

Secrecy Outage Analysis in Random Wireless Networks with Antenna Selection and User Ordering

Gaojie Chen, *Member, IEEE* and Justin P. Coon *Senior Member, IEEE*

Abstract—This paper investigates the secrecy outage probability in the downlink when the target user equipment (UE) is selected based on an ordering metric. UEs are positioned randomly according to a Poisson point process (PPP) in the presence of independently acting eavesdroppers (EDs), the locations of which are again modeled as a PPP. We propose the use of a transmit antenna selection (TAS) scheme at the base station (BS) to enhance secrecy performance and consider two metrics to order the UEs: one based on long-term average channel gain information from the BS to the UEs, and the other based on instantaneous channel gains. We derive closed form expressions for the secrecy outage probability subject to each of these ordering policies and verify our calculations through Monte Carlo simulations. Our results show that while TAS yields a performance improvement relative to single-antenna systems, the secrecy outage probability for TAS systems actually increases with the path loss exponent.

I. INTRODUCTION

Physical layer (PHY) security has gained a lot of interest since Wyner’s seminal paper [1]. The basic principle of PHY security is to exploit the inherent randomness of noise and wireless channels to ensure the confidentiality of messages against any eavesdropper (ED) regardless of its computing power [2]. Compared to cryptographic solutions, PHY security can offer major advantages, such as “provable” security, no need for key management/distribution, and superior scalability for next-generation networks [3].

Recently, studies have considered information theoretic security over wireless channels, covering such topics as cooperative relay and jammer networks, buffer-aided relay networks, multiple-input multiple-output communication (MIMO) with distributed beamforming, full-duplex networks, and cognitive radio networks [4]–[8]. However, all of these contributions focused on a small number of nodes and assumed the locations of EDs are known. In some cases, it may be impractical to estimate ED locations.

In the last decade, random graph and stochastic geometry formalisms have been employed extensively to model random node locations in wireless networks [9], [10]. More recently, these techniques have been applied to study the impact of random ED locations on secrecy performance [11]–[15]. Without any prior knowledge, the locations of EDs can be modeled as a Poisson point process (PPP). In [11], the average secrecy throughput of a network of multiple Poisson distributed legitimate node pairs operating in the presence of a Poisson field of EDs was analyzed. Following this work, MIMO beamforming was applied to enhance secrecy performance [12], [13]. In [16], ED collusion was modeled and achievable secrecy rates were analyzed based on the concept of *intrinsically secure graphs*.

This work was supported by EPSRC grant number EP/N002350/1 (“Spatially Embedded Networks”).

G. J. Chen and J. P. Coon are with the Department of Engineering Science, University of Oxford, Parks Road, Oxford, UK, OX1 3PJ, Emails: {gaojie.chen and justin.coon}@eng.ox.ac.uk.

In this paper, we take research on secrecy in random spatial networks one step further by considering the downlink of a cellular network (or similar system with a star topology) with Poisson distributed UEs and EDs, and analyze the secrecy outage probability for two different UE selection policies: one based on long-term average base station (BS)-to-UE channel gain information (equivalently BS-UE distance) ordering only, and one based on an ordering of instantaneous channel gains. We assume the BS employs transmit antenna selection (TAS) to improve secrecy performance. For each policy, we obtain a closed-form expression for the secrecy outage probability. Interestingly, our results show that while TAS yields a performance improvement relative to single-antenna systems, the secrecy outage probability for TAS systems actually increases with the path loss exponent for both policies. We also quantify the deterioration in secrecy performance with increasing ordinal UE index, i.e., cycling through the ordered list of UEs from best to worst.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

We consider the secure transmission from the BS to an ordered UE in \mathbb{R}^2 . The BS is equipped with K antennas, which it uses to perform TAS in order to maximize the instantaneous SNR at the intended UE. UEs and EDs are equipped with a single antenna each, which performs in a half-duplex mode. Without loss of generality, we locate the BS at the origin in \mathbb{R}^2 . We model the locations of the UEs and EDs as homogeneous PPPs in the plane – denoted by Φ_E and Φ_U , respectively – with intensities ρ_E and ρ_U . In our work, we consider independently acting eavesdropping, which means that EDs cannot share their received information.

