A New Model for Physical Layer Security in Cellular Networks

Giovanni Geraci, Harpreet S. Dhillon, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings

***Abstract*—In this paper, we study physical layer security for the downlink of cellular networks. In a cellular network, the confidential messages transmitted to each mobile user can be eavesdropped by the other users in the same cell and also by the users in the other cells. We model the locations of base stations and mobile users as two independent two-dimensional Poisson point processes. By combining tools from stochastic geometry and random matrix theory, we analyze the secrecy rates achievable with regularized channel inversion (RCI) precoding under Rayleigh fading. Our analysis shows that unlike isolated cells, the secrecy rate in a cellular network does not grow monotonically with the transmit power. Moreover, we find that the network tends to be in secrecy outage if the transmit power grows unbounded. Furthermore, we show that there exists an optimal value for the base station deployment density that maximizes the secrecy rate.**

***Index Terms*—Physical layer security, cellular networks, stochastic geometry, linear precoding, random matrix theory.**

I. Introduction

Wireless multiuser communication is very susceptible to eavesdropping, and it is of critical importance to protect the transmitted information. The emergence of large-scale and dynamic networks imposes new challenges on classical security approaches such as network layer cryptography. Physical layer security was proposed as an alternative to achieve perfect secrecy without requiring key distribution/management and complex encryption/decryption algorithms [1].

The broadcast channel with confidential messages (BCC) was considered in [2]–[5]. In the BCC, physical layer security is applied to a multi-user scenario where users can act maliciously as eavesdroppers. The presence of external eavesdropping nodes and its effect on the secure connectivity in random wireless networks were studied, among others, in [6]–[9] via stochastic geometry tools. The broadcast channel with confidential messages and external eavesdroppers (BCCE) was then introduced in [10] to model a more general setting where both malicious users and randomly located external nodes can act as eavesdroppers. We note that, as discussed above, almost all the prior work on physical layer security for multiuser systems focused on either an isolated cell or an ad hoc network.

In this paper we study physical layer security in the downlink of cellular networks, where each BS simultaneously transmits confidential messages to several users, and where the confidential messages transmitted to each user can be eavesdropped by the other users in the same cell and by the users in other cells. We model the locations of BSs and mobile users as two independent two-dimensional Poisson point processes (PPPs). By combining results from stochastic geometry and random matrix theory, we characterize the mean secrecy rate achievable by RCI precoding under Rayleigh fading, and the probability of secrecy outage. We find that RCI can achieve a non-zero secrecy rate. However, unlike the case of an isolated cell, the secrecy rate in a cellular network does not grow monotonically with the transmit power, and the network tends to be in secrecy outage if the transmit power grows unbounded. We finally show that in a cellular network there is an optimal value for the density of BSs λ_b that maximizes the mean secrecy rate. The value of λ_b trades off useful signal power, interference, and information leakage.

We note that an attempt to study the secrecy rate in the downlink of a cellular network has been made in [11]. This paper differs from and generalizes [11] in the following aspects: (i) in [11], the authors consider single antenna transmission with orthogonal resource allocation, whereas we consider a more general model with multiple transmit antennas serving multiple users with RCI-based linear precoding, which may result in intra-cell interference, (ii) while [11] assumes that the interfering BSs are far away and that the inter-cell interference can be incorporated in the constant noise power, we account for the exact inter-cell interference at the typical user, and (iii) while [11] assumes that only certain nodes in the network can eavesdrop without cooperation, in this paper we assume that all the users other than the typical user, for which we compute the secrecy rate and outage, can cooperate to eavesdrop the transmitted message.

II. System Model

A. Network Topology

We consider the downlink of a cellular network, as depicted in Fig. 1. Each BS transmits at power P and is equipped with N antennas. The locations of the BSs are drawn from a homogeneous PPP of density λ_b, where the realized points are represented by Φ_B. We consider single-antenna users, and assume that each user is connected to the closest BS. The locations of the users are drawn from an independent PPP of density λ_u. where the realized points are represented by Φ_U. We approximate the number of users served by each BS

G. Geraci and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia (e-mail: g.geraci@student.unsw.edu.au, j.yuan@unsw.edu.au).

H. S. Dhillon is with the Communication Sciences Institute (CSI), The University of Southern California, Los Angeles, CA (email: hdhillon@usc.edu).

J. G. Andrews is with the Wireless Networking and Communications Group (WNCG), The University of Texas at Austin, TX (email: jandrews@ece.utexas.edu).

