entropy

MDPI

Article

The Performance of Satellite-Based Links for Measurement-Device-Independent Quantum Key Distribution

Guoqi Huang [1], Qin Dong [1], Wei Cui [1] and Rongzhen Jiao [1,2,*]

[1] School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China; huangguoqi@bupt.edu.cn (G.H.); dongqin@bupt.edu.cn (Q.D.); cuiwei@bupt.edu.cn (W.C.)
[2] State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: rzjiao@bupt.edu.cn

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) protocol has high practical value. Satellite-based links are useful to build long-distance quantum communication network. The model of satellite-based links for MDI-QKD was proposed but it lacks practicality. This work further analyzes the performance of it. First, MDI-QKD and satellite-based links model are introduced. Then considering the operation of the satellite the performance of their combination is studied under different weather conditions. The results may provide important references for combination of optical-fiber-based links on the ground and satellite-based links in space, which is helpful for large-scale quantum communication network.

Keywords: measurement-device-independent quantum key distribution; satellite-based links; quantum communication network

Citation: Huang, G.; Dong, Q.; Cui, W.; Jiao, R. The Performance of Satellite-Based Links for Measurement-Device-Independent Quantum Key Distribution. *Entropy* **2021**, *23*, 1010. https://doi.org/10.3390/e23081010

Academic Editor: Vladyslav Usenko

Received: 15 July 2021
Accepted: 31 July 2021
Published: 3 August 2021

1. Introduction

Quantum key distribution (QKD) can generate keys to encrypt information. Theoretically, based on quantum mechanics, the security is absolutely guaranteed [1,2]. In 1984, BB84 protocol, the first QKD protocol, was proposed by Bennett [3]. After BB84 protocol was proposed, decades have passed. QKD has much progress [4]. However, due to the imperfect technology, there are some unavoidable security leaks [5–7]. Methods for different leaks are raised [8–10]. In 2012, MDI-QKD protocol was put forward by Lo [11], which can solve the problem of unsafe measurement, and it has been improved [12,13]. It adds an untrust measurement Charlie for bell-state measurement. Besides, Alice and Bob generate keys according to the postelection. In practice we use a weak coherent pulse (WCP) [14] source to emit single photon, whose number of photons obeys Poisson Distribution. So it must have multiphoton part. For this part, there is an attack called photon-number splitting (PNS). In order to solve this problem, decoy-state protocol was proposed and combined with MDI-QKD [15–17]. In this protocol, Alice and Bob can generate different intensities' pulses to hide the real signal states so that no one knows whether it is signal state except senders. Now MDI-QKD protocol with decoy-state is promising. It can communicate in optical-fiber-based links, and the max communication distance is up to 404 km [12], which can be widely used.

However, the optical-fiber-based links' loss limits the max communication distance and it leads to difficulties of building the long-distance quantum communication network. Quantum repeater, relying on quantum memory, is a way to solve this problem. We can connect many short-distance links to achieve long-distance communication. In 2021, Li and Zhou et al. [18] reported an elementary link of a quantum repeater based on absorptive quantum memories, which is a promising way of conducting quantum repeater's scheme. Another way is using satellite-based links to realize quantum key distribution in long distance. Classical light in atmosphere has been well improved [19–21].

Quantum light in atmosphere has also made some progress [22–25]. From 2016 to 2020, Vasylyev et al. [26,27] showed model of probability distribution of transmittance (PDT) in atmosphere under different weather conditions; Liorni et al. [28] applied PDT to satellite-based links and studied BB84 protocol in satellite-based links; Liang et al. [29] used MDI-QKD protocol instead of BB84 protocol in [29]. In 2021, Pan's team [30] reported an integrated space-to-ground quantum communication network by BB84. They used Micius satellite to connect quantum communication network on the ground over 4600 km. However, Liorni et al.'s work [28] using BB84 is not safe enough and satellite's position and weather conditions are single in Liang et al.'s work [29], which lead to lack of practicality. Considering that the operation of the satellite and different weather conditions, this paper further researches on the performance of satellite-based links for MDI-QKD protocol when the satellite's height is from 500 km to 2000 km and the angle from zenith is from 0° to 80°.

