2022 IEEE 61st Conference on Decision and Control (CDC)
December 6-9, 2022. Cancún, Mexico

Opacity and its Trade-offs with Security in Linear Systems

Varkey M. John and Vaibhav Katewa

2022 IEEE 61st Conference on Decision and Control (CDC) | 978-1-6654-6761-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CDC51059.2022.9992537

***Abstract*— Opacity and attack detectability are important properties for any system as they allow the states to remain private and malicious attacks to be detected, respectively. In this paper, we show that a fundamental trade-off exists between these properties for a linear dynamical system, in the sense that one cannot have an opaque system without making it vulnerable to undetectable attacks. We first characterize the opacity conditions for the system in terms of its weakly unobservable subspace (WUS) and show that the number of opaque states is proportional to the size of the WUS. Further, we establish conditions under which increasing the opaque sets also increases the set of undetectable attacks. This highlights a fundamental trade-off between security and privacy. We demonstrate our results on a team of delivery UAVs.**

I. Introduction

Cyber-physical attacks have become significantly prevalent in recent years, including the Stuxnet attack (2010) and the Maroochy Shire attack (2000) [1], [2]. Due to such vulnerabilities, there has been a larger thrust in the last decade to enable these systems to detect attacks upfront [3], [4]. Such detection mechanisms are especially relevant since traditional cyber-security solutions are not suitable to detect real-time physics-based attacks.

In parallel, increased demand for privacy has led to a focus on keeping information from Cyber-Physical Systems (CPS) confidential. In particular, the notion of opacity, which was first considered in the computer science literature with discrete events [5], [6], has been applied to CPS and dynamical systems with continuous state space in recent years [7]–[10]. Informally, opacity requires that same outputs should be produced by secret as well as a non-secret initial states. This prevents an eavesdropper to distinguish whether the system was initialized in a secret or a non-secret state based on the outputs. This indistinguishability is important since the knowledge of the system's initial state may enable an eavesdropper to perform targeted attacks on the system. For instance, consider the application of goods delivery using UAVs. Information about the starting location (warehouse) of a UAV can reveal the type of goods being transported (expensive vs. cheap), and this can be used by the attacker to attack only those UAVs that carry expensive items. Opacity is used in other real-world applications as well, for instance, to keep web services private [11].

Previous works have considered various frameworks and approaches to characterize opacity in CPS. In [7], the authors developed the notion of opacity for linear dynamical systems and established its relation to other system properties like output controllability. A relaxed notion of "approximate opacity" was developed in [8], 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 [9] and [10], respectively.

While research on security and privacy have produced a large spectrum of results individually, studies that assess the impact of security on privacy, and vice-versa, are fairly limited. Given that the goals, the information availability, and the mechanisms of the attacker and the eavesdropper are different, one may opine that security and privacy of a system are unrelated. Contrary to this, we show that a fundamental connection and trade-off exists between these two notions. Closely aligned to our work, the authors in [12] show that attack detection and differential privacy are linked to the system property called "input observability". In [13], 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 [14]. The security-privacy trade-off has also been evaluated from an information-theoretic standpoint in [15], and the authors in [16] 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. To the best of our knowledge, this is the first work to investigate connections between opacity and attack detectability. The main contributions of this paper are:

1. We characterize the fundamental relation between opacity and the Weakly Unobservable Subspace (WUS), and use this to derive conditions for opacity of initial states.
2. 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 team of delivery UAVs.

Notation: $\mathcal{R}(A)$ denotes the range space of matrix A. $A \bigotimes B$ represents Kronecker product of matrices A and B. For matrix A and set $\mathcal{S}$, $A\mathcal{S} = \{As : s \in \mathcal{S}\}$. $\mathcal{S}_1 \bigoplus \mathcal{S}_2$ represents the Minkowski sum of sets $\mathcal{S}_1$ and $\mathcal{S}_2$. $\mathcal{S}_1 \backslash \mathcal{S}_2$ denotes the set difference operation. I_m denotes the identity matrix of size $m \times m$. ϕ denotes the empty set.

V. M. John is with the Department of ECE at the Indian Institute of Science (IISc) Bangalore. He is supported by a fellowship grant from the Cisco Centre for Networked Intelligence at IISc. V. Katewa is with the Robert Bosch Center for CPS and Department of ECE at IISc Bangalore. Email IDs: {varkeym@iisc.ac.in, vkatewa@iisc.ac.in}

II. System, Opacity, and Attack Models

System Model: We consider a discrete-time linear time-invariant system under normal (unattacked) operation (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 $\mathcal{X}_0$ be the set of initial states in which the system is allowed to begin. We assume $\mathcal{X}_0 = \mathbb{R}^n$ unless otherwise stated. Let $U(k) = \begin{bmatrix} u(0)^T & u(1)^T & \dots & u(k)^T \end{bmatrix}^T$ denote the input sequence (represented as a vector) until time instant k. 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:

$$Y_{x(0),U(k)} = O_k x(0) + F_k^{\Gamma} U(k), \tag{2}$$

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

$$O_k = \begin{bmatrix} C^T & (CA)^T & \dots & (CA^k)^T \end{bmatrix}^T \quad \text{for } k \geq 0, \tag{3}$$

$$F_k^{\Gamma} = \begin{bmatrix} D & 0 & \dots & 0 \\ CB & D & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ CA^{k-1}B & CA^{k-2}B & \dots & D \end{bmatrix} \quad \text{for } k \geq 1, \tag{4}$$

and $F_0^{\Gamma} = D$. We assume that system Γ is observable.

