On the Secrecy of Interference-Limited Networks under Composite Fading Channels

Hirley Alves, *Student Member, IEEE*, Carlos H. M. de Lima, *Member, IEEE*, Pedro. H. J. Nardelli, *Member, IEEE*, Richard Demo Souza, *Senior Member, IEEE*, and Matti Latva-aho, *Senior Member, IEEE*

***Abstract*—This letter deals with the secrecy capacity of the radio channel in interference-limited regime. We assume that interferers are uniformly scattered over the network area according to a Point Poisson Process and the channel model consists of path-loss, log-normal shadowing and Nakagami-m fading. Both the probability of non-zero secrecy capacity and the secrecy outage probability are then derived in closed-form expressions using tools of stochastic geometry and higher-order statistics. Our numerical results show how the secrecy metrics are affected by the disposition of the desired receiver, the eavesdropper and the legitimate transmitter.**

***Index Terms*—Composite channel, secrecy capacity, secrecy outage probability, stochastic geometry.**

I. Introduction

DUE TO their broadcast nature, wireless communications are susceptible to security issues since non-intended nodes within the communication range of a given transmitter can overhear the transmission and possibly extract private information [3]. To ensure confidentiality, cryptographic techniques (usually implemented in higher layers) depend on secret keys and also rely on the limited computational power of eavesdroppers and on the reliability guaranteed by channel coding at the Physical Layer (PHY). However, future wireless systems tend to be deployed in large scale with ubiquitous coverage, dynamic operation and computational powerful devices, making encrypted communication through secret keys expensive and difficult to achieve. PHY security has reemerged [1]–[4] as a viable alternative to enhance the robustness and reduce the complexity of conventional cryptography systems since PHY offers unbreakable and quantifiable secrecy in confidential bps/Hz, regardless of the eavesdropper's computational power.

PHY security dates back to 1975, when Wyner in his pioneering work [5] introduced the wire-tap channel which is composed of a pair of legitimate users, known as Alice (transmitter) and Bob (receiver), communicating in the presence of an eavesdropper known as Eve. Alice and Bob communicate through the main channel in the presence of Eve, who perceives a degraded version of the message sent to Bob through the eavesdropper channel. In this context it is proved that there exist codes which guarantee both low error probabilities and a certain degree of confidentiality.

Later in [6], it was demonstrated that the secrecy capacity of the Gaussian wire-tap channel can be defined as the difference between the capacity of the main channel and the eavesdropper channel considering that the eavesdropper channel is noisier than the main channel. The wire-tap channel is extended to a fading scenario and secrecy outage probability is then characterized in [1], [2]. Cooperative and jamming techniques are reviewed in [4] and diversity schemes are assessed in [7].

Such recent works, however, focus on a small number of nodes, whose results provide few insights how PHY security performs in large-scale networks [2, Sec. VIII-C]. Different from the point-to-point communication wherein secrecy is guaranteed by keys or tokens, large-scale deployments impose new challenges to ensure secure communication, due to the complexity of distributing and maintaining secret keys [8].

Security in large-scale networks are also affected by the spatial distribution of the interferer nodes and eavesdroppers (for more details, refer to [2, Sec. VIII-C] and the references therein). Early contributions aim at characterizing the scaling laws of secrecy capacity [9] and the network connectivity [10] of randomly scattered nodes, or at computing the secure area spectral efficiency for predefined quality requirements. Recent papers have also shown that PHY-security can compensate for the vulnerability of wireless communications and reduce its implementation complexity by exploiting the spatial-temporal characteristics of the wireless medium [11].

In contrast, we characterize here the secrecy capacity of large-scale networks in the presence of uncoordinated interference by applying a general framework that jointly considers nodes spatial distribution and composite-fading channel, a model introduced in [12], [13]. Besides, as most of existing works consider thermal noise alone to compute the secrecy capacity, this letter also contributes to the literature by providing a framework that allows for evaluating the aggregate interference and hence computing the non-zero secrecy capacity and the secrecy outage probability in closed-form.

