Achievable Secrecy Rates of an Energy Harvesting Device with a Finite Battery

Achievable Secrecy Rates of an Energy Harvesting Device with a Finite Battery

Alessandro Biason, Atieh Rajabi Khamesi, Nicola Laurenti and Michele Zorzi
Department of Information Engineering, University of Padova - via Gradenigo 6b, 35131 Padova, Italy
{biasonal,khamesi,nil,zorzi}@dei.unipd.it

***Abstract*—In this paper, we investigate the achievable secrecy rates in an Energy Harvesting communication system composed of one transmitter and multiple receivers. In particular, because of the energy constraints and the channel conditions, it is important to understand when a device should transmit or not and how much power should be used. We introduce the *Optimal Secrecy Policy* in several scenarios. We show that, if the receivers demand high secrecy rates, then it is not always possible to satisfy all their requests. Thus, we introduce a scheme that chooses which receivers should be discarded. Also, we study how the system is influenced by the Channel State Information and, in particular, how the knowledge of the eavesdropper's channel changes the achievable rates.**

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 [1]. While most works in this area deal with security *protocols* [2], implementing security mechanisms at the physical layer represents an interesting complement to those networking approaches [3], and has the potential to provide stronger (information-theoretic) secrecy properties [4].

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 [5]–[8]. 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 [9], [10]. 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.

Perfect secrecy [4] is achieved when the mutual information between the information signal (s) and the signal received by the eavesdropper (z) is zero, *i.e.*, $I(s;z) = 0$. In this case, signal z is useless when trying to determine s. In [11], 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. It was shown in [12] that in a fading scenario it is also possible to obtain a non-zero secure rate even if the eavesdropper's channel is better than the legitimate one on average, by exploiting advantageous time intervals. In [13], the secrecy capacity of fading channels in the presence of multiple eavesdroppers is studied. Moreover, [14] presents a resource allocation algorithm for achieving secrecy in a Multiple-Input Single-Output (MISO) energy harvesting communication system based on energy transfer. Also [10] considered the energy transfer mechanism and studied how to efficiently allocate the power over several sub-carriers in an EH system. [15] studied the secrecy capacity of a Gaussian wiretap channel with an amplitude constraint. In [16] the secrecy capacity was analyzed in a batteryless energy harvesting communication system. In this paper, on the other hand, we focus on a system with a battery and characterize the problem with a dynamic programming approach.

The goal of the present work is to investigate the achievable secrecy rates when an Energy Harvesting transmitter with a finite battery is considered. In particular, because of the energy constraints, choosing when to transmit is fundamental to obtain higher rates, thus we derive the *Optimal Secrecy Policy* in several cases. First we consider a static channel and maximize the long-term average secrecy rate with and without minimum secrecy requirements. Then, in Section IV we extend the problem to the case in which the channel is affected by random fading and show how the achievable secrecy rate changes when only partial Channel State Information (CSI) is available.

The paper is structured as follows. Section II defines the system model and introduces the notion of secrecy rate. Section III studies the maximization of the secrecy rate in the case of complete CSI and static channel. This hypothesis is relaxed in Section IV where we consider partial CSI for a random fading channel. The numerical evaluation is presented in Section V. Section VI concludes the paper.

II. System Model and Secrecy Rate

We consider an *Energy Harvesting Device* (EHD) that simultaneously transmits data over N sub-carriers. In the next we suppose that every sub-carrier is associated to a

single *receiver*. (Equivalently, we can consider a transmitter that sends data to a single receiver in a large frequency band composed of N independent narrow bands, and similar results would be obtained [17].). Each receiver requires a secrecy rate greater than zero in order to guarantee secure transmission. For every receiver, there is one eavesdropper that attempts to intercept the transmitted data. We initially assume that the EHD knows the CSI of all the receivers and eavesdroppers instantaneously[1] and later relax this hypothesis (Section IV). 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 $E_k \in \mathcal{E} = \{0, 1, \dots, e_{\max}\}$ energy quanta stored. The harvesting is described through an energy quanta arrival process $\{B_k\}$, *e.g.*, deterministic, Bernoulli or truncated geometric (*e.g.*, see [18] for a characterization of the light energy). The average harvesting rate is $\bar{b}$, the maximum number of energy quanta harvested per slot is $b_{\max}$ and a quantum harvested in slot k can only be used in time slots $> k$. The system is described through a Markov Chain (MC) whose state e corresponds to having e energy quanta stored in the battery. We suppose that the device always has data to send and that the energy cost that the device sustains is mainly due to data transmission.

A. Secrecy Rates and Capacity

We introduce the concept of *Secrecy Rate* and *Secrecy Capacity* with only one sub-carrier [12], [16] (every sub-carrier can be analyzed independently and the overall definition of secrecy rate with N sub-carriers can be derived as in Equation (3)). The transmitter sends a message s to the legitimate receiver. An (M, l) code consists of three elements: 1) a message set $\mathcal{S} = \{1, \dots, M\}$, 2) a probabilistic encoder f_l^{enc} at the transmitter that maps a random message $s \in \mathcal{S}$ (realization of the r.v. S) into a codeword of length l, and 3) a decoder at the legitimate receiver that extracts $\hat{s}$ (realization of the r.v. $\hat{S}$) from the received message in $\mathcal{Y}_l$, *i.e.*, $f_l^{\text{dec}} : \mathcal{Y}_l \to \mathcal{S}$. The average error probability of an (M, l) code is given by

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

The equivocation rate at the eavesdropper is $R_e^l = (1/l)H(S|Z_l)$, *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 of the transmitted signal at the eavesdropper. Information theoretic secrecy (unconditional security) is obtained if $R_e^l = R$, where R is the message rate. The *secrecy rate* R_s is said to be achievable if there exists a set of $(2^{lR_s}, l)$ codes, $l = 1, 2, \dots$, such that

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

and the secrecy capacity is defined as the supremum of the set of achievable secrecy rates. In the next we discuss how the secrecy rate changes in several scenarios.

