Failure Diagnosis of Stochastic Automata

David Thorsley and Demosthenis Teneketzis

Department of Electrical Engineering and Computer Science
University of Michigan
Ann Arbor, MI, USA
{dthorsle,teneketzis}@eecs.umich.edu
www.eecs.umich.edu/umdes

June 12, 2003
14th Annual Workshop on Principles of Diagnosis
Washington, D.C., USA
Presentation Overview

- Motivation
- Literature Survey
- The Stochastic Automaton Model
- Review of Discrete-Event Diagnosability
- Introduction of A-Diagnosability
- Stochastic Diagnoser
- AA-Diagnosability
- Summary
Literature Survey

• Failure diagnosis is an important problem in complex systems

• Different approaches to the diagnosis problem include:
  ∗ Fault Detection and Isolation schemes
  ∗ Fault trees
  ∗ Model-Based reasoning methods
  ∗ Bayesian Networks
  ∗ Discrete-event systems

• Our approach to diagnosis is based on discrete event systems
Survey of Discrete-Event Diagnosis Literature

• Most research in discrete-event diagnosis has focussed on logical DES models
  * centralized models
    ○ Bavishi and Chong, Sampath et al., Jiang and Kumar
  * decentralized models
    ○ Pencolé, Boel and van Schuppen, Ricker and Rudie, Debouk et al.
  * timed models
    ○ Provan and Chen, Hashtrudi Zad et al.

• The diagnosis problem for stochastic automata was previously studied by Lunze and Schröder
Stochastic Automaton Model

- A *stochastic automaton* is a quadruple $G = (X, \Sigma, p, x_0)$ where
  - $X$ is the set of states
  - $\Sigma$ is the set of events
  - $x_0$ is the initial state
  - $p(x', e \mid x)$ is the state transition probability

- The event set $\Sigma$ is partitioned into observable events $\Sigma_o$ and unobservable events $\Sigma_{uo}$

- The set of possible failures ($\Sigma_f$) is modeled as a subset of $\Sigma_{uo}$

- Failures are assumed to be permanent
Stochastic Automaton Example

- $X = \{0, 1, 2, 3\}$, $x_o = 0$

- $\Sigma = \{a, b, \sigma_{uo}, \sigma_f\}$, $\Sigma_o = \{a, b\}$, $\Sigma_{uo} = \{\sigma_{uo}, \sigma_f\}$, $\Sigma_f = \{\sigma_f\}$
The Diagnosability Problem

• The objective of failure diagnosis is to detect the occurrence of failure events

• Roughly speaking, a system is diagnosable if every instance of a failure event can be detected after at most a finite delay

• Diagnosability is a key notion in our approach
Review of Previous Work on Diagnosability

• Our approach to the diagnosability of stochastic automata is based on the approach for logical automata developed in Sampath et al. (1995)

• A system is diagnosable if the following condition is satisfied:

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

where the diagnosability condition function \(D\) is given by

\[D(st) = \begin{cases} 1 & \text{if } \omega \in Proj^{-1}_L[Proj(st)] \Rightarrow \Sigma f_i \in \omega \\ 0 & \text{otherwise} \end{cases}\]
Interpretation of Diagnosability

- Every continuation of at least $n$ events allows the failure to be diagnosed

![Diagram showing the relationship between events and diagnosability]

- Every possible system behavior consistent with the observed behavior contains a failure event

![Diagram illustrating the relationship between true behavior and projected behavior]
Solution of Diagnosability Problem

- Necessary and sufficient conditions for diagnosability can be found by constructing a diagnoser (Sampath et al. (1995))
Diagnosability of Stochastic Automata

- Stochastic automata are more informative models than logical automata
- May be possible to derive stronger results on diagnosability
- Is the definition for logical automata too strict for stochastic automata?
Motivating Example

\[ (\sigma_{uo},.5) \]

\[ (\sigma_f,.5) \]

\[ (a,1) \]

\[ (a,.9) \]

\[ (b,1) \]

\[ (b,.1) \]
Formal Definition of A-Diagnosability

A system is A-diagnosable if

\[(\forall \epsilon > 0) (\exists n_i \in \mathbb{N}) [\forall s \in \Psi(\Sigma_{f_i})] \{ \text{Prob}(t : D(st) = 0 \land t \in L/s \land \|t\| \geq n_i) < \epsilon \}\]

where the diagnosability condition function \( D \) is:

\[
D(st) = \begin{cases} 
1 & \text{if } \omega \in \text{Proj}^{-1}_L[\text{Proj}(st)] \Rightarrow \Sigma_{f_i} \in \omega \\
0 & \text{otherwise}
\end{cases}
\]
Interpretation of A-Diagnosability

• With probability greater than \(1 - \epsilon\), a continuation of at least \(n\) events will diagnose the failure

\[ D(\text{st}) = 1 \]

\[ D(\text{st}) = 0 \]

\[ \text{Prob}(D(\text{st}) = 0) < \epsilon \]

• Every possible system behavior consistent with the observed behavior contains a failure event
Stochastic Diagnoser

- Our objective is to find necessary and sufficient conditions for a given stochastic automaton to be A-diagnosable

- For logical automata, these conditions were found through the construction of a diagnoser automaton

- We propose a stochastic analogue to the logical diagnoser for testing A-diagnosability of stochastic automata

- Unlike the logical diagnoser, the stochastic diagnoser is not, in general, a finite state machine
Formal Definition of Stochastic Diagnoser

