

Prefixed-Threshold Real-Time Selection for Free-Space Sending-or-Not Twin-Field Quantum Key Distribution

Yang Yu ¹, Rui Xu ¹, Le Wang ¹, Qianping Mao ^{2,3} and Shengmei Zhao ^{1,3,*}

¹ Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications (NUPT), Nanjing 210003, China; 2021010209@njupt.edu.cn (Y.Y.); 1318014614@njupt.edu.cn (R.X.); lewang@njupt.edu.cn (L.W.)

² College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China; maoqp1@njtech.edu.cn

³ Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing 210003, China

* Correspondence: zhaosm@njupt.edu.cn

Abstract: As a variant of the twin-field quantum key distribution (TF-QKD), the sending-or-not twin-field quantum key distribution (SNS TF-QKD) is famous for its higher tolerance of misalignment error, in addition to the capacity of surpassing the rate–distance limit. Importantly, the free-space SNS TF-QKD will guarantee the security of the communications between mobile parties. In the paper, we first discuss the influence of atmospheric turbulence (AT) on the channel transmittance characterized by the probability distribution of the transmission coefficient (PDT). Then, we present a method called prefixed-threshold real-time selection (P-RTS) to mitigate the interference of AT on the free-space SNS TF-QKD. The simulations of the free-space SNS TF-QKD with and without P-RTS are both given for comparison. The results showed that it is possible to share the secure key by using the free-space SNS TF-QKD. Simultaneously, the P-RTS method can make the free-space SNS TF-QKD achieve better and more stable performance at a short distance.

Keywords: sending-or-not twin-field quantum key distribution; free-space quantum key distribution; prefixed-threshold real-time selection; observable model



Citation: Yu, Y.; Xu, R.; Wang, L.; Mao, Q.; Zhao, S. Prefixed-Threshold Real-Time Selection for Free-Space Sending-or-Not Twin-Field Quantum Key Distribution. *Entropy* **2022**, *24*, 344. <https://doi.org/10.3390/e24030344>

Academic Editors: Rosario Lo Franco and Xiang-Bin Wang

Received: 10 January 2022

Accepted: 25 February 2022

Published: 27 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Even with a malicious third party, Eve, the quantum key distribution (QKD) can provide theoretically secure secret keys between two legitimate users, Alice and Bob, based on the mechanics of quantum physics. The first QKD protocol named BB84 was proposed in 1984 by Bennett and Brassard [1]. Ever since then, plenty of QKD protocols, such as decoy-state QKD protocols [2–4], measurement-device-independent quantum key distribution (MDI-QKD) protocols [5–10], round-robin differential-phase-shift quantum key distribution (RRDPS-QKD) protocols [11–13], etc., have been proposed to overcome the obstacles in the QKD's development.

When the TF-QKD was announced in 2018 [14], it broke the PLOB bound [15], held for all the previous QKD protocols without quantum repeaters. This work altered the relationship between the secure key rate (SKR) and the channel loss from linear dependence to square dependence. It was shown that the transmission distance was greatly enlarged in comparison to those existing protocols under the same circumstance. Inspired by the TF-QKD, a series of the twin-field-like protocols was presented [16–19], where the sending-or-not (SNS) TF-QKD stands out for its high tolerance of misalignment error in the QKD procedure [20–26].

Recently, the QKD through free-space channels has become a hot topic, since it allows the users to communicate on mobile platforms, which is inconvenient for optical fiber quantum communication. It became more attractive when the Micius quantum experiment

science satellite was launched [27,28]. Furthermore, it allows users to realize not only satellite-to-ground communications, but also communications on any mobile platforms via water and air. Compared with the other TF-QKD, the SNS TF-QKD has higher tolerance of misalignment error. There has already been an experimental demonstration of the SNS TF-QKD over a 509 km-long ultra-low loss optical fiber [29], which provided the implementation feasibility of the SNS TF-QKD in wire communication. However, a major obstacle of the free-space QKD is the interference caused by atmospheric turbulence (AT), where the channel transmittance is varied with time, not as the channel transmittance as a constant in fiber communications.

