Secret key distillation over realistic satellite-to-satellite free-space channel

Ziwen Pan[†], **John Gariano**[†], **William Clark**[‡], **Ivan B. Djordjevic**[†]

[†]*University of Arizona, Tucson, AZ;*
[‡]*General Dynamics Mission Systems, Scottsdale, AZ*
ziwenpan@email.arizona.edu

Abstract: In this paper, the satellite-to-satellite secret-key rate lower bounds are determined for two relevant scenarios in which the exclusion zone and Eve's aperture size are varied.

OCIS codes: 060.5565 Quantum communications

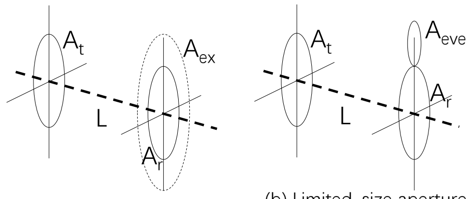
1. Introduction

With the development of satellite-based free-space communications [1], the capacity and security of communication between satellites have become relevant. The recent satellite-to-ground quantum key distribution (QKD) experiment [2] has shown that it is possible to use QKD for secure satellite-based communication. However, various realistic scenarios including those with spy satellites haven't been thoroughly studied so far from security point of view. Thus in this paper we look into two typical scenarios where eavesdropper's (Eve's) collecting ability is taken into consideration.

We first introduce in Sec. 2 and analyze the so-called "exclusion zone" scenario where Eve cannot eavesdrop without alerting the communicating parties. Then in Sec. 3 we study the scenario where Eve's collecting ability is limited by the size of her aperture. We demonstrate that for certain well-chosen parameters we can achieve significantly higher secure-key rate (SKR) lower bounds compared to traditional unrestricted Eve scenario.

2. Exclusion zone scenario

In this section we will evaluate the first scenario as is illustrated in Fig. 1 (a), here "exclusion zone" means that Eve cannot collect photons in this zone without alerting communicating parties. In satellite based secure communication, setting an "exclusion zone" is one of the most straightforward methods to improve security as this effectively decreases Eve's collecting ability. Here we assume that Eve can collect all photons outside of the exclusion zone.



(a) Exclusion Zone Scenario

(b) Limited-size aperture Scenario

Fig. 1: Geometric setup of (a) Exclusion zone scenario, (b) Limited-size aperture scenario. A_t is the transmitting aperture (Alice) area and A_r is the receiving aperture (Bob) area. L is the transmission distance between Alice and Bob. The exclusion zone area in (a) is denoted as A_{ex} which is a ring around Bob's aperture. In (b) A_{eve} is the eavesdropper (Eve) aperture area which is placed in the same plane as Bob's aperture.

According to similar analysis in [3–6], if the frequency used ω is restricted to $0 \leq \omega \ll \omega_0 = 2\pi cL/\sqrt{A_t A_r}$, then the transmissivity at frequency ω is determined by $\eta(\omega) = (\omega/\omega_0)^2 \ll 1$. Since the transmission is in space, for thermal noise frequency dependence we use the black body radiation equation (Eq. (1.49) in [7]) to calculate the mean photon number of noise thermal state: $n_e = \frac{1}{e^{h*f/(k*T)}-1}$. We set temperature to $T = 3$K in the simulation in Fig. 2.

As we can see in Fig. 2, the SKR lower bounds [3, 4] increase with increasing frequency. Although choosing a higher frequency can always result in higher SKR, this can pose potential challenges to the system design as we need higher frequency for longer transmission distance. This problem can be solved by enlarging the exclusion zone as it effectively decreases Eve's receiving area and thus relax the need for higher frequency as in Fig. 2

3. Limited-size aperture scenario

In Sec. 2 we didn't pose any restrictions on Eve's aperture size. Here we assume that Eve has a limited-size aperture A_{eve}, as in Fig. 1 (b). First we look at the straightforward case which actually gives us very interesting results when Eve's aperture is in the same plane as Bob's aperture with no overlapping. In this case, the optimal

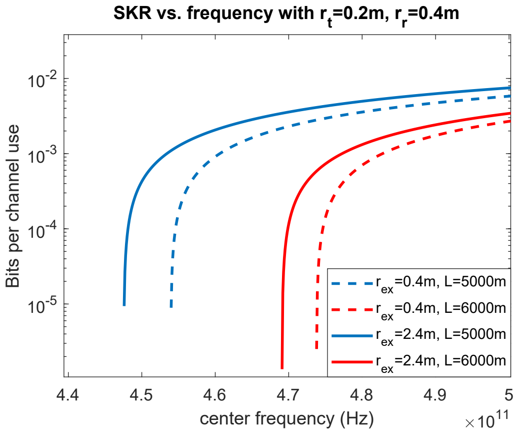


Fig. 2: SKR lower bound vs. center frequency. Radius of exclusion zone and transmission distance are given.

