SCIENCE CHINA
Information Sciences

• LETTER •

March 2023, Vol. 66 139202:1–139202:2
https://doi.org/10.1007/s11432-020-3168-1

Strong fault prognosability of partially-observed discrete event systems

Yingrui ZHOU[1], Zengqiang CHEN[1*], Zhongxin LIU[1] & Zhipeng ZHANG[2]

[1]*College of Artificial Intelligence, Nankai University, Tianjin* 300350, *China;*
[2]*School of Computer Science and Engineering, Tianjin University of Technology, Tianjin* 300384, *China*

Received 16 August 2020/Revised 11 December 2020/Accepted 6 January 2021/Published online 27 October 2022

Citation Zhou Y R, Chen Z Q, Liu Z X, et al. Strong fault prognosability of partially-observed discrete event systems. Sci China Inf Sci, 2023, 66(3): 139202, https://doi.org/10.1007/s11432-020-3168-1

Dear editor,

As an important model to analyze cyber-physical systems, the study of discrete event systems has always been prevailing [1–4]. Especially, the problem of fault prognosis becomes a crucial subject for its applications in security and maintenance [5]. In decentralized fault prognosis, the given system can be monitored by several agents and each agent sends its local observation to the global prognoser, which determines whether a fault alarm will be raised. The notion of prognosability was proposed in [6] to assess the correctness of a global decentralized prognoser, which should have "no missed alarm" and "no false alarm". Afterward, there have been a lot of results on decentralized fault prognosis under specific architectures [7–9]. However, it is necessary to provide a broader prognosability for general systems.

In this study, we investigate the decentralized fault prognosis with a state-estimate-based protocol. Compared with [8, 9], this study has the following main contributions: (1) constructing a novel decentralized prognoser based on state estimates, which has no requirement on diagnostic structures; (2) presenting the definition of strong prognosability, which breaks the incompatibility of several kinds of prognosability in [8, 9].

Notations. Consider a finite-state automaton $A = (X, \Sigma, f, x_0)$, where X is the set of states, Σ is the set of events, and $x_0 \in X$ is the initial state. $f : X \times \Sigma \to X$ is the deterministic state transition function, where $f(x, \sigma) = x'$ means that state x' can be reached from x by event σ. Σ^* is the set of all strings over Σ and f can be extended to $X \times \Sigma^* \to X$ with $f(x, s\sigma) = f(f(x, s), \sigma)$, $s \in \Sigma^*$, $\sigma \in \Sigma$. The language generated by A from state x is denoted as $\mathcal{L}(A, x) = \{s \in \Sigma^* : f(x, s)!\}$, where ! represents "is defined". It is usual to write $\mathcal{L}(A, x)$ as $\mathcal{L}(A)$ when $x = x_0$. The prefix-closure of language L is $\overline{L} = \{s \in \Sigma^* : \exists\, t \in \Sigma^*, st \in L\}$ and the post-language of s is $L/s = \{t \in \Sigma^* : st \in L\}$. $B = (X_B, \Sigma, f_B, x_0)$ is a specification automaton of A if $\mathcal{L}(B) \subseteq \mathcal{L}(A)$ and $\forall s \in \mathcal{L}(A) \backslash \mathcal{L}(B), f(x_0, s) \notin X_B$. In this case, $s \in \mathcal{L}(A)$ is a non-fault string if $f(x_0, s) \in X_B$. For any state $x \in X_B$, $l_{\min}(x)$ denotes the minimum length of a non-fault string from x, i.e., $l_{\min}(x) = \min_{s \in \mathcal{L}(A,x) \backslash \mathcal{L}(B,x)} |s| - 1$, and $l_{\max}(x)$ denotes the maximum length of a non-fault string from x, i.e., $l_{\max}(x) = \max_{s \in \mathcal{L}(B,x)} |s|$. M, K are two nonnegative integers. Define $\varrho_K = \{x \in X_B | l_{\min}(x) = K\}$ as the set of states from which a fault may occur after K steps at the earliest and $\psi_M = \{x \in X_B | l_{\max}(x) \leqslant M\}$ as the set of states from which a fault will happen definitely within M steps. Moreover, $\theta_i(P_i(s)) = \{x \in X_B | \exists\, u \in \mathcal{L}(B)$, s.t. $P_i(s) = P_i(u) \wedge f_B(u) = x\}$ is the state estimate of string $s \in \mathcal{L}(B)$ by agent $i \in \mathcal{I}$.

