Towards a Win-Win Spectrum Sharing Channel: A Secrecy Perspective

Amal Hyadi, Fabrice Labeau
Department of Electrical & Computer Engineering, McGill University, Montreal, Canada.
{amal.hyadi, fabrice.labeau}@mcgill.ca

***Abstract*—Spectrum sharing and device-to-device (D2D) transmission are among the key features of modern communication networks. In this work, we are particularly interested in these two techniques from a sharing for secrecy perspective. The considered communication model consists of a multi-user cellular system and an underlying secondary system comprising K D2D pairs. All cellular and D2D transmissions are subject to an eavesdropping attack. Given a predefined secrecy condition, imposed by the primary system to guarantee a desired secrecy throughput, K_{S} D2D pairs are allowed to share the spectrum and send their secret data while the remaining $K-K_{\mathrm{S}}$ device transmitters operate as cooperative jammers. First, we characterize the achievable secrecy rates for both systems under a joint secrecy constraint on all transmitted cellular and D2D messages. Then, we propose a device selection scheme to determine the optimal number of devices, K_{S}, that maximizes the secrecy throughput of the secondary system while satisfying the primary's secrecy condition. The obtained results show that both parties can win under the proposed transmission scheme; the cellular system can significantly improve its secrecy throughput, and the D2D pairs get to share the spectrum and achieve secure transmissions.**

I. Introduction

Spectrum sharing is an essential component in the soon to be released 5G communication systems [1], and undoubtedly also in the future generations to come. The spectrum sharing technique was proposed many years ago by the research community to overcome the spectrum scarcity handicap [2]. In fact, there is a rich variety of research works on spectrum sharing, mainly grouped under the umbrella of cognitive radio systems. A compelling case of spectrum sharing is when then the underlying secondary system allows D2D transmissions among its users [3]. A D2D communication means that a direct transmission between the devices, i.e., the mobile users, is carried out without having the data traffic go through an infrastructure node. Various benefits are associated with this D2D operation model, notably their ability to improve the resource utilization, to increase the energy efficiency, and to decrease the transmission delay among local users [4].

The emerging communication techniques, shaping the new era of wireless communications, face multiple challenges that hinder the reveal of their full potential. Security is among these challenges to beat, especially in the case of spectrum sharing and D2D communications. Exploiting the ability of the physical layer to secure the transmissions, at the bit level itself, is one of the promising research directions proposed to overcome the security challenge. Information theoretic security dates back to Shannon's pioneer work on cipher systems [5], published in 1949. Three decades later, Wyner proposed a new model for the degraded wiretap channel [6], where a source exploits the structure of the channel to transmit a message reliably to the legitimate receiver while asymptotically leaking no information to the eavesdropper. The work of Wyner was later on generalized to the case of non-degraded channels [7], Gaussian channels [8], and fading channels [9]. A detailed state-of-the-art review of the theoretical foundations, coding techniques, practical implementations, challenges and opportunities of physical layer security (PLS) is presented in [10].

In the context of spectrum sharing with underlying D2D communications, the PLS approach has been considered in a number of recent research works. In [11], the authors highlights that the interference caused by the D2D system can be advantageous to the cellular transmission in terms of secrecy. In particular, the work derives the optimal D2D transmission power that minimizes the secrecy outage probability of the primary system. Other works dealing with the secrecy performance of the primary cellular transmission include [12], where the signal-to-interference-plus-noise ratio (SINR) distributions and the primary secrecy outage probability are analyzed using stochastic geometry, and [13] where game theory is utilized to formulate and study the optimal joint power control scheme. On the other hand, the security of the underlying D2D transmissions, under no secrecy constraints on the cellular system, is investigated in [14]. A comprehensive review of security in D2D communications can be found in [15]. When considering security in both the cellular and the D2D systems, the problem could be seen as an interference channel with secrecy constraints. This issue has been theoretically examined in [16]–[18] for discrete and Gaussian channels. However, modeling the spectrum sharing channel with underlying D2D communications as an interference channel fails to capture the dependence that exists between the primary and the secondary systems. In a previous work [19], we examined the impact of this dependence on the secrecy rates of both systems. The considered model assumed a block-fading channel with a single transmission over each system.

In this work, we aim to investigate the optimality of sharing a cellular spectrum with an underlying D2D system when both systems are interested in transmitting secret data. The proposed transmission scheme allows specific underlying D2D pairs to communicate their secret messages while the remaining device transmitters send friendly jamming signals. The number of D2D pairs permitted to transmit is correlated to a secrecy condition imposed by the primary cellular system to maintain

This work was supported by Hydro-Quebec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/Hydro-Quebec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14)

the desired secrecy throughput. The proposed transmission model significantly improve the secrecy performance of the cellular system while also allowing secret transmission for the underlying D2D communications.

The remainder of this paper is organized as follows. Section II describes the system model. Preliminary results regarding the cellular system's secrecy throughput and the jamming signals' generation are presented in Section III. The secrecy rates for both the cellular and the D2D systems are characterized in Section IV. Section V introduces the primary's secrecy condition and discusses the device selection scheme. Selected simulation results are presented in Section VI, and finally Section VII concludes the work.

II. System Model

We consider a multi-user spectrum sharing system where both the primary and the secondary systems are subject to a common eavesdropping attack. The primary is a cellular system composed of a base station and N cellular users. The base station wants to communicate N secret messages W_{C_n}, $n \in \{1, \cdots, N\}$, to the cellular users in the presence of M non-colluding eavesdroppers. Each message W_{C_n} is intended for the n^{th} cellular user and should be kept secret from all eavesdroppers. In order to enhance its secrecy throughput, the cellular system allows a D2D system to share its spectrum. The underlying secondary system comprises K D2D pairs, each of which is interested in establishing a secret transmission.