I. B. Collings is with the Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Sydney, Australia (email: iain.collings@csiro.au).

$$\xi = \frac{-2\rho^2 (1-\beta)^2 + 6\rho\beta + 2\beta^2 - 2\left[\beta(\rho+1) - \rho\right] \cdot \sqrt{\beta^2\left[\rho^2+\rho+1\right] - \beta\left[2\rho(\rho-1)\right] + \rho^2}}{6\rho^2(\beta+2) + 6\rho\beta} \tag{2}$$

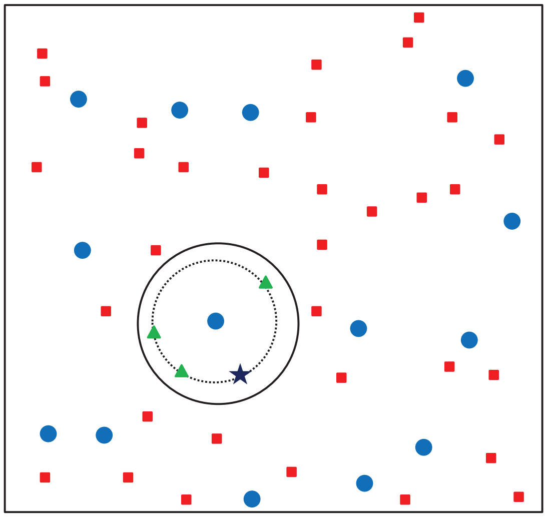

Fig. 1. Illustration of a cellular network. The circles, squares, and triangles denote BSs, out-of-cell users, and in-cell users, respectively. The star denotes a typical user as discussed in Subsection II-A.

by its average value $K = \frac{\lambda_u}{\lambda_b}$, given by the ratio between the density of users and the density of BSs. We denote by $\mathbf{H}_b = [\mathbf{h}_{b,1}, \ldots, \mathbf{h}_{b,K}]^\dagger$ the $K \times N$ channel matrix for the BS b, where $\mathbf{h}_{b,j} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the channel vector that accounts for the fading between the BS b and the j^{th} user served by b.

We consider a typical user o located at the origin, and served by the closest BS, located in $c \in \Phi_B$. The distance between the typical user and the closest BS is given by $\|c\|$. The cell where the typical user o is located is referred to as the *tagged cell*. We approximate the distance between the tagged BS c and each user c_j served by c with the distance between the BS c and the typical user o. Similarly to [12], we also approximate the Voronoi region of the tagged BS c with a ball centered at c and with radius $r = \frac{1}{\sqrt{\pi\lambda_b}}$, i.e., $\mathcal{B}(c, r) \triangleq \left\{p \in \mathbb{R}^2, \|p - c\| \leq r\right\}$, where the value of r is chosen to ensure that $\mathcal{B}(c, r)$ has the same area as the average cell.

Note that despite these assumptions, which are necessary to maintain tractability, our analysis captures all the key characteristics of the cellular networks that affect physical layer security, as discussed in the sequel. The simplified model also provides some fundamental insights into the dependence of key performance metrics, such as secrecy outage and mean secrecy rate, on the transmit power and BS deployment density. A more general model is discussed in the longer version of this paper [13].

B. RCI Precoding

Transmission takes place over a block fading channel, and the signal transmitted by the generic BS b is $\mathbf{x}_b = [x_{b,1}, \ldots, x_{b,N}]^T \in \mathbb{C}^{N \times 1}$. We consider RCI precoding because it is a linear scheme that allows low-complexity implementation [14]. Although suboptimal, RCI precoding is particularly interesting because it can control the amount of crosstalk between the users [15]. In RCI precoding, the transmitted vector $\mathbf{x}_b$ is obtained at the BS b by performing a linear processing on the vector of confidential messages $\mathbf{m}_b = [m_{b,1}, \ldots, m_{b,K}]^T$, whose entries are chosen independently, satisfying $\mathbb{E}[|m_{b,j}|^2] = 1$, for $j = 1, \ldots, K$. The transmitted signal $\mathbf{x}_b$ after RCI precoding can be written as $\mathbf{x}_b = \sqrt{P}\mathbf{W}_b\mathbf{m}_b$, where $\mathbf{W}_b = [\mathbf{w}_{b,1}, \ldots, \mathbf{w}_{b,K}]$ is the $N \times K$ RCI precoding matrix, given by [15]

$$\mathbf{W}_b = \frac{1}{\sqrt{\zeta_b}} \mathbf{H}_b^\dagger \left(\mathbf{H}_b\mathbf{H}_b^\dagger + N\xi\mathbf{I}_K\right)^{-1} \tag{1}$$

and $\zeta_b = \text{tr}\left\{\mathbf{H}_b^\dagger\mathbf{H}_b\left(\mathbf{H}_b^\dagger\mathbf{H}_b + N\xi\mathbf{I}_N\right)^{-2}\right\}$ is a long-term power normalization constant. The function of the regularization parameter $\xi \in \mathbb{R}$ is to achieve a tradeoff between the signal power at the legitimate user and the crosstalk at the other users served by the same BS. The optimal value for the parameter ξ in cellular networks is unknown, and we leave its calculation as a future work. Since the results obtained in this paper hold for any value of ξ, we will now assume that each BS sets ξ to the value that maximizes the large-system secrecy rate in an isolated cell, obtained in [5] and given by (2), where $\beta = K/N$ is the ratio between the number of users in the cell and the number of antennas at the BS.

