Synopsis Seminar

Seminar Title	: Development of Efficient Security Enhancement Techniques for Ultra-Reliable Low Latency Communication in 5G and 6G Wireless Networks
Speaker	: Annapurna Pradhan (Rollno : 518ee1016)
Supervisor	: Prof. Susmita Das
Venue	: New Seminar Room (EE 401)
Date and Time	: 11 Sep 2024 (5:00 PM)
Abstract	: The fifth generation (5G) wireless networks have revolutionized the current communication landscape by using the innovative service class like Ultra Reliable Low Latency communication (URLLC) to facilitate mission-critical 5G applications such as industrial automation, autonomous driving, smart healthcare, and smart grid operations. Most importantly, URLLC enables ultra-high reliability (i.e., up to 99.999%) and very low latency (i.e., 1ms) data transmission to achieve the desired Quality-of-Service (QoS) of these applications. However, due to the finite blocklength constraint and low latency criteria utilizing complex cryptography-based security techniques for URLLC is not feasible. In this regard, Physical layer security (PLS) has emerged as a potential technique for providing lightweight security enhancement for URLLC data transmission by exploiting the randomness of wireless channel characteristics. Therefore, this dissertation proposes the development of efficient security enhancement techniques utilizing PLS for URLLC mission-critical 5G applications. The first contribution of this dissertation is the development of an efficient PLS scheme for improving the secure energy efficiency (SEE) of URLLC users in an industrial IoT scenario. The proposed PLS-based security framework considers the availability of direct transmission link utilizing orthogonal multiple access (OMA) for the URLLC users in the system. However, in the case of a large separation distance between the base station (BS) and URLLC user present at the cell edge, ensuring security and reliability of signal transmission is challenging. Therefore, the second contribution of the dissertation proposes an efficient PLS enhancement scheme for URLLC users at cell-edge by utilizing the cooperative non-orthogonal multiple access (CNOMA) technique. On the other hand, the absence of a direct communication link between the BS and the cell-edge URLLC user increases the chance of signal interception by external eavesdroppers. To address this, the third research direction of the dissertation proposes a relay-assisted CNOMA URLLC signal transmission to enhance the reliability of cell edge users. In a large-scale IoT network enabling the security of URLLC signal transmission is challenging because of centralized computing of confidential user information. To address this, the fourth direction of the dissertation is to propose efficient and secure decentralized computation of information using a Quantum-enhanced Federated Learning (QFL) framework to preserve the data privacy of edge URLLC users. The proposed QFL framework efficiently addressed the data heterogeneity and utilized edge resources efficiently in comparison to classical FL-based methods. The fifth and final direction of this dissertation is to present a comprehensive overview of the next-generation wireless service for 6G, i.e., Hyper-Reliable Low Latency Communication (HRLLC), security challenges, enabling technologies, and future research directions. To sum up, this dissertation work focuses on developing efficient and intelligent security enhancement schemes for URLLC in 5G and future 6G wireless systems.