Analysis of atmospheric effects on satellite based quantum communication: A comparative study

Vishal Sharma
IIT Jodhpur, Rajasthan India

Subhashish Banerjee
IIT Jodhpur, Rajasthan, India

Quantum Key Distribution (QKD) is a key exchange protocol which is implemented over free space optical links and optical fiber cable. When direct communication is not possible, QKD is performed over fiber cables, but the imperfections in detectors used at receiver side and also the material properties of fiber cables limit the long distance communication. Free space based quantum key distribution is free from such limitations, and can pave way for satellite based quantum communication to set up a global network for sharing secret messages. To implement free space optical (FSO) links, it is essential to study the effect of atmospheric turbulence. Here, an analysis is made for satellite based quantum communication using QKD protocols. The results obtained indicate that SARG04 protocol is an effective approach for satellite based quantum communication.

Keywords: Free space optics, Quantum Teleportation, Geometric losses, Quantum Key Distribution, Turbulence, Total attenuation, Receiver power.

I. INTRODUCTION

Quantum key distribution [1–3] is an advanced secure key exchange technique in the field of quantum communications. Due to high losses, optical fibers are not the practical choice for direct transmission of photons for global distances. Direct satellite links and fiber-based quantum repeaters are the two methods to overcome this problem. Quantum repeater technique will enhance the communication distance significantly which is not possible by optical fibers [1][4]. Quantum repeaters based on optical fibers are unable to achieve true global distances and it is also difficult for other approaches based on error correction [3][4], which need repeater stations placed at intervals of a few kilometers. Therefore, in order to establish communication over global distances many repeater stations are needed, with large number of qubits per station [10].

Quantum secure communication is achieved by three different satellite scenarios. In the first case, a source of entangled photons is implemented on the satellite itself and photons are sent to two ground stations. This approach helps in distributing two photons to the two users at the same time, separated several thousands of kilometers, even for Lower Earth Orbit (LEO) satellites. After transmission, the correlation property is examined for testing whether the two photons are still entangled or not, in order to confirm the security. Random detection of photons are used for generating the secure key, and is not restricted to the entangled photon security of the source itself. This concept has an important impact on the satellite based quantum research, where an autonomous satellite with an entangled photon source could make the source functional. Attenuated laser pulses is the other alternative by which quantum sources can be realized. These laser pulses contain single photons by emitting pulses of low optical power, which results in only a single photon from the source. Decoy pulses must be deployed to avoid the side channel attack due to multi photons per pulse. In the third scenario, the transmitter and receiver are at the ground, and satellite station respectively. Hence, here the signal propagates from Earth to space. This method has a unique feature which includes adapting the quantum source according to the requirement during the complete mission. By this approach one can achieve both foundational tests of quantum mechanics and quantum cryptography. In this work, we concentrate on this particular scenario.

The quantum transceiver designed must be small enough to be launched on a nano-satellite, specially dedicated to this task. A straightforward model would possess one fixed telescope, around 10 - 30 cm aperture, for sending or receiving photons. A very suitable ground station is needed possessing an optical telescope which tracks the satellites. An optical telescope of diameter not less than 0.5 m can be used. In satellite quantum communication, losses are due to diffraction, which scale more with distance, and not due to absorption.

Satellite based quantum communication plays an important and efficient role in the setup of a global network [11][21]. These satellite based quantum communication schemes are designed on FSO communications [22]. For successful implementation of satellite based quantum communication, it is necessary to consider free-space QKD under atmospheric turbulence. Although the technological advancement in commercial applications of QKD have met with enormous success, quantum communication still needs more investigations to deal with issues related to security, data rate and communication distance [23][24].

∗pg2013835600@iitj.ac.in
†subhashish@iitj.ac.in
This paper is organized as follows: Section II sketches the methodology for an FSO communication link under various atmospheric conditions. In section III, secure key rate for different QKD protocols are briefly discussed. We discuss our results in section IV and conclude in section V.

II. METHODOLOGY FOR FSO LINKS UNDER VARIOUS ATMOSPHERIC CONDITIONS

It is well known that three effects mainly contribute to the total channel attenuation in an FSO link (denoted as \( \delta \in [0, 1] \)): diffraction, atmospheric propagation and efficiency of the receiver. Hence the total attenuation can be obtained using \[ \delta = \delta_{\text{diff}}\delta_{\text{atm}}\delta_{\text{rec}}. \] (1)

The basic building block for a LEO satellite quantum communication system is as shown in figure 1.

