# Gaussian Wiretap Channel with a Batteryless Energy Harvesting Transmitter

Omur Ozel Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland College Park, MD 20742
*omur@umd.edu* *ersen@umd.edu* *ulukus@umd.edu*

***Abstract*—We study the Gaussian wiretap channel with an energy harvesting transmitter which does not have a battery to save energy. In the absence of a battery, the necessary transmission energy is maintained by an i.i.d. energy arrival process. We observe that this channel is an instance of the state-dependent wiretap channel with state available only to the transmitter causally, where the state is the available energy at the transmitter. We prove that the entire capacity-equivocation region can be obtained by single-letter Shannon strategies and its boundary is achieved by input distributions with support set of Lebesgue measure zero.**

## I. Introduction

We consider the Gaussian wiretap channel [1], [2] with a batteryless energy harvesting transmitter [3]–[5], which consists of a transmitter, a legitimate user and an eavesdropper. The transmitter gathers the necessary energy from an exogenous energy arrival process, and each communication link is a memoryless additive white Gaussian noise (AWGN) channel, see Fig. 1. In this model, the transmitter wants to have secure communication with the legitimate user while keeping this communication as secret as possible from the eavesdropper.

The transmitter harvests energy from nature and does not have a battery to save energy for future use. Therefore, the code symbols of the channel input obey time-varying amplitude constraints which are dictated by the i.i.d. energy arrivals that are known causally by only the transmitter. Viewing the available energy at the transmitter as a channel state, the problem of data transmission with an energy harvesting transmitter and the problem of data transmission over state-dependent channels are inherently connected [5]. Consequently, by treating the i.i.d. energy arrivals as channel states, and since the energy arrivals are known only to the transmitter causally, our channel model becomes a state-dependent wiretap channel with causal state information only at the transmitter.

Once this observation is made[1], we show that single-letter Shannon strategies are sufficient to attain the entire capacity-equivocation region of the Gaussian wiretap channel with a batteryless energy harvesting transmitter. Next, we consider the boundary of the capacity-equivocation region as given by the single-letter description obtained, and in particular,

This work was supported by NSF Grants CNS 09-64632, CCF 09-64645, CCF 10-18185 and CNS 11-47811.

[1]Although there is literature on state-dependent wiretap channels [6]–[9], none of these works considers the wiretap channel with causal state information only at the transmitter.

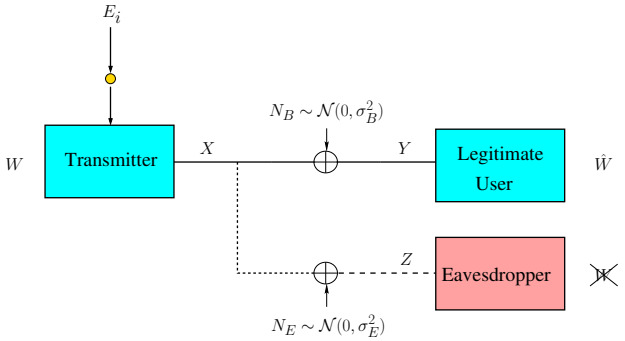


Fig. 1. The Gaussian wiretap channel with a batteryless energy harvesting transmitter.

the optimal distributions that can attain the boundary of the capacity-equivocation region. However, an explicit characterization of the optimal distributions seems to be hard, since i) the links of the extended wiretap channel by Shannon strategies are not additive noise channels, and ii) the inputs are amplitude constrained. We address these challenges by using the technique originally devised by Smith [10], and later, extended in [11]–[15].

In particular, we generalize our previous work in [5], [16] to study the optimal distributions attaining the boundary of the capacity-equivocation region of the Gaussian wiretap channel with a batteryless energy harvesting transmitter. We show that these optimal distributions are discrete and their support set have zero Lebesgue measure. Although this result does not imply the finiteness for the support set of optimal distributions, we numerically observe that the optimal distributions have finite support set.

