Achievable Secrecy Rates of an Energy Harvesting Device

Alessandro Biason, *Student Member, IEEE,* Nicola Laurenti, and Michele Zorzi, *Fellow, IEEE*

***Abstract*—The secrecy rate represents the amount of information per unit time that can be securely sent on a communication link. In this work, we investigate the achievable secrecy rates in an energy harvesting communication system composed of a transmitter, a receiver and a malicious eavesdropper. In particular, because of the energy constraints and the channel conditions, it is important to understand when a device should transmit and to optimize how much power should be used in order to improve security. Both full knowledge and partial knowledge of the channel are considered under a Nakagami fading scenario. We show that high secrecy rates can be obtained only with power *and* coding rate adaptation. Moreover, we highlight the importance of optimally dividing the transmission power in the frequency domain, and note that the optimal scheme provides high gains in secrecy rate over the uniform power splitting case. Analytically, we explain how to find the optimal policy and prove some of its properties. In our numerical evaluation, we discuss how the maximum achievable secrecy rate changes according to the various system parameters. Furthermore, we discuss the effects of a finite battery on the system performance and note that, in order to achieve high secrecy rates, it is not necessary to use very large batteries.**

***Index Terms*—energy harvesting, secrecy rate, physical layer security, WSN, MDP, optimization, policies, finite battery.**

I. Introduction

SECURITY and privacy are becoming more and more important in communications and networking systems, and have key applications in the Wireless Sensor Network (WSN) and Internet of Things (IoT) world [2]. While most works in this area deal with security *protocols* [3], [4], implementing security mechanisms at the physical layer represents an interesting complement to those networking approaches [5], and has the potential to provide stronger (information-theoretic) secrecy properties [6].

In the context of energy-constrained and green networking, the design of low-power systems and the use of renewable energy sources in network systems are prominent areas of investigation. In particular, the use of Energy Harvesting (EH) technologies as a way to prolong unattended operation of a network is becoming more and more appealing. However, despite these trends, security and privacy issues so far have been addressed mostly by neglecting low-power design principles (except possibly for some attempts at limiting the computation and processing costs and/or the number of messages needed to implement a secure protocol). In particular, the impact of power allocation policies and of system features related to energy harvesting has only been studied in some special cases [7], [8]. Since green aspects will play an increasingly large role in future networks, it is essential to bring low-power, energy-constrained and green considerations into this picture. In this paper, we try to partly fill this gap, studying how the use of energy harvesting affects the design and performance of physical layer security methods.

We consider an *Energy Harvesting Device* (EHD) (i.e., a device with the capability of gathering energy from the environment [9], e.g., through a solar panel or a rectenna) that sends data to a receiver over an insecure communication channel. The goal is to transmit data securely, i.e., in such a way that an adversary (or *eavesdropper*) with access to the communication link is not able to gather useful information about the data sent. We study how the specific EH characteristics influence the achievable *secrecy rate* (i.e., the information rate at which the EHD can reliably send data to the receiver while keeping it secret from the eavesdropper). Deciding whether the EHD should transmit or not, how much power should be transmitted or how to divide the power among the different sub-carriers is not obvious, and all these aspects need to be appropriately optimized. Moreover, while in the classic throughput optimization problem if the available resources were used improperly the corresponding penalty would be a performance reduction, in the secrecy optimization problem an improper use of the resources may imply not only a reduced transmission rate, but also a security loss, possibly making sensitive data accessible to a malicious party.

In the literature, many papers studied energy harvesting communication systems because of their ability to increase the network lifetime, provide self-sustainability and, ideally, allow perpetual operations [10]. [11] presented a survey on the several different environmental energy harvesting technologies for WSNs. Analytically, [12] formulated the problem of maximizing the average value of the reported data using a node with a rechargeable battery. In [13], [14], Sharma *et al.* studied heuristic delay-minimizing policies and sufficient stability conditions for a single EHD with a data queue. Ozel *et al.* set up the offline throughput optimization problem from an information theoretic point of view in [15], where they derived the information-theoretic capacity of the AWGN channel and presented two schemes that achieve such capacity (save-and-transmit and best-effort-transmit). In [16], the authors also modeled a battery-less system by a channel with state dependent amplitude constraints and causal information at the transmitter, and derived the capacity of this channel by making use of a result by Shannon. The throughput optimization problem with finite batteries in an EH system was studied in [17], [18].

Security aspects have been widely studied in the WSN

The authors are with the Dept. of Information Engineering, University of Padova, Padova, Italy. email: {biasonal,nil,zorzi}@dei.unipd.it.

A preliminary version of this paper has been presented at IEEE GLOBECOM 2015 [1].

literature [2], [3], [19]. Examples of relevant applications in a WSN/IoT context include health-care monitoring [20], [21], where the sensitive data of patients may be exposed to a malicious party, or military use [22], [23], where a WSN can be used for monitoring or tracking enemy forces. In particular, in addition to higher layers [24], that are relatively insensitive to the physical characteristics of the wireless medium, physical layer can be used to strengthen the security of digital communication systems and improve already existing security measures. The basic idea behind the concept of physical layer secrecy is to exploit the randomness of the communication channel to limit the information that can be gathered by the eavesdropper at the signal level. Through channel coding techniques, it is possible to simultaneously allow the legitimate receiver to correctly decode a packet and prevent a potential third party malicious eavesdropper from decoding it and thus provide information-theoretic or *unconditional* security. Differently from computational security methods, that are based on the limited computational capabilities of the adversary (as in a cryptographic system), unconditional security is considered the strongest notion of security [25] because no limits on the adversary's computing power are assumed. Perfect secrecy [6] is achieved when there is zero mutual information between the information signal, s, and the signal received by the eavesdropper, z, i.e., $I(s;z)=0$ and z is useless when trying to determine s. In [26], Wyner showed that if the eavesdropper's channel is degraded with respect to the legitimate channel, then it is possible to exchange secure information at a non-zero rate while keeping the information leakage to the eavesdropper at a vanishing rate. This result was extended in [27] for non-degraded channels provided the eavesdropper channel is not less noisy than the legitimate channel. In [28], the secrecy capacity of fading channels in the presence of multiple eavesdroppers is studied. It was shown in [29] that in a fading scenario it is also possible to obtain a non-zero secure rate even if, on average, the eavesdropper's channel is better than the legitimate one. The authors also established the importance of variable rate coding (i.e., matching the code rate to the channel rate) in enabling secure communications. In [30], the authors compute the secrecy capacity of a MIMO wiretap channel with one receiver and one eavesdropper and an arbitrary number of antennas. A survey of physical layer security in modern networks is presented in [31].

The secrecy capacity paradigm in an energy harvesting communication system was studied in [32], [33], where the authors considered the case of a batteryless transmitter and found the rate-equivocation region. [34] studied the deployment of an energy harvesting cooperative jammer to increase physical layer security. In [8] the authors presented a resource allocation algorithm for a multiple-input single-output secrecy system for a communication system based on RF energy harvesting. Also [35] studied how to efficiently allocate power over several sub-carriers in an EH system with secrecy constraints. In [36] the authors employed a physical layer secrecy approach in a system with a transmitter that sends confidential messages to a receiver and transfers wireless energy to energy harvesting receivers. Our focus is substantially different from those: in the present paper we consider an EHD that harvests energy from an external, non-controllable and renewable energy source. Our goal is to maximize the achievable secrecy rate, i.e., to define how to correctly exploit the available (random) energy according to the device battery dynamics.

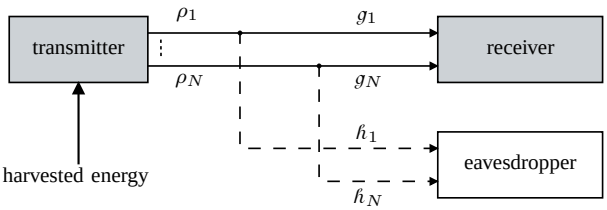

Figure 1: Block diagram of the system. $\boldsymbol{g}$ and $\boldsymbol{h}$ are the channel gains and $\boldsymbol{\rho}$ represents the power allocated over the N sub-carriers.

Our main contribution lies in the definition of a new practical and challenging problem. As in [32], [33], we investigate the physical layer secrecy in an EH system. However, differently from those papers, we explicitly consider the effects of a finite battery and we focus on finding the transmission strategy that maximizes the secrecy rate, namely the *Optimal Secrecy Policy* (OSP). Since in a WSN the devices operate under the same conditions for long periods, the steady-state regime is generally reached, and thus we focus on the long-term optimization. Similarly to [18], [37], we set up an optimization problem based on a Markov Decision Process (MDP) approach but, unlike in those works, we focus on the security aspects, considering the presence of a malicious eavesdropper and a generic number of sub-carriers. Thus, even if the proposed analytical framework is similar to those provided in the literature, since additional dimensions are considered, the optimization process is more challenging and different considerations and insights are derived. In particular, we prove several properties of OSP and describe a technique to compute it by decomposing the problem into two steps. We specify how to allocate the power over the different sub-carriers and remark that a smart power splitting scheme is important to achieve high secrecy rates. As in [29], we consider several degrees of knowledge of the channel state information, describing both variable and constant rate coding techniques and discussing how the achievable secrecy rate changes in these cases. However, unlike [29], we study an energy constrained system with N parallel sub-carriers, and accordingly formulate and solve an optimization problem to determine the maximum secrecy rate. Therefore, our paper considers aspects that either have not yet been considered or have been separately studied in the literature, and represents an advancement of the state of the art in the important areas of green networking and security, leading to novel insights about the interaction of many different system design aspects.

The paper is organized as follows. Section II defines the system model we analyze and introduces the notion of secrecy rate. In Section III we introduce the secrecy rate optimization problem. Section IV describes how to find OSP and some of its properties with full CSI. In Section V we study the case of imperfect CSI knowledge. Section VI presents our numerical results. Finally, Section VII concludes the paper.

II. System Model and Secrecy Rate

We consider an *Energy Harvesting Device* (EHD) that simultaneously transmits data in a wide frequency band composed of N narrow bands. The transmission power can be different for every sub-carrier. The transmission model can be described as a set of N parallel Gaussian wiretap channels, affected by independent fading, as in [38]. The goal of the transmitter is to send data to the legitimate receiver with a positive secrecy rate in order to guarantee secure transmission. An eavesdropper attempts to intercept the transmitted data (see Figure 1 for the block diagram of the system model).

We initially assume that the EHD knows the Channel State Information (CSI) of all the sub-carriers toward the receiver and the eavesdropper instantaneously, and will relax this hypothesis in Section V. Time is divided into slots of equal duration T, chosen according to the channel coherence time, in order to guarantee constant channel gains in every slot. The EHD is equipped with a battery of finite size $e_{\max}$ and in slot k the device has $E^{(k)} \in \mathcal{E} \triangleq \{0, \dots, e_{\max}\}$ energy quanta stored.[1] Knowledge of the state of charge is useful at the transmitter side only to determine when to schedule a transmission. The harvesting process is described through an energy quanta arrival process $\{B^{(k)}\}$, e.g., deterministic, Bernoulli or truncated geometric (for example, see [39] for a characterization of the light energy). The average harvesting rate is $\bar{b}$, the maximum (minimum) number of energy quanta harvested per slot is $b_{\max}$ ($b_{\min}$), and a quantum harvested in slot k can only be used in time slots $> k$. We assume that the device always has data to send and that the energy cost that the device sustains is mainly due to data transmission. Extensions to more general models are left for future work.

The channel gains in slot k are $\boldsymbol{g}^{(k)} = [g_1^{(k)}, \dots, g_N^{(k)}]$ and $\boldsymbol{\hbar}^{(k)} = [\hbar_1^{(k)}, \dots, \hbar_N^{(k)}]$ for the N legitimate and eavesdropper sub-carriers, respectively. $\boldsymbol{g}^{(k)}$ and $\boldsymbol{\hbar}^{(k)}$ can be interpreted as realizations of two jointly random vectors $\boldsymbol{G} = [G_1, \dots, G_N]$ and $\boldsymbol{H} = [H_1, \dots, H_N]$ (i.i.d. over time) with supports $\mathcal{G}$ and $\mathcal{H}$. We assume that the receiver has complete CSI of its channel in order to decode the received signal. Instead, the eavesdropper has knowledge on every aspect of the system (this is a reasonable worst-case assumption, as the transmission strategy should not rely on assuming the eavesdropper's ignorance of any state). Nevertheless, we should point out that, for a passive eavesdropper, knowledge of the main channel state is totally immaterial. In the following, when we refer to "full" or "partial" CSI, we always refer to the transmitter side.

A. Secrecy Rates and Capacity

We refer to the notions of *secrecy rate* and *secrecy capacity* as known in the physical layer secrecy literature [5], [26] and their ergodic counterparts in the fading scenario [40]. Specifically, we define an (M, N, ℓ) code for the parallel wiretap channel as consisting of: 1) a message set $\mathcal{S}$ with cardinality M, 2) a probabilistic encoder f_ℓ^{enc} at the transmitter that maps each message $s \in \mathcal{S}$ (realization of the r.v. S) to each $N \times \ell$ codeword $\boldsymbol{x} \in \boldsymbol{\mathcal{X}}^\ell$, with $\boldsymbol{\mathcal{X}} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_N$ according to some conditional distribution $p_{\boldsymbol{X}|S}(\boldsymbol{x}|s)$, and 3) a (deterministic) decoder at the legitimate receiver that extracts $\hat{s}$ (realization of the r.v. $\hat{S}$) from the received message $\boldsymbol{y} \in \boldsymbol{\mathcal{Y}}^\ell$, where $\boldsymbol{\mathcal{Y}} = \mathcal{Y}_1 \times \cdots \times \mathcal{Y}_N$ i.e., $f_\ell^{\text{dec}} : \boldsymbol{\mathcal{Y}}^\ell \to \mathcal{S}$.

