# Lecture Notes in Computer Science 5537

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Maria Papadopouli   Philippe Owezarski
Aiko Pras (Eds.)

# Traffic Monitoring and Analysis

First International Workshop, TMA 2009
Aachen, Germany, May 11, 2009
Proceedings

Springer

Volume Editors

Maria Papadopouli
University of Crete, Dept. of Computer Science
P.O. Box 2208, 714 09, Heraklion, Crete, Greece
and
F.O.R.T.H., Institute of Computer Science
Vassilika Vouton, P.O. Box 1385, 711 10, Heraklion, Greece
E-mail: mgp@ics.forth.gr

Philippe Owezarski
LAAS – CNRS
7 Avenue du Colonel Roche, 31077 Toulouse, cedex 4, France
E-mail: owe@laas.fr

Aiko Pras
University of Twente
Dept. of Electrical Engineering, Mathematics and Computer Science
Design and Analysis of Communication Systems Group
P.O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: a.pras@utwente.nl

Library of Congress Control Number: Applied for

CR Subject Classification (1998): C.2, D.4.4, H.3, H.4

LNCS Sublibrary: SL 5 – Computer Communication Networks and
Telecommunications

ISSN 0302-9743
ISBN-10 3-642-01644-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-01644-8 Springer Berlin Heidelberg New York

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12672158 06/3180 5 4 3 2 1 0

# Foreword

The First International Workshop on Traffic Monitoring and Analysis (TMA 2009) was an initiative from the COST Action IC0703 "Data Traffic Monitoring and Analysis: Theory, Techniques, Tools and Applications for the Future Networks" (www.cost-tma.eu).

The COST program is an intergovernmental framework for European Cooperation in Science and Technology, allowing the coordination of nationally funded research on a European level. Each COST Action contributes to reducing the fragmentation in research and opening the European Research Area to cooperation worldwide.

Traffic monitoring and analysis (TMA) is now an important research topic within the field of networking. It involves many research groups worldwide that are collectively advancing our understanding of the Internet.

The importance of TMA research is motivated by the fact that modern packet networks are highly complex and ever-evolving objects. Understanding, developing and managing such environments is difficult and expensive in practice. Traffic monitoring is a key methodology for understanding telecommunication technology and improving its operation, and the recent advances in this field suggest that evolved TMA-based techniques can play a key role in the operation of real networks. Moreover, TMA offers a basis for prevention and response in network security, as typically the detection of attacks and intrusions requires the analysis of detailed traffic records.

On the more theoretical side, TMA is an attractive research topic for many reasons. First, the inherent complexity of the Internet has attracted many researchers to face traffic measurements since the pioneering times. Second, TMA offers a fertile ground for theoretical and cross-disciplinary research—think of the various analysis techniques being imported into TMA from other fields—while at the same time providing a clear perspective for the exploitation of the results in real network environments. In other words, TMA research has the potential to reconcile theoretical investigations with practical applications, and to realign curiosity-driven with problem-driven research.

In the spirit of the COST program, the COST-TMA Action was launched in 2008 to promote building a research community in the specific field of TMA. Today, it involves 50+ research groups from academic and industrial organizations in 23 countries. In its first year the Action promoted a number of research exchanges mostly involving young researchers. A portal dedicated to TMA research is being set in place which aims at becoming a reference point for the research community in the field, in Europe and beyond (www.tma-portal.eu).

The TMA 2009 workshop marked an important moment in the lifetime of the (still young!) COST-TMA Action. The success of this first workshop—witnessed by the number of submissions and quality of the presented works—is very promising about the future development of the TMA workshop series into one of the reference venues for the larger research community in this field.

March 2009 Fabio Ricciato

# Preface

The First International Workshop on Traffic Monitoring and Analysis (TMA 2009) was an initiative from the COST Action IC0703 "Data Traffic Monitoring and Analysis (TMA): Theory, Techniques, Tools and Applications for the Future Networks" granted by the European Commission.

This TMA workshop extends the COST-TMA research and discussions to the world-wide community of researchers in the area of traffic monitoring and analysis. For this purpose, the TMA 2009 technical Program Committee selected the best papers submitted to the TMA 2009 workshop. Specifically, 15 out of the 34 submitted papers were accepted for publication in the workshop proceedings and were presented during a full-day event. They encompass research areas related to traffic analysis and classification, measurements, topology discovery, detection of specific applications and events, packet inspection, and traffic inference. In order to grant a long life and a high-visibility level to the TMA workshop, the proceedings of the TMA 2009 workshop are published by Springer in the LNCS series.

We address our sincere thanks to the technical Program Committee members for their diligence and hard work during the reviewing process, as well as to Springer for accepting to be the TMA workshop series publisher.

We are also very thankful to Michel Mandjes from CWI in The Netherlands, who accepted to give the keynote talk of this workshop on "Traffic Models, and Their Use in Provisioning and Traffic Management."

This year, the workshop was organized as a full-day event on the first day of the IFIP Networking conference. We would like to thank its organizers and patrons for accepting the TMA workshop as a joint event. In particular, we are grateful to Otto Spaniol for his generous support while preparing the workshop.

We hope you enjoy the proceedings.

March 2009

Maria Papadopouli
Philippe Owezarski
Aiko Pras
Udo Krieger

# Organization

## Technical Program Committee

| | |
|---|---|
| Pierre Borgnat | ENS Lyon |
| Prosper Chemouil | France Telecom R&D |
| Jean-Laurent Costeux | France Telecom R&D |
| Xenofontas Dimitropoulos | ETH Zurich |
| Constantine Dovrolis | Georgia Tech |
| Michalis Faloutsos | University of California at Riverside |
| Timur Friedman | UPMC Paris University and CNRS |
| Nuno M. Garcia | CICANT, ULHT, Lisbon, Portugal |
| James Hong | Postech Korea |
| Gianluca Iannaccone | Intel Research Berkeley |
| Lucjan Janowski | AGH University of Science and Technology |
| Merkourios Karaliopoulos | ETH Zurich |
| Jasleen Kaur | University of North Carolina at Chapel Hill |
| Evangelos Markatos | University of Crete and FORTH |
| Sandor Molnar | Budapest University of Technology and Economics |
| Jordi Domingo-Pascual | Universitat Politècnica de Catalunya |
| Kostas Pentikousis | VTT Technical Research Centre of Finland |
| Fabio Ricciato | University of Salento |
| Dario Rossi | ENST Telecom Paris |
| Luca Salgarelli | University of Brescia |
| Kave Salamatian | Lancaster University |
| Don Smith | University of North Carolina at Chapel Hill |
| Tanja Tzeby | Fraunhofer FOKUS |
| Steve Uhlig | T-labs/TU Berlin |
| Artur Ziviani | LNCC Brazil |

## Local Organizer

| | |
|---|---|
| Udo Krieger | Otto Friedrich University Bamberg |

## Technical Program Committee Co-chairs

| | |
|---|---|
| Philippe Owezarski | LAAS-CNRS, National Centre for Scientific Research |
| Maria Papadopouli | University of Crete and FORTH |
| Aiko Pras | University of Twente |

# Table of Contents

## QoS Measurement

## Rupture Detection

## Traffic Classification

## Traffic Analysis and Topology Measurements