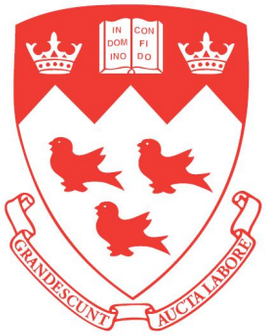
McGill University

(845 Sherbrooke St W, Montreal, QC H3A 0G4)



Optimal Device Selection in Spectrum Sharing Channel under Energy Harvesting Aided D2D Communication

Project Report

by

Shashank Murugesh

McGill ID: 260786369

Supervisor: **Prof. Fabrice Labeau**

A report presented for the degree of

Master of Engineering

Department of Electrical and Computer Engineering

August 28, 2020

Abstract

Spectrum sharing and device-to-device (D2D) communications are among the key enablers of the upcoming modern communication networks. These new technologies have gained widespread attention in cellular network standards for proximity communication as a means to improve cellular spectrum utilization. However, due to the broadcast nature of wireless communication, the information exchange between wireless devices is susceptible to numerous attacks.

In this project, we are interested in investigating physical layer security in the spectrum sharing channel when both the primary cellular and the underlying Energy Harvesting (EH) aided D2D secondary systems are interested in transmitting secret messages. The considered system model consists of a multi-user cellular system and an underlying secondary system comprising K EH-aided D2D pairs. All cellular and EH-aided D2D transmissions are subject to an eavesdropping attack. Given the primary's secrecy condition, K_S devices transmit secret messages and K_J devices operate as friendly jammers. The presented results are for two scenarios: In the first case, each EH-aided D2D pair have enough energy to transmit secret messages; however, the transmission of jamming signals is constrained by the amount of energy harvested. In the second case, we divide the device transmission operation time into multiple sub-slots, and each D2D pair utilizes its harvested energy to transmit secret messages or send jamming signals. For each scenario, we propose a device selection scheme to determine the optimal number of devices (K_S and K_J), that maximizes the secrecy throughput of the secondary system while satisfying the primary's secrecy sum-rate condition. The obtained results show that the proposed device selection model improves the primary secrecy performance while also allowing secret transmission for the underlying EH-aided D2D communication.

Acknowledgements

I am very fortunate to have had the support of the department, family, friends and colleagues near and far. Without this support, this project would not have been possible.

First of all, I would like to thank my supervisor, Professor Fabrice Labeau, for his continuous support and guidance during my graduate study. Every meeting has contributed to the progress of my project. His patience and understanding are also what makes this journey more enlightening and rewarding. I also want to thank my fellow researcher, Amal Hyadi, for her helpful suggestions and all the insightful discussions we had.

I would like to thank all my friends and lab colleagues for their help and encouragement throughout my studies. My special thanks to Nishanth, Barleen and Simita for all the time we spent cooking, chatting, discussing, playing, caring, and doing all the fun stuff together. My life away from home would not have been so wonderful without your company and support.

Last but not least, I would like to thank my parents and my sister for their unconditional love and support that give me the strength, energy, and motivation to achieve my goal and finish my degree.

Contents

List of Figures

List of Tables

List of Algorithms

1

Introduction

Widespread use of smartphones and mobile-ready portables, such as laptops or tablets, has led to a tremendous surge in demand for mobile data traffic. According to Cisco VNI global mobile data traffic report [1], by 2022, total data traffic is predicted to be 77 exabytes per month at a compound annual growth rate of 46 percent, illustrated in Fig. 1.1. In addition, smartphones will account for 90% share of total mobile data traffic [1]. This unprecedented increase in data traffic creates many challenges for existing cellular networks; one such problem is the lack of available radio spectrum.

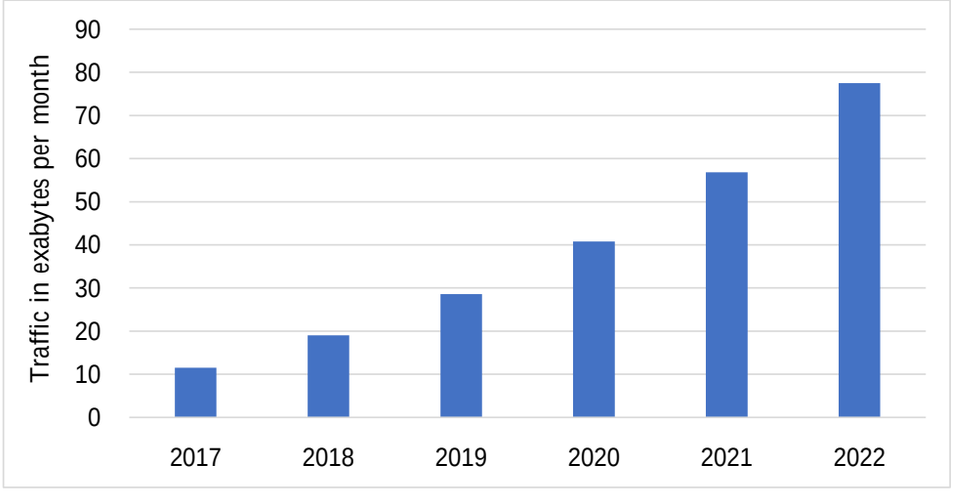


Figure 1.1: Mobile data traffic growth prediction [1]

1.1 Cellular Spectrum Usage

Driven by the steady increase in the number of wireless users as well as the proliferation of new wireless services, the demand for radio spectrum has increased dramatically. With most of the spectrum already utilized, it is becoming extremely hard to find a vacant band. However, this spectrum scarcity is mainly due to inefficient allocation rather than a physical shortage. Studies in the past [2, 3, 4], have shown that the available licensed radio spectrum is becoming more occupied, while the assigned spectrum is significantly under-utilized. The licensed users do not use their spectrum in all locations and all times. This scarcity and inefficiency of the spectrum usage necessitates a new communication paradigm to exploit the available spectrum opportunistically.

1.2 5G Networks and Key Enabling Technologies

The challenging design objective of the 5G network is to provide connectivity to more than one trillion devices with diverse characteristics and application requirements. Undoubtedly, there are many new concepts and design criteria, including spectrum sharing and D2D communication, that have been proposed for 5G, if implemented, can bring fundamental changes at the architectural level.

1.2.1 Spectrum Sharing

Under the umbrella of cognitive radio systems, Spectrum sharing, offers secondary users the ability to access the licensed spectrum in an opportunistic manner [5]. Moreover, it seems to be the perfect solution to address the spectrum challenges that the 5G system would face [6]. The main objective of spectrum sharing is to increase spectral efficiency based on a use-it or share-it, where primary users can share available spectrum with secondary users. This sharing is done based on predefined conditions to maximize the spectrum utilization and minimize the interference caused to primary users [7]. A prevalent use case of spectrum sharing is when the secondary system allows D2D transmissions among its users [8]

1.2.2 D2D Communication

Device-to-Device (D2D) communications emerged from the concept of cooperative communications and came into the spotlight when it was considered one of the key enabling technologies for 5G. D2D communication in cellular networks brings several benefits to both mobile users and network operators:

1. Users can experience high data rates, low latency, and reduced energy consumption because of a) the direct short-range communication and b) its potentially favourable propagation conditions.

2. The cellular-coverage range can be extended without additional infrastructure cost.

3. By allowing spectrum reuse between traditional cellular communications and direct D2D communications, spectrum efficiency can be enhanced [9].

4. As D2D communication offers the opportunity for local management of short-distance transmissions; it allows data offloading from the base station, easing network congestion and traffic management effort at the central nodes [10].

Given all these promising advantages, the integration of D2D communication in future cellular networks has become an attractive research area. However, due to the exposed nature of wireless communication, the information exchange between D2D users are susceptible to numerous attacks. Secure wireless communication needs to assure authenticity, privacy, confidentiality, integrity, and availability [11] to protect from a number of attacks, including Denial of Service, masquerading, eavesdropping [12].

Additionally, these devices move from one place to another [13], making power cable connection difficult. The rechargeable battery is a conventional power source for such portable devices; hence the lifetime will be a bottleneck for these power-limited devices. Energy harvesting (EH) has been considered as one of the promising energy solutions in D2D communication, attracting many academic and industrial researchers. Although there are few studies on EH-aided D2D communications, there are still many cases of interest, where more research is needed.

1.3 Project Objective

This project's main objective is to investigate physical layer security in the spectrum sharing channel where both primary and EH-aided secondary devices are interested in transmitting secret messages. First, we will review the achievable secrecy rates for both the primary cellular systems and the underlying D2D secondary transmission system when subject to an eavesdropping attack when there is no energy limitation on the devices in the D2D system [14]. Then, we extend the work to investigate the optimality of sharing cellular spectrum with an EH-aided underlying D2D system when both systems are interested in transmitting secret data. We propose an optimal device selection scheme to potentially improve the secrecy performance of both cellular system and EH-aided D2D pairs.

1.4 Project Outline

The project is organized as follows: Chapter 2 reviews the literature on physical layer security, device-to-device communications and energy harvesting aided D2D communications. Chapter 3 reviews a secrecy perspective of the spectrum sharing channel, introduces the communication system model, and analyzes secrecy sum rates of the cellular system with an underlying D2D system [14]. Chapter 4 investigates the optimality of sharing the cellular spectrum with the underlying EH-D2D network and presents simulation results. Finally, Chapter 5 concludes the work.

2

Background and Literature Review

Recent technological proposals in wireless communication have brought many innovative solutions in improving service quality and network efficiency of wireless systems. However, these technologies are still facing multiple challenges that hinder the reveal of their full potential. Lack of security is among these challenges to beat. It is the most critical element involved in enabling the growth of the wide range of wireless data networks and applications, including spectrum sharing and D2D communications. Therefore, with the proliferation of more complex modern infrastructure systems, there is an increasing need for secure communication solutions.

2.1 Physical Layer Security

Traditional cryptographic encryption techniques require a certain form of shared information (i.e. shared key) between the transmitter and the legitimate receiver to achieve security [15]. Moreover, this technique assumes that the communication of the secret key is error-free. However, error-free communication cannot always be guaranteed in non-deterministic wireless channels[16]. More importantly, cryptographic protocols are heavily based on unproven assumptions such as hardness of factoring large primes [17]. Because of improvements in computers' computing abilities and breaking encryption algorithms, there are concerns that such security methods no longer suffice. Furthermore, the use of data encryption/decryption algorithms introduces communication latency, high computational loads, and signalling overhead [18], all of which are unfavourable to the 5G network.

Physical Layer Security (PLS), a novel approach for wireless security, aims to ensure secure communications by exploiting the unique characteristics of the physical medium between communicating nodes. From a fundamental point of view, a natural way to approach the PLS problem is through information theory, which provides techniques to derive limits in the transmission capacity. Unlike the cryptography that ignores the difference between the received signals at different receivers, the physical layer security is achieved by exploring the differences between the physical properties of signal channels to achieve secrecy. To illustrate the general concept of physical layer security, Fig. 2.1 shows the typical example of a three-node network, which consists of three members, including a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve).

