Probabilistic Fault Diagnosis in Discrete Event Systems

Xi Wang  Ishanu Chattopadhyay  Asok Ray
xxw117@psu.edu  ixc128@psu.edu  axr2@psu.edu
Department of Mechanical Engineering
The Pennsylvania State University
University Park, PA 16802

Abstract—This paper presents a concept of discrete-event probabilistic fault diagnosis as an extension of the binary decision approach proposed by Sampath et al., where unobservable failure events are included in the representation of the system behavior under both normal and faulty conditions. It is assumed that the probability of each transition is known at the time of decision making. Based on this finite-state automaton model, probabilistic reasoning is applied for on-line diagnosis of dynamical systems. The major advantage of this approach is early detection of multi-component faults, which facilitates robust reconfiguration of the decision and control system.

I. INTRODUCTION

There has been considerable attention in the literature on fault diagnosis for discrete event systems focusing on both centralized [2][1] and decentralized [8][4] approaches. In both approaches, the objective of fault diagnosis is to estimate the discrete-event state of a physical process based upon available sensor data and other information and to infer the occurrence of component failure(s), if any, in the past. The physical process is modelled as a finite state automaton and its behavior is expressed in terms of the corresponding generated regular language. A regular language based failure diagnosis approach for discrete event systems has been proposed in [2]. The notion of diagnosability is introduced as a property of the diagnoser of the system. The diagnoser is constructed to test the diagnosability and can be further used to on-line diagnose the system if the system is diagnosable. However, this on-line diagnosis is a binary decision process in that the diagnoser can only tell either a fault has occurred or there is no fault up to now. In many cases, due to limited sensor information, drawing the conclusion of a fault occurrence can be already too late to reconfigure the decision and control system. It would be very desirable if the diagnoser has the information on respective probabilities of possible faults; this is a major extension of the diagnosis procedure presented in [2].

Sampath et al. [2] have introduced the notion of $F_i$-certainty (i.e., the underlying state indicates the same fault for all possible paths that the system may take to generate the current observed trace). It is shown in [2] that only when the current state $q_d$ of the diagnoser is $F_i$-certain, then the occurrence of a failure of the type $F_i$ can be concluded, regardless of the current state of the automaton. However, in engineering problems, it is desirable to have the knowledge about the current state of the diagnoser not being $F_i$-certain. A generalization of the notion of attaching labels to the states permits handling of multiple fault generations as well. The probabilities of each set of candidate faults is calculated using the standard Bayesian technique. It is important to note that only a specific set of faults can possibly be generated for a given observed trace of the system. The diagnostic policy of dictating occurrence of fault $F_i$ if and only if the diagnoser state is $F_i$-certain, is generalized to the policy of choosing the most likely set of faults in the system at its current state.

This paper extends the framework in [2] in the sense that the diagnoser carries failure information by means of labels attached to states as well as the probabilities associated with these labels. As such the the diagnoser in [2] is a special case of the approach proposed in this paper. Furthermore, the paper demonstrates the ability of this new technique to handle multiple component failures in the system, the importance of which is made evident by practical examples. This technique is conceptually independent of the language generated by the controlled plant and hence is equally suitable for fault diagnosis in systems modelled by finite state automata and untimed Petri Nets.

II. SYSTEM MODEL

This section models the physical process to be diagnosed as a deterministic finite state automaton (DFSA):

$$G = (Q, \Sigma, \delta, q_0)$$

where $Q$ is the finite state space; $\Sigma$ is the event alphabet and $\Sigma^*$ is its Kleene closure; $q_0 \in Q$ is the initial state; and $\delta : Q \times \Sigma \rightarrow Q$ is the partial transition function and its extension is defined as: $\delta^* : Q \times \Sigma^* \rightarrow Q$.

