

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

Final program

Morning session	
9:00-11:00	Keynotes
	Dr. Valeria Loscri, INRIA, France (BEiNG Wise) Prof. Hüseyin Arslan, Istanbul Medipol University, Turkey (INTERACT)
11:00-11:15	Coffee break
11:15-12:15	Panel discussion. Toward 6G: key technologies and security perspective
	Dr. Hamed Ahmadi, University of York, UK (INTERACT) Dr. Carles Antón, CTTC, Spain (INTERACT) Dr Ali Khalighi, Ecole Centrale Marseille, France (NEW FOCUS) Prof. Arsenia Chorti, ENSEA, France (6G-PHYSEC)
12:15-13:30	Lunch break
Afternoon session	
13:30-14:50	Technical presentations – session A
	Onur Günlü, Matthieu Bloch, Rafael F. Schaefer, and Aylin Yener: Secure Integrated Sensing and Communication (ISAC): An Information-theoretic Perspective
	Ferdi Kara, Emil Björnson, Alva Kosasih, Parisa Ramezani and Murat Babek Salman: Exploring Upper Mid-Band Massive MIMO: Envisioning 6G's Frontier
	Robert Zakrzewski: Detecting gNB Physical Layer Spoofing Attacks using Lightweight Integrated Sensing and Communications (ISAC) for Binary Classification Tasks
	João Martins, Marco Gomes, Vitor Silva and Rui Dinis: Leveraging CSI prediction toward Physical Layer Spoofing Detection
15:00-15:30	Coffee break
15:30-16:50	Technical presentations – session B
	Hong-fu Chou, Thang X. Vu, Ilora Maity, Sean Longyu Ma, Symeon Chatzinotas and Björn Ottersten: Empirical Risk-aware Machine Learning on Trojan-Horse Detection for Trusted Quantum Key Distribution Networks
	Kemal Guner: 6G Wireless Network Security with Blockchain & Artificial Intelligence for Resilient Wireless Communication
	Nikolaos Pappas: From Information Freshness to Semantics of Information and Goal-oriented Communications
	Mostafa Rahmani Ghourtani, Alister Burr: Enhancing Physical Layer Security in Scalable Cell-Free Massive MIMO Networks: A Dual Precoding and Color Graph-Based Pilot Assignment Approach

Organizers:

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

Keynote 1: Emerging Communication Technologies, Social Aspects and Legal Factors for evolved cybersecurity solutions: the BEiNG-WISE approach

Abstract:

Living in our perpetually connected world presents us with an abundance of novel advanced services and automated applications. These increasingly require minimal human intervention, thanks to the integration of Machine Learning (ML), Artificial Intelligence (AI), and cutting-edge wireless technologies. However, this connectivity also exposes us to new vulnerabilities, paving the way for sophisticated cyber-attacks leveraging ML/AI and advanced wireless tech to enhance effectiveness and evade detection. While user awareness can mitigate some security risks, it falls short against the evolving landscape of cyber threats.

Addressing this challenge requires a paradigm shift, emphasizing human involvement in devising innovative and robust cyber-security solutions. BEiNG-WISE focuses on leveraging human factors alongside technological advancements to develop unconventional, ethically-driven cyber-security solutions. Recognizing humans as both potential offenders and victims in the cyber realm, the project aims to integrate these human dynamics with advanced technologies responsibly.

Furthermore, BEiNG-WISE emphasizes the legal dimension, ensuring that conceived solutions are not only effective but also compliant with real-world legal frameworks. The project draws upon interdisciplinary expertise spanning cybersecurity, wireless communication, data science, sociology, psychology, and law to tackle these complex challenges comprehensively.

Biography of the speaker:

Valeria Loscri is a permanent researcher in the FUN Team at Inria Lille (France) since Oct. 2013. From Dec. 2006 to Sept. 2013, she was Research Fellow in the TITAN Lab of the University of Calabria, Italy. She received her MSc and PhD degrees in Computer Science in 2003 and 2007, respectively, from the University of Calabria and her HDR (Habilitation à diriger des recherches) in 2018 from Université de Lille (France). Her research interests focus on emerging technologies for new communication paradigms such as Visible Light Communication (VLC), mmWave, cooperation and coexistence of wireless heterogeneous devices and cyber security in wireless networks. She is involved in the activity of several European Projects (Horizon Europe MLSysOps, H2020 CyberSANE, FP7 EU project VITAL, etc.).

She has been nominated to the 2021 Women Stars in Computer Networking and Communications Communications by the IEEE Communication Society. She is in the editorial board of IEEE COMST, Elsevier ComNet, ComCom, JNCA, IEEE Transactions on Nanobioscience. She is Action Chair and scientific Holder of BEiNG-WISE COST Action (since 2023). She is serving as TPC members in several primary international conferences, such as IEEE ESORICS, IEEE CNS, IEEE INFOCOM, IEEE PerCom. Since 2019, she is Scientific International Delegate for Inria Lille.

Keynote 2: Physical Layer Security: Latest Trends, Threats, and Countermeasures

Speaker: Huseyin Arslan, Istanbul Medipol University, Professor, IEEE Fellow, Dean of Faculty of Engineering at Istanbul Medipol University, Member of Turkish Academy of Science

Abstract:

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. Also, with the evolution of adaptive and flexible physical layer (PHY) and medium access (MAC) layer techniques, our radios and networks have become extremely capable and rich. Utilizing these capabilities has created new ways of designing secure communication and wireless transmission.