Opacity Model: We consider that there exists a set of secret initial states, denoted by $\mathcal{X}_s$ ($\mathcal{X}_s \subseteq \mathcal{X}_0$), that a system operator wishes to keep private from external entities. The remaining set of non-secret initial states is denoted by $\mathcal{X}_{ns} = \mathcal{X}_0 \backslash \mathcal{X}_s$. Any element of $\mathcal{X}_{ns}$ is not considered sensitive to disclosure. We use $x_s(0)$ and $x_{ns}(0)$ to denote individual elements in $\mathcal{X}_s$ and $\mathcal{X}_{ns}$, respectively.

We consider a potential eavesdropper present in the system whose goal is to determine whether the system initialized from secret initial state set or non-secret set, using the outputs. We assume that the eavesdropper knows the system matrices A, B, C, D, and the initial state sets $\mathcal{X}_s$ and $\mathcal{X}_{ns}$. 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).

Definition 1 (*Opacity of Initial States*)**.** A secret initial state $x_s(0) \in \mathcal{X}_s$ is opaque with respect to a non-secret initial state set $\mathcal{X}'_{ns} \subseteq \mathcal{X}_{ns}$, if, for all $k \geq 0$, the following property holds: for every $U_s(k)$, there exist $x_{ns}(0) \in \mathcal{X}'_{ns}$ and $U_{ns}(k)$ such that

$$Y_{x_s(0),U_s(k)} = Y_{x_{ns}(0),U_{ns}(k)}.$$

We denote this relation by $x_s(0) \overset{\text{o}}{\to} \mathcal{X}'_{ns}$ and sometimes use the term opaque for such $x_s(0)$. □

The opacity definition implies that the same output sequence can result from either a secret or a non-secret initial state (with appropriate control input sequences). Therefore, the eavesdropper who observes the output sequence cannot distinguish whether the system started from a secret or non-secret initial state. This makes the secret initial state opaque. Next, we present opacity definitions for sets.

Definition 2 (*Opacity of Sets*)**.** The secret initial state set $\mathcal{X}_s$ is opaque with respect to non-secret initial state set $\mathcal{X}'_{ns} \subseteq \mathcal{X}_{ns}$, if, for every $x_s(0) \in \mathcal{X}_s$, it holds that $x_s(0) \overset{\text{o}}{\to} \mathcal{X}'_{ns}$. We denote this relation by $\mathcal{X}_s \overset{\text{o}}{\to} \mathcal{X}'_{ns}$ and sometimes use the term opaque for such $\mathcal{X}_s$. □

Remark 1. The above definitions are also referred to as "initial state opacity" in some papers (e.g., definition III.1 in [8]). Further, these definitions differ from the definitions of $\mathcal{K}$-ISO used in [7], 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 [7], 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 since it is the widely accepted definition in the discrete event systems literature [6], [8]. □

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 $\mathcal{X}_s^1$ and $\mathcal{X}_s^2$, we say $\mathcal{X}_s^1$ is *more opaque* than $\mathcal{X}_s^2$ if $\mathcal{X}_s^2 \subset \mathcal{X}_s^1$. □

Attack Model: We consider an attacker[1] 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 by 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:

$$\tilde{\Gamma}: \quad \begin{aligned} \tilde{x}(k+1) &= A\tilde{x}(k) + \tilde{B}\tilde{u}(k), \\ \tilde{y}(k) &= C\tilde{x}(k) + \tilde{D}\tilde{u}(k), \end{aligned} \tag{5}$$

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 $\tilde{U}(k) = \begin{bmatrix} \tilde{u}(0)^T & \tilde{u}(1)^T & \dots & \tilde{u}(k)^T \end{bmatrix}^T$ 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 can be expressed as:

$$\tilde{Y}_{x(0),\tilde{U}(k)} = O_k x(0) + F_k^{\tilde{\Gamma}} \tilde{U}(k), \tag{6}$$

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 (4). 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[2] that determines whether the system is under attack or not by using

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

[2]The attack detector is a dynamic detector as defined in [4], which operates on the entire output sequences.

the outputs. However, all attacks may not be detected, and next, we present the definition for undetectable attacks.

Definition 4 (*Undetectable Attacks* [4])**.** 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 $\tilde{U}_u(k) = \begin{bmatrix}\tilde{u}_u(0)^T & \tilde{u}_u(1)^T & \dots & \tilde{u}_u(k)^T\end{bmatrix}^T$ 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 whether the system is under attack or not. The existence of undetectable attacks depends on the weakly unobservable subspace of the system, which we define next.

Definition 5 (*Weakly Unobservable Subspace (WUS)* [17])**.** The weakly unobservable subspace of system (1) (denoted by $\mathcal{V}(\Gamma)$) is defined as:

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

where the second equality follows from the Cayley-Hamilton Theorem. □

The subspace $\mathcal{V}(\tilde{\Gamma})$ of the attacked system is fundamentally connected to existence of undetectable attacks. In particular, it is known that if $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$, then there exists an undetectable attack $\tilde{U}_u$ [3], [17]. In the next section, we show that $\mathcal{V}(\Gamma)$ of the normal system is connected to the opacity, and use this fact to characterize the trade-off between opacity and attack detectability in Section IV.

III. Characterization of Opaque Sets

We begin by characterizing the condition for existence of opaque sets.