The behavior of the DFSA $G$ is the generating language $L(G)$, or simply $L$, and is defined as usual [7]. The event
set is further partitioned into $\Sigma = \Sigma_o \cup \Sigma_{uo}$, where $\Sigma_o$ and $\Sigma_{uo}$ are the observable event set and unobservable event set, respectively. The observation projection $P_o : \Sigma^* \rightarrow \Sigma^*_o$ is defined as follows.

$$P_o(\epsilon) = \epsilon$$
$$P_o(\sigma) = \begin{cases} \sigma & \text{if } \sigma \in \Sigma_o \\ \epsilon & \text{if } \sigma \in \Sigma_{uo} \end{cases}$$
$$P_o(s\sigma) = P(s)P(\sigma) \quad \forall s \in \Sigma^*, \forall \sigma \in \Sigma$$

Therefore, the set of observable traces generated by the system $G$ is given by

$$L_o(G) = \{ s \in \Sigma^*_o \mid \exists t \in L(G), P_o(t) = s \}$$

Let $\Sigma_f \subseteq \Sigma_{uo}$ denote the set of failure events and be partitioned into disjoint sets corresponding to different failure types as: $P: \Sigma_f = \bigcup_{i=1}^m \Sigma_{f_i}, \Sigma_{f_i} \cap \Sigma_{f_j} = \emptyset, \forall i \neq j$ Let $F = \{ F_i, i \in I \}$, where $I = \{ 1, 2, \ldots, m \}$, represent the set of failure types. The failure type map $\psi: \Sigma_f \rightarrow F$ assigns every event $\sigma_f \in \Sigma_{f_i}$ the same failure type $F_i$, i.e., $\forall \sigma_f \in \Sigma_{f_i}, \psi(\sigma_f) = F_i, i \in I$.

To introduce diagnosability, we make the following assumptions on the language $L(G)$ as in [2].

1. $L(G)$ is live, i.e., $(\forall q \in Q)(\exists \sigma \in \Sigma, p \in Q) \Rightarrow \delta(q, \sigma) = p$.
2. $G$ has no cycle of unobservable events, i.e., $(\exists uvw \in L(G), v \in \Sigma_{uo} \Rightarrow \delta(q_0, u) = \delta(q_0, uv))$.

A. Diagnosability

The diagnosability for discrete event systems defined in [2] is stated below.

Definition 2.1: A prefix-closed and live language $L$ is said to be diagnosable with respect to $\Sigma_o$ and $\psi$ on $\Sigma_f$ if the following holds:

$$\left( \forall F_i \in F \right)(\exists n_i \in N)(\forall s = \alpha \sigma_f \in L, \sigma_f \in \Sigma_f, \psi(\sigma_f) = F_i)(\forall u = st \in L, |t| \geq n_i) \Rightarrow D$$

where the diagnosability condition $D$ is

$$\forall w \in L, P_o(w) = P_o(u) \Rightarrow \exists w = \beta \sigma_f' \in \Sigma_f, \psi(\sigma_f') = F_i$$

Definition 2.1 states that if an event string $s$ in $L$ ends with a $F_i$-type failure, and the observing extension of $s$ in $L$ is sufficient long (e.g., $|t| \geq n_i$), then every event string $w$ in $L$ that is observation equivalent to $v = st$ should contain a $F_i$-type failure.

A system $G$ is said to be diagnosable if its generating language $L(G)$ is diagnosable. A method for testing the diagnosability was introduced in [2], which is exponential in the number of states of the system. Recently, two methods of testing diagnosability have been presented in [5] and [6] that require polynomial time in the number of states of the system.

III. Probabilistic Fault Diagnosis

This section proposes probabilistic fault diagnosis as an extension of the diagnoser model presented in [2]. The main objective is to provide the diagnoser with additional probabilistic information in addition to the state estimate and failure label information. It is assumed that the system is diagnosable without multiple failures or otherwise the system has been made diagnosable by approaches such as those in [3]. Therefore, the emphasis is on diagnosers that do not have any $F_i$-indeterminate cycle for all types of failure and no state in the diagnoser is ambiguous, as stated in theorem 1 of [3].

A. Probability Space for System Model

It is assumed that a probability of occurrence can be assigned to all the transitions defined in state transition function $\delta$.

Definition 3.1: The event transition probability of the system $G$ is defined as a function $\tilde{\pi} : Q \times \Sigma \rightarrow [0, 1]$ such that

$$\forall q \in Q, \sum_{\sigma \in \Lambda(q)} \tilde{\pi}(q, \sigma) = 1$$

where $\Lambda(q) = \{ \sigma \in \Sigma | \exists q' \in Q, \delta(q, \sigma) = q' \}$ is the set of events defined on state $q$.

Definition 3.2: The state transition probability of the system $G$ is defined as a function $\pi : Q \times Q \rightarrow [0, 1]$ such that

$$\pi_{ij} \equiv \pi(q_i, q_j) = \sum_{\sigma \in \Lambda(q_i)} \tilde{\pi}(q_i, \sigma)$$

where $i, j \in I = \{ 1, \ldots, n \}, |Q| = n$.