Assume that Cassegrain type telescope architectures at sender and receiver sides and laser beams of Gaussian type are used for the said arrangement \[26, 27\], obscuration and beam diffraction generate attenuation and shown to be \[28, 29\].

\[ \delta_{\text{diff}} = (e^{-2\gamma^2\sigma^2} - e^{-2\gamma^2}) (e^{-2\gamma^2\sigma^2} - e^{-2\gamma^2}), \] (2)

\[ \gamma_t = \frac{b_t}{R_t}, \gamma_r = \frac{b_r}{R_r}, \alpha_t = \frac{R_t}{\omega_t}, \alpha_r = \frac{R_r}{\omega_r}, \]

\[ \omega_t = R_t, \omega_r = \sqrt{\frac{2\lambda L}{\pi R_t}} \]

where \( b_t, b_r \) and \( R_t, R_r \) represent radii of the secondary (\( b \)) and primary (\( R \)) mirrors at transmitter (\( t \)) and receiver (\( r \)) respectively; \( L \) is the distance between telescopes (also known as link distance), \( \lambda \) is the considered wavelength and \( \omega_{t,r} \) is the beam radius at transceiver ends. The atmospheric attenuation \( \delta_{\text{atm}} \) is due to various phenomena such as turbulence, scattering, absorption, rain, haze, fog. Hence it can be written as \( \delta_{\text{atm}} = \delta_{\text{scatt}}\delta_{\text{abs}}\delta_{\text{turb}}\delta_{\text{rain}} \), where each quantity represents the attenuation for the corresponding phenomena. More detailed description about free space optics and turbulence effects can be obtained from \[31, 34\].

Accounting the total attenuation given above excluding the rain effects, various experiments presented in \[16, 17, 22, 35–37\] have analyzed the performance of QKD in free space or optical fiber or both in different applications using

\[ P_R = P_T O \alpha_{geo} e^{-\sigma L}, \] (3)

where

\[ \sigma = \left( \frac{3.912}{V} \right) \left( \frac{\lambda}{500} \right)^{-q'}, \] (4)

\[ \alpha_{geo} = \frac{d_2^2}{(d_1 + (L\theta))^2}, \] (5)

with \( P_R \) is the received power at the receiver, \( P_T \) is the transmit power, \( O \) stands for optical losses, \( d_2 \) is the diameter of receiver aperture in meters, \( d_1 \) is the diameter of transmitter aperture in meters, \( \theta \) is the beam divergence in mrad, \( L \) is the link range in meters, \( \lambda \) denotes considered wavelength (nm), \( V \) is the visibility (km) and \( q' \) represents the size distribution of diffusing particles. To investigate the FSO links under harsh atmospheric conditions, power equation at the receiver side is

\[ P_R(dBm) = P_T(dBm) - O(dB) - \alpha_{geo}(dB) - \alpha(dB) - \alpha_{\text{haze/cloud}}(dB), \] (6)

\[ \alpha(dB) = 10 \log_{10} (\exp^{-\sigma L}) + L(aR^\gamma). \] (7)

where \( R \) is the rain rate and \( a, b \) are rain coefficients which are dependent on rain characteristics and wavelength of the FSO link. \( P_T(dBm), P_R(dBm), O(dB), \alpha_{geo}(dB) \) and \( \alpha(dB) \) are transmitted power, received power, optical losses, geometric attenuation and atmospheric attenuation coefficient in dB respectively. Signal at the receiver can be reconstructed if the received signal power \( P_R \) is greater than the minimum power level which is dependent on the sensitivity of the receiver.

Geometric loss increases with the increasing link range. In a free space optic model geometric loss can be reduced by deploying low value of divergence angle of laser beam. Under geometric attenuation light beam diverges from transmitter to receiver, hence most of the light beam does not reach the receiver’s telescope and signal loss occurs. It is necessary to increase the receiver aperture area, so that geometric losses can be controlled (minimized) by collecting more signal at the receiver telescope.
III. THE SECURE KEY RATE ANALYSIS WITH DIFFERENT PROTOCOLS

A. The BB84 Quantum Cryptography protocol

The BB84 protocol was proposed in [1], see [38, 39] for details. The attenuated laser pulses used in practical QKD schemes are coherent in nature and described by coherent states. The output pattern obtained from lasers follow the Poisson distribution [26, 40].

\[ |\alpha\rangle = e^{-\mu^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \]  

(8)

