Advances in Intelligent Systems and Computing 461

Maciej Grzenda
Ali Ismail Awad
Janusz Furtak
Jarosław Legierski *Editors*

# Advances in Network Systems

## Architectures, Security, and Applications

Springer

# Advances in Intelligent Systems and Computing

Volume 461

**Series editor**

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

## *About this Series*

The series “Advances in Intelligent Systems and Computing” contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within “Advances in Intelligent Systems and Computing” are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

More information about this series at http://www.springer.com/series/11156

Maciej Grzenda · Ali Ismail Awad
Janusz Furtak · Jarosław Legierski
Editors

# Advances in Network Systems

## Architectures, Security, and Applications

Springer

*Editors*
Maciej Grzenda
Faculty of Mathematics and Information Science
Warsaw University of Technology
Warsaw
Poland

and

Research and Development Center
Orange Polska
Warsaw
Poland

Ali Ismail Awad
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
Luleå
Sweden

and

Faculty of Engineering
Al Azhar University
Qena
Egypt

Janusz Furtak
Military University of Technology
Warsaw
Poland

Jarosław Legierski
Faculty of Mathematics and Information Science
Warsaw University of Technology
Warsaw
Poland

and

Research and Development Center
Orange Polska
Warsaw
Poland

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-319-44352-2 ISBN 978-3-319-44354-6 (eBook)
DOI 10.1007/978-3-319-44354-6

Library of Congress Control Number: 2016951683

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

Owing to the ever growing communication systems, modern networks currently encompass a wide range of solutions and technologies, including wireless and wired networks, and provide a basis for network systems from multiple partly overlapping domains such as the Internet of Things (IoT), cloud services, and network applications. This appears in numerous active research areas with particular attention paid to the architectures and security of network systems. In parallel, novel applications are developed, in some cases strongly linked to rapidly developing network-based data acquisition and processing frameworks.

In the domain of architectures, growing distribution of components interconnected in variety of ways is observed. This is exemplified by the growth of wireless sensor networks and development of algorithms they require. At the same time, information security works as a backbone for protecting both user data and electronic transactions in network systems. Security has emerged as an important scientific discipline whose many multifaceted complexities deserve the attention and synergy of the computer science, engineering, and information systems communities. Equally importantly, novel applications which both arise from and promote further development of network systems are evolved.

The significance of this book volume comes from the demand for a better understanding of the network systems. The volume provides a comprehensive selection of cutting-edge state-of-the-art algorithms, technologies, and applications, providing new insights into a range of fundamentally important topics in network infrastructures, network security, and network applications.

The volume includes 19 chapters in total that are divided into three parts. Part I is devoted to network architectures and is composed of 6 chapters. Part II includes 6 chapters that cover several network security aspects. The final 6 chapters grouped in Part III are covering some network applications. Additionally, an introduction chapter, Chapter "Network Architectures, Security, and Applications: An Introduction," is placed at the beginning of the volume for offering preliminary information for all the chapters in the three parts of the volume.

The volume has attracted authors from many countries worldwide such as France, Poland, Portugal, Romania, and United Kingdom. Several of the chapters result from the further research made by the authors of selected papers presented during the International Conference on Innovative Network Systems and Applications (iNetSApp) organized under the frame of Federated Conference on Computer Science and Information Systems.

The editors are very grateful to Dr. Janusz Kacprzyk, the editor of the Advances in Intelligent Systems and Computing (AISC) series by Springer for his support, which made the development of this module possible. The editors are indebted to the efforts of Dr. Thomas Ditzinger, the senior editor of the AISC series, and Mr. Holger Schäpe, the editorial assistant of the AISC. Finally, the editors and the authors acknowledge the efforts of Advances in Intelligent Systems and Computing team at Springer for their support and cooperation in publishing the book as a volume in the AISC series by Springer.

Warsaw, Poland Maciej Grzenda
Luleå, Sweden Ali Ismail Awad
Warsaw, Poland Janusz Furtak
Warsaw, Poland Jarosław Legierski
May 2016

# Program Committee

Ali Ismail Awad, Luleå University of Technology
Andrzej Białas, Institute of Innovative Technologies
Peter Brida, University of Zilina, Faculty of Electrical Engineering, Department of Telecommunications and Multimedia
Hacene Fouchal, Universite de Reims Champagne-Ardenne
Janusz Furtak, Military University of Technology
Antonio García-Domínguez, Departamento de Ingeniería Informática, Universidad de Cádiz
Gebhard Geiger, Technische Universitaet Muenchen
Maciej Grzenda, Warsaw University of Technology
Zineb Habbas, LCOMS, University of Lorraine
Michal Hodon, University of Zilina
Bernhard Hämmerli, Acris GmbH
Krzysztof Kaczmarski, Warsaw University of Technology
Ondrej Karpis, University of Zilina
Ioannis Katakis, University of Athens
Piotr Korbel, Lodz University of Technology
Emil Kowalczyk, Orange Polska
Jarosław Legierski, Orange Polska
Marcin Luckner, Warsaw University of Technology
Zakaria Maamar, Zayed University
Juraj Micek, Zilinska univerzita
Malgorzata Pankowska, University of Economics
Jan Papaj, Technical University of Košice
Eman Shaaban, Ain Shams University, Cairo
Zbigniew Suski, Military University of Technology
Maciej Szmit, Orange Polska
Devinder Thapa, University of Agder
Konrad Wrona, NATO Communications and Information Agency
Mee Yang, Auckland University of Technology
Zbigniew Zieliński, Military University of Technology

# Contents

**Part I Network Architectures**

**Part II Network Security**

**Part III Network Applications**

# About the Editors

**Dr. Maciej Grzenda** received his M.Sc. in computer science in 1997 from the Warsaw University of Technology, Poland. In 2001, he received his Ph.D. degree in technical sciences from the same university. He is currently an assistant professor at the Faculty of Mathematics and Information Science of the Warsaw University of Technology. In parallel, he participates as an expert and project manager in the works of Research and Development Center of Orange Polska. His areas of expertise are industrial applications of intelligent data processing techniques and the architecture of data processing systems with particular emphasis on storage and stream processing with Big Data frameworks. Maciej Grzenda participates also in program committees of international conferences on intelligent data processing.

**Dr. Ali Ismail Awad** is currently a senior lecturer (assistant professor) at Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden. He also holds a permanent position as an assistant professor at Electrical Engineering Department, Faculty of Engineering, Al Azhar University, Qena, Egypt. Dr. Awad received his B.Sc. from Al Azhar University, Egypt, 2001, the M.Sc. degree from Minia University, Egypt, 2007, and the Ph.D. degree from Kyushu University, Japan, 2012. He has been awarded his second Ph.D. degree from Minia University, Egypt, May 2013. Dr. Awad serves as an external reviewer in several international journals. His research interests include information security, information security laboratories, biometrics, image processing, pattern recognition, and networking.

