Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Large-Scale Systems (Shoji Kasahara (Professor))		
Student ID	2011420	Submission date	2022 / 1 / 21
Name	QU QIANYUE		
Thesis title	On Eavesdropping Region Characterization in Hybrid Wireless Communications On Eavesdropping Region Characterization in Hybrid Wireless Communications		

Abstract

Hybrid communication systems where microwave links coexist with millimeter-wave (mmWave) links have become an essential component in the fifth-generation (5G) mobile networks. Nevertheless, the open wireless medium of hybrid systems makes them vulnerable to eavesdropping attacks. Physical layer security (PLS) can be one of the reliable solutions to ensure the security of wireless systems. The core idea of the PLS technology is to exploit the inherent physical layer characteristics (e.g., fading and noise) of wireless channels to ensure almost no information is leaked to eavesdroppers. Compared with classical cryptographic methods, the PLS technology achieves a stronger form of security at less computational costs. Moreover, the PLS technology can be used as a complement to cryptographic methods to further improve security performance.

In addition, eavesdroppers in hybrid communication systems may enhance their eavesdropping performance by selecting to eavesdrop on different waves (i.e., mmWave and microwave). Hence, the entire hybrid system can be divided into a mmWave eavesdropping region and a microwave eavesdropping region. Therefore, we investigate the eavesdropping region characterization problem in hybrid wireless communication systems from the PLS perspective.

Firstly, we derive secrecy outage probabilities (SOPs) of mmWave links and microwave links, respectively. We then derive the lower bound for the secrecy rate of mmWave links and that of microwave links. Secondly, we use the ratio of the secrecy rate of microwave links to that of mmWave links and the ratio of the SOP of mmWave links to that of microwave links as the eavesdropping wave selection criteria to determine the mmWave eavesdropping regions. To validate the derivation, we show the simulation results of SOPs and secrecy rates, respectively. Finally, we provide numerical results to illustrate the mmWave eavesdropping region under various network parameter settings.

Furthermore, to better observe the eavesdropping behavior of eavesdroppers, we investigate the optimal eavesdropping location problems. We formulate the objective function based on the SOPs numerically to find the optimal eavesdropping location and discuss the numerical results in the end.