an initial state $x(0) \in \mathcal{X}(0)$. The output sequence can be written as:

$$Y_{x(0),U(k)} = O_k x(0) + F_k^\Gamma U(k), \tag{4}$$

where O_k and F_k^Γ are extended observability and forced response matrices, respectively, and are given by:

$$O_k = \begin{bmatrix} C^T & (CA)^T & \cdots & (CA^k)^T \end{bmatrix}^T \qquad \text{for } k \geq 0, \tag{5}$$

$$F_k^\Gamma = \begin{bmatrix} D & 0 & \cdots & 0 \\ CB & D & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{k-1}B & CA^{k-2}B & \cdots & D \end{bmatrix} \qquad \text{for } k \geq 1, \tag{6}$$

and $F_0^\Gamma = D$.

B. Opacity Model

We consider that there exists a set of secret states at time instant k, denoted by $\mathcal{X}_{s,k}$ ($\mathcal{X}_{s,k} \subseteq \mathcal{X}(k)$), that a system operator wishes to keep private from external entities. The remaining set of non-secret states is denoted by $\mathcal{X}_{ns,k} \triangleq \mathcal{X}(k) \backslash \mathcal{X}_{s,k}$. Any element of $\mathcal{X}_{ns,k}$ is not considered sensitive to disclosure. We use $x_{s,k}$ and $x_{ns,k}$ to denote individual elements in $\mathcal{X}_{s,k}$ and $\mathcal{X}_{ns,k}$, respectively.

We consider a potential eavesdropper present in the system whose goal is to use the outputs to determine whether the system's state at a particular time instant (present or past) is in the corresponding secret set or non-secret set.

Assumption 1. *We assume that the eavesdropper knows the system matrices A, B, C, D, and the sets $\mathcal{X}_{s,k}$ and $\mathcal{X}_{ns,k}$. Further, it has access to the system outputs $y(k)$ but not the inputs $u(k)$.*

Next, we provide opacity definitions corresponding to System Γ in (1). Let the set of output sequences for which the system reaches the particular secret state $x_{s,k} \in \mathcal{X}_{s,k}$ at time instant k, with initial states $x(0) \in \mathcal{X}(0)$ and corresponding $l \geq k$ length input sequences $U_s(l) \in \mathcal{U}_s(l)$, be denoted by

$$\mathcal{Y}^l_{x_{s,k}} = \Big\{ Y_{x(0),U_s(l)} : x_{x(0),T_{k-1}[U_s(l)]} = x_{s,k}, \\ x(0) \in \mathcal{X}(0), U_s(l) \in \mathcal{U}_s(l) \Big\}. \tag{7}$$

The above equation implies that any element in the set $\mathcal{Y}^l_{x_{s,k}}$ is an output sequence of length $l (\geq k)$ which results from a state trajectory whose value at time instant k is $x_{s,k}$. Similarly, let the set of output sequences for which the system reaches *any* non-secret state $x_{ns,k}$ that belongs to set $\mathcal{X}'_{ns,k} \subseteq \mathcal{X}_{ns,k}$ at time instant k, with initial states $x(0) \in \mathcal{X}(0)$ and corresponding $l \geq k$ length input sequences $U_{ns}(l) \in \mathcal{U}_{ns}(l)$, be denoted by

$$\mathcal{Y}^l_{\mathcal{X}'_{ns,k}} = \Big\{ Y_{x(0),U_{ns}(l)} : x_{x(0),T_{k-1}[U_{ns}(l)]} \in \mathcal{X}'_{ns,k}, \\ x(0) \in \mathcal{X}(0), U_{ns}(l) \in \mathcal{U}_{ns}(l) \Big\}. \tag{8}$$

Assumption 2. *We assume that $\mathcal{U}_s(k) = \mathbb{R}^{(k+1)p}$ and $\mathcal{U}_{ns}(k) = \mathbb{R}^{(k+1)p}$ for all $k \geq 0$ unless specified otherwise.*

With these notations, we define different forms of opacity.

Definition 1 (*Opacity of State*)**.** Let $K \geq 0$ be an integer. A secret state $x_{s,k} \in \mathcal{X}_{s,k}$ is opaque with respect to a non-secret state set $\mathcal{X}'_{ns,k} \subseteq \mathcal{X}_{ns,k}$, if

$$\mathcal{Y}^{k+K}_{x_{s,k}} \subseteq \mathcal{Y}^{k+K}_{\mathcal{X}'_{ns,k}}.$$

For brevity, we sometimes use the terminology "$x_{s,k}$ is opaque" rather than "$x_{s,k}$ is opaque w.r.t $\mathcal{X}'_{ns,k}$". Based on different values of k and K, we categorize opacity as:
(i) Initial-State Opacity (ISO): $k = 0$, $K = \infty$, denoted as $x_{s,0} \xrightarrow{\text{iso}} \mathcal{X}'_{ns,0}$.
(ii) Current-State Opacity (CSO): $k \geq 0$, $K = 0$, denoted as $x_{s,k} \xrightarrow{\text{cso}} \mathcal{X}'_{ns,k}$.
(iii) K-Step Opacity (KSO): $k \geq 0$, $K \geq 0$, denoted as $x_{s,k} \xrightarrow{\text{kso}} \mathcal{X}'_{ns,k}$.
(iv) Infinite-Step Opacity (Inf-SO): $k \geq 0$, $K = \infty$, denoted as $x_{s,k} \xrightarrow{\text{inf-so}} \mathcal{X}'_{ns,k}$. □

Opacity Definition 1 implies that for every possible output sequence resulting from a secret state, there exists a proxy (equal) output sequence resulting from a non-secret state. Thus, under the scenario when the system indeed starts from, or is currently in, a secret state, the eavesdropper who observes an output sequence of a specific length cannot distinguish whether the system is in a secret or non-secret state at a particular time instant. This makes the secret state opaque.

Notice that the above notions of opacity differ in terms of the time instant at which the secret state should be opaque, and what data is available to the eavesdropper for inferring opacity. In initial-state opacity, the secrecy of initial state $x(0)$ is preserved given an output sequence of any arbitrary length. In other opacity notions, the secrecy of state $x(k)$ is preserved and the corresponding output sequence is of length:
(i) k for current-state opacity,
(ii) $k + K$ ($K \geq 0$) for K-step opacity,
(iii) ∞ (equivalently, any arbitrary length) for infinite-step opacity.

It is required to study these four notions since each notion applies to a different scenario, based on the eavesdropper's resources and intentions. For instance, a system may be current-state opaque but not initial-state opaque, and the eavesdropper may want to get inference about the system's initial secret state, and not its current secret state.

From the definitions, we have that infinite-step opacity implies K-step opacity, which in turn implies current-state opacity. Also, K-step opacity reduces to current-state opacity for $K = 0$, and to infinite-step opacity for $K = \infty$. Further, infinite-step opacity of initial state $x_{s,0}$ is equivalent to its

initial-state opacity. This shows that K-step opacity is the most general notion and all other opacity notions can be derived from it. All these opacity notions are illustrated in Figure 1.

Remark 1. The ISO definition in Definition 1 differs from the definition of $\mathcal{K}$-ISO used in [6], as explained next. Let $y_{x(0),U(k)}$ denote the output of system Γ at time instant k with initial state $x(0)$ and input sequence $U(k)$. In [6], opacity of secret state $x_{s,0}$ is achieved when at each $k \in \mathcal{K}$, there exists some non-secret initial state $x_{ns,0}$ (that can depend on k) such that $y_{x_{s,0},U_s(k)} = y_{x_{ns,0},U_{ns}(k)}$. Hence, in this case, $x_{ns,0}$ is *allowed to be different at different time instants*. However, in our Definition 1, $x_{ns,0}$ should be same across all time instants. We consider this definition since it is the widely accepted one in the discrete event systems literature [5], [9], [14]. □

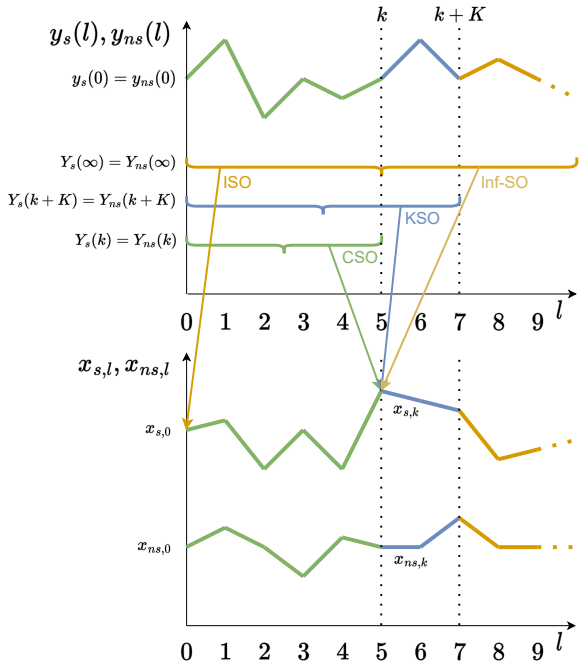

Fig. 1: Pictorial representation of different forms of opacity. The bottom graph represents the system's state trajectory resulting from some input sequences of lengths k (green), $k+K$ (blue) ($k = 5, K = 2$ here) and ∞ (orange), with secret states $x_{s,0}$ and $x_{s,k}$, and non-secret states $x_{ns,0}$ and $x_{ns,k}$. The top graph represents the corresponding outputs $(y_s(l), y_{ns}(l))$. As shown, the output trajectories are equal ($Y_s(l) = Y_{ns}(l)$). Therefore, by observing just the outputs, one cannot determine $x_{s,0}$ (when ISO with $l = \infty$ is considered), and $x_{s,k}$ (when CSO, KSO and Inf-SO with $l = k, k+K$ and ∞, respectively are considered) (as denoted by the arrows).

Definition 1 defines opacity of a secret *state*. Next, we generalize it to opacity of a secret *set*.

Definition 2 (*Opacity of Set*)**.** A secret state set $\mathcal{X}_{s,k}$ is opaque with respect to non-secret state set $\mathcal{X}'_{ns,k} \subseteq \mathcal{X}_{ns,k}$, if, for every $x_{s,k} \in \mathcal{X}_{s,k}$, it holds that $x_{s,k}$ is opaque with respect to $\mathcal{X}'_{ns,k}$.

For brevity, we sometimes use the terminology "$\mathcal{X}_{s,k}$ is opaque" rather than "$\mathcal{X}_{s,k}$ is opaque w.r.t $\mathcal{X}'_{ns,k}$". We denote this relation by $\mathcal{X}_{s,k} \xrightarrow{\text{iso}} \mathcal{X}'_{ns,k}$ (resp. cso, kso, inf-so) for initial-state (resp. current-state, K-step, infinite-step) opacity. Further, we say that "$\mathcal{X}'_{ns,k}$ provides a proxy for $\mathcal{X}_{s,k}$" or "$\mathcal{X}'_{ns,k}$ makes $\mathcal{X}_{s,k}$ opaque". □

Next, we define opacity ordering of sets. This will be used later to analyze the trade-off between opacity and attack detectability.

Definition 3 (*Opacity Ordering*)**.** Given two opaque sets $\mathcal{X}^1_{s,k}$ and $\mathcal{X}^2_{s,k}$, $\mathcal{X}^1_{s,k}$ is *more opaque* than $\mathcal{X}^2_{s,k}$ if $\mathcal{X}^2_{s,k} \subset \mathcal{X}^1_{s,k}$. □

C. Subspaces for Opacity

In this subsection, we define certain fundamental subspaces of linear dynamical systems. We use these subspaces in the next section to develop necessary and sufficient conditions for the existence of opaque sets in the system.

Definition 4 (*Weakly Unobservable Subspace (WUOS)* [18])**.** The weakly unobservable subspace of system (1) (denoted by $\mathcal{V}(\Gamma)$) is defined as:

$$\begin{aligned}\mathcal{V}(\Gamma) = \{x \in \mathbb{R}^n : \exists\, U(k) \in \mathbb{R}^{(k+1)p} \text{ such that } \\ Y_{x,U(k)} = 0,\ \forall\, k \geq 0\} \\ = \{x \in \mathbb{R}^n : \exists\, U(n-1) \in \mathbb{R}^{np} \text{ such that } Y_{x,U(n-1)} = 0\},\end{aligned}$$

where the second equality is due to equation (5) in [18]. Further, similar subspaces for $k \geq 0$ steps are defined as:

$$\mathcal{V}_k(\Gamma) = \{x \in \mathbb{R}^n : \exists\, U(k) \text{ such that } Y_{x,U(k)} = 0\}. \quad \square$$

A property of $\mathcal{V}_k(\Gamma)$ is [18]:

$$\mathcal{V}_0(\Gamma) \supseteq \mathcal{V}_1(\Gamma) \supseteq \cdots \supseteq \mathcal{V}_{n-1}(\Gamma) = \mathcal{V}_n(\Gamma) = \cdots = \mathcal{V}(\Gamma). \quad (9)$$

For all $k \geq n-1$, we denote $\mathcal{V}_k(\Gamma)$ by $\mathcal{V}(\Gamma)$. The WUOS represents the set of initial states which result in the all-zero output sequence (for some inputs).

Definition 5 (*Weakly Unconstructible Subspace (WUCS)* [20])**.** The weakly unconstructible subspace of system (1) (denoted by $\mathcal{C}(\Gamma)$) is defined as:

$$\begin{aligned}\mathcal{C}(\Gamma) = \{x \in \mathbb{R}^n : \exists\, U(k) \in \mathbb{R}^{(k+1)p}, x' \in \mathbb{R}^n \text{ such that } \\ x_{x',T_{k-1}[U(k)]} = x, Y_{x',U(k)} = 0\ \forall\, k \geq 0\} \\ = \{x \in \mathbb{R}^n : \exists\, U(n) \in \mathbb{R}^{(n+1)p}, x' \in \mathbb{R}^n \text{ such that } \\ x_{x',T_{n-1}[U(n)]} = x, Y_{x',U(n)} = 0\},\end{aligned}$$

where the second equality follows from [18]. Further, similar subspaces for $k \geq 0$ steps are defined as:

$$\begin{aligned}\mathcal{C}_k(\Gamma) = \{x \in \mathbb{R}^n :\ \exists\, U(k) \in \mathbb{R}^{(k+1)p}, x' \in \mathbb{R}^n \text{ such that } \\ x_{x',T_{k-1}[U(k)]} = x, Y_{x',U(k)} = 0\}. \quad \square\end{aligned}$$

For $\mathcal{C}_k(\Gamma)$, we have that [21]:

$$\mathcal{C}_0(\Gamma) \supseteq \mathcal{C}_1(\Gamma) \supseteq \cdots \supseteq \mathcal{C}_n(\Gamma) = \mathcal{C}_{n+1}(\Gamma) = \cdots = \mathcal{C}(\Gamma).$$

For all $k \geq n$, we denote $\mathcal{C}_k(\Gamma)$ by $\mathcal{C}(\Gamma)$. The WUCS represents the set of states reachable in k time instants when the system starting at some state $x' \in \mathbb{R}^n$ outputs the all-zero output sequence (for some inputs).

