2008 American Control Conference
Westin Seattle Hotel, Seattle, Washington, USA
June 11-13, 2008

Diagnosability of Stochastic Discrete-Event Systems Under Unreliable Observations

David Thorsley, Tae-Sic Yoo, and Humberto E. Garcia

***Abstract*— We investigate diagnosability of stochastic discrete-event systems where the observation of certain events is unreliable, that is, there are non-zero probabilities of the misdetection and misclassification of events based on faulty sensor readings. Such sensor unreliability is unavoidable in applications such as nuclear energy generation. We propose the notions of uA- and uAA-diagnosability for stochastic automata and demonstrate their relationship with the concepts of A- and AA-diagnosabilty defined in [1]. We extend the concept of the stochastic diagnoser to the unreliable observation paradigm and find conditions for uA- and uAA-diagnosability.**

I. Introduction

In this paper, we consider the property of diagnosability of stochastic discrete-event systems (DES) in situations where sensor readings are not always reliable. Our research is motivated by applications in nuclear power generation. Public confidence in the safety of nuclear energy generation can be improved through the use of realtime safety assessment and on-line detection of facility misuse. DES models have been demonstrated to be an effective tool for modeling the flow of entities in nuclear systems for the purposes of fault monitoring and anomaly detection [2]; furthermore, the ability to track flows of entities within a system has many other applications, including network security, mission planning, and operations safety [3].

The problem of failure diagnosis has been considered extensively in the literature for DES (see [4] and the references therein for an overview) and many techniques for both on-line state estimation and diagnosis and off-line verification of the property of diagnosability ([5], [6]) have been developed. In contrast to the "logical" automaton models and diagnosability results found in the above references, recent work has investigated diagnosability properties in stochastic DES ([1], [7]).

Most of the established literature on fault diagnosis makes a seemingly innocuous assumption as to the capabilities of sensors. The DES is observed through the events, or abrupt transitions between states, that occur along its trajectory. Events are classified as either observable, in which case a sensor outputs a reading when the event occurs, or unobservable, in which case no sensor outputs a reading. Failures are often modeled as instances of unobservable events.

The implicit assumption in this sensor model is that all the sensors reading observable events are perfectly reliable, that is, whenever an observable event occurs, the sensor charged with detecting an instance of that event will transmit its occurrence. In practice in nuclear systems, we cannot make this assumption; the difficulty in placing sensors and analyzing sensor data makes sensors inherently unreliable. Furthermore, the placement of additional equipment to improve the sensor reliability may degrade the overall performance of the system. Recently, the problem of unreliable sensors has been considered in [8]; the approach we take in this paper is complimentary to [8] and is based on the formal verification of diagnosability properties.

In this paper, we consider two main categories of sensor unreliability: *misclassification*, where a sensor reports an incorrect reading as a result of the occurrence of a particular event, or *misdetection*, where a sensor does not make a reading as a result of an event's occurrence. We consider an observation paradigm in which both of these types of incorrect reading can occur and develop a methodology for performing diagnosis in the presence of this sensor unreliability. Our paper builds upon the *stochastic diagnoser* methodology proposed in [1], which in turn builds upon the "logical" diagnoser approach first proposed in [9].

Our paper is organized as follows. In Section II, we define the system model, the observation model, and the failure model under consideration. In Section III, we present new definitions of stochastic diagnosability for systems with unreliable sensors. In Section IV, we discuss the construction of the stochastic diagnoser under unreliable observations. In Section V, we state conditions for stochastic diagnosability in terms of the stochastic diagnoser. A short discussion ends the paper in Section VI.

II. Formalism

A. System Model

Following [1], the system model used is a stochastic automaton. A stochastic automaton is defined as a quadruple $SA = (X^{SA}, \Sigma^{SA}, p^{SA}, x_0^{SA})$ where X^{SA}, Σ^{SA}, and x_0^{SA} are the finite state space, the set of events, and the initial state, respectively. These three elements are identical to those in a logical automaton.

Where the stochastic automaton model differs from a logical automaton is that instead of defining a partial transition function δ^{SA}, we instead define a state transition probability function $p^{SA} : X^{SA} \times \Sigma^{SA} \times X^{SA} \to [0, 1]$. For a pair of states x_1, x_2 and an event σ, $p^{SA}(x_2, \sigma \mid x_1)$ denotes the probability that, given the current state of the system is x_1, the event σ occurs and transitions the system to the state x_2.

D. Thorsley is with Department of Electrical Engineering, University of Washington, Seattle, WA, 98195, USA. T.-S. Yoo and H.E. Garcia are with the Idaho National Laboratory, Idaho Falls, ID, 83415, USA. E-mail: thorsley@u.washington.edu, {Tae-Sic.Yoo, Humberto.Garcia}@inl.gov

978-1-4244-2079-7/08/$25.00 ©2008 AACC.

To ensure that the system is live, we assume that

$$\forall x \in X^{SA}, \sum_{\sigma \in \Sigma^{SA}} \sum_{x' \in X^{SA}} p^{SA}(x', \sigma \mid x) = 1,$$

that is, the occurrence of a new transition is certain from every state. The state transition probability function can be extended to strings according to the equation

$$p^{SA}(x', es \mid x) = \sum_{x'' \in X^{SA}} p^{SA}(x'', e \mid x) p^{SA}(x', s \mid x''). \tag{1}$$

The probability of a given string occurring when the SA is in state x is defined as

$$\Pr(s \mid x) \triangleq \sum_{x' \in X^{SA}} p^{SA}(x', s \mid x). \tag{2}$$

The language generated by the state x is

$$\mathcal{L}(SA, x) \triangleq \{s \in \Sigma^* : \Pr(s \mid x) > 0\}.$$

The language generated by the stochastic automaton is $L^{SA} \triangleq \mathcal{L}(SA, x_0^{SA})$. We denote by τ the string consisting of no events. By convention, we set $p^{SA}(x, \tau \mid x) = 1$ for all $x \in X^{SA}$. Thus for all $x \in X^{SA}$, $\Pr(\tau \mid x) = 1$ and $\tau \in \mathcal{L}(SA, x)$. Where the context is clear, we will suppress the superscript SA in the notation.

