Stochastic Geometry-Based Comparison of Secrecy Enhancement Techniques in D2D Networks

Mustafa A. Kishk and Harpreet S. Dhillon

***Abstract*—This letter presents a performance comparison of two popular secrecy enhancement techniques in wireless networks: 1) *creating guard zones* by restricting transmissions of legitimate transmitters whenever any eavesdropper is detected in their vicinity, and 2) *adding artificial noise* to the confidential messages to make it difficult for the eavesdroppers to decode them. Focusing on a noise-limited regime, we use tools from stochastic geometry to derive the secrecy outage probability at the eavesdroppers as well as the coverage probability at the legitimate users for both these techniques. Using these results, we derive a threshold on the density of the eavesdroppers below which no secrecy enhancing technique is required to ensure a target secrecy outage probability. For eavesdropper densities above this threshold, we concretely characterize the regimes in which each technique outperforms the other. Our results demonstrate that guard zone technique is better when the distances between the transmitters and their legitimate receivers are higher than a certain threshold.**

***Index Terms*—Stochastic geometry, physical layer security, Poisson point process, secrecy outage, coverage probability.**

I. Introduction

OWING to the broadcast nature of wireless networks, physical layer security techniques are necessary to preserve confidentiality of the transmitted messages [1]–[4]. Two popular secrecy enhancing techniques that have been investigated in the literature are: (i) *creating guard zones* by restricting transmissions of the legitimate transmitters whenever eavesdroppers are detected in their vicinity [1], and (ii) *adding artificial noise* to the confidential messages to make it difficult for the eavesdroppers to decode them [2]. Despite the attention received by these techniques, to the best of our knowledge their explicit system-level performance comparison is still an open problem, which is the main focus of this letter.

The system-level analysis of wireless networks usually requires averaging the performance metric of interest over all possible topologies of the network. While this has traditionally been performed through Monte-Carlo trials, stochastic geometry has recently emerged as an attractive analytic alternative due to its remarkable tractability [5]. In fact, stochastic geometry has also gained popularity in the past few years for the system-level analysis of D2D networks, see [6]–[8], as well as physical layer security, see [1], [9]. In particular, [1] quantified the loss in system throughput that results from ensuring a specific level of secrecy in decentralized wireless networks. Similarly, [9] studied physical layer security in downlink cellular networks assuming the downlink messages meant for each user can be eavesdropped by all other users (both intra- and inter-cell) in the network.

In this letter, we will use tools from stochastic geometry for the comparison of secrecy enhancing techniques. In addition to the two techniques introduced already, namely, creating guard zones and adding artificial noise, there are two other techniques usually considered in the literature: (i) *protected zones*, and (ii) *beamforming*. Protected zones are similar to the guard zones defined earlier in this section, except that they are guaranteed to be free of eavesdroppers (physically enforced) [3]. If one assumes multi-antenna nodes, beamforming is also an attractive solution for enhancing secrecy [4]. In this letter, we consider a system with single-antenna nodes in which we do not have control over the physical removal of eavesdroppers, as a result of which we focus only on the first two techniques (guard zones and artificial noise).

Contributions: We consider a device-to-device (D2D) network that coexists with a network of eavesdroppers modeled by an independent Poisson point process (PPP). For this setup, focusing on the noise-limited regime, we first derive the secrecy outage probability at the eavesdroppers and coverage probability at the legitimate receivers for the two secrecy enhancement techniques considered in this letter. Using these results, we characterize the maximum density of eavesdroppers below which no secrecy enhancing technique is required to ensure the target secrecy outage probability. For eavesdropper densities above this threshold, we concretely characterize the regimes in which a given technique outperforms the other, which leads to useful system design insights.

