Security of satellite-based CV-QKD under realistic assumptions

Ziwen Pan and Ivan B. Djordjevic
The University of Arizona, Tucson, AZ 85721
e-mail: ziwenpan@email.arizona.edu

ABSTRACT
With the vastly growing need for secure communication, quantum key distribution (QKD) has been developed to provide high security for communications against potential attacks from the fast-developing quantum computers. Among different QKD protocols, continuous variable (CV-) QKD employing Gaussian modulated coherent states has been promising for its complete security proof and its compatibility with current communication systems in implementation with homodyne or heterodyne detection. Since satellite communication has been more and more important in developing global communication networks, there have been concerns about the security in satellite communication and how we should evaluate the security of CV-QKD in such scenarios. To better analyse the secure key rate (SKR) in this case, in this invited paper we investigate the CV-QKD SKR lower bounds under realistic assumptions over a satellite-to-satellite channel. We also investigate the eavesdropper's best strategy to apply in these scenarios. We demonstrate that for these channel conditions with well-chosen carrier centre frequency and receiver aperture size, based on channel parameters, we can optimize SKR correspondingly. The proposed satellite-based QKD system provides high security level for the coming 5G and beyond networks, the Internet of things, self-driving cars, and other fast-developing applications.
Keywords: quantum key distribution, satellite-based communication

1. INTRODUCTION

Theoretically quantum cryptography can ensure unconditional informational security in physical layer. In 1984 the first quantum key distribution (QKD) scheme was developed in [1] by Charles Bennett and Gilles Brassard and its security is based on no-cloning theorem and one-time pad encryption. This was the starting point for discrete variable QKD (DV-QKD) where single photons are transmitted, which puts forward rigorous conditions for realistic implementations while providing security, and various protocols have since been proposed [10-12].

Nowadays people have been working to implement QKD in realistic application scenarios and thus continuous variable QKD (CV-QKD) has become an attractive field thanks to its compatibility with existing communication systems, e.g., protocols based on coherent laser light and heterodyne detection [2,3]. However, most security analysis of QKD has assumed that the eavesdropper (Eve) has access to any operation that is allowed by physics law, which is not the case under realistic circumstances. In our recent papers [4,5] we have shown the security analysis of realistic secret key distillation scheme with certain restrictions to Eve's collecting ability by performing achievable rate calculation. Such restrictions are widely applicable in communication systems, for example the finite aperture size of Eve's receiver would limit her collection ability in wireless communication.

In recent years, since the work on satellite-to-ground QKD in 2017 [6], interests have been rising surrounding free-space secret key distillation for satellites. However, various realistic scenarios including those with spy satellites haven't been thoroughly studied from security point of view. Thus, in this invited paper we investigate three typical scenarios where eavesdropper's (Eve's) collecting ability is considered. In Sec. 2, we introduce and analyse the so-called "exclusion zone" scenario where Eve cannot eavesdrop without alerting the communicating parties in certain region near the legitimate receiver (Bob). Then in Sec. 3.1 we study the scenario where Eve's collecting ability is limited by the size of her aperture. In Sec. 3.2 we analyse the eavesdropper's (Eve's) optimal positioning behind Bob's aperture. In these sections we provide lower bounds on achievable secure key rate (SKR) without specifying the detection scheme for Bob. We show that an exclusion zone can mitigate the need for higher centre frequency in transmission. We demonstrate that a constant secure key rate lower bound independent of transmission distance can be achieved when Eve has a limited sized aperture and positions it in the same plane with Bob. We also show that Eve's position can be optimized especially when she is relatively close to Bob, which suggests that simple strategies such as setting an exclusion zone around legitimate satellites can be very useful against eavesdropping activity. It is demonstrated that significantly higher SKR lower bounds can be achieved compared to traditional unrestricted Eve scenario.

2. EXCLUSION ZONE ANALYSIS

In this section we evaluate the first scenario as is illustrated in Fig. 1, where we assume that the area of transmitter aperture is A_a and the area of receiver aperture as A_b with the area of so-called "exclusion zone" denoted as A_{ex}. The "exclusion zone" here means that Eve cannot collect photons in this zone without being noticed by Alice and Bob. 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.

