Quantum Noise Limited Optical Communication with Low Probability of Detection

Boulat A. Bash*, Saikat Guha†, Dennis Goeckel‡, Don Towsley*

*School of Computer Science, University of Massachusetts, Amherst, Massachusetts 01003–9264
†Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, Massachusetts 02138
‡Electrical and Computer Engineering Department, University of Massachusetts, Amherst, Massachusetts 01003–9292

***Abstract*—We demonstrate the achievability of a square root limit on the amount of information transmitted reliably and with *low probability of detection* (LPD) over the single-mode lossy bosonic channel if either the eavesdropper's measurements or the channel itself is subject to the slightest amount of excess noise. Specifically, Alice can transmit $\mathcal{O}(\sqrt{n})$ bits to Bob over n channel uses such that Bob's average codeword error probability is upper-bounded by an arbitrarily small $\delta > 0$ while a passive eavesdropper, Warden Willie, who is assumed to be able to collect all the transmitted photons that do not reach Bob, has an average probability of detection error that is lower-bounded by $\frac{1}{2} - \epsilon$ for an arbitrarily small $\epsilon > 0$. We analyze the thermal noise and pure loss channels. The square root law holds for the thermal noise channel even if Willie employs a quantum-optimal measurement, while Bob is equipped with a standard coherent detection receiver. We also show that LPD communication is not possible with coherent state transmission on the pure loss channel. However, this result assumes Willie to possess an ideal receiver that is not subject to excess noise. If Willie is restricted to a practical receiver with a non-zero dark current, the square root law is achievable on the pure loss channel.**

I. Introduction

Typically wireless data transmission is secured from an eavesdropping third party by a cryptographic encryption protocol. However, there are real-life scenarios where encryption arouses suspicion and even theoretically robust encryption can be defeated by a determined adversary using a non-computational method such as side-channel analysis. Thus, protection from interception is often insufficient and the adversary's ability to even *detect the presence* of a transmission must be limited. This is known as *low probability of detection* (LPD) communication.

While practical LPD communication on radio frequency (RF) channels has been explored in the context of spread-spectrum communications [1, Part 5, Ch. 1], our recent work [2], [3] addressed the fundamental limits of LPD communication on an additive white Gaussian noise (AWGN) RF channel. However, free-space communication at optical frequencies offers significant advantages over RF, motivating the need to analyze the LPD communication capability of optical communication. Electromagnetic waves are quantum-mechanical and since modern high-sensitivity optical detection systems are limited by noise of quantum-mechanical origin, assessing the fundamental limits of LPD optical communication necessitates an explicit quantum analysis.

Refs. [2], [3] analyze the LPD communication on an AWGN channel. This corresponds to an optical channel where: (i) transmitter Alice uses ideal laser light to modulate her information, and (ii) both the adversary Warden Willie as well as the legitimate receiver Bob use coherent detection receivers. However, coherent detection receivers can be decidedly suboptimal for both the intended receiver Bob and Warden Willie, and thus a more general analysis of LPD communication with no structural assumptions on Willie's receiver other than its realization being permissible by the laws of physics is desirable. The sub-optimality of coherent detection is particularly pronounced in the low photon number regime [4], [5], which is relevant to LPD communication. It is also preferable to show the possibility of LPD communication when Bob is equipped with a conventional (coherent detection or direct detection) optical receiver, while Willie remains quantum-powerful. Demonstrating how such is possible, even on a highly lossy and noisy channel, is our main contribution.

In this paper we provide the fundamental scaling limits for LPD communication on a lossy optical channel. We limit our analysis to coherent states since they are the quantum description of ideal laser light and are easy to generate. In applications involving highly lossy propagation, coherent states are usually optimal, e.g., they achieve the Holevo capacity of the pure loss channel [4]. They are the only states of light that retain their purity in propagation through a lossy channel, so it is unlikely that modulation using other (non-classical) states of light will improve our scaling law. However, we plan to extend our results to other optical states in the future work.