As sharing the spectrum is motivated by the cellular system's eagerness to improve its secrecy performance, and since it is not guaranteed whether or not the interference caused by the secondary transmissions would achieve this goal, it seems only right that the primary system would require the secondary one to satisfy a secrecy throughput constraint. We consider, then, that only K_{S} out of the K D2D pairs are allowed to communicate their respective secret messages W_{D_i}, $i \in \{1, \cdots, K_{\mathrm{S}}\}$, provided that they satisfy the primary's secrecy constraint. To increase its chances to get access to the spectrum, but also to enhance its own secrecy performance, the secondary system uses the remaining $K-K_{\mathrm{S}}$ transmitting devices to send friendly jamming signals. Details on the imposed primary secrecy constraint are discussed in section V.

The respective received signals at the n^{th} cellular user, $n \in \{1, \cdots, N\}$, the i^{th} secondary device receiver, $i \in \{1, \cdots, K_{\mathrm{S}}\}$, and the m^{th} eavesdropper, $m \in \{1, \cdots, M\}$, are given by

$$\begin{aligned} Y_{\mathrm{C}_n} &= h_{\mathrm{c}_n} X_{\mathrm{C}} + \mathbf{L}_{\mathrm{D}_n} \mathbf{X}_{\mathrm{D}} + \mathbf{L}_{\mathrm{A}_n} \mathbf{X}_{\mathrm{J}} + n_{\mathrm{C}_n} \\ Y_{\mathrm{D}_i} &= h_{\mathrm{d}_i} X_{\mathrm{D}_i} + l_{\mathrm{c}_i} X_{\mathrm{C}} + \widehat{\mathbf{L}}_{\mathrm{D}_i} \widehat{\mathbf{X}}_{\mathrm{D}} + \widehat{\mathbf{L}}_{\mathrm{A}_i} \mathbf{X}_{\mathrm{J}} + n_{\mathrm{D}_i} \quad , \quad (1) \\ Y_{\mathrm{E}_m} &= g_{\mathrm{c}_m} X_{\mathrm{C}} + \mathbf{G}_{\mathrm{D}_m} \mathbf{X}_{\mathrm{D}} + \mathbf{G}_{\mathrm{A}_m} \mathbf{X}_{\mathrm{J}} + n_{\mathrm{E}_m} \end{aligned}$$

Notations: Throughout the paper, we use the following notational conventions. The expectation operation is denoted by $\mathbb{E}[.]$, the modulus of a scalar x is expressed as $|x|$, and we define $\{\nu\}^+ = \max(0, \nu)$. The entropy of a discrete random variable X is denoted by $H(X)$, and the mutual information between random variables X and Y is denoted by $I(X;Y)$. The log operator is used for the binary logarithm, $\lfloor . \rfloor$ is the floor function, and $\binom{\cdot}{\cdot}$ is the binomial coefficient. In addition, we use the superscript $^{\intercal}$ for the transpose of a matrix, the superscript † for the Hermitian transpose, and $\mathbf{I}_N$ to denote the identity matrix of size N.

TABLE I: System Parameters

Notation	Description
BS	Base station
CU_n	n^{th} cellular user, $n \in \{1, \cdots, N\}$
E_m	m^{th} eavesdropper, $m \in \{1, \cdots, M\}$
$(\mathrm{D}_{\mathrm{T}_k}, \mathrm{D}_{\mathrm{R}_k})$	k^{th} device transmitter/receiver pair, $k \in \{1, \cdots, K\}$
$(\mathrm{D}_{\mathrm{T}-\mathrm{S}_i}, \mathrm{D}_{\mathrm{R}-\mathrm{S}_i})$	i^{th} pair transmitting/receiving secret data, $i \in \{1, \cdots, K_{\mathrm{S}}\}$
$\mathrm{D}_{\mathrm{T}-\mathrm{J}_j}$	j^{th} device sending jamming signals, $j \in \{1, \cdots, K-K_{\mathrm{S}}\}$
W_{C_n}	Primary secret message intended for the n^{th} cellular user
W_{D_i}	Secondary secret message intended for the i^{th} receiver
X_{C}	Primary transmitted signal
X_{D_i}	Secondary signal transmitted by the i^{th} device transmitter
X_{J_j}	Jamming signal transmitted by the j^{th} device transmitter
P_{c}	Transmission power of the primary system
P_{d}	Transmission power of each device transmitter

where X_{C} is the primary signal transmitted by the base station, $\mathbf{X}_{\mathrm{D}}$ is the vector of secondary secret data signals, i.e., $\mathbf{X}_{\mathrm{D}} = \begin{bmatrix} X_{\mathrm{D}_1} \cdots X_{\mathrm{D}_{K_{\mathrm{S}}}} \end{bmatrix}^{\intercal}$, $\widehat{\mathbf{X}}_{\mathrm{D}} = \begin{bmatrix} X_{\mathrm{D}_1} \cdots X_{\mathrm{D}_{p-1}} \; X_{\mathrm{D}_{p+1}} \cdots X_{\mathrm{D}_{K_{\mathrm{S}}}} \end{bmatrix}^{\intercal}$, $\mathbf{X}_{\mathrm{J}}$ is the vector of secondary jamming signals, i.e., $\mathbf{X}_{\mathrm{J}} = \begin{bmatrix} X_{\mathrm{J}_1} \cdots X_{\mathrm{J}_{K-K_{\mathrm{S}}}} \end{bmatrix}^{\intercal}$, $\mathbf{L}_{\mathrm{D}_n}$, $\mathbf{L}_{\mathrm{A}_n}$, $\widehat{\mathbf{L}}_{\mathrm{D}_i}$, $\widehat{\mathbf{L}}_{\mathrm{A}_i}$, $\mathbf{G}_{\mathrm{D}_m}$, and $\mathbf{G}_{\mathrm{A}_m}$ are vectors of channel gains, i.e., $\mathbf{L}_{\mathrm{D}_n} = \begin{bmatrix} l_{\mathrm{d}_{1,n}} \cdots l_{\mathrm{d}_{K_{\mathrm{S}},n}} \end{bmatrix}$, $\mathbf{L}_{\mathrm{A}_n} = \begin{bmatrix} l_{\mathrm{a}_{1,n}} \cdots l_{\mathrm{a}_{K-K_{\mathrm{S}},n}} \end{bmatrix}$, $\widehat{\mathbf{L}}_{\mathrm{D}_i} = \begin{bmatrix} \hat{l}_{\mathrm{d}_{1,i}} \cdots \hat{l}_{\mathrm{d}_{p-1,i}} \; \hat{l}_{\mathrm{d}_{p+1,i}} \cdots \hat{l}_{\mathrm{d}_{K_{\mathrm{S}},i}} \end{bmatrix}$, $\widehat{\mathbf{L}}_{\mathrm{A}_i} = \begin{bmatrix} \hat{l}_{\mathrm{a}_{1,i}} \cdots \hat{l}_{\mathrm{a}_{K-K_{\mathrm{S}},i}} \end{bmatrix}$, $\mathbf{G}_{\mathrm{D}_m} = \begin{bmatrix} g_{\mathrm{d}_{1,m}} \cdots g_{\mathrm{d}_{K_{\mathrm{S}},m}} \end{bmatrix}$, $\mathbf{G}_{\mathrm{A}_m} = \begin{bmatrix} g_{\mathrm{a}_{1,m}} \cdots g_{\mathrm{a}_{K-K_{\mathrm{S}},m}} \end{bmatrix}$, and n_{C_n}, n_{D_i}, and n_{E_m} represent the additive white Gaussian noise (AWGN) at the n^{th} cellular user, the i^{th} secondary device receiver, and the m^{th} eavesdropper, respectively. For the reader's convenience, a list of the system parameters is available in Table I, and an illustration of the different links and their corresponding channel gains is provided in Fig. 1.

