JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

This issue of the *Journal of Telecommunications and Information Technology* contains eleven papers that deal with a wide range of problems related to the security of computer and industrial networks, focusing primarily on assessing risks that affect critical infrastructures, as well as on protecting mobile service robots, the Internet of things and blockchain systems against cyber-attacks. The articles deal also with wire and wireless communications, various aspects of energy conservation in data centers and computer networks, and with the application of modern multimedia techniques in didactics.

The first four papers published in this issue of the Journal are devoted to the protection of critical national infrastructure. Research conducted in this field was inspired by the authors' participation in the National Cybersecurity Platform – a project funded by the National Centre for Research and Development, under the CyberSecIdent Program. The goal of this project is to develop a comprehensive, integrated system enabling to monitor, detect and warn about threats identified, virtually in real time, in the State's cyberspace. Two subsequent articles deal with the assessment of cyber risk existing at national level. Selected approaches to cyber risk management are discussed in the paper titled *A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence*. Marek Janiszewski, Anna Felkner and Piotr Lewandowski claim that there are no comprehensive platforms for national level risk assessment. In the majority of cases, the risk is estimated for specific institutions only. The authors propose a method for real-time risk analysis, performed by clients at various levels, and suggest a technique used for aggregating the results on the nationwide level. This technique allows to foresee cyber threats and to build situational awareness by monitoring the current situation in any computer network. Another approach to risk management is proposed by Andrzej Karbowski *et al*. in the paper titled *Critical Infrastructure Risk Assessment Using Markov Chain Model*. Application of the Markov chain model for the purpose of assessing the risk affecting critical infrastructure is described in the article. In this model, specific states represent the potential security levels of different services, assessed based on their availability. Results of preliminary experiments

performed in relation to a scenario involving two services, i.e. healthcare and power supply, are presented and discussed. The authors argue that application of Markov chains is one of the most promising approaches to modeling the propagation of risky events in the area of cybersecurity. The problem of security in operational technology networks (OT) is outlined in the paper titled *On Preventing and Detecting Cyber Attacks in Industrial Control System Networks*. Adam Padée *et al*. provide a review of techniques for protecting and detecting cyber-attacks affecting industrial systems. Their attention is focused on the nuclear industry. Common components of OT security systems are described and compared with those used in the IT domain. In the paper titled *Cyber-security for Mobile Service Robots – Challenges for Cyber-physical System Safety*, Wojciech Dudek and Wojciech Szynkiewicz consider the problem of cybersecurity of robot systems. They provide a brief overview of threats affecting cyber-physical robotic systems, caused by cybernetic attacks, and propose methods that may be relied upon to detect and mitigate the consequences of such attacks. The authors claim that there is a great need to develop new solutions for securing service robots against cyber-attacks, and present those issues regarding the cybersecurity of robot systems that still need to be resolved.

Next two papers focus on the security of IoT and blockchain networks. In the paper titled *Battery Drain Denial-of-Service Attacks and Defenses in the Internet of Things*, Philokypros P. Ioulianou, Vassilios G. Vassilakis and Michael D. Logothetis investigate the possibility of battery drain Denial-of-Service (DoS) attacks affecting the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) of the Contiki operating system. The authors present the results of simulation experiments that demonstrate the impact of DoS attacks on the power consumption of IoT devices. They discuss the potential defense techniques relying on distributed intrusion detection systems. In the paper *Blockchain Networks – Security Aspects and Consensus Models*, Andrzej Wilczyński and Adrian Widłak propose a generic architecture model of a blockchain system, and offer the concept of consensus models used in blockchain transactions. To illustrate the performance of the proposed solutions, the results of practical use cases are presented and discussed as well. The authors' attention focuses primarily on security-related aspects.

The paper titled *CL-mWSNs: Cross Layer Model-Based QoS Centric Routing Protocol for Mission-Critical Cooperative Communication in Mobile WSNs* deals with efficient wireless communication techniques and with practical application scenarios involving wireless sensor networks (WSN). A robust Quality of Service (QoS)-centric routing protocol that exploits dynamic network states from the various layers of the IEEE 802.15.4 standard is presented. The protocol is dedicated to mission-critical communication in mobile WSNs. Kummathi C. Reddy, Geetha D. Devanagavi and Thippeswamy M. N. argue that their protocol ensures high throughput, as well as minimum loss and low latency rates. The results of simulation experiments presented in the paper confirm the efficiency of the presented technique.

Communication protocols for Unmanned Aerial Vehicle (UAV) systems are investigated by Kiyoshi Ueda and Takumi Miyoshi in their paper titled *Autonomous Navigation Control of UAV Using Wireless Smart Meter Devices*. The authors introduce and describe a new routing protocol enabling to establish a safe route based on a network of smart meters. They propose a control method in which the UAV communicates with the nodes, acquires information necessary for sensing its position and navigates by following the route, as if the UAV were a data packet within a network. The current distance between the UAV and a given node within the network of smart meters is measured by means of radio transmission loss value. The solution may be used for performing home deliveries that rely on UAVs.

Two subsequent papers address the vital problem of infrastructure and energy conservation in computer networks and data centers. In the paper titled *Infrastructure and Energy Conservation in Big Data Computing: A Survey*, Ewa Niewiadomska-Szynkiewicz and Michał P. Karpowicz provide a review of recent Big Data processing technologies. The emphasis is placed on the most popular middleware and software platforms and energy saving approaches that may be relied upon by data centers. A heuristic algorithm for energy efficient allocation of network resources, based on the current workload, is presented in the paper titled *Optimized Energy Aware Resource Allocation Algorithm Using Software Defined Network Technology*. The solution presented is based on the architecture of a Software Defined Network (SDN). Ranya Al-Musawi and Obada Al Khatib present simulation results confirming

good performance of their method which allows to reduce energy consumption compared to solutions described in literature.

The last paper, titled *Multimedia Mathematical Communication in a Diverse Group of Students*, tackles the problem of learning mathematics by visually impaired persons. The emphasis is placed on efficiency of communication in the learning process. Jolanta Brzostek-Pawłowska presents interactive multimedia solutions fostering mathematical communication within a group of students with a range of diverse visual impairments, under the teacher's guidance. The results of qualitative surveys of the proposed approach confirm its usefulness and positive impact on the efficiency of the work of a group learning mathematic.

We do hope that our Readers will find this issue of the Journal both interesting and enjoyable.

Ewa Niewiadomska-Szynkiewicz
Guest Editor

https://doi.org/10.26636/jtit.2019.preface2