II. System Model

Focusing on the noise-limited regime, we consider a primary D2D link coexisting with a secondary network of potential eavesdroppers modeled as an independent PPP $\Phi_e \equiv \{y_i\} \subset \mathbb{R}^2$ with density λ_e. The D2D link is formed by a primary transmitter (PT) located at the origin and a primary receiver (PR) located at a fixed distance d from the PT (at an arbitrary angle from the origin). We assume independent Rayleigh fading on all wireless links. The PT is assumed to transmit at a fixed power P_t. For this setup, the received power at the PR associated with the PT is $P_t h \|d\|^{-\alpha}$, where $h \sim \exp(1)$ models Rayleigh fading, $\|d\|^{-\alpha}$ is the standard power-law path-loss with exponent $\alpha > 2$. Similarly, the received power at an arbitrary eavesdropper located at $y \in \Phi_e$ from the PT is $P_t g_y \|y\|^{-\alpha}$, where $g_y \sim \exp(1)$ models Rayleigh fading. For the secrecy outage analysis, we will need to analyze the performance of eavesdroppers that have the best

Manuscript received January 1, 2017; revised March 12, 2017; accepted April 11, 2017. Date of publication April 24, 2017; date of current version June 19, 2017. This work was supported by the U.S. NSF under Grant CCF-1464293 and Grant CNS-1617896. The associate editor coordinating the review of this paper and approving it for publication was M. Li. *(Corresponding author: Harpreet S. Dhillon.)*

The authors are with the Wireless@VT, Department of ECE, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: mkishk@vt.edu; hdhillon@vt.edu).

Digital Object Identifier 10.1109/LWC.2017.2696537

chance of decoding the messages from the PT. The location of this *strongest* eavesdropper corresponding to the PT is:

$$y^* = \arg\max_{y \in \Phi_e} g_y \|y\|^{-\alpha}. \tag{1}$$

According to Wyner encoding scheme [10], the transmitter chooses a rate of codeword transmission $\mathcal{C}_t$ and a rate of confidential message transmission $\mathcal{C}_s$. The rate difference, $\mathcal{C}_e = \mathcal{C}_t - \mathcal{C}_s$, represents the cost of securing the confidential message where perfect secrecy is achieved as long as mutual information between the PT and the eavesdropper is lower than $\mathcal{C}_e$. Please refer to [11, Sec. II-B] for further details on Wyner encoding scheme. As is usually the case in the literature, e.g., see [3], we assume a noise-limited scenario for analytical tractability. Therefore, in order to ensure successful decoding at the PR, we need to satisfy the condition $\log_2(1+\mathrm{SNR_P}) \geq \mathcal{C}_t$, where $\mathrm{SNR_P}$ is the SNR achieved at the PR. On the other hand, to ensure perfect secrecy we require $\log_2(1+\mathrm{SNR_S}) \leq \mathcal{C}_e$ at the eavesdropper located at y^*, where $\mathrm{SNR_S}$ is the SNR at the eavesdropper. Equivalently, we can define two thresholds $\beta_t = 2^{\mathcal{C}_t} - 1$ and $\beta_e = 2^{\mathcal{C}_e} - 1$ on $\mathrm{SNR_P}$ and $\mathrm{SNR_S}$ respectively. For this setup, we now define two main performance metrics that will be used in this letter.

Definition 1 (Coverage Probability): The SNR coverage probability at the PR is defined as

$$P_{\mathrm{cov}} = \mathbb{P}(\mathrm{SNR_P} \geq \beta_t, \delta_a = 1), \tag{2}$$

where $\delta_a = 1$ if the PT is transmitting information (referred to as an active PT), and $\delta_a = 0$ otherwise.

Definition 2 (Secure Communication Probability [12]): It is the probability of perfect secrecy of the confidential message from the PT (conditioned on the fact that PT is active):

$$P_{\mathrm{sec}} = \mathbb{P}(\mathrm{SNR_S} \leq \beta_e | \delta_a = 1) \tag{3}$$

Our main objective is to maximize the SNR coverage probability at the PR while ensuring that the secure communication probability is above a predefined threshold ϵ.

III. Secrecy Enhancing Techniques

A. Guard Zone Technique

In this technique, a given PT is allowed to transmit confidential messages to its paired PR only if there are no eavesdroppers in a circular *guard zone* of radius r_g around it. Therefore, the probability that the PT is active is:

$$P_{\mathrm{active}} = \mathbb{P}(\delta_a = 1) = \mathbb{P}\big(\mathcal{N}\big(\mathcal{B}(o, r_g)\big) = 0\big) = e^{-\lambda_e \pi r_g^2}, \tag{4}$$

