On Ergodic Secrecy Capacity of Random Wireless Networks with Protected Zones

Weigang Liu, *Student Member, IEEE*, Zhiguo Ding, *Member, IEEE*, Tharmalingam Ratnarajah, *Senior Member, IEEE* and Jiang Xue, *Member, IEEE*

***Abstract*—In this paper, we investigate physical layer security in a random wireless network where both legitimate and eavesdropping nodes are randomly deployed. In the first scenario, we study the basic random network without a protected zone around the source node. The probability density functions (PDF) for the composite channel gain with both fading and path loss is derived and used to calculate the probability of secure connection and ergodic secrecy capacity. In the second scenario, we consider the use of secrecy protected zone around the source node to enhance the security in a noise limited network. Here we study the two cases (i) the eavesdroppers are aware of the secrecy protected zone; (ii) the eavesdroppers are unaware of the secrecy protected zone. Moreover, the distribution of the distances between the origin and random nodes outside the secrecy protected zone is derived. In the last scenario, the interferer protected zones around the legitimate receivers are used to improve the physical layer security by restructuring the interference. The derived analytical results are verified by the Monte Carlo simulations. It is shown that the application of secrecy and interferer protected zones lead to significant improvement in the security depending on different system parameters.**

***Index Terms*—Ergodic secrecy capacity, interference, physical layer security, protected zone, stochastic geometry**

I. Introduction

Despite the rapid growth of wireless communication systems in recent years, wireless communication faces many security challenges due to the open nature of the wireless medium and the dynamic topology of wireless networks. Traditionally, security in wireless communication has been viewed as an upper layer issue to be addressed independent of the physical layer. The most widely used technique for security in wireless communication is cryptographic protocols, which are based on secret and public keys by assuming the computational advantage of legitimate transmission. Potentially, cryptographic schemes and channel coding techniques can be combined to exploit the randomness of wireless channels.

The basic principle of information-theoretic security, also termed as physical layer security, has been widely accepted as a promising means to realize security in the wireless networks. The objective of physical layer security is to ensure that the legitimate receivers can recover the source information reliably while the eavesdroppers will not be able to interpret any of the information. This principle of perfect security was first proposed by Shannon in his paper with the notion of *perfect* secrecy [1], which does not rely on any assumptions of the computational capability of eavesdroppers.

In recognition of growing security threats in wireless networks, great effort has been made to develop physical layer security schemes, based on the information-theoretical secrecy concept that explores the possibility of securing communication links without using cryptography in the presence of transparent eavesdroppers[1]. Wyner introduced the concept of wire-tap channels and analyzed the information-theoretical security of discrete memoryless channels [2]. It is shown that perfect secrecy could be achieved when the legitimate receiver has a better channel than that of the eavesdroppers. This notion was further generalized to additive white Gaussian noise (AWGN) channels by Cheong and Hellman [3]. In [4], Csiszár and Körner considered the broadcast wireless channels and showed that the security of a transmission can still be guaranteed by applying sophisticated channel codes, even if the eavesdropping channel is not a degraded version of the channel between the legitimate transceiver.

The rate at which information can be transmitted secretly from the source to its intended destination is called achievable *secrecy rate*, while the maximum achievable secrecy rate is called the *secrecy capacity*. By taking channel propagation effects into consideration, the secrecy capacity of wireless fading channels was investigated in [5], and expressions of the average secrecy capacity and the *secrecy outage* for quasi-static fading channels were derived in [6]. Exact expression of the secrecy capacity is hard to obtain, due to the limited knowledge of channel status information (CSI) and path loss in legitimate and eavesdropping channels. Ergodic secrecy capacity, derived from statistics of CSI and distances which are easier to obtain, can provide a single letter characterization for the secrecy capacity of an arbitrary wire-tap channel. It can also provide a helpful reference for the design of networks

The work of W. Liu was supported by the CSC (China Scholarship Council) and the EPSRC grant funded by the UK government (No. EP/I037156/2). The work of T. Ratnarajah and J. Xue was supported by the EPSRC grant funded by the UK government (No. EP/I037156/2). The work of Z. Ding was supported by the EPSRC grant funded by the UK government (No. EP/L025272/1).

W. Liu, T. Ratnarajah and J. Xue are with the Institute for Digital Communications, School of Engineering, The University of Edinburgh, Alexander Graham Bell Building, King's Buildings, Mayfield Road, Edinburgh, EH9 3JL, United Kingdom (email: {w.liu; t.ratnarajah and j.xue}@ed.ac.uk). Weigang Liu is the corresponding author.

Z. Ding is with the School of Computing and Communications, Lancaster University, Lancaster, LA1 4YW, United Kingdom (e-mail:z.ding@lancaster.ac.uk).

[1]By "*transparent eavesdropper*" we refer to an intruder as described by Wyner, with full knowledge of the system used by the legitimate pair.

such as allocating the transmission power and application of protected zones. The ergodic secrecy capacity of fading channels without considering path loss was derived independently in [5] and [7].

Previous works of physical layer security primarily focused on point-to-point transmissions [8]–[10]. Recent efforts are to achieve a better understanding of the inherent secrecy capabilities of wireless systems under more realistic conditions, such as the distribution of randomly deployed users in large-scale networks. When studying security in random wireless networks via stochastic geometric tools [11], the notion of *secrecy graphs* emerged in [12]. An important distinction between secrecy graphs and the conventional point-to-point wire-tap channel is that the *topology* of networks, with respect to both the legitimate and eavesdropping nodes, play a major role not only on *how much* secrecy rate is available, but also on *how to measure* it. Following this instinct, secrecy rate scaling laws were studied in [13], while the secrecy rates of unicast links in the presence of multiple eavesdroppers were studied in [14]. Secrecy connectivity over large-scale network were widely investigated in [11], [12] and [15].

To enhance physical layer security in large-scale networks, various strategies were investigated, such as guard zones [16], [17], sectorized transmission [18], precoding [19] and the use of artificial noise [20]–[22]. Specifically, guard zones were studied in [12] to improve secrecy connectivity without considering fading, while the study of [16] investigated how to enhance the secrecy transmission capacity using a guard zone, based on the assumption of fixed distances between the transmitters and the intended receivers. The concept of secrecy protected zone [21] that extinct the eavesdroppers in the zone is different from the guard zone that allows the existence of the eavesdroppers inside the protected area. The authors of [21] considered the use of artificial noise and a secrecy protected zone to enhance the security of random networks, in the presence of eavesdroppers and interferers randomly deployed according to two homogeneous Poisson point processes (PPPs). The study investigated the use of a secrecy protected zone surrounding the transmitter in order to stop eavesdroppers approaching, while still being affected by interference from other legitimate transmitters. Analysis in [16] and [21] derived the upper bound of the secrecy outage based on the uniform distribution of eavesdroppers and the lower bound by the distribution of the nearest eavesdropper, respectively.

In this paper, we investigate how to enhance physical layer security in random wireless networks with a secrecy protected zone surrounding the transmitter as well as the interferer protect zones surrounding the legitimate receivers. The impacts of fading, interference and protected zones are studied in order to analyze the secrecy performance. For large-scale networks, interference has usually been viewed as a harmful factor. However, the interference can be well structured by using interferer protected zones to benefit the secrecy transmission in a similar manner to artificial noise. Notice that, the interference studied in this work refers to the signals between other transmitters and receivers, rather than artificial noise introduced additionally as in the work of [16], [23] and [24]. Besides, the locations of interferers follow a Poisson hole process, due to the existence of the interferer protected zones. The contributions of this research are summarized as follows:

- We derive the distribution of channel gains from the transmitter to receivers which are ordered either according to the distance or their strength. The expression for the distribution of channel gains is an important tool for calculating the capacity at the worst-case eavesdropper[2], which can be applied to derive the secrecy outage, the probability of secure connection, and the ergodic secrecy capacity.
- The ergodic secrecy capacity of random wireless networks is analyzed by considering both large scale path loss and small scale fading. Additionally, we derive the distribution of path loss for the nodes outside the secrecy protected zone. To the best of the authors' knowledge, this has not been provided elsewhere before.
- Besides the secrecy protected zone, we also employ interferer protected zones to restructure interference and enhance the physical layer security. The distance distribution of legitimate receivers outside the secrecy protected zone is studied.
- By adopting interferer protected zones at legitimate receivers, interference can be restructured to benefit the security at the legitimate receiver without introducing artificial noise. It is worth to notice that interference is different from jamming noise, because it is the signal broadcasted by other transmitters. Moreover, the distribution of the active cooperative transmitters that follow a Poisson-hole process has also been exploited.

The rest of this paper is organized as follows. The system model and mathematical concepts for stochastic geometry modelling are presented in Section II. In Section III, we study the security in random wireless networks by deriving the distribution for the composite channel gain. The performance of adopting the protected zones with and without considering interference are presented in Section IV and V, respectively. The numerical results of secrecy characteristics are discussed in Section VI. Finally, concluding marks are drawn in Section VII.

II. System Model and Problem Formulation

A. Random network model

In this paper, we consider a random wireless network deployed in an unbound two dimensional space consisting of nodes modeled by a homogeneous PPP with intensity λ and denoted as Φ. According to the stationarity of PPP, we fix the source node at the origin as the distribution of Φ is translation-invariant. Let $\Xi = \left\{\xi_k = \frac{r_k^\alpha}{|h_k|^2}\right\}, k \in \mathbb{N}$ be the path loss process with small scale fading [11], where α is the path loss exponent, r_k and h_k denote the distance and the fading coefficient between the source node and the k_{th} receiving node, respectively. Ξ is also a PPP which will be discussed in section III. Note that $\{\xi_k\}$ is not ordered according to distance

[2]The worst-case eavesdropper means the eavesdropper which can obtain the largest instantaneous capacity.