In 1975 [19] Wyner initiated the study of physical layer security from a basic wire-tap channel, where Alice transmits a message to Bob through a discrete memoryless channel and another malicious node called Eve eavesdrops this message through another degraded version of the discrete memoryless channel. Wyner's results shows that a confidential message can be exchanged between Alice and Bob with a positive secrecy capacity if the Alice-to-Eve's signal is a degraded version of Alice-to-Bob's signal. Later, as an extension of Wyner's work, Csiszar and Korner in [20] studied the non-degraded channels and showed that is is possible to achieve a non-zero secrecy capacity if the main channel (Alice-to-Bob) is less noisy or more capable than the wiretapper channel (Alice-to-Eve). In [21], author calculates the secrecy capacity of a Gaussian wiretap channel as the difference between the

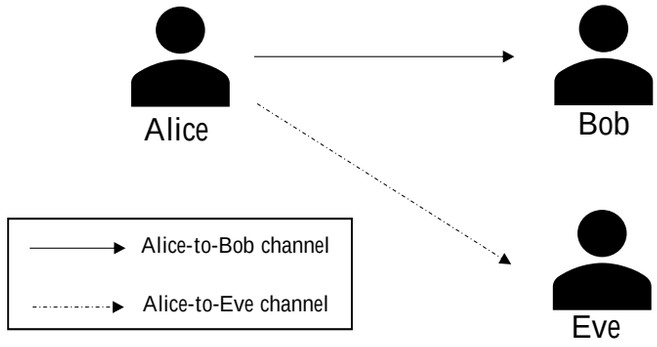


Figure 2.1: Illustration of eavesdropping scenario

capacities of Alice-to-Bob channel and Alice-to-Eve channel, given by

$$C_S = C_{AB} - C_{AE} \tag{2.1}$$

where $C_{AB} = \log_2(1+P/\sigma_{AB})$ is the Shannon capacity of Alice-to-Bob channel, $C_{AE} = \log_2(1+P/\sigma_{AE})$ is the Shannon capacity of Alice-to-Eve channel, P denotes the transmit power, and σ_{AB} and σ_{AE} are the noise power of Alice-to-Bob channel and Alice-to-Eve channel, respectively. Since Gaussian channel is time-invariant, it is notable that the non-zero secrecy capacity exists only when the received signal-to-noise ratio (SNR) at Bob is greater than that at Eve (*i.e.*, $P/\sigma_{AB} > P/\sigma_{AE}$).
In a quasi-static flat fading channel, the gains of Alice-to-Bob channel and Alice-to-Eve channel change randomly over different time slots but remain constant in each slot. Thus, the secrecy capacity for one realization of the quasi-static flat fading wiretap-channel is given by [22]

$$C_s = \begin{cases} \log_2\left(1 + |h_{AB}|^2 \frac{P}{\sigma_{AB}}\right) - \log_2\left(1 + |h_{AE}|^2 \frac{P}{\sigma_{AE}}\right), & \text{if } \gamma_B > \gamma_E; \\ 0, & \text{if } \gamma_B \leq \gamma_E; \end{cases} \tag{2.2}$$

where $|h_{AB}|$ and $|h_{AE}|$ denote the complex channel coefficients of Alice-to-Bob channel and Alice-to-Eve channel and γ_B and γ_E are the SNR at Bob and at Eve respectively. In [20], the capacity-secrecy tradeoff is characterized in extending wiretap channel to the broadcast channel. Afterwards, information theoretical results for secure communications are derived for several wireless networks [23, 24]. The secrecy rate of single-input single-output (SISO) fading channels [25, 26], Gaussian multiple access channels [27], interference channels [28, 29] and relay channels [30, 31] have been studied.

2.2 Physical Layer Security in D2D Communications

D2D communication is a promising concept that can provide several advantages such a low cost, plug-and-play convenience, and flexibility. In contrast, allowing D2D communication may bring interference to the cellular links, especially when it shares resources with the cellular system. Usually, the interference is a negative component in the cellular network. However, the interference caused by the D2D system can be advantageous to cellular transmission in terms of physical layer security [32].

There have been several works to enhance network security from the physical layer when the cellular system shares resources with D2D. In [32], the spectral efficiency of D2D users was maximized with the minimum secrecy outage probability of cellular users guaranteed. In [33], the secrecy sum rate of all the cellular users were maximized using joint power and access control technique. In [34], selection methods for the relay and the jammer were developed in order to minimize the secrecy outage probability. A comprehensive review to address the fundamental security and privacy issues in D2D communication can be found in [35]. In a block-fading channel, the author in [36] considers three scenarios between the primary and the secondary systems and for each scenario, the author derives an achievable ergodic secrecy rate.

2.3 Energy Harvesting aided D2D Communications

Although there have been several research studies on D2D communication, only a few studies have focused on EH-based D2D communications. In [37], the modelling and analysis for the random and prioritized access policy have been proposed for cognitive and EH-based D2D communications. In [38], a system with user-equipment relaying was considered for enhancing reliable communication, and the status of harvested energy was modelled using the Markov chain. In [39], D2D relays are equipped with EH to compensate and forward data for machine-type communications. An author in [40], proposed three wireless power transfer policies to study the security issue in D2D communication.

3

Spectrum Sharing Channel: A Secrecy Perspective

In this chapter, we summarize the optimality of sharing cellular spectrum with the underlying D2D network when both the systems are interested to send secret messages by reviewing [14].

3.1 Communication System Model

The system model in [14] consists of multi-user spectrum sharing system where both primary and secondary systems are subjected to eavesdropping attack.

The primary cellular system is composed of a base station and N cellular user. The base station transmits N secret message W_{C_n}, $n \in \{1, \ldots, N\}$ to the corresponding n^{th} cellular user in the presence of M eavesdroppers such that each message is kept secret from all eavesdroppers. To enhance its secrecy throughput, the primary system share its spectrum with the underlying D2D system.

The underlying secondary system comprises K D2D pairs, each of which is interested in establishing secret transmission. To avoid interference and improve secrecy performance, the primary system would require the secondary system to satisfy a secrecy throughput constraint. So, only K_S out of K D2D pairs are allowed to communicate their secret message W_{D_i}, $i \in \{1, \ldots, K_S\}$ so as to satisfy primary secrecy constraint. Not only to increase its chance to get access to spectrum but also to improve its secrecy rate, the secondary system uses $K - K_S$ transmitting devices to send friendly jamming signals.

The respective received signals at the n^{th} cellular user, $n \in \{1, ..., N\}$, the i^{th} secondary device

receiver, $i \in 1, ..., K_S$, and the m^{th} eavesdropper, $m \in \{1, ..., M\}$, are given by

$$\begin{aligned} Y_{C_n} &= h_{c_n} X_C + \mathbf{L}_{D_n} \mathbf{X}_D + \mathbf{L}_{A_n} \mathbf{X}_J + n_{C_n} \\ Y_{D_i} &= h_{d_i} X_{D_i} + l_{c_i} X_C + \hat{\mathbf{L}}_{D_i} \hat{\mathbf{X}}_D + \hat{\mathbf{L}}_{A_i} \mathbf{X}_J + n_{D_i} \\ Y_{E_m} &= g_{c_m} X_C + \mathbf{G}_{D_m} \mathbf{X}_D + \mathbf{G}_{A_m} \mathbf{X}_J + n_{E_m} \end{aligned} \tag{3.1}$$

where X_C is the primary signal transmitted by the basestation, $\mathbf{X}_D$ is the vector of secondary secret data signals,i.e., $\mathbf{X}_D = [X_{D_1} \dots X_{D_{K_S}}]^T$, $\hat{\mathbf{X}}_D = [X_{D_1} \dots X_{D_{p-1}}, X_{D_{p+1}} \dots X_{D_{K_S}}]^T$, $\mathbf{X}_J$ is the vector of secondary jamming signals, i.e., $\mathbf{X}_J = [X_{J_1} \dots X_{J_{K-K_S}}]^T$, $\mathbf{L}_{D_n}$, $\mathbf{L}_{A_n}$, $\hat{\mathbf{L}}_{D_i}$, $\hat{\mathbf{L}}_{A_i}$, $\mathbf{G}_{D_m}$, and $\mathbf{G}_{A_m}$ are vectors of channel gains, i.e., $\mathbf{L}_{D_n} = [l_{d_{1,n}} \dots l_{d_{K_S,n}}]$, $\mathbf{L}_{A_n} = [l_{a_{1,n}} \dots l_{a_{K-K_S,n}}]$, $\hat{\mathbf{L}}_{D_i} = [\hat{l}_{d_{1,i}} \dots \hat{l}_{d_{p-1,i}}, \hat{l}_{d_{p+1,i}} \hat{l}_{d_{K_S,i}}]$, $\hat{\mathbf{L}}_{A_i} = [\hat{l}_{a_{1,i}} \dots \hat{l}_{a_{K-K_S,i}}]$, $\mathbf{G}_{D_m} = [g_{d_{1,m}} \dots g_{d_{K_S,m}}]$, $\mathbf{G}_{A_m} = [g_{a_{1,m}} \dots g_{a_{K-K_S,m}}]$, 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.

3.2 Jamming Signals Generation

As discussed in section 3.1, the D2D network consists of K D2D pairs in which K_S secondary device transmit secret messages to their respective receivers while the remaining $K - K_S$ secondary device transmits jamming signals. 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:

$$\hat{\mathbf{L}}_A \mathbf{X}_J = 0 \tag{3.2}$$

$$\mathbf{L}_{A_{n^*}} \mathbf{X}_J = 0 \tag{3.3}$$

with $\hat{\mathbf{L}}_A = \left[\hat{\mathbf{L}}_{A_1}^\intercal \dots \hat{\mathbf{L}}_{A_{K_S}}^\intercal\right]$, $\hat{\mathbf{L}}_{A_{n^*}} = \left[l_{a_{1,n^*}} \dots l_{a_{K-K_S,n^*}}\right]$ and n^* represents the index for the optimal cellular user to transmit to. Let $\mathbf{W}$ be an orthonormal basis for null $\left(\left[\hat{\mathbf{L}}_A \ \mathbf{L}_{A_{n^*}}\right]^\intercal\right)$ Then, we can write,

$$\mathbf{X}_J = \mathbf{W}\mathbf{V} \tag{3.4}$$

where $\mathbf{V}$ is a random Gaussian vector satisfying $\mathbb{E}[\mathbf{V}\mathbf{V}^*] = P_d\mathbf{I}_{K-2K_S-1}$. To ensure that Eqs 3.2 and 3.3 could be solved, the number of devices allowed to secretly transmit should satisfy $K_S \leq \lfloor \frac{K-1}{2} \rfloor$

Using Eqs. 3.2 , 3.3 and 3.4 we can re-write the system of equations as follows:

$$\begin{aligned} Y_{C_{n^*}} &= h_{c_{n^*}} X_C + \mathbf{L}_{D_{n^*}} \mathbf{X}_D + n_{C_{n^*}} \\ Y_{D_i} &= h_{d_i} X_{D_i} + l_{c_i} X_C + \hat{\mathbf{L}}_{D_i} \hat{\mathbf{X}}_D + n_{D_i} \\ Y_{E_m} &= g_{c_m} X_C + \mathbf{G}_{D_m} \mathbf{X}_D + \mathbf{G}_{A_m} \mathbf{X}_J + n_{E_m} \end{aligned} \tag{3.5}$$

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

3.3 Secrecy Sum-Rates

In this section, we present the secrecy sum-rates results of primary cellular and secondary D2D systems, as discussed in [14] The results are derived based on the following assumptions: all the channel gains are considered to be independent, ergodic and stationary. Besides this, the instantaneous channel state information (CSI) of the legitimate receivers is globally known. 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.