III. Achievable Secrecy Rates

In this section, we derive a secrecy rate achievable by RCI precoding for the typical user in the downlink of a cellular network.

A. SINR at a Typical User

The typical user receives self-interference caused by the messages $m_{c,j}$ transmitted by the BS c to the other users $c_j \neq o$, and inter-cell interference caused by the signals transmitted by all the other BSs $b \in \Phi_B \backslash c$. The signal received by the typical user is given by

$$\begin{aligned} y_o = {} & \sqrt{P\,\|c\|^{-\eta}}\,\mathbf{h}_{c,o}^\dagger\mathbf{w}_{c,o}m_{c,o} \\ & + \sqrt{P\,\|c\|^{-\eta}} \sum_{c_j \neq o} \mathbf{h}_{c,o}^\dagger\mathbf{w}_{c,j}m_{c,j} \\ & + \sum_{b \in \Phi_B \backslash c} \sqrt{P\,\|b\|^{-\eta}} \sum_j \mathbf{h}_{b,o}^\dagger\mathbf{w}_{b,j}m_{b,j} + n_o \end{aligned} \tag{3}$$

where $\mathbf{h}_{c,o}$ (resp. $\mathbf{h}_{b,o}$) is the channel vectors between the BS c (resp. b) and the typical user, $\mathbf{w}_{c,o}$ is the precoding vector for the typical user, $\|b\|$ is the distance between the typical user and the generic BS b, and $\eta > 2$ is the path loss exponent. The four terms in (3) represent the useful signal, the crosstalk (or self-interference), the inter-cell interference, and the thermal noise seen at the typical user, respectively. The latter is given by $n_o \sim \mathcal{CN}(0, \sigma^2)$, and we define the SNR as $\rho \triangleq P/\sigma^2$.

We assume that the legitimate receiver at o treats the interference power as noise. The SINR γ_o at the legitimate receiver o is given by

$$\gamma_o = \frac{\rho\|c\|^{-\eta}\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,o}\right|^2}{\rho\|c\|^{-\eta}\sum_{c_j\neq o}\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,j}\right|^2 + \frac{\rho}{K}\sum_{b\in\Phi_B\setminus c} g_{b,o}\|b\|^{-\eta} + 1}, \tag{4}$$

where $g_{b,o} \triangleq \sum_{j=1}^{K}\left|\mathbf{h}_{b,o}^{\dagger}\tilde{\mathbf{w}}_{b,j}\right|^2$ and $\tilde{\mathbf{w}}_{b,j} \triangleq \sqrt{K}\mathbf{w}_{b,j}$.

B. SINR at the Malicious Users

In general, the BSs cannot determine the behavior of the users, i.e., whether they act maliciously as eavesdroppers or not. As a worst-case scenario, we assume that for each legitimate user, all the remaining users in the network can act as eavesdroppers. For a user o served by the BS c, there are $K-1$ intra-cell malicious users c_j located at distance $\|c\|$ from c. Moreover, there is a set of external malicious users given by $\Phi_U \cap \bar{\mathcal{B}}(c,r)$, with $\bar{\mathcal{B}}$ denoting the complement of the set $\mathcal{B}$. In Fig. 1, the legitimate user o, the set of intra-cell malicious users, and the set of external malicious users are represented by star, triangles, and squares, respectively. It is important to make such a distinction between the intra-cell malicious users and the external malicious users. In fact, the BS c knows the channels of the intra-cell malicious users, and exploits this information by choosing an RCI precoding matrix $\mathbf{W}_c$ which is a function of these channels. The RCI precoding thus controls the amount of information leakage at the malicious users. On the other hand, the BS c does not know the channels of all the other external malicious users, and $\mathbf{W}_c$ does not depend upon these channels. Therefore, the signal received by the inter-cell malicious users is not directly affected by RCI precoding.

In the following we will consider the worst-case scenario where all the malicious users can cooperate to eavesdrop on the message intended for the typical user in o. Since each malicious user is likely to decode its own message, it can cooperate with all the other malicious users and pass this information to them. In the worst-case scenario, all the malicious users can therefore subtract the interference generated by all the messages $m_{c,j}$, $c_j \neq o$.

After interference cancellation, the signal received at a malicious user c_j in the tagged cell is given by

$$y_j = \sqrt{P\,\|c\|^{-\eta}}\,\mathbf{h}_{c,j}^{\dagger}\mathbf{w}_{c,o}m_{c,o} + n_j, \tag{5}$$

whereas the signal received at a malicious user e outside the tagged cell is given by

$$y_e = \sqrt{P\,\|e-c\|^{-\eta}}\,\mathbf{h}_{c,e}^{\dagger}\mathbf{w}_{c,o}m_{c,o} + n_e, \tag{6}$$

with $n_j, n_e \sim \mathcal{CN}(0,\sigma^2)$, and where $\mathbf{h}_{c,e}$ is the channel between the BS c and the malicious user e. We denote by γ_j and γ_e the SINRs at the malicious users c_j and e, respectively.