Problem formulation. In decentralized fault prognosis, assume that there are n local agents and $\mathcal{I} = \{1, 2, \ldots, n\}$ is the index set. For each agent i, its observable events are denoted by $\Sigma_{o,i}$. The natural projection $P_i : \Sigma^* \to \Sigma_{o,i}^*$ is

$$P_i(\epsilon) = \epsilon \quad \text{and} \quad P_i(s\sigma) = \begin{cases} P_i(s)\sigma, & \text{if} \quad \sigma \in \Sigma_{o,i}, \\ P_i(s), & \text{if} \quad \sigma \notin \Sigma_{o,i}. \end{cases} \tag{1}$$

In fact, each agent is a local prognoser, which sends the information obtained by observation to a coordinator. Each prognoser $i \in \mathcal{I}$ is a function $\mathcal{C}_i : P_i(\mathcal{L}(B)) \to 2^X$. The coordinator is also a function $\{\mathcal{C}_i\}_{i \in \mathcal{I}} : \mathcal{L}(B) \to \{0, 1\}$, where "0" means there is no fault alarm and "1" means a fault will occur. The coordinator is called the decentralized prognoser. It is significant to guarantee that the decentralized prognoser has "no missed alarm" and "no false alarm". In [8], authors obtained two criteria with guatanteed performance bound (M, K) to assess a decentralized prognoser. (1) Any fault can be alarmed K steps before its occurrence, i.e., $\forall\, s \in \mathcal{L}(A) \backslash \mathcal{L}(B), \exists\, uv \in \overline{\{s\}}, |v| \geqslant K$, s.t. $\{\mathcal{C}_i\}_{i \in \mathcal{I}}(u) = 1$. (2) Once a fault alarm is raised, the fault is guaranteed to occur within M steps, i.e., $\forall\, s \in \mathcal{L}(B)$, $\{\mathcal{C}_i\}_{i \in \mathcal{I}}(s) = 1$, $\Rightarrow \forall\, u \in \mathcal{L}(A)/s$, $|u| \geqslant M$, s.t. $su \in \mathcal{L}(A) \setminus \mathcal{L}(B)$. Hereafter, we will also refer to (M, K) as the performance bound of a prognosis system.

Decentralized prognosis analysis. Based on the above preparations, we construct the decentralized prognoser $\{\mathcal{C}_i\}_{i \in \mathcal{I}}$ as follows: each local prognoser $\mathcal{C}_i$ is defined as

$$\forall\, s \in \mathcal{L}(B),\ \mathcal{C}_i(P_i(s)) = \theta_i(P_i(s)) \cap \psi_M. \tag{2}$$

* Corresponding author (email: chenzq@nankai.edu.cn)

And then, the global decentralized prognoser is

$$\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=\begin{cases}1, \text{ if } \cap_{i\in\mathcal{I}}\mathcal{C}_i(P_i(s))\neq\emptyset,\\ 0, \text{ if } \cap_{i\in\mathcal{I}}\mathcal{C}_i(P_i(s))=\emptyset.\end{cases}\tag{3}$$

Notice that for any local prognoser $\mathcal{C}_i(P_i(s)) = \theta_i(P_i(s))\cap\psi_M$, it sends the information "there exists a fault happening definitely within M steps" to the coordinator. Then, the coordinator combines $\mathcal{C}_i(P_i(s))$, $i\in\mathcal{I}$ to determine the raising of a fault alarm. If $\cap_{i\in\mathcal{I}}\mathcal{C}_i(P_i(s))\neq\emptyset$, it means that all local prognosers have common reasons and a fault alarm will be raised, i.e., $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=1$. Otherwise, there is no fault alarm, i.e., $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=0$. Its construction is different from other results. For example, in [8], the local prognoser in a disjunctive architecture collects whether $\theta_i(P_i(s))\subseteq\psi_M$, while the one in a conjunctive architecture focuses on $\theta_i(P_i(s))\cap\varrho_K\neq\emptyset$. Nonetheless, all decentralized prognosers should have "no missed alarm" and "no false alarm". Next, we present a definition of strong prognosability and a theorem to analyze whether the global decentralized prognoser $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ defined by (2) and (3) satisfies (M,K)-criteria.