All channels are assumed to undergo path loss and independent Rayleigh fading. Hence, the coefficient modeling the channel between nodes i and j can be decomposed as $g_{ij} = h_{ij}d_{ij}^{-\alpha/2}$, where α and d_{ij} denote the path loss exponent and the distance between the two nodes, respectively¹. The fading coefficient h_{ij} is modeled as a zero-mean complex Gaussian random variable with unit variance. Therefore, the corresponding channel gains $|g_{ij}|^2$ are independently exponentially distributed with mean $\lambda_{ij} = d_{ij}^{-\alpha}$. We assume that the channels are quasi-static, so that the channel coefficients remain unchanged during several packet transmissions but independently vary from one coherence time interval to another.

B. Secrecy Outage Probability

We define the secrecy outage probability based on the classical wireless wiretap theory but with multiple EDs and an ordered UE

¹We set the subscripts i and j to be elements in the set $\{B, U, E\}$ in order to denote transmissions from the BS, UEs and EDs, respectively. For example, g_{UE_1} denotes the channel coefficient between the UE and the first ED in Φ_E .

(see the next section for details of the ordering policies). We assume that the channel state information (CSI) between the BS and the UE is known by the BS². Therefore, the BS is able to send a symbol x_s to the n th UE from the k th selected antenna in the t th time slot. At the same time, the EDs receive this signal as well. The received signal at the n th UE can be written as

$$y_{B_k U_n}(t) = \sqrt{P_B} h_{B_k U_n}(t) x_s(t) + v_n(t), \quad (1)$$

and the signal intercepted by eavesdropper E_e can be written as

$$y_{B_k E_e}(t) = \sqrt{P_B} h_{B_k E_e}(t) x_s(t) + v_n(t), \quad (2)$$

where P_B denotes the BS transmit power and v_n denotes white Gaussian noise with power σ_n^2 . For notational convenience, the time index t is ignored below due to the quasi static channel assumption. In order to design the network parameters to achieve the maximum level of secrecy, we consider the worst-case scenario in which the EDs know the BS-ED CSI. According to (1) and (2), and incorporating the TAS principle at the BS, the end-to-end SNR at the n th UE and the worst-case eavesdropper can be obtained as

$$\gamma_{BU_n} = \frac{P_B \max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)}{\sigma_n^2 d_{BU_n}^\alpha} \quad \text{and} \quad \gamma_{BE_*} = \frac{P_B \max_{e \in \Phi} (|h_{B_* E_e}|^2)}{\sigma_n^2 d_{BE_e}^\alpha}, \quad (3)$$

respectively, where $B_* = \arg \max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)$. It follows that the relevant end-to-end capacities from the BS to the n th UE and the BS to the worst-case E_* can be written as

$$C_{BU_n} = \log_2 \left(1 + \frac{P_B \max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)}{\sigma_n^2 d_{BU_n}^\alpha} \right), \quad (4)$$

$$C_{UE_*} = \log_2 \left(1 + \frac{P_B \max_{e \in \Phi} (|h_{B_* E_e}|^2)}{\sigma_n^2 d_{BE_e}^\alpha} \right).$$

The secrecy outage probability for the n th UE is given by [17]³

$$P_{so} = \mathbb{P}([C_{BU_n} - C_{BE_*}]^+ < \epsilon) \simeq \mathbb{P}\left(\frac{\gamma_{BU_n}}{\gamma_{BE_*}} < \beta\right) \quad (5)$$

where $[x]^+ = \max(x, 0)$, $\mathbb{P}(\cdot)$ denotes probability, ϵ denotes the target secrecy rate, and $\beta = 2^\epsilon$ denotes the target secrecy SNR.