**Dr. Janusz Furtak** received his M.Sc. from the Cybernetics Faculty of Military University of Technology, Warsaw, Poland in 1982. For eight years, he was a member of the design team which developed software for command systems. Since 1990, he has been a university teacher at the Cybernetics Faculty of Military University of Technology. In 1999, he received Ph.D. degree in the field of computer science. Currently, he is an assistant professor in the Institute of Teleinformatics and Automation of Cybernetics Faculty, Military University of Technology and Director of this Institute. His main areas of expertise are computer networks, network security, security in Internet of Things, cyber defense, and administering of network operating systems.

**Dr. Jarosław Legierski** received his M.Sc. in electronics and telecommunication and Ph.D. degree in electronics from Technical University of Lodz. Since 1998, he has worked in the telecommunications industry. He is currently R&D Expert in Research and Development Center, Orange Labs at Orange Polska and assistant professor at Faculty of Mathematics and Information Science of Warsaw University of Technology. Jarosław Legierski is the cocreator of Open Middleware 2.0 Community (www.openmiddleware.pl). His research interest includes open application programming interfaces (APIs), Open (Big) Data, and next-generation service delivery platforms. Author of publications in the area of open API and Open Data exposure.

# Network Architectures, Security, and Applications: An Introduction

**Maciej Grzenda, Janusz Furtak, Jarosław Legierski and Ali Ismail Awad**

**Abstract** Owing to the ever growing communication systems, modern networks currently encompass a wide range of solutions and technologies, including wireless and wired networks and provide basis for network systems from multiple partly overlapping domains such as the Internet of Things (IoT), cloud services, and network applications. This appears in numerous active research areas with particular attention paid to the architecture and security of network systems. In parallel, novel applications are developed, in some cases strongly linked to rapidly developing network-based data acquisition and processing frameworks. This chapter presents a general introduction to the topics of network architectures, security, and applications in addition to short descriptions of the chapters included in this volume.

**Keywords** Network architectures · Network security · Network applications

M. Grzenda (✉) · J. Legierski (✉)
Faculty of Mathematics and Information Science,
Warsaw University of Technology, Warszawa, Poland
e-mail: m.grzenda@mini.pw.edu.pl

J. Legierski
e-mail: Jaroslaw.legierski@orange.com

M. Grzenda · J. Legierski
Research and Development Center, Orange Polska Warszawa, Warszawa, Poland

J. Furtak (✉)
Military University of Technology, Warszawa, Poland
e-mail: jfurtak@wat.edu.pl

A.I. Awad (✉)
Department of Computer Science, Electrical and Space Engineering,
Luleå University of Technology, Luleå, Sweden
e-mail: ali.awad@ltu.se; aawad@ieee.org

A.I. Awad
Faculty of Engineering, Al Azhar University, Qena, Egypt

M. Grzenda et al. (eds.), *Advances in Network Systems*, Advances in Intelligent
Systems and Computing 461, DOI 10.1007/978-3-319-44354-6_1

# 1 Introduction

A growing proportion of modern software systems are developed as network systems. The growth of network bandwidth, ever growing coverage of mobile networks and development of disruptive network services all contribute to this phenomenon. This volume reflects the variety of undertaken efforts in the research and development community working within the domain of network systems. The first part of this book covers items pertaining to the network architectures. It includes chapters related to server placement in regular networks, client-server architecture, analysis of TCP connections, wireless sensor networks, marker localisation methods, and photonic data transport networks.

We live in the era of dynamic development of Internet technologies. 5G technology, the Internet of Things (IoT) and its successor, the Internet of Everything, advanced applications of virtualization, and cloud computing are examples that can be mentioned in this context. Data security and user authentication are crucial concerns in all of these examples. Data encryption plays a major role in assuring the information confidentiality [1]. On the applications' level, and in addition to the traditional authentication methods, biometrics technology expands and offers a reliable user identification or verification solution, access control mechanism, that is required for most of the available network applications [2–5]. On the network infrastructure level, traffic passing though the network is a rich source of information [6, 7]. Network traffic collection and analysis can be a good tool for addressing security solutions to the network systems.

The second part of the book is dedicated to numerous issues in the security domain. We can find proposals of solving the following problems: securing the transmission in wireless sensor networks, partitioning of security policies in tactical service-oriented architecture, the usage of Trust Management of Credentials (TMC), estimating time delay and energy consumption when using the AES encryption in Wireless Sensor Networks, computer support for risk management in critical infrastructures, and risk management systems for monitoring flood hazards.

Network systems form the critical infrastructure and the foundation of a wide variety of applications. The network infrastructure includes high-speed wired networks, wireless networks, Wireless Sensor Networks, IoT networks, and mobile networks. Due to the diversity of the network systems, several business and industrial applications have emerged for each network infrastructure. The third part addresses several aspects for network applications such as automotive applications, live TV services, telemetry-oriented applications, drip irrigation systems, and energy harvesting platform using Wireless Sensor Networks.

## 2 Chapters of the Book

The rest of the volume contains 18 chapters which are divided into three categories. The following are brief summaries for the content of each chapter.

**Part I: Network Architectures**

Chapter "An Analytical Method of Server Placement in Regular Networks and its Evaluation by Simulation Experiments" illustrates the optimization issues present in the design of network systems. The chapter presents the challenge of determining optimal server placements in the hybercube network structure [8], which follows from hypercube structure of multiprocessor systems [9]. The latter network architecture is of particular importance for critical applications present in the field of military, aerospace or medical domains. The way the server placement can be followed by the generation of appropriate communication structure is proposed in the chapter. At the same time, the chapter illustrates how the needs of network systems promote the development of novel algorithms.

Another aspect of network systems that is of growing importance nowadays is the adaptation of these systems to serve user interface on variety of devices. Device-Independent Architecture (DIA) [10] and its relation to user interface adaptation are discussed in Chap. "Model and Case Studies of the Runtime UI Adaptation Process in Client-Server Systems". The chapter shows possible use of existing user interface adaptation in DIA systems and addresses the need for network systems serving their user interface on multiple devices of varied capabilities [11]. This issue can be considered in the context of ubiquitous computing, where dynamic adaptation to not only user interface changes, but also changes of user preferences, profile, location, and context becomes necessary [12]. At the same time, it shows an interesting example of the importance of network protocols reducing the volume of transmitted data. This remains a major objective even though the network bandwidth is constantly growing both in wired and wireless network environments.

