Ruiz Beltrán, Elvia; Orozco Mora, Jorge Luis
Reduced Petri Net Diagnosers for Detecting and Locating Faults
Conciencia Tecnológica, núm. 37, enero-junio, 2009, pp. 48-53
Instituto Tecnológico de Aguascalientes
Aguascalientes, México

Available in: http://www.redalyc.org/articulo.oa?id=94411773009
Reduced Petri Net Diagnosers for Detecting and Locating Faults

Research

Dra. Elvia Ruiz Beltrán¹ and Dr. Jorge Luis Orozco Mora²
¹Department of Systems and Computer, ²Department of Electrical-Electronic Engineering
Aguascalientes, Aguascalientes. México.
Phone/Fax +(52 449) 910-5002 Ext. 106 E-mail: eruiz@ita.mx, drorozco@ita.mx

Abstract

This paper deals with fault detection and location of Discrete Event Systems (DES) modeled using Interpreted Petri nets (IPN). In this paper two efficient methods for obtaining reduced diagnosers IPN models are proposed: based on the DES model, a Petri net is synthesized depending on each methodology; each net consists of a single place (or more) and the same number of transitions that the system model has; the current marking of this place (places) is enough to determine and locate faults occurring within the DES.

Keywords: Discrete Event Systems, Interpreted Petri Nets, Fault detection and location.

Introduction

The analysis of the diagnosability property of a DES has been addressed through several approaches and methods, namely that based on artificial intelligence techniques and that based on discrete event models. Recently, finite automata (FA) and Petri nets (PN) have been widely used as modeling formalisms and formal tools for fault diagnosis.

In [1] M. Sampath et al. introduced the notion of diagnosability and proposed a method for designing an on-line diagnoser for determining the diagnosability property.

In [4], [5] and [7] Prock, Genc and Hadjicostis respectively proposed methods based on PN models to detect and isolate the faults presented in the system. In [4] the tokens residing in P-semiflows are monitored and, depending on the quantity of these tokens, faults into the system are determined. In [5] the held approach analyzes the reachability graph to isolate faults, leading to NP-complete algorithms. The strategy presented in [7] consists in adding one more place to the system model, the marking of this place can be used to determine and isolate system faults; in this approach however, it is assumed that all places are measurable, that all transitions are controllable, and that system and observer can be synchronized each other. These conditions are hardly fulfilled in current systems.

Based on [7] and the structural characterization of diagnosability [9], we propose a novel diagnosis scheme that use simple and reduced IPN models for monitoring the DES behavior. The monitoring models play a similar role as used in [7], however they can operate using only partial information on the marking (measurable places), and their synchronization with the DES model are not longer needed.

This work is organized as follows: in preliminaries section basic definitions of IPN are provided. Later, it is presented a procedure to obtain an IPN model. Next, two methodologies for structuring the diagnosis scheme are proposed. Then, it is included an example for illustrating the notions herein introduced. Finally conclusions are given.

Preliminaries

This section presents the basic concepts and notation of PN and IPN used in this paper.

Definition 1: A Petri Net structure $G=(P,T,I,O)$ where:
• $P = \{p_1, p_2, ..., p_n\}$ and $T = \{t_1, t_2, ..., t_m\}$ are finite sets of vertices named places and transitions respectively,
In this work \( \varphi \) is a \( q \times n \) matrix. Each column of \( \varphi \) is an elementary or null vector. If the output symbol \( i \) is present (turned on) every time that \( M(p_i) \geq 1 \), then \( \varphi(i) = 1 \), otherwise \( \varphi(i) = 0 \).

A transition \( t_i \in T \) of an IPN fires it is enabled at marking \( M_0 \), and a) if \( \lambda(t_i) = a \not\in \varepsilon \) is provided to the system, or b) if \( \lambda(t_i) = \varepsilon \) and \( t_i \) is enabled then \( t_i \) can be fired. When an enabled transition \( t_i \) is fired in a marking \( M_0 \), then a new marking \( M_{k+1} \) is reached. This fact is represented as:

\[
M_k \xrightarrow{t_i} M_{k+1}; M_{k+1} \text{ can be computed using the state equation:}
\]

\[
M_{k+1} = M_k + C \varepsilon_i
\]

where \( C \) and \( \varepsilon_i \) are defined as in PN and \( y_k \in (Z^+)^g \) is the \( k \)-th output vector of the IPN.

According to functions \( \lambda \) and \( \varphi \), transitions and places of an IPN \((Q,M_0)\) can be classified as follows.

Definition 4: If \( \lambda(t_k) \not\in \varepsilon \) the transition \( t_k \) is said to be manipulated. Otherwise it is nonmanipulated. A place \( p_i \in P \) is said to be measurable if the \( i \)-th column vector of \( \varphi \) is not null, i.e., \( \varphi(i) \neq 0 \). Otherwise it is nonmeasurable.

