

## Chapter 2

# Random Cellular Networks and Stochastic Geometry

**Abstract** In this chapter, we discuss the physical layer security in stochastic geometric networks. We first present the randomness of cellular networks deployment, and summarize the challenges to solve the physical layer security issue. We then introduce some primary knowledge of stochastic geometry theory, especially some useful properties of Poisson point process, which will be extensively used in the following chapters. It is concluded that various random wireless networks can be modeled and analyzed using the framework of stochastic geometry. Moreover, we introduce the network security performance metrics to evaluate the physical layer security. Finally, we provide a brief survey of recent researches on physical layer security in wireless networks, and introduce three open problems in this field which we are going to deal with in the following chapters.

## 2.1 Deployment of Cellular Networks

With the rapidly increasing demand of big traffic and high data rate, emerging wireless networks, such as heterogeneous cellular networks (HCNs), cognitive radio networks (CRNs), wireless ad hoc networks, etc., have drawn significant research interests in both academia and industry over the last decade. To protect the confidentiality of the data and information transmitted through wireless links in these networks, physical layer security approach is a very competitive solution due to its low complexity and flexibility.

In Chap. 1 we have reviewed some techniques for enhancing the physical layer security of wireless transmissions. We note that all those techniques are initially developed for a *point-to-point* communication system, i.e., there is only one source destination pair under consideration. However, a wireless communication network can be viewed as a collection of transceivers located in an area. For example, a cellular network consists of a mass of base stations (BSs) and mobile user equipments (UEs) distributed in a city. Compared with a point-to-point communication system, the most significant difference in a wireless cellular network is that the transmission is highly *interference-limited*. In a cellular network, there are a large amount of concurrent transmissions between different BS-UE pairs sharing a same frequency band, which

causes ubiquitous interference in the whole network. For any receiver, the signals intended for the other receivers are treated as interferences.

The aggregated interference will result in a great impact on the secrecy performance of a wireless link. As can be seen from the fact that secrecy performance depends heavily on the achievable rates at the legitimate destination and the potential eavesdroppers in Chap. 1, the ubiquitous interference will bring in two effects. On the one hand, the legitimate link rate  $R_B$  will be reduced. On the other hand, the leakage rate  $R_E$  will be degraded as well since any potential eavesdroppers also receive interferences. Therefore, the secrecy performance, which is a function of  $R_B - R_E$ , should be carefully reevaluated.

In a wireless channel, all path loss, shadowing, and fading will bring impairments to the received signal strength, and all these effects depend heavily on the spatial locations of the terminals. In a wireless cellular network, concurrent transmissions located at different spatial positions cause significantly different levels of interference strength to the same receiver. It is not uncommon for the signal-to-interference-plus-noise ratios (SINRs) to vary over different receivers by up to a hundred dBs due to differences in path loss, shadowing and fading. Since all these effects depend heavily on the spatial locations of the terminals, the network geometry and spatial distribution of interferers become the primary factors in determining a receiver's SINR and hence the achievable rate. Therefore, it is eagerly needed to develop a tractable tool to model the network geometry and analyze the secrecy performance.

### ***2.1.1 Modeling and Analyzing Random Cellular Networks***

Traditionally, a tractable cellular deployment model commonly used by information theorists is the Wyner model [1, 2], which is typically one-dimensional. This model assumes a unit gain from each BS to the active user and an equal gain that is less than one to the two users in the two neighboring cells. This is obviously an overly simple and highly inaccurate model unless there is a very large amount of interference averaging over space, which greatly limits its application. On the other hand, a more realistic two-dimensional network of BS is usually modeled on a regular hexagonal lattice, or slightly more simply, a square lattice [3, 4]. However, tractable expressions for the SINR are unavailable in general for a random user location in the cell. More general results that provide guidance into typical SINR or the probability of outage/coverage over the entire cell only can be obtained by complex time-consuming Monte Carlo simulations.

It is also important to realize that although widely accepted, grid-based models are themselves highly idealized and may be increasingly inaccurate for the heterogeneous and ad hoc deployments common in urban and suburban areas, where cell size varies considerably due to differences in transmission power, tower height, and user density. Nowadays, a common characteristic of these wireless networks is the random network topology, for example, a femtocell access point (AP) in an HCN may access and quit dynamically; nodes in an ad hoc network are randomly distributed and are connected

with each other in a self-organizing manner; a cognitive user may opportunistically access the idle channel in a CRN; and so on.

The randomness of cellular network geometric topology has brought the following two fundamental challenges to network modeling and secrecy performance analysis.

- *How to model network geometry?* Secrecy performance of a wireless transmission in a cellular network is closely related to network geometry. As we know, information exchange between arbitrary transmitter and receiver depends heavily on the spatial positions of themselves and of other interfering nodes in the network, and also the interplay between them. The increase of transmit power at an arbitrary transmitter will in turn introduce greater interference to those undesired receivers. In addition, cellular networks are more and more heterogeneous and the node distribution are becoming more and more irregular, with the node density differing significantly for different areas. Thus, neither the position-independent Wyner model [1, 2] nor the regular lattice model can be used to describe today's cellular networks. Network designers are crying out for a network model that is tailored to characterize node distribution accurately and meanwhile is tractable.
- *How to analyze the randomness?* The number of uncertainties in a cellular network has far exceeded that in a point-to-point scenario: not only the received power is random because of the randomness inherent to wireless channels and the mobility of the desired user, but also the interference power is governed by a series of stochastic processes including nodes' spatial distribution, shadowing, and fading. It is impossible for a node to know or to forecast the spatial positions and the channel knowledge related to all the other nodes. In other words, transmitter is not able to configure transmission parameters for a concrete space realization. In order to efficiently assess or predict network performance, a sound stochastic process is required to capture the randomness of the cellular network, including both the positions of BSs and UEs, just as a fading distribution is used for modeling a variety of possible propagation environments.

### 2.1.2 Stochastic Geometry Approach

Fortunately, stochastic geometry has provided a new opportunity to deal with the aforementioned challenges. Using powerful tools from stochastic geometry, the randomness of a cellular network can be conveniently modeled with a sufficient accuracy, and we are able to study the average behavior of a wireless cellular network over many spatial realizations by modeling network nodes according to some probability distribution [5]. During recent years, stochastic geometry has also inspired a large number of researchers to perform security performance analysis and network parameter optimization for random cellular networks. In the following sections, we provide a brief introduction of some fundamentals of stochastic geometry. A more thorough reference work can be found in [6].

## 2.2 Fundamentals of Stochastic Geometry

Stochastic geometry is a rich branch of applied probability which is used to study random phenomena on the plane or in higher dimensions [6]. It has been widely applied in the areas of biology, astronomy and material sciences, etc. Nowadays, its application has also infiltrated into image analysis and communication networks.