Chapter "Analysis of TCP Connection Performance Using Emulation of TCP State" also directly refers to the performance aspects of network protocols. The chapter proposes methodology aiming at the identification of root causes of throughput degradation in TCP connections [13] i.e. connections fundamental for many, or even most modern network applications. Importantly, passive measurements performed through network probes are used to attain the objectives laid out in this chapter. This revisits the use of network probes [14], which is of particular importance for variety of monitoring and security-related purposes such as the collection of data for intrusion detection purposes [15]. What is interesting, the chapter describes the validation of proposed approach performed with the data collected in 4G mobile network. Therefore, a combination of TCP protocol and mobile environments serves to illustrate the chapter and its findings.

Chapter "Firefly-Based Universal Synchronization Algorithm in Wireless Sensor Network" also contributes to the survey of architecture challenges contained in this part of the book. The chapter concentrates on one of the crucial needs of the majority of Wireless Sensor Networks (WSN), being the synchronization of nodes. The algorithm answering this need and based on the fireflies synchronization process [16] is proposed and tested. The synchronisation algorithm proposed in the chapter belongs to a wider class of algorithms stimulated by the development of WSN [17]. The experimental evaluation of the proposed synchronization algorithm has been performed on physical wireless sensor nodes. This clearly illustrates novel challenges introduced with WSN deployments which involve the need for developing and testing network architectures with dedicated hardware devices. Moreover, the challenges caused by the need to minimize active power modes have to be addressed. These go beyond the needs typically present in wired scenarios with no restrictive power consumption constraints.

Chapter "Comparison of Various Marker Localization Methods" extends the analysis of unique needs of WSN networks to concentrate on the cases where even locating a network node can be a challenge. The chapter analyses two methods of marker localization, which rely on Radio Frequency Identification (RFID) [18]. The work addresses the need for underground localisation, discussed among others in [19]. By a marker, which has to be localised a passive RFID transponder (without or with identification chip) is meant. The term marker reflects the fact that the transponder is used to mark underground assets and trace underground networks such as cables and pipes in turn. Localization of the marker is based on evaluation of signal amplitude received from the excited marker. Notably, the location of a wireless device is determined based on signal amplitude received from the excited marker. This shows a wider tendency of using network-related data for variety of needs, going beyond monitoring the quality of network connection.

Chapter "Decomposition Scheme for Flow Design in Photonic Data transport Networks" proposes a mathematical model of network design problem in the context of modern photonic network with wavelength division multiplexing [20]. This answers the needs of modelling photonic data transport networks which is crucial to make the efficient use of this technology possible. To reduce the complexity of the proposed model, the authors applied the Dantzig-Wolfe based decomposition, which is not unusual also in modelling of other types of network systems such as power grid networks [21]. This resulted in significant reduction in the number of constraints and variables used. In a wider context, this chapter confirms the need for in-depth analysis and modelling of modern network technologies and architectures enabled by them. Equally importantly, this clearly shows the challenges in the mathematical domain, which are created by the complexity of modern network systems.

## Part II: Network Security

Wireless sensor networks provide basis for a growing number of applications. Such networks contribute also to the development of Internet of Things. Due to mobility of such networks, relatively low operating costs and the fact that these networks create an independent infrastructure communication, they can be successfully used in military applications [22, 23]. In military applications an extremely important problem is the authentication of the network nodes, which is more important than the problem of energy consumption by network nodes. The proposal to build such a network is presented in Chap. "Secure Transmission in Wireless Sensors' Domain Supported by the TPM". The proposed method of the transmission protection between nodes and the way of protecting the node resource, provide for utilization of the Trusted Platform Module (TPM) [24]. For this purpose, sensors create the domain in which one of them is the security authority of the domain. This node is also the recipient of the data from the sensors belonging to the domain. The experimental results confirm the usefulness of the solution. Experiments allow to pre-assess the delay in the transfer of data that is entered by cryptography procedures and the growth of energy demand during these procedures.

Chapter "Constraint Analysis for Security Policy Partitioning Over Tactical Service Oriented Architectures" is devoted to issues related to the partitioning of security policies in tactical service-oriented architecture [25, 26]. The proposed approach is based on the ontologically defined security infrastructure with the use of the Web Ontology Language (OWL) [27], and identification of the involved elements of tactical networks with critical impact. In the considerations were taken into account three categories of governing parameters, regarding to the attainment of the required security policy distribution. The first category refers to the evaluation of the policy from the point of view of the overall and local complexity. The second category refers to the evaluation and categorization of the deployed tactical nodes, based on their expected functional and operational specialization. The last category refers to the sufficient integration of dynamism, emerging from the characteristics of the tactical environment. The result of the work is the mechanism of adjusting the identified parameters for the optimal partitioning and distribution of security policies within the mission preparation stage.

Usually the decision-making procedure connected with access control uses the policy statements established by many principals. For trust management you can use Role-based Trust Management Language (RTML) [28, 29]. Such language allows to operate with security policies, authentication data and relationship in distributed and large scale access control systems. The extension of the Role-based Trust Management Language in the range of the determination of order, and time validity is described in Chap. "Practical Extensions of Trust Management Credentials" [30]. Presented solution proposes to add some extensions (including time data) to credentials to make a trust management system more useful in practice.

One of the most efficient ways of data encryption is AES encryption. Methods based on this encryption can operate in different modes. These modes include: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback), CTR (Counter), and GCM (Galois/Counter Mode) [31, 32]. Chapter "Performance and Energy Consumption Analysis of AES in Wireless Sensor Networks" describes the Performance and Energy Consumption Analysis of AES for the needs of Wireless Sensor Networks [33]. In the studies a system ATmega128 RFA1 was used. During the experiments the software implementation and the hardware implementation of AES encryption in different modes was tested. The achieved results show that in all cases the hardware implementations was at least five times faster than the software implementations. Energy consumption for AES was also examined (only CTR mode tested). The results indicate that the average power consumption is almost constant and does not depend on the size of the encrypted message (in the range of from 16 to 128 bytes), but for hardware implementation the average power consumption is about 5 % higher. Average energy consumption in both cases increases by leaps and bounds with an increase in message length. It is worth noting that in the whole range of message length the average power consumption for the software implementation is approximately 6-times greater than for the hardware implementation.

The assessment and management of risk is an essential part of any utilized system. It is particularly important for Critical Infrastructures (CI), such as energy (electricity, oil, gas) or transportation (road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping and ports). Chapter "Computer Support for Risk Management in Critical Infrastructures" shows the CIRAS Tool, which was created under the EU CIRAS project. In this solution the assessment and management of risk issues are computer aided [34]. The CIRAS Tool operations are based on three pillars: Risk Reduction Assessment (RRA), Cost-Benefit-Assessment (CBA), Qualitative Criteria Assessment (QCA). In the chapter, particular attention was paid to the use of the OSCAD software platform to perform the tasks of the RRA component. The experimentation tool, called OSCAD-Ciras, was developed. A case study for the railway CI collaborating with the electricity CI was planned and performed.