We consider two types of channels: the thermal noise and the pure loss channel. We show that if Willie has a thermal noise channel from Alice, then meaningful LPD communication between Alice and Bob is possible even if Willie employs an ideal quantum-optimal receiver. On the other hand, if Willie has a pure loss channel from Alice, then there is a receiver he can employ that is capable of perfectly determining when Alice is *not* transmitting. Even though this receiver can err

This research was sponsored by the National Science Foundation under grants CNS-0905349, CNS-1018464 and IIS-0964094, and by the DARPA Information in a Photon (InPho) program under contract number HR0011-10-C-0159.

when Alice is transmitting, we show that Willie can utilize it to prevent LPD communication even when Bob is equipped with an optimal receiver. However, while such a receiver is theoretically conceivable, it has not been and is unlikely to be built. Practical receivers suffer from dark current due to a spontaneous emission process. We thus show that LPD communication is possible if Willie has a pure loss channel from Alice but is limited to a direct detection receiver with non-zero dark current.

In order to state the theorems that govern the LPD scaling laws, we denote Willie's average error probability $\mathbb{P}_e^{(w)} = \frac{\mathbb{P}_{FA}+\mathbb{P}_{MD}}{2}$, where $\mathbb{P}_{FA}$ is the probability that Willie raises a false alarm when Alice did not transmit and $\mathbb{P}_{MD}$ is the probability that Willie misses the detection of Alice's transmission. We say that Alice communicates to Bob *reliably* when Bob's average decoding error probability $\mathbb{P}_e^{(b)} \leq \delta$ for an arbitrary $\delta > 0$ given large enough n. We use asymptotic notation where $f(n) = \mathcal{O}(g(n))$ denotes an asymptotically tight upper bound on $f(n)$, and $f(n) = o(g(n))$ and $f(n) = \omega(g(n))$ denote upper and lower bounds, respectively, that are not asymptotically tight [6, Ch. 3.1].

Theorem 1 (Square root law for the thermal noise channel)**.** *Suppose Willie has access to a quantum-optimal receiver but his channel from Alice is subject to the noise from a thermal environment that injects $N_B > 0$ photons per channel use on average. Then Alice can lower-bound $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$ while reliably transmitting $\mathcal{O}(\sqrt{n})$ bits to Bob in n channel uses even if Bob only has access to a (sub-optimal) coherent detection receiver.*

Theorem 2 (No LPD communication with quantum-powerful Willie on a pure loss channel)**.** *Suppose Willie has a pure loss channel from Alice and is only limited by the laws of physics in his receiver choice. Then Alice cannot reliably communicate to Bob using coherent states while limiting $\mathbb{P}_e^{(w)} \geq \epsilon$ for any $\epsilon > 0$ even if Bob employs a quantum-optimal receiver.*

Theorem 3 (Square root law when Willie experiences dark current)**.** *Suppose that Willie has a pure loss channel from Alice but is limited to a receiver with a non-zero dark current. Then Alice can lower-bound $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ for any $\epsilon > 0$ while reliably transmitting $\mathcal{O}(\sqrt{n})$ bits to Bob in n channel uses.*

Note that converses to Theorems 1 and 3 can be established in a straightforward manner as shown in Section IV-1.

After introducing our optical channel model and hypothesis testing in the next section we prove Theorems 1, 2, and 3 in Sections III, IV, and V. In Section IV-3 we point out some pitfalls of directly applying channel capacity formulas in the LPD communication setting, where the power allocation per symbol is a function of the block length n. Detailed proofs are available in [7]. Section VI concludes the paper.

II. Prerequisites

A. Channel model

Consider a single spatial mode free space optical channel, where each channel use corresponds to one signaling interval that carries one modulation symbol. We focus on single-mode quasi-monochromatic propagation, since our results readily generalize to multiple spatial modes (near-field link) and/or a wideband channel with appropriate power-allocation across spatial modes and frequencies [8]. For simplicity of exposition we limit our analysis to vacuum propagation, i.e., we do not address the effect of atmospheric turbulence. The Heisenberg-picture input-output relationship of the single-mode bosonic channel is captured by a 'beamsplitter' relationship, $\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{e}$, where $\hat{a}$ and $\hat{b}$ are modal annihilation operators of the input and output modes respectively, and $\eta \in [0, 1]$ is the power transmissivity, the fraction of power Alice puts in the input mode that couples into Bob's aperture. Classically, a power attenuation is captured by the relationship $b = \sqrt{\eta}\,a$, where a and b are complex field amplitudes of the input and output mode functions. The quantum description of the channel requires the 'environment' mode $\hat{e}$ in order to preserve the commutator brackets, i.e., $\left[\hat{b}, \hat{b}^\dagger\right] = 1$, which translates to preserving the Heisenberg uncertainty relationship of quantum mechanics. For the pure loss channel, the environment mode $\hat{e}$ is in a *vacuum* state, i.e., $\hat{\rho}^E = |0\rangle\langle 0|^E$. The vacuum state captures the minimum amount of noise that must be injected when 'nothing happens' other than pure power attenuation. For a thermal noise channel, $\hat{e}$ is in a zero-mean thermal state, i.e.,