To deal with the channel transmittances fluctuating with time, some methods have been proposed [30,31]. One is to monitor the real-time channel transmittances, optimize a threshold according to the recorded transmittance during the post-processing, and use it to discard all the rounds whose the transmittance is less than a threshold. However, this demands storage requirements for Bob and optimization calculation. In 2018, Lo et al. modified the idea and proposed a new method, called prefixed-threshold real-time selection (P-RTS), to prefix the threshold even before the experiment begins and used it to select the real-time signals [32]. In 2019, they further extended the idea from the one-way QKD protocol to a two-way QKD protocol [33]. The sending-or-not (SNS) TF-QKD is in principle a two-way QKD protocol, which makes the method applicable to it.

In this paper, we first present the mathematical model of the free-space channel and the characteristic of the channel transmittances. Then, we demonstrate the observable model and applied it to the SNS TF-QKD. After that, the function of the asymmetric SNS TF-QKD protocol versus channel transmittances η_a and η_b is presented. Furthermore, the SKR function $R(\eta_a, \eta_b)$ was plotted out in order to determine the domain where the signals were selected. Finally, some numerical simulations are given based on the observable model to analyze the performance of the free-space SNS TF-QKD under AT, with and without the P-RTS method.

2. Prefixed-Threshold Selection for the Free-Space SNS TF-QKD

2.1. Free-Space Channel Model

The channel transmittance η , which fluctuates with time, is one of the free-space channel's major characteristics, which is caused by AT. Such a characteristic can lead to a time-varying SKR. That is, the SKR may be low at some time points. It was discussed how the phase-matching quantum key distribution's SKR decreases greatly in the free space [34]. One solution is post-selecting signals based on the monitored channel transmittance. Therefore, the model of the free-space channel is required in order to mathematically describe the SKR performance of the free-space protocols with and without transmittance post-selection.

The time-varying transmittance η follows a probability distribution of the transmission coefficient (PDTC). There exist multiple models to describe the PDTC. Among those models, the log-normal model is widely used [35], which can be described as,

$$p_{\eta_0, \sigma}(\eta) = \frac{1}{\sqrt{2\pi\sigma\eta}} e^{-\frac{[\ln(\frac{\eta}{\eta_0}) + \frac{1}{2}\sigma^2]^2}{2\sigma^2}} \quad (1)$$

where p denotes the probability density, η_0 represents the expected atmospheric transmittance, and σ is the variance determined by the amount of turbulence and usually takes a value between zero and one. η_0 and σ are the intrinsic parameters of the channel and, thus, contain all the information of the PDTC.

After applying the post-selection of η with a threshold η_T and using the expected value formula for a truncated distribution, one can obtain a higher mean transmittance among the selected signals as,

$$\langle \eta \rangle = \frac{\int_{\eta_T}^1 \eta p_{\eta_0, \sigma}(\eta) d\eta}{\int_{\eta_T}^1 p_{\eta_0, \sigma}(\eta) d\eta}. \quad (2)$$

Assume the two channels in the SNS TF-QKD protocol (Alice to Charlie and Bob to Charlie) are free-space channels and the fluctuations of their transmittances can be described by the log-normal model. Owing to the assumption that the two channels are separate and independent, the joint PDTC can be written as [33],

$$p_{AB}(\eta_a, \eta_b) = p_{\eta_{A_0}, \sigma_A}(\eta_a) \cdot p_{\eta_{B_0}, \sigma_B}(\eta_b), \tag{3}$$

where (η_{A_0}, σ_A) and (η_{B_0}, σ_B) are the condition parameters of the two channels, respectively. The two variables η_a and η_b form a plane on which the joint PDTC is defined.

Since Charlie can post-select signals by observing both channels' transmittances, the threshold is actually extended to two dimensions, namely an area in the plane defined by (η_a, η_b) [33]. Thus, a double-integral should be performed in order to obtain the expected values of the transmittances η_a or η_b , that is,

$$\langle \eta_x \rangle = \frac{\int \int_{\Omega} \eta_x p_{AB}(\eta_a, \eta_b) d\eta_a d\eta_b}{\int \int_{\Omega} p_{AB}(\eta_a, \eta_b) d\eta_a d\eta_b}, x \in \{a, b\}. \tag{4}$$

where Ω is the domain in which the signals are selected. The simplest way to describe such a domain is,

$$\Omega^{square} = \{(\eta_a, \eta_b) | \eta_{T_A} \leq \eta_a \leq 1, \eta_{T_B} \leq \eta_b \leq 1\}. \tag{5}$$