2. Theory

MDI-QKD protocol in optical-fiber-based links model is shown in Figure 1a. The classical MDI-QKD with polarization state consists of Alice, Bob and Charlie. Alice and Bob prepare polarization states and encode them. Then Alice and Bob send them to untrust Charlie for the Bell Measurement. Alice and Bob use the Decoy-IM to add decoy-state. Considering the above, we can get the key rate of MDI-QKD,

$$R \geq P_{11}^{Z} Y_{11}^{Z} \left[1 - H_2\left(e_{11}^{X}\right)\right] - Q_{\mu_a \mu_b}^{Z} f_e H_2\left(E_{\mu_a \mu_b}^{Z}\right), \tag{1}$$

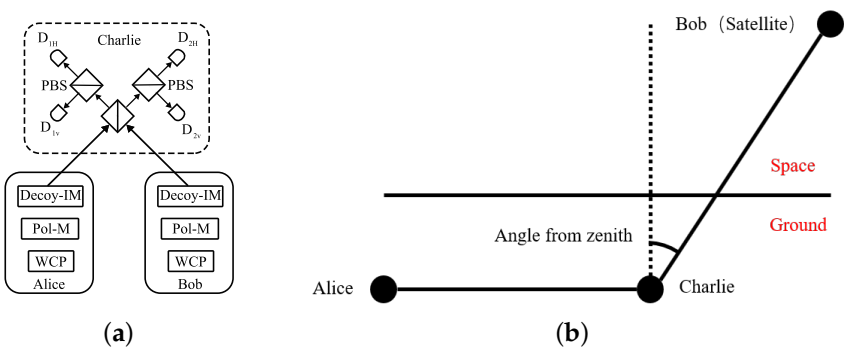
where $X(Z)$ is the diagonal(rectilinear) basis; $Q_{\mu_a \mu_b}^{Z}$ and $E_{\mu_a \mu_b}^{Z}$ are the gain and quantum bit error rate; Y_{11}^{Z} and e_{11}^{X} are the single-photon yield in the Z basis and the single-photon error rate; $\mu_a(\mu_b)$ is Alice(Bob)'s signal intensity; P_{11}^{Z} is the probability that both Alice and Bob send single-photon; f_e is the error correction inefficiency function; H_2 is the binary entropy function given by $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

We need practical parameters in Table 1 to get key rate. e_d is the total misalignment error, e_0 is the error probability of vacuum pulses, P_d is the dark count of each detector, f_e is the error correction inefficiency, a is the loss of fibers, η_{det} is the detector efficiency.

Table 1. List of practical parameters of MDI-QKD for numerical simulations [11].

e_d	e_0	P_d	f_e	a	η_{det}
1.5%	0.5	3×10^{-6}	1.16	0.2	14.5%

MDI-QKD protocol with satellite-based links model is shown in Figure 1b with main parameters on it. There are optical-fiber-based links between Alice and Charlie, which is on the ground, and satellite-based links between Bob and Charlie, which is in the air and space.



(**a**) (**b**)

Figure 1. (**a**) Schematic of MDI–QKD. (**b**) Schematic of satellite-based MDI–QKD.

For MDI-QKD protocol, we care about the transmittance of fibers. When applying it to Figure 1b, we should consider the same. In Liorni et al.'s work [28], the transmittance is affected by lot of factors but many of them have fixed distribution. Hence, we only get PDT. Here, we consider the operation of the satellite (the height and the angle from zenith) and weather, such as light intensity, turbulence, scattering particles and so on. Weather conditions' simulation relies on parameters of Table 2. C_n^2 is the value of the refractive index structure constant, n_0 is the density of scattering particles.