In the following lemma, we state a necessary and sufficient condition for the WUCS to be trivial when the WUOS is trivial. This lemma's corollary is used in Section IV-B to show the trade-off between current-state opacity and attack detectability.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3426549

Lemma 1. *Let F_n^Γ and N_n^Γ be as defined in* (6) *and* (3)*, respectively. Also, let $\mathcal{V}(\Gamma) = \{0\}$. Then, $\mathcal{C}(\Gamma) = \{0\}$ if and only if Null$(F_n^\Gamma) \subseteq$ Null$(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$.*

Proof. $\mathcal{C}(\Gamma) = \{0\}$ if and only if for all pairs $(x(0), U(n))$ that satisfy $Y_{x(0),U(n)} = 0$, we have $x(n) = x_{x(0),T_{n-1}[U(n)]} = 0$. Since $\mathcal{V}(\Gamma) = \{0\}$, the only pairs that satisfy $Y_{x(0),U(n)} = 0$ are of the form $(0, U(n))$. Thus, $\mathcal{C}(\Gamma) = \{0\}$ if and only if

$$\begin{aligned} & x_{0,T_{n-1}[U(n)]} = 0 \quad \forall\, U(n) : Y_{0,U(n)} = 0 \\ \iff \quad & N_n^\Gamma T_{n-1}[U(n)] = 0 \quad \forall\, U(n) : F_n^\Gamma U(n) = 0 \\ \iff \quad & \begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix} U(n) = 0 \quad \forall\, U(n) \in \text{Null}(F_n^\Gamma) \\ \iff \quad & \text{Null}(F_n^\Gamma) \subseteq \text{Null}(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix}). \end{aligned}$$

Hence proved. □

Corollary 1. *Let $\mathcal{C}(\Gamma) \neq \{0\}$ and Null$(F_n^\Gamma) \subseteq$ Null$(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$. Then, $\mathcal{V}(\Gamma) \neq \{0\}$.*

Proof. Since $\mathcal{C}(\Gamma) \neq \{0\}$ and Null$(F_n^\Gamma) \subseteq$ Null$(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$, we have that

$$\begin{aligned} & x_n = x_{x(0),T_{n-1}[U_n]} \neq 0 \quad \forall\, U(n) : Y_{x(0),U(n)} = 0 \\ \iff \quad & A^n x(0) + \begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix} U(n) \neq 0 \quad \forall\, U(n) : Y_{x(0),U(n)} = 0 \end{aligned}$$

Assume $x(0) = 0$ is the only initial state that reaches x_n and produces the zero output sequence. Then,

$$\begin{aligned} & \begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix} U(n) \neq 0 \quad \forall\, U(n) : Y_{0,U(n)} = 0 \\ \implies \quad & \begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix} U(n) \neq 0 \quad \forall\, U(n) : F_n^\Gamma U(n) = 0 \\ \implies \quad & \text{Null}(F_n^\Gamma) \not\subseteq \text{Null}(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix}), \end{aligned}$$

which is a contradiction. Hence, it is required that $x(0) \neq 0$ for which the zero output sequence is generated until $k = n$, which implies that $\mathcal{V}(\Gamma) \neq \{0\}$. □

III. Characterization of Opaque Sets

In this section, we show that WUOS and WUCS are connected to the different notions of opacity. We first consider systems whose state and input sets are unconstrained in Subsection III-A. Subsequently, in Subsection III-B, we relax this requirement and consider opacity for systems with constrained state and input sets.

A. Connections between Opacity and System Subspaces

In this subsection, we begin by characterizing the condition for existence of opaque sets. We use the following assumption on state and input sequence sets.

Assumption 3. *In this subsection, we assume $\mathcal{X}(0) = \mathbb{R}^n$ and $\mathcal{U}(k) = \mathbb{R}^{(k+1)p} \;\; \forall\, k \geq 0$.*

The above assumption implies that the reachable set $\mathcal{X}(k)$ is a subspace of $\mathbb{R}^n$ for all $k \geq 0$. Also, for a given $k \geq 0$, the condition $\mathcal{X}(k) = \mathbb{R}^n$ holds if and only if the System Γ in (1) is reachable. Further, if $\mathcal{X}(k_0) = \mathbb{R}^n$ for some k_0, it holds that $\mathcal{X}(k) = \mathbb{R}^n$ for all $k \geq k_0$.

Lemma 2. *For System Γ in* (1)*:*
1. There exists a secret set that is ISO if and only if $\mathcal{V}(\Gamma) \neq \{0\}$.
2. For a specific $k \geq 0$, let $\mathcal{X}(k) = \mathbb{R}^n$. Then, there exists a secret set at time instant k that is
(i) CSO if and only if $\mathcal{C}_k(\Gamma) \neq \{0\}$,
(ii) KSO if and only if $\mathcal{C}_k(\Gamma) \cap \mathcal{V}_K(\Gamma) \neq \{0\}$,
(iii) Inf-SO if and only if $\mathcal{C}_k(\Gamma) \cap \mathcal{V}(\Gamma) \neq \{0\}$.

Proof. Since KSO generalizes ISO, CSO and Inf-SO, we first prove Statement 2(ii), and then generalize the proof for the other statements.

Proof of Statement 2(ii): For any $k \geq 0$, suppose there exists a set $\mathcal{X}_{s,k}$ which is KSO with respect to $\mathcal{X}_{ns,k} = \mathbb{R}^n \backslash \mathcal{X}_{s,k}$. From Definition 2, we note that existence of $\mathcal{X}_{s,k}$ is equivalent to existence of a distinct $x_{s,k}$ and $x_{ns,k}$ such that $x_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$. This is equivalent to saying that for any $x(0)$ and $U_s(k+K)$, there exist $x'(0)$ and $U_{ns}(k+K)$, such that

$$x_{x(0),T_{k-1}[U_s(k)]} = x_{s,k}, \tag{10}$$

$$x_{x'(0),T_{k-1}[U_{ns}(k)]} = x_{ns,k}, \tag{11}$$

$$Y_{x(0),U_s(k+K)} = Y_{x'(0),U_{ns}(k+K)} \tag{12}$$

We subtract (11) from (10) (using linearity) and we decompose (12) into two output sequences with time instants $\{0, 1, \cdots, k\}$ and $\{k, k+1, \cdots, k+K\}$, respectively:

$$\begin{aligned} x_{x(0)-x'(0),T_{k-1}[U_s(k+K)-U_{ns}(k+K)]} &= x_{s,k} - x_{ns,k}, \\ Y_{x(0)-x'(0),T_k[U_s(k+K)-U_{ns}(k+K)]} &= 0, \\ Y_{x_{s,k}-x_{ns,k},U_s(k,k+K)-U_{ns}(k,k+K)} &= 0. \end{aligned}$$

Let $x_1 \triangleq x(0) - x'(0)$, $x_2 \triangleq x_{s,k} - x_{ns,k}$, $U(k, k+K) \triangleq U_s(k, k+K) - U_{ns}(k, k+K)$ and $U(k+K) \triangleq U_s(k+K) - U_{ns}(k+K)$. Since $x_{s,k}$ and $x_{ns,k}$ are different, we have $x_2 \neq 0$. Thus, the above is equivalent to

$$\left.\begin{aligned} x_{x_1,T_{k-1}[U(k+K)]} &= x_2, \\ Y_{x_1,T_k[U(k+K)]} &= 0 \end{aligned}\right\} \overset{(a)}{\implies} x_2 \in \mathcal{C}_k(\Gamma),$$

$$\begin{aligned} Y_{x_2,U(k,k+K)} = 0 \quad & \overset{(b)}{\implies} x_2 \in \mathcal{V}_K(\Gamma) \\ \iff x_2 \in \mathcal{C}_k(\Gamma) \cap \mathcal{V}_K(\Gamma) \; & \neq \{0\}, \end{aligned}$$

where (a) and (b) follow from Definitions 4 and 5. Hence Statement 2(ii) is proved.

Statements 2(i) and 2(iii) follow from 2(ii) by choosing $K = 0$ and $K = \infty$, respectively. Consequently, $\mathcal{V}_K(\Gamma)$ becomes $\mathcal{V}_0(\Gamma)$ and $\mathcal{V}(\Gamma)$, respectively. Since $\mathcal{C}_k(\Gamma) \subseteq \mathcal{C}_0(\Gamma)$, and by WUOS and WUCS definitions we have $\mathcal{C}_0(\Gamma) = \mathcal{V}_0(\Gamma)$, it holds that $\mathcal{C}_k(\Gamma) \cap \mathcal{V}_0(\Gamma) = \mathcal{C}_k(\Gamma)$.

Statement 1 is proven as follows:

$$\begin{aligned} & \exists \text{ ISO } \mathcal{X}_{s,0} \\ \iff \quad & \exists \text{ Inf-SO } \mathcal{X}_{s,0} \\ \iff \quad & \mathcal{C}_0(\Gamma) \cap \mathcal{V}(\Gamma) \neq \{0\} \\ \iff \quad & \mathcal{V}_0(\Gamma) \cap \mathcal{V}(\Gamma) \neq \{0\} \\ \iff \quad & \mathcal{V}(\Gamma) \neq \{0\}, \end{aligned}$$

where the last equivalence follows from (9). □

Lemma 2 highlights a fundamental connection between opacity and the subspaces WUOS and WUCS for linear systems, and shows that a corresponding non-trivial subspace is essential for the existence of opaque sets. Next, for systems which admit opaque sets, we characterize conditions for a given set to be opaque. We begin by providing opacity conditions for individual initial states. In the following, we will focus only on K-step opacity, since the results for

other opacity notions can be obtained from it with minor modifications. For better readability, we use the notation

$$\mathcal{T}_{k,K}(\Gamma) \triangleq \big(\mathcal{C}_k(\Gamma) \cap \mathcal{V}_K(\Gamma)\big). \tag{13}$$

Lemma 3. *Let $\mathcal{X}(k) = \mathbb{R}^n$. Given two different states $x_{s,k} \in \mathcal{X}_{s,k}$ and $x_{ns,k} \in \mathcal{X}_{ns,k}$, we have $x_{s,k} \xrightarrow{kso} \{x_{ns,k}\}$ if and only if $x_{s,k} - x_{ns,k} \in \mathcal{T}_{k,K}(\Gamma)$.*

Proof. Refer to the proof of Lemma 2. □

Corollary 2. *Let $\mathcal{X}(k) = \mathbb{R}^n$. The following two statements hold true:*
1. Given $x_{s,k}$, a state $x_{ns,k} \neq x_{s,k}$ satisfies $x_{s,k} \xrightarrow{kso} \{x_{ns,k}\}$ if and only if $x_{ns,k} \in x_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)$.
2. Given $x_{ns,k}$, a state $x_{s,k} \neq x_{ns,k}$ satisfies $x_{s,k} \xrightarrow{kso} \{x_{ns,k}\}$ if and only if $x_{s,k} \in x_{ns,k} \oplus \mathcal{T}_{k,K}(\Gamma)$.

Lemma 3 provides the necessary and sufficient condition to check the K-step opacity of a secret state, and shows that it is fundamentally connected, and completely determined by $\mathcal{T}_{k,K}(\Gamma)$. Further, Corollary 2 shows that the set of non-secret states that makes a secret state opaque (and vice-versa) is constrained by $\mathcal{T}_{k,K}(\Gamma)$. Next, we extend these results to specify conditions for opacity of *sets* of states.

Lemma 4. *Let $\mathcal{X}(k) = \mathbb{R}^n$. Given non-empty and disjoint sets $\mathcal{X}_{s,k}$ and $\mathcal{X}_{ns,k}$, we have $\mathcal{X}_{s,k} \xrightarrow{kso} \mathcal{X}_{ns,k}$ if and only if $\mathcal{X}_{s,k} \subset \mathcal{X}_{ns,k} \oplus \mathcal{T}_{k,K}(\Gamma)$.*

Proof. If: The condition $\mathcal{X}_{s,k} \subset \mathcal{X}_{ns,k} \oplus \mathcal{T}_{k,K}(\Gamma)$ implies that for any $x_{s,k} \in \mathcal{X}_{s,k}$, there exists an $x_{ns,k} \in \mathcal{X}_{ns,k}$ satisfying:

$$\begin{aligned} & x_{s,k} \in x_{ns,k} \oplus \mathcal{T}_{k,K}(\Gamma) \\ \iff \quad & x_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\} \quad \text{(by Corollary 2).} \end{aligned}$$

Since the above statement holds true for any $x_{s,k} \in \mathcal{X}_{s,k}$, we have $\mathcal{X}_{s,k} \xrightarrow{\text{kso}} \mathcal{X}_{ns,k}$.

Only if: We prove this part via contradiction. We show that the condition $\mathcal{X}_{s,k} \supseteq \mathcal{X}_{ns,k} \oplus \mathcal{T}_{k,K}(\Gamma)$ implies that the sets $\mathcal{X}_{s,k}$ and $\mathcal{X}_{ns,k}$ cannot be disjoint. Splitting $\mathcal{T}_{k,K}(\Gamma)$, we get:

$$\begin{aligned} & \mathcal{X}_{s,k} \supseteq \mathcal{X}_{ns,k} \oplus \Big(\{0\} \cup \Big(\mathcal{T}_{k,K}(\Gamma) \backslash \{0\}\Big)\Big) \\ \overset{\text{(a)}}{\implies} \quad & \mathcal{X}_{s,k} \supseteq \big(\mathcal{X}_{ns,k} \oplus \{0\}\big) \cup \Big(\mathcal{X}_{ns,k} \oplus \Big(\mathcal{T}_{k,K}(\Gamma) \backslash \{0\}\Big)\Big) \\ \implies \quad & \mathcal{X}_{s,k} \supseteq \big(\mathcal{X}_{ns,k} \oplus \{0\}\big) = \mathcal{X}_{ns,k} \\ \implies \quad & \mathcal{X}_{s,k} \cap \mathcal{X}_{ns,k} \neq \phi, \end{aligned}$$

where (a) follows from the fact that Minkowski sum is distributive over union of sets. □

For better clarity on Lemma 4, refer to Example 1 given later which provides a pictorial representation of the result. Same as before, the conditions in Lemma 4 are completely dependent on $\mathcal{T}_{k,K}(\Gamma)$.

Remark 2. Note that Lemma 3, Corollary 2 and Lemma 4 hold even when $\mathcal{X}(k) \subseteq \mathbb{R}^n$. Further, Lemma 4 also holds for an arbitrary non-secret set $\mathcal{X}'_{ns,k} \subseteq \mathcal{X}_{ns,k}$. □

Next, we analyze the largest possible opaque set for the system. Determining this largest set is important because it provides a fundamental limit beyond which a larger opaque set cannot be constructed. To this aim, we consider solving the following problem:

$$\begin{aligned} & \text{Find } \mathcal{X}_{s,k} \; s.t. \\ & (i)\; \mathcal{X}_{s,k} \xrightarrow{\text{kso}} \mathcal{X}(k) \backslash \mathcal{X}_{s,k} \text{ and} \\ & (ii)\; \nexists \mathcal{X}'_{s,k} \; s.t. \\ & \quad a.\; \mathcal{X}'_{s,k} \xrightarrow{\text{kso}} \mathcal{X}(k) \backslash \mathcal{X}'_{s,k} \text{ and} \\ & \quad b.\; \mathcal{X}'_{s,k} \supset \mathcal{X}_{s,k}. \end{aligned} \tag{14}$$

In this problem, (i) ensures $\mathcal{X}_{s,k}$ is KSO and (ii) ensures $\mathcal{X}_{s,k}$ is the largest set. The next lemma provides a solution to the above optimization problem.

