2017 IEEE 56th Annual Conference on Decision and Control (CDC)
December 12-15, 2017, Melbourne, Australia

Opacity for Switched Linear Systems: Notions and Characterization*

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

***Abstract*— A switched system consists of a finite number of subsystems and a rule that orchestrates switching among them. We develop notions of opacity for discrete-time switched linear systems. We distinguish between cases when the secret is specified as a set of initial modes, a set of initial states, or a combination of the two. The novelty of our schemes is in the fact that we place restrictions on: i) the allowed transitions between modes (specified by a directed graph), ii) the number of allowed changes of modes (specified by lengths of paths in the directed graph), and iii) the dwell times in each mode. Each notion of opacity is characterized in terms of allowed switching sequences and sets of reachable states and/ or modes. Finally, we present algorithmic procedures to verify these notions, and provide bounds on their computational complexity.**

I. Introduction

Cyberphysical systems (CPSs) integrate communication, control, and computing with physical processes. Examples of CPSs include power systems, water distribution networks, medical devices, and home control systems. Since these systems are often controlled over a network, the sharing of information among systems and across geographies makes them vulnerable to attacks carried out (remotely) by malicious adversaries. To gain illicit access to the system, an attacker must be able to extract information from the system which can then be used to subvert its operation. Several instances of attacks on CPSs have been documented in the literature([1],[2]). Therefore, ensuring the safety of information critical to nominal operation of the system is of utmost importance.

Opacity is a property that captures whether an adversarial observer can infer a "secret" of the system based on its observations of the system behavior. It was originally formulated in [3] as a technique to study cryptographic protocols. Its scope was widened when notions of opacity were defined for discrete event systems (DESs) in [4] and [5]. State([5],[6],[7]) and language([8],[9]) based notions of opacity were shown to be equivalent in [10], where polynomial algorithms to transform one form of opacity to another were presented. A comparison of opacity with other notions of privacy like security and anonymity, and properties of DESs like diagnosability and detectability was presented in [11]. A subsequent paper, [12], defined opacity in a setup with multiple adversaries, each carrying out its own observation. Enforcing opacity on DESs by using techniques from supervisory control were studied in [8] and [13], while an approach for the same using insertion functions was formulated in [14].

The preceding theory, although quite rich, suffers from the drawback that the states in a DES are discrete. The parameters and variables in CPSs (*eg.* power systems) usually take values in a continuous domain. A notion of opacity with a single adversary for CPSs modeled as discrete-time linear time-invariant (DT-LTI) systems was first defined in [15]. Necessary and sufficient conditions for opacity were presented in terms of sets of reachable states of the system, and in relation to the concept of output controllability. Extensions to the case with multiple adversaries was studied in [16], wherein the definitions of opacity broadly depended on the presence or lack of a centralized coordinator, and the presence or absence of collusion among the adversaries.

In this paper, we extend the aforementioned work by formulating notions of opacity for CPSs modeled as discrete-time switched linear systems (DT-SLSs). An SLS consists of a finite number of linear subsystems (called modes) and a rule that governs the switching among them. Many practical systems can be modeled as operating in one of several modes, often switching from one mode of operation to another. Further, it has been shown that switching control strategies can achieve better control performance than nonswitching strategies. The reader is referred to [17],[18],[19] for an introduction to the design and control of switched systems. In this paper, we will assume that each subsystem is governed by linear, time-invariant dynamics.

We present the model of the system that will be studied in this paper and underlying assumptions in Section II. Sections III, IV, and V present the main results of this paper, wherein we formulate several notions of opacity for SLSs. We distinguish between the cases when the secret is specified as an initial mode, an initial state, or a combination of the two, and whether the adversary observes a mode, a function of the state, or a combination of the two. In each case, we present conditions that will establish that notion of opacity. We place constraints on the modes that the system will be allowed to transition into from a given mode and impose bounds on the dwell times in each mode. Moreover, we constrain the number of changes of modes before the adversary can make its observation in our definitions of opacity for SLSs. Algorithmic procedures to verify these

*This work was supported by the National Science Foundation under Grants *CNS* – 1446665 and *CMMI* – 1362303, and by the Air Force Office of Scientific Research under Grant *FA*9550 – 15 – 10050.

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

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

notions of opacity are given in Section VI, where we also provide conservative upper bounds on their computational complexity. Illustrative examples are presented in Section VII. We conclude in Section VIII by commenting on possible future directions of research.

II. System Model and Preliminaries

Consider a DT-SLS is of the form:

$$x(t+1) = A(\mathscr{M}_t)x(t) + B(\mathscr{M}_t)u(t) \quad (1)$$
$$x(0) = x_0 \in X_0$$
$$y(t) = Cx(t) \quad (2)$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, $y \in \mathbb{R}^p$, and $A(\cdot)$, $B(\cdot)$, C are matrices of appropriate dimensions containing real entries. $\mathscr{M}_t \in \{1,2,\ldots,z\}$ denotes the mode active at time t. The solution to the state equation 1 is given by equation 3 (in Section IV). The system switches from a mode $\mathscr{M}'$ to $\mathscr{M}''$ at a time $t = t_s$, which is called a *switching time*. That is, $A(\mathscr{M}_{t_s-1}) = A(\mathscr{M}')$, while $A(\mathscr{M}_{t_s}) = A(\mathscr{M}'')$. The $B(\cdot)$ matrix switches similarly. A *switching sequence of length* N is a collection of N (possibly nonconsecutive) switching times $t_{s_1} < t_{s_2} < \cdots < t_{s_N}$. Let $\mathscr{K}$ be a set of positive integers corresponding to the instants of time the adversary makes an observation of the system. The subscript s (ns), when appended to the states, inputs, and outputs, will correspond to trajectories that start from the set of initial secret (nonsecret) states.