B. Observation Model

In this paper, we consider deterministic and non-deterministic *mask functions*, generalized versions of the projection function used in [1]. We define a set of output symbols Δ and define a deterministic mask function $M : \Sigma \to (\Delta \cup \{\varepsilon\})$. The symbol ε denotes the null output and corresponds to no signal being observed when an event takes place and is not an element of Δ. If $M(\sigma) = \varepsilon$, then σ is *unobservable* and we define $\Sigma_{uo} \triangleq \{\sigma \in \Sigma : M(\sigma) = \varepsilon\}$. All other events are *observable* and we define $\Sigma_o \triangleq \Sigma \setminus \Sigma_{uo}$. It is possible for two distinct observable events σ_1, σ_2 to have the same observed output, i.e. it may be that $M(\sigma_1) = M(\sigma_2)$.

The mask function can be extended to strings of events recursively by defining $M(\tau) = \varepsilon$ and $M(s\sigma) = M(s)M(\sigma)$. M_L^{-1}, the inverse mask function with respect to a language L, is defined as:

$$M_L^{-1}(t) = \{s \in L : M(s) = t\}$$

The language consisting of all strings generated from state x whose only observable event is the final event is denoted by

$$\mathcal{L}_o(SA, x) \triangleq \{s \in \mathcal{L}(SA, x) : s = u\sigma, u \in \Sigma_{uo}^*, \sigma \in \Sigma_o\}.$$

If $\sigma \in \Sigma_o$, than the set of all strings generated from state x whose only observable event is the final event σ is

$$\mathcal{L}_\sigma(SA, x) \triangleq \{s \in \mathcal{L}(SA, x) : s = u\sigma, u \in \Sigma_{uo}^*\}.$$

We also consider *non-deterministic* mask functions $M_p : \Sigma \to 2^{\Delta \cup \{\varepsilon\} \times (0,1] \setminus \emptyset}$. A non-deterministic mask function randomly selects an output symbol in $\Delta \cup \{\varepsilon\}$ as the observation made when an event σ occurs. Randomness in observation is independent of randomness in the system behavior; that is, the probability that a particular output symbol occurs when an event σ occurs is independent of the probability of the occurrence of σ.

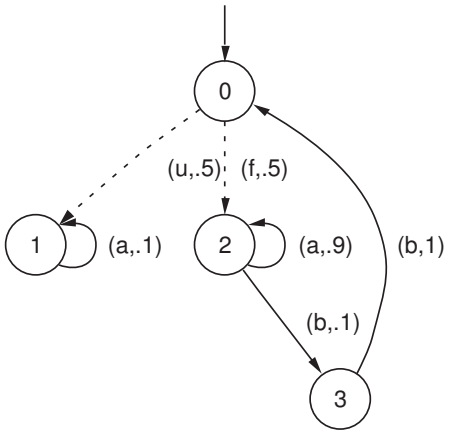

Fig. 1. A stochastic automaton to be used as a running example. The state transition probabilities are denoted by pairs (σ, q), where the labeling of an arrow $x_1 \to x_2$ indicates that $p(x_2, \sigma \mid x_1) = q$.

In the context of non-deterministic mask functions, an event σ is *unobservable* if $M_p(\sigma) = \{(\varepsilon, 1)\}$. σ is *reliably observed* if $M_p(\sigma) = \{(y, 1)\}$ for some $y \in \Delta$. If $(\varepsilon, q) \in M_p(\sigma)$ for some $0 < q < 1$, that σ is called *misdetectable* as there is a possibility that an occurrence of σ will not result in an output. If $\{(y_1, q_1), (y_2, q_2)\} \subseteq M_p(\sigma)$ for some $y_1, y_2 \in \Delta$ and $0 < q_1, q_2 < 1$, then σ is called *misclassifiable*.

We will write that

$$\Pr(M_p(\sigma) = y) = \begin{cases} q & \text{if } (y, q) \in M_p(\sigma) \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

C. Failure Model

We define a set of failure events $\Sigma_f \subseteq \Sigma$. The objective of the failure diagnosis problem is to determine the probability that an event in Σ_f has occurred given a sequence of observations $y \in \Delta^*$. The objective of the diagnosability problem is to determine conditions under which we can ensure that any occurrence of a failure will be detected. For simplicity, we will only consider failures of one type; the results of this paper can be extended to the situation where failures events are divided into multiple types.

Denote by $\Psi(\Sigma_f) \triangleq \{s \in L : s = s'f, f \in \Sigma_f\}$. If an event $f \in \Sigma_f$ is an element of a string s, we write that $\Sigma_f \in s$.

D. Example

We illustrate the extensions of the stochastic diagnoser framework using the example given in Figure 1. We denote this automaton by $SA = (X, \Sigma, p, x_0)$ where

- $X = \{0, 1, 2, 3\}$
- $\Sigma = \{a, b, u, f\}$
- p, the state transition probability, as shown in Figure 1

- $x_0 = 0$

We associate with SA the set of observable symbols $\Delta = \{\alpha, \beta\}$.

