Preprints of the 2012 20th Mediterranean Conference on Control & Automation (MED), Barcelona, Spain, July 3-6, 2012

Resolution of Initial-State in Security Applications of DES

Christoforos N. Hadjicostis

***Abstract*— A non-deterministic labeled finite automaton is initial-state opaque if the membership of its true initial state to a set of *secret states* S remains opaque (i.e., uncertain) to an intruder who observes system activity through some natural projection map. The verification of initial-state opacity has been shown to be a PSPACE-complete problem by establishing that it is equivalent to the language containment problem. In this paper we take a slightly different viewpoint and try to assess the ability of a user (who is dictating the activity in the system and indirectly the observations generated) to avoid revealing to the outside observer that the initial state of the system lied within the set of secret states S. A system that does not allow the user to act indefinitely in such a way is said to posses the property of *resolution of initial state with respect to* S. We show that in discrete event systems that can be modeled as non-deterministic labeled finite automata, this property can be verified with polynomial complexity in a way that resembles the verification of diagnosability.**

I. Introduction

Motivated by the increased reliance of many applications on shared cyber-infrastructures (ranging from defense and banking to health care and power distribution systems), various notions of *security and privacy* have received considerable attention from researchers. One category of such notions focuses on the *information flow* from the system to the intruder. In particular, *opacity* is a security notion that aims to determine whether a given system's *secret* behavior (i.e., a subset of the behavior of the system that is considered critical and is usually represented by a predicate) is kept opaque to outsiders [1], [2]. Typically, this requires that the intruder, who observes the system's behavior through some projection map, never be able to establish the truth of the predicate.

In earlier work [3], we considered opacity with respect to state-based predicates in a discrete event system (DES) that can be modeled as a non-deterministic finite automaton G with partial observation on its transitions. Specifically, assuming that the initial state of G is (partially) unknown, the notion of *initial-state opacity* requires that no sequence of transitions allows the intruder (who has full knowledge of the system model and tracks the sequence of observable transitions) to unambiguously determine that the initial state of the system belonged to a given set of secret states S. Examples to motivate the study of initial-state opacity in the context of sensor network coverage and encryption using pseudo-random generators can be found in [3], [4]. The verification of initial-state opacity for a given non-deterministic finite automaton G is polynomially equivalent to the language containment problem for non-deterministic finite automata and, thus, it is a PSPACE-complete problem (at least in its general form). One way to verify initial state opacity is to use the *initial-state estimator* for G as discussed in [3]; this method has complexity $O(2^{N^2})$ where N is the number of states of the given system G, but can be improved to $O(4^N)$ via the use of state-status mappings [5].

In this paper, we consider the related notion of resolution of initial state with respect to a set of secret states S. The setup is similar to the one described above: one is given a non-deterministic finite automaton G with partial observation on its transitions, and a set of secret states S. An observer, with full knowledge of the system model, tracks system activity through some natural projection map and aims to determine whether the initial state of the system definitely lied within the set of secret states S. Resolution of initial state with respect to set S requires that when the system starts from a secret state, the observer will be able to eventually (i.e., after a finite sequence of events/observations) determine with certainty that the system initial state lied within the set of secret states S. This should be contrasted to the notion of initial-state opacity which requires that the intruder never be able to determine with certainty that the system started within the set of secret states S, regardless of the sequence of events and the sequence of observations it generates. It is worth pointing out at this point that absence of resolution of initial state is necessary but not sufficient for initial-state opacity. As we show in this paper, resolution of initial state with respect to a set of secret states S can be verified with polynomial complexity. We establish this by reducing the problem to the verification of diagnosability for a given non-deterministic finite automaton, which is solvable with polynomial complexity [6], [7].

The work in this paper is related to earlier work that studied notions of opacity in discrete event systems, such as [8] and [9] (which focus on finite state Petri nets and define opacity with respect to state-based predicates), [10] (which considers multiple intruders that are modeled as observers with different observation capabilities and requires that no intruder be able to determine that the actual trajectory of the system belongs to the secret language assigned to that intruder), and [11] (which considers a single intruder that might observe different events than the ones

This work falls under the Cyprus Research Promotion Foundation's Framework Programme for Research, Technological Development and Innovation 2009-2010 (DESMI 2009-2010), co-funded by the Republic of Cyprus and the European Regional Development Fund, under Grant TIIE/OPIZO/0609(BE)/08. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the funding agency.

C. N. Hadjicostis is with the Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus. Author's address: 75 Kallipoleos Avenue, P.O. Box 20537, 1678 Nicosia, Cyprus. E-mail: chadjic@ucy.ac.cy.

