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: (i) creating guard zones by restricting transmissions of legitimate transmitters whenever a eavesdropper is detected in their vicinity, and (ii) 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, e.g., see [6]–[8], as well as physical layer security, e.g., 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 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 $\lambda_e$. 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 chance of decoding the messages from the PT. The location of this strongest eavesdropper corresponding to the PT is:

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

According to Wyner encoding scheme [10], the transmitter chooses a rate of codeword transmission $C_t$ and a rate of confidential message transmission $C_s$. The rate difference, $C_e = C_t - C_s$, 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 $C_e$. Please refer to Sec. II-B in [11] 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 $\log_2 (1 + \text{SNR}_P) \geq C_e$, where SNR$_P$ is the SNR achieved at the PR. On the other hand, to ensure perfect secrecy we require $\log_2 (1 + \text{SNR}_S) \leq C_e$ at the eavesdropper located at $y^*$, where SNR$_S$ is the SNR at the eavesdropper. Equivalently, we can define two thresholds $\beta_t = 2^{C_e} - 1$ and $\beta_s = 2^{C_s} - 1$ on SNR$_P$ and SNR$_S$ respectively. For this setup, we now define two main performance metrics that will be used in this work.

**Definition 1** (Coverage probability). The SNR coverage probability at the PR is defined as

$$P_{\text{cov}} = \mathbb{P}(\text{SNR}_P \geq \beta_t, \delta_a = 1),$$

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):

$$P_{\text{sec}} = \mathbb{P}(\text{SNR}_S \leq \beta_s | \delta_a = 1)$$

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 $\epsilon$.

**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:

$$P_{\text{active}} = \mathbb{P}(\delta_a = 1) = \mathbb{P}(\mathcal{N}(B(o, r_g)) = 0) = e^{-\lambda_c \pi r_g^2},$$

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

$$P_{\text{cov}}^G = P_{\text{active}} \mathbb{P}(\text{SNR}_P \geq \beta_t) = P_{\text{active}} \mathbb{P} \left( \frac{P_t}{\sigma_P^2} ||d||^{-\alpha} h \geq \beta_t \right) \quad \overset{(a)}{=} P_{\text{active}} \exp \left( -\beta_t \frac{\sigma_P^2 ||d||^\alpha}{P_t} \right) = \exp \left( -\lambda_c \pi r_g^2 - \beta_t \frac{\sigma_P^2 ||d||^\alpha}{P_t} \right),$$

where $\sigma_P^2$ 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 SNR$_S = \frac{P_t g_{o,y^*} ||y^*||^{-\alpha}}{\sigma_S^2}$. 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

$$P_{\text{sec}}^G = \mathbb{P} \left( \frac{P_t g_{o,y^*} ||y^*||^{-\alpha}}{\sigma_S^2} \leq \beta_s | \mathcal{N}(B(o, r_g)) = 0 \right) = \exp \left( -\frac{2 \lambda_c}{\alpha} \left( \frac{P_t}{\sigma_P^2} \right)^{\frac{\alpha}{2}} \Gamma \left( \frac{2}{\alpha}, \frac{2 \beta_s \sigma_P^2}{P_t} \right) \right),$$

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

**Proof:** See Appendix A.

As evident from Eq. 3, $P_{\text{cov}}^G$ is a decreasing function of $r_g$. On the other hand, as noted from Eq. 6 the value of $P_{\text{sec}}^G$ is an increasing function of $r_g$. Hence, the optimum value $r_g^*$ is the minimum guard zone radius that ensures $P_{\text{sec}}^G \geq \epsilon$. The value of $r_g^*$ is derived next.