### 2.2.1 Point Process

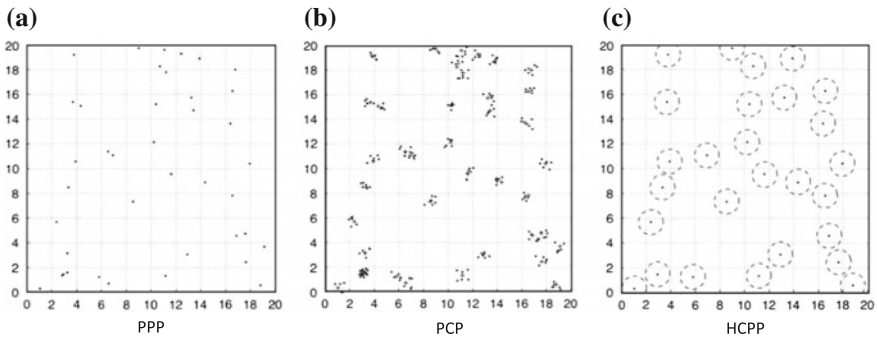
Stochastic geometry is intrinsically related to the theory of stochastic point process (PP) [6]. PP is the most basic research object studied in stochastic geometry. Here we just provide a basic introduction. A more rigorous definition can be found in [6].

Simply speaking, a PP  $\Phi \triangleq \{x_i, i \in \mathbb{N}\}$  is a random collection of points residing a measure space  $E$ , e.g., for wireless networks,  $E$  is the  $d$ -dimensional Euclidean space  $\mathbb{R}^d$ .  $\Phi$  can be interpreted in terms of the so called *random set formalism*, where  $\Phi = \{x_i\} \subset \mathbb{R}^d$  is a *countable* random set with each element  $x_i$  being a random variable. A more convenient way to describe the PP is to count the number of points falling in any Borel set  $A \subset \mathbb{R}^d$ , i.e.,

$$\Phi(A) = \sum_{x_i \in \Phi} \mathbb{I}(x_i \in A). \quad (2.1)$$

Note that,  $\Phi(A)$  is a random variable whose distribution depends on  $\Phi$ .

So far, there are four categories of PPs that have been widely studied to model the wireless network, namely, Poisson PP (PPP), binomial PP (BPP), Poisson cluster process (PCP) and Matérn hard core PP (HCPP). The strict definitions of these PPs can be found in [7]. Figure 2.1 depicts PPP, PCP and HCPP, respectively. PPP provides the baseline model (i.e., parent PP) for the other PPs, or, PPP can be converted into the other PPs [8]. Specifically,



**Fig. 2.1** Three typical PPs

(1) A PPP is used to abstract a network in which a possibly infinite number of nodes randomly and independently coexist in a finite or infinite region, e.g., users in a cellular network and nodes in a wireless ad hoc network;

(2) When given the number of nodes in a finite region, a PPP becomes a BPP;

(3) When nodes are clustered according to the Multiple Access Control (MAC) protocol, a PPP evolves into a PCP, e.g., users gathered around Wi-Fi hot spots;

(4) Due to geographical constraints, network planning, or MAC protocols, a minimum distance is required to separate any two nodes, then a PPP transforms into a repulsive PP, i.e., Matérn HCPP.

Among these four categories of PPs, PPP has provided a convenient mathematical framework for random wireless network. For the self-organized ad hoc network, closed-form expressions of performance metrics like the SINR and outage probability can be easily obtained. Using PPP we can also derive tight bound results for performance metrics in those infrastructure-based networks (e.g., cellular networks) and coordinated spectrum access networks (e.g., CRNs). Thanks to these advantages, PPP has become the most popular, tractable, and important PP.

## 2.2.2 Poisson Point Process

This subsection introduces the PPP basic and PPP's key properties.

### 2.2.2.1 Definitions

In the following, we define the PPP and the homogeneous PPP.

**Definition 2.1** (PPP) A PP  $\Phi \triangleq \{x_i\} \in \mathbb{R}^d$  is a PPP if and only if

- For an arbitrary set  $A \in \mathbb{R}^d$ ,  $\Phi(A)$  is a Poisson random variable;
- For any two disjoint subsets  $A_i, A_j \in \mathbb{R}^d$ ,  $\Phi(A_i)$  and  $\Phi(A_j)$  are independent.

**Definition 2.2** (Homogeneous PPP) If the intensity measure  $\Lambda$ <sup>1</sup> of a PPP  $\Phi$  satisfies  $\Lambda(A) = \lambda|A|$ , i.e., the product of a constant value  $\lambda$  and Lebesgue measure  $|A|$ ,<sup>2</sup> then  $\Phi$  is a homogeneous PPP with intensity  $\lambda$ .

Homogeneous PPP is a simple, isotropy, and stationary PP. By simple, we mean there are no two points at the same location; by isotropy and stationary, we mean that the law of a PP is invariant by rotation and translation, respectively [5]. Using homogeneous PPP will greatly simplify the mathematical analysis, which helps to reveal explicitly the influence of network parameters on network performance. Unless otherwise specified, the PPP in the following refers solely to the homogeneous one on a two-dimensional plane  $\mathbb{R}^2$ .

<sup>1</sup>For any Borel set  $A$ , its intensity measure  $\Lambda$  is defined by  $\Lambda(A) = \mathbb{E}[\Phi(A)]$ .

<sup>2</sup> $|A|$  denotes the area of  $A$  for a plane, and denotes the volume of  $A$  for a three-dimensional space.

### 2.2.2.2 Key Properties on PPP

Six properties are presented in the following. Knowledge regarding detailed derivations can be found in [7, 9].

**Property 2.1** *For a PPP  $\Phi \subset \mathbb{R}^2$  and an arbitrary finite region  $A$ ,  $\Phi(A)$  is a Poisson random variable with mean  $\lambda|A|$ , i.e.,*

$$\mathbb{P}\{\Phi(A) = n\} = e^{-\lambda|A|} \frac{(\lambda|A|)^n}{n!}. \quad (2.2)$$

**Property 2.2** *For a PPP  $\Phi \subset \mathbb{R}^2$  and conditionally on the fact that  $\Phi(A) = n$ , these  $n$  points are independently and uniformly distributed in  $A$ , i.e., forming a BPP in  $A$ .*

From Property 2.2, we are able to obtain two very useful formulas, namely, Campbell's formula and probability generating functional (PGFL), respectively.

**Lemma 2.1** (Campbell's formula) *For a PPP  $\Phi$  with density  $\lambda$  and an arbitrary real function  $f(x) : \mathbb{R}^2 \rightarrow \mathbb{R}^+$ , we have*

$$\mathbb{E}_\Phi \left[ \sum_{x \in \Phi} f(x) \right] = \lambda \int_{\mathbb{R}^2} f(x) dx. \quad (2.3)$$

Campbell's formula simplifies the calculation of the mean and variance of the aggregate interference power in a network.

*Example 2.1* Consider a PPP  $\Phi \subset \mathbb{R}^2$  with density  $\lambda$ , the aggregate interference power of the node at location  $y \in \mathbb{R}^2$  is given by  $I(y) = \sum_{x \in \Phi} \ell(x - y)$ , where  $\ell(x - y)$  denotes the path loss function from  $x$  to  $y$ . The mean and variance of  $I(y)$ , i.e.,  $\mathbb{E}[I(y)]$  and  $\mathbb{V}[I(y)]$  can be computed by using the Campbell's formula, given below

$$\mathbb{E}[I(y)] = \lambda \int_{\mathbb{R}^2} \ell(x) dx, \quad \mathbb{V}[I(y)] = \lambda \int_{\mathbb{R}^2} \ell(x)^2 dx. \quad (2.4)$$

**Lemma 2.2** (PGFL) *For a PPP  $\Phi \subset \mathbb{R}^2$  with density  $\lambda$  and an arbitrary real function  $f(x) : \mathbb{R}^2 \rightarrow [0, 1]$*

$$\mathbb{E}_\Phi \left[ \prod_{x \in \Phi} f(x) \right] = \exp \left( -\lambda \int_{\mathbb{R}^2} (1 - f(x)) dx \right). \quad (2.5)$$

An important application of PGFL is the Laplace transform of interference  $I(y)$ .