Secrecy sum-rate for three cases are discussed: 1) Multi-user cellular system with no D2D transmission. 2) Multi-user primary cellular system with D2D transmission. 3) Underlying D2D system with secret data transmission and jamming devices. The following results are based on [14].

Case 1: Secrecy sum-rate for multi-user cellular system with no D2D transmission. Secrecy achieving scheme for the multi-user wiretap channel consists of using an opportunistic communication approach. Here, the cellular system uses a time division multiplexing scheme and the base station instantaneously selects one cellular receiver to transmit its message. The secrecy achieving coding scheme consists of using independent standard single user wiretap codebooks.

Theorem 1. *An achievable secrecy sum-rate for the multi-user cellular system with no D2D transmission is given by [41]*

$$\mathcal{R}_{C_{sum}}^{no\text{-}D2D} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{c\text{-}\max}|^2}{\sigma^2_{C\text{-}\max}} P_c\right) - \log\left(1 + \frac{|g_{c\text{-}\max}|^2}{\sigma^2_{E\text{-}\max}} P_c\right)\right]\right\}^+ \tag{3.6}$$

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

Case 2: Secrecy sum-rate for multi-user primary cellular system with D2D transmission.

In this case, the opportunistic transmission model approach is used to derive achievable secrecy sum-rate as it takes advantage in dealing with the interference engendered by the transmission of the other messages, especially when the cellular users have no successive interference cancellation capabilities. Since there is 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).

Theorem 2. *An achievable secrecy sum-rate for the multi-user cellular system, described in Eq. 3.5 with* K_S *underlying D2D transmissions and* $K - K_S$ *friendly jamming devices. is given by*

$$\mathcal{R}_{C_{sum}} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{c_{n^*}}|^2 P_c}{\sigma^2_{C_{n^*}} + \sum_{i=1}^{K_S}\left|l_{d_{i,n^*}}\right|^2 P_d}\right) - \log\left(1 + \frac{|g_{c_{m^*}}|^2 P_c}{\sigma^2_{E_{m^*}} + \left(\sum_{i=1}^{K_S}\left|g_{d_{i,m^*}}\right|^2 + \Omega_{m^*}\right) P_d}\right)\right]\right\}^+, \tag{3.7}$$

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

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

Proof. The achievable secrecy sum-rate for Eq. 3.7 can be proved by showing $\mathcal{R}_{e,c_m} \geq \mathcal{R}_{C_{sum}}\text{-}\epsilon$, $\forall m \in \{1, \ldots, M\}$, where $\mathcal{R}_{e,c_m}$ is the information leakage rate and $\epsilon > 0$, presented in [14] □

Case 3: Underlying D2D system with secret data transmission and jamming devices.

In the underlying D2D system, 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 $K - K_S$ device transmitters send friendly jamming signals. 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 3. *A jointly achievable secrecy sum-rate for the underlying D2D system, described in Eq. 3.5 with K_S underlying D2D transmissions and $K - K_S$ friendly jamming devices. is given by*

$$\mathcal{R}_{D_k} = \left\{ \mathbb{E}\left[\log\left(1 + \frac{|h_{d_k}|^2 P_d}{\sigma^2_{D_k} + |l_{c_k}|^2 P_c + \sum_{\substack{p=1 \\ p\neq k}}^{K_S} |\hat{l}_{d_{p,k}}|^2 P_d} \right) \right.\right. \\ \left.\left. - \log\left(1 + \frac{|g_{d_{k,m_k^*}}|^2 P_d}{\sigma^2_{E_{m_k^*}} + \left(\sum_{p=k+1}^{K_S} |g_{d_{p,m_k^*}}|^2 + \Omega_{m_k^*} \right) P_d} \right) \right] \right\}^+, \tag{3.8}$$

with $k \in \{1, \ldots, K_S\}$, K_S satisfying $K_S \leq \lfloor \frac{K-1}{2} \rfloor$, $\Omega_{m_k^*} = G_{A_{m_k^*}} W W^\dagger G^\dagger_{A_{m_k^*}}$ and where m_k^* is given by

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

Proof. The achievable secrecy sum-rate for Eq. 3.8 can be proved by showing $\mathcal{R}_e \geq \mathcal{R}_{C_{sum}} + \sum_{k=1}^{K_S} R_{D_k} - \epsilon'$, $\forall m \in \{1, \ldots, M\}$, where $\mathcal{R}_{C_{sum}}$ is the cellular systems transmission rate, $\mathcal{R}_e$ is the joint equivocation rate and $\epsilon' > 0$, presented in [14] □

3.4 Optimal Device Selection

To maximize the secondary secrecy throughput and meet the primary secrecy requirement, we need to find the optimal number of K_S data transmitting devices in the underlying D2D network. In this section, we discuss the choice for the primary's secrecy threshold and formulate the optimal device selection problem.

3.4.1 Primary's secrecy threshold condition.

The primary cellular system allows K_S D2D pairs to share spectrum and transmit secret messages as long as it satisfy the following condition:

$$\mathcal{R}_{C_{sum}}(K_S) \geq \mathcal{R}_{th} \tag{3.9}$$

where $\mathcal{R}_{C_{sum}}(K_S)$ is the secrecy sum-rate of primary cellular system, for given K_S D2D transmitter and $K - K_S$ jamming devices, $\mathcal{R}_{th}$ is the secrecy sum-rate threshold.

Depending on the secrecy sum-rate requirement, primary can choose $\mathcal{R}_{th}$ value. An interesting choice for the primary secrecy sum-rate threshold is:

$$\mathcal{R}_{th} = \beta \ \mathcal{R}_{C_{sum}}^{no\text{-}D2D} \quad \beta \geq 0 \tag{3.10}$$

where $\mathcal{R}_{C_{sum}}^{no\text{-}D2D}$ is the secrecy sum-rate of cellular system with no D2D transmission.

3.4.2 Problem statement

Given the primary's secrecy sum-rate condition, find the optimal number of devices K_S^* that maximizes the secondary secrecy throughput, i.e.

$$K_S^* = \begin{cases} \underset{1 \leq K_S \leq \lfloor \frac{K-1}{2} \rfloor}{\text{argmax}} \ \sum_{k=1}^{K_S} \mathcal{R}_{D_k} \\ \text{subject to} \quad \mathcal{R}_{C_{sum}}(K_S) \geq \mathcal{R}_{th} \end{cases} \tag{3.11}$$

3.4.3 Device Selection Scheme Algorithm

Considering the complexity of the expressions of $\mathcal{R}_{C_{sum}}$ and $\mathcal{R}_{D_k}$, finding optimal solution to the problem in Eq. 3.11 is hard to do analytically. Thus the author [14] use a revised exhaustive search algorithm to select the optimal number of devices K_S.

The selection algorithm is as follows:[14]

Algorithm 1: Revised Exhaustive Search Selection (R-ESS)

Input : K, R_{th}
Output : K_S
Let $\mathcal{C}$ be set of all combination of K_S out of K elements with $K_S = 1, \ldots, \lfloor \frac{K-1}{2} \rfloor$; **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 $R_{C_{sum}}(i)$ for the i^{th} combination;
    if $R_{C_{sum}}(i) \geq R_{th}$ **then**
      Compute the secondary secrecy rate $R_{D_k}(i), k \in \{1, \ldots, K_S\}$;
      if $R_{D_k}(i) \neq 0$ **then**
        $(i) \in \mathcal{L}_{\mathcal{C}}$;
    else
      $\mathcal{C}(i) = \emptyset, \forall j \in \left\{1, \ldots, \sum_{K_S=1}^{\lfloor \frac{K-1}{2} \rfloor} \binom{K}{K_S}\right\}$
      such that $\mathcal{C}(i) \subset \mathcal{C}(j)$
if $\mathcal{L}_{\mathcal{C}} \neq 0$ **then**
  Choose the combination in $\mathcal{L}_{\mathcal{C}}$ that maximizes $\sum_{k=1}^{K_S} R_{D_k}(i, j)$;
  Return the corresponding K_S and K_J;
else
  $K_S = 0$; `/* No D2D Transmission */`

The simulation results in [14] illustrated that the proposed model enhances the secrecy performance of the primary cellular system while allowing secret transmission for the underlying D2D communication.

4

Optimal Device Selection: EH-aided D2D

Authors in [14] studied the optimality of sharing cellular spectrum with the underlying D2D system; however, they didn't consider EH. In this chapter, we propose an optimal scheme for device selection in a spectrum sharing channel, where the underlying D2D pairs have energy harvesting capabilities.

We consider two scenarios. In the first case, our goal is to maximize the secondary secrecy throughput, where each EH-D2D pair have enough energy to transmit secret messages; however, the transmission of jamming signals is constrained by the amount of energy harvested. In the second case, we divide the device transmission operation time into multiple sub-slots. Our goal is to maximize the long-term average of secondary secrecy throughput, where each D2D pair utilizes its harvested energy to transmit secret messages or send jamming signals.