The average error probability of an (M, N, ℓ) code is given by

$$P_{\text{err}}^\ell \triangleq \frac{1}{M} \sum_{s \in \mathcal{S}} \mathbb{P}\Big(\hat{S} \neq s | S = s\Big). \tag{1}$$

The equivocation rate at the eavesdropper is $R_e^\ell = (1/\ell) H(S|Z^\ell)$, i.e., the conditional entropy rate of the transmitted message given the eavesdropper's channel output Z^ℓ. R_e^ℓ represents the level of ignorance on the target secret message at the eavesdropper. Perfect secrecy (unconditional security) would be obtained if $R_e^\ell = R^\ell$, where $R^\ell = (1/\ell) H(S)$ is the secret message rate. However, this is not possible in general with wiretap coding techniques, so we must settle for a weaker requirement, that holds asymptotically. Therefore, a *secrecy rate* R_s is said to be achievable if there exists a sequence of $(2^{\ell R_s}, N, \ell)$ codes, $\ell = 1, 2, \dots$, such that

$$\lim_{\ell \to \infty} P_{\text{err}}^\ell = 0, \qquad R_s \leq \lim_{\ell \to \infty} R_e^\ell \tag{2}$$

and the secrecy capacity is defined as the supremum of the set of achievable secrecy rates.

B. Coding Strategy

The transmitter coding strategy influences the secrecy rate. In particular, in this paper we consider *constant* and *variable* rate coding defined as follows (a construction procedure for these codes can be derived as explained in [29, Theorems 1 and 2]).

Variable rate coding consists in adapting the code rate to the main channel state. This can be accomplished by constructing a separate codeword x for every realization of the channel, i.e., $x = x(\text{current channel})$. In this case, in every slot k and on every sub-carrier $r = 1, \dots, N$ the transmitter observes the channel and picks the symbols to be transmitted from the current codeword $x(g_r^{(k)})$. We study the long-term regime and thus we consider the case of infinite length codewords. With variable rate coding, when the gain of the legitimate channel in a given sub-carrier is g, the transmitter uses symbols from codewords at rate $\log(1 + g\rho)$ (where ρ is the transmission power, which will be the objective of our optimization). To achieve such a rate, it is required *to use a codeword specifically designed for this channel*, i.e., $x(g)$. Then, if the eavesdropper's channel gain is $\hbar > g$, thanks to the chosen coding rate, the mutual information between the transmitter and the eavesdropper is upper-bounded by $\log(1 + g\rho)$. Instead, when $\hbar \leq g$, the mutual information becomes $\log(1 + \hbar\rho)$ (Shannon's theorem). We can summarize the two previous cases as $\log(1 + \min\{g, \hbar\}\rho)$. Therefore, even if $\hbar > g$, the eavesdropper does not receive more information than the legitimate receiver (they both experience the same

[1] While in reality energy is a continuous quantity, we decide to adopt an approximate approach and discretize it in order to simplify the numerical optimization and apply the discrete MDP theory. However, we remark that it is always possible to use a finer quantization in order to improve the accuracy of the discrete approximation (which however implies higher complexity).

rate $\log(1+g\rho)$). In the long run, the average rate of the main channel and the information accumulated at the eavesdropper are

$$\liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} \sum_{r=1}^{N} \log(1+g_r^{(k)}\rho) \tag{3}$$

and

$$\liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} \sum_{r=1}^{N} \log(1+\min\{g_r^{(k)},\hbar_r^{(k)}\}\rho), \tag{4}$$

respectively. In this case, by constructing a code and the corresponding coding map, the long-term secrecy rate (amount of secret information that can be sent) is

$$\liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} \sum_{r=1}^{N} \Big(\log(1+g_r^{(k)}\rho) - \log(1+\min\{g_r^{(k)},\hbar_r^{(k)}\}\rho)\Big). \tag{5}$$

Constant rate coding consists in keeping the code rate constant, regardless of the legitimate and eavesdropper's channel states. In this case, a single codeword x is used in every fading condition. In every slot, the transmitter picks the symbols to be transmitter from the only available codeword x. In the long run, since we consider infinite length codewords, x spans the entire fading statistic of the channel. With constant rate coding, regardless of the current channel state, the transmitter uses codewords at a fixed rate R_{con} such that $R_{\text{con}} \geq \log(1+g\rho)$ for every g and ρ. In this case, if the current legitimate channel is g, the mutual information between transmitter and receiver is upper bounded by Shannon's theorem as $\log(1+g\rho)$. Similarly, the mutual information between transmitter and eavesdropper is given by $\log(1+\hbar\rho)$. The secrecy rate can be expressed as

$$\left[\liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} \sum_{r=1}^{N} \Big(\log(1+g_r^{(k)}\rho) - \log(1+\hbar_r^{(k)}\rho)\Big)\right]^+, \tag{6}$$

where $[\cdot]^+ \triangleq \max\{0,\cdot\}$ is used to obtain a non-negative rate. Note that (6) is lower than (or equal to) (5), i.e., higher secrecy is achieved with variable rate coding. However, its implementation is more difficult as the code rate has to be changed frequently according to the legitimate channel state.

For simplicity, in the next we use $R_{g,\hbar}(\rho)$ to indicate the terms of the sum in (5) if variable rate coding is considered, or (6) in the constant rate coding case, i.e.,

$$R_{g,\hbar}(\rho) \triangleq \begin{cases} \log(1+g\rho) - \log(1+\min\{g,\hbar\}\rho), & \text{var. rate,} \\ \log(1+g\rho) - \log(1+\hbar\rho), & \text{con. rate.} \end{cases} \tag{7}$$

$c(\boldsymbol{\rho},\boldsymbol{g},\boldsymbol{\hbar})$ is the generalization with a generic number of sub-carriers N:

$$c(\boldsymbol{\rho},\boldsymbol{g},\boldsymbol{\hbar}) = \sum_{r=1}^{N} R_{g_r,\hbar_r}(\rho_r), \tag{8}$$

and ρ^{tot} is the corresponding total transmission power, defined as

$$\rho^{\text{tot}} \triangleq \mathbf{1}_N^T \boldsymbol{\rho}. \tag{9}$$

The value of $c(\boldsymbol{\rho},\boldsymbol{g},\boldsymbol{\hbar})$ depends on the choice of the power allocation over the several sub-carriers, $\boldsymbol{\rho} \triangleq [\rho_1,\ldots,\rho_N]^T$, the channel conditions $\boldsymbol{g}$ and $\boldsymbol{\hbar}$, and the coding rate strategy. $\mathbf{1}_N$ is a column vector consisting of N ones. In the general case, the choice of $\boldsymbol{\rho}$ that maximizes the secrecy rate, among those satisfying (9), will in turn depend upon the channel conditions $\boldsymbol{g}$ and $\boldsymbol{\hbar}$.

III. Optimization Problem

The system state $\mathbf{S}^{(k)}$ in time slot k is defined by the $(2N+1)$-tuple $(E^{(k)},\boldsymbol{g}^{(k)},\boldsymbol{\hbar}^{(k)})$. A policy μ is a set of rules that, given the state of the system, specifies the power allocation over the N sub-carriers.

In the long run, the average *secrecy rate* under a policy μ is given by the average undiscounted reward C_μ

$$C_\mu(E^{(0)}) \triangleq \left[\liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} c(\boldsymbol{\Sigma}^{(k)},\boldsymbol{g}^{(k)},\boldsymbol{\hbar}^{(k)})\right]^+, \tag{10}$$

where $c(\cdot,\cdot,\cdot)$ is the instantaneous partial contribution defined in (8), $\boldsymbol{\Sigma}^{(k)}$ is the power allocation vector defined by the policy[2] and $E^{(0)}$ is the energy in the initial time slot. A secure communication can be performed if $C_\mu(E^{(0)}) > 0$. (10) is a generalization of (5) and (6) for N sub-carriers and a dynamic transmission power.

The battery evolution is as follows

$$E^{(k+1)} = \min\left\{E^{(k)} - \sum_{r=1}^{N} \Sigma_r^{(k)} + B^{(k)}, e_{\max}\right\}, \tag{11}$$

where $\Sigma_r^{(k)}$ is the r^{th} component of the vector $\boldsymbol{\Sigma}^{(k)}$, and the $\min$ is used to account for the finite battery. Note that $\boldsymbol{\Sigma}^{(k)}$ must satisfy $\sum_{r=1}^{N} \Sigma_r^{(k)} \leq E^{(k)},\ \forall k$ and $\Sigma_r^{(k)} \geq 0,\ \forall k,\ \forall r$. Thus, Problem (10) is implicitly influenced by the evolution of $E^{(k)}$ because of $\boldsymbol{\Sigma}^{(k)}$.

Our aim is to solve the following maximization problem

$$\mu^\star = \arg\max_{\mu} C_\mu(E^{(0)}). \tag{12}$$

A policy that solves (12) is an *Optimal Secrecy Policy* (OSP). In the next subsection we explain in more detail the optimization variables and the constraints of the above problem.

A. Markov Decision Process Formulation

Since we consider a *long-term* optimization, we recast the problem using a Markov Decision Process (MDP) formulation. In particular, we model our system by a Markov Chain (MC)

[2]Given a temporal sequence of energy arrivals and channel states, the policy μ can be applied to obtain the power allocation vector $\boldsymbol{\Sigma}^{(k)}$. In this case we use a deterministic policy for presentation simplicity, and prove later that this choice is optimal.

with a finite number of states. For every MC state $(e, \boldsymbol{g}, \boldsymbol{\hbar})$, a *power allocation policy* μ is the set of rules

$$\mu = \{\mu(\cdot; e, \boldsymbol{g}, \boldsymbol{\hbar}),\ \forall e \in \mathcal{E},\ \forall \boldsymbol{g} \in \mathcal{G},\ \boldsymbol{\hbar} \in \mathcal{H}\}, \tag{13}$$

where $\mu(\cdot; e, \boldsymbol{g}, \boldsymbol{\hbar})$ is the conditional distribution (pmf) of the power allocation vector defined as follows

$$\mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) \triangleq \mathbb{P}\left(\begin{matrix}\text{using a power}\\ \text{splitting vector } \boldsymbol{\rho}\end{matrix} \big| e, \boldsymbol{G}=\boldsymbol{g}, \boldsymbol{H}=\boldsymbol{\hbar}\right), \tag{14}$$

and, for every $\boldsymbol{g}$, $\boldsymbol{\hbar}$, is subject to

$$\sum_{\boldsymbol{\rho} \in \mathscr{P}_{\leq}(e)} \mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) = 1, \tag{15a}$$

$$\mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) \geq 0, \qquad \forall \boldsymbol{\rho} \in \mathscr{P}_{\leq}(e), \tag{15b}$$

$$\mathscr{P}_{\leq}(e) \triangleq \left\{\boldsymbol{\rho}\ :\ \boldsymbol{\rho} \succeq 0\ \cap\ \rho^{\mathrm{tot}} \triangleq \mathbf{1}_N^T \boldsymbol{\rho} \leq e\right\}. \tag{15c}$$

$\mathscr{P}_{\leq}(e)$ is the set of all feasible vectors $\boldsymbol{\rho}$ when the energy level is e. The reward function becomes

$$C_{\mu}(E^{(0)}) = \sum_{e \in \mathcal{E}} \pi_{\mu}(e|E^{(0)}) \times \int_{\mathcal{G}\times\mathcal{H}} \underbrace{\sum_{\boldsymbol{\rho} \in \mathscr{P}_{\leq}(e)} c(\boldsymbol{\rho}, \boldsymbol{g}, \boldsymbol{\hbar}) \mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar})}_{\text{secrecy rate given the MC state } (e, \boldsymbol{g}, \boldsymbol{\hbar})} \mathrm{d}F(\boldsymbol{g}, \boldsymbol{\hbar}), \tag{16}$$

where $\pi_{\mu}(e|E^{(0)}) \in [0, 1]$ is the steady-state probability of having e energy quanta stored starting from state $E^{(0)}$ under a policy μ and $F(\boldsymbol{g}, \boldsymbol{\hbar})$ is the joint cumulative distribution function of $\boldsymbol{G}$ and $\boldsymbol{H}$. $\pi_{\mu}(e|E^{(0)})$ summarizes the battery evolution and is evaluated according to (11). The optimization variables in Problem (12) are the pmfs $\mu(\cdot; e, \boldsymbol{g}, \boldsymbol{\hbar})$. Also, it can be shown (see Section IV-A) that an OSP which admits steady-state distribution always exists. Therefore, without loss of optimality, we decided to restrict our study to the class of policies with steady-state distribution. For these policies, since we focus on the average long-term optimization, (16) is equivalent to (10).

It is possible to separate μ into the product of a *transmit power policy*, which specifies the conditional distribution of the total transmission power given the current state, namely $\gamma_{\mu}(\rho^{\mathrm{tot}}; e, \boldsymbol{g}, \boldsymbol{\hbar})$, and the conditional distribution of the power allocation given the total transmission power and the current state, namely $\phi_{\mu}(\boldsymbol{\rho}; \rho^{\mathrm{tot}}, e, \boldsymbol{g}, \boldsymbol{\hbar})$:

$$\mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) = \phi_{\mu}(\boldsymbol{\rho}; \rho^{\mathrm{tot}}, e, \boldsymbol{g}, \boldsymbol{\hbar}) \gamma_{\mu}(\rho^{\mathrm{tot}}; e, \boldsymbol{g}, \boldsymbol{\hbar}). \tag{17}$$

The above expression will be useful to decompose the problem into two steps in Theorem 2.