The set of events whose occurrence we wish to diagnose is $\Sigma_f = \{f\}$. The probabilistic sensor map M_p is:

$$M_p(a) = \{(\alpha, 1)\}$$
$$M_p(b) = \{(\alpha, .1), (\beta, .8), (\varepsilon, .1)\}$$
$$M_p(u) = \{(\varepsilon, 1)\}$$
$$M_p(f) = \{(\varepsilon, 1)\}$$

The event a is reliably observed: an occurrence of a will always result in an output of α. The events u and f are unobservable and any occurrences of these events will result in the null output ε. The event b is both misclassifiable and misdetectable. An observation of β is the most likely outcome; however, there is probability .1 that an incorrect sensor reading of α will be observed, and there is probability .1 that no sensor reading at all will be made when β occurs.

III. Definitions of Stochastic Diagnosability

A. Prior Work on Diagnosability of DES

The starting point for this work on stochastic diagnosability is the definition of "logical" diagnosability proposed in [9].

Definition 3.1: (Logical Diagnosability) A live, prefix-closed language L is diagnosable with respect to a set of failures Σ_f and an observation mask M if

$$(\exists n \in \mathbb{N})[\forall s \in \Psi(\Sigma_f)](\forall t \in L/s)[\|t\| \geq n \Rightarrow D(st) = 1] \tag{4}$$

where the diagnosability condition function $D : \Sigma^* \to \{0, 1\}$ is given by

$$D(st) = \begin{cases} 1 & \text{if } \omega \in M_L^{-1}[M(st)] \Rightarrow \Sigma_f \in \omega \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

This definition makes two assertions. The first of these is that for any occurrence of a fault, any continuation following a fault of sufficient length will *surely* detect the occurrence of a fault. The second of these it that, in order to detect the occurrence of a fault, we must be *completely sure* that at least one occurrence of the fault has occurred.

Two definitions of stochastic diagnosability were proposed in [1]. We restate the first of these definitions, A-diagnosability, using a general deterministic mask function M instead of the projection operation.

Definition 3.2: A live, prefix-closed language L is A-diagnosable with respect to a set of failures Σ_f, a deterministic observation mask M, and a state transition probability p if

$$(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall s \in \Psi(\Sigma_f) \wedge n \geq N)$$
$$\{\Pr(t : D(st) = 0 \mid t \in L/s \wedge \|t\| = n) < \epsilon\} \tag{6}$$

where the diagnosability condition function $D : \Sigma^* \to \{0, 1\}$ is:

$$D(st) = \begin{cases} 1 & \text{if } \omega \in M^{-1}[M(st)] \Rightarrow \Sigma_f \in \omega \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

A-diagnosability is a weaker definition than logical diagnosability because the first of the assertions in the definition of logical diagnosability is weakened. Instead of it being necessary that we be sure that a continuation of sufficient length will diagnose a fault, we need only be *almost sure* (in a probabilistic sense) that we will make a diagnosis. Thus a system can be A-diagnosable, but not logically diagnosable, while still allowing for the possibility of a false negative; however, in the long run, the probability of a false negative must become zero.

The second definition of stochastic diagnosability we proposed, AA-diagnosability, is again weaker than A-diagnosability as the second of the assertions in the definition of logical diagnosability is also weakened.

Definition 3.3: A live, prefix-closed language L is AA-diagnosable with respect to a set of failures Σ_f, a deterministic observation mask M, and a state transition probability p if

$$(\forall \epsilon > 0 \wedge \forall \alpha < 1)(\exists N \in \mathbb{N})(\forall s \in \Psi(\Sigma_f) \wedge n \geq N)$$
$$\{\Pr(t : D_\alpha(st) = 0 \mid t \in L/s \wedge \|t\| = n) < \epsilon\} \tag{8}$$

where the diagnosability condition function $D_\alpha : \Sigma^* \to \{0, 1\}$ is:

$$D_\alpha(st) = \begin{cases} 1 & \text{if } \Pr(\omega : \Sigma_f \in \omega \mid \omega \in M^{-1}[M(st)]) > \alpha \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

In AA-diagnosability, the diagnosability condition function D used in logical diagnosability and A-diagnosability is replaced by D_α; using D_α, we no longer need to be exactly sure that a fault has occurred in order to consider it diagnosed - it is sufficient that the probability of failure be above the threshold α. Thus an AA-diagnosable system will allow false positives with a probability $1 - \alpha$. The definition of AA-diagnosability states that if we take a continuation of sufficient length, we can almost surely reduce the probability of false positives until it is eventually reaches zero.

B. Diagnosability Under Unreliable Observations

For the case of a non-deterministic observation mask, there are two sources of randomness affecting the probability of a particular output symbol being observed. The first is the randomness in the underlying system behavior; the second is the randomness introduced by the observation mask. We propose two new definitions of stochastic diagnosability, uA- and uAA-diagnosability, that are the analogs to A- and AA-diagnosability under non-deterministic observation masks.

Definition 3.4: A live, prefix-closed language L is uA-diagnosable with respect to a set of failures Σ_f, a non-deterministic observation mask M_p, and a state transition probability p if

$$(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall s \in \Psi(\Sigma_f) \wedge n \geq N)$$
$$\{\Pr(t \wedge y : M_p(st) = y \wedge D^u(y) = 0$$
$$\mid t \in L/s \wedge \|t\| = n) < \epsilon\} \tag{10}$$

where the diagnosability condition function $D^u : \Delta^* \rightarrow \{0,1\}$ is:

$$D^u(y) = \begin{cases} 1 & \text{if } \Pr(M_p(\omega) = y) > 0 \Rightarrow \Sigma_f \in \omega \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

Similarly, AA-diagnosability is extended to the case of non-deterministic observation masks by the following definition.