where $\mathcal{N}(\mathcal{B}(o, r_g))$ is the number of eavesdroppers inside a ball of radius r_g centered at the origin. Owing to the independence of $\mathrm{SNR_P}$ and $\mathcal{N}(\mathcal{B}(o, r_g))$, the SNR coverage probability for the D2D link is defined as:

$$\begin{aligned} P_{\mathrm{cov}}^{GZ} &= P_{\mathrm{active}} \mathbb{P}(\mathrm{SNR_P} \geq \beta_t) = P_{\mathrm{active}} \mathbb{P}\left(\frac{P_t \|d\|^{-\alpha} h}{\sigma_P^2} \geq \beta_t\right) \\ &\overset{(a)}{=} P_{\mathrm{active}} \exp\left(-\frac{\beta_t \sigma_P^2 \|d\|^{\alpha}}{P_t}\right) \\ &= \exp\left(-\lambda_e \pi r_g^2 - \frac{\beta_t \sigma_P^2 \|d\|^{\alpha}}{P_t}\right), \end{aligned} \tag{5}$$

where σ_P^2 is the noise power at the PT and step (a) follows from $h \sim \exp(1)$. Now we derive secure communication probability for this technique for which we focus on the SNR achieved at the strongest eavesdropper located at y^* (as defined in Eq. (1)), which can be defined as $\mathrm{SNR_S} = \frac{P_t g_{y^*} \|y^*\|^{-\alpha}}{\sigma_S^2}$. The secure communication probability is given in the next Lemma.

Lemma 1 (Secure Communication Probability): The secure communication probability for the guard zone technique is

$$\begin{aligned} P_{\mathrm{sec}}^{GZ} &= \mathbb{P}\left(\frac{P_t g_{y^*} \|y^*\|^{-\alpha}}{\sigma_S^2} \leq \beta_e \middle| \mathcal{N}(\mathcal{B}(o, r_g)) = 0\right) \\ &= \exp\left(-\frac{2\pi\lambda_e}{\alpha}\left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}} \Gamma\left(\frac{2}{\alpha}, \frac{r_g^{\alpha} \beta_e \sigma_S^2}{P_t}\right)\right), \end{aligned} \tag{6}$$

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

Proof: See Appendix A. ■

As evident from Eq. (5), P_{cov}^{GZ} is a decreasing function of r_g. On the other hand, as noted from Eq. (6), the value of P_{sec}^{GZ} is an increasing function of r_g. Hence, the optimum value r_g^* is the minimum guard zone radius that ensures $P_{\mathrm{sec}}^{GZ} \geq \epsilon$. The value of r_g^* is derived next.

Lemma 2 (Optimal Guard Zone Radius): The value of r_g^* that maximizes P_{cov}^{GZ} while satisfying the condition of $P_{\mathrm{sec}}^{GZ} \geq \epsilon$ is the one that satisfies the following equation:

$$\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^{\alpha} \beta_e \sigma_S^2}{P_t}\right) = \min\left\{\frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}}, \Gamma\left(\frac{2}{\alpha}\right)\right\} \tag{7}$$

Proof: Substituting the expression of P_{sec}^{GZ} from Eq. (6) in $P_{\mathrm{sec}}^{GZ} \geq \epsilon$, we get $\Gamma(\frac{2}{\alpha}, \frac{r_g^{\alpha} \beta_e \sigma_S^2}{P_t}) \leq \frac{\alpha \log(\frac{1}{\epsilon})}{2\pi\lambda_e(\frac{P_t}{\sigma_S^2 \beta_e})^{\frac{2}{\alpha}}}$. Now if $r_g = 0$ satisfies this inequality, then $r_g^* = 0$ and $\Gamma(\frac{2}{\alpha}, \frac{(r_g^*)^{\alpha} \beta_e \sigma_S^2}{P_t}) = \Gamma(\frac{2}{\alpha})$. Otherwise, the minimum value for r_g^* that satisfies this inequality follows from $\Gamma(\frac{2}{\alpha}, \frac{(r_g^*)^{\alpha} \beta_e \sigma_S^2}{P_t}) = \frac{\alpha \log(\frac{1}{\epsilon})}{2\pi\lambda_e(\frac{P_t}{\sigma_S^2 \beta_e})^{\frac{2}{\alpha}}}$. Combining the results for these two cases leads to the final result in Eq. (7). ■