## II. System Model and Main Results

The Gaussian wiretap channel is defined by

$$Y_i = X_i + N_{B_i}, \qquad i = 1, \ldots, n \tag{1}$$

$$Z_i = X_i + N_{E_i}, \qquad i = 1, \ldots, n \tag{2}$$

where $X_i, Y_i$, and $Z_i$ denote the channel input, the legitimate user's received signal and the eavesdropper's received signal, respectively. $N_{B_i}$ and $N_{E_i}$ are i.i.d. zero-mean Gaussian random variables with variances $\sigma_B^2$ and $\sigma_E^2$, respectively, where $\sigma_B^2 < \sigma_E^2$. The energy required to transmit code symbols is maintained by an i.i.d. energy arrival process $E_i$ and there is no battery to save unused energy. The transmitter observes the

energy arrivals causally. For convenience, we assume that the energy arrivals $E_i$ take one of two values $\mathcal{E} = \{e_1, e_2\}$ with probabilities $p_1$ and $p_2 = 1 - p_1$, respectively. Thus, there is a stochastic amplitude constraint on the channel input $X_i$ as

$$|X_i| \leq \sqrt{E_i}, \quad i = 1, \ldots, n \tag{3}$$

and the transmitter observes the arrived energy causally.

An $(n, 2^{nR})$ code for the Gaussian wiretap channel with a batteryless energy harvesting transmitter with causal information of energy arrivals consists of a message set $\mathcal{W} = \{1, \ldots, 2^{nR}\}$, a sequence of encoders at the transmitter $f_i : \mathcal{W} \times \mathcal{E}^i \to \mathbb{R}$ satisfying the constraint in (3), i.e., $|f_i(w, E_1, E_2, \ldots, E_i)| \leq \sqrt{E_i}$ for $i = 1, 2, \ldots, n$, and a decoder at the legitimate user $g_n : \mathbb{R}^n \to \mathcal{W}$. Equivocation of a code is measured by the normalized conditional entropy $(1/n)H(W|Z^n)$, where $W$ is a uniformly distributed random variable over $\mathcal{W}$. Probability of error for a code is defined as $P_e^n = \Pr[g_n(f_n(W)) \neq W]$. A rate-equivocation pair $(R, R_e)$ is said to be achievable if there exists an $(n, 2^{nR})$ code satisfying $\lim_{n\to\infty} P_e^n = 0$, and

$$R_e \leq \lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \tag{4}$$

The capacity-equivocation region consists of all achievable rate-equivocation pairs, and is denoted by $\mathcal{C}$. A rate $R$ is said to be perfectly secure if we have $R_e = R$, i.e., if there exists an $(n, 2^{nR})$ code satisfying $\lim_{n\to\infty}(1/n)I(W; Z^n) = 0$. Supremum of such rates is defined to be the secrecy capacity and denoted by $C_s$.

The energy arrivals can be viewed as channel states which are available only to the transmitter causally, as noticed in [5]. Using this observation, [5] obtains the capacity of the main channel. In particular, [5] shows that Shannon strategies [17] can attain the capacity of the main channel. Following this reasoning, we argue that the wiretap channel we consider here corresponds to an instance of the state-dependent wiretap channel with causal state information available only to the transmitter, where channel states are the memoryless energy arrivals. Once this connection has been made, we are able to obtain the capacity-equivocation region of the Gaussian wiretap channel with a batteryless energy harvesting transmitter as follows.

**Theorem 1** *The rate-equivocation region $\mathcal{C}$ of the Gaussian wiretap channel with a batteryless energy harvesting transmitter is the union of the rate-equivocation pairs $(R, R_e)$ satisfying*

$$R \leq I(T_1, T_2; Y) \tag{5}$$
$$R_e \leq I(T_1, T_2; Y) - I(T_1, T_2; Z) \tag{6}$$

*for some input distribution $F_{T_1,T_2} \in \Omega$, where the feasible set $\Omega$ is given by*

$$\Omega = \left\{ F_{T_1,T_2} : \int_{-\sqrt{e_1}}^{\sqrt{e_1}} \int_{-\sqrt{e_2}}^{\sqrt{e_2}} dF_{T_1,T_2} = 1 \right\} \tag{7}$$

*and the conditional densities $p_Y(y|t_1, t_2)$ and $p_Z(z|t_1, t_2)$ are given by*

$$p_Y(y|t_1, t_2) = p_1\phi_B(y - t_1) + p_2\phi_B(y - t_2) \tag{8}$$
$$p_Z(z|t_1, t_2) = p_1\phi_E(z - t_1) + p_2\phi_E(z - t_2) \tag{9}$$

*respectively, where $\phi_B(\cdot)$ and $\phi_E(\cdot)$ are Gaussian densities with variances $\sigma_B^2$ and $\sigma_E^2$, respectively.*

We show the achievability for Theorem 1 in two steps. First, we use single-letter Shannon strategies $T_1, T_2$ to convert the original state-dependent wiretap channel into a wiretap channel without states for which the conditional densities are given by (8)-(9). Next, since the wiretap channel we consider is degraded, we use Wyner's achievability [1] to complete the achievability proof. The converse proof of Theorem 1 combines the converses of wiretap and state-dependent channels. The details of the proof can be found in [18].

