Authors' accepted manuscript of the article published in *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2017.2700438

On the Uplink Secrecy Capacity Analysis in D2D-Enabled Cellular Network

Yohannes Jote Tolossa, *Student Member, IEEE*, Satyanarayana Vuppala, *Member, IEEE*, Georges Kaddoum, *Member, IEEE* and Giuseppe Abreu, *Senior Member, IEEE*

***Abstract*—Recent research prove that device-to-device (D2D) communications offer substantial gain through enhancing throughput and spectral efficiency as well as widening coverage area of cellular network. However, from security perspective, performance of such network has not been well investigated. With this motive and inspired by stochastic geometry approach, we provide secrecy rate analysis for D2D-enabled cellular network under Rayleigh fading channels. The minimum distance among mobile users is used to characterise the retention probability and hence, density of D2D nodes. Moreover, a fraction of the total transmitted power from D2D nodes is allocated to radiate artificial noise (AN) to degrade the eavesdroppers channel. Under such conditions, the closed-form expressions for the probability of achieving non-zero secrecy capacity for the uplink channel between user-equipment and cellular base-station in the presence of D2D nodes and eavesdropper(s). Throughout the paper, we consider the following eavesdropping strategies: (a) a single eavesdropper case; (b) multiple eavesdroppers that can cooperatively cancel the interference; (c) multiple cooperative eavesdroppers that can cooperatively cancel both the interference and AN; and (d) the case of cooperative colluding eavesdroppers. The derived expressions are validated via simulation as a function of antenna gain, eavesdropper density, D2D hard-core distance and D2D node density.**

***Index Terms*—Artificial noise, device-to-device, interference, point process, retention probability, secrecy capacity.**

I. Introduction

The world already has witnessed a number of generation changes in wireless mobile technology which has evolved from sector (cellular) based communications into a global set of interconnected networks. Following the current trend, the next generation wireless mobile communication systems has to cope with the demand for enormous rise in mobile broadband connections, ability to entertain vast and diverse number of users, prolonged battery life, minimal call latency, ultra-high-definition video streaming, extended coverage area, secure and reliable communication capabilities [1], [2]. According to a recent study, by the year 2020, the wireless network is expected to support voice, video and diverse sets of communication services simultaneously for tens of billions of customers and several more billions of interconnected devices. Consequently, the growing interest in fifth generation (5G) communications emanates from the need to find a solution for such inevitable crunch of traffic demand in the existing technology.

Recently, much of the literature on 5G networks focus on infrastructural and topological enhancements to the existing wireless networks. This will create additional spatial domain that will serve as a means to achieve the goals set by 5G standards. To name a few, designing a mixture of network tiers of different sizes provide improved spectral efficiency and wider coverage area [3]; deploying large numbers of antennas at the BS guarantee more degrees of freedom, higher throughput and energy efficiency [4]; full-duplex radio has a potential to double the spectral efficiency [5], and mmWave communication expands the availability of spectrum [6].

In this paper, we focus on device-to-device (D2D)-enabled cellular communication under shared time-frequency resources within the cell. In D2D communication, user equipments (UE) exchange information over a direct link with another device located in close proximity while remaining under the control of the BS. In fact, D2D communication is recognized as one of the major technological advancements of the evolving 5G architecture by the European Union project METIS-2020 [7]. So far, it has drawn widespread attention in academia and industry due to its potential in boosting spectral efficiency, enhancing the end-user experience and providing short range transmission with high data rate [8].

Albeit these advantages, D2D communication suffers from several challenges in the form of mode selection, device discovery and interference management issues [9]. In *underlay* D2D communication, *i.e.*, where D2D and cellular users share the same spectrum, intra-cell interference will have detrimental effect on the throughput performance unless dealt properly. As of recently, there exist several several studies dealing with interference management issues of D2D communications underlaying cellular network. To name a few, Zhang *et al.* [10] adopted fractional frequency reuse, and authors in [11] and [12] proposed a novel network coding approach that eventually improves the spectrum efficiency and throughput of the cellular system. However, from security perspective, we believe that the performance of D2D-enabled cellular network is not well investigated in the literature. With this motive, we have explored the security issues using mathematical and simulation tools in the subsequent sections of the paper.

Security issues are inevitable in wireless networks due to the broadcast nature of wireless medium, and the presence

Y. J. Tolossa is with School of Engineering and Science department of Jacobs University Bremen gGmbH, Campus Ring 1, 28759 Bremen. E-mail: y.tolossa@jacobs-university.de.

S. Vuppala is with the Institute for Digital Communications, the University of Edinburgh, King's Building, Edinburgh, UK, EH9 3JL. E-mail: s.vuppala@ed.ac.uk.

G. Kaddoum is with University of Quebec, ETS, 1100 Notre-Dame west, H3C 1K3, Montreal, Canada. E-mail: georges.kaddoum@etsmtl.ca.

G. Abreu is with School of Engineering and Science department of Jacobs University Bremen gGmbH, Campus Ring 1, 28759 Bremen. E-mail: g.abreu@jacobs-university.de and Ritsumeikan University, Noji-higashi 1-1-1, Kusatu, Shiga 525-8577, Japan. E-mail: g-abreu@fc.ritsumei.ac.jp.

Y. J. Tolossa and G. Abreu work has been supported by the EU project HIGHTS, grant number 636537. Correspondent Author: S.Vuppala.

of malicious users and eavesdroppers. Consequently, intrinsic physical layer secrecy becomes one of the major research topics in random wireless networks and much work has been done in analysing the secrecy performance. However, we would like to point out that a little attention is paid in evaluating the achievable secrecy capacities from 5G perspective [13]–[15]. Hence, it is imperative to devise general framework to evaluate the secrecy capacity taking the wireless propagation characteristics into account. In line with this, exploiting the physical layer characteristics to improve the security in 5G communication systems is a promising research domain.

A few decades before, Wyner coined the information-theoretic wire-tap channel and analyzed the existence of reliable transmission conditions to achieve perfect secrecy in discrete memoryless channels [16]. Later, the information-theoretic security has been extended to additive white Gaussian noise (AWGN) channel by Cheong and Hellman [17], and broadcast wireless channel by Csiszár and Körner [18]. More recently, information-theoretic security, *i.e.*, physical layer security, has motivated several research groups [19]–[21] to understand the inherent secrecy capabilities of wireless systems in more realistic conditions of the wireless medium. Following this trend, Zhou *et al.* [22] characterised the throughput of secure communications in decentralised wireless networks and derived closed-form solutions for secrecy transmission capacity. The probability of non-zero secrecy capacity of unicast links in the presence of multiple eavesdroppers was investigated in [23], where the transmission to the k-th legitimate node was based on the order of the distance between the source and the destination.

Intuitively, the addition of D2D nodes to a cellular network introduces intra-cell interference that severely curbs the throughput performance of the later. Several studies are conducted till date to mitigate such interference. Readers are advised to look into [24], [25]. However, considering security and privacy issues, the intra-cell interference can be exploited in such a way that the cellular network benefits from it. For instance, the work in [13] exploits interference from D2D transmitters, and [26] assumed the D2D users to play the role of cooperative jammers to improve the secrecy capacity of the cellular network.

Artificial noise (AN) transmission is another effective approach to guarantee security provided that the instantaneous channel state information (CSI) of each eavesdropper is not available [27]. The transmitter uses multiple antenna to allocate some of the available power to transmit artificially generated noise, in addition to the information bearing signal, in the null-space of the channel of the legitimate user. The sole purpose of AN transmission is to degrade the eavesdroppers channel so that the secrecy capacity of the legitimate channel is achieved. Recently, AN-aided secure transmission has gained immense research interest. To mention some, [28], [29] analysed an achievable secrecy rate and used this to optimise transmitted power allocation between AN and information signal. Whereas in [30], the authors adopted AN-aided secure communication to design the maximal throughput scheme under secrecy constraint where the CSI is updated adaptively through feedback. Cooperative jamming schemes where transmitters cooperate to transmit AN to trick the eavesdropper from wiretapping the desired information is proposed in [31], [32]. Here, we also adopt AN-aided secure communication in D2D-enabled cellular network where the D2D users allocate some power to radiate AN to mask the information signal from potential malicious users and eavesdropper(s).