Lemma 5. *Let $\mathcal{T}_{k,K}(\Gamma)^{\perp}$ denote the orthogonal complement of $\mathcal{T}_{k,K}(\Gamma)$. Assume $\mathcal{X}(k) = \mathbb{R}^n$ for a given $k \geq 0$. One solution to (14) is $\mathcal{X}_{s,k} = \mathbb{R}^n \backslash \mathcal{T}_{k,K}(\Gamma)^{\perp}$.*

Proof. Refer to the proof in Appendix VI-A. □

Note that the solution in Lemma 5 is not unique. For instance, for any particular $x(k) \in \mathbb{R}^n$, the set $\mathcal{X}_{s,k} = \mathbb{R}^n \backslash \big(x(k) \oplus (\mathcal{T}_{k,K}(\Gamma)^{\perp})\big)$ also solves (14).

Lemma 5 shows that the largest possible opaque set is constrained by $\mathcal{T}_{k,K}(\Gamma)$. Next, we show that when the system is changed, the expansion of opaque sets is also constrained by $\mathcal{T}_{k,K}(\Gamma)$.

Theorem 1. *Consider two systems Γ_1 and Γ_2, and let $\mathcal{X}(k) = \mathbb{R}^n$ for both systems for a given $k \geq 0$. For each KSO set in Γ_1, there exists a corresponding more KSO set in Γ_2 if and only if $\mathcal{T}_{k,K}(\Gamma_1) \subset \mathcal{T}_{k,K}(\Gamma_2)$.*

Proof. Refer to Appendix VI-B. □

Theorem 1 implies that expanding the subspace $\mathcal{T}_{k,K}(\Gamma)$ (by modifying the system matrices A, B, C, D) allows us to increase the size of any opaque set. This again highlights the fundamental connection between opacity and the subspaces, WUOS and WUCS. Note that Theorem 1 provides the condition under which *every* opaque set in Γ_1 can be expanded. However, even when the condition in Theorem 1 is violated, there may exist *some (but not all)* opaque sets in Γ_1 that can be expanded.

B. Constrained Initial State and Input Sets

In this subsection, we relax the former assumptions that the state and input sets are unconstrained. Hence, we develop necessary and sufficient conditions for opacity to hold when these sets are constrained.

For the results in this subsection, we require the notion of backward-reachable set, as defined next.

Definition 6 (*Backward-reachable set*)**.** For $k > 0$, we define the backward-reachable set from $\mathcal{X}(k)$ as

$$\begin{aligned} \mathcal{B}(\mathcal{X}(k)) \triangleq \{x \in \mathbb{R}^n : \; & \exists\, U(k-1) \in \mathcal{U}(k-1) \;\text{ such that} \\ & x_{x,U(k-1)} \in \mathcal{X}(k)\}. \end{aligned}$$ □

The backward-reachable set $\mathcal{B}(\mathcal{X}(k))$ is the set of all states at time instant $k = 0$ starting from which the system reaches a state $x(k) \in \mathcal{X}(k)$ (for some input sequence). Note that this

set may contain states other than those in the initial state set $\mathcal{X}(0)$. Hence, in general, $\mathcal{B}(\mathcal{X}(k)) \supseteq \mathcal{X}(0)$.

In the following lemma, we consider the initial state set $\mathcal{X}(0)$ to be constrained, such that $\mathcal{X}(k)$ need not be a subspace. After this, we consider the case where both the initial state set $\mathcal{X}(0)$ and the input set $\mathcal{U}(k)$ are constrained.

Lemma 6. *For a given $k \geq 0$, let $\mathcal{X}(k) \subseteq \mathbb{R}^n$ and $|\mathcal{X}(k)| > 1$,[1] and for all $k \geq 0$, let $\mathcal{U}(k) = \mathbb{R}^{(k+1)p}$. Further, if $k \geq 1$, let $\mathcal{X}(0) = \mathcal{B}(\mathcal{X}(k))$. For System Γ in (1), there exists a secret set at time instant k that is KSO if and only if $\Big(\mathcal{X}(k) \oplus \big(-\mathcal{X}(k)\big)\Big) \cap \mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element.*

Proof. We begin by noting that Lemma 3 holds even when $\mathcal{X}(0) = \mathcal{B}(\mathcal{X}(k))$. This follows from the proof of Lemma 2. The condition $\mathcal{X}(0) = \mathcal{B}(\mathcal{X}(k))$ is required to show that if $x_{s,k} - x_{ns,k} \in \mathcal{T}_{k,K}(\Gamma)$, then $x_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$. This is because $\mathcal{X}(0) = \mathcal{B}(\mathcal{X}(k))$ ensures that there exist initial states $x(0)$ and $x'(0)$ in $\mathcal{X}(0)$ starting from which the system reaches the states $x_{s,k}$ and $x_{ns,k}$, respectively, and produces the same outputs such that $x_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$.

Only if: Since there exists a KSO secret set, let us form the smallest such set $\mathcal{X}_{s,k} = \{x_{s,k}\}$. As $x_{s,k}$ is KSO, there exists some non-secret state $x_{ns,k} \in \mathcal{X}(k) \backslash \mathcal{X}_{s,k}$ such that $x_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$. Therefore, by Lemma 3, it holds that $x_{s,k} - x_{ns,k} \in \mathcal{T}_{k,K}(\Gamma)$. Further, $x_{s,k} \neq x_{ns,k}$. Hence, it holds that
(i) $x_{s,k} - x_{ns,k} \in \mathcal{T}_{k,K}(\Gamma)$ and,
(ii) $x_{s,k} - x_{ns,k} \neq \{0\}$.

Consequently, we have that $\big(x_{s,k} - x_{ns,k}\big) \cap \mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element. Since $x_{s,k} \in \mathcal{X}(k)$ and $-x_{ns,k} \in -\mathcal{X}(k)$, $\Big(\mathcal{X}(k) \oplus \big(-\mathcal{X}(k)\big)\Big) \cap \mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element.

If: Let us consider $|\mathcal{X}(k)| = 2$, such that $\mathcal{X}(k) = \{x_1(k), x_2(k)\}$. Since $\Big(\mathcal{X}(k) \oplus \big(-\mathcal{X}(k)\big)\Big) \cap \mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element, we have that either
(i) $\big(x_1(k) - x_2(k)\big) \cap \mathcal{T}_{k,K}(\Gamma) \neq \{0\}$ and $\big(x_1(k) - x_2(k)\big) \cap \mathcal{T}_{k,K}(\Gamma) \neq \phi$ or,
(ii) $\big(x_2(k) - x_1(k)\big) \cap \mathcal{T}_{k,K}(\Gamma) \neq \{0\}$ and $\big(x_2(k) - x_1(k)\big) \cap \mathcal{T}_{k,K}(\Gamma) \neq \phi$.

Since $x_1(k)$ and $x_2(k)$ are arbitrary elements, let us consider the former case. Therefore, if we consider the secret state $x_{s,k} = x_1(k)$ and the non-secret state $x_{ns,k} = x_2(k)$, we have $x_{s,k} - x_{ns,k} \neq \{0\}$ and $x_{s,k} - x_{ns,k} \in \mathcal{T}_{k,K}(\Gamma)$. Hence, by Lemma 3, we have that $\mathcal{X}_{s,k} = \{x_{s,k}\}$ is KSO, thereby showing the existence of KSO secret set.

This approach holds equally well for the case where $|\mathcal{X}(k)| > 2$. □

In the above results, we have considered constraining either the secret state set or the state set. However, the input sets were unconstrained. In the following lemma, we extend Lemma 6 for initial-state opacity to consider the case where the input set is also constrained, in addition to constraining the state set.

Lemma 7. *For all $k \geq 0$, let $U_s(k) \in \mathcal{U}_s(k) \subseteq \mathbb{R}^{(k+1)p}$, $U_{ns}(k) \in \mathcal{U}_{ns}(k) \subseteq \mathbb{R}^{(k+1)p}$ and $\mathcal{X}(k) \subseteq \mathbb{R}^n$. Further, let $\mathcal{X}(0) \subseteq \mathbb{R}^n$ and $|\mathcal{X}(0)| > 1$.[2] For System Γ in (1), there exists a secret set $\mathcal{X}_{s,0}$ that is ISO if and only if there exists $x \in \Big(\mathcal{X}(0) \oplus \big(-\mathcal{X}(0)\big)\Big) \backslash \{0\}$ such that*

$$F_k^\Gamma \mathcal{U}_s(k) \subseteq O_k x \oplus F_k^\Gamma \mathcal{U}_{ns}(k) \qquad \forall\, k \geq 0. \tag{15}$$

Proof. If: From (15), we have

$$\begin{aligned} &\forall\, U_s(k) \in \mathcal{U}_s(k), \exists\, U_{ns}(k) \in \mathcal{U}_{ns}(k) \text{ such that} \\ &\qquad F_k^\Gamma U_s(k) = O_k x + F_k^\Gamma U_{ns}(k)\, \forall\, k \geq 0, \end{aligned}$$

where $x \in \Big(\mathcal{X}(0) \oplus \big(-\mathcal{X}(0)\big)\Big) \backslash \{0\}$. Consequently, there exists $x_{s,0} \in \mathcal{X}(0)$ and $x_{ns,0} \in \mathcal{X}(0)$ such that $x_{ns,0} - x_{s,0} = x \neq 0$. Therefore, for all $k \geq 0$, it holds that

$$\begin{aligned} &\forall\, U_s(k) \in \mathcal{U}_s(k), \exists\, U_{ns}(k) \in \mathcal{U}_{ns}(k) : \\ &\qquad F_k^\Gamma U_s(k) = O_k(x_{ns,0} - x_{s,0}) + F_k^\Gamma U_{ns}(k) \\ \iff\ &O_k x_{s,0} + F_k^\Gamma U_s(k) = O_k x_{ns,0} + F_k^\Gamma U_{ns}(k). \end{aligned}$$

Only if: We prove the contrapositive. If there does not exist $x \in \Big(\mathcal{X}(0) \oplus \big(-\mathcal{X}(0)\big)\Big) \backslash \{0\}$ such that

$$F_k^\Gamma \mathcal{U}_s(k) \subseteq O_k x \oplus F_k^\Gamma \mathcal{U}_{ns}(k)\, \forall\, k \geq 0,$$

then one cannot choose $x_{s,0} \in \mathcal{X}(0)$ and $x_{ns,0} \in \mathcal{X}(0)$ such that for all $U_s(k) \in \mathcal{U}_s(k)$, there exists $U_{ns}(k) \in \mathcal{U}_{ns}(k)$ for which the following holds for all $k \geq 0$:

$$\begin{aligned} &F_k^\Gamma U_s(k) = O_k(x_{ns,0} - x_{s,0}) + F_k^\Gamma U_{ns}(k) \\ \iff\ &O_k x_{s,0} + F_k^\Gamma U_s(k) = O_k x_{ns,0} + F_k^\Gamma U_{ns}(k). \end{aligned}$$

This implies that an ISO set $\mathcal{X}_{s,0}$ cannot be formed. □

Remark 3. Note that Lemma 7 reduces to Lemma 6 (for ISO case) when the input set is unconstrained. To see this, we first note that when the input set is unconstrained, (15) is equivalent to the relation, $x \in \mathcal{V}(\Gamma)$. This is because in this case, (15) is equivalent to the fact that for all $U_1(k) \in \mathbb{R}^{(k+1)p}$, there exists $U_2(k) \in \mathbb{R}^{(k+1)p}$ such that

$$\begin{aligned} &F_k^\Gamma U_1(k) = O_k x + F_k^\Gamma U_2(k) \\ \iff\quad &O_k x + F_k^\Gamma (U_2(k) - U_1(k)) = 0. \end{aligned}$$

The above is equivalent to the fact that there exists $U(k) = U_2(k) - U_1(k)$ such that $O_k x + F_k^\Gamma U(k) = 0 \iff x \in \mathcal{V}(\Gamma)$. Hence, when the input set is unconstrained, the condition in Lemma 7, "$x \in \Big(\mathcal{X}(0) \oplus \big(-\mathcal{X}(0)\big)\Big) \backslash \{0\}$ satisfies (15)," is equivalent to the condition, "$\Big(\mathcal{X}(0) \oplus \big(-\mathcal{X}(0)\big)\Big) \cap \mathcal{V}(\Gamma)$ contains at least one non-zero element," which is the one in Lemma 6 (for ISO case).

Further, Lemma 6 reduces to Statement 2(ii) of Lemma 2 when $\mathcal{X}(k) = \mathbb{R}^n$. In this case, the condition, "$\Big(\mathcal{X}(k) \oplus \big(-\mathcal{X}(k)\big)\Big) \cap \mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element," reduces to "$\mathcal{T}_{k,K}(\Gamma)$ contains at least one non-zero element," which is the condition in Statement 2(ii) of Lemma 2. □

C. Example

In this subsection, we present an example to explain the former results.

[1] One cannot construct a KSO secret set when $|\mathcal{X}(k)| \leq 1$. Hence, this case is not considered.

[2] One cannot construct an ISO secret set when $|\mathcal{X}(0)| \leq 1$. Hence, this case is not considered.

Example 1. We consider a smart grid system, in which an electricity supplier observes the amount of energy utilized by a household over a network. The supplier also has the capability to modify the energy utilized. This is done, for instance, by remotely changing the temperature value of the user's home thermostat [28].

For this system, at time instant k, let $e(k)$ denote the energy utilized by the household, and let $s(k)$ denote the value set by the supplier of the maximum energy that could be utilized by the customer. We denote the state by $x(k) = \begin{bmatrix} e(k) & s(k) \end{bmatrix}^T$. We consider the following system:

$$\begin{aligned} \underbrace{\begin{bmatrix} e(k+1) \\ s(k+1) \end{bmatrix}}_{x(k+1)} &= \underbrace{\begin{bmatrix} 0.5 & 0.5\eta \\ 0 & 0 \end{bmatrix}}_{A_m} \underbrace{\begin{bmatrix} e(k) \\ s(k) \end{bmatrix}}_{x(k)} + \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{B_m} u(k), \\ y(k) &= \underbrace{\begin{bmatrix} 1 & 0 \end{bmatrix}}_{C_m} x(k). \end{aligned} \tag{16}$$

By this model, we have that whenever $s(k)$ is set to a constant by applying a constant input $u(k)$, the energy utilized $e(k)$ asymptotically approaches $\eta s(k)$. Hence, if $e(k) < s(k)$, then $e(k)$ increases asymptotically to $\eta s(k)$. Similarly, if $e(k) > s(k)$, then $e(k)$ decreases asymptotically to $\eta s(k)$. Here, $\eta \in (0, 1]$ is a parameter that describes usage of energy in the household. For instance, if the user is not present, the value of η will be close to 0. In this example, we consider that the household utilizes the entire energy supplied, that is, $\eta = 1$, and remark that the results hold equally well for other values of η.

