Modeling and Analysis of Dependable Systems

A Probabilistic Graphical Model Perspective

This page intentionally left blank

Modeling and Analysis of Dependable Systems

A Probabilistic Graphical Model Perspective

Luigi Portinale
Daniele Codetta Raiteri

University of Piemonte Orientale, Italy

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

MODELING AND ANALYSIS OF DEPENDABLE SYSTEMS

A Probabilistic Graphical Model Perspective

Copyright © 2015 by World Scientific Publishing Co. Pte. Ltd.

All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the publisher.

For photocopying of material in this volume, please pay a copying fee through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA. In this case permission to photocopy is not required from the publisher.

ISBN 978-981-4612-03-6

Printed in Singapore

*To my father Domenico, who did not have the possibility of
viewing this book.*

*To Maura, Lorenzo and Gaia, who are definitely more
important than any book or paper: you have patiently tolerated
my busy time during the writing of this book. I owe you a debt
of gratitude.*

Luigi Portinale

To my family.

Daniele Codetta Raiteri

This page intentionally left blank

Preface

For many physical systems (e.g., computer systems, computer networks, industrial plants, etc.) one of the most important property is definitely the *system dependability*. Dependability is a property involving several different aspects concerning the behavior of a system, such as reliability, availability, safety and security among the others. The main perception when thinking about a dependable system is to consider a system that does not fail during its regular activity. From the point of view of a system user, it reflects the extent of his/her confidence that the system will operate as the user expects, and thus that it will not fail during normal use.

In fact, system failures are often unavoidable and they may have widespread effects, by affecting other systems, as well as people somewhat related to the system itself; this includes system operators, system users, but also people indirectly involved in the system environment (we can think for instance to the population living around a potentially dangerous plant). Systems that are not dependable are in fact unreliable, unavailable when needed, unsafe or insecure, and because of that, they may be rejected by their users. Moreover, cost issues must also be taken into account; if a failure leads to economic losses or physical damage, both direct failure impacts, as well as recovery costs have to be seriously considered.

If one wants to reason about all the above mentioned aspects, it is clear that formal models must be introduced. Such models have to be properly defined with respect to a system specification, since a failure (and all the consequences of that) is a deviation from a specification. However specifications can rarely be complete, as well as deterministic; thus a problem arising in building dependability models is the problem of uncertainty. It follows that some of the most relevant problems related to system dependability concern the representation and modeling of the system, the quantification

of system model parameters and the representation, propagation and quantification of the uncertainty in the system behavior.

Moreover, in order to address a concrete dependability problem, other important issues to be considered are: the temporal dimension, with particular attention to the modeling and analysis of temporal dependencies that can arise among system components, the multi-state nature of several components (that cannot be constrained in the standard dichotomy *working/failed*), the risk/utility analysis, often related to the definition of suitable control or recovery policies on the system under examination.

Classical approaches to dependability modeling and analysis show several limitations with respect to the above mentioned issues: combinatorial approaches (such as Fault Trees or Reliability Block Diagrams) are simple to use and analyze, but they are limited in modeling power; on the other hand, state-space approaches (such as Markov models) pay their augmented representational power, with more complex or less efficient analysis techniques (and with the state space explosion problem, typical of such models).

The main problem is then to define an approach where important dependencies among system components can be captured, while keeping the analysis task manageable at the same time. In the Artificial Intelligence (AI) field, similar problems have been addressed and solved by the adoption of Probabilistic Graphical Models. Model languages belonging to such a class are Bayesian Network and Decision Network formalisms. The former is a graphical and compact representation of a joint probability distribution, allowing to localize dependencies among modeled entities (system components or sub-systems in the case of a dependability application), and exploiting such dependencies, in order to reduce the number of probabilistic parameters to be specified. This results in a sound probabilistic model, relying on local specifications, where different kinds of probabilistic queries can be asked (in particular, posterior probability queries, after the gathering of specific information). Several important tasks for dependability analysis can be naturally framed in the setting of such probabilistic queries. Temporal aspects and dynamic dependencies can be addressed with dynamic versions of Bayesian Networks, having the advantage, with respect to standard Markov models, of considering a factored state space. Decision Networks are finally extensions to Bayesian Networks, where also external actions, as well as the utility of specific system conditions can be modeled. This allows the analyst to exploit a decision theoretic framework to perform risk/utility analysis, which is very important in the dependability field (as noticed above).

