Automatica 86 (2017) 174–182

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Design of decentralized critical observers for networks of finite state machines: A formal method approach [☆]

Giordano Pola, Elena De Santis, Maria Domenica Di Benedetto, Davide Pezzuti

Department of Information Engineering, Computer Science and Mathematics, Center of Excellence DEWS, University of L'Aquila, 67100 L'Aquila, Italy

ARTICLE INFO

Article history:
Received 4 December 2014
Received in revised form 11 February 2017
Accepted 12 August 2017

Keywords:
Network of finite state machines
Critical observability
Decentralized observers
Bisimulation equivalence

ABSTRACT

Motivated by safety-critical applications in cyber–physical systems, in this paper we study the notion of critical observability and design of observers for networks of Finite State Machines (FSMs). Critical observability corresponds to the possibility of detecting if the current state of an FSM is in a given region of interest, called set of critical states. A critical observer detects on-line the occurrence of critical states. When a large-scale network of FSMs is considered, the construction of such an observer is prohibitive because of the large computational effort needed. We propose a decentralized architecture for critical observers of networks of FSMs, where on-line detection of critical states is performed by local critical observers, each associated with an FSM of the network, which do not need to interact. For the efficient design of decentralized critical observers we first extend on-the-fly algorithms traditionally used in the community of formal methods for the verification and control design of FSMs. We then extend to networks of FSMs, bisimulation theory traditionally given in the community of formal methods for single FSMs. The proposed techniques provide a remarkable computational complexity reduction, as discussed throughout the paper and also demonstrated by means of illustrative examples.

1. Introduction

Ensuring safety in large-scale and networked safety-critical applications, as for example Air Traffic Management (ATM) systems (MAREA, 2011; Pezzuti, 2015), is a tough but challenging problem. In particular, complexity is one of the most difficult issues that must be overcome to make theoretical methodologies applicable to real industrial applications. In this paper we address the analysis of critical observability and design of observers for networks of Finite State Machines (FSMs). A network of FSMs is a collection of FSMs interacting via parallel composition. Critical observability, introduced in De Santis, Di Benedetto, Di Gennaro, D'Innocenzo, and Pola (2005), corresponds to the possibility of detecting if the current state of an FSM belongs to a set of critical states, modeling operations that may be unsafe or, in general, operations of specific interest in a particular application. Current approaches to check critical observability are based on regular language theory as in Di Benedetto, Di Gennaro, and D'Innocenzo (2008) or on the design of the so-called critical observers (Cassandras & Lafortune, 1999; De Santis et al., 2005). The computational complexity of the first approach is polynomial in the number of states of the FSM, while the one of the second is exponential. Although disadvantageous from the computational complexity point of view, the construction of critical observers cannot be avoided at the implementation layer since it is necessary for the automatic on-line detection of critical situations. Motivated by this issue we present some results that can reduce, in some cases drastically, the computational effort in designing critical observers for large-scale networks of FSMs. We first propose a decentralized architecture for critical observers of the network, which is composed of a collection of local critical observers, each associated with an FSM of the network, which do not need to interact. Efficient algorithms for their synthesis are proposed, and based on on-the-fly techniques traditionally used for formal verification and control of FSMs (see e.g. Courcoubetis, Vardi, Wolper, & Yannakakis, 1992; Tripakis & Altisen, 1999). We then propose results on model reduction, which extend to networks of FSMs, bisimulation theory (Milner, 1989; Park, 1981) traditionally given for single FSMs. We define a bisimulation equivalence that takes into account criticalities. We then reduce the original network of FSMs to a smaller one, obtained as the quotient of the original network induced by the bisimulation equivalence. We first show that critical observability of the original network is equivalent to critical observability of the quotient network. We then show that a decentralized critical observer for the original

[☆] This work has been partially supported by the Center of Excellence for Research DEWS, University of L'Aquila, Italy. The material in this paper was partially presented at the 14th annual European Control Conference, July 15–17, 2015, Linz Austria. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: giordano.pola@univaq.it (G. Pola), elena.desantis@univaq.it (E. De Santis), mariadomenica.dibenedetto@univaq.it (M.D. Di Benedetto), davide.pezzuti@graduate.univaq.it (D. Pezzuti).