Further, we consider $\mathcal{X}(0) = \mathbb{R}^2$. This allows $e(0)$ and $s(0)$ to take negative values. This implies that the household is generating energy (for instance, by renewable means).

At any given time, the households transmit $y(k) = e(k)$ over a network to the supplier, which can be intercepted by an eavesdropper. Therefore, an eavesdropper observing $y(k) = e(k)$ over the network knows the amount of energy utilized by the household. However, in this example we show that this system is current-state opaque, and hence the eavesdropper cannot make an inference about the current value of $s(k)$.

For this system, $\mathcal{V}(\Gamma) = \mathcal{V}_1(\Gamma) = \{0\}$ and $\mathcal{C}(\Gamma) = \text{Range}(\begin{bmatrix} 0 & 1 \end{bmatrix}^T)$. We use this to illustrate the different notions of opacity.

• Part (i): We first consider opacity of individual initial states. We begin with initial-state opacity. Since $\mathcal{V}(\Gamma) = \{0\}$, we have that no secret state $x_{s,0}$ can be made initial-state opaque. For instance, the output sequence $\begin{bmatrix} 1 & 0 & 1 \end{bmatrix}^T$ can only be produced by the system with initial state $x(0) = \begin{bmatrix} 1 & -1 \end{bmatrix}^T$, regardless of the input sequence.

Next, we consider current-state opacity for $k = 2$. Let $x_{s,2} = \begin{bmatrix} 1 & 1 \end{bmatrix}^T$ and $x_{ns,2} = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$. Hence, $x_{s,2} - x_{ns,2} = \begin{bmatrix} 0 & 1 \end{bmatrix}^T \in \mathcal{C}(\Gamma)$.

Due to this, by Lemma 3, $x_{s,2} \xrightarrow{\text{cso}} \{x_{ns,2}\}$. This is because $x_{s,2} - x_{ns,2} \in \mathcal{C}(\Gamma)$ ensures that the same outputs are generated by the system to reach these states. We show this explicitly next. From opacity Definition 1, we have that for any $x(0)$ and $U_s(2)$ such that

$$x_{x(0),T_1[U_s(2)]} = x_{s,2}, \tag{17}$$

there should exist $x'(0)$ and $U_{ns}(2)$ for which

$$\begin{aligned} x_{x'(0),T_1[U_{ns}(2)]} &= x_{ns,2}, \\ Y_{x(0),U_s(2)} &= Y_{x'(0),U_{ns}(2)}. \end{aligned} \tag{18}$$

Due to (2), we have that (17) is equivalent to

$$\underbrace{\begin{bmatrix} 0.25 & 0.25 \\ 0 & 0 \end{bmatrix}}_{A^2} x(0) + \underbrace{\begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix}}_{N_2^\Gamma} T_1[U_s(2)] = \underbrace{\begin{bmatrix} 1 \\ 1 \end{bmatrix}}_{x_{s,2}}.$$

Therefore, whenever (17) holds, if we choose $x'(0) = x(0)$ and $U_{ns}(2) = U_s(2) - \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T$, we have that

$$\begin{aligned} x_{x'(0),T_1[U_{ns}(2)]} &= \underbrace{\begin{bmatrix} 0.25 & 0.25 \\ 0 & 0 \end{bmatrix}}_{A^2} x'(0) + \underbrace{\begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix}}_{N_2^\Gamma} T_1[U_{ns}(2)] \\ &= \underbrace{\begin{bmatrix} 0.25 & 0.25 \\ 0 & 0 \end{bmatrix} x(0) + \begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix} T_1[U_s(2)]}_{x_{s,2}} - \begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{x_{ns,2}}. \end{aligned}$$

Also, we have

$$\begin{aligned} Y_{x'(0),U_{ns}(2)} &= \underbrace{\begin{bmatrix} 1 & 0 \\ 0.5 & 0.5 \\ 0.25 & 0.25 \end{bmatrix}}_{O_2} x'(0) + \underbrace{\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.5 & 0 & 0 \end{bmatrix}}_{F_2^\Gamma} U_{ns}(2) \\ &= \underbrace{\begin{bmatrix} 1 & 0 \\ 0.5 & 0.5 \\ 0.25 & 0.25 \end{bmatrix} x(0) + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} U_s(2)}_{Y_{x(0),U_s(2)}} - \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.5 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \\ &= Y_{x(0),U_s(2)}. \end{aligned}$$

This shows that given an output sequence, an eavesdropper cannot know the current value of $s(k)$ set by the supplier.

Further, as $x_{s,2} \oplus \mathcal{C}(\Gamma) = x_{ns,2} \oplus \mathcal{C}(\Gamma) = \{\begin{bmatrix} 1 & c \end{bmatrix}^T : c \in \mathbb{R}\}$, it holds that $x_{ns,2} \in x_{s,2} \oplus \mathcal{C}(\Gamma)$ and $x_{s,2} \in x_{ns,2} \oplus \mathcal{C}(\Gamma)$. Thus, $x_{s,2}$ and $x_{ns,2}$ satisfy Corollary 2.

Finally, since $\mathcal{V}(\Gamma) = \mathcal{V}_1(\Gamma) = \{0\}$, by Lemma 2, we have that for all $k \geq 0$, we cannot make a secret state $x_{s,k}$ KSO for $K \geq 1$. Consequently, $x_{s,k}$ cannot be made Inf-SO either.

Thus, the system is CSO but not ISO, KSO or Inf-SO.

• Part (ii): Next, we focus on the opacity of sets. For $k \geq 0$, $\mathcal{X}(k) = \mathbb{R}^2$. Let $\mathcal{X}_{ns,k} = \left\{\begin{bmatrix} c & 0 \end{bmatrix}^T : c \in \mathbb{R}\right\}$. We note that $\mathcal{X}_{ns,k} \oplus \mathcal{C}(\Gamma) = \mathbb{R}^2$. Therefore, as seen in Fig. 2, any $x_{s,k} \in \mathcal{X}_{s,k} = \mathcal{X}(k) \backslash \mathcal{X}_{ns,k}$ belongs to $\mathcal{X}_{ns,k} \oplus \mathcal{C}(\Gamma)$. Thus, $\mathcal{X}_{s,k} \subset \mathcal{X}_{ns,k} \oplus \mathcal{C}(\Gamma)$ and $\mathcal{X}_{s,k} \xrightarrow{\text{cso}} \mathcal{X}_{ns,k}$ as per Lemma 4.□

D. Verification of Opacity Conditions

In this subsection, we develop methods to verify the conditions for opacity described in the previous sections.

Let W, W_1 and W_2 be matrices whose columns form the basis vectors of arbitrary subspaces $\mathcal{W}$, $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively. The subspaces W_1 and W_2 may correspond to two systems Γ_1 and Γ_2 (with different system matrices A, B, C, D). From

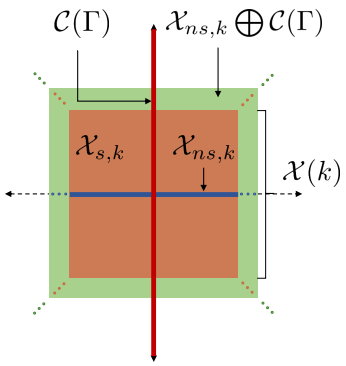

Fig. 2: Pictorial representation of Example 1, part(ii). $\mathcal{X}(k)$ is the infinite brown region, $\mathcal{X}_{ns,k}$ is the x axis, $\mathcal{X}_{s,k}$ is the infinite brown region without the x axis, $\mathcal{C}(\Gamma)$ is the y axis, and $\mathcal{X}_{ns,k} \oplus \mathcal{C}(\Gamma)$ is the infinite green region. Since $\mathcal{X}_{s,k} \subset \mathcal{X}_{ns,k} \oplus \mathcal{C}(\Gamma)$, we have $\mathcal{X}_{s,k} \xrightarrow{\text{cso}} \mathcal{X}_{ns,k}$.

basic linear algebra, we have the following results:

$$w \in \mathcal{W} \iff \text{rank}(\begin{bmatrix} w & W \end{bmatrix}) = \text{rank}(W), \quad (19)$$

$$\mathcal{W}_1 \subseteq \mathcal{W}_2 \iff \text{rank}(\begin{bmatrix} W_1 & W_2 \end{bmatrix}) = \text{rank}(W_2), \quad (20)$$

$$\mathcal{W}_1 \subset \mathcal{W}_2 \iff \text{rank}(\begin{bmatrix} W_1 & W_2 \end{bmatrix}) = \text{rank}(W_2) > \text{rank}(W_1). \quad (21)$$

Further, we have the following lemma:

Lemma 8. *Let $P_{\mathcal{W}^\perp}$ denote the projection matrix onto vector space $\mathcal{W}^\perp$. For any arbitrary disjoint sets $\mathcal{S}_1$ and $\mathcal{S}_2$, we have*

$$\mathcal{S}_1 \subset \mathcal{S}_2 \oplus \mathcal{W} \iff P_{\mathcal{W}^\perp}\mathcal{S}_1 \subseteq P_{\mathcal{W}^\perp}\mathcal{S}_2. \quad (22)$$

Proof. Refer to Appendix VI-E. □

With the above, we can verify opacity conditions described previously. Specifically, Lemma 3 can be verified using (19), Lemma 1 and Corollary 1 can be verified using (20), Theorem 1 can be verified using (21), and Lemmas 4 and 7,[3] and Corollary 2 can be verified using (22). Algorithms to find basis vectors for $\mathcal{V}_k(\Gamma)$ and $\mathcal{C}_k(\Gamma)$ are well known [20], [29].[4] □

IV. Opacity and Attack Detectability Trade-off

In this section, we use the relationship between opacity and the subspaces developed in Section III to characterize trade-offs between opacity and attack detectability. We do this in two ways by investigating the following questions:

- Does a system with opaque sets necessarily permit undetectable attacks? (Section IV-B)
- Does expanding opaque sets (by expanding $\mathcal{X}(0)$) expand the set of undetectable attacks? (Section IV-C)

[3]Verification of Lemma 7 may be more involved if $\mathcal{U}_s(k)$ and $\mathcal{U}_{ns}(k)$ are not subspaces since (15) has to be verified for all $k \geq 0$. We consider development of simpler algorithms to verify Lemma 7 as part of future work.

[4]The algorithm in [20] to compute basis vectors for $\mathcal{C}_k(\Gamma)$ can easily be extended to the case $D \neq 0$.

A. Attack Model

We consider an attacker[5] that is capable of injecting malicious attack inputs in the actuators and modify sensor readings of the System Γ. Let the attack inputs be denoted by $\tilde{u}(k)$. We allow the attack inputs to be injected via channels that are different than the channels for normal inputs. We model this using matrices $\tilde{B}$ and $\tilde{D}$ that can be different from B and D.

Since the normal input $u(k)$ is known to the system operator, its effect may be eliminated for the purposes of attack detection. Therefore, we set $u(k) = 0 \ \forall\, k \geq 0$ for the attack model. The attack model (denoted by $\tilde{\Gamma}$) is given as:

$$\tilde{\Gamma}: \quad \begin{aligned} \tilde{x}(k+1) &= A\tilde{x}(k) + \tilde{B}\tilde{u}(k), \\ \tilde{y}(k) &= C\tilde{x}(k) + \tilde{D}\tilde{u}(k), \end{aligned} \quad (23)$$

where $\tilde{x} \in \mathbb{R}^n$ and $\tilde{y} \in \mathbb{R}^m$ denote the attacked states and outputs, respectively, and $\tilde{u} \in \mathbb{R}^q$. Note that matrices A and C are same in the normal and the attack models. Let $\tilde{U}(k) = \begin{bmatrix} \tilde{u}(0)^T & \tilde{u}(1)^T & \cdots & \tilde{u}(k)^T \end{bmatrix}^T$ denote the attack input sequence (vector). Further, let $\tilde{Y}_{x(0),\tilde{U}(k)}$ denote the output sequence (vector) produced by applying the attack input sequence $\tilde{U}(k)$ to the initial state $x(0)$, which is expressed as:

$$\tilde{Y}_{x(0),\tilde{U}(k)} = O_k x(0) + F_k^{\tilde{\Gamma}} \tilde{U}(k), \quad (24)$$

where $F_k^{\tilde{\Gamma}}$ is computed by replacing B and D by $\tilde{B}$ and $\tilde{D}$, respectively, in the expression for F_k^{Γ} in (6).

Assumption 4. *In this section, we assume that System Γ is observable. Further, we assume $\mathcal{U}(k) = \mathbb{R}^{(k+1)p}\, \forall k \geq 0$.*

Assumption 5. *We assume that the attacker knows the system matrices A, B, C, D and the initial state set $\mathcal{X}(0)$.*

The system operator implements an attack detector[6] that determines whether the system is under attack or not by using the outputs. However, all attacks may not be detected, and next, we present the definition of undetectable attacks.

Definition 7 (*Undetectable Attacks* [30])**.** An attack $\tilde{U}(k)$ is said to be undetectable if there exist initial states $x(0), x'(0) \in \mathcal{X}(0)$ such that

$$\tilde{Y}_{x(0),\tilde{U}(k)} = \tilde{Y}_{x'(0),0} \iff \tilde{Y}_{x(0)-x'(0),\tilde{U}(k)} = 0.$$

We denote an undetectable attack sequence by $\tilde{U}_u(k) = \begin{bmatrix} \tilde{u}_u(0)^T & \tilde{u}_u(1)^T & \cdots & \tilde{u}_u(k)^T \end{bmatrix}^T$ and the set of all undetectable attack sequences in $\tilde{\Gamma}$ by $\tilde{\mathcal{U}}_u(k)$. For brevity, we use the notation $\tilde{U}_u$ to denote an attack sequence $\tilde{U}_u(k)$ that is undetectable for all $k \geq 0$ and $\tilde{\mathcal{U}}_u$ to denote the set of all such attack sequences in $\tilde{\Gamma}$. We also use the terms "attack sequences" and "attacks" interchangeably. □

For undetectable attacks, the output produced by the system is same as the output produced by a zero attack input sequence (no attack) with appropriate initial conditions. Therefore, the detector cannot determine if the system is under attack or not by using the outputs. The existence of undetectable attacks depends on the weakly unobservable subspace of the system.

[5]The attacker and the eavesdropper can be a single entity or two different entities.

[6]The attack detector is a dynamic detector as defined in [30], which operates on the entire output sequences.

In particular, it is known that if $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$ for the case where $\mathcal{X}(0) = \mathbb{R}^n$, then there exists an undetectable attack $\tilde{U}_u$ [13], [31].

B. Coexistence of Opaque Sets and Undetectable Attacks

In this section, we show that existence of opaque sets implies existence of undetectable attacks. In particular, we have the following theorem and its corollary.