Built upon the analytic results from [12], [13], we assess the joint effects of transmitter-receiver and transmitter-eavesdropper relative distances and density interfering nodes on such capacity metrics. Considering a scenario where interferers

Manuscript received September 02, 2014; revised November 13, 2014; accepted January 28, 2015. Date of publication January 30, 2015; date of current version February 10, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yan Sun.

H. Alves, P. H. J. Nardelli, and M. Latva-aho are with the Centre for Wireless Communications (CWC), University of Oulu, Oulu, Finland (e-mail: halves@ee.oulu.fi; nardelli@ee.oulu.fi; matla@ee.oulu.fi).

C. H. M. de Lima is with the Centre for Wireless Communications (CWC), University of Oulu, Oulu, Finland, and also with the São Paulo State University (UNESP), São João da Boa Vista, Brazil (e-mail: carlos.lima@sjbv.unesp.br).

R. D. Souza and H. Alves are with Federal University of Technology - Paraná (UTFPR), Curitiba, Brazil (e-mail: richard@utfpr.edu.br).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2015.2398514

follow a Point Poisson Process and the channel model consists in path-loss, log-normal shadowing and Nakagami-m fading, we show under which circumstances non-zero secrecy capacity is possible and how the secrecy outage probability behaves in terms of such dynamics.

II. System Model

This section describes the system model used here, following the basic concepts introduced in [12, Sec. II]. To begin with, the tagged legitimate pair is defined as the reference link (transmitter-receiver) so as to compute the aggregate CCI and performance metrics for the scenario under consideration. Specifically the mutual information of the tagged legitimate pair and its related eavesdropper are determined based on their instantaneous Signal-to-Interference Ratio (SIR) values. We adopt the notion for secrecy capacity, probability of existence of non-zero secrecy capacity and secrecy outage probability as in [2, Sec. II].

We consider large-scale wireless networks where legitimate transmitters (interferer nodes) constitute a homogeneous Poisson Point Processs (PPPs) Φ with density $\lambda[\text{TXs/m}^2]$ in $\mathbb{R}^2$ [12], [13]. Transmitters communicate using antennas with omni-directional radiation pattern and fixed transmit power.

Let us now consider the set of legitimate transmitters in an arbitrary region $\mathcal{R}$ of area A which thus follows a Poisson distribution with parameter λA. We then assume the (composite) fading effect as a random mark associated with each point of Φ. Using Marking theorem, the resulting process $\widetilde{\Phi} = \{(\varphi, x); \varphi \in \Phi\}$ corresponds to a Marked Point Process (MPP) on the product space $\mathbb{R}^2 \times \mathbb{R}^+$, whose points (transmitter locations) φ belong to the process Φ and the random variable x refers to the corresponding squared-envelop of the composite fading, as presented later.

The scenarios under study are interference-limited and hence the thermal noise is negligible in comparison to the resulting Co-Channel Interference (CCI) [12], [13]. We recall that as pointed out by [14] the aggregate interference dominates over AWGN noise and the distribution of the aggregate interference is positively skewed and heavy tailed, which suggests a Log-Normal distribution [14]. We assume the high mobility random walk model, so each observation period can be analyzed as an independent realization of the MPP [15]. Thus, fading and shadowing are modeled as independent random variables which are also independent from any specific spatial realization of the MPP.

Fig. 1 depicts the network model in a 2D grid. Notice that the legitimate pair–the tagged transmitter and receiver–is represented in black (star and square, respectively) and are separated by a distance of d_l. The field of interferers is denoted by red circles while the eavesdropper is represented by the blue diamond. We assume that the eavesdropper is at a known distance d_e from the tagged transmitter. Through the framework introduced in [12], [13], we are able to compute the aggregate interference seen by the receivers.

