From AI to Dependability: using Bayesian Networks for Reliability Modeling and Analysis

Luigi Portinale, Andrea Bobbio, Stefania Montani
Dipartimento di Informatica
Universita del Piemonte Orientale "A. Avogadro"
I-15100 Alessandria
Italy
portinal@di.unipmn.it

Extended Abstract

Bayesian Networks (BN) provide a robust probabilistic method of reasoning under uncertainty. They have been successfully proposed in the field of Artificial Intelligence (AI) as the most flexible formalism for reasoning under uncertain knowledge. Their success stands from several factors: the graphical representation of the knowledge to reason with, the restricted number of probabilities to be specified with respect to a complete joint probability model, the possibility of performing different kinds of inferences like predictive and diagnostic inference or inter-causal reasoning, the possibility of 'learning' the model from a database of observations.

For these reasons, they have been successfully applied in a variety of real-world tasks, however they have received little attention in the area of dependability. The present talk is aimed at exploring the capabilities of the BN formalism in the modeling and analysis of dependable systems. To this end, we compare BN with one of the most popular techniques for dependability analysis of large, safety critical systems, namely Fault Trees Analysis (FTA).

The talk shows that any Fault Tree (FT) can be directly mapped into a BN and that basic inference techniques on the latter may be used to obtain classical parameters computed from the former (i.e. reliability of the Top Event or of any sub-system, criticality of components, etc). Moreover, by using BN, some additional power can be obtained, both at the modeling and at the analysis level.

At the modeling level, several restrictive assumptions implicit in the FT methodology can be removed and various kinds of dependencies among components can be accommodated. In particular, while classical fault trees are essentially a binary formalism (i.e. dealing with binary events like 'component up' or 'component down'), Bayesian nets deals with multi-state variables, by allowing for example the modeling of different behavioral modes of a given system component. Moreover, while in FTA logical dependency between components can be only modeled through logical gates (AND/OR gates or similar), noisy probabilistic gates can be naturally introduced and modeled using a BN, as well as the incorporation in the model of *common cause failures*, *coverage* or similar dependencies.

At the analysis level, a general diagnostic analysis can be performed, by computing arbitrary posterior probabilities; this means that it is possible for instance to estimate the real criticality of a component, by asking for the posterior probability of its failure, given the the Top Event has occurred. Moreover, posterior analysis can provide what is called the Most Probable Explanation (MPE) of a fault, by providing the most probable configuration of system components given that a fault has occurred.

The above aspects will be presented by considering some real-world examples and applications ranging from the control of multiprocessor computer systems, to the analysis of the reliability of digital controllers (industrial PLCs, turbin control systems, etc...).

We will finally report on some work in progress concerning the use of formalisms extending BN to a parametric representation (particularly useful when modeling systems with several redundant components), as well as the use of Dynamic Bayesian Networks (DBN) when modeling so-called dynamic gates (e.g. spare gates, functional dependency, etc...).