As the rate-equivocation region $\mathcal{C}$ is convex due to time-sharing, it can be characterized by its supporting hyperplanes, i.e., by solving the following optimization problem

$$\max_{F_{T_1,T_2} \in \Omega} g_\mu(F_{T_1,T_2}) = \max_{F_{T_1,T_2} \in \Omega} (\mu + 1)I(T_1, T_2; Y) - I(T_1, T_2; Z) \tag{10}$$

for all $\mu \geq 0$. We will show that the support set of the optimal input distribution for (10) has zero Lebesgue measure in $\mathbb{R}^2$.

**Theorem 2** *Let $F^*_{T_1,T_2}$ be the maximizer of the optimization problem in (10) with a support set $\mathcal{S}_{F^*_{T_1,T_2}}$. The support set $\mathcal{S}_{F^*_{T_1,T_2}}$ has zero Lebesgue measure in $\mathbb{R}^2$.*

Theorem 2 implies that the secrecy capacity $C_s$ is also achieved by a discrete distribution with zero Lebesgue measure in $\mathbb{R}^2$.

**Corollary 1** *Let $F^*_{T_1,T_2}$ be the secrecy capacity achieving distribution for the extended input Gaussian wiretap channel. The support set $\mathcal{S}_{F^*_{T_1,T_2}}$ has zero Lebesgue measure in $\mathbb{R}^2$.*

In the following sections, we first prove Corollary 1 and then, we generalize it to prove Theorem 2.

## III. Proof of Corollary 1

The secrecy capacity of the extended input wiretap channel is given by

$$C_s = \max_{F_{T_1,T_2} \in \Omega} g_0(F_{T_1,T_2}) \tag{11}$$

where the objective function $g_0(F_{T_1,T_2})$ is a strictly concave functional of the input distribution $F_{T_1,T_2}$ due to the assumption $\sigma_B^2 < \sigma_E^2$ and the resulting degradedness of the wiretap channel. Moreover, the feasible set $\Omega$ is convex and sequentially compact with respect to the Levy metric. Thus, (11) is a convex optimization problem with a unique solution.

Next, we obtain the necessary and sufficient conditions that the optimal distribution $F^*_{T_1,T_2}$ should satisfy. We first note that the output densities for $Y$ and $Z$

exist for any input distribution $F_{T_1,T_2}$, and are given by $p_Y(y;F_{T_1,T_2}) = \int_{-\sqrt{e_1}}^{\sqrt{e_1}}\int_{-\sqrt{e_2}}^{\sqrt{e_2}} p_Y(y|t_1,t_2)dF_{T_1,T_2}$ and $p_Z(z;F_{T_1,T_2}) = \int_{-\sqrt{e_1}}^{\sqrt{e_1}}\int_{-\sqrt{e_2}}^{\sqrt{e_2}} p_Z(z|t_1,t_2)dF_{T_1,T_2}$, respectively.

We define the equivocation density $r_e(t_1,t_2;F_{T_1,T_2})$ as

$$r_e(t_1,t_2;F_{T_1,T_2}) \triangleq i_Y(t_1,t_2;F_{T_1,T_2}) - i_Z(t_1,t_2;F_{T_1,T_2}) \tag{12}$$

where $i_Y(t_1,t_2;F_{T_1,T_2})$ and $i_Z(t_1,t_2;F_{T_1,T_2})$ are:

$$i_Y(t_1,t_2;F_{T_1,T_2}) = \int_{\mathbb{R}} p_Y(y|t_1,t_2)\log\left(\frac{p_Y(y|t_1,t_2)}{p_Y(y;F_{T_1,T_2})}\right)dy \tag{13}$$

$$i_Z(t_1,t_2;F_{T_1,T_2}) = \int_{\mathbb{R}} p_Z(z|t_1,t_2)\log\left(\frac{p_Z(z|t_1,t_2)}{p_Z(z;F_{T_1,T_2})}\right)dz \tag{14}$$

Since the Gaussian wiretap channel is stochastically degraded, without loss of generality, we can assume $Z = Y + Z_D$ for some zero-mean Gaussian random variable $Z_D$ with variance $\sigma_D^2 = \sigma_E^2 - \sigma_B^2$. We denote the density of $Z_D$ by $\phi_D(x)$ which leads to the identity $\phi_E = \phi_B * \phi_D$.