After PDT is gotten from [10], the average key rate of MDI-QKD with satellite-based links can also be gotten:

$$\bar{R} = \int_0^1 R(\eta)P(\eta)\mathrm{d}\eta = \sum_{i=1}^{N_{bins}} R(\eta_i)P(\eta_i) \tag{2}$$

where $R(\eta)$ is the average key rate as a function of transmittance, which can be gotten by Equation (1); $P(\eta)$ is the PDT; N_{bins} is the quantity of PDT sampling.

Table 2. List of practical parameters of weather conditions [10].

Night	**Condition 1**	**Condition 2**
C_n^2	1.12×10^{-6} $\mathrm{m}^{-2/3}$	5.50×10^{-6} $\mathrm{m}^{-2/3}$
n_0	0.61 m^3	3.00 m^3
Day	**Condition 1**	**Condition 2**
C_n^2	1.64×10^{-6} $\mathrm{m}^{-2/3}$	8.00×10^{-6} $\mathrm{m}^{-2/3}$
n_0	0.01 m^3	0.05 m^3

3. Calculation Results

For MDI-QKD protocol, we chose vacuum + weak decoy states in the same scheme as [11]. For satellite-based links, it includes Down-link and Up-link and PDT is different through different links. However, both of them have the same simulation method. In this paper we only show Down-link.

By using PDT and Equation (2), Figure 2 is gotten. It only cares about the relationship between the average transmittance and the operation of the satellite visually, which is useful to the following researches. From Figure 2, the average transmittance is up to the max when the satellite is closed and nearly vertical to the ground and decreases with increasing height and angle.

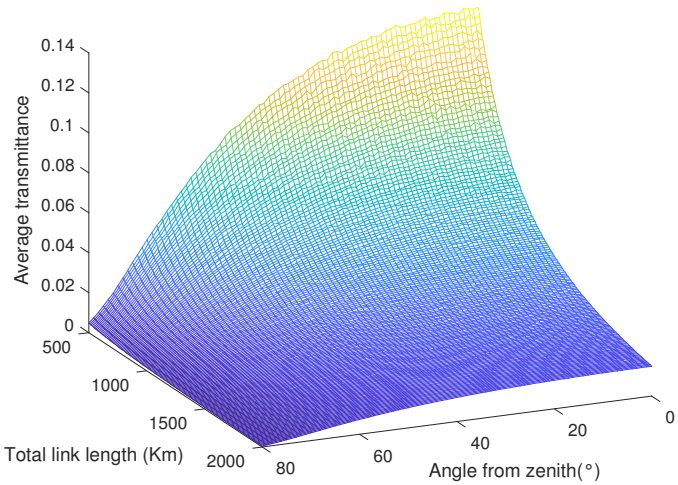


Figure 2. The convexity of average transmittance with the orbit's height and the angle from zenith changing in condition 1.

Considering that the height of satellite and the angle from zenith and the weather conditions, we simulate and get Figures 3 and 4. λ is the signal light's wavelength. It helps to study general optical communication window in satellite-based links. L_A is the length of optical-fiber-based links and also the distance between Alice and Bob on the ground.

