Physical Layer Security – background material

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 Internet of Things (IoT) and Cyber-Physical Systems (CPS) applications aim to bring people, data, processes, and things together to fulfil our needs. With the emergence of software defined networks, adaptive services and applications are gaining more attention since they allow the automatic configuration of devices and their parameters, systems, and services to the user's context change.

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 joint workshop, the actions want to bring all the related researchers from the workshop together and discuss PHY security in both communication and sensing security from a broader perspective. While the physical layer security is a direct topic of 6G-PHYSEC action, the technologies developed at INTERACT action are highly relevant to it. In addition to the participants from the two actions, there will be invited guests from other new COST actions: BEiNG-WISE and NEWFOCUS.

Discussion of the features and probability distributions of wireless channel from both communication and sensing perspectives, exploitation of these channel features for secure transmission will need expertise from INTERACT WG1 members.

ITERACT WG2 can exploit 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.

Other groups can also relate their domains with PHY, MAC, network, and application layer security of the communication and sensing, leading cross-layer security design.