Computer Science Journal of Moldova, vol.28, no.3(84), 2020

Analysis of Faults in Cyber-Physical Systems by Finite Discrete-Time Markov Chains

Volodymyr G. Skobelev, Volodymyr V. Skobelev

Abstract

In the given paper the problem of Cyber-Physical Systems behavior analysis in the occurrence of faults is investigated. To present the fault-free behavior of the investigated Cyber-Physical System as well as its behaviors in the presence of admissible faults, some Finite Discrete-Time Markov Chain is proposed and analyzed. It is shown that a single stationary probability distribution exists for the proposed model. This distribution is applied for characterization the behaviors of the investigated Cyber-Physical System in terms of the distance from the current fault to the set of critical faults. Besides, the algorithm for bounded probabilistic reachability analysis of the target set of faults is proposed.

Keywords: Cyber-Physical Systems, faults, Discrete-Time Markov Chains, bounded probabilistic reachability, probabilistic counterexamples.

1 Introduction

In the design and analysis of Cyber-Physical Systems (CPS), hybrid automata [1, 2, 3] are usually used as mathematical models for which automated verification procedures are performed by using these or the other Model Checkers.

The need to analyze some significant attributes, such as reliability, safety, and behaviors associated with the decrease in the performance has lead to the necessity to use stochastic models.

A stochastic hybrid automaton [4, 5] generalizes a deterministic hybrid automaton by assigning probabilities to the arcs of the graph as well as by allowing the values of continuous variables to be reset according to given continuous probability distributions. These generalizations result in the high complexity of both the model itself and its analysis methods. Besides, only a small amount of information presented in a stochastic hybrid automaton can be required for solving a sufficiently wide variety of specific problems of CPS analysis.

An important non-trivial sub-class of stochastic hybrid automata consists of probabilistic automata [6, 7], i.e. the generalization of deterministic hybrid automata only by assigning probabilities to the arcs of the graph. This model is much more simple than a stochastic hybrid automaton. Nevertheless, it has been shown in [8] that probabilistic automata can be successfully used for modeling the behavior of the analyzed CPS in the presence of faults.

When the decrease in the performance of the given CPS is analyzed, it is important to estimate the probability of the occurrences for the behaviors in the presence of these or the other faults.

In the given paper, for solving this problem the Finite Discrete-Time Markov Chain (FDTMC) associated with the analyzed CPS is proposed and investigated. The essential advantage of this model is that it is much simpler than a probabilistic automaton. Besides, it gives the possibility to generate probabilistic counterexamples [9], i.e. the sets of finite paths with a critical probability mass.

2 Proposed model

A fault in the analyzed CPS $\mathfrak{S}$ is called admissible if at its occurrence the CPS $\mathfrak{S}$ can continue to operate, possibly with some loss of its functionality.

Let $F_{\mathfrak{S}}^{(0)}$ ($|F_{\mathfrak{S}}^{(0)}| \geq 2$) be some finite set of all admissible single faults that can occur in the analyzed CPS $\mathfrak{S}$. As it is usually accepted, the set of all admissible faults that can occur in the analyzed CPS $\mathfrak{S}$ can be defined as some subset $F_{\mathfrak{S}}$ ($F_{\mathfrak{S}}^{(0)} \subset F_{\mathfrak{S}} \subseteq \mathcal{B}(F_{\mathfrak{S}}^{(0)}) \backslash \{\emptyset\}$). Everywhere further it is assumed that the set $F_{\mathfrak{S}}$ satisfies to the following condition:

$$(\forall f \in F_{\mathfrak{S}})(\forall f' \in \mathcal{B}(F_{\mathfrak{S}}^{(0)}) \setminus \{\emptyset\})(f' \subset f \Rightarrow f' \in F). \qquad (1)$$

Let $S_{\mathfrak{S}} = \{\emptyset\} \cup F_{\mathfrak{S}}$. Everywhere further it is supposed that the elements of the set $S_{\mathfrak{S}}$ are enumerated according to their cardinality non-decreasing, i.e.,

$$S_{\mathfrak{S}} = \{s_1, \ldots, s_k\},$$

where

$$|s_1| \leq |s_2| \leq \cdots \leq |s_k|.$$

The elements of the set $S_{\mathfrak{S}}$ can be interpreted as follows: the element $s_1 = \emptyset$ is associated with the fault-free CPS $\mathfrak{S}$, while any element s_i $(i = 2, \ldots, k)$ is associated with the CPS $\mathfrak{S}$ in the presence of the $|s_i|$-multiple fault s_i.