[1]This is reasonable if also the eavesdroppers are potential receivers of the transmitter, thus they are legitimate nodes [10].

III. Static Channel Analysis

The channel gains in slot k are $\boldsymbol{g}_k = [g_{1,k}, \dots, g_{N,k}]$ and $\boldsymbol{h}_k = [h_{1,k}, \dots, h_{N,k}]$ for the N receivers and their corresponding eavesdroppers, respectively. $\boldsymbol{g}_k$ and $\boldsymbol{h}_k$ can be interpreted as realizations of two joint random vectors $\boldsymbol{G} = [G_1, \dots, G_N]$ and $\boldsymbol{H} = [H_1, \dots, H_N]$ (assumed i.i.d. over time).

In this section we assume that $\boldsymbol{g}_k = \boldsymbol{g}$, $\boldsymbol{h}_k = \boldsymbol{h}$ are constant over time, *i.e.*, $\boldsymbol{G}$ and $\boldsymbol{H}$ are deterministic (in Section IV we will relax this hypothesis), and $\boldsymbol{g} \succ \boldsymbol{h}$ (element-to-element condition). Indeed, if $\exists i : g_i \leq h_i$, then the secrecy rate over sub-carrier i is zero and i cannot be used for secure transmission. In this case the problem can be reformulated by neglecting sub-carrier i.

A. Secrecy Capacity Expression

Under the assumption that the total transmission power ω is used and N sub-carriers are considered, the corresponding secrecy capacity is given by (we consider AWGN channels)

$$c(\boldsymbol{\sigma}) = \sum_{m=1}^{N} c_m(\sigma_m), \tag{3}$$

$$c_m(\sigma_m) = \begin{cases} 0, & \text{if } h_m \geq g_m, \\ R_{g_m, h_m}(\sigma_m), & \text{otherwise,} \end{cases} \tag{4}$$

$$R_{g_m, h_m}(\sigma_m) \triangleq \log_2 \left(\frac{1 + g_m \sigma_m}{1 + h_m \sigma_m} \right), \tag{5}$$

$$\omega \triangleq \sum_{m=1}^{N} \sigma_m, \tag{6}$$

i.e., $c(\boldsymbol{\sigma})$ is the sum of the secrecy capacities over the several sub-carriers. The value of $c(\boldsymbol{\sigma})$ changes according to the choice of the power allocation over the several sub-carriers $\boldsymbol{\sigma} \triangleq [\sigma_1, \dots, \sigma_N]$. Note that, in general, $c(\boldsymbol{\sigma}) = c(\boldsymbol{\sigma}(\boldsymbol{g}, \boldsymbol{h}), \boldsymbol{g}, \boldsymbol{h})$, *i.e.*, *both* the power allocation and the secrecy capacity depend upon the channel state vectors $\boldsymbol{g}$ and $\boldsymbol{h}$. Since in this section $\boldsymbol{g}$ and $\boldsymbol{h}$ are constant, we omit these dependencies for notational simplicity.

A policy μ specifies the power allocation $\boldsymbol{\sigma}$ that is used in slot k. In the long run, the *average secrecy rate* under a policy μ is given by the average undiscounted reward C_μ

$$C_\mu \triangleq \liminf_{K \to \infty} \frac{1}{K} \sum_{k=0}^{K-1} \mathbb{E}_{B_k}[c(\boldsymbol{\sigma}_k)], \tag{7}$$

where $\mathbb{E}_{B_k}[\cdot]$ is the expectation taken with respect to $\{B_k\}$.

Without loss of generality (see [17]), in the next we consider only unichain policies, *i.e.*, those that induce an irreducible MC. In this case, C_μ does not depend upon the initial state. The policy μ is described through the $(e_{\max} + 1) \times N$ *secrecy policy matrix*

$$\boldsymbol{\Omega} = \begin{pmatrix} \sigma_1(0) & \dots & \sigma_N(0) \\ \vdots & & \vdots \\ \sigma_1(e_{\max}) & \dots & \sigma_N(e_{\max}) \end{pmatrix}, \tag{8}$$

that, for every energy state $e \in \mathcal{E}$, represents the amount of energy that should be spent in every sub-carrier (in the next

we will use μ and $\mathbf{\Omega}$ interchangeably). We also define the row-sum of $\mathbf{\Omega}$ as

$$\omega(e) \triangleq \sum_{m=1}^{N} \sigma_m(e) \tag{9}$$

and the corresponding column vector of row sums is $\boldsymbol{\omega} = [\omega(0), \ldots, \omega(e_{\max})]^T$. $\omega(e)$ represents the amount of energy quanta that are drawn from the battery in state e, thus it is an integer value in $\{0, \ldots, e\}$. Instead, $\sigma_m(e)$ represents the amount of energy that is sent over sub-carrier m in state e and is not restricted to be an integer (*e.g.*, in state $e = 5$ with $N = 2$, we may extract $\omega(5) = 3$ energy quanta and assign $\sigma_1(5) = \sigma_2(5) = 1.5$).

It can be shown that (7) can be rewritten as:

$$C_{\mathbf{\Omega}} = \sum_{e \in \mathcal{E}} \pi_{\boldsymbol{\omega}}(e) c(\boldsymbol{\sigma}(e)), \tag{10}$$

where $\pi_{\boldsymbol{\omega}}(e)$ is the steady-state probability of being in state e and $\boldsymbol{\sigma}(e)$ is the power allocation choice in state e, given a policy matrix $\mathbf{\Omega}$. Note that, since the steady-state probabilities are found using the battery transition probabilities (that are influenced by $\boldsymbol{\omega}$ only), $\pi_{\boldsymbol{\omega}}(e)$ depends only upon the column vector $\boldsymbol{\omega}$.