Due to the cooperation among all malicious users, they can be seen as a single equivalent multi-antenna malicious user, denoted by M_o. After interference cancellation, M_o sees the useful signal embedded in noise, therefore applying maximal ratio combining is optimal, and it yields to an SINR given by

$$\begin{aligned}\gamma_{M_o} &= \sum_{c_j\neq o}\gamma_j + \sum_{e\in\Phi_U\cap\bar{\mathcal{B}}(c,r)}\gamma_e\\ &= \rho\sum_{c_j\neq o}\|c\|^{-\eta}\left|\mathbf{h}_{c,j}^{\dagger}\mathbf{w}_{c,o}\right|^2 + \frac{\rho}{K}\sum_{e\in\Phi_U\cap\bar{\mathcal{B}}(c,r)} g_{c,e}\|e-c\|^{-\eta},\end{aligned} \tag{7}$$

where $g_{c,e} \triangleq \left|\mathbf{h}_{c,e}^{\dagger}\tilde{\mathbf{w}}_{c,o}\right|^2$ and $\tilde{\mathbf{w}}_{c,o} \triangleq \sqrt{K}\mathbf{w}_{c,o}$.

C. Achievable Secrecy Rates

We are now able to obtain an expression for the secrecy rate achievable by RCI precoding for the typical user of a downlink cellular network.

Lemma 1. *A secrecy rate achievable by RCI precoding for the typical user o is given by*

$$\begin{aligned}R = \Bigg\{&\log_2\left(1 + \frac{\rho\|c\|^{-\eta}\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,o}\right|^2}{\rho\|c\|^{-\eta}\sum_{c_j\neq o}\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,j}\right|^2 + \rho I + 1}\right)\\ &-\log_2\left(1 + \rho\|c\|^{-\eta}\sum_{c_j\neq o}\left|\mathbf{h}_{c,j}^{\dagger}\mathbf{w}_{c,o}\right|^2 + \rho L\right)\Bigg\}^{+},\end{aligned} \tag{8}$$

where we use the notation $\{x\}^{+} \triangleq \max(x,0)$*, and where* I *and* L *are the interference and leakage term, given by*

$$I = \frac{1}{K}\sum_{b\in\Phi_B\setminus c} g_{b,o}\|b\|^{-\eta},\;\; L = \frac{1}{K}\sum_{e\in\Phi_U\cap\bar{\mathcal{B}}(c,r)} g_{c,e}\|e-c\|^{-\eta}. \tag{9}$$

Proof: The BS c, the user o, and the equivalent malicious user M_o form an equivalent multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [16]. As a result, an achievable secrecy rate is given by [5]

$$R = \left\{\log_2\left(1+\gamma_o\right) - \log_2\left(1+\gamma_{M_o}\right)\right\}^{+}. \tag{10}$$

Substituting (4) and (7) in (10) yields (8). ∎

For RCI precoding we have that (i) the inter-cell interference power gain at the typical legitimate user o is distributed as $g_{b,o} \sim \Gamma(K,1)$, and (ii) the leakage power gain at the malicious user e is distributed as $g_{c,e} \sim \exp(1)$ [17].

IV. Large-system analysis

In this section, we derive approximations for (i) the secrecy outage probability, i.e., the probability that the secrecy rate R achievable by RCI precoding for the typical user o is zero, and (ii) the mean secrecy rate achievable by RCI precoding in the downlink of a cellular network.

A. Characterization of Useful Signal and Intra-cell Crosstalk

We now carry out a large-system analysis by assuming that both (i) the average number of users K in each cell, and (ii) the number of transmit antennas N at each BS grow to infinity in a fixed ratio $\beta \triangleq \frac{K}{N}$. We can thus approximate the useful signal, the intra-cell interference, and the intra-cell leakage in

(8) by their respective large-system deterministic equivalents [18], [19]

$$\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,o}\right|^2 \approx \alpha, \ \sum_{c_j \neq o}\left|\mathbf{h}_{c,o}^{\dagger}\mathbf{w}_{c,j}\right|^2 \approx \sum_{c_j \neq o}\left|\mathbf{h}_{c,j}^{\dagger}\mathbf{w}_{c,o}\right|^2 \approx \chi, \tag{11}$$

where

$$\alpha = g\left(\beta,\xi\right)\left(\chi + \frac{\xi}{\beta}\right), \quad \chi = \frac{1}{\left[1+g\left(\beta,\xi\right)\right]^2}, \tag{12}$$

and

$$g\left(\beta,\xi\right) = \frac{1}{2}\left[\sqrt{\frac{\left(1-\beta\right)^2}{\xi^2} + \frac{2\left(1+\beta\right)}{\xi} + 1} + \frac{1-\beta}{\xi} - 1\right], \tag{13}$$

and where it follows from (2) that

$$\lim_{\rho\to\infty} \chi = 0, \quad \text{for } \beta \leq 1. \tag{14}$$

An approximated secrecy rate is therefore given by $R \approx \tilde{R}$, where

$$\tilde{R} = \left\{\log_2 \frac{1 + \frac{\rho\alpha\|c\|^{-\eta}}{\rho\chi\|c\|^{-\eta}+\rho I+1}}{1+\rho\,\chi\|c\|^{-\eta}+\rho L}\right\}^{+}. \tag{15}$$

B. Characterization of Inter-cell Crosstalk

We denote by f_I and f_L the pdfs of the inter-cell interference I and leakage L, respectively. Obtaining the exact pdfs f_I and f_L is an open problem. We now propose simple approximations for the pdfs f_I and f_L which will be useful in the rest of the paper.