That the adversary does not continuously observe the system is motivated by the following considerations: it might not want to reveal its presence to the system; alternatively, it might not have the resources to continuously monitor the system. In this paper, the set $\mathscr{K}$ is fixed, and we do not assume that the adversary incurs a cost in making an observation. Formulating observation strategies for the adversary in the presence of such constraints is an interesting direction of future research.

We briefly review initial state opacity (ISO) for LTI systems (i.e., $\mathscr{M}_t = \{1\}\ \forall t$, $A(1) := A$, $B(1) := B$).

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

Let $X(k)$ denote the set of states reachable at time k, starting from X at time 0. Define $\phi : \mathbb{R}^p \to 2^{\mathbb{R}^n \times \mathbb{R}^n}$ as $\phi(y(k)) := \{(x_1,x_2) \in X_s(k) \times X_{ns}(k) : Cx_1 = Cx_2 = y(k)\}$, and $\phi(CX(k)) := \bigcup\{\phi(y(k) : [y(k) = Cx(k)] \wedge [x(k) \in X(k)]\}$.

Theorem 2.2: ([15],[16]) The following are equivalent:

1) X_s is k-ISO with respect to X_{ns}.
2) $CX_s(k) \subseteq CX_{ns}(k)$.
3) $\phi(CX_s(k)) = (X_s(k), X'_{ns}(k))$, where $X'_{ns}(k) := \{x \in X_{ns}(k) : Cx \in CX_s(k)\}$.

Theorem 2.2 relates k-ISO to sets of reachable states, $X_s(k)$ and $X_{ns}(k)$. Thus, it suffices for the adversary to check membership of the output at time k in the sets $CX_s(k)$ and $CX_{ns}(k)$ to determine opacity of X_s with respect to X_{ns} at time 0. Further, it gives the states in $X_{ns}(k)$ that establish k-ISO of X_s with respect to X_{ns}.

The following assumptions will be needed to formalize notions of opacity for SLSs in this paper.

Assumption 2.3: The allowed transitions between modes is specified by a directed graph $\mathscr{G} = (\mathscr{V}, \mathscr{E})$ whose vertices are the modes $\{1,\ldots,z\}$ and edges are the possible transitions between modes.

Assumption 2.4: The mode changes at every switching time t_s.

Assumption 2.5: The switching sequence does not depend on initial states and controls[1].

Assumption 2.6: (*Nonblocking Property*) It is possible for the system to switch to at least one other mode from every mode.

Assumption 2.7: (*Dwell constraints*) The system is allowed to remain in a mode a for a duration of time $\tau_d^a \in [\tau_{d_{min}}^a, \tau_{d_{min}}^a + 1, \ldots, \tau_{d_{max}}^a]$. Further, $\tau_{d_{min}}^a \geq 1 \forall a$.

Assumption 2.8: The adversary has knowledge of the initial secret and nonsecret specifications, the $A(\cdot), B(\cdot)$ matrices, the observation map C, the graph $\mathscr{G}$, and the minimum and maximum dwell times in each mode.

A path in $\mathscr{G}$ is an alternating sequence of vertices and edges of $\mathscr{G}$, $v_0 e_1 v_1 e_2 \ldots$. A path will always begin and end in a vertex of $\mathscr{G}$. Further, if the sequence $v_{i-1} e_i v_i$ appears in a path, then v_{i-1} and v_i are respectively the source and target vertices of edge e_i in $\mathscr{G}$. The *length* of a path is defined to be the number of vertices in the path. Let $\Theta_{[N]}$ be the set of paths of length $N+1$ in $\mathscr{G}$. This corresponds to N changes of modes. Knowledge of $\mathscr{G}$ helps eliminate transitions that are impossible. An element $\theta \in \Theta_{[N]}$ can be written as $v_0 e_1 v_1 e_2 \ldots e_N v_N$, with $v_i \neq v_{i+1}$ (Assumption 2.4). We will represent $\theta \in \Theta_{[N]}$ as a sequence of vertices $v_0 v_1 \ldots v_N$ when the edges representing transitions between vertices are obvious.

Assumption 2.9: At a time $k \in \mathscr{K}$, the number of switches of modes, q, is strictly less than k.

Assumption 2.10: For given q and k, $t_{s_q} < k$. That is, the q mode changes occur before time k. Further, if k is a possible ($(q+1)^{st}$) switching time, and if the adversary is observing the mode of the system, its observation will be $\mathscr{M}_{k^-}$, that is, the mode the system is in just before the switching at time k[2].