In this vein, stochastic geometry approaches have been widely deployed to develop tractable models for the performance evaluation D2D wireless network [33], [34]. In these approaches, the wireless network is abstracted to a convenient point process that is used to capture the network properties. A Poisson point process (PPP) is the most popular and tractable point process to model the locations of users and base stations in wireless network in general. For instance, Andrews *et al.* [35] derived more tractable expressions of coverage and outage probability by assuming homogeneous PPP distributed BS in a practical cellular environment. In conjunction with D2D underlay cellular networks, the authors in [36] provided analytical coverage probability expressions for such networks under PPP distributed D2D and cellular users. Moreover, the shortest distance based selection of candidate nodes is adopted to form D2D pairs with density recalculated after thinning process of the parent marked PPP. In addition, the interference at the legitimate cellular user is characterised by the Laplace functional of point process. Furthermore, we would like to refer the readers to [35], [37] where several mathematical frameworks are formulated to model the propagation characteristics of D2D underlay cellular network.

In this paper, we provide a framework to characterise the probability of achieving non-zero secrecy capacity in D2D-enabled cellular network using stochastic geometry approach to model the existing users under Rayleigh fading channels. In particular, homogeneous PPP is assumed to model the spatial distribution of D2D users and eavesdroppers. Out of the D2D nodes, selected candidate nodes are retained according to reduced path loss model to form D2D pairs [36]. The density of retained D2D pairs can be derived via thinning the parent PPP based on the hardcore distance between nodes. Moreover, the inevitable interference at the legitimate user is modelled according to the Laplace functional of point process. On top of that, four different eavesdropping strategies are considered where the analytic expressions for the non-zero secrecy capacity are derived for each scenarios under certain antenna orientation and transmit power constraint to accommodate the exchange of information and AN transmission simultaneously.

In a nutshell, the contributions of this paper can be summarised as follows:

- The shortest path loss based retention probability of D2D nodes is introduced and the interference to the legitimate UE (BS) is modelled by the Laplace functional of PPP.
- We examine the effect of allocating fraction of the total transmitted power to send AN. Our results show that the more the power is allocated to transmit AN, the lower the capacity of the eavesdropper channel becomes and thus, the secrecy capacity increases.

- An analytic framework is proposed to characterise the probability of achieving non-zero secrecy capacity in D2D-enabled cellular network under the presence of single and multiple eavesdroppers. Our results show that the secrecy capacity depends on the antenna gain, power allocated to convey information bearing signals and AN, eavesdropper density and hard-core distance between candidate D2D nodes.
- The probability of achieving non-zero secrecy capacity is also derived for colluding and non-colluding eavesdroppers. Our result depicts the lower bound secrecy capacity expressions from analysing it solely on the nearest eavesdropper. Moreover, similar secrecy capacity expression is also characterised for the colluding eavesdropper case.

The remainder of this paper is organised as follows. Section II illustrates the system model, retention probability and SINR characterisations. Whereas, in section III, we provide the probability of non-zero secrecy capacity analysis with respect to four possible eavesdropping strategies. The discussions and conclusions of derived analytical expressions are given in section IV and V, respectively.

II. System model

We consider uplink transmission scenario in D2D communications underlay cellular network in the presence of eavesdroppers as shown in Fig. 1. D2D nodes ($\bar{\Phi}_d$) and eavesdroppers (Φ_{e}) are modelled as two dimensional homogeneous PPP with densities $\bar{\lambda}_d$ and λ_{e}, respectively. All the location processes are independent of each other.

Without loss of generality, we consider a typical user equipment (UE) located at the origin as shown in Fig. 1. The BS is located at a distance r_l from origin. In addition, multiple D2D and eavesdropper nodes are distributed throughout the coverage area of the cellular network following a specific point process distribution. The eavesdroppers attempt to make the cellular network prone to security threats via wiretapping the uplink received signal at the legitimate receiver, the cellular BS in this case. Furthermore, each eavesdropper is assumed to be passive, *i.e.*, it doesn't possess any information of its own to convey it to the BS. Hence, its location, and even its presence is not known. It is intuitive to note that the received uplink signal at BS is subjected to interference due to simultaneous D2D communication. This will make the cellular system interference dominated. In order to alleviate such problem, it is desirable for the SINR at the D2D receiver not to exceed a certain threshold level set by the standard adopted by particular telecom provider [38]. Moreover, a protected zone of radius R is set around the vicinity of the BS in order to hamper any interference arising from the transmission of concurrent D2D nodes. In general, D2D nodes are assumed to be randomly located between the coverage area of the cellular BS and the protected zone of radius R. The channel model comprises of generalised path loss and Rayleigh fading for all links.

A. Retention probability

In this paper, the distance among nodes is used as a metric to quantify the pairing probabilities of candidate D2D nodes.

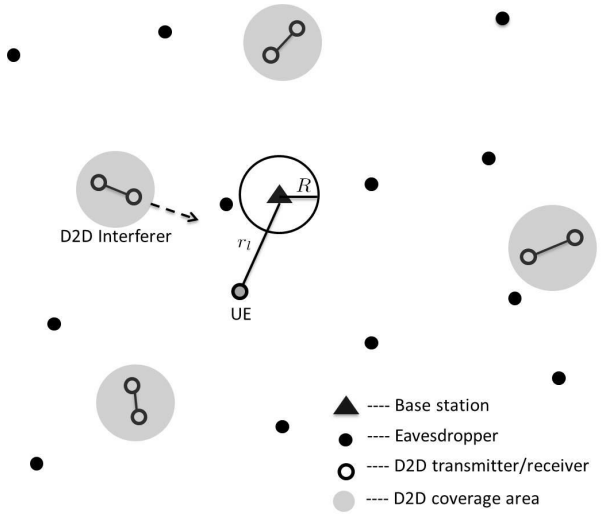

Fig. 1: Network model.

In other words, a D2D node is formed between two UEs which are located within distance r_d from each other and those UEs which do not satisfy this requirement are not considered in D2D pairing. Consequently, D2D pairing leads to a child process which is thinned from the parent marked PPP. A set of points which constitute the child process is denoted by Φ_d distributed with density λ_d. These terms are used in rest of our analysis to capture the shortest distance based selection of points. Note that the total number of points that generate interference are not same as the former after thinning process. However, such interference can still be characterised using Laplace functional of PPP.

In general, the characteristic functional of PPP is given by

$$\mathcal{L}\{f\} = \exp\left(-\int_{\mathbb{R}^2}(1-e^{-f(x)})\lambda\,\mathrm{d}x\right), \tag{1}$$

where $f(x)$ is any real valued function defined on $\mathbb{R}^2$ and λ is the density of PPP.

After thinning process, the Laplace functional can be re-written as

$$\hat{\mathcal{L}}\{f\} = \exp\left(-\int_{\mathbb{R}^2}(1-e^{-f(x)})\mathrm{Pr}(r_d)\lambda\mathrm{d}x\right), \tag{2}$$

where $\mathrm{Pr}(r_d) = \mathrm{Pr}(r_d < d)$ is the probability that any node meet the target hard-core distance d and is given by [36], [39]

$$\mathrm{Pr}(r_d) = 1 - \exp\left(-k\pi\lambda d^2\right). \tag{3}$$

This model has been leveraged from [36], [39] with k tuning factor to capture the shortest distance based selection of nodes. The k tuning factor is chosen in such a way that the analytic retention probability calculated as a function of the hard-core distance d matches with the simulation result.

B. SINR characterizations

In this section, we derive the SINR expressions for the legitimate and eavesdropper nodes with respect to the system model under consideration.

AN has been proved to be an important technique in providing secure communications in cellular systems [40], [41]. In this context, D2D users use some portion of the transmit power P_d, *i.e.* $(1-\phi)P_d$, to radiate AN in the null-space the channel of the BS, leaving the other portion of transmit power, ϕP_d, to transmit information bearing signal, provided that $0 \leq \phi \leq 1$. To further simplify the analysis, sectoring model with AN from [41] is leveraged in this paper. As a result, each D2D node has a main lobe of gain G_s with probability of angle of spread ϵ. Whereas, during AN transmission, D2D user possesses a main lobe of gain G_a with probability of angle of spread $1-\epsilon$. It is also assumed that the sectors of the information signals and AN are non-overlapping.

To this end, adopting AN driven security measures, the uplink received SINR at the BS[1] from a typical UE becomes

$$\zeta_l = \frac{P_{\mathrm{UE}}|h_l|^2 {r_l}^{-\alpha}}{\sigma^2 + \mathcal{I}_d^s + \mathcal{I}_d^a}, \tag{4}$$

where P_{UE} represent the transmit power from UE; h_l denotes the Rayleigh fading gain; r_l is the distance between BS and UE; σ^2 stands for AWGN power at BS; the path loss exponent is denoted by α; $\mathcal{I}_d^s$ and $\mathcal{I}_d^a$ stands for the aggregate interference power due to D2D communication accounting both the information signal and AN transmissions, respectively.