We highlight that μ performs a *power control* mechanism, i.e., it specifies how much power is used in every MC state but, in addition to power control, also the code rate can be changed according to Section II-B.

B. Finite Model

In the previous subsection, we assumed that the policy can be defined for every possible value of the channel gains. This can be done by simple enumeration if $|\mathcal{G}| < \infty$ and $|\mathcal{H}| < \infty$. However, the channel gains may be continuous variables in the general case. Instead of defining a policy for a continuously infinite set of values, we want to find a set of points where the policy can be computed and optimized efficiently. The following approach can be followed. Consider the random variable G_1 (for the others the reasoning is similar). We discretize the support of G_1 in n intervals with an *equally likely* strategy ($\mathbb{P}(G_1 \in [p_i, p_{i+1})) = 1/n$, $i = 1, \ldots, n$). Then, we specify the policy in the centroid of every interval. If the number of intervals n is sufficiently large, the approximation is very close to the continuous case.

Remark 1. *Since we consider a discrete channel, we focus without loss of generality on channel conditions with non-zero probability, i.e.,* $\mathbb{P}(\boldsymbol{G} = \boldsymbol{g}, \boldsymbol{H} = \boldsymbol{\hbar}) > 0$, $\forall \boldsymbol{g} \in \mathcal{G}, \boldsymbol{\hbar} \in \mathcal{H}$.

IV. Optimal Secrecy Policy with Complete CSI

In this section we study the case when the transmitter has perfect CSI knowledge, and introduce a technique to compute OSP and some of its properties. All our results are useful to simplify the numerical evaluation. In particular: 1) we prove that there exists a deterministic OSP (Theorem 1); 2) we propose a technique to derive a unichain OSP (Section IV-A); 3) we decompose the optimization process in two steps (Theorem 2); and 4) we show that the transmission power increases (decreases) with the channel gain of the legitimate receiver's (eavesdropper's) sub-carriers (Theorem 3).

Theorem 1. *There exists a deterministic OSP, i.e., an optimal secrecy policy in which, for every MC state* $(e, \boldsymbol{g}, \boldsymbol{\hbar})$

$$\mu^{\star}(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) = \begin{cases} 1, & \text{if } \boldsymbol{\rho} = \boldsymbol{\rho}^{\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}}, \\ 0, & \text{otherwise}, \end{cases} \tag{18}$$

for some $\boldsymbol{\rho}^{\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$ *depending upon the current MC state in general.*

Proof. See Appendix A. ∎

By exploiting Equation (17), it also follows that $\exists \rho^{\mathrm{tot}\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$ such that the transmit power policy γ_{μ} defined in (17) satisfies

$$\gamma_{\mu}(\rho^{\mathrm{tot}}; e, \boldsymbol{g}, \boldsymbol{\hbar}) = \begin{cases} 1, & \text{if } \rho^{\mathrm{tot}} = \rho^{\mathrm{tot}\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}}, \\ 0, & \text{otherwise.} \end{cases} \tag{19}$$

Definition 1 (Deterministic Policy)**.** *Since a deterministic OSP always exists, we only need to study deterministic policies, thus* μ *can be redefined as*

$$\mu = \{\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}} \in \mathscr{P}_{\leq}(e),\ \forall e \in \mathcal{E},\ \forall \boldsymbol{g} \in \mathcal{G},\ \boldsymbol{\hbar} \in \mathcal{H}\}. \tag{20}$$

$\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}} = [\rho_{1;e,\boldsymbol{g},\boldsymbol{\hbar}}, \ldots, \rho_{N;e,\boldsymbol{g},\boldsymbol{\hbar}}]$ *characterizes the transmission powers on different sub-carriers in state* $(e, \boldsymbol{g}, \boldsymbol{\hbar})$.

We also introduce the sub-policy μ^{tot} as

$$\mu^{\mathrm{tot}} = \{\rho^{\mathrm{tot}}_{e,\boldsymbol{g},\boldsymbol{\hbar}},\ \forall e \in \mathcal{E},\ \forall \boldsymbol{g} \in \mathcal{G},\ \boldsymbol{\hbar} \in \mathcal{H}\}, \tag{21}$$

which accounts for the total transmission powers only. μ^{tot} and μ are *consistent* if the sum of the elements of $\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$ in μ is equal to $\rho^{\mathrm{tot}}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$ in μ^{tot}, $\forall e \in \mathcal{E}, \boldsymbol{g} \in \mathcal{G}, \boldsymbol{\hbar} \in \mathcal{H}$.

The deterministic property is particularly useful to simplify the numerical evaluation because a policy needs to define only a scalar value for every state of the system and not a probability distribution.

A. Unichain Policies

We restrict our study to the class of *unichain* policies, i.e., those that induce a unichain MC (i.e., a MC with a single recurrent class). This is useful in order to apply the standard optimization algorithms in the next section.

Some sufficient conditions to obtain a unichain policy are presented in the following proposition (in this subsection we use deterministic policies for presentation simplicity, but the results can be easily extended).

Proposition 1. *If a policy satisfies one of the following conditions, then it is unichain. If it satisfies both conditions, the policy induces an irreducible, positive recurrent MC.*

1) *For every* $e \in \mathcal{E}\backslash\{e_{\max}\}$ *there exists a pair* $(\boldsymbol{g}', \boldsymbol{\hbar}')$ *such that* $\rho^{\text{tot}}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'} < b_{\max}$ *(maximum number of energy arrivals).*
2) *For every* $e \in \mathcal{E}\backslash\{0\}$ *there exists a pair* $(\boldsymbol{g}'', \boldsymbol{\hbar}'')$ *such that* $\rho^{\text{tot}}_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''} > b_{\min}$.

Proof. See Appendix B. ∎

In practice, the first and second points ensure that there is a positive probability that the battery moves from level e to higher and lower energy levels, respectively. When they are both verified, no transient state can exist, and the MC is irreducible.

When at least one point of Proposition 1 is satisfied, the corresponding policy is guaranteed to be unichain. However, in general, these conditions may not be satisfied and a policy may not be unichain. In addition, there may exist more than one policy with the same maximum achievable secrecy rate (the highest secrecy rate among $C_\mu(0), \dots, C_\mu(e_{\max})$). Some of these are unichain, whereas others are not. Consider the following example to justify these claims.

Example 1. *We want to show a case in which 1) multiple policies with the same maximum reward exist and 2) some of them are not unichain.*

Assume that the harvesting process is deterministic and equal to $b_{\max} < e_{\max}/2$, $N = 1$, *and the channel is constant* $g_1 > \hbar_1$. *Consider the following policies*

$$\mu_1 = \{\rho_{1;e,g_1,\hbar_1} = \min\{e, b_{\max}\},\ \forall e,\ \forall g_1,\ \hbar_1\},$$
$$\mu_2 = \begin{cases} \rho_{1;e,g_1,\hbar_1} = 2b_{\max}, & e = e_{\max},\ \forall g_1,\ \hbar_1 \\ \rho_{1;e,g_1,\hbar_1} = b_{\max}, & e = b_{\max},\ \forall g_1,\ \hbar_1 \\ \rho_{1;e,g_1,\hbar_1} = 0, & \textit{otherwise} \end{cases}.$$

μ_1 is a unichain policy (the recurrent class is the battery level $\{b_{\max}\}$) that provides a long-term secrecy rate $c(b_{\max}, g_1, \hbar_1)$. Instead, μ_2 is not unichain (the two recurrent classes are $\{b_{\max}\}$ and $\{e_{\max} - b_{\max}, e_{\max}\}$) and its long-term secrecy rate depends upon the initial state (it can be $c(b_{\max}, g_1, \hbar_1)$ or $0.5c(2b_{\max}, g_1, \hbar_1)$). Also, note that because of the concavity of Equation (8), $c(b_{\max}, g_1, \hbar_1) > 0.5c(2b_{\max}, g_1, \hbar_1)$. Therefore, there exist more than one policy with the same maximum achievable reward $c(b_{\max}, g_1, \hbar_1)$. Moreover, in μ_2, there are two recurrent classes, and thus it is not unichain.

This example shows that the long-term secrecy rate for a non-unichain policy may depend upon the starting state. Also, it shows that in general there may exist different policies, unichain and not unichain, with the same maximum achievable secrecy rate. The following proposition establishes that there is no loss in generality in considering only unichain policies.

Proposition 2. *Given a generic policy, it is always possible to derive another policy which is unichain and attains the same maximum achievable secrecy rate as the original policy, regardless of the initial state.*

Proof. We provide a constructive proof in Appendix C. ∎

In the rest of the paper we always refer to unichain policies, for which $C_\mu(E^{(0)})$ is independent of $E^{(0)}$ [41]. In particular, Proposition 2 holds for the optimal secrecy policies, i.e., there always exists a unichain OSP, and therefore we will focus on unichain policies with no loss in optimality. Note that, since we consider a finite MC (we discretized both the battery level and the channel gains), a unichain policy always implies the existence of a steady-state distribution as in Equation (16).

B. Computation of OSP

We now want to simplify the expression of C_μ by exploiting the results we have found so far. If μ and μ^{tot} are consistent, the long-term secrecy function C_μ can be rewritten as

$$C_\mu = \sum_{e\in\mathcal{E}} \pi_{\mu^{\text{tot}}}(e) \int_{\mathcal{G}\times\mathcal{H}} c(\overbrace{\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}}}^{\text{specified by } \mu}, \boldsymbol{g}, \boldsymbol{\hbar})\ \mathrm{d}F(\boldsymbol{g}, \boldsymbol{\hbar}). \tag{22}$$

An interesting fact is that the steady-state probability $\pi_{\mu^{\text{tot}}}(e)$ depends upon the sub-policy μ^{tot} only. This is because $\pi_{\mu^{\text{tot}}}(e)$ describes the battery energy evolution, that depends only upon the total energy consumption in a slot, not upon the particular power splitting scheme. This result leads to the following theorem.

Theorem 2. *The maximization of C_μ can be decomposed into two steps:*

1) *fix a value x and the channel gain vectors $\boldsymbol{g}$, $\boldsymbol{\hbar}$ and find the optimal power splitting choice*

$$\boldsymbol{\rho}^\star = \arg\max_{\boldsymbol{\rho}} c(\boldsymbol{\rho}, \boldsymbol{g}, \boldsymbol{\hbar}), \tag{23a}$$
$$\textit{s.t.:}\quad \boldsymbol{\rho} \in \mathscr{P}_=(x) \triangleq \left\{\boldsymbol{\rho}\ :\ \boldsymbol{\rho} \succeq 0,\ x = \mathbf{1}_N^T \boldsymbol{\rho}\right\}; \tag{23b}$$

2) *maximize C_μ by considering only μ^{tot}*

$$\mu^{\text{tot}\star} = \arg\max_{\mu^{\text{tot}}} C_\mu, \tag{24a}$$
$$\textit{s.t.:}\quad \mu^{\text{tot}} \textit{ and } \mu \textit{ are consistent,} \tag{24b}$$
$$\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}} \textit{ solves (23) with } x = \rho^{\text{tot}}_{e,\boldsymbol{g},\boldsymbol{\hbar}},\ \forall e \in \mathcal{E}, \forall \boldsymbol{g} \in \mathcal{G},\ \forall \boldsymbol{\hbar} \in \mathcal{H}. \tag{24c}$$

The optimal $\mu^\star$ can be found by fixing $\rho^{\text{tot}\star}$ according to point 2) and choosing $\boldsymbol{\rho}$ with the optimal power splitting choice of point 1).

Proof. See Appendix D. ∎

The *optimal power splitting choice* $\boldsymbol{\rho}^\star$ that solves (23) can be found with a Lagrangian approach (for further details, see Theorem 1 and Equation (7) in [29]):

$$\rho_r^\star = \left[\sqrt{\frac{\alpha_r^2}{4} + \frac{\alpha_r}{\eta}} - \frac{\beta_r}{2}\right]^+, \tag{25}$$

$$\alpha_r \triangleq \frac{1}{\hbar_r} - \frac{1}{g_r}, \qquad \beta_r \triangleq \frac{1}{\hbar_r} + \frac{1}{g_r}, \tag{26}$$

where η is a parameter used to satisfy $x = \sum_{r=1}^{N} \rho_r^\star$. In the remainder of the paper we assume that this optimal power splitting choice is used, unless otherwise stated. We highlight that OSP yields $\rho_r^\star = 0$ if $g_r \leq \hbar_r$, which implies that the achievable secrecy rate with complete CSI is independent of the coding scheme (the two expressions in Equation (7) coincide).

To solve Step 2) instead, the Optimal Secrecy Policy can be found numerically via dynamic programming techniques, e.g., using the Policy Iteration Algorithm (PIA) [42].[3] PIA alternates between a value determination phase, in which the current policy is evaluated, and a policy improvement phase, in which an attempt is made at improving the current policy. Policy improvement and evaluation can be performed in $\mathcal{O}((e_{\max})^3 n^{2N})$ and $\mathcal{O}((e_{\max})^3)$ arithmetic operations, respectively, where $\mathcal{O}(\cdot)$ is the standard asymptotic notation. This result is derived as follows. For every state of the system ($e_{\max} \times n^N \times n^N$), the policy improvement step requires to find the best transmission power (which is $\mathcal{O}(e_{\max})$) to reach every other battery level ($e_{\max}$). Instead, the $\mathcal{O}((e_{\max})^3)$ performance of the policy evaluation step is due to a matrix inversion cost (which can be reduced to $\mathcal{O}((e_{\max})^{2.373})$ using Coppersmith-Winograd like algorithms). The previous two steps are performed iteratively until the optimal policy is found, which, in general, requires few iterations (< 10). Therefore, PIA has a polynomial complexity in the number of states of the system.