TABLE I
LIST OF NOTATION

Notation	*Description*
Φ_l	Poisson point process of legitimate receivers
Φ_c	Poisson point process of interferers
Φ_e	Poisson point process of eavesdroppers
λ_l	Intensity of Φ_l
λ_c	Intensity of Φ_c
λ_e	Intensity of Φ_e
$C_{s:k}$	Ergodic secrecy capacity at the k_{th} legitimate receiver
P	Transmit power
h_k	Fading between transmitter and k_{th} legitimate receiver
h_e	Fading between transmitter and the worst-case eavesdropper
r_k	Distance between transmitter and k_{th} legitimate receiver
r_e	Distance between transmitter and the best eavesdropper
ξ_k	Composite channel gain, $\xi_k = r_k^\alpha/\lvert h_k\rvert^2$
ξ_e	Composite channel gain, $\xi_e = r_e^\alpha/\lvert h_e\rvert^2$
α	Path-loss exponent
ρ_t	Radius of secrecy protected zone at transmitter
ρ_d	Radius of interferer protected zone at legitimate receiver
$\mathbb{P}(.)$	Probability operator
$\mathbb{E}\{.\}$	Expectation operator

$\{r_k\}$ [11], but ordered by the combination of path loss and fading.

The random network model given above can be modeled by two overlaid PPPs of legitimate nodes and eavesdroppers, with corresponding densities denoted as λ_l and λ_e. The source node aims to transmit a signal to the k_{th} legitimate receiver in presence of eavesdroppers located at unknown distances. The legitimate and eavesdropping channels are subject to quasi-static fading and path loss.

Three scenarios are studied in this work. In the first scenario, the basic random network is studied without a protected zone. While in the second scenario, a secrecy protected zone surrounding the source node is used to enhance security in noise limited networks. In addition, two cases in which eavesdroppers are aware and unaware of the secrecy protected zone are investigated. Besides of utilizing a secrecy protected zone, in the third scenario we analyze the impact of interference restructuring on security by adopting interferer protected zones.

B. Problem Formulation

1) Secrecy capacity: The secrecy capacity is the maximum data rate at which the legitimate receiver can decode the signal information with arbitrarily small error, while the eavesdroppers' error probabilities of decoding approach to one. The secrecy capacity of the transmission from the source node to the k_{th} legitimate node is given by [4]

$$C_{l:k} = \left[\log_2\left(1+\frac{P}{\xi_k\sigma_l^2}\right) - \log_2\left(1+\frac{P}{\xi_e\sigma_e^2}\right)\right]^+, \quad (1)$$

where $[a]^+ = \max\{0,a\}$; $\xi_e = \frac{r_e^\alpha}{|h_e|^2}$, r_e and h_e denote the distance and fading coefficient between the transmitter and the worst-case eavesdropper; P, σ_l^2 and σ_e^2 denote the transmission power at the source node, the noise at the legitimate node and the worst-case eavesdropper, respectively.

2) Secrecy outage probability and probability of secure connection: Secrecy outage probability, known as the outage probability of secrecy capacity under small scale fading, is given by [6]

$$\begin{aligned}\mathbb{P}_{out}(\varrho) &= \mathbb{P}\left\{C_{l:k} \le \varrho\right\} \\ &= \mathbb{P}\left\{\left[\log_2\left(\frac{1+\eta_l/\xi_k}{1+\eta_e/\xi_e}\right)\right]^+ < \varrho\right\},\end{aligned} \quad (2)$$

where $\eta_l = \frac{P}{\sigma_l^2}$ and $\eta_e = \frac{P}{\sigma_e^2}$. The probability of secure connection is the probability to have a positive secrecy rate from the source node to the legitimate receiver [25], which can be obtained by substitute $\varrho = 0$ into equation (2).

3) Ergodic secrecy capacity: The ergodic capacity from the source node to the k_{th} legitimate receiver and the worst-case eavesdropper can be obtained, respectively, as [26]

$$\begin{aligned}R_{s:k} &= \mathbb{E}_{h_k,r_k}\left\{\log_2\left(1+\frac{|h_k|^2P}{r_k^\alpha\sigma_l^2}\right)\right\}, \\ R_{s:e} &= \mathbb{E}_{h_e,r_e}\left\{\log_2\left(1+\frac{|h_e|^2P}{r_e^\alpha\sigma_e^2}\right)\right\}.\end{aligned} \quad (3)$$

Note that, when analyzing the ergodic secrecy capacity, the legitimate receivers is ordered by their distances to the source node. This is different from the ordering based on the combined effect of path loss and small-scale fading, which will be used to derive the distribution of the secrecy capacity and the probability of secure connections in Section III-A, B and C. The adjustment of the ordering is motivated by the following reasons. The investigation of the legitimate receivers based on the ordering of the combined effect of path loss and fading can reflect the order of their secrecy capacity and the probability of secure connection, which is a better indication of how the fading and the point distribution affect the secrecy of a network. Besides, ordering the legitimate receivers based on the combined effects can also provide more insights, as the analysis of the worst-case eavesdropper is also based on the combined effect, which will be shown in Section III. However, as the derivation of the ergodic secrecy capacity should be based on the communication between the same transmitter-receiver pair over a period of time, it will be reasonable to order the legitimate receivers according to their distances to the source node.

The ergodic secrecy capacity can be derived by assuming that the worst-case eavesdropper can keep achieving the largest channel gain. Consequently, the ergodic capacity of the worst-case eavesdropper obtained in equation (3) is an upper bound. Because of this, a lower bound of the ergodic secrecy capacity can be obtained as [22], [27], [28]

$$C_{s:k} = \left[R_{s:k} - R_{s:e}\right]^+. \quad (4)$$

III. Security in random wireless networks

In this section, we will first derive the PDF of the composite channel gain in the interference-free scenario without considering protected zone. Afterwards, this PDF will be used to analyze the distribution of the secrecy capacity, the probability of secure connection and the ergodic secrecy capacity.

A. PDF for the composite channel gain

To obtain the distribution of $C_{l:k}$ for random networks under Nakagami-m fading, we need to derive the PDF of ξ_k and ξ_e.

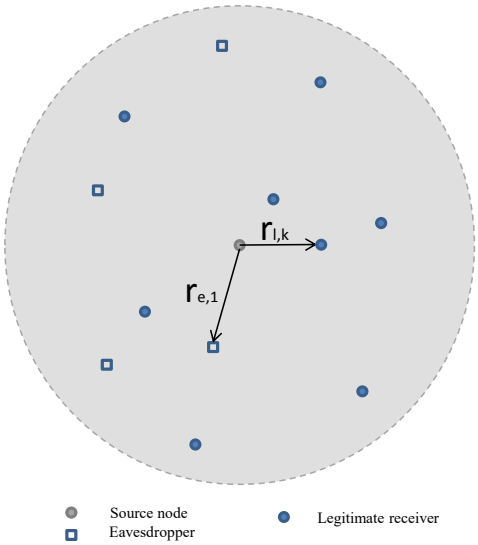


Fig. 1. Random network without protected zone.

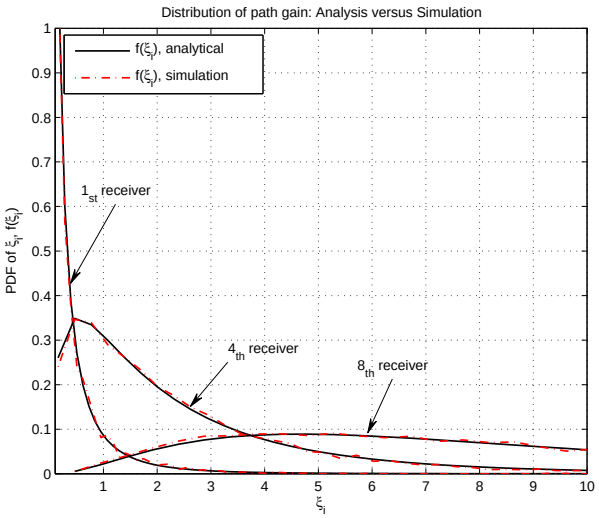


Fig. 2. PDF of ξ from the source node to the 1st, 4th and 8th receivers with $\lambda = 1$, $m = 1.5$ and $\alpha = 4$.

We define the path loss $x_k = r_k^\alpha$ and denote the intensity of the set $\Xi = \{x_k/h_k, k \in \mathbb{N}\}$ as λ_Ξ. Then the intensity function of Ξ is given in Lemma 1.

Lemma 1: Given that intensity of Φ is λ and the shape parameter of Nakagami fading is denoted as m, Ξ is a PPP and the intensity function of Ξ can be expressed by

$$\lambda_\Xi(x) = A_0 x^{\delta-1}, \tag{5}$$

where $\delta = \frac{2}{\alpha}$ and $A_0 = \pi\lambda\delta\frac{\Gamma(\delta+m)}{m^\delta\Gamma(m)}$.

Proof: The point process of Ξ can be obtained from the PPP of $\Phi = \{r_k\}$ by a deterministic mapping and independent displacement. According to the displacement theorem and mapping theorem for point process transformations, Ξ is also a PPP [11]. First, the intensity function of $\Psi = \{x_k\}$ can be derived from $\mathbb{E}\{\Phi([0,x))\} = \lambda\pi x^2$ by mapping theorem

$$\lambda_\Psi(x) = \lambda\pi\delta x^{\delta-1}. \tag{6}$$

Then, the intensity function $\lambda_\Xi(x)$ can be obtained by displacement theorem for the general Nakagami-m fading model by following Theorem 2.33 in [29]. ∎

Theorem 1: The PDF of ξ_k under Nakagami-m fading is

$$f_{\xi_k}(s) = \exp(-A_1 s^\delta)\frac{\delta(A_1 s^\delta)^k}{s\Gamma(k)}, \tag{7}$$

where $A_1 = \frac{A_0}{\delta}$.

