Engineering Science and Technology, an International Journal 18 (2015) 616–633

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: http://www.elsevier.com/locate/jestch

Full length article

Failure diagnosis in real time stochastic discrete event systems

Chaitali Biswas Dutta*, Utpal Biswas

Dept of CSE, University of Kalyani, Nadia, West Bengal, India

ARTICLE INFO

Article history:
Received 29 December 2014
Received in revised form
12 April 2015
Accepted 12 April 2015
Available online 6 June 2015

Keywords:
Failure detection and diagnosis
Discrete Event Systems
Real time systems
Stochastic systems

ABSTRACT

Discrete Event System (DES) has been used for Failure Detection and Diagnosis (FDD) of a wide range of systems. For real time systems, timed DES based frameworks diagnose failures leading to violation of delays or deadlines. These schemes declare a failure to be diagnosable if it always i.e., in all timed-traces, results in timing violations within finite time of its occurrence. The basic assumption is, probability of any trace can be 1 or 0. So, even if there is a trace where failure is manifested, still its probability can be 0, leading to non-diagnosability. However in many systems this basic assumption may not hold. To address this issue, Thorsley et al. have augmented probability values to transitions and termed the framework as stochastic DES. Here, failure is diagnosable if there are traces where failure effect is manifested and probability of occurrence of those traces increase with time and cross a threshold. However, the scheme was for un-timed systems. In the present paper we propose a DES based FDD framework for stochastic timed systems. The scheme is illustrated with an example of a hydraulic punching machine.

1. Introduction

With the raise of complexity of systems, the nature and frequency of failures have increased. Further, many of these systems work with hard real time constraints, where not only logical fault free responses are expected, but also the time at which the responses are produced matters. Such systems are termed as Real Time Systems with delays and deadlines. The problem of diagnosing failures for such complex systems requires a systematic approach and as a result, Failure Detection and Diagnosis (FDD) has become an important research paradigm.

Discrete Event System (DES) framework has been applied for FDD for a wide range of applications because of the simplicity of the framework and the associated algorithms. A DES is characterized by a discrete state space and state transitions are based on discrete events. Most of the real world systems involve continuous dynamics. However, they can also be viewed as DES at some level of abstraction by partitioning the continuous state space and capturing each sub-space in the partition as a discrete state. Hence, the DES framework applies not only to systems that fall naturally in the framework [1,2], (communication networks and digital circuits, for example), but also to continuous variable dynamic systems [3,4], (like heating systems, power plants, automotive and avionics systems etc.)

Within the DES paradigm, several variations have been proposed based on context of the system and failures being monitored. For the most simple type of systems, which are centralized and failure manifest themselves in terms of event sequences, Finite State Machine (FSM) based DES framework is well suited [5,6]. However, if the failures maintain the logical sequence of transitions but manifest in terms of timing deviations (i.e., pre-mature or delayed transitions), timed FSM based DES frameworks are proposed [7–10]. Many large complex systems, however, are physically distributed. To cater to such situations, the works reported in [11,12], studied distributed diagnosis using FSM based DES, in which diagnosis and diagnosability analysis are performed by several diagnosers communicating with each other either directly or through a coordinator and thereby collecting together the observations for analysis and inferencing. Distributed diagnosis using communicating diagnosers may sometimes lead to inconsistencies because of communication delays and communication errors. Petri-nets are known to be used for modeling asynchronous, concurrent and distributed systems. To address this issue of distributed diagnosis, Petri-net based DES frameworks have been developed, considering a so-called true concurrency approach, in which no global state and no global time are available [13–15]. Some other

* Corresponding author. Tel.: +91 8011016433.
E-mail addresses: mail.chaitali@yahoo.in (C.B. Dutta), utpal01in@yahoo.com (U. Biswas).

Peer review under responsibility of Karabuk University.

http://dx.doi.org/10.1016/j.jestch.2015.04.006

recent works on Petri-net based DES for FDD can be found in [16–19]. DES based Petri-net frameworks have also been applied for FDD of hybrid systems that have continuous dynamics. For such systems, continuous Petri-net modeling paradigm [20,21], is applied which works by the concept of discretization.

Broadly speaking, the above mentioned FSM, timed and Petri-net based DES frameworks may either diagnose a failure with certainty or state that the failure is not diagnosable. Diagnosable failures in such frameworks always (i.e., in all traces) result in manifestations like timing deviation, change in sequence of transitions etc. in finite time after occurrence of the failure. So if there is a trace where failure cannot be measured in finite time after its occurrence, it is considered non-diagnosable. The basic assumption for diagnosability decisions in these frameworks is — probability of any trace can be 1 (i.e., a trace can be executed infinitely long). This indirectly implies that for some traces probability of occurrence can be 0 (i.e., a trace many not be executed at all even if transitions of the traces are enabled). So, even if there is a trace where failure is manifested, still its probability can be 0 (never occurring), leading to non-diagnosability.