4.1 Communication System Model

We consider the system model as discussed in section 3.1 with slight modifications as detailed below - The underlying secondary system is comprised of K D2D pairs, each of which is capable of harvesting energy, and each device is interested in establishing secret transmission. K_S out of K D2D pairs are allowed to communicate their secret message to satisfy primary secrecy constraint. K_J transmitting devices send friendly jamming signals while the remaining $K - (K_S + K_J)$ device remains idle.
The respective received signals at the n^{th} cellular user, $n \in \{1, ..., N\}$, the i^{th} secondary device

receiver, $i \in 1, ..., K_S$, and the m^{th} eavesdropper, $m \in \{1, ..., M\}$, are given by

$$\begin{aligned} Y_{C_n} &= h_{c_n} X_C + \mathbf{L}_{D_n} \mathbf{X}_D + \mathbf{L}_{A_n} \mathbf{X}_J + n_{C_n} \\ Y_{D_i} &= h_{d_i} X_{D_i} + l_{c_i} X_C + \hat{\mathbf{L}}_{D_i} \hat{\mathbf{X}}_D + \hat{\mathbf{L}}_{A_i} \mathbf{X}_J + n_{D_i} \\ Y_{E_m} &= g_{c_m} X_C + \mathbf{G}_{D_m} \mathbf{X}_D + \mathbf{G}_{A_m} \mathbf{X}_J + n_{E_m} \end{aligned} \tag{4.1}$$

where X_C is the primary signal transmitted by the base station, $\mathbf{X}_D$ is the vector of secondary secret data signals,i.e., $\mathbf{X}_D = [X_{D_1} \dots X_{D_{K_S}}]^T$, $\hat{\mathbf{X}}_D = [X_{D_1} \dots X_{D_{p-1}}, X_{D_{p+1}} \dots X_{D_{K_S}}]^T$, $\mathbf{X}_J$ is the vector of secondary jamming signals, i.e., $\mathbf{X}_J = [X_{J_1} \dots X_{J_{K_J}}]^T$, $\mathbf{L}_{D_n}$, $\mathbf{L}_{A_n}$, $\hat{\mathbf{L}}_{D_i}$, $\hat{\mathbf{L}}_{A_i}$, $\mathbf{G}_{D_m}$, and $\mathbf{G}_{A_m}$ are vectors of channel gains, i.e., $\mathbf{L}_{D_n} = [l_{d_{1,n}} \dots l_{d_{K_S,n}}]$, $\mathbf{L}_{A_n} = [l_{a_{1,n}} \dots l_{a_{K_J,n}}]$, $\hat{\mathbf{L}}_{D_i} = [\hat{l}_{d_{1,i}} \dots \hat{l}_{d_{p-1,i}}, \hat{l}_{d_{p+1,i}} \hat{l}_{d_{K_S,i}}]$, $\hat{\mathbf{L}}_{A_i} = [\hat{l}_{a_{1,i}} \dots \hat{l}_{a_{K_J,i}}]$, $\mathbf{G}_{D_m} = [g_{d_{1,m}} \dots g_{d_{K_S,m}}]$, $\mathbf{G}_{A_m} = [g_{a_{1,m}} \dots g_{a_{K_J,m}}]$, 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.

4.2 Jamming Signals Generation

Jamming signals are generated to affect only the eavesdroppers and cancel out at the cellular users and the secondary device receivers. This can be formulated as:

$$\hat{\mathbf{L}}_A \mathbf{X}_J = 0 \tag{4.2}$$

$$\mathbf{L}_{A_{n^*}} \mathbf{X}_J = 0 \tag{4.3}$$

with $\hat{\mathbf{L}}_A = \left[\hat{\mathbf{L}}_{A_1}^{\intercal} \dots \hat{\mathbf{L}}_{A_{K_S}}^{\intercal}\right]$, $\hat{\mathbf{L}}_{A_{n^*}} = \left[l_{a_{1,n^*}} \dots l_{a_{K_J,n^*}}\right]$ and n^* represents the index for the optimal cellular user to transmit to. Let $\mathbf{W}$ be an orthonormal basis for null $\left(\left[\hat{\mathbf{L}}_A \ \mathbf{L}_{A_{n*}}\right]^{\intercal}\right)$ Then, we can write,

$$\mathbf{X}_J = \mathbf{W}\mathbf{V} \tag{4.4}$$

where $\mathbf{V}$ is a random Gaussian vector satisfying $\mathbb{E}[\mathbf{V}\mathbf{V}^*] = P_d \mathbf{I}_{K_J - K_S - 1}$. To ensure that Eqs. 4.2 and 4.3 could be solved, the number of devices allowed to secretly transmit should satisfy $1 \leq K_S \leq K_J - 1$ and $2 \leq K_J \leq K - 1$.

Using Eqs. 4.2 , 4.3 and 4.4 we can re-write the system of equations as follows:

$$\begin{aligned} Y_{C_{n^*}} &= h_{c_{n^*}} X_C + \mathbf{L}_{D_{n^*}} \mathbf{X_D} + n_{C_{n^*}} \\ Y_{D_i} &= h_{d_i} X_{D_i} + l_{c_i} X_C + \hat{\mathbf{L}}_{D_i} \hat{\mathbf{X}}_{\mathbf{D}} + n_{D_i} \\ Y_{E_m} &= g_{c_m} X_C + \mathbf{G}_{D_m} \mathbf{X_D} + \mathbf{G}_{A_m} \mathbf{X_J} + n_{E_m} \end{aligned} \tag{4.5}$$

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

4.3 Scenario 1: EH Without Memory

4.3.1 Energy Model

Energy harvesting helps prolong the lifetime of the network, where the secondary transmitting device becomes capable of accommodating the random arrivals of energy. In scenario 1, we consider that each of the K D2D transmitters have the energy harvesting ability. We assume that each of these devices has enough energy to transmit secret messages; however, only the devices with the harvested energy above certain energy threshold can be considered to send friendly jamming signals.

The energy threshold is given by

$$E_{min} = P_d \tag{4.6}$$

where P_d is the transmit power of secondary devices.

4.3.2 Problem Statement

We consider the expression for $\mathcal{R}_{C_{sum}}$, $\mathcal{R}_{D,k}$, and $\mathcal{R}_{th}$ as presented in section 3.3. Given the primary's secrecy sum-rate condition $\mathcal{R}_{C_{sum}}$ and energy constraint $E_k \geq E_{min}$ $\forall k \in \{1, \ldots, K\}$, we need to find the optimal number of data transmission devices K_S^* and friendly jamming devices K_J^* in the

underlying D2D network that maximizes the secondary secrecy throughput.

$$K_S^* \text{ and } K_J^* = \begin{cases} \underset{\substack{1\leq K_S\leq K_J-1 \\ 2\leq K_J\leq K-1}}{\text{argmax}} & \sum_{k=1}^{K_S} \mathcal{R}_{D_k} \\ \text{subject to} & \mathcal{R}_{C_{sum}}(K_S, K_J) \geq \mathcal{R}_{th} \\ \text{s.t.} & K_S + K_J \leq K \end{cases} \tag{4.7}$$

4.3.3 Algorithm

We use the exhaustive search selection (ESS) scheme in finding an optimal solution to the problem in Eq 4.7. Fig. 4.1 illustrates ESS algorithm. The D2D system comprises of K D2D pairs and only K_S out of these K D2D pairs are allowed to share the spectrum and send their secret messages while K_J 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 and K_J to satisfy $1 \leq K_S \leq K_J - 1$ and $2 \leq K_J \leq K - 1$ respectively, as explained in section 4.2. The total number of possible choices to select K_J out of K_A (K_A total number of D2D devices satisfying energy constraint $E_k \geq E_{min}$) is equal to $\sum_{K_J=2}^{K_A} \binom{K_A}{K_J}$ and the number of possible choices to select K_S D2D pair out of $min\{K_J - 1, K - K_J\}$ is$\sum_{K_S=1}^{min\{K_J-1,K-K_J\}} \binom{min\{K_J-1,K-K_J\}}{K_S}$. Given all possible combinations of D2D pairs, we determine the once that satisfy the primary secrecy sum-rate, i,e.,$\mathcal{R}_{C_{sum}}(i,j) \geq \mathcal{R}_{th}$, where $i = 1, \ldots, \sum_{K_S=1}^{min\{K_J-1,K-K_J\}} \binom{min\{K_J-1,K-K_J\}}{K_S}$, $j = 1, \ldots, \sum_{K_J=2}^{K_A} \binom{K_A}{K_J}$. Then from theses combinations we choose the ones that maximizes the sum of secondary secrecy rates $\sum_{k=1}^{K_S} \mathcal{R}_{D_k}(i,j)$

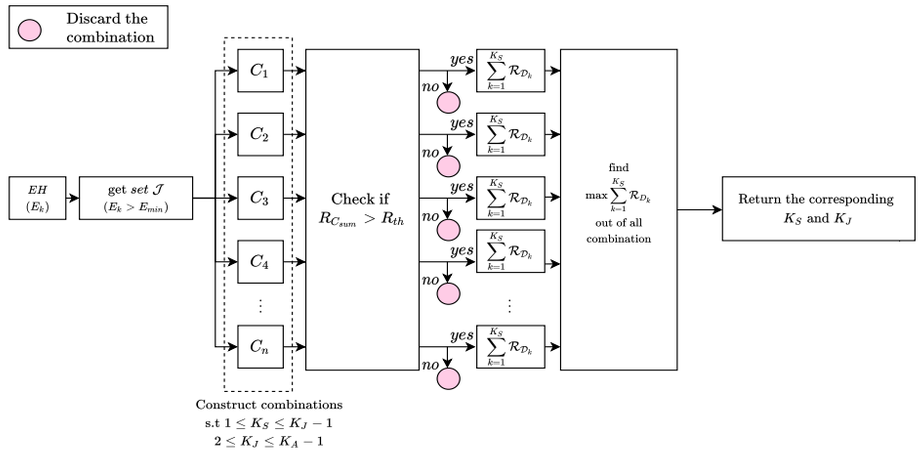


Figure 4.1: Exhaustive search selection algorithm

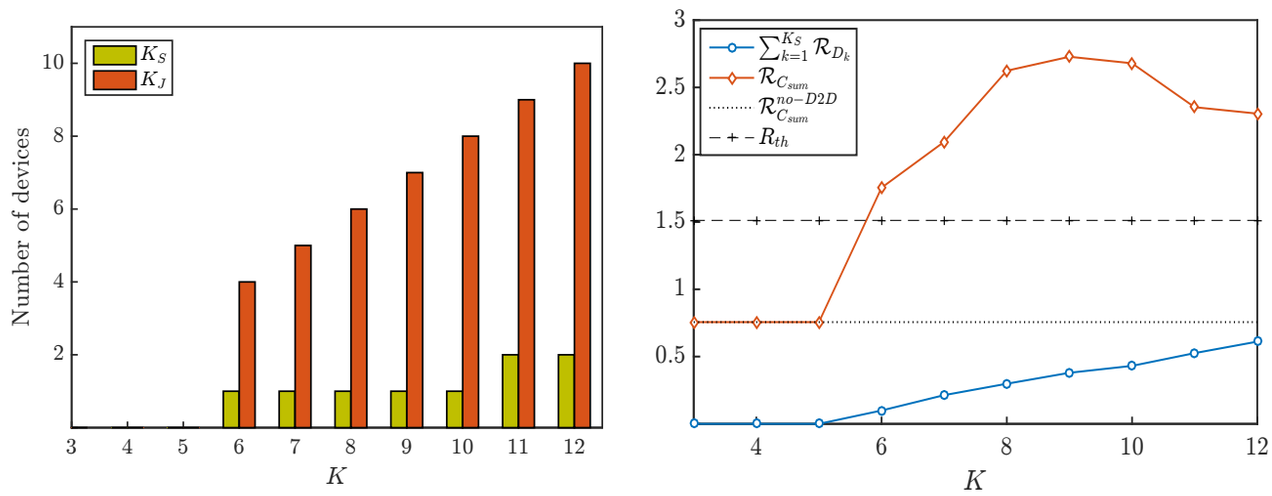
Algorithm 2: Exhaustive Search Selection (ESS)

