Preface

Special Issue on 5G & Cybersecurity

In an increasingly interconnected and technology-dependent world, cybersecurity has emerged as a cornerstone for safeguarding the very systems that underpin modern society. It is essential for protecting sensitive information – whether corporate or personal – from unauthorized access and cyberattacks. With the increasing reliance on digital systems, strong cybersecurity measures ensure the integrity and availability of critical infrastructure, such as telecommunication, logistics, healthcare, finance, or energy. Cybersecurity also helps safeguard privacy and builds trust between organizations and their customers. As cyber threats evolve, ongoing vigilance and adaptation are necessary to maintain security in this highly connected world.

The advent of 5G technology introduces profound changes to telecommunication networks, expanding the scope and complexity of cybersecurity challenges. 5G networks have significantly larger attack surface as they are able to connect more devices, operate at higher bandwidth, they are more attractive to attack as they are connecting together critical and edge computing infrastructures, foster network dependency of companies, institutions and individuals at national scale, promise higher degree of automation and control in industries like manufacturing and autonomous vehicles. As 5G infrastructures start to handle significantly larger scale data, any breach or disruption in 5G networks could have devastating consequences. Attackers can vary from unskilled skiddies, professional individuals, small expert groups or State-Sponsored Cyber Teams. As 5G becomes part of the global critical infrastructure, nation-state actors, organized crime members may seek to exploit vulnerabilities in 5G networks. With 5G's lower latency and higher speeds, cyberattacks can occur and propagate more quickly. This means that traditional defensive responses have to be revised and updated to cope with new problems and to prevent damage.

This special issue brings together a carefully curated selection of papers from an open call. Out of the many submissions, seven papers were rigorously reviewed and accepted thorough a two-level reviewing process. These research articles reflect the wide-ranging spectrum of contemporary cybersecurity challenges, covering topics from the analysis of cyber threats and vulnerabilities in vehicles, 5G radio noise vulnerability assessment, to automated cybersecurity risk evaluation for industrial systems and advanced 5G network monitoring with Security Operations Centers (SOCs). This volume offers a diverse collection of cybersecurity case studies, empirical research, and practical applications, specifically focusing on the 5G and automotive sectors. The research presented here will be valuable to both academic scholars and industry practitioners in the field of cybersecurity.

A unique aspect of this special issue is its multidisciplinary approach. It provides valuable insights into 5G network security, automotive and industrial systems, automated vulnerability assessments, and real-time monitoring technologies. The exploration of automated, multi-tier security operations and the advancement of threat elimination capabilities within 5G networks and self-driving vehicles are critical milestones for establishing trustworthy and resilient infrastructures in the near future.

Guest editors:

Miklos Kozlovszky

habil. Ph.D., Professor

Obuda University, John von Neumann Faculty of Informatics

Anna Bánáti

Ph.D., Associate Professor

Obuda University, John von Neumann Faculty of Informatics

Budapest, Hungary

January 2025