With a slight abuse of notation, let's consider Φ_d as the sets of interfering D2D users location. Using stochastic geometry tools, the interfering D2D nodes can be divided into two independent PPPs: (1) D2D nodes, Φ_d^s, that send information signals to the nearest receiver with intensity $\epsilon\lambda_d$; (2) D2D nodes, Φ_d^a, transmitting AN to the receiver with intensity $(1-\epsilon)\lambda_d$ for $0 \leq \epsilon \leq 1$. As a result, equation (4) can be rewritten as

$$\zeta_l = \frac{P_{\mathrm{UE}}|h_l|^2 {r_l}^{-\alpha}}{\sigma^2 + \sum\limits_{i\in\Phi_d^s}(\phi)P_d G_s |h_i|^2 r_i^{-\alpha} + \sum\limits_{i\in\Phi_d^a}(1-\phi)P_d G_a |h_i|^2 r_i^{-\alpha}}, \tag{5}$$

where P_d represents the transmitted power by the D2D user; h_i denotes the i-th interference fading coefficients and r_i is the distance between the BS and the i-th D2D user.

To characterise the received SINR from the eavesdropper perspective, the following four possible scenarios are analysed.

1) Single eavesdropper case: Here, a single eavesdropper is assumed coexist within the system at a distance r_{e} from cellular UE. Similar to the the legitimate user, the interfering D2D nodes can be grouped into two independent sets of homogeneous point processes; those interferers transmitting information signal and those sending AN to the respective receiver. Consequently, the received SINR at the eavesdropper ζ_{e} with the respective channel coefficient h_{e} is given by

$$\zeta_{\mathrm{e}} = \frac{P_{\mathrm{UE}}|h_{\mathrm{e}}|^2 {r_{\mathrm{e}}}^{-\alpha}}{\sigma^2 + \sum\limits_{i\in\Phi_d^s}(\phi)P_d G_s |h_i|^2 r_i^{-\alpha} + \sum\limits_{i\in\Phi_d^a}(1-\phi)P_d G_a |h_i|^2 r_i^{-\alpha}}. \tag{6}$$

[1]Note here that no decoding technique is deployed at the BS. As a result, the received signal at the BS suffers from interference due to the transmission of information signals and AN between the D2D transmit-receive pairs.

2) Multiple cooperative eavesdroppers:- interference cancellation scenario: In this case, multiple eavesdroppers are considered to coexist within the cellular network in the presence of interfering D2D nodes. Furthermore, we assume that the eavesdroppers do not collude. As a result, each eavesdropper decode the wiretapped uplink message to the BS individually. However, through cooperation, the eavesdroppers jointly process the received signal and thus can nullify the interference arising due to the information signal among D2D users [40]. Therefore, the aggregate interference at eavesdropper is only affected by the AN transmission and AWGN. Readers are advised to read [40, Section III-B] to get detailed insight on this specific eavesdropping strategy. The resulting SINR $\bar{\zeta}_{\mathrm{e}}$ becomes

$$\bar{\zeta}_{\mathrm{e}} = \frac{P_{\mathrm{UE}}|h_{\mathrm{e}}|^2 {r_{\mathrm{e}}}^{-\alpha}}{\sigma^2 + \sum\limits_{i\in\Phi_d^a}(1-\phi)P_d G_a |h_i|^2 r_i^{-\alpha}}. \tag{7}$$

3) Multiple cooperative eavesdroppers:- the 'best' eavesdropper case: In this scenario, we focus on the worst-case eavesdropping strategy in which the eavesdroppers can mitigate the interference via cooperation. Moreover, we overestimate the decoding capability of each eavesdropper. Consequently, each eavesdropper is able to decode the received message and share the information to all other nodes (eavesdroppers) within the system so that the generated interference and AN are subtracted subsequently [42]. In particular, we analysed the approximate secrecy performance of the system based on solely on the most malicious eavesdropper with the largest SINR of the received signal, *i.e.*, the lower bound secrecy performance which can be interpreted as the 'best' eavesdropper case. Therefore, the resulting SNR at the eavesdropper $\hat{\zeta}_{\mathrm{e}}$ can be derived from equation (5) as

$$\hat{\zeta}_{\mathrm{e}} = \max_{\mathrm{e}\in\Phi_{\mathrm{e}}} \left\{ \frac{P_{\mathrm{UE}}|h_{\mathrm{e}}|^2 {r_{\mathrm{e}}}^{-\alpha}}{\sigma^2} \right\}. \tag{8}$$

4) Multiple cooperative eavesdroppers:- colluding eavesdroppers case: Here, rather than generalising the secrecy capacity performance based on the most malicious eavesdropper, we consider colluding eavesdroppers such that the spatially dispersed eavesdroppers adopt maximal-ratio combining (MRC) in order to process the wiretapped transmission. Therefore, the aggregate SNR $\tilde{\zeta}_{\mathrm{e}}$ after MRC is given by [42], [43]

$$\tilde{\zeta}_{\mathrm{e}} = \frac{P_{\mathrm{UE}}}{\sigma^2} \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} |h_{\mathrm{e}}|^2 {r_{\mathrm{e}}}^{-\alpha}. \tag{9}$$

III. Probability of Non-Zero Secrecy capacity Characterisation

In this section, we have derived the closed-form expressions for the probability of achieving non-zero secrecy capacity for the eavesdropping scenarios discussed in Section II-B.

The *secrecy capacity* of the Gaussian wiretap channel in the presence of eavesdroppers distributed according to a certain point process can be expressed as the difference between the

capacity of the legitimate and the eavesdropper channel [44], [45]. Mathematically, the *secrecy capacity* $\mathcal{C}_s$ is given by

$$\mathcal{C}_s \triangleq [\mathcal{C}_l - \mathcal{C}_\mathrm{e}] = [\log_2(1+\zeta_l) - \log_2(1+\zeta_\mathrm{e})] \text{ b/s/Hz}. \quad (10)$$

Consequently, the probability of achieving non-zero secrecy capacity of a legitimate channel under a certain eavesdropping scenario can be expressed as [23]

$$\Pr\{\mathcal{C}_s > 0\} = \Pr\big\{[\log_2(1+\zeta_l) - \log_2(1+\zeta_\mathrm{e})] > 0\big\}. \quad (11)$$

It is evident from equation (11) that primarily we need to characterise the uplink received SINR distribution at the BS and eavesdroppers. In the subsequent subsections, we provide closed-form expressions for the cumulative distribution function (CDF) of the SINR and probability of non-zero secrecy capacity from BS and eavesdropper(s) perspective.

A. Single eavesdropper case

CDF of the received SINR at the legitimate node F_{ζ_l} and at the eavesdropper F_{ζ_e} under this particular eavesdropping scenario is given according to the following Lemma.

Lemma 1. *[46, Theorem. 1] CDF of the received SINR at the BS from a typical UE is given as*

$$F_{\zeta_l}(z) = 1 - \exp\left(\frac{-z\, r_l^{\alpha}\sigma^2}{P_\mathrm{UE}}\right) \times \quad (12)$$
$$e^{-\frac{\pi\epsilon\lambda_d r_l^2 z^{\frac{2}{\alpha}} \left(\frac{(\phi)G_s P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})} - \frac{\pi(1-\epsilon)\lambda_d r_l^2 z^{\frac{2}{\alpha}} \left(\frac{(1-\phi)G_a P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})}}.$$

Proof. A sketch of proof is given in Appendix A. □

Similarly, CDF of ζ_e, *i.e.* $F_{\zeta_\mathrm{e}}(z)$, can be obtained using Lemma 1.