Proof: As Ξ is a PPP, the cumulative distribution function (CDF) of ξ_k can be expressed by

$$\begin{aligned} F_{\xi_k}(s) &= \mathbb{P}(\xi_k < s), \\ &= 1 - \mathbb{P}\left(\Xi[0,s) < k\right), \\ &= 1 - \sum_{n=0}^{k-1}\exp\left(-\int_0^s \lambda_\Xi(x)\,\mathrm{d}x\right)\frac{(\int_0^s \lambda_\Xi(x)\,\mathrm{d}x)^n}{n!}, \\ &\overset{(a)}{=} 1 - \sum_{n=0}^{k-1}\exp\left(-A_1 s^\delta\right)\frac{(A_1 s^\delta)^n}{n!}, \end{aligned} \tag{8}$$

where $\Xi[0,s)$ denotes the counting measure induced by a random circular set of Ξ centered at the origin with radius s, and (a) follows from

$$\int_0^s \lambda_\Xi(x)\,\mathrm{d}x = \int_0^s A_0 x^{\delta-1}\,\mathrm{d}x = \frac{A_0}{\delta}s^\delta. \tag{9}$$

By denoting $A_1 = \frac{A_0}{\delta}$ and taking the derivative of $F_{\xi_k}(s)$, we can obtain the PDF for the composite channel gain as expressed in (7). ∎

Fig.2 is plotted to compare the PDF of the composite channel gain derived in (7) with the Monte Carlo simulation at various nodes. It shows that the proposed PDF is accurate, as verified by the simulation.

B. Distribution of the secrecy capacity

To derive the distribution of the secrecy capacity, we first investigate the distribution of the capacity at the legitimate receiver. The outage probability of the capacity at the k_{th} legitimate receiver can be derived by

$$\begin{aligned} \mathbb{P}_{out}(R_k < \varrho) &= \mathbb{P}\left(\log_2(1+\frac{\eta_l}{\xi_k}) < \varrho\right), \\ &= 1 - \int_0^{\frac{\eta_l}{2^\varrho-1}} f_{\xi_k}(s)\,\mathrm{d}s, \\ &\overset{(b)}{=} 1 - \frac{\delta A_1^k}{\Gamma(k)}\int_0^{\frac{\eta_l}{2^\varrho-1}}\exp(-A_1 s^\delta)s^{\delta k-1}\,\mathrm{d}s, \\ &\overset{(c)}{=} \frac{\Gamma\left(k, A_1\left[\frac{\eta_l}{(2^\varrho-1)}\right]^\delta\right)}{\Gamma(k)}, \end{aligned} \tag{10}$$

where (b) follows from Theorem 1 and (c) follows from [30, Eq. 3.381]. The PDF of the maximum achievable rate at the k_{th} legitimate receiver can be acquired by taking the derivation

of $\mathbb{P}_{out}\left(R_k < \varrho\right)$ as follows

$$\begin{aligned} f_{R_k}(\varrho) =& \ln 2\ \eta_l^{\delta k} \frac{\delta A_1^k}{\Gamma(k)} \frac{2^{\varrho}}{(2^{\varrho}-1)^{\delta k+1}} \\ & \times \exp\left(-A_1 \left(\frac{\eta_l}{2^{\varrho}-1}\right)^{\delta}\right). \end{aligned} \tag{11}$$

Similarly, the PDF of the maximum achievable rate at the worst-case eavesdropper can be obtained by setting $k=1$ and $A_e = \pi\lambda_e \frac{\Gamma(\delta+m)}{m^{\delta}\Gamma(m)}$ as

$$f_{R_e}(\varrho) = \ln 2\ \eta_e^{\delta} \frac{2^{\varrho}\delta A_e}{(2^{\varrho}-1)^{\delta+1}} \exp\left(-A_e \left(\frac{\eta_e}{2^{\varrho}-1}\right)^{\delta}\right). \tag{12}$$

Then the distribution of the secrecy capacity at the k_{th} legitimate node can be easily obtained through the convolution of $f_{R_k}(\varrho)$ for the k_{th} legitimate receiver and the worst-case eavesdropper similar to the steps used in [15] which ignored the effect of small scale fading. Note that in this scenario, we derive the PDF of the maximum achievable rate for the network under Nakagami-m fading. Since the PDF of ξ_k has already included the effect of fading, the density function for the composite channel gain of the worst-case eavesdropper can be calculated briefly by setting $k=1$. Otherwise, deriving the distribution of the channel gain at the worst-case eavesdropper will be quite complicated if considering distribution of fading coefficient and path loss separately.

C. Probability of secure connection

Probability of secure connection is the probability to have a positive secrecy rate from the source node to the k_{th} legitimate receiver [25]. It can be derived from the secrecy outage probability in (2) and expressed by

$$\mathbb{P}_{sc,k} = \mathbb{P}\left\{\log_2\left(1+\frac{\eta_l}{\xi_k}\right) - \log_2\left(1+\frac{\eta_e}{\xi_e}\right) > 0\right\}. \tag{13}$$

By using the algebraic operation similar to the one derived in (13) and Theorem 1, the probability of secure connection can be obtained as

$$\mathbb{P}_{con,k} = 1 - \left(\frac{\lambda_l}{\lambda_l+\lambda_e}\right)^k. \tag{14}$$

Comparing with the derivation in [15], this result shows that fading does not affect the probability of secure connection which is determined only by the ratio of intensities.

D. Ergodic secrecy capacity without the protected zone

In the scenario without the protected zone, the legitimate nodes and eavesdroppers are distributed as two independent PPPs with different intensities, λ_l and λ_e. It is worth to notice that the legitimate receivers are ordered by the distance between the source node and the legitimate receiver, meanwhile the ergodic capacity at the k_{th} legitimate receiver can be obtained based on Theorem 2. The ergodic capacity at the worst-case eavesdropper will be derived by applying the distribution of ξ_e as shown in the following theorem.

Theorem 2: The ergodic capacity of the channel between the source node and the k_{th} legitimate node ordered by distance can be expressed as

$$\begin{aligned} R_{s:k} =& \frac{(\pi\lambda_l)^k \delta m^m}{\ln 2\Gamma(m)\Gamma(k)} \int_0^{\infty}\int_0^{\infty} s^{m-1} \ln\left(1+\eta_l s\right) \\ & \times y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^{\delta}\right) \mathrm{d}y\, \mathrm{d}s. \end{aligned} \tag{15}$$

Proof: We denote the distance from the source node to the k_{th} legitimate receiver as r_k, and $x_{k,l} = r_k^{\alpha}$. According to the mapping theorem, the random variable $x_{k,l}$ is also distributed as a PPP [31] with its distribution given by

$$f_{x_{k,l}}(x) = \frac{(\pi\lambda_l)^k \delta}{\Gamma(k)} x^{k\delta-1} \exp(-\pi\lambda x^{\delta}). \tag{16}$$

The distribution of Nakagami-m (power) fading model is given by [11]

$$f_{|h_{k,l}|^2}(x) = \frac{m^m x^{m-1} exp(-mx)}{\Gamma(m)}. \tag{17}$$

Accordingly, the distribution of the channel gain $\zeta_k = \frac{|h_{k,l}|^2}{x_{k,l}}$ can be derived as

$$\begin{aligned} f_{\zeta_k}(s) =& \int_{-\infty}^{\infty} |y| f_{|h_{k,l}|^2,\ x_{k,l}}(sy, y)\, \mathrm{d}y, \\ =& \int_0^{\infty} y f_{|h_{k,l}|^2}(sy) f_{x_{k,l}}(y)\, \mathrm{d}y, \\ =& \int_0^{\infty} y \frac{m^m (sy)^{m-1} \exp(-msy)}{\Gamma(m)} \frac{(\pi\lambda_l)^k \delta}{\Gamma(k)} y^{k\delta-1} \\ & \times \exp(-\pi\lambda y^{\delta})\, \mathrm{d}y, \\ =& \frac{(\pi\lambda_l)^k \delta m^m s^{m-1}}{\Gamma(m)\Gamma(k)} \\ & \times \int_0^{\infty} y^{k\delta+m-1} \exp(-msy - \lambda_l \pi y^{\delta})\, \mathrm{d}y. \end{aligned} \tag{18}$$

By using (3) and (18), the ergodic capacity at the k_{th} legitimate receiver can be found as

$$\begin{aligned} R_{s:k} =& \mathbb{E}_{\zeta_k}\left\{\log_2\left(1+\eta_l\zeta_k\right)\right\}, \\ =& \frac{1}{\ln 2} \int_0^{\infty} \ln\left(1+\eta_l s\right) f_{\zeta_k}(s)\, \mathrm{d}s, \\ =& \frac{1}{\ln 2} \int_0^{\infty} \ln\left(1+\eta_l s\right) s^{m-1} \frac{(\pi\lambda_l)^k \delta m^m}{\Gamma(m)\Gamma(k)} \\ & \times \int_0^{\infty} y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^{\delta}\right) \mathrm{d}y\, \mathrm{d}s, \\ =& \frac{(\pi\lambda_l)^k \delta m^m}{\ln 2\Gamma(m)\Gamma(k)} \int_0^{\infty}\int_0^{\infty} \ln\left(1+\eta_l s\right) s^{m-1} \\ & \times y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^{\delta}\right) \mathrm{d}y\, \mathrm{d}s. \end{aligned} \tag{19}$$

■

For the case of $\alpha = 4$ and $m = 1$ which is corresponding to Rayleigh fading, the ergodic capacity at the nearest legitimate

receiver can be obtained as follows:

$$\begin{aligned} R_{s:1} &= \frac{\pi\lambda_l}{2\ln 2}\int_0^\infty\int_0^\infty \ln\left(1+\eta_l s\right) y^{\frac{1}{2}} \exp\left(-sy-\lambda_l\pi y^{\frac{1}{2}}\right) \mathrm{d}s\,\mathrm{d}y, \\ &\overset{(d)}{=} \frac{\pi\lambda_l}{2\ln 2}\int_0^\infty y^{-\frac{1}{2}} \exp\left(-\lambda_l\pi y^{\frac{1}{2}}\right) G_{3,2}^{3,1}\left(\frac{\eta_l}{y}\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right)\mathrm{d}y, \\ &\overset{(e)}{=} \frac{1}{\ln 2\sqrt{\pi}} G_{4,3}^{3,3}\left(\frac{4}{\eta_l(\pi\lambda_l)^2}\middle|\begin{matrix}0,\frac{1}{2},0,1\\1,0,0\end{matrix}\right), \end{aligned} \tag{20}$$

where $G(\cdot)$ is the Meijer-G function; (d) follows by expressing $\ln(1+x)$ as Meijier G-function $\ln(1+x)=G_{2,2}^{1,2}\left(x\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)$ and applying the integration relationship [30, Eq. 7.813.1]; (e) follows from [30, Eq. 7.813.2].

