Secret Key Distillation over Satellite-to-satellite Free-space Channel with Eavesdropper Dynamic Positioning

Ziwen Pan, John Gariano, Ivan B. Djordjevic
University of Arizona, Tucson, AZ 85721, USA
ziwenpan@email.arizona.edu

Abstract: In this paper, the satellite-to-satellite secret-key-rate lower bounds are determined for a realistic scenario where the eavesdropper has a limited size aperture. We also investigate eavesdropper's optimal eavesdropping position with respect to Bob.

OCIS codes: 060.5565 Quantum communications, 060.2605 Free-space optical communication

1. Introduction

In recent years, satellite communication has become more and more important with the fast development in communication and network applications such as 5G communications [1], Internet of things (IOT) [2], etc [3]. Given that security in these communication systems is increasingly important, interests have been rising surrounding free-space-optics (FSO) secret key distillation for satellites since the work on satellite-to-ground quantum key distribution (QKD) in 2017 [4]. However the security analysis for satellite-based secret key distillation hasn't been thoroughly studied especially when spy satellites are in the picture. As a continuation of our previous work where the eavesdropper is in the same plane with Bob, in this paper we study the case where the eavesdropper is behind Bob and can dynamically change her position.

In this paper we are going to first analyze the eavesdropper's (Eve's) optimal positioning behind Bob's aperture and provide a lower bound on secure key rate (SKR). Then we will fix Eve's position aligned with Alice and Bob, which is the optimal position when Bob-to-Eve distance is large. We will show how Eve can gain advantage by dynamical positioning, especially when she is close to Bob. This poses some simple but useful strategies against such as setting an exclusion zone around legitimate satellites.

2. Dynamic vs Static Positioning of the Eavesdropper

In this section we evaluate Eve's optimal positioning and give a lower bound on SKR. As is illustrated in Fig. 1, we assume that the area of transmitter aperture (Alice) is A_t, the area of receiver aperture (Bob) is A_r, and the area of eavesdropper aperture (Eve) is A_e. L_{AB} is the transmission distance between Alice's aperture plane and Bob's aperture plane and L_{BE} is the distance between Bob's aperture plane and Eve's aperture plane. Here D denotes the distance between the center of Eve's aperture and the beam propagation axis. We also assume that Gaussian beam has been transmitted with beam waist equal to transmitter aperture radius. Since Gaussian beam is cylindrical symmetric along the propagation path, we will use D as Eve's position.

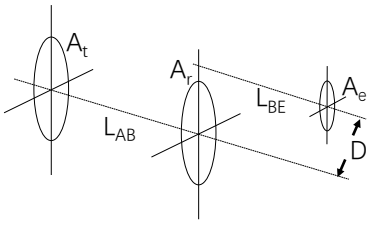

Fig. 1: Geometric setup of the eavesdropper dynamic positioning scenario. Here we use A_t to denote the transmitting aperture (Alice) area, A_r to denote receiving aperture (Bob) area and A_e to denote eavesdropper aperture (Eve) area. L_{AB} is the transmission distance between Alice and Bob and L_{BE} is the distance between Bob's aperture plane and Eve's aperture plane.

We use Rayleigh-Summerfeld transfer function in our simulation of the beam propagation. Since the transmission is in space, for thermal noise frequency dependence we can use the black body radiation equation: $n_e = \frac{1}{e^{h*f/(k*T)}-1}$. Here n_e is the mean photon number of noise thermal state, h is the Planck constant, k is the Boltzmann constant, T is the environmental Kelvin temperature and f is the center frequency we use. We take $T = 3$K, center wavelength $\lambda = 1550$nm, $L_{AB} = 1$km and summarize the simulation results in Fig. 2. The SKR calculation is based on the method developed in [5, 6].