Input : K, R_{th}
Output : K_S, K_J
First, determine the set $\mathcal{J}$ of all D2D transmitter devices satisfying the energy constraint $E_k > E_{min}, \forall k \in \{1, \ldots, K\}$ and let K_A be the total number of D2D devices which satisfies this energy constraint ;
Let $\mathcal{C}_{\mathcal{J}}$ be set of all combination of K_J out of K_A elements with $K_J = \{2, \ldots, K_A\}$;
Let $\mathcal{C}_{\mathcal{S}}$ be set of all combination of K_S out of $\min\{K_J - 1, K - K_J\}$ elements with $K_S = \{1, \ldots, \min\{K_J - 1, K - K_J\}\}$;
if $K_A < 2$ **then**
  /* No D2D Transmission */
if $K_A = K$ **then**
  /* R-ESS as in section 3.4.3 */
else
  for $j = 1$ *to* $\sum_{K_J=2}^{K_A} \binom{K_A}{K_J}$ **do**
    /* K_J elements are chosen from the set $\mathcal{J}$ */
    for $i = 1$ *to* $\sum_{K_S=1}^{\min\{K_J-1, K-K_J\}} \binom{\min\{K_J-1, K-K_J\}}{K_S}$ **do**
      Compute $R_{C_{sum}}(i, j)$ for the i^{th} and j^{th} combination of K_S and K_J ;
      if $R_{C_{sum}}(i, j) \geq R_{th}$ **then**
        Compute the secondary secrecy rate $R_{D_k}(i, j), k \in \{1, \ldots, K_S\}$;
        if $R_{D_k}(i, j) \neq 0$ **then**
          $(i, j) \in \mathcal{L}_{\mathcal{C}}$;
  if $\mathcal{L}_{\mathcal{C}} \neq 0$ **then**
    Choose the combination in $\mathcal{L}_{\mathcal{C}}$ that maximizes $\sum_{k=1}^{K_S} R_{D_k}(i, j)$;
    Return the corresponding K_S and K_J;
  else
    $K_S = 0$; /* No D2D Transmission */

4.3.4 Results

4.3.4.1 Simulation Set-Up

To illustrate the results, we consider Rayleigh fading channel where channel gains are modeled as zero mean complex Gaussian random variables. and we take unit variance AWGN for all terminals i.e., $\sigma^2_{C_n} = \sigma^2_{D_k} = \sigma^2_{E_m} = 1\ \forall n, \forall k, \forall m$. The number of simulation block for each illustrated point is considered to be 10^3. The harvesting energy is modeled as uniform random variable with mean 10 (unit Joule) and results are illustrated by averaging random harvested energy over 10 epochs (i.e., random seed from 0 to 10), the number of cellular users $N = 5$, number of eavesdroppers $M = 2$, scaling factor of the primary secrecy sum-rate threshold (discussed in section 3.4) $\beta = 2$, power of cellular user $P_c = 10$ dB, power of D2D user $P_d = 5$ dB.



(a) (b)

Figure 4.2: (a)Optimum number of device (b): Achievable secrecy rates when using ESS scheme with $N = 5$, $M = 2$, $P_c = 10$ dB, $P_d = 5$ dB and $\beta = 2$

Fig. 4.2 illustrates the optimal number of device selected and the achievable secrecy rate when using algorithm 2. By introducing the energy constraint in selecting friendly jamming devices, we observe a reduction in the number of devices allowed to communicate in the underlying system. We can see that the secrecy performance of the primary cellular system is enhanced while also allowing secret transmission for the underlying D2D communication.

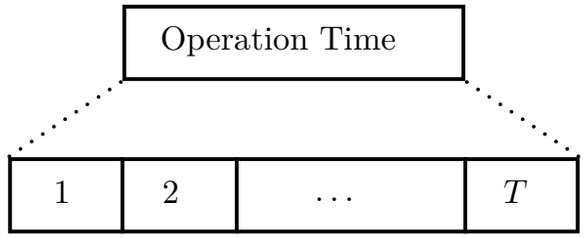


Figure 4.3: Sub-slot division

4.4 Scenarios 2: EH With Memory

4.4.1 Energy Model

We consider the EH-aided D2D network where each of the secondary D2D pairs can accommodate the random arrivals of energy. This harvested energy is utilized in transmitting either data signals or jamming signals. To increase the energy efficiency and spectral efficiency, we divide the operating time duration into T sub-slots of equal duration δ, as in Fig. 4.3. Now, the minimum energy required to transmit any signal for the duration δ is given by:

$$E_{min} = P_d * \delta \tag{4.8}$$

where P_d is the transmit power of secondary devices. Note that, at any given sub-slot, the secondary device can: 1) use the harvested energy to transmit secret data, or 2) use the harvested energy to send a friendly jamming signal, or 3) be idle to conserve energy for later use. By introducing the minimum energy requirement, we can formulate a new *set* $\mathcal{A}_\tau$ by picking all the secondary devices that are capable of either transmitting secret message or sending friendly jamming signal based on energy constraint $E_{k,\tau-1} \geq E_{min}$, where $E_{k,\tau}$ is the amount of energy of k^{th} D2D transmitter, $k \in \{1, \ldots, K\}$ at $\tau - 1^{th}$ sub-slot, $\tau \in \{1, \ldots, T\}$.

The energy is harvested before operation time; $E_{k,0}$ signifies the initial harvested energy across K D2D devices. Now, the available energy at τ^{th} sub-slot is given by:

$$E_{k,\tau} = \begin{cases} E_{k,(\tau-1)} - E_{min} & \text{if } \forall k \in \{1, \ldots, K_{S,\tau}\} \text{ or } \{1, \ldots, K_{J,\tau}\} \\ E_{k,(\tau-1)} & \text{if the device is idle and conserve energy for later use} \end{cases} \tag{4.9}$$

Where, $K_{S,\tau}$ are the devices that transmits secret messages and $K_{J,\tau}$ are the devices that send friendly jamming signal at τ^{th} sub-slot.

4.4.2 Joint Secrecy Sum-Rate

In this section, we characterize the achievable secrecy rates, discussed in sec 3.3, for all cellular and D2D at τ^{th} sub-slot. $K_{S,\tau}$ and $K_{J,\tau}$ represents the number of data transmitting device and friendly jamming devices at τ^{th} sub-slot respectively. All the channel gains are assumed constant within the operation time (i.e., across all the sub-slots).

Secrecy sum-rate for the multi-user cellular system at τ^{th} sub-slot, is given by

$$\begin{aligned}\mathcal{R}_{C_{sum,\tau}} = \Bigg\{\mathbb{E}\Bigg[\log\Bigg(1+\frac{|h_{c_{n^*}}|^2 P_c}{\sigma^2_{C_{n^*}}+\sum_{i=1}^{K_{S,\tau}}|l_{d_{i,n^*}}|^2 P_d}\Bigg) \\ -\log\Bigg(1+\frac{|g_{c_{m^*}}|^2 P_c}{\sigma^2_{E_{m^*}}+\left(\sum_{i=1}^{K_{S,\tau}}|g_{d_{i,m^*}}|^2+\Omega_{m^*,\tau}\right)P_d}\Bigg)\Bigg]\Bigg\}^+,\end{aligned} \tag{4.10}$$

with $K_{S,\tau}$ satisfying $1 \le K_{S,\tau} \le K_{J,\tau}-1$ and $2 \le K_{J,\tau} \le K-1$, $\Omega_{m^*,\tau} = G_{A_{m^*}} W W^\dagger G^\dagger_{A_{m^*}}$ and where n^* and m^* are respectively given by

$$\begin{cases} n^* = \underset{1\le n\le N}{\operatorname{argmax}}\left[\frac{|h_{c_n}|^2}{\sigma^2_{C_n}+\sum_{i=1}^{K_{S,\tau}}|l_{d_{i,n}}|^2 P_d}\right] \\ m^* = \underset{1\le m\le M}{\operatorname{argmax}}\left[\frac{|g_{c_m}|^2}{\sigma^2_{E_m}+\left(\sum_{i=1}^{K_{S,\tau}}|g_{d_{i,m}}|^2+\Omega_{m^*,\tau}\right)P_d}\right]\end{cases}$$

Secrecy rates for the underlying D2D system at τ^{th} sub-slot is given by

$$\begin{aligned}\mathcal{R}_{D_{k,\tau}} = \Bigg\{\mathbb{E}\Bigg[\log\Bigg(1+\frac{|h_{d_k}|^2 P_d}{\sigma^2_{D_k}+|l_{c_k}|^2 P_c+\sum_{\substack{p=1\\p\neq k}}^{K_{S,\tau}}|\hat{l}_{d_{p,k}}|^2 P_d}\Bigg) \\ -\log\Bigg(1+\frac{|g_{d_{k,m_k^*}}|^2 P_d}{\sigma^2_{E_{m_k^*}}+\left(\sum_{p=k+1}^{K_{S,\tau}}|g_{d_{p,m_k^*}}|^2+\Omega_{m_k^*,\tau}\right)P_d}\Bigg)\Bigg]\Bigg\}^+,\end{aligned} \tag{4.11}$$

with $k \in \{1,\dots,K_{S,\tau}\}$, $K_{S,\tau}$ satisfying $1 \le K_{S,\tau} \le K_{J,\tau}-1$ and $2 \le K_{J,\tau} \le K-1$, $\Omega_{m_k^*,\tau} = G_{A_{m_k^*}} W W^\dagger G^\dagger_{A_{m_k^*}}$ and where m_k^* is given by

$$m_k^* = \underset{1\le m\le M}{\operatorname{argmax}}\left[\frac{|g_{d_{k,m}}|^2}{\sigma^2_{E_m}+\left(\sum_{p=k+1}^{K_{S,\tau}}|g_{d_{p,m}}|^2+\Omega_{m^*,\tau}\right)P_d}\right]$$

Secondary secrecy throughput at τ^{th} sub-slot is given by

$$R_\tau = \sum_{k=1}^{K_{S,\tau}} R_{D_k,\tau} \tag{4.12}$$

4.4.3 Problem Statement

Given the primary's secrecy sum-rate condition $R_{C_{sum},\tau}$ and energy constraint $E_{k,\tau} \geq E_{min}$, $k \in \{1,\ldots,K\}$, $\tau \in \{1,\ldots,T\}$ in the secondary system. We need to find the optimal number of data transmission devices $K^*_{S,\tau}$ and friendly jamming devices $K^*_{J,\tau}$ in the underlying D2D network for each sub-slot τ, where $\tau \in \{1,\ldots,T\}$, that maximizes the secondary secrecy throughput over all the sub-slots i.e.

$$\begin{aligned}
\text{Find} \quad & \left[(K^*_{S,1}, K^*_{J,1}), \ldots, (K^*_{S,T}, K^*_{J,T})\right] \\
\textit{maximize} \quad & \sum_{\tau=1}^{T} \mathcal{R}_\tau \\
\text{subject to} \quad & \mathcal{R}_{C_{sum,\tau}}(K_{S,\tau}, K_{J,\tau}) \geq \mathcal{R}_{th} \quad \forall\tau \\
\text{s.t} \quad & 1 \leq K_{S,\tau} \leq K_{J,\tau} - 1 \text{ and } 2 \leq K_{J,\tau} \leq K-1, \\
& K_{S,\tau} + K_{J,\tau} \leq K
\end{aligned} \tag{4.13}$$

4.4.4 Algorithm

We use brute-force search scheme to select the optimal number of devices $(K_{S,1}, K_{J,1}), \ldots, (K_{S,T}, K_{J,T})$. Fig. 4.4 illustrates optimal device selection algorithm. The D2D system comprises K D2D pairs, each of which has random amount of harvested energy. Now, for each sub-slot:

1. Determine the set $\mathcal{A}_\tau$ of all D2D transmitter devices satisfying the energy constraint $E_{k,\tau-1} > E_{min}$ $k \in \{1,\ldots,K\}$.