The mean and the variance of I and L are given by [20]

$$\mu_I = \frac{2\pi\lambda_b\|c\|^{-(\eta-2)}}{\eta-2}, \quad \sigma_I^2 = \frac{\pi\lambda_b\left(K+K^2\right)\|c\|^{-2(\eta-1)}}{K^2\left(\eta-1\right)}, \tag{16}$$

$$\mu_L = \frac{2\pi\lambda_u r^{-(\eta-2)}}{K(\eta-2)}, \quad \sigma_L^2 = \frac{2\pi\lambda_u r^{-2(\eta-1)}}{K^2\left(\eta-1\right)}. \tag{17}$$

We can then approximate the probability density functions (pdfs) of I and L by lognormal distributions with the same respective mean and variance, as follows.

In Fig. 2 we compare the simulated cumulative distribution functions (CDFs) of I and L to the proposed lognormal approximations. The CDFs are plotted for an SNR $\rho = 10$dB, $N = 20$ transmit antennas, an average of $K = 20$ users per BS, $\|c\| = r$, $\eta = 4$, and three values of the density of BS λ_b. Figure 2 shows that the proposed lognormal approximations are accurate for all values of λ_b.

C. Probability of Secrecy Outage

We now obtain an approximation for the probability of secrecy outage with RCI precoding.

Theorem 1. *The probability of secrecy outage with RCI precoding can be approximated as $\mathcal{P}_o \approx \tilde{\mathcal{P}}_o$, where*

$$\tilde{\mathcal{P}}_o \triangleq \mathbb{P}(\tilde{R} \leq 0) = \int_0^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathbb{1}_{(z\geq\tau(x,y))}\, f_L(z)\,\mathrm{d}z \cdot f_I(x,y)\,\mathrm{d}x 2\lambda_b\pi y e^{-\lambda_b\pi y^2}\,\mathrm{d}y, \tag{18}$$

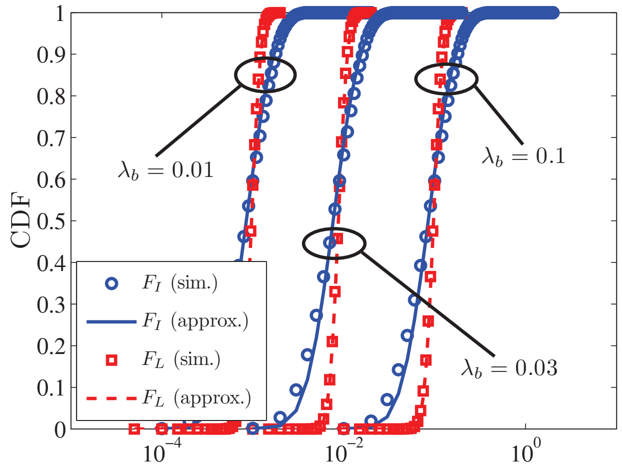

Fig. 2. Comparison between the simulated CDFs of I and L and the proposed lognormal approximations, for an SNR $\rho = 10$dB, $N = 20$ transmit antennas, $K = 20$ users per BS, $\|c\| = r$, and $\eta = 4$.

where $f_I(x,y)$ is the pdf of the interference I for $\|c\| = y$, $f_L(z)$ is the pdf of the leakage L, and where we have defined

$$\tau(x,y) \triangleq \frac{\alpha y^{-\eta}}{\rho\chi y^{-\eta}+\rho x+1} - \chi y^{-\eta}. \tag{19}$$

Proof: The approximated probability of secrecy outage is given by

$$\begin{aligned}\tilde{\mathcal{P}}_o &\triangleq \mathbb{P}(\tilde{R} \leq 0) = \mathbb{P}\left(\rho\,\chi\|c\|^{-\eta} + \rho L \geq \frac{\alpha\|c\|^{-\eta}}{\chi\|c\|^{-\eta}+I+\frac{1}{\rho}}\right) \\ &\overset{(a)}{=} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathbb{P}\left(L \geq \tau(x,y)\right) f_I(x,y\,|\,\|c\|{=}y)\, f_{\|c\|}(y)\mathrm{d}x\mathrm{d}y \\ &= \int_0^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathbb{1}_{(z\geq\tau(x,y))}\, f_L(z)\,\mathrm{d}z\, f_I(x,y)\,\mathrm{d}x \\ &\quad \cdot 2\lambda_b\pi y e^{-\lambda_b\pi y^2}\,\mathrm{d}y,\end{aligned} \tag{20}$$

where (a) holds by defining $\tau(x,y)$ as in (19), and by noting that the distance $\|c\|$ has Rayleigh distribution [21]. ■