In Chap. "An Innovative Web Platform for Flood Risk Management" an innovative real-time information system for enhanced support to flood risk emergency in urban and nearby coastal areas was presented [35–37]. The solution includes a description of the platform, its architecture, all innovative aspects related to the User Interface (UI), product creation and choice of technologies. The tool can be used not only for risk management, but also for the coordination of situational awareness and civil protection interaction.

### Part III: Network Applications

Chapter "A Distributed Active Vibration Control System Based on the Wireless Sensor Network for Automotive Applications" presents a new approach of an adaptive system for automotive applications based on the AVC—Active Vibration Control Systems concept [38, 39]. The authors assume that the porting of a centralized system in a distributed system can improve its effectiveness and present a Wireless Sensor Network for damping vibrations in automotive applications. Sensors with a piezoelectric element (Series-SSHI method) [40] were used to measure and damp the vibrations and harvest energy from vibrations. The Finite Element Simulations (FEM) using COMSOL 5.1 software were provided to simulate deformations of the mechanical system and were then compared with the measured results.

Chapter "Improvements of Video Delay in OTT Live TV Service" studies the end-to-end delay observed by users of the Over The Top (OTT) Live TV services using Adaptive Bit Rate (ABR) technology [41]. The analysis and measurements in a test environment demonstrate the extent to which the main architecture elements—encoder, packager, Content Delivery Network (CDN) and player (e.g. GPAC [42] or [43]) contribute to this overall delay. The work presented in this chapter has been carried out as part of the EUREKA/CELTIC research project NOTTS (Next-Generation Over-The-Top Services) [44].

Chapter "Power Aware MOM for Telemetry-Oriented Applications—Levee Monitoring Use Case" addresses the issue of the Message-Oriented Middleware [45] utilization in telemetry systems. The authors provide a survey and practical measurements of common data transmission protocols for telemetry applications and wireless sensing. Based on the survey the authors propose concepts of message aggregation mechanisms to improve power consumption of the data transmission channel. As an entry point, the authors assume the utilization of the MQTT protocol [46]. The results of the research have been successfully implemented in a smart levee monitoring system.

Chapter "Monitoring Drip Irrigation System Using Wireless Sensor Networks" presents a model of architecture for a drip irrigation system using the Wireless Sensor and Actuators Networks (WSANs). The investigated model includes the soil moisture, temperature and pressure sensors to monitor the irrigation operations [47, 48]. The researchers have performed extensive simulations with the use of TOSSIM simulators [49]. The results show that the presented solution allows for better performance in terms of the delay, PDR for the priority traffic.

Chapter "BARBEI: A New Adaptive Battery Aware and Reliable Beacon Enabled Technique for IEEE802.15.4 MAC" focuses on the IEEE 802.15.4 standard [50] which supports both physical and Media Access Control (MAC) layers of low rate Wireless Sensor Networks (WSNs). The authors propose a technique that improves the performance of the IEEE802.15.4 standard by allowing its MAC to exploit the nonlinear processes of the battery [51] to prolong the WSN lifetime. The performance of the new algorithm has been examined and compared against that of the legacy IEEE 802.15.4 MAC algorithm through extensive simulation experiments.

Chapter "A Multisource Energy Harvesting Platform for Wireless Methane Sensor" focuses on harvesting energy [52, 53] from ambient sources in order to extend the operation time of wireless sensor networks. In this article, the authors present a multi-source harvesting circuit consisting of wind and solar energy and its implementation for the Wireless Gas Sensor Node (WGSN) [54]. The researchers demonstrate that a catalytic gas sensor can operate for two days without batteries by using the developed scheme.

## 3 Concluding Remarks

Network systems play vital roles in all of our daily life. This volume provides comprehensive selection of cutting edge state-of-the-art algorithms, technologies, and applications, providing new insights into a range of fundamentally important topics in network architectures, network security, and network applications. The significance of this book comes from the demand for better understanding of the network models. Due to the rapid growth in network architectures, security, and applications, further contributions and research findings are anticipated in the future.

## References

1. King, J., Awad, A.I.: A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) **40**(1), 133–143 (2016)
2. Jain, A.K., Ross, A.A., Nandakumar, K.: Introduction to Biometrics. Springer (2011)
3. Awad, A.I., Baba, K.: Evaluation of a fingerprint identification algorithm with SIFT features. In: Proceedings of the 3rd 2012 IIAI International Conference on Advanced Applied Informatics, pp. 129–132. IEEE, Fukuoka, Japan (2012)
4. Egawa, S., Awad, A.I., Baba, K.: Evaluation of acceleration algorithm for biometric identification. In: Benlamri, R. (ed.) Networked Digital Technologies, Communications in Computer and Information Science, vol. 294, pp. 231–242. Springer, Berlin (2012)
5. Awad, A.I., Hassanien, A.E.: Impact of some biometric modalities on forensic science. In: Muda, A.K., Choo, Y.H., Abraham, A.N., Srihari, S. (eds.) Computational Intelligence in Digital Forensics: Forensic Investigation and Applications, Studies in Computational Intelligence, vol. 555, pp. 47–62. Springer International Publishing (2014)
6. Rubio-Loyola, J., Sala, D., Ali, A.I.: Maximizing packet loss monitoring accuracy for reliable trace collections. In: 16th IEEE Workshop on Local and Metropolitan Area Networks, LANMAN 2008, pp. 61–66. IEEE (2008)
7. Rubio-Loyola, J., Sala, D., Ali, A.I.: Accurate real-time monitoring of bottlenecks and performance of packet trace collection. In: 33rd IEEE Conference on Local Computer Networks, LCN 2008, pp. 884–891. IEEE (2008)
8. Chen, J., Kanj, I.A., Wang, G.: Hypercube network fault tolerance: a probabilistic approach. In: Proceedings of International Conference on Parallel Processing, pp. 65–72 (2002)
9. Ishikawa, T.: Hypercube multiprocessors with bus connections for improving communication performance. IEEE Trans. Comput. **44**(11), 1338–1344 (1995)
10. Chmielewski, J.: Device-independent architecture for ubiquitous applications. Pers. Ubiquit. Comput. **18**(2), 481–488 (2013)
11. Kobayashi, N., Tokunaga, E., Kimura, H., Hirakawa, Y., Ayabe, M., Nakajima, T.: An input widget framework for multi-modal and multi-device environments. In: Third IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (SEUS'05), pp. 63–70 (2005)
12. Moreira, R.S., Torres, J., Sobral, P., Morla, R., Rouncefield, M., Blair, G.S.: Dynamic adaptation of personal ubicomp environments. Pers. Ubiquit. Comput. **20**(2), 165–166 (2016)
13. Shah, P.A., Rehan, M., Chughtai, H.M.O., Qayyum, A.: On reducing throughput degradation of TCP connection after vertical handover. In: IEEE 13th International Multitopic Conference, INMIC 2009, pp. 1–4 (2009)
14. Gkatzikis, L., Tryfonopoulos, T., Koutsopoulos, I.: An efficient probing mechanism for next generation mobile broadband systems. In: 2012 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1191–1195 (2012)