B. Maximization of the Secrecy Rate

We study the following problem

$$\mathcal{P} \ : \mathbf{\Omega}^\star = \arg\max_{\mathbf{\Omega}} C_{\mathbf{\Omega}}. \tag{11}$$

The policy $\mu^\star$ that maximizes $C_{\mathbf{\Omega}}$ is named *Optimal Secrecy Policy* (OSP). In particular, in the previous section we implicitly restricted our study to deterministic policies because it can be proved that OSP is deterministic [17]. Note that, since we are considering two dimensions (battery size and sub-carriers), in this case the maximization of $C_{\mathbf{\Omega}}$ can be simplified in two steps.

Theorem 1. *The maximization of $C_{\mathbf{\Omega}}$ can be decomposed into two steps:*

1) *for every choice of ω, find the* optimal power splitting choice

$$\boldsymbol{\sigma}^\star = \arg\max_{\boldsymbol{\sigma}} \sum_{m=1}^{N} c_m(\sigma_m), \tag{12}$$

$$\textit{s.t.} \qquad \omega = \sum_{m=1}^{N} \sigma_m; \tag{13}$$

2) *maximize $C_{\mathbf{\Omega}}$ by considering only the vector $\boldsymbol{\omega}$*

$$\boldsymbol{\omega}^\star = \arg\max_{\boldsymbol{\omega} \ : \ \omega(e) = \sum_{m=1}^{N} \sigma_m^\star(e)} \sum_{e \in \mathcal{E}} \pi_{\boldsymbol{\omega}}(e) c(\boldsymbol{\sigma}^\star(e)). \tag{14}$$

The optimal secrecy policy matrix $\mathbf{\Omega}^\star$ can be found by fixing the sum of every row according to point 2) and choosing $\sigma_m(e)$ with the optimal power splitting choice of point 1).

Proof. Problem $\mathcal{P}$ can be rewritten in the following form:

$$\max_{\boldsymbol{\omega}} \left(\max_{\mathbf{\Omega} \ : \ \mathbf{\Omega}\mathbf{1} = \boldsymbol{\omega}} \left(\sum_{e \in \mathcal{E}} \pi_{\boldsymbol{\omega}}(e) c(\boldsymbol{\sigma}(e)) \right) \right), \tag{15}$$

i.e., we fix the row sums of $\mathbf{\Omega}$ (outer $\max$) and we focus on all the $\mathbf{\Omega}$ with column vector $\boldsymbol{\omega}$ (inner $\max$). This is equivalent to searching through all the possible entries of $\mathbf{\Omega}$ (as in (11)).

Let us start from the inner $\max$ operation. The structure of its argument can be divided into two parts: 1) the steady-state probabilities $\pi_{\boldsymbol{\omega}}(e)$ and 2) the secrecy capacities $c(\boldsymbol{\sigma}(e))$. Since $\boldsymbol{\omega}$ is fixed, so is $\pi_{\boldsymbol{\omega}}(e)$. Moreover, $c(\boldsymbol{\sigma}(e))$ depends only upon row e of matrix $\mathbf{\Omega}$. Therefore, (15) can be expressed as

$$\max_{\boldsymbol{\omega}} \left(\sum_{e \in \mathcal{E}} \pi_{\boldsymbol{\omega}}(e) \max_{\omega(e) = \sum_{m=1}^{N} \sigma_m(e)} \Big(c(\boldsymbol{\sigma}(e)) \Big) \right). \tag{16}$$

Points 1) and 2) of the theorem solve the inner and outer $\max$ operations in (16), respectively. ∎

For a fixed ω, the *optimal power splitting choice* $\boldsymbol{\sigma}^\star$ that solves (12)-(13) was found in [12]:

$$\sigma_m^\star = \left[\sqrt{\frac{\alpha_m^2}{4} + \frac{\alpha_m}{\eta}} - \frac{\beta_m}{2} \right]^+, \tag{17}$$

$$\alpha_m \triangleq \frac{1}{h_m} - \frac{1}{g_m}, \qquad \beta_m \triangleq \frac{1}{h_m} + \frac{1}{g_m}, \tag{18}$$

where η is a parameter used to satisfy $\omega = \sum_{m=1}^{N} \sigma_m^\star$ (note the dependence upon the channel coefficients). In the remainder of the paper we assume that this optimal power splitting choice is used, unless otherwise stated.

To solve point 2) instead, the Optimal Secrecy Policy can be found numerically via dynamic programming techniques, *e.g.*, the Policy Iteration Algorithm (PIA) [19]. Note that both points 1) and 2) can be easily solved, therefore the decomposition strategy of Theorem 1 greatly simplifies the numerical evaluation.

Analytically, the problem can be solved for a fixed $e_{\max}$. However, except for very small $e_{\max}$, the solutions are complicated and not easily readable, and do not provide further insight on the general structure of OSP.

C. Minimum Secrecy Rate Constraints

Problem $\mathcal{P}$ can be extended to consider also the following common requirements

$$c_m(\sigma_m(e)) \geq c_{m,\min}, \tag{19}$$

for $m = 1, \ldots, N$, *i.e.*, a minimum secrecy rate is required over every sub-carrier. If a constraint cannot be satisfied, then the device should not transmit over that sub-carrier.