978-1-4673-2529-5/12/$31.00 ©2012 IEEE

observed/controlled by the supervisor and establishes that a minimally restrictive supervisor always exists, but might not be regular). Work that has appeared in the context of testing digital sequential circuits, where the initial state might be unknown and the task is to identify the initial state of the machine, is also relevant. For instance, a distinguishing sequence is an input sequence that produces a unique output sequence for each possible starting state, thus allowing the observer to differentiate among possible starting states [12]. The work in [13] has shown that it is PSPACE-complete to determine whether or not a deterministic finite automaton has a distinguishing sequence (as there exist machines whose shortest distinguishing sequence is exponential in length). However, [13] has also shown that one can determine in polynomial time whether a deterministic finite automaton has an "adaptive" distinguishing sequence Our work here is more general in that it deals with non-deterministic automata and only requires the states to be resolved with respect to a set of states (that is not necessarily a singleton set). This is also the difference of our work in this paper with the work on observabiility/invertibility of DES in [14], [15] and the work on detectability in [16]. Note that [17] addresses the ability to distinguish between clusters of states which is closer to what the approach in this paper essentially boils down to (though we actually employ a reduction to diagnosabiliy instead of detectability).

II. Background on Initial State Estimation

A. Notation

Let Σ be an alphabet (set of events) and denote by Σ^* the set of all finite-length strings of elements of Σ (sequences of events), including the empty string ϵ (the length of a string s is denoted by $|s|$ with $|\epsilon| = 0$). A language $L \subseteq \Sigma^*$ is a subset of finite-length strings (sequences of events with the first event appearing on the left) from strings in Σ^* [18]. Given strings $s, t \in \Sigma^*$, the string st denotes the concatenation of s and t, i.e., the sequence of events captured by s followed by the sequence of events captured by t. For a string s, $\overline{s}$ denotes the *prefix-closure* of s and is defined as $\overline{s} = \{t \in \Sigma^* \mid \exists t' \in \Sigma^* : \ tt' = s\}$.

A discrete event system (DES) is modeled in this paper as a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$, where $X = \{0, 1, \ldots, N-1\}$ is the set of states, Σ is the set of events, $\delta : X \times \Sigma \to 2^X$ is the non-deterministic state transition function, and $X_0 \subseteq X$ is the set of possible initial states. For a set $Q \subseteq X$ and $\sigma \in \Sigma$, we define $\delta(Q, \sigma) = \cup_{q \in Q} \delta(q, \sigma)$; with this notation at hand, the function δ can be extended from the domain $X \times \Sigma$ to the domain $X \times \Sigma^*$ in a routine recursive manner: $\delta(x, ts) := \delta(\delta(x, t), s)$ for $x \in X$, $s \in \Sigma^*$ and $t \in \Sigma$ with $\delta(i, \epsilon) := \{i\}$. The behavior of DES G is captured by $L(G) := \{s \in \Sigma^* \mid \exists x_0 \in X_0, \delta(x_0, s) \neq \emptyset\}$. We use $L(G, x)$ to denote the set of all traces that originate from state x of G (so that $L(G) = \bigcup_{x_0 \in X_0} L(G, x_0)$).

In general, only a subset Σ_{obs} ($\Sigma_{obs} \subseteq \Sigma$) of the events can be observed, so that Σ is partitioned into the set of observable events Σ_{obs} and the set of unobservable events $\Sigma_{uo} = \Sigma - \Sigma_{obs}$. The natural projection $P_{\Sigma_{obs}} : \Sigma^* \to \Sigma_{obs}^*$ can be used to map any trace executed in the system to the sequence of observations associated with it. This projection is defined recursively as $P_{\Sigma_{obs}}(\sigma s) = P_{\Sigma_{obs}}(\sigma) P_{\Sigma_{obs}}(s), \ \sigma \in \Sigma, s \in \Sigma^*$, with $P_{\Sigma_{obs}}(\sigma) = \sigma$ if $\sigma \in \Sigma_{obs}$ and $P_{\Sigma_{obs}}(\sigma) = \epsilon$ otherwise. In the sequel, the subscript Σ_{obs} in $P_{\Sigma_{obs}}$ will be dropped when it is clear from context.

Any $m \in 2^{X^2}$ is a subset of X^2 and contains some pairs of states. In this paper, m will be viewed as a *state mapping* consisting of pairs of a starting state and an ending state. The set of states included as the first (second) component in these pairs is called the set of starting (ending) states of m. We denote the set of starting states for state mapping m by $m(1)$ and the set of ending states by $m(2)$. The composition operator $\circ : 2^{X^2} \times 2^{X^2} \to 2^{X^2}$ for state mappings $m_1, m_2 \in 2^{X^2}$ is defined as

$$m_1 \circ m_2 := \{(i_1, i_3) | \exists i_2 \in X \{(i_1, i_2) \in m_1, (i_2, i_3) \in m_2\}\}$$

We can map any observation of finite but arbitrary length in DES G to a state mapping by using the mapping $M : \Sigma_{obs}^* \to 2^{X^2}$ defined for $\omega \in \Sigma_{obs}^*$ as

$$M(\omega) = \{(i, j) \mid i, j \in X, \exists s \in \Sigma^* \{P(s) = \omega, j \in \delta(i, s)\}\}$$

which we call the ω-induced state mapping. The pair $(i, j) \in M(\omega)$ implies that there exists a sequence of events that starts from state i and ends in state j, and produces observation ω. Finally, for any $Z \subseteq X$, we define the operator $\odot : 2^X \to 2^{X^2}$ to represent $Z \odot Z := \{(i, i) \mid i \in Z\}$.