The probability of secrecy outage in Theorem 1 also denotes the fraction of time for which a BS cannot transmit to a typical user at a non-zero secrecy rate. The result provided in Theorem 1 allows to evaluate the probability of secrecy outage without the need for Monte-Carlo simulations. Moreover, Theorem 1 yields to the following asymptotic result without the need to solve the integral. In an isolated cell, a sufficient number of transmit antennas allows the BS to cancel the intra-cell interference and leakage, and to drive the probability of secrecy outage to zero [10]. In a cellular network, the secrecy outage is also caused by the inter-cell interference and leakage, which cannot be controlled by the BS. It is easy to show that $\lim_{\rho\to\infty} \tau(x,y) \leq 0$, which from Theorem 1 implies $\lim_{\rho\to\infty} \tilde{\mathcal{P}}_o = 1$. We therefore have the following observation.

Remark 1. *In cellular networks, RCI precoding can achieve confidential communication with probability of secrecy outage*

$\tilde{\mathcal{P}}_o < 1$. *However unlike an isolated cell, cellular networks tend to be in secrecy outage w.p.* 1 *if the transmit power grows unbounded, irrespective of the number of transmit antennas.*

D. Mean Secrecy Rate

In the following, we derive an approximation for the mean secrecy rate achievable by RCI precoding.

Theorem 2. *The mean secrecy rate achievable by RCI precoding can be approximated as* $R_m \approx \tilde{R}_m$, *where*

$$\tilde{R}_m \triangleq \mathbb{E}\left[\tilde{R}\right] = \int_0^\infty \int_{-\infty}^{\frac{\alpha}{\rho\chi}-\frac{1}{\rho}-\chi y^{-\eta}} \Bigg\{ \log_2\left(1+\frac{\rho\alpha y^{-\eta}}{\rho\chi y^{-\eta}+\rho x+1}\right) \cdot \int_{-\infty}^{\tau(x,y)} f_L(z) - \int_{-\infty}^{\tau(x,y)} \log_2\left(1+\rho\chi y^{-\eta}+\rho z\right) \cdot f_L(z)\,\mathrm{d}z \Big\}\, f_I(x,y)\,\mathrm{d}x\, 2\lambda_b\pi y e^{-\lambda_b\pi y^2}\,\mathrm{d}y. \tag{21}$$

Proof: The approximated mean secrecy rate is given by

$$\tilde{R}_m \triangleq \mathbb{E}\left[\tilde{R}\right] = \mathbb{E}\Bigg[\Bigg[\log_2\left(1+\frac{\rho\alpha\|c\|^{-\eta}}{\rho\chi\|c\|^{-\eta}+\rho I+1}\right) - \log_2\left(1+\rho\chi\|c\|^{-\eta}+\rho L\right)\Bigg]\mathbb{1}_{(L<\tau(I,\|c\|))}\Bigg]$$
$$\overset{(a)}{=} \int_0^\infty \int_{-\infty}^{\frac{\alpha}{\rho\chi}-\frac{1}{\rho}-\chi y^{-\eta}} \Bigg\{ \log_2\left(1+\frac{\rho\alpha y^{-\eta}}{\rho\chi y^{-\eta}+\rho x+1}\right) \cdot \int_{-\infty}^{\tau(x,y)} f_L(z) - \int_{-\infty}^{\tau(x,y)} \log_2\left(1+\rho\chi y^{-\eta}+\rho z\right) \cdot f_L(z)\,\mathrm{d}z \Big\}\; f_I(x,y)\,\mathrm{d}x\, 2\lambda_b\pi y e^{-\lambda_b\pi y^2}\,\mathrm{d}y, \tag{22}$$

where (a) follows from $0 \leq L < \tau(I,\|c\|)$. ■

The result provided in Theorem 2 allows to evaluate the mean secrecy rate without the need for computationally expensive Monte-Carlo simulations. Moreover, a simple study of the integral in Theorem 2 yields to the following asymptotic result. In an isolated cell, a sufficient number of transmit antennas allows the BS to cancel the intra-cell interference and leakage, and the secrecy rate increases monotonically with the SNR [5]. In a cellular network, the secrecy rate is also affected by the inter-cell interference and leakage, which cannot be controlled by the BS. It is easy to show that $\lim_{\rho\to\infty} \frac{\alpha}{\rho\chi} - \frac{1}{\rho} - \chi y^{-\eta} \leq 0$, which from Theorem 2 implies $\lim_{\rho\to\infty} \tilde{R}_m = 0$. We therefore have the following observation.