Similarly, by using (3) and (7), the ergodic capacity of the channel between the source node and the worst-case eavesdropper can be expressed by

$$\begin{aligned} R_{s:e} &= \mathbb{E}_{\xi_e}\left\{\log_2\left(1+\frac{\eta_e}{\xi_e}\right)\right\}, \\ &= \frac{\delta A_{1e}}{\ln 2}\int_0^\infty \ln\left(1+\frac{\eta_e}{s}\right) s^{\delta-1}\exp\left(-A_e s^\delta\right)\mathrm{d}s, \\ &= \frac{\delta A_{1e}}{\ln 2}\int_0^\infty s^{\delta-1}\exp\left(-A_e s^\delta\right) G_{2,2}^{1,2}\left(\frac{\eta_l}{s}\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathrm{d}s, \\ &\overset{(f)}{=} \frac{1}{\ln 2\sqrt{\pi}} G_{4,2}^{2,3}\left(\frac{4}{\eta_e A_e^2}\middle|\begin{matrix}0,\frac{1}{2},0,1\\1,0\end{matrix}\right), \end{aligned} \tag{21}$$

where (f) follows from $\alpha=4$ and [30, Eq. 7.813.2]. Then, substitute (15) and (21) into (4), the lower bound of the ergodic secrecy capacity at the k_{th} legitimate node in the random network without a protected zone can be derived.

IV. Enhancing Security with the Secrecy Protected Zone

To enhance the security of the legitimate transmission, we adopt the scheme of the secrecy protected zone [23] where the source node can keep a circular area free of eavesdroppers, denoted as $\mathfrak{D}_t(0,\rho_t)$ and ρ_t is the radius of the secrecy protected zone. Notice that legitimate nodes are still deployed as a PPP in $\mathbb{R}^2$ while eavesdroppers are distributed as a PPP in $\bar{\mathfrak{D}}_t$, where $\bar{\mathfrak{D}}_t$ represents the complement set of $\mathfrak{D}_t(0,\rho_t)$ in $\mathbb{R}^2$. In this paper, we will study the case that eavesdroppers are not colluding.

Since the ergodic capacity of the worst-case eavesdropper in this scenario is complicated to calculate, we will first consider the worst case. To maximize its data rate, the eavesdropper will try to approach the source node and stay at the boundary of the secrecy protected zone. In this case, the distance between the source node and the nearest eavesdropper is the radius of the secrecy protected zone, ρ_t. Later in this section, it will be proved that the nearest eavesdropper is the worst-case eavesdropper since it can acquire the largest ergodic capacity. Furthermore, the scenario that the eavesdroppers are distributed as a PPP outside the secrecy protected zone will also be investigated.

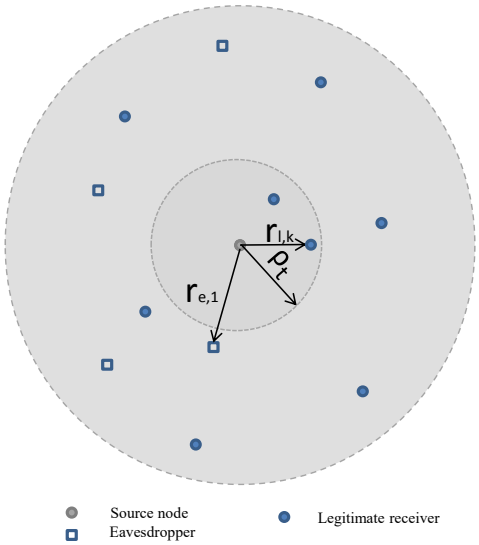


Fig. 3. Random network with the secrecy protected zone, $\mathfrak{D}_t(0,\rho_t)$, at the source node.

A. Eavesdropper on the Boundary of the Secrecy Protected Zone

For the case that the eavesdroppers are aware of the secrecy protected zone, we study the worst case that the eavesdroppers try to maximize their data rate by approaching the boundary of the zone. We will first prove that the nearest eavesdropper to the source node has the largest ergodic capacity in Proposition 1 and then derive the ergodic capacity at the worst-case eavesdropper.

Proposition 1: The ergodic capacity $R_{s:r}$ of the channel between the source node and the receiving node is monotonically decreasing with their distance r for arbitrary fading channels.

Proof: See Appendix A. ∎

From Proposition 1, we can see that the nearest eavesdropper can obtain the largest ergodic capacity. Therefore, the worst case is that there will be eavesdroppers on the boundary of the secrecy protected zone, i.e. $r_e=\rho_t$. By expressing $\ln(1+x)$ as Meijier G-function and applying the integration relationships [30, Eq. 7.813.1] and [30, Eq. 7.813.2], the ergodic capacity of the channel between the source node and the nearest eavesdropper can be calculated by

$$\begin{aligned} R_{s:e} =& \mathbb{E}_{|h_e|^2}\left\{\log_2\left(1+\frac{\eta_e|h_e|^2}{\rho_t^\alpha}\right)\right\}, \\ =& \frac{m^m}{\ln 2\Gamma(m)}\int_0^\infty \ln\left(1+\frac{\eta_e}{\rho_t^\alpha}x\right) x^{m-1}\exp(-mx)\,\mathrm{d}x. \\ =& \frac{m^m}{\ln 2\Gamma(m)}\int_0^\infty x^{m-1}\exp(-mx) \\ & \times G_{2,2}^{1,2}\left(\frac{\eta_e}{\rho_t^\alpha}x\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathrm{d}x, \\ =& \frac{1}{\ln 2\Gamma(m)} G_{3,2}^{1,3}\left(\frac{\eta_e}{m\rho_t^\alpha}\middle|\begin{matrix}1-m,1,1\\1,0\end{matrix}\right). \end{aligned} \tag{22}$$

For the case with Nakagami-m fading, the ergodic secrecy capacity lower bound at the k_{th} legitimate receiver with a secrecy protected zone can be obtained by substituting (15)

and (22) into (4). For the case with Rayleigh fading, (22) can be simplified as

$$R_{s:e} \overset{(g)}{=} \frac{1}{\ln 2}\int_0^{\infty} \ln\left(1+\frac{\eta_e}{\rho_t^{\alpha}}x\right)\exp(-x)\,\mathrm{d}x, \\ \overset{(h)}{=} \frac{1}{\ln 2} G_{3,2}^{1,3}\left(\frac{\eta_e}{\rho_t^4}\middle|\begin{matrix}0,1,1\\1,0\end{matrix}\right), \tag{23}$$

where (g) follows from that h_e is Rayleigh fading and its power is exponentially distributed; (h) follows from [30, Eq. 7.813.1].

B. Random Eavesdroppers Outside of the Secrecy Protected Zone

For the general case, the eavesdroppers may be unaware of the boundary that their locations are still distributed as a PPP in the field outside the secrecy protected zone. According to Proposition 1, the worst-case eavesdropper is the nearest eavesdropper which will obtain the largest ergodic capacity. To calculate the ergodic capacity at the worst-case eavesdropper, we derive the distribution of its distance from the source node as shown in Theorem 3.

Theorem 3: Consider a random network in which the nodes are modeled by a PPP outside a circular area. The PDF of the distance from the origin to the n_{th} nearest node is given by

$$d_n(r) = 2\pi\lambda r \exp\left[-\pi\lambda\left(r^2-\rho^2\right)\right]\frac{\left[\pi\lambda\left(r^2-\rho^2\right)\right]^{n-1}}{(n-1)!}, \tag{24}$$

where $r > \rho$, λ is the intensity and ρ is the radius of the circular area.

Proof: See Appendix B. ∎

The PDF of the distance from the source node to the n_{th} receiving node outside a circular area in (24) has been verified by Monte Carlo simulations in Fig. 4. When there is no protected zone, i.e. $\rho = 0$, the distribution of the distance from the origin to the n_{th} node can be obtain from (24) as

$$d_n(r) = 2\pi\lambda r \exp(-\pi\lambda r^2)\frac{(\pi\lambda r^2)^{n-1}}{(n-1)!}. \tag{25}$$

This is exactly the PDF of the Euclidean distance from the source node to the n_{th} neighbor provided in [31]. The distribution of the distance from the nearest node to the origin can be obtained by setting $n = 1$ in (24) as

$$d_1(r) = 2\pi\lambda r \exp[-\pi\lambda(r^2-\rho^2)],\ r > \rho. \tag{26}$$

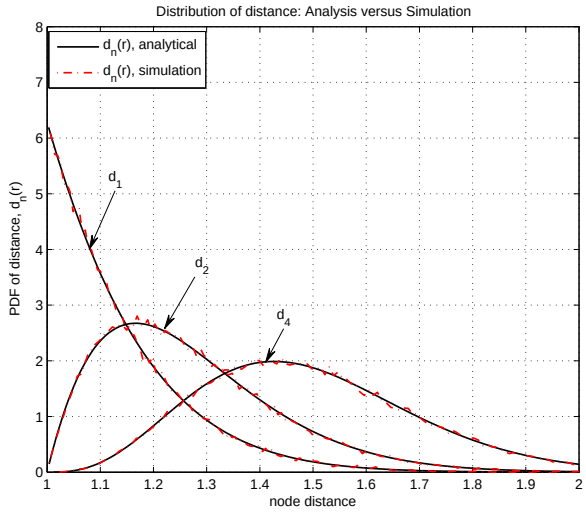


Fig. 4. PDF of the distance from the source node to the n_{th} neighbor with $\lambda = 1, \rho_t = 1$; d_1, d_2 and d_4 show the distribution of the distances from the source node to the 1st, 2nd, and 4th nodes, respectively.