The notions of opacity developed in this paper will be defined in terms of q and k. Informally, for a given number of mode changes q, the secret is said to be opaque at a time k if for every 'allowed' switching sequence of length q starting from the secret modes and/ or states, there is an 'allowed' switching sequence of length q starting from a nonsecret mode and/ or state, such that the observation at time k will be indistinguishable to

[1] A standard assumption in the SLS literature is that there is only a finite number of switches in any finite time interval. This is needed to rule out the Zeno phenomenon in continuous time systems. It will not be needed here since we are dealing with discrete time systems.

[2] This assumption is needed because the state, and consequently, the output of the system at a time t depends only on the modes of the system upto time $t-1$.

the adversary. The 'allowed' switching sequences will be those that respect the dwell time constraints in the modes along paths of length $q+1$. Throughout this paper, a switching sequence of length q will correspond to a path of length $q+1$ in $\mathcal{G}$.

III. Initial Mode Opacity

In this case, the secret is specified as a set of modes. Let $\mathcal{M}^s \subset \{1,\dots,z\}$ and $\mathcal{M}^{ns} \subset \{1,\dots,z\}$ be the set of initial secret and nonsecret modes, with $\mathcal{M}^s \cap \mathcal{M}^{ns} = \emptyset$. The mode at time t, starting from a mode in $\mathcal{M}^s$ ($\mathcal{M}^{ns}$) at time 0 will be denoted $\mathcal{M}^s_t$ ($\mathcal{M}^{ns}_t$). The adversary observes the mode of the system at a time $k \in \mathcal{K}$. Its goal is to use this observation and other information that it has access to (Assumption 2.8) to deduce if the system started from a secret mode.

Definition 3.1: Given $\mathcal{M}^s, \mathcal{M}^{ns}, k \in \mathcal{K}$, and $q < k$, $\mathcal{M}^s$ is (k,q)-**initial mode opaque ((k,q)-IMO)** with respect to $\mathcal{M}^{ns}$ if for all $\theta = v_0 \dots v_q \in \Theta_{[q]}$ satisfying $v_0 \in \mathcal{M}^s$ and $\sum_\theta \tau_d = k$, there exists $\theta' = v'_0 \dots v'_q \in \Theta_{[q]}$ that satisfies $v'_0 \in \mathcal{M}^{ns}$ and $\sum_{\theta'} \tau_d = k$, such that $\mathcal{M}^s_k = \mathcal{M}^{ns}_k$.

The term $\sum_\theta \tau_d = k$ means that there exists a sequence of $q+1$ dwell times $\{\tau_d^{v_j} \in [\tau_{d_{min}}^{v_j}, \tau_{d_{max}}^{v_j}]\}, j = 0,\dots,(q-1)$, and $1 \le \tau_d^{v_q} \le \tau_{d_{max}}^{v_q}$ along the path $\theta = v_0 \dots v_q$, such that $\sum_{j=0}^{q-1} \tau_d^{v_j} + \tau_d^{v_q} = k$. Thus, we only consider paths of length $q+1$ in $\mathcal{G}$ for which the dwell times in modes along the path are 'sufficiently long'.

Theorem 3.2: $\mathcal{M}_s$ is (k,q)-IMO with respect to $\mathcal{M}_{ns}$ iff

$$\bigcup_{\substack{\theta = v_0 \dots v_q \in \Theta_{[q]}: \\ \sum_\theta \tau_d = k \wedge v_0 \in \mathcal{M}_s}} \mathcal{M}^s_k \subseteq \bigcup_{\substack{\theta = v_0 \dots v_q \in \Theta_{[q]}: \\ \sum_\theta \tau_d = k \wedge v_0 \in \mathcal{M}^{ns}}} \mathcal{M}^{ns}_k.$$

Proof: $\Rightarrow$: Follows from Definition 3.1.

$\Leftarrow$: Every mode the system can reach at time k starting from a secret mode at time 0 after q mode changes and respecting dwell time constraints along the path can also be reached by starting from a nonsecret mode at time 0, and an allowed switching sequence of length q. This establishes Definition 3.1. ∎

It is important that the system dwell in a mode for sufficiently long in order to meaningfully establish initial mode opacity.

Proposition 3.3: If $\tau^a_{d_{max}} = 1$ for every mode $a \in \{1,\dots,z\}$, then for any choice of $\mathcal{M}^s$ and $\mathcal{M}^{ns}$, and for every $q < k-1$, $\mathcal{M}^s$ will not be (k,q)-IMO w.r.t. $\mathcal{M}^{ns}$.

The main result of this section provides guarantees on (k',q')-IMO for $k' > k$, $q' > q$ if it has been established that (k,q)-IMO holds. In the sequel, we will write $\sum_q \tau_d$ to denote the sum of the dwell times in the modes along a path of length $q+1$ in the directed graph.

Theorem 3.4: If $\mathcal{M}^s$ is (k,q)-IMO with respect to $\mathcal{M}^{ns}$, then for every $Q > 0$, $\mathcal{M}^s$ is $(k+K, q+Q)$-IMO w.r.t. $\mathcal{M}^{ns}$ for all $K \in [\sum_q \tau_d - k + \sum_Q \tau_{d_{min}}, \sum_q \tau_d - k + \sum_Q \tau_{d_{max}}]$.