Remark 2. *In cellular networks, RCI precoding can achieve a non-zero secrecy rate* $\tilde{R}_m$. *However unlike an isolated cell, the secrecy rate in a cellular network is interference-and-leakage-limited, and it cannot grow unbounded with the SNR, irrespective of the number of transmit antennas.*

Theorem 2 shows that an optimal value for the BS deployment density λ_b should be found as a tradeoff between (i) increasing the useful power $\alpha y^{-\eta}$, and (ii) reducing the intra-cell interference $\chi y^{-\eta}$ and leakage $\chi y^{-\eta}$, and the inter-cell interference x and leakage z. We know from (14) that χ vanishes at high SNR, thus the terms x and z become dominant in (21). For a given cell load $K = \frac{\lambda_u}{\lambda_b}$, the terms x and z are minimized by small densities λ_b and λ_u, because fewer BSs generate smaller inter-cell interference x, and fewer users receive smaller inter-cell leakage z. We therefore have the following result.

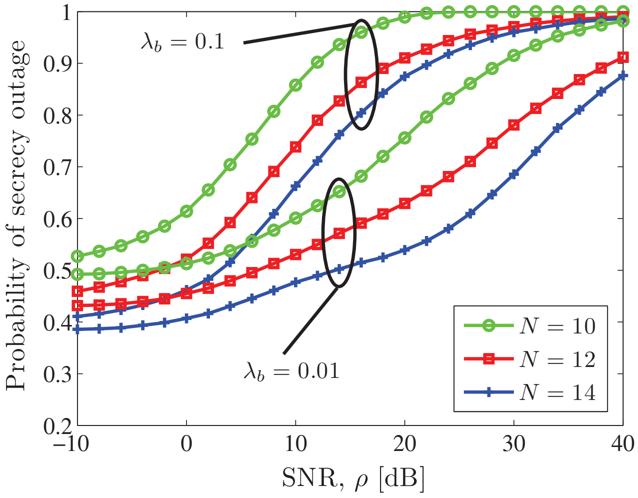

Fig. 3. Simulated probability of secrecy outage versus SNR, for $K = 10$ users per BS and various values of the number of antennas N and density of BSs λ_b.

Remark 3. *In a cellular network with a fixed load, i.e., average number of users per BS, there is an optimal value for the deployment density of BSs* λ_b *that maximizes the mean secrecy rate, and this value is a decreasing function of the SNR. The optimal value of* λ_b *can be found from (21) by performing a linear search.*

V. Numerical Results

In Fig. 3 we plot the simulated probability of secrecy outage versus the SNR, for $K = 10$ users per BS and three values of the number of transmit antennas $N \geq K$. For $N < K$ the secrecy performance is poor, even in the case of an isolated cell [5]. In this figure, two cases are considered for the density of BSs λ_b, namely 0.01 and 0.1, while the density of users is given by $\lambda_u = K\lambda_b$. Fig. 3 shows that RCI precoding achieves confidential communications in cellular networks with probability of secrecy outage $\tilde{\mathcal{P}}_o < 1$, and that having more transmit antennas is beneficial as it reduces the probability of secrecy outage. However unlike an isolated cell [10], cellular networks tend to be in secrecy outage w.p. 1 if the transmit power grows unbounded, irrespective of the number of transmit antennas. These observations are consistent with Remark 1.

In Fig. 4 we plot the simulated per-user ergodic secrecy rate versus the SNR, for $K = 10$ users per BS and three values of the number of transmit antennas N. In this figure, again, two cases are considered for the density of BSs λ_b, namely 0.01 and 0.1, while the density of users is given by $\lambda_u = K\lambda_b$. Fig. 4 shows that in cellular networks RCI precoding can achieve a non-zero secrecy rate, and that having more transmit antennas

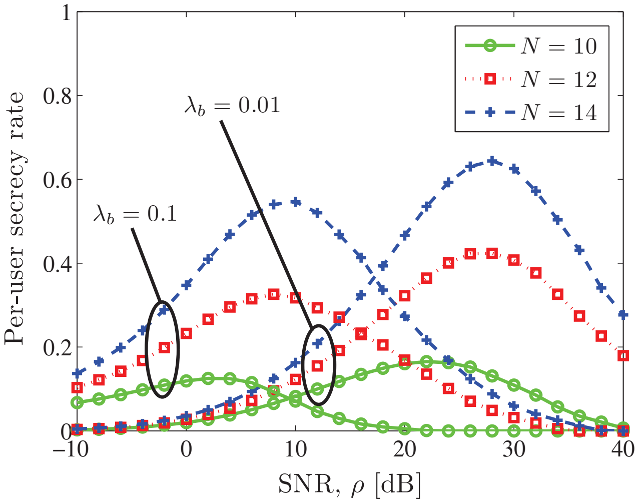

Fig. 4. Simulated ergodic secrecy rate versus SNR, for $K = 10$ users per BS and various values of the number of antennas N and density of BSs λ_b.

