Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zürich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7411>

Steven Latré · Marinos Charalambides
Jérôme François · Corinna Schmitt
Burkhard Stiller (Eds.)

Intelligent Mechanisms for Network Configuration and Security

9th IFIP WG 6.6 International Conference
on Autonomous Infrastructure,
Management, and Security, AIMS 2015
Ghent, Belgium, June 22–25, 2015
Proceedings

Editors

Steven Latré
Universiteit Antwerp
Antwerp
Belgium

Corinna Schmitt
Universität Zürich
Zürich
Switzerland

Marinos Charalambides
University College London
London
UK

Burkhard Stiller
Universität Zürich
Zürich
Switzerland

Jérôme François
Inria Nancy Grand Est
Villers-lès-Nancy
France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-20033-0

ISBN 978-3-319-20034-7 (eBook)

DOI 10.1007/978-3-319-20034-7

Library of Congress Control Number: 2015940762

LNCS Sublibrary: SL5 – Computer Communication Networks and Telecommunications

Springer Cham Heidelberg New York Dordrecht London

© IFIP International Federation for Information Processing 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

The International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2015) is a single-track event integrating regular conference paper sessions, tutorials, keynotes, and a PhD student workshop into a highly interactive event. Within the network and service management community, AIMS is focused on PhD students and young researchers. One of the key goals of AIMS is to provide early-stage researchers with constructive feedback by senior scientists and give them the possibility to grow in the research community by means of targeted lab sessions on technical and educational aspects of the research activity. This focus on early-stage researchers is immediately observable in the program, featuring a high number of educational sessions and PhD sessions, where young PhD students present their research.

AIMS 2015 – which took place during June 22–25, 2015, in Ghent, Belgium, and was hosted by Ghent University and iMinds – was the ninth edition of a conference series on management and security aspects of distributed and autonomous systems. It followed the already established tradition of an unusually vivid and interactive conference series, after successful events in Brno, Czech Republic in 2014, Barcelona, Spain in 2013, Luxembourg, Luxembourg in 2012, Nancy, France in 2011, Zürich, Switzerland in 2010, Enschede, The Netherlands in 2009, Bremen, Germany in 2008, and Oslo, Norway in 2007.

This year, AIMS 2015 focused on intelligent mechanisms for network configuration and security. This theme is addressed in the technical program with papers related to monitoring, security, and management methodologies in the application areas of wired and wireless networks, Internet-of-Things, and Cloud infrastructures. AIMS 2015 was organized as a 4-day program to encourage the interaction with and the active participation of the conference’s audience. The program consisted of technical sessions for the main track and PhD sessions, interleaved with a research and an educational keynote and three lab sessions.

The lab sessions offered hands-on experience in network and service management topics and they were organized in on-site labs preceded by short tutorial-style teaching sessions. The first tutorial presented the Hadoop framework, explaining common design patterns and how to program using the MapReduce paradigm. The second tutorial covered the topic of deploying Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) on large-scale test-bed facilities. Finally, the third tutorial focused on indexing, searching, and visualizing management tools.

In line with its educational mission, this year the conference also included an educational keynote, which was given by Piet Demeester (Ghent University, iMinds, Belgium) on “Providing Tips and Tricks for Young Researchers” advancing in their PhD career. Additionally, AIMS 2015 featured a research keynote on the “Management of Big Data: The Areas of Conflict” provided by Burkhard Stiller (University of Zürich, Switzerland).

The technical program consisted of two sessions – covering the topics of autonomic and decentralized management, and security, privacy, and management – and included seven full papers, which were selected after a thorough reviewing process out of a total of 22 submissions. Each paper received at least three independent reviews.

The AIMS PhD workshop is a venue for doctoral students to present and discuss their research ideas, and more importantly to obtain valuable feedback from the AIMS audience about their planned PhD research work. This year, the workshop was structured into two technical sessions covering the management of future networks and security management. All PhD papers included in this volume describe the current state of these investigations, including their clear research problem statements, proposed approaches, and an outline of results achieved so far. A total of nine PhD papers were presented and discussed. These papers were selected after a separate review process out of 24 submissions, while all PhD papers received at least three independent reviews, too.

The present volume of the *Lecture Notes in Computer Science* series includes all papers presented at AIMS 2015 as defined within the overall final program. It demonstrates again the European scope of this conference series, since most of the accepted papers originate from European research groups. Also, AIMS 2015 has proven true to its defined DNA of a conference with a strong educational goal, as indicated by the high number of submissions attracted by the PhD Workshop.