However in many systems the assumption that some trace can be executed infinitely long while another may not execute at all, may not hold. In those systems, along with transitions, information regarding their relative probability of occurrence is modeled. In such cases, even if there are failures which do not manifest themselves in all traces, still they can be diagnosed with a probability. If the probability of traversing through the traces where failure effect is manifested (and is also detectable) becomes higher than a threshold with increase in time, then failure is considered diagnosable. Stochastic DES framework proposed by Thorsley et al. [22] caters to such systems. However, the scheme was developed only for un-timed systems and the failure considered were the ones that violate the sequence of transitions.

This paper is focussed towards FDD of stochastic timed DES, termed as Stochastic Real Time DES (SRTDES). SRTDES framework is obtained from Timed Transition Model (TTM), proposed by Ostroff et al. [23] for modeling real time systems, by augmenting it with stochastic information. In TTM, real time constraints are associated in terms of delay and deadline requirements to each of the transitions. SRTDES is obtained from TTM by associating probabilities at two levels namely.

- Probability values to transitions, which model the likelihood of firing of transitions. This would enable diagnosis of "violation of delay-deadlines failures" which manifest in *some* traces only. For example, if there is a transition (under normal condition) whose delay-deadline is [2–4] then violation (under failure) may be a corresponding transition with delay-deadline as [5,6]. This transition under failure is called failure manifesting transition. In the model there may be some traces where failure manifesting transition is present and some where it is not. Timed (non-stochastic) DES frameworks [7–10], would render such failures non-diagnosable because it assumes that any trace may execute indefinitely long. In SRTDES model, as probability values are associated with transitions, probability of occurrence of a trace can be calculated. If the probability of all traces where failure manifesting transitions are present increase with time, failure is diagnosable by SRTDES framework. Equivalently in a reverse logic, if probability of traces where failure manifesting transition is not present decrease with time, SRTDES framework considers the failure as diagnosable.
- Probability values to time ticks within the delay-deadline for each transition. This enables diagnosis of even those failures which result in "partial" violation of delay-deadlines. For example, if there is a transition whose delay-deadline is [2–4] then partial violation may be a corresponding (failure manifesting) transition with delay-deadline as [3–5]. It is called "partial" violation because there is a common interval ([3,4] in the example) between the delay-deadline intervals of the normal transition compared to the failure manifesting one. So if the failure manifesting transition fires within the common interval, failure cannot be diagnosed. Since such failures may not violate delay-deadlines in some of the traces in finite time, so they are considered non-diagnosable by non-stochastic timed DES frameworks [7–10]. However, as there is probability values associated with time ticks in SRTDES framework, there is a positive probability that in some traces the failure manifesting transition would fire at a clock tick which is outside common interval. Those traces will make the failure diagnosable if probability of executing such traces increase with time.

In practice, there may be many parameters in a system, modeled as variables in SRTDES framework, which are difficult to be measured; e.g., temperature in the core of a nuclear reaction chamber. In order to model such situations, measurement limitation is considered by partitioning the state variables into measurable and unmeasurable ones. This notion of measurement limitation has been included in the SRTDES formalism. The occurrences of a failure is represented in terms of sub-models. There is a sub-model corresponding to normal behaviour of the system and another sub-model representing the failure. Transition from normal sub-model to failure sub-model is modeled through changes in unmeasurable variables, implying that occurrence of failures cannot be directly detected. Following that an SRTDES diagnoser is designed using an automated procedure. The diagnoser is basically a stochastic state-transition estimator, which can ascertain with a probability the present model state, the present transition and the tick at which the transition has fired. Certain conditions can be checked in the diagnoser to ascertain if the failure is diagnosable. Conditions of diagnosability for SRTDES have been proposed and their necessity and sufficiency have been proved. The theory is illustrated with an example of a hydraulic punching machine.

There are a very few works on FDD of timed DES which model stochastic information. Zemouri et al. in [24] have proposed an FDD technique for stochastic timed DES by augmenting a continuous probability distribution (Gaussian) function over the time between two consecutive transitions. Changes in temporal distance of transitions are considered as failures. So, under each failure, Gaussian functions are determined for each pair of consecutive transitions. These functions are generated by running the system under failure and analyzing the timing of transitions. For FDD on the fly, the transition sequences of the system in execution are monitored. Following that, an attempt is made to match the temporal distances between transitions with the corresponding Gaussian functions of the normal or any failure model. The closest match is taken and status of the system is reported accordingly. As this work is basically based on matching of two functions, it is prone to false alarms.

The main differences between our work proposed in this paper and [24] are the following. The stochastic information augmented on the timed DES framework in [24] is continuous over the temporal distance between two consecutive transitions. So no logical diagnoser could be built nor any logical diagnosability conditions could be proved.[1] In our case, the probability values are discrete

[1] Thorsley et al. in [22] have used the term "logical" (i.e., comprises logic constructs) for DES framework, failure diagnosability condition and diagnoser, if all the parameters used are discrete.