Radio links are subject to distance-dependent path-loss and shadowed fading, which is assumed to be independent over distinct network entities and positions. A signal strength decay function describes the average power attenuation (unbounded model) as $l(d_i) = d_i^{-\alpha}$, where α is the path loss exponent and d_i represents the distance between a transmitter-receiver pair with $i \in \{l, e\}$, which can be either a legitimate receiver or the eavesdropper. Each interferer then disrupts the communication of the tagged receiver with a component given by $pl(d)x$, where p represents the interferer's transmit power, d is the separation distance from an interferer to the tagged receiver or eavesdropper. From this assumption, we can compute an approximation to the distribution of the aggregate interference caused by all active transmitters, defined by the MPP, as presented in the next section.

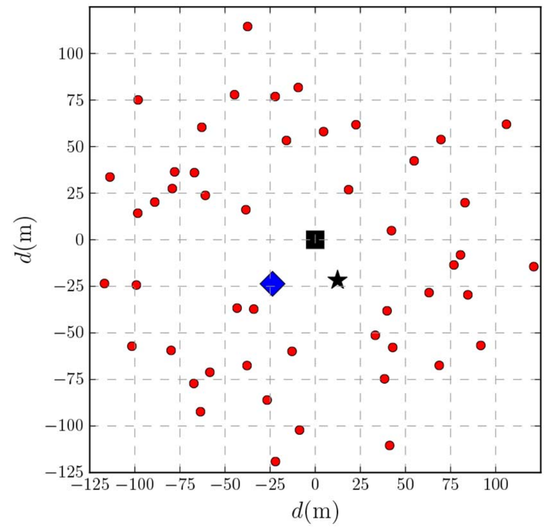

Fig. 1. Example of the network model. Legitimate pair is represented in black (square and star) and are separated by a distance d_l, while Eve is depicted in blue (diamond) and at distance d_e from the tagged transmitter. Note that the interferers are in red (circles) and that the aggregate power of the interferers disrupt the communication of the tagged receiver and the eavesdropper.

The received squared-envelop due to multipath fading and shadowing is represented by a Random Variable (RV) $X \in \mathbb{R}^+$ with Cumulative Distribution Function (CDF), $F_X(x)$, and Probability Distribution Function (PDF), $f_X(x)$. Then, the composite distribution of the received squared-envelop due to Log-Normal (LN) shadowing and Nakagami-m fading has a Gamma-LN distribution, whose PDF is given as [12], [13]:

$$f_X(x) = \int_0^\infty \left(\frac{m}{\omega}\right)^m \frac{x^{m-1}}{\Gamma(m)} \exp\left(-\frac{m}{\omega}x\right) \times \frac{\xi}{\sqrt{2\pi}\sigma\omega} \exp\left[-\frac{\left(\xi \ln \omega - \mu_{\Omega_p}\right)^2}{2\sigma_{\Omega_p}^2}\right] d\omega. \quad (1)$$

In this case, m is the shape parameter of the Gamma (Nakagami-m) distribution, $\Gamma(\cdot)$ is the gamma function [17, Eq. 8.310-1], $\xi = \ln(10)/10$, Ω_p is the mean squared-envelop, μ_{Ω_p} and σ_{Ω_p} is the mean and standard deviation of Ω_p, respectively.

Moreover, Ho and Stüber show in [16] that a composite Gamma–LN distribution can be approximated by a single LN distribution with mean and variance (in logarithmic scale) given by $\mu_{\text{dB}} = \xi[\psi(m) - \ln(m)] + \mu_{\Omega_p}$ and $\sigma_{\text{dB}}^2 = \xi^2\zeta(2, m) + \sigma_{\Omega_p}^2$, where $\psi(m)$ is the Euler psi function [17, Eq. 8.360-1] and $\zeta(2, m)$ is the generalized Riemann zeta function [17, Eq. 9.551].