15. do Carmo, R., Hollick, M.: Analyzing active probing for practical intrusion detection in wireless multihop networks. In: 11th Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp. 77–80 (2014)
16. Tyrrell, A., Auer, G., Bettstetter, C.: Fireflies as role models for synchronization in Ad Hoc networks. In: Proceedings of the 1st International Conference on Bio Inspired Models of Network, Information and Computing Systems. BIONETICS '06, ACM, New York, NY, USA (2006)
17. Iyengar, S.S., Parameshwaran, N., Phoha, V.V., Balakrishnan, N., Okoye, C.D.: Algorithms for Wireless Sensor Networks, pp. 131–154. Wiley-IEEE Press (2011)
18. Hall, D.A.: Conventional and radio frequency identification (RFID) tags. In: Cadrin, S.X., Kerr, L.A., Mariani, S. (eds.) Stock Identification Methods, pp. 365–395, 2nd edn. Academic Press, San Diego (2014)
19. Hautcoeur, J., Talbi, L., Nedil, M.: High gain RFID tag antenna for the underground localization applications at 915 MHz band. In: 2013 IEEE Antennas and Propagation Society International Symposium (APSURSI), pp. 1488–1489 (2013)
20. Vinolee, R., Bhaskar, V.: Performance analysis of mixed integer linear programming with wavelength division multiplexing. In: 2014 2nd International Conference on Devices, Circuits and Systems (ICDCS), pp. 1–6 (2014)
21. Altay, C., Deli, H.: Distributed energy management of microgrids with Dantzig-Wolfe decomposition. In: IEEE PES Innovative Smart Grid Technologies, Europe, pp. 1–5 (2014)
22. Chudzikiewicz, J., Furtak, J., Zielinski, Z.: Secure protocol for wireless communication within internet of military things. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 508–513. IEEE (2015)
23. Hennebert, C., Dos Santos, J.: Security protocols and privacy issues into 6LoWPAN stack: a synthesis. IEEE Internet Things J. **1**(5), 384–398 (2014)
24. Furtak, J., Chudzikiewicz, J.: Securing transmissions between nodes of WSN using TPM. In: 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, Sept 13–16, pp. 1059–1068. IEEE (2015)
25. Johnsen, F.T., Bloebaum, T.H., Schenkels, L., Fiske, R., Van Selm, M., de Sortis, V., van der Zanden, A., Sliwa, J., Caban, P.: SOA over disadvantaged grids experiment and demonstrator. In: 2012 Military Communications and Information Systems Conference (MCC), pp. 1–8. IEEE (2012)
26. Maule, R.W., Lewis, W.C.: Security for distributed SOA at the tactical edge. In: 2010 Military Communications Conference, (MILCOM 2010), pp. 13–18. IEEE (2010)
27. Souag, A., Salinesi, C., Comyn-Wattiau, I.: Ontologies for security requirements: a literature survey and classification. In: Advanced Information Systems Engineering Workshops, pp. 61–69. Springer (2012)
28. Gorla, D., Hennessy, M., Sassone, V.: Inferring dynamic credentials for role-based trust management. In: Proceedings of the 8th ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming, pp. 213–224. ACM (2006)
29. Li, N., Winsborough, W.H., Mitchell, J.C.: Distributed credential chain discovery in trust management. J. Comput. Secur. **11**(1), 35–86 (2003)
30. Felkner, A., Kozakiewicz, A.: More practical application of trust management credentials. In: 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, Sept 13–16, pp. 1125–1134. IEEE (2015)
31. Zhang, F., Dojen, R., Coffey, T.: Comparative performance and energy consumption analysis of different AES implementations on a wireless sensor network node. Int. J. Sens. Netw. **10**(4), 192–201 (2011)
32. Lee, J., Kapitanova, K., Son, S.H.: The price of security in wireless sensor networks. Comput. Netw. **54**(17), 2967–2978 (2010)
33. Panait, C., Dragomir, D.: Measuring the performance and energy consumption of AES in wireless sensor networks. In: 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, Sept 13–16, pp. 1261–1266. IEEE (2015)
34. Bialas, A.: Experimentation tool for critical infrastructures risk management. In: 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, Sept 13–16, pp. 1099–1106. IEEE (2015)

35. Gomes, J.L., Jesus, G., Rogeiro, J., Oliveira, A., Tavares da Costa, R., Fortunato, A.B.: Molines-towards a responsive web platform for flood forecasting and risk mitigation. In: 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, Sept 13–16, pp. 1171–1176. IEEE (2015)
36. Oliveira, A., Jesus, G., Gomes, J., Rogeiro, J., Azevedo, A., Rodrigues, M., Fortunato, A., Dias, J., Tomas, L., Vaz, L., Oliveira, E., Alves, F., den Boer, S.: An interactive WebGIS observatory platform for enhanced support of integrated coastal management. J. Coastal Res. **70**, 507–512 (2014), Special Issue 70— Proceedings of the 13th International Coastal Symposium
37. Deng, Z., Namwamba, F., Zhang, Z.: Development of decision support system for managing and using recreational beaches. J. Hydroinformatics **16**(2), 447–457 (2014)
38. Elliott, S.: A review of active noise and vibration control in road vehicles. Tech. Rep. 981, University of Southampton. http://eprints.soton.ac.uk/65371/ (2008)
39. Svaricek, F., Fueger, T., Karkosch, H.J., Marienfeld, P., Bohn, C.: Automotive Applications of Active Vibration Control. INTECH Engineering—Control Engineering, INTECH (2010)
40. Lefeuvre, E., Badel, A., Richard, C., Petit, L., Guyomar, D.: A comparison between several vibration-powered piezoelectric generators for standalone systems. Sens. Actuators A: Phys. **126**(2), 405–416 (2006)
41. Stockhammer, T.: Dynamic adaptive streaming over HTTP–standards and design principles. In: Proceedings of the Second Annual ACM Conference on Multimedia Systems, pp. 133–144. MMSys'11, ACM, New York, NY, USA (2011)
42. GPAC: GPAC, multimedia player with MPEG-DASH support. https://gpac.wp.mines-telecom.fr/player/ (2015). Last access 27.4.2016
43. DASH-IF: DASH-IF, a reference mpeg-dash client. http://dashif.org/reference/players/javascript/1.4.0/samples/dash-if-reference-player/ (2015). Last access 27.4.2016
44. NOTTS: Eureka/celtic notts. http://projects.celticplus.eu/notts/ (2015). Last access 27.4.2016
45. Curry, E.: Message-Oriented Middleware, pp. 1–28. Wiley (2005)
46. MQTT: Mq telemetry transport (MQTT) documentation. http://mqtt.org/documentation (2015). Last access 30.11.2015
47. Gutiérrez, J., Villa-Medina, J.F., Nieto-Garibay, A., Porta-Gándara, M.A.: Automated irrigation system using a wireless sensor network and GPRS module. IEEE Trans. Instrum. Meas. **63**(1), 166–176 (2014)
48. Mafuta, M., Zennaro, M., Bagula, A., Ault, G., Gombachika, H., Chadza, T.: Successful deployment of a wireless sensor network for precision agriculture in Malawi. In: IEEE International Conference on Networked Embedded Systems for Enterprise Applications, pp. 1–7. IEEE Computer Society, Los Alamitos, CA, USA (2012)
49. TOSSIM: Tossim simulator. http://tinyos.stanford.edu/tinyos-wiki/index.php/TOSSIM (2015). Last access 27.4.2016
50. Ergen, S.C.: Zigbee/ieee 802.15.4 summary. http://home.iitj.ac.in/~ramana/zigbee.pdf (2004). Last access 27.4.2016
51. Jongerden, M.R., Haverkort, B.R.H.M.: Battery modeling. Technical Report TR-CTIT-08-01, Centre for Telematics and Information Technology University of Twente, Enschede (Jan 2008)
52. Vullers, R., van Schaijk, R., Doms, I., Hoof, C.V., Mertens, R.: Micropower energy harvesting. Solid-State Electron. **53**(7), 684–693 (2009), Papers Selected from the 38th European Solid-State Device Research Conference—ESSDERC'08
53. Akbari, S.: Energy harvesting for wireless sensor networks review. In: Ganzha, M., Maciaszek, L.A., Paprzycki, M. (eds.) Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS), Warsaw, Poland, Sept 7–10, pp. 987–992 (2014)
54. Somov, A., Baranov, A., Spirjakin, D., Passerone, R.: Circuit design and power consumption analysis of wireless gas sensor nodes: one-sensor versus two-sensor approach. IEEE Sens. J. **14**(6), 2056–2063 (2014)

