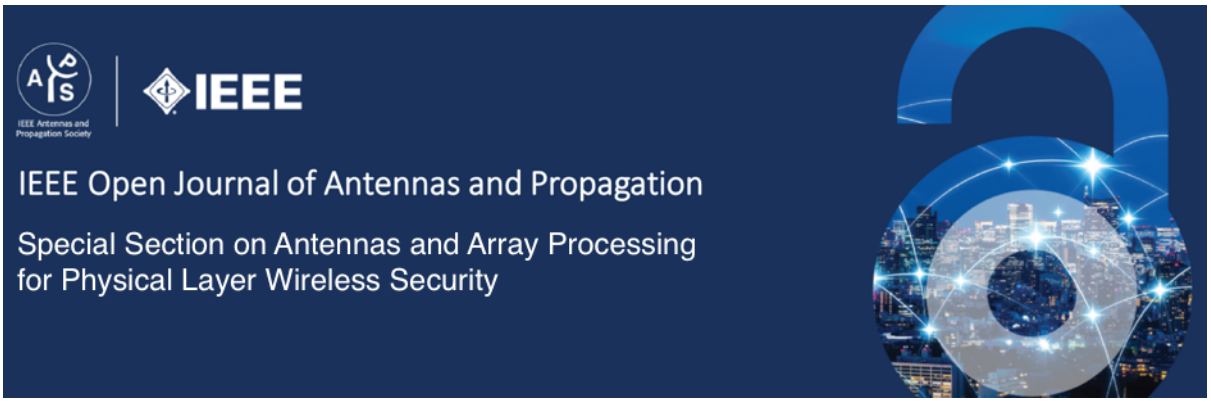
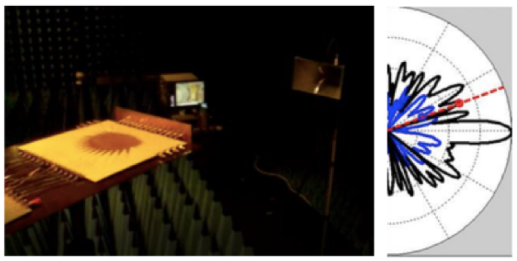


Antennas and Array Processing for Physical Layer Wireless Security

Submission deadline: 30 September 2021



Aims & Scope: How to ensure communication confidentiality represents a key issue for wireless communication, given the broadcasting nature of the wireless transmission media. It becomes even more challenging, owing to the fast advancement of computing technology and wide proliferation of various Internet-of-Things (IoT) devices. Through exploiting the randomness and uniqueness of the channels, physical layer security can help secure the wireless communication confidentiality, thereby representing a promising complementary and/or alternative to conventional mathematical-based encryption techniques. Here the wireless channels include the effects of antennas (arrays) and associated RF fronts and array processing, as well as the reconfigurable intelligent surface that is able to alter the electromagnetic wave propagations.

Physical-layer wireless data transmission security aims to contaminate the analogue signal waveforms such that the useful information signals are masked by high noise levels for eavesdroppers located away from the legitimate recipients. Consequently, the capability to extract information away from the legitimate receivers is fundamentally limited. The waveform manipulation can be achieved using digital signal processing approaches and/or agile analogue RF frontends. For example, the transmitter can synthesize artificial noise in digital baseband to project interference purposely towards eavesdroppers to degrade eavesdropping channels. Alternatively, the transmitter can equip reconfigurable RF frontends to dynamically adapt radiation patterns to scramble waveforms in signal radiation and propagation stages. Another popular technique is key generation and agreement from wireless channels. The common randomness between any two legitimate users can be extracted as possible cryptographic keys. When an eavesdropper is located far away, it experiences uncorrelated channels, and hence cannot observe the same keys.

Despite huge advances made in recent years, it is expected that the advanced antenna systems, including excitation strategy, beamforming strategy, reconfigurability capability, and the tailored array signal processing algorithms will further enhance the security performance. Equally important, this paves the path to address many challenges hindering the practical applications of physical layer wireless security, such as the need for excess computation resources and compromise on energy efficiency, especially in hardware- and energy- constrained systems.

The aim of this Special Section is to solicit original research articles, bringing together researchers and industry professionals to report recent research advances in antennas (and array) enhanced physical-layer security for wireless communication systems. Innovation concepts with experimental validation are especially welcome. We also invite researchers to contribute comprehensive review articles that identify challenges and opportunities for this fast-evolving research area.

Potential topics include but are not limited to the following:

- Active antennas for directional modulation techniques and their supporting algorithms
- Antenna and/or RF enabled physical-layer wireless security in resource-constrained systems
- Antenna and/or RF enhanced key generation and agreement from wireless channels
- Physical-layer wireless security in emerging wireless systems: analysis and synthesis from electromagnetic perspective
- Demonstrable reconfigurable intelligent surface enabled physical-layer wireless security

- Practical experimental validation and demonstration

Keywords:

1. Directional modulation
2. Wireless key generation
3. Array signal processing
4. Physical layer wireless security
5. Reconfigurable intelligent surface
6. Advanced antenna systems

Accepted papers will immediately appear on IEEE Xplore®, forming an expanding collection of reference material on Antennas and Array Processing for Physical Layer Wireless Security.

Lead Guest Editor

Yuan Ding
Heriot-Watt University, UK
yuan.ding@hw.ac.uk

Guest Editors

Xingwang Li
Henan Polytechnic University, China
lixingwang@hpu.edu.cn

Stefano Tomasin
University of Padova, Italy
stefano.tomasin@unipd.it

Junqing Zhang
University of Liverpool, UK
junqing.zhang@liverpool.ac.uk

Wei Liu
University of Sheffield, UK
w.liu@sheffield.ac.uk

Ming Zeng
Université Laval, Canada
ming.zeng@gel.ulaval.ca