Consequently, the ergodic capacity at the worst-case eavesdropper can be obtained by

$$\begin{aligned} R_{s:e} =& \mathbb{E}_{h_e,r_{e,1}}\left\{\log_2\left(1+\frac{\eta_e|h_e|^2}{r_{e,1}^{\alpha}}\right)\right\}, \\ =& \mathbb{E}_{r_{e,1}}\left\{\int_0^{\infty}\log_2\left(1+\frac{\eta_e}{r_{e,1}^{\alpha}}x\right)f_{|h_e|^2}(x)\,\mathrm{d}x\right\}, \\ =& \int_{\rho_t}^{\infty}\int_0^{\infty}\log_2\left(1+\frac{\eta_e}{y^{\alpha}}x\right)f_{|h_e|^2}(x)\,\mathrm{d}x f_{r_{e,1}}(y)\,\mathrm{d}y, \\ =& -\frac{2\pi\lambda_e}{\ln 2}\exp(\pi\lambda_e\rho_t^2)\int_0^{\infty} y\exp\left(\frac{y^{\alpha}}{\eta_e}-\pi\lambda_e y^2\right) \\ & \times Ei\left(-\frac{y^{\alpha}}{\eta_e}\right)\mathrm{d}y, \end{aligned} \tag{27}$$

where $E_i(\cdot)$ is the exponential integral. Notice that, to avoid confusion, we use $f_{r_{e,1}}(y)$ to denote the function of $d_1(r)$. Similarly, the lower bound on the ergodic secrecy capacity can be obtained by substituting (15) and (27) into (4).

V. Enhancing Security with Both the Secrecy Protected Zone and the Interferer Protected Zone

A. Problem Formulation

In addition to adopting a secrecy protected zone around the source node, we introduce the interferer protected zones which will contribute to restructuring the interference and enhance the physical layer security. For the interference limited random network, properly restructuring the interference can reduce its detriment to the legitimate receivers more than that of the eavesdroppers.

To reduce the interference in the legitimate channels, the legitimate receivers will broadcast beacon signals with the same power P_b [32]. The cooperative nodes that have received the beacon signals will stop transmission. Note that these cooperative nodes are different from those externally introduced jammers in [16], but similar to the secondary

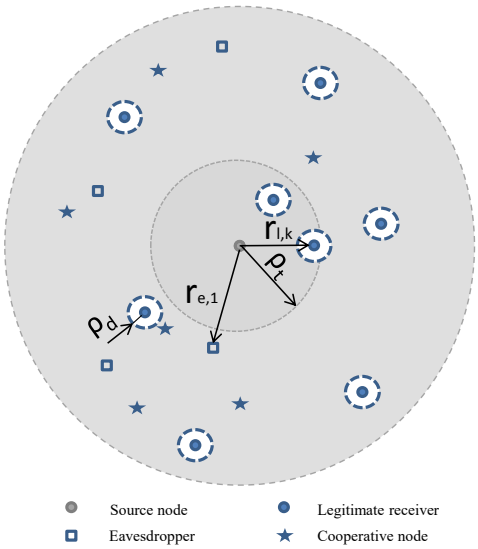


Fig. 5. Random network with a secrecy protected zone at the source node denoted by $\mathfrak{D}(0,\rho_t)$ and interferer protected zones surrounding the legitimate receivers denoted by $\mathfrak{D}(x,\rho_d)$.

transmitters in cognitive radio (CR) networks. The legitimate receivers will formulate another kind of protected zones $\Phi_d=\{\mathfrak{D}(x,\rho_d)|x\in\Phi_l\}$, where $\mathfrak{D}(x,\rho_d)$ is the circular area centered at x with radius ρ_d and x is the coordinate of the legitimate receiver. Then, the set of the cooperative nodes can be expressed by

$$\Phi_c=\left\{u_i\Big|u_i\in\left\{\mathbb{R}^2-\bigcup_{x\in\Phi_l}\mathfrak{D}(x,\rho_d)\right\}\right\},\ i\in\mathbb{N}.$$

The description of the system model is given as follows and illustrated in Fig. 5,

- The distribution of the source node and the legitimate receivers are the same as the previous scenarios in Section II, III and IV;
- The cooperative nodes are modeled by a homogeneous PPP with intensity λ_c;
- To reduce the detriment from the interference, interferer protected zones are adopted surrounding the legitimate receivers. The legitimate receivers will prevent cooperative nodes that are located in a nearby region from transmitting signals inside the interferer protected zones, by adopting the request-to-send/clear-to-send (RTS/CTS) protocol in IEEE 802.11 [24].

To calculate the ergodic secrecy capacity, we will first derive the distribution of the aggregate interference and the ergodic capacity at the legitimate receivers and the eavesdroppers.

B. Distribution of the aggregated interference and ergodic capacity at the legitimate receiver

The locations of the active cooperative nodes are depending on the exclusion regions which are set up by the legitimate receivers. The random set of cooperative nodes, Φ_c, can be considered as a Poisson hole process [29] with primary intensity λ_l and secondary intensity λ_c. The probability of a point retained in the Poisson hole process is the probability that no active cooperative node exists within the distance r from the legitimate receiver. Consequently, the intensity of the Poisson hole process is given by

$$\lambda_{eqc}=\lambda_c\exp\left(-\lambda_l\pi r^2\right). \tag{28}$$

Since the distribution of the active cooperative nodes is restructured by independent thinning of the cognitive users outside the exclusion regions, we approximate the Poisson hole process with a PPP by some adjustment of the intensity [33]. In the following subsection, we will calculate the distribution of the aggregate interference from the cooperative nodes to the legitimate receivers based on this approximation.

1) Interference at the legitimate receivers: The higher-order statistics of the interference formed by the active cooperative nodes will have less impact on the signal-to-interference-plus-noise ratio (SINR) at the legitimate receivers than that of the lower-order statistics, such as expectation and variance [34], [35]. As a result, the interference from the Poisson hole process can be approximately modeled by a PPP. The aggregate interference from the cooperative nodes to the legitimate receivers can be obtained by using Eq.(3.46) in [36], while the interference in our case is analyzed based on an approximated PPP with intensity $\lambda_c\exp(-\lambda_l\pi r^2)$. Denote the moment generating function (MGF) of aggregated interference at the legitimate receivers as $\mathcal{L}_{I_{cd}}(s)$, it is given by

$$\begin{aligned}\mathcal{L}_{I_{cd}}(s)=&\exp\Bigg\{-\lambda_{eqc}\pi\Bigg(s^{\delta}\mathbb{E}_h\left(h^{\delta}\gamma(1-\delta,sh\rho^{-\alpha})\right)\\&-\rho^2\mathbb{E}_h\left(1-\exp(-sh\rho^{-\alpha})\right)\Bigg)\Bigg\}.\end{aligned} \tag{29}$$

For Rayleigh fading, equation (29) can be written as

$$\begin{aligned}\mathcal{L}_{I_{cd}}(s)=&\exp\Bigg\{-\lambda_{eqc}\pi\Bigg(\frac{s\rho^2}{s+\rho^{\alpha}}+\frac{s\Gamma(2)}{(1-\delta)\rho^{\alpha(1-\delta)}}\\&\times_2F_1(1-\delta,2;2-\delta;-s\rho^{-\alpha})\Bigg)\Bigg\}.\end{aligned} \tag{30}$$

2) Ergodic capacity at the legitimate receivers: We denote the SINR at the k_{th} legitimate receiver as $\gamma_{s:k}$, then

$$\begin{aligned}\gamma_{s:k}&=\frac{P|h_k|^2r_k^{-\alpha}}{P_c\sum_{i\in\Phi_c}|h_{i,k}|^2r_{i,k}^{-\alpha}+\sigma_k^2},\\&=\frac{S_{td}}{I_{cd}+N},\end{aligned} \tag{31}$$

where $h_{i,k}$ denotes the fading coefficient between the i_{th} cooperative node and the k_{th} legitimate receiver. Assuming that the noise at the legitimate receivers are dominated by the interference, the success probability at the k_{th} legitimate receiver can be approximated by

$$\begin{aligned}\mathbb{P}_{td}(\tau)&\approx\mathbb{P}\left(\gamma_{s:k}>\tau\right),\\&=\mathbb{P}\left(S_{td}>\tau I_{cd}\right),\\&\overset{(i)}{=}\mathbb{E}_{I_{cd}}\left(\exp(-\tau P^{-1}r_k^{\alpha}I_{cd})\right),\\&\overset{(j)}{=}\mathcal{L}_{I_{cd}}\left(\frac{\tau}{P\ r_k^{-\alpha}}\right),\end{aligned} \tag{32}$$

where (i) follows from that $|h_k|^2$ is exponentially distributed and (j) follows from Laplace transformation. Substitute (30)

into (32), we can obtain the expression of success probability at the k_{th} legitimate receiver. The CDF of the SIR at the k_{th} legitimate receiver can be denoted by $F_{\gamma_{s:k}}(\tau) = 1 - \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)$. Then we derive the PDF of the SIR from $F_{\gamma_{s:k}}(z)$ and analyze the ergodic capacity at the k_{th} legitimate receiver as [26]. Assuming that the distance r_k is known at the transmitter, the ergodic capacity at the k_{th} legitimate receiver can be obtained as

$$\begin{aligned} R_{s:k} =& \int_0^\infty \log_2(1+\tau) f_{\gamma_{s:k}}(\tau)\,\mathrm{d}\tau, \\ =& \frac{1}{\ln 2}\int_0^\infty \ln(1+\tau)\,\mathrm{d}\left[1-\mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\right], \\ =& -\frac{1}{\ln 2}\ln(1+\tau)\mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\Big|_0^\infty \\ &+\frac{1}{\ln 2}\int_0^\infty \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\frac{1}{1+\tau}\,\mathrm{d}\tau, \\ =& \frac{1}{\ln 2}\int_0^\infty \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\frac{1}{1+\tau}\,\mathrm{d}\tau. \end{aligned} \tag{33}$$