Lemma 1. *There exists an opaque set $\mathcal{X}_s$ for System Γ in* (1) *if and only if $\mathcal{V}(\Gamma) \neq \{0\}$.*

Proof. Suppose there exist a set $\mathcal{X}_s$ which is opaque with respect to $\mathcal{X}_{ns} = \mathbb{R}^n \backslash \mathcal{X}_s$. From Definition 2, we observe that existence of $\mathcal{X}_s$ is equivalent to existence of a distinct $x_s(0)$ and $x_{ns}(0)$ such that $x_s(0) \overset{o}{\to} \{x_{ns}(0)\}$. This is equivalent to saying that for any $U_s(k)$, there exists a $U_{ns}(k)$, such that

$$\begin{aligned}& Y_{x_s(0),U_s(k)} = Y_{x_{ns}(0),U_{ns}(k)} && \forall\, k \geq 0 \\ \iff\quad & Y_{x_s(0)-x_{ns}(0),U_s(k)-U_{ns}(k)} = 0 && \forall\, k \geq 0 \\ \iff\quad & \exists\, U(k), x(0) \neq 0 : Y_{x(0),U(k)} = 0 && \forall\, k \geq 0 \\ \iff\quad & \mathcal{V}(\Gamma) \neq \{0\},\end{aligned}$$

where the last statement follows from Definition 5. □

Lemma 1 highlights a fundamental connection between opacity and WUS $\mathcal{V}(\Gamma)$ for linear systems, and shows that a non-zero $\mathcal{V}(\Gamma)$ 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.

Lemma 2. *Let $\mathcal{X}_0 \subseteq \mathbb{R}^n$. Given two different initial states $x_s(0) \in \mathcal{X}_s$ and $x_{ns}(0) \in \mathcal{X}_{ns}$, we have $x_s(0) \overset{o}{\to} \{x_{ns}(0)\}$ if and only if $x_s(0) - x_{ns}(0) \in \mathcal{V}(\Gamma)$.*

Proof. Refer to the proof of Lemma 1. □

Corollary 1. *Let $\mathcal{X}_0 \subseteq \mathbb{R}^n$. The following two statements hold true:*
1. Given $x_s(0)$, a state $x_{ns}(0) \neq x_s(0)$ satisfies $x_s(0) \overset{o}{\to} \{x_{ns}(0)\}$ if and only if $x_{ns}(0) \in x_s(0) \bigoplus \mathcal{V}(\Gamma)$.
2. Given $x_{ns}(0)$, a state $x_s(0) \neq x_{ns}(0)$ satisfies $x_s(0) \overset{o}{\to} \{x_{ns}(0)\}$ if and only if $x_s(0) \in x_{ns}(0) \bigoplus \mathcal{V}(\Gamma)$.

Lemma 2 provides the necessary and sufficient condition for opacity of an initial state, and shows that it is fundamentally connected, and completely determined by $\mathcal{V}(\Gamma)$. Further, Corollary 1 shows that the set of non-secret states that makes a secret state opaque (and vice-versa) is constrained by $\mathcal{V}(\Gamma)$. Next, we extend these results to specify conditions for opacity of *sets* of initial states.

Lemma 3. *Let $\mathcal{X}_0 \subseteq \mathbb{R}^n$. Given non-empty and disjoint sets $\mathcal{X}_s$ and $\mathcal{X}'_{ns} \subseteq \mathcal{X}_{ns}$, we have $\mathcal{X}_s \overset{o}{\to} \mathcal{X}'_{ns}$ if and only if $\mathcal{X}_s \subset \mathcal{X}'_{ns} \bigoplus \mathcal{V}(\Gamma)$.*

Proof. If: The condition $\mathcal{X}_s \subset \mathcal{X}'_{ns} \bigoplus \mathcal{V}(\Gamma)$ implies that for any $x_s(0) \in \mathcal{X}_s$, there exists a $x_{ns}(0) \in \mathcal{X}'_{ns}$ satisfying:

$$\begin{aligned}& x_s(0) \in x_{ns}(0) \bigoplus \mathcal{V}(\Gamma) \\ \iff\quad & x_s(0) \overset{o}{\to} \{x_{ns}(0)\} \quad \text{(by Corollary 1).}\end{aligned}$$

Since the above statement holds true for any $x_s(0) \in \mathcal{X}_s$, we have $\mathcal{X}_s \overset{o}{\to} \mathcal{X}'_{ns}$.

Only if: We prove this part via contradiction. We will show that the condition $\mathcal{X}_s \supseteq \mathcal{X}'_{ns} \bigoplus \mathcal{V}(\Gamma)$ implies that the sets $\mathcal{X}_s$ and $\mathcal{X}'_{ns}$ cannot be disjoint. Splitting $\mathcal{V}(\Gamma)$, we get:

$$\begin{aligned}& \mathcal{X}_s \supseteq \mathcal{X}'_{ns} \bigoplus \big(\{0\} \cup (\mathcal{V}(\Gamma) \backslash \{0\})\big) \\ \overset{(a)}{\implies}\quad & \mathcal{X}_s \supseteq \big(\mathcal{X}'_{ns} \bigoplus \{0\}\big) \cup \big(\mathcal{X}'_{ns} \bigoplus (\mathcal{V}(\Gamma) \backslash \{0\})\big) \\ \implies\quad & \mathcal{X}_s \supseteq \big(\mathcal{X}'_{ns} \bigoplus \{0\}\big) = \mathcal{X}'_{ns} \\ \implies\quad & \mathcal{X}_s \cap \mathcal{X}'_{ns} \neq \phi,\end{aligned}$$

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

Same as before, the conditions in Lemma 3 are completely dependent on $\mathcal{V}(\Gamma)$.