We define the set $S_{\mathfrak{S}}^{crtcl}$ of critical faults in the CPS $\mathfrak{S}$ as the set of all maximal due to the inclusion relation elements of the set $S_{\mathfrak{S}}$, i.e.

$$S_{\mathfrak{S}}^{crtcl} = \{s \in S_{\mathfrak{S}} | (\forall s' \in S_{\mathfrak{S}})(s \not\subset s')\}. \qquad (2)$$

We can associate with the analyzed CPS $\mathfrak{S}$ some FDTMC $\mathfrak{M}_{\mathfrak{S}}$ defined by the stochastic $(k \times k)$-matrix

$$P_{\mathfrak{S}} = \begin{array}{c|cccc|}
 & s_1 & s_2 & \cdots & s_k \\
\hline
s_1 & p_{11} & p_{12} & \cdots & p_{1k} \\
s_2 & p_{21} & p_{22} & \cdots & p_{2k} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
s_k & p_{k1} & p_{k2} & \cdots & p_{kk} \\
\hline
\end{array}$$

such that the following two formulae are true:

$$(\forall i = 1, \ldots, k)(0 < p_{ii} < 1), \qquad (3)$$

$$(\forall i = 1, \ldots, k)(\forall j \in \{1, \ldots, k\} \backslash \{i\})(p_{ij} > 0 \Leftrightarrow$$
$$\Leftrightarrow s_i \subset s_j \& |s_j| = |s_i| + 1 \vee s_j \subset s_i \& |s_i| = |s_j| + 1). \qquad (4)$$

Due to (1)-(4):

1. The analyzed CPS $\mathfrak{S}$ can operate with positive probability either it is fault-free or if any admissible fault s_i $(i = 2, \ldots, k)$ occurs.

2. If $\mathfrak{S}$ is fault-free, then with positive probability only any single fault can occur.

3. If $\mathfrak{S}$ operates in the presence of any critical fault $s \in S_{\mathfrak{S}}^{crtcl}$, then no additional faults can occur, and with positive probability only any single fault $f \in s$ can be repaired.

4. If $\mathfrak{S}$ operates in the presence of any fault $s \in S_{\mathfrak{S}} \backslash (\{\emptyset\} \cup S_{\mathfrak{S}}^{crtcl})$, then with positive probability only either any single fault $f \in s$ can be repaired or any single fault $f \in F_{\mathfrak{S}}^{(0)} \backslash s$ can occur.

Example 1. Let the analyzed CPS $\mathfrak{S}_1$ be the water tanks system considered in [2]. It consists of two tanks, namely the left tank and the right tank. Both tanks are leaking at a constant rate. Water is added to the system at a constant rate through a hose. At any point in time the hose is dedicated either to the left tank or to the right tank. The hose can switch between the tanks instantaneously.

Let $F_{\mathfrak{S}_1}^{(0)} = \{f_1, f_2\}$, where f_1 means that the water-level sensor in the left tank is faulty, and f_2 means that the water-level sensor in the right tank is faulty.

We set $F_{\mathfrak{S}_1} = \{\{f_1\}, \{f_2\}, \{f_1, f_2\}\}$. Therefore,

$$S_{\mathfrak{S}_1} = \{s_1, s_2, s_3, s_4\},$$

where $s_1 = \emptyset$, $s_2 = \{f_1\}$, $s_3 = \{f_2\}$, $s_4 = \{f_1, f_2\}$.

With the CPS $\mathfrak{S}_1$ we can associate some FDTMC $\mathfrak{M}_{\mathfrak{S}_1}$, defined by the following stochastic (4×4)-matrix

$$P_{\mathfrak{S}_1} = \begin{array}{c|cccc|} & s_1 & s_2 & s_3 & s_4 \\ \hline s_1 & p_1 & a_1p_1 & a_1p_1 & 0 \\ s_2 & a_2p_2 & p_2 & 0 & a_3p_2 \\ s_3 & a_2p_2 & 0 & p_2 & a_3p_2 \\ s_4 & 0 & a_4p_3 & a_4p_3 & p_3 \\ \hline \end{array} ,$$

where $0 < p_i < 1$ $(i = 1, 2, 3)$. The digraph of the FDTMC $\mathfrak{M}_{\mathfrak{S}_1}$ is shown in Figure 1.