*Example 2.2* (Laplace transform) Recalling the aggregate interference power  $I(y) = \sum_{x \in \Phi} \ell(x - y)$  given in Example 2.1, the Laplace transform of  $I(y)$  is given by

$$\mathcal{L}_{I(y)}(s) = \mathbb{E}_{\Phi} [e^{-sI(y)}] = \exp \left( -\lambda \int_{\mathbb{R}^2} (1 - e^{-s\ell(x)}) dx \right). \quad (2.6)$$

If we execute operations, including superposition, thinning and displacement on a PPP, we can obtain the following invariant laws.

**Property 2.3** (Superposition) *The superposition of multiple independent PPP with density  $\lambda_k$  is still a PPP with new density  $\sum_k \lambda_k$ .*

Property 2.3 can be used to analyze the interference in a network consisting of multiple independent tiers. For example, the aggregate interference power of a random user in a  $K$ -tier heterogeneous cellular network can be expressed as  $I = \sum_{k=1}^K \sum_{x \in \Phi_k} \ell_k(x)$ , where  $\Phi_k$  models the locations of the interfering BSs in the  $k$ th tier with density  $\lambda_k$ , then the Laplace transform of  $I$  can be calculated as

$$\mathcal{L}_I(s) = \prod_{k=1}^K \mathbb{E}_{\Phi_k} \left[ e^{-s \sum_{x \in \Phi_k} \ell_k(x)} \right] = \exp \left( -\sum_{k=1}^K \lambda_k \int_{\mathbb{R}^2} (1 - e^{-s\ell_k(x)}) dx \right). \quad (2.7)$$

**Property 2.4** (Thinning) *The thinning of a PPP of density  $\lambda$  with retention probability  $p$  is still a PPP of new density  $p\lambda$ .*

Property 2.4 can be used to analyze the performance of a network in which the interfering nodes opportunistically transmit at a certain activation probability. For example, each BS in a cellular network of density  $\lambda$  is activated at a probability  $p$ , then the aggregate interference power of a random user can be given by  $I = \sum_{x \in \Phi_A} \ell(x)$ , where  $\Phi_A$  denotes the set of the locations of those active BSs. Accordingly, the Laplace transform of  $I$  can be calculated as

$$\mathcal{L}_I(s) = \mathbb{E}_{\Phi} \left[ e^{-s \sum_{x \in \Phi_A} \ell(x)} \right] = \exp \left( -p\lambda \int_{\mathbb{R}^2} (1 - e^{-s\ell(x)}) dx \right). \quad (2.8)$$

**Property 2.5** (Displacement) *The displacement of a PPP of density  $\lambda$  by a Markov kernel  $\rho(x, y)$  from  $x$  to  $y$  is still a of density  $\lambda$ .*

Property 2.5 can be used to model mobile wireless networks. For example, consider a mobile ad hoc network where the locations of nodes in the current time slot are modeled as a PPP  $\Phi \triangleq \{x_i\} \subset \mathbb{R}^2$  of density  $\lambda$ , if each node moves from  $x_i$  to a new location  $y_i$  independently in the next time slot, then the new locations set  $\Phi^\circ \triangleq \{y_i\}$  is still a PPP of density  $\lambda$ .

**Property 2.6** (Slivnyak theorem) *Consider a PPP  $\Phi$  with a point  $\delta_x$  located at  $x$ , if we remove  $\delta_x$  from  $\Phi$ , the distribution of the reduced PPP  $\Phi - \delta_x$  is the same as that of the original PPP  $\Phi$ .*

Slivnyak theorem implies that the addition or removal of a user in a network does not change the distribution of the other users, hence we can always place the user of interest at the origin in coordinates as a typical user to analyze user performance in aspects like outage probability and end-user throughput.

## 2.3 Using Stochastic Geometry to Model Wireless Networks

PPP is recognized as the most random stationary process friendly presenting a wireless network with nodes randomly distributed or with substantial mobility. In addition, using PPP to model the positions of network nodes simplifies the analysis, which facilitates the investigation of the relationships between network performance and network parameters.

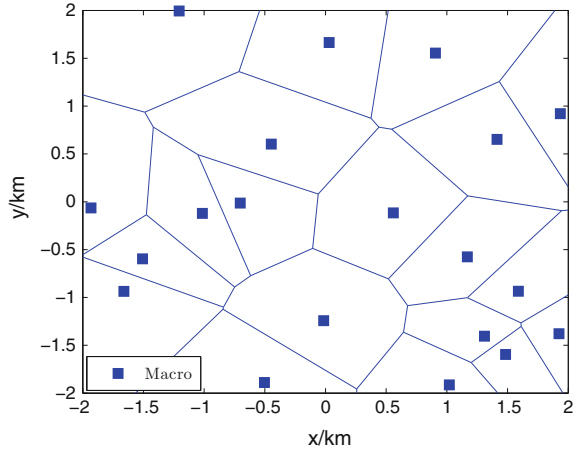
Based on whether there is public infrastructure or not, wireless networks can be divided into two classes, namely, infrastructure-based networks (e.g., cellular networks) and infrastructureless networks (e.g., ad hoc networks and CRNs). PPP has been widely applied in both classes. In the following, we concentrate on cellular networks and wireless ad hoc networks, and the application of PPP in CRNs can be found in [10–13].

### 2.3.1 Cellular Networks

A cellular network is an infrastructure-based network possessing fixed BSs or APs as well as explicit MAC protocols. Traditionally, cellular network is characterized by using a regular hexagonal grid model, in which each BS covers a hexagonal cell. The biggest weakness of such a model is that it makes modeling and analyzing intercell interference extremely sophisticated. Moreover, demands of transmission capacity in downtown, uptown and rural areas, etc., differ a great deal, and therefore traditional grid planning can no longer capture the deployment of BSs nowadays. During the past few years, due to the built-out urban areas, BSs are deployed in an increasingly irregular and random way. These contribute to modeling the locations of BSs using tools from stochastic geometry.

Considering that no service provider will deploy its two BSs arbitrarily close to each other in a real cellular network, using a repulsive PP such as the Matérn HCPP to model a cellular network topology is more practical [14]. However, an HCPP-based cellular network suffers a great loss of analytical tractability and the Matérn HCPP itself is flawed, i.e., the nonexistence of the PGFL [15]. By contrast, PPP is much more appealing given the simplicity and tractability. In a PPP-base cellular network, each mobile user is associated with the nearest BS, thus forming a Poisson Voronoi diagram, just as shown in Fig. 2.2. Assuming the locations of BSs are completely uncorrelated seems a bit unrealistic, but Andrews et al. [16] has figured out that the PPP yields a tight lower bound on the coverage probability provided by an actually deployed cellular network as well as an approximation on the upper bound mean transmission rate provided by the idealized grid-based model. Such validations can be further found in [14, 17].