Following from equation (11), CDF of the non-zero secrecy capacity under high SINR regime can be expressed as

$$\begin{aligned}\Pr\{\mathcal{C}_s > 0\} &= 1 - \Pr\left\{\frac{\zeta_l(y)}{\zeta_\mathrm{e}(x)} \le 1\right\} \\ &= 1 - \int_0^{\infty}\int_0^{\beta(x)} f_{\zeta_l}(y) f_{\zeta_\mathrm{e}}(x)\,\mathrm{d}y\mathrm{d}x \\ &= 1 - \int_0^{\infty}\left[\int_0^{\beta(x)} f_{\zeta_l}(y)\,\mathrm{d}y\right] f_{\zeta_\mathrm{e}}(x)\,\mathrm{d}x \\ &= 1 - \int_0^{\infty} F_{\zeta_l}(\beta(x)) f_{\zeta_\mathrm{e}}(x)\mathrm{d}x. \end{aligned} \quad (13)$$

Note that the evaluation of the above integral is not tractable analytically. However, we give approximate closed-form expression in interference limited scenario where the effect of AWGN is assumed to be negligible as compared to the interference from D2D users. Similar analysis under such assumption is made in [35], [42].

Proposition 1. *Probability of non-zero secrecy capacity of the legitimate channel in presence of a single eavesdropper and under interference limited scenario can be given as*

$$\Pr\{\mathcal{C}_s > 0\} = \frac{\Xi_\mathrm{e}}{\Xi_l + \Xi_\mathrm{e}}, \quad (14)$$

where

$$\Xi_l = \frac{\pi\lambda_d r_\ell^2 \left(\frac{P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}} [\epsilon\,(\phi G_s)^{\frac{2}{\alpha}} + (1-\epsilon)\,((1-\phi)G_a)^{\frac{2}{\alpha}}]}{\mathrm{sinc}(\frac{2}{\alpha})}, \quad (15)$$

$$\Xi_\mathrm{e} = \frac{\pi\lambda_d r_\mathrm{e}^2 \left(\frac{P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}} [\epsilon\,(\phi G_s)^{\frac{2}{\alpha}} + (1-\epsilon)\,((1-\phi)G_a)^{\frac{2}{\alpha}}]}{\mathrm{sinc}(\frac{2}{\alpha})}. \quad (16)$$

Proof. See Appendix B. □

***Corollary* 1.** *Considering similar fading, path loss and interference conditions at the BS and eavesdropper, the probability of non-zero secrecy capacity can be given as*

$$\Pr\{\mathcal{C}_s > 0\} = \frac{r_\mathrm{e}^2}{r_l^2 + r_\mathrm{e}^2}. \quad (17)$$

Proof. Proof follows directly from Proposition 1. □

B. Multiple cooperative eavesdroppers:- interference cancellation scenario

In this subsection, we consider the scenario where the interference incurred by the set of nodes transmitting information bearing signal Φ_d^s is mitigated via cooperation at the eavesdroppers rendering the system to be affected only by the sets of nodes Φ_d^a which transmit AN. Assuming interference-limited scenario, the SIR distribution from the eavesdropper perspective, $F_{\bar{\zeta}_\mathrm{e}}(z)$, can be obtained by invoking the result of Lemma 1 as

$$F_{\bar{\zeta}_\mathrm{e}}(z) = 1 - \exp\left[-\frac{\pi(1-\epsilon)\lambda_d r_\mathrm{e}^2 z^{\frac{2}{\alpha}} \left(\frac{(1-\phi)G_a P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})}\right]. \quad (18)$$

Using a similar approach as Appendix B, the probability of achieving non-zero secrecy capacity under this scenario is given according to the following Proposition.

Proposition 2. *Probability of achieving non-zero secrecy capacity in the presence of multiple cooperative eavesdroppers under interference cancelation scenario is given according to*

$$\Pr\{\mathcal{C}_s > 0\} = \frac{\bar{\Xi}_\mathrm{e}}{\Xi_l + \bar{\Xi}_\mathrm{e}}, \quad (19)$$

where

$$\bar{\Xi}_\mathrm{e} = \frac{\pi\lambda_\mathrm{e} r_l^2 \left(\frac{P_d}{P_\mathrm{UE}}\right)^{\frac{2}{\alpha}} [(1-\epsilon)\,((1-\phi)G_a)^{\frac{2}{\alpha}}]}{\mathrm{sinc}(\frac{2}{\alpha})}. \quad (20)$$

Proof. This proof directly follows from Proposition 1. □

C. Multiple cooperative eavesdroppers:- the 'best' eavesdropper case

The cooperation from malicious side provides a greater flexibility in eavesdropping [43]. Hence, through cooperation and adopting the worst-case eavesdropping strategy, the interference generated due to D2D nodes transmitting information signals and AN can be subtracted perfectly at the eavesdropper. Thereafter, the 'best' eavesdropper that dominates the secrecy rate, *i.e.*, with the largest received SINR is selected afterwards.

Lemma 2. *CDF of the received SNR at the 'best' eavesdropper node is given by*

$$F_{\hat{\zeta}_{\mathrm{e}}}(z) = \exp\left(-\pi\lambda_{\mathrm{e}}(\tfrac{P_{\mathrm{UE}}}{\sigma^2})^{\frac{2}{\alpha}} z^{\frac{-2}{\alpha}} \mathbb{E}\left(h_{\mathrm{e}}^{\frac{2}{\alpha}}\right)\right). \tag{21}$$

Proof. A detailed proof is given in Appendix C. □

Now, denoting $\hat{\Xi}_{\mathrm{e}} = \pi\lambda_{\mathrm{e}}(\frac{P_{\mathrm{UE}}}{\sigma^2})^{\frac{2}{\alpha}}\Gamma(1+\frac{2}{\alpha})$, the probability of attaining non-zero secrecy capacity becomes

$$\begin{aligned}\Pr\{\mathcal{C}_s > 0\} &= \int_0^{\infty} e^{-z^{\frac{2}{\alpha}}\Xi_l} f_{\hat{\zeta}_{\mathrm{e}}}(z)\mathrm{d}z, \\ &= \frac{2\hat{\Xi}_{\mathrm{e}}}{\alpha}\int_0^{\infty} e^{-\Xi_l z^{\frac{2}{\alpha}}} e^{-\hat{\Xi}_{\mathrm{e}} z^{-\frac{2}{\alpha}}} z^{-\frac{2}{\alpha}-1}\mathrm{d}z.\end{aligned} \tag{22}$$

Unfortunately, the above integral does not admit closed-form for an arbitrary path loss exponent α. Hence, we provide a closed-form expression under $\alpha = 4$ as in following Lemma.

Lemma 3. *Probability of non-zero secrecy capacity for the 'best' eavesdropper case under $\alpha = 4$ is given as*

$$\Pr\{\mathcal{C}_s > 0\} = \left(2\sqrt{\Xi_l\hat{\Xi}_{\mathrm{e}}}\mathrm{BesselK}[1, 2\sqrt{\hat{\Xi}_{\mathrm{e}}}\sqrt{\Xi_l}]\right), \tag{23}$$

where $\mathrm{BesselK}[.,.]$ *is the modified Bessel function of the second kind.*

Proof. This proof follows directly from equation (22) after substituting $\alpha = 4$ and evaluating the resulting integral. □

***Corollary* 2.** *When $\lambda_d \to \infty$, the probability of non-zero secrecy capacity $\Pr\{\mathcal{C}_s > 0\} \to 0$. This shows that the secrecy capacity fades away with respect to the increase in the interference from D2D nodes.*

D. Multiple eavesdroppers:- colluding eavesdroppers case

The optimum outcome of eavesdropping collusion is to aggregate the power of all eavesdropping signals which can leads to maximum secrecy outage. Thus, it is at most important to characterise such eavesdropper collusion. In the following Lemma, we will provide an approximated closed-form expressions for such collusion and probability of non-zero secrecy capacity.

Lemma 4. *CDF of the aggregate power of the colluding eavesdroppers $F_{\tilde{\zeta}_{\mathrm{e}}}(z)$ can be given as*

$$F_{\tilde{\zeta}_{\mathrm{e}}}(z) \approx \sum_{n=1}^{N}(-1)^{n+1}\binom{N}{i}\exp\left(-\pi\lambda_{\mathrm{e}}\left(\tfrac{a\,n\,P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} z^{\frac{-2}{\alpha}}\right). \tag{24}$$

where $a = (N!)^{\frac{1}{N}}$ and N is the number of terms used in approximation.

Proof. The proof can be obtained from [41]. However, a sketch of proof is given in Appendix D for the sake of completeness. □

The probability of non-zero secrecy capacity in this scenario follows from equation (22) with $\tilde{\Xi}_{\mathrm{e}} = \pi\lambda_{\mathrm{e}}\left(\frac{a\,n\,P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}}$.