# Part I
# Network Architectures

# An Analytical Method of Server Placement in Regular Networks and Its Evaluation by Simulation Experiments

Jan Chudzikiewicz, Tomasz Malinowski and Zbigniew Zieliński

**Abstract** In the paper, the problem of determining the optimal server placement in the hypercube network structure and its influence on the values of some performance metrics is investigated. The method for the optimal server placement is proposed. It consists of two phases: in the first one the server placement is determined and in the second phase the appropriate communication structure is generated. The usefulness of the method has been verified through simulation experiments prepared and performed in Riverbed Modeler environment. Some results of these simulation tests for exemplary structures along with degradation of the 4-dimensional hypercube network are presented.

**Keywords** Server placement • Hypercube network • Reconfiguration • Fault-tolerant system

## 1 Introduction

This work is an extended version of the paper *The method of server placement in the hypercube networks* [1]. In order to guarantee the quality of service and performance of the specialized system with critical application, it is essential for the system to be able to detect faults, and to perform something akin to healing and recovering from events that might cause faults or misbehavior nodes in the network. Some of critical applications are used in near real-time mode and required both very high reliability and high efficiency of data processing throughout all the network life cycle. Furthermore, assuming harsh or even hostile physical environment for

J. Chudzikiewicz (✉) · T. Malinowski · Z. Zieliński
Military University of Technology, Warsaw, Poland
e-mail: jan.chudzikiewicz@wat.edu.pl

T. Malinowski
e-mail: tomasz.malinowski@wat.edu.pl

Z. Zieliński
e-mail: zbigniew.zielinski@wat.edu.pl

M. Grzenda et al. (eds.), *Advances in Network Systems*, Advances in Intelligent
Systems and Computing 461, DOI 10.1007/978-3-319-44354-6_2

the system a number of factors including self-diagnosing, fault tolerance and reconfiguration should be seriously considered in the designing phase. One of the possible ways to achieve fault tolerance is reconfiguring the network to a smaller sized system after faults diagnosing, i.e. realization of a soft degradation strategy. New (degraded) network continues work after resources reassigning and under the condition that it meets special requirements. In turn, the efficiency of the system will depend heavily on the availability of resources (data bases, files or web data), which is determined by their placement in the network. So, for this kind of networks there is necessity for applying effective methods of resources placement.

In the paper, we focus upon one of the problems of reconfiguration in the regular networks with soft degradation: how to reconfigure application servers and allocate resources in the network to reduce the overall cost of delivering of services to the number of clients? It is known that this cost varies depending on the physical server placement in the network, type of server and delivered content to the clients. In general, there are static content (such as images, videos, text) or dynamic content. For the static type of content, the best server placement could be the one which minimize (overall or in average) the distance to the client. Intuitively this cost could be measured by the average hops. Network hops could be defined as the number of routers present in the path between client and server. Although typical network services are data base services or web application services some others could also be network-critical applications. One of exemplary services which might be regarded as the critical application is VoIP communication (Voice over IP) through a network. In the paper the influence of the network communication structure and its characteristics for values of different type application performance parameters is also investigated.

The computer networks with a regular structure as torus or hypercube [2–5] could be used in many kinds of specialized critical application (for instance military, aerospace or medical systems). An interconnection network with the hypercube logical structure is a well-known interconnection model for multiprocessor systems [6, 7] and still hypercube networks are the field of interest of many theoretical studies concerning (among others) resource placement problem, which has been intensively studied in [8–13].

In order to achieve high reliability of the system the network could be considered as soft degradable computer network [13–15]. In this kind of networks a processor identified as faulty is not repaired (or replaced) but access to it is blocked. In the work [13] an analysis of the different schemas of resources placement in the 4-dimensional hypercube network with soft degradation was conducted.

Designing and exploitation of special networks in critical application is a comprehensive task that requires addressing a number of theoretical and practical problems. One of the problems is a skillful resources deployment in the network and modification of resources deployment after each phase of the network degradation. One of considered in the literature the resource placement problem is a combination the distance-d and the m adjacency problems, where a non-resource node must be a distance of at most d from m processors nodes [8–11, 13]. In [11] a perfect deployment has been introduced and analyzed which is defined as the minimum number of resources processors which are accessible by working processors. The definition—perfect deployment is a characteristic of the value of the generalized cost of information traffic in the network at a given load of tasks. In [13] the notion of (*m*, *d*)-perfect resources placement in the hypercube type structure *G* has been extended to the such allocation of k resources which minimizes the average distances between the working processors and resource processors in the structure *G*.

We thoroughly investigate the case when a specialized computer system is based on the 4-dimensional hypercube skeleton network with communication nodes which could communicate between themselves via cable connections. The main task of the hypercube network is to provide efficient access to resources managed by the server (or cluster of servers) connected directly to one of the network nodes and semi-stationary clients communicating with the assigned network nodes via wireless links. The execution of applications by a client processor requires an access to server services and resources, also some results returned by the server must be submitted to other clients. We assume that all clients are responsible for performing the same or very similar tasks. Thus all clients will generate similar workload of the network. The problem which arises for the given network structure is to determine the most effective server placement in the network structure.

