



Cybersecurity for Wireless Networking

Guest Editors:

Dr. Neetesh Saxena

School of Computer Science and Informatics, Cardiff University, Queen's Buildings, 5 The Parade, Newport Road, Cardiff CF24 3AA, UK

nsaxena@ieee.org

Dr. Prosanta Gope

Department of Computer Science, University of Sheffield, Sheffield S1 4DP, UK

p.gope@sheffield.ac.uk

Dr. Daisuke Mashima

Illinois at Singapore Pte Ltd., Advanced Digital Sciences Center, Singapore

daisuke.m@adsc-create.edu.sg

Deadline for manuscript submissions:

closed (31 December 2020)

Message from the Guest Editors

Today's connected world is full of internet-connected devices. Internet-connected devices also often collect personal information, compromise communicated or stored data, and steal identities over insecure wireless networks. Hardware- and/or software-based solutions help in securing wireless networks against advanced cyberattacks. The main aim of this Special Issue is to report on recent high-quality research that addresses the key issues with novel and state-of-the-art solutions that could provide the right level of security to wireless networking. Topics of interest include but are not limited to the following:

- Authentication techniques for IoT and sensor networks;
- Access control techniques for IoT and sensor networks;
- Techniques for securing software-defined networking;
- Cloud-computing based techniques for secure networking;
- Identity and data privacy in IoT and sensor networks;
- Techniques for securing industrial control systems infrastructure;
- Techniques for securing RFID based systems;
- AI/ML-driven techniques for securing IoT and sensor networks.