The aim of the book is to present approaches to the dependability (reliability, availability, risk and safety, security) of systems, using the Artificial Intelligence framework of Probabilistic Graphical Models. This framework (and in particular the Bayesian Network formalism) has been extensively employed in several sub-fields of AI which are strictly related to dependability and reliability issues, like diagnostic problem solving, intelligent monitoring and recovery planning.

After a survey on the main concepts and methodologies adopted in dependability analysis, the book discusses the main features of Probabilistic Graphical Models, by considering Bayesian Networks, Dynamic Bayesian Networks and Decision Networks. The advantages, both in terms of modeling and analysis, with respect to classical dependability formalisms are deeply discussed. Methodologies for deriving Probabilistic Graphical Models from standard dependability languages (such as Fault Tree or Dynamic Fault Tree) are introduced, by pointing out tools able to support such a process.

Several case studies are presented and analyzed in the book, in order to support the claim concerning the suitability of the use of Probabilistic Graphical Models in the study of dependable systems. Such case studies concentrates on different facets of the dependability concept, like standard reliability, dynamic reliability, selection of optimal repair policies, cascading failures, fault detection, identification and recovery, safety and security assessment. Some of such examples refer to real-world case studies, where the approach based on Probabilistic Graphical Models has proven to be very successful.

This book would not have come into existence without the direct or indirect contribution of several people, many of them part of the PROGRAM research lab at UPO¹. First of all, we are very indebted to *Andrea Bobbio*, who introduced us to the world of reliability and dependability; with his unique open mind, he pursued with us the vision that Probabilistic Graphical Models could have been a breakthrough for reliability and dependability engineers. Most of the work described in the present book is the result of a strict research collaboration with him.

We would also like to thank the various people who contributed to different parts of the work presented in the book, and in particular (in alphabetical order): *Ester Ciancamerla*, *Stefano Di Nolfo*, *Andrea Guiotto*,

¹PROGRAM: Probabilistic Graphical Models Research Group and Lab at the University of Piemonte Orientale, Alessandria, Italy (<http://www.di.unipmn.it/program>)

Helge Langseth, Michele Minichino, Stefania Montani, Roberta Terruggia, Marco Varesio, Yury Yusthein.

Last but not least, we are very grateful to *Steven Patt*, who has been our official interface at World Scientific Publishing. His help and support has been really appreciated.

L. Portinale and D. Codetta Raiteri
Alessandria, April, 2015

Luigi Portinale received a Ph.D. and a M.Sc. in Computer Science from the University of Torino (Italy). He is Full Professor of Computer Science and Head of the Computer Science Institute at the University of Piemonte Orientale (Italy). His main research interests are in the Artificial Intelligence field, with particular attention to case-based reasoning and probabilistic uncertain reasoning for dependability and reliability applications. He's author of more than 120 publications on the above topics. He's member of IEEE Computer Society, of the Italian Association for AI (AI*IA) and of the Association for the Advancement of AI (AAAI).

Daniele Codetta Raiteri received the Ph.D. in Computer Science from the University of Torino (Italy) in 2006. He is currently an assistant professor at the University of Piemonte Orientale (Italy). He works on probabilistic models for reliability analysis, with a particular experience in fault trees, Petri nets, Bayesian networks.

