



UvA-DARE (Digital Academic Repository)

Stochastic methods for measurement-based network control

Ellens, W.

[Link to publication](#)

Citation for published version (APA):

Ellens, W. (2015). Stochastic methods for measurement-based network control

General rights

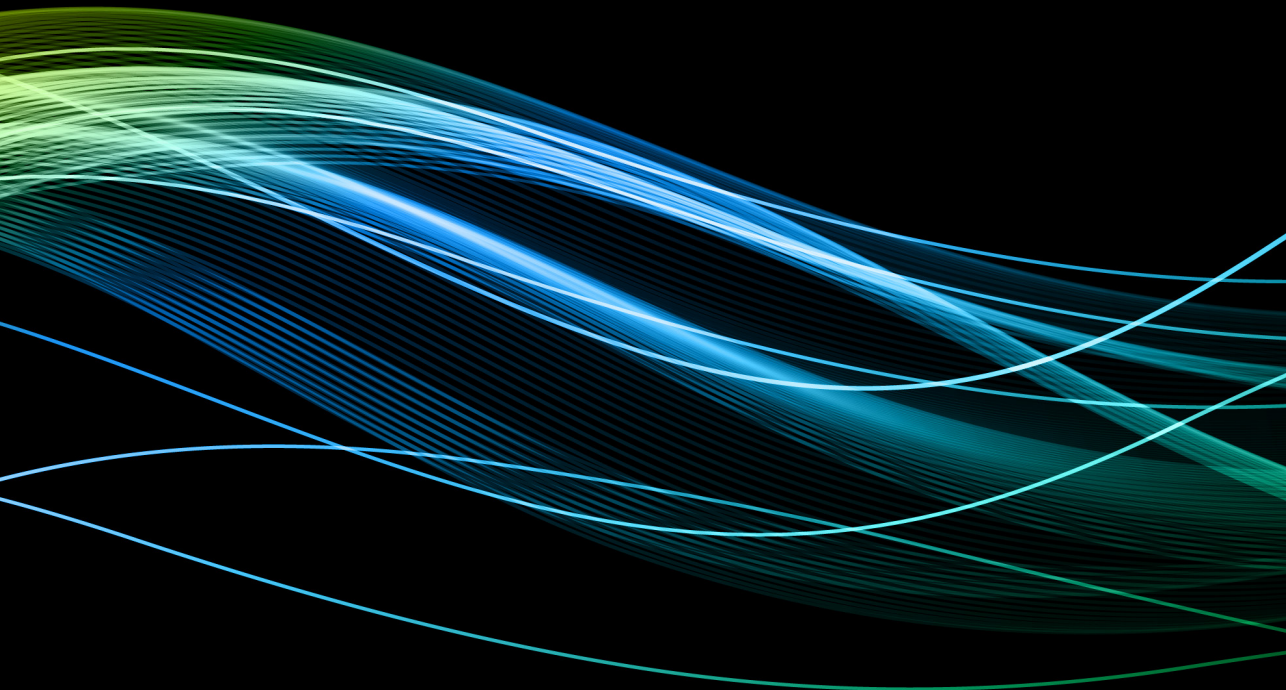
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <http://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

Stochastic Methods
for
Measurement-based Network Control

Wendy Ellens



Stochastic Methods
for
Measurement-based Network Control

Wendy Ellens
Korteweg-de Vries Instituut voor Wiskunde
Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Universiteit van Amsterdam

Printing: GVO drukkers & vormgevers
Cover illustration: Abstract dark wave background, BSG Studio

Copyright © 2015 Wendy Ellens. All rights reserved. No part of this publication may be reproduced, in any form or by any means, without permission in writing from the author.

Stochastic Methods
for
Measurement-based Network Control

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus prof. dr. D. C. van den Boom
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op donderdag 10 december 2015, te 14:00 uur

door

Wendy Ellens

geboren te Grijpskerk

Promotiecommissie

Promotores:	Prof. dr. M. R. H. Mandjes	Universiteit van Amsterdam
	Prof. dr. J. L. van den Berg	Universiteit Twente
Overige leden:	Prof. dr. G. M. Koole	Vrije Universiteit
	Dr. F. M. Spieksma	Universiteit Leiden
	Prof. dr. ir. R. E. Kooij	Technische Universiteit Delft
	Prof. dr. J. de Mast	Universiteit van Amsterdam
	Prof. dr. ir. C. T. A. M. de Laat	Universiteit van Amsterdam
	Prof. dr. R. Núñez-Queija	Universiteit van Amsterdam

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Acknowledgements

The work presented in this dissertation is the output of several fruitful collaborations while I was employed at consecutively the Dutch research institute TNO and the University of Amsterdam (UvA). More specifically, this dissertation is based on a series of papers that I have published together with peers from within and without these institutions.