Here \(|\alpha\rangle = \sqrt{\frac{\mu}{\pi}}, \mu\) is the mean photon number of a pulse. The probability corresponding to \(n\) photons in a pulse is given by

\[ p_n = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} |\alpha|^{2n} \frac{1}{n!}. \]  

(9)

In QKD, the transmitter transmits the bit stream in the form of optical pulses via a quantum channel [41, 42]. These optical pulses are specified by a number known as beam intensity \(\mu\) (mean photon number) which ranges from 0.1 to 0.5. Here 0.1 indicates 1 photon every 10 pulses [13, 16, 17]. For bit encoding in QKD system, polarization filters are used to polarize the photon of only a single photon is used. In BB84 protocol, polarization filters are used to polarize the photons [13, 18, 19]. The Shannon mutual information, \(I(A : B)\) and \(I(B : E)\), shared between Alice (A)-Bob (B) and Bob (B)-Eve (E), respectively are calculated in bits/pulse [1, 43]. Here,

\[ I(A : B) = \sum_{n=0}^{\infty} \left(1 - (1 - \delta)^n\right) P_n(\mu) \approx \mu \delta, \]  

(10)

\[ I(B : E) = \sum_{n=2}^{\infty} P_n(\mu). \]  

(11)

Eve’s Information, \(I_{Eve}\), is defined as

\[ I_{Eve} \approx \frac{I(B : E)}{I(A : B)}. \]  

(12)

The lowest value for the key generation rate \(R\) (in bits/pulse) is expressed in [38, 43, 44]

\[ R \geq q \left( -Q_\mu f(E_\mu) H_2 E_\mu + \Omega Q_\mu \left( 1 - H_2 \left( \frac{E_\mu}{\Omega} \right) \right) \right), \]  

(13)

where \(\Omega\) denotes those photons, from which Eve cannot extract any information, also known as untagged photons [44]. Also \(q\) represents the efficiency of the considered protocol, the values of \(q\) are 1/2 and 1/4 for BB84 and SARG04 protocols, respectively. \(f(x)\) represents the bi-directional error correction efficiency, whose value is 1.22 for the Cascade protocol [45]. Yield of the n-photon pulses is represented as \(Y_n [44]\).

The expected raw key rate, can be written as

\[ Q_\mu = \sum_{n=0}^{\infty} Y_n P_n(\mu). \]  

(14)

Quantum Bit Error Ratio (QBER), \(E_\mu\), is

\[ E_\mu = \frac{\sum_{n=0}^{\infty} Y_n P_n(\mu) e_n}{Q_\mu} = \frac{Y_0}{2Q_\mu}. \]  

(15)

B. The SARG04 Quantum Cryptography Protocol

The SARG04 protocol was proposed in [46] and is more powerful compared to BB84 against the photon number splitting attack. The quantum communication phase in SARG04 is similar to that in the BB84 protocol, but the distinction exists in the encryption and decryption of Shannon’s classical information part [2]. In this protocol, the bases are not communicated, but Alice declares one nonorthogonal state out of the four pairs \(A_\omega, \omega'\) = \(|\omega x\rangle, |\omega' z\rangle\), where \(\omega, \omega' \in \{+, -\}\) and \(|\pm x\rangle = 0, |\pm z\rangle = 1\). [47, 48]. While performing attacks, Eve introduces attenuation which is expressed as

\[ \delta = \frac{(1 - t)P_1 + P_2(\mu) + \chi}{\mu}, \ t \in [0, 1]. \]  

(16)

Here \(\chi\) is expressed as

\[ \chi = \sum_{n=3}^{\infty} P_n(\mu) P_{ok}(n), \]  

(17)

where \(P_{ok}\) represents the probability of acceptance. For BB84 protocol, this value is 0.5 [43, 48].

The attenuation in this case can be written as

\[ \delta = \frac{(1 - s)P_2(\mu) + \chi}{\mu}, \ s \in [0, 1]. \]  

(18)

Figure 2 represents the comparison between \(I_{Eve}\) and distance in km under the BB84 and SARG04 protocols. This is calculated based on the link parameters described in subsequent sections. From this figure, it is observed that Eve obtains more information in BB84 protocol as compared to SARG04 protocol. Hence, it can be concluded that SARG04 protocol outperforms the BB84 protocol under such conditions.
C. Protocols with the decoy-states: An effective approach against Eavesdropping

The decoy-state method was proposed in [49] and further studied in [50–52]. Introducing decoy-states (also known as extra test states) help in detecting the presence of eavesdropping, whereas signal states are deployed for key generation only. The shared mutual information is

\[ I(A : B) = P_1(\mu)(1-t) + P_2(\mu)(1-s) + \sum_{n \geq 3} P_n(\mu)P_{ok}(n), \]

(19)

\[ I(B : E) = P_2(\mu)(1-s)I_2 + \sum_{n \geq 3} P_n(\mu)P_{ok}(n), \]

(20)

here \( t \) represents the fraction of the single photon pulses blocked by Eve, and \( s \) denotes a fraction of the two-photon pulses. \( I_2 \) is the amount of information that Eve can obtain from a single copy of the state [46]. Next we analyze the security of the protocols under consideration.