Now, we are ready to obtain the necessary and sufficient conditions for the optimal distribution of the optimization problem in (11). To this end, first, we note that the objective function $g_0(F_{T_1,T_2})$ in (11) is Frechet differentiable and the derivative of $g_0(F_{T_1,T_2})$ at $F^0_{T_1,T_2}$ in the direction of $F_{T_1,T_2}$ is expressed using the equivocation density as [12]

$$\begin{aligned}\lim_{\theta\to 0}\frac{1}{\theta}&\left[g_0(\theta F_{T_1,T_2} + (1-\theta)F^0_{T_1,T_2}) - g_0(F^0_{T_1,T_2})\right]\\ &= \int_{-\sqrt{e_1}}^{\sqrt{e_1}}\int_{-\sqrt{e_2}}^{\sqrt{e_2}} r_e(t_1,t_2;F^0_{T_1,T_2})dF_{T_1,T_2} - g_0(F^0_{T_1,T_2})\end{aligned} \tag{15}$$

Following similar arguments to those in [10], the necessary and sufficient Kuhn-Tucker conditions for the optimal distribution $F^*_{T_1,T_2}$ maximizing (11) can be obtained from (15) as

$$r_e(t_1,t_2;F^*_{T_1,T_2}) \le C_s,\ t_1 \in [-\sqrt{e_1},\sqrt{e_1}], t_2 \in [-\sqrt{e_2},\sqrt{e_2}] \tag{16}$$

$$r_e(t_1,t_2;F^*_{T_1,T_2}) = C_s, \quad (t_1,t_2) \in \mathcal{S}_{F^*_{T_1,T_2}} \tag{17}$$

where $C_s$ is the secrecy capacity.

Next, we prove by contradiction that the support set $\mathcal{S}_{F^*_{T_1,T_2}}$ of the optimal distribution has zero Lebesgue measure in $\mathbb{R}^2$. It suffices to show that $\mathcal{S}_{F^*_{T_1,T_2}}$ cannot include an open set in $\mathbb{R}^2$. To reach a contradiction, we will use the optimality conditions in (16)-(17). We first note that both $i_Y(t_1,t_2;F_{T_1,T_2})$ and $i_Z(t_1,t_2;F_{T_1,T_2})$ have analytic extensions over the two-dimensional complex numbers $\mathbb{C}^2$ [5], and, hence, the equivocation density $r_e(t_1,t_2;F_{T_1,T_2})$ also has an analytic extension over $\mathbb{C}^2$. Now, we assume that $\mathcal{S}_{F^*_{T_1,T_2}}$ includes an open set in $\mathbb{R}^2$. In view of the optimality condition (17), analyticity of $r_e(z_1,z_2,F_{T_1,T_2})$ over all $\mathbb{C}^2$ and the identity theorem, we should have $r_e(z_1,z_2;F^*_{T_1,T_2}) = C_s$ for all $z_1,z_2 \in \mathbb{C}$, which, in turn, implies

$$r_e(t_1,t_2;F^*_{T_1,T_2}) = C_s, \qquad \forall t_1,t_2 \in \mathbb{R} \tag{18}$$

Next, we show that (18) causes a contradiction. In particular, we show that the equality in (18) causes a contradiction over the line $t_1 = t_2$. Therefore, we set $t_1 = t_2 = t$ and obtain

$$\begin{aligned}r_e(t,t;F_{T_1,T_2}) &= \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right)\\ &- \phi_B(t) * \left[\log\left(p_Y(t;F_{T_1,T_2})\right) - \phi_D(t) * \log\left(p_Z(t;F_{T_1,T_2})\right)\right]\end{aligned} \tag{19}$$

Next, we rearrange (18) by using (19) and get

$$\int_{\mathbb{R}} \phi_B(y-t)v(y)dy = 0, \quad \forall t \in \mathbb{R} \tag{20}$$

where $v(y)$ and $c$ are defined as

$$\begin{aligned}v(y) &= c + \log\left(p_Y(y;F^*_{T_1,T_2})\right)\\ &\quad - \int_{\mathbb{R}} \phi_D(\tau)\log\left(p_Z(y-\tau;F^*_{T_1,T_2})\right)d\tau\end{aligned} \tag{21}$$

$$c = C_s - \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right) \tag{22}$$