Remark 2 (*Verifying Opacity Conditions*). The verification of opacity conditions in Lemma 3 requires computation of Minkowski sum of sets. Algorithms to compute these for polytope sets in $\mathbb{R}^n$ are well developed in the literature, e.g., [18], [19]. Also, Minkowski sum of an arbitrary set and a subspace can be computed by using the basis vectors of the subspace. An algorithm to find a basis for $\mathcal{V}(\Gamma)$ is given in [20]. The exact computation of these sets is not the focus of this paper and we defer this for future work. □

Next, we analyze the effect of changing the subspace $\mathcal{V}(\Gamma)$ on the opaque sets.

Theorem 1. *Consider two systems Γ_1 and Γ_2. For any opaque set $\mathcal{X}_s^1$ in Γ_1, there exists a more opaque set $\mathcal{X}_s^2$ in Γ_2 if and only if $\mathcal{V}(\Gamma_1) \subset \mathcal{V}(\Gamma_2)$.*

Proof. Refer to the proof in [21]. □

Theorem 1 implies that expanding the subspace $\mathcal{V}(\Gamma)$ (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 WUS. Next, we present an example to explain the results of this section.

Example 1. Consider the following system:

$$x(k+1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} x(k) + \begin{bmatrix} 0.5 \\ 1 \end{bmatrix} u(k),$$
$$y(k) = \begin{bmatrix} 1 & 0 \end{bmatrix} x(k).$$

For this system, $\mathcal{V}(\Gamma) = \text{span}\{\begin{bmatrix} 0 & 1 \end{bmatrix}^T\}$.

• Part (i): We first consider opacity of individual initial states. Let $x_s(0) = \begin{bmatrix} 1 & 1 \end{bmatrix}^T$ and $x_{ns}(0) = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$. Then, $x_s(0) - x_{ns}(0) = \begin{bmatrix} 0 & 1 \end{bmatrix}^T \in \mathcal{V}(\Gamma)$. Thus, by Lemma 2, $x_s(0) \overset{o}{\to} \{x_{ns}(0)\}$. We show this explicitly for $k = 2$. From opacity Definition 1, we have that for any $U_s(2)$, there should exist a $U_{ns}(2)$ such that $Y_{x_s(0),U_s(2)} = Y_{x_{ns}(0),U_{ns}(2)}$. Using (2), this is equivalent to $O_2 x_s(0) + F_2^\Gamma U_s(2) = O_2 x_{ns}(0) + F_2^\Gamma U_{ns}(2)$. Substituting $O_2, F_2^\Gamma, x_s(0), x_{ns}(0)$ and rearranging, we get the following linear equation:

$$\underbrace{\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}}_{O_2(x_s(0)-x_{ns}(0))} + \underbrace{\begin{bmatrix} 0 & 0 & 0 \\ 0.5 & 0 & 0 \\ 1.5 & 0.5 & 0 \end{bmatrix}}_{F_2^\Gamma} U_s(2) = F_2^\Gamma U_{ns}(2).$$

Since $O_2(x_s(0) - x_{ns}(0)) \in \mathcal{R}(F_2^\Gamma)$, we observe that for any $U_s(2)$, there exists a $U_{ns}(2)$ that solves this equation. For instance, both $U_s(2) = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T$ and $U_{ns}(2) = \begin{bmatrix} 3 & -1 & 3 \end{bmatrix}^T$ with corresponding initial states result in the output sequence $\begin{bmatrix} 1 & 2.5 & 5 \end{bmatrix}^T$. Further, as $x_s(0) \bigoplus \mathcal{V}(\Gamma) = x_{ns}(0) \bigoplus \mathcal{V}(\Gamma) = \{\begin{bmatrix} 1 & c \end{bmatrix}^T : c \in \mathbb{R}\}$, it holds that $x_{ns}(0) \in x_s(0) \bigoplus \mathcal{V}(\Gamma)$ and $x_s(0) \in x_{ns}(0) \bigoplus \mathcal{V}(\Gamma)$. Thus, $x_s(0)$ and $x_{ns}(0)$ satisfy Corollary 1.

• Part (ii): Next, we focus on the opacity of sets. Let $\mathcal{X}_0 = \{x \in \mathbb{R}^2 : \|x\|_\infty = 1\}$ and let $\mathcal{X}_{ns} = \{\begin{bmatrix} c & 0 \end{bmatrix}^T : c \in [-1, 1]\}$. We note that $(\mathcal{X}_{ns} \bigoplus \mathcal{V}(\Gamma)) = \{\begin{bmatrix} c & d \end{bmatrix}^T : c \in [-1, 1], d \in \mathbb{R}\}$. Therefore, as seen in Fig. 1, any $x_s(0) \in \mathcal{X}_s = \mathcal{X}_0 \backslash \mathcal{X}_{ns}$ belongs to $\mathcal{X}_{ns} \bigoplus \mathcal{V}(\Gamma)$. Thus, $\mathcal{X}_s \subset \mathcal{X}_{ns} \bigoplus \mathcal{V}(\Gamma)$ and $\mathcal{X}_s \overset{o}{\to} \mathcal{X}_{ns}$ as per Lemma 3. □

IV. Opacity and Attack Detectability Trade-off

In this section, we use the relationship between opacity and WUS 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? (Subsection IV-A)
- Does expanding opaque sets (by expanding $\mathcal{X}_0$) expand the set of undetectable attacks? (Subsection IV-B)