We define the problem $\mathcal{P}'$ as the extension of $\mathcal{P}$ with constraints induced by (19). Using (5), the inequality can be rewritten in the power domain:

$$(19) \ \Leftrightarrow \ \sigma_m(e) \geq \frac{2^{c_{m,\min}} - 1}{g_m - h_m 2^{c_{m,\min}}} \triangleq \sigma_{m,\min}. \tag{20}$$

If in state e we have $\sum_{m=1}^{N} \sigma_{m,\min} > e$ (see Eq. (9)), then it is not possible to satisfy all the constraints because too much transmission energy is demanded (we cannot consume more energy than the stored amount). Thus, we have to identify a proper set of *discarded receivers* $\mathcal{I}(e)$ such that

$$\sum_{\substack{m=1 \\ m \notin \mathcal{I}(e)}}^{N} \sigma_{m,\min} \leq e. \tag{21}$$

Several techniques can be adopted to choose $\mathcal{I}(e)$, *e.g.*, random, overall secrecy maximization, maximum fairness.

$$C_\mu = \sum_{e=0}^{e_{\max}} \left(\pi_{\boldsymbol{\omega}}(e) \int_{\mathbb{R}_+^N} \int_{\mathbb{R}_+^N} \sum_{m=1}^{N} \left[R_{\gamma_m,\nu_m}\big(\sigma_m(e,\boldsymbol{\gamma},\boldsymbol{\nu})\big) \right]^+ \prod_{m=1}^{N} \Big(f_{G_m}(\gamma_m) f_{H_m}(\nu_m) \Big) \mathrm{d}\boldsymbol{\gamma}\mathrm{d}\boldsymbol{\nu} \right) \tag{22}$$

Here we choose a simple scheme, namely *Maximum Active Receivers* (MAR), that keeps the maximum number of receivers, and leave considerations of other techniques as future work. The first element to put in $\mathcal{I}(e)$ is chosen as

$$i = \arg\max_m \{\sigma_{m,\min},\ m = 1, \ldots, N\}. \tag{23}$$

In this way, we remove the highest constraint, thus it is more likely that $\sum_{\substack{m=1 \\ m\neq i}}^{N} \sigma_{m,\min} \leq e$. If there exist m_1, m_2 such that $\max_m \boldsymbol{\sigma}_{\min} = \sigma_{m_1,\min} = \sigma_{m_2,\min}$, then i is chosen randomly. If, even after removing $\sigma_{i,\min}$, the sum of $\sigma_{m,\min}$ is still greater than e, the procedure is repeated. Note that this choice results in the maximization of the number of used sub-carriers because we are discarding the highest constraints.

In order to maximize $C_{\boldsymbol{\Omega}}$, the technique in Theorem 1 can still be employed but the optimal power splitting choice in point 1) changes accordingly.

IV. Analysis With Fading and Statistical CSI

In this section we focus on problem $\mathcal{P}$ when fading is considered. Here, we explicitly write the dependences upon the channel gains. With fading, the ergodic secrecy rate can be computed according to

$$C_\mu = \sum_{e=0}^{e_{\max}} \pi_{\boldsymbol{\omega}}(e) \int_{\mathbb{R}_+^{2N}} c(\boldsymbol{\sigma}(e,\boldsymbol{\gamma},\boldsymbol{\nu}),\boldsymbol{\gamma},\boldsymbol{\nu}) f_{\boldsymbol{G},\boldsymbol{H}}(\boldsymbol{\gamma},\boldsymbol{\nu}) \mathrm{d}\boldsymbol{\gamma}\mathrm{d}\boldsymbol{\nu}, \tag{24}$$

where $\boldsymbol{\gamma} \in \mathbb{R}_+^N$ and $\boldsymbol{\nu} \in \mathbb{R}_+^N$ are the channel gains vectors for the N receivers and eavesdroppers, respectively. $f_{\boldsymbol{G},\boldsymbol{H}}(\boldsymbol{\gamma},\boldsymbol{\nu})$ is the joint probability density function of $\boldsymbol{G}$, $\boldsymbol{H}$. $\pi_{\boldsymbol{\omega}}(e)$ is the steady-state probability of having e energy quanta stored. The system state is defined by the $(2N+1)$-tuple $(e,\boldsymbol{\gamma},\boldsymbol{\nu})$. A policy μ defines the value of the transmission power for every possible system state. As in the previous section, the optimal secrecy policy can still be found with PIA.[2]

A more explicit expression of C_μ is given in Eq. (22) on the top of the page. For the sake of simplicity, the random variables G_m and H_m (with means $\bar{g}_m$ and $\bar{h}_m$) are assumed independent among the several sub-carriers and of each other, which justifies the product inside the integrals in (22).

We also assume that, while the power allocation depends on the channel state, the coding scheme is constant rate [12] and its choice only depends on the overall channel statistics.

A. Partial Channel State Information

In this section we focus on $N = 1$ that represents a realistic special case where there is only one receiver, and makes it possible to derive analytical results. In the general case, the optimal power splitting scheme has to be found for every possible state of the system (in particular, the parameter η in (17) cannot be easily expressed in closed form).

[2]Note that, when there is an infinite number of system states, it is possible to discretize the channel gains and apply PIA to solve the problem.

We study the case where $\boldsymbol{G} = [G_1]$ and $\boldsymbol{H} = [H_1]$ (in the next we omit the "1" subscript) are affected by fading but CSI is available only for G. This is a realistic assumption, *i.e.*, the legitimate channel gain can be found by collaborating with the receiver, whereas the eavesdropper's channel is unknown. In this case it may happen that EHD transmits even when the eavesdropper's channel gain is higher than the legitimate one. Because of this, from Eq. (5), without full CSI it is unavoidable to have some slots with $R_{\gamma,\nu}(\omega) < 0$. A policy defines the values of the transmission power ω for every state (e,γ) (ν is unknown). The secrecy rate expression becomes

$$C_\mu = \left[\sum_{e=0}^{e_{\max}} \pi_{\boldsymbol{\omega}}(e) \int_{\mathbb{R}_+^2} R_{\gamma,\nu}(\omega(e,\gamma)) f_G(\gamma) f_H(\nu) \mathrm{d}\gamma\mathrm{d}\nu \right]^+. \tag{25}$$

Note that in this case 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. A secure transmission can be performed only if $C_\mu > 0$. By integrating over ν and assuming Rayleigh fading ($H \sim Exp(1/\bar{h})$) we obtain

$$C_\mu = \left[\sum_{e=0}^{e_{\max}} \pi_{\boldsymbol{\omega}}(e) \int_{\mathbb{R}_+} f_G(\gamma) T(\gamma,\bar{h},\omega(e,\gamma)) \mathrm{d}\gamma \right]^+, \tag{26}$$

$$T(\gamma,\bar{h},\omega) \triangleq \log_2(1+\gamma\omega) - \frac{e^{\frac{1}{\omega\bar{h}}}}{\ln(2)} \Gamma\left(0, \frac{1}{\omega\bar{h}}\right), \tag{27}$$

where $\Gamma(\cdot,\cdot)$ is the incomplete gamma function.[3] In order to maximize C_μ, we want to sum as many positive terms as possible. We have the following intuitive results.