Lemma 5. *Considering $\alpha = 4$ for tractable analysis, probability of non-zero secrecy capacity under colluding eavesdroppers scenario is given by*

$$\begin{aligned}&\Pr\{\mathcal{C}_s > 0\} = \\ &\sum_{n=1}^{N}(-1)^{n+1}\left(2\sqrt{\Xi_l\tilde{\Xi}_{\mathrm{e}}}\mathrm{BesselK}[1, 2\sqrt{\tilde{\Xi}_{\mathrm{e}}}\sqrt{\Xi_l}]\right).\end{aligned} \tag{25}$$

Proof. The proof follows similar approach as Lemma 3. □

IV. Numerical Results

In this section, we validate the analytical expressions derived to characterise the non-zero secrecy capacity of the legitimate UE-BS link under the presence of D2D and eavesdropper nodes following Rayleigh fading channels. Analytical results are verified via simulation for different eavesdropper strategies and simulation parameters. In particular, the effect of parameters such as: G_s, ϵ, ϕ, λ_{e} and d on secrecy performance of such network are depicted and the corresponding results are shown in the respective Figures below. The transmit power is set at 30 dBm for UEs with AWGN of -174 dBm/Hz and path loss exponent α is 4.

Fig. 2 illustrates the probability of non-zero secrecy capacity as a function of the angle of spread probability under multiple cooperative eavesdroppers given in scenario III-B for $r_\ell = 20$

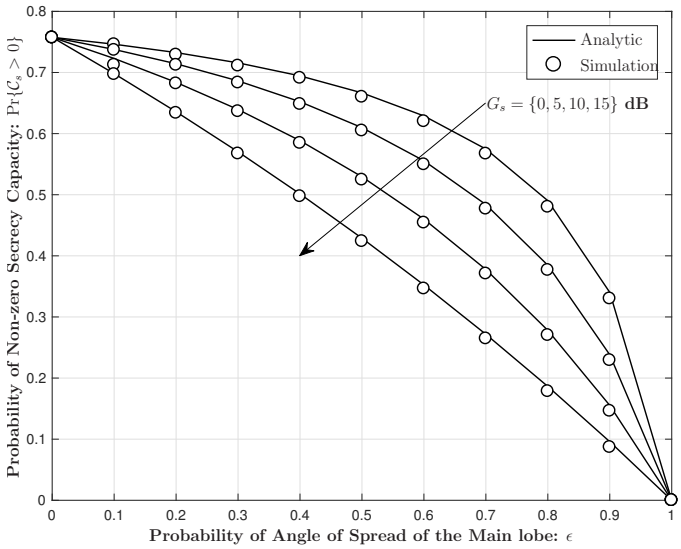

Fig. 2: Probability of non-zero secrecy capacity as a function of angle of spread probability for $G_s = \{0, 5, 10, 15\}$ dB and $G_a = 5$ dB.

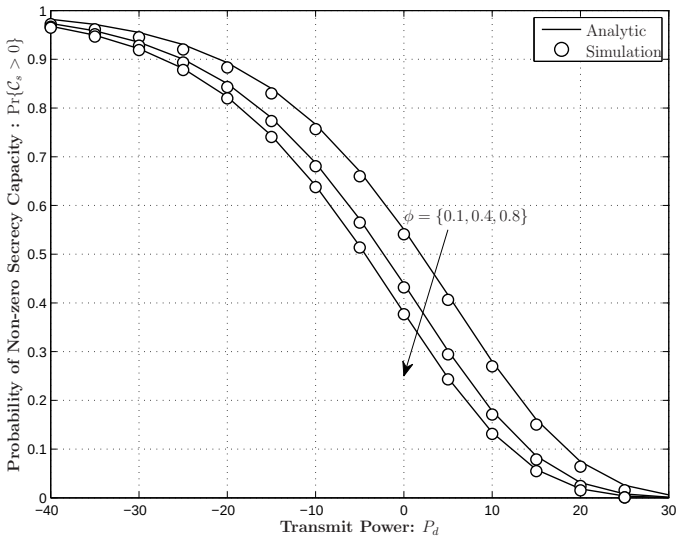

Fig. 3: Probability of non-zero secrecy capacity as a function of transmit power of D2D node for $\phi = \{0.1, 0.4, 0.8\}$.

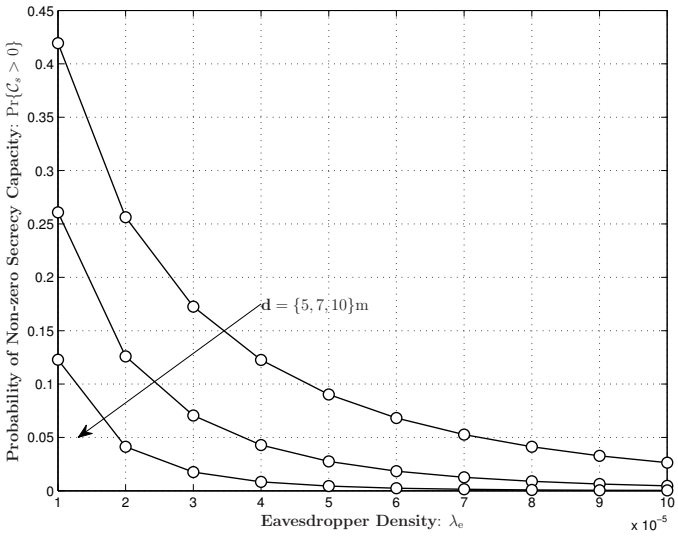

Fig. 4: Probability of non-zero secrecy capacity as a function of λ_e for target distance between candidate D2D pairs $d = \{5, 7, 10\}$ meters.

m, $r_l = 25$ m, $\lambda_d = 0.000005$ and $\lambda_e = 0.00001$. Note that the result follows the expression derived in Proposition 2. A simulation result is also plotted to consolidate the accuracy of the analytical one. It can be concluded from the figure that as the probability of angle of spread (ϵ) increases to unity, the probability of achieving non-zero secrecy capacity vanishes to zero, *i.e.*, the system will be in secrecy outage. This can be explained through the fact that higher ϵ values imply that an increased main lobe gain for D2D users to transmit information signal. Hence, less power will be allocated for AN transmission irrespective of the hard-core distance and total transmit power. As a result, the eavesdropper channel will suffer a little as a result of AN transmission. Thus, the secrecy capacity of the UE-BS channel will decrease as a result. Moreover, the advantage of AN transmission is clearly illustrated in Fig. 2. We can conclude from the figure that the more the gain is allocated to transmit AN, the worse the eavesdropper channel becomes; consequently, the higher the probability of non-zero secrecy capacity is achieved.

In Fig. 3, the probability of non-zero secrecy capacity as a function of the transmitted power of D2D users is depicted. It can be seen from the figure that the secrecy capacity decreases with the increase in D2D users transmit power, due to higher intra-cell interference, which is quite obvious. But the important point to consider is that with decreasing the fraction of total transmitted power, ϕ, the secrecy capacity can be improved slightly. This is because low values of ϕ implies allocating higher share of power to convey AN rather than information bearing signal. This will increase the density D2D nodes Φ_d^a which will ultimately degrade the eavesdropper's channel and thus, yields an improved secrecy capacity.

Fig. 4 depicts the probability of the non-zero secrecy capacity as a function of eavesdropper density for $\lambda_d = 0.00001$, $r_\ell = 25$ m, $P_d = 30$ dBm, $G_s = 18$ dB, $G_a = 2$ dB, $\epsilon = 0.5$ and $\phi = 0.5$ for different hard-core distances among the candidate D2D nodes. This result follows from Lemma 2 stated in Scenario III-C. From the Figure, we can observe that the likelihood of the system to be susceptible to security breaches rises together with the density of eavesdroppers. Furthermore, the effect of hard-core distance d for D2D pairing on secrecy performance is shown in Fig. 4. It is illustrated in the figure that as the hard-core distance among the candidate D2D users increases, the secrecy capacity falls. This is due to as the distance between D2D pairs increases, the retention probability given by equation (3) will almost surely approaches to 1. This means interfering density of D2D nodes changes slightly from the parent PPP and thus, resulting in reduced secrecy capacity.

