Covert Communication over a Physically Degraded Relay Channel with Non-Colluding Wardens

Keerthi S. K. Arumugam, Matthieu R. Bloch, Ligong Wang

Covert Communication over a Physically Degraded Relay Channel with Non-Colluding Wardens

Keerthi Suria Kumar Arumugam and Matthieu R. Bloch
School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, USA
Email: keerthi.arumugam@gatech.edu
matthieu.bloch@ece.gatech.edu

Ligong Wang
ETIS—Université Paris Seine
Université de Cergy-Pontoise
ENSEA, CNRS, Cergy-Pontoise, France
Email: ligong.wang@ensea.fr

***Abstract*—We analyze a physically degraded relay channel, in which the transmitter sends a covert message to the legitimate receiver with the help of a relay. Two wardens, who do not collude with each other, monitor communication from the transmitter and the relay, respectively, through two Discrete Memoryless Channels (DMCs) to detect the presence of a covert message. The objective of the transmitter is to deliver the covert message successfully to the receiver without exceeding the covertness threshold of either warden. We identify the optimal asymptotic scaling of message and key bits and the dependence of the covert throughput on the two covertness thresholds.**

I. Introduction

After Bash et al. proved that the amount of information that can be transmitted with Low Probability of Detection (LPD) is governed by the square-root law [1], the following works have investigated reliable communication with LPD in a variety of settings. The fundamental limit of covert communication over a point-to-point channel was characterized in [2], [3], and the possibility of keyless covert communication if the receiver's channel is better than the warden's channel was put forward in [4], [5]. Since any large communication network is fundamentally made up of multiple-access, broadcast, and relay channels, the analysis of covert communication over such models is of interest. Exact characterizations of the information-theoretic limits of covert communication over some multiple-access and broadcast channels are known [6], [7], [8], [9]. A relay channel in which the relay communicates its own message covertly while hiding it from the transmitter, who also serves as the warden, is studied in [10]. Note that our channel model is significantly different since the relay does not have its own covert message. In addition, [10] simplifies covertness analysis by using independent and identically distributed (i.i.d.) Gaussian codebooks.

In this work, we show that the achievability and converse techniques developed in [2], [4], [6], [8] extend to physically degraded relay channels. We characterize the exact number of covert bits that can be transmitted over a physically degraded relay channel when communications from the transmitter and the relay are monitored by two non-colluding wardens. The presence of a second warden at the relay is justified by the fact that a node that assists covert communication would want to keep its assistance covert as well.

This work was supported by the Chateaubriand Fellowship of the Office for Science & Technology of the Embassy of France in the United States and the National Science Foundation Award CNS 1527387.

The paper is organized as follows. Section II sets the notation and introduces the channel model, and Section III presents our main result. We omit some proofs for brevity.

II. Covert communication model

A. Notation

We denote random variables and their realizations in upper and lower cases, respectively. We denote sequences in boldface with their start and end index as subscript and superscript, respectively. For instance, $\mathbf{y}_a^b$ denotes a sequence $(y_a, y_{a+1}, \ldots, y_b)$. We drop the subscript and superscript when the context is clear. Throughout this work, $\log$ and $\exp$ are to the base e. Following standard information-theoretic notation, $\mathbb{H}(X)$ and $\mathbb{I}(X;Y)$ represent the entropy of X and the mutual information between X and Y, respectively. For $p \in [0,1]$, let $\mathbb{H}_b(p)$ represent the binary entropy: $\mathbb{H}_b(p) \triangleq -p\log p - (1-p)\log(1-p)$. For $x \in \mathbb{R}$, we define $[x]^+ \triangleq \max(x, 0)$. For distributions P and Q defined on the same alphabet $\mathcal{X}$, the Kullback-Leibler (KL) divergence $\mathbb{D}(P\|Q) \triangleq \sum_{x\in\mathcal{X}} P(x)\log\frac{P(x)}{Q(x)}$, and the variational distance $\mathbb{V}(P,Q) \triangleq \frac{1}{2}\sum_{x\in\mathcal{X}}|P(x)-Q(x)|$. The two quantities are related via Pinsker's inequality: $\mathbb{V}(P,Q)^2 \leqslant \frac{1}{2}\mathbb{D}(P\|Q)$. If P is absolutely continuous with respect to (w.r.t.) Q, we write $P \ll Q$. We denote the cardinality of a set $\mathcal{S}$ by $|\mathcal{S}|$.

B. Channel Model

Consider the setup illustrated in Figure 1. We consider a discrete memoryless relay channel $\left(\mathcal{X}_1, \mathcal{X}_2, W_{Y_2Y_3|X_1X_2}, \mathcal{Y}_2, \mathcal{Y}_3\right)$ that is physically degraded. Then, for all x_1, x_2, y_2, y_3, $W_{Y_2Y_3|X_1X_2}$ decomposes as [11]

$$\begin{aligned} &W_{Y_2Y_3|X_1X_2}(y_2, y_3|x_1, x_2) \\ &\quad = W_{Y_2|X_1X_2}(y_2|x_1, x_2)W_{Y_3|Y_2X_2}(y_3|y_2, x_2). \end{aligned} \tag{1}$$

Warden 1 monitors transmissions from the transmitter through a DMC $\left(\mathcal{X}_1, W_{Z_1|X_1}, \mathcal{Z}_1\right)$, and Warden 2 monitors transmissions from the relay through another DMC $\left(\mathcal{X}_2, W_{Z_2|X_2}, \mathcal{Z}_2\right)$. We assume that $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X} \triangleq \{0,1\}$, with 0 being the innocent symbol, i.e., the channel input when no communication occurs. We also assume finite output alphabets.

