

**IEEE International Workshop on Computer Aided Modelling and Design of Communication
Links and Networks (CAMAD)**
<https://camad2021.ieee-camad.org/>

CALL FOR PAPERS

Special Session on **“Physical-Layer Methods for Security and Privacy in Beyond
5G/6G and Internet of Things Networks”**

Scope

The 5G network employs novel networking paradigms such as the incorporation massive Machine-Type Communication (mMTC) which enables Internet of Things (IoT) networks. These IoT networks have a wide range of applications, including military and security applications but are often neglected in terms of security and privacy. These security vulnerabilities can be hard to tackle since the distributed nodes in IoT networks are usually constrained by limited energy and processing capabilities. As such, employing conventional and complex data security mechanisms represents a challenge to IoT nodes due to the induced complexity and high energy consumption. Physical-layer security schemes are characterized by their abilities to enable secure transmissions without reliance on computational complex systems and are therefore suitable to secure IoT network communications. Furthermore, security mechanism that reach sufficient levels of security are also of interest to general applications of 5G network communications.

Topics of Interest

This special session aims to soliciting high-quality research articles that aim at providing security and privacy through the exploitation of physical layer parameters. These includes the proposals and investigations of physical-layer security mechanisms that can be applied to 5G and IoT networks. Potential topics of this workshop include, but are not limited to, the following:

- Physical-layer methods for secrecy and privacy for 5G and the IoT
- Physical-layer security in co-located and distributed massive MIMO
- Physical-layer methods for secret key generation
- Secure transmission using Physical Layer Characteristics at mmWave and THz frequencies



- Integration of physical-layer security into full duplex systems
- Secure orthogonal and non-orthogonal connectivity for massive numbers of devices
- Energy-efficient and low-overhead physical-layer secure transmission
- Physical layer security techniques for eMBB, mMTC, and URLLC applications
- Prototype, testbed, simulation, and performance evaluation of physical layer security schemes
- Wireless, biometric, and physical unclonable functions (PUF)-based authentication
- Private information retrieval (PIR)
- Covert and stealth communications

Important Dates

Paper Submission (Extended) Deadline	August 15, 2021
Paper Acceptance Notification	September 15, 2021
Camera-Ready	September 30, 2021
Conference Date	October 25-27, 2021

Submission Guideline

Prospective authors are invited to submit a full paper of not more than six (6) IEEE style pages including results, figures and references. Papers should be submitted via EDAS. Papers submitted to the conference, must describe unpublished work that has not been submitted for publication elsewhere. All submitted papers will be reviewed by at least three TPC members, while submission implies that at least one of the authors will register and present the paper at the conference. Electronic submission will be carried out through the EDAS web site at the following link: <https://edas.info/N28270>

All accepted papers will be included in the conference proceedings and IEEE digital library (<https://ieeexplore.ieee.org/>)

Organizers

Dr. Marcus de Ree, Instituto de Telecomunicações, Portugal

Prof. Jonathan Rodriguez, Instituto de Telecomunicações, Portugal

Dr. Georgios Mantas, Instituto de Telecomunicações, Portugal

Prof. Saud Althunibat, Al-Hussein Bin Talal University, Jordan

Dr. Marwa Qaraqe, Hamad Bin Khalifa University, Qatar