III. ANALYSIS FOR TWO UE ORDERING POLICIES

In this section, we investigate two ordering policies for UE selection. One is the based on the distance between the BS and the UE (d_{BU}), the other one is the based on channel gain, i.e., the ratio ($|h_{B_* U}|^2/d_{BU}^\alpha$).

A. Policy I: Ordering by Distance

We assume all channels are i.i.d. Consequently, the conditional cumulative distribution function (CDF) and probability density function (PDF) of γ_{BU_n} are

$$F_{\gamma_{BU_n}}(x | d_{BU_n}) = \left(1 - e^{-x d_{BU_n}^\alpha}\right)^K = \sum_{k=0}^K C_K^k (-1)^k e^{-k x d_{BU_n}^\alpha},$$

$$f_{\gamma_{BU_n}}(x | d_{BU_n}) = \sum_{k=1}^K C_K^k (-1)^{k+1} k d_{BU_n}^\alpha e^{-k x d_{BU_n}^\alpha}, \quad (6)$$

²This can be achieved by feeding back CSI from the UE to the BS directly.

³The approximation in (5) is a standard assumption for systems operating in the high SNR region [17].

respectively, where $C_K^k = K!/[k!(K-k)!]$ is the binomial coefficient. Then, the CDF of γ_{BE_*} can be calculated as

$$F_{\gamma_{BE_*}}(y) = \mathbb{P}\left(\max_{e \in \Phi_E} \left(\frac{|h_{B_* E_e}|^2}{d_{BE_e}^\alpha}\right) < y\right)$$

$$\stackrel{(a)}{=} E_{\Phi_E} \left[\prod_{e \in \Phi_E} \mathbb{P}(|h_{B_* E_e}|^2 < y d_{BE_e}^\alpha | \Phi_E) \right]$$

$$\stackrel{(b)}{=} \exp\left(-\rho_E \int_0^{2\pi} \int_0^\infty r (e^{-y r^\alpha}) dr d\theta\right) = \exp\left(-\frac{2\pi\rho_E}{\alpha y^{\frac{2}{\alpha}}} \Gamma\left(\frac{2}{\alpha}\right)\right), \quad (7)$$

where $\Gamma(\cdot)$ is the gamma function; (a) follows from the independence of $\{|h_{B_* E_e}|^2; E_e \in \Phi\}$; and (b) holds by the probability generating functional lemma [18]. The PDF of γ_{BE_*} is

$$f_{\gamma_{BE_*}}(y) = \frac{2\pi\rho_E \Gamma\left(\frac{2}{\alpha} + 1\right)}{\alpha y^{\frac{2}{\alpha} + 1}} \exp\left(-\frac{\pi\rho_E \Gamma\left(\frac{2}{\alpha} + 1\right)}{y^{\frac{2}{\alpha}}}\right). \quad (8)$$

According to the definition of secrecy outage probability (5), and using (6) and (7), the conditional secrecy outage probability given the BS-UE distance for UE ordering policy I can be written as

$$F_{so}^{(I)}(\beta | d_{BU_n}) = 1 - \int_0^\infty f_{\gamma_{BU_n}}(x | d_{BU_n}) F_{\gamma_{BE_*}}\left(\frac{x}{\beta}\right) dx$$

$$= 1 - \sum_{i=1}^K C_K^i (-1)^{i+1} \frac{\sqrt{pq}}{2^{\frac{p+2q-3}{2}} \pi^{\frac{p+2q-1}{2}}} \times G_{0,p+2q}^{p+2q,0} \left(\frac{a_k^{2q} b^p}{p^{p+2q} q^{2q}} \middle| 0, \frac{1}{p}, \dots, \frac{p-1}{p}, \frac{1}{2q}, \frac{2}{2q}, \dots, 1 \right) \quad (9)$$

where $G_{s,t}^{m,n}(z | u_1, \dots, u_s; v_1, \dots, v_t)$ is the Meijer G function, $\alpha = p/q$ with $p, q \in \mathbb{Z}^+$, $a = k d_{BU_n}^\alpha$, and $b = \pi\rho_E \Gamma\left(\frac{2}{\alpha} + 1\right) \beta^{2/\alpha}$.