B. Artificial Noise Technique

In this secrecy enhancing technique, the transmission power P_t is split into two parts: (i) γP_t, which is used for the transmission of confidential information, and (ii) $(1-\gamma)P_t$, which is used to transmit artificial noise (AN). The AN is generated by using random sequences, which can only be decoded using the keys available at the PRs. Since eavesdroppers do not have access to these keys, they cannot decode AN. Hence, the SNR achieved at the PR is $\mathrm{SNR_P} = \frac{\gamma P_t h \|d\|^{-\alpha}}{\sigma_P^2}$. Please note that unlike the guard zone technique, the PT in this technique is always active, i.e., we have $\delta_a = 1$. Hence, the probability of SNR coverage at the PR can be derived as follows:

$$P_{\mathrm{cov}}^{AN} = \mathbb{P}(\mathrm{SNR_P} \geq \beta_t) \overset{(b)}{=} \exp\left(-\frac{\beta_t \sigma_P^2 \|d\|^{\alpha}}{\gamma P_t}\right), \tag{8}$$

where (b) follows from $h \sim \exp(1)$. On the other hand, we assume that the eavesdropper is unable to decode the AN, which implies that the SNR at the eavesdropper located at y^* is $\mathrm{SNR_S} = \frac{\gamma P_t g_{y^*} \|y^*\|^{-\alpha}}{(1-\gamma) P_t g_{y^*} \|y^*\|^{-\alpha} + \sigma_S^2}$. Hence, the secure communication probability can be derived as follows:

$$\begin{aligned} P_{\mathrm{sec}}^{AN} &= \mathbb{P}\left(\frac{\gamma P_t g_{y^*} \|y^*\|^{-\alpha}}{(1-\gamma) P_t g_{y^*} \|y^*\|^{-\alpha} + \sigma_S^2} \leq \beta_e\right) \\ &\overset{(c)}{=} \mathbb{P}\left(\frac{(\gamma - (1-\gamma)\beta_e) P_t g_{y^*} \|y^*\|^{-\alpha}}{\sigma_S^2} \leq \beta_e\right), \end{aligned} \tag{9}$$

where step (c) results from simple manipulations of the inequality. This implies that $P_{\text{sec}}^{AN} = 1$ as long as $\gamma \leq \frac{\beta_e}{1+\beta_e}$. When $\gamma > \frac{\beta_e}{1+\beta_e}$, we can derive a closed-form expression for P_{sec}^{AN} by replacing β_e with $\frac{\beta_e}{\gamma-(1-\gamma)\beta_e}$ and $r_g = 0$ in Eq. (6). This provides the following closed-form expression for P_{sec}^{AN}:

$$P_{\text{sec}}^{AN} = \exp\left(-\frac{2\pi\lambda_e}{\alpha}\left(\frac{P_t(\gamma-(1-\gamma)\beta_e)}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}\Gamma\left(\frac{2}{\alpha}\right)\right). \tag{10}$$

Since the power used for information transmission is directly proportional to γ, P_{cov}^{AN} is an increasing function of γ, which is evident from Eq. (8). On the other hand, since the power used for transmitting AN is directly proportional to $1-\gamma$, P_{sec}^{AN} decreases with increase in γ, which is evident from Eq. (10). Therefore, the optimum value of γ^* is the maximum value of γ that ensures $P_{\text{sec}}^{AN} \geq \epsilon$. This optimal γ^* is derived in the following Lemma.

Lemma 3 (Optimal Power Split): The value of γ^* that maximizes P_{cov}^{AN} while satisfying the condition $P_{\text{sec}}^{AN} \geq \epsilon$ is

$$\gamma^* = \min\left\{1, \frac{\beta_e}{1+\beta_e}\left(1+\frac{\sigma_S^2}{P_t}\left(\frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\Gamma\left(\frac{2}{\alpha}\right)}\right)^{\frac{\alpha}{2}}\right)\right\}. \tag{11}$$

Proof: The result follows by substituting Eq. (10) in the inequality $P_{\text{sec}}^{AN} \geq \epsilon$, and following similar approach as in the proof of Lemma 2. ■