2. Get set of all possible combination of $K_{S,\tau}$ and $K_{J,\tau}$. That is, The total number of possible choices to select $K_{J,\tau}$ out of K_A (K_A total number of D2D devices satisfying energy constraint $E_{k,\tau} \geq E_{min}$) is equal to $\sum_{K_{J,\tau}=2}^{K_A-1} \binom{K_A-1}{K_{J,\tau}}$ and the number of possible choices to select $K_{S,\tau}$ D2D pair out of $K_{J,\tau}-1$ is $\sum_{K_{S,\tau}=1}^{K_{J,\tau}-1} \binom{K_{J,\tau}-1}{K_{S,\tau}}$.

3. Given all possible combinations of D2D pairs, we determine the once that satisfy the primary secrecy sum-rate, i,e.,$\mathcal{R}_{C_{sum}}(i,j) \geq \mathcal{R}_{th}$, where $i = 1, \ldots, \sum_{K_{S,\tau}=1}^{K_{J,\tau}-1} \binom{K_{J,\tau}-1}{K_{S,\tau}}$, $j = 1, \ldots, \sum_{K_{J,\tau}=2}^{K_A-1} \binom{K_A-1}{K_{J,\tau}}$.

4. For these combinations, we calculate secondary secrecy rates $R_\tau = \sum_{k=1}^{K_{S,\tau}} \mathcal{R}_{D_k}(i,j)$ and update the device energy as follows: $E_{k,\tau} = E_{k,\tau-1} - E_{min}$ if the device k either transmits secrete data or send jamming signal, $E_{k,\tau} = E_{k,\tau-1}$ if k remains idle.

Then, from theses combinations across all sub-slots, we choose the ones that maximizes the sum of secondary secrecy throughput rate $\sum_{\tau=1}^{T} \mathcal{R}_\tau$

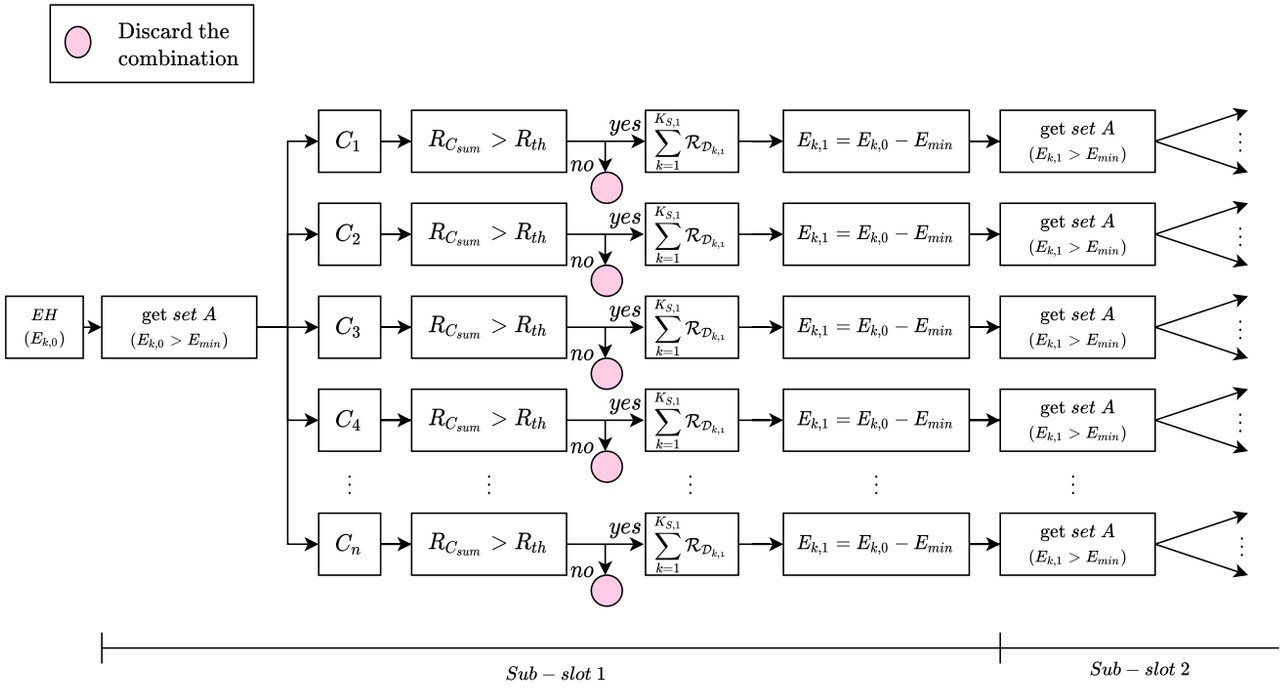


Figure 4.4: Optimal device selection algorithm

Algorithm 3: Pseudo-code to obtain optimal number of data transmitting and jamming devices across each sub-slot.

Input : K, R_{th}, T
Output : $(K_{S,1}, K_{J,1}), \ldots, (K_{S,T}, K_{J,T})$
Let $\mathcal{L}_\tau$ be the total number of combination of secondary device at τ sub-slot
Initialize $\mathcal{L}_1 = 1$
for $\tau = 1$ *to* T **do**
    $\mathcal{L}_{\tau+1} \leftarrow 0$
    for $i = 1$ *to* $\mathcal{L}_\tau$ **do**
        set $\mathcal{A}_\tau \leftarrow$ satisfying $E_{k,\tau-1} \geq E_{min}$
        /* Let K_A total number of D2D devices in set $\mathcal{A}_\tau$ */
        $\mathcal{C}_\tau \leftarrow$ set of all combinations of $K_{S,\tau}$ and $K_{J,\tau}$ with
            $1 \leq K_{S,\tau} \leq K_{J,\tau} - 1$ and $2 \leq K_{J,\tau} \leq K_A - 1$
        /* The devices for the set of all combinations of $K_{S,\tau}$ and $K_{J,\tau}$ are chosen from the set $\mathcal{A}_\tau$ */
        $\mathcal{R}_\tau \leftarrow \sum_{k=1}^{K_{s,\tau}} \mathcal{R}_{D_k,\tau}(\ \forall \mathcal{C}_\tau$ satisfying $\mathcal{R}_{C_{sum,\tau}} \geq \mathcal{R}_{th})$
        $E_{k,\tau} = E_{k,\tau-1} - E_{min}\ \forall k \in \{1, \ldots, K_{S,\tau}\}$ or $\{1, \ldots, K_{J,\tau}\}$
        $\mathcal{L}_{\tau+1} \leftarrow \mathcal{L}_{\tau+1} + |\mathcal{R}_\tau|$
Choose combinations across each sub-slot, that maximizes $\sum_{\tau=1}^{T} \mathcal{R}_\tau$
Return the corresponding $(K_{S,1}, K_{J,1}), \ldots, (K_{S,T}, K_{J,T})$

4.4.5 Results

Simulation parameters are set as discussed in section 4.3.4.1.

Table 4.1: Optimum number of devices and secrecy throughput for $K = 7$ with fixed random seed ($seed = 1$) and varying number of sub-slots

Number of sub-slots	(KS,KJ)						RD throughput	Rc_sum
	S1	S2	S3	S4	S5	S6		
No sub-slot	(0,0)						0	0.7362
2	(1,5)	(0,0)					0.1637	2.415
3	(1,5)	(0,0)	(0,0)				0.1637	2.415
4	(1,5)	(1,5)	(0,0)	(0,0)			0.3275	2.415
5	(1,5)	(1,5)	(0,0)	(0,0)	(0,0)		0.3275	2.415
6	(1,5)	(1,5)	(1,5)	(0,0)	(0,0)	(0,0)	0.3275	2.415

Table 4.1 shows optimum number of devices and secrecy throughput for $K = 7$ with fixed random seed ($seed = 1$) and varying number of sub-slots. From Table 4.1, we can see that by increasing the number of sub-slots, secrecy throughput of secondary system is improved.

4.4.5.1 Sub-Optimal Solution

In algorithm 3 we go through all D2D combinations to check whether or not the primary condition is satisfied. As the total number of combinations is very large, the computation complexity grows exponentially as the number of sub-slots increases. To overcome this issue, we need to reduce the number of combinations at each sub-slot that algorithm 3 has to cover. There are several techniques to reduce the search space and to find a sub-optimal solution. Fig 4.5 shows the sub-optimal solution used in this work.

From looking at the optimal solution we can observe that:

- With no sub-slot, finding max $\sum_{k=1}^{K_S} \mathcal{R}_{D_k}$ would give optimal number of K_S and K_J.

- With sub-slot, combination of $K_{S,\tau}$ and $K_{J,\tau}$ are reasonably stable from one sub-slot to the next.

Therefore, looking for a good solution close to max $\sum_{k=1}^{K_{S,\tau}} \mathcal{R}_{D_{k,\tau}}$ (optimal) at each sub-slot may yield a close-to-optimal solution. we can find a sub-optimal solution by following below steps:

- First, obtain set of all combination of secondary devices from set $\mathcal{A}$.
- Determine $\sum_{k=1}^{K_{S,\tau}} \mathcal{R}_{D_{k,\tau}}$, for all the combination satisfying $\mathcal{R}_{C_{sum,\tau}} \geq \mathcal{R}_{th}$.
- Find max $\sum_{k=1}^{K_{S,\tau}} \mathcal{R}_{D_{k,\tau}}$ of all combination, set a threshold (say 20%, 50%) of the max. $\sum_{k=1}^{K_S} \mathcal{R}_{D_{k,\tau}}$. And, prune a tree if the combination is not within the specified threshold.

Repeat the above 3 steps for all subsequent sub-slots.