All that remains is to average over the BS-UE distance. The statistics of the n th nearest neighbor in a PPP are well known. Using these results, we have that the PDF of d_{BU_n} is [19]

$$f_{d_{BU_n}}(d_{BU_n}) = e^{-\rho_U \pi d_{BU_n}^2} \frac{2\rho_U^n \pi^n d_{BU_n}^{2n-1}}{\Gamma(n)}. \quad (10)$$

Finally, by using (9) and (10), we arrive at the expression for the secrecy outage probability given by

$$P_{so}^{(I)}(\beta) = \int_0^\infty F_{so}^{(I)}(\beta | d_{BU_n}) f_{d_{BU_n}}(d_{BU_n}) dd_{BU_n}$$

$$= \begin{cases} 1 - \sum_{k=1}^K C_K^k \frac{(-1)^{k+1}}{\Gamma(n)} G_{0,1}^{2,1} \left(\frac{\beta A_e k}{\rho_U \pi} \middle| \frac{1-n}{1,0} \right), & \alpha = 2, \\ 1 - \sum_{k=1}^K C_K^k \frac{(-1)^{k+1} 2^{n-1} (\beta k)^{\frac{1}{4}} \sqrt{\rho_E \Gamma\left(\frac{2}{\alpha} + 1\right)}}{\pi \Gamma(n) \sqrt{\rho_U}} \times G_{0,2}^{3,2} \left(\frac{\beta A_e^2 k}{\rho_U \pi} \middle| \frac{1}{4}, \frac{n}{2}, \frac{3}{4}, \frac{n}{2} \right), & \alpha = 4, \end{cases} \quad (11)$$

where $A_e = \pi\rho_E \Gamma\left(\frac{2}{\alpha} + 1\right)$.

B. Policy II: Ordering by Channel Gain

For this ordering policy, let

$$x_n = \frac{d_{BU_n}^\alpha}{\max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)} \quad (12)$$

and define the set $\Psi = \{x_n, n \in \mathbb{N}\}$. The following lemmata allow us to make progress based on these definitions.

Lemma 2: The set Ψ is a PPP with intensity function given by

$$\rho_{\Psi}(\psi) = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{2\pi\rho_U K \psi^{\frac{2}{\alpha}-1} \Gamma(\frac{2}{\alpha} + 1)}{\alpha(l+1)^{\frac{2}{\alpha}+1}}. \quad (13)$$

Proof: See Appendix I.

Lemma 3: The PDF of x_n is given by

$$f_{x_n}(x) = \frac{2(A_u x^{\frac{2}{\alpha}})^n \exp(-A_u x^{\frac{2}{\alpha}})}{\alpha x \Gamma(n)}, \quad (14)$$

where $A_u = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{\pi\rho_U K \Gamma(\frac{2}{\alpha}+1)}{(l+1)^{\frac{2}{\alpha}+1}}$, and the CDF of $1/x_n$ is given by

$$F_{\frac{1}{x_n}}(x) = \frac{\Gamma(n, A_u x^{\frac{2}{\alpha}})}{\Gamma(n)}, \quad (15)$$

where $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function.

Proof: See Appendix II.

Now, by using (8) and (15), we can obtain the secrecy outage probability for the second UE ordering policy as follows:

$$P_{so}^{(II)}(\beta) = 1 - \int_0^{\infty} F_{\frac{1}{x_n}}(\beta y) f_{\gamma_{BE^*}}(y) dy = 1 - \left(\frac{A_u \beta^{-\frac{2}{\alpha}}}{A_u \beta^{-\frac{2}{\alpha}} + A_e} \right)^n \quad (16)$$

IV. SIMULATIONS RESULTS

Here, we provide simulation results to verify our analysis. In the simulations, we assume the noise variance $\sigma_n^2 = 1$, and the transmission-power-to-noise ratio $P_B/\sigma_n^2 = 50$ dB. The simulation results are obtained by averaging over 10^5 independent Monte Carlo trials. The single-antenna case is our benchmark.

