Automatica 98 (2018) 28–33

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Fault tolerant control for a class of interconnected asynchronous sequential machines☆

Jung-Min Yang

School of Electronics Engineering, Kyungpook National University, 80 Daehakro, Bukgu, Daegu, 41566, Republic of Korea

ARTICLE INFO

Article history:
Received 27 September 2017
Received in revised form 30 January 2018
Accepted 24 July 2018

Keywords:
Asynchronous sequential machines (ASMs)
Corrective control
Fault tolerant control
Parallel composition
Output feedback

ABSTRACT

This paper considers fault tolerant control for parallel interconnected asynchronous sequential machines (ASMs) governed by a single corrective controller with output feedback. The control objective is to diagnose unauthorized state transitions and to recover the normal input/output behavior of the closed-loop system in an asynchronous mechanism. The existence condition and design algorithm for a fault tolerant controller is addressed in the framework of corrective control. The proposed scheme is efficient in that it does not require complete modeling of parallel composition nor output bursts in the feedback channel. An illustrative example is provided to demonstrate the procedure of controller synthesis.

1. Introduction

Corrective control is an automatic control theory aiming at compensating for the closed-loop behavior of asynchronous sequential machines (ASMs). In particular, it shows superior performance in fault diagnosis and tolerance since both can be achieved instantaneously by virtue of asynchrony (Hammer, 2016; Peng & Hammer, 2010; Yang, 2015). This paper addresses fault tolerant control for a composite ASM that consists of a number of single ASMs, called *submachines*, in a parallel connection. Many practical systems are made of various compositions of unit systems for the purpose of enlarging workspace and system performance (Lee & Varaiya, 2011). One interesting problem for composite systems is how to detect malfunctions occurring to each sub-system and to recover the normal operation in terms of the global behavior, possibly with less size of controllers.

In our study, each submachine is subjected to transient faults in which adversarial inputs infiltrating into the machine cause unauthorized state transitions. We propose a control scheme that employs a single controller for achieving fault tolerance. The main objective is to present the existence condition and design procedure for a corrective controller that detects unauthorized state transitions and takes the composite ASM towards the normal input/output behavior. Specifically, the proposed controller has only access to unit output feedback instead of output bursts or state feedback, and yet no state observer is needed to estimate the current state as done in Peng and Hammer (2012). In this sense, the way the controller composes feedback paths is similar to the author's previous work (Yang, 2015). However, Yang (2015) considers fault tolerant control for single ASMs. While the author's another work (Yang, 2016) also studies fault tolerant control for composite ASMs, the considered machine has cascade composition in the study.

Parallel composition is widely used in supervisory control for discrete-event systems (DESs). As pointed out in Cassandras and Lafortune (2008), a serious problem of parallel composition is that the number of states grows exponentially with respect to that of components. We try to alleviate this computational burden by proposing a scheme that does not need complete modeling of the composite ASM in designing a controller. In the field of DESs, supervisory control for parallel interconnected systems or concurrent DESs is first studied in Willner and Heymann (1991). Decentralized control (Jiang & Kumar, 2000) and hierarchical interface-based control (Leduc, Lawford, & Dai, 2006) are also reported to tackle the supervisory control problem of concurrent DESs. Our work differs from these studies in that whereas local supervisors are assigned to each sub-system in the previous results, only a single corrective controller is utilized in our work. Further, those results are not applicable to composite ASMs since they do not guarantee fundamental mode.

Since direct access to the state of each submachine is unavailable in our framework, certain conditions on the dynamics of

☆ This research was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. NRF-2015R1D1A1A01056764), and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1A5A1025137). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Joerg Raisch under the direction of Editor Christos G. Cassandras.