As we can see in Fig. 2, the SKR doesn't increase when we increase the distance between Bob and Eve, which represents a problem for Eve since transmission loss would diminish Eve's collecting ability. This downside can

be mitigated by Eve dynamically adapting her position. Here we also include the scatter plot of Eve's optimal position $D_{optimal}$ as a function of L_{BE}. We can see that although for a short distance after Bob's aperture it is possible for Eve to collect more photons moving away from the propagation axis, when L_{BE} is large enough, Eve's optimal position remains aligned with Alice and Bob and the SKR starts to increase. This is due to the fact that the beam after Bob's aperture is a truncated Gaussian beam with a circular void at its center. This beam starts to reconverge to its center because of diffraction. In Fig. 2 we also provided the insets of the beam wavefront with $L_{BE} = 100$m, 10^3m, 10^4m and 10^5m. We can see that the wavefront with $L_{BE} = 100$m still mimics the shape of a truncated Gaussian whereas the wavefront with $L_{BE} = 10^3$m already starts to reconverge. When $L_{BE} = 10^4$m and $L_{BE} = 10^5$m the beam wavefront is already reconverged and stable, thus the optimal position of Eve remains aligned with Alice and Bob. This is even more clear when we align Eve's position with Alice and Bob ($D = 0$) in

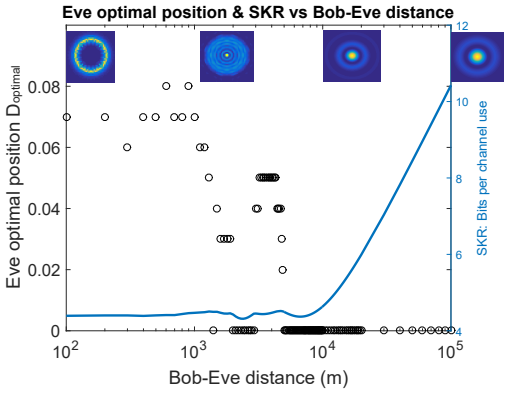

Fig. 2: Eve optimal position & SKR versus L_{BE}. The radius of Alice, Bob and Eve aperture are all taken as 0.1 m. Beam wavefront plots at different L_{BE} are also provided.

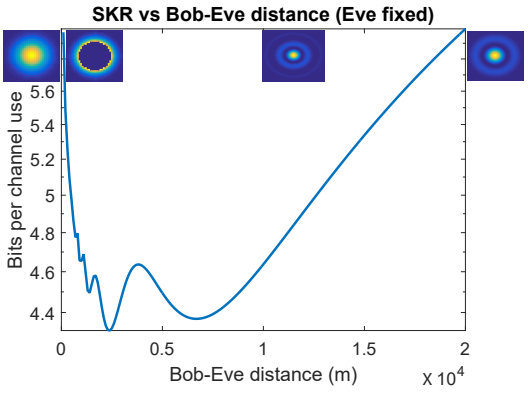

Fig. 3: SKR versus L_{BE}. Here the radius of Alice aperture, Bob aperture and Eve aperture are all taken as 0.1m. Plots of beam wavefront at different L_{BE} are also provided.

Fig. 3. We can see that the SKR first decreases up to the certain distance and then increases with some oscillations. This means that Eve's received power first increases and then decreases with increasing L_{BE}. By comparing Fig. 2 and Fig. 3 we can see that Eve can get advantages by optimizing her eavesdropping aperture position.

3. Conclusion

We have analyzed SKR lower bounds for realistic scenarios over FSO satellite-to-satellite channel where Eve can optimize her position to gain an advantage when she is close to Bob. This actually suggests that simple measures such as setting an exclusion zone around Bob's receiver could be very effective to ensure higher security.

Acknowledgement

This paper was supported by NSF under grants 1907918 and 1828132. The authors thankfully acknowledge helpful discussions with Saikat Guha, Kaushik Seshadreesan from the University of Arizona, Jeffrey Shapiro from Massachusetts Institute of Technology and William Clark, Mark R. Adcock from General Dynamics.

References

1. X. Lin *et al.*, *arXiv preprint arXiv:1903.11219*, 2019.
2. M. De Sanctis *et al.*, *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 113–123, 2015.
3. M. Toyoshima, *Journal of Optical Networking*, vol. 4, no. 6, pp. 300–311, 2005.
4. S.-K. Liao *et al.*, *Nature*, vol. 549, no. 7670, p. 43, 2017.
5. Z. Pan *et al.*, *arXiv preprint arXiv:1903.03136*, 2019.
6. ——, in *2019 IEEE International Symposium on Information Theory (ISIT)*, July 2019, pp. 3032–3036.