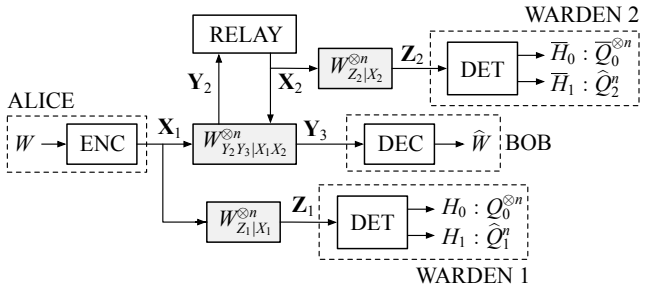

Fig. 1. Model of covert communication over a physically degraded relay channel with two non-colluding wardens.

For $a, b \in \{0,1\}$, we denote the output distributions at the relay and at the receiver Bob by $\overline{P}_{ab}(y_2) \triangleq W_{Y_2|X_1X_2}(y_2|a,b)$, $y_2 \in \mathcal{Y}_2$, and $P_{ab}(y_3) \triangleq W_{Y_3|X_1X_2}(y_3|a,b)$, $y_3 \in \mathcal{Y}_3$, respectively. We assume that $P_{ab} \ll P_{00}$ and $\overline{P}_{ab} \ll \overline{P}_{00}$ for all $a, b \in \{0,1\}$. For $a \in \{0,1\}$, we denote the output distributions at the two wardens by $Q_a(z_1) \triangleq W_{Z_1|X_1}(z_1|a)$, $z_1 \in \mathcal{Z}_1$, and $\overline{Q}_a(z_2) \triangleq W_{Z_2|X_2}(z_2|a)$, $z_2 \in \mathcal{Z}_2$, respectively. We assume that $Q_1 \ll Q_0$, $\overline{Q}_1 \ll \overline{Q}_0$, $Q_1 \neq Q_0$, and $\overline{Q}_1 \neq \overline{Q}_0$ as in [4].

Alice wishes to communicate a covert message $W \in [\![1, M]\!]$ to Bob, with the help of a relay and a secret key $S \in [\![1, K]\!]$. We assume both W and S to be uniformly distributed. Alice maps W and S to her transmission sequence $\mathbf{X}_1$. The relay generates its current symbol based on its past observations; hence, $X_{2,i}$ is a function of $(Y_{2,1}, \ldots, Y_{2,i-1})$ and S. Upon observing the entire output sequence $\mathbf{Y}_3$, Bob maps $\mathbf{Y}_3$ and S to the estimated message $\widehat{W}$. We measure reliability at Bob by the error probability $P_e \triangleq \mathbb{P}\Big(\widehat{W}\Big) \neq W$. Warden 1 observes $\mathbf{Z}_1$ while Warden 2 observes $\mathbf{Z}_2$. Let us denote the distributions induced at the wardens when communication takes place by $\widehat{Q}_1^n$ and $\widehat{Q}_2^n$, respectively. We measure covertness at the wardens in terms of the respective KL divergences, $\mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big)$ and $\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big)$. If our communication scheme ensures that both the KL divergence terms above are small, then any statistical test used by the wardens is futile in detecting the presence of a covert message. Our objective is to characterize the optimal scalings of $\log M$ and $\log K$ with n such that, for $\delta_1, \delta_2 > 0$,

$$\lim_{n\to\infty} P_e = 0, \tag{2}$$

$$\limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \leqslant \delta_1, \quad \limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big) \leqslant \delta_2. \tag{3}$$

We refer to δ_1 and δ_2 as the covertness thresholds.

III. Main result and proof

Define

$$\chi_2 \triangleq \sum_{z_1 \in \mathcal{Z}_1} \frac{\big(Q_1(z_1) - Q_0(z_1)\big)^2}{Q_0(z_1)} \tag{4}$$

$$\overline{\chi}_2 \triangleq \sum_{z_2 \in \mathcal{Z}_2} \frac{\big(\overline{Q}_1(z_2) - \overline{Q}_0(z_2)\big)^2}{\overline{Q}_0(z_2)}. \tag{5}$$

For any $\gamma \geqslant 0$ and $\beta \in [0,1]$, define

$$\Gamma(\gamma, \beta) \triangleq \min\left(\frac{1}{(1+\gamma\beta)}\sqrt{\frac{\delta_1}{\chi_2}}, \frac{1}{\gamma}\sqrt{\frac{\delta_2}{\overline{\chi}_2}}\right), \tag{6}$$

$$\kappa_2(\gamma, \beta) \triangleq \max\Big((1+\gamma\beta)\,\mathbb{D}(Q_1\|Q_0), \gamma\mathbb{D}\big(\overline{Q}_1\|\overline{Q}_0\big)\Big), \tag{7}$$

and $\kappa_1(\gamma, \beta)$ as in (8) at the top of the next page. Our main result is the following.