E-mail address: jmyang@ee.knu.ac.kr.

https://doi.org/10.1016/j.automatica.2018.09.018
0005-1098/

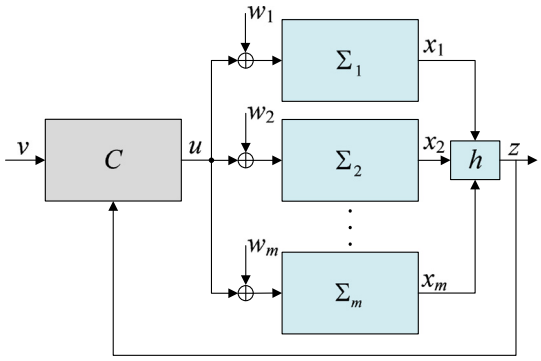

Fig. 1. Corrective control system for the composite ASM in parallel connection.

the composite ASM should be valid for the controller to identify the end of transitions. We show that the latter condition, called strong (fault) detectability, is more restrictive in the case of parallel interconnected ASMs. Note that our notion of strong detectability differs from detectability of DESs (Shu, Lin, & Ying, 2007) or diagnosability in fault diagnosis and fault tolerant control of DESs (Paoli, Sartini, & Lafortune, 2011; Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1995). The exact fault or state at which the fault occurs is not identified in our study. Instead, the controller determines when the normal or faulty transition terminates in order to initiate the correction procedure asynchronously, hence maintaining fundamental mode operations.

The rest of this paper is organized as follows. In Section 2, we present the modeling of parallel interconnected ASMs with faulty transitions. In Section 3, fault detectability is introduced to investigate whether a corrective controller can detect the end of state transitions to preserve fundamental mode. In Section 4, the existence condition and design algorithm for a fault tolerant corrective controller is presented with an emphasis on using only dynamics of submachines in controller design. In Section 5, we validate the proposed notions and controller construction in an illustrative example. A brief summary is followed in Section 6.

2. Notations and basics

Fig. 1 shows the corrective control system where m parallel interconnected single ASMs $\Sigma_1, \ldots, \Sigma_m$ make a composite ASM Σ and C is the corrective controller. Denote by Σ_c the closed-loop system composed of C and Σ. Each Σ_i, $i \in M := \{1, \ldots, m\}$, is an input/state stable-state ASM modeled as $\Sigma_i = (A, X_i, s_i)$ where A is the input set, X_i is the state set with $|X_i| = n_i$, and $s_i : X_i \times A \to X_i$ is the stable recursion function partially defined on $X_i \times A$.

With asynchronous mechanisms, Σ_i stays at a stable state indefinitely, and only by an input change does it transfer to the next stable state, passing through a number of transient states instantaneously. Since transient transitions of ASMs are very fast, one usually describes their state transitions solely in terms of stable states, termed *stable transitions*. In this regard we represent each Σ_i by defining s_i as $s_i(x_i, u) := x_i'$ where $x_i' \in X_i$ is the next stable state of $(x_i, u) \in X_i \times A$ and no transient states are traversed between x_i and x_i'. The domain of s_i can be extended to $X_i \times A^+$ in a natural way, e.g., $s_i(x_i, u_1u_2) := s_i(s_i(x_i, u_1), u_2)$.

Σ is an input/output ASM described as

$$\Sigma = \Sigma_1 \| \cdots \| \Sigma_m = (A, Z, X, s, h)$$

where A is the input set, Z is the output set, $X := X_1 \times \cdots \times X_m$ is the state set with $|X| = \prod_{i=1}^m n_i$, $s : X \times A \to X$ and $h : X \to Z$ are the stable recursion function and output function, respectively. Define $\Pi_i : X \to X_i$ as the standard projection of X onto X_i, i.e., $\Pi_i x = x_i$ for $x = (x_1, \ldots, x_m)$. The order of stable transitions between Σ_i's is nondeterministic in general. Regardless of the order, however, the next stable states reached by $\Sigma_1, \ldots, \Sigma_m$ are always deterministic.