All channel gains are assumed to be independent, ergodic and stationary. Besides, we consider that the instantaneous channel state information (CSI) of the legitimate receivers are globally known and that only the statistics of the eavesdroppers' channels are known to the cellular and the D2D systems. The eavesdroppers are assumed to know all channel gains.

III. Preliminary Results

In this section, we present two preliminary results that will be used in the remaining of the paper. First, we characterize the secrecy sum-rate of the cellular system without the underlying D2D system. Then, we introduce and discuss an optimal generation process for the transmitted jamming signals.

A. Cellular Secrecy Sum-Rate with no D2D Transmission

A compelling secrecy achieving scheme for the multi-user wiretap channel consists of using an opportunistic communication approach. We consider, then, that the cellular system uses a time division multiplexing scheme and selects instantaneously one cellular receiver to transmit to. That is, at each time, the base station only transmits to the cellular user with the best channel gain. Since we are transmitting to only one cellular receiver at a time, the achieving coding scheme consists of using independent standard single user wiretap codebooks.

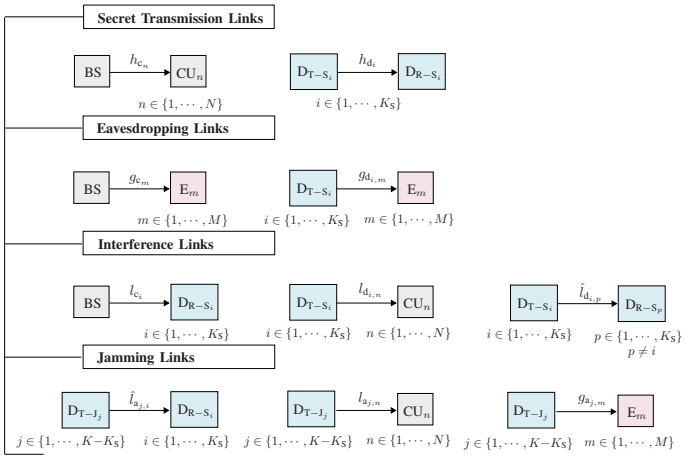

Fig. 1: Depiction of the different channel links and their corresponding channel gains.

Corollary 1. *An achievable secrecy sum-rate for the multi-user cellular system with no D2D transmission is given by*

$$\mathcal{R}_{C_{sum}}^{\text{no-D2D}} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{c\text{-}max}|^2}{\sigma^2_{C\text{-}max}} P_c\right) - \log\left(1 + \frac{|g_{c\text{-}max}|^2}{\sigma^2_{E\text{-}max}} P_c\right)\right]\right\}^+, \quad (2)$$

where $|h_{c\text{-}max}|^2 = \max_{1\leq n\leq N} |h_{c_n}|^2$, $|g_{c\text{-}max}|^2 = \max_{1\leq m\leq M} |g_{c_m}|^2$, *and* $\sigma^2_{C\text{-}max}$ *and* $\sigma^2_{E\text{-}max}$ *are the respective variances of the AWGN at the cellular receiver with channel gain* $h_{c\text{-}max}$ *and at the eavesdropper with channel gain* $g_{c\text{-}max}$.

Proof. The achievability proof for (2) follows from the results on the fading broadcast wiretap channel with independent messages transmission, presented in [20]. □

B. Jamming Signals Generation

Driven by the possibility of increasing its secrecy throughput, the cellular system allows the D2D network to share its spectrum. The D2D system operates in the following way: K_S secondary device transmitters are permitted to share the spectrum and secretly transmit to their respective receivers while the remaining $K-K_S$ secondary device transmitters send jamming signals. The transmission of these jamming signals is beneficial for both the primary and the secondary systems as they are both trying to secure their communications. To significantly improve the secrecy performance of both systems, the transmitted jamming signals should only affect the eavesdroppers and should cancel out at the cellular users and the secondary device receivers. These two constraints could be formulated as follows