Proof: Let $\Theta_{[q,Q]}$ denote the set of valid extensions of length Q to a switching sequence of length q. Then, every $\theta'' \in \Theta_{[q+Q]}$ can be written as $\theta.\theta_e$, where $\theta \in \Theta_{[q]}$ and $\theta_e \in \Theta_{[q,Q]}$, and . denotes the concatenation of the paths. (k,q)-IMO ensures that for every $\theta \in \Theta_{[q]}$ starting from a secret mode and satisfying the dwell time constraints along the path, there exists $\theta' \in \Theta_{[q]}$ starting from a nonsecret mode and satisfying the dwell time constraints along θ', such that $\mathcal{M}^s_k = \mathcal{M}^{ns}_k$. Using Assumption 2.6, any extension of θ (θ') of length Q can be written as $\alpha = \theta.\theta_e$ ($\alpha' = \theta'.\theta_e$), where $\theta_e \in \Theta_{[q,Q]}$. This shows that $(k+K, q+Q)$-IMO holds for some $K \ge Q$.

The lower and upper bounds on K are obtained by considering the minimum and maximum dwell times along the extension of length Q to a path of length q, and noting that $\tau^a_{d_{min}} \ge 1$ for every mode (Assumption 2.7). Two cases need to be considered:

Case I: $k - (\sum_{j=0}^{q-1} \tau_d^{v_j}) \ge \tau_{d_{min}}^{v_q}$. In this case, the term $\sum_q \tau_d - k = 0$, and $K \in [\sum_Q \tau_{d_{min}}, \sum_Q \tau_{d_{max}}]$.

Case II: $k - (\sum_{j=0}^{q-1} \tau_d^{v_j}) < \tau_{d_{min}}^{v_q}$. Here, the $(q+1)^{st}$ change of mode can occur only after a time $\sum_{j=0}^{q-1} \tau_d^{v_j} + \tau_{d_{min}}^{v_q}$. Thus, we have $K \in [\sum_q \tau_d - k + \sum_Q \tau_{d_{min}}, \sum_q \tau_d - k + \sum_Q \tau_{d_{max}}]$ ∎

This formulation of (k,q)-IMO is reminiscent of 'state-based' notions of DES opacity [6]. However, unlike in the DES case, we do not insist that the entire secret trace be indistinguishable from the entire nonsecret trace; we require indistinguishability only at time k, with the caveat that there be only q changes of modes. (k,q)-IMO does not depend on the dynamics within each mode.

IV. Initial Mode and State Opacity

In this case, the adversary observes $y(k)$ and $\mathcal{M}_k$ at a time $k \in \mathcal{K}$. This formulation is similar in flavor to pathwise observability (PWO) in [20]. However, in their framework, the entire mode sequence and the output up to time k are available. Here, we only have snapshots of the output-mode pair at a time $k \in \mathcal{K}$. The secret in this case is specified as a state-mode pair.

Definition 4.1: For the system 2, given $k \in \mathcal{K}, q < k, \bar{X}_s := (X_s; \mathcal{M}^s)$, and $\bar{X}_{ns} := (X_{ns}; \mathcal{M}^{ns})$, with $X_s, X_{ns} \subset X_0$, $\bar{X}_s$ is (k,q)-**initial mode and state opaque ((k,q)-IMSO)** with respect to $\bar{X}_{ns}$ if for every $x_s(0) \in X_s$, every sequence of admissible controls U_s^k, and every $\theta = v_0 \dots v_q \in \Theta_{[q]}$ satisfying $v_0 \in \mathcal{M}^s$ and $\sum_\theta \tau_d = k$, there exist an $x_{ns}(0) \in X_{ns}$, a sequence of admissible controls U_{ns}^k, and $\theta' = v'_0 \dots v'_q \in \Theta_{[q]}$, satisfying $v'_0 \in \mathcal{M}^{ns}$ and $\sum_{\theta'} \tau_d = k$ such that: i)$\mathcal{M}^s_k = \mathcal{M}^{ns}_k$, and ii)$y_s(k) = y_{ns}(k)$.

The set of reachable states at time k with q mode changes, starting from $\bar{X}_s$ ($\bar{X}_{ns}$), and applying k admissible controls and respecting the dwell constraints of the modes is given by equation 4 (equation 5).

Theorem 4.2: $\bar{X}_s$ is (k,q)-IMSO with respect to $\bar{X}_{ns}$ iff:

i) $$\bigcup_{\substack{\theta = v_0 \dots v_q \in \Theta_{[q]}: \\ \sum_\theta \tau_d = k \wedge v_0 \in \mathcal{M}^s}} \mathcal{M}^s_k \subseteq \bigcup_{\substack{\theta = v_0 \dots v_q \in \Theta_{[q]}: \\ \sum_\theta \tau_d = k \wedge v_0 \in \mathcal{M}^{ns}}} \mathcal{M}^{ns}_k, \text{ and}$$

ii) $CX_s(k,q) \subseteq CX_{ns}(k,q)$.

