"© 2013 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

On the Physical Layer Security in Large Scale Cellular Networks

He Wang*†, Xiangyun Zhou* and Mark C. Reed‡*
*Research School of Engineering, the Australian National University, ACT 0200, Australia
†National ICT Australia (NICTA), ACT 2601, Australia
‡UNSW Canberra, ACT 2600, Australia
Email: {he.wang, xiangyun.zhou}@anu.edu.au, mark.reed@unsw.edu.au

***Abstract*—This paper studies the information-theoretic secrecy performance in large-scale cellular networks based on a stochastic geometry framework. The locations of both base stations and the mobile users are modeled as independent two-dimensional Poisson point processes. We consider a key feature of the cellular network, namely, information exchange between base stations, and characterize its impact on the achievable secrecy rate of an arbitrary downlink transmission with a certain portion of the mobile users acting as potential eavesdroppers. In particular, analytical results are presented under diverse assumptions on the availability of eavesdroppers' location information at the serving base station, which captures the benefit from the exchange of mobile users' location information between base stations.**

I. Introduction

Communication security is always a crucial issue for cellular systems. Traditionally, most of security techniques in modern cellular standards involve means of encryption algorithms in the upper layers of the protocol stacks [1]. In contrast, the concept of achieving information-theoretic security by protecting physical layer of wireless networks has attracted attention widely in the research community. Wyner proposed the wiretap channel model and the notion of perfect secrecy for point-to-point communication in his pioneering work [2]. Based on these initial results, the achievable secrecy rate, defined as the maximum transmission rate at which the eavesdropper is unable to obtain any information, can be achieved if the intended receiver enjoys a better channel than the potential eavesdropper.

Unlike point-to-point scenarios, the studies on the secure communications in large-scale wireless networks have been carried out recently, from the information-theoretic viewpoint. Secrecy communication graphs describing secure connectivity over a large-scale network with eavesdroppers presented were investigated in [3]–[7]. In order to derive the network throughput, these works on connectivity were further extended for secrecy capacity analysis. Specifically, the maximum achievable secrecy rate under the worst-case scenario with colluding eavesdroppers was given in [8]. Scaling laws for secrecy capacity in large networks have been investigated in [9]–[11]. Focusing on the transmission capacity of secure communications, the throughput cost of achieving a certain level of security in an interference-limited network was analyzed in [12]. It should be noticed that all works mentioned above concentrated on ad hoc networks.

In this work, we focus on the secrecy performance in large-scale cellular networks, considering cellular networks' unique characteristics different from ad hoc networks: the carrier-operated high-speed backhaul networks connecting individual base stations (BSs) and the core-network infrastructures, which provide us potential means of BS cooperation, such as exchanging information to guarantee better secure links.

Fortunately, modeling BSs to be randomly placed points in a plane and utilizing stochastic geometry [13] [14] to analyze cellular networks has been used extensively as an analytical tool for improving tractability [15]–[17]. Recent works [18]–[21] have shown that the network models with BS locations drawn from a homogeneous Poisson point process (PPP) are as accurate as the traditional grid models compared to the result of an practical network deployment, and can provide more tractable analytical results which give pessimistic lower bounds on coverage and throughput. For these reasons we adopt PPPs to model the locations of BSs of the cellular networks in this paper.

The following scenario of secure communication in cellular networks is considered in this work: confidential messages are prepared to be conveyed to a mobile user, while certain other mobile users should not have the access to the messages and hence are treated as potential eavesdroppers. The serving BS should ensure the messages successfully delivered to the intended user while keeping perfect secrecy against all potential eavesdroppers. Considering the fact that the cellular service area is divided into cells, each BS knows both the location as well as the identity of each user (i.e., whether the user is a potential eavesdropper or not) in its own cell. The identity and location information of mobile users in other cells can be obtained by information exchange between the BSs via the backhaul networks.

Our contribution is that we provide probabilistic characterizations of the secrecy rate and quantify the average secrecy rate achievable for a randomly located mobile user in such a cellular network. The serving BS acquires the potential eavesdroppers' locations via information exchange with neighboring BSs. We analytically show how the achievable secrecy rate increases as more nearby BSs participate in the information exchange with the serving BS. This result provides network designers with useful guidelines in deciding on the necessary information exchange range to achieve the desired secrecy

performance.