Theorem 2. *Let $\mathcal{X}(0) = \mathbb{R}^n$ and $\mathcal{X}(k) \subseteq \mathbb{R}^n \; \forall \; k > 0$.[7] If there exists a secret set for System Γ that is:*

1. *ISO or,*
2. *CSO for some $k \geq n$ and Null$(F_n^\Gamma) \subseteq$ Null$(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$[8] or,*
3. *KSO for some $k \geq 0$ and $K \geq n-1$ or,*
4. *Inf-SO for some $k \geq 0$,*

then there exists an attacked system $\tilde{\Gamma}$ (that is, a pair $(\tilde{B}, \tilde{D})$) that admits an undetectable attack $\tilde{U}_u \neq 0$.

One such set of attacked systems is given by:

$$\left\{\tilde{\Gamma} : \textit{Range}\left(\begin{bmatrix} \tilde{B}^T & \tilde{D}^T \end{bmatrix}^T\right) \supseteq \textit{Range}\left(\begin{bmatrix} B^T & D^T \end{bmatrix}^T\right)\right\}.$$

Proof. Refer to Appendix VI-C. □

Corollary 3. *Let $\tilde{\Gamma} = \Gamma$ and let $\begin{bmatrix} B^T & D^T \end{bmatrix}^T$ be full column rank. Then, there exists an ISO set if and only if there exists an undetectable attack $\tilde{U}_u \neq 0$.*

The conditions 2-4 of Theorem 2 imply that the System Γ is ISO (refer to the proof for details). Thus, the initial state cannot be estimated from the output sequence. Consequently, this makes the system vulnerable to undetectable attacks.

Theorem 2 shows that existence of opaque set always implies existence of an attacked system with undetectable attack inputs (Corollary 3 shows that the converse also holds if the attacked and original systems are identical). Thus, one cannot have opacity in the system without making it inevitably vulnerable to undetectable attacks. This implies that a fundamental trade-off exists between opacity and attack detectability for linear systems. Theorem 2 is also valid for systems that are not observable. However, for such systems, existence of opaque sets does not guarantee that $\tilde{U}_u \neq 0$.

This trade-off is further illustrated in the following example where the system is modified to eliminate undetectable attacks.

Example 1. (Continued) In the system considered in Example 1, since it was current-state opaque, the eavesdropper could not infer the set-point $s(k)$ but could infer the energy utilized by each household $e(k)$ by observing the output sequence over the network. This causes a privacy issue, which can result in serious concerns. This issue can be mitigated by sending the aggregate energy utilization of a group of households (instead of individual values). Consequently, the eavesdropper cannot infer $e(k)$ also. Such privacy mechanisms have been proven to be both effective and lightweight [32], [33].

[7] Attack detectors in the literature generally require $\mathcal{X}(0) = \mathbb{R}^n$ [13], [30].

[8] The condition Null$(F_n^\Gamma) \subseteq$ Null$(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$ ensures the existence of non-zero initial states from which the system reaches $x(k)$ while producing the zero output sequence (Refer to the proof of Corollary 1).

By enforcing privacy in this manner, we illustrate how the trade-off exists for a group of N households. The model for the i^{th} household is given as:

$$x_i(k+1) = A_m x_i(k) + B_m u_i(k),$$
$$y_i(k) = C_m x_i(k),$$

where A_m, B_m and C_m are as given in (16). The aggregate model Γ of the smart grid system is:

$$\begin{bmatrix} x_1(k+1) \\ x_2(k+1) \\ \vdots \\ x_N(k+1) \end{bmatrix} = \begin{bmatrix} A_m & 0 & 0 \\ & \ddots & \\ 0 & 0 & A_m \end{bmatrix} \begin{bmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_N(k) \end{bmatrix} + \begin{bmatrix} B_m & 0 & 0 \\ & \ddots & \\ 0 & 0 & B_m \end{bmatrix} \begin{bmatrix} u_1(k) \\ u_2(k) \\ \vdots \\ u_N(k) \end{bmatrix},$$

$$y(k) = \begin{bmatrix} C_m & C_m & \cdots & C_m \end{bmatrix} \begin{bmatrix} x_1(k) \\ x_2(k) \\ \vdots \\ x_N(k) \end{bmatrix}.$$

Note that $y(k)$ denotes the aggregate energy utilization. Let us consider the case where $N = 2$, $\eta = 1$ and $e_1(0) = e_2(0) = s_1(0) = s_2(0) = 100$. Thus, these two households initially utilize 100 units of power. If the supplier would require the energy utilized in both households to be reduced to, say, 50 units, the supplier sends the input values $u_1(k) = u_2(k) = 50$ for all $0 \leq k < k_0$, where k_0 is some time instant at which the supplier would change the set-points to $s_1(k_0)$ and $s_2(k_0)$. Let $k_0 = 6$. In this case, the sequence $e_1(k)$ and $e_2(k)$ (described as vector) is given by $\begin{bmatrix} 100 & 100 & 75 & 62.5 & 56.25 & 53.125 \end{bmatrix}^T$ for $0 \leq k \leq 5$. Similarly, the aggregate output sequence generated, that is $y(k)$ (vector), is given by $\begin{bmatrix} 200 & 200 & 150 & 125 & 112.5 & 106.25 \end{bmatrix}^T$. Since the supplier observes only the aggregate value $y(k)$ (as shown in Fig. 3), the privacy of the energy utilization of the individual households is maintained.

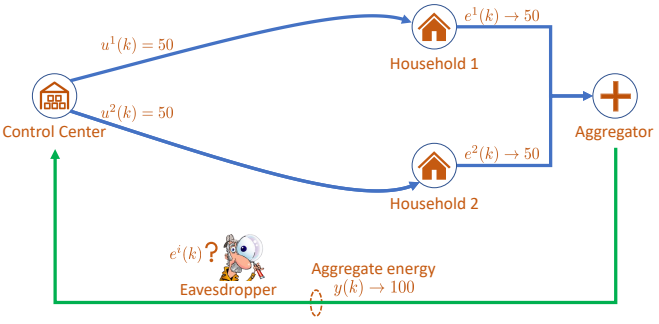

Fig. 3: Opacity of Smart Grid system: Energy utilized by households 1 and 2 are opaque (for all notions), since same aggregate energy $y(k)$ (green line) is output by the Aggregator.

However, an attacker could intercept the communication in the network and modify the values of $u_1(k)$ and $u_2(k)$ (thus changing $s_1(k)$ and $s_2(k)$), such that the aggregate outputs $y(k)$ remain the same as in the unattacked case, while causing the energy utilized in individual households to change significantly. For an attack detector on the supplier's side that has access to only the aggregate output $y(k)$, such an attack will remain undetected. For instance, for the attacked system identical to the normal system ($\tilde{\Gamma} = \Gamma$), the attacker

can modify the set-point values $\tilde{s}_1(k)$ and $\tilde{s}_2(k)$ with attack inputs $\tilde{u}_1(k) = 50$ and $\tilde{u}_2(k) = -50$ for $0 \leq k \leq 5$. This causes the energy utilized in the households to be changed to the sequences $e_1(k) = \begin{bmatrix}100 & 100 & 100 & 100 & 100\end{bmatrix}^T$ and $e_2(k) = \begin{bmatrix}100 & 100 & 50 & 25 & 12.5 & 6.25\end{bmatrix}^T$. Consequently, in the attack case, the aggregate output sequence $y(k)$ (inclusive of the attack) is same as in the unattacked case, that is, $\begin{bmatrix}200 & 200 & 150 & 125 & 112.5 & 106.25\end{bmatrix}^T$ (as shown in Fig. 4). Therefore, this attack remains undetected. This shows that opacity implies existence of undetectable attacks.

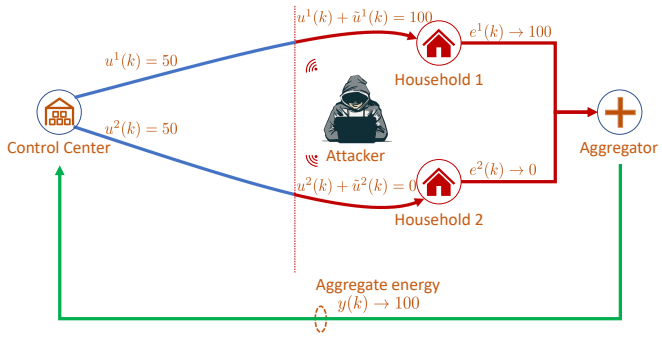

Fig. 4: Undetectable attacks on Smart Grid system: Attacker injects an attack to change the set-point values (blue arcs to red arcs), while maintaining unattacked outputs (green line).

Next, we modify the system in order to eliminate undetectable attacks, and show that this also eliminates opaque sets. Consider a modified system with the output equation $y(k) = x(k)$. Consider $\tilde{\Gamma} = \Gamma$ for this modified system. All attacks in $\tilde{\Gamma}$ are detectable at some time instant k, including the previously considered undetectable attack $\tilde{u}_1(k) = 50$ and $\tilde{u}_2(k) = -50$ for $0 \leq k \leq 5$, as shown next. For this attack to remain undetected, there should exist an initial condition $x(0)$ such that the outputs are zero. Since $\mathcal{V}(\tilde{\Gamma}) = \{0\}$, the only initial condition that satisfies this is $x(0) = \begin{bmatrix}0 & 0\end{bmatrix}^T$ (c.f. Definition 4). However, this attack with this initial condition produces non-zero output sequence $\tilde{y}(k)$, and therefore, is detectable. Moreover, since $\mathcal{V}(\Gamma) = \mathcal{C}(\Gamma) = \{0\}$, no opaque sets exist (c.f. Lemma 2), that is, an eavesdropper is able to infer the energy utilized by the household. Therefore, we observe that eliminating undetectable attacks also eliminates opaque sets, indicating the trade-off between the two.

C. Relation between Sizes of Opaque and Undetectable Attacks Set

In this subsection, we consider an observable system and examine the effect of expanding the opaque set on the size of undetectable attack set, and vice-versa, and show that there exists a trade-off between the two. In particular, we demonstrate that expanding the opaque set always leads to expansion of the undetectable attack set.

One way to expand the opaque set without changing the system is to expand the initial state set $\mathcal{X}(0)$.[9] An expansion of $\mathcal{X}(0)$ may be performed by the operator, for instance, to include a larger set of opaque secret states.

To assess the trade-off, we first characterize the set of undetectable attacks in terms of initial state set $\mathcal{X}(0)$.

Lemma 9. *Let $\mathcal{X}(0) \subseteq \mathbb{R}^n$. For all $k \geq 0$, the set of undetectable attacks is given by*

$$\tilde{\mathcal{U}}_u(k) = \left\{\tilde{U}_u(k) : F_k^{\tilde{\Gamma}}\tilde{U}_u(k) \in O_k(\mathcal{X}(0) \oplus -\mathcal{X}(0))\right\}.$$

Proof. From undetectable attack Definition 7, we have for any undetectable attack $\tilde{U}_u(k)$ with $k \geq 0$, there exists $x(0), x'(0) \in \mathcal{X}(0)$ such that $O_k x(0) + F_k^{\tilde{\Gamma}}\tilde{U}_u(k) = O_k x'(0)$. Therefore, $F_k^{\tilde{\Gamma}}\tilde{U}_u(k) = O_k(x'(0) - x(0))$. Taking into consideration all possible combinations of $x'(0)$ and $x(0)$, we have that $F_k^{\tilde{\Gamma}}\tilde{U}_u(k) \in O_k(\mathcal{X}(0) \oplus -\mathcal{X}(0))$. □

The above lemma shows that $\tilde{\mathcal{U}}_u(k)$ depends on $\mathcal{X}(0)$. By using this fact and the definition of opacity, the following theorem describes the trade-off when $\mathcal{X}(0)$ is expanded.

Theorem 3. *Consider two initial state sets $\mathcal{X}^1(0) \subset \mathcal{X}^2(0) \subseteq \mathbb{R}^n$ such that for some particular $k \geq 0$, $\mathcal{X}^1(0) = \mathcal{B}(\mathcal{X}^1(k))$ (c.f. Definition 6). Let $\tilde{\mathcal{U}}_u^1$ and $\tilde{\mathcal{U}}_u^2$ denote the set of undetectable attacks (c.f. Definition 7) on an attacked system $\tilde{\Gamma}$ with initial state set $\mathcal{X}^1(0)$ and $\mathcal{X}^2(0)$, respectively. Then, the following statements hold true:*

1. For each KSO set $\mathcal{X}_{s,k}^1 \subset \mathcal{X}^1(k)$, there exists a KSO set $\mathcal{X}_{s,k}^2 \subset \mathcal{X}^2(k)$ such that:

a. $\mathcal{X}_{s,k}^1 \subseteq \mathcal{X}_{s,k}^2$ always.

b. $\mathcal{X}_{s,k}^1 \subset \mathcal{X}_{s,k}^2$ if and only if there exists $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ that satisfies:

$$\left(x(k) \oplus \mathcal{T}_{k,K}(\Gamma)\right) \cap \mathcal{X}^2(k) \neq \{x(k)\}.$$

2. The set of undetectable attacks are related as:

a. $\tilde{\mathcal{U}}_u^1 \subseteq \tilde{\mathcal{U}}_u^2$ always.

b. $\tilde{\mathcal{U}}_u^1 \subset \tilde{\mathcal{U}}_u^2$ if and only if there exists some k_0 such that for all $k \geq k_0$,

$$Range(F_k^{\tilde{\Gamma}}) \cap O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \supset Range(F_k^{\tilde{\Gamma}}) \cap O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big).$$

c. $\tilde{\mathcal{U}}_u^1 \subset \tilde{\mathcal{U}}_u^2$ if $\tilde{D}$ is square and full rank.

Proof. Refer to Appendix VI-D. □

Statements 1(a) and 2(a) of Theorem 3 show that on expanding $\mathcal{X}(0)$, the opaque and undetectable attack sets either expand or remain unchanged, but never contract. Statements 1(b) and 2(b) of the theorem provide conditions under which these sets strictly expand, leading to a strict trade-off between opaque and undetectable attack sets. The condition in Statement 1(b) implies that there exists an additional state $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ that can be chosen as a KSO secret state, whose proxy non-secret state exists in $\mathcal{X}^2(k)$, and is not the state $x(k)$ itself (illustrated in Fig. 5).[10] . Further, the condition in Statement 2(b) implies that there exists a new initial state in $\mathcal{X}^2(0)$ that allows a new undetectable attack in the attacked system $\tilde{\Gamma}$.

[9]Note that expanding $\mathcal{X}_{s,k}$ without changing $\mathcal{X}(0)$ does not affect the undetectable attack set.

[10]If $\mathcal{X}^1(0) \neq \mathcal{B}(\mathcal{X}^1(k))$, further conditions are required for expansion of opaque sets.