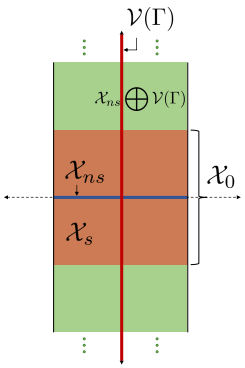


Fig. 1: Pictorial representation of Example 1, part(ii). $\mathcal{X}_0$ is the brown square, $\mathcal{X}_{ns}$ is the blue line segment, $\mathcal{V}(\Gamma)$ is the y axis, and $\mathcal{X}_{ns} \bigoplus \mathcal{V}(\Gamma)$ is the infinite green strip. Since $\mathcal{X}_s \subset \mathcal{X}_{ns} \bigoplus \mathcal{V}(\Gamma)$, we have $\mathcal{X}_s \overset{o}{\to} \mathcal{X}_{ns}$.

A. Coexistence of Opaque Sets and Undetectable Attacks

In this subsection, we show that existence of opaque sets implies existence of undetectable attacks.

Theorem 2. *If there exists an opaque set $\mathcal{X}_s$ for Γ, then there exists an attacked system $\tilde{\Gamma}$ (that is, a pair $(\tilde{B}, \tilde{D})$) that admits an undetectable attack $\tilde{U}_u \neq 0$.*

A set of such attacked systems is given by:

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

Proof. Refer to the Appendix. □

Corollary 2. *Let $\tilde{\Gamma} = \Gamma$ and let $\begin{bmatrix} B & D \end{bmatrix}^T$ be full column rank. Then, there exists an opaque set $\mathcal{X}_s$ if and only if there exists an undetectable attack $\tilde{U}_u \neq 0$.*

Theorem 2 shows that existence of opaque set always implies existence of an attacked system with undetectable attack inputs (Corollary 2 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. Also, note that if all attacks are detectable for all $(\tilde{B}, \tilde{D})$, then no opaque set exists in the system. 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 $\tilde{U}_u \neq 0$.

The above results elucidate that opaque sets and undetectable attacks co-exist in linear systems. This is further illustrated in the following example where the system is modified to eliminate undetectable attacks.

Example 1. (Continued) We illustrate the results of Corollary 2. Since $\mathcal{V}(\Gamma) = \text{span}\{\begin{bmatrix} 0 & 1 \end{bmatrix}^T\}$ contains elements other than the origin, there exist opaque sets in Γ (c.f. Lemma 1). Examples of such sets were shown previously in Fig. 1. Existence of these opaque sets also imply existence of undetectable attacks (c.f. Corollary 2), as shown next.

Consider attacked system identical to normal system, that is, $\tilde{\Gamma} = \Gamma$. The attack $\tilde{U}_u(2) = \begin{bmatrix}-2 & 2 & -2\end{bmatrix}^T$ with initial condition $x(0) = \begin{bmatrix}0 & 1\end{bmatrix}^T$ produces zero outputs till $k = 2$. Thus, $\tilde{U}_u(2)$ is undetectable until $k = 2$ (c.f. Definition 4).

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 attack $\tilde{U}_u(2) = \begin{bmatrix}-2 & 2 & -2\end{bmatrix}^T$, as shown next. For $\tilde{U}_u(2)$ 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 5). However, $\tilde{U}_u(2)$ with this initial condition produces non-zero output sequence $\begin{bmatrix}0 & 0 & -1 & -2 & -2 & 0\end{bmatrix}^T$, and therefore, is detectable.

Moreover, since $\mathcal{V}(\Gamma) = \{0\}$, no opaque set exists (c.f. Lemma 1). Therefore, we observe that eliminating undetectable attacks also eliminates opaque sets, indicating the trade-off between the two.

B. Relation between Sizes of Opaque and Undetectable Attacks Set

We 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. The variations in these sets is achieved by changing the initial state set $\mathcal{X}_0$.[3] An expansion of $\mathcal{X}_0$ may be performed by the operator, for instance, to include a larger set of opaque secret states.

Theorem 3. *Consider initial state sets $\mathcal{X}_0^1 \subset \mathcal{X}_0^2 \subseteq \mathbb{R}^n$. Let $\tilde{\mathcal{U}}_u^1$ and $\tilde{\mathcal{U}}_u^2$ denote the set of undetectable attacks (as defined in Definition 4) on a system $\tilde{\Gamma}$ with initial state set $\mathcal{X}_0^1$ and $\mathcal{X}_0^2$, respectively. Then, the following statements hold true:*
1. For any opaque set $\mathcal{X}_s^1 \subset \mathcal{X}_0^1$, there exists an opaque set $\mathcal{X}_s^2 \subset \mathcal{X}_0^2$ such that:
a. $\mathcal{X}_s^1 \subseteq \mathcal{X}_s^2$ always.
b. $\mathcal{X}_s^1 \subset \mathcal{X}_s^2$ if and only if there exists $x(0)$ that satisfies:

$$x(0) \in (\mathcal{X}_0^2 \backslash \mathcal{X}_0^1) \quad \text{and} \quad (x(0) \bigoplus \mathcal{V}(\Gamma)) \cap \mathcal{X}_0^2 \neq \{x(0)\}.$$

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 $z(0)$ that satisfies:

$$z(0) \in (\mathcal{X}_0^2 \bigoplus -\mathcal{X}_0^2) \text{ and } -O_k z(0) \in F_k^{\tilde{\Gamma}}(\mathbb{R}^{(k+1)q} \backslash \tilde{\mathcal{U}}_u^1).$$

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

Proof. Refer to the proof in [21]. □

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 expand, leading to a strict trade-off between opaque and undetectable attack sets. Statement 2(c) implies that there exists a $\tilde{\Gamma}$ ($\tilde{D}$ is square and full rank and $\tilde{B}$ is arbitrary) for which the undetectable attack set always expands. In this case, expanding $\mathcal{X}_0$ always expands the set of undetectable attacks, but the set of opaque secret states expands only under specific conditions (illustrated in Fig. 2).