$$\hat{\rho}^E = \sum_{i=0}^{\infty} \frac{{N_B}^i}{(1+N_B)^{1+i}} |i\rangle\langle i|^E = \int_{\mathbb{C}} \frac{e^{-\frac{|\alpha|^2}{N_B}}}{\pi N_B} |\alpha\rangle\langle\alpha|^E \mathrm{d}^2\alpha,$$

where the mean number of photons injected by the thermal environment is $N_B \approx \pi 10^6 \lambda^3 N_\lambda / \hbar\omega^2$, where N_λ is the background spectral radiance (in W/m^2 sr-μm) [9]. A typical daytime value $N_\lambda \approx 10$ W/m^2 sr-μm at $\lambda = 1.55\mu$m leads to $N_B \approx 10^{-6}$ photons/mode. For $N_B = 0$, the thermal noise channel reduces to the pure loss channel.

B. Hypothesis Testing

Willie collects part of the transmitted light during the transmission of Alice's n modulation symbols and performs a hypothesis test on whether Alice transmitted or not. Willie's null hypothesis H_0 is that Alice did not transmit, and thus he observed vacuum plus noise photons, injected either by a thermal environment or due to dark current generated by a spontaneous emission process in his own measurement apparatus. His alternate hypothesis H_1 is that Alice did transmit.

III. Thermal Noise Channel ($N_B > 0$)

We begin by providing a proof of achievability of $\mathcal{O}(\sqrt{n})$ LPD bits in n channel uses. The proof is constructive: we describe Alice and Bob's communication system and prove that Willie's average probability of detection error is lower-bounded arbitrarily close to $\frac{1}{2}$, while Bob's average probability of codeword decoding error is upper-bounded arbitrarily close to zero. Since we focus on communication using coherent states, the converse follows from the analysis in Section IV-1.

Proof (Theorem 1): **Construction**: Let Alice use a zero-mean isotropic Gaussian-distributed coherent state input $\{p(\alpha), |\alpha\rangle\}$, where $\alpha \in \mathbb{C}$, $p(\alpha) = e^{-|\alpha|^2/\bar{n}}/\pi\bar{n}$ with mean photon number per symbol $\bar{n} = \int_{\mathbb{C}} |\alpha|^2 p(\alpha) \mathrm{d}^2\alpha$. Alice encodes M-bit blocks of input into codewords of length n symbols at the rate $R = M/n$ bits/symbol by generating 2^{nR} codewords $\{\bigotimes_{i=1}^{n} |\alpha_i\rangle_k\}_{k=1}^{2^{nR}}$, each according to $p(\bigotimes_{i=1}^{n} |\alpha_i\rangle) = \prod_{i=1}^{n} p(\alpha_i)$, where $\bigotimes_{i=1}^{n} |\alpha_i\rangle = |\alpha_1 \ldots \alpha_n\rangle$ is an n-mode tensor-product coherent state. The codebook is used only once to send a single message and is kept secret from Willie, though he knows how it is constructed.[1]

Analysis (Willie): Let's assume that when Alice transmits, Willie captures all of the transmitted energy that does not reach Bob's receiver. This is a fairly strong assumption for a line-of-sight diffraction-limited far-field optical link. Since Willie does not have access to Alice's codebook, the n-channel use average quantum states at Willie's receiver under the two hypotheses are given respectively by the density operators,

$$\rho_0^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{(\eta N_B)^i}{(1+\eta N_B)^{1+i}} |i\rangle \langle i| \right)^{\otimes n}, \text{ and} \tag{1}$$

$$\rho_1^{\otimes n} = \left(\sum_{i=0}^{\infty} \frac{((1-\eta)\bar{n} + \eta N_B)^i}{(1+(1-\eta)\bar{n}+\eta N_B)^{1+i}} |i\rangle \langle i| \right)^{\otimes n}. \tag{2}$$