The ergodic capacity in (33) can be calculated by using numerical methods. Since deriving the closed-form expression of the ergodic capacity at the k_{th} legitimate receiver is complicated, we analyze the lower bound of the interference at the legitimate receiver and obtain

$$\begin{aligned} \mathcal{L}_{I_{cd}}(s) =& \exp\Big\{-\lambda_{eqc}\pi\Big[s^\delta \mathbb{E}_h(h^\delta\gamma(1-\delta, sh\rho^{-\alpha})) \\ &-\rho^2\mathbb{E}_h(1-\exp(-sh\rho^{-\alpha}))\Big]\Big\}, \\ \overset{(k)}{\geq}& \exp\Big\{-\lambda_{eqc}\pi\Big[s^\delta \mathbb{E}_h(h^\delta\Gamma(1-\delta)) \\ &-\rho^2\mathbb{E}_h(1-\exp(-sh\rho^{-\alpha}))\Big]\Big\}, \\ =& \exp\Big\{-\lambda_{eqc}\pi\Big[s^\delta\Gamma(1+\delta)\Gamma(1-\delta)-\frac{s\rho^2}{s+\rho^\alpha}\Big]\Big\}, \end{aligned} \tag{34}$$

where (k) follows from $\gamma(a,x) \leq \Gamma(a)$. According to (33), the lower bound of the ergodic capacity at the k_{th} legitimate receiver can be expressed by

$$\begin{aligned} R_{s,k} \overset{(l)}{=}& \frac{Pr_k^{-\alpha}}{\ln 2}\int_0^\infty \mathcal{L}_{I_{cd}}(s)\frac{1}{1+Pr_k^{-\alpha}\cdot s}\,\mathrm{d}s, \\ \overset{(m)}{\geq}& \frac{Pr_k^{-\alpha}}{\ln 2}\int_0^\infty \frac{1}{1+Pr_k^{-\alpha}\cdot s}\exp\Big\{\lambda_{eqc}\pi\frac{s\rho^2}{s+\rho^\alpha}\Big\} \\ &\times\exp\Big\{-\lambda_{eqc}\pi\Gamma(1+\delta)\Gamma(1-\delta)s^\delta\Big\}\,\mathrm{d}s, \\ \overset{(n)}{=}& \frac{P\Gamma(1+\frac{1}{\delta})}{a^{\frac{1}{\delta}}r_k^\alpha\ln 2}\mathbb{E}_s\Big[\frac{1}{1+Pr_k^{-\alpha}s}\exp\Big(\lambda_{eqc}\pi\frac{s\rho^2}{s+\rho^\alpha}\Big)\Big], \\ \overset{(o)}{\geq}& \frac{Pr_k^{-\alpha}\Gamma(1+\frac{1}{\delta})}{a^{\frac{1}{\delta}}\ln 2}\frac{1}{1+Pr_k^{-\alpha}\mathbb{E}_s(s)} \\ &\times\exp\Big(\lambda_{eqc}\pi\frac{\mathbb{E}_s(s)\rho^2}{\mathbb{E}_s(s)+\rho^\alpha}\Big), \end{aligned} \tag{35}$$

where (l) follows by substituting τ with $Pr_k^{-\alpha}s$; (m) follows from (34); (n) follows by defining the PDF of s as $f_s(x) = \frac{a^{1/\delta}}{\Gamma(1+1/\delta)}\exp(-ax^\delta)$ and $a = \pi\lambda_{eqc}\Gamma(1+\delta)\Gamma(1-\delta)$; (o) follows from Jenson's inequality with the expectation of s been given by

$$\mathbb{E}_x(s) = \int_0^\infty s f_x(s)\,\mathrm{d}s = \frac{\Gamma(2/\delta)}{\delta a^{1/\delta}\Gamma(1+1/\delta)}.$$

C. Distribution of the aggregated interference and ergodic capacity at the worst-case eavesdropper

1) The interference at the eavesdroppers: Similarly, the aggregate interference from the cooperative nodes to the eavesdroppers can be obtained by using Eq.(3.21) in [36] and

$$\mathcal{L}_{I_{ce}}(s) = \exp\left(-\lambda_{eqc}\pi s^\delta\frac{\pi\delta}{\sin(\pi\delta)}\right). \tag{36}$$

2) Ergodic capacity at the eavesdroppers: Ergodic capacity at the eavesdroppers can be derived following the work of [26]. Denoting the SINR at the eavesdroppers as $\gamma_{s:e}$, we have

$$\begin{aligned} \gamma_{s:e} =& \frac{P|h_e|^2 r_{t,e}^{-\alpha}}{P_c\sum_{i\in\Phi_c}|h_{i,e}|^2 r_{i,e}^{-\alpha}+\sigma_e^2}, \\ =& \frac{S_{te}}{I_{ce}+N}, \end{aligned} \tag{37}$$

where $h_{i,e}$ denotes the fading coefficient from the i_{th} cooperative node to the nearest eavesdropper. Assuming that the noise at the eavesdroppers are dominated by the interference, the success probability at the eavesdroppers is given by

$$\begin{aligned} \mathbb{P}(\tau) \approx& \mathbb{P}(S_{te} > \tau I_{ce}), \\ =& \mathbb{E}_h\left(\exp(-\tau P^{-1}r_{t,e}^\alpha I_{ce})\right), \\ =& \mathcal{L}_{I_{ce}}\left(\frac{\tau}{P\ r_{t,e}^{-\alpha}}\right). \end{aligned} \tag{38}$$

Substitute (28) and (36) into (38), we can obtain the success probability at the eavesdroppers. The CDF of the SIR at the eavesdroppers can be denoted by

$$\begin{aligned} F_{\gamma_{s:e}}(\tau) =& 1-\mathcal{L}_{I_{ce}}\left(\frac{\tau}{Pr_e^{-\alpha}}\right), \\ =& 1-\exp\left(-b_e r_e^2\tau^\delta\right), \end{aligned} \tag{39}$$

where $b_e = \frac{\pi^2\lambda_{eqc}\delta}{P^\delta\sin(\pi\delta)}$. Then the PDF of the SIR $f_{\gamma_{s:e}}(\tau)$ can be derived from $F_{\gamma_{s:e}}(\tau)$ as

$$f_{\gamma_{s:e}}(\tau) = \delta b_e r_e^2\tau^{\delta-1}\exp\left(-b_e r_e^2\tau^\delta\right). \tag{40}$$

Considering the security constraint, we study the ergodic capacity at the nearest eavesdropper which can obtain the maximum ergodic capacity as shown in Proposition 1. The

ergodic capacity at the nearest eavesdropper is given by

$$\begin{aligned} R_{s,e} &= \int_{\rho_t}^{\infty}\int_{0}^{\infty} \log_2(1+\tau) f_{\gamma_{t:e}}(\tau) f_{r_{e,1}}(x)\,\mathrm{d}\tau\,\mathrm{d}x, \\ &= \frac{1}{\ln 2}\int_{\rho_t}^{\infty} f_{r_{e,1}}(x)\int_{0}^{\infty} \ln(1+\tau)\,\mathrm{d}\left[-F_{\gamma_{t:e}}(\tau)\right]\mathrm{d}x, \\ &= \frac{1}{\ln 2}\int_{\rho_t}^{\infty} f_{r_{e,1}}(x)\int_{0}^{\infty} \exp(-b_e x^2\tau^{\delta})\frac{1}{1+\tau}\,\mathrm{d}\tau\,\mathrm{d}x, \\ &= \frac{2\pi\lambda_e \exp(\pi\lambda_e\rho_t^2)}{\ln 2} \\ &\quad\times \int_{\rho_t}^{\infty}\int_{0}^{\infty} \frac{x}{1+\tau}\exp\left[-(\pi\lambda_e + b_e\tau^{\delta})r_{e,1}^2\right]\mathrm{d}x\,\mathrm{d}\tau, \\ &= \frac{\pi\lambda_e}{\ln 2}\int_{0}^{\infty} \frac{\exp(-b_e\rho_t^2\tau^{\delta})}{(1+\tau)(\pi\lambda_e + b_e\tau^{\delta})}\,\mathrm{d}\tau. \end{aligned} \tag{41}$$

VI. Numerical Results

In section III and IV, we have simulated the distribution of the composite channel gain and the distance, in Fig.2 and Fig.4, respectively. In this section, we will study the effect of various factors on the lower bound of the ergodic secrecy capacity, including the intensity ratio, the radius of the protected zones, path loss, interference and transmission power.

A. Lower bound of the ergodic secrecy capacity with no interference

Fig.6 illustrates the lower bound of the ergodic secrecy capacity between the source node and the legitimate receivers without a protected zone. In this scenario, the impact of path loss and the intensity ratio between the legitimate receivers and eavesdroppers is investigated. As shown in Fig.6, the lower bound of ergodic secrecy capacity is monotonically increasing with the increase of the intensity ratio between the legitimate and eavesdropping nodes. When both of the legitimate receivers and eavesdroppers experience the same fading and path loss, the ergodic secrecy capacity at all the legitimate receivers are zero if their intensity is equal to or smaller than the intensity of eavesdroppers, i.e. $\lambda_l/\lambda_e \leq 1$. An interesting point shown in Fig.6 is that increasing the path loss exponent will be beneficial for enhancing the ergodic secrecy capacity which is due to the difference of their distance to the source under the condition of $\lambda_l/\lambda_e > 1$.