Our next step towards reaching a contradiction is to show that if (20) holds, we should have $v(y) = 0,\ \forall y \in \mathbb{R}$. To this end, we note that by using Jensen's inequality, one can show that $|\log\left(p_Y(y;F^*_{T_1,T_2})\right)| \le ay^2 + b$ for some $a,b > 0$ and $|\log\left(p_Z(z;F^*_{T_1,T_2})\right)| \le mz^2 + n$ for some $m,n > 0$. Consequently, we have $|v(y)| \le qy^2 + f$ for some $q,f > 0$, which, in conjunction with (20) and using [14, Corollary 9], implies that we should have $v(y) = 0$ for all $y \in \mathbb{R}$.

Next, we show that $v(y) = 0,\ \forall y \in \mathbb{R}$ causes a contradiction. We have the following lemma [18].

**Lemma 1** *For any given $F_{T_1,T_2} \in \Omega$, there exists sufficiently large $y'$ such that $\forall y \ge y'$, we have*

$$\int_{\mathbb{R}} \phi_D(\tau)\log\left(p_Z(y-\tau;F_{T_1,T_2})\right)d\tau \ge \log\left(p_Y(y;F_{T_1,T_2})\right) \tag{23}$$

Applying Lemma 1 for $F^*_{T_1,T_2}$ and using the fact that $c < 0$ as shown in [18], we conclude that $v(y) < 0, \forall y \ge y'$, which implies that (20) cannot hold. This leads us to the conclusion that $\mathcal{S}^*_{F_{T_1,T_2}}$ cannot include an open set in $\mathbb{R}^2$; completing the proof of Corollary 1.

As emphasized by [11], [15], analyticity arguments in multi-dimensional problems may not yield much insight about the optimal input distribution, in particular, may not imply the finiteness of the support set $\mathcal{S}_{F^*_{T_1,T_2}}$. However, here, we provide a numerical result which shows that the support set $\mathcal{S}_{F^*_{T_1,T_2}}$ might be finite. In particular, we consider the wiretap channel whose parameters are $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$, $e_1 = 2.25$, $e_2 = 0.25$, $p_1 = 0.6$, and numerically verify that the optimal input distribution is quaternary located at $(t_1,t_2) = (0.75,0.5)$, $(t_1,t_2) = (-0.75,-0.5)$, $(t_1,t_2) = (1.5,0.5)$ and $(t_1,t_2) = (-1.5,-0.5)$ with probability masses $0.0635$,

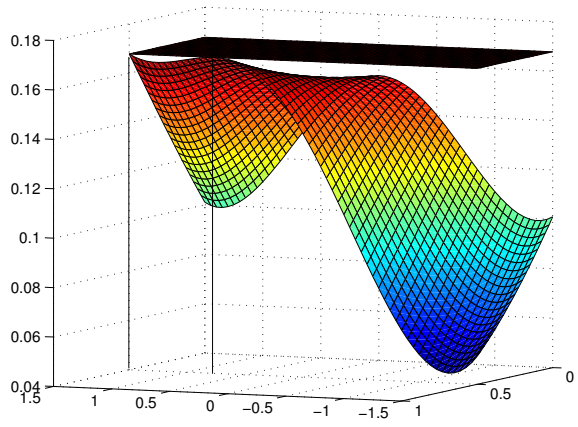


Fig. 2. Equivocation density corresponding to the optimal input distribution when $\sigma_B^2 = 1$, $\sigma_E^2 = 2$, $e_1 = 2.25$, $e_2 = 0.25$, $p_1 = 0.6$.

0.0635, 0.4365 and 0.4365, respectively. The equivocation density generated by this input distribution is given in Fig. 2. The plot shows the range $t_1 \in [-1.5, 1.5]$ and $t_2 \in [0, 0.5]$ and the remaining range is obtained by symmetry with respect to the origin. We observe that the equivocation density for this distribution is less than or equal to the secrecy capacity with equality at the mass points; satisfying the optimality conditions in (16)-(17). Since the distribution satisfying these optimality conditions should be unique, the aforementioned distribution is optimal for the prespecified channel; implying that the support set $\mathcal{S}_{F^*_{T_1,T_2}}$ is finite.