Proof: $\Rightarrow$: From the definition of (k,q)-IMSO, i) holds. $X_s(k,q)$ ($X_{ns}(k,q)$) is the set of states reachable at time k starting from states in X_s (X_{ns}) and modes in $\mathcal{M}^s$ ($\mathcal{M}^{ns}$), performing q changes of modes along the way, while respecting dwell constraints of each mode.

$$x(t+1) = A(\mathscr{M}_t)\dots A(\mathscr{M}_0)x(0) + \sum_{j=0}^{t-1}(A(\mathscr{M}_t)\dots A(\mathscr{M}_{j+1}))B(\mathscr{M}_j)u(j) + B(\mathscr{M}_t)u(t) \tag{3}$$

$$X_s(k,q) = \bigcup_{x_0\in X_s}\bigcup_{U_s^k}\bigcup_{\substack{\theta=v_0\dots v_q\in\Theta_{[q]}:\\ \sum_\theta \tau_d = k \wedge v_0\in\mathscr{M}^s}} \{x : x(i+1) = A(\mathscr{M}_i)x(i) + B(\mathscr{M}_i)u(i), \forall i < k\} \tag{4}$$

$$X_{ns}(k,q) = \bigcup_{x_0\in X_{ns}}\bigcup_{U_{ns}^k}\bigcup_{\substack{\theta=v_0\dots v_q\in\Theta_{[q]}:\\ \sum_\theta \tau_d = k \wedge v_0\in\mathscr{M}^{ns}}} \{x : x(i+1) = A(\mathscr{M}_i)x(i) + B(\mathscr{M}_i)u(i), \forall i < k\} \tag{5}$$

Therefore, for each $x' \in X_s(k,q)$, there exists $x'' \in X_{ns}(k,q)$ such that $y_s(k) = Cx' = Cx'' = y_{ns}(k)$. This gives ii).

$\Leftarrow$: i) ensures that for every allowed switching sequence of length q starting from $\mathscr{M}^s$, there exists an allowed switching sequence starting from $\mathscr{M}^{ns}$ such that the mode at time k is indistinguishable. ii) ensures that for every $x' \in X_s(k,q)$, there exists an $x'' \in X_{ns}(k,q)$ such that $y_s(k) = Cx' = Cx'' = y_{ns}(k)$. From equation 4 (5), x' (x'') is a state got by starting from an initial secret state and secret mode (nonsecret initial state and nonsecret mode), while satisfying dwell constraints and number of allowed changes of mode. This proves (k,q)-IMSO. ■

V. Opacity for Unobserved Modes

In this case, the adversary observes the output $y(k)$ at a time $k \in \mathscr{K}$, and using only this information, it needs to determine if the system started from a secret state or mode. We consider two possible scenarios: when the secret is specified as a set of initial modes, and when the secret is specified as a set of initial states. This is like the unobservable mode case considered in [20], where they separately study the possibilities of recovering only the mode or only the state, after observing (at each time instant) the output. These notions are more general than (k,q)-IMSO in the sense that there is no constraint that the system start from a particular mode (Section V-A) or a particular state (Section V-B). Moreover, *the modes at time k corresponding to the secret and nonsecret trajectories need not be the same*. The subscript $\not{\mathscr{M}}$ will serve to indicate that the modes remain unobserved.

A. Initial Mode Opacity

The secret is specified as a set of modes, and the adversary has to deduce if the system started from a secret mode based on observing $y(k)$ at a time $k \in \mathscr{K}$.

Definition 5.1: For system 2, given $X_0, \mathscr{M}_s, \mathscr{M}_{ns}, k \in \mathscr{K}$, and $q < k$, $\mathscr{M}^s$ is $(k,q)_{\not{\mathscr{M}}}$**-initial mode opaque** ($(k,q)_{\not{\mathscr{M}}}$**-IMO**) with respect to $\mathscr{M}^{ns}$ if for every initial state, every sequence of admissible controls, and every $\theta = v_0\dots v_q \in \Theta_{[q]}$ satisfying $v_0 \in \mathscr{M}^s$ and $\sum_\theta \tau_d = k$, there exist an initial state, a sequence of admissible controls, and a $\theta' = v_0'\dots v_q' \in \Theta_{[q]}$ that satisfies $v_0' \in \mathscr{M}^{ns}$ and $\sum_{\theta'} \tau_d = k$, such that $y_s(k) = y_{ns}(k)$.

Let $X_s'(k,q)$ ($X_{ns}'(k,q)$) denote the set of states reachable at time k after q changes of modes starting from a secret mode (nonsecret mode) at time 0. That is, the condition $x_0 \in X_s$ ($x_0 \in X_{ns}$) in equation 4 (5) is replaced by $x_0 \in X_0$, and the subscript on U_s^k (U_{ns}^k) is dropped.

Theorem 5.2: $\mathscr{M}^s$ is $(k,q)_{\not{\mathscr{M}}}$-IMO with respect to $\mathscr{M}^{ns}$ if and only if $CX_s'(k,q) \subseteq CX_{ns}'(k,q)$.

B. Initial State Opacity

The adversary has to determine if the system started from a secret state, based on its observation $y(k)$ at time $k \in \mathscr{K}$. The underlying idea behind this notion is similar to k-ISO (Definition 2.1), with the difference that the system switches among several modes.