Fig.7 reveals the impact of adopting a secrecy protected zone surrounding the source node to enhance the ergodic secrecy capacity. ρ_t denotes the radius of the secrecy protected zone. As shown in Fig.7, for the same intensity ratio between the legitimate receivers and the eavesdroppers, increasing the radius of the protected zone can be helpful to enhance the ergodic secrecy capacity. Compared to the results shown in Fig.6 where the ergodic secrecy capacity will be zero if $\lambda_l/\lambda_e \leq 1$, the application of a protected zone ensures that positive ergodic secrecy capacity can still be achieved even if $\lambda_l/\lambda_e \leq 1$, for example, $\lambda_l/\lambda_e = 0.5$. Another insight gained

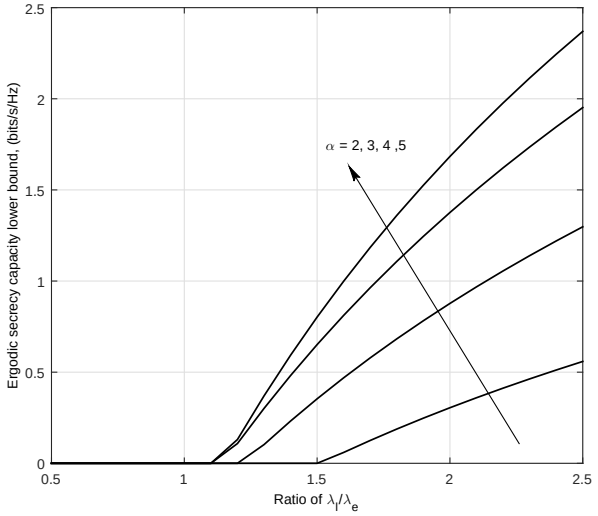


Fig. 6. The ergodic secrecy capacity as a function of the legitimate and eavesdropping node intensities with different path-loss exponents, $\lambda_e = 1$ and $m = 1$.

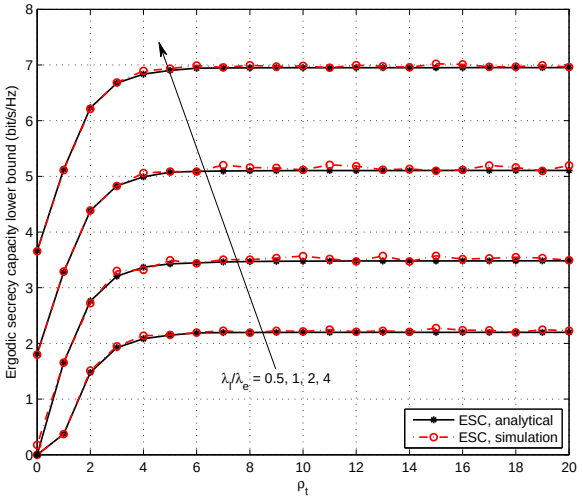


Fig. 7. The impact of the secrecy protected zone size on the ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 30, \lambda_e = 0.1, \alpha = 4$ and $\rho_d = 2$.

from Fig.7 is that the increase of ρ_t has limited impact on the ergodic secrecy capacity. This limitation is the value of the ergodic capacity at the legitimate receiver, since the ergodic secrecy capacity cannot be larger than ergodic capacity at the legitimate receiver.

Fig.8 and Fig.9 show the impact of the protected zone surrounding the source node, as well as the impact of the intensity ratio on ergodic secrecy capacity. The legitimate receiving nodes are ordered by their distances to the source node. As shown in Fig.8, it is clear that, if the radius of the protected zone is zero, i.e., there will be no protected zone, the three scenarios will have the same performance. For different scenarios with the same value of intensity ratio and protected zone radius, adopting a protected zone will significantly improve the lower bound of the ergodic secrecy capacity. When eavesdroppers are aware of the secrecy

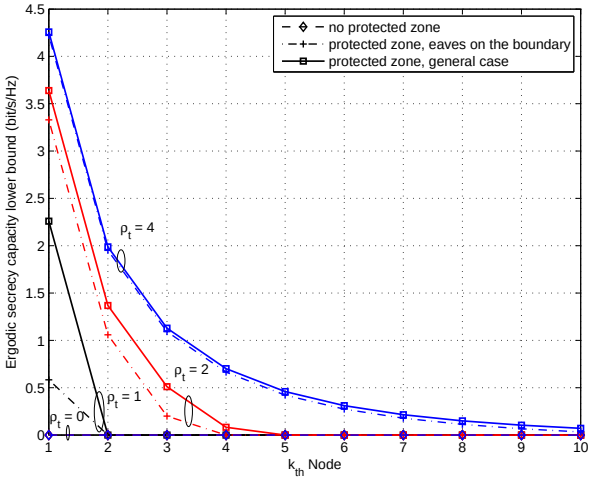


Fig. 8. The impact of the secrecy protected zone size on ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 20, \lambda_l = \lambda_e = 0.2, \alpha = 4$ and $\rho_d = 2$.

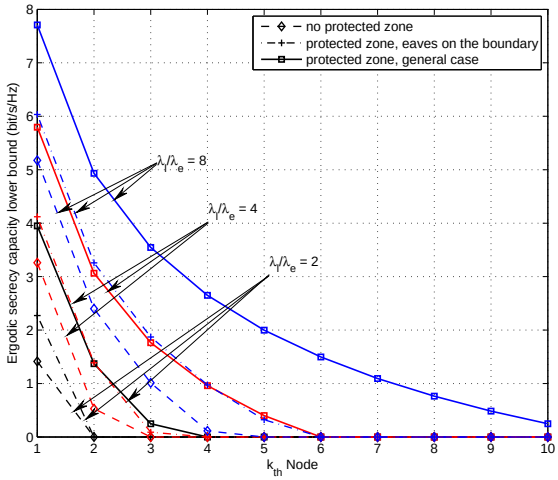


Fig. 9. The impact of intensity ratio on ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 20, \lambda_e = 0.2, \alpha = 4, \rho_t = 1$ and $\rho_d = 2$.

protected zone boundary, security will be undermined, but it can still achieve higher ergodic secrecy capacity comparing to the case without a protected zone. Fig.8 and Fig.9 also suggest that increasing the intensity ratio and radius of the secrecy protected zone is helpful to increase ergodic secrecy capacity. Fig.9 further indicates that increasing the intensity ratio between legitimate receivers and eavesdroppers will lead to a higher ergodic secrecy capacity for all scenarios.

B. Ergodic secrecy capacity with interference

Fig.10 shows the comprehensive impact of the protected zone radius at the legitimate receivers and the intensity of the cooperative nodes. It is apparent that increasing transmission power at the source node increases the ergodic capacity lower bound at the legitimate receivers. Although simply increasing the intensity of cooperative nodes will undermine the security performance at legitimate receivers, the adoption of a secrecy protected zone can increase the ergodic secrecy capacity lower bound. In other words, combined with a secrecy protected zone, using an interferer protected zone in order to restructure interference can improve the ergodic secrecy capacity lower bound. This is because a larger protected zone radius, ρ_d, will reduce interference noise at the legitimate nodes compared to that at the eavesdroppers.

VII. Conclusion

In this work, we studied physical layer security in random wireless networks. The PDF of the channel gains by considering both fading and path loss was considered and a closed form expression of its reciprocal is derived. This result was then applied to analyze the probability of secure connection and ergodic secrecy capacity. Furthermore, we investigated the scenario with a secrecy protected zone to enhance physical layer security and the analytical expression of ergodic secrecy capacity is obtained. Moreover, interferer protected zones surrounding legitimate receivers are also considered to reduce the detriment from interference.

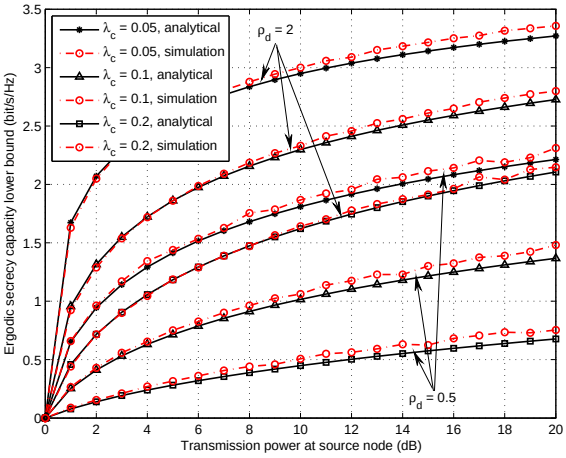


Fig. 10. The impact of the interferer protected zones on ergodic secrecy capacity, with $\alpha = 4, \lambda_l = \lambda_e = 0.1, \rho_t = 5$ and $P_c/\sigma_l^2 = P_c/\sigma_e^2 = 1$.

By employing protected zones, positive ergodic secrecy capacity can be achieved even if the intensity of the legitimate nodes is smaller than that of the eavesdropping nodes in random wireless networks. The application of interferer protected zones can make the interference beneficial to the security of the wireless network. Both the PDFs and the concept of ergodic secrecy capacity provided in this paper can be easily extended to the analysis of other secrecy characteristics in random wireless networks, such as secrecy outage. They can also be extended to investigate the cases with eavesdropper colluding and multiple antennas at the source node.