## IV. Proof of Theorem 2

The boundary of the rate-equivocation region can be characterized by solving the following optimization problem

$$\max_{\mathcal{F}_{T_1,T_2}\in\Omega} (\mu+1)I(T_1,T_2;Y) - I(T_1,T_2;Z) \tag{24}$$

for all $\mu \geq 0$. Since the objective function $g_\mu(F_{T_1,T_2})$ in (24) is strictly concave, and the feasible set $\Omega$ is convex and sequentially compact with respect to the Levy metric, the optimization problem in (24) has a unique maximizer, which we denote as $F^*_{T_1,T_2}$.

Using similar arguments to those in [10], the necessary and sufficient conditions for the optimal input distribution of the optimization problem in (24) can be obtained as follows: For all $t_1 \in [-\sqrt{e_1}, \sqrt{e_1}]$, $t_2 \in [-\sqrt{e_2}, \sqrt{e_2}]$:

$$\begin{aligned}\mu i_Y(t_1,t_2;F^*_{T_1,T_2}) + r_e(t_1,t_2;F^*_{T_1,T_2}) \\ \leq (\mu+1)I_Y(F^*_{T_1,T_2}) - I_Z(F^*_{T_1,T_2})\end{aligned} \tag{25}$$

with equality for $(t_1,t_2) \in \mathcal{S}_{F^*_{T_1,T_2}}$, where $I_Y(F^*_{T_1,T_2})$ and $I_Z(F^*_{T_1,T_2})$ are $I(T_1,T_2;Y)$ and $I(T_1,T_2;Z)$ evaluated at $F^*_{T_1,T_2}$, respectively.

Now, we show that the support set of the optimal input distribution $F^*_{T_1,T_2}$ should have zero Lebesgue measure. Similar to the proof of Corollary 1, here also, we prove the desired result by contradiction using the optimality condition in (25). Assume that $\mathcal{S}_{F^*_{T_1,T_2}}$ includes an open set in $\mathbb{R}^2$. Under this assumption, equality in (25), analyticity of $i_Y(t_1,t_2;F^*_{T_1,T_2})$ and $r_e(t_1,t_2;F^*_{T_1,T_2})$ over all $\mathbb{C}^2$ and identity theorem imply

$$\begin{aligned}\mu i_Y(t_1,t_2;F^*_{T_1,T_2}) + r_e(t_1,t_2;F^*_{T_1,T_2}) \\ = (\mu+1)I_Y(F^*_{T_1,T_2}) - I_Z(F^*_{T_1,T_2}), \quad \forall t_1,t_2 \in \mathbb{R}\end{aligned} \tag{26}$$

Next, we show that (26) results in a contradiction. We again set $t_1 = t_2 = t$ and rearrange (26) to get:

$$\int_{\mathbb{R}} \phi_B(y-t)\hat{v}(y)dy = 0 \tag{27}$$

where $\hat{v}(y)$ and $\hat{c}$ are given by

$$\begin{aligned}\hat{v}(y) = \hat{c} + (\mu+1)\log\left(p_Y(y;F^*_{T_1,T_2})\right) \\ - \int_{\mathbb{R}} \phi_D(\tau)\log\left(p_Z(y-\tau;F^*_{T_1,T_2})\right)d\tau\end{aligned} \tag{28}$$

$$\begin{aligned}\hat{c} = \mu(I_Y(F^*_{T_1,T_2}) + \frac{1}{2}\log\left(2\pi e\sigma_B^2\right)) \\ + (I_Y(F^*_{T_1,T_2}) - I_Z(F^*_{T_1,T_2}) - \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right))\end{aligned} \tag{29}$$

By using similar arguments to those in the proof of Corollary 1, one can show that $|\hat{v}(y)| \leq ay^2 + b$ for some $a, b > 0$. By [14, Corollary 9], this implies that if (27) holds, we should have $\hat{v}(y) = 0, \forall y \in \mathbb{R}$. Next, we show that $\hat{v}(y) = 0, \forall y \in \mathbb{R}$ cannot be true. Using Lemma 1 and the fact that $I_Y(F^*_{T_1,T_2}) - I_Z(F^*_{T_1,T_2}) - \frac{1}{2}\log\left(\frac{\sigma_E^2}{\sigma_B^2}\right) < 0$ in (28) due to [18], we get

$$\hat{v}(y) - \mu\big(q + \log\left(p_Y(y;F^*_{T_1,T_2})\right)\big) < 0, \quad \forall y \geq y' \tag{30}$$