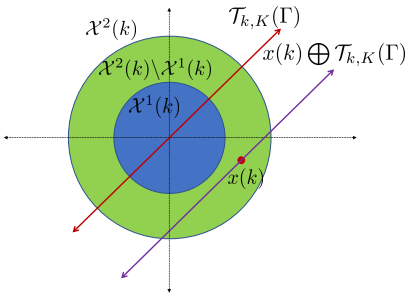

Fig. 5: Pictorial representation of Theorem 3, Statement 1(b). $\mathcal{X}^1(k)$ is the blue disk, $\mathcal{X}^2(k)$ is the union of blue disk and green region, $\mathcal{T}_{k,K}(\Gamma)$ is the red line passing through the origin, $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ is the red dot and $x(k) \oplus \mathcal{T}_{k,K}(\Gamma)$ is the purple line passing through $x(k)$. Since $(x(k) \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) \neq \{x(k)\}$, for an opaque $\mathcal{X}^1_{s,k} \subset \mathcal{X}^1(k)$, there exists an opaque $\mathcal{X}^2_{s,k} \subset \mathcal{X}^2(k)$ that satisfies $\mathcal{X}^1_{s,k} \subset \mathcal{X}^2_{s,k}$.

Finally, Statement 2(c) implies that there exists a $\tilde{\Gamma}$ (with $\tilde{D}$ square and full rank, and $\tilde{B}$ arbitrary) for which the undetectable attack set always expands without any conditions. Hence, in this case, expanding $\mathcal{X}(0)$ always expands the set of undetectable attacks, but the set of opaque secret states expands only under the condition in Statement 1(b).

We remark that except for Statement 2(c), Theorem 3 is also valid for systems that are not observable.

Example 1. (Continued) We verify Statements 1(b) and 2(b) of Theorem 3. We begin with Statement 1(b). We consider current-state opacity where $K = 0$. Hence, we have $\mathcal{T}_{k,0}(\Gamma) = \mathcal{C}_k(\Gamma)$. Let $N = 2$ and $\eta = 1$. With this, the system dynamics is:

$$\begin{aligned}\begin{bmatrix} x_1(1) \\ x_2(1) \end{bmatrix} &= \begin{bmatrix} A_m & 0 \\ 0 & A_m \end{bmatrix} \begin{bmatrix} x_1(0) \\ x_2(0) \end{bmatrix} + \begin{bmatrix} B_m & 0 \\ 0 & B_m \end{bmatrix} \begin{bmatrix} u_1(0) \\ u_2(0) \end{bmatrix} \\ &= \underbrace{\begin{bmatrix} 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{A} \begin{bmatrix} x_1(0) \\ x_2(0) \end{bmatrix} + \underbrace{\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}}_{B} \begin{bmatrix} u_1(0) \\ u_2(0) \end{bmatrix}, \\ y(k) &= \begin{bmatrix} C_m & C_m \end{bmatrix} \begin{bmatrix} x_1(k) \\ x_2(k) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 1 & 0 \end{bmatrix}}_{C} \begin{bmatrix} x_1(k) \\ x_2(k) \end{bmatrix}.\end{aligned}$$

The weakly unconstructible subspace for $k = 1$ is given by:

$$\mathcal{C}_1(\Gamma) = \text{Range}\left(\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \right).$$

Let $\mathcal{X}^1(0) = \text{Null}(A)$. This results in $\mathcal{X}^1(1) = \text{Range}(B)$. Since $\text{Range}(A) \cap \text{Range}(B) = \{0\}$, we satisfy $\mathcal{X}^1(0) = \mathcal{B}(\mathcal{X}^1(1))$. This is because if $x(0) \notin \text{Null}(A) (= \mathcal{X}^1(0))$, we have $x(1) = Ax(0) + Bu(0) \notin \text{Range}(B) (= \mathcal{X}^1(1))$. Further, let $\mathcal{X}^2(0) = \mathbb{R}^4$. This results in $\mathcal{X}^2(1) = \mathbb{R}^4$.

Next, we show that for an arbitrary CSO secret set $\mathcal{X}^1_{s,1} \subset \mathcal{X}^1(1)$, there exists a larger CSO secret set $\mathcal{X}^2_{s,1} \subset \mathcal{X}^2(1)$, that is, $\mathcal{X}^1_{s,1} \subset \mathcal{X}^2_{s,1}$. To this end, we consider $x(1) = \begin{bmatrix} 1 & 0 & -1 & 0 \end{bmatrix}^T$ and claim that $\mathcal{X}^2_{s,1}$ can be constructed as $\mathcal{X}^2_{s,1} = \mathcal{X}^1_{s,1} \cup \{x(1)\}$. Clearly, $x(1) \in \mathcal{X}^2(1) \backslash \mathcal{X}^1(1)$, which implies $x(1) \notin \mathcal{X}^1_{s,1}$, and therefore $\mathcal{X}^1_{s,1} \subset \mathcal{X}^2_{s,1}$. Thus, to verify the claim, what remains is to show that $x(1)$ is a CSO secret state, or equivalently, there exists a non-secret state in $\mathcal{X}^2(1)$ that makes $x(1)$ CSO. By Corollary 2, such a non-secret state should belong to the set $\big(x(1) \oplus \mathcal{C}_1(\Gamma)\big)$. Combining the above two arguments, we have that $\big(x(1) \oplus \mathcal{C}_1(\Gamma)\big) \cap \mathcal{X}^2(1)$ should not be empty, and contain an element other that $x(1)$, which is essentially the condition in Statement 1(b) of Theorem 3. Finally, note that since in our example $x(1) \oplus \mathcal{C}_1(\Gamma) = \mathcal{C}_1(\Gamma)$, the above condition is satisfied:

$$\big(x(1) \oplus \mathcal{C}_1(\Gamma)\big) \cap \mathcal{X}^2(1) = \mathcal{C}_1(\Gamma) \neq \{x(1)\}.$$

Next, we consider undetectable attacks. Consider an attacked system $\tilde{\Gamma}$ with $\tilde{B} = I_4$, $\tilde{D} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$ and $k = 1$. We first check the condition in Statement 2(b) of Theorem 3. Since $\mathcal{X}^2(0) = \mathbb{R}^4$, we have

$$\begin{aligned}\text{Range}(F_1^{\tilde{\Gamma}}) \cap O_1\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) &= \text{Range}(F_1^{\tilde{\Gamma}}) \cap O_1(\mathbb{R}^4) \\ &= \text{Range}(F_1^{\tilde{\Gamma}}) \cap \text{Range}(O_1).\end{aligned}$$

On computing the above range spaces, we have that the above is equal to:

$$\text{Range}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \cap \text{Range}\left(\begin{bmatrix} 1 & 0 \\ 0.5 & 0.5 \end{bmatrix} \right) = \text{Range}\left(\begin{bmatrix} 0 \\ 0.5 \end{bmatrix} \right).$$

Similarly, we also have:

$$\begin{aligned}&\text{Range}(F_1^{\tilde{\Gamma}}) \cap O_1\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big) \\ =&\text{Range}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \cap \text{Range}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) = \{0\}.\end{aligned}$$

Hence, the condition in Statement 2(b) holds for $k = 1$. For $k > 1$, it can be shown empirically that in the condition of Statement 2(b), the left-hand side expression is $\text{Range}\left(\begin{bmatrix} 0 & 0.5 & 0.25 & \cdots & 0.5^k \end{bmatrix}^T \right)$ and the right-hand side expression is $\{0\}$. Hence Statement 2(b) holds with $k_0 = 1$, implying the existence of additional undetectable attacks with initial state set $\mathcal{X}^2(0)$. For instance, the following attack sequence is undetectable with $\mathcal{X}^2(0)$ but not with $\mathcal{X}^1(0)$: $\tilde{u}(0) = \begin{bmatrix} -0.25 & 0 & -0.25 & 0 \end{bmatrix}^T$, $\tilde{u}(k) = 0 \, \forall k \geq 1$. This is because for $x(0) = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T \in \mathcal{X}^2(0)$, this attack input will produce the zero output sequence. Thus, by Definition 7, this attack is undetectable. Note that this attack is not undetectable with initial state set $\mathcal{X}^1(0)$ since there exists no $x(0) \in \mathcal{X}^1(0)$ (including $x(0) = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T$) that produces the zero output sequence with this attack input. This implies that $\tilde{\mathcal{U}}^1_u \subset \tilde{\mathcal{U}}^2_u$.

Finally, we check Statement 2(c) of Theorem 3. Let $C = I_4$ such that $y(k) = x(k)$ (System Γ is observable). Further, let $\tilde{B} = 0$ and $\tilde{D} = I_4$. With this, Statement 2(c) holds since $\tilde{D}$ is square and full rank. Thus, there exist more undetectable attacks with $\mathcal{X}^2(0)$ as the initial state set. For instance, with $x(0) = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}^T$, the attack input sequence $\tilde{u}(k) = \begin{bmatrix} -0.5^{k+1} & 0 & 0 & 0 \end{bmatrix}^T \, \forall k \geq 0$, is undetectable with initial state set $\mathcal{X}^2(0)$ but not with $\mathcal{X}^1(0)$.

V. Conclusion

We analyzed the underlying connections between the notion of opacity and attack detectability for linear dynamical systems. The fundamental relation between opacity and the

weakly unobservable and weakly unconstructible subspaces was studied from multiple perspectives. Using this relation, we showed that a trade-off exists between opaque sets and undetectable attacks.

This work has been primarily qualitative in nature. As part of future work, these relations can be studied quantitatively by developing metrics that measure opacity and security. Further, the trade-off can be studied for more general systems such as non-linear, hybrid and stochastic systems. Also, the connections and trade-offs of other notions of opacity, such as pre-opacity, language-based opacity, etc. can be explored.

VI. Appendix

A. Proof of Lemma 5

For an arbitrary $x \in \mathbb{R}^n$, consider the set $\mathcal{S} = x \oplus \mathcal{T}_{k,K}(\Gamma)$. The set $\mathcal{S}$ is formed by shifting the subspace $\mathcal{T}_{k,K}(\Gamma)$ parallel to itself to contain x. Hence, we note that $\mathcal{X}(k) = \mathbb{R}^n$ is the union of all such sets $\mathcal{S}$ with different values of $x \in \mathbb{R}^n$.

Next, in the set $\mathcal{S}$, let x be a non-secret state $x_{ns,k}$ and let all other elements in $\mathcal{S}$ be secret states. We have by Corollary 2 that all the secret states in $\mathcal{S}$ are made KSO by the set's single non-secret state $x_{ns,k}$. If we wish to form a larger KSO set in $\mathcal{S}$, we would need to convert the non-secret state $x_{ns,k}$ to a secret state. However, this would make all the secret states in $\mathcal{S}$ to be not KSO. Hence, we cannot construct a larger KSO set in $\mathcal{S}$. Therefore, the largest KSO set is formed in $\mathcal{S}$ when it has only one non-secret state.

From the discussions above, we can construct the largest opaque set $\mathcal{X}_{s,k}$ in $\mathcal{X}(k) = \mathbb{R}^n$ by keeping only one non-secret state in each set $\mathcal{S}$. One such construction is by having $\mathcal{X}_{ns,k} = \mathcal{T}_{k,K}(\Gamma)^\perp$, such that $\mathcal{X}_{s,k} = \mathbb{R}^n \backslash \mathcal{T}_{k,K}(\Gamma)^\perp$ is KSO. In this construction, every element of $\mathcal{X}_{ns,k} = \mathcal{T}_{k,K}(\Gamma)^\perp$ composes the single non-secret state $x_{ns,k}$ in each set $\mathcal{S}$.

B. Proof of Theorem 1

For brevity, we omit the time instant and system notations in $\mathcal{T}_{k,K}(\Gamma)$ in this proof. Hence, for $i \in \{1, 2\}$, $\mathcal{T}_i \triangleq \mathcal{T}_{k,K}(\Gamma_i)$.

If: Consider any opaque set $\mathcal{X}^1_{s,k}$ in Γ_1. Since $\mathcal{X}^1_{s,k}$ is KSO, it holds that $\mathcal{X}^1_{s,k} \xrightarrow{\text{kso}} \mathcal{X}(k) \backslash \mathcal{X}^1_{s,k}$. We begin with a preliminary analysis for System Γ_1 that we use later in the proof. By Corollary 2, we have that for a secret state $x_{s,k}$, its proxy non-secret state $x_{ns,k}$ must belong to the set $x_{s,k} \oplus \mathcal{T}_1$. For a particular $x(k)$, consider the set $\mathcal{S} \triangleq \{x(k) \oplus \mathcal{T}_1\}$.

Since in Γ_1, all secret states are KSO, we have that if secret states exist in the set $\mathcal{S}$, then they are made opaque by the set's non-secret states (c.f. Corollary 2). If secret states do not exist in $\mathcal{S}$, then all its elements are non-secret states. Hence, since $\mathcal{X}_{s,k}$ is KSO, we have that the set $\mathcal{S}$ contains at least one non-secret state. Further, we have that the state space $\mathcal{X}(k) = \mathbb{R}^n$ is the union of all such sets $\mathcal{S}$ (for different values of $x(k)$).

Next we continue the proof. We need to form a KSO set $\mathcal{X}^2_{s,k}$ in Γ_2 such that $\mathcal{X}^2_{s,k} \supset \mathcal{X}^1_{s,k}$. For this, we need to form a new secret state $x^{\text{new}}_{s,k} \in \mathcal{X}^2_{s,k} \backslash \mathcal{X}^1_{s,k}$ for which $\mathcal{X}^2_{s,k} = \mathcal{X}^1_{s,k} \cup x^{\text{new}}_{s,k}$. Let us choose any $x_{ns,k} \in \mathcal{X}^1_{ns,k}$ $(= \mathcal{X}(k) \backslash \mathcal{X}^1_{s,k})$ and convert it to be the required $x^{\text{new}}_{s,k}$. Since $x^{\text{new}}_{s,k}$ is a new secret state, $\mathcal{X}^2_{s,k} \supset \mathcal{X}^1_{s,k}$. Hence, what remains to be shown is that $\mathcal{X}^2_{s,k}$ is KSO. We show this by proving that all $x_{s,k} \notin x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$ and all $x_{s,k} \in x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$ are KSO. This means that all $x_{s,k} \in \mathcal{X}^2_{s,k}$ are KSO, and hence, $\mathcal{X}^2_{s,k}$ is KSO.

First, we consider a secret state $x_{s,k} \in \mathcal{X}^2_{s,k}$ for which $x_{s,k} \notin x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$. For this, we know from the preliminary analysis above that there exists a non-secret state $x_{ns,k} \in x_{s,k} \oplus \mathcal{T}_1$. Since $x_{s,k} \oplus \mathcal{T}_1 \subset x_{s,k} \oplus \mathcal{T}_2$, it also holds that $x_{ns,k} \in x_{s,k} \oplus \mathcal{T}_2$. Hence, by Corollary 2, $x_{s,k}$ is KSO.