**Fig. 2.2** Single-tier cellular network

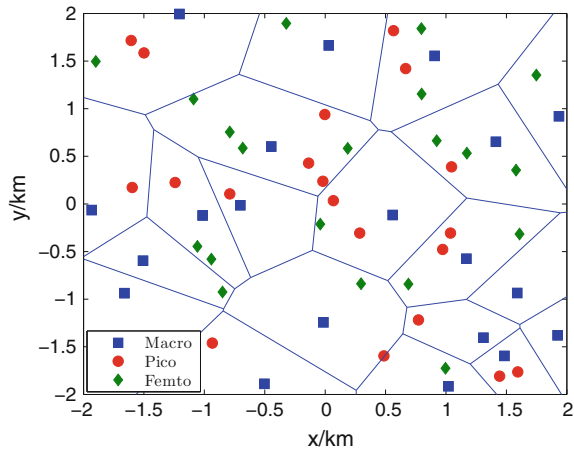


### 2.3.2 Heterogeneous Cellular Networks

Traditional single-tier macrocellular network has been incapable of meeting a  $1000\times$  average data rate increase in 5G networks [18], and the deployment of HCNs is an irreversible trend in future wireless networks. An HCN is generally formed by overlay a variety of low-power infrastructure on an existing macrocellular network. Figure 2.3 depicts a three-tier HCN with picocells and femtocells coexisting with macrocells. These pico/femto BSs are often low-end and in large numbers and demand-based. For example, femtocell BSs can either be installed by individuals and enterprises to enlarge household and office coverage, or be planned by network operators to increase capacity for airports, stadiums and other areas of dense demand [19]. In addition, femto APs support “plug-and-play,” i.e., accessing and quitting the network may happen at any minute, and the division of service areas is much more irregular compared with conventional macrocellular networks. All these make it reasonable to use PPP to characterize the deployment of picocells and femtocells APs. In [20–22], the authors have investigated the spectrum allocation, access control and interference avoidance for both downlink and uplink communications in a two-tier HCN, where the locations of macrocell BSs are modeled as hexagonal grid and the locations of femtocell BS and of users are modeled as independent PPPs. It is shown in [23] that, even modeling all tiers of an HCN including the macrocell tier as independent PPPs, the distribution of the SINR of a typical user greatly approximates that provided by a grid-based macrocell tier case.

#### 2.3.2.1 Femto Access Control

Based on the PPP HCN, femto access control including closed access [24] and open access [23] have been discussed in [25, 26]. In closed access, femto access points

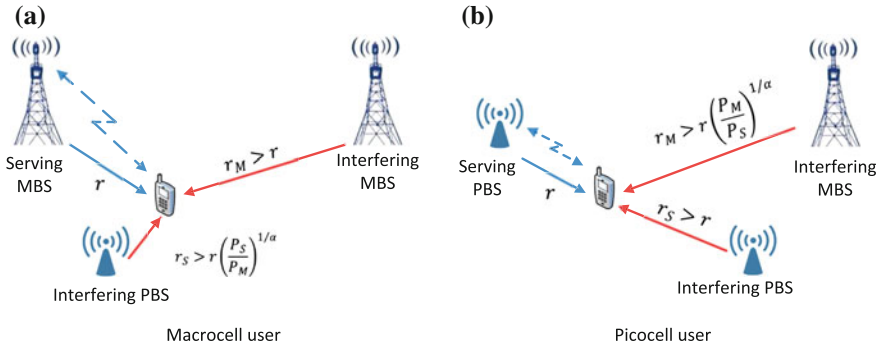
**Fig. 2.3** Three-tier HCN

(FAPs) provide service to only specified subscribers to monopolize their own femto-cell and its backhaul to ensure privacy and security; whereas in open access, arbitrary nearby users can use the femtocell. Xia et al. [26] have pointed that, compared with closed access, open access is preferred by network operators not only because it expands network capacity in an inexpensive way by leveraging third-party backhaul for free, but also because it greatly reduces cross-tier interference by allowing macro-cell user to access femtocell nearby. Under different access strategies, the issues of load balancing [27, 28], coverage probability [24, 29], throughput [30, 31], etc., have been investigated.

### 2.3.2.2 Mobile Association Policy

Mobile association, or, cell selection, is one of the core issues in designing an HCN. There are two general classes of mobile association policies: (1) average received power based (long-term results), where each mobile user connects to the BS providing the largest average received power [23, 27, 29], (2) instantaneous received power or SINR based, where each user connects to the BS providing the largest instantaneous received power or SINR [24, 28]. It is shown in [23] that, network designers prefer the average power based policy, with which the “ping-pong” effect, i.e., the unnecessary information exchange caused by shadowing and fading, can be avoided. Under such a mobile association policy, users do not connect to the nearest BSs any more due to the differences in transmit power of different tier of BSs, and thus the tessellation corresponds to a weighted Voronoi diagram instead of a standard Voronoi diagram formed in the conventional single-tier cellular network.

Figure 2.4 depicts the mobile association policy in an HCN consisting of a macro-cell tier and a picocell tier. Specifically, Fig. 2.4a shows, a user connects to a macro BS instead of a much nearer pico BS since the latter provides a lower average received power for this user. Figure 2.4b shows, although the macro-BS has a high transmit



**Fig. 2.4** Mobile association policy in a two-tier macro/pico HCN

power, it actually does not provide a sufficiently large average received power for a user due to a large distance, thus making this user connect to a pico BS nearby. Visibly, the deployment of pico BSs allows macro-BSs to offload more users, and in addition setting an extra bias for pico BSs toward admitting users [32] further provides relief to the macrocell tier.

### 2.3.2.3 Multiple-Antenna HCNs

As a natural extension, the study of downlink HCNs has been carried out in multiple-antenna scenarios recently [33–37]. Specifically, Heath et al. [33] have investigated the interference distribution of a user associated with a fixed-size cell, which is inscribed within a weighted Voronoi cell in a Poisson field of interferers. Dhillon and Gupta et al. [34, 35] have derived closed-form expressions for both coverage probability and per user rate by using tools from stochastic orders, which nevertheless are not analytically tractable. Adhikary et al. [36] have proposed interference coordination strategies through spatial blanking by exploiting the directionality in channel vectors at the massive MIMO regime. Li et al. in a very recent contribution [37] have developed a semi-closed expression for success probability in a multi-user MIMO HCN, where the tradeoff between link reliability and the area spectrum efficiency has been discussed.

### 2.3.3 Wireless Ad hoc Networks

Wireless ad hoc networks are fully distributed, autonomous and infrastructureless networks, and have been the most important application field of PPP. In an ad hoc network, all transmitter and receiver nodes are randomly distributed, connecting with each other in any way they want; the connection relation varies all the time. In addition, transmitters make their transmission decisions in a non-coordinated fashion, but adopt slotted Aloha as the MAC protocol, i.e., each node independently decides whether transmits or not in each time slot.

**Fig. 2.5** Wireless ad hoc network

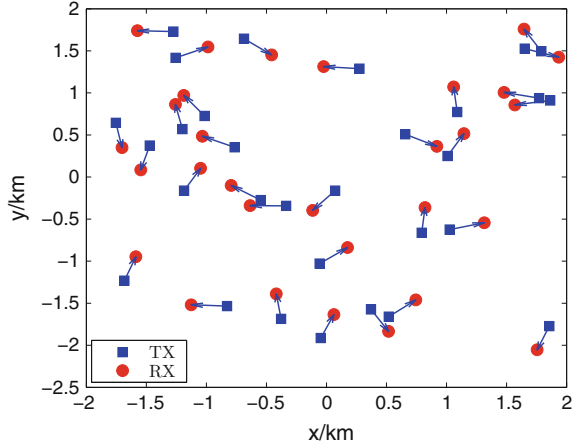


Figure 2.5 illustrates a snapshot of a single-hop wireless ad hoc network, where the locations of all transmitters are modeled as a PPP and each of them connects to a unique receiver. It has been more than three decades that PPP has been used to model wireless ad hoc networks, and a flood of literature has studied the PPP-based ad hoc networks, providing analytically tractable expressions for metrics such as the PDF of interference [38], outage probability [39–41], scaling laws of network capacity [42–44], and more recently the area spectral efficiency [45–47], etc.