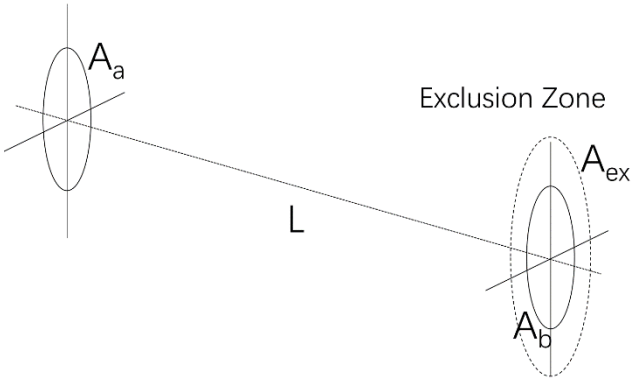

Figure 1. Exclusion zone scenario geometric setup. The Alice-to-Bob transmission distance is denoted as L. The transmitting aperture (Alice) area is denoted as A_a and the receiving aperture (Bob) area is denoted as A_b is. A_{ex} is the exclusion zone area which is a circular area centred at Bob's aperture.

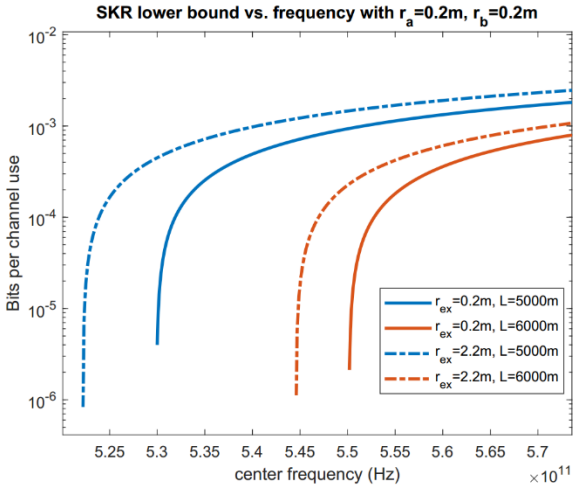

Figure 2. SKR lower bound vs. centre frequency for different exclusion zones and transmission distances.

According to some similar analysis in [7,8], if the frequency used ω is restricted to $0 \le \omega \ll \omega_0 = 2\pi cL/\sqrt{A_a A_b}$, then the Alice-to-Bob transmissivity η at frequency ω is $\eta(\omega) = \left(\frac{\omega}{\omega_0}\right)^2 \ll 1$. Thus, we have:

$$\omega_0 = 2\pi\, cL/\sqrt{A_a A_b}, \tag{1}$$

$$\eta(\omega) = \left(\frac{\omega}{\omega_0}\right)^2, \tag{2}$$

$$\omega_{0Ex} = 2\pi\, cL/\sqrt{A_a A_{ex}}, \tag{3}$$

$$\eta_{AEx} = \left(\frac{\omega}{\omega_{0Ex}}\right)^2, \tag{4}$$

$$\eta_{AE} = 1 - \eta_{AEx} = \big(1 - \eta(\omega)\big)\kappa(\omega). \tag{5}$$

Here κ denotes how much power Eve can collect from the part that isn't collected by Bob [4]. The Alice to Eve transmissivity (η_{AE}) can be denoted as $\big(1-\eta(\omega)\big)\kappa(\omega)$ in Eq. (5). We can compute the Alice-to-exclusion zone transmissivity (η_{AEx}) by assuming a virtual receiver covering the entire exclusion zone and substitutes A_b with A_{ex} in Eq. (1) to get ω_{0Ex} in Eq. (3). Then Alice-to-Eve transmissivity (η_{AE}) can be computed as $1 - \eta_{\mathrm{AEx}}$ assuming Eve covers everywhere outside of the exclusion zone, calculated in Eq. (5).

Also, we use the black body radiation function for noise frequency dependence:

$$n_e = \frac{1}{e^{\frac{hf}{kT}} - 1}. \tag{6}$$

where n_e is the mean photon number per mode for the thermal noise, $h = 6.626\times10^{-34}$ m^{2}kg/s is the Planck constant, $k = 1.38064852\times10^{-23}$ m^{2}kg/(Ks^2) is the Boltzmann constant, $T = 3K$ is the estimated space temperature, and f is the centre frequency in Hz that we use in transmission.

