Reliability Engineering and System Safety 000 (2017) 1–13

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Generalized Continuous Time Bayesian Networks as a modelling and analysis formalism for dependable systems

Daniele Codetta-Raiteri*, Luigi Portinale

DiSIT, Computer Science Institute, University of Piemonte Orientale, Alessandria, Italy

A R T I C L E I N F O

Keywords:
Generalized Continuous Time Bayesian Networks
Reliability analysis
Diagnosis
Sensitivity analysis
Probabilistic models

A B S T R A C T

We discuss the main features of Generalized Continuous Time Bayesian Networks (GCTBN) as a dependability formalism: we resort to two specific case studies adapted from the literature, and we discuss modelling choices, analysis results and advantages with respect to other formalisms. From the modelling point of view, GTCBN allow the introduction of general probabilistic dependencies and conditional dependencies in state transition rates of system components. From the analysis point of view, any task ascribable to a posterior probability computation can be implemented, among which the computation of system unreliability, importance indices, system monitoring, prediction and diagnosis.

1. Introduction

In the reliability field, an interesting trade-off between combinatorial models [1] (e.g. *Fault Trees, Reliability Block Diagrams*, etc.) and state space based models [1] (e.g. *Markov Chains, Petri Nets*, etc.) is given by *Probabilistic Graphical Models* (**PGM**[1]) [2–4], among which *Bayesian Networks* (**BN**) are the most popular formalism [5]. Standard BN are however static models representing a snapshot at a given time point of the system of interest. When time is taken into account, the main choice concerns whether to consider it as a discrete or a continuous dimension. In the former case, models like *Dynamic Bayesian Networks* (**DBN**) [6] have become a natural choice [7–9]. However, there is not always an obvious discrete time unit, so *Continuous Time Bayesian Networks* (**CTBN**) [10] have started to be investigated.

In [11] a generalisation of CTBN is proposed by introducing the presence of nodes which have no explicit temporal evolution; the values of such nodes are, in fact, "immediately" determined, depending on the values of other nodes in the network. This allows us to model processes having both a continuous-time temporal component and a static component capturing the logical/probabilistic aspects determined by specific events occurring in the modelled process. This formalism is called *Generalized Continuous Time Bayesian Network* (**GCTBN**).

In the present paper, we show how the GCTBN language can be suitably used to model dependable systems, and in particular, both static as well as dynamic dependencies among system components, like those introduced in *Dynamic Fault Trees* (**DFT**) [12]: the combination of principal and spare components, functional dependencies and priority AND are specific dynamic dependencies that can be easily accounted for, in a GCTBN model. In addition, specific dependencies, more general than those envisioned by DFT, can be captured through GCTBN; this makes possible to overcome the often adopted assumption of independent binary components, without the need of explicitly enumerating the whole system state space, as in standard state space based models like *Continuous Time Markov Chain* (**CTMC**) [1]. Repairable components can also be introduced, together with the possibility of modelling repair or maintenance strategies conditioned on the occurrence of specific events in the modelled system.

From the analytical point of view, probabilistic inference can be performed through the computation of arbitrary posterior probabilities, where the status of system components as well as subsystems can be queried at any required time point, given that a temporal stream of observations (the evidence) is provided. This allows us to perform standard dependability analyses, like system reliability or importance of components, as well as to perform more general fault detection and identification procedures.

This paper (which is an elaborated extension of the work presented in [13]) is organised as follows: in Section 2 we present the details about the involved formalisms; in Section 3 we provide the rules to generate a GCTBN from a DFT model; in Sections 4 and 5 we present two case studies and we discuss modelling choices and analysis results. In particular, we show how to exploit posterior probability computation for implementing dependability analysis: for each case study we compute dependability measures (like system unreliability), importance measures (like *Birnbaum index* or *Fussell–Vesely index* [14]), and diagnostic

* Corresponding author.
E-mail addresses: dcr@di.unipmn.it (D. Codetta-Raiteri), luigi.portinale@di.unipmn.it (L. Portinale).