2.2. Free-Space SNS TF-QKD Based on Asymmetric Transmittance

Considering the fact that the users can only obtain the corresponding counts and error counts and use them to calculate the overall gain and quantum bit-error rate throughout the whole experiment and the two channels' transmittances are asymmetric, the observable model proposed in [33] was adopted to calculate the SKR of the free-space SNS TF-QKD, that is:

$$\begin{aligned} R_{SNS}^{Observable} &= R[\langle Q^Z \rangle, \langle EQ^Z \rangle, \langle Q_d^X \rangle, \langle EQ_d^X \rangle], \\ \langle Q \rangle &= \frac{\int \int_{\Omega} [Q(\eta_a, \eta_b) \cdot p_{AB}(\eta_a, \eta_b)] d\eta_a d\eta_b}{\int \int_{\Omega} p_{AB}(\eta_a, \eta_b) d\eta_a d\eta_b}, \\ \langle EQ \rangle &= \frac{\int \int_{\Omega} [EQ(\eta_a, \eta_b) \cdot p_{AB}(\eta_a, \eta_b)] d\eta_a d\eta_b}{\int \int_{\Omega} p_{AB}(\eta_a, \eta_b) d\eta_a d\eta_b}. \end{aligned} \tag{6}$$

Here, the superscripts Z and X respectively represent the Z-window (both users choose a signal window) and the X-window (both users choose a decoy window with other conditions met) in the SNS TF-QKD. The subscript $d \in \{v, w, 0\}$ denotes the intensities of light that they choose in different X-windows.

It should be noted that since the transmittances of the two channels' are not the same in most cases, the method of calculating the original SNS TF-QKD's SKR [20] is no longer suitable. Since the only asymmetric parameters considered in this work are channel transmittances, some simplifications could be adopted in the formulas for SKR [22]. Under this constraint, the Z-windows' overall gains and quantum-bit errors can be written as the functions of η_a and η_b when other parameters are fixed,

$$\begin{aligned} Q^Z(\eta_a, \eta_b) &= (1 - \epsilon)^2 Y_0 + 2\epsilon^2 (1 - P_d) e^{-\frac{\eta_a + \eta_b}{2} \mu} \cdot [1 - (1 - P_d) e^{-\frac{\eta_a + \eta_b}{2} \mu}] \\ &\quad + 2\epsilon(1 - \epsilon)(1 - P_d) \{e^{-\frac{\eta_a}{2} \mu} [1 - (1 - P_d) e^{-\frac{\eta_a}{2} \mu}] + e^{-\frac{\eta_b}{2} \mu} [1 - (1 - P_d) e^{-\frac{\eta_b}{2} \mu}]\}, \\ EQ^Z(\eta_a, \eta_b) &= (1 - \epsilon)^2 Y_0 + 2\epsilon^2 (1 - P_d) e^{-\frac{\eta_a + \eta_b}{2} \mu} \cdot [1 - (1 - P_d) e^{-\frac{\eta_a + \eta_b}{2} \mu}], \end{aligned} \tag{7}$$

where $Y_0 = 2P_d(1 - P_d)$ is the yield of the zero-photon, P_d is the dark count rate, and ϵ is the probability of a user sending the signal state in a Z-window.

In the SNS TF-QKD protocol, each user should add a random continuous phase $\delta_a(\delta_b)$ to their states. If the conditions below are satisfied in the same round: (1) both users determine a decoy window; (2) their chosen intensities happen to be the same; (3) their

added phases meet the criterion during the post-selection: $|\delta_a - \delta_b - m\pi| \leq \frac{2\pi}{M}$, where $m = 0, 1$ and M is the number of phase slices the users predetermine to divide the phase interval $[0, 2\pi)$ into; (4) only one detector clicks, then that time window is called an effective X-window, and the formulas of its corresponding overall gain and quantum-bit error can be listed as functions of four parameters,