It follows from Definition 3.1 that $\sum_j \pi_{ij} = 1$. An efficient algorithm for estimation of the parameters $\pi_{ij}$ is reported in [9]. We now define a probability space for the DSFA $G$. Let the sample space $\Omega = L(G)$ and the event space $B = 2^\Omega$. We define a map $p : B \rightarrow [0, 1]$ as follows.

1. $\forall s = \sigma_1 \cdots \sigma_k \in L(G)$, let $q_{i-1} \in Q, i = 1, \ldots, k$, such that $\delta(q_{i-1}, \sigma_i) = q_i$, then

$$p(\{ s \}) = \prod_{i=1}^k \tilde{\pi}(q_{i-1}, \sigma_i)$$

2. $\forall E \in B, p(E) = \sum_{s \in E} p(s)$. (With a slight abuse of notation, we have dropped the curly bracket.)

It follows from above definitions that $p(\Omega) = 1$. Therefore, $p$ is a probability distribution on $B$ and $(\Omega, B, p)$ is a probability space. Salient properties of the probability measure $p$ are delineated below.

1. For $s_1, s_2 \in L(G)$, if $s_2 = s_1t$, where $t \in \Sigma^*$, then

$$p(s_1|s_2) = \frac{p(s_1, s_2)}{p(s_2)} = \frac{p(s_2)}{p(s_2)} = 1 \quad (1)$$

2. For $s_1, s_2 \in L(G)$, if $s_2 = s_1 \sigma_1 \cdots \sigma_k$, then

$$p(s_2|s_1) = \frac{p(s_2, s_1)}{p(s_1)} = \frac{p(s_2)}{p(s_1)} = \prod_{i=1}^k \tilde{\pi}(q_i, \sigma_i) \quad (2)$$
where \( \delta(q_0, s_1) = q_1, \delta(q_i, \sigma_i) = q_{i+1}, i = 1, \ldots, k \).

(3) For \( s_1, s_2 \in L(G) \), if \( s_2 \neq s_1 t \) and \( s_1 \neq s_2 t \), then

\[
p(s_2|s_1) = \frac{q(s_2, s_1)}{p(s_1)} = \frac{q(0)}{p(s_1)} = 0
\]

Property (1) is due to the fact that the traces \( s_1 \) and \( s_2 \equiv s_1 t \) have occurred is equivalent to the outcome that trace \( s_2 \) has occurred. That is, occurrence of a trace \( s \) implies occurrence of every prefix of \( s \). Property (2) states that if a trace \( s_1 \) has occurred, then the probability of occurrence \( s_2(\equiv s_1 \sigma_1 \cdots \sigma_k) \) solely depends on whether the trace \( \sigma_1 \cdots \sigma_k \) has occurred. Property (3) states that two mutually exclusive traces cannot occur without returning to the initial state. Therefore, \( \forall A, B \subseteq L(G) \),

\[
p(A|B) = p \left( \bigcup_{s \in A} \{s \in A\} \bigcup_{s \in B} \{s \in B\} \right)
\]

B. Probabilistic Diagnoser

This subsection briefly reviews the diagnoser construction procedure in [2] and then generalizes the diagnoser with respect to the probability space described above. Let \( Q_o \equiv \{q_0\} \cup \{q \in Q \mid \exists \sigma \in \Sigma_o, p \in Q, s.t., \delta(p, \sigma) = q\} \)

as the observable state set in the DFSA \( G \). Since \( G \) is assumed to be diagnosable (that can be tested by procedures in [5] [6]), the complete set of possible labels reduces to

\[
\Delta = \{N\} \cup 2^\mathcal{F}
\]

For the purpose of state estimate and failure label propagation, let us define

\[
Q_{do} \equiv 2^{Q_o \times \Delta}
\]

