Reliability Engineering and System Safety **41** (1993) 1–4

Sojourn times in semi-Markov reward processes: application to fault-tolerant systems modeling

Gerardo Rubino & Bruno Sericola

IRISA/INRIA, Campus de Beaulieu, 35042 Rennes Cedex, France

(Received 12 April 1992; accepted 27 October 1992)

The paper considers fault-tolerant systems with operational periods in which the system works, and repair periods in which the system performs a reconfiguration from a recovering point. The aim is to obtain information about the successive operational periods before a fatal breakdown. In order to be able to deal with arbitrary probability distributions for the holding times in each state of the system, it is assumed that the system is modeled by a semi-Markov process. In this paper the distribution of the nth operational period is given. It often happens that the user wants to make a distinction among the operational states in order to get more detailed information. The use of rewards on the model states is then allowed, i.e. the results are presented for semi-Markov reward processes. An example illustrates this work.

1 MODEL DESCRIPTION

This paper considers a fault-tolerant system that is able to recover from breakdowns. At any instant t, there are three possibilities: the system can be operational, i.e. performing the tasks assigned to it (perhaps in a degradated way); it can be attempting to reconfigure itself after a failure without doing any useful work; finally, it can be dead, after some fatal breakdown.

The system is modeled by a right continuous homogeneous semi-Markov process denoted by $X = \{X_t, t \geq 0\}$. The semi-Markov assumption, instead of considering Markov processes, allows us to use general probability distributions in the individual states. The finite state space, denoted by E, is assumed to be composed by transient states and recurrent states. Since we are interested in transient measures, all the recurrent classes can be lumped into only one absorbing state. That is, we suppose that $E = \{1, \dots, N, a\}$ where $1, \dots, N$ are transient and a is absorbing. Let T_k be the time of the kth transition ($T_0 = 0$) and define $V_k = T_{k+1} - T_k$, the sojourn time in the $(k+1)$th visited state ($k \in \mathbb{N}$). The state reached after the kth transition is denoted by $X(k) = X_{T_k}$. The process X is defined by its kernel $\mathbf{Q}_t$ and its initial probability distribution $\boldsymbol{\alpha}$. The transition probability matrix of the embedded Markov chain $\{X(k), k \in \mathbb{N}\}$ is denoted by $\mathbf{P}$. For every $i, j \in E$, we have

$$\mathbf{Q}_t(i, j) \stackrel{\text{def}}{=} \mathbb{P}(X(k+1) = j, V_k \leq t \mid X(k) = i)$$
$$\mathbf{P}(i, j) \stackrel{\text{def}}{=} \mathbf{Q}_\infty(i, j) = \mathbb{P}(X(k+1) = j \mid X(k) = i)$$

We assume for instance that $\mathbf{Q}_t(a, a) = \delta(t-1)$, where

$$\delta(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases}$$

Note also that $\mathbf{Q}_t(a, j) = 0$ for every $j \neq a$.

A non-negative real-valued reward rate r_i is associated with each state $i \in E$. This allows the modeler to differentiate the states of B and, in this way, to capture not only failure and repair impact but also, for instance, different performance levels.

We denote by B the subset of E containing the operational states and by B' the subset of E containing the others transient states, so we have: $E = B \cup B' \cup \{a\}$. With the operational states we associate strictly positive reward rates. We will see that the reward rates associated with the other states have no influence on the results.

Reliability Engineering and System Safety 0951-8320/93/$06.00

The distribution of the nth sojourn time in a subset of states for an irreducible and homogeneous Markov process can be found in Ref. 1. Here the process is neither irreducible nor Markov and has reward rates. However, the two results are closely related. For $n \geq 1$, let $S_{i,B,n}$ denote the total time that X spends in state $i \in B$ during its nth visit to B. In the next section, the random variable $S_{B,n} \stackrel{\text{def}}{=} \sum_{i \in B} r_i S_{i,B,n}$ is analyzed. The distribution of $S_B \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} S_{B,n}$ which represents the total accumulated reward until absorption can be found in Ref. 2. Section 3 presents a short application.

In the sequel, we denote by $\mathbf{1}^T$ the column vector with all its coordinates equal to 1 (row vectors are always used and $(.)^T$ denotes the transpose operator) and by $\mathbf{I}$ the identity matrix, their dimensions being defined by the context.