[3]Note that expanding $\mathcal{X}_s$ without changing $\mathcal{X}_0$ does not affect the undetectable attack set.

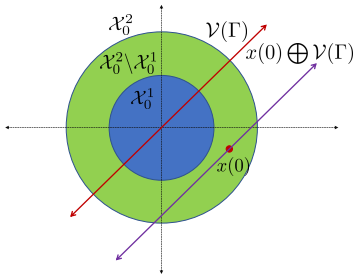


Fig. 2: Pictorial representation of Theorem 3, Statement 1(b). $\mathcal{X}_0^1$ is the blue disk, $\mathcal{X}_0^2$ is the union of blue disk and green region, $\mathcal{V}(\Gamma)$ is the red line passing through the origin, $x(0) \in \mathcal{X}_0^2 \backslash \mathcal{X}_0^1$ is the red dot and $x(0) \bigoplus \mathcal{V}(\Gamma)$ is the purple line passing through $x(0)$. Since $(x(0) \bigoplus \mathcal{V}(\Gamma)) \cap \mathcal{X}_0^2 \neq \{x(0)\}$, for an opaque $\mathcal{X}_s^1 \subset \mathcal{X}_0^1$, there exists an opaque $\mathcal{X}_s^2 \subset \mathcal{X}_0^2$ that satisfies $\mathcal{X}_s^1 \subset \mathcal{X}_s^2$.

V. Illustrative Example

We consider a team of UAVs used for item delivery to illustrate our results. The UAVs originate from warehouses located in the same geographical area and deliver items to a customer's home (destination)[4]. The locations of the warehouses are required to be private, and one should not be able to identify the origin warehouse of any UAV.

The real-time UAV locations are sent to a remote operator for monitoring purposes. To maintain warehouse privacy, instead of sending location of individual UAVs, only the average location of all the UAVs is sent to the operator. This prevents an eavesdropper that intercepts communication between UAVs and operator from determining the origin warehouse of any particular UAV. However, this choice of sending only the average location introduces vulnerabilities in the system. For instance, an attacker that hacks into the UAVs can inject malicious inputs and alter the trajectories of the UAVs while keeping the average location same to that of the unattacked case. Such attacks will remain undetected by the remote operator. This demonstrates the trade-off shown in the paper. Next, we illustrate this phenomenon for a team of N UAVs. The model for the i^{th} UAV is given as:

$$\underbrace{\begin{bmatrix} p_x^i(k+1) \\ v_x^i(k+1) \\ p_y^i(k+1) \\ v_y^i(k+1) \end{bmatrix}}_{x^i(k+1)} = \underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}}_{A_m} \underbrace{\begin{bmatrix} p_x^i(k) \\ v_x^i(k) \\ p_y^i(k) \\ v_y^i(k) \end{bmatrix}}_{x^i(k)} + \underbrace{\begin{bmatrix} 0.5 & 0 \\ 1 & 0 \\ 0 & 0.5 \\ 0 & 1 \end{bmatrix}}_{B_m} \underbrace{\begin{bmatrix} a_x^i(k) \\ a_y^i(k) \end{bmatrix}}_{u^i(k)},$$

$$y^i(k) = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{C_m} \begin{bmatrix} p_x^i(k) \\ v_x^i(k) \\ p_y^i(k) \\ v_y^i(k) \end{bmatrix},$$

[4]The example can be extended easily to the case of multiple destinations.

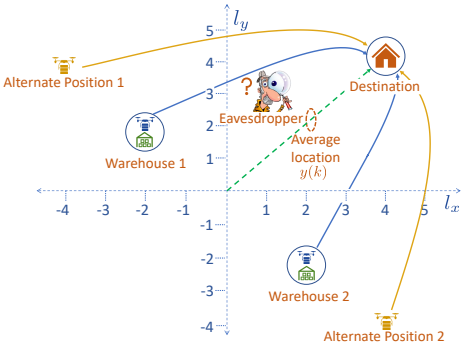
where (p_x, v_x, a_x) and (p_y, v_y, a_y) represent the position, velocity, acceleration along the l_x-axis and l_y-axis (as shown in Fig. 3), respectively. This is a simplified model that captures the motion of a UAV in a plane parallel to the ground, and is used commonly in literature [22], [23].