Definition 3.5: A live, prefix-closed language L is uAA-diagnosable with respect to a set of failures Σ_f, a non-deterministic observation mask M_p, and a state transition probability p if

$$(\forall \epsilon > 0 \wedge \forall \alpha < 1)(\exists N \in \mathbb{N})(\forall s \in \Psi(\Sigma_f) \wedge n \geq N) \{\Pr(t \wedge y : M_p(st) = y \wedge D^u_\alpha(y) = 0 \mid t \in L/s \wedge \|t\| = n) < \epsilon\} \quad (12)$$

where the diagnosability condition function $D^u_\alpha : \Delta^* \rightarrow \{0,1\}$ is:

$$D^u_\alpha(y) = \begin{cases} 1 & \text{if } \Pr(\omega \in L : \Sigma_f \in \omega \mid M_p(\omega) = y) > \alpha \\ 0 & \text{otherwise} \end{cases} \quad (13)$$

In these definitions, the diagnosability condition function's domain is the set of output symbols, not the underlying string as in A- and AA-diagnosability. As one string of events in the stochastic automaton may produce many different strings of observable symbols, we define a diagnosis as being made with respect to what is observed and not with respect to the underlying system behavior. However, if the non-deterministic observation mask M_p is such that all events in Σ are either reliably observable or unobservable, then the conditions for uA- and uAA-diagnosability are identical to those for A- and AA-diagnosability.

IV. Diagnosers for Systems with Unreliable Observations Masks

A. Sensor Output Automata

The stochastic diagnoser approach developed in [1] can be used for stochastic automata with deterministic observation masks. In order to apply this approach to non-deterministic observation masks, we construct a *sensor output automaton* SOA that has a deterministic observation mask and possesses the same diagnosability properties as the original stochastic automaton with a non-deterministic mask.

The sensor output automaton is a stochastic automaton constructed from SA, Δ^{SA}, and M_p. It is defined by

$$SOA \triangleq (X^{SA}, \Delta^{SA} \cup \Delta^{SA}_f \cup \{\varepsilon, \varepsilon_f\}, p^{SOA}, x^{SA}_0),$$

where the constituent elements are explained below.

The state space of SOA is identical to that of SA and the initial state is identical as well. The event set of SOA, $\Sigma^{SOA} = \Delta^{SA} \cup \Delta^{SA}_f \cup \{\varepsilon, \varepsilon_f\}$, consists of two versions of the set of output symbols $\Delta^{SA} \cup \{\varepsilon\}$: one corresponding to "normal" events and another corresponding to "faulty" events.

The sensor output automaton's deterministic observation mask, M^{SOA}, is:

$$M^{SOA}(y) = y \qquad \text{if } y \in \Delta \cup \{\varepsilon\}$$
$$M^{SOA}(y_f) = y \qquad \text{if } y_f \in \Delta_f \cup \{\varepsilon_f\} \quad (14)$$

Thus "normal" events in $\Delta \cup \{\varepsilon\}$ are observed directly, and "faulty" events in $\Delta_f \cup \{\varepsilon_f\}$ appear identical to their corresponding normal events. We set $\Sigma^{SOA}_{uo} = \{\varepsilon, \varepsilon_f\}$. The set of faulty events to be diagnosed is $\Sigma^{SOA}_f = \Delta^{SA}_f \cup \{\varepsilon_f\}$.

We construct the state transition probabilities p^{SOA} according to the following equations:

$$p^{SOA}(x_1, y, x_2) = \sum_{\sigma \in \Sigma \setminus \Sigma_f} (p^{SA}(x_1, \sigma \mid x_2) \times \Pr[M^{SA}_p(\sigma) = y]) \quad \text{if } y \in \Delta \cup \{\varepsilon\}, \quad (15)$$

$$p^{SOA}(x_1, y_f, x_2) = \sum_{\sigma \in \Sigma_f} (p^{SA}(x_1, \sigma \mid x_2) \times \Pr[M^{SA}_p(\sigma) = y]) \quad \text{if } y_f \in \Delta_f \cup \{\varepsilon_f\}. \quad (16)$$

Following the procedure to construct the sensor output automaton associated with Figure 1 results in the stochastic automaton is shown in Figure 2. The equivalence between the diagnosability properties of a stochastic automaton and its corresponding sensor output automaton is demonstrated in the following theorem.

Theorem 1: A stochastic automaton SA subject to an unreliable sensor mask M_p is A-diagnosable (or AA-diagnosable) with respect to M_p and Σ_f if and only if its corresponding sensor output automaton SOA is A-diagnosable (or AA-diagnosable) with respect to M^{SOA} and Σ_f.

Proof: See Appendix A. ■

B. Stochastic Diagnoser Construction

Because the diagnosability properties of a stochastic automaton with a non-deterministic observation mask are equivalent to those of its sensor output automaton, we can test whether a stochastic automaton is uA- or uAA-diagnosable by constructing the *stochastic diagnoser* of its SOA.

The procedure for constructing a stochastic diagnoser described in [1] makes two assumptions that are untenable in the setting of sensor output automata. Firstly, it is assumed that there are no cycles of unobservable events in the stochastic automaton whose diagnoser is being constructed. Secondly, it is assumed that for each $x \in X^{SOA}, \sigma \in \Sigma^{SOA}$, there is only one unique $x' \in X^{SOA}$ such that $p(x', \sigma \mid x) > 0$.