It should be noted that similar work to evaluate secrecy performance of large scale cellular networks was conducted in [22]; however, it mainly focused on the scaling behavior of the eavesdropper's density to allow full coverage over the entire network, without taking the achievable secrecy rate into account. In contrast, we characterize the statistics of the secrecy rate at an arbitrary mobile user under different assumptions on the information exchange of the eavesdroppers' location .

The remainder of the paper is organized as follows. In Section II, we present the system model and general assumptions. Section III shows the main result of this paper, in which we obtain simple tractable expressions for achievable secrecy rates. Section IV provides numerical results and concluding remarks are given in Section V.

II. System Model

We consider the downlink scenario of a cellular network utilizing an orthogonal multiple access technique and composing of a single class of BSs, macro BS for instance. We focus on the performance achieved by a randomly chosen typical mobile user. The BSs are assumed to be spatially distributed as a two-dimensional homogeneous PPP Φ_{BS} of density λ_{BS}, and all BSs have the same transmit power value P_{BS}. An independent collection of mobile users, located according to an independent homogeneous PPP Φ_{MS} of density λ_{MS}, is considered. We consider the process $\Phi_{MS} \cup \{0\}$ obtained by adding a user to the origin of the coordinate system, which is the typical user under consideration. This is allowed by Slivnyak's Theorem [13] which states that the properties observed by a typical point of the PPP Φ_{MS}, is the same as those observed by node at origin in the process $\Phi_{MS} \cup \{0\}$.

A. Cell Association Model

In this analysis, we associate users to the nearest BS[1], which is commonly used in related cellular modeling works [15] [18]. Since each mobile user camps on the closest BS, equivalently, a BS is associated with the users in its Voronoi cell (formed by the PPP Φ_{BS}), thus resulting the Voronoi tessellation [13] for BS coverage areas, as shown in Fig. 1.

B. Signal Model

The standard power loss propagation model is used with path loss exponent $\alpha > 2$. Hence, the received power at the receiver x_i from the transmitter x_j is written as

$$P_{rx}(x_i, x_j) = P_{BS}\|x_i - x_j\|^{-\alpha}. \quad (1)$$

[1]Note that in the presence of eavesdroppers, it is generally not optimal to associate the mobile user to the nearest BS, since the nearest BS may not be the one providing the maximum secrecy rate. For example, if the nearest BS is closely surrounded by eavesdroppers whereas the second nearest BS does not have any eavesdroppers located close by, it is better to associate the mobile user to the second nearest BS. However, it is shown in the journal version of this paper [23] that optimally selecting the BS for user association provide a very marginal secrecy rate improvement over nearest BS association.

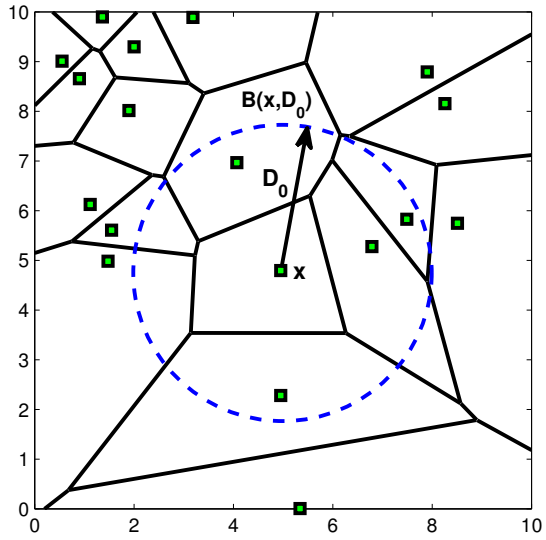

Fig. 1. Illustration of Poisson distributed BSs' cell boundaries. Each user is associated with the nearest BS, and BSs (represented by green squares) are distributed according to PPP.

The noise power is assumed to be additive and constant with value σ^2 for all users, but no specific distribution is assumed in general.

In this work, we also assume there is no in-band interference at downlink receivers. This assumption is achievable by a carefully planned frequency reuse pattern, where the interfering BSs are far away to have the serving BS occupying some resource blocks exclusively in a relatively large area, and the interference can be incorporated in the constant noise power.