Note that Theorem 2 with (25)-(26) decompose the optimization into two steps. Therefore, the numerical evaluation only requires to study the two points separately instead of performing a (more computationally intensive) bi-dimensional optimization.

We also remark the following.

Lemma 1. *By restricting the study to the unichain policies constructed as in Appendix C, OSP is uniquely determined.*

Proof. In all the transient states, by construction (Appendix C), we have $\rho^{\text{tot}\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}} = 0$. For the recurrent states, thanks to [42, Vol. II, Sec. 4], we know that $\rho^{\text{tot}\star}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$ is uniquely determined. ■

C. Properties

We now derive a property that is useful to understand when the transmission power increases or decreases.

[3] A key assumption of PIA is that, at every algorithm step, a *unichain* policy is produced. In order to satisfy this condition, we apply the technique of Appendix C.

Proposition 3. *Consider two channel states $\boldsymbol{g}'$, $\boldsymbol{\hbar}'$ and $\boldsymbol{g}''$, $\boldsymbol{\hbar}''$ and define*

$$D(\rho^{\text{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'') \triangleq \frac{\partial}{\partial \rho^{\text{tot}}} \Big(c(\boldsymbol{\rho}^\star_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\rho}^\star_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \Big), \tag{27}$$

where $\boldsymbol{\rho}^\star_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''}$ and $\boldsymbol{\rho}^\star_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$ are defined as the solutions[4] of Problem (23) with $x = \rho^{\text{tot}}$.

OSP has the following trend

- *if $D(\rho^{\text{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'') \geq 0$, $\forall \rho^{\text{tot}}$, then $\rho^{\text{tot}\star}_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''} \geq \rho^{\text{tot}\star}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$;*
- *if $D(\rho^{\text{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'') \leq 0$, $\forall \rho^{\text{tot}}$, then $\rho^{\text{tot}\star}_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''} \leq \rho^{\text{tot}\star}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$.*

Proof. See Appendix E. ■

In practice, it is better to use more energy in the directions where the function $c(\cdot,\cdot,\cdot)$ increases. A consequence of the previous proposition is derived in the following theorem.

Theorem 3. *Consider $N = 1$. The transmission power of OSP is non-decreasing with g and non-increasing with $\hbar$ (we omit the "1" subscripts). Formally*

- *if $g'' \geq g'$, then $\rho^{\text{tot}\star}_{e,g'',\hbar} \geq \rho^{\text{tot}\star}_{e,g',\hbar}$;*
- *if $\hbar'' \geq \hbar'$, then $\rho^{\text{tot}\star}_{e,g,\hbar''} \leq \rho^{\text{tot}\star}_{e,g,\hbar'}$.*

Proof. See Appendix F. ■

This is an expected result, i.e., when the legitimate channel improves, then it is reasonable to use more energy in order to get a higher rate. Conversely, when the eavesdropper's channel improves, it is better not to use a lot of energy because only low rates can be obtained. In this case, it is better to conserve energy and wait for a better slot. The previous theorem is useful to prune the action space in the numerical computation: if we found the optimal transmission power for a given channel state, we could exploit it as lower [upper] bound for better [worse] channel states.

We expect that a result similar to Theorem 3 holds for a generic $N > 1$. A formal proof would require to explicitly compute $D(\rho^{\text{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'')$ and show that it is non-negative or non-positive (see Appendix F). However, this would require the computation of an analytical expression for η in Equation (25). Even though this is in principle possible for any fixed N, the corresponding expression is very complicated and, in practice, the resulting $D(\rho^{\text{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'')$ is too long to be analytically tractable.

V. Optimal Secrecy Policy with Partial CSI

In the previous sections we assumed that the realizations of $\boldsymbol{G}$ and $\boldsymbol{H}$, namely $\boldsymbol{g}$ and $\boldsymbol{\hbar}$, are known at the transmitter. This may not be true in practice. In particular, it is likely that, since the eavesdropper does not cooperate with the transmitter, its channel gain is unknown. In this section we gradually remove these assumptions and discuss how the achievable secrecy rate changes as a result.

[4] Note that $\boldsymbol{\rho}^\star_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''}$ and $\boldsymbol{\rho}^\star_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$ depend upon ρ^{tot}.

We assume that $\boldsymbol{G} = [G_1, \dots, G_N]$ and $\boldsymbol{H} = [H_1, \dots, H_N]$ have independent components and are independent of each other. In this section we assume that all links are affected by i.i.d. Nakagami fading. This means that the amplitude of a received signal has a Nakagami pdf with parameters m and κ, i.e.,

$$f(x; m, \kappa) = 2\left(\frac{m}{\kappa}\right)^m \frac{1}{\Gamma(m)} x^{2m-1} e^{-\frac{m}{\kappa}x^2}, \quad x \geq 0, \quad (28)$$

$$\Gamma(m) \triangleq \int_0^\infty e^{-t} t^{m-1} \, \mathrm{d}t. \quad (29)$$

Therefore, G_r and H_r exhibit a Gamma distribution. The pdf of G_r (with mean $\bar{g}_r$) is

$$f_{G_r}(g; m) = \left(\frac{m}{\bar{g}_r}\right)^m \frac{1}{\Gamma(m)} g^{m-1} e^{-\frac{m}{\bar{g}_r}g}, \quad \begin{matrix} g \in \mathbb{R}_+, \\ m \geq 1 \end{matrix} \quad (30)$$

and similarly for H_r (for presentation simplicity, we assume that the legitimate receiver and the eavesdropper have the same index m, but the analysis can be extended to a more general case). Note that $m = 1$ corresponds to Rayleigh fading and $f_{G_r}(g; 1) = \frac{1}{\bar{g}_r} e^{-g/\bar{g}_r}$ is an exponential distribution. As m increases, the strength of the line of sight component increases. For ease of notation, in the remainder of the paper we drop the dependence on m and implicitly assume $f_{G_r}(g) = f_{G_r}(g; m)$.

A. Unknown Eavesdropper's Channel

In this section, we assume that both the legitimate and the eavesdropper's channels are affected by fading but CSI is available only for $\boldsymbol{G}$. In this case, due to this lack of information, it may happen that EHD transmits even when the eavesdropper's channel gain is higher than the legitimate one.

Similarly to Expression (20) in the previous section, a policy μ can be defined as

$$\mu = \{\boldsymbol{\rho}_{e,\boldsymbol{g}} \triangleq [\rho_{1;e,\boldsymbol{g}}, \dots, \rho_{N;e,\boldsymbol{g}}] \in \mathscr{P}_{\leq}(e), \ \forall e \in \mathcal{E}, \ \forall \boldsymbol{g} \in \mathcal{G}\}, \quad (31)$$

and similarly for μ^{tot}. $\boldsymbol{\rho}_{e,\boldsymbol{g}}$ represents the transmission power used in state $(e, \boldsymbol{g})$ (since $\boldsymbol{\hbar}$ is unknown, it cannot be included in the state of the system). We remark that μ performs a *power control* mechanism, i.e., a policy specifies only the transmission power $\boldsymbol{\rho}_{e,\boldsymbol{g}}$. However, in addition to power control, in every slot also the code rate can be changed (see Section II-B). In particular, variable rate coding provides higher secrecy rates than constant rate coding, but is more difficult to implement. In the following we analyze both these approaches.[5]

1) Constant Rate Coding: The simplest assumption is that the coding scheme has constant rate and its choice only depends on the overall channel statistics. Using constant rate coding, the eavesdropper is able to gather more information than the legitimate receiver when its channel is better. Because of this, for some r, we may have (see Equation (7))

$$R_{g_r,\hbar_r}(\rho_{r;e,\boldsymbol{g}}) < 0. \quad (32)$$

The secrecy rate expression becomes

$$C_\mu = \sum_{e=0}^{e_{\max}} \pi_{\mu^{\mathrm{tot}}}(e) \int_{\mathbb{R}_+^N} \int_{\mathbb{R}_+^N} \sum_{r=1}^N \log_2\left(\frac{1 + g_r \rho_{r;e,\boldsymbol{g}}}{1 + \hbar_r \rho_{r;e,\boldsymbol{g}}}\right) \times \prod_{r=1}^N \left(f_{G_r}(g_r) f_{H_r}(\hbar_r)\right) \mathrm{d}\boldsymbol{g} \ \mathrm{d}\boldsymbol{\hbar}, \quad (33)$$

Note that in (33) we integrate both positive and negative terms. The negative terms are due to the fact that the eavesdropper's channel may be better than the legitimate one ($\hbar_r > g_r$).

We now want to extract some properties of the optimal secrecy policy in this context. We start by performing the following computations, which will be used to extend the first point of Theorem 3.

The channel memoryless property can be used to simplify (33) and recast the problem using an MDP. By integrating over $\boldsymbol{\hbar}$, we obtain

$$C_\mu = \sum_{e=0}^{e_{\max}} \pi_{\mu^{\mathrm{tot}}}(e) \int_{\mathbb{R}_+^N} \sum_{r=1}^N T_r^{\mathrm{con}}(g_r, \rho_{r;e,\boldsymbol{g}}) \prod_{r=1}^N f_{G_r}(g_r) \ \mathrm{d}\boldsymbol{g}. \quad (34)$$

$$T_r^{\mathrm{con}}(g, \rho) \triangleq \int_{\mathbb{R}_+} \log_2\left(\frac{1 + g\rho}{1 + \hbar\rho}\right) f_{H_r}(\hbar) \ \mathrm{d}\hbar. \quad (35)$$

The function $T_r^{\mathrm{con}}(g, \rho)$ is presented in Equation (36), where $\mathrm{Ei}(z) = -\int_{-z}^\infty \frac{e^{-t}}{t} \ \mathrm{d}t$ is the exponential integral function and s_i, t_i are constants.[6]

$$T_r^{\mathrm{con}}(g, \rho) = \log_2(1 + g\rho) + \frac{1}{\log 2} \sum_{i=2}^m \left(s_i \left(\rho \bar{h}_r\right)^{i-m} + e^{\frac{m}{\rho \bar{h}_r}} \mathrm{Ei}\left(-\frac{m}{\rho \bar{h}_r}\right) \sum_{i=1}^m t_i \left(\rho \bar{h}_r\right)^{i-m} \right). \quad (36)$$

A secure transmission can be performed only if $C_\mu > 0$. The maximum of (34) can be found with an MDP approach, where the MC state is given by the pair $(e, \boldsymbol{g})$.

A property, that directly follows from the definitions of $T_r^{\mathrm{con}}(g, \rho)$, is the following.

Proposition 4. *If for $\rho > 0$ we obtain $T_r^{\mathrm{con}}(g, \rho) < 0$, then allocating a power ρ over sub-carrier r is strictly sub-optimal.*

This result is intuitive. Indeed, if $T_r^{\mathrm{con}}(g, \rho) < 0$ and $\rho > 0$, then in (34) we are adding negative terms. This is clearly sub-optimal because it lowers the secrecy rate and wastes energy at the same time.

Even if $T_r^{\mathrm{con}}(g, \rho)$ has a complicated expression, as we will see, we are interested in its double derivative with respect to g and ρ:

$$\frac{\partial^2}{\partial \rho \partial g} T_r^{\mathrm{con}}(g, \rho) = \frac{1}{\log 2} \frac{1}{(1 + g\rho)^2}. \quad (37)$$

We now show that even with partial CSI the optimal secrecy policy increases with the legitimate channel gain. As for

[5]Differently from the complete CSI case of Section IV, ρ_r cannot be set to 0 if $g_r \leq \hbar_r$ (see Equation (25)), thus using constant rate or variable rate coding leads to different results.

[6]Closed form expressions for s_i and t_i can be derived but are quite complicated. Moreover, we will see that they do not contribute to our next results.

