



2026

Professor Yi-Han Chiang

Department of Electrical and Electronic Systems
Engineering, Osaka Metropolitan University, Osaka, Japan.

WIRELESS RESOURCE ALLOCATION FOR SECURE OVER-THE-AIR FEDERATED LEARNING

Federated learning (FL) enables Artificial Intelligence of Things (AIoT) devices to collaboratively train shared machine learning (ML) models without sharing their raw data, making it a promising paradigm towards privacy-preserving distributed ML. To facilitate FL over wireless networks, over-the-air (OTA) computation has recently attracted growing research attention. By exploiting the waveform-superposition property of wireless signals, OTA computation enables simultaneous communication and computation over wireless multiple-access channels. Integrating OTA computation with FL allows locally trained model updates to be aggregated wirelessly, thereby effectively reducing bandwidth consumption. In this talk, we investigate wireless resource allocation for OTA-FL systems. Since OTA-FL systems are vulnerable to jamming attacks due to the difficulty of decoupling normal signals from received signals, we first propose a coordinated dropout strategy to mitigate the adverse effects of jamming signals in a reactive manner. Then, we develop a proactive defense strategy based on dummy-symbol insertion, which discards received signals when potential jamming is detected. Through these two complementary strategies, we demonstrate how wireless resource allocation can be designed to enhance the security and robustness of OTA-FL systems.

31 AUGUST 2026

2 PM - 4 PM

Room 260904-1

College of Commerce,
National Chengchi University