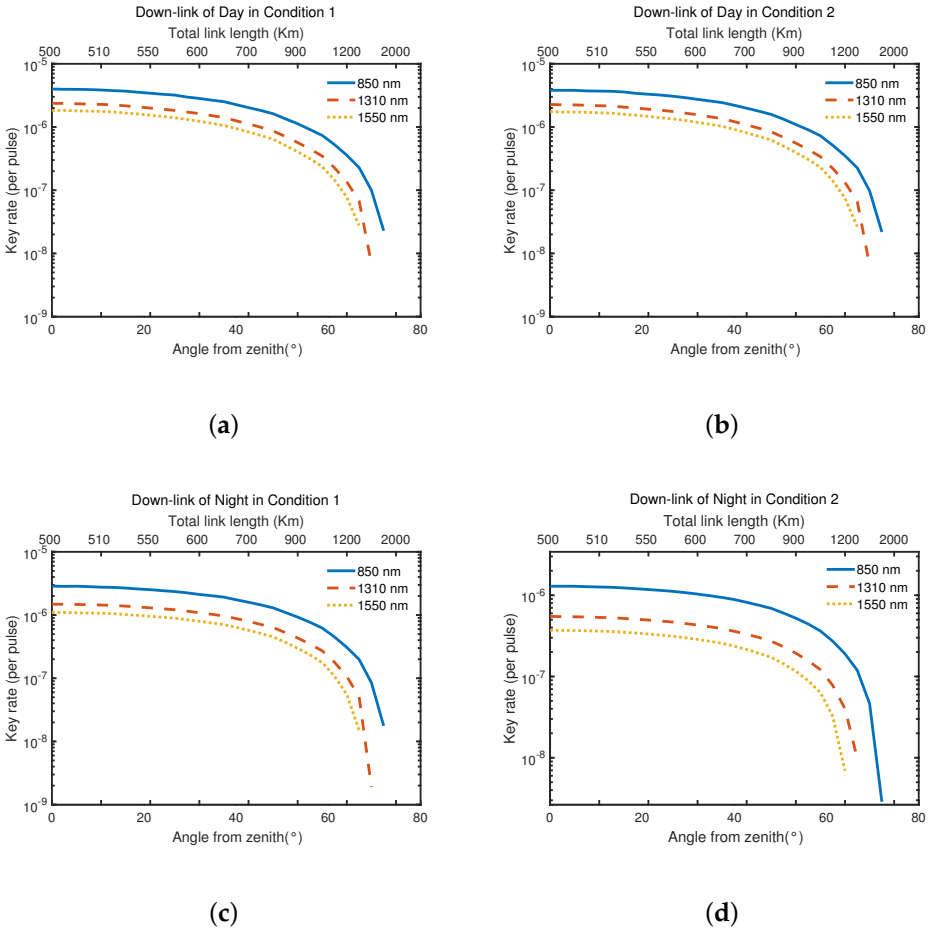


Figure 3. The secret key rates of the MDI-QKD protocol in two different weather conditions, as functions of the angle from zenith and the orbit's height, are reported at signal light's wavelength $\lambda = 850$ nm, 1310 nm, 1550 nm respectively. L_A is fixed at 50 km.

As we can see, by the longitudinal comparison, due to the weather such as the light and so on, the average key rate is higher in the same condition during the day than that at night.; by the horizontal comparison, in different weather conditions, it changes little during the day, but changes a lot at night.

Figure 3 shows that the large tolerance of general optical communication window. Changing the wavelength of signal light has little effect on the average key rate. In Figure 4, we can find that the ground loss has large effect on the average key rate. When L_A = 100 km, the lowest average key rate is almost as low as 10^{-9}. Besides, when the satellite operates between (500 km, 0°) and (700 km, 45°), the average key rate is relatively stable. The average key rate decreases fast when the satellite's height and angle from zenith exceed (700 km, 45°). It almost reaches 0 at (1500 km, 75°), which means that it can hardly communicate with MDI-QKD when the satellite is too high and almost parallels to the ground.

From the two figures, what we should be noticed is the large effect of the loss of optical-fiber-based links on the ground. However, it also can cover a general city. The large tolerance of general optical communication window helps combine optical-fiber-based links with satellite-based links.