Theorem 3, the following result can be used to prune the action space.[7]

Theorem 4. *Consider $N = 1$. With partial CSI, the transmission power of OSP is non-decreasing with g (we omit the "1" subscripts). Formally, if $g'' \geq g'$, then $\rho^{\text{tot}\star}_{e,g''} \geq \rho^{\text{tot}\star}_{e,g'}$.*

Proof. The proof follows the same steps presented in Appendices A, E, F. To prove the theorem the key point is that

$$\frac{\partial^2}{\partial\rho\partial g} T_r^{\text{con}}(g,\rho) \geq 0. \tag{38}$$

Note that, considering the derivative with respect to ρ, it follows from (38) that $\frac{\partial}{\partial g} T_r^{\text{con}}(g,\rho_B) - \frac{\partial}{\partial g} T_r^{\text{con}}(g,\rho_A) \geq 0$, for $\rho_A \leq \rho_B$. We can rewrite the inequality as $\frac{\partial}{\partial g}\big(T_r^{\text{con}}(g,\rho_B) - T_r^{\text{con}}(g,\rho_A)\big) \geq 0$ and obtain

$$\begin{aligned} &T_r^{\text{con}}(g+\Delta,\rho_A) - T_r^{\text{con}}(g,\rho_A) \\ &\leq T_r^{\text{con}}(g+\Delta,\rho_B) - T_r^{\text{con}}(g,\rho_B), \end{aligned} \tag{39}$$

$\forall \Delta \geq 0$ and $\rho_A \leq \rho_B$. This condition can be replaced with Equation (64) in Appendix E to prove the theorem. ∎

2) Variable Rate Coding: Better performance can be obtained with variable rate coding (see Equations (5) and (6)). In this case, in every slot, the code rate is matched to the legitimate channel rate. Thus, even if $g_r \leq \hbar_r$ (eavesdropper's channel is better), the eavesdropper can gather at most R_{g_r} bits (legitimate transmission rate) and not $R_{\hbar_r}$ (eavesdropper's transmission rate). The secrecy rate expression is

$$\begin{aligned} C_\mu = \sum_{e=0}^{e_{\max}} \pi_{\mu^{\text{tot}}}(e) \int_{\mathbb{R}_+^N} \int_{\mathbb{R}_+^N} \sum_{r=1}^{N} \left[\log_2\left(\frac{1+g_r\rho_{r;e,\boldsymbol{g}}}{1+\hbar_r\rho_{r;e,\boldsymbol{g}}}\right)\right]^+ \\ \times \prod_{r=1}^{N} \Big(f_{G_r}(g_r) f_{H_r}(\hbar_r)\Big)\, \mathrm{d}\boldsymbol{g}\, \mathrm{d}\boldsymbol{\hbar}, \end{aligned} \tag{40}$$

As before, we introduce a function $T_r^{\text{var}}(g,\rho_{r;e,\boldsymbol{g}})$ such that

$$C_\mu = \sum_{e=0}^{e_{\max}} \pi_{\mu^{\text{tot}}}(e) \int_{\mathbb{R}_+^N} \sum_{r=1}^{N} T_r^{\text{var}}(g_r,\rho_{r;e,\boldsymbol{g}}) \prod_{r=1}^{N} f_{G_r}(g_r)\, \mathrm{d}\boldsymbol{g}. \tag{41}$$

$$T_r^{\text{var}}(g,\rho) \triangleq \int_{\mathbb{R}_+} \left[\log_2\left(\frac{1+g\rho}{1+\hbar\rho}\right)\right]^+ f_{H_r}(\hbar)\, \mathrm{d}\hbar \tag{42}$$

$$= \int_0^g \log_2\left(\frac{1+g\rho}{1+\hbar\rho}\right) f_{H_r}(\hbar)\, \mathrm{d}\hbar. \tag{43}$$

In Equation (43) we integrate from zero to g, thus we remove the $[\cdot]^+$ notation (see the structure of Equation (7) with variable rate coding).

Note that $T_r^{\text{var}}(g,\rho) \geq T_r^{\text{con}}(g,\rho)$, which justifies the fact that the achievable secrecy rate with variable rate coding is higher than with constant rate coding.

The analogous of Theorem 4 holds in this case, as can be proved by exploiting the structure of the double derivative of $T_r^{\text{var}}(g,\rho)$:

$$\frac{\partial^2}{\partial\rho\partial g} T_r^{\text{var}}(g,\rho) = \frac{1}{\log 2} \frac{\Gamma(m) - \Gamma\left(m, \frac{mg}{\bar{h}_r}\right)}{(1+g\rho)^2\Gamma(m)}, \tag{44}$$

[7]We provide a formal proof only for the case $N = 1$ because, even if theoretically possible, the proof for a generic $N > 1$ is not analytically tractable (see the related discussion just after Theorem 3).

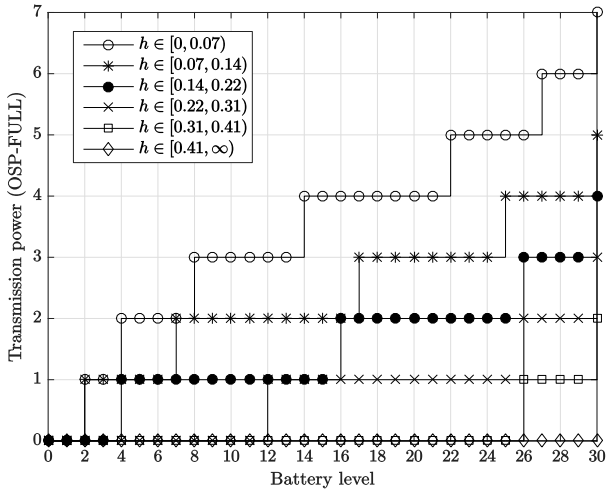

Figure 2: Transmission power $\rho^{\text{tot}\star}_{e,g,\hbar}$ as a function of the battery level e for several values of $\hbar$ and $g \in [0.41, 0.51)$.

where $\Gamma(m,z) \triangleq \int_z^\infty e^{-t} t^{m-1}\, \mathrm{d}t$ is the incomplete gamma function.

B. No Channel State Information

Lower secrecy rates are obtained when also the legitimate receiver's channel is unknown. In particular, the transmission power cannot be adapted to the current channel state. It is easy to show that C_μ can be greater than zero only if $\bar{g}_r > \bar{h}_r$ for some r. However, the mean values of the channel gains are not controlled by the transmitter (they are physical quantities), thus if the legitimate channel is (statistically) worse, no secrecy can be achieved.

VI. Numerical Evaluation

In this section we discuss how the secrecy rate changes as a function of the different system parameters.

We compare the following scenarios: OSP with full CSI (OSP-FULL), OSP with only legitimate channel knowledge and constant rate coding (OSP-PAR-CON) or variable rate coding (OSP-PAR-VAR) and OSP with only statistical channel knowledge (OSP-STAT).

If not otherwise stated, the simulation parameters are: $e_{\max} = 30$, truncated geometric energy arrivals with $b_{\max} = 6$ and $\bar{b} = 1$, $n = 15$ quantization intervals (see Section III-B), $N = 1$ (single sub-carrier), $\bar{g} = \bar{h} = 1$ (symmetric scenario), $\mathcal{G} = \mathcal{H} = \mathbb{R}_+$ with $m = 1$ (Rayleigh fading). After showing results for this choice of parameters, we study the sensitivity of the system performance by changing one or more parameters while keeping the others fixed.

1) Fixed Parameters: Figure 2 shows the optimal transmission power $\rho^{\text{tot}\star}_{e,g,\hbar}$ as a function of the battery level e when $g \in [0.41, 0.51)$ and $\hbar \in \mathbb{R}_+$. We recall that, when $\mathcal{G} = \mathcal{H} = \mathbb{R}_+$, we use the technique explained in Section III-B, i.e., we have a finite number of points where the transmission power is computed ($n = 15$). When $\hbar \geq 0.51$, the transmission power is identically zero because the eavesdropper is always advantaged. Also when $\hbar \in [0.41, 0.51)$ the transmission

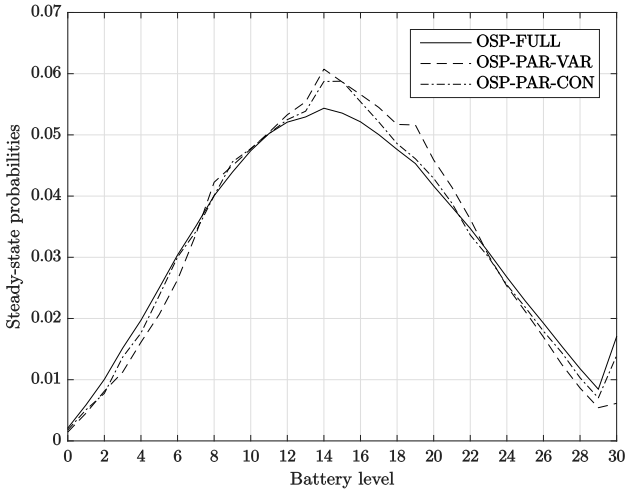

Figure 3: Steady-state probabilities $\pi_{\mu^{\mathrm{tot}}}(e)$ as a function of the battery level e.

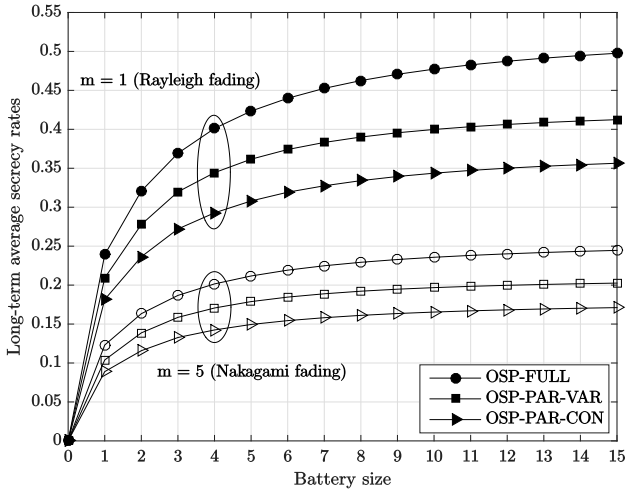

Figure 4: Secrecy rate C_μ as a function of the battery size $e_{\max}$ in the case of symmetric channel conditions.

power is zero. This is not obvious a priori and strongly depends upon the considered interval of g. It can be seen that Theorem 3 holds, i.e., $\rho^{\mathrm{tot}\star}_{e,g,\hbar}$ does not increase with $\hbar$. Finally, we note that the behavior of the transmission power is not obvious a priori, e.g., it is significantly different from a simple greedy policy ($\rho^{\mathrm{tot}\star}_{e,g,\hbar} = e$) even when $\hbar$ is low.

Figure 3, instead, shows the steady-state probabilities as a function of the energy level e, for fixed $e_{\max}$ and in the different scenarios. In all cases, the curves are similar. This is because the device tends to operate in an efficient region, i.e., approximately at $e_{\max}/2$. This is in order to avoid energy outage and overflow, that degrade the performance of the system. When e approaches $e_{\max}$, the steady-state tails increase because of the overflow (when the battery is almost full, all harvesting events leading to overflow contribute to increasing the steady-state probability of state $e_{\max}$, which is then higher than those of the immediately lower states).

2) Battery Size: In Figure 4 we show the rate achieved by the various policies as a function of the battery size $e_{\max}$. We use Rayleigh ($m = 1$) and a general Nakagami fading with a strong Line of Sight (LoS) component ($m = 5$). The curves of OSP-STAT are identically zero because $\bar{g} = \bar{h}$. As expected, OSP-FULL has the highest secrecy rate for every value. It can be seen that the curves saturate after a certain value. This is due to the combination of two effects: 1) the harvesting rate of the EHD is limited (it can be shown that the performance of an EH system is bounded) and 2) the achievable secrecy rate always saturates in the high power regime (because of the structure of Equation (7)). Note that the curves saturate already for small $e_{\max}$, therefore, in practice, it may be sufficient to use small batteries to obtain high secrecy rates.

In [29, Section IV-B] the authors showed that, when the transmission is subject to an average power constraint, the performance of the optimal transmission scheme with variable rate coding and partial CSI knowledge approaches the performance of the full CSI case when the transmission power is sufficiently high. In our previous example, OSP-PAR-VAR does not achieve OSP-FULL when $e_{\max}$ increases because an energy harvesting system imposes an average power constraint $\bar{b}$.[8] It can be verified that, when $\bar{b}$ increases, if the battery size is sufficiently large, the gap between OSP-PAR-VAR and OSP-FULL is smaller.

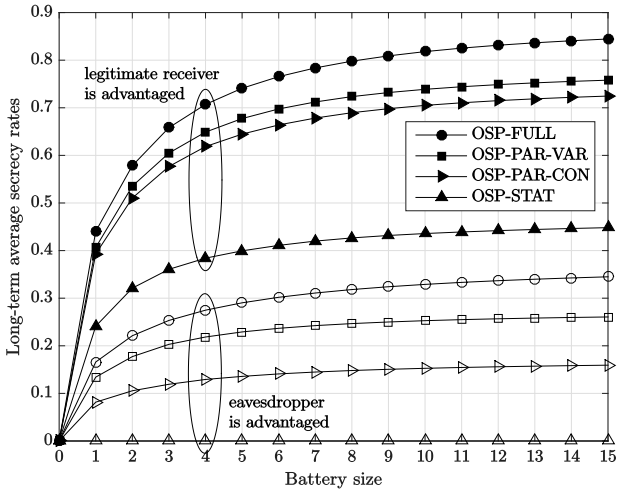

Figure 5: Secrecy rate C_μ as a function of the battery size $e_{\max}$ in the case of asymmetric channel conditions and Rayleigh fading.

Note that the achievable secrecy rates strongly depend upon the fading statistics. With $m = 5$, we have strong LoS components, i.e., the channel pdfs tend to be narrow around their means ($\bar{g} = \bar{h}$). It follows that the legitimate and eavesdropper's channel gains are close to each other most of the time. This corresponds to low values of $R_{g_r,\rho_r}(\rho_r)$, thus a low secrecy rate. With Rayleigh fading, instead, exploiting

[8]This can be easily derived starting from the causality constraint

$$\sum_{k=0}^{K}\sum_{r=1}^{N}\Sigma_r^{(k)} \le E^{(0)} + \sum_{k=0}^{K-1} B^{(k)}, \qquad \forall K = 0, 1, \dots \tag{45}$$

where, according to Equation (11), $\Sigma_r^{(k)}$ is the transmission power over subcarrier r in time slot k, $B^{(k)}$ is the amount of energy harvested in slot k and $E^{(0)}$ is the amount of energy initially available in the battery. In the long run, the right-hand side becomes the power constraint of our system.