$$\widehat{\mathbf{L}}_A \mathbf{X}_J = \mathbf{0}, \quad (3)$$

$$\mathbf{L}_{A_{n^*}} \mathbf{X}_J = 0, \quad (4)$$

with $\widehat{\mathbf{L}}_A = \left[\widehat{\mathbf{L}}_{A_1}^\intercal \dots \widehat{\mathbf{L}}_{A_{K_S}}^\intercal\right]$, $\mathbf{L}_{A_{n^*}} = \left[l_{a_{1,n^*}} \dots l_{a_{K-K_S,n^*}}\right]$, and n^* represents the index for the optimal cellular user to transmit to. Note that (4) abides by the opportunistic transmission model adopted by the primary system. Let $\mathbf{W}$ be an orthonormal basis for null$\left(\left[\widehat{\mathbf{L}}_A \;\; \mathbf{L}_{A_{n^*}}\right]^\intercal\right)$. Then, we can write $\mathbf{X}_J = \mathbf{WV}$, where $\mathbf{V}$ is a random Gaussian vector satisfying $\mathbb{E}[\mathbf{VV}^*] = P_d\, \mathbf{I}_{K-2K_S-1}$. To ensure that (3) and (4) could be solved, the number of devices allowed to secretly transmit should satisfy $K_S \leq \left\lfloor \frac{K-1}{2} \right\rfloor$. Taking $\mathbf{X}_J = \mathbf{WV}$, we get $\widehat{\mathbf{L}}_A \mathbf{X}_J = \mathbf{0}$ and $\mathbf{L}_{A_{n^*}} \mathbf{X}_J = 0$, which allows us to re-write the system of equations in (1) as follows

$$\begin{aligned} Y_{C_{n^*}} &= h_{c_{n^*}} X_C + \mathbf{L}_{D_{n^*}} \mathbf{X}_D + n_{C_{n^*}} \\ Y_{D_i} &= h_{d_i} X_{D_i} + l_{c_i} X_C + \widehat{\mathbf{L}}_{D_i} \widehat{\mathbf{X}}_D + n_{D_i} \\ Y_{E_m} &= g_{c_m} X_C + \mathbf{G}_{D_m} \mathbf{X}_D + \mathbf{G}_{A_m} \mathbf{X}_J + n_{E_m} \end{aligned}, \quad (5)$$

with $i \in \{1,\cdots,K_S\}$, and $m \in \{1,\cdots,M\}$.

IV. Joint Secrecy Rates

In this section, we characterize the achievable secrecy rates satisfying joint secrecy[1] for all cellular and D2D messages.

A. Secrecy Sum-Rate for the Primary Cellular System

In subsection III-A, we saw that when no D2D transmission is allowed, the secrecy sum-rate in Corollary 1 is achieved using an opportunistic transmission model where the BS instantaneously transmits to the cellular user with the best channel gain. This opportunistic transmission is particularly interesting when transmitting to multiple receivers over non-orthogonal channels as it avoids dealing with the interference engendered by the transmission of the other messages, especially when the cellular users have no successive interference cancellation capabilities. Here, we will extend this time division multiplexing scheme to the case with K_S D2D secret transmissions and $K-K_S$ friendly jamming signals. Since now we have to account for the interference coming from the underlying system, we consider that the BS transmits to the cellular user with the best signal to interference noise ratio (SINR). The secrecy sum-rate, achievable under this opportunistic transmission model, is provided in the following theorem.

Theorem 1. *An achievable secrecy sum-rate for the multi-user cellular system described in* (5)*, with* K_S *underlying D2D transmissions and* $K-K_S$ *friendly jamming devices, is given by*

$$\mathcal{R}_{C_{sum}} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{c_{n^*}}|^2 P_c}{\sigma^2_{C_{n^*}} + \sum_{i=1}^{K_S} |l_{d_{i,n^*}}|^2 \; P_d}\right) - \log\left(1 + \frac{|g_{c_{m^*}}|^2 P_c}{\sigma^2_{E_{m^*}} + \left(\sum_{i=1}^{K_S} |g_{d_{i,m^*}}|^2 + \Omega_{m^*}\right) P_d}\right)\right]\right\}^+, \quad (6)$$

with K_S *satisfying* $K_S \leq \left\lfloor \frac{K-1}{2} \right\rfloor$, $\Omega_{m^*} = \mathbf{G}_{A_{m^*}} W W^\dagger \mathbf{G}_{A_{m^*}}^\dagger$, *and where* n^* *and* m^* *are respectively given by*

$$\begin{cases} n^* = \underset{1\leq n\leq N}{\text{argmax}} \left[\dfrac{|h_{c_n}|^2}{\sigma^2_{C_n} + \sum_{i=1}^{K_S} |l_{d_{i,n}}|^2 P_d}\right] \\ m^* = \underset{1\leq m\leq M}{\text{argmax}} \left[\dfrac{|g_{c_m}|^2}{\sigma^2_{E_m} + \left(\sum_{i=1}^{K_S} |g_{d_{i,m}}|^2 + \Omega_{m^*}\right) P_d}\right] \end{cases}.$$

Proof. The proof of Theorem 1 is given in Appendix A. □

[1]The joint secrecy constraint ensures that even if the security of one of the systems is ruptured, the security of the other one is not necessarily ruptured too.

To prove that the adopted transmission scheme guarantees secrecy up to the equivocation rates, we showed that

$$\forall m \in \{1,\cdots,M\}, \tag{7}$$
$$\frac{1}{\eta}H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N}|Y^{\eta}_{\mathrm{E}_m},\mathbf{\Gamma}^{\eta}_{\mathrm{C}},\mathbf{\Gamma}^{\eta}_{\mathrm{D}},g^{\eta}_{\mathrm{c}_m},\mathbf{G}^{\eta}_{\mathrm{D}_m},\mathbf{G}^{\eta}_{\mathrm{A}_m}) \geq \mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}-\epsilon.$$

Note that the condition in (7) ensures the secrecy of the cellular messages, $W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N}$, but not the joint secrecy of both these cellular messages and the secondary D2D messages, $W_{\mathrm{D}_1},\cdots,W_{\mathrm{D}_{K_{\mathrm{S}}}}$, against the eavesdropping attack. The reason behind this is that since its the cellular system who is sharing its spectrum with the D2D system, he can choose to maintain the best secrecy rates that could be achieved and requires the D2D transmissions to satisfy the joint secrecy constraint. This is discussed in the following section.