The aggregate model Γ of the UAV system is:

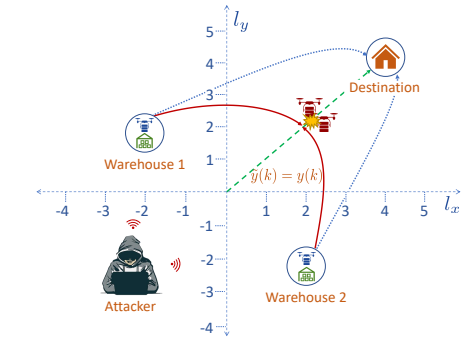
$$\begin{bmatrix} x^1(k+1) \\ x^2(k+1) \\ \vdots \\ x^N(k+1) \end{bmatrix} = \begin{bmatrix} A_m & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_m \end{bmatrix} \begin{bmatrix} x^1(k) \\ x^2(k) \\ \vdots \\ x^N(k) \end{bmatrix} + \begin{bmatrix} B_m & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & B_m \end{bmatrix} \begin{bmatrix} u^1(k) \\ u^2(k) \\ \vdots \\ u^N(k) \end{bmatrix},$$

$$y(k) = \frac{1}{N} \begin{bmatrix} C_m & C_m & \dots & C_m \end{bmatrix} \begin{bmatrix} x^1(k) \\ x^2(k) \\ \vdots \\ x^N(k) \end{bmatrix}.$$

For ease of representation we consider the case $N = 2$,



(a) Opacity of UAV swarm



(b) Undetectable attacks on UAV swarm

Fig. 3: In Fig. 3a, initial locations of UAVs (Warehouses 1, 2) are opaque since same average location $y(k)$ (green line) is output by the actual (blue arcs) and hypothetical (yellow arcs) trajectories. In Fig. 3b, attacker injects an attack to change the trajectory (blue arcs to red arcs), while maintaining unattacked outputs (green line).

and remark that a similar scenario can be studied for $N > 2$ as well. For the above system Γ, we have $\mathcal{V}(\Gamma) \neq \{0\}$. Let the two UAVs start from $\begin{bmatrix} -2 & 2 \end{bmatrix}^T$ and $\begin{bmatrix} 2 & -2 \end{bmatrix}^T$, respectively. An eavesdropper observing $y(k)$ over any time duration should not be able to determine either of these initial locations. To ensure this, all initial locations formed by the sets $\mathcal{S}_1 = \left\{ \begin{bmatrix} -2 & 0 & 2 & 0 & a & 0 & b & 0 \end{bmatrix}^T : a, b \in \mathbb{R} \right\}$ and $\mathcal{S}_2 = \left\{ \begin{bmatrix} c & 0 & d & 0 & 2 & 0 & -2 & 0 \end{bmatrix}^T : c, d \in \mathbb{R} \right\}$ should also be kept secret. Hence, the secret set is $\mathcal{X}_s = \mathcal{S}_1 \cup \mathcal{S}_2$. Let the region in which the UAVs start be $\mathcal{X}_0 = \left\{ \begin{bmatrix} p_x^1(0) & 0 & p_y^1(0) & 0 & p_x^2(0) & 0 & p_y^2(0) & 0 \end{bmatrix}^T : \| \begin{bmatrix} p_x^1(0) & p_y^1(0) & p_x^2(0) & p_y^2(0) \end{bmatrix}^T \|_\infty = 4 \right\}$.

Let the UAVs start from the warehouses and traverse the symmetric arcs of the parabola $l_x^2 - 2l_x l_y + 2l_x + l_y^2 + 2l_y - 16 = 0$, to reach the destination at $\begin{bmatrix} 4 & 4 \end{bmatrix}^T$ (blue arcs in Fig. 3a). These trajectories are calculated by the UAVs (e.g., using Dijkstra's algorithm), and then sampled over time into reference location points $\begin{bmatrix} \gamma_x^i(k) & \gamma_y^i(k) \end{bmatrix}^T$ which are followed by the UAVs. Using these reference points, the control inputs $u^i(k)$ are determined using a Linear-Quadratic (LQ) tracking controller. This controller is obtained by solving the discrete algebraic Ricatti equation for the individual UAV model [22]:

$$\begin{bmatrix} a_x^i(k) \\ a_y^i(k) \end{bmatrix} = - \begin{bmatrix} 0.1589 & 0.5747 & 0 & 0 \\ 0 & 0 & 0.1589 & 0.5747 \end{bmatrix} \begin{bmatrix} p_x^i(k) - \gamma_x^i(k) \\ v_x^i(k) \\ p_y^i(k) - \gamma_y^i(k) \\ v_y^i(k) \end{bmatrix}.$$

Next, we show that the initial UAV locations are opaque. Consider the hypothetical case where the UAVs start from $\begin{bmatrix} -4 & 4 \end{bmatrix}^T$ and $\begin{bmatrix} 4 & -4 \end{bmatrix}^T$, respectively, and traverse the arcs of the parabola $l_x^2 - 2l_x l_y + 8l_x + l_y^2 + 8l_y - 64 = 0$, to reach the same destination $\begin{bmatrix} 4 & 4 \end{bmatrix}^T$ (yellow arcs in Fig. 3a). Then, the average trajectory would remain the same as the actual UAV trajectory, that is, along the $l_x = l_y$ line (green line in Fig. 3a). Thus, an eavesdropper observing $y(k)$ cannot estimate the initial UAV locations $\begin{bmatrix} -2 & 2 \end{bmatrix}^T$ and $\begin{bmatrix} 2 & -2 \end{bmatrix}^T$.

However, undetectable attacks are also present in this system. For instance, an attacker could modify the actual UAV trajectory to make the UAVs move along the arcs of the parabola $l_x^2 - 2l_x l_y + 4l_x + l_y^2 + 4l_y - 16 = 0$ (red arcs in Fig. 3b). This leads to a collision at the location $\begin{bmatrix} 2 & 2 \end{bmatrix}^T$. Since the average location in this attack case $\tilde{y}(k)$ is same as in normal operation (along the $l_x = l_y$ line), this attack is undetectable. This shows that opacity implies existence of undetectable attacks in this system.