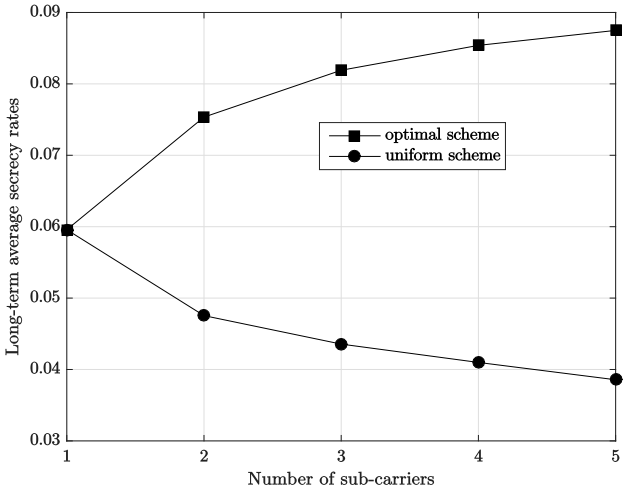

Figure 6: Secrecy rate C_μ as a function of the number of sub-carriers N.

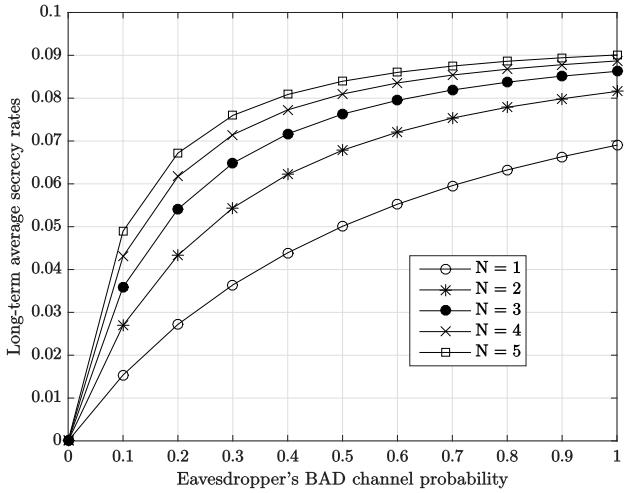

Figure 7: Secrecy rate C_μ of OSP-FULL as a function of the eavesdropper's BAD channel probability in a binary channel system.

channel diversity allows to obtain higher rewards. This is also the reason why, with Rayleigh fading, full channel state information (OSP-FULL) provides a great improvement with respect to the partial knowledge cases.

Figure 5 is similar to the previous one but with asymmetric channel gains. When the eavesdropper is advantaged ($\bar{g} = 1$, $\bar{h} = 2$), even if low performance can be achieved, secret transmission is still possible. When OSP-PAR-CON is used, it is likely that EHD transmits even when the eavesdropper's channel is better and in this case, from Equation (34), the secrecy rate is lower. This effect is emphasized if the eavesdropper's channel is advantaged, because it is more likely that the legitimate channel is the worse of the two.

On the other hand, if the legitimate channel is better ($\bar{g} = 2$, $\bar{h} = 1$), the secrecy rate can reach high values. In this case, OSP-STAT is also considered and, as expected, is the worst among the optimal policies.

3) Number of sub-carriers: When $N = 1$, finding the optimal policies for high values of n (fine quantization of the channel gains) is feasible. We recall that the number of states of the MC is directly proportional to the number of possible combinations of channel gains. Thus, with $N = 1$, the possible combinations are $n \times n$ (legitimate channel $\times$ eavesdropper's channel). With a generic N, the combinations become $n^N \times n^N$. Thus, the number of states grows exponentially with the number of sub-carriers, making the optimization process for high N infeasible in practice (curse-of-dimensionality). Even when the problem symmetry can be exploited (when G_r and H_r are i.i.d.), the computational effort still remains heavy. In pratice, this approach can be applied to multi-carrier scenarios if the number of carriers, N, and the number of quantization levels for the channel, n, are not too large. Note however that our solution suffers from a dimensionality problem because it is the *optimal* solution. Part of our future work agenda includes the design of sub-optimal schemes and the study of trade-offs between computational times and performance.

In the following, as an example, we consider a discrete GOOD-BAD channel and discuss the importance of the power splitting scheme. We define $\mathcal{G} = \mathcal{H} = \{\mathrm{B}, \mathrm{G}\} = \{1/30, 3/30\} = \{-15 \text{ dB}, -10 \text{ dB}\}$ with probabilities 0.7 and 0.3, respectively. We also set $e_{\max} = 10$ because, generally, the saturation region is almost reached for this battery size (see Figures 4 and 5). In Figure 6, we plot OSP-FULL as a function of the number of sub-carriers N when the optimal (Equations (25)-(26)) or a uniform power splitting is used. In the optimal case, as N increases, the reward also increases. This is expected because, when one user experiences a bad channel condition, then the power can be directed to other good sub-carriers. Instead, with uniform power splitting, the secrecy rate decreases with N. In practice, this happens because, instead of sending all the transmission power in the "good" sub-carriers, a fraction of this is wasted in the "bad" sub-carriers. For example, with $N = 2$, it may happen that over sub-carrier 1 the pair legitimate-eavesdropper's channel gain is (G, B) whereas, for sub-carrier 2, the pair is (B, B), i.e., sub-carrier 1 is a "good" sub-carrier while sub-carrier 2 is not. In this case, if a positive transmission power were used, the corresponding reward would be greater than zero but the power sent over sub-carrier 2 would be wasted (only when the two pairs are (G, B) and (G, B), is no power wasted during the transmission). This explains why the performance degrades as the number of sub-carriers increases. Moreover, the effect is emphasized with larger N because there are more cases where the transmission power cannot be fully exploited.

When the legitimate and the eavesdropper's channel gains are known in every slot, using a smart power splitting scheme is convenient because it can significantly improve the network performance. If this is not possible (e.g., because this information is not available or not reliable), a sub-optimal strategy needs to be adopted, e.g., uniform power splitting, which is simpler to implement but yields lower performance in general. The study of the information/performance tradeoff for power splitting strategies is left for future work.

Finally, Figure 7 shows how the optimal secrecy rate changes as a function of $\mathbb{P}(h_1 = \mathrm{B}) = \mathbb{P}(h_2 = \mathrm{B}) \in [0, 1]$

for different numbers of sub-carriers. It can be noticed that the case with five sub-carriers and $\mathbb{P}(h_1 = \mathrm{B}) = 0.2$ achieves the same performance as the system with only one sub-carrier but $\mathbb{P}(h_1 = \mathrm{B}) = 1$. In practice, the diversity offered by a greater number of sub-carriers can be efficiently exploited to obtain higher secrecy rates. An interesting point is that, as N increases, the improvement obtained from N to $N+1$ decreases. This is due to the concavity properties of Equation (8). Therefore, it may not be necessary to use a large number of sub-carriers to obtain high secrecy rates.

VII. Conclusions

In this work we analyzed an Energy Harvesting Device that has a finite energy storage and transmits secret data to a receiver over N parallel channels exploiting physical layer characteristics. We found the best power allocation technique, namely the Optimal Secrecy Policy (OSP), in several contexts depending on the degree of channel knowledge the device has. We proved several properties of OSP and in particular that it is deterministic and monotonic. We also described a technique to compute OSP by decomposing the problem in two steps and using a dynamic programming approach. When only partial channel state information is available, we described how the maximum secrecy rate varies with constant and variable rate coding, explaining and numerically evaluating the advantages of variable rate coding. We numerically showed that, because of the limited harvesting rate that is inherently provided by the renewable energy source, OSP-PAR-VAR does not achieve the same performance of OSP-FULL as the battery size increases, and noted that it is not necessary to use very large batteries to achieve close to optimal performance. We also set up the problem when more than one sub-carrier is considered, and discussed the scalability problems related to such scenario. Also, we found that using the optimal power splitting scheme provides a significant advantage with respect to the simpler uniform splitting approach.

Future work may include the study of sub-optimal strategies for the case with N sub-carriers in order to avoid the curse-of-dimensionality problem. Also, other optimization techniques can be investigated, e.g., offline approach, Lyapunov optimization or reinforcement learning approach. Finally, it would be interesting to set up a simulation experiment with real data measurements (e.g., for the harvesting process) in order to validate our results in a realistic scenario.

Appendix A
Proof of Theorem 1

We want to show that OSP is a deterministic policy, i.e., given the state of the system, $\mu(\boldsymbol{\rho}; e, \boldsymbol{g}, \boldsymbol{\hbar}) = \delta_{\boldsymbol{\rho}, \boldsymbol{\rho}^\star_{e,\boldsymbol{g},\boldsymbol{\hbar}}}$, where $\delta_{\cdot,\cdot}$ is the Kronecker delta function.[9]

Note that the study can be split into two parts according to Equation (17). Thus, we only need to prove that both $\gamma_\mu(\rho^{\mathrm{tot}}; e, \boldsymbol{g}, \boldsymbol{\hbar})$ (transmit power policy) and $\phi_\mu(\boldsymbol{\rho}; \rho^{\mathrm{tot}}, e, \boldsymbol{g}, \boldsymbol{\hbar})$ are deterministic. In the following we prove the first part. The latter is derived in [29].

[9] A proof of this result in the discounted horizon case can be found in [43, Theorems 6.2.9 and 6.2.10]. In our discussion we follow a different approach which will also be useful to prove Proposition 3.

A. Deterministic Transmit Power Policy

As a preliminary result, we need the following proposition (in this subsection, the expectation is always taken with respect to $\boldsymbol{G}$ and $\boldsymbol{H}$).

Proposition 5. *$\mathbb{P}(E^{(k)} = e | E^{(0)})$ depends upon the policy only through $\mathbb{E}[\gamma_\mu(\rho^{\mathrm{tot}}; e, \boldsymbol{G}, \boldsymbol{H})]$, $\forall \rho^{\mathrm{tot}} \in \{0, \dots, e\}$, $\forall e \in \mathcal{E}$.*

Proof. The proof is by induction on k. At $k = 0$, $\mathbb{P}(E^{(0)} = e | E^{(0)} = e_0)$ is equal to 1 if $e = e_0$ and to 0 otherwise. In this case there is no dependence upon the policy.

Assume that the thesis is true for k (inductive hypothesis). Using the chain rule, the probability that $E^{(k+1)} = e'$ given the initial state is

$$\mathbb{P}(E^{(k+1)} = e' | E^{(0)}) = \sum_{e=0}^{e_{\max}} \mathbb{P}(E^{(k+1)} = e' | E^{(k)} = e) \times \mathbb{P}(E^{(k)} = e | E^{(0)}). \quad (46)$$

Thus, to prove the thesis, we focus on $\mathbb{P}(E^{(k+1)} = e' | E^{(k)} = e)$, whereas for $\mathbb{P}(E^{(k)} = e | E^{(0)})$ we use the inductive hypothesis. Assume $e' < e_{\max}$

$$\mathbb{P}(E^{(k+1)} = e' | E^{(k)} = e) = \sum_{b=\max\{0, e'-e\}}^{\min\{e', b_{\max}\}} p_B(b) \mathbb{E}[\gamma_\mu(e - e' + b; e, \boldsymbol{G}, \boldsymbol{H})], \quad (47)$$

whereas, if $e' = e_{\max}$

$$\mathbb{P}(E^{(k+1)} = e_{\max} | E^{(k)} = e) = \sum_{b=\max\{0, e_{\max}-e\}}^{b_{\max}} p_B(b) \sum_{d=0}^{e-e_{\max}+b} \mathbb{E}[\gamma_\mu(d; e, \boldsymbol{G}, \boldsymbol{H})]. \quad (48)$$

Note that we used the *transmit power policy* $\gamma_\mu(\cdot)$ and not the *power allocation policy* $\mu(\cdot)$. Indeed, the battery evolution does not depend upon the particular power splitting scheme but only on the total energy consumed. Thus, $\mathbb{P}(E^{(k+1)} = e' | E^{(0)})$ depends upon the policy only through the expectations $\mathbb{E}[\gamma_\mu(\rho^{\mathrm{tot}}; E^{(k)}, \boldsymbol{G}, \boldsymbol{H})]$. ∎

Define now the long-term probabilities of being in the energy level e given the initial level $E^{(0)}$ as $\pi(e|E^{(0)}) = \liminf_{K\to\infty} \frac{1}{K+1} \sum_{k=0}^{K} \mathbb{P}(E^{(k)} = e | E^{(0)})$. Thanks to the above proposition, we know that $\pi(e|E^{(0)})$ depends upon the policy only through $\mathbb{E}[\gamma_\mu(\rho^{\mathrm{tot}}; e, \boldsymbol{G}, \boldsymbol{H})]$, $\forall \rho^{\mathrm{tot}} \in \{0, \dots, e\}$, $\forall e \in \mathcal{E}$.