$$\begin{aligned}
 Q_d^X(\eta_a, \eta_b, \delta_a, \delta_b) &= (1 - P_d)e^{-\frac{\eta_a + \eta_b}{2}d} [e^{-\cos(\delta_a - \delta_b)\sqrt{\eta_a\eta_b}d} + e^{\cos(\delta_a - \delta_b)\sqrt{\eta_a\eta_b}d}] \\
 &\quad - 2(1 - P_d)^2e^{-(\eta_a + \eta_b)d}, \\
 EQ_d^X(\eta_a, \eta_b, \delta_a, \delta_b) &= (1 - P_d)e^{-\frac{\eta_a + \eta_b}{2}d - \cos(\delta_a - \delta_b)\sqrt{\eta_a\eta_b}d} - 2(1 - P_d)^2e^{-(\eta_a + \eta_b)d}.
 \end{aligned}
 \tag{8}$$

Since both δ_a and δ_b are continuous, the probability of their difference strictly equaling zero or π will tend to zero, and this situation together with the asymmetric channel transmittances and the optical system’s misalignment error E_d will cause an optical system error $\frac{1 - \cos(\Delta)}{2}$ [23]. Furthermore, such an error can be equivalently considered as the consequence of an extra phase difference $\Delta = \arccos(1 - 2E_{sys}) = \frac{\sqrt{\eta_a\eta_b}d}{(\eta_a + \eta_b)d}(1 - 2E_d)$ [22]. Furthermore, as can be seen, the above equations can be treated as functions of δ_a and δ_b . One more step of integrating is needed to obtain the average overall gains and quantum-bit errors,

$$\begin{aligned}
 Q_d^X(\eta_a, \eta_b) &= \frac{M^2}{4\pi^2} \int_{\Delta}^{\Delta + \frac{2\pi}{M}} \int_0^{\frac{2\pi}{M}} Q_d^X(\eta_a, \eta_b, \delta_a, \delta_b) d\delta_a d\delta_b, \\
 EQ_d^X(\eta_a, \eta_b) &= \frac{M^2}{4\pi^2} \int_{\Delta}^{\Delta + \frac{2\pi}{M}} \int_0^{\frac{2\pi}{M}} EQ_d^X(\eta_a, \eta_b, \delta_a, \delta_b) d\delta_a d\delta_b.
 \end{aligned}
 \tag{9}$$

Now that the X-windows’ and Z-windows’ overall gains and quantum-bit errors have been introduced, the model mentioned above can finally be applied to calculate these parameters in the free space with and without the P-RST method. After all these been performed, the SKR can be calculated as [20],

$$\begin{aligned}
 R_{SNS}^{Observable}(\Omega) &= \int \int_{\Omega} R[\langle Q^Z \rangle, \langle EQ^Z \rangle, \langle Q^X \rangle, \langle EQ^X \rangle] \cdot p_{AB}(\eta_a, \eta_b) d\eta_a d\eta_b \\
 R &= 2\epsilon(1 - \epsilon)\mu e^{-\mu} Y_1^L [1 - H(e_1^U)] - fQ^Z H(E^Z),
 \end{aligned}
 \tag{10}$$

where $E^Z = \frac{EQ^Z}{Q^Z}$ is the Z-windows’ quantum bit-error rate, f is the error correction efficiency factor, $H(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ is the binary entropy, and Y_1^L and e_1^U are respectively the lower and upper bound of the single-photon’s yield and quantum bit-error rate, which can be calculated following a common decoy-state method [20]. Since the observable model should be applied, one should obtain $\langle Q^Z \rangle$, $\langle EQ^Z \rangle$, $\langle Q^X \rangle$ and $\langle EQ^X \rangle$ with Equation (6) and then turn to Equation (10) for the free-space SNS TF-QKD’s SKR with these expectation values.

Note that the normal steps of post-selecting signals based on transmittance are setting a threshold, monitoring each rounds’ real-time channel transmittances, and discarding those less than the threshold. This can be obtained by numerical optimization when the experiment is performed [30,31]. However, the P-RTS method demonstrates a different way. It was firstly proposed in [32]. Due to the fact that the selection threshold is independent of the PDTC and can only be determined by the experimental parameters, the threshold is able to be predetermined before the experiment. Thus, determining the threshold will be the first thing to perform in the next section after plotting out $R(\eta_a, \eta_b)$.