When modeling a system such as a nuclear flow network, it is likely that the resulting non-deterministic observation mask on the event set will have few reliably observable events. Most events will have at least a small non-zero probability of being misdetected or misclassified; as a result, the assumptions used in [1] will not hold. For example, the system in Figure 1 is simple and has only one event, b, that can be misclassified or misdetected. However, its

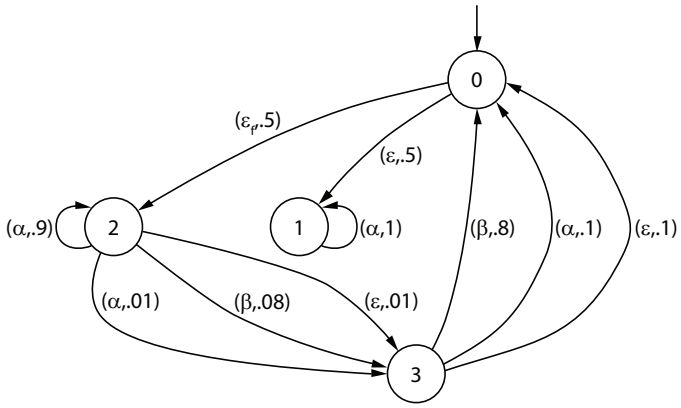

Fig. 2. Sensor output automaton for the system in Figure 1.

sensor output automata, shown in Figure 2, contains an unobservable cycle between states 0, 2, and 3. It also contains a state $x = 2$ and an event α such that there are two states, $x' = 2$ and $x' = 3$, such that $p(x', \alpha, x) > 0$. In more complex systems, these conditions are even more likely to be present in the SOA. In this paper, we present the technique for constructing the stochastic diagnoser that does not require these assumptions.

We first define a pair of failure labels N and F. The label N denotes that no failure event in Σ_f had occurred; the label F denotes that there has been at least one occurrence of an event in Σ_f. The change in the labels as the system evolves is described by the *label propagation function* $LP : \{N, F\} \times \Sigma^{SOA*}$

$$LP(\ell, s) = \begin{cases} N & \text{if } \ell = N \text{ and } \Sigma_f \notin s \\ F & \text{otherwise.} \end{cases}$$

A stochastic diagnoser $SD = (Q^{SD}, \Sigma^{SD}, \delta^{SD}, q_0^{SD}, \Phi^{SD}, \phi_0^{SD})$ associated with a sensor output automaton SOA consists of six elements:

- $Q^{SD} \subseteq 2^{X \times \{N,F\}}$ is the set of diagnoser logical elements
- $\Sigma^{SD} = \Delta^{SOA}$ is the event set
- $\delta^{SD} : Q^{SD} \times \Sigma^{SD} \to Q^{SD}$ is the state transition function
- $q_0^{SD} = \{(x_0, N)\}$ is the initial logical element
- Φ^{SD} is the set of probability transition matrices
- $\phi_0^{SD} = [1]$ is the initial probability vector

The first four elements $(Q^{SD}, \Sigma^{SD}, \delta^{SD}, q_0^{SD})$ are still exactly the "logical" diagnoser described in [9]. Each logical element $q \in Q^{SD}$ is a list of *components*, where each component is of the form (x, ℓ), where $x \in X^{SOA}$ and $\ell \in \{N, F\}$. A set of components $\{(x_1, \ell_1), (x_2, \ell_2), \ldots, (x_n, \ell_n)\}$ is *certain* if $\ell_1 = \ell_2 = \cdots = \ell_n$. The components in each logical element need to be placed into a particular order; this order can be chosen arbitrarily.

The construction of δ^{SD} is modified to take into account the relaxed assumptions. The state transition function is defined as

$$\delta^{SD}(q, s) \triangleq \bigcup_{(x,\ell) \in q} \bigcup_{s \in \mathcal{L}_\sigma(SOA,x)} \bigcup_{x' : p(x', s|x) > 0} (x', LP(\ell, s)).$$

From this definition, it may not be possible to compute δ^{SD} as for some $x \in X^{SOA}$, there may be strings in $\mathcal{L}_\sigma(SOA, x)$ of arbitrarily large length. However, any string in $\mathcal{L}_\sigma(SOA, x)$ containing more than $\|X^{SOA}\|$ events will contain cycles, and there will exists a string with no more than $\|X^{SOA}\|$ events that transitions the diagnoser to the same component (x, ℓ).

To define δ^{SD} in the presence of unobservable cycles, we thus first define

$$\mathcal{L}_\sigma^r(SOA, x) \triangleq \{s \in \mathcal{L}_\sigma(SOA, x) : |u| \leq \|X^{SOA}\|\},$$

and use the following equivalent expression for δ^{SD}:

$$\delta^{SD}(q, s) = \bigcup_{(x,\ell) \in q} \bigcup_{s \in \mathcal{L}_\sigma^r(SOA,x)} \bigcup_{x' : p(x', s|x) > 0} (x', LP(\ell, s)).$$

The major change between the procedure used to construct the stochastic diagnoser in [1] and the procedure necessary here is in the construction of Φ^{SD}.

Each matrix in Φ^{SD} is defined as $\Phi : Q^{SD} \times \Sigma^{SD} \to \mathcal{M}_{[0,1]}$

$$\Phi_{ij}(q, \sigma) = \sum_{s \in L_\sigma(SOA,x_i) : LP(\ell_i, s) = \ell_j} p(x_j, s \mid x_i) \quad (17)$$

where the range $\mathcal{M}_{[0,1]}$ represents the set of finite-dimensional matrices whose values are contained in the interval $[0, 1]$. The size of the matrix outputted by $\Phi(q, \sigma)$ is $\|q\| \times \|\delta^{SD}(q, \sigma)\|$. If an event transitions SD from a logical element with m components to a logical element with n components, the size of the matrix associated with that event will be $m \times n$. Each element $\Phi_{ij}(q, \sigma)$ denotes the probability of the system transitioning from the ith component of diagnoser state q to the jth component of diagnoser state $\delta^{SD}(q, \sigma)$ along the transition σ.