B. Secrecy Rates for the Secondary D2D System

Concurrently to the cellular transmission, K_{S} out of K device transmitters are allowed by the primary system to share the spectrum and send their secret messages while the remaining $K-K_{\mathrm{S}}$ device transmitters send friendly jamming signals. Each of the K_{S} device transmitters sending secret data has a secret message W_{D_k}, $k \in \{1,\cdots,K_{\mathrm{S}}\}$, intended for its corresponding receiver. The D2D system is expected to improve the secrecy throughput of the primary cellular system and is required to ensure that both the primary and the secondary messages are jointly secured against the eavesdroppers.

Theorem 2. *The following secrecy rates for the underlying D2D system described in* (5)*, with K_S D2D secret transmissions and $K-K_S$ friendly jamming devices, are achievable under the joint secrecy condition*

$$\mathcal{R}_{D_k} = \left\{ \mathbb{E}\left[\log\left(1+\frac{|h_{d_k}|^2 P_d}{\sigma^2_{D_k}+|l_{c_k}|^2 P_c+\sum_{\substack{p=1\\p\neq k}}^{K_S}\left|\hat{l}_{d_{p,k}}\right|^2 P_d}\right) - \log\left(1+\frac{\left|g_{d_{k,m^*_k}}\right|^2 P_d}{\sigma^2_{E_{m^*_k}}+\left(\sum_{p=k+1}^{K_S}\left|g_{d_{p,m^*_k}}\right|^2+\Omega_{m^*_k}\right)P_d}\right)\right]\right\}^+, \tag{8}$$

with $k \in \{1,\cdots,K_S\}$, K_S satisfying $K_S \leq \left\lfloor\frac{K-1}{2}\right\rfloor$, $\Omega_{m^*_k} = \mathbf{G}_{A_{m^*_k}} W W^{\dagger} \mathbf{G}^{\dagger}_{A_{m^*_k}}$, and where m^*_k is given by

$$m^*_k = \underset{1\leq m\leq M}{\operatorname{argmax}} \left[\frac{\left|g_{d_{k,m}}\right|^2}{\sigma^2_{E_m}+\left(\sum_{p=k+1}^{K_S}\left|g_{d_{p,m}}\right|^2+\Omega_{m^*}\right)P_d}\right].$$

Proof. The proof of Theorem 2 is given in Appendix B. □

In the previous section, we saw that the equivocation analysis for the secrecy sum-rate in (6) only account for the security of the primary messages and do not guarantee the joint secrecy of those messages along with the secondary ones. In fact, the D2D system is required to assure the joint secrecy constraint, given the pre-established secrecy rates of the cellular system. In that light, the secrecy analysis in Appendix B show that

$$\forall m \in \{1,\cdots,M\}, 1/\eta H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N},W_{\mathrm{D}_1},\cdots,W_{\mathrm{D}_{K_{\mathrm{S}}}}|$$
$$Y^{\eta}_{\mathrm{E}_m},\mathbf{\Gamma}^{\eta}_{\mathrm{C}},\mathbf{\Gamma}^{\eta}_{\mathrm{D}},g^{\eta}_{\mathrm{c}_m},\mathbf{G}^{\eta}_{\mathrm{D}_m},\mathbf{G}^{\eta}_{\mathrm{A}_m}) \geq \mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}+\sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k}-\epsilon', \tag{9}$$

which ensures the joint secrecy of all transmitted messages.

V. Optimal Devices Selection

A. The Primary's Secrecy Condition

The cellular system allows K_{S} D2D pairs to share the spectrum and communicate their secret messages as long as the underlying D2D system satisfies the following condition $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(K_{\mathrm{S}}) \geq \mathcal{R}_{\mathrm{th}}$, where $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(K_{\mathrm{S}})$ is the secrecy sum-rate of the cellular system, given K_{S} underlying D2D transmissions and $K-K_{\mathrm{S}}$ friendly jamming devices, and $\mathcal{R}_{\mathrm{th}}$ is a secrecy sum-rate threshold. The expression of $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}$ is presented in Theorem 1. An interesting choice for the primary's secrecy sum-rate threshold is $\mathcal{R}_{\mathrm{th}} = \beta\ \mathcal{R}^{\text{no-D2D}}_{\mathrm{C}_{\mathrm{sum}}}$, with $\beta \geq 0$, and $\mathcal{R}^{\text{no-D2D}}_{\mathrm{C}_{\mathrm{sum}}}$ being the secrecy sum-rate of the cellular system with no D2D transmission, given in Corollary 1. Note that in order to ameliorate its secrecy rates, the cellular system would be more interested in taking $\beta > 1$. Choosing $\beta < 1$ may be possible when the D2D system incentivizes the cellular one to share the spectrum. Besides, when $\mathcal{R}^{\text{no-D2D}}_{\mathrm{C}_{\mathrm{sum}}} = 0$, the threshold should be chosen differently.

Given the primary's secrecy sum-rate condition, we need to find the optimal number of devices K^*_{S} that maximizes the secondary secrecy throughput, i.e.

$$K^*_{\mathrm{S}} = \begin{cases} \underset{1\leq K_{\mathrm{S}}\leq\left\lfloor\frac{K-1}{2}\right\rfloor}{\operatorname{argmax}} & \sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k} \\ \text{subject to} & \mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(K_{\mathrm{S}}) \geq \mathcal{R}_{\mathrm{th}} \end{cases}. \tag{10}$$