B. Initial State Estimation and Initial-State Opacity

Definition 1 (Initial-State Estimate): Given a deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ and a natural projection map P with respect to the set of observable events Σ_{obs}, the initial-state estimate after observing string $\omega \in \Sigma_{obs}^*$ is defined as

$$\hat{X}_0(\omega) = \{x_0 \in X_0 \mid \exists s \in \Sigma^* \ \{P(s) = \omega, \delta(x_0, s) \neq \emptyset\}\} \ .$$

In [3] we introduced the construction of the initial-state estimator (ISE), i.e., a deterministic finite automaton $G_{Iobs} = (X_{Iobs}, \Sigma_{obs}, \delta_{Iobs}, X_{Iobs0})$ that is driven by observable events in Σ_{obs} and its states are state mappings, i.e., $X_{Iobs} \subseteq 2^{X^2}$. The ISE construction ensures the following property: given the observation of a sequence of labels $\omega \in \Sigma_{obs}^*$, $\omega \neq \epsilon$ (generated by unknown underlying activity in the system G), the ISE reaches a state $m = \delta_{Iobs}(X_{Iobs0}, \omega)$ such that the set of possible initial states is captured by the initial states associated with m, i.e., for $\omega \neq \epsilon$

$$\hat{X}_0(\omega) = m(1) \text{ where } m = \delta_{Iobs}(X_{Iobs0}, \omega) \ .$$

Note that the ISE, formally described below, has at most 2^{N^2} states where N is the number of states of the finite automaton G.

Definition 2 (Initial-State Estimator (ISE)): Given a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ and a projection map P with respect to the set of observable events Σ_{obs}, we define the initial-state estimator as the deterministic finite automaton $G_{Iobs} = AC(2^{X^2}, \Sigma_{obs}, \delta_{Iobs}, X_{Iobs0})$ with

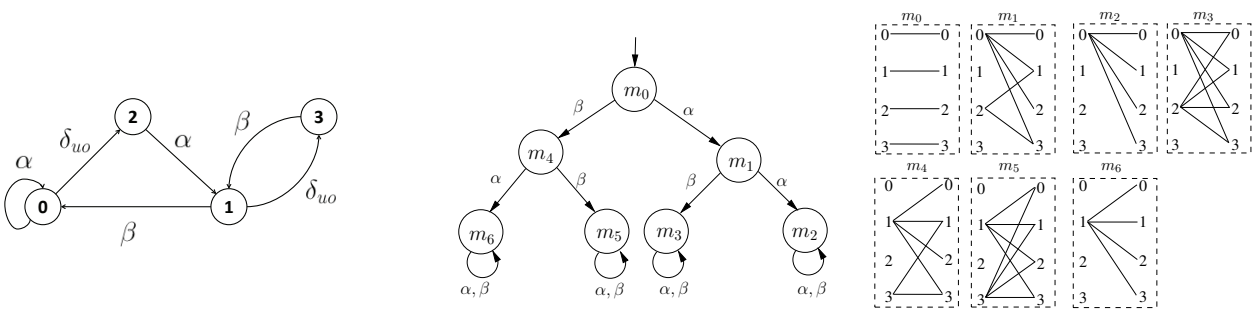

Fig. 1. Non-deterministic finite automaton G with $\Sigma_{obs} = \{\alpha, \beta\}$ (left) and its initial-state estimator (right).

state set 2^{X^2} (power set of $X \times X$), event set Σ_{obs}, initial state $X_{Iobs0} = X_0 \odot X_0$, and state transition function $\delta_{Iobs} : 2^{X^2} \times \Sigma_{obs} \to 2^{X^2}$ defined for $\alpha \in \Sigma_{obs}$ as

$$m' = \delta_{Iobs}(m, \alpha) := m \circ M(\alpha),$$

where $m, m' \in 2^{X^2}$. Recall that $M(\alpha)$ denotes the state mapping that is induced by symbol $\alpha \in \Sigma_{obs}$ and AC denotes the states that are accessible from initial state X_{Iobs0} via δ_{Iobs}. If we let $X_{Iobs} \subseteq 2^{X^2}$ be the reachable states from the initial state X_{Iobs0} under δ_{Iobs}, then $G_{Iobs} = (X_{Iobs}, \Sigma_{obs}, \delta_{Iobs}, X_{Iobs0})$.

