Automatica 52 (2015) 76–82

Contents lists available at ScienceDirect

Automatica

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

Brief paper

A simple fault tolerant control for input/output asynchronous sequential machines☆

Jung-Min Yang [1]

School of Electronics Engineering, Kyungpook National University, 80 Daehakro, Bukgu, Daegu, 702-701, Republic of Korea

ARTICLE INFO

Article history:
Received 22 August 2013
Received in revised form
13 September 2014
Accepted 3 October 2014
Available online 19 November 2014

Keywords:
Asynchronous sequential machines
Corrective control
Fault tolerance
Input/output control
Transient faults

ABSTRACT

This paper presents a fault tolerant controller for asynchronous sequential machines subject to unauthorized state transitions caused by adversarial inputs. The input/output machines are considered where direct access to the machine's state is unavailable. If the asynchronous machine satisfies some condition on transition feature and reachability, we can design a simple output feedback controller that needs neither a state observer nor output bursts. Despite insufficient knowledge of the current state, the proposed controller automatically counteracts any transient fault so that the closed-loop system can maintain the normal input/output behavior.

1. Introduction

By virtue of fast response speed, asynchronous sequential machines have been extensively used in many areas such as the construction of high-speed computing systems, microprocessors, digital communication, etc. (Martin & Nyström, 2006; Sparsø & Furber, 2001). Their applications also include hazardous and safety-critical environments like space and nuclear power plants. Asynchronous machines working in these environments are vulnerable to unpredictable faults that cause undesired reactions and, if not overcome, may lead to total breakdown of the system. For ensuring robust and safe behavior, asynchronous sequential machines must be equipped with competent fault diagnosis and tolerance functioning. In this paper, we address a fault diagnosis and tolerance scheme based on the feedback control mechanism for asynchronous machines (Geng & Hammer, 2005; Murphy, Geng, & Hammer, 2003; Xu & Hong, 2013; Yang, 2011). A feedback controller, often termed a corrective controller, is placed in front of the considered asynchronous machine and whenever diagnosing fault occurrences, the controller generates a control input sequence to the machine so that the closed-loop system can seem immune against adversarial effects of the faults with no degraded performance (Peng & Hammer, 2010; Yang, 2010; Yang & Kwak, 2012a,b).

The main objective of this paper is to propose a fault tolerant controller for input/output asynchronous machines where direct access to the state information is unavailable. The considered machine is subject to transient faults, in which adversarial inputs infiltrate into the machine, causing unauthorized state transitions. The control goal is to return the machine to the normal behavior instantaneously before further change of the external input. Control of input/output asynchronous machines was initiated by Geng and Hammer (2005) for the problem of model matching, and recently fault tolerant control of input/output machines was proposed for transient faults (Yang, 2010), intermittent faults (Yang & Kwak, 2012a), and permanent faults (Yang & Kwak, 2012b), respectively. According to this assortment, the present study is a continuation of Yang (2010). However, compared with the former studies, this paper has the following contribution.

(1) All of the former studies use the state observer that estimates the exact state of the machine. While the use of the state observer facilitates the controller construction, it requires additional design load. In this study, we propose a control scheme that needs no state observer. The output of the machine is thus directly delivered to the controller.
(2) In most of the former studies, the output has the form of bursts, a rapidly progressing string of outputs. Fault detectability and

☆ This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2012R1A2A2A01003419), and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. NRF-2010-0007271). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Bart De Schutter under the direction of Editor Ian R. Petersen.

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

[1] Tel.: +82 53 950 7235; fax: +82 53 950 5505.

http://dx.doi.org/10.1016/j.automatica.2014.10.107
0005-1098/

existence conditions for a controller are more relaxed with access to bursts. On the other hand, we need buffers and memories to store output bursts. Aiming to reduce the resource of fault tolerant controllers, the present study does not utilize burst information in fault tolerant control. While Peng and Hammer (2010) also present a research result that does not use output bursts, their control objective is to invalidate critical races.

The rest of this paper is structured as follows. In Section 2, starting with background material on modeling of asynchronous sequential machines, we present the notion of state uncertainty and detectability for input/output machines with no use of state observers. In Section 3, we present the existence condition and design procedure of a fault tolerant controller for input/output asynchronous machines. We focus our concern on robust feedback paths, namely correction trajectories through which the faulty machine can recover the normal input/output behavior despite the underlying state uncertainty. In Section 4, we demonstrate the proposed notions and controller construction in an illustrative example. Finally, in Section 5, we summarize the main contributions of the paper.

2. Preliminaries

2.1. Modeling

For a finite non-empty alphabet A, $|A|$ denotes its cardinality and A^+ the set of all non-empty strings of characters in A. For a string $t \in A^+$, $|t|$ is the length of t, and $t_i \in A$ is the ith element of t ($1 \leqslant i \leqslant |t|$). Also, let $t_{|i} := t_1 \dots t_i$ be the prefix of t up to the ith element.