## 2.4 Interference Characterization

Equipped with the tool of stochastic geometry and its validation to model the spatial distribution of a random network, in this section we explain how to analyze the effect of the aggregate interference on a receiver in the network. We associate mathematical characterization of the SINR with a *typical user* in the network, which plays a critical role for the secrecy performance analysis in the subsequent chapters.

Given that radio signals suffer from small-scale fading (multiple-path fading and shadowing) and large-scale path loss (power law attenuation with respect to the path distance), the power gain can be characterized as

$$G_{xy} = g_{xy} r_{xy}^{-\alpha}, \quad (2.9)$$

where  $x$  and  $y$  denote the locations of transmitter and receiver,  $g_{xy}$  denotes the small-scale fading gain,  $r_{xy}$  denotes the path distance, and  $\alpha$  denotes the path loss exponent.<sup>3</sup>

<sup>3</sup>In free space,  $\alpha = 2$ , whereas over ground with scattering and absorption, the value of  $\alpha$  is usually better modeled by a value between 2.5 and 4.

Consider a random wireless network where the locations of all potential transmitters are modeled as a PPP  $\Phi \in \mathbb{R}^2$  of density  $\lambda$ . Without loss of generality, we place a receiver of interest at the origin  $o$  of the coordinate system as a typical user. According to the Slivnyak theorem provided by Property 2.6, this operation does not affect the distribution of other nodes. The SINR of the typical user is given by

$$\text{SINR} \triangleq \frac{S}{I + W}, \quad \text{with} \quad I = \sum_{z \in \Phi_t} P_z g_{zo} r_{zo}^{-\alpha}, \quad (2.10)$$

where  $S$ ,  $I$  and  $W$  denote the received signal power, interference power and noise power;  $P_z$  denotes the transmit power of an interfering node located at location  $z$ ,  $\Phi_t$  denotes the set of the locations of those interfering nodes transmitting concurrently, which is obviously a subset of  $\Phi$ . Note that the determination of  $\Phi_t$  depends heavily on the network behavior and related MAC protocols (e.g., Aloha, TDMA). For example, in a wireless ad hoc network with slotted Aloha, all interfering nodes transmit independently and randomly with probability  $p$ , then  $\Phi_t$  is a thinning of  $\Phi$ , i.e., a PPP of density  $p\lambda$ . As to a multiple-tier HCN where the mobile association policy based on the average received power is adopted [23], as depicted in Fig. 2.4, if the typical user access the  $k$ th tier and the distance to its serving BS is  $r$ , there always exists an exclusion region where no interfering BSs in the  $j$ th tier can be found in it. The exclusion region is centered at the typical user with radius  $r_j = r \left( \frac{P_k}{P_j} \right)^{1/\alpha}$ , which can be denoted as  $\mathcal{B}(o, r_j)$ . Then  $\Phi_t$  can be given by  $\Phi_t = \bigcup_j (\Phi \setminus \mathcal{B}(o, r_j))$ .

Due to the randomness of both wireless channels and network geometry, the interference term  $I$  in Eq. (2.10) can be regarded as a random variable, the distribution of which can be characterized via the Laplace transform. Taking a multiple-tier HCN as an example, assuming that all interfering BSs in the  $j$ th tier transmit at power  $P_j$  with locations obeying PPP  $\Phi_j$  of density  $\lambda_j$  and small-scale channel gain  $g_{zo}$  is independent and identically distributed (i.i.d.) obeying Rayleigh fading, i.e., exponent distribution with unit mean. Given that the interfering BSs in the  $j$ th tier are outside the exclusion region  $\mathcal{B}(o, r_j)$ , the Laplace transform of the aggregate interference power from the  $j$ th tier  $I_j = \sum_{z \in \Phi_j} P_j g_{zo} r_{zo}^{-\alpha}$  can be calculated as

$$\begin{aligned} \mathcal{L}_{I_j}(s) &\triangleq \mathbb{E}_{I_j} [e^{-sI_j}] = \mathbb{E}_{\Phi_j, g} \left[ \prod_{z \in \Phi_j} e^{-sP_j g_{zo} r_{zo}^{-\alpha}} \right] \\ &\stackrel{(a)}{=} \exp \left( -2\pi\lambda_j \int_{r_j}^{\infty} (1 - \mathcal{L}_g(sP_j r^{-\alpha})) r dr \right) \\ &\stackrel{(b)}{=} \exp \left( -2\pi\lambda_j \int_{r_j}^{\infty} \left( 1 - \frac{1}{1 + sP_j r^{-\alpha}} \right) r dr \right), \end{aligned} \quad (2.11)$$

where  $\delta \triangleq 2/\alpha$ , (a) follows from the PGFL in Lemma 2.2 along with the independence of  $\Phi_t$  and  $g$ , and (b) holds for exponent distribution of  $g$ .

As to an ad hoc network, due to the absence of an exclusion region around the receiver of interest, to which any interfering node can be arbitrarily close, and thus  $r_j$  in Eq. (2.11) is set to zero. Therefore, we obtain a closed-form expression of  $\mathcal{L}_I(s)$ , which is

$$\mathcal{L}_I(s) = \exp \left( -\pi \lambda_j \Gamma(1 + \delta) \Gamma(1 - \delta) (P_j s)^\delta \right). \quad (2.12)$$

One can see that  $\mathcal{L}_I(s)$  solely depends on the density of interfering nodes  $\lambda_I$  and path loss exponent  $\alpha$  (or  $\delta$ ). Note that only if  $\delta < 1$  does  $\mathcal{L}_I(s)$  in Eq. (2.12) makes sense.

Kindly note that the derivations in Eqs. (2.11) and (2.12) can be applied to more general channel distributions but not limited to Rayleigh fading.

## 2.5 Physical Layer Security in Random Cellular Networks

Recently, stochastic geometry has been extensively used for physical layer security analysis in random wireless networks, where the locations of both legitimate nodes and eavesdropping nodes are modeled as independent PPPs. As discussed previously, modeling legitimate nodes as a PPP is mainly due to the mobility and the random distribution and also the tractability of PPP itself. The reasons behind PPP eavesdroppers is twofold

- On one hand, although the locations of eavesdroppers are unknown in real wiretap scenarios, modeling them as a PPP is still reasonable for the following two cases: 1) for the regular but unlicensed users in the network who are treated as potential eavesdroppers, they share the same mobility as the legitimate nodes do; 2) for the malicious eavesdroppers in the network, they need to imitate the mobility and other behaviors as legitimate nodes to hide their identities, or otherwise they can be easily detected [48].
- On the other hand, PPP is the most random stochastic process, the secure transmission techniques or schemes designed base on which have sufficiently strong robustness.

In the following, we describe several performance metrics to evaluate the physical layer security in a random cellular network, which will be used in the whole book.