Example 1: The following example (adopted from [3]) is used to clarify the notation and the ISE construction. Consider the finite automaton $G = (X, \Sigma, \delta, X_0)$ shown on the left of Fig. 1, where $X = \{0, 1, 2, 3\}$, $\Sigma = \{\alpha, \beta, \delta_{uo}\}$, δ is as defined by the transitions in the figure, and $X_0 = X = \{0, 1, 2, 3\}$. Assume that $\Sigma_{obs} = \{\alpha, \beta\}$ and $\Sigma_{uo} = \{\delta_{uo}\}$. To construct the α-induced state mapping, i.e., $M(\alpha)$, note that α can be observed from states 0 and 2. Upon this observation, if the initial state was 0, the ending state can be any of the states in $\{0, 1, 2, 3\}$. However, if the initial state was 2, the ending state could only be any state in $\{1, 3\}$. Hence $M(\alpha) = \{(0,0), (0,1), (0,2), (0,3), (2,1), (2,3)\}$. Following the same reasoning, we obtain $M(\beta) = \{(1,0), (1,1), (1,2), (1,3), (3,1), (3,3)\}$. The composition of these two state mappings yields $M(\alpha) \circ M(\beta) = \{(0,0), (0,1), (0,2), (0,3), (2,0), (2,1), (2,2), (2,3)\}$ and indicates that if we observe $\alpha\beta$, we could start from state 0 or 2 and (in each case) end up in any of the system states (0, 1, 2 or 3). The bottom left of Fig. 1 shows the initial-state estimator for this system. The initial uncertainty is assumed to be equal to the state space and hence $m_0 = X_0 \odot X_0 = \{(0,0), (1,1), (2,2), (3,3)\}$. (On the right of Fig. 1, we use a graphical way to describe the pairs associated with each state of the ISE.) Upon observing α, the next state of the ISE becomes

$$m' = \delta_{Iobs}(m_0, \alpha) = m_0 \circ M(\alpha)$$
$$= \{(0,0), (0,1), (0,2), (0,3), (2,1), (2,3)\} = M(\alpha) \equiv m_1 .$$

Next, assume that we observe β; following the same reasoning as in the case of $M(\alpha)$, we first obtain $M(\beta) = \{(1,0), (1,1), (1,2), (1,3), (3,1), (3,3)\}$ and then we have

$$m' = \delta_{Iobs}(m_1, \beta) = m_1 \circ M(\beta) = M(\alpha) \circ M(\beta) =$$
$$= \{(0,0), (0,1), (0,2), (0,3), (2,0), (2,1), (2,2), (2,3)\} .$$

Using this approach for all possible observations (from each state), the ISE construction can be completed as shown on the right of Fig. 1. □

The notion of initial-state opacity in DES that are modeled as non-deterministic finite automata requires that the membership of the initial state to a given set of secret states S remain opaque to an external observer who is observing the events that occur in the system through the natural projection map P [3].

Definition 3 (Initial-State Opacity): Given a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$, a natural projection map P with respect to the set of observable events Σ_{obs}, and a set of secret states $S \subseteq X$, automaton G is initial-state opaque with respect to S and P if for all $x_s \in S \cap X_0$ and for all $s \in L(G, x_s)$ we have $\exists x_{ns} \in X_0 - S, \exists t \in L(G, x_{ns}), P(s) = P(t)$.

A system is initial state opaque if and only if [3]

$$\forall \omega \in \Sigma^*_{obs} \{\hat{X}_0(\omega) \not\subseteq S \text{ OR } \hat{X}_0(\omega) = \emptyset\} .$$

It is worth pointing out that the verification of initial-state opacity is a PSPACE-complete problem when the number of observable events satisfies $|\Sigma_{obs}| > 1$ [5]. The non-deterministic finite automaton G is initial state opaque with respect to a set of secret states S under natural projection map P if and only if [3]

$$\forall x_{Iobs} \in X_{Iobs} : x_{Iobs}(1) \not\subseteq S \text{ OR } x_{Iobs} = \emptyset ,$$

where X_{Iobs} is the set of (reachable) states of the ISE G_{Iobs}.

Thus, one way to verify initial-state opacity is to first construct the ISE and then check whether the above condition holds. For instance, due to the existence of state m_6 in the ISE on the right of Fig. 1, the system G on the left of Fig. 1 is not initial state opaque with respect to the set of secret states $S = \{1\}$; however, the system is initial state opaque with respect to the set of secret states $S = \{2, 3\}$. Note that one can simplify the verification method via the use of state-status mappings [5].

III. Resolution of Initial State

Consider a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ under a natural projection map P with respect to a set of observable events Σ_{obs}, $\Sigma_{obs} \subseteq \Sigma$, and a set of secret states S, $S \subseteq X$. We assume that (i) the system is live (i.e., there is a transition defined at each state $x \in X$, thus the system cannot reach a state from which no transition is possible), and (ii) there does not exist a cycle of unobservable events in the system (i.e., there exists integer n_0 such that for all strings $ust \in L(G)$, $s \in \Sigma_{uo}^*$, $u, t \in \Sigma^*$, we have $|s| \leq n_0$). Note that the above assumptions are rather standard in the field of fault diagnosis and are made here in order to make the connections with results in that area more direct. Both of these assumptions can easily be relaxed at the cost of slightly modifying the definitions (e.g., by focusing on infinite behaviors and by expressing requirements in terms of observations rather than events).

