Physical Layer Security Enhancement in Next-Generation Heterogeneous Networks

Name	Qianyue Qu
Laboratory's name	Large-Scale Systems Management Laboratory
Supervisor's name	Professor Shoji Kasahara

Abstract

With the development of 5G/6G networks, wireless heterogeneous networks play an increasingly important role in future communication systems. However, the open nature of wireless channels makes the system vulnerable to security threats. From the perspective of physical layer security (PLS), this dissertation studies two typical heterogeneous network scenarios: hybrid millimeter wave (mmWave)-microwave systems and unmanned aerial vehicle (UAV) multicasting networks.

In the first study, the behavioral selection characteristics of eavesdroppers were analyzed, and a model for characterizing eavesdropping region based on secrecy outage probability and secrecy rate was proposed. Through theoretical analysis and numerical simulation, the impact of different parameters on the eavesdropping region is revealed, which provides a theoretical basis for improving system security.

With the rapid development of wireless technology, UAVs have emerged as a promising solution for diverse applications in 5G/6G communication systems. In this context, we study the security challenges in UAV multicasting networks, considering a scenario including an aerial base station, ground users (GUs), jammers, and an eavesdropper. A Poisson point process is used to model the user distribution, while considering the line-of-sight (LoS) and non-line-of-sight (NLoS) characteristics of air-to-ground channels. Two secure transmission schemes are proposed: the first involves the UAV trajectory optimization to maximize the system secrecy rate; the second identifies the optimal relay among GUs with the fixed UAV position. The research findings provide theoretical foundations for enhancing physical layer security in next-generation wireless networks.