Theorem 1. *For the degraded channel model described in Section II-B, let $M^*(n,\epsilon)$ be the largest possible value of M such that a length-n channel code can be constructed to satisfy* (3) *and $P_e \leq \epsilon$. Then,*

$$\lim_{\epsilon\downarrow 0} \lim_{n\to\infty} \frac{\log M^*(n,\epsilon)}{\sqrt{n}} = \sup_{\substack{\gamma\geqslant 0,\\ \beta\in[0,1]}} \sqrt{2}\Gamma(\gamma,\beta)\,\kappa_1(\gamma,\beta). \tag{9}$$

Furthermore, this optimal scaling can be achieved if

$$\liminf_{n\to\infty} \frac{\log K}{\sqrt{n}} > \sqrt{2}\Gamma(\gamma^*,\beta^*)[\kappa_2(\gamma^*,\beta^*) - \kappa_1(\gamma^*,\beta^*)]^+, \tag{10}$$

and only if

$$\liminf_{n\to\infty} \frac{\log K}{\sqrt{n}} \geqslant \sqrt{2}\Gamma(\gamma^*,\beta^*)[\kappa_2(\gamma^*,\beta^*) - \kappa_1(\gamma^*,\beta^*)]^+, \tag{11}$$

for some (γ^*, β^*) pair that achieves the limit in (9)*.*

Note that both $\Gamma(\gamma,\beta)\kappa_1(\gamma,\beta)$ and $\Gamma(\gamma,\beta)\kappa_2(\gamma,\beta)$ are bounded for all $\gamma \geqslant 0$ and $\beta \in [0,1]$. If there exist multiple (γ^*, β^*) pairs, we choose the one that minimizes the lower bound in (11).

Remark 1. *If $\gamma^* = 0$, then $\Gamma(0,\beta^*) = \sqrt{\frac{\delta_1}{\chi_2}}$ and $\kappa_1(0,\beta^*) = \mathbb{D}(P_{10}\|P_{00})$, since $\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) \geqslant \mathbb{D}(P_{10}\|P_{00})$ due to the degraded channel assumption. Then,*

$$\lim_{\epsilon\downarrow 0} \lim_{n\to\infty} \frac{\log M^*(n,\epsilon)}{\sqrt{n}} = \sqrt{\frac{2\delta_1}{\chi_2}}\mathbb{D}(P_{10}\|P_{00}), \tag{12}$$

which matches the covert throughput achieved when the relay is not used to transmit any covert information.

A. Proof of achievability for Theorem 1

For $B \in \mathbb{N}^*$, divide the message $w \in [\![1, M]\!]$ into B equal-sized messages $\mathbf{w}_1^B$ each of length $\log M'$, where $\log M' = \frac{\log M}{B}$. Similarly, divide the key $s \in [\![1, K]\!]$ into $B+1$ parts: $\mathbf{s}_1^B$, each of length $\log K'$ and another part $\hat{s}$. We specify $\log K'$ and the length of $\hat{s}$ later. Alice randomly chooses a pair $(m_0, k_0) \in [\![1, M']\!] \times [\![1, K']\!]$ and reveals it to Bob and the relay. Note that, unlike block-Markovian encoding in traditional problems [11], [12], m_0 cannot be fixed in advance, because the warden can detect a fixed codeword with ease. To this end, we employ the key $\hat{s}$, whose length needs to be $\log M' + \log K'$. Thus, as B grows, $\log K'$ approximately equals $\frac{\log K}{B}$. For $n \in \mathbb{N}^*$, define

$$\alpha_n \triangleq \sqrt{\frac{2}{n}} \cdot \Gamma(\gamma,\beta), \tag{13}$$

$$\kappa_1(\gamma,\beta) \triangleq \min\Big(\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big)+\gamma(1-\beta)\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big)+\gamma\beta\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big)-\gamma\mathbb{D}\big((1-\beta)\overline{P}_{01}+\beta\overline{P}_{11}\|\overline{P}_{00}\big),$$
$$\mathbb{D}(P_{10}\|P_{00})+\gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00})+\gamma\beta\mathbb{D}(P_{11}\|P_{00})\Big). \quad (8)$$

and fix $\gamma \geqslant 0$ and $\beta \in [0,1]$ such that $\alpha_n \in [0,1]$. For a large n, define the input distribution Π_{X_2} as

$$\Pi_{X_2}(1) = 1 - \Pi_{X_2}(0) = \gamma\alpha_n, \quad (14)$$

and define the conditional distribution $\Pi_{X_1|X_2}$ as

$$\Pi_{X_1|X_2}(1|0) = 1 - \Pi_{X_1|X_2}(0|0) = \alpha_n, \quad (15)$$
$$\Pi_{X_1|X_2}(1|1) = 1 - \Pi_{X_1|X_2}(0|1) = \beta. \quad (16)$$