We say that the system possesses the property of *resolution of initial state with respect to the set of secret states* S if there does *not* exist an arbitrarily long sequence of events $s \in L(G, X_0 \cap S)$ that generates an arbitrarily long sequence of observations $P(s)$ such that an external observer (modeled as an initial state estimator) cannot eventually be certain that the initial state of the system lied within the set of secret states S. In other words, if the system starts exclusively from one or more secret states in S, the fact that its initial state lied in S eventually gets resolved by the observer. Formally, we have the following definition.

Definition 4 (Resolution of Initial State): Given a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ under a natural projection map P with respect to the set of observable events Σ_{obs}, $\Sigma_{obs} \subseteq \Sigma$, we say that system G possesses the property of resolution of initial state with respect to a set of secret states S, $S \subseteq X$, if there exists integer n_0, such that for all $x_s \in X_0 \cap S$ and for all $s \in L(G, x_s)$ of length $|s| \geq n_0$, we have $\hat{X}_0(P(s)) \subseteq S$.

Note that S can be taken without loss of generality to be a subset of X_0 (one can easily show that $G = (X, \Sigma, \delta, X_0)$ under the natural projection map P possesses the property of initial state resolution with respect to S if and only if it possesses the property of initial state resolution with respect to $S' = X_0 \cap S$).

IV. Verification of Resolution of Initial State

Consider a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ under a natural projection map P with respect to a set of observable events Σ_{obs}, $\Sigma_{obs} \subseteq \Sigma$. We assume that G is live and does not exhibit cycles of unobservable events. In this section we describe how resolution of initial state with respect to a set of secret states S, $S \subseteq X$, can be verified. We present two approaches, one approach using the ISE (which has complexity $O(2^{N^2})$ where N is the number of states of G) and one approach using a verifier which has complexity polynomial in the size of G. Due to space limitations, we aim primarily to provide intuition and only sketch the proof for each approach.

A. Verification using the ISE

Resolution of initial state with respect to a set of secret states S, where $S \subseteq X$, can be verified by constructing[1] the ISE G_{Iobs} and performing the following steps:

Step 1: Mark all states m in G_{Iobs} for which the set of initial states $m(1)$ has at least one state in S and at least one state in $X - S$. These are states associated with estimates of the initial state that are confusing in the sense that it is possible that the system started from a secret state, but the observer cannot be certain about it (because it is also possible that the system started from a non-secret state).

Step 2: Determine whether there exist cycles of such marked states in the system. To do that, one essentially treats G_{Iobs} as a graph, where states represent nodes, and transitions from a state to another state represent links from a node to another node; then, one tries to find cycles involving nodes that (correspond to states that) have been marked in Step 1.

Step 3: If there exists at least one cycle from Step 2, declare that the system does not possess the property of resolution of initial state with respect to the set of secret states S; otherwise, declare that the system possesses the property.

For the reader who is familiar with work on fault diagnosis in finite automata (starting with [19] and subsequently pursued by many other researchers), the above approach is quite natural. The cycles identified in Step 2, if any, essentially correspond to indeterminate cycles and imply that there is an arbitrarily long sequence of events that can occur in the system and keep the observer uncertain whether the initial state belonged to the set of secret states or not.[2] Note that checking for cycles of marked states in Step 2 is of linear complexity in the number of states of G_{Iobs} (which, however, is of size $O(2^{N^2})$ with N being the number of states of the given system G).

B. Verification using a Verifier

In this section we describe how resolution of initial state can be reduced to the problem of fault diagnosis in an appropriately constructed automaton. We first recall a simplified problem formulation for fault diagnosis in finite automata [19], [7], [6]. Specifically, we consider a non-deterministic finite automaton $G_F = (X_F, \Sigma_F, \delta_F, x_{F0})$ where X_F is the set of states, Σ_F is the set of events, $\delta_F : X_F \times \Sigma_F \rightarrow 2^{X_F}$ is the non-deterministic next state transition function, and $x_{F0} \in X_F$ is the initial state. We assume a natural projection map with respect to the set of observable events Σ_{Fobs}, $\Sigma_{Fobs} \subseteq \Sigma_F$. Among the remaining (unobservable) events $\Sigma_{Fuo} = \Sigma_F - \Sigma_{Fobs}$, a subset F comprises the fault events that need to be detected; in other words, we have $\Sigma_F = \Sigma_{Fobs} \dot{\cup} \Sigma_{Fuo}$ and $F \subseteq \Sigma_{Fuo}$. Detection of the fault events requires that, once a fault event occurs, an external

[1] More details about the construction of the ISE can be found in [3] where it was used to verify initial state opacity; the property of resolution of initial state and its verification were not considered in [3].