### 2.5.1 Connection Outage and Secrecy Outage

As mentioned in Chap. 1, Wyner's wiretap encoding scheme will be discussed in this book. In such a coding scheme, two rate parameters, i.e., transmission rate  $R_t$  and confidential information rate  $R_s$ , should be carefully designed to meet the requirements of reliable and secrecy transmissions. Usually, the performances are evaluated in terms of connection outage, secrecy outage probabilities, and network-wide secrecy throughput.

### 2.5.1.1 Connection Outage

Connection outage probability measures the probability of a unsuccessful transmission. If a legitimate link has capacity  $C_B$  and the transmission rate  $R_t$  of the adopted Wyner's code satisfies  $R_t < C_B$ , the legitimate receiver is able to decode the secret message correctly and perfect connection is assured in this link; otherwise a connection outage occurs. The probability that this connection outage event takes place is referred to as the connection outage probability, denoted as  $\mathcal{P}_{co}$ .

### 2.5.1.2 Secrecy Outage

According to the basic definition of secrecy outage in Sect. 1.3.3 and under Wyner's coding scheme, SOP is defined as the probability that the confidential information rate  $R_s$  exceeds that of the secrecy capacity  $C_s$ , which is denoted as  $\mathcal{P}_{so}$ .

Since  $R_e = R_t - R_s$ ,  $R_s > C_s$  is equivalent to  $R_e < C_E$  where  $C_E$  is channel capacity from the transmitter to the eavesdropper. In a wireless network there are a large number of potential eavesdroppers distributed randomly. Under a reasonable assumption that these eavesdroppers do not collude with each other due to the differences in geographic positions but only decode messages individually, which corresponds to a compound wiretap channel model [49],  $C_E$  is the capacity of the most detrimental eavesdropping link.

The connection outage and secrecy outage probabilities have played a key role in analyzing physical layer security in random wireless networks, and have been extensively investigated in cellular networks [50–52], wireless ad hoc networks [53, 54], CRNs [55, 56], and relay networks [57], etc.

## 2.5.2 Secrecy Throughput

Secrecy throughput is used to evaluate the average capability of secrecy information transmission of a wireless link. Under a predefined connection outage probability  $\mathcal{P}_{co} = \sigma$  and a secrecy outage probability  $\mathcal{P}_{so} = \varepsilon$ , the confidential information rate  $R_s$  of the Wyner's coding could be adjusted if some CSI of the wireless link is available at the transmitter. Mathematically, secrecy throughput is defined as

$$\mathcal{T}_s = \mathbb{E}(R_s(\sigma, \varepsilon)). \quad (2.13)$$

Note that secrecy rate  $R_s$  is a function of  $\sigma$  and  $\varepsilon$ , which can be expressed as  $R_s(\sigma, \varepsilon) = [R_t(\sigma) - R_e(\varepsilon)]^+$ , where codeword rate  $R_t$  and redundant rate  $R_e$  satisfy  $\mathcal{P}_{co}(R_t) = \sigma$  and  $\mathcal{P}_{so}(R_e) = \varepsilon$ , respectively. Clearly, only under the condition  $R_t(\sigma) > R_e(\varepsilon)$  can a positive secrecy rate  $R_s(\sigma, \varepsilon)$  be achieved. This implies, not all selected parameters  $\sigma$  and  $\varepsilon$  can be simultaneously satisfied.

### 2.5.3 Network-Wide Secrecy Throughput

In a wireless network, apart from the security performance of a typical node, e.g., outage probability, achievable secrecy rate and capacity, etc., the *network-wide* security performance and the potential benefits brought by secure transmission techniques and strategies are also highly interested. In this monograph, we concern ourselves with the important metric, named network-wide secrecy throughput, to assess the efficiency of secure transmissions, which is defined as the achievable rate of successful transmission of information bits per unit area under required connection outage and secrecy outage probabilities [53, 54].

The network-wide secrecy throughput under a connection outage probability  $\mathcal{P}_{co} = \sigma$  and a secrecy outage probability  $\mathcal{P}_{so} = \varepsilon$  is given by

$$\mathcal{T}_s \triangleq \lambda(1 - \sigma)R_s(\sigma, \varepsilon), \quad (2.14)$$

where the unit is bits/s/Hz/m<sup>2</sup>. Note that here we assume all the secrecy transmission links in the wireless network adopt a common and constant confidential information rate  $R_s$  rather than adjust it for each transmitter. This is a practical assumption to make the network-wide performance analysis more tractable.

Through investigating outage probabilities and network-wide secrecy throughput, we can gain a better understanding of the significance of physical layer security in random wireless networks, and provide a more explicit guideline for secure transmission techniques and schemes tailored for future wireless networks.

### 2.5.4 A Brief Survey on Physical Layer Security in Wireless Networks

Physical layer security in wireless networks has become an emerging topic very recently, and there have been already some advances reported in the last five years. Here we provide a brief survey where the works are not limited to the cellular network but a general random wireless network.

Early studies on wireless network security from an information-theoretic viewpoint have mainly characterized the secure connectivity of large-scale wireless networks utilizing the concept of secrecy random graph. For example, the statistical characteristic of in-degree and out-degree of network connectivity under security constraints are investigated by Haenggi [58], Pinto et al. [59], and Goel et al. [60]. The existence of a secrecy graph is analyzed in [58, 60] using tools from percolation theory. The authors in [61] show that using directional antenna elements and eigen-beamforming efficiently improves secure connectivity. Scaling laws for secrecy capacity/rate in large wireless networks have been investigated in [62, 63], which are characterized as the order-of-growth of the secrecy capacity/rate as the node number increases. Although scaling laws can provide insights into the secrecy capac-

ity of large-scale networks, they can not reflect the impact of key system parameters and transmission protocols, since most of these factors affect network throughput but not the scaling laws [5].

Research on physical layer security has been further extended to cellular networks [51, 52, 64–66] and ad hoc networks [53, 54, 57, 67], where placement of both legitimate and wiretapping nodes are modeled as PPPs. Specifically, the authors in [51] evaluate the secrecy rate of a cellular network considering cell association as well as information exchange between BSs, under different assumptions on eavesdroppers' location information. This work is extended by [64–66] with both small-scale fading and intercell interference taken into account, and a regularized channel inversion linear precoding is proposed to improve the average secrecy rate. In [53, 54], the authors measure the secrecy transmission capacity with single and multiple-antenna transmitters in ad hoc networks, and provide a tradeoff analysis between connectivity and secrecy. In [57], the authors consider a secure transmission via randomize-and-forward relays in a wireless ad hoc network and discuss the problem that when relay transmission gives a more secure connection. In [67], the authors investigate the issue of secure routing using decode-and-forward relays in a multiple-hop ad hoc network. In [68], the authors investigate physical layer security in a multiple-tier wireless sensor network, and introduce the concept of distributed network secrecy throughput to quantize the network security performance. This topic has also been carried out in emerging wireless networks, including cognitive radio networks, device-to-device networks, Internet of Things, etc., and more details can be found in [56, 69, 70].

Although many efforts have been devoted to physical layer security in random wireless networks, there are still some open problems in this field. In the following, we introduce three of them which we are going to deal with in the following three chapters, respectively.