Contents

<i>Preface</i>	vii
<i>Acronym List</i>	xv
1. Dependability and Reliability	1
1.1 System Dependability: Basic Notions	1
1.1.1 Dependability evaluation	4
1.1.2 Measures of dependability	5
1.1.3 The probabilistic approach	6
1.2 Combinatorial Models	10
1.2.1 Fault Tree	10
1.2.2 Dynamic Fault Tree	23
1.3 State Space Models	28
1.3.1 Markov Chains	28
1.3.2 Petri Nets	29
2. Probabilistic Graphical Models	37
2.1 Bayesian Belief Networks	39
2.1.1 Conditional independence and factorization	42
2.1.2 Causal independence	44
2.1.3 Inference	45
2.2 Decision Networks	49
2.2.1 Policies and strategies	52
2.3 Dynamic Models	58
2.3.1 Inference in Dynamic Bayesian Networks	61
3. From Fault Trees to Bayesian Networks	69

3.1	Mapping Fault Trees to Bayesian Networks	70
3.2	Common Cause Failures	74
3.3	Noisy Gates	76
3.4	Coverage Factors	78
3.5	Multi-state Variables	78
3.6	Sequentially Dependent Failures	79
3.7	Dependability Analysis through BN Inference	81
4.	From Dynamic Fault Tree to Dynamic Bayesian Networks	87
4.1	Translating Dynamic Gates	88
4.1.1	Warm spare gate	88
4.1.2	Probabilistic dependency gate	92
4.1.3	Priority AND	95
4.2	Combining the Modules into a Single DBN	96
4.3	Modelling Repair	104
4.4	A Case-study Example	114
5.	Decision Theoretic Dependability	123
5.1	Decision Networks for Repairable Systems	124
5.2	A Repairable System	125
5.2.1	The Decision Network model	127
5.2.2	System unreliability and expected cost	129
5.2.3	Importance measures of components under given strategies	130
5.2.4	Computation of the best repair strategy	132
6.	The RADyBAN Tool: Supporting Dependability Engineers to Exploit Probabilistic Graphical Models	137
6.1	Tool Architecture	138
6.2	Editing a DFT	139
6.3	Editing a DBN	141
6.4	Compilation of a DFT into a DBN	142
6.5	Analyzing a DBN	142
7.	Case Study 1: Cascading Failures	145
7.1	Problem Introduction	145
7.2	Modeling Cascading Failures by Means of DBN	147
7.2.1	Building the DBN model	149

7.2.2	The cascading failure scenario	152
7.3	Quantitative Results	153
8.	Case Study 2: Autonomous Fault Detection, Identification and Recovery	157
8.1	Problem Introduction	157
8.2	The Testing Environment	159
8.3	Off-board Process	161
8.3.1	DFT model of the case study	162
8.3.2	DBN model of the case study	163
8.4	On-board Process	166
8.5	Testing ARPHA	169
9.	Case Study 3: Security Assessment in Critical Infrastructures	175
9.1	Problem Introduction	175
9.2	Attack Tree Based Formalisms	176
9.3	Decision Networks for Attack/Defense Scenarios	177
9.3.1	From Attack Countermeasure Trees to Decision Networks	178
9.3.2	Quantitative analysis	183
10.	Case Study 4: Dynamic Reliability	191
10.1	Problem Introduction	191
10.2	The Benchmark	192
10.2.1	Version 1: basic system	192
10.2.2	Version 2: state dependent failure rates	193
10.2.3	Version 3: controller failure on demand	194
10.2.4	Version 4: repairable components	194
10.3	Related Work	195
10.4	DBN Models of the Benchmark	196
10.4.1	Modelling Version 1	196
10.4.2	Modelling Versions 2 and 3	202
10.4.3	Modelling Version 4	202
10.5	DBN Analysis Results	205
10.5.1	Predictive analysis	205
10.5.2	Diagnostic analysis	206
Appendix A	The Junction Tree Algorithms	219

A.1	JT Algorithm for Static Bayesian Networks	219
A.1.1	Constructing the Junction/Join Tree	219
A.1.2	Belief Propagation on Junction Tree	223
A.2	JT Algorithm for Dynamic Bayesian Networks	226
A.2.1	The 1.5JT algorithm	227
A.2.2	The Boyen-Koller algorithm	232
<i>Bibliography</i>		235
<i>Index</i>		247