Definition 5: An IPN \((Q,M_0) = (N,\Sigma,\Phi,\lambda,\varphi, D, \varnothing)\) described by the state equation (1) is event-detectable iff the firing of any pair of transition \( t_k \) of \((Q,M_0)\) can be distinguished from each other by the observation of the sequences of input-output symbols.

The following lemma [8] gives a polynomial characterization of event-detectable IPN.

Lemma 6: Let \((Q,M_0) = (N,\Sigma,\Phi,\lambda,\varphi, D, \varnothing)\) be an IPN described by the state equation (1). \((Q,M_0)\) is event-detectable iff all \( \varphi C \) columns are not null and different from each other.

Building IPN Models

We deal with IPN models representing normal and faulty events and states. In a DES an internal event representing a fault is associated to a transition that leads to a place that represents the failed operation. Below is included the procedure followed in the construction of an IPN model.

Procedure 7: Building an IPN model \((Q,M_0)\)

1. Build an IPN model of the normal behavior of the system \((Q^0, M_0^{(0)})\), i.e. when no failures are considered. The set of places of this model is named \( P^0 \) (normal places) and the set of transitions of this model is
named $T^N$ (normal transitions). Define the initial marking $M_0^N$. 
2. Define a set of possible failure states $F^f$. For every state in $F^f$ build another set of places, named $P^f$. 
3. Connect $(Q^N, M_0^N)$ to the places of $P^f$ through new transitions representing the faults ($T^f$). 
4. The matrix $\varphi$ is extended; one row is added for each $p^f \in P^f$; where $\varphi (p^N, \ast)=\varphi (p^f, \ast)$ if place $p^N$ is connected to $p^f$ through a unique transition in $T^f$.

**Diagnoser Model with one place**

Definition 8: The proposed diagnoser model structure for the system normal behavior $(Q^N, M_0^N)$ is an IPN $(Q^d, M_0^d)$ where the set of places $P^d=\{p_d\}$ and the set of transitions is $T^d=T^N$, the incidence matrix $C^d$ of $(Q^d, M_0^d)$ is the following

$$C^d = B^T \varphi^N C^N$$

where $C^N$ is the incidence matrix of $(Q^N, M_0^N)$, $\varphi^N$ is the output function of $(Q^N, M_0^N)$ and $B$ is a $q=1$ nonnegative vector ($q$ is the number of measurable places of $(Q^N, M_0^N)$) matrix with nonnegative entries.

The matrix $B$ is computed as follows:

Algorithm 9: Building B

**Inputs:** C-incidence matrix of an IPN, 
$q$ - number of measurable places in the IPN,

**Outputs:** The matrix $B$

1. The “base number” $b$ should be computed. 
   In this case $b = 2 \max(\text{abs}(c_i)) + 1$, where $c_i$ is an element of incidence matrix $C$.
2. Define a $q=1$ vector. 
3. \[ b^0 \ b^1 \ \cdots \ b^{q-1} \]

This procedure computes matrix $B$.

According to the way in which $B$ was constructed, all columns of $C^d$ will be different from zero and different from each other.

The initial marking of the diagnoser model structure is computed as:

$$M_0^d = B^T \varphi(M_0^N)$$

**Error Computation of the DM with one place**

Definition 10: Error computation. The $k$-th error is computed by the following equation:

$$e_k = M_0^d - B^T (\varphi M_k)$$

Notice that $e_k$ is computed from the diagnoser-model output and not from the marking $M_k$. It means that the proposed diagnoser is using the system output and not internal system signals (those signals that are non measurable).
Diagnoser Model with more than place

When there is a considerable quantity of tokens contained into the place of the diagnoser model, then a diagnoser model with more than one place is proposed in order to reduce the number of tokens contained into it.

For a diagnoser-model with more than one place, the incidence matrix $C^d$ of $(Q^d,M^d)$ is computed using the following equation:

$$C^d = B \sigma C^N$$  \hspace{1cm} (5)

where $B$ is a $1 \times q$ matrix, where $1 \leq q$.

The matrix $B$ for this diagnoser model is obtained using the following algorithm.

**Algorithm 11: Building matrix $B$**

**Inputs:** $C$-incidence matrix of an IPN, $1$ - number of places in the diagnoser-model, $q$ - number of measurable places in the IPN, $M$ - The matrix $B$

**Outputs:** The matrix $B$

1. The "base number" $b$ should be computed. In this case $b=2\max(\text{abs}(e_i))+1$, where $e_i$ is an element of incidence matrix $C$.
2. Define a matrix $B$ with $1 \times q$, where $1 \leq q$.