III. Secrecy Capacity Analysis

The cumulant-based framework from [12, Secs. II, IV and VII] and [13, Sec. VI] is now used to asses achievable levels of secrecy and the resulting performance of legitimate link.

Suppose that the legitimate transmitter has only CSI of the desired receiver, which is known as passive eavesdropping [3], [7]. In such case, we resort to a probabilistic view of security in order to characterize the probability of information leakage to the eavesdropper. Then, in order to protect the transmission from an inimical attack, we consider the use of a wiretap code with 2^{nR} codewords, where R is made equal to the instantaneous capacity of the legitimate channel, namely C_l [1]. Then, the number of codewords per bin is set equal to 2^{nR_e}, where R_e represents the eavesdropper's equivocation rate. Thus, a fixed secure transmission rate is attained as $R_s = R - R_e = C_l - R_e$, which implies that $R_e = C_l - R_s$ varies according to the legitimate channel condition. Therefore, as introduced in [1], an outage event occurs when R_s exceeds the difference between the instantaneous capacities of the legitimate and the eavesdropper channels, thus $\Pr[[C_l - C_e]^+ < R_s]$, with $[\cdot]^+ \triangleq \max\{\cdot, 0\}$.

Let us first characterize the probability of existence of non-zero secrecy capacity ($\Pr[C_l > C_e]$) when the legitimate link experiences interference from concurrent transmissions. We use Γ_l and Γ_e to denote the SIR of the legitimate and eavesdropper links, respectively. Then, the following expression shows the secrecy capacity of shadowed fading channels

$$C_s = [C_l - C_e]^+ = [\log(1+\Gamma_l) - \log(1+\Gamma_e)]^+, \quad (2)$$

The distributions of Γ_l and Γ_e can be recovered using [13, Th. 1].

Theorem 1: For the system model described in this letter and the distances d_l (from the receiver) and d_e (from the eavesdropper) to the tagged legitimate transmitter, the probability of existence of non-zero secrecy capacity is

$$\Pr[C_s > 0] = \mathrm{Q}\left[\frac{\mu_e - \mu_l}{\sqrt{\sigma_l^2 + \sigma_e^2}}\right] \quad (3)$$

Proof: The non-zero secrecy capacity probability is

$$\Pr[C_s > 0] = \Pr[\Gamma_l > \Gamma_e] = \int_0^\infty \int_0^{\gamma_l} f_l(\gamma_l)\, f_e(\gamma_e)\, \mathrm{d}\gamma_e \mathrm{d}\gamma_l, \quad (4)$$

where C_s is defined in (2), the SIR PDFs $f_l(\gamma_l)$ and $f_e(\gamma_e)$ of the legitimate and eavesdropper nodes follow $\texttt{Lognormal}(\mu_l, \sigma_l^2)$ and $\texttt{Lognormal}(\mu_e, \sigma_e^2)$. Integrating in terms of γ_e, we have

$$\Pr[\Gamma_l > \Gamma_e] = \int_0^\infty \frac{1}{2}\mathrm{Erfc}\left[\frac{\mu_e - \log(\gamma_e)}{\sqrt{2}\sigma_e}\right] f_l(\gamma_l)\, \mathrm{d}\gamma_l. \quad (5)$$

Thereafter, we substitute $\eta = (\mu_e - \log\gamma_e)/\sqrt{2}\sigma_e$ in (5) and adjust the limits of integration accordingly to obtain

$$\Pr[\Gamma_l > \Gamma_e] = \int_{-\infty}^{\infty} \frac{e^{-\eta^2}}{2\sqrt{\pi}} \mathrm{Erf}\left[\frac{-\mu_l + \mu_e + \sqrt{2}\alpha\sigma_l}{\sqrt{2}\sigma_e}\right] \mathrm{d}\eta. \quad (6)$$

Eq. (3) is obtained from (6) by using [17, Eq. 8.259-1]. ■

We now need to identify the circumstances whereby secrecy is compromised by defining the secrecy outage probability.