http://dx.doi.org/10.1016/j.automatica.2017.08.025
0005-1098/© 2017 Elsevier Ltd. All rights reserved.

network can be easily derived from the one designed for the quotient network. To the best of our knowledge, the formal methods techniques proposed in this paper have not yet been explored neither for the analysis of critical observability nor for the analysis of any other observability notion, with the only exception of Zad, Kwong, and Wonham (2003). We defer to the last section a discussion on connections with the existing literature. A full version of this paper can be found in Pola, Pezzuti, Santis, and Benedetto (2017) which also includes an application to biological networks.

2. Networks of finite state machines and critical observability

2.1. Notation and preliminary definitions

The symbols $\wedge$ and $\vee$ denote the *And* and *Or* logical operators, respectively. The symbol $\mathbb{N}$ denotes the set of nonnegative integers. Given $n, m \in \mathbb{N}$ with $n < m$ let $[n; m] = [n, m] \cap \mathbb{N}$. The symbol $|X|$ denotes the cardinality of a finite set X. The symbol 2^X denotes the power set of a set X. Given a function $f : X \rightarrow Y$ we denote by $f(Z)$ the image of a set $Z \subseteq X$ through f, i.e. $f(Z) = \{y \in Y | \exists z \in Z \text{ s.t. } y = f(z)\}$; if $X' \subset X$ and $Y' \subset Y$ then $f|_{X' \rightarrow Y'}$ is the restriction of f to domain X' and co-domain Y', i.e. $f|_{X'\rightarrow Y'}(x) = f(x)$ for any $x \in X'$ with $f(x) \in Y'$. We now recall from Cassandras & Lafortune (1999) some basic notions of language theory. Given a set Σ, a finite sequence $w = \sigma_1\sigma_2\sigma_3\ldots$ with symbols $\sigma_i \in \Sigma$ is called a word in Σ; the empty word is denoted by ε. The Kleene closure w^* of a word w is the collection of words ε, w, ww, www, … . The symbol Σ^* denotes the set of all words in Σ, including the empty word ε. The concatenation of two words $u, v \in \Sigma^*$ is denoted by $uv \in \Sigma^*$. Any subset of Σ^* is called a language. The projection of a language $L \subseteq \Sigma^*$ onto a subset $\widehat{\Sigma}$ of Σ is the language $P_{\widehat{\Sigma}}(L) = \{t \in \widehat{\Sigma}^* | \exists w \in L \text{ s.t. } P_{\widehat{\Sigma}}(w) = t\}$ where $P_{\widehat{\Sigma}}(w)$ is inductively defined for any $w \in L$ and $\sigma \in \Sigma$ by $P_{\widehat{\Sigma}}(\varepsilon) = \varepsilon$ and $P_{\widehat{\Sigma}}(w\sigma) = P_{\widehat{\Sigma}}(w)\sigma$ if $\sigma \in \widehat{\Sigma}$ and $P_{\widehat{\Sigma}}(w\sigma) = P_{\widehat{\Sigma}}(w)$, otherwise.

2.2. Networks of finite state machines

In this paper we consider the class of nondeterministic FSMs with observable labels:

Definition 2.1. A Finite State Machine (FSM) M is a tuple (X, X^0, Σ, δ) where X is the set of states, $X^0 \subseteq X$ is the set of initial states, Σ is the set of input labels and $\delta : X \times \Sigma \rightarrow 2^X$ is the transition map.

