Reliability Engineering and System Safety 140 (2015) 122–129

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Mission reliability of semi-Markov systems under generalized operational time requirements

Xiaoyue Wu [a,*], Jane Hillston [b]

[a] College of Information Systems and Management, National University of Defense Technology, Changsha, Hunan 410073, China
[b] School of Informatics, University of Edinburgh, Edinburgh, Scotland EH8 9AB, UK

ARTICLE INFO

Article history:
Received 15 December 2014
Received in revised form
2 March 2015
Accepted 3 April 2015
Available online 13 April 2015

Keywords:
Mission reliability
System
Markov
Semi-Markov
Algorithm
Simulation

ABSTRACT

Mission reliability of a system depends on specific criteria for mission success. To evaluate the mission reliability of some mission systems that do not need to work normally for the whole mission time, two types of mission reliability for such systems are studied. The first type corresponds to the mission requirement that the system must remain operational continuously for a minimum time within the given mission time interval, while the second corresponds to the mission requirement that the total operational time of the system within the mission time window must be greater than a given value. Based on Markov renewal properties, matrix integral equations are derived for semi-Markov systems. Numerical algorithms and a simulation procedure are provided for both types of mission reliability. Two examples are used for illustration purposes. One is a one-unit repairable Markov system, and the other is a cold standby semi-Markov system consisting of two components. By the proposed approaches, the mission reliability of systems with time redundancy can be more precisely estimated to avoid possible unnecessary redundancy of system resources.

1. Introduction

In engineering applications, there exist many systems designed to support the accomplishment of critical missions. For example, during a space flight mission, it is necessary to use the spaceflight telemetry, tracking, and control (TT&C) system [1] to provide connection between the spacecraft and facilities on the ground, and to ensure that the spacecraft performs its mission correctly. Often, to avoid the risk of mission failure or waste of TT&C resources, space system engineers are interested in quantitatively assessing the mission reliability of the TT&C system which will support a planned spaceflight, so they can make reasonable decisions about the system design before practical execution of the mission.

Mission reliability of a system is the probability of successful completion of a stated mission by the system deployed in a given environment. Depending on different criteria of mission success, mission reliability may be defined more specifically. In some engineering applications, a mission must be successfully accomplished within a given time interval. Taking TT&C systems as an example, since the spacecraft orbits the earth, the time for which it is passing overhead a ground facility is limited to a specific interval (called the *time window*), so the facility can only provide TT&C services within this time window. However, for the mission to be successful, sometimes the system does not need to work normally for the whole time window. In this paper, we identify two specific cases. In the first case, to ensure mission success, the system needs only to remain operational for a time period greater than a certain value within the mission time window. For example, to accomplish certain remote control instruction injection operations on a spacecraft, the ground facility only needs to function normally for a short period of time while the spacecraft passes over. We call this type of mission reliability, *mission reliability of type I*. In the second case, we require that the total sum of the system's operational periods within the given time window is greater than a given value. We call the mission reliability of this kind *mission reliability of type II*. For a TT&C system, if the mission is to transfer a certain amount of onboard data, as long as the total sum of transmission time is sufficient, the mission will be regarded as successfully completed.

Although there are papers on mission reliability for special systems of one mission phase [2,3], most existing literature on mission reliability focuses on phased-mission systems (PMS) that have multiple phases [4–6]. However, a commonly adopted assumption in existing research work is that for the mission to succeed in a phase, the system must remain operational throughout the whole time of the phase [3,7]. Recent theoretical research

* Corresponding author. Tel.: +86 13308491401.
E-mail addresses: xioayuewucn@nudt.edu.cn (X. Wu), Jane.Hillston@ed.ac.uk (J. Hillston).

http://dx.doi.org/10.1016/j.ress.2015.04.002
0951-8320/

work on PMS has mainly focused on two fields. One is on the improvement of computational efficiency [8,9,7]; another is on modelling and analysis methods of various kinds of PMS with special features, such as demand-based PMS [10], PMS with common-cause failures [11,12], propagated failures [13] and imperfect coverage [14]. For the two cases considered in our paper, if we apply the assumption that the system must remain operational throughout the whole time of the phase, we can only get a conservative estimate of the real mission reliability, because the assumption is stricter than really necessary. This is only acceptable if the mission time interval is short enough. For some TT&C services, the required TT&C task time may be just several minutes. For a low earth orbit (LEO) satellite, since the time of passing overhead a ground station (i.e. the time window) is of about the same magnitude, the errors due to such an assumption are insignificant. However, for some medium earth orbit (MEO) satellites or if inter-satellite links are used, the time window can be as long as several hours and the adoption of this assumption in mission reliability evaluation will unavoidably lead to serious underestimation of the real value, and may result in unnecessary redundancy in the deployment of expensive TT&C resources. Therefore, more precise modelling and solution methods are needed in such situations.