An input/output asynchronous sequential machine Σ is characterized by a finite state machine $\Sigma = (A, Y, X, x_0, f, h)$, where A is the input set, Y is the output set, X is the state set, and $x_0 \in X$ is the initial state; the state transition function $f : X \times A \to X$ and the output function $h : X \to Y$ are partial functions. We partition A into two disjoint subsets $A := A_n \cup A_d$ where A_n is the normal input set and A_d is the set of adversarial inputs.

A state x can be either *stable* or *transient* according to the current input u. If $f(x, u) = x$, x is a stable state; otherwise, it is a transient state. A transient combination (x, u) makes Σ go through a chain of transient transitions $x_1 = f(x, u), x_2 = f(x_1, u), \dots$, until reaching the *next stable state* $x_k = f(x_k, u)$. Since the duration that Σ stays at a transient state is instantaneous due to the lack of a synchronizing clock, we properly exclude all transient states and consider only the *stable transition*, namely from a stable state to its next stable state. The *stable recursion function* $s : X \times A \to X$ embodies the stable transitions. For a valid pair $(x, u) \in X \times A$, $s(x, u) := x_k$ is defined as the next stable state of (x, u). s is often extended from inputs to sequences recursively: for $x \in X$ and $u_1 u_2 \dots u_k \in A^+$,

$$s(x, u_1 u_2 \dots u_k) := s(s(x, u_1), u_2 \dots u_k).$$

In the stable transition from x to x_k, Σ generates a sequence of outputs $h(x), h(x_1), \dots, h(x_k)$. This string, termed the output burst (Geng & Hammer, 2005), has played a key role in corrective control for input/output asynchronous machines at the cost of higher controller complexity and additional resource. In this study, we present a scheme of controller design that does not utilize the output burst. Thus the controller will receive the output feedback only in the form of a single character.

Fig. 1 is the basic control configuration. C is the corrective controller that achieves fault tolerance for Σ. $v \in A_n$ is the external input, $u \in A_n$ is the control input generated by C, and $y \in Y$ is the output that is delivered to C as the output feedback. Σ_c denotes the closed-loop system consisting of C and Σ. $w \in A_d$ is the adversarial input that forces unauthorized state transitions to Σ. w is not observable nor disabled by C, which fits into the nature of adversarial entities. Whenever w occurs to Σ, it overrides the control input u and vice versa. Hence, the input to Σ is defined as one of u and w of which value changes at the last.

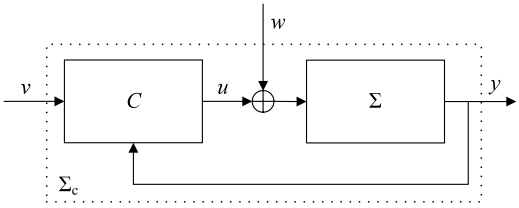

Fig. 1. Fault tolerant control system.

Owing to the lack of a synchronizing clock, we have to design an asynchronous machine in such a way that the input does not change while the machine undergoes state transitions; otherwise one could not identify the exact state at which the input change occurs. This operating policy is referred to as *fundamental mode operation* (Kohavi & Jha, 2010). Throughout this paper, all asynchronous machines are supposed to operate in fundamental mode.

2.2. State uncertainty and detectability

Suppose that Σ stays at a stable state with the external input v and the output y. Although direct access to the current state is impossible, the information on v and y allows us to estimate all the possible states where Σ may stay. We term the set of such states the *state uncertainty*. The more information we have access to, the more we can reduce the size of the state uncertainty. First, we express the state uncertainty solely in terms of the output. Define $E_1(y) \subset X$ as

$$E_1(y) := \{x \in X | h(x) = y\}.$$

Using v, we can reduce the state uncertainty further since the current state makes a stable combination with v as well as it provides the output y. Let $E_2(v, y)$ denote the set of such states:

$$E_2(v, y) := \{x \in E_1(y) | s(x, v) = x\}.$$

If we know the previous state uncertainty, further reduction of the state uncertainty is possible. Let $\chi \subset X$ be the previous state uncertainty, that is, Σ has experienced a stable transition from a state with the state uncertainty χ to the current state. What we deduce from χ is that the current state is the next stable state of a state in χ with the external input v. $E_3(\chi, v, y)$ represents those states as follows.

$$E_3(\chi, v, y) := \{x \in E_2(v, y) | \exists x' \in \chi \text{ s.t. } s(x', v) = x\}.$$

To preserve fundamental mode operation, the input must not change while the machine undergoes transitions. Hence, the controller C must determine *whether* Σ has reached a next stable state either by the normal input or by the adversarial input. Assume that Σ stays at a stable state with the state uncertainty χ, when the input changes to $v \in A_n$. Then, the pair (χ, v) is said to be *strongly detectable* if it can be determined from inputs and outputs of Σ whether the next stable state of (χ, v) has been reached. This notion was first introduced by Peng and Hammer (2010) for describing nondeterminism by critical races.

While Σ undergoes a stable transition, it passes through a number of transient states, providing the corresponding sequence of outputs. With no use of the output burst, the only condition for knowing the end of a stable transition is that the outputs of the possible next stable states must be different from all the other outputs generated in the transitions. To formalize this condition,