- Chapter 2 is based on Section 4 of [1], which has been written in equal cooperation with Michel Mandjes (UvA) and Piotr Żuraniewski (TNO). Most of my efforts were focused on Sections 4.1, 4.2 and 4.5 of this publication.
- The major part of the contents of Chapter 3 and Chapter 4 have been taken from [2], which is a joint effort of Julia Kuhn (at that time a Master student at UvA and intern at TNO), Michel Mandjes and me. The work was based on earlier discussions between Michel and Piotr Żuraniewski. I have added the numerical results from [7], a paper written by Julia, under the supervision of Michel and me.
- The work described in Chapter 5 has been carried out within the Cyber Attack Detection (CAD) project, a project partially funded by the Dutch Ministry of Economic Affairs as part of the ‘Maatschappelijke Innovatie Agenda Veiligheid’ (IMV 1100032). The field experiment was performed by Anna Sperotto (University of Twente) and Harm Schotanus (TNO), the traffic flow analysis by Piotr Żuraniewski, Anna and me, guided by Erik Meeuwissen (TNO) and Michel Mandjes. I took the lead in writing the paper [3] that has led to this chapter.
- The results of Chapter 6 and Chapter 7 were earlier described in [6] and [4]. The former paper is an output of the TNO project CAMERA and reports results produced by Daniël Worm (TNO), Michel Mandjes and me, with the help of Hans van den Berg (TNO and University of Twente). The latter paper has extended the former by adding further theory and numerical results produced by Daniël, Michel, me and our Master student Sylwester Błaszczuk.

Acknowledgements

- Chapter 8 corresponds to [5], a paper with Peter Kovács (UvA), Sindo Núñez-Queija (UvA) and Hans van den Berg. Most of my effort has gone into Sections 2, 3 and 5 of this paper and the overall coordination, while Peter and Sindo took the lead in Section 4.

I wish to thank all the people I worked with in the past years — especially my supervisors (‘promotores’) Michel Mandjes and Hans van den Berg — as well as everyone who supported me during my time as a researcher at TNO and, after that, as a PhD candidate at UvA.

Wendy Ellens

Delft, 20 August 2015

Contents

	Page
<i>Acknowledgements</i>	v
1 Introduction	1
1.1 The research field	2
1.2 Applications	4
1.3 Methodological background	7
1.4 Contribution	12
1.5 Organisation of this dissertation	17
Part I Methods for change point detection	21
2 A review of some existing methods	23
2.1 The change point detection problem	24
2.1.1 Problem description	24
2.1.2 Performance metrics	25
2.2 A parametric method	26
2.2.1 The CUSUM method	26
2.2.2 Large deviations approximation of CUSUM	30
2.3 Two non-parametric methods	32
2.3.1 A non-parametric version of CUSUM	32
2.3.2 The method of Brodsky-Darkhovsky	33
2.4 Conclusion	34
3 New methods for sequences of dependent data	37
3.1 Likelihood ratio test for multivariate normal data	38
3.2 Extensions of CUSUM	42
3.2.1 Method I: change in mean for dependent data	43
3.2.2 Method II: change in variance for independent data	46
3.2.3 Method III: change in scale for dependent data	47
3.3 Conclusion	50

4	Numerical evaluation of the new methods	51
4.1	Method I: change in mean	52
4.1.1	Experiment design	52
4.1.2	Results: alarm rate	54
4.1.3	Results: detection delay	58
4.1.4	Sensitivity analysis	60
4.2	Method III: change in scale	63
4.2.1	Experiment design	63
4.2.2	Results	64
4.2.3	Multidimensional detection methods	66
4.3	Conclusion	68
5	A cyber attack detection application	69
5.1	DNS tunnel attacks	70
5.2	Experiment design	71
5.3	Analysis of the experiments	74
5.4	Proposal of detection methods	77
5.5	Evaluation of the detection methods	80
5.6	Conclusion	82
Part II Partially observable queueing systems		83
6	Behaviour between periodic system-state measurements	85
6.1	Probability to stay below a certain level	86
6.2	Time, area and arrivals above a certain level	92
6.3	Conclusion	98
7	Numerical results for a periodically observed queue	101
7.1	The queueing model	102
7.2	Numerical evaluation of the four metrics	103
7.3	Illustration of practical use	108
7.4	Conclusion	109
7.5	Appendix: limits for small time-scales	111
8	Routing under partial observability and controllability	115
8.1	Model	116
8.1.1	The queueing system	116

8.1.2	Routing policies	117
8.2	Simulations	120
8.2.1	Policy comparison	121
8.2.2	The penetration level	124
8.3	Fluid model approximation	126
8.3.1	Description of the setting	127
8.3.2	Introduction and analysis of the model	128
8.3.3	Numerical verification	131
8.4	Conclusion	134
	<i>Summary</i>	137
	<i>Samenvatting</i>	141
	<i>About the author</i>	145
	<i>Publications of the author</i>	147
	<i>References</i>	149
	<i>Index</i>	157