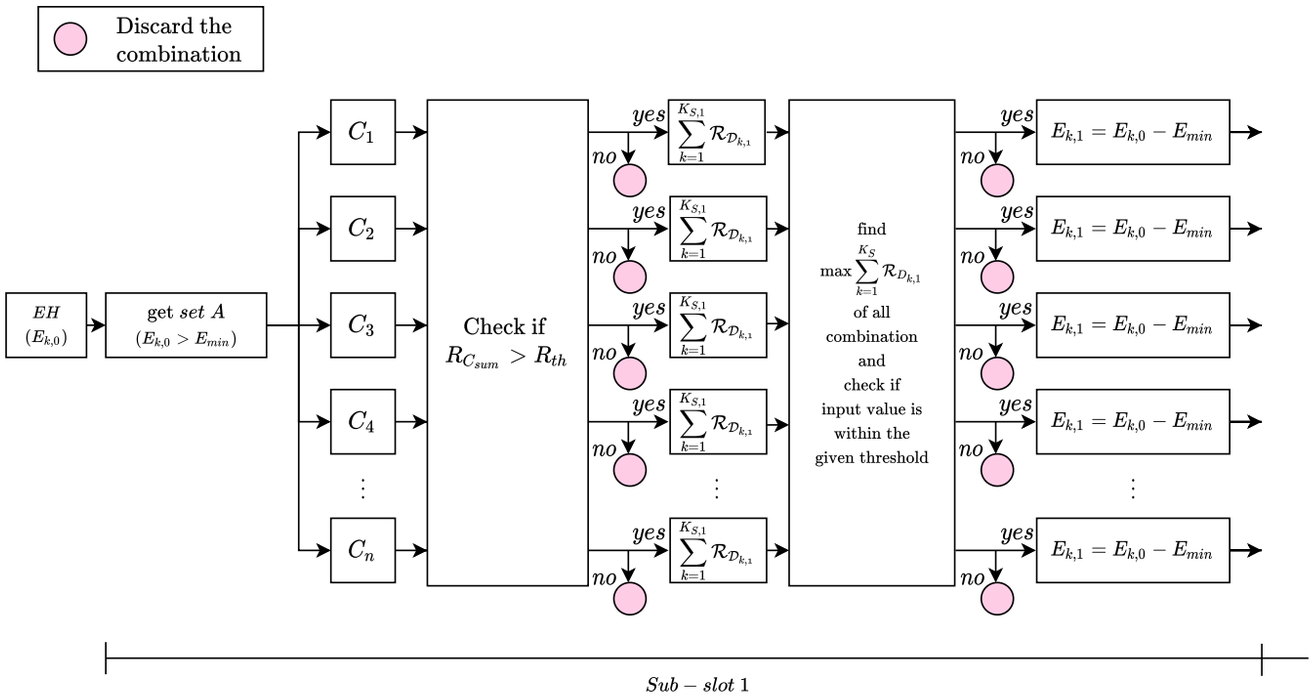


Figure 4.5: Sub-optimal device selection algorithm

Table 4.2: Comparison of computation time between optimal and sub-optimal solutions with a fixed random seed ($seed = 0$) and running on 2.3GHz Intel Xeon octa-core processor

Device selection scheme	K	Time taken (sec) (sub-slot 1)	Time taken (sec) (sub-slot 2)
Optimal	6	2.7947	16.7562
	7	24.322	1214.189
Sub-optimal (maxRD threshold 20%)	6	2.7429	8.3673
	7	24.616	172.402

Table 4.2 compares the computation time between optimal and sub-optimal scheme when a fixed random seed ($seed = 0$) and running on 2.3GHz Intel Xeon octa-core processor. From the table we see that, the computation time for sub-slot 2 has significantly reduce when using sub-optimal device selection scheme.

Table 4.3: Comparison of device selection and secrecy throughput between optimal and sub-optimal solutions

Device selection scheme	K	(KS,KJ)		RD throughput	Rc_sum
		S1	S2		
Optimal	6	(0,2)	(0,2)	0.115	0.872
	7	(1,5)	(1,4)	0.356	2.46
Sub-optimal (maxRD threshold 20%)	6	(0,2)	(0,2)	0.115	0.872
	7	(1,5)	(1,4)	0.356	2.46

Table 4.3 compares secrecy throughput and device selection between optimal and sub-optimal scheme. we can see that, for device 6 and 7 the optimal and sub-optimal solution converge.

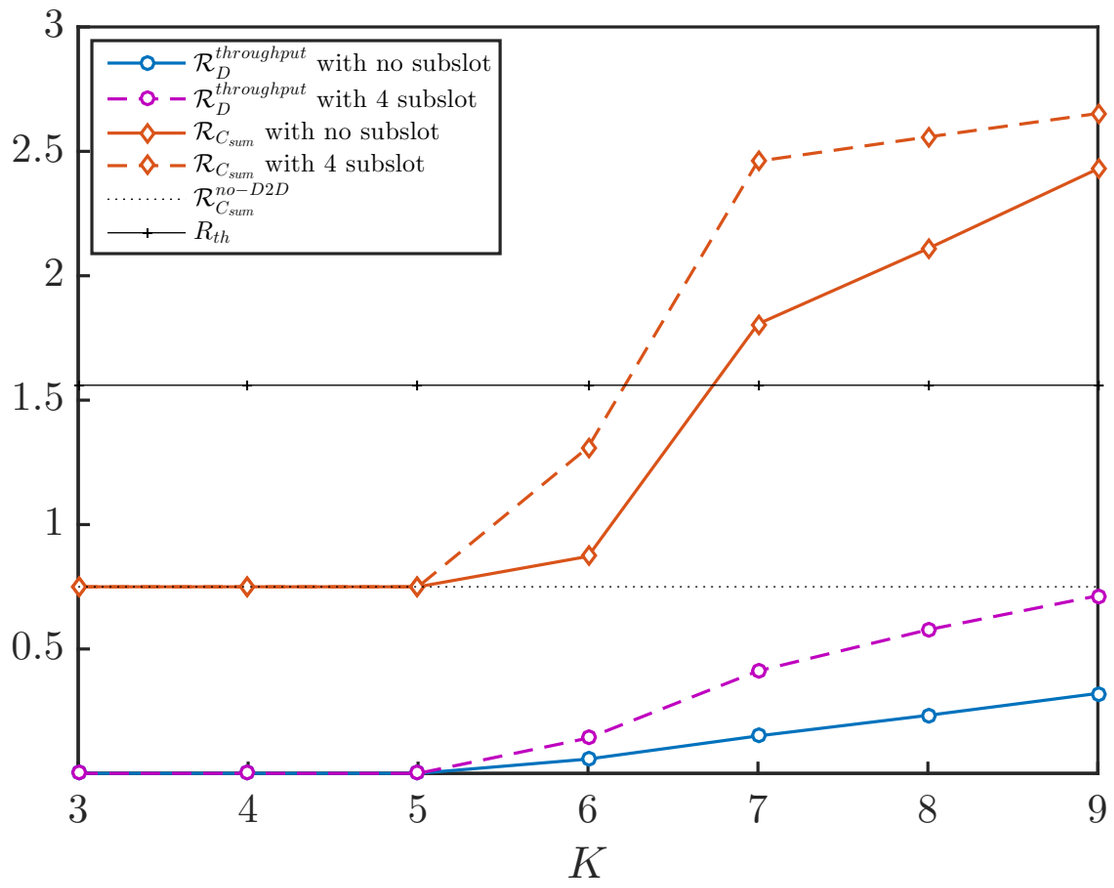


Figure 4.6: Achievable secrecy rate with 4 sub-slots and no sub-slot by fixing sub-optimal max $\mathcal{R}_D$ threshold (Γ_{th}^{maxRD}) to 20%, with $N = 5$, $M = 2$, $P_c = 10$ dB,$P_d = 5$ dB and $\beta = 2$

In Fig 4.6, we fix sub-optimal max $\mathcal{R}_D$ threshold (Γ_{th}^{maxRD}) to 20%, compare achievable secrecy rate between 4 sub-slots and no sub-slot. From the results, we observe an improvement in the secrecy performance of the secondary system and the primary system when increasing the number of sub-slots.

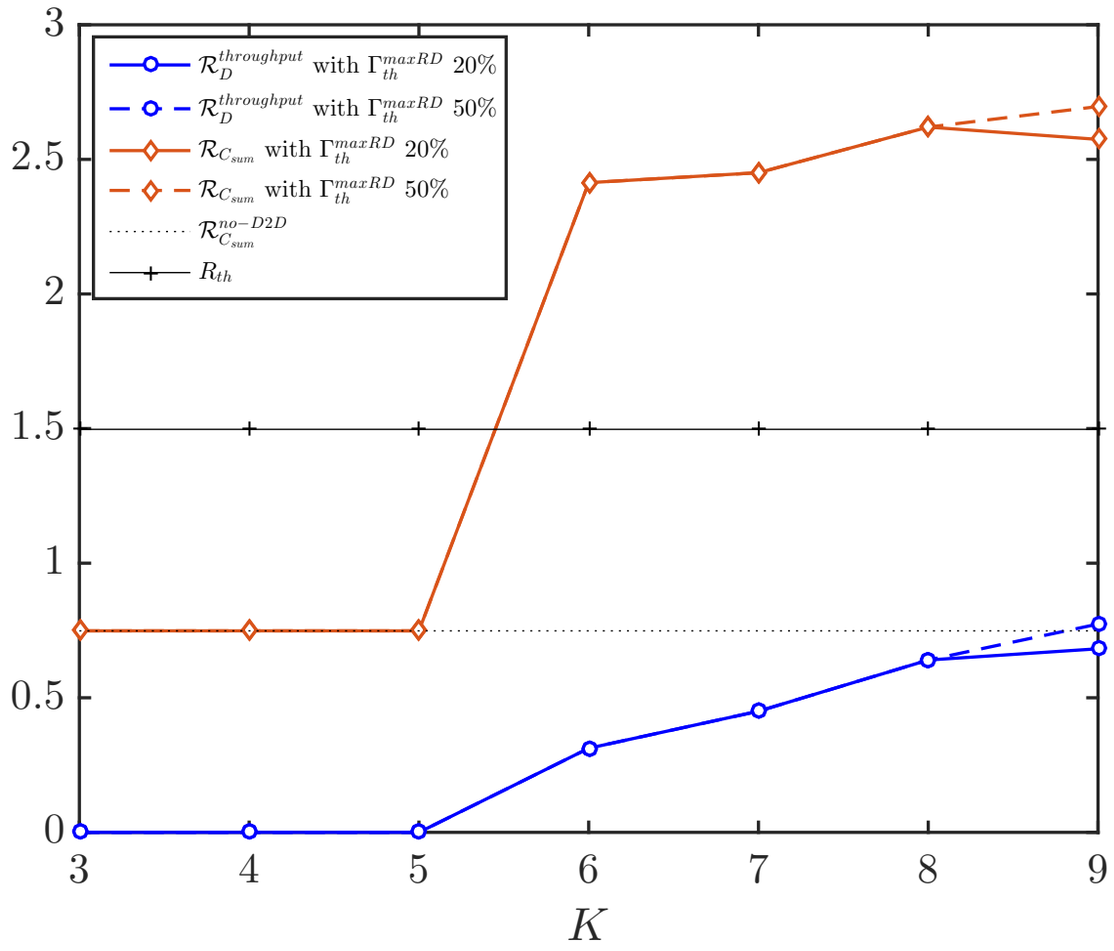


Figure 4.7: Achievable secrecy rate with Γ_{th}^{maxRD} 20% and Γ_{th}^{maxRD} 50% using sub-optimal device selection scheme, with 4 sub-slots, $N = 5$, $M = 2$, $P_c = 10$ dB, $P_d = 5$ dB and $\beta = 2$

Fig. 4.7 compares that secrecy sum rate of sub-optimal solutions for max $\mathcal{R}_D$ threshold of 20% and 50% with 4 sub-slots. We observe that the secrecy rate performance of both primary and secondary system when $K = 6, 7, 8$ remains same whereas when $K = 9$ the sum-rate performance for max $\mathcal{R}_D$ threshold of 20% is very close to max $\mathcal{R}_D$ threshold of 50%.