1) BB84 quantum cryptography protocol: Vacuum + weak decoy state:

A lower bound on the key generation rate [44], based on entanglement distillation described in [53], which in turn use the concept of decoy-state, is

\[ R_{BB84} \geq q \left( -Q_\mu f(E_\mu)H_2(E_\mu) + Q_1 \left( 1 - H_2(e_1) \right) \right), \]

(21)

where \( Q_\mu \) represents the gain of the signal state, \( E_\mu \) denotes the QBER, \( Q_1 \) represents the gain of single-photon states and \( e_1 \) denotes the error rate of single-photon states.

The parameter \( Q_1 \) is [54]

\[ Q_1 = Y_1 e^{-\mu}. \]

(22)

The lower bound for \( Q_1 \) and upper bound for \( e_1 \) with the vacuum and a weak decoy state (\( \nu \)) is [50]

\[ Y_1^L = \frac{\mu}{(\mu \nu - \nu^2)} \left( Q_\mu e^{\nu} - Q_\mu e^{\mu} \left( \frac{\nu^2}{\mu^2} \right) - \frac{(\mu^2 - \nu^2)}{\mu^2} Y_0 \right) \leq Y_1, \]

(23)

\[ Q_1^L = \mu e^{-\mu} Y_1^L \leq Q_1, \]

(24)

\[ e_1^U = \frac{e_1 Y_0}{Y_1^L} \geq e_1. \]

(25)

2) The SARG04 quantum cryptography protocol: Vacuum + two weak decoy states:

Single-photon states help in key generation rate in BB84 protocol, whereas both single-photon and two-photon states contribute to the key generation rate in SARG04 protocol [54]. Taking this into account with the approach developed in [53], the gain in case of two photon pulses is [43, 54]

\[ Q_2 = Y_2 e^{-\mu} \frac{\mu^2}{2}. \]

(26)

The SARG04 protocol uses three decoy states, \( \nu_0, \nu_1 \) and \( \nu_2 \), assuming that \( \nu_0 \) is the vacuum (i.e. \( \nu_0 = 0 \)), and the two weak decoy states are \( \nu_1 \) and \( \nu_2 \). For these decoy states, gain and quantum bit error rate are

\[ Q_{\nu_i} = \sum_{n=0}^{\infty} Y_n P_n(\nu_i), \]

(27)

\[ E_{\nu_i} = \sum_{n=0}^{\infty} Y_n P_n(\nu_i) e_n Q_{\nu_i}. \]

(28)

The bit error ratio of the \( n \)-photon signals, which is due to only the dark counts \( Y_0 \), is

\[ e_n = \frac{Y_0}{2Y_n}. \]

Let the legitimate users (Alice, Bob) select \( \nu_1 \) and \( \nu_2 \) which satisfy

\[ 0 < \nu_1 < \nu_2, \quad \nu_1 + \nu_2 < \mu. \]

(29)

Now the key generation can be shown to be

\[ R_{SARG04} \geq q \left( -Q_\mu f(E_\mu)H_2(E_\mu) + Q_1 \left( 1 - H_2 \left( \frac{e_1}{X_n} \right) \right) + Q_2 \left( 1 - H(Z_2) \right) \right), \]

(30)

where \( X_n \) and \( Z_n \) represents the binary random variables. \( H_2(.) \) is the Shannon’s binary entropy function

The lower limit of the two photon gain is

\[ Q_2^L = \frac{Y_2^L \mu^2 e^{-\mu}}{2} \leq Q_2. \]

(31)

The upper limit of \( e_2 \) can be manipulated by considering quantum bit error rate of weak decoy states.

\[ E_{\nu_i} Q_{\nu_i} e^{\nu_i} = e_0 Y_0 + e_1 Y_1 + e_2 \frac{\nu^2}{2} Y_2 + \sum_{n=3}^{\infty} e_n Y_n \frac{\nu^n}{n!}. \]

