THE IEEE 5G WORLD FORUM IS NOW THE

IEEE Future Networks™ WORLD FORUM • 2022

MONTREAL, CANADA - 12-14 OCTOBER


# Call for Papers

## SYMPOSIUM ON SECURITY FOR 5G AND FUTURE NETWORKS

### SYMPOSIUM CO-CHAIRS

**Antonio Skarmeta**, Universidad de Murcia, Spain, skarmeta@um.es
**Pascal Bisson,** Thales, France, pascal.bisson@thalesgroup.com
**Ved P. Kafle**, National Institute of Information & Communications Technology, Japan, kafle@nict.go.jp
**Chamseddine Talhi**, École de technologie supérieure, Canada, Chamseddine.Talhi@etsmtl.ca

### SCOPE AND MOTIVATION

The 5G long term vision is to "turn the network into an energy-efficient distributed computer system that enables agile and dynamic creation, move and suppression of processes and services in response to changing customer demands and information flows, and that supports interaction with humans through new communication modes, such as gestures, facial expressions, sound, and haptics. To make this vision a reality, a shift towards a full automation of network and service management and operation is a necessity. However, a major challenge facing full automation is the protection of the network and system assets (i.e., services, data and network infrastructure) against potential cybersecurity risks introduced by the unprecedented evolving 5G threat landscape. Indeed, the risk of full automation is the ability to replicate a small isolated error or attack broadly and rapidly, putting the entire critical ecosystem (multi-party/tenant/technologies) into peril.

Although 5G and beyond-5G offer a multitude of benefits to the emerging applications, they are susceptible to the malicious or inadvertent introductions of vulnerabilities, such as malicious software or hardware, counterfeit components, and poor designs. Even worse, these new technologies are facing a series of inherent security and privacy threats, which intensify the vulnerabilities of the 5G networks. In addition, vastly increased numbers of devices and an elevated use of virtualization result in more 5G security threats and a broader, multifaceted attack surface. To realize strong and healthy communication networks, exploring the approaches to address the security and privacy threats are vital for both industry and academia. To address the aforementioned challenges in beyond 5G or 6G telecommunication infrastructure and services, the inherent support of full automation operations in

network and service management is a necessity. One of the most critical areas of application for zero touch automation is the protection of the network and system assets against potential cybersecurity risks introduced by the unprecedented evolution of the 5G threat landscape.

Our aim is to promote the development of 5G security by design.

## TOPICS OF INTEREST

We invite submissions on a wide range of research topics, spanning both theoretical and systems research, including results from industry and academic/industrial collaborations, related but not restricted to the following topics:

- 5G and Beyond architecture with security and privacy considerations
- Security for new service delivery models
- AI and Machine Learning for 5G and Beyond security
- Verticals and business (non-technical) 5G and Beyond security requirements and solutions
- Big data analytics tools and techniques in 5G and Beyond Security
- Advances in lightweight cryptography and IoT security
- Wireless virtualization and slicing security
- Authentication, authorization, and accounting (AAA) for 5G and Beyond security
- Diameter security in 5G and Beyond
- Tera-Hertz communication and security for 5G and Beyond
- Millimeter wave and security for 5G and Beyond
- Quantum Safe Cryptography for 5G and Beyond
- Secure Integration of IoT and Cloud Computing
- Secure Device-to-Device communications in 5G and Beyond
- Secure integration of IoT and other networks
- Intrusion Detection/Prevention Techniques and System Integrity
- Secure data storage, communications and computing
- Energy efficient security in IoT
- Heterogeneous system modeling for 5G and Beyond security
- Secure sensing and computing techniques in 5G and Beyond
- Big data analytics for 5G and Beyond security
- Secure, privacy-aware and trustworthy IoT communications
- Trust models and trust handling/propagation for 5G and Beyond security
- Physical layer security for 5G and Beyond
- 5G and Beyond security standardization
- Privacy-preserving Machine Learning or Deep Learning in 5G and Beyond
- Adversarial Machine Learning or Deep Learning in 5G and Beyond
- Trustworthiness and Fairness in Artificial Intelligence for 5G and Beyond
- Security and Privacy for Blockchain Technology in 5G and Beyond
- Security and Privacy for Data-centric Networks in 5G and Beyond
- Security and Privacy for Fog Computing in 5G and Beyond
- Security and Privacy for Software-Defined Networks
- Security and Privacy for Network Function Virtualization
- Security and Privacy for Drone Communications in 5G and Beyond

## IMPORTANT DATES

Paper Submission: **21 August 2022 (firm)**
Notification: Rolling basis until 31 August 2022
Camera Ready: 7 September 2022

## HOW TO SUBMIT A PAPER

All papers for technical symposia should be submitted via EDAS.
Full instructions on how to submit papers are provided on the IEEE FNWF 2022: https://fnwf.ieee.org/