[2] In the case of diagnosis some of these cycles might not be problematic in the sense that, if the fault occurs, the cycles will necessarily be broken within a finite number of events; in our case, we need not worry about this case (the reason will become evident in the next section when the verification of resolution of initial state is reduced to the verification of diagnosability).

diagnoser (that observes the activity in the system via the natural projection map $P_{\Sigma_{Fobs}}$) is able to determine with certainty that a fault has occurred and it can do so after the occurrence of at most n_0 events, where n_0 is some finite integer. This problem is described more formally below.

Definition 5: Consider a non-deterministic finite automaton $G_F = (X_F, \Sigma_F, \delta_F, x_{F0})$ under a natural projection map P with respect to the set of observable events Σ_{Fobs}, and assume that G_F is live and exhibits no cycles of unobservable events. Given a set of fault events F, $F \subseteq \Sigma_{Fuo}$ (where $\Sigma_{Fuo} \equiv \Sigma_F - \Sigma_{Fobs}$), we say that G_F is diagnosable with respect to F if there exists an integer n_0 such that for all $(sft) \in L(G_F)$, $s \in (\Sigma_F - F)^*$, $f \in F$, $t \in \Sigma_F^*$: if $|t| \geq n_0$ then

$$(\forall u \in L(G_F), P(u) = P(sft))(\exists v \in \Sigma_F^*, \exists f \in F\{vf \in \overline{u})\})$$

where $\overline{u}$ is the set of prefixes for u.

In words, G_F is diagnosable with respect to F if, once a fault event $f \in F$ occurs, we will be able (after the occurrence of at most n_0 events — and thus at most n_0 observations) to determine that a fault has occurred. The reason is that all sequences of events that might have generated the observed sequence include the occurrence of a fault event at some point in the past. Determining whether G_F is diagnosable or not is a problem that can be verified with complexity that is polynomial in the size of G_F. In fact, the literature studies more complex versions of the problem stated above, also addressing the need to classify faults into different fault classes. The authors of [7] establish that the complexity of verifying diagnosability for a non-deterministic finite automaton G_F is $O(N_F^4 \times K_F)$ where $N_F = |X_F|$ is the number of states and $K_F = |\Sigma_{Fobs}|$ is the number of observable events in G_F (the algorithm is actually exponential in the number of fault types but in our case there is only one fault type). For the case of a deterministic G_F, the authors of [6] establish that the verification of diagnosability can be done with complexity $O(N_F^2 \times K_F)$ (the algorithm presented is linear in the number of fault types but this is not relevant in the discussion here).

We now return to the problem of resolution of initial state for a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ under a natural projection map P with respect to a set of observable events Σ_{obs}, $\Sigma_{obs} \subseteq \Sigma$. We assume that the set of secret states is given by $S \subseteq X$ and that G is live and does not exhibit cycles of unobservable events. We first construct the non-deterministic finite automaton $G_F = (X_F, \Sigma_F, \delta_F, x_{F0}) \equiv (X \dot\cup \{x_{F0}\}, \Sigma \dot\cup \{f\} \dot\cup \{\delta_{nf}\}, \delta_F, x_{F0})$ where δ_F is defined as follows:

$$\begin{aligned}
\delta_F(x_{F0}, f) &= X_0 \cap S\ , \\
\delta_F(x_{F0}, \delta_{nf}) &= X_0 - S\ , \\
\delta_F(x_{F0}, \sigma) &= \emptyset \text{ for } \sigma \in \Sigma\ , \\
\delta_F(x, f) &= \emptyset \text{ for } x \in X\ , \\
\delta_F(x, \delta_{nf}) &= \emptyset \text{ for } x \in X\ , \\
\delta_F(x, \sigma) &= \delta(x, \sigma) \text{ for } x \in X, \sigma \in \Sigma\ .
\end{aligned}$$

Note that f and δ_{nf} denote new events (not in Σ) that are both taken to be unobservable. This implies that in G_F the set of observable events is $\Sigma_{Fobs} = \Sigma_{obs}$, and the set of unobservable events is $\Sigma_{Fuo} = \Sigma_{uo} \dot\cup \{f, \delta_{nf}\}$. The next state transition function δ_F is chosen so that G_F starts from state x_{F0} and transitions to secret states in $X_0 \cap S$ under fault f and to non-secret states in $X_0 - S$ under unobservable event δ_{nf}. From that point onwards, the behavior of G_F is identical to the behavior of G.

We are now ready to prove the following theorem.

Theorem 1: Consider a non-deterministic finite automaton $G = (X, \Sigma, \delta, X_0)$ under a natural projection map P with respect to a set of observable events Σ_{obs}, $\Sigma_{obs} \subseteq \Sigma$. Let the set of secret states be given by S, $S \subseteq X$, and assume that G is live and does not exhibit cycles of unobservable events. Construct the non-deterministic finite automaton G_F as described above, with observable events $\Sigma_{Fobs} = \Sigma_{obs}$, unobservable events $\Sigma_{Fuo} = \Sigma_{uo} \dot\cup \{f, \delta_{nf}\}$, and set of fault events $F = \{f\}$. Then, G possesses the property of resolution of initial state under the natural projection map $P_{\Sigma_{obs}}$ with respect to secret set of states S if and only if G_F is diagnosable under the natural projection map $P_{\Sigma_{Fobs}}$ and set of fault events $F = \{f\}$.