where $q \triangleq I_Y(F^*_{T_1,T_2}) + \frac{1}{2}\log\left(2\pi e\sigma_B^2\right)$. Hence, if $\hat{v}(y) = 0, \forall y \in \mathbb{R}$ holds, due to (30), we have

$$q + \log\left(p_Y(y;F^*_{T_1,T_2})\right) > 0, \quad \forall y \geq y' \tag{31}$$

which implies

$$p_Y(y;F^*_{T_1,T_2}) \geq e^{-q}, \quad \forall y \geq y' \tag{32}$$

However, since $p_Y(y;F^*_{T_1,T_2})$ is a density function, it has to vanish as $y \to \infty$, and (32) cannot hold. This is a contradiction and hence the support set of the optimal input distribution cannot include an open set, completing the proof.

## V. Numerical Results

In this section, we provide numerical illustrations for the secrecy capacity and the rate-equivocation region of the Gaussian wiretap channel with a batteryless energy harvesting transmitter. We consider a binary on-off energy arrival process at the transmitter with $e_1 > 0$, $e_2 = 0$, and probabilities $p_{on}$, $1 - p_{on}$, respectively. For this specific case, optimal input distribution can be shown to have finite support set [18], since the problem is one dimensional in this case.

We first examine the secrecy capacity. In Fig. 3, we set $p_{on} = 0.6$ and plot the secrecy capacity with respect to the non-zero energy arrival $e_1$. We also plot the secrecy capacity when energy state information (ESI) is available at the transmitter, legitimate user and the eavesdropper. The secrecy

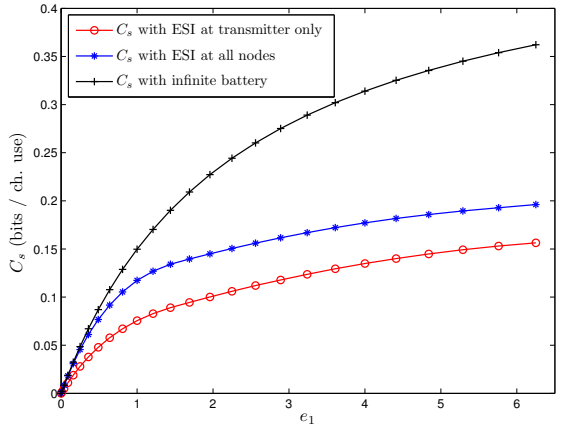


Fig. 3. Comparison of the secrecy capacities with causal ESI at only the transmitter, with ESI at all nodes and with an infinite battery transmitter. $p_{on} = 0.6$, $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$.

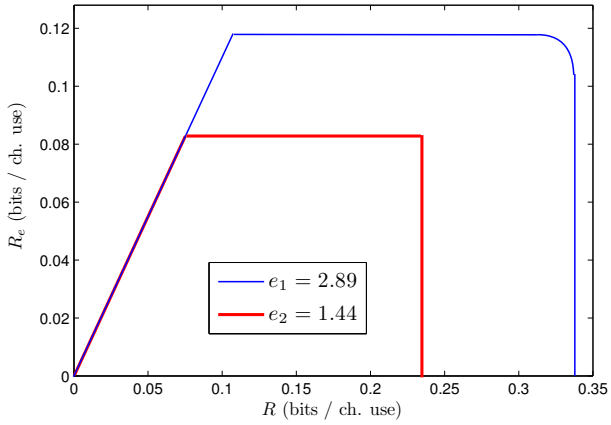


Fig. 4. The rate-equivocation regions for $\sigma_B^2 = 1$ and $\sigma_E^2 = 2$ under on-off energy arrivals with $p_{on} = 0.6$ and $e_1 = 2.89$ and $e_1 = 1.44$.

capacity in this case is equal to the average of amplitude constrained secrecy capacity [16] over the energy arrivals:

$$p_{on}\left(\max_{|X|\leq\sqrt{e_1}} I(X;Y) - I(X;Z)\right) \tag{33}$$

Moreover, we plot the secrecy capacity of the Gaussian wiretap channel with an energy harvesting transmitter with infinite battery, which is the secrecy capacity of the Gaussian wiretap channel with average power constraint $p_{on}e_1$ [4]:

$$\frac{1}{2}\log\left(\frac{1+\frac{p_{on}e_1}{\sigma_B^2}}{1+\frac{p_{on}e_1}{\sigma_E^2}}\right) \tag{34}$$

We observe that the secrecy capacity with an infinite capacity battery is significantly higher than the secrecy capacities in the other cases.