The quantum-limited minimum average probability of error in discriminating the n-copy states $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ is:

$$\mathbb{P}_{e,\min}^{(w)} = \frac{1}{2}\left[1 - \frac{1}{2}\|\rho_1^{\otimes n} - \rho_0^{\otimes n}\|_1\right], \tag{3}$$

where $\|\rho - \sigma\|_1$ is the *trace distance* between states ρ and σ. We can lower-bound[2] $\mathbb{P}_{e,\min}^{(w)}$ using quantum Pinsker's Inequality [12, Th. 11.9.2]:

$$\|\rho - \sigma\|_1 \leq \sqrt{2D(\rho\|\sigma)}, \tag{4}$$

where $D(\rho\|\sigma) \equiv \mathrm{Tr}\{\rho(\ln(\rho) - \log(\sigma))\}$ is the quantum relative entropy (QRE) between states ρ and σ. We thus have:

$$\mathbb{P}_e^{(w)} \geq \mathbb{P}_{e,\min}^{(w)} \geq \frac{1}{2} - \sqrt{\frac{1}{8} D(\rho_0^{\otimes n}\|\rho_1^{\otimes n})}. \tag{5}$$

Since QRE is additive for tensor product states, $D(\rho_0^{\otimes n}\|\rho_1^{\otimes n}) = nD(\rho_0\|\rho_1)$. Since ρ_0 and ρ_1 are diagonal in the photon-number basis, the QRE is:

$$D(\rho_0\|\rho_1) = \eta N_B \ln \frac{(1+(1-\eta)\bar{n}+\eta N_B)\eta N_B}{((1-\eta)\bar{n}+\eta N_B)(1+\eta N_B)} + \\ + \ln \frac{1+(1-\eta)\bar{n}+\eta N_B}{1+\eta N_B}. \tag{6}$$

The details of the derivation of (6) are given in [7, App. A]. The first two terms of the Taylor series expansion of (6) around $\bar{n} = 0$ are zero and the fourth term is negative. Thus, using Taylor's Theorem we can upper-bound (6) by the third term as follows:

$$D(\rho_0\|\rho_1) \leq \frac{(1-\eta)^2 \bar{n}^2}{2\eta N_B(1+\eta N_B)}. \tag{7}$$

Therefore, setting

$$\bar{n} = \frac{4\epsilon\sqrt{\eta N_B(1+\eta N_B)}}{\sqrt{n}(1-\eta)} \tag{8}$$

ensures that Willie's error probability is lower-bounded by $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$ over n optical channel uses by Alice.

Analysis (Bob): Suppose Bob uses a coherent detection receiver. A homodyne receiver, which is more efficient than a heterodyne receiver in the low photon number regime [4], induces an AWGN channel with noise power $\sigma_b^2 = \frac{2(1-\eta)N_B+1}{4\eta}$. Since Alice uses Gaussian modulation with symbol power $\bar{n}$ defined in (8), we can upper-bound $\mathbb{P}_e^{(b)}$ as follows [2, Eq. (7)]:

$$\mathbb{P}_e^{(b)} \leq \delta = 2^{B_{\text{hom}}(n,\epsilon,\delta) - \frac{n}{2}\log_2\left(1+\bar{n}/2\sigma_{b,\text{hom}}^2\right)}. \tag{9}$$

Substituting the expression for $\bar{n}$ from (8) and σ_b^2, and solving for the maximum number of bits $B_{\text{hom}}(n,\epsilon,\delta)$ that can be transmitted from Alice to Bob in n channel uses, we obtain:

$$B_{\text{hom}}(n,\epsilon,\delta) = C_d(\delta) + \sqrt{n}C_c(\epsilon,\eta,N_B) + \mathcal{O}(1), \tag{10}$$

where $C_d(\delta) = \log_2 \delta$ is the 'cost' of upper-bounding Bob's decoding error probability by $\mathbb{P}_e^{(b)} \leq \delta$, and $C_c(\epsilon,\eta,N_B) = \frac{\epsilon\sqrt{\eta N_B(1+\eta N_B)}}{(1-\eta)} \times \frac{4\eta}{2(1-\eta)N_B+1}$ is the cost of lower-bounding Willie's probability of detection by $\mathbb{P}_{e,\min}^{(w)} \geq \frac{1}{2} - \epsilon$. ■

Remark. Eq. (10) illustrates that while the cost of reducing Bob's decoding error has an additive impact that is insignificant at large enough n, the cost of limiting Willie's detection capabilities is multiplicative and proportional to ϵ.