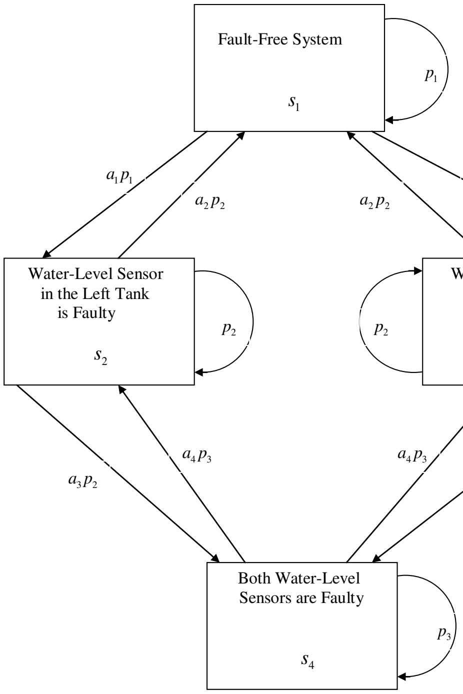
Fault-Free System
s_1
p_1
a_1p_1
a_2p_2
a_2p_2
a_1p_1
Water-Level Sensor in the Left Tank is Faulty
s_2
p_2
p_2
Water-Level Sensor in the Right Tank is Faulty
s_3
a_3p_2
a_4p_3
a_4p_3
a_3p_2
Both Water-Level Sensors are Faulty
s_4
p_3

Figure 1. The digraph of the FDTMC $\mathfrak{M}_{\mathfrak{S}_1}$

Since $P_{\mathfrak{S}_1}$ is a stochastic matrix, we get

$$p_1 + a_1p_1 + a_1p_1 = 1 \Rightarrow a_1 = 0.5(p_1^{-1} - 1),$$

$$a_2p_2 + p_2 + a_3p_2 = 1 \Rightarrow a_2 + a_3 = p_2^{-1} - 1,$$

$$a_4p_3 + a_4p_3 + p_3 = 1 \Rightarrow a_4 = 0.5(p_3^{-1} - 1).$$

□

We denote $G_{\mathfrak{M}_{\mathfrak{S}}}$ the digraph associated with the FDTMC $\mathfrak{M}_{\mathfrak{S}}$.

Theorem 1. *The FDTMC $\mathfrak{M}_{\mathfrak{S}}$ is aperiodic and irreducible.*

Proof. Due to (3), $p_{ii} > 0$ for all $i = 1, \ldots, k$. Therefore, each state s_i $(i = 1, \ldots, k)$ of the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ is aperiodic, i.e. $\mathfrak{M}_{\mathfrak{S}}$ is an aperiodic FDTMC.

Due to (4), in the digraph $G_{\mathfrak{M}_{\mathfrak{S}}}$ of the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ for the state $s_1 = \emptyset$ and any state $s = \{f_1, \ldots, f_r\} \in S_{\mathfrak{S}} \backslash \{s_1\}$ there are pathes

$$s_1 = \emptyset \to \{f_1\} \to \{f_1, f_2\} \to \cdots \to s = \{f_1, \ldots, f_r\}$$

and

$$s = \{f_1, \ldots, f_r\} \to \{f_1, \ldots, f_{r-1}\} \to \cdots \to \{f_1\} \to s_1 = \emptyset,$$

where each transition occurs with positive probability, i.e. the state $s_1 = \emptyset$ communicates with any state $s = \{f_1, \ldots, f_r\} \in S_{\mathfrak{S}} \backslash \{s_1\}$.

This factor implies that the digraph $G_{\mathfrak{M}_{\mathfrak{S}}}$ is strongly connected, i.e. in the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ the set of states $S_{\mathfrak{S}}$ forms the single communicating class.

Therefore, $\mathfrak{M}_{\mathfrak{S}}$ is an irreducible FDTMC.

□

Theorem 1 implies that for the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ there exists exactly one stationary distribution

$$\overrightarrow{\psi} = (\psi_{s_1}, \ldots, \psi_{s_k}),$$

where the component ψ_{s_i} $(i = 1, \ldots, k)$ is the long-term proportion of transitions that the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ makes into the state s_i, i.e. the stationary probability for the FDTMC $\mathfrak{M}_{\mathfrak{S}}$ to transit to the state s_i.

The vector $\overrightarrow{\psi}$ can be computed as the solution of the system of equations

$$\begin{cases} \overrightarrow{\psi} P_{\mathfrak{S}} = \overrightarrow{\psi} \\ \sum\limits_{i=1}^{k} \psi_{s_i} = 1 \end{cases} . \tag{5}$$

It is worth to note that each component ψ_{s_i} $(i = 1, \ldots, k)$ of the vector $\overrightarrow{\psi}$ is a strictly positive number.