Determining $\Phi_{ij}(q, \sigma)$ involves calculating the sum of the probabilities of strings in the language $L_\sigma(SOA, x_i)$, which may contain an arbitrarily large number of strings due to the presence of unobservable cycles. This sum can be determined

$$\mathbf{R}(\alpha) = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & \frac{1}{1999} & \frac{1}{3998} & \frac{900}{1999} & \frac{10}{1999} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{1000} & \frac{1}{2000} & \frac{9}{10} & \frac{1}{100} & \frac{1}{1999000} & \frac{1}{3998000} & \frac{9}{19990} & \frac{1}{199900} \\ \frac{200}{1999} & \frac{100}{1999} & 0 & 0 & 0 & 0 & \frac{90}{1999} & \frac{1}{1999} \\ 0 & 0 & 0 & 0 & \frac{1}{1999} & \frac{1000}{1999} & \frac{900}{1999} & \frac{10}{1999} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{2}{1999} & \frac{1}{1999} & \frac{1800}{1999} & \frac{20}{1999} \\ 0 & 0 & 0 & 0 & \frac{200}{1999} & \frac{100}{1999} & \frac{90}{1999} & \frac{1}{1999} \end{bmatrix} \quad \mathbf{R}(\beta) = \begin{bmatrix} 0 & 0 & 0 & 0 & \frac{8}{1999} & 0 & 0 & \frac{80}{1999} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{125} & 0 & 0 & \frac{2}{25} & \frac{1}{249875} & 0 & 0 & \frac{2}{49975} \\ \frac{4}{5} & 0 & 0 & 0 & \frac{4}{9995} & 0 & 0 & \frac{8}{1999} \\ 0 & 0 & 0 & 0 & \frac{8}{1999} & 0 & 0 & \frac{80}{1999} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{16}{1999} & 0 & 0 & \frac{160}{1999} \\ 0 & 0 & 0 & 0 & \frac{1600}{1999} & 0 & 0 & \frac{8}{1999} \end{bmatrix}$$

by finding the absorption probabilities of an appropriately constructed Markov chain.

C. Construction of Probability Transition Matrices

In this subsection, we construct a Markov chain whose absorption probabilities are equal to the values for $\Phi_{ij}(q,\sigma)$ defined in Equation 17. Let $f : X^{SOA} \rightarrow \{1, 2, \ldots, N_s\}$ be a bijective function that assigns a unique index in the set $\{1 \ldots N_s\}$ to each state in X^{SOA}, where $N_s = \|X^{SOA}\|$. For each $\delta \in \Delta \cup \{\varepsilon\}$, define a matrix $\mathbf{Q}(\delta)$ according to

$$\mathbf{Q}_{ij}(\delta) \triangleq p(f^{-1}(j), \delta \mid f^{-1}(i)).$$

Similarly define for each $\delta \in \Delta_f \cup \{\varepsilon_f\}$

$$\mathbf{Q}_{ij}(\delta_f) \triangleq p(f^{-1}(j), \delta_f \mid f^{-1}(i)).$$

For each δ, We combine $\mathbf{Q}_{ij}(\delta)$ and $\mathbf{Q}_{ij}(\delta_f)$ to yield

$$\hat{\mathbf{Q}}(\delta) = \begin{bmatrix} \mathbf{Q}(\delta) & \mathbf{Q}(\delta_f) \\ \mathbf{0}_{N_s \times N_s} & \mathbf{Q}(\delta) + \mathbf{Q}(\delta_f) \end{bmatrix} \tag{18}$$

Using the matrices $\hat{\mathbf{Q}}(\delta)$, we define the one-step observation matrix as follows.

Definition 4.1: Let $g : \Delta^{SOA} \cup \{\varepsilon\} \rightarrow \{0 \ldots N_d\}$ be any bijective function where $g(0) = \varepsilon$ that assigns a unique index to each symbol in Δ^{SOA}, when $N_d = \|\Delta^{SOA}\|$.The *one-step observation matrix* associated with SOA is

$$\mathbf{P}^{SOA} \triangleq \begin{bmatrix} \hat{\mathbf{Q}}(\epsilon) & \hat{\mathbf{Q}}(g^{-1}(1)) \cdots \hat{\mathbf{Q}}(g^{-1}(N_d)) \\ \mathbf{0}_{2N_d N_s \times 2N_s} & \mathbf{I}_{2N_d N_s} \end{bmatrix} \tag{19}$$

Each state in $\mathbf{P}^{SOA}$ corresponds to a component (x, ℓ) and an event σ. This correspondence is captured by the function $h : X \times \{N, F\} \times \Sigma^{SOA} \rightarrow \{1, 2 \ldots, (N_d + 1)N_s\}$

$$h(x, \ell, \delta) = 2N_s g(\delta) + f(x) + N_s 1_F(\ell),$$

where $1_F(\ell) = 1$ if $\ell = F$ and 0 if $\ell = N$. $\mathbf{P}^{SOA}$ contains $2N_s$ transient states and $2N_d N_s$ recurrent states. The transient states are given by $h(x, \ell, \varepsilon)$ for all (x, ℓ); for any $\delta \in \Delta$, $h(x, \ell, \delta)$ is a recurrent state regardless of the values of x and ℓ.

By construction, each recurrent state is also an absorbing state as the Markov chain remains in any recurrent state it enters with probability one. To find the absorption probability of a state z_R in $\mathbf{P}^{SOA}$, given that the chain is currently instate z_T, we must solve the equation

$$\rho_{z_R}(z_T) = \mathbf{P}_{z_T, z_R} + \sum_{z \in \mathcal{T}} \mathbf{P}_{z_T, z} \rho_{z_R}(z), \tag{20}$$

where $\mathbf{P}_{z_1, z_2}$ denotes the one step transition probability from state z_1 to state z_2 in $\mathbf{P}^{SOA}$ and $\mathcal{T}$ denotes the set of transient states in the Markov chain [10].