IV. Pure Loss Channel ($N_B = 0$) with Quantum-powerful Willie

Unlike the previous section, here we prove that Alice and Bob cannot hide their communication from Willie if Willie has a pure loss channel from Alice and a choice of a receiver restricted only by the laws of physics. First, we let Willie pick a receiver that does not necessarily capture all the transmitted energy that does not reach Bob's receiver. Alice uses an arbitrary coherent state codebook. While Willie is oblivious to its structure, we show that Alice must constrain her mean photon number to limit the detection capability of Willie's particular receiver. We then show that this constraint prevents Bob from decoding Alice's transmissions without error, proving the theorem.[3] We conclude the section with remarks that establish the converse to Theorems 1 and 3, provide the intuitive interpretation of the result, and show the necessity of this analysis by pointing out the pitfalls of directly

[1] Conceptually, the codebook is similar to a one-time pad [10] and the shared secret requirement follows 'best practices' in security system design where the security of the system depends only on the secret key [11].

[2] Since ρ_0 and ρ_1 are diagonal in the number basis, Willie's quantum-optimal measurement to discriminate $\rho_0^{\otimes n}$ and $\rho_1^{\otimes n}$ is an ideal photon number resolving direct detection receiver with POVM elements given by the photon number operators $\{|i\rangle\langle i|\}$, $i \in \{0, 1, \ldots\}$. We can derive $\mathbb{P}_{e,\min}^{(w)}$ exactly, however, Pinsker's Inequality is simple and sufficient for the bound we need.

[3] While we constrain Alice to using only coherent states in this work, we believe that the result of Theorem 2 holds for general input states; that is, Alice cannot transmit covert data reliably to Bob using a codebook constructed from arbitrary states if Willie has a pure loss channel from her. However, this generalization is an open problem and a subject of future work.

applying the channel capacity formulas when evaluating LPD communication.

Proof (Theorem 2): Suppose Alice transmits an arbitrary codeword $\bigotimes_{i=1}^{n} |\alpha_i\rangle$ and Willie captures a fraction of the transmitted energy, γ, where $0 < \gamma \leq 1 - \eta$. Then Willie's hypothesis test reduces to choosing between the states,

$$\rho_0^{\otimes n} = |0\rangle \langle 0|^{\otimes n}, \text{ and} \tag{11}$$

$$\rho_1^{\otimes n} = \bigotimes_{i=1}^{n} |\sqrt{\gamma}\alpha_i\rangle \langle \sqrt{\gamma}\alpha_i| . \tag{12}$$

Let Willie use an ideal single photon sensitive direct detection receiver given by positive operator-valued measure (POVM) $\{|0\rangle \langle 0|, \sum_{i=1}^{\infty} |i\rangle \langle i|\}^{\otimes n}$ over all n channel uses. Then Willie's probability of error is $\mathbb{P}_e^{(w)} = \frac{1}{2} e^{-\gamma \sum_{i=0}^{n} |\alpha_i|^2}$. Note that the error is entirely due to the missed codeword detections, as Willie's receiver detects vacuum perfectly and never raises a false alarm. Also note that this is a nearly-optimal quantum measurement to distinguish $\rho_0^{\otimes n}$ from $\rho_1^{\otimes n}$; the optimal probability of error (which Willie can achieve only with the knowledge of Alice's codeword $\bigotimes_{i=1}^{n} |\alpha_i\rangle$) is $\frac{1-\sqrt{1-e^{-\gamma \sum_{i=0}^{n} |\alpha_i|^2}}}{2}$ [13, Ch. VI §1(a)]. Since Alice's mean photon number is $\frac{1}{n}\sum_{i=0}^{n} |\alpha_i|^2 = \bar{n}$, if she sets $\bar{n} = \omega(1/n)$, then Willie's probability of error approaches zero as n increases. Thus, Alice sets $\bar{n} = c/n$ for some constant c.