Acronym List

2-TBN	2 time-slice Temporal Bayesian Network
ABB	Autonomy Building Block
ACT	Attack Countermeasure Tree
ADT	Attack Defence Tree
ARPHA	Anomaly Resolution and Prognostic Health management for Autonomy
AT	Attack Tree
BDD	Binary Decision Diagram
BE	Basic Event
BGP	Border Gateway Protocol
BI	Birnbaum Index
BK	Boyer-Koller algorithm
BN	Bayesian Network
BP	Belief Propagation
CAS	Cardiac Assist System
cdf	cumulative distribution function
CCF	Common Cause Failure
CFR	Constant Failure Rate
CI	Causal Independence
CIF	Critical Importance Factor
Cov	Coverage set
CPT	Conditional Probability Table
CR	Component Repair
CSM	Combinatorial Solution Module
CSP	Cold SPare gate
CTMC	Continuous Time Markov Chain

DAG	Direct Acyclic Graph
DBN	Dynamic Bayesian Networks
DDN	Dynamic Decision Network
DDP	Defect, Detection and Prevention
DFR	Decreasing Failure Rate
DFT	Dynamic Fault Tree
DIF	Diagnostic Impact Factor
DN	Decision Network
DRBD	Dynamic Reliability Block Diagram
DTMC	Discrete Time Markov Chain
EDFT	Extended Dynamic Fault Tree
ET	Event Tree
EU	Expected Utility
FDEP	Functional DEPEndency gate
FDIR	Failure Detection, Identification and Recovery
FMEA	Failure Mode Effect Analysis
FSPN	Fluid Stochastic Petri Net
FT	Fault Tree
FTA	Fault Tree Analysis
FVI	Fussell-Vesely Index
GSPN	Generalized Stochastic Petri Net
GUI	Graphical User Interface
HBN	Hybrid Bayesian Network
HMM	Hidden Markov Model
HSP	Hot SPare gate
ID	Influence Diagram
IDPF	Inter-Domain Packet Filter
IE	Intermediate Event
IFR	Increasing Failure Rate
JT	Junction Tree
k:n	k out of n
LBP	Loopy Belief Propagation
LIMID	Limited Memory Influence Diagram
MAP	Maximum A Posteriori
MC	Markov Chain
MCMC	Markov Chain Monte Carlo
MCS	Minimal Cut Set
MCS _{Seq}	Minimal Cut Sequence

MDP	Markov Decision Process
MEC	Minimum Expected Cost
MEU	Maximum Expected Utility
MIF	Marginal Impact Factor
MPE	Most Probable Explanation
MPS	Minimal Path Set
MRF	Markov Random Field
MSP	Most Severe Prevailing
MTE	Mixture of Truncated Exponentials
MTTF	Mean Time to Failure
OD	Optical Depth
PAND	Priority AND gate
PDEP	Probabilistic DEpendency gate
PGM	Probabilistic Graphical Model
pdf	probability density function
PF	Particle Filtering
PN	Petri Net
PNL	Probabilistic Networks Library
POMPD	Partially Observable Markov Decision Process
PPTC	Probability Propagation in Trees of Clusters
PRA	Probabilistic Risk Analysis
PSS	Power Supply Subsystem
RAW	Risk Achievement Worth
RB	Repair Box
RBD	Reliability Block Diagram
RBPF	Rao-Blackwellised Particle Filtering
ROI	Return On Investment index
RRW	Risk Reduction Worth
SA	Solar Array
SAA	Sun Aspect Angle
SAN	Stochastic Activity Network
SEQ	SEquence enforcing gate
SGR	Subsystem Global Repair
SLR	Subsystem Local Repair
SIS	Sequential Importance Sampling
SPU	Single Policy Updating
SSM	State-space solution Module
TCP	Transfer Control Protocol

TE	Top Event
UML	Unified Modelling Language
VE	Variable Elimination
WSP	Warm SPare gate
XML	eXtensible Markup Language
XOR	eXclusive OR