Next, we find the capacity-equivocation region with causal energy state information at only the transmitter[2]. In Fig. 4, we plot the entire capacity-equivocation region of the wiretap channel when $\sigma_B^2 = 1, \sigma_E^2 = 2$ for two different values of $e_1$. When $e_1 = 1.44$, both the secrecy capacity and the capacity can be attained simultaneously. In particular, for $e_1 = 1.44$, the binary input distribution located at $\pm\sqrt{e_1}$ achieves both the capacity and the secrecy capacity. On the other hand, when $e_1 = 2.89$, the secrecy capacity and the capacity cannot be achieved simultaneously. In particular, for $e_1 = 2.89$, the binary input distribution located at $\pm\sqrt{e_1}$ achieves the capacity, while a ternary distribution located at $\pm\sqrt{e_1}$ and 0 with probability masses 0.357 at $\pm\sqrt{e_1}$ and 0.286 at 0 achieves the secrecy capacity, i.e., the optimal input distributions for the secrecy capacity and the capacity are different and therefore, there is tradeoff between the rate and the equivocation.

## VI. Conclusion

We study the Gaussian wiretap channel with a batteryless energy harvesting transmitter. We first obtain a single-letter description of the capacity-equivocation region. Next, we show that the optimal distributions attaining the boundary of the capacity-equivocation region are discrete with support set of Lebesgue measure zero.

[2]We obtain the corresponding optimal distributions by numerical verifications of the necessary and sufficient optimality conditions in (25).

## References


[1] A. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, pp. 1355–1387, October 1975.

[2] S. K. Leung-Yan-Cheung and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Inform. Theory*, vol. 24, pp. 451–456, July 1978.

[3] O. Ozel and S. Ulukus, "Information theoretic analysis of an energy harvesting communication system," in *Workshop on Green Wireless (W-GREEN) at IEEE PIMRC*, September 2010.

[4] O. Ozel and S. Ulukus, "Achieving AWGN capacity under stochastic energy harvesting," *IEEE Trans. on Inform. Theory*, to appear.

[5] O. Ozel and S. Ulukus, "AWGN channel under time-varying amplitude constraints with causal information at the transmitter," in *Asilomar Conference*, November 2011.

[6] C. Mitrpant, A. J. Han Vinck, and Y. Luo, "An achievable region for the wiretap channel with side information," *IEEE Trans. on Inform. Theory*, vol. 52, pp. 2181–2190, May 2006.

[7] W. Liu and B. Chen, "Wiretap channel with two-sided state information," in *Asilomar Conference*, November 2007.

[8] Y. Chen and A. J. Han Vinck, "Wiretap channel with side information," *IEEE Trans. on Inform. Theory*, vol. 54, pp. 395–402, January 2008.

[9] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," in *IEEE ISIT*, June 2010.

[10] J. G. Smith, "The information capacity of amplitude and variance-constrained scalar Gaussian channels," *Information and Control*, vol. 18, pp. 203–219, April 1971.

[11] R. Palanki, "On the capacity achieving distribution of some fading channels," in *Allerton Conference*, September 2002.

[12] I. Abu-Faycal, M. Trott, and S. Shamai, "The capacity of discrete-time memoryless Rayleigh fading channels," *IEEE Trans. on Inform. Theory*, vol. 47, pp. 1290–1301, May 2001.

[13] A. Tchamkerten, "On the discreteness of capacity achieving distributions," *IEEE Trans. on Inform. Theory*, vol. 50, pp. 2273–2278, November 2004.

[14] T. H. Chan, S. Hranilovic, and F. Kschischang, "Capacity-achieving probability measure for conditionally Gaussian channels with bounded inputs," *IEEE Trans. Inform. Theory*, vol. 51, pp. 2073–2088, June 2005.

[15] J. Sommerfeld, I. Bjelakovic, and H. Boche, "On the boundedness of the support of optimal input measures for rayleigh fading channels," in *IEEE ISIT*, July 2008.

[16] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *IEEE ITW*, September 2012.

[17] C. Shannon, "Channels with side information at the transmitter," *IBM Jour. of Research and Development*, vol. 2, October 1958.

[18] O. Ozel, E. Ekrem, and S. Ulukus, "The Gaussian wiretap channel under stochastic energy harvesting," in preperation, 2012.