Definition 5.3: For the system 2, given $X_s, X_{ns} \subset X_0$, $k \in \mathscr{K}$, and $q < k$, X_s is $(k,q)_{\not{\mathscr{M}}}$**-initial state opaque** ($(k,q)_{\not{\mathscr{M}}}$**-ISO**) with respect to X_{ns} if for every $x_s(0) \in X_s$, every sequence of admissible controls U_s^k, and every $\theta \in \Theta_{[q]}$ satisfying $\sum_\theta \tau_d = k$, there exist an $x_{ns}(0) \in X_{ns}$, a sequence of admissible controls U_{ns}^k, and a $\theta' \in \Theta_{[q]}$, satisfying $\sum_{\theta'} \tau_d = k$ such that $y_s(k) = y_{ns}(k)$.

Let $X_s''(k,q)$ ($X_{ns}''(k,q)$) denote the set of states reachable at time k after q changes of modes starting from X_s (X_{ns}) at time 0, without restrictions on the initial modes. That is, the condition $v_0 \in \mathscr{M}^s$ ($v_0 \in \mathscr{M}^{ns}$) is removed from equation 4 (equation 5).

Theorem 5.4: X_s is $(k,q)_{\not{\mathscr{M}}}$-ISO with respect to X_{ns} if and only if $CX_s''(k,q) \subseteq CX_{ns}''(k,q)$.

VI. Computational Complexity

This section presents procedures to verify (k,q)-IMO and (k,q)-IMSO. Algorithm 1 depends on determining paths of length $q+1$ in $\mathscr{G}$, and determining a set of $q+1$ numbers that sum to k. Algorithm 2 depends on determining sets of reachable states, and Algorithm 1.

The *SUBSETSUM* problem asks the following question: given a set of nonnegative integers S and a target number t, is there a subset of S whose elements sum to t? This problem is known to be NP-Complete [21][3]. The *rSUM* problem asks: given a set of nonnegative integers S and numbers r and t, is there is a subset of S of size r whose elements sum to t? The brute-force algorithm for *rSUM* runs in time $O(|S|^r)$. More recent results have significantly lowered this bound [22].

In our setting, given a set of $q+1$ lists $L_i := [\tau^i_{d_{min}}, \tau^i_{d_{min}}+1, \dots, \tau^i_{d_{max}}], i \in \{1,2,\dots,q+1\}$, we ask if there

[3]A decision problem is in class NP if all instances of the problem to which the answer is 'yes' can be efficiently verified by a deterministic Turing machine. It is NP-complete if, additionally, it is as hard as any problem in NP.

is an assignment of nonzero numbers $\tau_1,\ldots,\tau_{q+1}$, with $\tau_i \in L_i$ such that $\sum_i \tau_i = k$. This is equivalent to the $rSUM$ problem, with $r = q+1$[4]. Let $\mathscr{C}_{sum}$ denote the number of operations needed to solve this problem.

Given the adjacency matrix $\mathscr{A}$ of $\mathscr{G}$ [5], the ij entry of $\mathscr{A}^q$ gives the number of paths in $\Theta_{[q]}$ with $v_0 = i$ and $v_q = j$. Let $\mathscr{C}_{pow}$ denote the complexity of computing $\mathscr{A}^q$. This typically takes $O(z^\omega log\ q)$ operations, where z is the number of vertices of $\mathscr{G}$ (modes of the system), and z^ω ($\omega < 3$) is the complexity of matrix multiplication. Let $\mathscr{C}_{path}$ be the maximum number of operations needed to determine a path of length q in $\mathscr{G}$. This problem is trivially solvable in $O(z^q)$, but can be more efficient, depending on the structure $\mathscr{G}$. Let $b_i := \sum_j [\mathscr{A}^q]_{ij}$ denote the total number of paths in $\Theta_{[q]}$ from vertex i. Then, the number of operations to determine all $\theta \in \Theta_{[q]}$ such that $v_0 = i$ is at most $b_i \mathscr{C}_{path}$. Let $b := \sum_i b_i;\ i \in (\mathscr{M}^s \bigcup \mathscr{M}^{ns})$. Algorithm 2 invokes Algorithm 1, and further, computes

Algorithm 1 Verifying (k,q)-IMO

Input: $\mathscr{M}^s, \mathscr{M}^{ns}, k, q, [\tau^a_{d_{min}}, \tau^a_{d_{max}}]$ for each mode a, $\mathscr{G} = (\mathscr{V}, \mathscr{E})$ specifying allowed mode transitions.
Output: YES, if $\mathscr{M}^s$ is (k,q)-IMO w.r.t. $\mathscr{M}^{ns}$; NO, if not.

```
1: M^s_k = M^ns_k = ∅
2: Θ^{M^s}_[q] := {v_0 e_1 ... v_q ∈ G: v_0 ∈ M^s}
3: Θ^{M^ns}_[q] := {v_0 e_1 ... v_q ∈ G: v_0 ∈ M^ns}
4: for each θ ∈ Θ^{M^s}_[q] do
5:    if (Σ_θ τ_d = k) then
6:       M^s_k = M^s_k ⋃ v_q
7:    end if
8: end for
9: for each θ' ∈ Θ^{M^ns}_[q] do
10:   if (Σ'_θ τ_d = k) then
11:      M^ns_k = M^ns_k ⋃ v'_q
12:   end if
13: end for
14: if M^s_k ⊆ M^ns_k then                    ▷ Theorem 3.2
15:   return YES
16: else
17:   return NO
18: end if
```

sets of states that are reachable at time k after q mode changes. Let $\mathscr{C}_{reach}$ denote the complexity of computing the sets of reachable states. Under reasonable assumptions on the structures of the sets of controls and initial states, approximations of sets of reachable states can be calculated with arbitrary precision using procedures that are linear in the time horizon(k) and polynomial in the dimension of the state space(n) ([23],[24],[25]). Let $\mathscr{C}_{mult}$ denote the complexity of the matrix-vector multiplication Cx, $x \in X(\cdot,\cdot)$. This typically takes $O(pn)$ operations.

