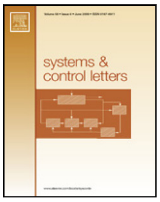
Systems & Control Letters 105 (2017) 48–54

Contents lists available at ScienceDirect

Systems & Control Letters

journal homepage: www.elsevier.com/locate/sysconle



Correctability of fault-tolerant stochastic discrete-event systems[☆]

Fuchun Liu [*], Rixiang Mo

School of Computers, Guangdong University of Technology, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 9 October 2016
Received in revised form 13 April 2017
Accepted 24 April 2017

Keywords:
Failure diagnosis
Discrete-event systems
Stochastic system
Fault-tolerant system
Correctability

ABSTRACT

Failure diagnosis and correction of discrete-event systems (DESs) have received considerable attention in recent years due to the practical and theoretical importance. As a continuation of our prior work on diagnosability of stochastic DESs (i.e., Liu et al., 2008; Liu and Qiu, 2008), this paper aims to investigate the correctability issue, where the considered system is equipped with a probabilistic structure to estimate the likelihood of events occurring. More specifically: (1) We formalize the notion of k-step corrective probability to calculate the correctability of stochastic systems. Roughly speaking, the k-step corrective probability represents the probability that the stochastic system may recover to accepted states from the current state within k steps. (2) By introducing the strategy of adjusting the transition probability of the current state of system, an optimal correction mechanism is presented to achieve the maximal k-step corrective probability. (3) In addition, a novel approach of the computation of supremal corrective probability is developed by constructing the decision tree after introducing the infinitely expandable states. Finally, an example for the evolution process of the voltage in a circuit system modeled by a stochastic automaton is provided to illustrate the proposed results.

1. Introduction

Discrete event systems (DESs) are dynamical systems with discrete states whose evolution is governed by the abrupt occurrence at possibly unknown and irregular intervals of physical discrete events. Even though DESs quite differ from the conventional continuous variable systems, they clearly involve objectives of control and optimization, and a large number of technological and engineering systems including manufacturing systems, transportation systems, military command systems, and computer networks have been successfully modeled by DESs [1].

In order to guarantee performance to a reliable system, the control engineers should design a system that runs safely within its normal boundaries. Thus, failure diagnosis and fault-tolerant control of systems is of practical and theoretical importance, and has received considerable attention in recent years. In [2], a notion of failure diagnosis for DESs was formalized, and a necessary and sufficient condition of diagnosability was obtained by constructing a diagnoser. Then, the work was extended to timed systems [3], decentralized systems [4], linear-time temporal logic specification systems [5], and telecommunication network systems [6]. Fault-tolerance in Petri nets was considered in [7], in which a method for error recovery in automated manufacturing systems was proposed by designing an adaptive Petri net controller. Hsieh [8] studied fault tolerant liveness analysis for Petri nets considering that many real systems usually suffer from failure prone resources, which was subsequently extended to deal with multi-agent manufacturing systems by exploiting the structure of the corresponding collaborative Petri nets [9]. In [10], fault-tolerant supervisor was designed for DESs modeled by bounded Petri nets whose behavior needs to be supervised to meet certain desired specifications. By contrast, a kind of bisimilar Petri net controllers with fault tolerance capabilities was designed in [11], and an optimal design approach for fault-tolerant Petri net controllers was proposed by using arc weights minimization in [12]. Two different approaches for fault-tolerant control were developed by introducing controller's measures to cope with the failure events occurring in the sensors, in which the controllers can be switched [13] or reset [14], respectively. Shu and Lin [15] presented a fault-tolerant control framework for safety of DESs by dividing the system modes into healthy modes and faulty modes, which was subsequently used to deal with the recoverability issue of DESs with faults [16]. Wen et al. [17] also developed a fault-tolerant control framework for DESs from a different aspect with the desire to enforce the specification of the nonfaulty plant such that it can recover from any fault within a bounded delay. In [18,19], the reliable control architecture for decentralized DESs was proposed in face of possible failures of some local supervisors.

[☆] This work was supported by the National Natural Science Foundation (61673122, 61273118), the Provincial Major Program of Guangdong Province (2014KZDXM033), the Public Welfare Research and Capacity Building Project of Guangdong Province (2015A030402006), the Major Award Training Program of School of Computers of GDUT (2016PY01) of China.

[*] Corresponding author.
E-mail address: fliu2011@163.com (F. Liu).

http://dx.doi.org/10.1016/j.sysconle.2017.04.009
0167-6911/© 2017 Elsevier B.V. All rights reserved.

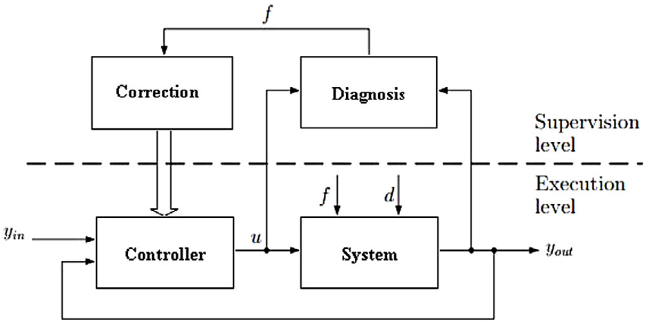


Fig. 1. Architecture of fault-tolerant control with correction.

