

IEEE International Workshop on 5G & Beyond Wireless Security (IEEE Wireless-Sec 2021)

June 14–18, 2021
Montreal, Canada



General Chairs

Min Song, Stevens Institute of
Technology, USA

Danda B Rawat, Howard
University, USA

TPC Chairs

Danda B Rawat, Howard
University, USA

Min Song, Stevens Institute of
Technology, USA

Main contact

db.rawat@ieee.org,
danda.rawat@howard.edu

Important Dates

- ❖ Paper submission
deadline: **Jan. 20, 2021**
- ❖ Notification of acceptance:
February 20, 2021
- ❖ Camera-ready papers:
March 1, 2021

Submission link

<https://edas.info/N27579>

Webpage link

[Webpage at ICC](#)

or

<http://shorturl.at/tER47>

Scope

Future wireless systems will require a paradigm shift in how they are networked, organized, configured, optimized, and recovered automatically, based on their operating situations. Emerging Internet of Things (IoT) and Cyber-Physical Systems (CPS) applications aim to bring people, data, processes, and things together, to fulfill the needs of our everyday lives. With the emergence of software defined networks, adaptive services and applications are gaining much attention since they allow automatic configuration of devices and their parameters, systems, and services to the user's context change. It is expected that upcoming Fifth Generation and Beyond (5G&B) wireless networks, known as more than an extension to 4G, will be the backbone of IoT and CPS, and will support IoT systems by expanding their coverage, reducing latency and enhancing data rate. However, there are several challenges to be addressed to provide resilient connections supporting the massive number of often resource-constrained IoT and other wireless devices. Hence, due to several unique features of emerging applications, such as low latency, low cost, low energy consumption, resilient and reliable connections, traditional communication protocols and techniques are not suitable. In this regard, it is crucial to have security by design in 5G and Beyond wireless networks, considering the constraints imposed by heterogeneous IoT and CPS systems. Our aim is to promote the development of 5G security by design. The proposed ICC workshop *Wireless-Sec 2021* will serve as a forum for researchers from academia, government and industries, to exchange ideas, present new results, and provide future visions on these topics.

Topics

We seek original completed and unpublished work not currently under review by any other journal/magazine/conference. Topics of interest include, but are not limited to:

- 5G & Beyond architecture with security and privacy
- Security for new service delivery models
- AI and Machine Learning for 5G and Beyond security
- Verticals and business (non-technical) 5G & Beyond security requirements and solutions
- Big data analytics in 5G & Beyond Security
- Advances in lightweight cryptography for IoT/CPS
- Wireless virtualization and slicing security
- Authentication, authorization, and accounting
- AI and Machine Learning for 5G & Beyond security
- Diameter security in 5G & Beyond
- Quantum Safe Cryptography for 5G & Beyond
- Secure Integration of IoT/CPS and Cloud Computing
- Secure integration of IoT /CPS and other networks
- Secure Device-to-Device communications
- Intrusion Detection/Prevention Techniques
- Secure data storage, communications and computing
- Energy efficient security in IoT and CPS
- Heterogeneous system modeling for 5G security
- Secure sensing and computing techniques
- Big data analytics for 5G & Beyond security
- Secure, privacy-aware and trustworthy IoT/CPS communications
- Trust models and trust handling/propagation for 5G & Beyond security
- Physical layer security for 5G & Beyond
- 5G & Beyond security standardization

Paper Submission

The workshop accepts only novel, previously unpublished papers. The page length limit for all initial submissions for review is SIX (6) printed pages (10-point font) and must be written in English. All final submissions of accepted papers must be written in English with a maximum paper length of six (6) printed pages (10-point font) including figures. No more than one (1) additional printed page (10-point font) may be included in final submissions and the extra page (the 7th page) will incur an over length page charge of USD100. For more information, please see IEEE ICC 2021 official website: <https://icc2021.ieee-icc.org/authors>