Proof: Note that if G is live and does not exhibit any cycles of unobservable events, these properties also hold for G_F. Also, if a fault appears in a sequence of events $s_F \in L(G_F)$ generated by G_F, then f is the first event of s_F and, in addition, $s_F = fs$ for some $s \in L(G, X_0 \cap S)$. Conversely, if a fault does not appear in the sequence of events $s_F \in L(G_F)$, then s_F is of the form $s_F = \delta_{nf} s$ for some $s \in L(G, X_0 - S)$. With the above observation, it is not hard to complete the proof as follows:

(i) If G_F is diagnosable, from Definition 5 and the above observation, there exists an integer n_0 such that $(\forall (ft) \in L(G_F), t \in \Sigma^*) : \{|t| \geq n_0\} \Rightarrow \{(\forall u \in L(G_F), P_{\Sigma_{Fobs}}(u) = P_{\Sigma_{Fobs}}(ft))(u = fu' \text{ for some } u' \in \Sigma^*\}$. Since for strings $s \in \Sigma_{obs}^*$, $P_{\Sigma_{Fobs}}(s) = P_{\Sigma_{obs}}(s)$, this means that for all $t \in L(G, X_0 \cap S)$ with $|t| \geq n_0$, all $u' \in L(G)$ that have the same projection as t (i.e., all u' such that $P_{\Sigma_{obs}}(u') = P_{\Sigma_{obs}}(t)$) are strings that belong in $L(G, X_0 \cap S)$. Thus, if the system has started from a state in S (more precisely, a state in $X_0 \cap S$), we will be able to determine this after the occurrence of at most n_0 events. Therefore, G possesses the property of resolution of initial state with respect to the set of secret states S.

(ii) If G_F is not diagnosable, from Definition 5 and the observations in the beginning of the proof, we have that for any integer n_0, there exists $(ft) \in L(G_F), |t| \geq n_0$, such that there exists $u \in L(G_F)$ with $P_{\Sigma_{Fobs}}(u) = P_{\Sigma_{Fobs}}(ft)$ and $u = \delta_{nf} u'$ for some $u' \in \Sigma^*$. Since for strings $s \in \Sigma_{obs}^*$, $P_{\Sigma_{Fobs}}(s) = P_{\Sigma_{obs}}(s)$, this means that for any n_0 we can find a $t \in L(G, X_0 \cap S)$ with $|t| \geq n_0$ and a $u' \in L(G, X_0 - S)$ that has the same projection as t (i.e., $P_{\Sigma_{obs}}(u') = P_{\Sigma_{obs}}(t)$). Thus, if the system has started from a state in S (more precisely a state in $X_0 \cap S$), we will not able to conclude, despite the subsequent occurrence of n_0 events, that the state of the system belonged in S. Therefore, G does not possess the property of resolution of initial state with respect to the set of secret states S. ■

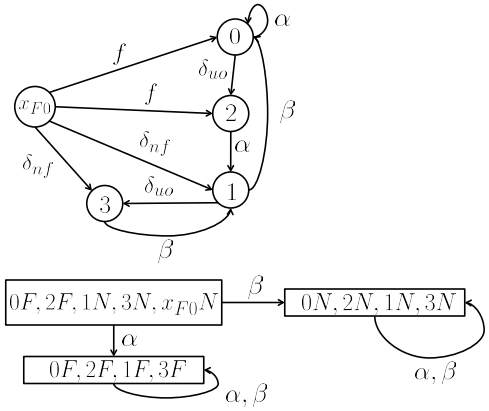

Fig. 2. Automaton G_F corresponding to the finite automaton G in Fig. 1 (top) and its diagnoser (bottom).

Remark 1: The complexity of the above verification method is the complexity of verifying diagnosability for G_F. Using the method in [7], this complexity (in terms of the parameters of G) is $O((N+1)^4K)$ where $N = |X|$ and $K = |\Sigma_{obs}|$. Note that another method for verifying diagnosability is to construct the diagnoser for G_F and look for indeterminate cycles in it. This resembles the method mentioned at the end of Section II-B based on the use of state-status mappings and it is likely to be more efficient because the diagnoser has state complexity $O(2^N)$ (unlike the ISE which has state complexity $O(2^{N^2})$). □

Example 2: The finite automaton G_F that corresponds to the finite automaton G on the left of Fig. 1 for set of secret states $S = \{0, 2\}$ is shown at the top of Fig. 2, and the diagnoser for G_F with $F = \{f\}$ is shown at the bottom of the figure (events f and δ_{nf} are unobservable). We can see that there are no indeterminate cycles in the diagnoser; therefore, we conclude that G_F is diagnosable with respect to F which is equivalent to G having the property of resolution of initial state with respect to the set of secret states $S = \{0, 2\}$. This also agrees with the conclusion we would reach if we used the three-step method described at the beginning of Section IV-A: in the ISE for G shown in Fig. 1, the only marked state would be state m_0 which is not associated with a cycle.