The editors would like to thank the many people who helped make AIMS 2015 such a high-quality and successful event. Firstly, many thanks are addressed to all authors, who submitted their contributions to AIMS 2015, and to the lab session speakers, namely, Jérôme François, Niels Bouten, Rachid Mijumbi, Abdelkader Lahmadi, and Frederick Beck, and the keynote speakers Piet Demeester and Burkhard Stiller. The great review work performed by the members of both the AIMS Technical Program Committee and the PhD Student Workshop Committee as well as additional reviewers is highly acknowledged. Thanks are addressed also to Ricardo Schmidt and Tim Wauters for setting up and organizing the lab sessions. Additionally, many thanks are addressed to the local organizers for enabling all logistics and hosting the AIMS 2015 event.

Finally, the editors would like to express their thanks to Springer, and in particular Anna Kramer, for the smooth cooperation in finalizing these proceedings. Additionally, special thanks go to the AIMS 2015 supporters, Ghent University, iMinds, and the European FP7 NoE FLAMINGO under Grant No. 318488.

April 2015

Steven Latré
Marinos Charalambides
Jérôme François
Corinna Schmitt

NoE FLAMINGO

Organization

General Co-chairs

Filip De Turck
Piet Demeester

Ghent University, iMinds, Belgium
Ghent University, iMinds, Belgium

Technical Program Committee Co-chairs

Steven Latré
Marinos Charalambides

University of Antwerp, iMinds, Belgium
University College London, UK

PhD Student Workshop Co-chairs

Jérôme François
Corinna Schmitt

Inria Grand Est Nancy, France
University of Zürich, Switzerland

Labs Co-chairs

Ricardo Schmidt
Tim Wauters

University of Twente, The Netherlands
Ghent University, iMinds, Belgium

Publications Chair

Burkhard Stiller

University of Zürich, Switzerland

Local Chair

Peter Van Daele

Ghent University, iMinds, Belgium

AIMS Steering Committee

Ramin Sadre
Guillaume Doyen
Anna Sperotto
Pavel Čeleda
David Hausheer
Aiko Pras
Burkhard Stiller

Université Catholique de Louvain, Belgium
Troyes University of Technology, France
University of Twente, The Netherlands
Masaryk University, Czech Republic
Technical University Darmstadt, Germany
University of Twente, The Netherlands
University of Zürich, Switzerland

Technical Program Committee

Alessandro Finamore	Politecnico di Torino, Italy
Alexander Clemm	Cisco Systems, USA
Alexander Keller	IBM Global Technology Services, USA
Alva L. Couch	Tufts University, USA
Anandha Gopalan	Imperial College London, UK
Anna Sperotto	University of Twente, The Netherlands
Bertrand Mathieu	Orange Labs, France
Bruno Quoitin	Université de Mons, Belgium
Daniele Sgandurra	Imperial College London, UK
Danny Raz	Technion, Israel
David Hausheer	Technical University Darmstadt, Germany
Gabi Dreö Rodosek	University of Federal Armed Forces Munich, Germany
Grégory Bonnet	University of Caen Lower Normandy, France
Guillaume Doyen	Troyes University of Technology, France
Isabelle Chrisment	TELECOM Nancy, Université de Lorraine, France
Jan Kořenek	Brno University of Technology, Czech Republic
Jürgen Schönwälder	Jacobs University Bremen, Germany
Kurt Tutschku	Blekinge Institute of Technology, Sweden
Lisandro Zambenedetti Granville	UFRGS, Brazil
Mauro Tortonesi	University of Ferrara, Italy
Michelle Sibilla	Paul Sabatier University, France
Olivier Festor	Telecom Nancy, University of Lorraine, France
Philippe Owezarski	LAAS-CNRS, France
Piotr Cholda	AGH University of Science and Technology, Poland
Ramin Sadre	Université Catholique de Louvain, Belgium
Remi Badonnel	Inria, TELECOM Nancy, Université de Lorraine, France
Thomas Bocek	University of Zürich, Switzerland

PhD Student Workshop Committee

Aiko Pras	University of Twente, The Netherlands
Alberto Schaeffer-Filho	UFRGS, Brazil
Bradley Simmons	Independent Researcher, Canada
Clarissa Marquezan	Huawei European Research Center, Germany
Desislava Dimitrova	University of Bern, Switzerland
Dimitrios Pezaros	University of Glasgow, UK
Jan Vykopal	Masaryk University, Czech Republic
Jeroen Famaey	University of Antwerp, iMinds, Belgium

Joan Serrat	Universitat Politècnica de Catalunya, Spain
Kostas Tsagkaris	University of Piraeus, Greece
Lefteris Mamatras	University College London, UK
Maxwell Young	Drexel University, USA
Paulo Simoes	University of Coimbra, Portugal
Pavel Čeleda	Masaryk University, Czech Republic
Steven Davy	Waterford Institute of Technology, Ireland
Stylianios Georgoulas	University of Surrey, UK
Sven van der Meer	Ericsson, Ireland
Thibault Cholez	Inria Nancy Grand Est, France