The main goal of this paper is to give an effective method of solving the server placement problem for the hypercube network along with its soft degradation process.

A generalized cost of a network traffic with a specified resources deployment and workload of a network is usually tested through experimental measurements or examined with the use of simulation methods. In the paper we apply a two phased approach. In the first stage we solve the problem of a server placement in the given network structure on the base of analytically determined attainability measure, which was proposed in [13]. It should be noticed that real cost of information traffic in a network for a given deployment of the server with resources depends on the nature of the tasks performed by clients in the network. In the second stage we have examined this problem with the use of simulation methods for the specified server deployment determined by the simple analytical method and given type of task load of the network.

We see our contributions as follows. Firstly, we have extended the approach proposed in [1, 13] to the determining server placement in the hypercube network with soft degradation on the base of nodes attainability calculation. Secondly, we propose the algorithm of the communication structure assignation with the use of dendrite calculation. Next, we show the feasibility of this approach by applying obtained results to some possible structures of degraded 4-dimensional hypercube network and verifying effectiveness of server placement by simulation experiments.

The rest of the paper is organized as follows. In Sect. 2, a basic definitions and properties were introduced. The calculation of radius and attainability for exemplary structures were presented. In Sect. 3, the proposal of the algorithm determining server placement was presented. An illustration of the main algorithm steps for the exemplary structure was given. In Sect. 4, the results of simulation tests for verification the algorithm (implemented in Riverbed Modeler environment) were described. In Sect. 5, some concluding remarks were presented.

## 2 The Basic Definitions and Assumptions

**Definition 1** The logical structure of processors network we call the structure of $n$-dimensional cube if is described by coherent ordinary graph $G = E, U$ ($E$—set of computer, $U$—set of bidirectional data transmission links), which nodes can be described (without repetitions) by $n$-dimensional binary vectors (labels) in such a way that

$$\left[\delta\left(\varepsilon\left(e^{'}\right), \varepsilon\left(e^{''}\right)\right) = 1\right] \Leftrightarrow \left[\left(e^{'}, e^{''}\right) \in U\right] \tag{1}$$

where $\delta\left(\varepsilon\left(e^{'}\right), \varepsilon\left(e^{''}\right)\right)$ is Hamming distance between the labels of nodes $e^{'}$ and $e^{''}$. The Hamming distance between two binary vectors $\varepsilon\left(e^{'}\right)$ and $\varepsilon\left(e^{''}\right)$. complies with the dependency:

$$\delta\left(\varepsilon\left(e^{'}\right), \varepsilon\left(e^{''}\right)\right) = \sum_{k \in \{1, \ldots, n\}} \left(\varepsilon\left(e^{'}\right)_k \oplus \varepsilon\left(e^{''}\right)_k\right)$$

where:

- $\varepsilon\left(e^{'}\right)_k$—the $k$-th element of the binary vector $\varepsilon\left(e^{'}\right)$,
- $\oplus$—modulo 2 sum.

We investigate the case when skeleton of the network has the logical structure of 4-dimensional hypercube (Fig. 1).

A topology of the hypercube may be represented by an ordinary consistent graph whose nodes are described by 4-dimensional binary vectors such that the Hamming distance between vectors (labels) of the adjacent nodes equals one. If $|E| = 2^4$ and $|U| = 2|E|$, then such graph we called (non labeled) 4-dimensional cube and will be denote by $H^4$. Thus $H^4$ is a regular graph of degree of 4 i.e. such that the degree of a node $e \in E$ we determine as $\mu(e) = |E(e)|$, where $E(e)$ is a set of nodes adjacent to the node $e \in E$ and $\mu(e) = 4$ for each node $e$ of the graph $H^4$.

Let $d\left(e, e^{'}|G\right)$ be the distance between nodes $e$ and $e^{'}$ in a coherent graph $G$, that is the length of the shortest chain (in the graph $G$) connecting node $e$ with the node $e^{'}$.

Let $r(e|G) = \underset{e^{'} \in E(G)}{max} d\left(\left(e, e^{'}\right)|G\right)$ be the greatest distance from the node $e \in E(G)$ to another node of the set $E(G)$, and $r(G)$, and $D(G)$ (respectively) denote the radius and the diameter of a graph $G$ i.e. $r(G) = min\{r(e|G) : e \in E(G)\}$ and $D(G) = max\left\{d\left(e^{'}, e^{''}|G\right) : \left\{e^{'}, e^{''}\right\} \subset E(G)\right\}$.

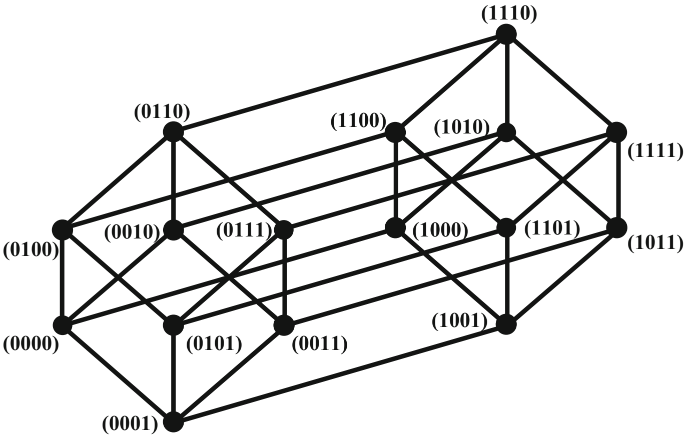


**Fig. 1** 4-dimensional hypercube with labeled nodes

**Property 1** *For the 4-dimensional cube $H^4$ the equation is complied*

$$D\left(H^4\right) = r\left(H^4\right) = 4.$$

*It is known that $D(G) \leq 2r(G)$.*

If $r(e|G) = r(G)$ then the node $e$ is called the central node of the network $G$.