Furthermore, defining $\rho_n \triangleq 1+\gamma\beta-\gamma\alpha_n$ we have $\Pi_{X_1}(1) = \rho_n\alpha_n$. Note that $\lim_{n\to\infty}\rho_n = 1+\gamma\beta$. We generate a separate codebook $\mathcal{C}_b$ for each block $b \in [\![1, B+1]\!]$. Define $N \triangleq \frac{n}{B+1}$. For block b, generate $M'K'$ codewords $\mathbf{x}_{2b,s}(w)$ of length N, where $w \in [\![1,M']\!]$ and $s \in [\![1,K']\!]$, according to the distribution $\Pi_{X_2}^{\otimes N}$. For each $\mathbf{x}_{2b,s}(w)$, generate $M'K'$ codewords $\mathbf{x}_{1b,(s,s')}(w,w')$ of length N, where $w,w' \in [\![1,M']\!]$ and $s,s' \in [\![1,K']\!]$, conditionally independently according to the distribution $\Pi_{X_1|X_2}^{\otimes N}(\cdot|\mathbf{x}_{2b,s}(w))$. Bob and the relay observe the N-length sequences $\mathbf{y}_{2b}$ and $\mathbf{y}_{3b}$, respectively, in block b. Similarly, the wardens observe the N-length sequences $\mathbf{z}_{1b}$ and $\mathbf{z}_{2b}$, respectively, in block b. Let $w_{B+1} = s_{B+1} = 1$. We follow the decode-and-forward scheme detailed in [12]. We skip details of the reliability analysis to claim that, for any $\xi \in (0,1)$, the above scheme can achieve

$$\lim_{n\to\infty}\frac{\log M}{\sqrt{n}} = (1-\xi)\,\frac{\sqrt{2}B}{B+1}\Gamma(\gamma,\beta)\kappa_1(\gamma,\beta). \quad (17)$$

By letting $\xi \downarrow 0$ and $B \to \infty$, we conclude that this scheme approaches the right-hand side of (9).

Next, we show that the proposed scheme satisfies the covertness conditions in (3). Following [4], we define the covert processes at the wardens as

$$Q_{\alpha_n}(z_1) \triangleq \sum_{x_1} W_{Z_1|X_1}(z_1|x_1)\Pi_{X_1}(x_1) \quad (18)$$
$$\overline{Q}_{\alpha_n}(z_2) \triangleq \sum_{x_2} W_{Z_2|X_2}(z_2|x_2)\Pi_{X_2}(x_2) \quad (19)$$

We denote the corresponding n-fold product distributions by

$$\Pi_{X_1X_2}^{\otimes n} \triangleq \prod_{i=1}^{n}\Pi_{X_1X_2},\ Q_{\alpha_n}^{\otimes n} \triangleq \prod_{i=1}^{n}Q_{\alpha_n},\ \overline{Q}_{\alpha_n}^{\otimes n} \triangleq \prod_{i=1}^{n}\overline{Q}_{\alpha_n}. \quad (20)$$

Using similar steps as in [4], we obtain

$$\frac{\rho_n^2\alpha_n^2}{2}\left(1+\sqrt{\rho_n\alpha_n}\right)\chi_2 \geqslant \mathbb{D}(Q_{\alpha_n}\|Q_0) \geqslant \frac{\rho_n^2\alpha_n^2}{2}\left(1-\sqrt{\rho_n\alpha_n}\right)\chi_2, \quad (21)$$

$$\frac{\gamma^2\alpha_n^2}{2}\left(1+\sqrt{\gamma\alpha_n}\right)\overline{\chi}_2 \geqslant \mathbb{D}\big(\overline{Q}_{\alpha_n}\|\overline{Q}_0\big) \geqslant \frac{\gamma^2\alpha_n^2}{2}\left(1-\sqrt{\gamma\alpha_n}\right)\overline{\chi}_2. \quad (22)$$

Using our choice of α_n in (13), we obtain

$$\lim_{n\to\infty} n\mathbb{D}(Q_{\alpha_n}\|Q_0) = 2\Gamma(\gamma,\beta)^2\cdot\frac{(1+\gamma\beta)^2}{2}\chi_2 \leq \delta_1, \quad (23)$$
$$\lim_{n\to\infty} n\mathbb{D}\big(\overline{Q}_{\alpha_n}\|\overline{Q}_0\big) = 2\Gamma(\gamma,\beta)^2\cdot\frac{\gamma^2}{2}\overline{\chi}_2 \leq \delta_2. \quad (24)$$