3. 

$$B = \begin{bmatrix} b^0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & b^0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & b^0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b^0 & b^1 & b^2 & \cdots & b^{i-1} & \end{bmatrix}$$

This procedure computes the matrix $B$.

According to the way in which $B$ was constructed, all columns of $C^d$ must be different from zero and different from each other.

The initial marking for this diagnoser model is computed as:

$$M^d_0 = B\varphi(M^N_0)$$  \hspace{1cm} (6)

**Error Computation of the DM with one place**

$$e_i = M^d_i - B(p^\varphi M^d_k)$$  \hspace{1cm} (7)

**Firing Rules of the diagnoser model with one or more places**

If a transition $t \in T - (T^k \cup T^f)$ is fired in $(Q,M^d_k)$ then it is fired in $(Q^k,M^d_k)$ (it is possible since these transitions are event

The event-detection module determines which transition is fired into the system model and ordering that this transition must be fired into the diagnoser model.

**Fault Isolation Algorithm for the DM's**

Definition 12: Fault isolation. When $e_i \neq 0$, an error is detected, then a faulty marking was reached. The mechanism used to find out the faulty marking is named fault isolation. This work proposes the following algorithm to accomplish this task.

**Algorithm 13: Fault isolation**

**Inputs:** $M_k$, $M^d_k$, $e_i$  
**Outputs:** $p$ (faulty place), $M_i$ (faulty marking)

**Constants:** $C^d$ is the IPN diagnoser structure incidence matrix

- $i = \text{index of the column of } C^d \text{ such that } C^d(i,i)=e_i$
- $\forall p \in T^k, M_k(p) = 0$
- $\forall p \in T^f, M_k(p) = 0$
- $\forall p \in C^d \cap P^f, M_i(p^f) = 1$
- $M_i = M_k$
- Return ($p$, $M_i$)

Definition 14: Let $(Q,M^d_0)$ be an input-output diagnosable IPN. The 3-tuple $(N_0,e_i,A)$, where

- $N_0 = (Q^d,M^d_0)$ is the diagnoser structure of $(Q,M^d_0)$
- $e_i$ is the error produced by error computation,
- $A$ is the algorithm Fault isolation,

is named an input-output diagnoser for $(Q,M^d_0)$.

We will prove that after the firing of a finite sequence, the input-output diagnoser for $(Q,M^d_0)$ detects when a place $p \in P^f$ is marked, i.e., it isolates the faulty state.
Example

Consider the producer-consumer scheme depicted in figure 2. The model consists of a producer unit (PU), a consumer unit (CU) and a buffer of 2-slots. The behavior of this system is the following. The producer unit PU creates and delivers products into the free buffer positions. The consumer unit CU retrieves products from the buffer when there is a product stored into a buffer slot. The producer unit PU could reach a faulty state from its producing state. Similarly, the consuming unit could reach a faulty state from its consuming state. Then the places p1, p2, p3 represent the normal behavior of PU and p10 represents the faulty behavior. Places p4, p5, p6 represent the normal behavior of the CU and p12 represents the faulty behavior. The places p7, p8, p9 and p10 represent the 2-slots of the buffer.

The IPN (obtained with procedure 7) depicted in figure 3 represents the behavior of the producer-consumer system. Since this IPN is input-output diagnosable [9], then a diagnoser can be built for this system. In this case we will use the structure presented in previous section. The normal behavior of this IPN is depicted in figure 4; its incidence matrix and output function are:

The base obtained to compute B is $b = 2*1 + 1 = 3$; since we build B using algorithm 9. We obtain the following vector:

$$B^t = [1 \ 3 \ 9 \ 27]^T$$

Therefore $C^d$ is:

$$C^d = [-1 \ 27 \ 1 \ 9 \ -9 \ -27 \ 3 \ -3]$$

Hence, its associated IPN is depicted in figure 5.
Fig. 6 The IPN diagnoser-model with three places.

It is easy to see that the diagnoser model almost uses 4 tokens into its places. Nevertheless, the diagnoser model (with one place) reaches almost 31 tokens. Thus, the number of tokens is considerably reduced in the diagnoser model with more than one place. But, this diagnoser needs more places for monitoring the system than the diagnoser model with one place needs.

Conclusions

We presented a diagnosis scheme allowing detecting and locating faults of partially observed DES. The diagnosability of the system implies the existence of a monitoring model; then two methods to conceive such models are proposed. Due to the simplicity of the monitoring IPN, the procedure for fault detection and isolation can be efficiently performed. Current research addresses the analysis of a methodology that reduces the potency that the base b is powered.

References


Artículo recibido: 3 marzo de 2009
Aceptado para publicación: 29 mayo 2009