

Studies in Computational Intelligence

Volume 565

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series “Studies in Computational Intelligence” (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

More information about this series at <http://www.springer.com/series/7092>

Elias Kyriakides · Marios Polycarpou
Editors

Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems

 Springer

Editors

Elias Kyriakides
Marios Polycarpou
KIOS Research Center for Intelligent
Systems and Networks
Department of Electrical and Computer
Engineering
University of Cyprus
Nicosia
Cyprus

Legal notice by COST Office

Neither the COST Office nor any person acting on its behalf is responsible for the use which might be made of the information contained in this publication. The COST Office is not responsible for the external websites referred to in this publication.

ISSN 1860-949X

ISSN 1860-9503 (electronic)

ISBN 978-3-662-44159-6

ISBN 978-3-662-44160-2 (eBook)

DOI 10.1007/978-3-662-44160-2

Library of Congress Control Number: 2014948739

Springer Heidelberg New York Dordrecht London

© Springer-Verlag Berlin Heidelberg 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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

COST Information

COST—the acronym for European Cooperation in Science and Technology—is the oldest and widest European intergovernmental network for cooperation in research. Established by the Ministerial Conference in November 1971, COST is presently used by the scientific communities of 35 European countries to cooperate in common research projects supported by national funds.

The funds provided by COST—less than 1% of the total value of the projects—support the COST cooperation networks (COST Actions) through which, with €30 million per year, more than 30,000 European scientists are involved in research having a total value which exceeds €2 billion per year. This is the financial worth of the European added value which COST achieves.

A “bottom up approach” (the initiative of launching a COST Action comes from the European scientists themselves), “à la carte participation” (only countries interested in the Action participate), “equality of access” (participation is open also to the scientific communities of countries not belonging to the European Union) and “flexible structure” (easy implementation and light management of the research initiatives) are the main characteristics of COST.

As a precursor of advanced multidisciplinary research COST has a very important role for the realization of the European Research Area (ERA) anticipating and complementing the activities of the Framework Programs, constituting a “bridge” toward the scientific communities of emerging countries, increasing the mobility of researchers across Europe, and fostering the establishment of “Networks of Excellence” in many key scientific domains such as: Biomedicine and Molecular Biosciences; Food and Agriculture; Forests, their Products and Services; Materials, Physical and Nanosciences; Chemistry and Molecular Sciences and Technologies; Earth System Science and Environmental Management; Information and Communication Technologies; Transport and Urban Development; Individuals, Societies, Cultures and Health. It covers basic and more applied research and also addresses issues of pre-normative nature or of societal importance.

Web: <http://www.cost.eu>

Preface

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed *Critical Infrastructure Systems*. Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, health, security services, and oil/natural gas pipelines. Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures.

The citizens expect that critical infrastructure systems will always be available, 24 hours a day, 7 days a week, and at the same time, they will be managed efficiently so that the services are provided at a low cost. Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic. For example, if a large geographical area experiences a blackout for an extended period of time, that may result in huge economic costs, as well as societal costs. In November 2006, a local fault in Germany's power grid cascaded through large areas of Europe, resulting in 10 million people left in the dark in Germany, France, Austria, Italy, Belgium, and Spain. Severe cascading blackouts have taken place in North America as well. Similarly, there may be significant health hazards when there is a serious fault in the water supply, especially if it is not detected and accommodated quickly. When the telecommunication networks are down, many businesses can no longer operate. In the case of faults or unexpected events in transportation systems, we witness the effect of traffic congestion quite often in metropolitan areas of Europe and around the world. In general, failures in critical infrastructure systems are low probability events, which however may have a huge impact on everyday life and well-being.

Technological advances in sensing devices, real-time computation and the development of intelligent systems, have instigated the need to improve the

performance of critical infrastructure systems in terms of security, accuracy, efficiency, reliability, and fault tolerance. Consequently, there is a strong effort in developing new algorithms for monitoring, control, and security of critical infrastructure systems, typically based on computational intelligence techniques and the real time processing of data received by networked embedded systems and sensor/actuator networks, dispersed throughout the system. Depending on the application, such data may have different characteristics: multidimensional, multiscale, spatially distributed, time series, event-triggered, etc. Furthermore, the data values may be influenced by controlled variables, as well as by external environmental factors. However, in some cases the collected data may be incomplete, or it may be faulty due to sensing or communication problems, thus compromising the sensor-environment interaction and possibly affecting the ability to manage and control key variables of the environment.

Despite the technological advances in sensing/actuation design and data processing techniques, there is still an urgent need to intensify the efforts towards intelligent monitoring, control, and security of critical infrastructure systems. The problem of managing critical infrastructure systems is becoming more complicated since they were not designed to be so large in size and geographical distribution; instead, they evolved due to the growing demand, while new technologies have been combined with outdated infrastructures in a single system that is required to perform new and more complex tasks. Furthermore, deregulation and the new market structure in several of these infrastructures has resulted in more heterogeneous and distributed infrastructures, which make them more vulnerable to failures and attacks. The introduction of renewable energy sources and environmental issues have incorporated new objectives to be met and new challenges in the operation and economics of some of these infrastructures (for example, power systems, telecommunication, water distribution networks, and transportation).

Two important notions that captivate the attention of researchers and of the industry are the concepts of *cyber-physical systems* and *system of systems*. Cyber-physical systems are the result of the interconnection and interaction of the cyber (computation) and the physical elements in a system. Embedded sensors, computers, and networks monitor and collect data from the physical processes; in turn, it is possible to control the physical processes through the analysis and use of the data collected to take appropriate actions for retaining the stability and security of the system.