In Fig. 5, the probability of the non-zero secrecy capacity is plotted against eavesdropper density λ_e with $\lambda_d = 0.00001$, $r_\ell = 25$ m, $P_d = 30$ dBm, $G_s = 18$ dB, $G_a = 2$ dB, $\epsilon = 0.5$ and $d = 5$ m for both non-colluding (Scenario III-C)

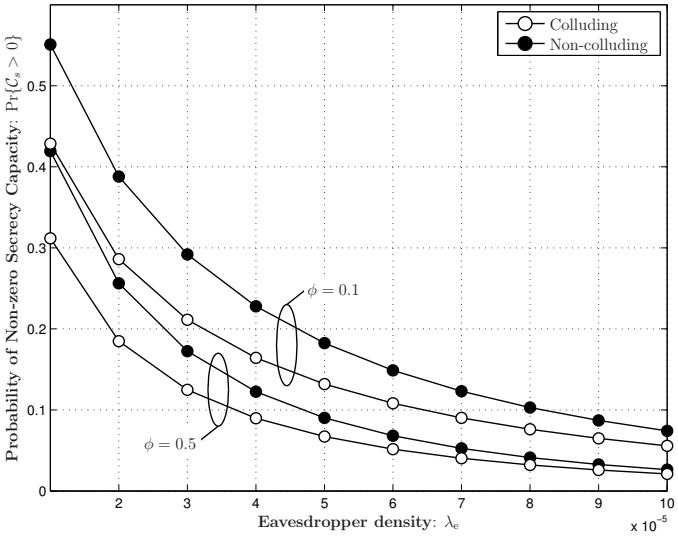

Fig. 5: Probability of non-zero secrecy capacity for colluding and non-colluding eavesdropper scenario as a function of λ_e for $\phi = \{0.1, 0.5\}$.

and colluding (Scenario III-D) eavesdropper strategies. In a similar manner to Fig. 4, the non-zero secrecy capacity drops with increase in eavesdropper collusion density. However, for a particular λ_e, the lower bound secrecy capacity derived based on the 'best' eavesdropper in terms of the received SINR as stated in Scenario III-C is also plotted together with the colluding eavesdroppers case (Scenario III-D). It is evident from the figure that the secrecy performance under the 'best' and colluding eavesdropping scenario will be as more power is allocated for AN transmission which eventually nullify the effect of coexisting eavesdropper(s). Similar to Figures 2 and 3, the benefit of AN in boosting the secrecy capacity is also illustrated in Fig 5. By allocating respective power to transmit the information signal and AN simultaneously, higher the secrecy capacity can be achieved for both non-colluding and colluding eavesdropper scenarios.

V. Conclusion

In this paper, the probability of non-zero secrecy capacity in D2D-enabled cellular network is analysed where the BS is subjected to interference from the uplink transmissions of several D2D nodes. Distance among the candidate D2D nodes is taken as a metric to generate a set of D2D users which exchange information among each other without routing though the BS. Different sets of eavesdropping strategies are analysed and the corresponding probability of non-zero secrecy capacity is derived. Furthermore, the benefit of AN-aided secure communication is illustrated in such a way that some portion of the total transmitted power is allocated to transmit AN in addition to the information bearing signal. At the end, numerical and simulation results are given to verify the analytical outcomes.

As a future work, we plan to evaluate the impact that ordering D2D nodes has on the uplink secrecy performance of D2D-enabled cellular network. Ordering is based on either the maximum received path gain or distance from the source node. This can be achieved via deriving the path gain distribution between the k-th 'best' D2D user and the BS. The Secrecy outage probability can be derived thereafter to quantify the security performance of such D2D-enabled cellular networks. In addition, this work can be extended in such a way that the optimal transmit power allocated to transmit information signal and AN is determined under the following conditions. (a) the secrecy capacity at the UE and D2D pairs is kept above a certain threshold; and (b) the interference incurred to the cellular users has to minimal.

Appendix A
Proof of Lemma 1

The CCDF of conditional SINR distribution, $F_{\zeta_l}(z)$, is

$$F_{\zeta_l}(z) = \Pr\{\zeta_l > z\} = \Pr\left[\frac{P_{\mathrm{UE}}\,|h_l|^2\, r_l^{-\alpha}}{\sigma^2 + \mathcal{I}_d} > z\right] = \Pr\left[|h_l|^2 > \frac{z\, r_l^{\alpha}}{P_{\mathrm{UE}}}\left(\sigma^2 + \mathcal{I}_d\right)\right]. \tag{26}$$

Under the assumption of Rayleigh fading channel, equation (26) can be further simplified to

$$F_{\zeta_l}(z) = \mathbb{E}_{\mathcal{I}_d}\left[\exp\left(\frac{-z\, r_l^{\alpha}}{P_{\mathrm{UE}}}(\sigma^2 + \mathcal{I}_d)\right)\right]. \tag{27}$$

Considering both Φ_d^s and Φ_d^a D2D nodes, we have

$$\mathcal{I}_d = \mathcal{I}_d^s + \mathcal{I}_d^a. \tag{28}$$

Accordingly, we can rewrite (27) as

$$F_{\zeta_l}(z) = \exp\left(\frac{-z\, r_l^{\alpha}\sigma^2}{P_{\mathrm{UE}}}\right) \prod_{j\in s,a} \mathbb{E}_{\mathcal{I}_d^j}\left[\exp\left(\frac{-z r_l^{\alpha}\mathcal{I}_d^j}{P_{\mathrm{UE}}}\right)\right]. \tag{29}$$

The expectation (Laplace function) of I_s^a thus becomes

$$\begin{aligned}
&\mathbb{E}_{\mathcal{I}_d^s}\left[\exp\left(\frac{-z r_l^{\alpha}\mathcal{I}_d^s}{P_{\mathrm{UE}}}\right)\right] \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_d^s}\left\{\prod_{i\in\Phi_d^s} \mathbb{E}_{h_i}\left[\exp\left(-z\frac{r_l^{\alpha}}{P_{\mathrm{UE}}}\phi G_s P_d\, h_i r_i^{-\alpha}\right)\right]\right\} \\
&\overset{(b)}{=} \mathbb{E}_{\Phi_d^s}\left\{\prod_{i\in\Phi_d^s}\left(\frac{1}{1+z\frac{r_l^{\alpha}}{P_{\mathrm{UE}}}\phi G_s P_d\, h_i r_i^{-\alpha}}\right)\right\} \\
&\overset{(c)}{=} \exp\left[-2\pi\epsilon\lambda_d\int_R^{\infty} r\left(1-\left(\frac{1}{1+z\frac{r_l^{\alpha}}{P_{\mathrm{UE}}}\phi G_s P_d r^{-\alpha}}\right)\right)\mathrm{d}r\right] \\
&= \exp\left[-\frac{\pi\epsilon\lambda_d r_l^2 z^{\frac{2}{\alpha}}\left(\frac{\phi G_s P_d}{P_{\mathrm{UE}}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})}\right].
\end{aligned} \tag{30}$$

where (a) follows from the assumption of independent small scale fading, (b) follows from the use of exponential distributed random variables and (c) follows from the use of probability generating functionals of PPPs and $R \sim 0$.

Similarly, the Laplace transform of I_d^a can be obtained following a similar procedure and is given by

$$\begin{aligned}
&\mathbb{E}_{\mathcal{I}_d^s}\left[\exp\left(\frac{-z r_l^{\alpha}\mathcal{I}_d^a}{P_{\mathrm{UE}}}\right)\right] \\
&\qquad = \exp\left[-\frac{\pi\,(1-\epsilon)\,\lambda_d r_l^2 z^{\frac{2}{\alpha}}\left(\frac{(1-\phi)G_a P_d}{P_{\mathrm{UE}}}\right)^{\frac{2}{\alpha}}}{\mathrm{sinc}(\frac{2}{\alpha})}\right].
\end{aligned} \tag{31}$$

The proof concludes after substituting equations (30) and (31) into (29).

Appendix B
Proof of Proposition 1

Considering interference limited environment, CDF of the SIR received at the BS from a typical UE is given by

$$F_{\zeta_l}(z) = 1 - e^{-z^{\frac{2}{\alpha}}\Xi_\ell}. \tag{32}$$

Similarly, the received SIR distribution and its density function at the eavesdropper respectively becomes

$$F_{\zeta_{\mathrm{e}}}(z) = 1 - e^{-z^{\frac{2}{\alpha}}\Xi_{\mathrm{e}}}, \tag{33}$$

$$f_{\zeta_{\mathrm{e}}}(z) = \frac{2\Xi_{\mathrm{e}}}{\alpha} z^{\frac{2}{\alpha}-1} e^{-z^{\frac{2}{\alpha}}\Xi_{\mathrm{e}}}. \tag{34}$$

where Ξ_{e} follows from Ξ_{ℓ}.