The diagnoser \( G_d \) is a deterministic finite state machine built from the DFSA \( G \) and is defined as:

\[
G_d = (Q_d, \Sigma_o, \delta_d, q_{do})
\]

where \( Q_d, \Sigma_o, \delta_d \) and \( q_{do} \) follow the notation of [2]. The initial state of the diagnoser \( q_0 \) is defined to be \( \{(q_0, \{N\})\} \). The state space \( Q_d \) is the resulting subset of \( Q_{do} \) composed of the states of the diagnoser that are reachable from \( q_0 \) under \( \delta_d : Q_o \times \Sigma_o \rightarrow Q_o \). Since the state space \( Q_d \) of the diagnoser is a subset of \( Q_{do} \), a state \( q_d \in Q_d \) is of the form

\[
q_d = \{(q_i, l_i) | i = 1, \ldots, r\}
\]

where \( q_i \in Q_o \) and \( l_i \in \Delta \). In general, \( l_i \) is of the form

\[
l_i = \{N\}, l_i = \{F_{k_1}, \ldots, F_{k_j}\} \text{ where } k_1, \ldots, k_j \subseteq \mathcal{I}.
\]

However, if only a single failure is encountered, \( l_i = \{F_{k_j}\} \) for some \( k_j \in \mathcal{I} \), i.e., \( |l_i| = 1 \). The properties of each state \( q_d \) in \( G_d \) are stated below.

1) Any state \( q \in Q_o \) appears in at most one pair \((q, l)\) in any state of \( Q_d \).
2) If \( q_d \in Q_d \), then

\[
(q_i, l_i), (q_j, l_j) \in q_d
\]

is equivalent to two traces \( s_1 = u\sigma \) and \( s_2 = v\sigma \) in \( L(G) \), such that

\[
\sigma \in \Sigma_o, \delta(q_0, s_1) = q_i, \delta(q_0, s_2) = q_j
\]

and

\[
P_o(s_1) = P_o(s_2)
\]

3) Let \( q_{d1}, q_{d2} \in Q_d \) and \( t \in \Sigma^* \) such that \( (q_1, l_1) \in q_{d1}, (q_2, l_2) \in q_{d2}, \delta(q_1, t) = q_2, \) and \( \delta_d q_{d1}, F(t) = q_{d2}, \) then

\[
(F_i \notin l_2) \rightarrow (F_i \notin l_1)
\]

As \( G \) is diagnosable, there is no ambiguous label \( A \) in the diagnoser \( G_d \).

At each state \( q_d \) in \( G_d \), the collection of states that might be the current state of \( G \) is denoted as \( S(q_d) \). Similarly, a set of failure candidates that may have occurred in \( G \) is denoted as \( \mathcal{L}(q_d) \). Formally,

\[
S(q_d) = \{q \in Q_o \mid (q, l) \in q_d\}
\]

\[
\mathcal{L}(q_d) = \{l \in \mathcal{F} \mid (q, l) \in q_d\}
\]

It follows from the above properties that \( |S(q_d)| \geq |\mathcal{L}(q_d)| \).

Therefore, the diagnoser \( G_d \) can serve as an extended state estimator of \( G \) in the sense that failure information is also carried with every state estimate. The details of transition function \( \delta_d \) can be found in [2]. For the purpose of online diagnosis, the notion of \( F_i \)-certainty is defined as follows.

**Definition 3.3:** A state \( q_d \in Q_d \) is said to be \( F_i \)-certain if for all \((q, l) \in q_d, F_i \in l\).

It is shown in [2] that only if the current state \( q_d \) of the diagnoser is \( F_i \)-certain, then it can be concluded that a failure of the type \( F_i \) has occurred, regardless of the current state of the system \( G \). This paper generalizes the formulation to incorporate multiple-failure situations where the current state of the diagnoser is not \( F_i \)-certain. Multiple component failures may give rise to strings of failure labels for each state \( q_i \). Therefore, the complete set of possible labels must be redefined for the multiple-failure case:

\[
\hat{\Delta} = \{N\} \cup \mathcal{F}^*
\]

where \(* \) is the Kleene Closure and hence

\[
Q_{do} = 2^{Q_o \times \hat{\Delta}}
\]