Recall from [4] that the lower bound for direct ($K_{\rightarrow}$) and reverse ($K_{\leftarrow}$) reconciliation respectively in a pure loss wiretap channel without transmitting power constraints are given by:

$$\lim_{\mu\to\infty} K_{\rightarrow} \ge \log_2 \frac{\eta}{\kappa(1-\eta)}, \tag{7}$$

$$\lim_{\mu\to\infty} K_{\leftarrow} \ge \log_2 \frac{1}{\kappa(1-\eta)} - \left(\mathrm{g}\left(\frac{1-\eta}{\eta}\right) - \mathrm{g}\left(\frac{(1-\eta)\kappa}{\eta}\right)\right). \tag{8}$$

In Fig. 2 we plot the SKR lower bound versus the transmission centre frequency. Here solid curves denote that no exclusion zone is set ($r_{ex} = r_b$), while the dashed curve is with $r_{ex} = r_b + 2$m. As we can see in Fig. 2, the SKR lower bound increases with increasing frequency assuming that there is no restriction on Eve's aperture size. From the solid curves in Fig. 2 we can conclude that although choosing a higher frequency can always result in higher SKR, this can pose potential challenges to the system design as we need much higher frequency for longer transmission distance. This downside can be mitigated by enlarging the exclusion zone as it effectively decreases Eve's receiving ability, relaxing the need for higher frequency as is illustrated in Fig. 2 with dashed curves.

3. LIMITED APERTURE SIZE ANALYSIS

In this section, different from Sec. 2, we assume limited aperture size for Eve and investigate her strategies in eavesdropping. First, we investigate the straightforward case where her aperture is in the same plane as Bob's in Sec. 3.1. Then we present the case where Eve can move her aperture around behind Bob in Sec. 3.2.

3.1 Eve is in the same plane as Bob

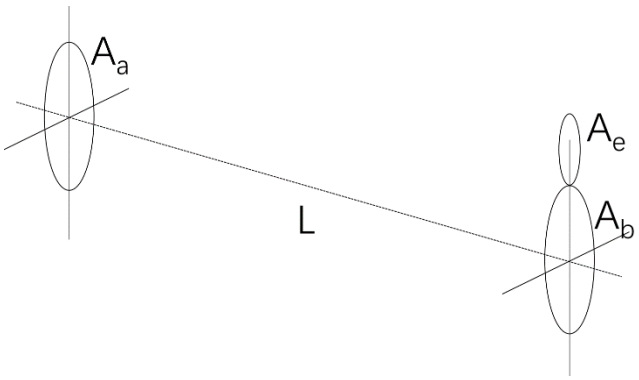

Figure 3. Limited-size aperture scenario geometric setup. A_a and A_b are the transmitting aperture (Alice) area and the receiving aperture (Bob) area respectively. The eavesdropper (Eve) aperture area is A_e which is placed in the same plane as Bob's aperture.

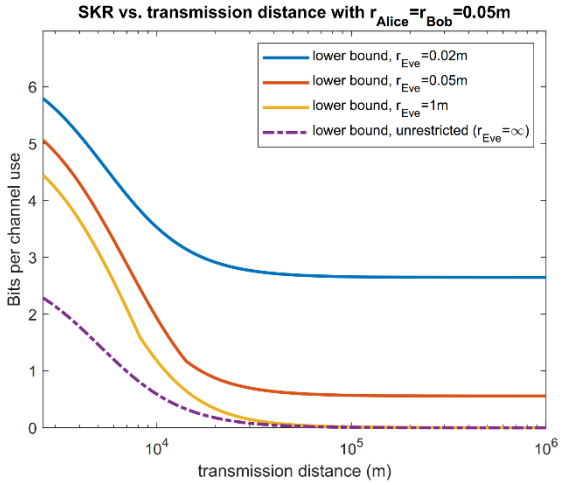

Figure 4. SKR lower bounds vs. distance. Unrestricted Eve's case [4] is also included for comparison purpose.