C. Location Information Exchange

We consider a scenario where confidential messages are prepared to be delivered to the typical user, while certain individuals among other mobile users, treated as potential malicious eavesdroppers (or called Eve for brevity) by the network, should be kept from accessing them. We model a fraction of the other mobile users randomly chosen from Φ_{MS} (the process constructed by all other users except the typical user) as the eavesdroppers, i.e. a thinned PPP Φ_e with the density of λ_e.

Considering the backhaul bandwidth cost in practice and core-network implementation complexity for BS cooperation, each BS may only know the location and identity (i.e., whether the user is a potential eavesdropper or not) of each mobile user in its neighboring region, in which neighboring BSs participating in the information exchange with the serving BS, and the area outside the cells covered by these BSs is the unknown region. By considering the worse case scenario that the eavesdroppers can be located anywhere inside the unknown region, the secrecy performance is limited by the minimum distance from the unknown region to the serving BS. As long as the minimum distance is the same, the secrecy performance stays the same regardless of the shape of the unknown region.

D. Achievable Secrecy Rate

Firstly, if we suppose the ideal case where the serving BS located at x knows the locations of all eavesdroppers, which requires the location and identity information of all users is shared completely through the backhaul network, the maximum secrecy rate achievable at the typical mobile user is given by [4], [24]

$$R_s = \max\Bigg\{ \log_2\Big(1+\frac{P_{rx}(0,x)}{\sigma^2}\Big) - \log_2\Big(1+\frac{P_{rx}(e^*(x),x)}{\sigma^2}\Big), 0\Bigg\}, \quad (2)$$

where

$$e^*(x) = \arg\max_{e\in\Phi_e} P_{rx}(e,x) = \arg\min_{e\in\Phi_e} \|e-x\|, \quad (3)$$

i.e., $e^*(x)$ is the location of the most detrimental eavesdropper, which is the nearest one from the serving BS in this case.

Then, assuming limited information exchange between BSs, there will be areas in which the eavesdroppers' location information is unknown to the serving BS, which is denoted by $\Theta \subset \mathbb{R}^2$. When this happens, the serving BS assumes the worst case, i.e., eavesdroppers can lie at any points in Θ. Then the achievable secrecy rate is still given by (2), but $e^*(x)$ should be given as

$$e^*(x) = \arg\max_{e\in\Phi_e\cup\Theta} P_{rx}(e,x), \quad (4)$$

where the detrimental eavesdropper is chosen from the union of the eavesdropper set Φ_e and the unknown areas Θ.

It should be noticed that the randomness introduced by Φ_{BS} and Φ_e makes the achievable secrecy rate R_s at the typical user be a random variable. Furthermore, the distribution of R_s is mixed, i.e., R_s has a continuous distribution on $(0,\infty)$ and a discrete component at 0.

By assuming that the receivers of both legitimate user and eavesdroppers are operated in the high signal-to-noise ratio (SNR) regime, i.e., $P_{rx}(0,x)/\sigma^2 \gg 1$ and $P_{rx}(e^*(x),x)/\sigma^2 \gg 1$, we can obtain an approximation of R_s denoted by $\hat{R}_s$, i.e., $\hat{R}_s = \max\big\{\log_2\big(P_{rx}(0,x)/\sigma^2\big) - \log_2\big(P_{rx}(e^*(x),x)/\sigma^2\big), 0\big\}$, whose CCDF can be derived as

$$\bar{F}_{\hat{R}_s}(R_0) = \mathbb{P}\left(\|e^*(x)-x\| > \beta^{1/\alpha}\|x\|\right), \quad \text{where } R_0 \geqslant 0, \quad (5)$$

where the threshold β is defined as $\beta \triangleq 2^{R_0}$. In this work, we focus on high SNR scenarios and use the above expression to obtain tractable results on the secrecy rate performance. The obtained analytical results give approximations on the secrecy performance at finite SNR values.

Furthermore, from the fact that the achievable secrecy rate R_s should always be non-negative, we can easily reach the conclusion that the high SNR approximation $\bar{F}_{\hat{R}_s}(R_0)$ serves as an upper bound for the CCDF of R_s at finite SNR. Therefore, our analytical results on $\bar{F}_{\hat{R}_s}(R_0)$ and $\mathbb{E}[\hat{R}_s]$ under the high SNR assumption, give valid upper bounds on the secrecy performances at finite SNR values.

