National Institute of Technology Rourkela

Defence Seminar

Seminar Title	: Efficient Security Enhancement Techniques for Ultra-Reliable Low Latency Communication in 5G and 6G Wireless Networks
Speaker	: Annapurna Pradhan (Rollno : 518ee1016)
Supervisor	: Susmita Das
Venue	: Smart Seminar Room (EE 401)
Date and Time	: 12 Mar 2025 (5:30 PM)

Abstract

: : The 5G wireless networks have revolutionized the current communication landscape by introducing an innovative service 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. However, the exponential rise in wireless data traffic generated from billions of smart Internet-of-Things (IoT) devices utilizing URLLC service is highly vulnerable to external eavesdropping and security threats. In this regard, Physical layer security (PLS) has emerged as a potential technique for providing lightweight security enhancement for URLLC 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 to ensure the security of URLLC signal transmission to the cell edge users in an IoT network using cooperative non-orthogonal multiple access (CNOMA) technology. A coordinated direct and relayed transmission (CDRT) scheme is proposed for the CNOMA system to ensure the reliability and security of URLLC. A dedicated relay node is used to transmit an artificial noise (AN) signal along with the URLLC information intended for legitimate user to mitigate the impact of eavesdropping. Then the second contribution of the dissertation proposes an efficient AN-assisted jamming based PLS enhancement scheme for URLLC users at the cell edge by utilizing the CNOMA technique. An AN-assisted jamming, and full-duplex communication utilizing the near user to the BS as relay is proposed to improve the PLS of cell-edge URLLC users. However, critical control information transmission among low-power IoT devices in an industrial IoT (IIoT) scenario is vulnerable to information leakage and security threats due to the openness of wireless medium. Then, the third contribution of this dissertation is the development of an efficient PLS scheme for improving the secure energy efficiency of URLLC signal transmission in a multi-user and multi-eavesdropping scenario of the mission-critical IIoT application. 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 in presence of heterogenous service types and security threats. Finally, the dissertation presents the concluding remarks on the research contributions and discusses the security challenges, enabling technologies, and future research directions for next-generation security service in 6G.