It then remains to show that the induced distributions at the wardens are close to the respective covert processes. For some $b \in [\![1,B+1]\!]$ and $\tau_1 > 0$, define the set

$$\mathcal{B}_{\tau_1}^N \triangleq \left\{(\mathbf{x}_{1b},\mathbf{z}_{1b}) \in \mathcal{X}^N \times \mathcal{Z}_1^N \colon \log\frac{W_{Z_1|X_1}^{\otimes N}(\mathbf{z}_{1b}|\mathbf{x}_{1b})}{Q_{\alpha_n}^{\otimes N}(\mathbf{z}_{1b})} < \tau_1\right\}. \quad (25)$$

For $\left(\mathbf{w}_0^B,\mathbf{s}_0^B\right),\left(\mathbf{u}_0^B,\mathbf{t}_0^B\right) \in [\![1,M']\!]^{B+1}\times[\![1,K']\!]^{B+1}$, we denote the expectation over all random codewords $\left\{\left\{\mathbf{X}_{1b,(t_{b-1},t_b)}(u_{b-1},u_b)\right\}_{b\in[\![1,B+1]\!]}\right\}_{\left(\mathbf{u}_0^B,\mathbf{t}_0^B\right)\neq\left(\mathbf{w}_0^B,\mathbf{s}_0^B\right)}$ by $\mathbb{E}_{\sim\left(\mathbf{w}_0^B,\mathbf{s}_0^B\right)}$. The KL divergence between $\widehat{Q}_1^n$ and $Q_{\alpha_n}^{\otimes n}$ averaged over all random codebooks $\mathcal{C}$ can be upper bounded as in (26) at the top of the next page. For every set $\mathcal{S}_{b'} \subseteq [\![0,B]\!]$ such that $|\mathcal{S}_{b'}| = b'$, where $b' \in [\![0,B+1]\!]$, define another set $\mathcal{T}_{b'} \triangleq \{i+1 \colon i \in \mathcal{S}_{b'}\}$. Here, $\mathcal{S}_{b'}$ denotes the set of block indices whose message-key pairs do not match the corresponding message-key pairs of $\left(\mathbf{w}_0^B,\mathbf{s}_0^B\right)$. Defining $\mu_1 \triangleq \min_{z_1\in\mathcal{Z}_1}Q_0(z_1)$, we upper bound the log term in (26) as in (30). Combining (26) and (30), we obtain (31). Defining $\tau_1 \triangleq (1+\mu)N\mathbb{I}(X_1;Z_1)$ and expanding $\mathbb{I}(X_1;Z_1)$, we obtain

$$\tau_1 = (1+\mu)\,N\rho_n\alpha_n\mathbb{D}(Q_1\|Q_0) + n\mathcal{O}\left(\alpha_n^2\right). \quad (32)$$

Using Bernstein's inequality and choosing M' and K' such that, for n large enough,

$$\log M' + \log K' > (1+\mu)\,N\rho_n\alpha_n\mathbb{D}(Q_1\|Q_0), \quad (33)$$

we upper bound the average KL divergence at warden 1 by

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_1^n\|Q_{\alpha_n}^{\otimes n}\right)\right) \leqslant \exp\left(-cn\alpha_n\right), \quad (34)$$

for some constant $c > 0$. Similarly, by using Bernstein's inequality and choosing M' and K' such that, for a large n,

$$\log M' + \log K' > (1+\mu)\,N\gamma\alpha_n\mathbb{D}\big(\overline{Q}_1\|\overline{Q}_0\big), \quad (35)$$

we can show that

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_2^n\|\overline{Q}_{\alpha_n}^{\otimes n}\right)\right) \leqslant \exp\left(-cn\alpha_n\right), \quad (36)$$

for an appropriate constant $c > 0$. Combining (21), (22), (34), and (36), we prove that the proposed scheme indeed satisfies the covertness conditions in (3).

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\right)\right)$$
$$\leqslant \sum_{\mathbf{z}_1} \frac{1}{(M'K')^{B+1}} \sum_{\mathbf{w}_0^B} \sum_{\mathbf{s}_0^B} \left(\prod_{b=1}^{B+1} \sum_{\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)\right) \Pi_{X_1}^{\otimes N}\left(\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)\right) \right)$$
$$\times \log \mathbb{E}_{\sim(\mathbf{w}_0^B,\mathbf{s}_0^B)} \left(\frac{\sum_{\mathbf{u}_0^B} \sum_{\mathbf{t}_0^B} \left(\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{X}_{1b,(t_{b-1},t_b)}(u_{b-1},u_b)\right)\right)}{(M'K')^{B+1} Q_{\alpha_n}^{\otimes n}(\mathbf{z}_1)} \right). \tag{26}$$