Fix a value $\alpha(\rho^{\mathrm{tot}}; e)$ for every pair ρ^{tot} and e, and consider the set of policies Ξ that induce $\mathbb{E}[\gamma_\mu(\rho^{\mathrm{tot}}; e, \boldsymbol{G}, \boldsymbol{H})] = \alpha(\rho^{\mathrm{tot}}; e)$ for every pair. For every policy in Ξ, the long-term probabilities are the same. The long-term average secrecy rate given an initial state $E^{(0)}$ can be expressed as in Equation (16)

$$C_\mu(E^{(0)}) = \sum_{e\in\mathcal{E}} \pi(e|E^{(0)}) \times \mathbb{E}\left[\sum_{\boldsymbol{\rho} \in \mathscr{P}_{\leq}(e)} \mu(\boldsymbol{\rho}; e, \boldsymbol{G}, \boldsymbol{H}) c(\boldsymbol{\rho}, \boldsymbol{G}, \boldsymbol{H}) \right]. \quad (49)$$

For every policy in Ξ, the terms $\pi(e|E^{(0)})$ of the previous expression are the same. Therefore, in order to maximize $C_\mu(E^{(0)})$, we focus on the terms $\mathbb{E}[\cdot]$ for each value of e. In particular, the problem can be decomposed in $e_{\max}+1$ simpler optimization problems (according to (13), define $\mu(e) \triangleq \{\mu(\cdot; e, \boldsymbol{g}, \hbar),\ \forall \boldsymbol{g} \in \mathcal{G},\ \hbar \in \mathcal{H}\}$)

$$\max_{\mu(e)} \ \mathbb{E}\Bigg[\sum_{\boldsymbol{\rho} \in \mathscr{P}_{\leq}(e)} \mu(\boldsymbol{\rho}; e, \boldsymbol{G}, \boldsymbol{H}) c(\boldsymbol{\rho}, \boldsymbol{G}, \boldsymbol{H}) \Bigg], \tag{50a}$$

s.t.:

$$\text{Constraints in (15);} \tag{50b}$$

$$\mathbb{E}[\gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{G}, \boldsymbol{H})] = \alpha(\rho^{\text{tot}}; e),\ \forall \rho^{\text{tot}} \in \{0, \dots, e\}. \tag{50c}$$

We rewrite the first expression as follows

$$\max_{\mu(e)} \ \mathbb{E}\Bigg[\sum_{\rho^{\text{tot}} \in \{0,\dots,e\}} \gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{G}, \boldsymbol{H}) \times \sum_{\boldsymbol{\rho} \in \mathscr{P}_{=}(\rho^{\text{tot}})} \phi_\mu(\boldsymbol{\rho}; \rho^{\text{tot}}, e, \boldsymbol{g}, \hbar) c(\boldsymbol{\rho}, \boldsymbol{G}, \boldsymbol{H}) \Bigg]. \tag{51}$$

where $\mathscr{P}_{=}(\rho^{\text{tot}}) \triangleq \{\boldsymbol{\rho} : \boldsymbol{\rho} \succeq 0,\ \rho^{\text{tot}} = \sum_{r=1}^{N} \rho_r\}$. As derived in [29, Eq. 7] with a Lagrangian approach, $\phi_\mu(\boldsymbol{\rho}; \rho^{\text{tot}}, e, \boldsymbol{g}, \hbar) = \delta_{\boldsymbol{\rho}, \boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{g}, \hbar}}$ ($\phi_\mu(\cdot)$ is deterministic and there is no dependence upon e when ρ^{tot} is fixed). $\boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{g}, \hbar}$ is the optimal transmit power splitting given the total transmission power ρ^{tot} and the channel gains (we use $\boldsymbol{\tau}$ instead of $\boldsymbol{\rho}$ for notation clarity). Therefore, we can rewrite (51) as

$$\max_{\gamma_\mu(e)} \ \mathbb{E}\Bigg[\sum_{\rho^{\text{tot}} \in \{0,\dots,e\}} \gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{G}, \boldsymbol{H}) c(\boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{G}, \boldsymbol{H}}, \boldsymbol{G}, \boldsymbol{H}) \Bigg]. \tag{52}$$

For every fixed e, we want to define $\gamma_\mu(e) \triangleq \{\gamma_\mu(\cdot; e, \boldsymbol{g}, \hbar),\ \forall \boldsymbol{g} \in \mathcal{G},\ \hbar \in \mathcal{H}\}$. Note that the problem is concave, thus a Lagrangian approach can be used. The Lagrangian function is

$$\mathcal{L}(e) = \mathbb{E}\Bigg[\sum_{\rho^{\text{tot}} \in \{0,\dots,e\}} \gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{G}, \boldsymbol{H}) \times \Big(c(\boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{G}, \boldsymbol{H}}, \boldsymbol{G}, \boldsymbol{H}) - \lambda(\rho^{\text{tot}}; e) \Big) \Bigg], \tag{53}$$

where $\lambda(\rho^{\text{tot}}; e)$ is the Lagrange multiplier associated with constraint $\mathbb{E}[\gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{G}, \boldsymbol{H})] = \alpha(\rho^{\text{tot}}; e)$.

We now show that an optimal policy is $\gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{g}, \hbar) = 1$ if $\rho^{\text{tot}} = {\rho^{\text{tot}}_{e, \boldsymbol{g}, \hbar}}^\star$ and zero otherwise, with

$${\rho^{\text{tot}}_{e, \boldsymbol{g}, \hbar}}^\star = \arg\max_{\rho^{\text{tot}} \in \{0,\dots,e\}} \Big\{ c(\boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{g}, \hbar}, \boldsymbol{g}, \hbar) - \lambda(\rho^{\text{tot}}; e) \Big\}. \tag{54}$$

In order to maximize (53), we can focus on each argument of the expectation

$$\max_{\substack{\gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{g}, \hbar), \\ \forall \rho^{\text{tot}} \in \{0,\dots,e\}}} \ \sum_{\rho^{\text{tot}} \in \{0,\dots,e\}} \gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{g}, \hbar) \times \underbrace{\Big(c(\boldsymbol{\tau}^\star_{\rho^{\text{tot}}, \boldsymbol{g}, \hbar}, \boldsymbol{g}, \hbar) - \lambda(\rho^{\text{tot}}; e) \Big)}_{u(\rho^{\text{tot}}, e, \boldsymbol{g}, \hbar)}. \tag{55}$$

We recall that $\sum_{\rho^{\text{tot}} \in \{0,\dots,e\}} \gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{g}, \hbar) = 1$. (55) is a weighted sum that is maximized when $\gamma_\mu(\rho^{\text{tot}}; e, \boldsymbol{g}, \hbar) = 1$ if $\rho^{\text{tot}} = {\rho^{\text{tot}}_{e, \boldsymbol{g}, \hbar}}^\star$ and zero otherwise. Indeed, suppose by contradiction that there exist ρ^{tot}_1 and ρ^{tot}_2 (the argument can be generalized to more than two) such that $\gamma_\mu(\rho^{\text{tot}}_1; e, \boldsymbol{g}, \hbar) > 0$, $\gamma_\mu(\rho^{\text{tot}}_2; e, \boldsymbol{g}, \hbar) > 0$ and $\gamma_\mu(\rho^{\text{tot}}_1; e, \boldsymbol{g}, \hbar) + \gamma_\mu(\rho^{\text{tot}}_2; e, \boldsymbol{g}, \hbar) = 1$. The max argument in (55) would be $\gamma_\mu(\rho^{\text{tot}}_1; e, \boldsymbol{g}, \hbar) u(\rho^{\text{tot}}_1, e, \boldsymbol{g}, \hbar) + (1 - \gamma_\mu(\rho^{\text{tot}}_1; e, \boldsymbol{g}, \hbar)) u(\rho^{\text{tot}}_2, e, \boldsymbol{g}, \hbar)$, which is smaller than or equal to $u({\rho^{\text{tot}}_{e, \boldsymbol{g}, \hbar}}^\star, e, \boldsymbol{g}, \hbar)$.

Appendix B
Proof of Proposition 1

The MC has three dimensions: the battery, the legitimate channel and the eavesdropper's channel. Since the fading is not controlled by the EHD, the MC is always free to move along the last two dimensions (we assume that the channel evolution is i.i.d. over time). Thus, the only potential problem is related to the battery dimension, i.e., if the policy is not unichain, the device energy level may be stuck in different subsets of $\mathcal{E}$.

Also, we recall that we consider only discrete channel conditions with non-zero probability (Remark 1). We now discuss Point 1). We want to show that the recurrent class is composed by the states with high energy levels, i.e., for every $e < e_{\max}$, there exists a positive probability of increasing the energy level. This is true by hypothesis because the maximum transmit power in state e is lower than the maximum number of energy arrivals $b_{\max}$ ($\rho^{\text{tot}}_{e, \boldsymbol{g}', \hbar'} < b_{\max}$). Therefore, since it is possible to reach the energy level $e_{\max}$ (fully charged battery) within a certain number of steps from every state, the policy is unichain. To prove Point 2), a symmetric reasoning can be followed.

If both conditions hold, it is possible to reach every $e \in \mathcal{E}$ from any element of $\mathcal{E}$, thus the policy induces an irreducible MC. Since the number of states is finite, the MC is positive recurrent.

Appendix C
Deriving a Unichain Policy

As in Appendix B, it is always possible to move along the channel dimensions. Therefore, we focus on the battery dimension, which represents the only limitation for obtaining a unichain policy.

Consider a policy μ_A that has two recurrent classes, namely Π'_A and Π''_A (this approach can be generalized to more than two classes) and assume, without loss of generality, that if $E^{(0)} \in \Pi''_A$ the greatest long-term reward is reached. We now propose a technique to derive a new policy that, regardless of the initial state, achieves the same maximum reward of μ_A.

Consider a second policy, namely μ_B, obtained from μ_A as follows. For every $e_A = 0, \dots, \max\{\Pi''_A\}$, set $\boldsymbol{\rho}^{\mu_B}_{e_B, \boldsymbol{g}, \hbar} = \boldsymbol{\rho}^{\mu_A}_{e_A, \boldsymbol{g}, \hbar}$, with $e_B = e_A + e_{\max} - \max_e\{\Pi''_A\}$, i.e., we shift the recurrent class Π''_A toward higher energy levels (we name Π''_B the new recurrent class). For $e_B \in \{0, \dots, e_{\max} - \max\{\Pi''_A\} - 1\}$, set $\boldsymbol{\rho}^{\mu_B}_{e_B, \boldsymbol{g}, \hbar} = 0$. In this way, the device cannot be stuck in energy levels lower than $e_{\max} - |\Pi''_B| + 1$ (the harvested

energy increases the battery level) and, after a certain number of transitions, it reaches the recurrent class Π''_B. Finally, since the power splitting vectors in the recurrent classes Π''_A and Π''_B coincide, μ_B achieves the same maximum reward of μ_A, regardless of the initial $E^{(0)}$.

This proves that it is always possible to obtain a unichain policy with the same maximum long-term secrecy rate as the initial one and shows how to derive it.

Appendix D
Proof of Theorem 2

Problem (12) can be rewritten using (21) in the following form:

$$\max_{\mu} C_\mu = \max_{\mu^{\mathrm{tot}}} \max_{\mu \in \mathcal{X}(\mu^{\mathrm{tot}})} C_\mu \tag{56}$$

$$\mathcal{X}(\mu^{\mathrm{tot}}) \triangleq \{\mu \ : \ \mu^{\mathrm{tot}} \text{ and } \mu \text{ are consistent}\}, \tag{57}$$

i.e., we fix the transmission powers (outer $\max$) and focus on all the policies which are consistent with such choice (inner $\max$). This is equivalent to searching through all the possible feasible policies (as in (12)).

Consider the expression of C_μ in Equation (22) and note that $\pi_{\mu^{\mathrm{tot}}}(e)$ does not depend upon the particular power splitting scheme, but only upon μ^{tot}. Thus, the inner $\max$ can be moved inside the integral

$$\max_{\mu^{\mathrm{tot}}} \Bigg(\sum_{e=0}^{e_{\max}} \pi_{\mu^{\mathrm{tot}}}(e) \times \int_{\mathcal{G}\times\mathcal{H}} \max_{\mu \in \mathcal{X}(\mu^{\mathrm{tot}})} \Big(c(\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}}, \boldsymbol{g}, \boldsymbol{\hbar}) \Big) \, \mathrm{d}F(\boldsymbol{g}, \boldsymbol{\hbar}) \Bigg). \tag{58}$$

Note that inside the integral e, $\boldsymbol{g}$ and $\boldsymbol{\hbar}$ are fixed. Therefore, the only degree of freedom in the inner $\max$ operation is given by the power splitting choice $\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}}$.

Since μ^{tot} and μ are consistent, in the inner $\max$ we have $\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}} \in \mathscr{P}_{=}(\rho^{\mathrm{tot}}_{e,\boldsymbol{g},\boldsymbol{\hbar}})$ (specified in (23)). Therefore,

$$\max_{\mu \in \mathcal{X}(\mu^{\mathrm{tot}})} \Big(c(\boldsymbol{\rho}_{e,\boldsymbol{g},\boldsymbol{\hbar}}, \boldsymbol{g}, \boldsymbol{\hbar}) \Big) \equiv \text{Problem (23) with } x = \rho^{\mathrm{tot}}_{e,\boldsymbol{g},\boldsymbol{\hbar}} \tag{59}$$

Thus, Points 1) and 2) of the theorem solve the internal and external $\max$ operations, respectively.

Appendix E
Proof of Proposition 3

The proof exploits the results of Appendix A, and in particular Equation (54). Also, we focus on the energy levels in the unique recurrent class (for the transient states the proposition is trivial to prove since $\rho^{\mathrm{tot}\star}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$ is always zero).