(32)
IV. RESULTS

The results shown here are based on three scenarios. The parameters for link establishment are detector efficiency ($\delta_{\text{rec}}$), satellite telescope radius ($R_{t,r}$), satellite secondary mirror radius ($b_{t,r}$), ground telescope radius ($R_{t,r}$), ground secondary mirror radius ($b_{t,r}$), dark counts ($Y_0$) and wavelength ($\lambda$) whose values are 65%, 15 cm, 1 cm, 50 cm, 5 cm, $50 \times 10^{-6}$ counts/pulse and 650 nm, respectively. $\lambda = 650 \text{nm}$ represents an absorption window with a commercial detector made of silicon avalanche photo diode with high detection efficiency. Telescope radius values are taken from [55, 56].

In figure 2 we have shown the dependency of key generation rates on the communication distance for each protocol. The pulses emitted from the laser source can be converted from bits/pulse to bits/second [36]. In figure 4, we have optimized $\mu$ and $\nu_i$ in each protocol for both the states to obtain the highest key rate.

In figure 3, it is observed that critical distance obtained for SARG04 is comparatively higher than BB84, both with and without decoy states. Also in figure 2, it is shown that SARG04 is more robust against eavesdropping than BB84 with an optimal mean photon number. The decoy state method used in BB84 protocol enhances the critical distance. Decoy state method is a powerful technique that increases both the critical distances and key generation rate for both the entangled and non-entangled based protocols [59].

In case of increasing attenuation, the number of multi photon pulses must be minimized which helps in reducing the chance of attacks performed by Eve (in this case $\mu$ must be decreased) as shown in figure 4. At higher value of $\mu$, the protocol becomes more robust. With increasing mean photon number, we achieve enhanced communication distance and at the same time the considered protocols are resistant to Eve’s photon number splitting (PNS) attack. Due to movement of satellite along its orbit, its distance with the ground station varies. The value of $\mu$ has to be adjusted to achieve the maximum secure rate, which is the challenging part of the problem.

The results depicted in figure 5, for each protocol indicates the maximum key generation rates, keeping $\mu$ constant to that of optimal $\mu$ for maximum distance. It is clearly observed that in case of protocols based on decoy states the secure rate decreases to a level below 3%, which means that in this situation the variation in mean photon number with distance is not necessary. The result is opposite to that of protocols based on non-decoy states where rate degradation occurs rapidly. This implies that the value of mean photon number should vary with distance for obtaining optimum results for secure rates. The rest of the three cases (downlink, uplink on clear weather conditions and inter satellite links) fol-
allows the same steps. The critical distance (in Km) for

BB84 protocol are seen to be: 1540 Km in downlink case, 430 Km in intersatellite case, 460 Km in uplink case ($\delta = 5dB$) and almost negligible critical distance in case of uplink with $\delta = 11dB$. Similarly, the critical distance (in Km) for SARG04 protocol are seen to be: 3290 Km in downlink case, 920 Km in intersatellite case, 1520 Km in uplink case ($\delta = 5dB$) and 500 Km in case of uplink with $\delta = 11dB$. Following the same approach, the critical distance (in Km) for BB84 protocol with vacuum state and weak decoy state obtained from simulations are: 9450 Km in downlink case, 2660 Km in intersatellite case, 4050 Km in uplink case ($\delta = 5dB$) and 2200 Km in case of uplink with $\delta = 11dB$. The maximum possible secure rate (in Bits/Pulse) for BB84 protocol achieved from simulations are: $1.7 \times 10^{-2}$ in downlink case, $2.0 \times 10^{-2}$ in intersatellite case, $1.4 \times 10^{-4}$ in uplink case ($\delta = 5dB$) and almost negligible secure rate in case of uplink with $\delta = 11dB$. The maximum possible secure rate (in Bits/Pulse) for SARG04 protocol are as follows: $2.4 \times 10^{-2}$ in downlink case, $2.6 \times 10^{-2}$ in intersatellite case, $1.2 \times 10^{-3}$ in uplink case ($\delta = 5dB$) and $7.5 \times 10^{-5}$ in case of uplink with $\delta = 11dB$. Following the same procedure, the maximum possible secure rate (in Bits/Pulse) for BB84 protocol with vacuum state and weak decoy state are as follows: $4.4 \times 10^{-2}$ in downlink case, $4.8 \times 10^{-2}$ in intersatellite case, $5.8 \times 10^{-3}$ in uplink case ($\delta = 5dB$) and $1.4 \times 10^{-3}$ in case of uplink with $\delta = 11dB$. The maximum possible secure rate (in Bits/Pulse) for SARG04 protocol with vacuum state and two weak decoy state are as follows: $4.6 \times 10^{-2}$ in downlink case, $5.0 \times 10^{-2}$ in intersatellite case, $6.5 \times 10^{-3}$ in uplink case ($\delta = 5dB$) and $1.6 \times 10^{-3}$ in case of uplink with $\delta = 11dB$. In these cases values are different but the curves follow the same steps.