III. Main Results

In this section, we provide the main results on the probabilistic characteristics of the achievable secrecy rates $\hat{R}_s$ and the average secrecy rates achievable $\mathbb{E}[\hat{R}_s]$ under the assumption that the serving BS can partially or fully acquire the location information of the eavesdroppers, corresponding to the different levels of BS cooperation introduced. It should be noticed that the BS cooperation considered in this paper includes only exchanging the identity and location information of the mobile users.

A. Location and identity information exchange limited with neighboring cells only

In order to characterize how the availability of the location and identity information affects the secrecy performance, we will investigate the secrecy rate for the case where the location information and identity exchange is restricted among neighboring cells only.

We define the (closed) ball centered at p and of radius r as $B(p,r)$, i.e., $B(p,r) \triangleq \{m \in \mathbb{R}^2, \|m-p\| \leqslant r\}$. Here, we apply the following model to represent the known and unknown regions: only the location information of the eavesdroppers with a distance less than D_0 from the serving BS is available to it, i.e., the eavesdroppers outside the area $B(x,D_0)$ are unknown to a BS at x, as shown in Fig. 1. The value D_0 is called *detection radius* in our analysis. Indeed, the detection radius models the distance from the serving BS to the nearest point in the unknown region. As discussed in Section II-C, as long as the minimum distance from the unknown region remains the same, the secrecy performance stays the same regardless of the shape of the unknown region. Therefore, the consideration of a disk-shape known region does not lose the generality of the result on secrecy rates.

From a network design perspective, a larger D_0 represents information exchanging feasible with BSs farther away, and in other words, a larger D_0 means more BSs participate in the information exchange with the serving BS. This scenario provides limited information exchange, which reflects practical considerations, such as the limited bandwidth of the backhaul network and the complexity introduced by extensive information sharing in practical implementation. By investigating how the achievable secrecy rate changes with D_0, one can obtain insights on the improvement in the secrecy performance as more BSs participate in the information exchange process.

Proposition 1: When the detection radius is D_0, the CCDF of the achievable secrecy rate obtained at the typical user is given by

$$\bar{F}_{\hat{R}_s}(R_0) = \Big(1-\exp\big[-\pi(\lambda_e+\lambda_{BS}2^{-\frac{2R_0}{\alpha}})D_0{}^2\big]\Big) \cdot \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2R_0)/\alpha}}, \quad \text{where } R_0 \geqslant 0. \quad (6)$$

Proof: Based on the available location information of eavesdroppers with a distance less than D_0 and the typical

user served by the nearest BS at x_0, (5) can be derived as follows,

$$\begin{aligned}\bar{F}_{\hat{R}_s}(R_0) &= \mathbb{P}\left(\|e^*(x_0)-x_0\| > \beta^{1/\alpha}\|x_0\|\right)\\ &= \mathbb{P}\left[\text{No Eve in } B(x_0,\beta^{\frac{1}{\alpha}}r_u); r_u < \beta^{-\frac{1}{\alpha}}D_0\right],\end{aligned} \tag{7}$$

where x_0 denotes the nearest BS from the origin and r_u is the distance from the typical user to the nearest BS, namely, $r_u = \|x_0\|$, the probability density function (pdf) of r_u has been provided in [25], as

$$f_{r_u}(r) = 2\pi\lambda_{BS} r \exp(-\pi\lambda_{BS} r^2). \tag{8}$$

Hence, (7) becomes

$$\begin{aligned}&\bar{F}_{\hat{R}_s}(R_0)\\ &= \int_0^{\beta^{-\frac{1}{\alpha}}D_0} \mathbb{P}\big[\text{No Eve in } B(x_0,\beta^{\frac{1}{\alpha}}r_u) \mid r_u = y\big] f_{r_u}(y)\mathrm{d}y\\ &\overset{(a)}{=} \int_0^{\beta^{-\frac{1}{\alpha}}D_0} \mathbb{P}\big[\text{No Eve in } B(x_0,\beta^{\frac{1}{\alpha}}y)\big] f_{r_u}(y)\mathrm{d}y\\ &\overset{(b)}{=} \int_0^{2^{-\frac{R_0}{\alpha}}D_0} 2\pi\lambda_{BS} y \exp(-\pi\lambda_e 2^{\frac{2R_0}{\alpha}}y^2 - \pi\lambda_{BS}y^2)\mathrm{d}y\\ &= \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2R_0)/\alpha}}\cdot\\ &\qquad \Big(1-\exp\big[-\pi(\lambda_e+\lambda_{BS}2^{-\frac{2R_0}{\alpha}})D_0{}^2\big]\Big),\end{aligned} \tag{9}$$