Using equation (13), the probability of non-zero secrecy capacity is given by

$$\Pr\{\mathcal{C}_s>0\} = 1 - \int_0^{\infty} F_{\zeta_l}(\beta(z)) f_{\zeta_{\mathrm{e}}}(z)\mathrm{dz} = \int_0^{\infty} \mathrm{e}^{-\mathrm{z}^{\frac{2}{\alpha}}\Xi_{\mathrm{l}}} \mathrm{f}_{\zeta_{\mathrm{e}}}(\mathrm{z})\mathrm{dz}$$

$$= \frac{2\Xi_{\mathrm{e}}}{\alpha} \int_0^{\infty} e^{-(\Xi_l+\Xi_{\mathrm{e}})z^{\frac{2}{\alpha}}} z^{\frac{2}{\alpha}-1}\mathrm{dz}. \tag{35}$$

The proof concludes after evaluating the above integral.

APPENDIX C
PROOF OF LEMMA 2

Here let's assume a point process where the points represents the received SNR at the 'best' (nearest) eavesdropper. Let the SNR of the 'best' eavesdropper be defined according to $\hat{\zeta}_{\mathrm{e}} \triangleq \left\{ \frac{P_{\mathrm{UE}}\, r_{\mathrm{e}}^{-\alpha}}{\sigma^2}, r_{\mathrm{e}} \in \Phi_{\mathrm{e}} \right\}$. The intensity function of $\hat{\zeta}_{\mathrm{e}}$ (before fading) can be obtained by using Mapping theorem [47] as

$$\lambda_{\mathrm{e}}(x) = \frac{2\pi\lambda_{\mathrm{e}}}{\alpha} \left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} r_i^{-\frac{2}{\alpha}-1}. \tag{36}$$

As a result of fading, a point of $\hat{\zeta}_{\mathrm{e}}$ will get displaced to a new location according to $\{y_{\mathrm{e}} = h_{\mathrm{e}}\hat{\zeta}_{\mathrm{e}}\}$. Hence, the intensity of the new marked point process of intensity $\hat{\lambda}_{\mathrm{e}}$ can be obtained by the displacement theorem [47] as

$$\hat{\lambda}_{\mathrm{e}}(y) = \int_0^{\infty} \lambda_{\mathrm{e}}(x) f(x,y)\, \mathrm{d}x, \tag{37}$$

where

$$f(x,y) = \frac{\mathrm{d}}{\mathrm{dy}}(1 - F_H(x/y)) = \tfrac{x}{y^2} f_H(y/x). \tag{38}$$

After substituting equations (36) and (38) into (37), we get

$$\hat{\lambda}_{\mathrm{e}}(y) = \frac{1}{\alpha}\int_0^{\infty} 2\pi\lambda_{\mathrm{e}} \left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} x^{\frac{-2}{\alpha}-1} f(x,y)\,\mathrm{d}x,$$

$$= \frac{1}{\alpha}\int_0^{\infty} 2\pi\lambda_{\mathrm{e}} \left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} x^{\frac{-2}{\alpha}-1} f_H(y/x)\tfrac{x}{y^2}\,\mathrm{d}x,$$

$$\overset{(z=\frac{y}{x})}{=} \frac{1}{\alpha} 2\pi\lambda_{\mathrm{e}} \left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} y^{\frac{-2}{\alpha}-1} \int_0^{\infty} z^{\frac{2}{\alpha}} f_H(z)\,\mathrm{d}z,$$

$$= \frac{1}{\alpha} 2\pi\lambda_{\mathrm{e}} \left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} y^{\frac{-2}{\alpha}-1} \mathbb{E}_{h_{\mathrm{e}}}\left(h_{\mathrm{e}}^{\frac{2}{\alpha}}\right). \tag{39}$$

Thus, the path gain distribution for the 'best' eavesdropper can be obtained using the void probability of PPP [47] in the interval (z,∞) as

$$F_{\hat{\zeta}_{\mathrm{e}}}(t) = \exp\left(-\int_z^{\infty} \hat{\lambda}_{\mathrm{e}}(y)\mathrm{dy}\right) \tag{40}$$

$$= \exp\left(-\frac{2\pi\lambda_{\mathrm{e}}}{\alpha}\left(\frac{P_{\mathrm{UE}}}{\sigma^2}\right)^{\frac{2}{\alpha}} \mathbb{E}_{h_{\mathrm{e}}}\left(h_{\mathrm{e}}^{\frac{2}{\alpha}}\right) \int_z^{\infty} y^{\frac{-2}{\alpha}-1}\mathrm{dy}\right).$$

The proof concludes after solving the above integral.

APPENDIX D
PROOF OF LEMMA 4

From the equation (9), the CDF of $\tilde{\zeta}_{\mathrm{e}}$ can be written as

$$F_{\tilde{\zeta}_{\mathrm{e}}}(T_{\mathrm{e}}) = \Pr\left\{\frac{P_{\mathrm{UE}}\mathcal{I}_{\mathrm{e}}}{\sigma^2} < T_{\mathrm{e}}\right\}, \tag{41}$$

where $\mathcal{I}_{\mathrm{e}} = \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} |h_{\mathrm{e}}|^2 r_{\mathrm{e}}{}^{-\alpha}$ and T_{e} is the target rate at eavesdropper.

Invoking a tight approximation described in [41], [46], we have

$$F_{\tilde{\zeta}_{\mathrm{e}}}(z) = \Pr\left\{\frac{P_{\mathrm{UE}}\mathcal{I}_{\mathrm{e}}}{\sigma^2} < T_{\mathrm{e}}\right\} \approx \Pr\left\{\frac{P_{\mathrm{UE}}\mathcal{I}_{\mathrm{e}}}{\sigma^2 T_{\mathrm{e}}} < z\right\}, \tag{42}$$

where z is a normalised Gamma random variable with a shape parameter N.

Furthermore, the CDF of $\tilde{\zeta}_{\mathrm{e}}$ can be upper bounded with parameter $a \triangleq \frac{N}{(N!)^{-1/N}}$ by

$$F_{\tilde{\zeta}_{\mathrm{e}}}(z) < 1 - \mathbb{E}_{\mathcal{I}_{\mathrm{e}}}\left[\left(1 - e^{-\frac{aP_{\mathrm{UE}}\mathcal{I}_{\mathrm{e}}}{\sigma^2 T_{\mathrm{e}}}}\right)^N\right]. \tag{43}$$

After performing the binomial expansion, $F_{\tilde{\zeta}_{\mathrm{e}}}$ reduces to

$$F_{\tilde{\zeta}_{\mathrm{e}}}(z) = \sum_{n=1}^{N} (-1)^{n+1} \binom{N}{i} \mathbb{E}_{\mathcal{I}_{\mathrm{e}}}\left[e^{-\frac{a\,n\,P_{\mathrm{UE}}\mathcal{I}_{\mathrm{e}}}{\sigma^2 T_{\mathrm{e}}}}\right]. \tag{44}$$

This proof concludes after deriving Laplace transform of the interference as depicted in Appendix A.

REFERENCES

[1] R. N. Clarke, "Expanding Mobile Wireless Capacity: The Challenges Presented by Technology and Economics," *Telecommunications Policy*, vol. 38, no. 8–9, pp. 693–700, 2014.

[2] A. Osseiran, J. F. Monserrat, and W. Mohr, "*Mobile and Wireless Communications for IMT-Advanced and Beyond*", 1st ed., Wiley Publishing, 2011.

[3] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic Geometry for Modeling, Analysis and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 3, pp. 996–1019, April 2013.

[4] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for Next Generation Wireless Systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[5] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-Driven Characterization of Full-Duplex Wireless Systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[6] S. Akoum, O. E. Ayach, and R. W. Heath, "Coverage and Capacity in mmWave Cellular Systems," in *Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pp. 688–692, Nov 2012.

[7] H. Ju, E. Oh, and D. Hong, "Catching Resource-Devouring Worms in Next-Generation Wireless Relay Systems: Two-way Relay and Full-Duplex Relay," *IEEE Commun. Mag.*, vol. 47, no. 9, pp. 58–65, 2009.

[8] J. Lehtomäki, I. Suliman, J. Vartiainen, M. Bennis, A. Taparugssanagorn, and K. Umebayashi, "Direct Communication Between Terminals in Infrastructure Based Networks," *Proc. ICT Mobile Wireless Commun. Summit*, pp. 1–8, 2008.