Proposition 1. *Consider $N = 1$ and an unknown eavesdropper's channel. In the optimal secrecy policy we have $\omega^\star(e,\gamma) = 0$, $\forall e \leq \omega_0$, where $\omega_0 = \min\{\omega : T(\gamma,\bar{h},\omega') > 0, \forall \omega' > \omega\}$. If such a ω_0 does not exist, then $\omega^\star(e,\gamma) = 0$, $\forall e$. Moreover,*

1) *if $\lim_{\omega\to\infty} T(\gamma,\bar{h},\omega) \leq 0$, then ω_0 does not exist;*
2) *if $\lim_{\omega\to\infty} T(\gamma,\bar{h},\omega) > 0$, then ω_0 exists.*

Proof. It can be verified that in general $T(\gamma,\bar{h},\omega)$ decreases in ω in the range $(0,\omega_{\min})$ and then increases in $(\omega_{\min},\infty)$. It may also be that $\omega_{\min} = 0$, *i.e.*, $T(\gamma,\bar{h},\omega)$ is always increasing. If the asymptote is positive, then there exists $\omega_0 \geq 0$, otherwise the function is always negative. Thus, if a transmission is performed with $T(\gamma,\bar{h},\omega) < 0$, the device wastes energy and degrades its reward at the same time, which is sub-optimal. ∎

From the above results, if ω_0 exists and the battery is sufficiently large, it is possible to achieve positive secrecy rate by knowing the statistics of the eavesdropper fading process only. With a finite battery, the secrecy achievability depends

[3]The incomplete gamma function is defined as $\Gamma(a,z) \triangleq \int_z^\infty t^{a-1} e^{-t} \mathrm{d}t$.

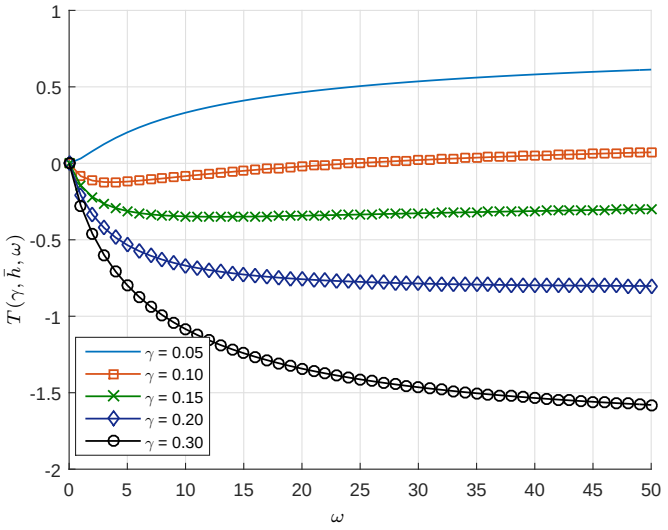


Figure 1: $T(\gamma,\bar{h},\omega)$ as a function of ω for several values of γ when $\bar{h}=0.30$.

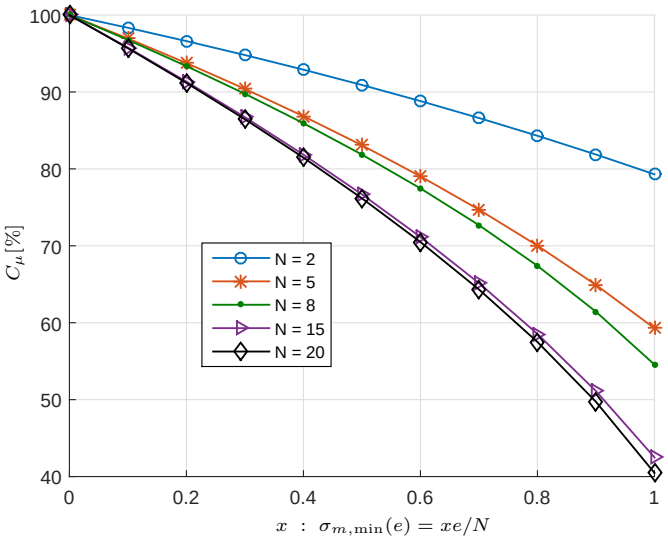


Figure 2: Secrecy rate C_μ as a function of x.

upon $e_{\max}$, $\bar{g}$ and $\bar{h}$ (ω_0 has to exist and to be sufficiently small). In this case, instead of $\lim_{\omega\to\infty}$ it is sufficient to evaluate $T(\gamma,\bar{h},\omega(e_{\max},\gamma))$.

In Fig. 1, we plot the function $T(\gamma,\bar{h},\omega)$ for several cases. It can be seen that the curve for $\gamma=0.30$ is always greater than zero, *i.e.*, $\omega_0=0$. Instead, when $\gamma=0.20$, ω_0 is greater than zero but there still exists a region where $T(\gamma,\bar{h},\omega)>0$. The other cases fall under point 1) of Prop. 1, *i.e.*, no transmission should be performed in these cases, regardless of the available energy. Note that, when $\gamma=0.30$, we have $\gamma=\bar{h}$ and the curve is always positive. This happens because it is more likely that $\nu<\bar{h}$ (prob. $(e-1)/e$) than $\nu\geq\bar{h}$ (prob. $1/e$).