Probabilistic information is propagated by extending the definition of the states as

\[
q_d = \{(q_1, s_1, p_{s_1}), \ldots, (q_i, s_i, p_{s_i}), \ldots, (q_r, s_r, p_{s_r})\}
\]

where \( s_i \) represents a failure label string denoting the set of plausible failures at state \( q_i \) and \( p_{s_i} \) is the probability of the system attaining state \( q_i \) and experiencing all failures listed in \( s_i \). Equivalently,

\[
q_d = \{(q_1, p_{q_1}, l_{11}, p_{l_{11}}, \ldots, l_{1i}, p_{l_{1i}}, \ldots, l_{1k}, p_{l_{1k}}), \ldots, (q_j, p_{q_j}, l_{j1}, p_{l_{j1}}, \ldots, l_{ji}, p_{l_{ji}}, \ldots, l_{jk}, p_{l_{jk}}), \ldots, (q_r, p_{q_r}, l_{r1}, p_{l_{r1}}, \ldots, l_{ri}, p_{l_{ri}}, \ldots, l_{rk}, p_{l_{rk}})\}\
where \( p_q \) is the probability of the DFSA being at state \( q \), and \( p'_l \) the probability of failure type \( l \), given the current state. The definitions of \( S(q_d) \) and \( L(q_d) \) are modified to reflect their natural extension to this framework:

\[
S(q_d) = \{ q \in Q_o \mid q \in q_d \} \\
L(q_d) = \sum_{k=1}^{r} L_k(q_k)
\]

where

\[
L_k(q_k) = \{ l \in F \mid l \text{ has occurred when the current state of } G \text{ is } q_k \}
\]

Let the state in the diagnoser \( G_d \) be at \( q_d \in Q_d \) upon occurrence of an observing trace \( s \in L_o(G) \) (i.e., \( \delta_d(q_{d0}, s) = q_d \)). Then, for every state \( q \in S(q_d) \subseteq Q \), the inverse image of a trace \( s \) in \( L(G) \) that reaches the state \( q \) is obtained as:

\[
P_o^{-1}(s, q) = \{ t \in L(G) \mid P_o(t) = s, \delta(q_0, t) = q \}
\]

Let \( P_o^{-1}(s) \) be the set of all possible traces in \( L(G) \) giving the observed event sequence \( s \):

\[
P_o^{-1}(s) = \{ t \in L(G) \mid \delta_d(q_{d0}, s) = q_d, \exists q \in S(q_d), s.t., P_o(t) = s, \delta(q_0, t) = q \}
\]

\[
= \{ t \in L(G) \mid \exists q \in S(q_d), s.t., t \in P_o^{-1}(s, q) \}
\]

The probability of being at state \( q \) of the DFSA \( G \) after observing \( s \), is then given by

\[
p(q|s) = \frac{p(s, q)}{\sum_{q \in S(q_d)} p(s, q')} = \frac{p(P_o^{-1}(s, q))}{\sum_{q' \in S(q_d)} p(P_o^{-1}(s, q'))}
\]

The above expression implies that, out of all possible traces in \( L(G) \) that appears like \( s \) under the observation projection, \( p(q|s) \) is the probability that the state \( q \in Q \) could be reached after observing \( s \). Then,

\[
\sum_{q \in S(q_d)} p(q|s) = 1
\]

Given an event \( \sigma \in \Sigma \) and a trace \( t \in L(G) \), we use the notation \( \sigma \vdash t \) to represent that event \( \sigma \) has happened somewhere in the trace \( t \). A faulty event \( \sigma_f \in F_1 \) has occurred means there exists a string \( t \in P_o^{-1}(s) \subseteq L(G) \) such that \( \sigma_f \vdash t \). Therefore, a posteriori probability of a faulty event \( \sigma_f \in F_1 \) after observing \( s \) is given by

\[
p(\sigma_f | s) = \frac{p(l \in P_o^{-1}(s) \mid \sigma_f \vdash t) | P_o^{-1}(s))}{\sum_{q \in S(q_d)} p((l \in P_o^{-1}(s, q) | \sigma_f \vdash t))}
\]

For every \( (q, l) \in q_d \), where \( l = F_i \) for some \( i \in I \), indicates that \( \exists \) a failure event \( \sigma_f \in F_i \) such that \( \sigma_f \vdash t \); therefore, we denote \( p(l|s) = p(\sigma_f|s) \). For every \( i \in I \)

\[
p(F_i | s) = \sum_{\sigma_f \in F_i} p(\sigma_f | s) = \sum_{l=F_i:i \in L(q_d)} p(l | s)
\]

Thus, given any trace, a comparison of a posteriori probabilities determines the likelihood of occurrence of the individual members in the set of possible faults at that instant. This information is presented in the so-called fault-likelihood matrix \( \Pi_f(q_d) \) defined below.