- Formally, a stochastic diagnoser is a sextuple \((Q_d, \Sigma_o, \delta_d, q_0, \Phi, \phi_0)\) where
  - \(Q_d\) is the set of discrete states
  - \(\Sigma_o\) is the set of observable events
  - \(\delta_d\) is the partial transition function
  - \(q_0\) is the initial diagnoser state
  - \(\Phi\) is a set of matrices defined for each transition
  - \(\phi_0\) is the initial probability vector \((\phi_0 = [1])\)

- The quadruple \((Q_d, \Sigma_o, \delta_d, q_0)\) is the logical diagnoser of Sampath et al. (1995)

- The pair \((\Phi, \phi_0)\) updates the probabilistic model
Stochastic Diagnoser Example

\[
\begin{aligned}
\phi_0 &= [1] \\
0 &\xrightarrow{a} 1N \\
1 &\xrightarrow{(a,1)} 1 \\
2 &\xrightarrow{(a,.9)} 1N \\
2 &\xrightarrow{(\sigma_{uo}, .5)} 1 \\
3 &\xrightarrow{(b,.1)} 2 \\
3 &\xrightarrow{(b,1)} 3 \\
N &\xrightarrow{b} 3F \\
F &\xrightarrow{b} F
\end{aligned}
\]
Suppose the observed system behavior is $aaa$. The probability vector $\phi$ can be calculated as

$$\phi_{un}(aaa) = [1] \begin{bmatrix} .5 & .45 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & .9 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ .9 \end{bmatrix}$$

$$= [0.5 \ 0.3645]$$

$$\phi(aaa) = [0.5784 \ 0.4216]$$

- $\text{Prob}(1N \mid aaa) = .5784$ and $\text{Prob}(2F \mid aaa) = .4216$
Properties of the Stochastic Diagnoser

- Each discrete state of the stochastic diagnoser is a set of components.
- The components of all the discrete states in the diagnoser can be used to construct a Markov chain.
- Therefore, components of the stochastic diagnoser can be thought of as transient or recurrent.
- This observation allows us to derive conditions for A-diagnosability.
• **Necessary and Sufficient Condition**: A stochastic automaton is A-diagnosable if and only if every recurrent component bearing the label $F_i$ in its associated stochastic diagnoser is part of an $F_i$-certain state.

• A state is $F_i$-certain if either all components in the state carry the label $F_i$ or no components in the state carry that label.
Is A-Diagnosability All There is?

- The definition for A-diagnosability was motivated by the observation the logical diagnosability conditions may be violated, despite the fact that they hold everywhere except on a set that has zero probability in the limit.

- Is this the only way in which the diagnosability conditions can be violated by only a “negligible” set?
Motivating Example

\[ \phi_0 = [1] \]

\[
\begin{array}{c}
\text{ON} \\
[1] \\
\end{array} \quad \begin{array}{c}
\text{1N} \\
[.9 .1] \\
\end{array} \quad \begin{array}{c}
\text{ON} \\
[1 0] \\
\text{0F} \\
[.9 .1] \\
\end{array} \quad \begin{array}{c}
\text{1N} \\
[0 1] \\
\text{1F} \\
[0 .1] \\
\end{array}
\]

\[ (a, 1) \]
\[ (b, .9) \]
\[ (b, 1) \]
\[ (\sigma_f, .1) \]
Formal Definition of AA-Diagnosability

A system is AA-diagnosable if

$$(\forall \epsilon > 0 \land \forall \alpha < 1)(\exists n_i \in \mathbb{N})[\forall s \in \Psi(\Sigma_{f_i})]$$

$$\{\text{Prob}(t : D_{\alpha}(st) = 0 \land t \in L/s \land \|t\| \geq n_i) < \epsilon\}$$

where the diagnosability condition function $D_{\alpha}$ is:

$$D_{\alpha}(st) = \begin{cases} 1 & \text{if } \text{Prob}(\omega : \omega \in \text{Proj}^{-1}_L[\text{Proj}(st)] \land \Sigma_{f_i} \in \omega) > \alpha \\ 0 & \text{otherwise} \end{cases}$$
Comparison of A- and AA-Diagnosability

![Diagram showing comparison of A- and AA-diagnostics probability](image)

- **A-Diagnosability**
- **AA-Diagnosability**

- Probability of Diagnosing the Failure (A Priori)
- Probability of Failure Required for Diagnosis (A Posteriori)

- $1 - \varepsilon$

David Thorsley and Demosthenis Teneketzis, University of Michigan - June 12, 2003
Conditions for AA-Diagnosability

• A sufficient condition for AA-diagnosability can be determined using the stochastic diagnoser

• **Sufficient but Not Necessary Condition:** A stochastic automaton is AA-diagnosable if in every state of its associated stochastic diagnoser, the set of recurrent components in each diagnoser state is $F^*_i$-certain.
Example of an AA-Diagnosable System
Example showing the Non-Necessity of the Condition

\[ \phi_0 = [1] \]

\[
\begin{bmatrix}
.25 & .35 \\
.25 & .15
\end{bmatrix}
\]

\[
\begin{bmatrix}
.5 & 0 \\
0 & .7
\end{bmatrix}
\]

\[
\begin{bmatrix}
.5 & 0 \\
0 & .3
\end{bmatrix}
\]
Conclusion and Summary

• Stochastic automata suggest different ideas for diagnosability than logical automata

• A- and AA-diagnosability modify a definition for logical diagnosability by disregarding improbable system behaviors

• The diagnoser method can be extended to stochastic automata and used to derive conditions for A- and AA-diagnosability