Definition 1. The specification automaton B is strongly prognosable with respect to A, $\Sigma_{o,i}, i\in\mathcal{I}$ and (M,K) if $\forall\, s\in\mathcal{L}(B),\ f(x_0,s)\in\varrho_K,$ s.t. $[\cap_{i\in\mathcal{I}}\theta_i(P_i(s))]\cap\psi_M\neq\emptyset$.

Remark 1. We can discover differences between the strong prognosability and others in terms of definitions. Take (M,K)-disjunctive prognosability and (M,K)-conjunctive prognosability in [8] for example. B is (M,K)-disjunctively prognosable if $\forall s\in\mathcal{L}(B),\ f(x_0,s)\in\varrho_K$, s.t. $\exists\, i\in\mathcal{I},\ \theta_i(P_i(s))\subseteq\psi_M$, which raises a fault alarm as early as possible. And B is (M,K)-conjunctively prognosable if $\forall s\in\mathcal{L}(B),\ f(x_0,s)\notin\psi_M$, s.t. $\exists\, i\in\mathcal{I},\ \theta_i(P_i(s))\cap\varrho_K=\emptyset$, which raises a fault alarm as late as possible. Besides, the strong prognosability extends the condition and actualizes that the fault alarm is raised within a performance bound.

Smoothly, we have Theorem 1.

Theorem 1. A decentralized prognoser $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ is defined by (2) and (3). $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ satisfies (M,K)-criteria if and only if the specification automaton B is strongly prognosable with respect to A, $\Sigma_{o,i}, i\in\mathcal{I}$ and (M,K).

Proof. (Necessity) By contradiction. Assume that B is not strongly prognosable. Then, we have that $\exists\ s\in\mathcal{L}(B)$, $f(x_0,s)\in\varrho_K$, s.t. $[\cap_{i\in\mathcal{I}}\theta_i(P_i(s))]\cap\psi_M=\emptyset$. It means that for the $s\in\mathcal{L}(B)$, $f(s)\in\varrho_K$, $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=0$, i.e., there is no fault alarm. However, for $f(s)\in\varrho_K$, we know that $\exists\ u\in\mathcal{L}(A)/s$, $su\in\mathcal{L}(A)\setminus\mathcal{L}(B)$, $|u|=K$, where a fault alarm should be raised. It is inconsistent with criterion (1).

(Sufficiency) B is strongly prognosable. First, we prove that $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ satisfies criterion (1). There is no denying that $l_{\min}(x_0)\geqslant K$. For any string $s\in\mathcal{L}(A)\setminus\mathcal{L}(B)$, $\exists\ u\in\overline{\{s\}}\cap\mathcal{L}(B)$, s.t. $f(x_0,u)\in\varrho_K$. Then, we have that $[\cap_{i\in\mathcal{I}}\theta_i(P_i(u))]\cap\psi_M\neq\emptyset$, i.e., $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(u)=1$. It means that $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ satisfies criterion (1). Second, we prove that $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ satisfies criterion (2) by contradiction. Suppose that criterion (2) is not satisfied. We have that $\exists\ s\in\mathcal{L}(B)$, $u\in\mathcal{L}(B)/s$, s.t. $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=1$ and $|u|\geqslant M$. For $\{\mathcal{C}_i\}_{i\in\mathcal{I}}(s)=1$, we can get that $f(x_0,s)\in[\cap_{i\in\mathcal{I}}\theta_i(P_i(s))]\cap\psi_M\neq\emptyset$. On the other hand, for $u\in\mathcal{L}(B)/s$ and $|u|\geqslant M$, we get that $f(x_0,s)\notin\psi_M$. The results are contradictory. Therefore, $\{\mathcal{C}_i\}_{i\in\mathcal{I}}$ must satisfies criterion (2).