Assume that $\rho^{\mathrm{tot}'} \triangleq \rho^{\mathrm{tot}\star}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'}$ is the optimal transmission power given the state of the system $(e, \boldsymbol{g}', \boldsymbol{\hbar}')$, i.e., $\rho^{\mathrm{tot}\star}_{e,\boldsymbol{g}',\boldsymbol{\hbar}'} = \arg\max_{\rho^{\mathrm{tot}} \in \{0,\ldots,e\}} \{c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}}; e)\}$ (we remark that $\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}},\boldsymbol{g}',\boldsymbol{\hbar}'}$ is the *optimal* power splitting vector given ρ^{tot} and the channel gains). Similarly, $\rho^{\mathrm{tot}''} \triangleq \rho^{\mathrm{tot}\star}_{e,\boldsymbol{g}'',\boldsymbol{\hbar}''}$ is the optimal power for state $(e, \boldsymbol{g}'', \boldsymbol{\hbar}'')$.

We first show by contradiction that if $D(\rho^{\mathrm{tot}}; \boldsymbol{g}', \boldsymbol{\hbar}'; \boldsymbol{g}'', \boldsymbol{\hbar}'') \geq 0, \forall \rho^{\mathrm{tot}}$, then $\rho^{\mathrm{tot}''} \geq \rho^{\mathrm{tot}'}$. Assume $\rho^{\mathrm{tot}'} > \rho^{\mathrm{tot}''}$. We now derive some properties of $\rho^{\mathrm{tot}'}$ and $\rho^{\mathrm{tot}''}$ and combine these with the hypothesis to obtain the contradiction. From the definitions of $\rho^{\mathrm{tot}'}$ and $\rho^{\mathrm{tot}''}$, we have

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}'}; e) \\ &\qquad \geq c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}''}; e), \end{aligned} \tag{60}$$

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - \lambda(\rho^{\mathrm{tot}''}; e) \\ &\qquad \geq c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - \lambda(\rho^{\mathrm{tot}'}; e). \end{aligned} \tag{61}$$

By hypothesis, we have, for every ρ^{tot},

$$\frac{\partial}{\partial \rho^{\mathrm{tot}}} \Big(c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \Big) \geq 0. \tag{62}$$

Assume that the inequality is strict. This implies, for every $\rho_A < \rho_B$

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho_A,\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho_A,\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \\ &< c(\boldsymbol{\tau}^{\star}_{\rho_B,\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho_B,\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}'). \end{aligned} \tag{63}$$

In particular, since $\rho^{\mathrm{tot}'} > \rho^{\mathrm{tot}''}$, choose $\rho_A = \rho^{\mathrm{tot}''}$ and $\rho_B = \rho^{\mathrm{tot}'}$ and obtain

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \\ &< c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}'). \end{aligned} \tag{64}$$

Finally, by combining (61) with (64), we obtain

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - \lambda(\rho^{\mathrm{tot}'}; e) + \lambda(\rho^{\mathrm{tot}''}; e) \\ &\leq c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') \\ &< c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \\ &\quad + c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}'), \end{aligned} \tag{65}$$

which is equivalent to

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}'}; e) \\ &< c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}''}; e), \end{aligned} \tag{66}$$

and violates Equation (60), leading to a contradiction.

Assume now that (62) holds with equality. Following the previous reasoning, we obtain

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \\ &= c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}'',\boldsymbol{\hbar}''}, \boldsymbol{g}'', \boldsymbol{\hbar}'') - c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') \end{aligned} \tag{67}$$

and, instead of (66),

$$\begin{aligned} &c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}'},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}'}; e) \\ &\leq c(\boldsymbol{\tau}^{\star}_{\rho^{\mathrm{tot}''},\boldsymbol{g}',\boldsymbol{\hbar}'}, \boldsymbol{g}', \boldsymbol{\hbar}') - \lambda(\rho^{\mathrm{tot}''}; e), \end{aligned} \tag{68}$$

(68) must be satisfied with equality, otherwise it would violate (60). This means that, for the same state $(e, \boldsymbol{g}', \boldsymbol{\hbar}')$, there exist two distinct values of ρ^{tot} (i.e., $\rho^{\mathrm{tot}'}$ and $\rho^{\mathrm{tot}''}$) that maximize (54). This is not possible because in the recurrent states the optimal solution is unique [42, Vol. II, Sec. 4].

The first point of Proposition 3 is thus proved. The proof of the second point is symmetric.

APPENDIX F
PROOF OF THEOREM 3

We want to prove that, for OSP and $N = 1$, $\rho^{\mathrm{tot}\star}_{e,g,\hbar}$ does not decrease with g and does not increase with $\hbar$.

$D(\rho^{\mathrm{tot}}; g', \hbar'; g'', \hbar'')$ can be written as

$$D(\rho^{\mathrm{tot}}; g', \hbar; g'', \hbar) \tag{69}$$
$$= \frac{\partial}{\partial \rho^{\mathrm{tot}}} \left(\left[\log_2 \left(\frac{1 + g'' \rho^{\mathrm{tot}}}{1 + \hbar \rho^{\mathrm{tot}}} \right) \right]^+ - \left[\log_2 \left(\frac{1 + g' \rho^{\mathrm{tot}}}{1 + \hbar \rho^{\mathrm{tot}}} \right) \right]^+ \right).$$

Assume $g'' \geq g'$. If $g'' \leq \hbar$, then both terms are zero because $g' \leq g'' \leq \hbar$. If $g' \leq \hbar < g''$, then only the right term is zero. In this case, $D(\rho^{\mathrm{tot}}; g', \hbar; g'', \hbar) \propto g'' - \hbar > 0$. If $\hbar < g' \leq g''$, then $D(\rho^{\mathrm{tot}}; g', \hbar; g'', \hbar) \propto g'' - g' \geq 0$.

The proof of the second part is similar.

REFERENCES

[1] A. Biason, A. R. Khamesi, N. Laurenti, and M. Zorzi, "Achievable secrecy rates of an energy harvesting device with a finite battery," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015.

[2] J. López and J. Zhou, *Wireless sensor network security*. Ios Press, Apr. 2008, vol. 1.

[3] A. Pandey and R. Tripathi, "A survey on wireless sensor networks security," *Int. J. Computer Applications*, vol. 3, no. 2, pp. 43–49, June 2010.

[4] N. Bruce, Y. Kang, H. R. Kim, S. Park, and H.-J. Lee, "A security protocol based on mutual authentication application toward wireless sensor network," in *Information Science and Applications*. Springer, Feb. 2015, pp. 27–34.

[5] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, Nov. 2011.

[6] C. Shannon, "Communication theory of secrecy systems," *Bell System Tech. Journ.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[7] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks," *Int. J. Distributed Sensor Networks*, 2013.

[8] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[9] D. Gunduz, K. Stamatiou, N. Michelusi, and M. Zorzi, "Designing intelligent energy harvesting communication systems," *IEEE Commun. Magazine*, vol. 52, no. 1, pp. 210–216, Jan. 2014.

[10] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, "Energy harvesting wireless communications: A review of recent advances," *IEEE J. Selected Areas in Commun.*, vol. 33, no. 3, pp. 360–381, Mar. 2015.

[11] G. Zhou, L. Huang, W. Li, and Z. Zhu, "Harvesting ambient environmental energy for wireless sensor networks: A survey," *J. Sensors*, June 2014.

[12] J. Lei, R. Yates, and L. Greenstein, "A generic model for optimizing single-hop transmission policy of replenishable sensors," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 547–551, Feb. 2009.

[13] V. Sharma, U. Mukherji, V. Joseph, and S. Gupta, "Optimal energy management policies for energy harvesting sensor nodes," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1326–1336, Apr. 2010.

[14] V. Sharma and R. Rajesh, "Queuing theoretic and information theoretic capacity of energy harvesting sensor nodes," in *Proc. 45th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR)*, Nov. 2011, pp. 383–388.

[15] O. Ozel and S. Ulukus, "Achieving AWGN capacity under stochastic energy harvesting," *IEEE Trans. Inf. Theory*, vol. 58, no. 10, pp. 6471–6483, Oct. 2012.

[16] ——, "AWGN channel under time-varying amplitude constraints with causal information at the transmitter," in *Proc. 45th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR)*, Nov. 2011, pp. 373–377.

[17] K. Tutuncuoglu and A. Yener, "Optimum transmission policies for battery limited energy harvesting nodes," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1180–1189, Mar. 2012.

[18] N. Michelusi, K. Stamatiou, and M. Zorzi, "Transmission policies for energy harvesting sensors with time-correlated energy supply," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2988–3001, July 2013.

[19] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, June 2004.

[20] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. of Medical Systems*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[21] V. Agrawal, "Security and privacy issues in wireless sensor networks for healthcare," in *Internet of Things. User-Centric IoT*. Springer, June 2015, pp. 223–228.

[22] M. Winkler, K.-D. Tuchs, K. Hughes, and G. Barclay, "Theoretical and practical aspects of military wireless sensor networks," *J. Telecommunications and Information Technology*, no. 2, pp. 37–45, 2008.

[23] M. P. Đurišić, Z. Tafa, G. Dimić, and V. Milutinović, "A survey of military applications of wireless sensor networks," in *Proc. IEEE Mediterranean Conf. on Embedded Computing (MECO)*, June 2012, pp. 196–199.

[24] S. M. Zin, N. B. Anuar, M. L. M. Kiah, and A.-S. K. Pathan, "Routing protocol design for secure WSN: review and open research issues," *J. Network and Computer Applications*, vol. 41, pp. 517–530, May 2014.

[25] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[26] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[28] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symposium on Information Theory (ISIT)*, June 2007, pp. 1301–1305.

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

[30] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[31] A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[32] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *Proc. IEEE Information Theory Workshop (ITW)*, Sept. 2012, pp. 139–143.

[33] ——, "Gaussian wiretap channel with a batteryless energy harvesting transmitter," in *Proc. IEEE Information Theory Workshop (ITW)*, Sept. 2012, pp. 89–93.

[34] A. Mukherjee and J. Huang, "Deploying multi-antenna energy-harvesting cooperative jammers in the MIMO wiretap channel," in *Proc. 46th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR)*, Nov. 2012, pp. 1886–1890.

[35] M. Zhang, Y. Liu, and S. Feng, "Energy harvesting for secure OFDMA systems," in *Proc. IEEE 6th Int. Conf. on Wireless Communications and Signal Processing (WCSP)*, Sept. 2014.

[36] Q. Li, W.-K. Ma, and A. M.-C. So, "Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 1596–1600.

[37] A. Biason and M. Zorzi, "Joint transmission and energy transfer policies for energy harvesting devices with finite batteries," *IEEE J. Selected Areas in Commun.*, vol. 33, no. 12, pp. 2626–2640, Dec. 2015.

[38] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forens. and Sec.*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[39] M. Gorlatova, A. Wallwater, and G. Zussman, "Networking low-power energy harvesting devices: Measurements and algorithms," *IEEE Trans. Mobile Computing*, vol. 12, no. 9, pp. 1853–1865, Sept. 2013.

[40] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[41] D. A. Levin, Y. Peres, and E. L. Wilmer, *Markov chains and mixing times*. American Mathematical Soc., 2009.

[42] D. Bertsekas, *Dynamic programming and optimal control*. Athena Scientific, Belmont, Massachusetts, 2005.

[43] M. L. Puterman, *Markov decision processes: Discrete stochastic dynamic programming*. John Wilson and Sons Ed., 1995, vol. 46, no. 6.

Alessandro Biason (S'15) received the B.Sc. degree (with honors) in Information Engineering and the M.S. degree (with honors and perfect GPA) in Telecommunication Engineering from the University of Padua, Italy, in 2012 and 2014, respectively. In 2015, he was on leave at the University of Southern California, Los Angeles, USA, as a visiting Ph.D. student. He is currently pursuing the Ph.D. degree with the SIGNET Research Group, University of Padua. His research interests lie in the areas of communication theory, wireless networks, energy harvesting systems, stochastic optimization and optimal control.

He has served as a reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

Nicola Laurenti received his Laurea Degree in Electrical Engineering in 1995 and his PhD in Electronic and Telecommunication Engineering in 1999 both from the University of Padua, Italy. Since 2001 he has been an Assistant Professor at the Department of Information Engineering of University of Padua. In 2008-09 he was a Visiting Scholar at the Coordinated Science Laboratory of the University of Illinois at Urbana-Champaign. In 1992-93 he was an exchange student at the University of California at Berkeley. His research interests mainly focus on wireless network security at lower layers (physical, data link and network), GNSS security, information theoretic security and quantum key distribution.

Michele Zorzi (S'89, M'95, SM'98, F'07) received his Laurea and PhD degrees in electrical engineering from the University of Padova in 1990 and 1994, respectively. During academic year 1992-1993 he was on leave at UCSD, working on multiple access in mobile radio networks. In 1993 he joined the faculty of the Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy. After spending three years with the Center for Wireless Communications at UCSD, in 1998 he joined the School of Engineering of the University of Ferrara, Italy, where he became a professor in 2000. Since November 2003 he has been on the faculty of the Information Engineering Department at the University of Padova. His present research interests include performance evaluation in mobile communications systems, random access in wireless networks, ad hoc and sensor networks, Internet-of-Things, energy constrained communications protocols, cognitive networks, and underwater communications and networking.

He was the Editor-In-Chief of IEEE Wireless Communications from 2003 to 2005 and the Editor-In-Chief of the IEEE Transactions on Communications from 2008 to 2011, and is currently the founding Editor-In-Chief of the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He has also been an Editor for several journals and a member of the Organizing or the Technical Program Committee for many international conferences, as well as guest editor for special issues in IEEE Personal Communications, IEEE Wireless Communications, IEEE Network and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He served as a Member-at-Large of the Board of Governors of the IEEE Communications Society from 2009 to 2011, and as its Director of Education and Training in 2014-15. He currently serves as a member of the 2016 IEEE PSPB/TAB Products and Services Committee.