Additional Reviewers

Detailed reviews for papers submitted to AIMS 2015 were carried out by the Technical Program Committee as well as the PhD Student Workshop Committee as listed in the previous sections and additionally by the following reviewers:

Alain Ploix	Mattijs Jonker
Bart Braem	Patrick Truong
Christian Koch	Radek Fujdiak
Christos Tsiaras	Radhika Garg
José Jair Santanna	Remi Cогranne
Lautaro Dolberg	Theoni Petropoulou
Martin Vizváry	Vassilis Foteinos

Keynotes

Educational Keynote

Current Trends in Network Research and Advice for Young Researchers

Piet Demeester

Ghent University, iMinds, Belgium
`piet.demeester@intec.ugent.be`

Abstract. Based on his 30 year of experience in research, this talk will provide a viewpoint on current and important challenges in network-related research. Addressed topics will include wireless networks, Internet-of-Things, Software-defined Networks (SDN), and Network Function Virtualization (NFV): the current status and future perspectives will be addressed. In addition, the importance of Future Internet Research Infrastructures will be stressed and examples will be given of current experimental research facilities.

Furthermore, based on extensive research experience, advice will be provided for young researchers, who want to pursue either an academic career or a career in industry.

Research Keynote

Management of Big Data — The Areas of Conflict: Data Volume, Analysis Methods, and Protection

Burkhard Stiller

Communication Systems Group CSG@IfI
University of Zürich, Zürich, Switzerland
stiller@ifi.uzh.ch

Abstract. In the past decades Information and Communication Technology (ICT) did not only change radically interaction patterns between humans and machines, ICT did more recently enable the support of such enormous Big Data sourcing, especially in terms of volumes transferred, distribution across various distances, and remote correlations of distinct data sets. To an undreamt scale, numbers, facts, and data streams (a) put the challenge onto existing storage architectures, (b) push well-known analysis and data mining methods to and beyond their limits, and (c) result in a major worry to data protection demands. However, without the knowledge of a suitable theory or even a very basic insight into fundamental and coherent relationships of such data, data patterns and data correlations will remain purely random.

Thus, this keynote will introduce and partially define the term “Big Data”, it will discuss the embedding of Big Data into today’s society, and will work out key details of the Big Data management dimension, driven by selected examples, which face a diversity of opportunities and risks.

Due to the fact that traditional and technical constraints of ICT are today oversteered by emerging economic and security-related perspectives, large data sets — by now commonly termed as Big Data — outline a broad set of challenges in terms of (a) the identity protection of the individual or selected single data items, (b) the statistical validity of analysis methods, and (c) the raise and effect of initially unknown or unintended meta data becoming part of a new analysis. All approaches technically doable today may be ethically questionable, although legally justifiable, since suitable privacy laws are not in place yet. Finally, by taking a look into the future, a picture is crafted carefully consisting of current trends and visions, which offer opportunities for the development of new big data management mechanisms.

Lab Sessions

Lab Session 1

Map-Reduce and Hadoop

Jérôme François

Inria Grand Est Nancy, France
`jerome.francois@inria.fr`

Abstract. This tutorial introduces Hadoop and how it can be applied to different challenges today's community is facing in network management. Data analytics is, thus, the focus of this tutorial as networks are producing tons of various logs, for example network traffic measures, firewall alerts, or SNMP messages. They form the basis of many management functions, which may necessitate basic processing like accounting or more complex calculations in particular for providing predictions on the future for (a) configuration purposes, (b) detecting security anomalies, or (c) supporting fault management.

This lab session introduces the Map-Reduce paradigm before explaining how to implement a program for Hadoop. Common programming patterns (join, filter, aggregation) are presented using short examples. Usual problems are discussed also, for example sorting or optimizing and chaining multiple tasks. Finally, the lab session presents Hadoop extensions like Pig for writing requests without any programming needs.

Lab Session 2

Deploying Network Function Virtualization Experiments on the Virtual Wall Test-Bed

Niels Bouten¹ and Rashid Mijumbi²

¹ Ghent University, iMinds, Belgium

² Universitat Politècnica de Catalunya, Spain

`niels.bouten@intec.ugent.be`, `rashid@tsc.upc.edu`

Abstract. Network Function Virtualization (NFV) takes advantage of IT virtualization technologies and network programming to virtualize physical network functions (e.g., firewall, NAT, and DHCP) and interconnect them to create new communication services. This allows service providers to create new communication services on top of existing network and datacenter infrastructure enabling shorter time-to-market at lower cost. Combining IT virtualization and Software-defined Networking (SDN) technologies allows NFV to increase greatly the network management flexibility by decoupling network functions from physical machines and by decoupling the control plane from traffic forwarding in network equipment.