The absorption probabilities of recurrent states in $\mathbf{P}^{SOA}$ are the values of the elements of the probability transition matrices Φ that are necessary to complete the construction of the stochastic diagnoser, as shown in the following theorem.

Theorem 2: Let (x_i, ℓ_i) be the ith component of $q \in Q^{SD}$ and let (x_j, ℓ_j) be the jth component of $\delta^{SD}(q, \delta)$. The corresponding element of the probability transition matrix $\Phi_{ij}(q, \delta)$ is

$$\Phi_{ij}(q, \delta) = \rho_{h(x_i, \ell_i, \varepsilon)}(h(x_j, \ell_j, \sigma)). \tag{21}$$

Proof: See Appendix B. ■

To find every possible element of every matrix in Φ^{SD}, we need to find the absorption probability of any recurrent state $h(x, \ell, \delta)$ given that $\mathbf{P}^{SOA}$ is in any transient state $h(x, \ell, \varepsilon)$. We accomplish this by rewriting Equation 20 in matrix form,

$$\mathbf{R}(g^{-1}(m)) = \hat{\mathbf{Q}}(g^{-1}(m)) + \hat{\mathbf{Q}}(\epsilon)\mathbf{R}(g^{-1}(m)), \tag{22}$$

and solving this system of linear equations. The elements of the probability transition matrices are then $\Phi_{ij}(q, g^{-1}(m)) = \mathbf{R}(g^{-1}(m))_{h(x_i, \ell_i, \varepsilon), h(x_j, \ell_j, \varepsilon)}$.

D. Example

For the example in Figure 2, $\Delta^{SA} \cup \{\varepsilon\} = \{\varepsilon, \alpha, \beta\}$ and let $f(x) = x + 1$ for all $x \in X^{SOA} = \{0, 1, 2, 3\}$. The six $\mathbf{Q}$ matrices associated with SOA are:

$$\mathbf{Q}(\varepsilon) = \begin{bmatrix} 0 & 0 & .5 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & .01 \\ .1 & 0 & 0 & 0 \end{bmatrix}, \mathbf{Q}(\varepsilon_f) = \begin{bmatrix} 0 & 0 & .5 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\mathbf{Q}(\alpha) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & .9 & .01 \\ .1 & 0 & 0 & 0 \end{bmatrix}, \mathbf{Q}(\alpha_f) = \mathbf{0}_{4 \times 4},$$

$$\mathbf{Q}(\beta) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.08 \\ .8 & 0 & 0 & 0 \end{bmatrix}, \mathbf{Q}(\beta_f) = \mathbf{0}_{4 \times 4}.$$

Set $g(\alpha) = 1$ and $g(\beta) = 2$. The one-step transition matrix $\mathbf{P}^{SOA}$ is constructed according to Equations 18 and

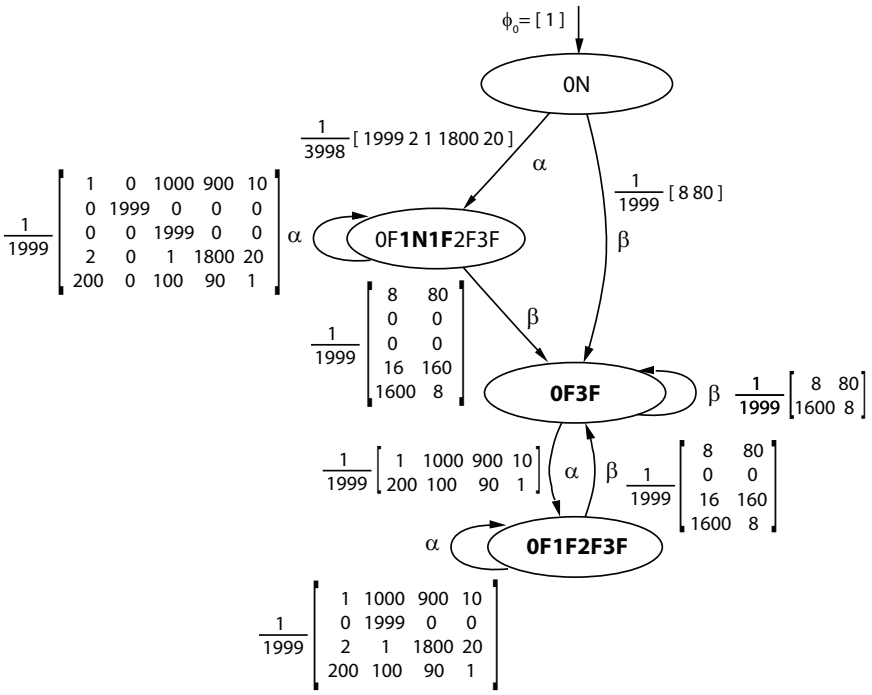

Fig. 3. Stochastic diagnoser under unreliable sensor configuration for the system in Figure 1. Recurrent components are indicated by boldface.

19, yielding

$$\mathbf{P}^{SOA} = \left[\begin{array}{c|cc} \hat{\mathbf{Q}}(\varepsilon) & \hat{\mathbf{Q}}(\alpha) & \hat{\mathbf{Q}}(\beta) \\ \hline \mathbf{0}_{16\times 8} & \multicolumn{2}{c}{\mathbf{I}_{16\times 16}} \end{array}\right].$$

The absorption probabilities for $\mathbf{P}^{SOA}$ can be found be solving the systems of linear equations defined in Equation 22, yielding $\mathbf{R}(\alpha)$ and $\mathbf{R}(\beta)$ shown at the top of this page.