where step (a) follows the independence between Φ_e and Φ_{BS}, and step (b) is derived based on the null probability of PPP and the pdf of r_u. It should be noticed that the probability expression $\mathbb{P}\big[\text{No Eve within } B(x_0,\beta^{\frac{1}{\alpha}}y)\big]$ is only dependent on the density of eavesdroppers λ_e and the ball's area $\pi\beta^{2/\alpha}y^2$ and independent of x_0. The integration from 0 to $2^{-\frac{R_0}{\alpha}}D_0$ gives the result which completes the proof. ■

Corollary 1: When the detection radius is D_0, the average secrecy rate achievable at the typical user is provided by

$$\begin{aligned}\mathbb{E}[\hat{R}_s] &= \frac{\alpha}{2\ln 2}\cdot\ln\Big(\frac{\lambda_{BS}+\lambda_e}{\lambda_e}\Big)\\ &\quad - \frac{\alpha}{2\ln 2}\cdot\Big[E_1\big(\pi\lambda_e D_0^2\big) - E_1\big(\pi(\lambda_e+\lambda_{BS})D_0^2\big)\Big],\end{aligned} \tag{10}$$

where $E_1(x) = \int_x^\infty \exp(-t)\frac{1}{t}\mathrm{d}t$ is the exponential integral.

Proof: Based on the CCDF expression given in Proposition 1, the average secrecy rate achievable at the typical user can be provided by integrating (6) from 0 to ∞,

$$\begin{aligned}\mathbb{E}[\hat{R}_s] &= \int_0^\infty \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\cdot\\ &\qquad \Big(1-\exp\big[-\pi(\lambda_e+\lambda_{BS}2^{-\frac{2t}{\alpha}})D_0^2\big]\Big)\mathrm{d}t\\ &= \int_0^\infty \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\mathrm{d}t\\ &\qquad - \int_0^\infty \frac{\exp\big[-\pi(\lambda_e+\lambda_{BS}2^{-\frac{2t}{\alpha}})D_0^2\big]}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\mathrm{d}t,\end{aligned} \tag{11}$$

where the former part of the last step can be derived by using the indefinite integral result in [26], i.e.,

$$\begin{aligned}&\int_0^\infty \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\mathrm{d}t\\ &= \left[\frac{1}{\ln(2^{2/\alpha})}\cdot\ln\left(\frac{\exp\big[\ln(2^{2/\alpha})t\big]}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot\exp\big[\ln(2^{2/\alpha})t\big]}\right)\right]_0^\infty\\ &= \frac{1}{\ln(2^{2/\alpha})}\ln\left(\frac{1}{\lambda_e/\lambda_{BS}}\right) - \frac{1}{\ln(2^{2/\alpha})}\ln\left(\frac{1}{1+\lambda_e/\lambda_{BS}}\right)\\ &= \frac{\alpha}{2\ln 2}\cdot\ln\Big(\frac{\lambda_{BS}+\lambda_e}{\lambda_e}\Big).\end{aligned} \tag{12}$$