Example 2. Solving the system of equations (5) for the CPS $\mathfrak{S}_1$ (see Example 1), we compute the stationary distribution

$$\overrightarrow{\psi} = (\psi_{s_1}, \psi_{s_2}, \psi_{s_3}, \psi_{s_4}),$$

where:

$$\psi_{s_1} = \frac{a_2 p_2}{1-p_1}\left(\frac{a_2 p_2}{1-p_1} + \frac{a_3 p_2}{1-p_3} + 1\right)^{-1},$$

$$\psi_{s_2} = \psi_{s_3} = 0.5\left(\frac{a_2 p_2}{1-p_1} + \frac{a_3 p_2}{1-p_3} + 1\right)^{-1},$$

$$\psi_{s_4} = \frac{a_3 p_2}{1-p_3}\left(\frac{a_2 p_2}{1-p_1} + \frac{a_3 p_2}{1-p_3} + 1\right)^{-1}.$$

□

Dealing with the digraph $G_{\mathfrak{M}_{\mathfrak{S}}}$ of the FDTMC $\mathfrak{M}_{\mathfrak{S}}$, we can define the pair-wise disjoint subsets $S_{\mathfrak{S}}^{(i)}$ $(i = 0, 1, \dots)$ of the set $S_{\mathfrak{S}}$, such that

$$S_{\mathfrak{S}}^{(i)} = \{s \in S_{\mathfrak{S}} \mid \text{Distance}(s, S_{\mathfrak{S}}^{crtcl}) = i\} \ \ (i = 0, 1, \dots).$$

Therefore, $S_{\mathfrak{S}}^{(0)} = S_{\mathfrak{S}}^{crtcl}$ and the set $S_{\mathfrak{S}}^{(i)}$ $(i = 1, 2, \dots)$ consists of all states such that i is the least number for sequential occurring of additional single faults that lead the CPS $\mathfrak{S}$ to operate in the presence of critical faults.

The stationary probability $\mathbb{P}_{st}(S_{\mathfrak{S}}^{(i)})$ $(i = 0, 1, \dots)$ that the CPS $\mathfrak{S}$ operates in some state that is an element of the set $S_{\mathfrak{S}}^{(i)}$ can be computed as follows:

$$\mathbb{P}_{st}(S_{\mathfrak{S}}^{(i)}) = \sum_{s \in S_{\mathfrak{S}}^{(i)}} \psi_s \ \ (i = 0, 1, \dots).$$

In particular, the stationary probability that the CPS $\mathfrak{S}$ operates in the presence of some critical fault can be computed as follows:

$$\mathbb{P}_{st}(S_{\mathfrak{S}}^{crtcl}) = \mathbb{P}_{st}(S_{\mathfrak{S}}^{(0)}) = \sum_{s \in S_{\mathfrak{S}}^{crtcl}} \psi_s.$$

The probability distribution

$$\mathbb{P}_{st}(S_{\mathfrak{S}}^{(0)}), \mathbb{P}_{st}(S_{\mathfrak{S}}^{(1)}), \ldots. \tag{6}$$

characterizes situations in which the analyzed CPS $\mathfrak{S}$ operates in the presence of some fault that is an element of the set of faults determined by its "distance" to the set of critical faults.

It should be noted that an essential characteristic of the CPS $\mathfrak{S}$ behavior is the study of the changes of the probability distribution (6) under variations of the probabilities p_{ij} $(i, j = 1, \ldots, k)$.

Example 3. For the CPS $\mathfrak{S}_1$ (see Examples 1 and 2) we get

$$S_{\mathfrak{S}_1}^{(0)} = S_{\mathfrak{S}_1}^{crtcl} = \{s_4\},$$

$$S_{\mathfrak{S}_1}^{(1)} = \{s_2, s_3\},$$

and

$$S_{\mathfrak{S}_1}^{(2)} = \{s_0\}.$$

Therefore,

$$\mathbb{P}_{st}(S_{\mathfrak{S}_1}^{(0)}) = \psi_{s_4} = \frac{a_3 p_2}{1 - p_3}\left(\frac{a_2 p_2}{1 - p_1} + \frac{a_3 p_2}{1 - p_3} + 1\right)^{-1},$$

$$\mathbb{P}_{st}(S_{\mathfrak{S}_1}^{(1)}) = \psi_{s_2} + \psi_{s_3} = \left(\frac{a_2 p_2}{1 - p_1} + \frac{a_3 p_2}{1 - p_3} + 1\right)^{-1},$$

$$\mathbb{P}_{st}(S_{\mathfrak{S}_1}^{(2)}) = \psi_{s_1} = \frac{a_2 p_2}{1 - p_1}\left(\frac{a_2 p_2}{1 - p_1} + \frac{a_3 p_2}{1 - p_3} + 1\right)^{-1}.$$