Example. Consider two systems in Figure 1. Assume that $\mathcal{I}=\{1,2\}$, $\Sigma_{o,1}=\{a,o\}$, $\Sigma_{o,1}=\{b,o\}$, $M=5$, $K=0$. For A_1, we have $\varrho_K=\{4\}$, $\psi_M=\{4\}$, and the unique string o reaching state 4 satisfies $[\cap_{i\in\mathcal{I}}\theta_i(P_i(o))]\cap\psi_M=\{4\}\neq\emptyset$. For A_2, we have $\varrho_K=\{3\}$, $\psi_M=\{2,3\}$, and there are two strings ao, bo reaching state 3. It proves that $[\cap_{i\in\mathcal{I}}\theta_i(P_i(s))]\cap\psi_M=\{3\}\neq\emptyset$, where $s=ao$ or $s=bo$. Therefore, the two systems in Figure 1 are strongly prognosable.

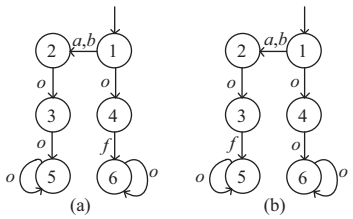

Figure 1 Two systems (a) A_1 and (b) A_2.

Remark 2. In fact, the two systems in Figure 1 illustrate the difference between strong prognosability and others in [8, 9]. For string o in A_1, $f(x_0,o)=4\in\varrho_K$, but $\theta_i(P_i(o))=\{3,4\}\not\subseteq\psi_M$, $i\in\mathcal{I}$. Therefore, A_1 is not (M,K)-disjunctively prognosable. For string o in A_2, $f(x_0,o)=4\notin\psi_M$, but $\theta_i(P_i(o))=\{3,4\}\cap\varrho_K\neq\emptyset$. Therefore, A_2 is not (M,K)-conjunctively prognosable. That is, (M,K)-disjunctive prognosability and (M,K)-conjunctive prognosability are incomparable. The case is similar to the results in [9].

Conclusion. We analyzed the problem of decentralized fault prognosis of partially-observed discrete event systems. We followed (M,K) as the prognostic performance for a given system and proposed a notion of strong prognosability, which could be applied to more general systems than several existing results. In the future study, we hope to extend the approach to multiple types of faults and find out an efficient algorithm to verification.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61973175) and Tianjin Natural Science Foundation (Grant Nos. 20JCYBJC01060, 20JCQNJC01450).

References

1 Cassandras C G, Lafortune S. Introduction to Discrete Event Systems. 2nd ed. Berlin: Springer, 2008
2 Chen Z Q, Zhou Y R, Zhang Z P, et al. Semi-tensor product of matrices approach to the problem of fault detection for discrete event systems (DESs). IEEE Trans Circ Syst II, 2020, 67: 3098–3102
3 Zhang Z P, Xia C Y, Chen S Y, et al. Reachability analysis of networked finite state machine with communication losses: a switched perspective. IEEE J Sel Areas Commun, 2020, 38: 845–853
4 Han X G, Wang P F, Chen Z Q. Matrix approach to verification and enforcement of nonblockingness for modular discrete-event systems. Sci China Inf Sci, 2020, 63: 219204
5 Ammour R, Leclercq E, Sanlaville E, et al. Fault prognosis of timed stochastic discrete event systems with bounded estimation error. Automatica, 2017, 82: 35–41
6 Kumar R, Takai S. Decentralized prognosis of failures in discrete event systems. IEEE Trans Autom Control, 2010, 55: 48–59
7 Khoumsi A, Chakib H. Conjunctive and disjunctive architectures for decentralized prognosis of failures in discrete-event systems. IEEE Trans Autom Sci Eng, 2012, 9: 412–417
8 Yin X, Li Z J. Decentralized fault prognosis of discrete event systems with guaranteed performance bound. Automatica, 2016, 69: 375–379
9 Yin X, Li Z J. Decentralized fault prognosis of discrete-event systems using state-estimate-based protocols. IEEE Trans Cybern, 2019, 49: 1302–1313