The system of systems concept arose from the interconnection of independent systems in a larger, more complex system. These formerly independent systems may now be interacting or be interdependent. There are dependencies between infrastructures (e.g., a fault in the power system removes the supply to a water pump and thus, the water supply to an area), or in some cases interdependencies (e.g., a fault in the power system causes the oil/natural gas pipeline pumping stations to stop working, and as a consequence the supply of fuel to the power station is interrupted). Critical infrastructure dependencies and interdependencies pose an even higher degree of complexity, particularly on the appropriate modeling and simulation of the effects that one infrastructure has on another

infrastructure. The fact that fewer people nowadays understand how these networks operate and the interactions between all the components, creates a necessity for further research and in-depth analysis of the various infrastructures.

Given the current challenges faced by critical infrastructures and given that it is not realistic to consider rebuilding them from scratch, it is necessary to derive approaches and develop methods to transform and optimize these infrastructures through the use of instrumentation, embedded software, and “smart” algorithms. In the global effort towards developing a more systematic and efficient approach for all critical infrastructures, it is useful to consider that these systems have some common characteristics. Critical infrastructure systems are safety critical systems that are complex in operation, spatially distributed, dynamic, time-varying, and uncertain. There is a wealth of data that can be obtained from various parts of these systems. Their dynamics have significant similarities in their analysis, while the effects of faults or disturbances can be modeled in similar ways.

This book was motivated by the European Science Foundation COST Action *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems* IC0806 (IntelliCIS) and is supported by the COST (European Cooperation in Science and Technology) Office. The book aims at presenting the basic principles as well as new research directions for intelligent monitoring, control, and security of critical infrastructure systems. Several critical infrastructure application domains are presented, while discussing the key challenges that each is facing. Appropriate state-of-the-art algorithms and tools are described that allow the monitoring and control of these infrastructures, based on computational intelligence and learning techniques. Some of the book chapters describe key terminology in the field of critical infrastructure systems: risk evaluation, intelligent control, interdependencies, fault diagnosis, and system of systems.

The Chapter “[Critical Infrastructure Systems—Basic Principles of Monitoring, Control, and Security](#)” provides an overview of critical infrastructure systems. It describes the basic principles of monitoring, control, and security and sets the stage for the rest of the book chapters. Chapters “[Electric Power Systems](#)”, “[Telecommunication Networks](#)”, “[Water Distribution Networks](#)”, and “[Transportation Systems: Monitoring, Control, and Security](#)” concentrate on four key critical infrastructure systems: electric power systems, telecommunication networks, water distribution networks, and transportation systems. Their basic principles and key challenges are described.

Chapters “[Algorithms and Tools for Intelligent Monitoring of Critical Infrastructure Systems](#)”, “[Algorithms and Tools for Intelligent Control of Critical Infrastructure Systems](#)”, and “[Algorithms and Tools for Risk/Impact Evaluation in Critical Infrastructures](#)” focus on algorithms and associated tools for intelligent monitoring, control, and security of critical infrastructure systems, as well as risk/impact evaluation. The chapters provide the necessary theory, but also provide real life examples in the application of these tools and methodologies.

The Chapter “[Infrastructure Interdependencies—Modeling and Analysis](#)” presents several approaches for modeling critical infrastructure interdependencies. The Chapter “[Fault Diagnosis and Fault Tolerant Control in Critical Infrastructure](#)

Systems” provides a theory-based overview of fault diagnosis and fault tolerant control in critical infrastructure systems and illustrates the application of these methodologies in the case of water distribution networks.

The Chapter “**Wireless Sensor Network Based Technologies for Critical Infrastructure Systems**” examines the role of telecommunication networks in supporting the monitoring and control of critical infrastructure applications. The physical network is examined, as well as reliability and security issues. The Chapter “**System-of-Systems Approach**” concentrates on the reliability, security, risk, and smart self-healing issues in critical infrastructures, viewed from a system of systems perspective. The interdependencies between systems are examined with a focus on the electric power grid. Finally, the Chapter “**Conclusions**” discusses the main attributes that a future critical infrastructure system is expected to have and provides some potential future research directions in the areas of intelligent monitoring, control, and security of critical infrastructure systems.

Contents

Critical Infrastructure Systems: Basic Principles of Monitoring, Control, and Security	1
Georgios Ellinas, Christos Panayiotou, Elias Kyriakides and Marios Polycarpou	
Electric Power Systems	31
Antonello Monti and Ferdinanda Ponci	
Telecommunication Networks	67
Rasmus L. Olsen, Kartheepan Balachandran, Sara Hald, Jose Gutierrez Lopez, Jens Myrup Pedersen and Matija Stevanovic	
Water Distribution Networks	101
Avi Ostfeld	
Transportation Systems: Monitoring, Control, and Security	125
Stelios Timotheou, Christos G. Panayiotou and Marios M. Polycarpou	
Algorithms and Tools for Intelligent Monitoring of Critical Infrastructure Systems	167
Cesare Alippi, Romolo Camplani, Antonio Marullo and Manuel Roveri	
Algorithms and Tools for Intelligent Control of Critical Infrastructure Systems	185
Mietek A. Brdys	
Algorithms and Tools for Risk/Impact Evaluation in Critical Infrastructures	227
Chiara Foglietta, Stefano Panzieri and Federica Pascucci	

Infrastructure Interdependencies: Modeling and Analysis 239
Gabriele Oliva and Roberto Setola

Fault Diagnosis and Fault Tolerant Control in Critical Infrastructure Systems 263
Vicenç Puig, Teresa Escobet, Ramon Sarrate and Joseba Quevedo

Wireless Sensor Network Based Technologies for Critical Infrastructure Systems 301
Attila Vidács and Rolland Vida

System-of-Systems Approach 317
Massoud Amin

Conclusions 355
Elias Kyriakides and Marios Polycarpou