electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.397

CITESCORE 2.7 SCOPUS

Security of Wireless Communications

Guest Editors:

Prof. Dr. Xun Yi
School of Computer Science and Software Engineering, RMIT University, Melbourne 3000, Australia

xun.yi@rmit.edu.au

Dr. Andrei Kelarev
School of Computer Science and Software Engineering, RMIT University, Melbourne 3000, Australia

andrei.kelarev@rmit.edu.au

Dr. Xingliang Yuan
Department of Software Systems and Cybersecurity, Monash University, Clayton, VIC 3168, Australia

xingliang.yuan@monash.edu

Deadline for manuscript submissions:
closed (28 February 2022)

Message from the Guest Editors

Dear Colleagues,

Various aspects of the security of wireless communications are extremely important for the successful operation and widespread adoption of modern information technologies. Wireless communications have special requirements and vulnerabilities, and therefore are of special concern. In particular, wireless networks are vulnerable to malicious attacks and the number of potential threats has been increasing dramatically. Recently, considerable novel challenges have emerged in view of the rapid growth of advanced applications of wireless communications in commercial and industrial domains embracing Wireless Sensor Networks and the Internet of Things. In order to overcome these challenges, it is vitally important to develop a range of novel approaches as well as sophisticated combinations of useful and efficient security techniques. Relevant security measures include data encryption and device and user authentication. Privacy-preserving data mining is also essential for secure analysis of the big data pertaining to wireless communications.