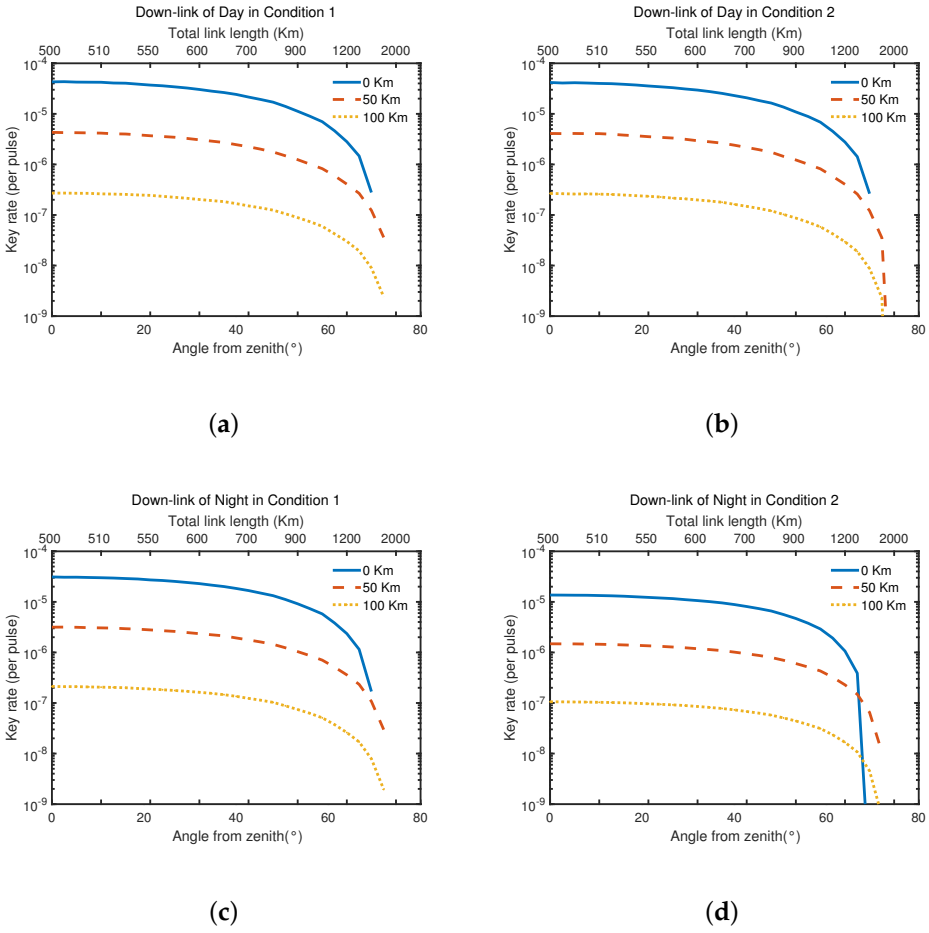


Figure 4. The secret key rates of the MDI-QKD protocol in two different weather conditions, as functions of the angle from zenith and the orbit's height, are reported at L_A = 0 km, 50 km, 100 km respectively. λ is fixed at 785 nm.

4. Conclusions

In this paper, the performance of satellite-based links for measurement-device-independent quantum key distribution has been further evaluated. The effect of weather conditions, the different wavelengths of signal light and the ground loss on the model is analyzed. All the results are reported by changing the satellite's height and the angle from zenith. Compared with previous work, it is more close to the reality. It combines the traditional optical-fiber-based links with free-space links. It is significant for long-distance quantum communication. Moreover, it also offers important reference to build long-distance quantum communication network with satellite-to-ground links. More progress can be made in transmittance and key rate and better results may be gotten with optimizing by machine learning.

Author Contributions: Conceptualization, R.J. and G.H.; methodology, G.H.; validation, R.J.; formal analysis, G.H.; investigation, Q.D. and W.C.; writing—original draft preparation, G.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Fundamental Research Funds for the Central Universities grant number 2019XD-A02, Ministry of Science and Technology of China grant number 2016YFA0301300 and National Natural Science Foundation of China grant number 61571060.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing 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
MDI-QKD	Measurement-device-independent quantum key distribution
WCP	Weak coherent pulse
PDT	Probability of transmittance