However, as we know, the classical DES models cannot distinguish between the high probable and less probable strings or states, which leads to the answer for failure diagnosis and fault-tolerant control of systems is only "all-or-nothing" [20]. Stochastic automata, as a natural generalization for deterministic automata of different types, are a more precise formulation of the general DES models, in which a probabilistic structure is appended to estimate the likelihood of specific events occurring. Recently, the diagnosability of systems modeled by stochastic automata was considered and the centralized diagnosis approach for stochastic DESs was presented in [21], which was generalized to the decentralized case and the decentralized failure diagnosis for stochastic DESs was developed in our previous work [20]. Then, we further addressed the safe diagnosability of stochastic DESs [22], which is viewed as the first necessary step of fault-tolerant supervision since the safe diagnosable systems require that fault detection occurs before any forbidden string in the failed mode of systems is executed.

More recently, we studied the correction issue for fault-tolerant classical DESs, in which the notion of correctability of DESs was formalized [23] and a test algorithm was proposed after introducing the concept of correctable states in classical DESs [24]. As a continuation of [20,22], in this paper we focus on the correction related issue under the framework of fault-tolerant control with correction in the setting of stochastic DESs, which represents a generalization of correctability of classical DESs [23,24] to stochastic DESs. Actually, the architecture of fault-tolerant control with correction is depicted in Fig. 1, which extends the usual feedback control framework to the one with the diagnosis and the correction blocks as that described in [25]: In the faultless case, the nominal controller attenuates the disturbance d and ensures the requirements on the closed-loop system. The main control activities occur on the execution level. On the supervision level, the diagnosis block simply recognizes that the closed-loop system is faultless and no correction is necessary. But if a fault f occurs, the supervision level makes the control loop fault-tolerant. The diagnosis block identifies the fault and the correction block performs the recovery action such that the system can return to normal states by repairing the system or re-designing the controller and so on, and afterwards the execution level continues to satisfy the control aims. Based on the architecture of fault-tolerant control with correction shown in Fig. 1, after the diagnosis issue for stochastic DESs was investigated in our prior work [20,22], it is motivated to further consider the correction related issue in this paper.

The main contributions of this paper are as follows. Firstly, the notion of k-step corrective probability is formalized to calculate the correctability of stochastic systems after introducing the state tree structure proposed in [26,27]. Intuitively, k-step corrective probability describes the probability that the stochastic system may recover to accepted states from the current state within k steps once failures occur. Then, a correction mechanism is presented to achieve the maximal k-step corrective probability by adjusting the transition probability of the current state of system. Moreover, a novel approach of the computation of supremal corrective probability is developed by constructing the decision tree after introducing the infinitely expandable states. Finally, an example of the evolution process of the voltage in a circuit system modeled by a stochastic automaton is provided to illustrate the proposed results.

The rest of the paper is organized as follows. In Section 2, some preliminaries including the representation of stochastic automata by using decision trees are reviewed. In Sections 3 and 4, the corrective probability and the supremal corrective probability of stochastic DESs are respectively formalized to capture the ability that the stochastic system recovers from unaccepted states to accepted states. In Section 5, an illustrative example is provided, and we summarize the paper in Section 6.

2. Preliminaries

A stochastic DES is a system modeled by a stochastic automaton

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

where Q is the set of states with the initial state q_0; Σ is the set of events; $\delta : Q \times \Sigma \to 2^Q$ is the transition function; and $P : Q \times \Sigma \times Q \to [0, 1]$ is the probability function appended to transitions for estimating the likelihood that the occurrence of events governs the evolution of the corresponding states, which satisfies: for any state $q \in Q$,

$$\sum_{a\in\Sigma}\sum_{q'\in Q} P(q, a, q') = 1 \tag{1}$$

or

$$\sum_{a\in\Sigma}\sum_{q'\in Q} P(q, a, q') = 0. \tag{2}$$

Intuitively, Eq. (1) means that the sum of the probabilities of all transitions from each state is equal to one, which indicates that transitions of the state q definitely occur, and Eq. (2) means that the state q is a dead state without any transition.

The set of states is divided into the subsets of accepted states and unaccepted states, which are denoted by Q_a and Q_{ua}, respectively, where $Q_a \subseteq Q$ and $Q_{ua} = Q - Q_a$. Denote Σ^* as the Kleene closure of Σ, which is the set of all finite strings over Σ including the empty string ϵ.

Given a state $q \in Q$, the neighbor of q, denoted by $N(q)$, is defined as the set

$$\{p \in Q : (\exists a \in \Sigma)p \in \delta(q, a) \wedge P(q, a, p) \neq 0\}.$$

In the following, the representation of decision trees of stochastic automata is introduced.

A tree is a connected graph without any cycle, in which the vertices and the edges are called nodes and branches, respectively.

Definition 1. Let $G = (Q, \Sigma, \delta, q_0, P)$ be a stochastic automaton. A state tree of G is a tuple

$$t = (n_r, R(n_r)),$$

in which $n_r \in Q$ is the root node of t, $R(n_r) \subseteq T$ is the set of all state trees out of n_r with the form $(n_r', R(n_r'))$, where $n_r' \in Q$, $R(n_r') \subseteq T$, T is the set of state trees of t.

For example, consider the stochastic automata shown in Fig. 2. The state tree of G in Fig. 2(a) is $t = (1, R(1))$, where $R(1) = \{(3, \emptyset), (4, R(4)), (2, \emptyset)\}$ and $R(4) = \{(5, \emptyset), (6, \emptyset)\}$. The state tree of G shown in Fig. 2(b) is $t = (1, R(1))$, where $R(1) = \{(2, R(2)), (3, R(3))\}$ with $R(2) = \{(4, \emptyset), (5, \emptyset)\}$, $R(3) =$