Fundamental limits of discrete-modulation quantum-secure covert optical communication

Boulat Bash[1,2], Christos Gagatsos[2], and Saikat Guha[1,2]

[1] Department of Electrical and Computer Engineering, University of Arizona, Tucson, Arizona 85721, USA

[2] College of Optical Sciences, University of Arizona, Tucson, Arizona 85721, USA

Abstract

We report on a fundamental difference between detectability of discrete modulation schemes over thermal-noise bosonic channels by quantum vs. classical adversaries: while discrete modulation is as effective in hiding data as the optimal Gaussian modulation against classical adversaries, it is strictly less effective against a quantum-enabled adversary. This impacts the design of quantum-secure covert communication systems as well as demonstrates yet another fundamental advantage of quantum detection techniques.

Covert, or low probability of detection/intercept (LPD/LPI), communication prevents transmission's detection by an adversary. This is a stricter security requirement than protection of transmission's content from unauthorized access provided by standard methods, e.g., quantum key distribution. *Square root law* (SRL) governs covert communication over additive white Gaussian noise (AWGN) [1] and bosonic [2] channels: no more than $\propto \sqrt{n}$ covert bits can be transmitted reliably to the intended receiver in n uses of the channel; attempting to transmit more results in either detection by the adversary with high probability, or unreliable transmission. For optical channels, n is the number of available spatio-temporal-polarization modes. Even though the capacity of covert channel is zero, as n increases, SRL allows transmission of a significant number of covert bits even when the adversary is quantum-capable, provided he does not control some noise on his channel to transmitter [2].

SRL is the consequence of covertness requiring the mean transmitted photon number per mode to scale as $\bar{n}_{\rm S} = c/\sqrt{n}$, with the SRL constant c characterizing the amount of transmissible covert data. Here we report on the impact of restriction to discrete modulation on c in communication over the thermal-noise lossy bosonic channel of transmissivity η, with $\bar{n}_{\rm T}$ mean photons injected per mode by a thermal environment. We compare the covertness of two modulation formats: 1) coherent state modulation using isotropic Gaussian prior, $\mathcal{M}_{\rm G} = \{\{|\alpha\rangle\}, p(\alpha) = \frac{e^{-|\alpha|^2/\bar{n}_{\rm S}}}{\pi\bar{n}_{\rm S}}\}$ and 2) binary coherent state modulation using equal prior $\mathcal{M}_{\rm B} = \{\{|\beta\rangle, |-\beta^*\rangle\}, p(\beta) = p(-\beta^*) = \frac{1}{2}\}$ with $|\beta|^2 = \bar{n}_{\rm S}$.

When the adversary uses a homodyne receiver, he experiences an AWGN channel with noise power $\sigma_{\rm T}^2 = \frac{2\eta\bar{n}_{\rm T}+1}{4(1-\eta)}$. Then, maximum $c_{\rm AWGN} = 2\sigma_{\rm T}^2$ [1, 3, 4]. While the optimality is proven using $\mathcal{M}_{\rm G}$ [3, 4], we can also attain $c_{\rm AWGN}$ using $\mathcal{M}_{\rm B}$ [1, Theorem 1.2]. Thus, it is as difficult to detect $\mathcal{M}_{\rm B}$ as it is $\mathcal{M}_{\rm G}$, resulting in identical covert communication performance. Similar result holds for an adversary using a heterodyne receiver.

Surprisingly, $\mathcal{M}_{\rm B}$ fares worse than $\mathcal{M}_{\rm G}$ when adversary is given an arbitrary receiver. We show that the maximum is $c_{\rm bos} = \sqrt{2\eta\bar{n}_{\rm T}(1+\eta\bar{n}_{\rm T})}$, achieved by $\mathcal{M}_{\rm G}$. However, maximum SRL constant achievable by $\mathcal{M}_{\rm B}$ is $c_{\rm BPSK} \leq \left(\frac{1}{2\eta\bar{n}_{\rm T}(1+\eta\bar{n}_{\rm T})} + \frac{1}{1+2\eta\bar{n}_{\rm T}}\log\left(1+\frac{1}{\eta\bar{n}_{\rm T}}\right)\right)^{-\frac{1}{2}}$. We note that we do not contradict that the Holevo capacity is achieved by $\mathcal{M}_{\rm B}$ at low signal-to-noise ratios [5], and, in fact, our calculations confirm this. Rather, we claim that a quantum receiver may make $\mathcal{M}_{\rm B}$ easier to detect than $\mathcal{M}_{\rm G}$, requiring smaller $\bar{n}_{\rm S}$ and degradation in performance for $\mathcal{M}_{\rm B}$. In addition to obvious implications for quantum-secure covert communication system design, this is yet another example of a classical-quantum gap in optical receiver performance.

[1] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," IEEE J. Select. Areas Commun. **31**, 1921–1930 (2013).

[2] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," Nat. Commun. **6** (2015).

[3] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," IEEE Trans. Inf. Theory **62**, 2334–2354 (2016).

[4] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," IEEE Trans. Inf. Theory **62**, 3493–3503 (2016).

[5] F. Lacerda, J. M. Renes, and V. B. Scholz, "Coherent-state constellations and polar codes for thermal gaussian channels," Phys. Rev. A **95**, 062343 (2017).