Joint 6G-PHYSEC & INTERACT Workshop on 6G technologies and PHY layer security June 17th, 2024, Helsinki, Finland

Call for participation

With the rapid evolution of wireless networks across a broad technological environment which includes virtualization, IoT and Industry 4.0+, our lives are surrounded by electronic devices capable of wireless radio transmission and reception, not only for communication purposes but also for radar, wireless sensing, and radio environment monitoring and mapping. Emerging 6G, Internet of Things (IoT) and Cyber-Physical Systems (CPS) applications aim to bring people, data, processes, and things together to fulfil our needs. However, the rise of large-scale, dynamic wireless networks and IoT devices presents new challenges for security. Data and communication security have always been a focal point in wireless communication, and we have had great success with bit level cryptographic techniques and associated protocols at various levels of the data processing stack. Recently, new security approaches built on information theory fundamentals and by exploiting the secrecy capacity of the propagation channel have gained significant interest. This context has prompting researchers to explore complementary technologies to enhance security across PHY, MAC, and network layers.

This joint workshop aims to gather researchers from both INTERACT and 6G-PHYSEC actions to discuss emerging wireless technologies for 6G in both communication and sensing applications, as well as related PHY layer security aspects. Topics of interest are, but not limited to, the following:

- Wireless communication trends, requirements and use-cases
- Wireless channels and channel sounding
- Reconfigurable Intelligent Surfaces
- Integrated sensing and communications
- Exploiting emerging 6G technologies for security provisioning
- Attacks: Eavesdropping, Spoofing & Jamming
- Cross-layer security
- Secure communication & other advanced radio access technologies
- Security in URLLC (URLL & Secure communication)
- Security in vehicular networks (V2V and V2I), IoT, health, or mission critical applications

Deadline for response to CFP: March 31st, 2024 (tentative title, authors and half-page summary)

Organizers:
Diana Pamela Moya Osorio (Linköping University, Sweden),
Hüseyin Arslan (Istanbul Medipol University, Turkey),
Roman Maršálek (Brno University of Technology, Czechia)