[4]An additional requirement is that the lists be of equal sizes. This can be achieved by padding them with zeros.

[5]$\mathscr{A}_{ij} = 1$ if there is an edge in $\mathscr{G}$ from v_i to v_j, and $\mathscr{A}_{ij} = 0$ otherwise.

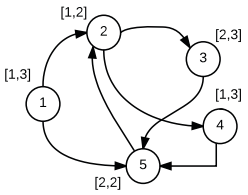

Fig. 1: Switched system considered in Example 7.1

Proposition 6.1: $\mathscr{C}_{alg1} \le k_1 b \mathscr{C}_{path} + k_2 \mathscr{C}_{sum} + k_3 \mathscr{C}_{pow}$; $\mathscr{C}_{alg2} \le k'_1 \mathscr{C}_{alg1} + k'_2 \mathscr{C}_{reach} + k'_3 \mathscr{C}_{mult}$ for constants $k_1, k_2, k_3, k'_1, k'_2, k'_3 > 0$.

Algorithm 2 Verifying (k,q)-IMSO

Input: $\bar{X}_s = (X_s, \mathscr{M}^s), \bar{X}_{ns} = (X_{ns}, \mathscr{M}^{ns}), k, q, \mathscr{G} = (\mathscr{V}, \mathscr{E})$, $[\tau^a_{d_{min}}, \tau^a_{d_{max}}]$ for each mode a.
Output: YES, if $\bar{X}_s$ is (k,q)-IMSO w.r.t. $\bar{X}_{ns}$; NO, if not.

```
1: ANS ← Result of Algorithm 1
2: if ANS == YES then
3:    Compute X_s(k,q) using equation 4
4:    Compute X_ns(k,q) using equation 5
5:    if CX_s(k,q) ⊆ CX_ns(k,q) then
6:       return YES                          ▷ Theorem 4.2
7:    else
8:       return NO
9:    end if
10: else
11:   return NO
12: end if
```

VII. Examples

Example 7.1: Figure 1 shows the allowed mode transitions in a switched system with five modes and the minimum and maximum dwell times in each mode. Notice that the system is nonblocking. Let $\mathscr{M}^s = \{1\}$ and $\mathscr{M}^{ns} = \{3,5\}$. Let $q = 2$. Then, $\Theta_{[2]} \supset \{(1,2,3),(1,2,4),(1,5,2),(3,5,2),(5,2,3),(5,2,4)\}$ (only considering paths starting from $\mathscr{M}^s$ or $\mathscr{M}^{ns}$). For $k = 6$, $\mathscr{M}^s$ is $(6,2)$-IMO w.r.t. $\mathscr{M}^{ns}$, since for all paths in Figure 1 of length $q+1 = 3$ starting from mode 1 such that the dwell times in the modes along the path sum to 6, there is a corresponding path of length 3 starting from modes 3 or 5 also satisfying the dwell constraints along the path, such that $\mathscr{M}^s_6 = \mathscr{M}^{ns}_6$. However, $\mathscr{M}^s$ is not $(3,2)$-IMO w.r.t. $\mathscr{M}^{ns}$. Consider the path $(1,2,3)$ starting from $\mathscr{M}^s$ with $\tau^1_d = 1, \tau^2_d = 1, \tau^3_d = 1$. There does not exist a corresponding path starting from $\mathscr{M}^{ns}$ such that $\mathscr{M}^{ns}_3 = 3$.

Example 7.2: Consider the system in figure 1, with the following additional specifications [26]:

$$A(1) = A(2) = \begin{pmatrix} 18 & -4 \\ 25 & -10 \end{pmatrix};\ A(3) = A(4) = A(5) = \begin{pmatrix} -2 & 4 \\ 7 & -6 \end{pmatrix}$$

$$B(1) = B(2) = \begin{pmatrix} 16 & 24 \end{pmatrix}^\top;\ B(3) = B(4) = B(5) = \begin{pmatrix} 8 & 12 \end{pmatrix}^\top$$

TABLE I: Example 7.2: (3,1)-IMSO

$\Theta_{[1]}$	$(\tau'_d,\tau''_d):\tau'_d+\tau''_d=3$	$\mathscr{M}_0\mathscr{M}_1\mathscr{M}_2$
1 2	1, 2	1 2 2
1 2	2, 1	1 1 2
5 2	2, 1	5 5 2
1 5	1, 2	1 5 5
1 5	2, 1	1 1 5
3 5	2, 1	3 3 5