B. Exhaustive Search Selection (ESS)

Considering the complexity of the expressions of the cellular and the D2D secrecy rates, finding an optimal solution to the problem in (10) is hard to do analytically. In this subsection, we use a brute-force search scheme to select the optimal number of devices K_{S}. The D2D system comprises K D2D pairs and only K_{S} out of these K D2D pairs are allowed to share the spectrum and send their secret messages. The remaining $K-K_{\mathrm{S}}$ device transmitters send friendly jamming signals in the null space of the primary and the secondary legitimate receivers. This null space constraint requires K_{S} to satisfy $K_{\mathrm{S}} \leq \left\lfloor\frac{K-1}{2}\right\rfloor$, as explained in Section III-B. It follows that the total number of possible choices to select K_{S} D2D pairs out of the K available ones is equal to $\sum_{K_{\mathrm{S}}=1}^{\left\lfloor\frac{K-1}{2}\right\rfloor}\binom{K}{K_{\mathrm{S}}}$. Given all possible combinations of D2D pairs, we determine the ones that satisfy the primary's secrecy condition, i.e., $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(K_{\mathrm{S}},i) \geq \mathcal{R}_{\mathrm{th}}$, where $i = 1,\cdots,\sum_{K_{\mathrm{S}}=1}^{\left\lfloor\frac{K-1}{2}\right\rfloor}\binom{K}{K_{\mathrm{S}}}$, and $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(K_{\mathrm{S}},i)$ is the primary's secrecy sum-rate corresponding to the i^{th} possible combination of size K_{S}. Then, from these combinations, we choose the one that maximizes the sum of secondary secrecy rates $\sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k}(i)$. Also, since a D2D pair with a zero secrecy rate would not contribute to increasing the secondary secrecy throughput, we only account for the combinations that satisfy

$$\forall\, k \in \{1,\cdots,K_{\mathrm{S}}\},\ \mathcal{R}_{\mathrm{D}_k}(i) \neq 0. \tag{11}$$

C. Revised Exhaustive Search Selection (R-ESS)

The ESS scheme has to go through all D2D combinations to check whether or not the primary's condition is satisfied. As the total number of possible combinations amounts to $\sum_{K_{\mathrm{S}}=1}^{\left\lfloor\frac{K-1}{2}\right\rfloor}\binom{K}{K_{\mathrm{S}}}$, the complexity of the ESS will grow exponentially as K increases. In this subsection, we will look

at reducing the number of combinations that ESS has to cover. By considering the adopted transmission model for the D2D system, and the expressions of the secrecy sum-rate for the cellular transmissions, we can see that when a D2D combination of size K_{S} fails to satisfy the primary's secrecy condition, let us say combination i, any other combination of a size larger than K_{S}, containing all elements in i, will also fail to satisfy the constraint. As a matter of fact, when increasing K_{S}, we are also increasing the amount of interference caused to the cellular system while reducing the number of jamming signals. That being said, when we know that a D2D combination do not satisfy the constraint of the cellular system, there is no point in checking the combinations containing it. This observation is formally expressed in Lemma 1.

Lemma 1. *Let $\mathcal{C}$ be the set of all combinations of K_S out of K elements, with $K_S = 1, \cdots, \lfloor \frac{K-1}{2} \rfloor$, and let i be a combination index, $i \in \left\{1, \cdots, \sum_{K_S=1}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K}{K_S}\right\}$.*
If $\mathcal{R}_{C_{sum}}(i) < \mathcal{R}_{th}$, **then** $\mathcal{R}_{C_{sum}}(j) < \mathcal{R}_{th}$, $\forall j \in \left\{1, \cdots, \sum_{K_S=1}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K}{K_S}\right\}$ *such that* $\mathcal{C}(i) \subset \mathcal{C}(j)$.

Proof. The proof of Lemma 1 is obtained by showing that $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(j) < \mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(i)$ when $\mathcal{C}(i) \subset \mathcal{C}(j)$. Based on Lemma 1, a revised ESS is proposed in Algo. 1. □

VI. Numerical Results and Discussions

To illustrate the results, we consider the case of Rayleigh fading channels, i.e., all channel gains are modeled as zero-mean complex Gaussian random variables. We consider unit variance AWGN for all terminals, i.e., $\sigma^2_{\mathrm{C}_n} = \sigma^2_{\mathrm{D}_k} = \sigma^2_{\mathrm{E}_m} = 1$, $n \in \{1, \cdots, N\}$, $k \in \{1, \cdots, K_{\mathrm{S}}\}$, and $m \in \{1, \cdots, M\}$. The number of simulations for each illustrated point is $L = 10^4$.

Algorithm 1: R-ESS

Input : K, $\mathcal{R}_{\mathrm{th}}$.
Output: K_{S}.
Let $\mathcal{C}$ be the set of all combinations of K_{S} out of K elements with $K_{\mathrm{S}} = 1, \cdots, \lfloor \frac{K-1}{2} \rfloor$;
for $i = 1$ **to** $\sum_{K_S=1}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K}{K_S}$ **do**
  if $\mathcal{C}(i) \neq \emptyset$ **then**
    Compute $\mathcal{R}_{\mathrm{C}_{\mathrm{sum}}}(i)$ for the i^{th} combination;
    if $\mathcal{R}_{C_{sum}}(i) \geq \mathcal{R}_{th}$ **then**
      Compute the secondary secrecy rates $\mathcal{R}_{\mathrm{D}_k}(i), k \in \{1, \cdots, K_{\mathrm{S}}\}$;
      if $\forall k \in \{1, \cdots, K_S\}$, $\mathcal{R}_{D_k}(i) \neq 0$ **then**
        $i \in \mathcal{L}_{\mathrm{c}}$;
    else
      $\mathcal{C}(j) = \emptyset$, $\forall j \in \left\{1, \cdots, \sum_{K_S=1}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K}{K_S}\right\}$ such that $\mathcal{C}(i) \subset \mathcal{C}(j)$;
if $\mathcal{L}_c \neq \emptyset$ **then**
  Choose the combination in $\mathcal{L}_{\mathrm{c}}$ that maximizes $\sum_{k=1}^{K_{\mathrm{S}}} \mathcal{R}_{\mathrm{D}_k}(i)$;
  Return the corresponding K_{S};
else
  $K_{\mathrm{S}} = 0$; *% No D2D Transmission*

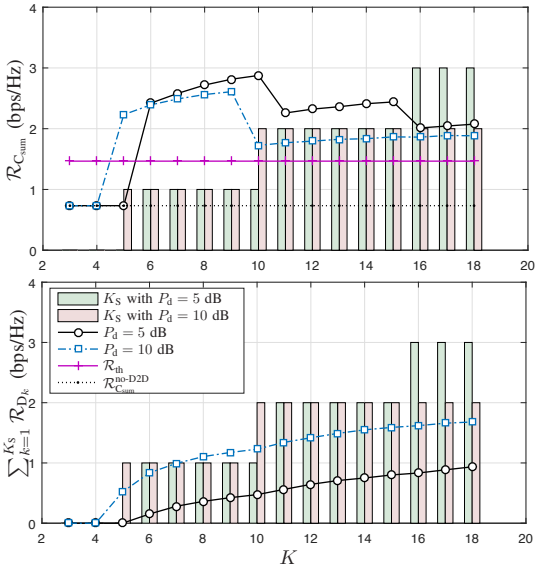

Fig. 2: Achievable secrecy rates when using the R-ESS scheme, with $N = 5$, $M = 2$, $P_{\mathrm{c}} = 10$ dB, and $\beta = 2$.