Now we use classical Fano's inequality to lower-bound Bob's decoding error probability similar to the proof of [2, Th. 2]. Denote by W the message transmitted by Alice to Bob, and by $\hat{W}$ Bob's decoding of the codeword sent by Alice, and, for the maximum reduction of the entropy, let each of the e^{nR} messages be chosen equiprobably. Then:

$$nR = H(W) = I(W;\hat{W}) + H(W|\hat{W}) \tag{13}$$

$$\leq I(W;\hat{W}) + 1 + nR\mathbb{P}_e^{(b)} \tag{14}$$

$$\leq \chi\left(p_W(k); \rho_k^W\right) + 1 + nR\mathbb{P}_e^{(b)}, \tag{15}$$

where (13) is from the definition of mutual information, (14) is due to the classical Fano's inequality [14, Eq. (9.37)], and (15) is the Holevo's bound $I(X;Y) \leq \chi(p_i, \hat{\rho}_i)$, with $\chi(p_i, \hat{\rho}_i)$ being the Holevo information for a channel with input alphabet X, $\{p_i, \hat{\rho}_i\}$ the priors and the modulating states, and Y the resulting output alphabet (assuming a POVM $\{\Pi_j\}$) [15]. Since the Holevo information of a single-mode bosonic channel with mean photon number constraint is maximized by a zero-mean thermal state $\rho^B = \sum_{i=0}^{\infty} \frac{(\eta\bar{n})^i}{(1+\eta\bar{n})^{1+i}} |i\rangle \langle i|$ [4],

$$nR \leq \chi\left((\rho^B)^{\otimes n}\right) + 1 + nR\mathbb{P}_e^{(b)} \tag{16}$$

$$= n(\ln(1+\eta\bar{n}) + \eta\bar{n}\ln(1+1/\eta\bar{n})) + 1 + nR\mathbb{P}_e^{(b)} \tag{17}$$

with $\chi(\rho^B) = H(\rho^B)$ since thermal states are pure, and (17) is due to additivity of the Holevo information across the modes of the bosonic channels. This implies:

$$\mathbb{P}_e^{(b)} \geq 1 - \frac{\ln(1+\eta\bar{n}) + \eta\bar{n}\ln(1+1/\eta\bar{n}) + 1/n}{R} \tag{18}$$

$$\geq 1 - \frac{c\eta + c\eta\ln(1+n/c\eta) + 1}{nR} \tag{19}$$

where (19) is due to $\ln(1+x) \leq x$ and substituting $\bar{n} = c/n$. Unless $R = o(1/n)$, Bob's error probability $\mathbb{P}_e^{(b)}$ is lower-bounded above zero for increasing n. However, $R = o(1/n)$ only allows transmitting $o(1)$ bits in n channel uses, which implies that Alice cannot communicate with Bob covertly and reliably using coherent states over the pure loss channel. ■

Remarks

1) Converse to Theorems 1 and 3: When Willie's receiver is subject to excess noise, Alice must set her mean photon number $\bar{n} = \mathcal{O}(1/\sqrt{n})$ to avoid detection by Willie. Since we limit Alice to using coherent states, this follows from letting Willie use a coherent detection receiver and applying the analysis in the first part of the proof of the converse to the square root law for AWGN channels [2, Th. 2]. However, by (18), $\omega(\sqrt{n})$ bits cannot be transmitted both covertly and reliably when $\bar{n} = \mathcal{O}(1/\sqrt{n})$, even if Bob has a pure loss channel from Alice and an optimal receiver.

2) Intuitive Interpretation: At least two codewords are required to convey *any* message that has positive entropy. One of these can be the all-vacuum codeword $|0\rangle^{\otimes n}$. The other codeword *necessarily* must have a positive mean photon number. On the pure loss channel, Willie observes vacuum when Alice is not transmitting, thus allowing him to detect Alice by photon counting measurement. To prevent detection, Alice must make her non-vacuum codeword closely resemble vacuum. However, the more that codeword looks like vacuum, the harder it is for Bob to distinguish it from vacuum since, with the knowledge of the codeword, $\mathbb{P}_e^{(b)} \geq \frac{1-\sqrt{1-e^{-\eta n\bar{n}}}}{2}$ [13, Ch. VI §1(a)]. Thus, in the pure loss case, Bob's decoding error probability increases with Willie's detection error probability. Effectively, Alice has nowhere to hide reliable transmissions if she has a pure loss channel to Willie.