[9] S. Hakola, T. Chen, J. Lehtomaki, and T. Koskela, "Device-to-Device Communication in Cellular Network - Performance Analysis of Optimum and Practical Communication Mode Selection," in *IEEE Wireless Communication and Networking Conference (WCNC)*, pp. 1–6, April 2010.

[10] Z. Zhang, R. Q. Hu, Y. Qian, A. Papathanassiou, and G. Wu, "D2D Communication Underlay Uplink Cellular Network with Fractional Frequency Reuse," in *International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 247–250, March 2015.

[11] S. Wang, R. Hou, K. S. Lui, H. Li, and J. Li, "A Novel Interference Management Scheme in Underlay D2DCommunication," in *IEEE Vehicular Technology Conference (VTC)*, pp. 1–5, Sept. 2015.

[12] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Enable Device-to-Device Communications Underlaying Cellular Networks: Challenges and Research Aspects," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 90–96, June 2014.

[13] C. Ma, J. Liu, X. Tan, H. Yu, Y. Cui, and X. Wang, "Interference Exploitation in D2D-Enabled Cellular Networks: A Secrecy Perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[14] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless Network Intrinsic Secrecy," *IEEE/ACM Trans. on Networking*, vol. 23, no. 1, pp. 56–69, Feb. 2015.

[15] Y. Dang, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," *IEEE Trans. Inf. Forens. Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[16] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 –1367, Oct. 1975.

[17] L. Y. Cheong and M. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[18] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[19] P. K. Gopala, L. Lai, and H. El-Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[20] 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, Jun. 2008.

[21] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks - Part I: Connectivity," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[22] 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.

[23] S. Vuppala and G. Abreu, "Unicasting on the Secrecy Graph," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 9, pp. 1469–1481, Sep. 2013.

[24] B. Kaufman, J. Lilleberg, and B. Aazhang, "Spectrum Sharing Scheme Between Cellular Users and Ad-hoc Device-to-Device Users," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1038–1049, March 2013.

[25] Y. Pei and Y. C. Liang, "Resource Allocation for Device-to-Device Communications Overlaying Two-Way Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3611–3621, July 2013.

[26] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference Assisted Secret Communication," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[27] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Wireless Communications Magazine*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[28] X. Zhou and M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct 2010.

[29] 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 Transactions on Communications*, vol. 63, no. 11, pp. 4347–4362, Nov 2015.

[30] X. Zhang, X. Zhou, and M. R. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, Jun 2013.

[31] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, March 2011.

[32] C. Wang, H. M. Wang, X. G. Xia, and C. Liu, "Uncoordinated Jammer Selection for Securing SIMOME Wiretap Channels: A Stochastic Geometry Approach," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2596–2612, May 2015.

[33] J. Liu, S. Zhang, H. Nishiyama, N. Kato, and J. Guo, "A Stochastic Geometry Analysis of D2D Overlaying Multi-Channel Downlink Cellular Networks," in *IEEE Conference on Computer Communications (INFOCOM)*, pp. 46–54, Apr. 2015.

[34] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Stochastic Geometry Study on Device-to-Device Communication as a Disaster Relief Solution," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3005–3017, May 2016.

[35] 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.

[36] H. A. Mustafa, M. Z. Shakir, M. A. Imran, and R. Tafazolli, "Coverage Gain and Device-to-Device User Density: Stochastic Geometry Modeling and Analysis," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1742–1745, Oct. 2015.

[37] 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.

[38] D. Tsolkas, E. Liotou, N. Passas, and L. Merakos, *LTE-A Access, Core, and Protocol Architecture for D2D Communication*. Cham: Springer International Publishing, pp. 23–40, 2014.

[39] X. Lin, J. G. Andrews, and A. Ghosh, "Specturm Sharing for Device-to-Device Communication in Cellular Networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec. 2014.

[40] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing Secrecy With Multi-Antenna Transmission in Wireless Ad-Hoc Networks," *IEEE Trans. Inf. Forens. Security*, 2013.

[41] C. Wang and H. M. Wang, "Physical Layer Security in Millimeter Wave Cellular Networks," *IEEE Trans. Wireless Commun. (in press)*, vol. xx, no. xx, pp. xx–xx, May. 2016.

[42] G. Geraci, S. Singh, 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, June 2014.

[43] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks - Part II: Maximum Rate and Collusion," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 139 – 147, Feb. 2012.

[44] A. D. Wyner and J. Ziv, "A Theorem on the Entropy of Certain Binary Sequences and Applications," *IEEE Trans. Inform. Theory*, vol. 19, no. 6, pp. 769 – 777, Nov. 1973.

[45] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[46] T. Bai and R. W. Heath, "Coverage and Rate Analysis for Millimeter-Wave Cellular Networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.

[47] M. Haenggi, *Stochastic Geometry for Wireless Networks*, Cambridge University Press, 2012.

Yohannes Jote Tolossa (S'14) received the B.Sc. degree in Electrical Engineering from Hawassa University, Ethiopia in 2010. In September 2012, he joined Jacobs University Bremen to pursue M.Sc. degree in Communication, system and Electronics until January 2014. From this time onwards, he is working as a Ph.D. student (research assistant) in Electrical Engineering at Jacobs University Bremen under supervision of Prof. Dr. Giuseppe Abreu. His research interests include interference mitigation in wireless communication systems, digital signal processing, convex optimization, stochastic beamforming, physical layer security and stochastic geometry.

Satyanarayana Vuppala (S'12-M'17) received the B.Tech. degree with distinction in Computer Science and Engineering from JNTU Kakinada, India, in 2009, and the M.Tech. degree in Information Technology from the National Institute of Technology, Durgapur, India, in 2011. He received the Ph.D. degree in Electrical Engineering from Jacobs University Bremen in 2014. He is currently a post-doctoral researcher at IDCOM in University of Edinburgh. His main research interests are physical, access, and network layer aspects of wireless security. He also works on performance evaluation of mmWave systems. He is a recipient of MHRD, India scholarship during the period of 2009-2011.

Georges Kaddoum (M'11) received the B.Sc. degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées, Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, University of Toulouse, Toulouse, France, in 2009. Since 2010, he has been a Scientific Consultant of space and wireless telecommunications for several U.S. and Canadian companies. He is currently an Associate Professor of Electrical Engineering with the École de Technologie Supérieure, University of Quebec, Montr éal, QC, Canada. He has authored over 100 journal and conference papers. He holds two pending patents. His recent research activities cover mobile communication systems, modulations, secure transmissions, and space communications and navigation. In 2014, he received the ETS Research Chair in physical layer security for wireless networks. He received the Best Paper Award at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications, with three co-authors, and the 2015 and 2017 IEEE TRANSACTIONS ON COMMUNICATIONS Top Reviewer Award. He is currently serving as an Editor of the IEEE COMMUNICATIONS LETTERS.

Giuseppe Abreu (S'99-M'04-SM'09) received the B. Eng. degree in electrical engineering and a specialization (Latu Sensu) degree in telecommunications engineering from the Universidade Federal da Bahia (UFBa), Salvador, Brazil, in 1996 and 1997, respectively, and the M. Eng. degree in physics and the Ph.D. degree in electrical and computer engineering from the Yokohama National University, Yokohama, Japan, in 2001 and 2004, respectively. He was a Postdoctoral Fellow and Adjunct Professor (Docent) of statistical signal processing and communications theory with the Department of Electrical and Information Engineering, University of Oulu, Oulu, Finland, from 2004 to 2006 and 2006 to 2011, respectively. Since 2011, he has been a Professor of electrical engineering with Jacobs University Bremen, Bremen, Germany, and since 2015, he has been a Professor of electrical engineering with Ritsumeikan University, Kyoto, Japan. His research interests include communications and signal processing, such as communications theory, estimation theory, statistical modelling, wireless localization, cognitive radio, wireless security, MIMO systems, energy harvesting networks, random networks, connected vehicles network, and many other topics. He served as an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2009 to 2014 and currently serves as an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS. He coauthored articles short-listed for the Best Paper Awards at the Asilomar Conference on Signals Systems and Computers in 2009, 2012, and 2014, and was the corecipient of the Best Paper Award at the Workshop on Positioning Navigation and Communications in 2012 and 2014. He was also the recipient of the prestigious JSPS, Heiwa Nakajima and NICT Fellowships in 2010, 2013, and 2015, respectively and the Uenohara Award by Tokyo University in 2000 for his Graduate work.