Let $\bar{X}_s = (X_s;\mathscr{M}^s) := \left(\begin{pmatrix}0 & 1\end{pmatrix}^\top \cup \{\begin{pmatrix}x_1 & x_2\end{pmatrix}^\top : x_1 = -1\};1\right)$, $\bar{X}_{ns} = (X_{ns};\mathscr{M}^{ns}) := \left(\mathbb{R}^3 \setminus X_s;3,5\right)$, and $C = I_{2\times 2}$. For $q = 1$ and $k = 3$, the set of switching sequences of length 1 starting from $\mathscr{M}_s$ or $\mathscr{M}_{ns}$, the dwell times along the path that sum to k, and the modes of the system is given in table I. If the controls are restricted in the following way: $(2u_s(0),u_s(1),u_s(2)) = (u_{ns}(0),u_{ns}(1),u_{ns}(2)) = (u_0,u_1,u_2)$, where $u_0,u_1,u_2 \in \mathbb{R}$, then for $x(0) = \begin{pmatrix}0 & 1\end{pmatrix}^\top \in X_s$, the state which ensures $y_s(3) = y_{ns}(3)$ is $x'(0) = \begin{pmatrix}-1 & 0.23\end{pmatrix}^\top$. However, $x'(0) \notin X_{ns}$ (in fact, $x'(0) \in X_s$), which means that $\bar{X}_s$ is not (3,1)-IMSO w.r.t. $\bar{X}_{ns}$.

VIII. Conclusion

We have formulated several notions of opacity for discrete-time switched linear systems. We distinguished between the cases when the secret was specified in terms of initial modes, initial states, or a combination of the two. A characterization of each of notion of opacity was developed taking into account constraints on allowed transitions between modes, dwell times in each mode, and allowed number of transitions between modes before the adversary made an observation. Examples were presented to illustrate our results.

The nominal operation of many real-world systems relies on switching among a set of modes whose dynamics are nonlinear. Formulating notions of opacity for such systems will contribute to the development of a comprehensive framework for opacity for general cyberphysical systems. An equivalence between k-ISO and output controllability was established in [15]. A notion of output controllability of a DT-SLS from a particular initial mode has been defined in [26]. Establishing a similar equivalence for switched systems under additional constraints on number of mode transitions and dwell times is more subtle. The possibility of different switches of modes yielding the same output at time k makes the analysis of comparing opacity with output controllability nontrivial. It remains an interesting problem to study, nonetheless. Another interesting problem is to model the scenario when the adversary incurs a cost to make an observation and has to decide on opacity by incurring as low a cost as possible. The results in this paper have been qualitative in nature. A fourth direction is to pursue methods of quantifying opacity, and investigate its relation to the notion of differential privacy [27].

References

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

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

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

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

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

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

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

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

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

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

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

[12] A. Paoli and F. Lin, "Decentralized opacity of discrete event systems," in *Proceedings of the American Control Conference*, pp. 6083–6088, IEEE, 2012.

[13] A. Saboori and C. N. Hadjicostis, "Opacity-enforcing supervisory strategies via state estimator constructions," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1155–1165, 2012.

[14] Y.-C. Wu and S. Lafortune, "Synthesis of insertion functions for enforcement of opacity security properties," *Automatica*, vol. 50, no. 5, pp. 1336–1348, 2014.

[15] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus, "A framework for opacity in linear systems," in *Proceedings of the American Control Conference*, pp. 6337–6344, IEEE, 2016.

[16] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus, "A framework for decentralized opacity in linear systems," *Annual Allerton Conference on Communications, Control, and Computing*, 2016.

[17] Z. Sun and S. Ge, *Switched linear systems: control and design*. Springer Science & Business Media, 2006.

[18] H. Lin and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: a survey of recent results," *IEEE Transactions on Automatic control*, vol. 54, no. 2, pp. 308–322, 2009.

[19] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2012.

[20] M. Babaali and M. Egerstedt, "Observability of switched linear systems," in *International Workshop on Hybrid Systems: Computation and Control*, pp. 48–63, Springer, 2004.

[21] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT Press Cambridge, 2001.

[22] A. Lincoln, V. V. Williams, J. R. Wang, and R. R. Williams, "Deterministic time-space trade-offs for k-sum," in *43rd International Colloquium on Automata, Languages, and Programming*, pp. 58:1–58:14, 2016.

[23] A. A. Kurzhanskiy and P. Varaiya, "Ellipsoidal techniques for reachability analysis of discrete-time linear systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 1, pp. 26–38, 2007.

[24] A. Girard, C. Le Guernic, and O. Maler, "Efficient computation of reachable sets of linear time-invariant systems with inputs," in *International Workshop on Hybrid Systems: Computation and Control*, pp. 257–271, Springer, 2006.

[25] C. Le Guernic and A. Girard, "Reachability analysis of linear systems using support functions," *Nonlinear Analysis: Hybrid Systems*, vol. 4, no. 2, pp. 250–262, 2010.

[26] A. Babiarz, A. Czornik, and M. Niezabitowski, "Output controllability of the discrete-time linear switched systems," *Nonlinear Analysis: Hybrid Systems*, vol. 21, pp. 1–10, 2016.

[27] C. Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security*, pp. 338–340, Springer, 2011.