SPCC

Signal Processing and Computing for Communications (SPCC) TC
Workshop and Presentation of Student Challenge Finalists

October 22nd, 2024
15:00 – 17:00 CEST
Online

The IEEE Signal Processing and Computing for Communications (SPCC) technical committee (TC) has organized a contest for student teams that involves:
- innovative ideas and proposals to provide an answer to a technical challenge, to be chosen from a set of possible proposed ones
- and the preparation of video to present the proposal.

In this online workshop the finalists will present their proposals and will be inspired by some knowledgeable speakers in the chosen areas.

Technical challenges

The following are the technical challenges that the students have selected to address.

Finalist Team 1: Towards a greener and more energy efficient network, reconfigurable intelligent surfaces (RISs) are envisaged to be a promising 6G technology. Please identify one major challenge introduced to cellular networks in terms of signal processing after deploying RISs, and provide possible solutions.

Finalist Team 2: How can you use physical layer security techniques to address the security challenges in 6G?

Workshop schedule

1. Introduction by SPCC TC Chair
2. Presentations prepared by the two teams of students
3. Invited talk: Eirini Eleni Tsiropoulou, Wireless communications in Concentrated Solar Power Fields
4. Invited talk: Linda Senigagliesi, Robust physical layer authentication techniques based on angle-of-arrival estimation and machine learning algorithms
5. Final remarks

Workshop attendance

The workshop is open to the SPCC TC members as well as to any external attendees.
Please use the following link to connect:

https://eu.bbcollab.com/guest/daa1f74fbc7c47cba1637d120bff2621

Invited talks

Wireless communications in Concentrated Solar Power Fields, by Eirini Eleni Tsiropoulou

Abstract: This tutorial introduces the audience to the use of wireless communications to automate control processes in Concentrated Solar Power (CSP) fields. First, Integrated Access and Backhaul (IAB) technology is introduced as a solution to overcome the constraints of traditional wired or basic mesh networks. The IAB technology separates the access and backhaul communication links and also optimizes the spectrum usage in order to guarantee more efficient, high-bandwidth data transmissions of the heliostats' wireless communication modules communicating with the Central Station (CS). Second, the introduction of AI-driven Network Reconfiguration and Entropy-based Routing represents a significant leap in wireless communication within CSP systems. With Reinforcement Learning algorithms, the heliostats are capable of autonomously adapting their communication strategies based on the environmental conditions, e.g., shadowing, interference, and energy constraints. These adaptive RL algorithms ensure that the heliostats select the most energy-efficient communication clusters and routes, and they reduce the overall network congestion while maintaining reliable data transmission. The third innovation focuses on the Dynamic Spectrum Management and Interference Mitigation. By employing a joint optimization framework, the proposed wireless communication system maximizes the spectrum efficiency across both the access and backhaul communication links while it minimizes the interference within the network of wirelessly connected heliostats. Lastly, the tutorial addresses the Validation and Testing processes of these wireless technologies in CSP settings.

Dr. Eirini Eleni Tsiropoulou (IEEE Senior Member) is an Associate Professor at the School of Electrical, Computer and Energy Engineering, Ira A. Fulton Schools of Engineering, Arizona State University. She obtained her Diploma in Electrical and Computer Engineering from National Technical University of Athens in 2008 and her MBA in techno-economics from the same institute in 2010. She graduated with a Ph.D in Electrical and Computer Engineering from National Technical University of Athens in 2014. Her main research interests lie in the area of cyber-physical systems and wireless heterogeneous networks, with emphasis on network modeling and optimization, resource orchestration in interdependent systems, reinforcement learning, game theory, network economics, and Internet of Things. Five of her papers received the Best Paper Award at IEEE WCNC in 2012, ADHOCNETS in 2015, IEEE/IFIP WMNC 2019, INFOCOM 2019 by the IEEE ComSoc Technical Committee on Communications Systems Integration and Modeling, and IEEE/ACM BRAINS 2020. She was selected by the IEEE Communication Society - N2Women - as one of the top ten Rising Stars of 2017 in the communications and networking field. She received the NSF CRII Award in 2019, the Early Career Award from the IEEE Communications Society Internet Technical Committee in 2019, the Junior Faculty Teaching Excellence Award, Dean's Excellence Award, and Research and Creative Works Leader Award, School of Engineering, University of New Mexico in 2018, 2021, and 2023, respectively. Her research is mainly supported by the Department of Energy, National Science Foundation, and industry. She is an Associate Editor for IEEE Transactions on Green Communications and Networking, IEEE Transactions on Machine Learning in Communications and Networking, IEEE Networking Letters, IEEE Transactions on Network Science and Engineering, IEEE IT Professional, IEEE Vehicular Technology Magazine, IEEE Transactions on Consumer Electronics, and IEEE/ACM Transactions on Networking. Dr. Tsiropoulou is a Co-Chair of the N^2 Women discipline-specific community.

Robust physical layer authentication techniques based on angle-of-arrival estimation and machine learning algorithms, by Linda Senigagliesi

Abstract: While prior research predominantly focuses on physical layer authentication (PLA) leveraging physical attributes like channel frequency/impulse response or received signal strength, the exploration of angle-of-arrival (AoA) in this capacity remains largely unexplored concerning its potential in fortifying defenses against impersonation (spoofing) attacks.

In this talk we will discuss the use of AoA as an authentication a feature for establishing resilient PLA through machine learning (ML) in both digital and analog array MIMO systems.

Regarding analog arrays, we will investigate several attacks of increasing intensity (captured through the availability of side information at the attackers) and assess the performance of AoA-based authentication using

one-class classifiers for various distances and angles. We show that a successful impersonation requires knowledge of the location of the attacker and the victim, as well as the combiners at the verifier. The effectiveness of the attack also depends on the available transmission power at the attacker.
We then prove that, with digital arrays, an effective impersonation attack on AoA estimation can only be done under very stringent conditions on the attacker in terms of location and hardware capabilities, and thus, the AoA can in many scenarios be used as a robust feature for authentication. We utilize ML in our study to provide lightweight, model-free, intelligent authentication. We demonstrate the effectiveness of the proposed PLA solutions by running the algorithms on experimental outdoor massive multiple input multiple output data.

Dr. Linda Senigagliesi (Member, IEEE) received the Ph.D. degree in information engineering from the Università Politecnica delle Marche, Ancona, Italy, in 2019. During her Ph.D., she was a Visiting Student with the Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden. She is currently an Assistant Professor of Telecommunications with the Information Engineering Department (DII), Università Politecnica delle Marche. Her main research interests include information-theory and physical layer security, with application to distributed storage systems and wireless communications. Her activity is focused on machine learning techniques for physical layer authentication and security. Dr. Senigagliesi is a member of the IEEE INGR Physical Layer Security Focus Group and Cost Action CA22168—Physical Layer Security for Trustworthy and Resilient 6G Systems (6G-PHYSEC).