Fig. 1 verifies the secrecy outage probability expressions given in (11) for the nearest UE ($n = 1$) for ordering policy I. The path loss exponents considered are $\alpha = 2$ and 4, and we let $\beta = 1$ and $\rho_U = 0.5 \text{ m}^{-2}$. Both the simulation and the theoretical results are presented, which are shown to match perfectly. Furthermore, it is clear that the secrecy outage probability decreases as the number of transmit antennas increases for both cases. For the single-antenna case, the secrecy outage probability decreases when the path loss exponent increases. Physically, this behavior implies that cluttered environments exhibiting high propagation losses are more beneficial for secrecy, which was also confirmed in [16]. However, with TAS, propagation losses have a deleterious effect on the diversity offered by selection. This effect outweighs the benefit that such losses provide in terms of secrecy. So as the path loss exponent increases, the secrecy outage probability also increases when TAS is used.

Results corresponding to the second UE ordering are illustrated in Fig. 2. Here, we let $n = 1$, $\beta = 1$ and $\rho_U = 0.5 \text{ m}^{-2}$. Again, the theoretical results (generated with the help of (16)) are well matched to the simulation results. The expected trends are observed in this figure: the secrecy outage probability increases with the intensity of EDs and decreases with increasing numbers of transmit antennas. Importantly, we see from Fig. 2 that performance is independent of the path loss exponent for $K = 1$. However, we also observe the same trends noted above regarding the worsening of performance with increasing path loss exponent for $K > 1$.

Fig. 3 shows the secrecy outage probability versus the different ordered UE index for both policy I and policy II, where $\rho_E = 0.01 \text{ m}^{-2}$ and $\rho_U = 0.5 \text{ m}^{-2}$. We can see that with increasing indices (i.e., second, third, fourth best and so on), the secrecy outage

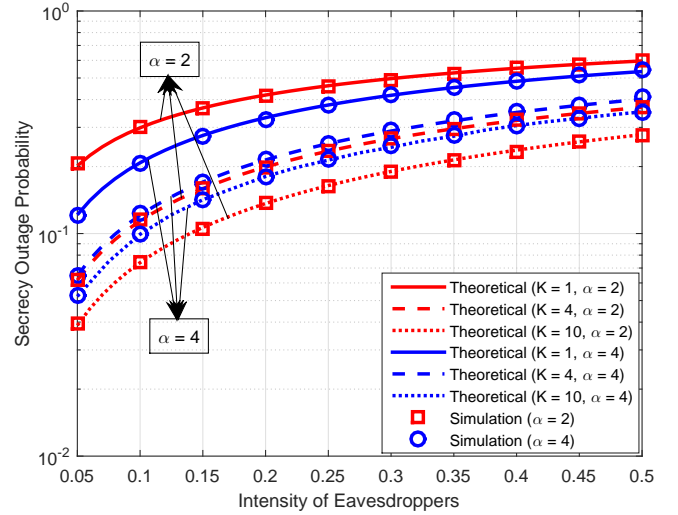


Fig. 1. Theoretical vs. numerical secrecy outage probabilities for UE ordering policy I, where $n = 1$, $\beta = 1$ and $\rho_U = 0.5 \text{ m}^{-2}$.