□

3 Bounded probabilistic analysis of the CPS $\mathfrak{S}$

For the analyzed CPS $\mathfrak{S}$ estimation the occurrences of behaviours associated with the decreasing in the performance in the presence of faults can be reduced to computation the probability $\mathbb{P}_{st}(s_1, S_{\mathfrak{S}}^{trgt})$ to reach this or the other target set $S_{\mathfrak{S}}^{trgt}$ ($\emptyset \neq S_{\mathfrak{S}}^{trgt} \subset S_{\mathfrak{S}}$) of states starting in the state s_1, as follows.

Let $\Pi_{s_1, S_{\mathfrak{S}}^{trgt}}$ be the set of all strings $\pi = s_{i_0} s_{i_1} \ldots s_{i_r} \in S_{\mathfrak{S}}^{+}$ such that

$$s_{i_0} = s_1,$$

$$s_{i_j} \notin S_{\mathfrak{S}}^{trgt} \;\; (j = 0, 1, \ldots, r-1),$$

$$s_{i_r} \in S_{\mathfrak{S}}^{trgt},$$

and

$$p_{i_j i_{j+1}} > 0 \;\; (j = 0, 1, \ldots, r-1).$$

Due to [10, 11], with a string $\pi = s_{i_0} s_{i_1} \ldots s_{i_r}$ it is associated the probability

$$\mathbb{P}(\pi) = \mathbb{P}(\mathrm{Cyl}(\pi)) = \prod_{j=0}^{r-1} p_{i_j i_{j+1}}.$$

Therefore,

$$\mathbb{P}(s_1, S_{\mathfrak{S}}^{trgt}) = \sum_{\pi \in \Pi_{s_1, S_{\mathfrak{S}}^{trgt}}} \mathbb{P}(\pi).$$

For real CPS, it is computationally infeasible to deal with the infinite set $\Pi_{s_1, S_{\mathfrak{S}}^{trgt}}$. Instead, bounded reachability properties [9, 12] can be analysed as follows.

For the given positive number λ ($\lambda < 1,$) and positive integer h we denote $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ the property that for the analysed CPS $\mathfrak{S}$ the probability to reach a state in $S_{\mathfrak{S}}^{trgt}$ starting in the state s_1 by at most h steps is not greater then λ.

Let

$$\Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}} = \Pi_{s_1, S_{\mathfrak{S}}^{trgt}} \cap S_{\mathfrak{S}}^{l} \;\; (l = 2, \ldots, h+1).$$

It is evident that the sets $\Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}}$ ($l = 2, \ldots, h{+}1$) can be computed sufficiently easily than the set $\Pi_{s_1, S_{\mathfrak{S}}^{trgt}}$.

Example 4. Let us consider the CPS $\mathfrak{S}_1$ (see Example 1). Setting

$$S_{\mathfrak{S}_1}^{trgt} = S_{\mathfrak{S}_1}^{crtcl} = \{s_4\},$$

we get

$$\Pi^{(2)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}} = \emptyset,$$

$$\Pi^{(3)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}} = \{s_1 s_2 s_4, s_1 s_3 s_4\},$$

$$\Pi^{(4)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}} = \{s_1^2 s_2 s_4, s_1^2 s_3 s_4, s_1 s_2^2 s_4, s_1 s_3^2 s_4\},$$

$$\Pi^{(5)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}} = \{s_1^3 s_2 s_4, s_1 s_2 s_1 s_2 s_4, s_1^2 s_2^2 s_4, s_1^3 s_3 s_4,$$

$$s_1 s_3 s_1 s_3 s_4, s_1^2 s_3^2 s_4, s_1 s_2 s_1 s_3 s_4, s_1 s_3 s_1 s_2 s_4\}$$

and so on.