Definition 1: **Secrecy Outage Probability** is defined as the probability that the instantaneous secrecy capacity C_s does not match the target secrecy rate $R_s > 0$ and is expressed as [2]:

$$\Pr[C_s < R_s] = \Pr[C_s < R_s | \Gamma_l > \Gamma_e] \Pr[\Gamma_l > \Gamma_e] + \Pr[C_s < R_s | \Gamma_l \le \Gamma_e] \Pr[\Gamma_l \le \Gamma_e]. \quad (7)$$

Theorem 2: For the system model described in this letter, the secrecy outage probability with respect to the legitimate link and an arbitrary eavesdropper is given by

$$\Pr[C_s < R_s] = \frac{1}{2} - \sum_{n=1}^{N} \frac{\omega_n}{2\sqrt{\pi}} \times \mathrm{Erf}\left[\frac{\mu_l - \log\left[-1 + 2^{R_s} + 2^{R_s}\exp\left(\mu_e - \sqrt{2}\eta_n\sigma_e\right)\right]}{\sqrt{2}\sigma_l}\right]. \quad (8)$$

Proof: Let us start evaluating each summand in (7) separately. Recall from Theorem 1 that $\Pr[\Gamma_l > \Gamma_e] = Q[(\mu_e - \mu_l)/\sqrt{\sigma_l^2 + \sigma_e^2}]$ and since $R_s > 0$, it follows that $\Pr[C_s < R_s | \Gamma_l \le \Gamma_e] = 1$.

Then, we rewrite the secrecy capacity in terms of its SIR distribution and then proceed as

$$\begin{aligned}\Pr[C_s < R_s | \Gamma_l > \Gamma_e] &= \Pr[\log_2(1+\Gamma_l) - \log_2(1+\Gamma_e) < R_s | \Gamma_l > \Gamma_e] \\ &= \Pr\left[\Gamma_l < 2^{R_s}(1+\Gamma_e) - 1 | \Gamma_l > \Gamma_e\right]. \end{aligned} \quad (9)$$

Under the assumption that legitimate and eavesdropper channels are independent, one computes (9) as follows.

$$\Pr[C_s < R_s | \Gamma_l > \Gamma_e] = \frac{1}{\Pr[\Gamma_l > \Gamma_e]} \int_0^\infty \int_0^{\epsilon(1+\gamma_e)-1} f_l(\gamma_l)\, f_e(\gamma_e)\, \mathrm{d}\gamma_l \mathrm{d}\gamma_e, \quad (10)$$

where $\epsilon = 2^{R_s}$. After integrating over γ_l, we attain

$$\Pr[C_s < R_s | \Gamma_l > \Gamma_e] = \frac{1}{\Pr[\Gamma_l > \Gamma_e]}(\Xi_1 - \Xi_2). \quad (11)$$

Employing the same method used in the previous proof [17, Eq. 8.259-1], we have (12), shown at the bottom of the page,

$$\Xi_1 = \int_0^\infty f_e(\gamma_e)\, \mathrm{Erf}\left[\frac{\mu_l - \log\gamma_e}{\sqrt{2}\sigma_l}\right] \mathrm{d}\gamma_e = \mathrm{Q}\left[\frac{\mu_l - \mu_e}{\sqrt{\sigma_l^2 - \sigma_e^2}}\right], \quad (12)$$