A state run r of an FSM M is a sequence $x^0 \xrightarrow{\sigma^1} x^1 \xrightarrow{\sigma^2} x^2 \xrightarrow{\sigma^3} x^3 \ldots$ such that $x^0 \in X^0$, $x^i \in X$, $\sigma^i \in \Sigma$ and $x^{i+1} \in \delta(x^i, \sigma^{i+1})$ for any x^i and σ^i in the sequence; the sequence $\sigma^1\sigma^2\sigma^3 \ldots$ is called the trace associated with r. For $X' \subseteq X$ and $\sigma \in \Sigma$, we abuse notation by writing $\delta(X', \sigma)$ instead of $\bigcup_{x \in X'} \delta(x, \sigma)$. The extended transition map $\hat{\delta}$ associated with δ is inductively defined for any $w \in \Sigma^*$, $\sigma \in \Sigma$ and $x \in X$ by $\hat{\delta}(x, \varepsilon) = \{x\}$ and $\hat{\delta}(x, w\sigma) = \bigcup_{y \in \hat{\delta}(x,w)} \delta(y, \sigma)$. The language generated by M, denoted $L(M)$, is composed by all traces generated by M, or equivalently, $L(M) = \{w \in \Sigma^* | \exists x^0 \in X^0 \text{ s.t. } \hat{\delta}(x^0, w) \neq \varnothing\}$. An FSM M is deterministic if $|X^0| = 1$ and $|\delta(x, \sigma)| \leq 1$, for any $x \in X$ and $\sigma \in \Sigma$. In this paper we are interested in studying whether it is possible to detect if the current state of an FSM M is or is not in a set of critical states $C \subset X$ modeling operations that may be unsafe or, in general, operations of specific interest in a particular application. We refer to an FSM (X, X^0, Σ, δ) equipped with a set of critical states C by the tuple $(X, X^0, \Sigma, \delta, C)$ and to an FSM with outputs by a tuple $(X, X^0, \Sigma, \delta, Y, H)$, where Y is the set of output labels and $H : X \rightarrow Y$ is the output function. For simplicity we call an FSM equipped with critical states or with outputs as an FSM. The operator $\mathrm{Ac}(\cdot)$ extracts the accessible part from an FSM $M = (X, X^0, \Sigma, \delta, C)$ (resp. $M = (X, X^0, \Sigma, \delta, Y, H)$), i.e. $\mathrm{Ac}(M) = (X', X^0, \Sigma, \delta', C')$ (resp. $\mathrm{Ac}(M) = (X', X^0, \Sigma, \delta', Y, H')$) where $X' = \{x \in X | \exists x^0 \in X^0 \wedge w \in \Sigma^* \text{ s.t. } x \in \hat{\delta}(x^0, w)\}$, $\delta' = \delta|_{X' \times \Sigma \rightarrow X'}$, $C' = C \cap X'$ and $H' = H|_{X' \rightarrow Y}$. Interaction among FSMs is captured by the following.

Definition 2.2. The parallel composition $M_1 \parallel M_2 = \big(X_{1,2}, X^0_{1,2}, \Sigma_{1,2}, \delta_{1,2}, C_{1,2}\big)$ between two FSMs $M_1 = (X_1, X_1^0, \Sigma_1, \delta_1, C_1)$ and $M_2 = (X_2, X_2^0, \Sigma_2, \delta_2, C_2)$ is the FSM $\mathrm{Ac}(X'_{1,2}, X'^{,0}_{1,2}, \Sigma'_{1,2}, \delta'_{1,2}, C'_{1,2})$ where $X'_{1,2} = X_1 \times X_2$, $X'^{,0}_{1,2} = X_1^0 \times X_2^0$, $\Sigma'_{1,2} = \Sigma_1 \cup \Sigma_2$, $C'_{1,2} = (C_1 \times X_2) \cup (X_1 \times C_2)$ and $\delta'_{1,2} : X'_{1,2} \times \Sigma'_{1,2} \rightarrow 2^{X'_{1,2}}$ is defined for any $x_1 \in X'_1$, $x_2 \in X'_2$ and $\sigma \in \Sigma'_{1,2}$ by