2 DISTRIBUTION OF $S_{B,n}$

Let us consider another semi-Markov process without rewards, denoted by $Y = \{Y_t, t \geq 0\}$, defined on the state space $B \cup \{b\}$ where the state b is absorbing. The initial probability distribution of Y is $(\boldsymbol{\alpha}_\mathbf{B}, 1 - \boldsymbol{\alpha}_\mathbf{B}\mathbf{1}^T)$ where $\boldsymbol{\alpha}_\mathbf{B}$ denotes the subvector of $\boldsymbol{\alpha}$ corresponding to the states of B. The kernel $\hat{\mathbf{Q}}_\mathbf{t}$ of Y is defined as follows:

$$\hat{\mathbf{Q}}_\mathbf{t}(i, j) \stackrel{\text{def}}{=} \mathbf{Q}_{t/r_i}(i, j) \qquad \text{for } i, j \in B$$

$$\hat{\mathbf{Q}}_\mathbf{t}(i, b) \stackrel{\text{def}}{=} \mathbf{Q}_{t/r_i}(i, a) + \sum_{j \in B'} \mathbf{Q}_{t/r_i}(i, j) \qquad \text{for } i \in B$$

$$\hat{\mathbf{Q}}_\mathbf{t}(b, j) \stackrel{\text{def}}{=} \mathbf{Q}_t(a, j) \qquad \text{for } j \in B$$

$$\hat{\mathbf{Q}}_\mathbf{t}(b, b) \stackrel{\text{def}}{=} \mathbf{Q}_t(a, a)$$

We are now able to derive the conditional distribution of $S_{B,1}$ given that the initial state is in the subset B.

Lemma 2.1 For every $i \in B$, $\mathbb{P}(S_{B,1} \leq t / X_0 = i) = \mathbb{P}(Y_t = b / Y_0 = i)$.

Proof. For every $i \in B$,

$$\begin{aligned}\mathbb{P}(S_{B,1} \leq t / X_0 = i) &= \sum_{j \in B} \int_0^{t/r_i} \mathbb{P}(S_{B,1} \leq t - r_i s / X_0 = j)\, \mathrm{d}\mathbf{Q}_s(i, j) \\ &\quad + \sum_{j \in B'} \mathbf{Q}_{t/r_i}(i, j) + \mathbf{Q}_{t/r_i}(i, a) \\ &= \sum_{j \in B} \int_0^t \mathbb{P}(S_{B,1} \leq t - s / X_0 = j)\, \mathrm{d}\hat{\mathbf{Q}}_s(i, j) + \hat{\mathbf{Q}}_t(i, b)\end{aligned}$$

On the other hand, we have

$$\mathbb{P}(Y_t = b / Y_0 = i) = \sum_{j \in B} \int_0^t \mathbb{P}(Y_{t-s} = b / Y_0 = j)\, \mathrm{d}\hat{\mathbf{Q}}_s(i, j) + \hat{\mathbf{Q}}_t(i, b)$$

So, these two quantities are solutions to the same integral equation. Since this equation has an unique solution (see Ref. 3), the enounced result follows.

Let us decompose the matrix $\mathbf{P}$ and the initial probability vector $\boldsymbol{\alpha}$ with respect to the partition $E = B \cup B' \cup \{a\}$ as follows.

$$\mathbf{P} = \begin{pmatrix} \mathbf{P_B} & \mathbf{P_{BB'}} & \mathbf{P_{Ba}} \\ \mathbf{P_{B'B}} & \mathbf{P_{B'}} & \mathbf{P_{B'a}} \\ \mathbf{0} & \mathbf{0} & 1 \end{pmatrix}, \qquad \boldsymbol{\alpha} = (\boldsymbol{\alpha}_\mathbf{B} \quad \boldsymbol{\alpha}_\mathbf{B'} \quad \alpha_a)$$

We denote by $\mathbf{H}$ the $B' \times B$ matrix defined by $\mathbf{H} \stackrel{\text{def}}{=} (\mathbf{I} - \mathbf{P_{B'}})^{-1}\mathbf{P_{B'B}}$. We define the vectors

$$\mathbf{u_B}(n, t) \stackrel{\text{def}}{=} (\mathbb{P}(S_{B,n} \leq t / X_0 = i),\ i \in B)$$
$$\mathbf{u_{B'}}(n, t) \stackrel{\text{def}}{=} (\mathbb{P}(S_{B,n} \leq t / X_0 = i),\ i \in B')$$

With this notation, we prove the following lemma.