□

It is evident, that the analyzed CPS $\mathfrak{S}$ satisfies to the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ if and only if the following inequality holds:

$$\sum_{l=2}^{h+1} \sum_{\pi \in \Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}}} \mathbb{P}(\pi) \leq \lambda.$$

Therefore, the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ fails for the analyzed CPS $\mathfrak{S}$ if and only if for some subset

$$\mathcal{C} \subseteq \bigcup_{l=2}^{h+1} \Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}}$$

the following inequality holds:

$$\mathbb{P}(\mathcal{C}) = \sum_{\pi \in \mathcal{C}} \mathbb{P}(\pi) > \lambda.$$

This subset $\mathcal{C}$ is called a counterexample.

An attempt to design a counterexample can be used to reduce computations in the process of checking the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ for the analyzed CPS $\mathfrak{S}$.

Indeed, let us suppose that the elements of any non-empty set of strings $\Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}}$ $(l = 2, \ldots, h+1)$ are enumerated according to their probabilities non-increasing. Then the following algorithm can be applied for checking the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ for the analyzed CPS $\mathfrak{S}$.

Algorithm 1. (Checking the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$).

Step 1. $l := 2$, $\mathcal{C} := \emptyset$, $\mathbb{P}(\mathcal{C}) := 0$.

Step 2. If $\Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}} \neq \emptyset$, then go to Step 3, else go to Step 6.

Step 3. Select the first element $\pi \in \Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}}$, $\mathcal{C} := \mathcal{C} \cup \{\pi\}$, $\Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}} := \Pi^{(l)}_{s_1, S_{\mathfrak{S}}^{trgt}} \backslash \{\pi\}$, $\mathbb{P}(\mathcal{C}) := \mathbb{P}(\mathcal{C}) + \mathbb{P}(\pi)$.

Step 4. If $\mathbb{P}(\mathcal{C}) > \lambda$, then go to Step 5, else go to Step 2.

Step 5. Print ”For the system $\mathfrak{S}$ the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ is false”, print the designed counterexample $\mathcal{C}$ in the explicit form, and HALT.

Step 6. $l := l + 1$.

Step 7. If $l \leq h + 1$, then go to Step 2, else go to Step 8.

Step 8. Print ”For the system $\mathfrak{S}$ the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ is true”, and HALT.

Theorem 2. *Algorithm 1 is complete and sound.*

Proof. Due to Steps 1-4, 6, and 7, in the process of sequential generation of the sets of strings

$$\Pi^{(2)}_{s_1, S_{trgt}}, \Pi^{(3)}_{s_1, S_{trgt}}, \ldots$$

the validity of the properties

$$\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, 1), \mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, 2), \ldots$$

are checked sequentially.

Due to Step 5, if for some $l \in \{2, \ldots, h+1\}$ the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, l-1)$ is false, then Algorithm 1 prints "For the system $\mathfrak{S}$ the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ is false", prints the designed counterexample $\mathcal{C}$ in the explicit form, and halts.

Due to Step 8, if all properties $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, l-1)$ $(l = 2, \ldots, h+1)$ are true, then Algorithm 1 prints "For the system $\mathfrak{S}$ the property $\mathcal{P}(s_1, S_{\mathfrak{S}}^{trgt}, \lambda, h)$ is true", and halts.

Therefore Algorithm 1 is complete and sound.

□

Example 5. Let us consider the CPS $\mathfrak{S}_1$ (see Example 1). Setting $p_1 = 0.80$, $p_2 = p_3 = 0.40$, and $a_2 = a_3$, we get $a_1 = 0.125$, and $a_2 = a_3 = a_4 = 0.75$. Therefore, the FDTMC $\mathfrak{M}_{\mathfrak{S}_1}$ is defined by the following stochastic (4×4)-matrix

$$P_{\mathfrak{S}_1} = \begin{array}{c|cccc|} & s_1 & s_2 & s_3 & s_4 \\ \hline s_1 & 0.80 & 0.10 & 0.10 & 0 \\ s_2 & 0.30 & 0.40 & 0 & 0.30 \\ s_3 & 0.30 & 0 & 0.40 & 0.30 \\ s_4 & 0 & 0.30 & 0.30 & 0.40 \\ \hline \end{array} .$$

Let us check the property $\mathcal{P}(s_1, S_{\mathfrak{S}_1}^{crtcl}, 0.1, 3)$, i.e. $\lambda = 0.1$, $h = 3$, and $S_{\mathfrak{S}_1}^{trgt} = S_{\mathfrak{S}_1}^{crtcl} = \{s_4\}$.