Fig. 2 illustrates the case when $N = 5$, $M = 2$, $P_{\mathrm{c}} = 10$ dB, and $\beta = 2$. The variances for the channel gains describing the interference links are equal to 0.5 while all the other channel gain variances are equal to one. The main point to note here is that, under the proposed transmission scheme, and by taking $\beta = 2$, the cellular system ensures that its secrecy sum-rate is at least doubled when sharing its spectrum with the underlying devices. Also, by increasing its transmission power, the secondary system can improve its secrecy throughput. However, this will reduce the number of devices allowed to communicate as the level of interference caused to the cellular system and among the secondary devices themselves will rise. So, finding the optimal number of devices K_{S} is key to ensure a win-win gain for both systems.

VII. Conclusion

We considered a spectrum sharing channel where both the cellular system and the underlying D2D pairs are interested in transmitting secret data. The obtained results show the undeniable potential of the proposed transmission model to improve the secrecy performance of the primary while also allowing secret transmission for the underlying D2D communications.

Appendix A
Proof of Theorem 1

We construct N independent random Gaussian codebooks. For each message W_{C_n}, $n \in \{1, \cdots, N\}$, codebook $\mathcal{C}_n$ is randomly partitioned into $2^{\eta \mathcal{R}_{\mathrm{C}_n}}$ bins, with

$$\mathcal{R}_{\mathrm{C}_n} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{\mathrm{c}_{n^*}}|^2 P_{\mathrm{c}}}{\sigma^2_{\mathrm{C}_{n^*}} + \sum_{i=1}^{K_{\mathrm{S}}} |h_{\mathrm{d}_{i,n^*}}|^2 P_{\mathrm{d}}}\right) - \Pr[n^* = n] \right.\right.$$
$$\left.\left. \times \log\left(1 + \frac{|g_{\mathrm{c}_{m^*}}|^2 P_{\mathrm{c}}}{\sigma^2_{\mathrm{E}_{m^*}} + \left(\sum_{i=1}^{K_{\mathrm{S}}} |g_{\mathrm{d}_{i,m^*}}|^2 + \Omega_{m^*}\right) P_{\mathrm{d}}}\right) \middle| n^* = n \right] \right\}^+ - \delta_1,$$

such that each bin contains $2^{\eta \mathcal{R}_{\mathrm{e,c}_{m^*}}}$ codewords, with $\mathcal{R}_{\mathrm{e,c}_{m^*}}$ being the corresponding information leakage rate. The BS encodes the message tuple $(w_{\mathrm{C}_1}, \cdots, w_{\mathrm{C}_N})$ into codeword x^{η}_{C}. At time instant t, the BS transmits codeword $x^{\eta}_{\mathrm{C}}(t)$ corresponding

to message $w_{\mathrm{C}_{n^*}}$. The error probability analysis are based on joint typicality and follows along similar lines as for the standard Gaussian wiretap channel [7]. Now, we need to prove $\forall m \in \{1,\cdots,M\}$, $\mathcal{R}_{\mathrm{e},\mathrm{c}_m} \geq \mathcal{R}_{\mathrm{C_{sum}}} - \epsilon$. On one hand, we have

$$\begin{aligned}
\eta\mathcal{R}_{\mathrm{e},\mathrm{c}_{m^*}} =& H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N}|Y^{\eta}_{\mathrm{E}_{m^*}},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}})\\
\geq& H(X^{\eta}_{\mathrm{C}}|\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}) - H(X^{\eta}_{\mathrm{C}}|W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N},Y^{\eta}_{\mathrm{E}_{m^*}},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}})\\
&+H(Y^{\eta}_{\mathrm{E}_{m^*}}|X^{\eta}_{\mathrm{C}},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}) - H(Y^{\eta}_{\mathrm{E}_{m^*}}|\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}) \qquad (12)\\
\geq& H(X^{\eta}_{\mathrm{C}}|\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}) - I(X^{\eta}_{\mathrm{C}};Y^{\eta}_{\mathrm{E}_{m^*}}|\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}) - \eta\epsilon_1, \qquad (13)
\end{aligned}$$

with $\mathbf{\Gamma}^{\eta}=[\mathbf{\Gamma}^{\eta}_{\mathrm{C}}\ \mathbf{\Gamma}^{\eta}_{\mathrm{D}}]$, $\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}} = \left[g^{\eta}_{\mathrm{c}_{m^*}}\ \mathbf{G}^{\eta}_{\mathrm{D}_{m^*}}\ \mathbf{G}^{\eta}_{\mathrm{A}_{m^*}}\right]$, and where (13) is obtained using Fano's inequality. Then, using the described coding scheme, we get $\eta\mathcal{R}_{\mathrm{e},\mathrm{c}_{m^*}} \geq \eta\sum_{n=1}^{N}\mathcal{R}_{\mathrm{C}_n} - \eta\epsilon_1$. On the other hand, since the eavesdropper with the best SINR has better chances to decode the information, we can write

$$\begin{aligned}
\forall m \in \{1,\cdots,M\},\ \ & H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N}|Y^{\eta}_{\mathrm{E}_m},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_m})\\
&\geq H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N}|Y^{\eta}_{\mathrm{E}_{m^*}},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}}). \qquad (14)
\end{aligned}$$