3. Numerical Simulation

The letter Ω in Equation (6) denotes the area, a 2D threshold for the signals’ selection. In order to obtain this area, the key rate function $R(\eta_a, \eta_b)$ should be firstly plotted out. It should be noted that this key rate function is only determined by the signals’ intensities and experimental parameters. We list the experimental parameters such as misalignment

error rate, dark count rate, etc., in Table 1. The signals’ intensities and the probability of the signals being sent or not are given as $u = 0.4, v = 0.01, w = 0.005$, and $\epsilon = 0.02$, and only the infinite data size was considered.

Table 1. The parameters of the numerical simulation.

Parameters	p_d	e_0	e_d	η_d	α	f
Value	1×10^{-10}	0.5	0.15	0.5	0.2	1.1

Figure 1 shows the key rate function of the free-space SNS TF-QKD with asymptotic lines. In Figure 1, the contour, the two asymptotic lines, and the horizontal/vertical tangents of the $R = 0$ contour respectively represent the SKR, the minimum and maximum channel transmittance mismatch $k = \frac{\eta_b}{\eta_a}$ that can be reached, and the minimum channel transmittances.

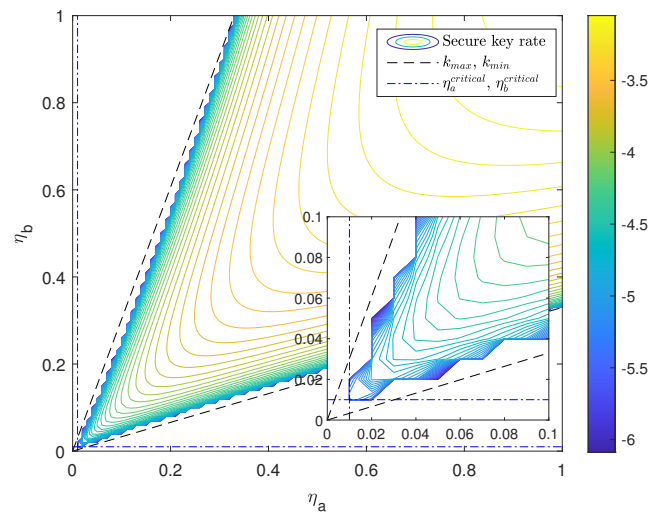


Figure 1. The SNS TF-QKD’s key rate function $R(\eta_a, \eta_b)$ with asymptotic lines, x_{min} and x_{max} , and horizontal/vertical tangents, $\eta_a^{critical}$ and $\eta_b^{critical}$, of the $R = 0$ contour.

Clearly, the most suitable area of the signals’ selection is the domain of Figure 1 where the condition $R(\eta_a, \eta_b) \geq 0$ is satisfied,

$$\Omega^{Selected} = \{(\eta_a, \eta_b) | R(\eta_a, \eta_b) \geq 0\}. \tag{11}$$

However, it may be difficult to directly apply the domain above to the double-integral for the 2D threshold of signals’ selection. For simplicity, a replaced threshold domain, which can play an approximate role in the double-integral, is proposed [33]. The replaced domain is formed by the four lines in Figure 1 and is similar to $\Omega^{Selected}$,

$$\Omega^{Similar} = \{(\eta_a, \eta_b) | \eta_a^{critical} \leq \eta_a \leq 1, \eta_b^{critical} \leq \eta_b \leq 1, k_{min} \leq \frac{\eta_b}{\eta_a} \leq k_{max}\}, \tag{12}$$

where k_{min} and k_{max} are the slope of x_{min} and x_{max} , respectively.

Since the function $R(\eta_a, \eta_b)$ only depends on the experimental parameters and the signals’ intensities, the four lines x_{min} , x_{max} , $\eta_a^{critical}$, and $\eta_b^{critical}$ are all independent of the PDTC of the channels. Thus, this 2D threshold formed by these four lines can be predetermined even before the experiment.

Here, in order to demonstrate the effect of the P-RTS method, the SKR function $R(\eta_a, \eta_b)$ of the free-space SNS TF-QKD with and without the P-RTS method based on the observable model is plotted out in Figures 2 and 3. The parameters in Table 1 are also used in the same way. The variance of the PDTC was set to 0.75. Obviously, the near-hyperbolic

$R = 0$ contour of the function $R(\eta_a, \eta_b)$ without the P-RTS is narrower than that of the function with the P-RTS. In other words, the area of $R(\eta_a, \eta_b) \geq 0$ with the P-RTS method becomes larger, so that the protocol can reach a larger channel transmittance mismatch.