In addition to data communication, recent studies have suggested the use of wireless transmissions for sensing radio and physical environment to enable flexible, aware networks and environment monitoring applications. Anything related to wireless transmission, anything that the signal interacts with, can be or is being sensed, including user mobility and spectrum usage behavior, objects in the environment, and much more. This is no doubt an immense opportunity from both an academic and a commercial perspective.

Wireless physical layer secrecy has attracted much attention in recent years due to the broadcast nature of the wireless medium and its inherent vulnerability to eavesdropping, jamming, and interference. As a result, several key technologies have been advocated for improving PHY security. While most articles on physical layer secrecy focus on the information-theoretic aspect, there has been a significant amount of research which advocated using the randomness of the wireless channel through various diversity techniques including adaptive modulation and channel coding alongside the use of artificial noise signals to disrupt the wiretap user. On the other hand, recent progress in radio access technologies has enabled several enhanced secure transmission schemes, such as massive MIMO, beamforming, precoding, the integration of non-orthogonal multiple-access (NOMA), coordinated multiple access, advanced and rich set of modulation and waveform techniques, etc. However, the emergence of large-scale, dynamic, and decentralized wireless networks, along with the increased importance of Internet of Things (IoT) devices and applications, impose new challenges on classical point-to-point PHY layer security measures. To this end, researchers have been seeking for new security technologies to complement PHY layer security and significantly improve the overall security of wireless communication networks. All of these highly sophisticated radio access technologies can be exploited in order to design robust PHY, MAC, network, and cross-layer security schemes to cope with the continuous secrecy demand. Considering their potential applications in future wireless networks, these security mechanisms will receive even more research interest from both academia and industry.

In this presentation, we will cover both communication and sensing security from a broader perspective. Even though, more emphasis on PHY security is given, other security measures will also be covered for the sake of completeness and as a step towards cross-layer security and cognitive security vision. After discussing the features and probabilities of wireless channel from both communication and sensing perspectives, exploitation of these for secure transmission will be treated in detail utilizing various approaches. We will cover wireless sensing and radio environment concepts along with the related security implications in terms of eavesdropping, disruption, manipulation and, in general, the exploitation of wireless sensing by illegitimate users. Various solutions for these threats

from the domains of wireless communication, military radars, machine learning and more will be discussed. The tentative outline of the presentation will be as follows:

- Wireless Communication trends, requirements
- Importance of secure communication
- Classification of communication security
- PHY security: Communication and REM
- PHY security: Eavesdropping, Spoofing & Jamming
- Anti-jamming capable communication
- Cross-layer security
- Secure communication & other advanced radio access technologies
- Case- studies:
 - a- Security in URLLC (URLL & Secure communication)
 - b- Security in vehicular network (V2V and V2I)
 - c- Security in NOMA
 - d- Security in LIS

Biography of the speaker:

Dr. Arslan (IEEE Fellow, NAI Fellow, Member of Turkish Academy of Science) received his BS degree from the Middle East Technical University (METU), Ankara, Turkey in 1992; his MS and Ph.D. degrees were received respectively in 1994 and 1998 from Southern Methodist University (SMU), Dallas, TX. From January 1998 to August 2002, he was with the research group of Ericsson, where he was involved with several projects related to 2G and 3G wireless communication systems. Between August 2002 and August 2022, he was with the Electrical Engineering Department, at the University of South Florida, where he was a Professor. In December 2013, he joined Istanbul Medipol University to found the Engineering College, where he has been working as the Dean of the School of Engineering and Natural Sciences. In addition, he has worked as a part-time consultant for various companies and institutions including Anritsu Company, Savronik Inc., and The Scientific and Technological Research Council of Turkey. Dr. Arslan served as the founding Chairman of The Board Of Directors of ULAK Communication company, which is the Turkish telecom equipment provider. He was also the member of the Tubitak Scientific Board. Since May 2021, he is serving as a Member of the Board of Directors for Turkcell, the biggest cellular operator in Turkey while also operating in Ukrain, Belarus, and Cyprus.

Dr. Arslan conducts research in wireless systems, with emphasis on the physical and medium access layers of communications. His current research interests are on 6G and beyond radio access technologies, physical layer security, interference management (avoidance, awareness, and cancellation), cognitive radio, multi-carrier wireless technologies (beyond OFDM), dynamic spectrum access, co-existence issues, non-terrestrial communications (High Altitude Platforms), joint radar (sensing) and communication designs. Dr. Arslan has been collaborating extensively with key national and international industrial partners and his research has generated significant interest in companies such as InterDigital, Anritsu, NTT DoCoMo, Raytheon, Honeywell, Aselsan, Vestel, Türkcell, Keysight technologies. Collaborations and feedback from industry partners has significantly influenced his research. In addition to his research activities, Dr. Arslan has also contributed to wireless communication education. He has integrated the outcomes of his research into education which lead him to develop a number of courses at the University of South Florida and Istanbul Medipol University. He has developed a unique “Wireless Systems Laboratory” course (funded by the National Science Foundation and Keysight technologies) where he was able to teach not only the theory but also the practical aspects of wireless communication system with the most contemporary test and measurement equipment.

Dr. Arslan has served as general chair, technical program committee chair, session and symposium organizer, workshop chair, and technical program committee member in several IEEE conferences. He is currently a member of the editorial board for the IEEE Surveys and Tutorials and the Sensors Journal. He has also served as a member of the editorial board for the IEEE Transactions on Communications, the IEEE Transactions on Cognitive Communications and Networking (TCCN), and several other scholarly journals by Elsevier, Hindawi, and Wiley Publishing.