Next, we consider a secret state $x_{s,k} \in \mathcal{X}^2_{s,k}$ for which $x_{s,k} \in x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$. Since a non-secret state was chosen and converted to be the secret state $x^{\text{new}}_{s,k}$, it may be possible that the set $x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$ does not have non-secret states. Note that in System Γ_2, $x_{s,k}$ is KSO if and only if the set $x_{s,k} \oplus \mathcal{T}_2$ has non-secret states (c.f. Corollary 2). Since $x_{s,k} \in x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$,

$$x_{s,k} \oplus \mathcal{T}_1 \subseteq x^{\text{new}}_{s,k} \oplus \mathcal{T}_1 \oplus \mathcal{T}_1 = x^{\text{new}}_{s,k} \oplus \mathcal{T}_1.$$

Since the Minkowski sum $x(k) \oplus \mathcal{T}_1$ just shifts the subspace $\mathcal{T}_1$ to the location of the vector $x(k)$, the relation $x_{s,k} \oplus \mathcal{T}_1 \subset x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$ cannot hold. Hence, we have $x_{s,k} \oplus \mathcal{T}_1 = x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$. Since, $\mathcal{T}_1 \subset \mathcal{T}_2$, we also have $\mathcal{T}_2 = \mathcal{T}_1 \oplus \mathcal{T}_2$. Consequently,

$$x_{s,k} \oplus \mathcal{T}_2 = x_{s,k} \oplus \mathcal{T}_1 \oplus \mathcal{T}_2 = x^{\text{new}}_{s,k} \oplus \mathcal{T}_2.$$

Hence, for $x_{s,k}$ to be KSO, we need to show that there exist non-secret states in the set $x^{\text{new}}_{s,k} \oplus \mathcal{T}_2$. We have that the set $x^{\text{new}}_{s,k} \oplus \mathcal{T}_2$ is the union of $x(k) \oplus \mathcal{T}_1$ for some states $x(k) \in \mathbb{R}^n$. We have that $x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$ may not have non-secret states. However, from the preliminary analysis above, we have that for $x(k) \notin x^{\text{new}}_{s,k} \oplus \mathcal{T}_1$, there exists at least one non-secret state in $x(k) \oplus \mathcal{T}_1$. Hence, there exists a non-secret state in $x^{\text{new}}_{s,k} \oplus \mathcal{T}_2$. Consequently, by Corollary 2, we have that $x_{s,k}$ is KSO.

From this, we have that all $x_{s,k} \in \mathcal{X}^2_{s,k}$ is KSO. Hence, $\mathcal{X}^2_{s,k}$ is KSO.

Only if: We prove by contrapositive argument. Therefore, for $\mathcal{T}_1 \not\subset \mathcal{T}_2$, it is to be shown that for each KSO set $\mathcal{X}^1_{s,k}$ in Γ_1 there does not exist a set $\mathcal{X}^2_{s,k}$ that is more KSO in Γ_2. We consider the following three cases:

(i) $\mathcal{T}_1 = \mathcal{T}_2 = \mathcal{T}$: For System Γ_1, let us consider the opaque set $\mathcal{X}_{s,k} = \mathbb{R}^n \backslash \mathcal{T}^\perp$. Due to Lemma 5, there does not exist a more opaque[11] set in Γ_1. Therefore, since $\mathcal{T}_1 = \mathcal{T}_2$, there does not exist a more opaque set in Γ_2 also.

(ii) $\mathcal{T}_1 \supset \mathcal{T}_2$: We consider the same set $\mathcal{X}_{s,k}$ in Case (i). For System Γ_2, even $\mathcal{X}_{s,k}$ cannot be made KSO since $\mathcal{T}_1 \supset \mathcal{T}_2$. Therefore, a more KSO set also cannot be constructed.

(iii) $\mathcal{T}_1 \cap \mathcal{T}_2 \neq \mathcal{T}_2$: This case accounts for all the remaining possibilities. In this case, we have that there exists at least one basis vector belonging to $\mathcal{T}_1$ and not in $\mathcal{T}_2$ and vice-versa. Let t_1 be a basis vector in $\mathcal{T}_1$ that is not in $\mathcal{T}_2$. For System Γ_1, consider the KSO set $\mathcal{X}_{s,k} = \mathcal{T}_2$. This set is opaque since every $x_{s,k} \in \mathcal{X}_{s,k}$ is opaque due to a non-secret state $x_{ns,k} \in \mathcal{X}_{s,k} \oplus t_1$ (c.f. Corollary 2). However, for System Γ_2, $\mathcal{X}_{s,k}$ cannot be made KSO since by Corollary 2, the corresponding proxy non-secret state must belong to the set

$$(\mathcal{X}_{s,k} \oplus \mathcal{T}_2) = (\mathcal{X}_{s,k} \oplus \mathcal{X}_{s,k}) = \mathcal{X}_{s,k}.$$

Hence, proxy non-secret states do not exist for $\mathcal{X}_{s,k}$. Therefore, we cannot construct a more KSO set in Γ_2.

[11] The terms *more opaque* and *more KSO* used in this proof are defined in Definition 3.

This article has been accepted for publication in IEEE Transactions on Automatic Control. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAC.2024.3426549

C. Proof of Theorem 2

We will show that existence of an opaque secret set $\mathcal{X}_{s,k}$ in Γ implies that an undetectable attack $\tilde{U}_u \neq 0$ exists for a particular attacked system $\tilde{\Gamma} = \Gamma$. Later, we generalize this for other attacked systems. We consider K-step opacity first.

When $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$, there exists an undetectable $\tilde{U}_u$ for $\tilde{\Gamma}$ (c.f. discussion below Definition 7). Therefore, we show that when KSO set $\mathcal{X}_{s,k}$ exists, we have $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$. We show it as follows. Let there exist a KSO set for some $K \geq n-1$. Then, we have by Lemma 6, $\Big(\mathcal{X}(k) \oplus \big(-\mathcal{X}(k)\big)\Big) \cap \mathcal{T}_{k,K}(\Gamma) \neq \{0\}$. Hence, we have $\mathcal{T}_{k,n-1}(\Gamma) \neq \{0\} \implies \mathcal{C}_k(\Gamma) \cap \mathcal{V}(\Gamma) \neq \{0\} \implies \mathcal{V}(\Gamma) \neq \{0\} \implies \mathcal{V}(\tilde{\Gamma}) \neq \{0\}$.

In the above proof, if we put $k = 0$ and $K = \infty$, we have the proof for the ISO case. Similarly, for arbitrary k, the proofs for CSO and Inf-SO follow from the above proof when $K = 0$ and $K = \infty$, respectively. For the CSO case, we also require Corollary 1 to show that since $\mathcal{C}(\Gamma) \neq \{0\}$ and $\text{Null}(F_n^\Gamma) \subseteq \text{Null}(\begin{bmatrix} N_n^\Gamma & 0 \end{bmatrix})$, we have that $\mathcal{V}(\Gamma) \neq \{0\}$, and hence, $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$.

Therefore, since $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$, an undetectable attack $\tilde{U}_u$ exists for $\tilde{\Gamma}$. Next we show that $\tilde{U}_u \neq 0$.

Since $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$, there exists a non-zero $\tilde{x}(0) \in \mathcal{V}(\tilde{\Gamma})$. Consequently, there exists a $\tilde{U}_u$ satisfying:

$$F_k^{\tilde{\Gamma}} \tilde{U}_u(k) = -O_k \tilde{x}(0) \qquad \forall\, k \geq 0. \tag{25}$$

Since Γ is observable (Assumption 4), $\tilde{\Gamma}$ is also observable (as $\tilde{\Gamma} = \Gamma$). Hence, we have that for all $k \geq n$, $O_k \tilde{x}(0) \neq 0$. Therefore, due to (25), we have that

$$\tilde{U}_u(k) \neq 0 \qquad \forall\, k \geq n \quad \implies \exists\, \tilde{U}_u \neq 0.$$

Next, we show that for all $\tilde{\Gamma}$ that satisfy $\text{Range}\left(\begin{bmatrix} \tilde{B}^T & \tilde{D}^T \end{bmatrix}^T\right) \supseteq \text{Range}\left(\begin{bmatrix} B^T & D^T \end{bmatrix}^T\right)$ (this includes $\tilde{\Gamma} = \Gamma$), it holds that $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$ (and thus, there exists $\tilde{U}_u \neq 0$ as shown above). Since $\mathcal{V}(\Gamma) \neq \{0\}$, there exist $x(0) \neq 0$ and $U(n-1)$ satisfying:

$$Y_{x(0),U_{n-1}} = O_{n-1} x(0) + F_{n-1}^\Gamma U(n-1) = 0. \tag{26}$$

Through matrix manipulations, we get:

$$F_{n-1}^\Gamma = \begin{cases} \begin{bmatrix} (I_n \otimes C)(\hat{F}_{n-1}) & I_{nm} \end{bmatrix} \begin{bmatrix} I_n \otimes B \\ I_n \otimes D \end{bmatrix} & \text{for } n > 1, \\ \begin{bmatrix} 0 & I_{nm} \end{bmatrix} \begin{bmatrix} I_n \otimes B \\ I_n \otimes D \end{bmatrix} & \text{for } n = 1, \end{cases}$$

where $\hat{F}_{n-1}$ is equal to F_{n-1}^Γ in (6) with $B = C = I_n$ and $D = 0$. Further manipulations yield:

$$\begin{bmatrix} I_n \otimes B \\ I_n \otimes D \end{bmatrix} = \begin{bmatrix} I_{n(n+m)} & P & \cdots & P^{n-1} \end{bmatrix} \left[I_n \otimes \left(T \begin{bmatrix} B \\ D \end{bmatrix} \right) \right],$$

where P is a $n(n+m) \times n(n+m)$ permutation matrix and T is a $n(n+m) \times (n+m)$ matrix, defined as:

$$P = \begin{bmatrix} 0 & I_m \\ I_{n^2+(n-1)m} & 0 \end{bmatrix}, T = \begin{bmatrix} \underbrace{\begin{matrix} I_n & 0 \\ 0 & 0 \end{matrix}}_{n^2} & \underbrace{\begin{matrix} 0 & 0 \\ I_m & 0 \end{matrix}}_{nm} \end{bmatrix}^T.$$

Next, we consider the fact that for any matrices M, Q, W, $\text{Range}(M) \supseteq \text{Range}(Q)$ implies (i) $\text{Range}(WM) \supseteq \text{Range}(WQ)$, and (ii) $\text{Range}(I_n \otimes M) \supseteq \text{Range}(I_n \otimes Q)$. Using these, we have:

$$\begin{aligned} & \text{Range}\left(\begin{bmatrix} \tilde{B} \\ \tilde{D} \end{bmatrix}\right) \supseteq \text{Range}\left(\begin{bmatrix} B \\ D \end{bmatrix}\right) \\ \implies \quad & \text{Range}\left(\begin{bmatrix} I_n \otimes \tilde{B} \\ I_n \otimes \tilde{D} \end{bmatrix}\right) \supseteq \text{Range}\left(\begin{bmatrix} I_n \otimes B \\ I_n \otimes D \end{bmatrix}\right) \\ \implies \quad & \text{Range}\left(F_{n-1}^{\tilde{\Gamma}}\right) \supseteq \text{Range}\left(F_{n-1}^{\Gamma}\right). \end{aligned} \tag{27}$$

Equation (27) implies that there exists a $\tilde{U}(n-1)$ that satisfies, $F_{n-1}^{\tilde{\Gamma}} \tilde{U}(n-1) = F_{n-1}^{\Gamma} U(n-1)$. Substituting this, and $\tilde{x}(0) = x(0) \neq 0$ in (26), we have:

$$Y_{\tilde{x}(0),\tilde{U}(n-1)} = O_{n-1} \tilde{x}(0) + F_{n-1}^{\tilde{\Gamma}} \tilde{U}(n-1) = 0,$$

which implies $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$ (c.f. Definition 4).

D. Proof of Theorem 3

Statement 1(a): Note that the condition $\mathcal{X}^1(0) \subset \mathcal{X}^2(0)$ implies $\mathcal{X}^1(k) \subseteq \mathcal{X}^2(k)$. Therefore, since $\mathcal{X}^1(k) \subseteq \mathcal{X}^2(k)$ and $\mathcal{X}_{s,k}^1 \xrightarrow{\text{kso}} \left(\mathcal{X}^1(k) \backslash \mathcal{X}_{s,k}^1\right)$, we have that $\mathcal{X}_{s,k}^1 \xrightarrow{\text{kso}} \left(\mathcal{X}^2(k) \backslash \mathcal{X}_{s,k}^1\right)$. Hence, if we form the set $\mathcal{X}_{s,k}^2 \subset \mathcal{X}^2(k)$ as $\mathcal{X}_{s,k}^2 = \mathcal{X}_{s,k}^1$, we have that $\mathcal{X}_{s,k}^2$ is KSO and $\mathcal{X}_{s,k}^1 \subseteq \mathcal{X}_{s,k}^2(k)$.

Statement 1(b): Only if: We prove by contrapositive argument. The contrapositive of Statement 1(b) is: If there does not exist $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ that satisfies

$$(x(k) \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) \neq \{x(k)\},$$

then there does not exist $\mathcal{X}_{s,k}^2 \supset \mathcal{X}_{s,k}^1$ that is KSO.

This is equivalent to the following statement: If every $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ satisfies:

$$(x(k) \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) = \{x(k)\}, \tag{28}$$

then there does not exist $\mathcal{X}_{s,k}^2 \supset \mathcal{X}_{s,k}^1$ that is KSO.

In the following, we prove the above statement. If $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ is chosen as a non-secret state, it will not add any KSO secret states (since $\mathcal{X}_{s,k}^1$ is KSO). Therefore, let us consider $x(k)$ to be a new secret state $x_{s,k}^{\text{new}}$ that is KSO. Hence, the proxy non-secret state $x_{ns,k}$ must be in the set specified by Corollary 2, that is,

$$x_{ns,k} \in (x_{s,k}^{\text{new}} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) = \{x_{s,k}^{\text{new}}\} \text{ (due to (28))}.$$

However, this is not possible since $x_{s,k}^{\text{new}}$ and $x_{ns,k}$ must be different. Thus, if $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ is taken as a secret state, it will not be KSO. Therefore, $\mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ does not add any KSO secret states beyond what was present in $\mathcal{X}^1(k)$.

Finally, note that Statement 1(b) holds for each KSO secret set. Hence, the other option of constructing a larger KSO secret set from $\mathcal{X}^1(k)$ by converting a non-secret state in $\mathcal{X}^1(k)$ to a secret state is also not possible. This is because if this is done, then the largest KSO secret set in $\mathcal{X}^1(k)$ will no longer be KSO.

If: Since there exists $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ for which

$$(x(k) \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) \neq \{x(k)\},$$

we have that there exists $x'(k) \neq x(k)$ for which

$$x'(k) \in (x(k) \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k). \tag{29}$$

The state $x'(k)$ belongs in either the set $\mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ or the set $\mathcal{X}^1(k)$. We consider these two cases separately:

Case 1: $x'(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$

If $x(k)$ and $x'(k)$ are chosen as a new secret and a non-secret state, respectively, that is, $x(k) = x^{\text{new}}_{s,k}$ and $x'(k) = x_{ns,k}$, then due to (29), $x^{\text{new}}_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$ (c.f. Corollary 2).