1. How to optimally allocate the power between information-bearing signal and artificial noise for the artificial noise scheme against randomly distributed eavesdroppers? Although artificial noise scheme has been applied to confuse randomly located eavesdroppers [54, 71], there is still no explicit solution on the optimal power allocation. Providing explicit optimization solutions is of significance for practical secure transmission designs.
2. How to analyze physical layer security for an HCN? Existing literature on HCNs has mainly focused on loading balance, spectrum efficiency, energy efficiency [27, 28, 31, 37], etc.; little of it has involved security issues. It is of necessity to establish a fundamental analysis framework to evaluate the security performance of an HCN in order to protect secure transmissions in HCNs.
3. How to improve the security performance when the transmitter has only one antenna and meanwhile no friendly jammer exists? Many research works on physical layer security in random wireless networks assume that there are either multi-antenna transmitters or friendly jammers [53, 54], which sometimes might not be available due to constraints of size, hardware cost, etc. New approaches are needed to protect information security in these unfavorable scenarios.

## References

1. A.D. Wyner, Shannon-theoretic approach to a Gaussian cellular multiple-access channel. *IEEE Trans. Inf. Theory* **40**(11), 1713–1727 (1994)
2. S. Shamai, A.D. Wyner, Information-theoretic considerations for symmetric, cellular, multiple-access fading channels-parts I & II. *IEEE Trans. Inf. Theory* **43**(11), 1877–1911 (1997)
3. T.S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd edn. (Prentice-Hall, Upper Saddle River, 2002)
4. A.J. Goldsmith, *Wireless Communications* (Cambridge Univ. Press, Cambridge, 2005)
5. M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, M. Franceschetti, Stochastic geometry and random graphs for the analysis and design of wireless networks. *IEEE J. Sel. Areas Commun.* **27**(7), 1029–1046 (2009)
6. D. Stoyan, W. Kendall, J. Mecke, *Stochastic Geometry and Its Applications*, 2nd edn. (Wiley, New York, 1996)
7. M. Haenggi, *Stochastic Geometry for Wireless Networks* (Cambridge University Press, Cambridge, 2012)
8. H. ElSawy, E. Hossain, M. Haenggi, Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: a survey. *IEEE Commun. Surv. Tutor.* **15**(3), 996–1019 (2013)
9. F. Baccelli, B. Blaszczyzyn, *Stochastic Geometry and Wireless Networks in Foundations and Trends in Networking*, vol. 1 (Now Publishers, Breda, 2009)
10. S. Cheng, S. Lien, F. Hu, K. Chen, On exploiting cognitive radio to mitigate interference in macro/femto heterogeneous networks. *IEEE Wirel. Commun.* **18**(3), 40–47 (2011)
11. A. Ghasemi, E. Sousa, Interference aggregation in spectrum sensing cognitive wireless networks. *IEEE J. Sel. Topics Signal Process.* **2**(1), 41–56 (2008)
12. C.-H. Lee, M. Haenggi, Interference and outage in Poisson cognitive networks. *IEEE Trans. Wirel. Commun.* **11**(4), 1392–1401 (2012)
13. A. Rabbachin, T.Q.S. Quek, H. Shin, M.Z. Win, Cognitive network interference. *IEEE J. Sel. Areas Commun.* **29**(2), 480–493 (2011)
14. A. Guo, M. Haenggi, Spatial stochastic models and metrics for the structure of base stations in cellular networks. *IEEE Trans. Wirel. Commun.* **12**(11), 5800–5812 (2013)
15. M. Haenggi, Mean interference in hard-core wireless networks. *IEEE Commun. Lett.* **15**(8), 792–794 (2011)
16. J.G. Andrews, F. Baccelli, R.K. Ganti, A tractable approach to coverage and rate in cellular networks. *IEEE Trans. Commun.* **59**(11), 3122–3134 (2011)
17. B. Blaszczyzyn, M.K. Karray, H.-P. Keeler, Using Poisson processes to model lattice cellular networks, in *Proceedings of 32th Annual IEEE International Conference on Computer Communications (INFOCOM'13), Turin, Italy* (2013), pp. 14–19
18. J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C.K. Soong, J.C. Zhang, What will 5G be? *IEEE J. Sel. Areas Commun.* **32**(6), 1065–1082 (2014)
19. V. Chandrasekhar, J.G. Andrews, A. Gatherer, Femtocell networks: a survey. *IEEE Commun. Mag.* **46**(9), 59–67 (2008)
20. V. Chandrasekhar, J. Andrews, Spectrum allocation in tiered cellular networks. *IEEE Trans. Commun.* **57**(10), 3059–3068 (2009)
21. W. Cheung, T. Quek, M. Kountouris, Throughput optimization, spectrum allocation, and access control in two-tier femtocell networks. *IEEE J. Sel. Areas Commun.* **30**(3), 561–574 (2012)
22. V. Chandrasekhar, J. Andrews, Uplink capacity and interference avoidance for two-tier femto-cell networks. *IEEE Trans. Wirel. Commun.* **8**(7), 3498–3509 (2009)
23. H.-S. Jo, Y.J. Sang, P. Xia, J.G. Andrews, Heterogeneous cellular networks with flexible cell association: a comprehensive downlink SINR analysis. *IEEE Trans. Wirel. Commun.* **11**(10), 3484–3495 (2012)
24. H.S. Dhillon, R.K. Ganti, F. Baccelli, J.G. Andrews, Modeling and analysis of K-tier downlink heterogeneous cellular networks. *IEEE J. Sel. Areas Commun.* **30**(3), 550–560 (2012)