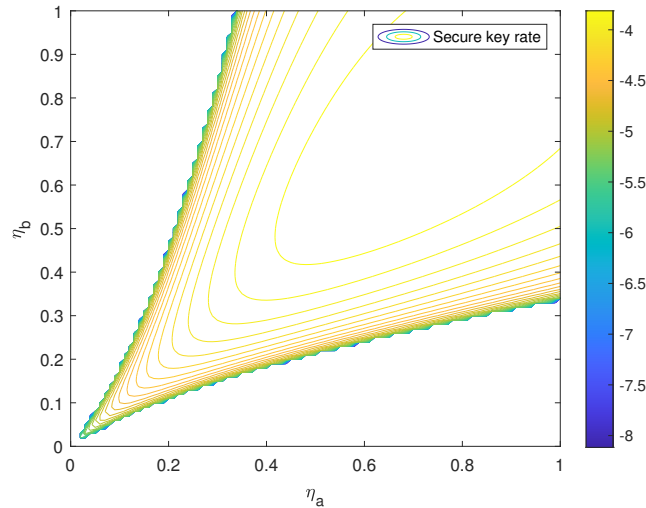


Figure 2. $R(\eta_a, \eta_b)$ without the P-RTS method based on the observable model.

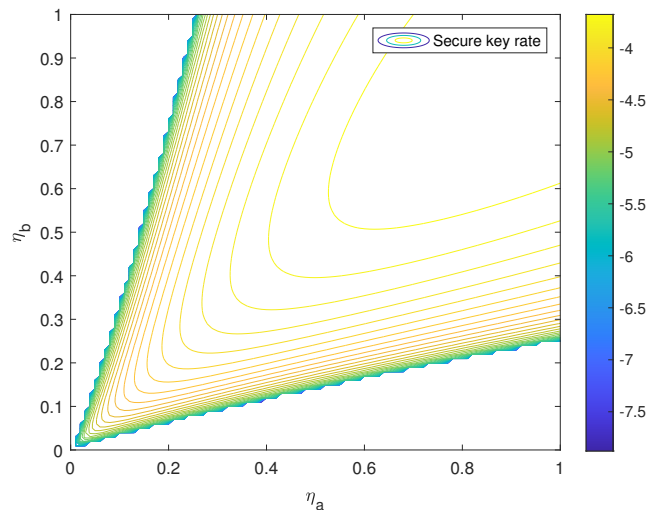


Figure 3. $R(\eta_a, \eta_b)$ with the P-RTS method based on the observable model.

In order to vividly compare the SKR performance of the free-space SNS TF-QKD with and without the P-RTS, we further plotted out the functions versus total transmission distance, i.e., sum of L_{AC} (channel length between Alice and Charlie) and L_{BC} (channel length between Bob and Charlie), with $L_{AC} = L_{BC} + 10$, in Figure 4. The parameters in Table 1 were also used in the same way. The PDTC’s variance was set to 0.75, meaning AT is quite strong. The channel transmission loss rate was assumed to be the same as that of optical fiber, $\alpha = 0.2$ dB/km. The black solid line denotes the PLOB bound in the free space. Based on the ratewise integration model in [32] and Equation (26) in [36], we used Equation (13) as the formula for calculating the PLOB bound in the free space with a certain mean transmittance η_0 , which corresponds to a certain transmission distance,

$$K = \int_0^1 -\log_2(1 - \eta \cdot \eta_d) \cdot p_{\eta_0, \sigma}(\eta) d\eta. \tag{13}$$