3) Necessity of the proof of Theorem 2: A naïve application of the Holevo capacity formula for the pure loss channel [4],

$$C(\eta\bar{n}) = g(\eta\bar{n}) \equiv (1+\eta\bar{n})\ln(1+\eta\bar{n}) - \eta\bar{n}\ln(\eta\bar{n}), \tag{20}$$

can result in the following error. Substituting $\bar{n} = c/n$ in (20) may lead one to conclude that Alice can covertly and reliably transmit $\mathcal{O}(\ln n)$ bits to Bob in n channel uses. However, we have just shown this to be false. Furthermore, if Willie's detector is subject to excess noise and Alice uses $\bar{n} = \mathcal{O}(1/\sqrt{n})$ per Theorems 1 and 3, direct application of (20) implies that $\mathcal{O}(\sqrt{n}\ln n)$ bits can be covertly transmitted in n channel uses to Bob, contradicting the converse proven above. Therefore one must exercise care when using the results of coding theorems (Shannon or Holevo) for analyzing LPD communication (on a classical or a quantum channel), since the implicit assumption in most channel capacity proofs of a transmission rate independent of codeword blocklength n may not hold.

We have shown above that there exists a quantum measurement that Willie can employ to prevent Alice from covertly using a pure loss channel. However, Alice's situation is not completely hopeless, since the ideal direct detection is nearly impossible to realize in practice.

V. Pure Loss Channel ($N_B = 0$) with Willie Limited by Practical Receiver

Let us reconsider the pure loss channel but assume that Willie's photon counting receiver registers a Poisson dark count process with rate λ_d. On each symbol interval (channel use) of τ seconds, the probability of a dark count at Willie's receiver $p_d \approx \lambda_d \tau$. For instance, $p_d = 10^{-7}$ for a typical superconducting nanowire detector with 100 counts/sec dark count rate and 1 ns time slots. The constructive structure of the proof below is similar to that of Theorem 1.

Proof (Theorem 3): Let Alice use a coherent state on-off keying (OOK) modulation $\{\pi_i, S_i = |\psi_i\rangle\langle\psi_i|\}$, $i = 1, 2$, where $\pi_1 = 1-q$, $\pi_2 = q$, $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = |\alpha\rangle$. When Alice transmits $|\alpha\rangle$, Bob receives $|\sqrt{\eta}\alpha\rangle$. Alice and Bob generate a random codebook with each codeword symbol chosen i.i.d. from the above binary OOK constellation. Since the codebook is kept secret from Willie, Willie observes a sequence of n i.i.d. Bernoulli random variables $\{X_i\}$, $1 \leq i \leq n$, where X_i denotes the output of Willie's receiver on the i^{th} observation. When Alice is not transmitting (i.e., when H_0 is true), the distribution of X_i is $\mathbb{P}_0 = \text{Bernoulli}(p_d)$. When Alice is transmitting a codeword (i.e. when H_1 is true), it is $\mathbb{P}_1 = \text{Bernoulli}(p_d + q(1-p_d)(1-e^{-(1-\eta)|\alpha|^2}))$ since, as in the proof of Theorem 1, Willie captures all of the transmitted energy that does not reach Bob's receiver and $|\langle\sqrt{1-\eta}\alpha|0\rangle|^2 = e^{-(1-\eta)|\alpha|^2}$.

Willie's hypothesis test here is classical and we can thus use the classical relative entropy (CRE) as we do for the AWGN channel in [2], [3] to lower-bound $\mathbb{P}_e^{(w)}$. CRE is given by $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) = \sum_{x\in\mathcal{X}} p_0(x)\log\frac{p_0(x)}{p_1(x)}$ where $p_0(x)$ and $p_1(x)$ are the respective densities of $\mathbb{P}_0$ and $\mathbb{P}_1$, and $\mathcal{X}$ is the support of $p_1(x)$. CRE is additive for independent distributions, and lower-bounds $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \sqrt{\frac{n}{8}\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1)}$. The Taylor series expansion of $\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1)$ around $|\alpha|^2 = 0$ yields (via Taylor's Theorem) the following upper bound:

$$\mathcal{D}(\mathbb{P}_0\|\mathbb{P}_1) \leq \frac{(1-p_d)(q(1-\eta)|\alpha|^2)^2}{2p_d} \tag{21}$$