$$\log \mathbb{E}_{\sim(\mathbf{w}_0^B,\mathbf{s}_0^B)} \left(\frac{\sum_{\mathbf{u}_0^B} \sum_{\mathbf{t}_0^B} \left(\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{X}_{1b,(t_{b-1},t_b)}(u_{b-1},u_b)\right)\right)}{(M'K')^{B+1} Q_{\alpha_n}^{\otimes n}(\mathbf{z}_1)} \right)$$
$$\leqslant \log \left(\sum_{b'=0}^{B+1} \frac{1}{(M'K')^{B+1-b'}} \sum_{\mathcal{S}_{b'} \subseteq [\![0,B]\!]} \prod_{\substack{b=1 \\ b \notin \mathcal{S}_{b'} \cup \mathcal{T}_{b'}}}^{B+1} \frac{W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)\right)}{Q_{\alpha_n}^{\otimes N}(\mathbf{z}_{1b})} \right) \tag{27}$$
$$= \log \left(\frac{\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)\right)}{(M'K')^{B+1} Q_{\alpha_n}^{\otimes n}(\mathbf{z}_1)} + 1 \right.$$
$$\left. + \sum_{b'=1}^{B} \frac{1}{(M'K')^{B+1-b'}} \sum_{\mathcal{S}_{b'} \subset [\![0,B]\!]} \prod_{\substack{b=1 \\ b \notin \mathcal{S}_{b'} \cup \mathcal{T}_{b'}}}^{B+1} \frac{W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(s_{b-1},s_b)}(w_{b-1},w_b)\right)}{Q_{\alpha_n}^{\otimes N}(\mathbf{z}_{1b})} \right) \tag{28}$$
$$\leqslant \log \left(\left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1} + \sum_{b'=1}^{B} \binom{B+1}{b'} \frac{(e^{\tau_1})^{B-b'}}{(M'K')^{B+1-b'}} + 1 \right) + \log\left(\frac{2^{B+1}}{Q_{\alpha_n}^{\otimes n}(\mathbf{z}_1)}\right) \sum_{b=1}^{B+1} \mathbb{1}\left\{(\mathbf{x}_{1b},\mathbf{z}_{1b}) \notin \mathcal{B}_{\tau_1}^N\right\} \tag{29}$$
$$\leqslant \left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1} + \sum_{b'=1}^{B} \binom{B+1}{b'} \frac{(e^{\tau_1})^{B-b'}}{(M'K')^{B+1-b'}} + n \log\left(\frac{2^{B+1}}{(1-\rho_n\alpha_n)\,\mu_1}\right) \sum_{b=1}^{B+1} \mathbb{1}\left\{(\mathbf{x}_{1b},\mathbf{z}_{1b}) \notin \mathcal{B}_{\tau_1}^N\right\}. \tag{30}$$

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_1^N \| Q_{\alpha_n}^{\otimes N}\right)\right) \leqslant \left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1} + \sum_{b'=1}^{B} \binom{B+1}{b'} \frac{(e^{\tau_1})^{B-b'}}{(M'K')^{B+1-b'}} + n(B+1)\log\left(\frac{2^{B+1}}{(1-\rho_n\alpha_n)\,\mu_1}\right) \mathbb{P}\left(\mathcal{B}_{\tau_1}^{N\,c}\right). \tag{31}$$

B. Proof of converse for Theorem 1

Consider a covert communication scheme for a physically degraded relay channel that satisfies (2) and (3). Let W be the covert message and S be the secret key. Alice and the relay transmit n-length sequences $\mathbf{X}_1 = (X_{11}, X_{12}, \ldots, X_{1n})$ and $\mathbf{X}_2 = (X_{21}, X_{22}, \ldots, X_{2n})$, respectively. For $i \in [\![1,n]\!]$, define the joint distribution of the symbol pair (X_{1i}, X_{2i}) as $\Pi_{X_{1i}X_{2i}}$. We define two random variables $\widetilde{X}_1$ and $\widetilde{X}_2$ with joint distribution, $\Pi_{\widetilde{X}_1\widetilde{X}_2} \triangleq \frac{1}{n}\sum_{i=1}^{n} \Pi_{X_{1i}X_{2i}}$. For $a, b \in \{0,1\}$, define $\mu_{ab}^{(n)} \triangleq \Pi_{\widetilde{X}_1\widetilde{X}_2}(a,b)$. The corresponding marginal distributions of $\widetilde{X}_1$ and $\widetilde{X}_2$ are denoted by $\Pi_{\widetilde{X}_1}$ and $\Pi_{\widetilde{X}_2}$, respectively. Let $\widehat{P}_{Y_{2i}}$ and $\widehat{P}_{Y_{3i}}$ be the distributions of outputs $\mathbf{Y}_2$ and $\mathbf{Y}_3$, respectively, at bit position $i \in [\![1,n]\!]$. We also define random variables $\widetilde{Y}_2$ and $\widetilde{Y}_3$ with distributions

$$P_{\widetilde{Y}_2}(y_2) = \sum_{x_1,x_2} \Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1,x_2) W_{Y_2|X_1X_2}(y_2|x_1x_2), \tag{37}$$
$$P_{\widetilde{Y}_3}(y_3) = \sum_{x_1,x_2} \Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1,x_2) W_{Y_3|X_1X_2}(y_3|x_1x_2), \tag{38}$$

respectively. Using the cut-set bound and the fact that our channel is physically degraded, we upper bound $\log M$ by (see [11])

$$\log M \leqslant n\mathbb{I}\left(\widetilde{X}_1\widetilde{X}_2; \widetilde{Y}_3\right) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M, \tag{39}$$
$$\log M \leqslant n\mathbb{I}\left(\widetilde{X}_1; \widetilde{Y}_2|\widetilde{X}_2\right) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M, \tag{40}$$