Remark 1. *As $\gamma e_{\max}\to 0$ and $\bar{h}e_{\max}\to 0$ (low SNR regime), $\omega_0=0$ if $\gamma>\bar{h}$ and ω_0 does not exist if $\gamma\leq\bar{h}$.*

Proof. In the low SNR regime, we have $\gamma\omega\to 0$ for any $\omega\leq e_{\max}$ and $\nu\omega\to 0$ with high probability, therefore we can approximate $\log(\frac{1+\gamma\omega}{1+\nu\omega})$ as $\frac{\omega}{\ln 2}(\gamma-\nu)$. Thus, $T(\gamma,\bar{h},\omega)$ is equal to $\frac{\omega}{\ln(2)}(\gamma-\bar{h})$, that is greater than zero if and only if $\gamma>\bar{h}$. ■

B. No Channel State Information

We now suppose that the state of the legitimate receiver's and the eavesdropper's channels are both unknown at the transmitter. Following the reasoning of the previous section, we have

$$C_\mu=\left[\sum_{e=0}^{e_{\max}}\pi_{\boldsymbol{\omega}}(e)U(\bar{g},\bar{h},\omega(e))\right]^+,$$

$$U(\bar{g},\bar{h},\omega)\triangleq\frac{e^{\frac{1}{\omega\bar{g}}}}{\ln(2)}\Gamma\left(0,\frac{1}{\omega\bar{g}}\right)-\frac{e^{\frac{1}{\omega\bar{h}}}}{\ln(2)}\Gamma\left(0,\frac{1}{\omega\bar{h}}\right).$$

In this case, it is harder to obtain a positive secrecy rate because it is not possible to choose the transmission power based on the channel gains. C_μ can be greater than zero only if $\bar{g}>\bar{h}$. However, the values of the channel gains are not controlled by the transmitter (they are given by the physical scenario), thus if the legitimate channel is (statistically) worse, no secrecy can be achieved.

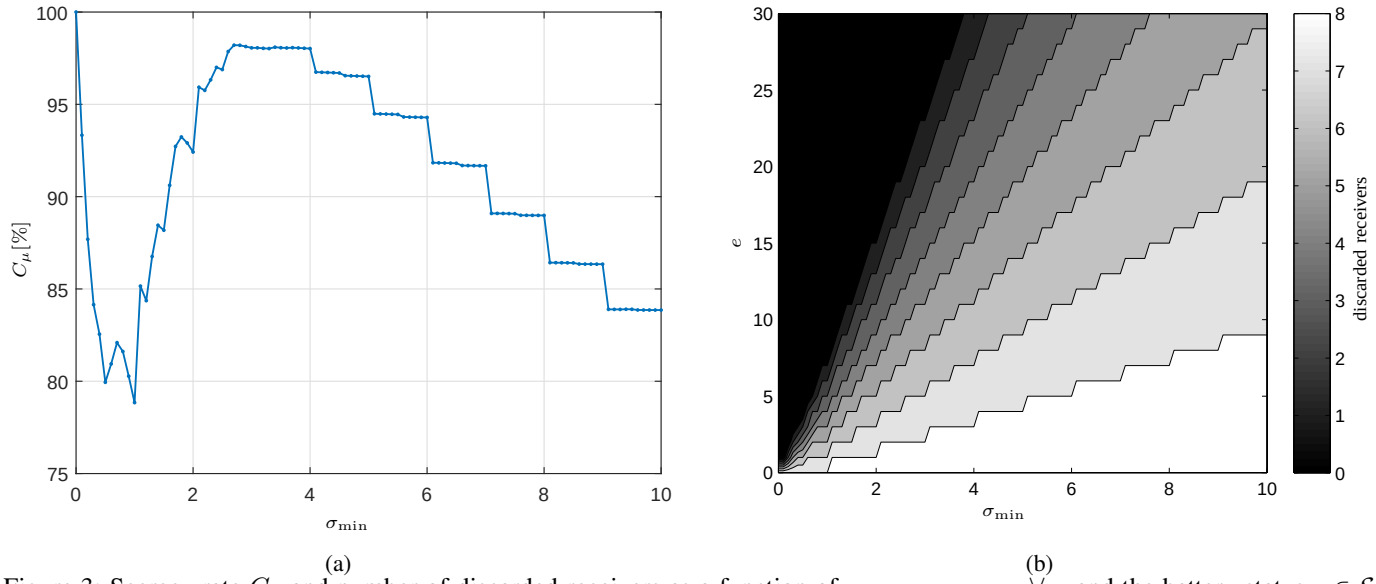
V. Numerical Evaluation

A. Static Channel

In our numerical evaluation we show how the secrecy rate $C_{\boldsymbol{\Omega}}$ is influenced by the system parameters. If not otherwise stated, we use $e_{\max}=30$ and a truncated geometric energy arrival process with $\bar{b}=5$ and $b_{\max}=25$. We set $N=8$ and the channel gains are generated by an exponential distribution with mean $\bar{g}=\bar{h}=1/30$. The results shown have been obtained by averaging 30 independent channel realizations, which has been found to provide adequate statistical accuracy.

First of all, we want to show the importance of the optimal power splitting scheme. In Fig. 2 we plot the optimal secrecy rate $C_{\boldsymbol{\Omega}^\star}$ for several values of N when $\sigma_{m,\min}(e)\leq xe/N$, $\forall m$, $x\in[0,1]$, *i.e.*, the minimum transmission power is a fraction of the current energy state. When no smart power splitting scheme is used (high values of x), the reward decreases significantly, especially for higher N, becoming even lower than 50% of the maximum achievable. The maximum is obtained when no constraints are imposed to $c_{m,\min}$, *i.e.*, $x=0$, because in this case the optimal power splitting choice (17)-(18) can be used. Note that, by choosing $\sigma_{m,\min}(e)=xe/N$, it is always possible to satisfy all the constraints, thus MAR is not necessary in this case. Even if imposing that $\sigma_{m,\min}(e)$ depends upon the current battery state e is not a realistic assumption, Fig. 2 is useful to understand the importance of the power splitting scheme.