The first four rows in $\mathbf{R}(\alpha)$ are the absorption probabilities corresponding to the case when the label of the component in $\delta(q,\alpha)$ is N, and the last four rows correspond to the case when that label is F. If the ith component of $q \in Q^{SD}$ is (x_1,ℓ) and the jth component of $\delta(q,\alpha)$ is (x_2,ℓ), then the corresponding value of the probability transition matrix is

$$\Phi_{ij}(q,\alpha) = \mathbf{R}_{f(x_1)+N_s 1_F(\ell_1), f(x_2)+N_s 1_F(\ell_2)}(\alpha).$$

Using the probabilities in $\mathbf{R}(\alpha)$ and $\mathbf{R}(\beta)$, we can now construct the set of probability transition matrices Φ and complete the construction of the stochastic diagnoser following the procedure described in Section IV-B. The completed stochastic diagnoser under unreliable observations is shown in Figure 3.

V. Conditions for uA- and uAA-diagnosability

Necessary and sufficient conditions for A-diagnosability and sufficient conditions for AA-diagnosability in terms of the stochastic diagnoser were derived in [1]. These conditions depend on the concept of the *recurrent component*. A component (x,ℓ) in a logical element $q \in Q^{SD}$ is called recurrent if, in a Markov chain constructed using the set of probability transition matrices Φ, the pair $(q,(x,\ell))$ corresponds to a recurrent state of that Markov chain. These conditions are immediately applicable to this paper because the final result of our construction is also a stochastic diagnoser. The theorems are stated below without proof.

Theorem 3: A language L generated by an SOA is A-diagnosable with respect to a set of failures Σ_f and an observation mask M if, and only if, every logical element of its associated stochastic diagnoser SD containing a recurrent component bearing the label F is certain. ■

Theorem 4: A language L generated by an SOA is AA-diagnosable with respect to a set of failures Σ_f and an observation mask M if, in every logical element in its associated stochastic diagnoser SD, the set of recurrent components is certain. ■

Combining these results with Theorem 1 yields the following results.

Theorem 5: A language L generated by an SA is uA-diagnosable with respect to a set of failures Σ_f and an observation mask M_p if, and only if, in every logical element of SD, the stochastic diagnoser constructed from the sensor output automaton of SA, that contains a recurrent component bearing the label F is certain. ■

Theorem 6: A language L generated by an SA is uAA-diagnosable with respect to a set of failures Σ_f and an observation mask M_p if, and only if, in every logical element of SD, the stochastic diagnoser constructed from the sensor output automaton of SA, the set of recurrent components is certain. ■

The stochastic diagnoser in Figure 3 has a logical element $\{0F, 1N, 1F, 2F, 3F\}$ that contains a pair of recurrent components $\{1N, 1F\}$ with inconsistent labels. Thus this logical

element is not certain, and thus the stochastic automaton shown in Figure 1 is not uA-diagnosable. Furthermore, since the pair of recurrent components is not certain, the stochastic automaton is also not uAA-diagnosable.

VI. Discussion

In this paper, we extend the notion of stochastic diagnosability to DES with unreliable observation masks. We demonstrate that a system with an unreliable observation mask can be transformed into a system with equivalent diagnosability properties that has a deterministic observation mask. We then extend the stochastic diagnoser approach to find conditions for diagnosability of stochastic automata with unreliable observations.

The conditions for stochastic diagnosability discussed in this paper require near certainty of a correct diagnosis being made in the long term. However, in certain applications, it is possible to tolerate a small probability of making an incorrect diagnosis in the long term. Our future work involves weakening the notions of uA- and uAA-diagnosability proposed in this paper so as to determine if systems have the desired property of making correct diagnoses in the long run with a sufficiently high degree of confidence that need not be near certainty.

VII. Acknowledgements

Part of this research was performed when D. Thorsley was supported by the Idaho National Laboratory, and another part was performed when D. Thorsley was supported by the AFOSR MURI "High Confidence Design for Distributed Embedded Systems." D. Thorsley would like to thank D. Teneketzis and S. Lafortune, Department of EECS, University of Michigan, for their support while part of this research was being completed.

References

[1] D. Thorsley and D. Teneketzis, "Diagnosability of stochastic discrete-event systems," *IEEE Trans. Automatic Control*, vol. 50, no. 4, pp. 476–492, Apr. 2007.

[2] H. Garcia and T.-S. Yoo, "Methodology to optimize and integrate safeguards sensor configurations and measurements in large nuclear processing facilities," in *Proc. Institute of Nuclear Material Management (INMN) Annual Meeting*, July 2003.

[3] ——, "Model-based detection of routing events in discrete flow networks," *Automatica*, vol. 41, no. 4, pp. 583–594, Apr. 2005.

[4] S. Lafortune, D. Teneketzis, M. Sampath, R. Sengupta, and K.Sinnamohideen, "Failure diagnosis of dynamic systems: An approach based on discrete event systems," in *Proc. 2001 American Control Conference*, June 2001, pp. 2058–2071.

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

[6] S. Jiang, Z. Huang, V. Chandra, and R. Kumar, "A polynomial algorithm for testing diagnosability of discrete-event systems," *IEEE Trans. Automatic Control*, vol. 46, no. 8, pp. 1318–1320, Aug. 2001.

[7] J. Lunze and J. Schröder, "State observation and diagnosis of discrete-event systems described by stochastic automata," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 11, no. 4, pp. 319–369, 2001.

[8] E. Athanasopoulou, L. Li, and C. Hadjicostis, "Probabilistic failure diagnosis in finite state machines under unreliable observations," in *Proc. 8th Intl. Workshop on Discrete Event Systems*, Ann Arbor, MI, USA, July 2006, pp. 301–306.

[9] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. Automatic Control*, vol. 40, no. 9, pp. 1555–1575, Sept. 1995.

[10] P. Hoel, S. Port, and C. Stone, *Introduction to Stochastic Processes*. Prospect Heights, IL: Waveland Press, 1987.