[1] The acronyms and their meaning are listed in Table 1.

http://dx.doi.org/10.1016/j.ress.2017.04.014
Available online xxx
0951-8320/© 2017 Elsevier Ltd. All rights reserved.

measures (like general posterior probability of faults, given specific sensor observations). The first case study is aimed at showing the advantages of GCTBN inference, with respect to standard DFT analysis. The second case study focuses on advantages of GCTBN with respect to DBN, as discussed into details in Section 6 where we highlight the features making GCTBN suitable to dependability modelling and analysis.

2. Formal definitions

2.1. Dynamic Fault Trees

Fault Trees (**FT**) [1] are a combinatorial formalism (with a widespread use in reliability) that represent how the failure propagates from the components (*basic events*) to the system (*top event*); *Boolean gates* (AND, OR, *k* out of *n* (*k:n*), etc.) are used to this end. *Dynamic Fault Trees* (**DFT**) [12] augment standard FT with dynamic gates, with the aim of introducing specific dynamic (i.e., time-dependent) dependencies in the system structure and behaviour; more specifically such gates are the following (see [12]):

- *Functional Dependency gate* (**FDEP**)—given a trigger event *T*, the dependent events $D_1, \ldots, D_n$ are immediately forced to occur when *T* occurs (Fig. 3a and b).
- *Priority And gate* (**PAND**)—given $X_1, \ldots, X_n$ as input events and *Y* as output event, *Y* fails if all $X_1, \ldots, X_n$ have occurred and only in a specified order (Fig. 4a).
- *Spare gate*—this gate models the presence of the spare components $S_1, \ldots, S_n$ able to replace a main component *M* when it fails (Fig. 5a). Spares can be in three states: dormant (or stand-by), working, failed. The spare failure rate changes depending on its current state: if the failure rate of the spare is λ in the working state, $\alpha\lambda$ is its failure rate in the dormant state, with $0 \leq \alpha \leq 1$; α is called dormancy factor. The output event occurs if the main component fails and there are no spares available to replace it. The gate is called Hot (**HSP**) when $\alpha = 1$, Warm (**WSP**) when $0 < \alpha < 1$, and Cold (**CSP**) when $\alpha = 0$.
- *Sequence Enforcing gate* (**SEQ**)—this gate forces a set of basic events to occur in a specific order. We omit to discuss SEQ here, since it can be modelled as a special case of a CSP [15].

2.2. Bayesian Networks

Bayesian Networks (**BN**) (also known as *Belief Networks*) [5] are a widely used formalism for representing uncertain knowledge in Artificial Intelligence [16,17]. They have then gained a great popularity in the reliability field as well, because of their flexibility in modelling and analysing dependable systems [5,7,18,19].

A Bayesian Network (**BN**) is a pair $N = \langle\langle V, E\rangle, P\rangle$ where $\langle V, E\rangle$ are the nodes and the edges of a *Directed Acyclic Graph* (**DAG**) respectively, and *P* is a probability distribution over *V*. Discrete random variables $V = \{X_1, X_2, \ldots X_n\}$ are assigned to the nodes, while each edge $e \in E$ from node *X* to node *Y* represents a probabilistic relationship between the variables represented by *X* and *Y*, where *Y* directly depends on *X*. This interpretation allows us to factorise the joint probability of the variables of the model, by considering only the conditional distribution of each variable with respect to their parent variables in the DAG, as shown in Eq. (1).

$$P[X_1, X_2, \ldots, X_n] = \prod_{i=1}^{n} P[X_i | Parent(X_i)] \quad (1)$$

In the standard case of discrete variables, each local distribution can be described in tabular form (i.e., a column for each combination of states of the parent variables), called *Conditional Probability Table* (**CPT**).