A is further divided into $A = A_n \dot\cup A_d$ where A_n and A_d are the set of normal and adversarial inputs, respectively. $w_i \in A_d$ in Fig. 1 denotes the adversarial input occurring to Σ_i. When w_i enters Σ_i, it overrides the current input $u \in A_n$, causing Σ_i to undergo an unauthorized transition. Unless recovered immediately, Σ_i would have incorrect transitions thereafter, leading to malfunction of Σ. Define $W(x_i) := \{w_i \in A_d | s_i(x_i, w_i) \neq x_i\}$ as the set of adversarial inputs that can occur to Σ_i when Σ_i stays at the stable state x_i. Further, define $W(x) := \cup_{i \in M} W(x_i)$ for $x = (x_1, \ldots, x_m)$ and $W(X') := \cup_{x \in X'} W(x)$ for $X' \subset X$.

In Fig. 1, C is an input/output ASM receiving the external input $v \in A_n$ and the output feedback $z \in Z$ to provide the control input $u \in A_n$. C is modeled as

$$C = (A_n \times Z, A_n, \Xi, \xi_0, \phi, \eta)$$

where $A_n \times Z$ and A_n are the input and output set, Ξ is the state set, $\xi_0 \in \Xi$ is the initial state, $\phi : \Xi \times A_n \times Z \to \Xi$ is the recursion function, and $\eta : \Xi \to A_n$ is the output function. The main objective is to design C that achieves immediate fault recovery against any unauthorized transitions caused by w_i, $i \in M$. Since only the output of Σ is available to C, the exact state of Σ is not identified in general. Thus we regard that fault recovery is achieved if Σ_c is controlled to reach a state that generates the same output as possessed by Σ at the moment of fault occurrence.

To prevent incorrect outcomes caused by the lack of a synchronizing clock, Σ_c is supposed to maintain the principle of fundamental mode operations (Kohavi & Jha, 2010) under which a variable changes its value only when both C and Σ are in stable states, and no two or more variables are altered simultaneously.

In corrective control for a single ASM $\Sigma_i = (A, X_i, s_i)$, stable reachability between two states measured in $n_i - 1$ ($n_i = |X_i|$) or less steps is sufficient to describe the entire reachability (Peng & Hammer, 2010). On the other hand, when $\Sigma_1, \ldots, \Sigma_m$ are combined into parallel composition, we must take into account more steps since even though the current input induces a valid transition with an ASM, it may not do with another machine. To this end, we first introduce a generalized stable recursion function of Σ_i defined as a total function $\hat{s}_i : X_i \times A \to X_i$ such that

$$\hat{s}_i(x_i, u) := \begin{cases} s_i(x_i, u) & \text{if } s_i(x_i, u) \text{ is defined} \\ x_i & \text{otherwise} \end{cases}$$

All the invalid state–input pairs are regarded as stable ones in $\hat{s}_i$. This formalism is not restrictive since an ASM would not respond to an incoming input that is not defined at the current state, hence staying at the same state. In association with $\hat{s}_i$, s can be written as

$$s(x_1, \ldots, x_m, u) := (\hat{s}_1(x_1, u), \ldots, \hat{s}_m(x_m, u)).$$

The domain of s can be also extended to $P(X) \times A$ as ($P(X)$ is the power set of X) $s(X', u) := \{s(x, u) | x \in X'\}$ for $X' \subset X$. Similarly, we extend the domain and range of the output function to $h : P(X) \to P(Z)$ as $h(X') := \{h(x) | x \in X'\}$.

Definition 1. Denote by $X_i := \{x_i^1, \ldots, x_i^{n_i}\}$ for $\Sigma_i = (A, X_i, s_i)$. $\hat{R}(\Sigma_i)$, the extended matrix of stable transitions of Σ_i, is an $n_i \times n_i$ matrix whose (p, q) entry is

$$\hat{R}_{p,q}(\Sigma_i) := \{t \in A_n^+ | \hat{s}_i(x_i^p, t) = x_i^q, |t| \leq n - m\}$$

where $n := \sum_{i=1}^m n_i$.

$\hat{R}(\Sigma_i)$ contains not only essential input sequences representing stable reachability of Σ_i, but also redundant ones that can make valid transitions with other ASMs (note that $n - m = \sum_{i=1}^m (n_i - 1)$).