Thus, to ensure that $\mathbb{P}_e^{(w)} \geq \frac{1}{2} - \epsilon$, Alice can set her average symbol power to

$$\bar{n} = q|\alpha|^2 = \frac{4\epsilon}{\sqrt{n}(1-\eta)}\sqrt{\frac{p_d}{1-p_d}} \tag{22}$$

This allows Alice to transmit $\mathcal{O}(\sqrt{n})$ covert bits reliably to Bob if he also uses a direct detection receiver. The details of the reliability proof are available in [7, App. B]. ■

Theorems 1 and 3 suggest that some form of noise in the adversary's measurements, however small, is essential in making LPD communication possible, as LPD communication masquerades as noise. The nature of the noise appears to be immaterial. It can come from the thermal environment, be Johnson noise, or be generated locally at the adversary's receiver as dark current due to a spontaneous emission process.

Essentially, Alice takes advantage of Willie's measurement noise by transmitting messages, which, when mixed with noise, closely resemble the noise that Willie expects to see on his channel when Alice is quiet. Bob also has to deal with noise in his measurements while decoding, but he has a crucial advantage over Willie: his knowledge of the codebook allows him to reduce the size of his search space, allowing him to compare only the codewords to their received noisy versions.

VI. Conclusion

We demonstrated that, provided Willie experiences noise in his measurements (either due to thermal noise in the channel or excess local noise in his receiver), Alice can transmit $\mathcal{O}(\sqrt{n})$ bits in n channel uses to Bob such that Bob's average decoding error probability approaches zero as n gets large while Willie's average probability of detection error is lower-bounded arbitrarily close to $\frac{1}{2}$. Surprisingly, this scaling law holds even if Willie obtains a quantum-optimal joint-detection measurement over n channel uses and Alice's transmissions are subject to thermal noise on the channel. We also showed that in the absence of any excess noise in Willie's measurements (i.e., on a pure loss channel and an ideal detector for Willie), reliable LPD communication with coherent state transmission is not possible.

Generalizing the proofs of Theorem 2 and the converse of Theorems 1 and 3 by lifting the coherent state assumption is an open problem that we plan on tackling in the future work.

References

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, revised ed. McGraw-Hill, 1994.

[2] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of Reliable Communication with Low Probability of Detection on AWGN Channels," arXiv:1202.6423, 2012, to appear in *JSAC: Special Issue on Signal Processing for Physical Layer Security.*

[3] ——, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Cambridge, MA, Jul. 2012.

[4] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical capacity of the lossy bosonic channel: The exact solution," *Phys. Rev. Lett.*, vol. 92, p. 027902, Jan 2004.

[5] S. Guha, "Structured optical receivers to attain superadditive capacity and the holevo limit," *Phys. Rev. Lett.*, vol. 106, p. 240502, June 2011.

[6] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. Cambridge, Massachusetts: MIT Press, 2001.

[7] B. A. Bash, S. Guha, D. Goeckel, and D. Towsley, "Quantum Noise Limited Communication with Low Probability of Detection," University of Massachusetts, Tech. Rep. UM-CS-2013-002.

[8] J. H. Shapiro, S. Guha, and B. I. Erkmen, "Ultimate channel capacity of free-space optical communications," *Journal of Optical Networking*, vol. 4, no. 8, pp. 501–516, August 2005.

[9] N. Kopeika and J. Bordogna, "Background noise in optical communication systems," *Proc. of the IEEE*, vol. 58, no. 10, pp. 1571–1577, Oct. 1970.

[10] C. E. Shannon, "Communication theory of security," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[11] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st ed. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[12] M. M. Wilde, "From Classical to Quantum Shannon Theory," arXiv:1106.1445, 2011.

[13] C. W. Helstrom, *Quantum Detection and Estimation Theory*. New York: Academic Press, Inc., 1976.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. John Wiley & Sons, Hoboken, NJ, 2002.

[15] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, pp. 269–273, 1998.