**Lemma 2** (Optimal guard zone radius). The value of $r_g^*$ that maximizes $P_{\text{cov}}^G$ while satisfying the condition of $P_{\text{sec}}^G \geq \epsilon$ is the one that satisfies the following equation:

$$\Gamma \left( \frac{2}{\alpha}, \frac{(r_g^*)^2 \lambda_c}{P_t} \right) = \min \left\{ \frac{\alpha \log \left( \frac{1}{\epsilon} \right)}{2 \lambda_c}, \Gamma \left( \frac{2}{\alpha}, \frac{(r_g^*)^2 \lambda_c}{P_t} \right) \right\}.$$

**Proof:** Substituting the expression of $P_{\text{cov}}^G$ from Eq. 6 in $P_{\text{sec}}^G \geq \epsilon$, we get $\Gamma \left( \frac{2}{\alpha}, \frac{(r_g^*)^2 \lambda_c}{P_t} \right) \leq \frac{\alpha \log \left( \frac{1}{\epsilon} \right)}{2 \lambda_c \sigma_P^2} \frac{2 \lambda_c}{\sigma_S^2}$. 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) $\gamma P_t$, 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 $\text{SNR}_P = \frac{\gamma P_t h ||d||^{-\alpha}}{\sigma_P^2}$. 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:

$$P_{\text{cov}}^A = \mathbb{P}(\text{SNR}_P \geq \beta_t) = \exp \left( -\beta_t \frac{\sigma_P^2 ||d||^\alpha}{\gamma P_t} \right),$$

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 the SNR at the eavesdropper located at $y^*$ is $\text{SNR}_S = \frac{\gamma P_t g_{o,y^*} ||y^*||^{-\alpha}}{(1 - \gamma) P_t g_{o,y^*} ||y^*||^{-\alpha} + \sigma_S^2}$. Hence, the secure communication probability can be derived as follows:

$$P_{\text{sec}}^A = \mathbb{P} \left( \frac{\gamma P_t g_{o,y^*} ||y^*||^{-\alpha}}{(1 - \gamma) P_t g_{o,y^*} ||y^*||^{-\alpha} + \sigma_S^2} \leq \beta_s \right) \quad \overset{(c)}{=} \mathbb{P} \left( \gamma - (1 - \gamma) \beta_s \frac{P_t g_{o,y^*} ||y^*||^{-\alpha}}{\sigma_S^2} \leq \beta_s \right),$$

where step (c) results from simple manipulations of the inequality. This implies that $P_{\text{sec}}^A = 1$ as long as $\gamma \leq \frac{\beta_s}{1 + \beta_s}$. When $\gamma > \frac{\beta_s}{1 + \beta_s}$, we can derive a closed-form expression for
\[ P_{AN}^{\sec} \] by replacing \( \beta_c \) with \( \frac{\beta_e}{\gamma(1-\gamma)\beta_c} \) and \( r_g = 0 \) in Eq. 6. This provides the following closed-form expression for \( P_{AN}^{\sec} \):
\[
P_{AN}^{\sec} = \exp \left( -\frac{2\pi\lambda_e}{\alpha} \left( \frac{P_t(1 - (1-\gamma)\beta_e)}{\sigma^2_\beta e} \right)^{\frac{1}{2}} \Gamma \left( \frac{2}{\alpha} \right) \right).
\]

(10)

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

**Lemma 3** (Optimal power split), The value of \( \gamma^* \) that maximizes \( P_{cov}^{AN} \) while satisfying the condition \( P_{AN}^{\sec} \geq \epsilon \) is
\[
\gamma^* = \min \left\{ 1, \frac{\beta_e}{1 + \beta_e} \left( 1 + \frac{\sigma^2_\beta e}{P_t} \left( \alpha \log \left( \frac{1}{\epsilon} \right) \right)^{\frac{1}{2}} \right) \right\}.
\]

(11)

**Proof:** The result follows by substituting Eq. 10 in the inequality \( P_{AN}^{\sec} \geq \epsilon \), 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 \( \lambda_e \) below which the secrecy enhancing techniques are not required \((r_g^* = 0 \text{ and } \gamma^* = 1)\). Note that when \( r_g^* = 0 \) and \( \gamma^* = 1 \) the performance is the same for both techniques: \( P_{cov}^{GZ} = P_{cov}^{AN} \) and \( P_{sec}^{GZ} = P_{sec}^{AN} \). For the guard zone technique, we can derive this threshold by solving the following inequality:
\[
\Gamma \left( \frac{2}{\alpha} \right) \leq \frac{\alpha \log \left( \frac{1}{\epsilon} \right)}{2\pi\lambda_e \left( \frac{P_t}{\sigma^2_\beta e} \right)}
\]
\[
\text{where this inequality ensures that the result of Eq. 7 is } r_g^* = 0.
\]
Solving this inequality, we deduce that \( r_g^* \) as long as
\[
\lambda_e \leq \frac{\alpha}{2\pi} \log \left( \frac{1}{\epsilon} \right) \left( \frac{P_t}{\sigma^2_\beta e} \right)^{-\frac{1}{2}}.
\]