In Fig. 3, instead, we change $\sigma_{m,\min}=\sigma_{\min}$, $\forall m$ independently of e. This hypothesis is more realistic. In practice, we are imposing that a receiver demands to receive data with a sufficiently high secrecy rate. At $\sigma_{\min}=0$, we have that no receiver is discarded a priori, *i.e.*, $\mathcal{I}(e)=\emptyset$, $\forall e$. This is because $\sum_{m=1}^{N}\sigma_{m,\min}=N\times\sigma_{\min}=0\leq e$ for every e. As $\sigma_{\min}$ increases, $N\times\sigma_{\min}\leq e$ may not be satisfied for every battery state. In these cases, MAR is performed and



(a) (b)

Figure 3: Secrecy rate C_μ and number of discarded receivers as a function of $\sigma_{m,\min} = \sigma_{\min},\ \forall m$ and the battery status $e \in \mathcal{E}$ with the same parameters of Fig. 2.

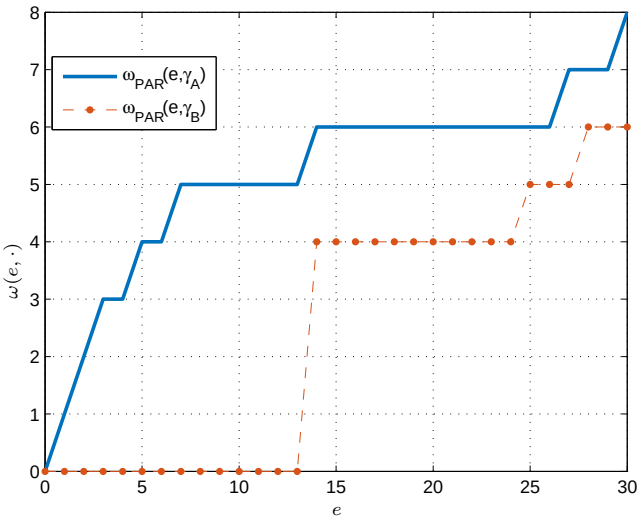


Figure 4: Transmission power $\omega^\star(e,\cdot)$ as a function of the battery status e.

some receivers are discarded, *i.e.*, $\mathcal{I}(e) \neq \emptyset$ for some e. Note that $C_{\boldsymbol{\Omega}}$ may also increase as $\sigma_{\min}$ increases. To understand this behavior, focus on a fixed e and suppose $N \times \sigma'_{\min} = e$. Now, increase $\sigma'_{\min}$ to $\sigma''_{\min}$ such that $N \times \sigma''_{\min} > e$ but $(N-1) \times \sigma''_{\min} < e$. When $\sigma'_{\min}$ is considered, the power splitting scheme forces all the sub-carriers to transmit with power equal to $\sigma'_{\min}$ (as in the right side of Fig. 2). In this case the power splitting scheme is inefficient, thus the corresponding secrecy rate is low. With $\sigma''_{\min}$, instead, the power splitting scheme has to satisfy less strict constraints (because $(N-1) \times \sigma''_{\min} < e$), resulting in a higher secrecy rate.

Also, we plot the number of discarded receivers as a function of $\sigma_{\min}$ and of the battery status. Note that the number of discarded receivers can be simply found as the minimum value $|\mathcal{I}(e)|$ in $0, \ldots, N$ that satisfies $(N - |\mathcal{I}(e)|) \times \sigma_{\min} \leq e$. When $e = 0$, no receiver can be served, *i.e.*, $|\mathcal{I}(0)| = 8$ in this example. As e increases, also the number of possible receivers increases because there is more energy available. When $\sigma_{\min}$ is high, the number of served receivers is low and vice-versa.

B. Fading and Statistical CSI

As in Section IV-A, we set $N = 1$. We consider $H \sim Exp(1/0.9)$, $e_{\max} = 30$, and a truncated geometric arrival process with $\bar{b} = 4$ and $b_{\max} = 10$. We suppose that the legitimate channel can assume only two values $\gamma_A = 1.125$ and $\gamma_B = 0.750$ with probabilities 0.4 and 0.6, respectively. Note that $\bar{g} = \bar{h}$. With no CSI (Section IV-B), the maximum secrecy rate is zero, *i.e.*, no security, because $U(\bar{g}, \bar{h}, \omega) = 0$, independent of ω. In Fig. 4, instead, we show the optimal secrecy policy when only partial knowledge of the channel states is available (Section IV-A). We depict two curves $\omega^\star(e, \gamma_A)$, $\omega^\star(e, \gamma_B)$, one for every possible realization of G. Note that $\omega^\star(e, \gamma_B) \leq \omega^\star(e, \gamma_A)$ because $\gamma_B < \gamma_A$. $\omega^\star(e, \gamma_B)$ is greater than zero only for high values of e. If we had considered the low SNR regime, then $\omega^\star(e, \gamma_B)$ would have been identically zero (see Remark 1).

Fig. 5 presents the secrecy rate as a function of the battery size for $\bar{h} \in \{0.6, 0.9, 1.2\}$. The rate saturates at constant values that depend upon the eavesdropper's channel, thus it is not necessary to use very large batteries to obtain high capacities. For example, to reach 95% of the secrecy rate at $e_{\max} = 30$, it is sufficient to have a battery of size 12, 12 and 19 for $\bar{h} \in \{0.6, 0.9, 1.2\}$, respectively. Note that even when the eavesdropper's channel is statistically better, C_μ is greater than zero.