The latter part of (11) can be derived as,

$$\begin{aligned}&\int_0^\infty \frac{\exp\big[-\pi(\lambda_e+\lambda_{BS}2^{-\frac{2t}{\alpha}})D_0^2\big]}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\mathrm{d}t\\ &= \exp(-\pi\lambda_e D_0^2)\int_0^\infty \frac{\exp\big[-\pi\lambda_{BS}D_0^2\cdot 2^{-\frac{2t}{\alpha}}\big]}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}}\mathrm{d}t\\ &\overset{(a)}{=} \exp(-\pi\lambda_e D_0^2)\int_{\frac{\lambda_e}{\lambda_{BS}}}^\infty \frac{\exp(-\pi\lambda_e D_0^2 v^{-1})}{1+v}\cdot\frac{1}{v\ln(2^{2/\alpha})}\mathrm{d}v\\ &\overset{(b)}{=} \frac{\alpha\exp(-\pi\lambda_e D_0^2)}{2\ln 2}\int_{\pi\lambda_e D_0^2}^{\pi(\lambda_{BS}+\lambda_e)D_0^2}\frac{1}{s\exp(s-\pi\lambda_e D_0^2)}\mathrm{d}s\\ &= \frac{\alpha}{2\ln 2}\int_{\pi\lambda_e D_0^2}^{\pi(\lambda_{BS}+\lambda_e)D_0^2}\frac{1}{s\exp(s)}\mathrm{d}s\\ &= \frac{\alpha}{2\ln 2}\Big[E_1\big(\pi\lambda_e D_0^2\big) - E_1\big(\pi(\lambda_e+\lambda_{BS})D_0^2\big)\Big],\end{aligned} \tag{13}$$

where the step (a) and the step (b) are obtained by employing changes of variables $v = \frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2t)/\alpha}$ and $s = \frac{\pi\lambda_e D_0^2}{v} + \pi\lambda_e D_0^2$ respectively, and the last step can be derived by using the definition of the exponential integral. Plugging (13) into (11) gives the desired result in (10), which completes the proof. ■

Remark: As expected, the general trend can be understood as follows: when detection radius D_0 decreases, the location information of eavesdroppers surrounding the serving BS reduces, which makes a lower probability to maintain the secrecy rate larger than R_0.

B. Extreme Case: Full Information Exchange

Next, we consider the case: all eavesdroppers' location information is accessible to the serving BS, which can be achieved by an ideal information exchange among all the BSs. This case can be viewed as the extreme case of the one presented in Section III-A, by increasing the detection radius D_0 to infinity.

Proposition 2: With the availability of full location information for all eavesdroppers, the CCDF of the achievable secrecy rate obtained at the typical user is given by

$$\bar{F}_{\hat{R}_s}(R_0) = \frac{1}{1+\frac{\lambda_e}{\lambda_{BS}}\cdot 2^{(2R_0)/\alpha}},\ \text{where } R_0 \geqslant 0. \tag{14}$$

Proof: The equation (14) can be easily obtained by substituting the condition of $D_0 \to \infty$ into (6). ■

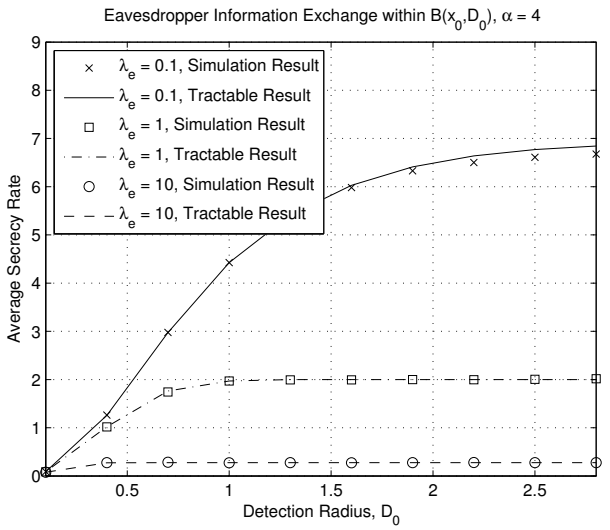

Fig. 2. The average secrecy rate achievable versus the detection radius D_0 (location information for users with a distance less than D_0). Simulation and tractable results are shown for $\lambda_{BS} = 1$ and path loss exponent $\alpha = 4$.