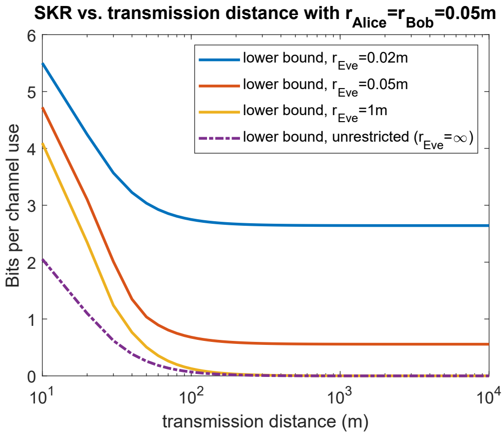


Fig. 3: SKR lower bounds vs. distance. Unrestricted Eve's case [3] is also included for comparison.

position is when Eve's aperture is tangential to Bob's aperture, as illustrated in Fig. 1 (b). More generalized scenarios will be included in a complete version of this paper which will be available online soon.

Here we also use the same noise frequency dependence as in Sec. 2. We assume that Gaussian beam is transmitted. In Fig. 3 we plot the SKR lower bound versus transmission distance at wavelength $\lambda = 0.5$mm, $r_t = r_r = 5$cm. The channel actually approximates a pure loss channel [3] as $n_e \approx 0$ in space ($T = 3$K) at this wavelength.

In Fig. 3 we can see that the SKR lower bounds first decrease with increasing distance.When Eve has a infinite size aperture (unrestricted case in Fig. 3), the SKR would drop to zero as distance goes to infinity since increased distance only decreases Bob's collecting ability. However if we assume limited aperture size for Eve then the SKR goes to a non-zero value as distance goes to infinity. This is because when distance is large, we will have $\lim_{L\to\infty} \frac{\eta_{AE}}{\eta_{AB}} = \frac{A_{eve}}{A_r} = m$, where η_{AB} and $\eta_{AE} = (1-\eta_{AB})\kappa$ refer to Alice-to-Bob and Alice-to-Eve transmissivity, respectively. Here κ is the restriction factor [3] on Eve. This would return a constant SKR lower bound as η_{AB} goes to zero: $\lim_{L\to\infty} SKR \geq \max\left(-\log_2(m), -\log_2\left(\left(\frac{m}{1+m}\right)^{1+m} e\right)\right)$. In Fig. 3 we can see that when Eve's aperture is much larger than Bob's then the SKR lower bound approximates the unrestricted Eve's case when distance is large. However when Bob's aperture is larger than Eve's, or even when they are equal, the SKR tends to a non-zero value almost independent on distance. This situation would be more complex when Eve can move her aperture around or has access to multiple apertures, which would be discussed in the following work.

4. Conclusion

We have analyzed SKR lower bounds for two realistic scenarios for free-space satellite-to-satellite secure communication and shown their performance with respect to relevant channel parameters. In exclusion zone scenario, by enlarging the exclusion zone area we can relax the need for high frequency in long distance transmission. In limited-size aperture scenario, we found out that when Bob's aperture is comparable to Eve's we can get a distance independent SKR at a large transmission distance.

Acknowledgement

This paper was supported in part by MURI ONR, NSF, and GD. The authors thankfully acknowledge helpful discussions with Saikat Guha, Kaushik Seshadreesan from the University of Arizona, Jeffrey Shapiro from Massachusetts Institute of Technology and Mark R. Adcock from General Dynamics.

References

1. M. Toyoshima, *Journal of Optical Networking*, vol. 4, no. 6, pp. 300–311, 2005.
2. S.-K. Liao *et al.*, *Nature*, vol. 549, no. 7670, p. 43, 2017.
3. Z. Pan *et al.*, *arXiv preprint arXiv:1903.03136*, 2019.
4. ——, in *2019 IEEE International Symposium on Information Theory (ISIT)*, July 2019, pp. 3032–3036.
5. J. Shapiro *et al.*, *Journal of Optical Networking*, vol. 4, no. 8, pp. 501–516, 2005.
6. V. Giovannetti *et al.*, *Quantum Information & Computation*, vol. 4, no. 6, pp. 489–499, 2004.
7. G. B. Rybicki *et al.*, *Radiative processes in astrophysics*. John Wiley & Sons, 2008.