Because of the availability of the joint probability distribution, any kind of probabilistic query of the form $P(Q|e)$ can be computed, where *Q* is any set of unobserved variables and *e* is a configuration of a set of observed variables called the *evidence*.

2.3. Dynamic Bayesian Networks

Given a set of time-dependent state variables $X_1, \ldots, X_n$, and given a BN *N* defined on such variables, a *Dynamic Bayesian Network* (**DBN**) [6] is essentially a replication of *N* over two time slices $t - \Delta$ and *t* (Δ is the time discretisation step), with the addition of a set of arcs representing the transition model. Let X_i^t denote the copy of variable X_i at time slice *t*, the transition model is defined through a distribution $P[X_i^t | X_i^{t-\Delta}, Y^{t-\Delta}, Y^t]$ where $Y^{t-\Delta}$ is any set of variables at slice $t - \Delta$ different from X_i (possibly the empty set), and Y^t is any set of variables at slice *t* different from X_i (possibly the empty set).

An edge connecting a variable $X_i^{t-\Delta}$ in the slice $t - \Delta$ to the variable X_j^t in the slice *t*, is called *temporal arc* (if $i = j$ the arc connects the two instances of the same variable). The dependency of a given node on its parent nodes (possibly including its historical copy) is quantified in its CPT.

2.4. Continuous Time Bayesian Networks

Following the original paper [10], a *Continuous Time Bayesian Network* (**CTBN**) is defined as follows: let $V = \{X_1, \ldots, X_n\}$ be a set of discrete variables, a CTBN over X consists of two components. The first one is an initial distribution P_V^0 over *V* (possibly specified as a standard BN over *V*). The second component is a continuous-time transition model specified as:

- a directed graph G whose nodes are $X_1, \ldots, X_n$ ($Pa(X_i)$ denotes the parents of X_i in G);
- a *Conditional Intensity Matrix* (**CIM**) $Q_{X_i|Pa(X_i)}$ for every $X_i \in V$. The CIM of a variable X_i provides the transition rates[2] for each possible pair of values of X_i, given any possible combination of the parent nodes' values.

With respect to BN and DBN, having an acyclic graph structure (DAG), cycles are instead permitted in CTBN where a node (variable) X_i, ancestor of X_j, can be reachable from X_j. A cycle could be even composed by one node X_i: $X_i \in Pa(X_i)$.

2.5. Generalised Continuous Time Bayesian Networks

2.5.1. Definition

Given a set of discrete variables $V = \{X_1, \ldots, X_n\}$ partitioned into the sets *D* (delayed variables) and *I* (immediate variables), a *Generalised Continuous Time Bayesian Network* (**GCTBN**) [11] is a pair $\langle P_V^0, G\rangle$ where

- P_V^0 is an initial probability distribution over *D*;
- *G* is a directed graph whose nodes are $X_1, \ldots, X_n$ such that
  - there is no directed cycle in *G* composed only by nodes in the set *I*;
  - for each node $X \in I$ a CPT $P[X|Pa(X)]$ is defined (as in standard BN and DBN);
  - for each node $X \in D$ a CIM $Q_{X|Pa(X)}$ is defined (as in CTBN).

Delayed (or temporal) nodes represent variables with a continuous time evolution; we consider the case when they are ruled by exponential transition rates conditioned by the values of parent variables (that may be either delayed or immediate). Delayed nodes have a CIM of rates associated with them; entries of a CIM $Q_{Y|Pa(Y)}$ can take values in $\mathbb{R} \cup \infty$ with ∞ meaning an immediate (i.e., a zero time) transition between two states of a variable. Immediate nodes instead, are introduced in order to capture variables whose evolution is not ruled by transition rates, but is conditionally determined, at a given time point, by other variables in the model. Therefore immediate nodes are treated as usual chance nodes in a BN and have a standard CPT associated with them.

[2] In the following we will assume an exponential distribution for the sojourn time in a given state and constant transition rates.