Table 4.4: Device selection using sub-optimal solution across 4 sub-slots

Number of sub-slots	K	(KS, KJ)			
		S1	S2	S3	S4
No sub-slot	6	(0,2)			
	7	(1,4)			
	8	(1,5)			
	9	(1,6)			
4	6	(1,3)	(0,2)	(0,2)	(0,2)
	7	(1,6)	(1,5)	(1,4)	(1,4)
	8	(1,6)	(1,6)	(1,6)	(1,7)
	9	(1,7)	(1,7)	(1,7)	(1,7)

Table. 4.4 illustrates the device selection using sub-optimal solution with max $\mathcal{R}_D$ threshold of 20% across 4 sub-slots. We can notice here is that, under the sub-optimal EH aided D2D device selection scheme, secondary device selected at each sub-slot varies so as to maximize the overall secondary throughput across all the given sub-slots.

5

Conclusions

In this project, we considered a spectrum sharing channel where both the cellular and the underlying EH aided D2D pairs are interested in transmitting secrete data. We studied two scenarios where our primary goal in each case was to maximize secrecy throughput of the secondary system, given the primary's secrecy sum-rate condition.

The first scenario examines the case where each EH-D2D pair in the underlying system have enough energy to transmit secret messages; however, the transmission of jamming signals is constrained by the amount of energy harvested. The obtained results show that by introducing the energy constraint on the transmission of friendly jamming signals, we see the reduction in the number of devices allowed to communicate in the underlying system.

In the second case, we divide the device transmission operation time into multiple sub-slots. Each D2D pair utilizes its harvested energy to transmit secret messages or send jamming signals at each given sub-slot. We notice that the computation complexity grows exponentially as the number of sub-slots increases. Hence, we decreased the search space to obtain a sub-optimal solution. The obtained results show that under the sub-optimal EH aided D2D device selection scheme, the secondary device selected at each sub-slot varies to maximize the overall secondary throughput across all the given sub-slots. We also observe an improvement in the secrecy performance of the secondary system and the primary system when increasing the number of sub-slots.

Finally, the proposed device selection model improves the primary secrecy performance while also allowing secret transmission for the underlying EH-aided D2D communication.

Bibliography

[1] Global Mobile Data Traffic Forecast. "Cisco visual networking index: global mobile data traffic forecast update, 2017–2022". In: *Update* 2017 (2019), p. 2022.

[2] Gregory Staple and Kevin Werbach. "The end of spectrum scarcity [spectrum allocation and utilization]". In: *IEEE spectrum* 41.3 (2004), pp. 48–52.

[3] Mark McHenry. "Frequency agile spectrum access technologies". In: *FCC Workshop on Cognitive Radios*. Vol. 19. 5. 2003.

[4] Paul Kolodzy et al. "Next generation communications: Kickoff meeting". In: *Proc. DARPA*. Vol. 10. 2001.

[5] Simon Haykin. "Cognitive radio: brain-empowered wireless communications". In: *IEEE journal on selected areas in communications* 23.2 (2005), pp. 201–220.

[6] Priyanka Rawat, Kamal Deep Singh, and Jean Marie Bonnin. "Cognitive radio for M2M and Internet of Things: A survey". In: *Computer Communications* 94 (2016), pp. 1–29.

[7] Moshe Timothy Masonta, Mjumo Mzyece, and Ntsibane Ntlatlapa. "Spectrum decision in cognitive radio networks: A survey". In: *IEEE Communications Surveys & Tutorials* 15.3 (2012), pp. 1088–1107.

[8] Klaus Doppler, Mika Rinne, Carl Wijting, Cássio B Ribeiro, and Klaus Hugl. "Device-to-device communication as an underlay to LTE-advanced networks". In: *IEEE communications magazine* 47.12 (2009), pp. 42–49.

[9] Gábor Fodor, Erik Dahlman, Gunnar Mildh, Stefan Parkvall, Norbert Reider, György Miklós, and Zoltán Turányi. “Design aspects of network assisted device-to-device communications”. In: *IEEE Communications Magazine* 50.3 (2012), pp. 170–177.

[10] Sergey Andreev, Alexander Pyattaev, Kerstin Johnsson, Olga Galinina, and Yevgeni Koucheryavy. “Cellular traffic offloading onto network-assisted device-to-device connections”. In: *IEEE Communications Magazine* 52.4 (2014), pp. 20–31.

[11] Di Ma and Gene Tsudik. “Security and privacy in emerging wireless networks”. In: *IEEE Wireless Communications* 17.5 (2010), pp. 12–21.

[12] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. “Security in wireless sensor networks: issues and challenges”. In: *2006 8th International Conference Advanced Communication Technology*. Vol. 2. IEEE. 2006, 6–pp.

[13] Antonino Orsino, Dmitri Moltchanov, Margarita Gapeyenko, Andrey Samuylov, Sergey Andreev, Leonardo Militano, Giuseppe Araniti, and Yevgeni Koucheryavy. “Direct connection on the move: Characterization of user mobility in cellular-assisted D2D systems”. In: *IEEE Vehicular Technology Magazine* 11.3 (2016), pp. 38–48.

[14] Amal Hyadi and Fabrice Labeau. “Towards a Win-Win Spectrum Sharing Channel: A Secrecy Perspective”. In: *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE. 2019, pp. 1–6.

[15] James L Massey. “An introduction to contemporary cryptology”. In: *Proceedings of the IEEE* 76.5 (1988), pp. 533–549.

[16] Amitav Mukherjee, S Ali A Fakoorian, Jing Huang, and A Lee Swindlehurst. “Principles of physical layer security in multiuser wireless networks: A survey”. In: *IEEE Communications Surveys & Tutorials* 16.3 (2014), pp. 1550–1573.

[17] Hans Delfs, Helmut Knebl, and Helmut Knebl. *Introduction to cryptography*. Vol. 2. Springer, 2002.

[18] Furqan Jameel, Shurjeel Wyne, and Ioannis Krikidis. “Secrecy outage for wireless sensor networks”. In: *IEEE Communications Letters* 21.7 (2017), pp. 1565–1568.

[19] Aaron D Wyner. “The wire-tap channel”. In: *Bell system technical journal* 54.8 (1975), pp. 1355–1387.

[20] Imre Csiszár and Janos Korner. “Broadcast channels with confidential messages”. In: *IEEE transactions on information theory* 24.3 (1978), pp. 339–348.

[21] S Leung-Yan-Cheong and M Hellman. “The Gaussian wire-tap channel”. In: *IEEE transactions on information theory* 24.4 (1978), pp. 451–456.

[22] Matthieu Bloch, João Barros, Miguel RD Rodrigues, and Steven W McLaughlin. “Wireless information-theoretic security”. In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2515–2534.

[23] Patricio Parada and Richard Blahut. “Secrecy capacity of SIMO and slow fading channels”. In: *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* IEEE. 2005, pp. 2152–2155.

[24] Peiya Wang, Guanding Yu, and Zhaoyang Zhang. “On the secrecy capacity of fading wireless channel with multiple eavesdroppers”. In: *2007 IEEE International Symposium on Information Theory*. IEEE. 2007, pp. 1301–1305.

[25] Yingbin Liang, H Vincent Poor, and Shlomo Shamai. “Secure communication over fading channels”. In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2470–2492.

[26] Zang Li, Roy Yates, and Wade Trappe. “Secret communication with a fading eavesdropper channel”. In: *2007 IEEE International Symposium on Information Theory*. IEEE. 2007, pp. 1296–1300.

[27] Ender Tekin and Aylin Yener. “The Gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming”. In: *2007 Information Theory and Applications Workshop*. IEEE. 2007, pp. 404–413.

[28] Ruoheng Liu, Ivana Maric, Predrag Spasojevic, and Roy D Yates. "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2493–2507.

[29] Yingbin Liang, Anelia Somekh-Baruch, H Vincent Poor, Shlomo Shamai, and Sergio Verdú. "Capacity of cognitive interference channels with and without secrecy". In: *IEEE Transactions on Information Theory* 55.2 (2009), pp. 604–619.

[30] Yasutada Oohama. "Capacity theorems for relay channels with confidential messages". In: *2007 IEEE International Symposium on Information Theory*. IEEE. 2007, pp. 926–930.

[31] Lifeng Lai and Hesham El Gamal. "The relay–eavesdropper channel: Cooperation for secrecy". In: *IEEE transactions on information theory* 54.9 (2008), pp. 4005–4019.

[32] Jianting Yue, Chuan Ma, Hui Yu, and Wei Zhou. "Secrecy-based access control for device-to-device communication underlaying cellular networks". In: *IEEE Communications Letters* 17.11 (2013), pp. 2068–2071.

[33] Rongqing Zhang, Xiang Cheng, and Liuqing Yang. "Joint power and access control for physical layer security in D2D communications underlaying cellular networks". In: *2016 IEEE International Conference on Communications (ICC)*. IEEE. 2016, pp. 1–6.

[34] Hui Hui, A Lee Swindlehurst, Guobing Li, and Junli Liang. "Secure relay and jammer selection for physical layer security". In: *IEEE Signal Processing Letters* 22.8 (2015), pp. 1147–1151.

[35] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. "Security and privacy in device-to-device (D2D) communication: A review". In: *IEEE Communications Surveys & Tutorials* 19.2 (2017), pp. 1054–1079.

[36] A. Hyadi, Z. Rezki, F. Labeau, and M. Alouini. "Joint Secrecy for D2D Communications Underlying Cellular Networks". In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 2017, pp. 1–6.

[37] Ahmed Hamdi Sakr and Ekram Hossain. "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis". In: *IEEE Transactions on Communications* 63.5 (2015), pp. 1867–1880.

[38] Howard H Yang, Jemin Lee, and Tony QS Quek. "Heterogeneous cellular network with energy harvesting-based D2D communication". In: *IEEE Transactions on Wireless communications* 15.2 (2015), pp. 1406–1419.

[39] Rachad Atat, Lingjia Liu, Nicholas Mastronarde, and Yang Yi. "Energy harvesting-based D2D-assisted machine-type communications". In: *IEEE Transactions on Communications* 65.3 (2016), pp. 1289–1302.

[40] Yuanwei Liu, Lifeng Wang, Syed Ali Raza Zaidi, Maged Elkashlan, and Trung Q Duong. "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model". In: *IEEE Transactions on Communications* 64.1 (2015), pp. 329–342.

[41] Ashish Khisti, Aslan Tchamkerten, and Gregory W Wornell. "Secure broadcasting over fading channels". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2453–2469.