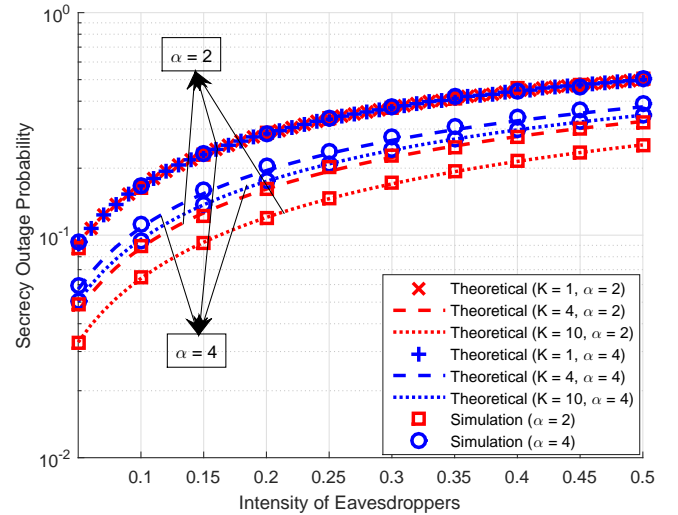


Fig. 2. Theoretical vs. numerical secrecy outage probabilities for UE ordering policy II, where $n = 1$, $\beta = 1$ and $\rho_U = 0.5 \text{ m}^{-2}$.

probability increases for both policies, as expected. When the densities of EDs and UEs are known or can be estimated, this result enables us to determine how many UEs (for a given ordering policy) can communicate securely via the BS⁴ by using TAS. It is clear that the secrecy outage probability corresponding to policy II is lower than that related to policy I, again as one might expect. In practice, however, policy II requires knowledge of the instantaneous BS-UE channel gains, which cannot always be estimated accurately. Policy I, however, is dependent only on distance, or equivalently long-term average BS-UE channel gains. Such information can be more easily obtained at the BS in practice.

V. CONCLUSION

In this paper, we proposed a method of enhancing secrecy in wireless networks with randomly located EDs and UEs. Two UE

⁴Here, security is measured in terms of the satisfaction of a target secrecy outage probability threshold, i.e., a 1% chance of secrecy outage.

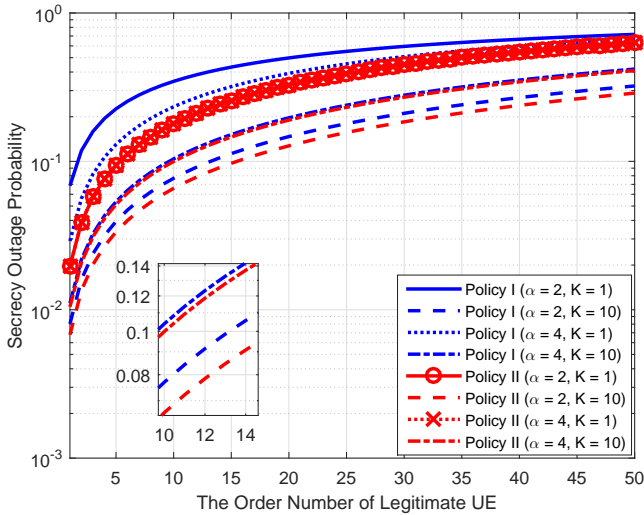


Fig. 3. The comparison of secrecy outage probabilities for the different UE ordinal indices, where $\rho_E = 0.01$, $\rho_U = 0.5 \text{ m}^{-2}$.

selection policies were analyzed: one requires only distance or long-term BS-UE channel gain information, whereas the other requires knowledge of instantaneous BS-UE SNR. TAS was incorporated into the model, and closed-form expressions for the secrecy outage probability for each ordering scheme were presented. These results were been confirmed by numerical simulations. Our results show that while TAS yields a performance improvement relative to single-antenna systems, the secrecy outage probability for TAS systems actually increases with the path loss exponent.