When Eve's aperture is in the same plane with Bob's, it is easy to see that Eve's optimal strategy is to place her aperture tangential to Bob's, as is illustrated in Fig. 3. Here we assume that Gaussian beam with a total power of P_{total} is transmitted without turbulence and we calculated Bob and Eve's received power (P_{Bob} and P_{Eve}) respectively. Then we can calculate η and κ as below and apply the methods in [4] to give the lower bounds:

$$\eta = \frac{P_{Bob}}{P_{total}}, \tag{9}$$

$$\kappa = \frac{P_{Eve}}{(1-\eta)P_{total}}. \tag{10}$$

In Fig. 4 we plot the SKR lower bounds versus transmission distance with centre wavelength $\lambda = 1550$nm, Gaussian beam waist $W_0 = r_b = r_a = 5$cm. From Fig. 4 we can see that a constant rate can be obtained which doesn't change with increasing transmission distance. The channel condition is close to a pure loss channel ($n_e \approx 0$) in space ($T \approx 3$K) at this wavelength where the SKR would drop to zero as distance goes to infinity assuming that Eve has an infinite size aperture (unrestricted case in Fig. 4). However, the SKR goes to a non-zero constant value as distance goes to infinity if we assume limited aperture size for Eve. This is because when distance is large, the collected power of Bob and Eve will be approximately proportional to their aperture size, which we define as m here:

$$\lim_{L\to\infty} \frac{P_{Eve}}{P_{Bob}} = \lim_{L\to\infty} \frac{\eta_{AE}}{\eta_{AB}} = \frac{A_e}{A_b} = \left(\frac{r_e}{r_b}\right)^2 = m, \tag{11}$$

$$\eta_{AE} = (1-\eta_{AB})\kappa. \tag{12},$$

where η_{AB} and η_{AE} refer to Alice-to-Bob and Alice-to-Eve transmissivity, respectively.

Relating to Eqs. (7) and (8), this would return a constant SKR lower bound as η_{AB} goes to zero (transmission distance L goes to infinity):

$$\lim_{\mu\to\infty, L\to\infty} K_{\rightarrow} \geq -\log_2 m, \tag{13}$$

$$\lim_{\mu\to\infty, L\to\infty} K_{\leftarrow} \geq -\log_2\left(\left(\frac{m}{1+m}\right)^{1+m} e\right). \tag{14}$$

3.2 Eve is behind Bob with dynamic positioning

In this section we investigate Eve's optimal positioning behind Bob's aperture plane and give a lower bound on SKR. An extension of this section's results has been accepted to 2020 OSA Advanced Photonics Congress [9]. As is illustrated in Fig. 5, we assume that A_a is the area of transmitter aperture (Alice), A_b is the area of receiver aperture (Bob), and A_e is the area of eavesdropper aperture (Eve). The transmission distance between Alice's aperture plane and Bob's aperture plane is L_{AB} and the distance between Bob's aperture plane and Eve's aperture plane is L_{BE}. Here D is the distance between the centre of Eve's aperture and the beam propagation axis. Gaussian beam is also assumed to be transmitted with beam waist equal to transmitter aperture radius. We will use D as Eve's position since Gaussian beam is cylindrical symmetric along the propagation path.

As we can see in Fig. 6, the SKR doesn't increase when we increase the distance between Bob and Eve since Eve adapts her position accordingly. Here we also include the scatter plots of Eve's optimal position $D_{optimal}$ as a function of L_{BE}. We can see that Eve's adapting her position only gives her advantages for a short distance after Bob's aperture whereas her optimal position stays aligned with Alice and Bob when L_{BE} is sufficiently large.