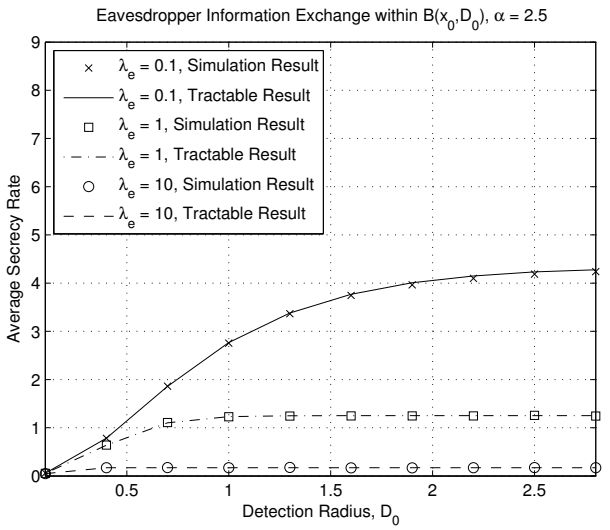

Fig. 3. The average secrecy rate achievable versus the detection radius D_0 (location information for users with a distance less than D_0). Simulation and tractable results are shown for $\lambda_{BS} = 1$ and path loss exponent $\alpha = 2.5$.

Corollary 2: With the availability of full location information for all eavesdroppers, the average secrecy rate achievable at the typical user is provided by

$$\mathbb{E}[\hat{R}_s] = \frac{\alpha}{2\ln 2} \cdot \ln\Big(\frac{\lambda_{BS} + \lambda_e}{\lambda_e}\Big). \tag{15}$$

Proof: This proof can be done based on (12). ■

IV. Numerical Illustrations

In this section, we present numerical results on the achievable secrecy rates. Here we define the value SNR as the received SNR from the serving BS at the distance $r = 1$, i.e. $SNR = P_{BS}/\sigma^2$. All simulation results are conducted under a high SNR condition $SNR = 20$dB, and unitary BS density, i.e., $\lambda_{BS} = 1$, to compare with our analysis for the purpose of model validation.

By presenting the average secrecy rate achievable versus the detection radius D_0 in Fig. 2 and Fig. 3, we can see the importance of eavesdroppers' location information on the secrecy performance. In case of relatively small values of D_0, any increase of the detection radius brings remarkable benefit to the achievable secrecy rate. On the other hand, in case of large D_0, any further increase in the detection radius does not substantially impact the secrecy rate, since the eavesdropper that limits the secrecy performance is usually located not too far away from the serving BS and its distance is likely to be smaller than D_0 when D_0 is sufficiently large. Take the curve with $\alpha = 4$ and $\lambda_e = 0.1$ for instance, the secrecy performance improves significantly as D_0 is increased up to 2, and any further increase from $D_0 = 2$ has a limited effect. This performance trend over the range of detection radius can be utilized to appropriately choose the number of neighboring BSs for information exchange in order to achieve a good secrecy performance whilst taking the implementation cost of such information exchange into consideration. It should be noticed that the slight mismatches between simulation and tractable results in these figures come from the high SNR assumption used in our analysis, and become almost invisible at $SNR = 30$dB (plot omitted for brevity).

For each curve in Fig. 4, we show the extreme case's average secrecy rates achievable in Section III-B, for both path loss exponents of $\alpha = 4$ and $\alpha = 2.5$. As can be seen the curves representing the analytical expression (15) in Corollary 2 match with the simulated results.

Another fact clearly shown from Fig. 2 to Fig. 4 is that better performance can be obtained for larger values of path loss exponent α, e.g., the average secrecy rate achievable is higher for $\alpha = 4$ than the counterpart for $\alpha = 2.5$. This is because the resultant larger path loss from larger α indicates worse signal condition both to the eavesdroppers and typical user, whereas the former effect turns out to be more influential on secrecy performance.

V. Conclusion

In this work, we studied the secrecy performance of cellular networks considering information exchange between BSs potentially provided by the carrier-operated high-speed backhaul and core-networks. Using the tools from stochastic geometry, tractable results to characterize the secrecy rate were obtained under different ranges of the location information exchange between BSs. The numerical results validated the tractable expressions, which provided the important message: the location information plays a crucial role in determining the average secrecy rate achievable at the typical user. A near optimal secrecy rate performance can usually be achieved by allowing a small number of neighboring BSs to exchange information. Our analytical result helps network designers to achieve good