The goal of this hands-on tutorial is to familiarize all participants with the concept of NFV in general and possible benefits of combining it with SDN. This will be accomplished by deploying several network functions on the Virtual Wall and interconnecting them using OpenFlow. This allows for the creation of individual Service Function Chains (SFC) for different users.

These experiments will be run in a live network setting, facilitated by the Virtual Wall test-bed. The Virtual Wall is a test-bed facility for setting up large-scale network topologies. Its nodes can be assigned different functionality and organized in arbitrary network topologies on the fly. As such, it is a generic experimental environment for advanced network, distributed software and service evaluation, and supports scalability research. The facility has been made available to the research community through different FP7 FIRE projects. This tutorial will provide, too, a brief theoretical introduction about the Virtual Wall's capabilities in preparation of the hands-on part. By using the jFed framework for test-bed federation, experiments on the Virtual Wall will be set-up.

Lab Session 3

Powering Monitoring Analytics with ELK Stack

Abdelkader Lahmadi¹ and Frederick Beck²

¹ University of Lorraine, France

² INRIA Nancy, France

`abdelkader.lahmadi@loria.fr, frederic.beck@inria.fr`

Abstract. Machine-generated data, including logs and network flows, are considerably growing and their collection, searching, and visualization is a challenging task for (a) daily administrator activities and (b) researchers aiming to better find out analytics and insights from monitoring data regarding their research goals, including amongst others security or modeling of network and systems.

This lab session introduces the open source ELK stack and its components, including Elasticsearch for deep search and data analytics, Logstash for centralized logging, log enrichment, and parsing, and Kibana for powerful and beautiful data visualizations. ELK enables the analysis and visualization of monitoring data, such as logs and netflows. A first step details these individual components and the second step provides guidelines for their deployment and configuration. In the third step participants will perform hands-on practical work for collecting, processing, and enriching logs and netflows, combined with the creation of associated visualization and dashboards aspects.

Contents

Autonomic and Decentralized Management

Disruption-Free Link Wake-Up Optimisation for Energy Aware Networks	3
<i>Obinna Okonor, Ning Wang, Zhili Sun, and Stylianos Georgoulas</i>	
Towards the Description and Execution of Transitions in Networked Systems	17
<i>Alexander Frömmgen, Björn Richerzhagen, Julius Rückert, David Hausheer, Ralf Steinmetz, and Alejandro Buchmann</i>	
A Network-Driven Multi-Access-Point Load-Balancing Algorithm for Large-Scale Public Hotspots	30
<i>Patrick Bosch, Bart Braem, and Steven Latré</i>	

Ph.D. Student Workshop — Management of Future Networking

SON Mechanism for Green Heterogeneous Cellular Networks	45
<i>Luis Alejandro Fletscher, Catalina Valencia, and Juan Felipe Botero</i>	
QoE-Centric Management of Advanced Multimedia Services	50
<i>Stefano Petrangeli and Filip De Turck</i>	
Exploring IoT protocols Through the Information-Centric Networking's Lens	56
<i>Salvatore Signorello, Radu State, and Olivier Festor</i>	
Towards a Fluid Cloud: An Extension of the Cloud into the Local Network	61
<i>Bart Spinnewyn and Steven Latré</i>	
Measuring and Modeling Multipath TCP	66
<i>Viet-Hoang Tran, Ramin Sadre, and Olivier Bonaventure</i>	

Security, Privacy, and Measurements

Learning to Detect Network Intrusion from a Few Labeled Events and Background Traffic	73
<i>Gustav Šourek, Ondřej Kuželka, and Filip Železný</i>	

Using Application-Aware Flow Monitoring for SIP Fraud Detection	87
<i>Tomas Cejka, Vaclav Bartos, Lukas Truxa, and Hana Kubatova</i>	
Schengen Routing: A Compliance Analysis	100
<i>Daniel Dönni, Guilherme Sperb Machado, Christos Tsiaras, and Burkhard Stiller</i>	
How Asymmetric Is the Internet?	
A Study to Support the Use of Traceroute	113
<i>Wouter de Vries, José Jair Santanna, Anna Sperotto, and Aiko Pras</i>	

Ph.D. Student Workshop — Security Management

Mitigating DDoS Attacks Using OpenFlow-Based Software Defined Networking	129
<i>Mattijs Jonker and Anna Sperotto</i>	
Towards an Adaptive and Effective IDS Using OpenFlow	134
<i>Sebastian Seeber and Gabi Dreo Rodosek</i>	
Towards a Cyber-Physical Resilience Framework for Smart Grids	140
<i>Ivo Friedberg, Kieran McLaughlin, and Paul Smith</i>	
Characterizing the IPv6 Security Landscape by Large-Scale Measurements	145
<i>Luuk Hendriks, Anna Sperotto, and Aiko Pras</i>	
Author Index	151