Lemma 2.2 For all $n \geq 1$, $\mathbf{u}^T_\mathbf{B'}(n, t) = \mathbf{1}^T - \mathbf{H}(\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(n, t))$

Proof. For every $i \in B'$,

$$\begin{aligned}\mathbb{P}(S_{B,n} \leq t / X_0 = i) &= \sum_{j \in B} \mathbf{P}(i, j)\mathbb{P}(S_{B,n} \leq t / X_0 = j) \\ &\quad + \sum_{j \in B'} \mathbf{P}(i, j)\mathbb{P}(S_{B,n} \leq t / X_0 = j) + \mathbf{P}(i, a)\end{aligned}$$

In matrix notation, we obtain

$$\mathbf{u}^T_\mathbf{B'}(n, t) = \mathbf{P_{B'B}}\mathbf{u}^T_\mathbf{B}(n, t) + \mathbf{P_{B'}}\mathbf{u}^T_\mathbf{B'}(n, t) + \mathbf{P_{B'a}}$$

which can easily be written

$$\mathbf{u}^T_\mathbf{B'}(n, t) = \mathbf{1}^T - \mathbf{H}(\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(n, t))$$

since $\mathbf{P_{B'B}}\mathbf{1}^T + \mathbf{P_{B'}}\mathbf{1}^T + \mathbf{P_{B'a}} = \mathbf{1}^T$.

Let us denote by $\mathbf{G}$ the $B \times B$ matrix $\mathbf{G} \stackrel{\text{def}}{=} (\mathbf{I} - \mathbf{P_B})^{-1}\mathbf{P_{BB'}}\mathbf{H}$, and by $\mathbf{v_1}$ the vector $\mathbf{v_1} \stackrel{\text{def}}{=} \boldsymbol{\alpha}_\mathbf{B} + \boldsymbol{\alpha}_\mathbf{B'}\mathbf{H}$. We get the following expression of the distribution of $S_{B,n}$.

Theorem 2.3 For all $n \geq 1$, $\mathbb{P}(S_{B,n} \leq t) = 1 - \mathbf{v_1}\mathbf{G}^{n-1}(\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(1, t))$.

Proof. Let $i \in B$ and $n \geq 2$.

$$\begin{aligned}\mathbb{P}(S_{B,n} \leq t / X_0 = i) &= \sum_{j \in B} \mathbf{P}(i, j)\mathbb{P}(S_{B,n} \leq t / X_0 = j) \\ &\quad + \sum_{k \in B'} \mathbf{P}(i, k)\mathbb{P}(S_{B,n-1} \leq t / X_0 = k) + \mathbf{P}(i, a)\end{aligned}$$

which gives in matrix notation, using Lemma 2.2,

$$\begin{aligned}\mathbf{u}^T_\mathbf{B}(n, t) &= \mathbf{P_B}\mathbf{u}^T_\mathbf{B}(n, t) + \mathbf{P_{BB'}}\mathbf{u}^T_\mathbf{B'}(n-1, t) + \mathbf{P_{Ba}} \\ &= \mathbf{1}^T - \mathbf{G}\mathbf{1}^T + \mathbf{G}\mathbf{u}^T_\mathbf{B}(n-1, t)\end{aligned}$$

It follows that, for all $n \geq 1$,

$$\begin{aligned}\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(n, t) &= \mathbf{G}(\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(n-1, t)) \\ &= \mathbf{G}^{n-1}(\mathbf{1}^T - \mathbf{u}^T_\mathbf{B}(1, t))\end{aligned}$$

Finally, we obtain

$$\begin{aligned}\mathbb{P}(S_{B,n} \le t) &= \boldsymbol{\alpha}_{\mathbf{B}}\mathbf{u}_{\mathbf{B}}^{T}(n,t) + \boldsymbol{\alpha}_{\mathbf{B}'}\mathbf{u}_{\mathbf{B}'}^{T}(n,t) + \alpha_a \\ &= 1 - \boldsymbol{\alpha}_{\mathbf{B}}(1^T - \mathbf{u}_{\mathbf{B}}^{T}(n,t)) - \boldsymbol{\alpha}_{\mathbf{B}'}(1^T - \mathbf{u}_{\mathbf{B}'}^{T}(n,t)) \\ &= 1 - \mathbf{v}_1(\mathbf{1}^T - \mathbf{u}_{\mathbf{B}}^{T}(n,t)) \quad \text{using Lemma 2.2} \\ &= 1 - \mathbf{v}_1\mathbf{G}^{n-1}(\mathbf{1}^T - \mathbf{u}_{\mathbf{B}}^{T}(1,t))\end{aligned}$$

Consider the sequence of states in which the successive visits of X to B begin. If we add to the end end of each sequence the absorbing state a for each trajectory in which X is absorbed (this happens with probability 1), a homogeneous discrete time Markov chain is defined with state space $B \cup \{a\}$. It can be shown that the submatrix of the transition probability matrix of this chain, obtained by deleting the row and column corresponding to the absorbing state a, is $\mathbf{G}$. In the same way, $(\mathbf{v}_1, 1 - \mathbf{v}_1\mathbf{1}^T)$ is its starting probability distribution. The reader is referred to Ref. 1 for a proof in a similar context (irreducible Markov processes without rewards).