Appendix A
Proof of Proposition 1

Proof: The ergodic capacity $R_{s;r}$ of a general fading channel with the PDF of the fading coefficient denoted as

$f_{|h|^2}(x)$, can be expressed as follows:

$$\begin{aligned} R_{s:r} &= \mathbb{E}_{|h|^2}\left\{\log_2\left(1+\frac{\eta|h|^2}{r^\alpha}\right)\right\}, \\ &= \int_0^\infty \log_2\left(1+\frac{\eta}{r^\alpha}x\right) f_{|h|^2}(x)\,\mathrm{d}x. \end{aligned} \tag{42}$$

Then, the derivation of $R_{s:e}$ as a function of r is given by

$$\begin{aligned} \frac{\partial R_{s:r}}{\partial r} &= \int_0^\infty \left[\log_2\left(1+\frac{\eta}{r^\alpha}x\right)\right]' f_{|h|^2}(x)\,\mathrm{d}x, \\ &= -\frac{\alpha\eta}{r\ln 2}\int_0^\infty \frac{x}{r^\alpha+\eta x} f_{|h|^2}(x)\,\mathrm{d}x. \end{aligned} \tag{43}$$

For any fading channel, PDF $f_{|h|^2}(x) \geq 0$ always hold. It is apparent that, as $x \geq 0, \eta \geq 0$ and $r^\alpha \geq 0$, the integration

$$\int_0^\infty \frac{x}{r^\alpha+\eta x} f_{|h|^2}(x)\,\mathrm{d}x \geq 0. \tag{44}$$

Then we have $\frac{\partial R_{s:r}}{\partial r} \leq 0$. Thus, the ergodic capacity $R_{s:r}$ is a monotonically decreasing function of r. ■

Appendix B
Proof of Theorem 3

Proof: To derive the distribution of the distance from the origin to the n_{th} node outside the secrecy protected zone, we first investigate the intensity function of the node at a distance $r(r > 0)$ from the origin. Then the CDF and PDF of the distance from the n_{th} node to the origin will be computed based on this intensity function.

As the nodes outside the secrecy protected zone are distributed as a PPP, according to the mapping theory, the intensity measure and intensity function can be separately expressed by

$$\Lambda_{opz} = \begin{cases} \pi\lambda(r^2-\rho^2) & \text{if } r > \rho, \\ 0 & \text{if } r \leq \rho, \end{cases} \tag{45}$$

and

$$\lambda_{opz}(r) = \begin{cases} 2\lambda\pi r & \text{if } r > \rho, \\ 0 & \text{if } r \leq \rho. \end{cases} \tag{46}$$

Since the locations of the nodes outside the secrecy protected zone can still be modeled by a PPP, the probability of k nodes located in the annual region $A_{\rho:r}$ with internal radius ρ and external radius r can be calculated by

$$\begin{aligned} &\mathbb{P}[N(A_{\rho:r}) = k] \\ &= \exp\left(-\int_{A_{\rho:r}} \lambda_{opz}(x)\mathrm{d}x\right)\frac{\left(\int_{A_{\rho:r}} \lambda_{opz}(x)\mathrm{d}x\right)^k}{k!}, \\ &= \exp\left[-\pi\lambda(r^2-\rho^2)\right]\frac{[\pi\lambda(r^2-\rho^2)]^k}{k!}. \end{aligned} \tag{47}$$

Consequently, the CDF of the distance $D_n(r)$ from the origin to the n_{th} nearest node can be computed by

$$\begin{aligned} D_n(r) &= 1-\mathbb{P}\left[N(A_{\rho:r}) < n\right], \\ &= 1-\exp\left[-\pi\lambda(r^2-\rho^2)\right]\sum_{k=0}^{n-1}\frac{[\pi\lambda(r^2-\rho^2)]^k}{k!}. \end{aligned} \tag{48}$$

By taking the derivation of (48), the PDF of the distance from the origin to the n_{th} node outside the secrecy protected zone with radius ρ can be obtained as (24). ■

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[2] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687 – 4698, October 2008.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[7] Y. Liang, H. Poor, and S. Shamai, "Secrecy capacity region of fading broadcast channels," *IEEE International Symposium on Information Theory (ISIT 2007)*, pp. 1291–1295, June 2007.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[9] ——, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, November 2010.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[11] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5500–5510, December 2008.

[12] P. Pinto, J. Barros, and M. Win, "Secure communication in stochastic wireless networks-part I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, February 2012.

[13] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000 – 3015, May 2012.

[14] S. Vuppala and G. Abreu, "Unicasting on the secrecy graph," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1469 – 1481, September 2013.

[15] P. Pinto, J. Barros, and M. Win, "Secure communication in stochastic wireless networks-part II: Maximum rate and collusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 139–147, February 2012.

[16] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, August 2011.

[17] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "Physical layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, May 2013.

[18] Y. Jeong, T. Quek, and H. Shin, "Stochastic wireless secure multicasting," *IEEE International Conference on Communications (ICC 2013)*, pp. 4718–4723, June 2013.

[19] G. Geraci, S. Singh, J. Andrews, J. Yuan, and I. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[20] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," *IEEE International Conference on Communications Workshops (ICC 2011)*, pp. 1–5, June 2011.

[21] S. Chae, W. Choi, J. Lee, and T. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, October 2014.

[22] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, October 2010.

[23] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, May 2013.

[24] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, September 2011.

[25] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 425–430, February 2011.

[26] Y. Li, M. Peng, A. Manzoor, and C. Wang, "Co-channel interference in two-tier heterogeneous networks: Analytical model and ergodic capacity," *Transactions on Emerging Telecommunications Technologies*, pp. n/a–n/a, 2014. [Online]. Available: http://dx.doi.org/10.1002/ett.2802

[27] L. Sun and S. Jin, "On the ergodic secrecy rate of multiple-antenna wiretap channels using artificial noise and finite-rate feedback," *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2011)*, pp. 1264–1268, September 2011.

[28] X. Zhou and M. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," *3rd International Conference on Signal Processing and Communication Systems (ICSPCS 2009)*, pp. 1–5, September 2009.

[29] M. Haenggi, *Stochastic Geometry for Wireless Networks [electronic resource]*. Cambridge: Cambridge University Press., 2012.

[30] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA: Academic, 2000.

[31] M. Haenggi, "On distances in uniformly random networks," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, October 2005.

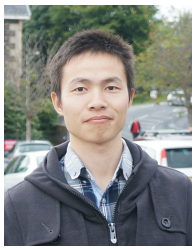
[32] L. Zhang, H.-C. Yang, and M. Hasna, "On ergodic capacity of wireless transmission subject to Poisson distributed interferers over Rayleigh fading channels," *IEEE 77th Vehicular Technology Conference (VTC Spring 2013)*, pp. 1–6, June 2013.

[33] C. han Lee and M. Haenggi, "Interference and outage in doubly Poisson cognitive networks," *Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN 2010)*, pp. 1–6, August 2010.

[34] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Communications Letters*, vol. 15, no. 8, pp. 792–794, August 2011.

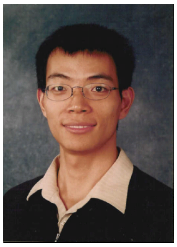
[35] C. han Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 4, pp. 1392–1401, April 2012.

[36] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations and Trends in Networking*, vol. 3, no. 2, pp. 127–248, November 2009.



Weigang Liu (S'12) received the B.Eng degree from Wuhan University of Technology, Wuhan, China, in 2008, and the M.Eng degree from Chongqing University, Chongqing, China, in 2011.

He is currently working toward the Ph.D degree at the Institute of Digital Communication (IDCOM), University of Edinburgh, Edinburgh, UK. His research interests include cooperative communication, convex optimization, stochastic geometry, and physical layer security in wireless communication.



Zhiguo Ding (S'03-M'05) received his B.Eng in Electrical Engineering from the Beijing University of Posts and Telecommunications in 2000, and the Ph.D degree in Electrical Engineering from Imperial College London in 2005. From Jul. 2005 to Aug. 2014, he was working in Queen's University Belfast, Imperial College and Newcastle University. Since Sept. 2014, he has been with Lancaster University as a Chair Professor.

Dr Ding' research interests are 5G networks, game theory, cooperative and energy harvesting networks and statistical signal processing. He is serving as an Editor for *IEEE Transactions on Communications*, *IEEE Transactions on Vehicular Networks*, *IEEE Wireless Communication Letters*, *IEEE Communication Letters*, and *Journal of Wireless Communications and Mobile Computing*. He received the best paper award in IET Comm. Conf. on Wireless, Mobile and Computing, 2009, IEEE Communication Letter Exemplary Reviewer 2012, and the EU Marie Curie Fellowship 2012-2014.

Tharmalingam Ratnarajah (A'96-M'05-SM'05) is currently with the Institute for Digital Communications, University of Edinburgh, Edinburgh, UK, as a Professor in Digital Communications and Signal Processing. His research interests include signal processing and information theoretic aspects of 5G wireless networks, full-duplex radio, mmWave communications, random matrices theory, interference alignment, statistical and array signal processing and quantum information theory. He has published over 260 publications in these areas and holds four U.S. patents. He is currently the coordinator of the FP7 projects HARP (3.2M€) in the area of highly distributed MIMO and ADEL (3.7M€) in the area of licensed shared access. Previously, he was the coordinator of FP7 Future and Emerging Technologies project CROWN (2.3M€) in the area of cognitive radio networks and HIATUS (2.7M€) in the area of interference alignment. Dr Ratnarajah is a Fellow of Higher Education Academy (FHEA), U.K., and an associate editor of the IEEE Transactions on Signal Processing.

Jiang Xue (S'09-M'13) received the B.S. degree in Information and Computing Science from the Xi'an Jiaotong University, Xi'an, China, in 2005, the M.S. degrees in Applied Mathematics from Lanzhou University, China and Uppsala University, Sweden, in 2008 and 2009, respectively. Dr. J. Xue reveived the Ph.D. degree in Electrical and Electronic Engineering from ECIT, the Queen's University of Belfast, U.K., in 2012. He is currently a Research Fellow with the University of Edinburgh, UK. His main interest lies in the performance analysis of general multiple antenna systems, Stochastic geometry, cooperative communications, and cognitive radio.