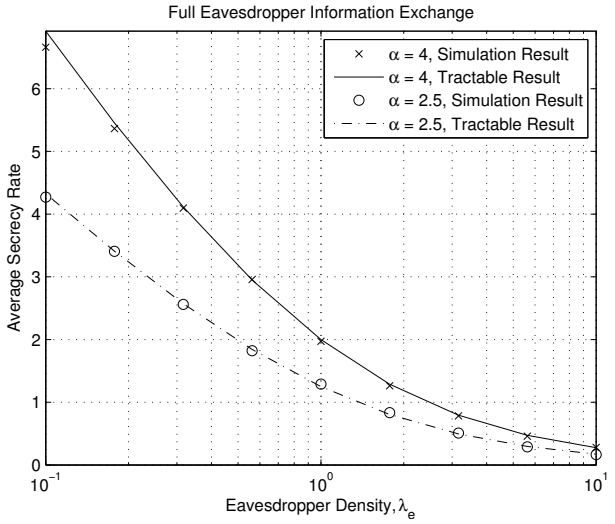

Fig. 4. The average secrecy rate achievable versus the eavesdropper density λ_e for full location and identity information exchange. Simulation and tractable results are shown for different pathloss exponents α.

secrecy performance whilst keeping the complexity and overhead at a minimal level.

The result in this work applies to scenarios where a carefully planned frequency reuse pattern is assumed, and the serving BS can occupy some resource blocks exclusively in a relatively large area. In future cellular networks, however, interference will become an important factor. Since the channel conditions of both legitimate user and eavesdropper will be degraded by introducing interference, the impact of the co-channel interference on the secrecy performance of large scale cellular network is still unknown. Another limitation is that the BS cooperation considered in this paper is confined to location information exchange. Coordinated multipoint (CoMP) transmission, as an emerging BS cooperation technique in future cellular networks, can be potentially utilized, and the benefit on secrecy performance is an interesting problem to investigate.

ACKNOWLEDGMENT

H. Wang is with the Australian National University and NICTA. NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program. This work was supported by the Australian Research Councils Discovery Projects funding scheme (Project No. DP110102548 and Project No. DP130101760).

REFERENCES

[1] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.

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

[3] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'08)*, Toronto, Canada, July 2008, pp. 539–543.

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

[5] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'10)*, Austin, USA, June 2010, pp. 2627–2631.

[6] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. 2010 Int'l Symp. on Information Theory and its Applications (ISITA'10)*, Taichung, Taiwan, Oct. 2010, pp. 349–354.

[7] 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, Feb. 2011.

[8] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks - Part II: Maximum rate and collusion," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

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

[10] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'09)*, Seoul, Korea, June 2009, pp. 1189–1193.

[11] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. 31st Annual IEEE Int'l Conf. on Computer Commun. (IEEE INFOCOM'12)*, Orlando, USA, Mar. 2012, pp. 1152–1160.

[12] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[13] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. New York, NY: John Wiley & Sons Ltd., 1995.

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

[15] T. X. Brown, "Cellular performance bounds via shotgun cellular systems," *IEEE J. Select. Areas Commun.*, vol. 18, no. 11, pp. 2443–2455, Nov. 2000.

[16] X. Yang and A. P. Petropulu, "Co-channel interference modeling and analysis in a Poisson field of interferers in wireless communications," *IEEE Trans. Signal Processing*, vol. 51, no. 1, pp. 64–76, Jan. 2003.

[17] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5500–5510, Dec. 2008.

[18] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

[19] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 3, pp. 550–560, Apr. 2012.

[20] W. C. Cheung, T. Q. Quek, and M. Kountouris, "Throughput optimization, spectrum allocation, and access control in two-tier femtocell networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 3, pp. 561–574, Apr. 2012.

[21] C. S. Chen, V. M. Nguyen, and L. Thomas, "On small cell network deployment: A comparative study of random and grid topologies," in *Proc. IEEE 76th Vehic. Tech. Conf. (VTC'12-Fall)*, Québec City, Canada, Sept. 2012, pp. 1–5.

[22] A. Sarkar and M. Haenggi, "Secrecy Coverage," *Internet Mathematics*, 2012, accepted. Available at http://www.nd.edu/ mhaenggi/pubs/im12.pdf.

[23] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, submitted for publication.

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

[25] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.

[26] A. Jeffrey and H.-H. Dai, *Handbook of mathematical formulas and integrals*, 4th ed. Burlington, MA: Academic Press, 2008.