APPENDIX I

Firstly, based on the displacement theorem and mapping theorem for point process transformations [20], Ψ is also a PPP, because the point process of Ψ can be obtained from the PPP of $\phi_U = \{d_{BU_n}\}$ by a deterministic mapping and independent displacement. Then the intensity function of $\Lambda = \{\lambda = d_{BU_n}^\alpha\}$ can be calculated from $E[\Phi_U([0, x])] = \rho_U \pi x^2$ by mapping theorem

$$\rho_\Lambda(\lambda) = \frac{2\rho_U \pi \lambda^{\frac{2}{\alpha}-1}}{\alpha}. \quad (17)$$

We let $Y = \max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)$, and because all channels from each antenna at the BS are assumed to be i.i.d., the CDF of Y can be written as $F_Y(y) = (1 - e^{-y})^K$. Next, we use the displacement theorem to determine the intensity function Ψ . One UE of Φ_U at d_{BU_n} gets displaced to $x_n = \lambda/Y$; therefore,

$$\mathbb{P}(d_{BU_n}/Y < \psi) = 1 - F_Y(\lambda/\psi), \quad (18)$$

and the displacement kernel follows as

$$\rho(\lambda, \psi) = \frac{d}{dy} (1 - F_Y(\lambda/\psi)) = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{\lambda K}{\psi^2} e^{-\frac{(l+1)\lambda}{\psi}}. \quad (19)$$

Finally, by using the displacement theorem and (17), the intensity function of Ψ can be obtained as

$$\rho_\Psi(\psi) = \int_0^\infty \rho_\Lambda(\lambda) \rho(\lambda, \psi) d\lambda = \sum_{l=0}^{K-1} C_K^l (-1)^l \frac{2\pi\rho_U K \psi^{\frac{2}{\alpha}-1} \Gamma(\frac{2}{\alpha} + 1)}{\alpha(l+1)^{\frac{2}{\alpha}+1}}. \quad (20)$$

APPENDIX II

According to [20], the complementary CDF of $x_n = \frac{d_{BU_n}^\alpha}{\max_{k \in \{1, \dots, K\}} (|h_{B_k U_n}|^2)}$ is the probability that there are less than n nodes closer than x , which can be derived by using (20) to be

$$\begin{aligned} F_{x_n}(x) &= \mathbb{P}(x_n < x) = 1 - \mathbb{P}(\Psi[0, x] < n) \\ &= 1 - \sum_{i=0}^{n-1} \frac{e^{-\int_0^x \rho_\Psi(\psi) d\psi} (\int_0^x \rho_\Psi(\psi) d\psi)^i}{i!} \\ &= 1 - \sum_{i=0}^{n-1} e^{-A_u x^{\frac{2}{\alpha}}} \frac{(A_u x^{\frac{2}{\alpha}})^i}{i!}. \end{aligned} \quad (21)$$

The PDF of x_n , as given in (15), follows by differentiating (21).

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.
- [2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, June 2014.
- [3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Magazine*, vol. 53, pp. 20–27, April 2015.
- [4] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 2, pp. 242–256, June 2009.
- [5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, June 2009.
- [6] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.
- [7] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Apr. 2015.
- [8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.
- [9] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory, Toronto, Canada*, pp. 539–543, July 2008.
- [10] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Syst., Guangzhou, China*, pp. 974–979, Nov. 2008.
- [11] 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, pp. 2764–2775, Aug. 2011.
- [12] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 2931–2943, May 2014.
- [13] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, pp. 1299–1302, Aug. 2014.
- [14] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE ICC*, pp. 1–5, June 2011.
- [15] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. on Commun.*, vol. 63, pp. 4347–4362, Nov. 2015.
- [16] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks-part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics and Security*, vol. 7, pp. 139–147, Feb 2012.
- [17] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks-part I: Connectivity," *IEEE Trans. Inf. Forensics and Security*, vol. 7, pp. 125–138, Feb. 2012.
- [18] M. Haenggi, "Stochastic geometry for wireless networks," *Cambridge Univ. Press*, 2012.
- [19] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3584–3586, Oct 2005.
- [20] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inf. Theory*, vol. 54, pp. 5500–5510, Dec 2008.