Denote by $E^{(d)}(e|G) = \left\{e' \in E(G): d\left(e, e'|G\right) = d\right\}$ for $d \in \{1, \ldots, D(G)\}$, and by

$$\varsigma(e|G) = \left(\varsigma_1(e|G), \ldots, \varsigma_{r(e|G)}(e|G)\right) \text{ for}$$

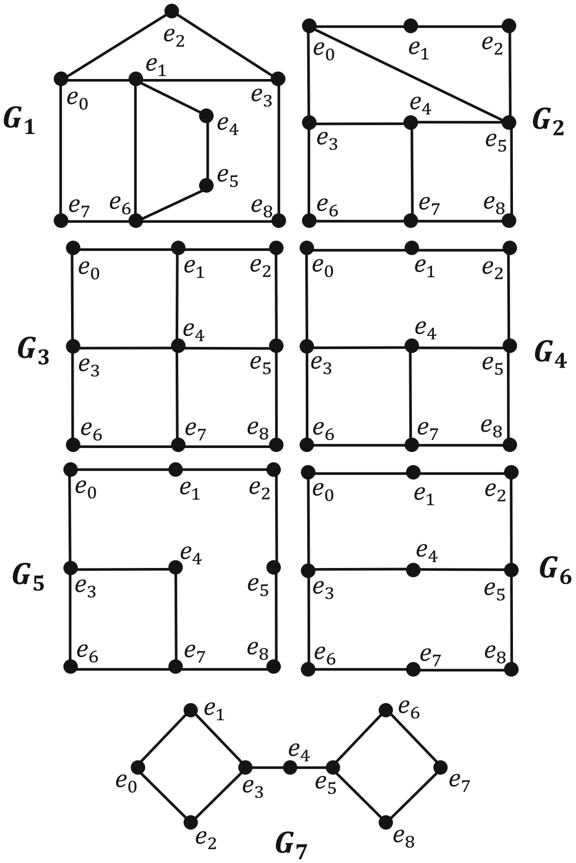
$$\varsigma_d(e|G) = \left|E^{(d)}(e|G)\right| \tag{2}$$

**Definition 2** Let $\varphi(e|G) = \sum_{e' \in E(G)} d\left(e, e'|G\right)(e \in E(G))$ be attainability of the computer $e$ in the network $G$ and $\Phi(G) = \sum_{e \in E(G)} \varphi(e|G)$ be attainability of the network $G$.

Using (2) we have

$$\varphi(e|G) = \sum_{d=1}^{r(e|G)} d\varsigma_d(e|G) \tag{3}$$

**Property 2** $\Phi(H^4) = 512$ because $\forall_{e \in E(H^4)}: \left(r(e|H^4) = 4 \wedge \varsigma_d(e|H^4) = \begin{pmatrix} 4 \\ d \end{pmatrix}\right)$. Using (3) we have $\forall_{e \in E(H^4)}: \varphi(e|H^4) = 32$ and $\left|E(H^4)\right| = 2^4$, then $\Phi(H^4) = \left|E(H^4)\right| \varphi(e|H^4)$ [13].



$G_1$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_2$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_3$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_4$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_5$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_6$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$
$G_7$
$e_0$ $e_1$ $e_2$ $e_3$ $e_4$ $e_5$ $e_6$ $e_7$ $e_8$

**Fig. 2** Example of cyclic subgraphs of $H^4$ order 9 [14]

*Example 1* Figure 2 presents all the seven possible cyclic structures upon the occurrence of $k = 7$ consecutive failures of processors of the network $H^4$ which are the subgraphs of $H^4$ [14].

It should be noticed, that for the given network structure $G$ on the base of the obtained measures $r(e|G)$ it would be rational to choose the server placement at the central node of the network or in the node with the minimum value $r(e|G)$. In some cases (let's consider the structures $G_2, G_4, G_5, G_6$ see Table 1) we are not able to choose the best server placement. Then we can have determined $\varsigma(e|G)$ using (2) and $\varphi(e|G)$ using (3) for these structures. Table 2 shows the values of $\varsigma(e|G)$ and $\varphi(e|G)$ and $\Phi(G)$ for all structures presented in Fig. 2.

**Definition 3** Let $T = E, U^*$ be the dendrite i.e. such coherent acyclic partial graph of $G$ that:

$$\exists e^{'}, e^{''} \in U \Rightarrow e^{'}, e^{''} \in U^{*} \Leftrightarrow \left[\left(d\left(e_i, e^{'}\right) \neq d\left(e_i, e^{''}\right)\right) \wedge d\left(e^{'}, e^{''}\right) = 1\right] \text{ for } r(e_i) = \underset{e \in E(G)}{min} r(e).$$

**Table 1** The $r(e,G)$, $r(G)$, and $D(G)$ for the structures presented in the Fig. 2

| $r(e\|G_i)$ <br> $e \in E(G)$ | $r(e\|G_1)$ | $r(e\|G_2)$ | $r(e\|G_3)$ | $r(e\|G_4)$ | $r(e\|G_5)$ | $r(e\|G_6)$ | $r(e\|G_7)$ |
|---|---|---|---|---|---|---|---|
| $e_0$ | 3 | 3 | 4 | 4 | 4 | 4 | 6 |
| $e_1$ | 2 | 4 | 3 | 4 | 4 | 4 | 5 |
| $e_2$ | 4 | 4 | 4 | 4 | 4 | 4 | 5 |
| $e_3$ | 3 | 3 | 3 | 3 | 4 | 3 | 4 |
| $e_4$ | 3 | 3 | 2 | 3 | 4 | 3 | 3 |
| $e_5$ | 4 | 3 | 3 | 3 | 4 | 3 | 4 |
| $e_6$ | 3 | 4 | 4 | 4 | 4 | 4 | 5 |
| $e_7$ | 3 | 4 | 3 | 4 | 4 | 4 | 6 |
| $e_8$ | 3 | 3 | 4 | 4 | 4 | 4 | 5 |
| $r(G)$ | 2 | 3 | 2 | 3 | 4 | 3 | 3 |
| $D(G)$ | 4 | 4 | 4 | 4 | 4 | 4 | 6 |

The dendrite $T$ is a communication structure of $G$. The algorithm for determined the dendrite $T$ is presented in Sect. 3.

## 3 The Method of Optimal Server Placement and a Network Communication Structure Determining

The method consists of two phases. In the first phase, the node satisfying the equations $r(e_i) = \min_{e \in E(G)} r(e)$ or $\varphi(e_i|G) = \min_{e \in E(G)} \varphi(e|G)$ is chosen as the *server placement*. In the second phase, for chosen node the dendrite $T$ (communication structure satisfying the condition $d_{max}(e_i|T) = r(e_i)$) is determined. Based on the presented method, the algorithm for determining the server placement and the communication structure was developed.

*The algorithm for determining the server placement and communication structure.*

Step 1. Determine $r(e|G)$ for $e \in E(G)$.

Step 2. Choose a node $e_i \in E(G)$ such that $r(e_i) = \min_{e \in E(G)} r(e)$.
If $|\{e_i\}| > 1$ go to step 3 else go to step 5.

Step 3. Determine $\varphi(e|G)$ for $e \in E(G)$.

Step 4. Choose a node $e_i \in E(G)$ such that $\left(\varphi(e_i|G) = \min_{e \in E(G)} \varphi(e|G)\right) \wedge \left(\mu(e_i) = \max_{e \in E(G)} \mu(e)\right)$.
Selected node $e_i$ will be a central node of dendrite.