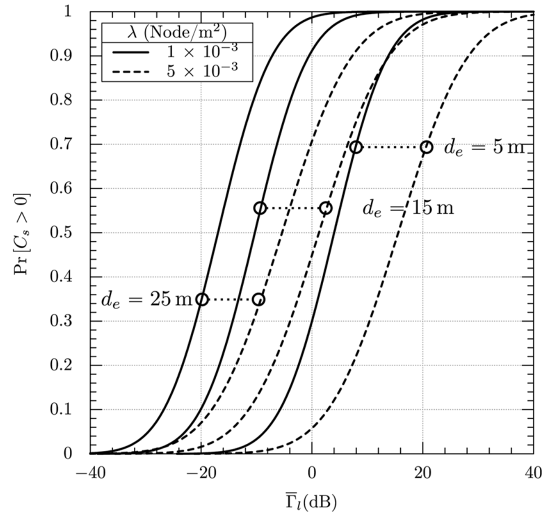

Fig. 2. Probability of existence of non-zero secrecy capacity as a function of the perceived SIR at the legitimate receiver for different distance between legitimate transmitter and eavesdropper d_e, and density of interfering nodes λ, considering $d_l = 15$ m.

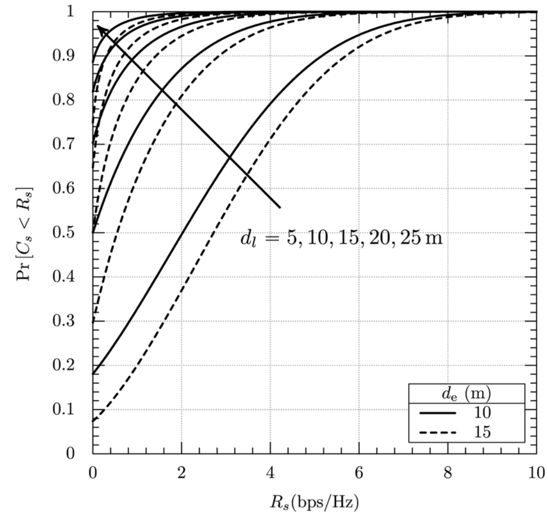

Fig. 3. Secrecy outage probability as a function of the secrecy rate for $d_l = 5, 10, 15, 20, 25$ m, while the eavesdropper is positioned $d_e = 10$ m and $d_e = 15$ m away from the transmitter.

where the second term is integrated using Gauss-Hermite quadrature [18] and $\eta = (\mu_e - \log \gamma_e)/\sqrt{2}\sigma_e$, so that

$$\Xi_2 = \int_0^\infty f_e(\gamma_e)\, \mathrm{Erf}\left[\frac{\mu_l - \log(-1 + \epsilon + \epsilon\gamma_e)}{\sqrt{2}\sigma_l}\right] \mathrm{d}\gamma_e = \sum_{n=1}^{N} \frac{\omega_n}{2\sqrt{\pi}} \mathrm{Erf}\left[\frac{\mu_l - \log[-1 + \epsilon + \epsilon\zeta]}{\sqrt{2}\sigma_l}\right], \qquad (13)$$

where $\zeta = \exp(\mu_e - \sqrt{2}\eta_n\sigma_e)$. Inserting (3), (12) and (13) into (11), yields the secrecy outage probability as in (8). ■

IV. Numerical Results

In this section, we apply the framework to evaluate the feasibility of PHY security in terms of the existence of secrecy capacity and the outage secrecy probability. Eavesdropper and legitimate nodes are affected by shadowed fading with the LN shadowing following a zero-mean Gaussian distribution with variance $\sigma = 4$, Rician fading factor of $K = 14.8$ dB, and Hermite polynomial order of $N = 24$ to evaluate our performance metrics. We consider that active nodes operate at a fixed transmit power of 20 dBm.

Fig. 2 depicts the probability of existence of non-zero secrecy capacity of the legitimate tagged link by varying its average SIR, eavesdropper distance to the tagged transmitter and density of interfering nodes for $d_l = 15$ m. We observe that the probability of non-zero secrecy capacity increases when the average SIR of the legitimate receiver increases, whereas it decreases by positioning the eavesdropper close the legitimate transmitter, namely, $d_e = 5$ m away. In other words, the closer the eavesdropper is to the legitimate transmitter, the higher should be the link quality of the legitimate pair so as to guarantee its secrecy.