Define $P_{\widetilde{Y}_2|\widetilde{X}_2}(\cdot|x_2) \triangleq \sum_{x_1} \Pi_{\widetilde{X}_1|\widetilde{X}_2}(x_1|x_2) W_{Y_2|X_1X_2}(\cdot|x_1x_2)$, where $\Pi_{\widetilde{X}_1|\widetilde{X}_2}$ is the conditional distribution of $\widetilde{X}_1$ given $\widetilde{X}_2$. Expanding the mutual information terms in (39) and (40), we obtain the bounds in (41) and (42). Defining a random variable $\widetilde{Z}_1$ with distribution $Q_{\widetilde{Z}_1}(z_1) \triangleq \sum_{x_1} \Pi_{\widetilde{X}_1}(x_1) W_{Z_1|X_1}(z_1|x_1)$, $z_1 \in \mathcal{Z}_1$, we can write (see [2])

$$\delta_1 \geqslant \limsup_{n\to\infty} \mathbb{D}\left(\widehat{Q}_1^n \| Q_0^{\otimes n}\right) \geqslant \limsup_{n\to\infty} n\mathbb{D}\left(Q_{\widetilde{Z}_1} \| Q_0\right). \tag{43}$$

In particular, $\lim_{n\to\infty} \mathbb{D}\left(Q_{\widetilde{Z}_1} \| Q_0\right) = 0$. This combined with $Q_1 \neq Q_0$ and Pinsker's inequality implies that $\lim_{n\to\infty} \Pi_{\widetilde{X}_1}(1) = \lim_{n\to\infty} \left(\mu_{10}^{(n)} + \mu_{11}^{(n)}\right) = 0$. Similarly,

$$\log M \leqslant n\left(\mu_{10}^{(n)}\mathbb{D}(P_{10}\|P_{00})+\mu_{01}^{(n)}\mathbb{D}(P_{01}\|P_{00})+\mu_{11}^{(n)}\mathbb{D}(P_{11}\|P_{00})\right)+\mathbb{H}_b\left(\epsilon_n\right)+\epsilon_n\log M, \tag{41}$$

$$\log M \leqslant n\left(\mu_{10}^{(n)}\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big)+\mu_{01}^{(n)}\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big)+\mu_{11}^{(n)}\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big)-\left(\mu_{01}^{(n)}+\mu_{11}^{(n)}\right)\mathbb{D}\Big(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\Big)\right)$$
$$+\mathbb{H}_b\left(\epsilon_n\right)+\epsilon_n\log M. \tag{42}$$

$$\mathbb{D}\Big(\widehat{Q}_1^n\|Q_0^{\otimes n}\Big)\geqslant\sum_{z_1}\Big(1-\xi_1^{(n)}(z_1)\Big)\,n\left(\mu_{10}^{(n)}+\mu_{11}^{(n)}\right)^2\frac{\left(Q_1(z_1)-Q_0(z_1)\right)^2}{2Q_0(z_1)}, \tag{44}$$

$$\mathbb{D}\Big(\widehat{Q}_2^n\|\overline{Q}_0^{\otimes n}\Big)\geqslant\sum_{z_2}\Big(1-\xi_2^{(n)}(z_2)\Big)\,n\left(\mu_{01}^{(n)}+\mu_{11}^{(n)}\right)^2\frac{\left(\overline{Q}_1(z_2)-\overline{Q}_0(z_2)\right)^2}{2\overline{Q}_0(z_2)}. \tag{45}$$

---

we have $\lim_{n\to\infty}\Pi_{\widetilde{X}_2}(1)=\lim_{n\to\infty}\left(\mu_{01}^{(n)}+\mu_{11}^{(n)}\right)=0$. Let us define $\Psi_1^{(n)}(z_1)\triangleq\Pi_{\widetilde{X}_1}(1)\left(Q_1(z_1)-Q_0(z_1)\right)$, $\xi_1^{(n)}(z_1)\triangleq\frac{\Psi_1^{(n)}(z_1)}{Q_0(z_1)}+\frac{4\left|\Psi_1^{(n)}(z_1)\right|}{3Q_0(z_1)}$, $\Psi_2^{(n)}(z_2)\triangleq\Pi_{\widetilde{X}_2}(1)\left(\overline{Q}_1(z_2)-\overline{Q}_0(z_2)\right)$, and $\xi_2^{(n)}(z_2)\triangleq\frac{\Psi_2^{(n)}(z_2)}{\overline{Q}_0(z_2)}+\frac{4\left|\Psi_2^{(n)}(z_2)\right|}{3\overline{Q}_0(z_2)}$. We lower bound $\mathbb{D}\Big(\widehat{Q}_1^n\|Q_0^{\otimes n}\Big)$ and $\mathbb{D}\Big(\widehat{Q}_2^n\|\overline{Q}_0^{\otimes n}\Big)$ as in (44) and (45). Applying limits to (44) and (45), we have

$$\delta_1\geqslant\limsup_{n\to\infty}\frac{n\left(\mu_{10}^{(n)}+\mu_{11}^{(n)}\right)^2}{2}\chi_2, \tag{46}$$

$$\delta_2\geqslant\limsup_{n\to\infty}\frac{n\left(\mu_{01}^{(n)}+\mu_{11}^{(n)}\right)^2}{2}\overline{\chi}_2. \tag{47}$$

