Abstract

Security has become an increasingly significant and urgent issue in wireless communication networks. The growing computational capability of the eavesdropper and the evolution of wireless communications pose more and more stringent requirements to the conventional cryptographic methods. As an alternative solution, physical layer security achieves secure communication by exploiting the inherent randomness of wireless channels, which is quite suitable for the emerging distributed large-scale networks. In this thesis, we aim to develop different physical layer security techniques to improve the secrecy performance in emerging wireless communication systems.

First, the security of an AF successive relaying network with multiple untrusted relay nodes is investigated, where the conventional detrimental inter-relay interference is exploited to jam the untrusted nodes without assistance of external helpers. Considering different complexity requirements, several relay selection schemes are proposed, and the closed-form expressions of the lower bound of SOP and the maximum secrecy diversity order are derived accordingly.

Second, the secure transmission strategy for a multi-input-single-output multi-eavesdropper (MISOME) system with coexistence of a secure user (Bob) and a normal user (NU) is investigated. The power allocation among Bob, NU and AN, as well as the wiretap code rates, are jointly optimized to maximize the effective secrecy throughput (EST), under the average throughput constraint of the NU and statistical channel state information (CSI) of eavesdroppers.

Third, physical layer security in a multi-antenna small-cell network is investigated, where the multi-antenna base stations (BSs), cellular users, and eavesdroppers are all randomly distributed according to independent Poisson point processes. Stochastic geometry is applied to derive the closed-form expressions of the connection outage and secrecy outage probabilities and the achievable average secrecy rate. The impact of different parameters, including power allocation and BS/Eve density, on the secrecy performance is also analyzed.

Finally, we comprehensively study the physical layer security performance in a large-scale heterogeneous network consisting both sub-6 GHz massive multi-input multi-output (MIMO) macro cells and millimeter wave (mmWave) small cells. By considering pilot spoofing attacks from the eavesdroppers, the coverage and secrecy probabilities are derived using stochastic geometry and the conditions under which the millimeter wave system outperforms the sub-6 GHz counterpart are discussed in terms of both coverage and secrecy.