\[
\Pi_f(q_d) = \begin{bmatrix}
p_{11}^f & p_{12}^f & \cdots & p_{1m}^f \\
p_{21}^f & p_{22}^f & \cdots & p_{2m}^f \\
\vdots & \vdots & \ddots & \vdots \\
p_{r1}^f & p_{r2}^f & \cdots & p_{rm}^f
\end{bmatrix}
\]

where the \( ij \)th element of \( \Pi_f(q_d) \) is:

\[
p_{ij}^f(q_d) = p(F_j|q_i) = p(F_j|s)
\]

Since, in general \( S(q_d) \neq Q_o \),

\[
q_j \notin S(q_d) \Rightarrow \pi_{ij}^f = 0, \quad \forall j \in \{1, 2, \ldots, m\}
\]

where \( m \) is the cardinality of the set \( F \) of possible faults. Thus, the probability that fault \( F_j \) has already occurred when the diagnoser is in state \( q_d \) is given by

\[
p_{F_j}(q_d) = \sum_{i=1}^{m} \pi_{ij}^f
\]

Fig. 1. A DES G

Fig. 2. The diagnosed \( G_d \)
Definition 3.4: A prefix-closed and live language \( L \) is said to be \( p \)-diagnosable with respect to \( \Sigma_o \) and \( \psi \) on \( \Sigma_f \) if the following holds:

\[
(\forall F_i \in \mathcal{F})(\exists n_i \in N)(\forall s = \alpha \sigma_f \in L, \sigma_f \in \Sigma_f, \\
\psi(\sigma_f) = F_i(\forall u = st \in L, |t| \geq n_i) \Rightarrow D_p
\]

where the diagnosability condition \( D_p \) is

\[
\forall w \in L, P_o(w) = P_o(w) \Rightarrow \\
\exists \beta = \beta \sigma_f' \gamma, \sigma_f' \in \Sigma_f, \psi(\sigma_f') = F_i, p(F_i) \geq p
\]

Clearly, Definition 3.4 is reduced to Definition 2.1 if the probability threshold \( p \) is equal to 1.

Example 3.1: Figure 2 presents a DES model \( G \) and its diagnoser \( G_2 \). \( \Sigma_o = \{\alpha, \beta\}, \Sigma_{uo} = \{\sigma_f, \sigma_{f2}, \sigma_{f3}\}, \Sigma_{f1} = \{\sigma_{f1}\}, \Sigma_{f2} = \{\sigma_{f2}\} \) and \( \Sigma_{f3} = \{\sigma_{f3}\} \).

Let the up-to-date observation be the single symbol \( s = \beta \). It is seen in Figure 2(b) that \( q_4 = \{(3, F_1), (4, F_1, F_2), (6, F_2, F_3)\} \), \( S(q_4) = \{3, 4, 6\} \), and \( L(q_4) = \{F_1, F_2, F_3\} \). So the probability of the DFSA being at state 3 is given by

\[
p(q_3 | s) = \frac{p(q_3, s)}{\sum_{q \in S(q_4)} p(q, s)} = \frac{p(\sigma_{f1}, \beta)}{p(\sigma_{f1}, \beta) + p(\sigma_{f1}, \sigma_{f2}, \beta) + p(\sigma_{f2}, \sigma_{f3}, \beta)} \\
= 0.2 \times 0.8 + 0.2 \times 0.2 \times 1.0 + 0.3 \times 1.0 \times 0.4 \\
= 0.5
\]

Similarly,

\[
p(q_5 | s) = 0.04 \times 0.32 = 0.125 \\
p(q_6 | s) = 0.32 \times 0.32 = 0.375
\]

Based on the above probability estimate of current system state, we want to estimate the probability of the system being at normal condition or type \( F_i \) faulty condition.

\[
p(\sigma_{f1} | s) = \frac{\sum_{q \in S(q_4)} p(\{t \in P^{-1}_{o}(s, q) | \sigma_{f1}, \tilde{t}\})}{\sum_{q \in S(q_4)} p(\{t \in P^{-1}_{o}(s, q)\})} \\
= \frac{p(\sigma_{f1}, \beta) + p(\sigma_{f1}, \sigma_{f2}, \beta)}{0.16 + 0.04 + 0.12} \\
= 0.625 \\
i.e. we have
\[
p(F_1 | s = \beta) = \sum_{\sigma_f \in F_1} p(\sigma_f | s) = 0.625 \\
p(F_2 | s = \beta) = \sum_{\sigma_f \in F_1} p(\sigma_f | s) = 0.5 \\
p(F_3 | s = \beta) = \sum_{\sigma_f \in F_2} p(\sigma_f | s) = 0.375
\]