In Fig. 6 we plot C_μ as a function of $\bar{h}$ for $\gamma_A = 0.1$ with probability 0.4833 and $\gamma_B = 0.0333$ with probability 0.5167. As expected, the higher $\bar{h}$, the lower C_μ because the eavesdropper's channel improves with $\bar{h}$. However, note that even with $\bar{h} = 0$ we have a limited secrecy rate (because the channel capacity is bounded). Between γ_A and γ_B, the rate is

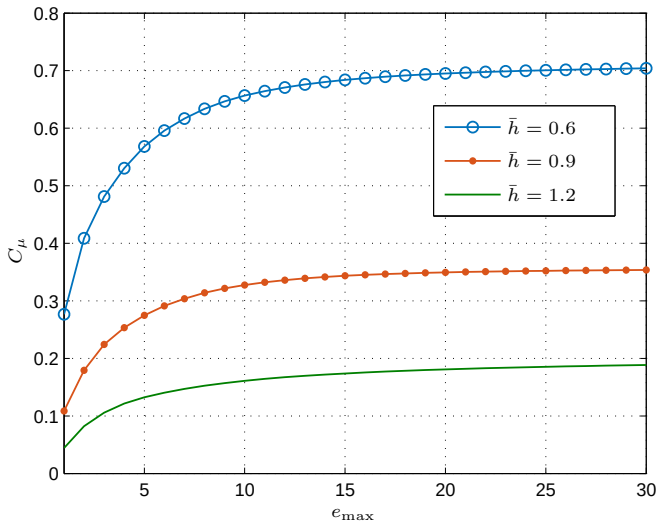


Figure 5: Secrecy rate C_μ as a function of the battery size $e_{\max}$.

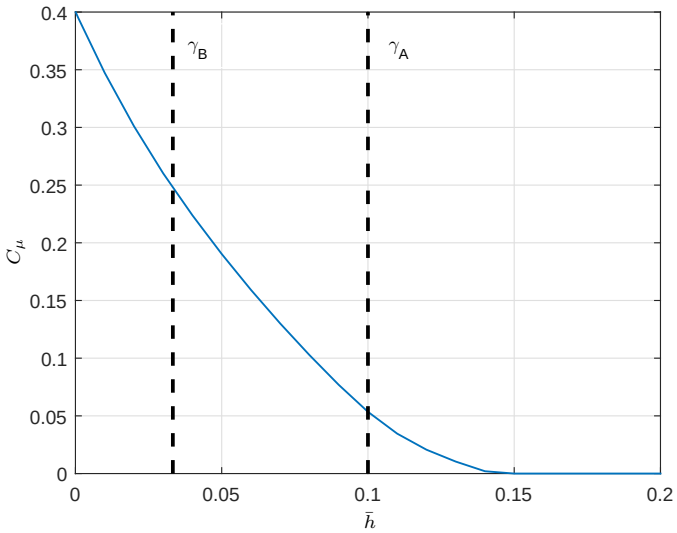


Figure 6: Secrecy rate C_μ as a function of the average eavesdropper channel gain $\bar{h}$.

still greater than zero. We have $C_\mu = 0$ at $\bar{h} = 0.14 > \gamma_A$, *i.e.*, there exists a set of values such that, even if the eavesdropper's channel is statistically better, it is still possible to have secrecy. If we had chosen very small values of γ_A and γ_B, then we would have obtained $C_\mu = 0$ for all $\bar{h} \geq \gamma_A$ (see Remark 1).

VI. Conclusions

In this work we analyzed an Energy Harvesting Device that transmits secret data to N receivers exploiting physical layer characteristics. First, we considered a static channel and introduced the Optimal Secrecy Policy, *i.e.*, the technique that maximizes the secrecy rate with and without minimum secrecy constraints. We showed that the secrecy rate is related to the number of served receivers. In particular, it may not always be possible to satisfy all the secrecy constraints, thus we introduced the *Maximum Active Receivers* scheme to select the receivers that should be discarded. In the second part we considered random fading and studied how the secrecy rate changes when only partial CSI knowledge is available. We numerically showed that, even when the eavesdropper's channel is statistically better, it is still possible to obtain positive capacities also with finite batteries. We showed that the secrecy rate is bounded and that, in general, it is not necessary to use very large batteries.

Future work includes extensions to the model (*e.g.*, considering the circuitry costs and correlated channels), the introduction of alternatives to MAR and the study of larger networks.

References

[1] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM)*, Sep. 2011, pp. 308–311.

[2] M. Sharma *et al.*, "Wireless sensor networks: Routing protocols and security issues," in *International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2014.

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

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

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

[6] O. Ozel and S. Ulukus, "Information-theoretic analysis of an energy harvesting communication system," in *21st International Symposium on Personal, Indoor and Mobile Radio Communications Workshops (PIMRC Workshops)*, Sep. 2010, pp. 330–335.

[7] A. Biason and M. Zorzi, "Transmission policies for an energy harvesting device with a data queue," in *International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2015, pp. 189–195.

[8] 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. on Selected Areas in Commun.*, vol. 33, no. 3, pp. 360–381, Mar. 2015.

[9] 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, Apr. 2014.

[10] M. Zhang, Y. Liu, and S. Feng, "Energy harvesting for secure OFDMA systems," in *Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*, Sep. 2014, pp. 1–6.

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

[12] 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.

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

[14] D. Ng and R. Schober, "Resource allocation for secure communication in systems with wireless information and power transfer," in *IEEE Globecom Workshops*, Jun. 2013, pp. 1251–1257.

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

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

[17] A. Biason, N. Laurenti, and M. Zorzi, "Achievable secrecy rates of an energy harvesting device," in *arXiv:1508.05181*, Aug. 2015.

[18] 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, Jul. 2013.

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