IV. Performance Comparison

A. Useful Threshold on the Density of Eavesdroppers

In this subsection, we first aim to find the threshold on λ_e below which the secrecy enhancing techniques are not required ($r_g^* = 0$ and $\gamma^* = 1$). Note that when $r_g^* = 0$ and $\gamma^* = 1$ the performance is the same for both techniques: $P_{\text{cov}}^{GZ} = P_{\text{cov}}^{AN}$ and $P_{\text{sec}}^{GZ} = P_{\text{sec}}^{AN}$. For the guard zone technique, we can derive this threshold by solving the following inequality:

$$\Gamma\left(\frac{2}{\alpha}\right) \leq \frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}}, \tag{12}$$

where this inequality ensures that the result of Eq. (7) is $r_g^* = 0$. Solving this inequality, we deduce that $r_g^* = 0$ as long as

$$\lambda_e \leq \frac{\alpha}{2\pi\Gamma\left(\frac{2}{\alpha}\right)}\log\left(\frac{1}{\epsilon}\right)\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{-\frac{2}{\alpha}}. \tag{13}$$

Similarly, for the artificial noise technique, we can derive this threshold on λ_e by solving the following inequality:

$$\frac{\beta_e}{1+\beta_e}\left(1+\frac{\sigma_S^2}{P_t}\left(\frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\Gamma\left(\frac{2}{\alpha}\right)}\right)^{\frac{\alpha}{2}}\right) \geq 1, \tag{14}$$

where the above inequality ensures that the result of Eq. (11) is $\gamma^* = 1$. Solving the above inequality, we infer that artificial noise addition is not required as long as

$$\lambda_e \leq \frac{\alpha}{2\pi\Gamma\left(\frac{2}{\alpha}\right)}\log\left(\frac{1}{\epsilon}\right)\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{-\frac{2}{\alpha}}. \tag{15}$$

As can be expected intuitively, the threshold on λ_e derived in Eq. (13) and Eq. (15) for the two techniques is the same. We denote this threshold by λ_e^*. As long as $\lambda_e < \lambda_e^*$, the secure communication probability is guaranteed to be above ϵ.

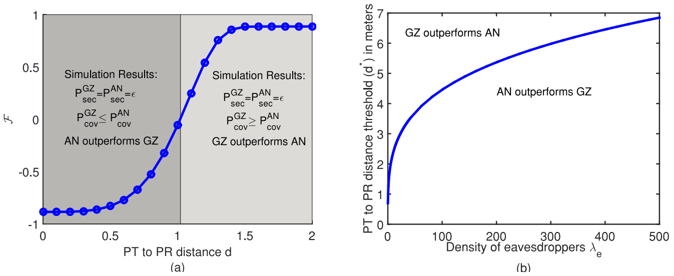

Fig. 1. (a) Technique selection function $\mathcal{F}$ as a function of d, and (b) PT to PR distance threshold d^* for different values of λ_e.

B. Comparison of Secrecy Enhancement Techniques

In this subsection, we focus on $\lambda_e \geq \lambda_e^*$ for which secrecy enhancement techniques are required to ensure desired secrecy performance level. In particular, we will characterize regimes in which a given technique outperforms the other. Since both techniques select their parameters (r_g^* or γ^*) in order to ensure that $P_{\text{sec}} \geq \epsilon$, optimal parameter choices will naturally satisfy the desired secrecy conditions. As a result, we focus our comparison on the other system performance metric: P_{cov}^{GZ} and P_{cov}^{AN}. Hence, for $\lambda_e \geq \lambda_e^*$, a given secrecy technique is said to perform better than the other if it provides higher coverage probability at the PR while ensuring $P_{\text{sec}} \geq \epsilon$. In the following theorem, we characterize the regimes in which a given secrecy enhancing technique outperforms the other.