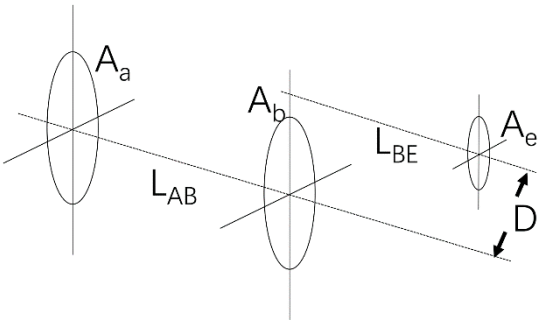

Figure 5. Geometric setup when Eve is behind Bob with dynamic positioning. A_a, A_b and A_e are the transmitting aperture (Alice) area the receiving aperture (Bob) area and the eavesdropper (Eve) aperture area respectively. L_{AB} is the transmission distance between Alice and Bob. L_{BE} is the distance between Bob's aperture plane and Eve's whereas D is the distance between Eve's aperture center and Alice-to-Bob line-of-sight transmission path.

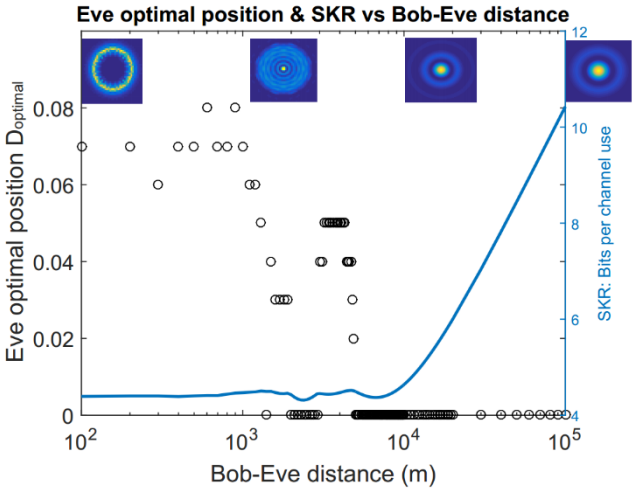

Figure 6. SKR & Eve optimal position versus L_{BE}. Here the radius of Alice aperture, Bob aperture and Eve aperture are all set to 0.1m. Plots of beam wavefront at different L_{BE} are also provided. Here L_{AB} is taken as 1km.

4. CONCLUSIONS

In this paper, we have analysed SKR lower bounds for realistic free-space satellite-to-satellite communication scenarios and studied 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 Eve is in the same plane with Bob, we can get a distance independent on SKR at a sufficiently large transmission distance if Bob's aperture is greater than or at least comparable to Eve's. When Eve can optimize her position to gain advantages, simple approaches such as setting an exclusion zone around Bob's receiver could be very effective to ensure higher security.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] Bennett, Charles. H., and Gilles Brassard. "Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing." (1984).
[2] Laudenbach, Fabian, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Advanced Quantum Technologies 1.1 (2018): 1800011.
[3] Diamanti, Eleni, and Anthony Leverrier. Entropy 17.9 (2015): 6072-6092.
[4] Pan, Ziwen, Kaushik P. Seshadreesan, William Clark, Mark R. Adcock, Ivan B. Djordjevic, Jeffrey H. Shapiro, and Saikat Guha. arXiv preprint arXiv:1903.03136 (2019).
[5] Pan, Ziwen, Kaushik P. Seshadreesan, William Clark, Mark R. Adcock, Ivan B. Djordjevic, Jeffrey H. Shapiro, and Saikat Guha. In 2019 IEEE International Symposium on Information Theory (ISIT), pp. 3032-3036. IEEE, 2019.
[6] Liao, Sheng-Kai, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin et al. Nature 549.7670 (2017): 43-47.
[7] Shapiro, Jeffrey, Saikat Guha, and Baris Erkmen. Journal of Optical Networking 4.8 (2005): 501-516.
[8] Giovannetti, Vittorio, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Jeffrey H. Shapiro, Brent J. Yen, and Horace P. Yuen. Quantum Information & Computation 4.6 (2004): 489-499.
[9] Pan, Ziwen, John Gariano and Ivan B. Djordjevic. Signal Processing in Photonic Communications. Optical Society of America, 2020. Forthcoming on 2020 OSA Advanced Photonics Congress.
[10] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. Physical review letters 89, no. 3 (2002): 037902.
[11] Pan, Ziwen, Jiarui Cai, and Chuan Wang. International Journal of Theoretical Physics 56, no. 8 (2017): 2622-2634.
[12] Hwang, Won-Young. Physical Review Letters 91, no. 5 (2003): 057901.