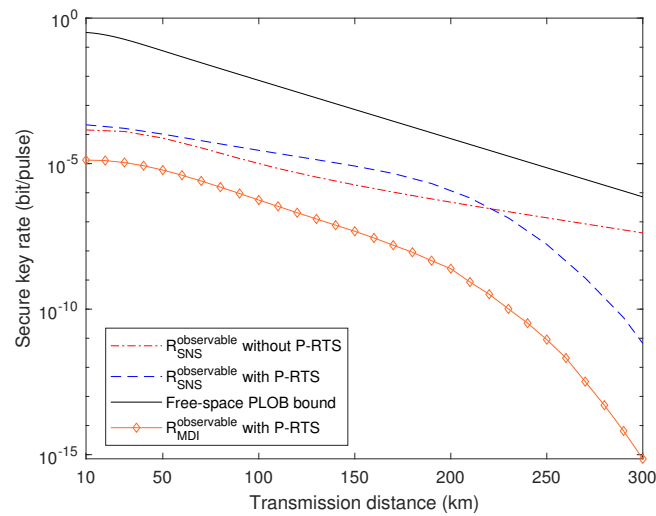


Figure 4. Comparison of the free-space SNS TF-QKD with and without the P-RTS method based on the observable model and the free-space PLOB bound versus the transmission distance.

As can be seen in Figure 4, $R_{SNS}^{observable}$ with the P-RTS has better performance than that without the method when the transmission distance is below around 220 km. The former one drops more sharply than the latter one after 190 km. The reason for this should be that after a certain point, as the channel transmittance increases with the transmission distance, it becomes more difficult to find the experiment round that satisfies the condition of the P-RTS, making the SKR decrease more quickly. Meanwhile, neither of these two can surpass the free-space PLOB bound. The reasons may be that the atmospheric turbulence's effect on the SNS TF-QKD is very large or this free-space PLOB bound we evaluated is not tight enough. The solid line with diamond symbols represents the MDI-QKD with the P-RTS with the misalignment error $e_d = 0.075$ since $e_d = 0.15$ in Table 1 is intolerable for the protocol. One can see that its performance is not as good as that of the SNS-TF QKD with and without the P-RTS.

4. Conclusions

In the paper, we presented a prefixed-threshold selection for the free-space SNS TF-QKD, where we demonstrated the more accurate observable model for the free-space channel to calculate the SKR in the case of AT. Based on the contour of the SKR function $R(\eta_a, \eta_b)$, we can predetermine the $2D$ threshold for the signals' selection. The numerical simulation results showed that it is possible to share a secure key by using the free-space SNS TF-QKD. The results also showed that the free-space SNS QKD protocol with the P-RTS can decrease the influence caused by AT at a short distance, and the performance of the protocol with and without the P-RTS is better than the MDI-QKD with the method, even with larger misalignment error. Thus, our work has some benefits for the free-space SNS TF-QKD in practice.

Author Contributions: Conceptualization, Y.Y.; methodology, Y.Y. and R.X.; software, Y.Y. and R.X.; validation, L.W.; writing—original draft preparation, Y.Y.; writing—review and editing, Y.Y., Q.M., and S.Z.; supervision, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (NSFC) (61871234, 62001249) and the Open Research Fund of the Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), the Ministry of Education (JZNY202104).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
TF-QKD	Twin-field quantum key distribution
SNS TF-QKD	Sending-or-not twin-field quantum key distribution
MDI-QKD	Measurement-device-independent quantum key distribution
RRDPS-QKD	Round-robin differential-phase-shift quantum key distribution
AT	Atmospheric turbulence
P-RTS	Prefixed-threshold real-time selection
PDTC	Probability distribution of the transmission coefficient