Theorem 1 (Secrecy Enhancement Technique Selection): Defining the functions $\mathcal{F}$, $\mathcal{H}$, and $\mathcal{G}$ as

$$\mathcal{F} = \frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}} - \Gamma\left(\frac{2}{\alpha}, \mathcal{H}\right) \tag{16}$$

$$\mathcal{H} = \frac{\beta_e\sigma_S^2}{P_t}\left[\frac{\beta_t d^\alpha\sigma_S^2}{P_t\lambda_e\pi}\left(\frac{1}{\mathcal{G}}-1\right)\right]^{\frac{\alpha}{2}} \tag{17}$$

$$\mathcal{G} = \frac{\beta_e}{1+\beta_e}\left(1+\frac{\sigma_S^2}{P_t}\left(\frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\Gamma\left(\frac{2}{\alpha}\right)}\right)^{\frac{\alpha}{2}}\right), \tag{18}$$

the guard zone technique is a better choice as long as $\mathcal{F} > 0$, while artificial noise technique is a better choice when $\mathcal{F} \leq 0$.

Proof: See Appendix B. ■

Remark 1: Observing the dependence of $\mathcal{F}$ on D2D link distance d in Eq. (16), we note that the value of d plays an important role in determining which technique performs better. Since $\mathcal{F}$ is an increasing function of d, it is easy to conclude that for a given set of system parameters, the artificial noise technique provides better performance at lower values of d, while the guard zone technique starts performing better when d exceeds a specific threshold. These comments will be verified next in the numerical results section.

C. Numerical Results

For numerical comparisons, we consider the following system parameters: $\alpha = 4$, $P_t = 1$, $\beta_t = 2$, $\beta_e = 1$, $\epsilon = 0.9$, $\sigma_P^2 = 1$, and $\sigma_S^2 = 1$. For this setup, $\lambda_e^* = 0.0378$ because of which we choose $\lambda_e = 0.1 > \lambda_e^*$. In Fig. 1.a, we use Monte-Carlo simulations to evaluate the values of $P_{\rm sec}^{GZ}$, $P_{\rm sec}^{AN}$, $P_{\rm cov}^{GZ}$, and $P_{\rm cov}^{AN}$ to determine which technique is better at different values of d. On the same figure, we plot the function $\mathcal{F}$ derived in Theorem 1. The comparison of the simulation and analytical results supports the main consequence of our analysis that the guard zone technique is a better choice when $\mathcal{F} > 0$ while the artificial noise technique is a better choice when $\mathcal{F} \leq 0$. In addition, our comment in Remark 1 that artificial noise technique is better for lower values of d is verified. It is clear from this comparison that the value of d at which $\mathcal{F}$ switches from being negative to positive is critical to the choice of the secrecy enhancement technique. We refer to this threshold value of d as d^*. In Fig. 1.b, we study the effect of λ_e on d^*. The resulting curve partitions the (d^*, λ_e) plane into two parts: lower part in which AN outperforms GZ and the upper part in which GZ outperforms AN. We notice that with increasing λ_e, d^* increases, which means AN starts becoming optimal choice for a larger range of values for d.

V. Conclusion

In this letter, we provided a concrete performance comparison of two popular secrecy enhancement techniques: (i) creating guard zones around legitimate transmitters, and (ii) adding artificial noise to the confidential messages. Using tools from stochastic geometry, we first derived a closed-form expression for the threshold on the density of eavesdroppers below which no secrecy enhancement techniques are required. For densities greater than this threshold, we characterized regimes in which a given secrecy enhancement technique outperforms the other. Our results demonstrate that guard zone technique is a better choice when the distances between the D2D pairs are higher than a specific threshold.

A key technical extension for this line of work is the inclusion of interference in the analysis. This requires a significantly more complicated analysis due to spatial correlation between interference levels at the PR and the eavesdropper which requires joint analysis of coverage probability at the PR and secure communication probability at the eavesdropper.

Appendix A
Proof of Lemma 1

By definition, the secure communication probability is

$$\begin{aligned} P_{\rm sec}^{GZ} &= \mathbb{P}\left(\frac{P_t}{\sigma_S^2}\max_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\{g_y\|y\|^{-\alpha}\} \leq \beta_e\right) \\ &\overset{(a)}{=} \mathbb{E}_{\Phi_e}\left[\prod_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\mathbb{P}\left(g_y \leq \|y\|^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}\Big|\Phi_e\right)\right] \\ &\overset{(b)}{=} \mathbb{E}_{\Phi_e}\left[\prod_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\left(1-e^{-\|y\|^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}}\right)\right] \\ &\overset{(c)}{=} \exp\left(-2\pi\lambda_e\int_{r_g}^{\infty}e^{-r_y^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}}r_y{\rm d}r_y\right), \end{aligned} \tag{19}$$

where $\mathcal{B}(0, r_g)^c$ is the compliment of the area covered by the ball centered at the origin with radius r_g. Step (a) follows from the independence of g_y across all wireless links, (b) is due to $g_y \sim \exp(1)$, (c) follows from applying PGFL of PPP and converting to polar coordinates. With simple algebraic manipulations, the final result presented in Lemma 1 follows.