We can also see from Fig. 2 that the increase of the interferers' density decreases the non-zero secrecy capacity probability for the same average SIR, regardless of the distance d_e. This fact evinces that the increase of co-channel interference caused by increasing λ equally decreases the channel capacity for both legitimate and eavesdropper links and therefore the gap between the curves with different densities tends to be constant when the same distance d_e is set.

Fig. 3 shows the secrecy outage probability for increasing secrecy rate R_s, considering that the eavesdropper is at distance $d_e = 10$ and $d_e = 15$ m. Note that the distance between the legitimate pair varies with increments of 5 m. We can infer that secrecy outage probability worsens with the increase of the distance between the legitimate nodes and also with the proximity of the eavesdropper to the transmitter. However, higher secrecy rates can be achieved with shorter legitimate links once the transmitted signal is much stronger than the interference seen at the receivers.

V. Final Remarks and Conclusion

We investigated the secrecy capacity of the channel in large scale, interference-limited networks. Using a more general model that captures randomness due to interferers' position, shadowing and fast fading, we derive closed form expressions for the probability of non-zero secrecy capacity and secrecy outage probability. For the proposed scenario, our numerical results show under which conditions secrecy can be achieved for different network configurations, evincing the effects of the proximity of the eavesdroppers to the legitimate transmitter and the interferer density on the secrecy outage probability.

We plan to continue the investigation introduced in this letter in scenarios legitimate transmitters use random access protocols and links are subject to quality constraints. In this way, we plan to evaluate both the effective secrecy throughput and the network spatial secrecy throughput, as in [19]. Another extension is to assess the secrecy capacity of Poisson distributed networks where multi-hop links are allowed [20] such that the relative positions between relays (defined by some specific hopping strategy) and eavesdroppers are expect to impact the system performance.

Acknowledgment

The authors would like to thank Aka and Infotech Oulu Graduate School from Finland, and CNPq and Special Visiting Researcher fellowship CAPES 076/2012 from Brazil.

REFERENCES

[1] M. Bloch *et al.*, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[2] A. Mukherjee *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, 2014.

[3] Y.-S. Shiu *et al.*, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, 2011.

[4] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, 2013.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, 1975.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, 1978.

[7] H. Alves *et al.*, "Performance of transmit antenna selection PHY security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, 2012.

[8] E. D. Silva *et al.*, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, 2008.

[9] O. Koyluoglu, C. Koksal, and H. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, 2012.

[10] P. Pinto *et al.*, "Secure communication in stochastic wireless networks - part I: Connectivity," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, 2012.

[11] X. Zhou *et al.*, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, 2011.

[12] C. de Lima *et al.*, "Coordination mechanisms for self-organizing femtocells in two-tier coexistence scenarios," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, 2012.

[13] C. de Lima *et al.*, "Statistical analysis of self-organizing networks with biased cell association and interference avoidance," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 1950–1961, 2013.

[14] A. Ghasemi and E. S. Sousa, "Statistical analysis of self-organizing networks with biased cell association and interference avoidance," *IEEE J. Sel. Topics Signal Process.*, vol. 2, pp. 41–56, Feb. 2008.

[15] F. Baccelli and B. Blaszczyszyn, "Stochastic Geometry and Wireless Networks: Volume I Theory," *Found. Trends Netw.*, vol. 3, no. 3–4, 2010.

[16] M.-J. Ho and G. L. Stüber, "Capacity and power control for CDMA microcells," *ACM J. Wireless Netw.*, vol. 1, no. 3, pp. 355–363, 1995.

[17] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, A. Jeffrey and D. Zwillinger, Eds. New York, NY, USA: Academic, 2007.

[18] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Academic, 1965.

[19] P. H. J. Nardelli *et al.*, "Throughput optimization in wireless networks under stability and packet loss constraints," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, 2014.

[20] P. H. J. Nardelli *et al.*, "Efficiency of wireless networks under different hopping strategies," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, 2012.