Then, using the fact that $\sum_{n=1}^{N}\mathcal{R}_{\mathrm{C}_n} = \mathcal{R}_{\mathrm{C_{sum}}} - n\delta_1$, and the inequality in (14), we obtain

$$\forall m \in \{1,\cdots,M\}, \qquad \mathcal{R}_{\mathrm{e},\mathrm{c}_m} \geq \mathcal{R}_{\mathrm{C_{sum}}} - \overbrace{(n\delta_1+\epsilon_1)}^{\epsilon}. \qquad (15)$$

Appendix B
Proof of Theorem 2

Due to space limitations, we skip the codebook generation, the encoding, and the decoding process here. For the secrecy analysis, since the D2D system has to ensure that both the cellular and the D2D transmissions are jointly secured against the eavesdroppers, we need to prove that, given the cellular system's transmission rates, the secondary transmissions guarantees secrecy up to the joint equivocation rate, i.e., $\forall m, \mathcal{R}_{\mathrm{e}_m} \geq \mathcal{R}_{\mathrm{C_{sum}}} + \sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k} - \epsilon'$. We have

$$\eta\mathcal{R}_{\mathrm{e}_m} = H(W_{\mathrm{C}_1},\cdots,W_{\mathrm{C}_N},W_{\mathrm{D}_1},\cdots,W_{\mathrm{D}_{K_{\mathrm{S}}}}|Y^{\eta}_{\mathrm{E}_m},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_m}).$$

Using a similar reasoning as in Appendix A, we can show that

$$\begin{aligned}
\eta\mathcal{R}_{\mathrm{e}_m} \geq& \sum_{t=1}^{\eta}\Big[H(X_{\mathrm{C}}(t),X_{\mathrm{D}_1}(t),\cdots,X_{\mathrm{D}_{K_{\mathrm{S}}}}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t))\\
&-I(X_{\mathrm{C}}(t),X_{\mathrm{D}_1}(t),\cdots,X_{\mathrm{D}_{K_{\mathrm{S}}}}(t);Y_{\mathrm{E}_m}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t))\Big] - \eta\epsilon'_1, \qquad (16)
\end{aligned}$$

Then, given the mutual independence of the codewords $X_{\mathrm{C}}(t)$, $X_{\mathrm{D}_1}(t),\cdots$, and $X_{\mathrm{D}_{K_{\mathrm{S}}}}(t)$, we have

$$\begin{aligned}
&H(X_{\mathrm{C}}(t),X_{\mathrm{D}_1}(t),\cdots,X_{\mathrm{D}_{K_{\mathrm{S}}}}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t)) = \qquad (17)\\
&\qquad H(X_{\mathrm{C}}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t)) + \sum_{k=1}^{K_{\mathrm{S}}}H(X_{\mathrm{D}_k}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t)).
\end{aligned}$$

On one hand, we have

$$\begin{aligned}
&\sum_{t=1}^{\eta}\Big[H(X_{\mathrm{C}}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t)) - I(X_{\mathrm{C}}(t);Y_{\mathrm{E}_m}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t))\Big]\\
&\geq \eta\mathcal{R}_{\mathrm{C_{sum}}} - \eta\epsilon, \qquad (18)
\end{aligned}$$

where (18) is obtained in Appendix A. On the other hand, since the eavesdropper with the best SINR has better chances to decode the messages, we have

$$\begin{aligned}
&\sum_{t=1}^{\eta}\sum_{k=1}^{K_{\mathrm{S}}}\Big[H(X_{\mathrm{D}_k}(t)|\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t)) -\\
&I(X_{\mathrm{D}_k}(t);Y_{\mathrm{E}_m}(t)|X_{\mathrm{C}}(t),X_{\mathrm{D}_1}(t),\cdots,X_{\mathrm{D}_{k-1}}(t),\mathbf{\Gamma}(t),\mathbf{\Gamma}_{\mathrm{E}_m}(t))\Big]\\
&\geq \sum_{k=1}^{K_{\mathrm{S}}}\Big[H(X^{\eta}_{\mathrm{D}_k}|\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_m})\\
&- I(X^{\eta}_{\mathrm{D}_k};Y^{\eta}_{\mathrm{E}_{m^*}}|X^{\eta}_{\mathrm{C}},X^{\eta}_{\mathrm{D}_1},\cdots,X^{\eta}_{\mathrm{D}_{k-1}},\mathbf{\Gamma}^{\eta},\mathbf{\Gamma}^{\eta}_{\mathrm{E}_{m^*}})\Big] \qquad (19)\\
&= \eta\sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k}. \qquad (20)
\end{aligned}$$

Substituting (20) and (18) in (16), we obtain

$$\mathcal{R}_{\mathrm{e}_m} \geq \mathcal{R}_{\mathrm{C_{sum}}} + \sum_{k=1}^{K_{\mathrm{S}}}\mathcal{R}_{\mathrm{D}_k} - \overbrace{(\epsilon+\epsilon'_1)}^{\epsilon'}. \qquad (21)$$

References

[1] A. Osseiran, J. Monserrat, and P. Marsch, *5G Mobile and wireless communications technology*. Cambridge University Press, 2016.

[2] J. Mitola, "Cognitive radio for flexible mobile multimedia communication," in *Proc. IEEE Int. Workshop on Mobile Multimedia Commun. (MoMuC'99)*, San Diego, CA, USA, 1999, pp. 3–10.

[3] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[4] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, Nov.r 2014.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–719, Oct. 1949.

[6] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

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

[11] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[12] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[13] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[14] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[15] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, no. 99, Jan. 2017.

[16] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[17] O. O. Koyluoglu and H. E. Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[18] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735 – 2751, Jun. 2008.

[19] A. Hyadi, Z. Rezki, F. Labeau, and M.-S. Alouini, "Joint secrecy for D2D communications underlying cellular networks," in *Proc. IEEE Global Commun. Conf. (Globecom'2017)*, Singapore, Dec. 2017.

[20] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.