Appendix B
Proof of Theorem 1

Technique selection is done using the following inequality:

$$\begin{aligned} P_{\rm cov}^{GZ}\underset{AN}{\overset{GZ}{\gtrless}}P_{\rm cov}^{AN} &\Rightarrow \exp\left(-\lambda_e\pi r_g^{*2}-\frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{P_t}\right)\underset{AN}{\overset{GZ}{\gtrless}}\exp\left(-\frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{\gamma^*P_t}\right) \\ &\Rightarrow \frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{\gamma^*P_t}\underset{AN}{\overset{GZ}{\gtrless}}\lambda_e\pi r_g^{*2}+\frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{P_t} \\ &\Rightarrow \frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{P_t}\left(\frac{1}{\gamma^*}-1\right)\underset{AN}{\overset{GZ}{\gtrless}}\lambda_e\pi r_g^{*2} \end{aligned} \tag{20}$$

Since $\lambda_e \geq \lambda_e^*$, then $\Gamma(\frac{2}{\alpha}, \frac{(r_g^*)^{\alpha}\beta_e\sigma_S^2}{P_t}) = \frac{\alpha\log(\frac{1}{\epsilon})}{2\pi\lambda_e(\frac{P_t}{\sigma_S^2\beta_e})^{\frac{2}{\alpha}}}$ and $\gamma^* = \mathcal{G} = \frac{\beta_e}{1+\beta_e}(1+\frac{\sigma_S^2}{P_t}(\frac{\alpha\log(\frac{1}{\epsilon})}{2\pi\lambda_e\Gamma(\frac{2}{\alpha})})^{\frac{\alpha}{2}})$. Substituting this in Eq. (20), we get:

$$\begin{aligned} &\frac{\beta_e\sigma_S^2}{P_t}\left(\frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{\lambda_e\pi P_t}\left(\frac{1}{\gamma^*}-1\right)\right)^{\frac{\alpha}{2}}\underset{AN}{\overset{GZ}{\gtrless}}\frac{(r_g^*)^{\alpha}\beta_e\sigma_S^2}{P_t} \\ &\Rightarrow \Gamma\left(\frac{2}{\alpha},\frac{(r_g^*)^{\alpha}\beta_e\sigma_S^2}{P_t}\right)\underset{AN}{\overset{GZ}{\gtrless}}\Gamma\left(\frac{2}{\alpha},\mathcal{H}\right) \end{aligned} \tag{21}$$

$$\Rightarrow \frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}}\underset{AN}{\overset{GZ}{\gtrless}}\Gamma\left(\frac{2}{\alpha},\mathcal{H}\right)\Rightarrow\mathcal{F}\underset{AN}{\overset{GZ}{\gtrless}}0, \tag{22}$$

where (21) follows by substituting $\gamma^* = \mathcal{G}$ and substituting for $\mathcal{H}$ as defined in Theorem 1 and taking Γ on both sides, while (22) follows by substituting for $\mathcal{F}$ as defined in Theorem 1. This concludes the proof.

References

[1] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "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.

[2] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[3] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[4] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.

[5] J. G. Andrews, A. K. Gupta, and H. S. Dhillon. (2016). *A Primer on Cellular Network Analysis Using Stochastic Geometry*. [Online]. Available: arxiv.org/abs/1604.03183

[6] H. Sun, M. Wildemeersch, M. Sheng, and T. Q. S. Quek, "D2D enhanced heterogeneous cellular networks with dynamic TDD," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4204–4218, Aug. 2015.

[7] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1867–1880, May 2015.

[8] M. Afshang, H. S. Dhillon, and P. H. J. Chong, "Modeling and performance analysis of clustered device-to-device networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4957–4972, Jul. 2016.

[9] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[11] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[12] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.