Note that the vector $\mathbf{u}_{\mathbf{B}}^{\mathbf{T}}(1, t)$ is given by Lemma 2.1. A numerical inversion of Laplace transform can be used to compute it (see, for example, Ref. 4).

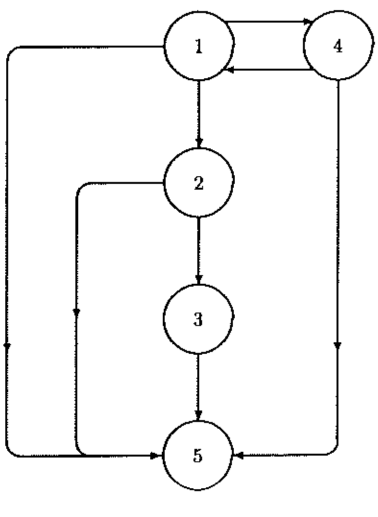
3 APPLICATION

As an application of the previous results, we consider a fault-tolerant structure in which three identical processors work in parallel running the same code. The three processors receive the same input and take synchroneously a binary decision. A voter device controls the three outputs and in case of disagreement between them, it chooses the value which is present twice. There can be software or hardware faults on the processors and the voter is assumed here perfectly reliable. The system starts with the three processors performing correctly (state 1 in Fig. 1). Due to design faults in the software, the system can be shut down and a recovery procedure is started (state 4). We assume that the software faults occur with rate λ_s and that the repairing time is constant and lasts K. The probability of a software fault recovery is denoted by d (the *software fault coverage* parameter).

With respect to the hardware faults, the three processor behaviors are assumed to be independent. The hardware faults occur at rate λ_h for any processing unit. When such an error occurs, a procedure to put the system back in operation is tried. Its success probability is constant c (the *hardware fault coverage* parameter). This procedure is assumed to be executed instantaneously. So, with probability c, the system continues to perform (in a degradated mode) with only one processor, the other non-failed unit staying in passive redundancy (state 2). The voter is no more used in this situation and, for simplicity, the system is assumed to be unable to recover from software errors when there is only one active processor. The redundant unit cannot fail and when there is a new hardware breakdown, a second procedure is started to try to reconfigure again. If it is successful, the system uses the remaining operational processor (state 3) until the last (fatal) hardware fault (state 5).

This model leads to the five-states semi-Markov process described in Fig. 1, where the holding time in state 4 is constant and equal to K. The other holding times are exponentially distributed (excepting, of course, for state 5 which corresponds to the crash of the system). The set of operational states is then $B = \{1, 2, 3\}$.

Assume that an active unit gives the wrong answer



$$\mathbf{Q}_t(1,2) = \frac{3\lambda_h c}{3\lambda_h + \lambda_s}(1 - \exp(-(3\lambda_h + \lambda_s)t))$$

$$\mathbf{Q}_t(1,4) = \frac{\lambda_s}{3\lambda_h + \lambda_s}(1 - \exp(-(3\lambda_h + \lambda_s)t))$$

$$\mathbf{Q}_t(1,5) = \frac{3\lambda_h(1-c)}{3\lambda_h + \lambda_s}(1 - \exp(-3\lambda_h + \lambda_s)t))$$

$$\mathbf{Q}_t(2,3) = \frac{\lambda_h c}{\lambda_h + \lambda_s}(1 - \exp(-(\lambda_h + \lambda_s)t))$$

$$\mathbf{Q}_t(2,5) = \frac{\lambda_h(1-c) + \lambda_s}{\lambda_h + \lambda_s}(1 - \exp(-(\lambda_h + \lambda_s)t))$$

$$\mathbf{Q}_t(3,5) = 1 - \exp(-(\lambda_h + \lambda_s)t)$$

$$\mathbf{Q}_t(4,1) = d\delta(t - K)$$

$$\mathbf{Q}_t(4,5) = (1 - d)\delta(t - K)$$

Fig. 1. A three-processors fault-tolerant structure.

with probability p. When three processors are working in parallel (and independently), the probability of obtaining a wrong output is $p^3+3p^2(1-p)$. Furthermore, it is assumed that the workload of the system is high, i.e. the system is required to give a large number of outputs per unit of time. So, we consider the following reward rates for the states of B: $r_1=1-3p^2+2p^3$, $r_2=r_3=r=1-p$. With these assumptions, the random variables $S_{B,n}$ can be viewed as the total time while the system gives the right answer during the nth operational period.

