Call for Papers

The International Workshop on

Physical Layer Security in Future Integrated Networks (**PLSFIN**)

Scope and Motivations

The sixth generation (6G) mobile communications will integrate current networks to provide ubiquitous connectivity for massive devices and applications. The future networks are facing new security and privacy challenges. The future networks should provide three-dimensional coverage in a wide range so that the links are vulnerable to be attacked. The integration of heterogeneous systems and architectures introduces high complexity to satisfy diverse security and privacy requirements. Massive nodes are distributed in a wide range and some of them have limited energy and processing capability.

Physical layer security (PLS) leverages the native features in wireless links and communicating hardware, and provides a lightweight paradigm to guarantee secure transmissions. Secrecy capacity-based PLS approaches enhance channel capacity of the legitimate link compared to its eavesdropping counterpart to secure transmissions. Knowledge extracted from signals, such as channel characteristics and radio fingerprinting, can be used for key establishment, authentication, and malice detection. Nowadays, artificial intelligence and machine learning (AI/ML) have raised changes on almost every level of industry, including information protection. The fusion of AI/ML and PLS is a promising solution to achieve stronger security in future network.

Topics of Interest

Emerging techniques will spark more innovative ideas that can improve the security of future integrated networks. This workshop invites researches and contributions of PLS in addressing the challenges of security protection. The topics of interest include, but are not limited to:

- Physical layer methods for secure communication
- Novel architecture design for PLS
- Modeling and performance analysis for PLS
- Prototype, testbed, simulation, and performance evaluation of PLS schemes
- Efficient and effective physical layer secure transmission
- Security and privacy protection in integrated networks
- Physical layer methods for key establishment, management, and distribution
- Physical layer methods authentication and malicious nodes detection
- Optimization of system design, deployment, and management for secure transmission
- AI/ML for PLS
- Covert communications

Important Dates

- Paper submission deadline: 1 August, 2025
- Author notification: 5 October, 2025
- Final manuscript due: 20 October, 2025
- Registration due: in accordance with TrustCom 2025

Submission Instructions

All papers need to be submitted electronically through the conference submission website https://edas.info/N34127 with PDF format. The length of the papers should not exceed 6 pages +2 pages for over length charges. Manuscript Templates for Conference Proceedings can be found at: https://www.ieee.org/conferences_events/conferences/publishing/templates.html.

Once accepted, at least one of the authors of any accepted paper is requested to register the paper at the conference

Workshop Chairs

ZHU Wei-Ping, Concordia University, Canada
LIN Min, Nanjing University of Posts and Telecommunications, China
LUO Liping, Guangxi Minzu University, China
CHENG Ming, Nanjing University of Posts and Telecommunications, China

Contact

Please email inquiries concerning the workshop to: mingcheng@njupt.edu.cn.