The elements of the sets $\Pi^{(3)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}}$ and $\Pi^{(4)}_{s_1, S_{\mathfrak{S}_1}^{crtcl}}$ (see Example 4) are enumerated according to their probabilities non-increasing. Indeed,

$$\mathbb{P}(s_1 s_2 s_4) = \mathbb{P}(s_1 s_3 s_4) = 0.030,$$

$$\mathbb{P}(s_1^2 s_2 s_4) = \mathbb{P}(s_1^2 s_3 s_4) = 0.024,$$

and

$$\mathbb{P}(s_1 s_2^2 s_4) = \mathbb{P}(s_1 s_3^2 s_4) = 0.012.$$

Applying Algorithm 1, we get:

Step 1. $l := 2$, $\mathcal{C} := \emptyset$, $\mathbb{P}(\mathcal{C}) := 0$.

Step 2. $\Pi^{(2)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} = \emptyset$. We go to Step 6.

Step 6. $l := 2 + 1 = 3$.

Step 7. $3 \leq 3 + 1$. We go to Step 2.

Step 2. $\Pi^{(3)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} \neq \emptyset$. We go to Step 3.

Step 3. $\pi := s_1 s_2 s_4$, $\mathcal{C} := \{s_1 s_2 s_4\}$, $\Pi^{(3)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} := \{s_1 s_3 s_4\}$,
$\mathbb{P}(\mathcal{C}) := \mathbb{P}(s_1 s_2 s_4) = 0.030$.

Step 4. $\mathbb{P}(\mathcal{C}) = 0.030 \leq 0.1$. We go to Step 2.

Step 2. $\Pi^{(3)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} \neq \emptyset$. We go to Step 3.

Step 3. $\pi := s_1 s_3 s_4$, $\mathcal{C} := \{s_1 s_2 s_4, s_1 s_3 s_4\}$, $\Pi^{(3)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} := \emptyset$,
$\mathbb{P}(\mathcal{C}) := \mathbb{P}(\mathcal{C}) + \mathbb{P}(s_1 s_3 s_4) = 0.030 + 0.030 = 0.060$.

Step 4. $\mathbb{P}(\mathcal{C}) = 0.60 \leq 0.1$. We go to Step 2.

Step 2. $\Pi^{(3)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} = \emptyset$. We go to Step 6.

Step 6. $l := 3 + 1 = 4$.

Step 7. $4 \leq 3 + 1$. We go to Step 2.

Step 2. $\Pi^{(4)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} \neq \emptyset$. We go to Step 3.

Step 3. $\pi := s_1^2 s_2 s_4$, $\mathcal{C} := \{s_1 s_2 s_4, s_1 s_3 s_4, s_1^2 s_2 s_4\}$,
$\Pi^{(4)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} := \{s_1^2 s_3 s_4, s_1 s_2^2 s_4, s_1 s_3^2 s_4\}$,
$\mathbb{P}(\mathcal{C}) := \mathbb{P}(\mathcal{C}) + \mathbb{P}(s_1^2 s_2 s_4) = 0.060 + 0.024 = 0.084$.

Step 4. $\mathbb{P}(\mathcal{C}) = 0.084 \leq 0.1$. We go to Step 2.

Step 2. $\Pi^{(4)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} \neq \emptyset$. We go to Step 3.

Step 3. $\pi := s_1^2 s_3 s_4$, $\mathcal{C} := \{s_1 s_2 s_4, s_1 s_3 s_4, s_1^2 s_2 s_4, s_1^2 s_3 s_4\}$,
$\Pi^{(4)}_{s_1, S^{trgt}_{\mathfrak{S}_1}} := \{s_1 s_2^2 s_4, s_1 s_3^2 s_4\}$,
$\mathbb{P}(\mathcal{C}) := \mathbb{P}(\mathcal{C}) + \mathbb{P}(s_1^2 s_3 s_4) = 0.084 + 0.024 = 0.108$.

Step 4. $\mathbb{P}(\mathcal{C}) = 0.108 > 0.1$. We go to Step 5.

Step 5. Print "For the system $\mathfrak{S}_1$ the property $\mathcal{P}(s_1, S^{trgt}_{\mathfrak{S}_1}, 0.1, 3)$ is false", print the designed counterexample

$$\mathcal{C} := \{s_1s_2s_4, s_1s_3s_4, s_1^2s_2s_4, s_1^2s_3s_4\},$$

and HALT.

□

It is evident that Algorithm 1 can be easily applied for the study of the violation of the property $\mathcal{P}(s_1, S^{trgt}_{\mathfrak{S}}, \lambda, h)$ under variations of the probabilities p_{ij} $(i, j = 1, \dots, k)$, as well as under variations of the values of λ and h.