25. G. de la Roche, A. Valcarce, D. López-Pérez, J. Zhang, Access control mechanisms for femtocells. *IEEE Commun. Mag.* **48**(1), 33–39 (2010)
26. P. Xia, V. Chandrasekhar, J.G. Andrews, Open vs. closed access femtocells in the uplink. *IEEE Trans. Wirel. Commun.* **9**(12), 3798–3809 (2010)
27. S. Singh, H.S. Dhillon, J.G. Andrews, Offloading in heterogeneous networks: modeling, analysis, and design insights. *IEEE Trans. Wirel. Commun.* **12**(5), 2484–2497 (2013)
28. H.S. Dhillon, R.K. Ganti, J.G. Andrews, load-aware modeling and analysis of heterogeneous cellular networks. *IEEE Trans. Wirel. Commun.* **12**(4), 1666–1677 (2013)
29. S. Mukherjee, Distribution of downlink SINR in heterogeneous cellular networks. *IEEE J. Sel. Areas Commun.* **30**(3), 575–585 (2012)
30. M.D. Renzo, A. Guidotti, G.E. Corazza, Average rate of downlink heterogeneous cellular networks over generalized fading channels: A stochastic geometry approach. *IEEE Trans. Commun.* **61**(7), 3050–3071 (2013)
31. H.S. Dhillon, J.G. Andrews, Downlink rate distribution in heterogeneous cellular networks under generalized cell selection. *IEEE Wirel. Commun. Lett.* **3**(1), 42–45 (2014)
32. S. Parkvall, A. Furuskar, E. Dahlman, Evolution of LTE toward IMT-advanced. *IEEE Commun. Mag.* **49**(2), 84–91 (2011)
33. R.W. Heath, M. Kountouris, T. Bai, Modeling heterogeneous network interference using Poisson Point Processes. *IEEE Trans. Signal Process.* **61**(16), 4114–4126 (2013)
34. H.S. Dhillon, M. Kountouris, J.G. Andrews, Downlink MIMO HetNets: modeling, ordering results and performance analysis. *IEEE Trans. Wirel. Commun.* **12**(10), 5208–5222 (2013)
35. A.K. Gupta, H.S. Dhillon, S. Vishwanath, J.G. Andrews, Downlink multi-antenna heterogeneous cellular network with load balancing. *IEEE Trans. Commun.* **62**(11), 4052–4067 (2014)
36. A. Adhikary, H.S. Dhillon, G. Caire, Massive-MIMO meets HetNet: interference coordination through spatial blanking. *IEEE J. Sel. Areas Commun.* **33**(6), 1171–1186 (2015)
37. C. Li, J. Zhang, J.G. Andrews, K.B. Letaief, Success probability and area spectral efficiency in multiuser MIMO HetNets. *IEEE Trans. Commun.* **64**(4), 1544–1556 (2016)
38. E.S. Sousa, Optimum transmission range in a direct-sequence spread spectrum multihop packet radio network. *IEEE J. Sel. Areas Commun.* **8**(5), 762–771 (1990)
39. R. Mathar, J. Mattfeldt, On the distribution of cumulated interference power in Rayleigh fading channels. *Wirel. Netw.* **1**(1), 31–36 (1995)
40. M. Souryal, B. Vojcic, R. Pickholtz, Ad hoc, multihop CDMA networks with route diversity in a Rayleigh fading channel, in *Proceedings of IEEE Military Communication Conference (MILCOM'01)* (2001), pp. 1003–1007
41. S. Weber, J.G. Andrews, N. Jindal, An overview of the transmission capacity of wireless networks. *IEEE Trans. Commun.* **58**(12), 3593–3604 (2010)
42. O. Lévêque, I.E. Teletar, Information-theoretic upper bounds on the capacity of large extended ad hoc wireless networks. *IEEE Trans. Inf. Theory*, 858–865 (2005)
43. M. Franceschetti, A note on Lévêque and Telatar's upper bound on the capacity of wireless ad hoc networks. *IEEE Trans. Inf. Theory* **53**(9), 3207–3211 (2007)
44. A. Özgür, O. Lévêque, D. Tse, Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks. *IEEE Trans. Inf. Theory* **53**(10), 3549–3572 (2007)
45. S. Weber, X. Yang, J.G. Andrews, G. de Veciana, Transmission capacity of wireless ad hoc networks with outage constraints. *IEEE Trans. Inf. Theory* **51**(12), 4091–4102 (2005)
46. K. Huang, V.K.N. Lau, Y. Chen, Spectrum sharing between cellular and mobile ad hoc networks: transmission-capacity trade-off. *IEEE J. Sel. Areas Commun.* **27**(7), 1256–1267 (2009)
47. V. Mordachev, S. Loyka, On node density-outage probability tradeoff in wireless networks. *IEEE J. Sel. Areas Commun.* **27**(7), 1120–1131 (2009)
48. Y. Liang, H.V. Poor, L. Ying, Secrecy throughput of MANETs with malicious nodes, in *Proceedings of IEEE ISIT Seoul, Korea* (2009), pp. 1189–1193
49. Y. Liang, G. Kramer, H.V. Poor, S. Shamai, Compound wiretap channels. *EURASIP J. Wirel. Commun. Netw.* (2009)
50. T.-X. Zheng, H.-M. Wang, Q. Yin, On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers. *IEEE Commun. Lett.* **18**(8), 1299–1302 (2014)

51. H. Wang, X. Zhou, M.C. Reed, Physical layer security in cellular networks: a stochastic geometry approach. *IEEE Trans. Wirel. Commun.* **12**(6), 2776–2787 (2013)
52. H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, M.H. Lee, Physical layer security in heterogeneous cellular networks. *IEEE Trans. Commun.* **64**(3), 1204–1219 (2016)
53. X. Zhou, R. Ganti, J. Andrews, A. Hjørungnes, On the throughput cost of physical layer security in decentralized wireless networks. *IEEE Trans. Wirel. Commun.* **10**(8), 2764–2775 (2011)
54. X. Zhang, X. Zhou, M.R. McKay, Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **8**(11), 1802–1814 (2013)
55. Y. Deng, L. Wang, S.A.R. Zaidi, J. Yuan, M. ElKashlan, Artificial-noise aided secure transmission in large scale spectrum sharing networks. *IEEE Trans. Commun.* **64**(5), 2116–2129 (2016)
56. X.M. Xu, B. He, W.W. Yang, X. Zhou, Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **11**(2), 373–387 (2016)
57. C. Cai, Y. Cai, X. Zhou, W. Yang, W. Yang, When does relay transmission give a more secure connection in wireless ad hoc networks? *IEEE Trans. Inf. Forensics Secur.* **9**(4), 624–632 (2014)
58. M. Haenggi, The secrecy graph and some of its properties, in *Proceedings of IEEE ISIT, Toronto, Canada*, (2008), pp. 539–543
59. P.C. Pinto, M.Z. Win, Percolation and connectivity in the intrinsically secure communications graph. *IEEE Trans. Inf. Theory* **58**(3), 1716–1730 (2010)
60. S. Goel, V. Aggarwal, A. Yener, A.R. Calderbank, Modeling location uncertainty for eavesdroppers: a secrecy graph approach, in *Proceedings of IEEE ISIT, Austin, USA* (2010), pp. 2627–2631
61. P.C. Pinto, J. Barros, M.Z. Win, Secure communication in stochastic wireless networks Part I: Connectivity. *IEEE Trans. Inf. Forensics Secur.* **7**(1), 125–138 (2012)
62. O.O. Koyluoglu, C.E. Koksall, H.E. Gamal, On secrecy capacity scaling in wireless networks. *IEEE Trans. Inf. Theory* **58**(5), 3000–3015 (2012)
63. C. Capar, D. Goeckel, B. Liu, D. Towsley, Secret communication in large wireless networks without eavesdropper location information, in *Proceedings of IEEE INFOCOM, Orlando, USA* (2012), pp. 1152–1160
64. G. Geraci, R. Couillet, J. Yuan, M. Debbah, I.B. Collings, Large system analysis of linear precoding in MISO broadcast channels with confidential messages. *IEEE J. Sel. Areas Commun.* **31**(9), 1660–1671 (2013)
65. G. Geraci, S. Singh, J.G. Andrews, J. Yuan, I.B. Collings, Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. *IEEE Trans. Wirel. Commun.* **13**(5), 2931–2943 (2014)
66. G. Geraci, H.S. Dhillon, J.G. Andrews, J. Yuan, I.B. Collings, Physical layer security in downlink multi-antenna cellular networks. *IEEE Trans. Commun.* **62**(6), 2006–2021 (2014)
67. J. Yao, S. Feng, X. Zhou, Y. Liu, Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying. *IEEE Trans. Commun.* **64**(2), 753–764 (2016)
68. J. Lee, A. Conti, A. Rabbachin, M.Z. Win, Distributed network secrecy. *IEEE J. Sel. Areas Commun.* **31**(9), 1889–1900 (2013)
69. D. Wu, J. Wang, R.Q. Hu, Y. Cai, Energy-efficient resource sharing for mobile device-to-device multimedia communications. *IEEE Trans. Veh. Technol.* **63**(5), 2093–2103 (2014)
70. A. Mukherjee, Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. *Proc. IEEE* **103**(10), 1747–1761 (2015)
71. M. Ghogho, A. Swami, Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers, in *Proceedings of IEEE ICC Workshops* (2011), pp. 1–5

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