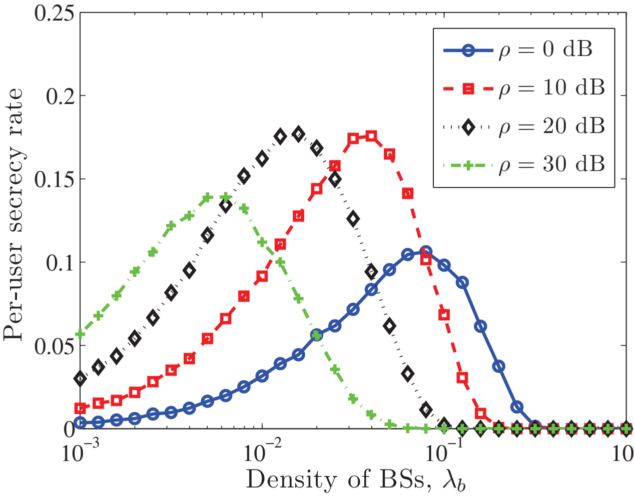

Fig. 5. Simulated ergodic secrecy rate versus density of BSs, for $N = 20$ transmit antennas, $K = 20$ users per BS, and various values of the SNR ρ.

is beneficial as it increases the secrecy rate. However unlike the secrecy rate in an isolated cell [5], the secrecy rate in a cellular scenario does not grow unbounded with the SNR, even with a large number of transmit antennas. These observations are consistent with Remark 2.

In Fig. 5 we plot the simulated per-user ergodic secrecy rate as a function of the density of BSs λ_b, for $N = 20$ transmit antennas, $K = 20$ users per BS, and various values of the SNR. Fig. 5 shows that there is an optimal value for the density of BSs λ_b that maximizes the secrecy rate, and that such value is smaller for higher values of the SNR. This observation is consistent with Remark 3.

VI. Conclusion

In this paper, we considered physical layer security for the downlink of cellular networks. We found that under Rayleigh fading, RCI precoding can achieve a non-zero secrecy rate. However unlike isolated cells, the network tends to be in secrecy outage if the transmit power grows unbounded. We further showed that there is an optimal value for the density of BSs that maximizes the secrecy rate. Our analysis clearly established the importance of designing the transmit power and the BS deployment density to make communications robust against malicious users in other cells.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell System Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] E. Ekrem and S. Ulukus, “Capacity region of Gaussian MIMO broadcast channels with common and confidential messages,” *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[4] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “New results on multiple-input multiple-output broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, pp. 1346–1359, Mar. 2013.

[5] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, “Large system analysis of linear precoding in MISO broadcast channels with confidential messages,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[6] M. Haenggi, “The secrecy graph and some of its properties,” in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, July 2008.

[7] P. Pinto, J. Barros, and M. Win, “Secure communication in stochastic wireless networks – Part I: Connectivity,” *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[8] X. Zhou, R. K. Ganti, and J. G. Andrews, “Secure wireless network connectivity with multi-antenna transmission,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Dec. 2011.

[9] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, “On secrecy capacity scaling in wireless networks,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[10] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, “Secrecy rates in the broadcast channel with confidential messages and external eavesdroppers,” to appear in *IEEE Trans. Wireless Commun.*, 2013, available arXiv:1306.2101.

[11] H. Wang, X. Zhou, and M. C. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” *IEEE Trans. Wireless Commun.*, 2013, accepted for publication, available arXiv:1303.1609.

[12] R. W. Heath Jr., M. Kountouris, and T. Bai, “Modeling heterogeneous network interference using Poisson point process,” *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4114–4126, Apr. 2013.

[13] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, “Physical layer security in downlink multi-antenna cellular networks,” submitted to *IEEE Trans. Commun.*, 2013, available arXiv:1307.7211.

[14] Q. Li, G. Li, W. Lee, M. Lee, D. Mazzarese, B. Clerckx, and Z. Li, “MIMO techniques in WiMAX and LTE: a feature overview,” *IEEE Comms. Mag.*, vol. 48, no. 5, pp. 86–92, May 2010.

[15] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, “A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization,” *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[16] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[17] H. S. Dhillon, M. Kountouris, and J. G. Andrews, “Downlink MIMO HetNets: Modeling, ordering results and performance analysis,” *IEEE Trans. Wireless Commun.*, 2013, accepted for publication, available arXiv:1301.5034.

[18] V. Nguyen and J. Evans, “Multiuser transmit beamforming via regularized channel inversion: A large system analysis,” in *Proc. IEEE Global Commun. Conf. (Globecom)*, Dec. 2008.

[19] S. Wagner, R. Couillet, M. Debbah, and D. T. M. Slock, “Large system analysis of linear precoding in correlated MISO broadcast channels under limited feedback,” *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4509–4537, July 2012.

[20] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume I: Theory*, 1st ed. Hanover, MA: Now Publishers Inc., 2009.

[21] M. Haenggi, “On distances in uniformly random networks,” *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.