Case 2: $x'(k) \in \mathcal{X}^1(k)$

In this case, $x'(k)$ is either a non-secret state or a KSO secret state in the set $\mathcal{X}^1(k)$ (since $\mathcal{X}^1(k)$ is KSO). These two sub-cases are analyzed below:

Sub-case (i): $x'(k) = x_{ns,k} \in \mathcal{X}^1(k)$

Here, if $x(k)$ is chosen as a new secret state $x^{\text{new}}_{s,k}$, then, due to (29), we have that $x^{\text{new}}_{s,k} \xrightarrow{\text{kso}} \{x_{ns,k}\}$ (c.f. Corollary 2).

Sub-case (ii): $x'(k) = x_{s,k} \in \mathcal{X}^1_{s,k}$

Let $x(k)$ be chosen as a new secret state, denoted by $x^{\text{new}}_{s,k}$. Also, let us denote the secret state $x'(k)$ by $x^1_{s,k}$. By (29),

$$x^1_{s,k} \in (x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k). \tag{30}$$

Further, since $x^1_{s,k}$ is KSO, there exists a proxy $x^1_{ns,k} \in \mathcal{X}^1_{ns,k}$ that satisfies

$$x^1_{ns,k} \in (x^1_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^1(k). \tag{31}$$

Finally, in order to make $x^{\text{new}}_{s,k}$ KSO, there should exist a proxy non-secret state $x_{ns,k}$ that satisfies

$$x_{ns,k} \in (x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k). \tag{32}$$

In the following, we show that the non-secret state $x^1_{ns,k} \in \mathcal{X}^1_{ns,k}$ can acts as proxy for $x^{\text{new}}_{s,k}$ by satisfying (32). We use (30) and (31) to obtain:

$$\begin{aligned}
&(x^1_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^1(k) \\
&\subseteq \Big(\Big((x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k) \Big) \oplus \mathcal{T}_{k,K}(\Gamma) \Big) \cap \mathcal{X}^1(k) \\
&\subseteq \big((x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \oplus \mathcal{T}_{k,K}(\Gamma) \big) \cap \mathcal{X}^1(k) \\
&= (x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^1(k).
\end{aligned} \tag{33}$$

Due to (31) and (33), we have that

$$\begin{aligned}
x^1_{ns,k} &\in (x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^1(k) \\
&\subseteq (x^{\text{new}}_{s,k} \oplus \mathcal{T}_{k,K}(\Gamma)) \cap \mathcal{X}^2(k).
\end{aligned}$$

Hence, we have that $x^1_{ns,k}$ satisfies (32) and $x^1_{ns,k} \in \mathcal{X}^1_{ns,k}$. Therefore, $x^1_{ns,k}$ exists in $\mathcal{X}^1(k)$ such that $x^{\text{new}}_{s,k} \xrightarrow{\text{kso}} \{x^1_{ns,k}\}$.

Note that in all the cases above, $\mathcal{X}^1(0) = \mathcal{B}(\mathcal{X}^1(k))$ ensures that for all output sequences produced by the system to reach $x^{\text{new}}_{s,k}$ (with some initial states and input sequences), there exist initial states in $\mathcal{X}^1(0)$ (and also $\mathcal{X}^2(0)$) such that the system reaches $x^1_{ns,k}$ while producing the same outputs (with corresponding input sequences).

In all the former cases, it is seen that there exists $x(k) \in \mathcal{X}^2(k) \backslash \mathcal{X}^1(k)$ that can be chosen as a KSO secret state. This implies that there is an addition of a KSO secret state due to expansion of $\mathcal{X}^1(k)$ to $\mathcal{X}^2(k)$. Hence, $\mathcal{X}^2_{s,k} \supset \mathcal{X}^1_{s,k}$.

Statement 2(a): We have by Lemma 9 that:

$$\mathcal{X}^1(0) \subset \mathcal{X}^2(0) \implies \tilde{\mathcal{U}}^1_u(k) \subseteq \tilde{\mathcal{U}}^2_u(k) \, \forall \, k \geq 0.$$

Statement 2(b): We have that $\tilde{\mathcal{U}}^1_u \subset \tilde{\mathcal{U}}^2_u$ if and only if there exists $\tilde{U}^2_u \in (\mathbb{R}^{(k+1)p} \backslash \tilde{\mathcal{U}}^1_u)$ such that for all $k \geq 0$,

$$F^{\tilde{\Gamma}}_k T_k[\tilde{U}^2_u] \in O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \quad \text{(c.f. Lemma 9)},$$

and there exists some k_0 such that for all $k \geq k_0$,

$$F^{\tilde{\Gamma}}_k T_k[\tilde{U}^2_u] \notin O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big) \quad \text{(c.f. Lemma 9)}.$$

The above is equivalent to the fact that there exists some k_0 such that for all $k \geq k_0$,

$$F^{\tilde{\Gamma}}_k T_k[\tilde{U}^2_u] \in \Big(O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \backslash O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big) \Big),$$

which is again equivalent to: $\text{Range}(F^{\tilde{\Gamma}}_k) \cap \Big(O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \backslash O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big) \Big) \neq \phi$. Since $O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \supseteq O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big)$, we have that the above is equivalent to:

$$\begin{aligned}
&\text{Range}(F^{\tilde{\Gamma}}_k) \cap O_k\Big(\mathcal{X}^2(0) \oplus -\mathcal{X}^2(0)\Big) \supset \\
&\text{Range}(F^{\tilde{\Gamma}}_k) \cap O_k\Big(\mathcal{X}^1(0) \oplus -\mathcal{X}^1(0)\Big).
\end{aligned}$$

Statement 2(c). If $\tilde{\Gamma}$ is chosen such that $\tilde{D}$ is square full rank, then $F^{\tilde{\Gamma}}_k$ is also square and full rank for all $k \geq 0$ (minimum rank of lower triangular matrix is sum of rank of diagonal blocks). Therefore,

$$\tilde{\mathcal{U}}_u(k) = \left(F^{\tilde{\Gamma}}_k\right)^{-1} O_k(\mathcal{X}(0) \oplus -\mathcal{X}(0)) \, \forall \, k \geq 0.$$

Consequently, since $\tilde{\Gamma}$ is observable (by Assumption 4), it holds that:

$$\mathcal{X}^1(0) \subset \mathcal{X}^2(0) \implies \tilde{\mathcal{U}}^1_u(k) \subset \tilde{\mathcal{U}}^2_u(k) \, \forall \, k \geq n.$$

Note that Statement 2(c) also follows from Statement 2(b) because both O_k and $F^{\tilde{\Gamma}}_k$ are full rank when $\tilde{D}$ is square and full rank. Consequently, Statement 2(b) holds in this case.

E. Proof of Lemma 8

$\mathcal{S}_1$ cannot be equal to $\mathcal{S}_2 \oplus \mathcal{W}$. This is because if it were equal, there will exist some state s in both $\mathcal{S}_1$ and $\mathcal{S}_2$, which is not possible since these sets are disjoint.

Let W be a matrix whose columns form a basis of $\mathcal{W}$. Since $\mathcal{S}_1 \neq \mathcal{S}_2 \oplus \mathcal{W}$, we have that $\mathcal{S}_1 \subset \mathcal{S}_2 \oplus \mathcal{W}$ is equivalent to the fact that for all $s_1 \in \mathcal{S}_1$, there exists $s_2 \in \mathcal{S}_2$ and vector w such that $s_1 = s_2 + Ww \iff s_1 - s_2 \in \text{Range}(W)$. This is again equivalent to $P_{\mathcal{W}^\perp}(s_1 - s_2) = 0 \iff P_{\mathcal{W}^\perp} s_1 = P_{\mathcal{W}^\perp} s_2 \iff P_{\mathcal{W}^\perp} \mathcal{S}_1 \subseteq P_{\mathcal{W}^\perp} \mathcal{S}_2$.

REFERENCES

[1] D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum, 50(3):48-53, 2013.

[2] R. M. Lee, M. J. Assante and T. Conway, "Analysis of the Cyber Attack on the Ukraine Power Grid," [Online] Available: https://ics.sans.org/duc5, Accessed: November, 2023.

[3] Y. Lu and M. Zhu, "A Control-theoretic Perspective on Cyber-physical Privacy: Where Data Privacy Meets Dynamic Systems," Annual Reviews in Control, 47:423-440, 2019.

[4] L. Mazaré, "Using Unification for Opacity Properties," Workshop on Issues in the Theory of Security, pp. 165–176, 2004.

[5] J. W. Bryans, M. Koutny and P. Y. A. Ryan, "Modelling Opacity Using Petri Nets," Electronic Notes in Theoretical Computer Science, 121:101–115, 2005.

[6] B. Ramasubramanian, R. Cleaveland and S. I. Marcus, "Notions of Centralized and Decentralized Opacity in Linear Systems," IEEE Transactions on Automatic Control, 65(4):1442-1455, 2020.

[7] L. An and G. Yang, "Opacity Enforcement for Confidential Robust Control in Linear Cyber-Physical Systems," IEEE Transactions on Automatic Control, 65(3):1234-1241, 2020.

[8] L. An and G. Yang, "Enhancement of Opacity for Distributed State Estimation in Cyber–Physical Systems," Automatica, vol. 136, 2022.

[9] X. Yin, M. Zamani and S. Liu, "On Approximate Opacity of Cyber-Physical Systems," IEEE Transactions on Automatic Control, 66(4):1630-1645, 2021.

[10] A. Bourouis, K. Klai, Y. El Touati and N. B. Hadj-Alouane, "Opacity Preserving Abstraction for Web Services and Their Composition Using SOGs," IEEE International Conference on Web Services, pp. 313-320, 2015.

[11] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson and A. Chakrabortty, "A Systems and Control Perspective of CPS Security," Annual Reviews in Control, 47:394-411, 2019.

[12] J. Giraldo et al., "A Survey of Physics-Based Attack Detection in Cyber-Physical Systems," ACM Computing Surveys, 51(4):1-36, 2018.

[13] F. Pasqualetti, F. Dörfler and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," IEEE Transactions on Automatic Control, 58(11):2715-2729, 2013.

[14] A. Saboori and C. N. Hadjicostis, "Notions of Security and Opacity in Discrete Event Systems," IEEE Conference on Decision and Control, pp. 5056-5061, 2007.

[15] S. Liu and M. Zamani, "Verification of Approximate Opacity via Barrier Certificates," IEEE Control Systems Letters, 5(4):1369-1374, 2021.

[16] S. Liu, A. Trivedi, X. Yin and M. Zamani, "Secure-by-construction Synthesis of Cyber-Physical Systems," Annual Reviews in Control, 53:30-50, 2022.

[17] B. Zhong, S. Liu, M. Caccamo and M. Zamani, "Secure-by-Construction Controller Synthesis via Control Barrier Functions," IFAC-PapersOnLine, 56(2):239-245, 2023.

[18] B. Molinari, "Extended Controllability and Observability for Linear Systems," IEEE Transactions on Automatic Control, 21(1):136-137, 1976.

[19] B. Molinari, "A Strong Controllability and Observability in Linear Multivariable Control," IEEE Transactions on Automatic Control, 21(5):761-764, 1976.

[20] F. Hamano, G. Basile, "Unknown-Input Present-State Observability of Discrete-Time Linear Systems," Journal of Optimization Theory and Applications, 40:293–307, 1983.

[21] S. Hara, "Observability and Dead-Beat Observers for Discrete-Time Linear Systems With Unknown Inputs," IFAC Symposium on Theory and Application of Digital Control, 15(1):173-178, 1982.

[22] Y. Kawano and M. Cao, "Revisit Input Observability: A New Approach to Attack Detection and Privacy Preservation," IEEE Conference on Decision and Control, pp. 7095-7100, 2018.

[23] J. Giraldo, A. A. Cardenas and M. Kantarcioglu, "Security vs. Privacy: How Integrity Attacks can be Masked by the Noise of Differential Privacy," IEEE American Control Conference, pp. 1679-1684, 2017.

[24] V. Katewa, R. Anguluri and F. Pasqualetti, "On a Security vs Privacy Trade-off in Interconnected Dynamical Systems," Automatica, vol. 125, 2021.

[25] K. Sun, I. Esnaola, S. M. Perlaza and H. V. Poor, "Stealth Attacks on the Smart Grid," IEEE Transactions on Smart Grid, 11(2):1276-1285, 2020.

[26] R. Jin, X. He and H. Dai, "On the Security-Privacy Tradeoff in Collaborative Security: A Quantitative Information Flow Game Perspective," IEEE Transactions on Information Forensics and Security, 14(12):3273-3286, 2019.

[27] V. M. John and V. Katewa, "Opacity and its Trade-offs with Security in Linear Systems," IEEE Conference on Decision and Control, pp. 5443-5449, 2022.

[28] N. Natario, "Smart Thermostat Owners Might Find Their Temperatures Rising During Concerning Heat Wave in Texas", [Online] Available: https://abc13.com/smart-thermostats-disable-lower-temperatures-texas-energy-conservation-heat-wave/12059404/, Accessed: November, 2023.

[29] H. L. Trentelman, A. A. Stoorvogel and M. Hautus, "Control Theory for Linear Systems," Springer, ch. 7, 2001.

[30] Y. Chen, S. Kar and J. M. F. Moura, "Dynamic Attack Detection in Cyber-Physical Systems With Side Initial State Information," IEEE Transactions on Automatic Control, 62(9):4618-4624, 2017.

[31] L. Fridman, J. Davila and A. Levant, "High-Order Sliding-Mode Observation and Fault Detection via Weakly Unobservable Subspace Reconstruction," European Control Conference, pp. 5139-5146, 2007.

[32] P. Gope and B. Sikdar, "Lightweight and Privacy-Friendly Spatial Data Aggregation for Secure Power Supply and Demand Management in Smart Grids," in IEEE Transactions on Information Forensics and Security, 14(6):1554-1566, 2019.

[33] Z. Guan, G. Si, X. Du, P. Liu, Z. Zhang and Z. Zhou, "Protecting User Privacy Based on Secret Sharing With Fault Tolerance for Big Data in Smart Grid," IEEE International Conference on Communications, pp. 1-6, 2017.

Varkey M. John (Member, IEEE) received a dual degree of bachelor's in electrical and electronics engineering and master's in economics from BITS-Pilani (Goa Campus), Goa, India, in 2017, and he received the M.Tech. (Res.) degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, India, in 2023.

He is currently a Graduate Research Assistant at the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. His research interests include security and privacy of cyber-physical systems, game theory and reinforcement learning.

Vaibhav Katewa (Member, IEEE) received the bachelor's degree in electrical engineering from the Indian Institute of Technology Kanpur, Kanpur, India, in 2007, and the M.S. and Ph.D. degrees in electrical engineering from the University of Notre Dame, Notre Dame, IN, USA, in 2012 and 2016, respectively.

He is currently an Assistant Professor with the Robert Bosch Center for Cyber Physical Systems with a joint appointment with the Department of Electrical Communication Engineering, Indian Institute of Science, Bengaluru, India. From 2017 to 2019, he was a Postdoctoral Scholar with the Department of Mechanical Engineering, University of California, Riverside. His research interests include analysis and design of security and privacy methods for cyber-physical systems and complex networks, decentralized and sparse feedback control, and protocol design for networked control systems.