We can also set up the fault-likelihood matrix in this case

\[
\Pi^f(q_4) = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0.5 & 0 & 0 \\
0.125 & 0.125 & 0 \\
0 & 0 & 0 \\
0.375 & 0.375 & 0
\end{bmatrix}
\]

The probability that failure type \( F_i \) has occurred is then given by the \( i \)-th column sum of the \( \Pi^f(q_4) \) matrix. In [2], a failure is detected only if it is a \( F_i \)-certain. One can see this is indeed a special case of the proposed probabilistic failure diagnoser. For example, after observing \( s = \beta \), the current state in the diagnoser is \( q_4 = \{(3, F_1), (4, F_1, F_2), (6, F_2, F_3)\} \). Neither \( F_1 \) nor \( F_2 \) or \( F_3 \) is certain here but we can still talk about the likelihoods of their occurrences. The calculations indicate that observation of \( \beta \) from the initial state means \( F_1 \) may have occurred with probability of 62.5% and \( F_2 \) with a probability of 50% and \( F_3 \) with that of 37.5%. If we consider the case where we observe \( \beta \), we see that the diagnoser state is given by \( q_4 = \{(4, F_1), (6, F_1, F_2, F_3)\} \), \( S(q_4) = \{4, 6\} \), and \( L(q_4) = \{F_1, F_2, F_3\} \). The possible paths leading to the observed trace \( s = \beta \) are \( \sigma_{f1}, \sigma_{f2}, \beta \sigma_{f3}, \beta \). A similar calculation as to the first case results in

\[
p(q_4 | s) = \frac{p(q_4, s)}{\sum_{q \in S(q_4)} p(q, s)} = \frac{p(\sigma_{f1}, \beta)}{p(\sigma_{f1}, \beta) + p(\sigma_{f1}, \sigma_{f2}, \beta)} \\
= 0.2 \times 0.8 + 0.2 \times 0.2 \times 1.0 \times 1.0 \times 0.4 \\
= 0.91
\]

\[
p(q_6 | s) = \frac{p(q_6, s)}{\sum_{q \in S(q_4)} p(q, s)} = \frac{p(\sigma_{f1}, \sigma_{f2}, \beta)}{p(\sigma_{f1}, \sigma_{f2}, \beta) + p(\sigma_{f1}, \sigma_{f2}, \beta) + p(\sigma_{f2}, \sigma_{f3}, \beta)} \\
= 0.2 \times 0.8 \times 1.0 \times 0.2 \times 0.2 \times 1.0 \times 1.0 \times 0.4 \\
= 0.09
\]

\[
\Pi^f(q_4) = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0.5 & 0 & 0 \\
0.125 & 0.125 & 0 \\
0 & 0 & 0 \\
0.375 & 0.375 & 0
\end{bmatrix}
\]
\[ p(F_1 | s = \beta) = \sum_{i=1}^{6} \Pi^f(i, 1) = 1 \]
\[ p(F_2 | s = \beta) = \sum_{i=1}^{6} \Pi^f(i, 2) = 0.09 \]
\[ p(F_3 | s = \beta) = \sum_{i=1}^{6} \Pi^f(i, 3) = 0.09 \]

In this case, the state \( q_d \) is \( F_1 \) certain (i.e. the fault \( F_1 \) has occurred with probability 1), whereas each of \( F_2 \) and \( F_3 \) may have occurred with a probability of 0.09.

IV. SUMMARY AND CONCLUSIONS

This paper presents a discrete-event probabilistic fault diagnosis approach that generalizes the binary decision approach in [2] where unobservable failure events are used to represent the complete system behavior under both normal and faulty conditions in the form of an automaton. With the knowledge of each state transition probability, this paper makes use of probabilistic reasoning for on-line diagnosis of faults in dynamical systems. The advantage of this approach is that one may be able to apply control reconfiguration at an early stage to handle incipient simultaneous faults in multiple components.

The fault diagnosis algorithm allows formulation of an efficient algorithm to determine \( p \)-diagnosability for a specified a probability threshold.

REFERENCES