References

- Bennet, C. Quantum cryptography: Public key distribution and coin tossing. *arXiv* **2020**, arXiv:2003.06557.
- Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [[CrossRef](#)]
- Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [[CrossRef](#)]
- Wang, X.B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **2005**, *72*, 012322. [[CrossRef](#)]
- Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [[CrossRef](#)]
- Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [[CrossRef](#)]
- Le, W.; Sheng, M.Z.; Long, Y.G.; Wei, W.C. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chin. Phys. B* **2015**, *24*, 120307.
- Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [[CrossRef](#)]
- Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.; Huang, M.Q.; Zhang, W.J.; et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [[CrossRef](#)]
- Cao, Y.; Li, Y.H.; Yang, K.X.; Jiang, Y.F.; Li, S.L.; Hu, X.L.; Abulizi, M.; Li, C.L.; Zhang, W.; Sun, Q.C.; et al. Long-distance free-space measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2020**, *125*, 260503. [[CrossRef](#)]
- Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **2014**, *509*, 475–478. [[CrossRef](#)] [[PubMed](#)]
- Mao, Q.P.; Wang, L.; Zhao, S.M. Plug-and-play round-robin differential phase-shift quantum key distribution. *Sci. Rep.* **2017**, *7*, 15435. [[CrossRef](#)] [[PubMed](#)]
- Nan, R.Z.; Gui, H.Z.; Li, H.G.; San, Q.L. Quantum communication protocol for data link layer based on entanglement. *Acta Phys. Sin.* **2007**, *56*, 5066–5070.
- Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [[CrossRef](#)] [[PubMed](#)]
- Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [[CrossRef](#)]
- Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [[CrossRef](#)]
- Yu, Y.; Wang, L.; Zhao, S.; Mao, Q. Decoy-state phase-matching quantum key distribution with source errors. *Opt. Express* **2021**, *29*, 2227–2243. [[CrossRef](#)]
- Cui, C.; Yin, Z.Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **2019**, *11*, 034053. [[CrossRef](#)]
- Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *Npj Quantum Inf.* **2019**, *5*, 64. [[CrossRef](#)]
- Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [[CrossRef](#)]
- Yu, Z.W.; Hu, X.L.; Jiang, C.; Xu, H.; Wang, X.B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **2019**, *9*, 3080. [[CrossRef](#)] [[PubMed](#)]

22. Zhou, X.Y.; Zhang, C.H.; Zhang, C.M.; Wang, Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. *Phys. Rev. A* **2019**, *99*, 062316. [[CrossRef](#)]
23. Zhang, C.H.; Zhang, C.M.; Wang, Q. Twin-field quantum key distribution with modified coherent states. *Opt. Lett.* **2019**, *44*, 1468–1471. [[CrossRef](#)]
24. Jiang, C.; Yu, Z.W.; Hu, X.L.; Wang, X.B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Appl.* **2019**, *12*, 024061. [[CrossRef](#)]
25. Qiao, Y.; Chen, Z.; Zhang, Y.; Xu, B.; Guo, H. Sending-or-not-sending twin-field quantum key distribution with light source monitoring. *Entropy* **2020**, *22*, 36. [[CrossRef](#)]
26. Xue, K.; Zhao, S.; Mao, Q.; Xu, R. Plug-and-play sending-or-not-sending twin-field quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 320. [[CrossRef](#)]
27. Yin, J.; Cao, Y.; Li, Y.H.; Ren, J.G.; Liao, S.K.; Zhang, L.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **2017**, *119*, 200501. [[CrossRef](#)] [[PubMed](#)]
28. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y.; et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **2018**, *120*, 030501. [[CrossRef](#)]
29. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [[CrossRef](#)]
30. Vallone, G.; Marangon, D.G.; Canale, M.; Savorgnan, I.; Bacco, D.; Barbieri, M.; Calimani, S.; Barbieri, C.; Laurenti, N.; Villoresi, P. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A* **2015**, *91*, 042320. [[CrossRef](#)]
31. Erven, C.; Heim, B.; Meyer-Scott, E.; Bourgoin, J.; Laflamme, R.; Weihs, G.; Jennewein, T. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New J. Phys.* **2012**, *14*, 123018. [[CrossRef](#)]
32. Wang, W.; Xu, F.; Lo, H.K. Prefixed-threshold real-time selection method in free-space quantum key distribution. *Phys. Rev. A* **2018**, *97*, 032337. [[CrossRef](#)]
33. Wang, W.; Xu, F.; Lo, H.K. Prefixed-threshold Real-Time Selection for Free-Space Measurement-Device-Independent Quantum Key Distribution. *arXiv* **2019**, arXiv:1910.10137.
34. Yu, Y.; Wang, L.; Zhao, S.; Mao, Q. Free-Space Phase-Matching Quantum Key Distribution. In Proceedings of the 2021 13th International Conference on Wireless Communications and Signal Processing (WCSP), Changsha, China, 20–22 October 2021; pp. 1–4.
35. Semenov, A.; Vogel, W. Quantum light in the turbulent atmosphere. *Phys. Rev. A* **2009**, *80*, 021802. [[CrossRef](#)]
36. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **2021**, *3*, 013279. [[CrossRef](#)]