(13)

Similarly, for the artificial noise technique, we can derive this threshold on \( \lambda_e \) by solving the following inequality:
\[
\frac{\beta_e}{1 + \beta_e} \left( 1 + \frac{\sigma^2_\beta e}{P_t} \left( \alpha \log \left( \frac{1}{\epsilon} \right) \right)^{\frac{1}{2}} \right) \geq 1,
\]
\[
\text{where the above inequality ensures that the result of Eq. 11 is } \gamma^* = 1.
\]
Solving the above inequality, we infer that artificial noise addition is not required as long as
\[
\lambda_e \leq \frac{\alpha}{2\pi} \log \left( \frac{1}{\epsilon} \right) \left( \frac{P_t}{\sigma^2_\beta e} \right)^{-\frac{1}{2}}.
\]

(15)

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

**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 \((r_g^* \text{ or } \gamma^*)\) in order to ensure that \( P_{sec} \geq \epsilon \), 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 \( P_{sec} \geq \epsilon \). 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 \( F \), \( H \), and \( G \) as
\[
F = \frac{\alpha \log \left( \frac{1}{\epsilon} \right)}{2\pi\lambda_e \left( \frac{P_t}{\sigma^2_\beta e} \right)} - \Gamma \left( \frac{2}{\alpha} \right)
\]
\[
H = \beta_e \frac{P_t}{\sigma^2_\beta e} \beta_e \left( \frac{1}{g_e} - 1 \right)^{\frac{1}{2}}
\]
\[
G = \beta_e \frac{P_t}{\sigma^2_\beta e} \left( \frac{\alpha \log \left( \frac{1}{\epsilon} \right)}{2\pi\lambda_e \Gamma \left( \frac{2}{\alpha} \right)} \right)^{\frac{1}{2}}
\]
the guard zone technique is a better choice as long as \( F > 0 \), while artificial noise technique is a better choice when \( F \leq 0 \).

**Proof:** See Appendix B

**Remark 1**. Observing the dependence of \( F \) on 2D link distance \( d \) in Eq. 16, we note that the value of \( d \) plays an important role in determining which technique performs better. Since \( F \) 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: \( \alpha = 4, P_t = 1, \beta_e = 2, \beta_c = 1, \epsilon = 0.9, \sigma^2_\beta = 1, \) and \( \sigma^2_\beta = 1 \). For this setup, \( \lambda_e^* = 0.0378 \) because of which we choose \( \lambda_e = 0.1 > \lambda_e^* \). In Fig. 1a, we use Monte-Carlo simulations to evaluate the values of \( P_{sec}^{GZ}, P_{sec}^{AN}, P_{cov}^{GZ}, \) and \( P_{cov}^{AN} \) to determine which technique is better at different values of \( d \). On the same figure, we plot the function \( F \) 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 $F > 0$ while the artificial noise technique is a better choice when $F \leq 0$.

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 $F$ 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 $\lambda_c$ on $d^*$. The resulting curve partitions the $(d^*, \lambda_c)$ 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 $\lambda_c$, $d^*$ 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.

A. Proof of Lemma[7]

APPENDIX

By definition, the secure communication probability is

$$P_{\text{sec}}^{\text{GZ}} = P \left( \max_{y \in \Phi_c, \cap B(0, r_y)} \{ g_y \| y \|^{-\alpha} \} \leq \beta_c \right)$$

(19)

where (b) follows from the independence of $y_g$ across all wireless links, (b) is due to $g_y \sim \exp(1)$, and (c) follows from applying PGFL of PPP and converting to polar coordinates. With simple algebraic manipulations, the final result presented in Lemma[1] follows.

B. Proof of Theorem[7]

Technique selection is done using the following inequality:

$$p_{\text{GZ}}^{\text{AN}} \geq p_{\text{AN}}^{\text{AN}}$$