For $n\in\mathbb{N}^*$, define $\beta_n\triangleq\frac{\mu_{11}^{(n)}}{\mu_{01}^{(n)}+\mu_{11}^{(n)}}$ and $\gamma_n=\frac{\mu_{01}^{(n)}+\mu_{11}^{(n)}}{\mu_{10}^{(n)}}$. Note that the last KL divergence term in (42) can be written as

$$\mathbb{D}\Big(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\Big)=\mathbb{D}\big((1-\beta_n)\overline{P}_{01}+\beta_n\overline{P}_{11}\|\overline{P}_{00}\big). \tag{48}$$

We now combine (41) and (42) as

$$\log M\leqslant\frac{n\mu_{10}^{(n)}\kappa_1\left(\gamma_n,\beta_n\right)}{1-\epsilon_n}+\frac{\mathbb{H}_b\left(\epsilon_n\right)}{1-\epsilon_n}. \tag{49}$$

For any $\eta>0$, (46) and (47) imply that, for an n large enough,

$$\sqrt{n}\mu_{10}^{(n)}\leq(1+\eta)\sqrt{2}\Gamma(\gamma_n,\beta_n). \tag{50}$$

Combining (49) and (50), and letting $\eta\downarrow 0$ proves the converse part of (9).

Next, we lower bound $\log MK$. Note that, if a sequence of codes achieves the limit in (9), then it must contain a subsequence satisfying $\gamma_n\to\gamma^*$, $\beta_n\to\beta^*$, and $\sqrt{n}\mu_{10}^{(n)}\to\sqrt{2}\Gamma(\gamma^*,\beta^*)$ as $n\to\infty$, for some (γ^*,β^*) that achieves the limit on the right-hand side of (9). For any code in this subsequence, we have

$$\log MK\geqslant\mathbb{I}(\mathbf{X}_1;\mathbf{Z}_1) \tag{51}$$

$$=n\sum_x\sum_z\Pi_{\widetilde{X}_1}(x)W_{Z_1|X_1}(z|x)\log\frac{W_{Z_1|X_1}(z|x)}{Q_0(z)}$$
$$-\mathbb{D}\Big(\widehat{Q}_1^n\|Q_0^{\otimes n}\Big) \tag{52}$$

$$=n\mu_{10}^{(n)}\left(1+\gamma_n\beta_n\right)\mathbb{D}(Q_1\|Q_0)-\mathbb{D}\Big(\widehat{Q}_1^n\|Q_0^{\otimes n}\Big), \tag{53}$$

and, similarly,

$$\log MK\geqslant n\mu_{10}^{(n)}\gamma_n\mathbb{D}\big(\overline{Q}_1\|\overline{Q}_0\big)-\mathbb{D}\Big(\widehat{Q}_2^n\|\overline{Q}_0^{\otimes n}\Big). \tag{54}$$

Normalizing (53) and (54) by $\sqrt{n}$ and applying the limits, we have (for the entire sequence of codes)

$$\liminf_{n\to\infty}\frac{\log MK}{\sqrt{n}}\geqslant\sqrt{2}\Gamma(\gamma^*,\beta^*)\kappa_2\left(\gamma^*,\beta^*\right). \tag{55}$$

Combining (9) and (55) proves that K must satisfy (11).

REFERENCES

[1] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1921–1930, September 2013.

[2] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, pp. 3493–3503, June 2016.

[3] M. Tahmasbi and M. R. Bloch, "First and second order asymptotics in covert communication with pulse-position modulation," *arXiv preprint arXiv:1703.01362v2*, 2017.

[4] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, pp. 2334–2354, May 2016.

[5] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. of IEEE International Symposium on Information Theory*, pp. 2945–2949, July 2013.

[6] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *Proc. of IEEE International Symposium on Information Theory*, pp. 2229–2233, July 2016.

[7] K. S. K. Arumugam and M. R. Bloch, "Covert communication over a K-user multiple access channel," *arXiv preprint arXiv:1803.06007*, 2018.

[8] K. S. K. Arumugam and M. R. Bloch, "Covert communication over broadcast channels," in *Proc. of IEEE Information Theory Workshop*, pp. 299–303, November 2017.

[9] V. Y. Tan and S. H. Lee, "Time-division transmission is optimal for covert communication over broadcast channels," *arXiv preprint arXiv:1710.09754*, 2017.

[10] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. of IEEE Global Communications Conference*, pp. 1–6, December 2017.

[11] A. El Gamal and Y. H. Kim, *Network information theory*. Cambridge University Press, 2011.

[12] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 4–5, pp. 265–444, 2008.