Note that the verification of diagnosability for G_F using the method in [6] (note that in this case G_F is a deterministic finite automaton) could be used as an alternative approach with polynomial complexity. □

V. Conclusions

In this paper, motivated by a variety of security applications, we define, analyze and verify the property of resolution of initial-state with respect to a set of secret states S for a given non-deterministic finite automaton G under some natural projection map P with respect to a set of observable events Σ_{obs}. We have shown that resolution of initial state is a property that can be verified with complexity polynomial in the size of G; to do that, we obtained a reduction of the problem to the problem of diagnosability (which is known to be verifiable with polynomial complexity). Future work should try to extend these ideas to systems beyond finite automata. It might also be worthwhile to identify classes of systems for which resolution of initial state does not hold and try to obtain strategies (sequences of events) that keep the observer uncertain regarding the initial state of the system while achieving some pre-specified control or performance goal. This can have important implications in security applications where the system needs to be driven to specific states without revealing properties of its initial state.

References

[1] J. W. Bryans, M. Koutny, L. Mazare, and P. Y. A. Ryan, "Opacity generalised to transition systems," in *Proceedings of the 3rd Int. Workshop on Formal Aspects in Security and Trust*, July 2005, pp. 81–95.

[2] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *Proceedings of the 46th IEEE Conference on Decision and Control*, December 2007, pp. 5056–5061.

[3] ——, "Initial-state estimation and its application to security problems," in *Proceedings of the 9th International Workshop on Discrete Event Systems*, Gotenborg, Sweden, May 2008, pp. 328–333.

[4] ——, "Coverage analysis of mobile agent trajectory via state-based opacity formulations," *Control Engineering Practice (Special Section: DCDS'09 – The 2nd IFAC Workshop on Dependable Control of Discrete Systems)*, vol. 19, no. 9, pp. 967–977, September 2011.

[5] A. Saboori, "Verification and enforcement of state-based notions of opacity in discrete event systems," Ph.D. dissertation, University of Illinois, Urbana, IL, 2010.

[6] T.-S. Yoo and S. Lafortune, "Polynomial-time verification of diagnosability of partially observed discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 47, no. 9, pp. 1491–1495, September 2002.

[7] S. Jiang, Z. Huang, V. Chandra, and R. Kumar, "A polynomial algorithm for testing diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 46, no. 8, pp. 1318–1321, August 2001.

[8] J. W. Bryans, M. Koutny, and P. Y. A. Ryan, *Modelling dynamic opacity using Petri nets with silent actions*, ser. Formal Aspects in Security and Trust. Springer, 2005, vol. 173, pp. 159–172.

[9] ——, "Modelling opacity using Petri nets," *Electronic Notes in Theoretical Computer Science*, vol. 121, pp. 101–115, February 2005.

[10] E. Badouel, M. Bednarczyk, A. Borzyszkowski, B. Caillaud, and P. Darondeau, "Concurrent secrets," in *Proceedings of the 8th International Workshop on Discrete Event Systems*, July 2006, pp. 51–57.

[11] J. Dubreil, P. Darondeau, and H. Marchand, "Opacity enforcing control synthesis," in *Proceedings of the 9th International Workshop on Discrete Event Systems*, May 2008, pp. 28–35.

[12] F. C. Hennie, *Finite State Models for Logical Machines*. New York: Wiley, 1968.

[13] M. Yannakakis and D. Lee, "Testing finite-state machines: state identification and verification," *IEEE Transactions on Computers*, vol. 43, no. 3, pp. 209–227, March 1994.

[14] C. M. Özveren and A. S. Willsky, "Observability of discrete event dynamic systems," *IEEE Transactions on Automatic Control*, vol. 35, no. 7, pp. 797–806, July 1990.

[15] ——, "Invertibility of discrete event dynamic systems," *Mathematics of Control, Signals, and Systems*, vol. 5, no. 4, pp. 365–390, July 1992.

[16] S. Shu, F. Lin, and H. Ying, "Detectability of discrete event systems," *IEEE Transactions on Automatic Control*, vol. 52, no. 12, pp. 2356–2359, December 2007.

[17] W. Wang, S. Lafortune, and F. Lin, "An algorithm for calculating indistinguishable states and clusters in finite-state automata with partially observable transitions," *Systems and Control Letters*, vol. 56, pp. 656–661, 2007.

[18] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Kluwer Academic Publishers, 1999.

[19] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete event systems," *IEEE Transactions on Control Systems Technology*, vol. 40, no. 9, pp. 1555–1575, September 1995.