$$\begin{cases} \delta_1(x_1, \sigma) \times \delta_2(x_2, \sigma), \text{ if } \delta_1(x_1, \sigma) \neq \varnothing \wedge \ \delta_2(x_2, \sigma) \neq \varnothing \\ \qquad\qquad\qquad \wedge \ \sigma \in \Sigma_1 \cap \Sigma_2, \\ \delta_1(x_1, \sigma) \times \{x_2\}, \text{ if } \delta_1(x_1, \sigma) \neq \varnothing \wedge \ \sigma \in \Sigma_1 \setminus \Sigma_2, \\ \{x_1\} \times \delta_2(x_2, \sigma), \text{ if } \delta_2(x_2, \sigma) \neq \varnothing \wedge \ \sigma \in \Sigma_2 \setminus \Sigma_1, \\ \varnothing, \text{ otherwise.} \end{cases}$$

By definition, a state $(x_1, x_2) \in C_{1,2}$, i.e. (x_1, x_2) is considered as critical for $M_1 \parallel M_2$, if and only if $x_1 \in C_1$ or $x_2 \in C_2$. Vice versa, $(x_1, x_2) \notin C_{1,2}$ if and only if $x_1 \notin C_1$ and $x_2 \notin C_2$. It is well known that

Proposition 2.3 (Cassandras & Lafortune, 1999). *The parallel composition operation is commutative up to isomorphisms and associative.*

By the result above, we may write in the sequel $M_1 \| M_2 \| M_3$, $X_{1,2,3}$ and $C_{1,2,3}$ instead of $M_1 \| (M_2 \| M_3)$, $X_{1,(2,3)}$ and $C_{1,(2,3)}$ or, instead of $(M_1 \| M_2) \| M_3$, $X_{(1,2),3}$ and $C_{(1,2),3}$. In this paper we consider a network

$$\mathcal{N} = \{M_1, M_2, \ldots, M_N\}$$

of N FSMs M_i whose interaction is captured by the notion of parallel composition; the corresponding FSM is given by $\mathbf{M}(\mathcal{N}) = M_1 \parallel M_2 \| \cdots \| M_N$. The FSM $\mathbf{M}(\mathcal{N})$ is well defined because the composition operator $\|$ is associative. For the computational complexity analysis, we will use in the sequel the number $n_{\max} = \max_{i \in [1;N]} |X_i|$ as indicator of the sizes of the FSMs composing the network $\mathcal{N}$. An upper bound to space and time computational complexity in constructing $\mathbf{M}(\mathcal{N})$ is $O(2^{N \log(n_{\max})})$.

2.3. Critical observability and observers

Critical observability corresponds to the possibility of detecting whether the current state x of a run of an FSM is or is not critical on the basis of the information given by the corresponding trace at state x:

Definition 2.4. An FSM $M = (X, X^0, \Sigma, \delta, C)$ is critically observable if $[\hat{\delta}(x^0, w) \subseteq C] \vee [\hat{\delta}(x^0, w) \subseteq X \setminus C]$, for any initial state $x^0 \in X^0$ and any trace $w \in L(M)$.

Any FSM M having an initial state that is critical and another initial state that is not critical, is never critically observable. Moreover, if $X^0 = C$ then FSM M is critically observable and no further analysis for the detection of critical states is needed. For these reasons in the sequel we assume that $[\,X^0 \subset C\,] \vee [\,X^0 \subseteq X \setminus C\,]$ for any FSM M. An illustrative example follows.

Example 2.5. Consider FSMs $M_i = (X_i, X_i^0, \Sigma_i, \delta_i, C_i)$, $i = 1, 2$, depicted in Fig. 1, where $X_1 = \{1, 2, 3, 4\}$, $X_1^0 = \{1\}$, $\Sigma_1 = \{a, b, c, d\}$, $C_1 = \{4\}$, $X_2 = \{5, 6, 7, 8\}$, $X_2^0 = \{5\}$, $\Sigma_2 = \{a, b, e\}$, $C_2 = \{7, 8\}$ and transition maps δ_1 and δ_2 are represented by labeled arrows in Fig. 1; labels on the arrows represent the input label associated with the corresponding transition. FSM M_1 is not critically observable because it is possible to reach both noncritical state 3 and critical state 4 starting from the initial state 1, by