The computations can be easily made by hand since the holding times in the states of B are exponentially distributed. The distribution of the nth accumulated reward $S_{B,n}$ is given by the following expression.

$$\mathbb{P}(S_{B,n}\le t) = 1-\left(\frac{d\lambda_s}{3\lambda_h+\lambda_s}\right)^{n-1}\left[(1+U)\exp\left(-\frac{3\lambda_h+\lambda_s}{r_1}t\right) - \left(\frac{3\lambda_h^2c^2}{L}t+U\right)\exp\left(-\frac{\lambda_h+\lambda_s}{r}t\right)\right]$$

where

$$L=\lambda_h(r_1-3r)+\lambda_s(r_1-r)$$

and

$$U=\frac{3\lambda_h cr}{L}+\frac{3\lambda_h^2c^2r_1r}{L^2}$$

If we compute the corresponding distribution for the set B', reduced here to state 4, we obtain

$$\mathbb{P}(S_{B',n}\le t)=1-\frac{\lambda_s}{3\lambda_h+\lambda_s}\left(\frac{d\lambda_s}{3\lambda_h+\lambda_s}\right)^{n-1}\delta(K-t)$$

Observe that if $p=0$ (i.e. $r_1=r=1$), $S_{B,n}$ represents the time spent by X in B during its nth visit to this set. Given that the system starts in a state of B, the expectation of the time spent until the end of the Mth visit to B is then

$$\left.\left(\sum_{n=1}^{M}\mathbb{E}(S_{B,n})+\sum_{n=1}^{M-1}\mathbb{E}(S_{B',n})\right)\right|_{p=0}$$

As $\sum_{n=1}^{M}\mathbb{E}(S_{B,n})$ represents the average total time while the system works and gives the right answer during the M first operational periods, a quantity of interest is the ratio

$$\rho(M)=\frac{\sum_{n=1}^{M}\mathbb{E}(S_{B,n})}{\left.\left(\sum_{n=1}^{M}\mathbb{E}(S_{B,n})+\sum_{n=1}^{M-1}\mathbb{E}(S_{B',n})\right)\right|_{p=0}}$$

and

$$\rho(1)\stackrel{\text{def}}{=}1$$

which represents the expected rate of right answers during the M first operational periods. In this case, we obtain for every $M\ge 2$,

$$\rho(M)=\frac{F_p}{F_0+\dfrac{1-q^{M-1}}{1-q^M}\dfrac{q}{d}K}$$

where

$$F_p=\frac{1-3p^2+2p^3}{3\lambda_h+\lambda_s}+(1-p)\times\left(\frac{3\lambda_h c}{(\lambda_h+\lambda_s)(3\lambda_h+\lambda_s)}+\frac{3\lambda_h^2c^2}{(\lambda_h+\lambda_s)^2(3\lambda_h+\lambda_s)}\right)$$

and

$$q=\frac{\lambda_s}{3\lambda_h+\lambda_s}$$

See that $F_0\ge F_p$ and that for any fixed value of K, we have

$$\frac{F_p}{F_0+\dfrac{q}{d}K}<\rho(M)\le 1$$

For a given level β with $0<\beta<1$ (and $\beta\approx 1$), we can evaluate, for instance, the maximal value of the parameter K (the execution time of the software recovery procedure) such that $\rho(M)\ge\beta$. Observe that if the number M of operational periods is fixed and $M\ge 2$, the best theoretically possible value for the ratio $\rho(M)$ is F_p/F_0. If $\beta<F_p/F_0$ we have

$$\rho(M)\ge\beta\quad\text{for every } M\ge 2\Leftrightarrow 0<K\le\frac{F_p-\beta F_0}{\beta}\frac{d}{q}$$

REFERENCES

1. Rubino, G. & Sericola, B., Sojourn times in finite Markov processes. *J. Applied Probability*, **27** (1989) 744–56.
2. Ciardo, G., Marie, R., Sericola, B. & Trivedi, K., Performability analysis using semi-Markov reward processes. *IEEE Transactions on Computers*, **29** (1990) 1251–64.
3. Cinlar, E., *Introduction to Stochastic Processes*. Prentice Hall, NJ, 1975.
4. Jagerman, D. L., An inversion technique for the Laplace transforms. *Bell System Technical Journal*, **61** (1982) 1995–2002.