

Preface

The main objective of this book is to investigate the wireless physical layer security in random cellular networks. Security is a fundamental issue in data communications. In wireless communications, security becomes more challenging due to the openness of wireless medium and its inherent vulnerability to eavesdropping. Recently, physical layer security has become an emerging research front which provides promising confidentiality for wireless transmissions. The theoretical basis of physical layer security approaches is dated back to information theory, which takes full consideration of the characteristic of wireless channels. Compared to conventional cryptographic encryption and decryption technologies to guarantee secrecy, physical layer security approaches bypass the secret key generation and distribution issues, thereby resulting in significantly lower complexity and more savings in computational resources, which makes it very competitive in many wireless applications.

Although there already have been great advances in the topic of physical layer security, most of the researches focus on the point-to-point secrecy communications. In a wireless cellular network there are a large amount of concurrent transmissions between different base station-user pairs sharing a same frequency band, which causes ubiquitous interference in the whole network. The most significant difference in a wireless cellular network is that the transmission is highly interference-limited. Basically for any receiver, the signals for the other receivers are interferences. The aggregated interference can greatly influence the secrecy performance of a wireless link. There are significantly different levels of interference that will be caused due to different path loss, shadowing, and fading, and all these effects depend heavily on the spatial locations of the terminals. Therefore, the network geometry and spatial distribution of interferers become the primary factor to impact the secrecy performance of a wireless transmission.

In this book, we will focus on the networks under the framework of stochastic geometry, which is used to model the random distributions of legitimate users/eavesdroppers and the random deployment of base stations/access points. In the first two chapters, we introduce the basic ideas of physical layer security and primary knowledge of stochastic geometry theory, especially several useful

properties of Poisson point process. In Chap. 3, we introduce the physical layer security in a single-cell cellular under time division multiple access (TDMA) when the eavesdroppers are randomly located as a Poisson point process. Moreover, in Chap. 4, we elaborate the network-wide physical layer security in a multi-tier heterogeneous network, where all the locations of users, eavesdroppers and deployment of base stations are modeled as Poisson point processes. Chapter 5 includes the impact of the full-duplex transceivers on security performance of random ad hoc network, which could be considered as a special case of uplink transmissions in a random cellular network. Lastly, Chap. 6 concludes the book and discusses the possible future research directions. This book will present the readers a timely report of state-of-the-art techniques about physical layer security under the framework of stochastic geometry, and provide an explicit snapshot of this emerging topic.

Xi'an, China
July 2016

Hui-Ming Wang
Tong-Xing Zheng

Physical Layer Security in Random Cellular Networks

Wang, H.-M.; Zheng, T.-X.

2016, XVIII, 113 p. 37 illus., Softcover

ISBN: 978-981-10-1574-8