4 Conclusions

The proposed FDTMC is intended for characterization behaviors of the analyzed CPS in the presence of admissible faults. For this FDTMC there exists the single stationary distribution (see Theorem 1). Therefore, probabilities of decreasing in performance of the analyzed CPS in the presence of faults can be estimated. Besides, the proposed FDTMC can be used for the bounded probabilistic analysis of the reachability of the target set of faults for the analyzed CPS (see Algorithm 1).

The essential characteristic of the proposed FDTMC is that it can be used for analysis of the effect of variations of faults probabilities on the probability distribution (6), as well as on the reachability of the target set of faults. Moreover, the proposed FDTMC can be used for symbolic modeling of the analyzed CPS by using these or the other suitable software tools.

References

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine, "The Algorithmic analysis of hybrid systems," *Theoretical Computer Science*, vol. 138, no. 1, pp. 3–34, 1995.

[2] J. Lygeros, "Lecture notes on hybrid systems," *Notes for an ENSIETA short course*, vol. 2–6, no. 2, 2004, Available: https://people.eecs.berkeley.edu/ sastry/ee291e/lygeros.pdf

[3] J.-F. Raskin, "An introduction to hybrid automata," in *Handbook of Networked and Embedded Control Systems. Control Engineering*, D. Hristu-Varsakelis and W.S. Levine, Eds. Boston, Basel, Berlin: Birkhäuser, pp. 491–518, 2005.

[4] G.A. Pérez Castañeda, J.-.F Aubry, and N. Brinzei, "Stochastic hybrid automata model for dynamic reliability assessment," *Journal of Risk and Reliability*, vol. 225, no. 1, pp. 28–41, 2011.

[5] M. Franzle, E.M. Hahn, H. Hermanns, N. Wolovick, and L. Zhang, "Measurability and safety verification for stochastic hybrid systems," in *Proc. of The* 14^{th} *International Conference on Hybrid Systems: Conmputation and Control - HSCC'11*, (April 12–14, 2011, Chicago, IL, USA), 2011, pp. 43–52.

[6] J. Sproston, "Decidable Model Checking of Probabilistic Hybrid Automata," in *Formal Techniques in Real-Time and Fault-Tolerant Systems. FTRTFT 2000* (Lecture Notes in Computer Science, vol. 1926), M. Joseph, Ed., 2000, pp. 31–45.

[7] L. Zhang, Z. She, S. Ratschan, H. Hermanns, and E. M. Hahn, "Safety Verification for Probabilistic Hybrid Systems," in *Computer Aided Verification. CAV 2010* (Lecture Notes in Computer Science, vol. 6174), T. Touili, B. Cook, and P. Jackson, Eds., 2010, pp. 196–211.

[8] J. Sproston, "Exact and approximate abstraction for classes of stochastic hybrid systems," *Electronic Communication of the European Association of Software Science and Technology*, vol. 70, 2014, pp. 79–88.

[9] E. Abraham, B. Becker, C. Dehnert, N. Jansen, J.-P. Katoen, and R. Wimmer, "Counterexample generation for Discrete-Time Markov Models: An introductory survey," in *Formal Methods for*

Executable Software Models. SFM 2014 (Lecture Notes in Computer Science, vol. 8483), M. Bernardo, F. Damiani, R. Hähnle, E.B. Johnsen, and I. Schaefer, Eds., 2014, pp. 65–121.

[10] J.G. Kemeney, J.L. Snell, and A. W. Knapp, *Denumerable Markov Chains*, NY, USA: Springer-Verlag, 1976.

[11] M. Kwiatkowska, G. Norman, and D. Parker, "Stochastic model checking," in *Formal Methods for Performance Evaluation. SFM 2007* (Lecture Notes in Computer Science, vol. 4486), M. Bernardo and J. Hillston, Eds., 2007, pp. 220–270.

[12] A. Biere, A. Cimatti, E. M. Clarke, O. Strichman, and Y. Zhu, "Bounded model checking," *Advances in Computers*, vol. 58, 2003, pp. 118–149.

Volodymyr G. Skobelev, Volodymyr V. Skobelev Received May 27, 2020

Volodymyr G. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 063 431 86 05
E–mail: `skobelevvg@gmail.com`

Volodymyr V. Skobelev
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
40 Glushkova ave., Kyiv, Ukraine, 03187
Phone: +38 066 276 85 72
E–mail: `volodimirvskobelev@gmail.com`