References

1. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2001**, *74*, 145–195. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
4. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
5. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum Cryptography with Coherent States. *Phys. Rev. A* **1995**, *51*, 1863–1869. [CrossRef] [PubMed]
6. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.-J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
7. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2015**, *8*, 595–604. [CrossRef]
8. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 57901. [CrossRef] [PubMed]
9. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
10. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
11. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
12. 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]
13. Dellantonio, L.; Sørensen, A.S.; Bacco, D. High dimensional measurement device independent quantum key distribution on two dimensional subspaces. *Phys. Rev. A* **2018**, *98*, 62301. [CrossRef]
14. Agnesi, C.; Lio, B.D.; Cozzolino, D.; Cardi, L.; Bakir, B.B.; Hassan, K.; Frera, A.D.; Ruggeri, A.; Giudice, A.; Vallone, G.; et al. Hong-Ou-Mandel interference between independent III–V on silicon waveguide integrated lasers. *Opt. Lett.* **2019**, *44*, 271–274. [CrossRef]
15. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2015**, *93*, 42324. [CrossRef]
16. Wang, Q.; Zhou, X.Y.; Guo, G.C. Realizing the measure-device-independent quantum-key-distribution with passive heralded-single photon sources. *Sci. Rep.* **2016**, *6*, 35394. [CrossRef] [PubMed]
17. Jiang, C.; Yu, Z.W.; Wang, X.B. Measurement-device-independent quantum key distribution with source state errors in photon number space. *Phys. Rev. A* **2016**, *94*, 62323. [CrossRef]
18. Liu, X.; Jun, H.; Li, J.F.; Li, X.; Li, P.Y.; Liang, P.J.; Zhou, Z.Q.; Li, C.F.; Guo, G.C. Heralded entanglement distribution between two absorptive quantum memories. *Nature* **2021**, *594*, 41–45. [CrossRef] [PubMed]
19. Tatarskii, V.I. *The Effects of the Turbulent Atmosphere on Wave Propagation*; Israel Program for Scientific Translations: Jerusalem, Israel, 1971.
20. Ishimaru, A. *Wave Propagation and Scattering in Random Media*; Academic Press: New York, NY, USA, 1978.
21. Andrews, L.C.; Philips, R.L.; Hopen, C.Y. *Laser Beam Scintillation With Applications*; SPIE Press: Bellingham, WA, USA, 2001.
22. Diament, P.; Teich, M.C. Photodetection of Low-Level Radiation through the Turbulent Atmosphere. *Opt. Soc.* **1970**, *60*, 1489–1494. [CrossRef]
23. Vasylyev, D.Y.; Semenov, A.A.; Vogel, W. Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality. *Phys. Rev. Lett.* **2012**, *108*, 220501. [CrossRef] [PubMed]
24. Sidhu, J.S.; Joshi, S.K.; Gundogan, M.; Brougham, T.; Lowndes, D.; Mazzarella, L.; Krutzik, M.; Mohapatra, S.; Dequal, D.; Vallone, G.; et al. Advances in Space Quantum Communications. *arXiv* **2021**, arXiv:2103.12749.
25. Semenov, A.A.; Vogel, W. Entanglement transfer through the turbulent atmosphere. *Phys. Rev. A* **2010**, *81*, 23835. [CrossRef]
26. Vasylyev, D.; Semenov, A.A.; Vogel, W. Atmospheric Quantum Channels with Weak and Strong Turbulence. *Phys. Rev. Lett.* **2016**, *117*, 90501. [CrossRef]
27. Vasylyev, D.; Semenov, A.A.; Vogel, W.; Günthner, K.; Thurn, A.; Bayraktar, Ö.; Marquardt, C. Free-space quantum links under diverse weather conditions. *Phys. Rev. A* **2017**, *96*, 043856. [CrossRef]

28. Liorni, C.; Kampermann, H.; Bruß, D. Satellite-based links for quantum key distribution: Beam effects and weather dependence. *New J. Phys.* **2019**, *21*, 093055. [CrossRef]
29. Liang, W.; Jiao, R.Z. Satellite-based measurement-device-independent quantum key distribution. *New J. Phys.* **2020**, *22*, 83074. [CrossRef]
30. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef] [PubMed]