VI. Conclusion

We analyzed the underlying connection between the notion of opacity and attack detectability for linear systems. The fundamental relation between opacity and the weakly unobservable subspace was studied from multiple perspectives. Using this relation, we showed that a trade-off exists between opaque sets and undetectable attacks. Future directions include investigating the effect of changing system matrices A and C on opacity and attack detectability, exploring numerical algorithms to efficiently verify the opacity conditions, extending the results to general class of non-linear and hybrid systems, and determining if the attack inputs have any effect of opacity of certain states.

VII. Appendix

A. Proof of Theorem 2

We will show that existence of an opaque set $\mathcal{X}_s$ in Γ implies that an undetectable attack $\tilde{U}_u \neq 0$ exists for the

particular attacked system $\tilde{\Gamma} = \Gamma$. Later, we generalize this for other attacked systems.

Existence of an opaque $\mathcal{X}_s$ in Γ implies that $\mathcal{V}(\Gamma) \neq \{0\}$ (c.f. Lemma 1), which in turn implies $\mathcal{V}(\tilde{\Gamma}) \neq \{0\}$ (since $\tilde{\Gamma} = \Gamma$). Therefore, there exists an undetectable $\tilde{U}_u$ for $\tilde{\Gamma}$ (c.f. discussion below Definition 5). Next we show that $\tilde{U}_u \neq 0$.

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

$$F_k^{\tilde{\Gamma}} \tilde{U}_u(k) = -O_k \tilde{x}(0) \qquad \forall\, k \geq 0. \tag{7}$$

Since Γ is observable, $\tilde{\Gamma}$ is also observable (as matrices (A, C) are same for Γ and $\tilde{\Gamma}$). Using this fact and (7), we have:

$$\begin{aligned} & O_k \tilde{x}(0) \neq 0 \qquad \forall\, k \geq n \\ \implies \qquad & \tilde{U}_u(k) \neq 0 \qquad \forall\, k \geq n \quad \implies \exists\, \tilde{U}_u \neq 0. \end{aligned}$$

Next, we show that for all $\tilde{\Gamma}$ that satisfy $\mathcal{R}(\begin{bmatrix}\tilde{B}^T & \tilde{D}^T\end{bmatrix}^T) \supseteq \mathcal{R}(\begin{bmatrix}B^T & D^T\end{bmatrix}^T)$ (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:

$$Y_{x(0),U_{n-1}} = O_{n-1} x(0) + F_{n-1}^{\Gamma} U(n-1) = 0. \tag{8}$$

Through matrix manipulations, we get:

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

where $\hat{F}_{n-1}$ is equal to F_{n-1}^{Γ} in (4) with $B = C = I_n$ and $D = 0$. Further manipulations yield:

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

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:

$$P = \begin{bmatrix} 0 & I_m \\ I_{n^2+(n-1)m} & 0 \end{bmatrix},$$

$$T = \begin{bmatrix} \underbrace{\begin{matrix} I_n & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \end{matrix}}_{n} & \underbrace{\begin{matrix} 0 & 0 & \dots & 0 \\ I_m & 0 & \dots & 0 \end{matrix}}_{n} \end{bmatrix}^T.$$

Next, we consider the fact that for any matrices M, Q, W, $\mathcal{R}(M) \supseteq \mathcal{R}(Q)$ implies (i) $\mathcal{R}(WM) \supseteq \mathcal{R}(WQ)$, and (ii) $\mathcal{R}(I_n \bigotimes M) \supseteq \mathcal{R}(I_n \bigotimes Q)$. Using this, we have:

$$\begin{aligned} & \mathcal{R}(\begin{bmatrix}\tilde{B}^T & \tilde{D}^T\end{bmatrix}^T) \supseteq \mathcal{R}(\begin{bmatrix}B^T & D^T\end{bmatrix}^T) \\ \implies \quad & \mathcal{R}(\begin{bmatrix} I_n \bigotimes \tilde{B} & I_n \bigotimes \tilde{D} \end{bmatrix}^T) \supseteq \mathcal{R}(\begin{bmatrix} I_n \bigotimes B & I_n \bigotimes D \end{bmatrix}^T) \\ \implies \quad & \mathcal{R}(F_{n-1}^{\tilde{\Gamma}}) \supseteq \mathcal{R}(F_{n-1}^{\Gamma}). \end{aligned} \tag{9}$$

Equation (9) 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 (8), 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 5).

REFERENCES

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

[2] N. Sayfayn and S. Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," working paper cisl# 2017-09. Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology, 2017.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

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

[9] 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.

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

[11] 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

[12] 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.

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

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

[15] 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.

[16] 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, vol. 14(12):3273-3286, 2019.

[17] 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.

[18] V. Delos and D. Teissandier, "Minkowski Sum of Polytopes Defined by their Vertices," Journal of Applied Mathematics and Physics, 3:62–67, 2015.

[19] V. Delos and D. Teissandier, "Minkowski Sum of HV-Polytopes in Rn," International Conference on Computational Mathematics, Computational Geometry and Statistics, 2015.

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

[21] V. M. John and V. Katewa, "On Connections between Opacity and Security in Linear Systems," arXiv Preprint, arXiv:2206.06074 [eess.SY], 2022.

[22] A. Reizenstein, "Position and Trajectory Control of a Quadcopter Using PID and LQ Controllers," Student Thesis, Linköping University, Sweden, 2017.

[23] L. Martins, C. Cardeira and P. Oliveira, "Linear Quadratic Regulator for Trajectory Tracking of a Quadrotor," IFAC Symposium on Automatic Control in Aerospace, 52(12):176-181, 2019.