To the best of our knowledge, little previous research has been done on these two types of mission reliability. The first type was studied for the first time in [15], and a numerical method was given for its calculation based on the probabilities of mission success in mutually exclusive cases and order statistics. However, in that paper the system under study was restricted to a one-unit system with both exponential failure and repair times.

By a *Markov system* we mean a system whose behaviour can be described by its state evolution over a time horizon, and at any moment the future behaviour of the system, given its current state, is independent of its past history. A *semi-Markov system* is a generalization of a Markov system [16]. Compared with a Markov system, the main feature of a semi-Markov system is that the time required for each successive state transition can be a non-exponential random variable, which may depend on both its current state and the next state to be visited.

Whilst we believe our type I and type II mission reliability measures to be novel, a similar measure has previously appeared in the literature as *interval reliability* [17,18], *remaining probability* [19] or *interval availability* [20]. Interval reliability is defined as the probability that a system will work normally for a specific time interval of given length without failure given that it begins to work at a fixed start moment. Barlow gave a general formula for computing interval reliability by use of a renewal property [18] and obtained its limit solution as time tends to infinity. It has been shown that for repairable semi-Markov systems, either a double Laplace transform or an integral equation approach can be used to obtain interval reliability [2]. For semi-Markov systems with general state space (not limited to finite or countable state space), in both continuous time and discrete time cases, Markov renewal equations (MRE) can be built to give the formulae of interval reliability and its limiting expression [20–22].

However, interval reliability is defined only for a fixed interval time horizon, whereas our mission reliability of type I is defined for a mission that can be executed in an interval that is not prescribed prior to the mission, within a given mission time window. Moreover, by definition, the meaning of interval reliability is totally different from that of mission reliability of type II.

In this paper, we define two types of mission reliability. Furthermore, for the general case of semi-Markov systems, by the renewal property of semi-Markov processes, we derive matrix integral equations and provide numerical algorithms for calculating these two types of mission reliability.

The remainder of this paper is organized as follows. Section 2 introduces the equations for sojourn time distributions of semi-Markov systems, and gives numerical methods for their solution. Section 3 establishes the integral matrix equations for mission reliability of type I. Section 4 is devoted to mission reliability of type II: a group of matrix integral equations is derived, and algorithms are provided for their solution. Section 5 presents a simulation procedure for estimating both types of mission reliability for semi-Markov systems. Two numerical examples are developed to verify our proposed analytical solution methods, and the results are compared with simulation. In the last section, some concluding remarks are given.

2. Sojourn time distributions

2.1. Semi-Markov systems

Suppose we have a system whose state changes only at discrete time moments and takes values in a finite space S. Let S_n denote the time of nth state transition, $n \ge 0$, and the corresponding state of the system is Z_n. Assume the sequence $\{(Z_n, S_n), n \ge 0\}$ is a *Markov renewal sequence* [23], define $N(t) = \sup\{n \ge 0 | S_n \le t\}$, then the state of the system at time t will be $Y(t) = Z_{N(t)}$, which is a *continuous time semi-Markov process* (SMP) [23,24]. In this case, the system is defined as a *semi-Markov system*.

For convenience, we will use Y_t, Y to denote $Y(t)$, $\{Y_t, t \ge 0\}$ respectively in the sequel.

For any $i, j \in S$, let

$$K^n_{i,j}(t) = P\{Z_{n+1} = j, S_{n+1} - S_n \le t | Z_n = i\}.$$

In this paper, we only consider time-homogeneous semi-Markov systems. So, we can define the semi-Markov kernel of Y as $Q(t) = [q_{i,j}(t)]$, where

$$q_{i,j}(t) = \begin{cases} K^0_{i,j}(t) & i \ne j \\ 0 & i = j \end{cases} \quad \forall i, j \in S \tag{1}$$

Notice that we assume that the system already has a minimal representation [23], so all Markov renewal moments represent real state transitions, which is why in Eq. (1) we define $q_{i,i}(t) \equiv 0, \forall i \in S$.

Suppose S is partitioned into U and D, where U is the set of *up states*, in which the system is operational, and D is the set of *down states*, in which the system has failed and is under repair. Hence from a reliability point of view, the state of the system alternates between U and D during system evolution.

For convenience, we will also use U, D to denote the tuples of the corresponding sets of state:

$$U = (u_1, u_2, \ldots, u_{|U|})$$
$$D = (d_1, d_2, \ldots, d_{|D|})$$

where $|U|, |D|$ stand for the number of elements in the corresponding sets .

2.2. Equations for sojourn time distributions

For later use, here we introduce the main results by Csenki [2,25] about the sojourn time of a semi-Markov system before it makes a state transition.

Let $k_{u,d}(t)$ denote the distribution function of the sojourn time of the system holding in state $u \in U$ before first entering or re-entering into down state $d \in D$, and $k_{d,u}(t)$ denotes the distribution function of the sojourn time of the system holding in state $d \in D$ before first entering or re-entering up state $u \in U$.