From figures, it is clear that we achieve maximum distance in case of downlink which is due to absence of turbulence in downlink and hence no attenuation. In case of Medium-Earth-Orbit (MEO) satellites, cryptography techniques can be implemented by deploying SARG04 with decoy states. Inter satellite links suffer from reduced telescope dimensions and hence cannot achieve maximum distance. In all these operations two major hurdles are telescope dimensions and turbulence induced attenuation which influence the optimum results.

Geometric attenuation is responsible for the light beam to diverge in its propagation path. To minimize these signal losses, receiver aperture area is increased to collect more light by the telescope to diminish the geometric losses. Hence SARG04 protocol deploying with decoy states obtains highest key rate as well as maximum link range. Finally, we can claim that the optimum results are obtained when we use pulses with two photons plus optimum $\mu$.

V. CONCLUSION

From the above results is borne out the point that the SARG04 protocol achieves optimum result as compared to the BB84 protocol under the considered attack such as PNS attack. Based on these results we can claim that two decoy states based SARG04 protocol is the best choice for QKD based satellite communication. Here we have optimized all the results for the optimum value of mean photon number to achieve maximum communication distance and secure key generation rate.

In order to achieve long distance communication, it is necessary to reduce the link losses. Actual data may be used to better understand the atmospheric turbulence and define a propagation model that should help the receiver and transmitter design. Moreover, new communication protocols that exploit the atmospheric turbulence as a resource can be defined. Our telescope design data could be used in future for single photons long distance free space experiments, like teleportation and QKD. This study will help to experimentally demonstrate the feasibility of Earth-space quantum links.

The uplink allows the complex quantum source to be kept on the ground while only simple receivers are in space, but suffers from high link loss due to atmospheric turbulence, necessitating the use of specific photon detectors and highly tailored photon pulses. For better performance and to enhance the communication distance one could use six or more nonorthogonal states. Further, the effect of adding pointing and misalignment errors need to be taken into account for greater improvement.

ACKNOWLEDGEMENTS

VS would like to thank the Ministry of Human Resource Development, Govt. of India, for offering a doctoral fellowship as a Ph.D. research scholar at Indian Institute of Technology Jodhpur, Rajasthan, India. VS
thanks Professor K. K. Sharma for useful discussions pertaining to the work.

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and con tos. 1984.
[2] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dusék, Norbert Lütkenhaus, and Moncthil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.
[3] N Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, and Wolfgang Tittel. Rate-loss analysis of an efficient quantum repeater architecture. *Physical Review A*, 92(2):022357, 2015.
[4] KJ Resch, M Lindenthal, B Blauensteiner, HR Böhm, A Fedrizzi, C Kurtsiefer, A Poppe, T Schmitt-Manderbach, M Taraba, R Ursin, et al. Distributed entanglement and single photons through an intra-city, free-space quantum channel. *Optics Express*, 13(1):202–209, 2005.
[5] WJ Munro, AM Stephens, SJ Devitt, KA Harrison, and Kae Nemoto. Quantum communication without the necessity of quantum memories. *Nature Photonics*, 6(11):777–781, 2012.
[6] Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Physical review letters*, 112(25):250501, 2014.
[7] Nicholas Sangouard, Christoph Simon, Hugues De Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, 2011.
[8] S Saikat Guha, Hari Krovi, Christopher A Fuchs, Zachary Dutton, Joshua A Slater, Christoph Simon, and Wolfgang Tittel. Rate-loss analysis of an efficient quantum repeater architecture. *Physical Review A*, 92(2):022357, 2015.
[9] Richard J Hughes, Jane E Nordholt, Derek Derkacs, and Charles G Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New journal of physics*, 4(1):43, 2002.
[10] Andrew Shields and Zhiliang Yuan. Key to the quantum industry. *Physics World*, 20(3):24, 2007.
[11] Andrew Shields and Zhiliang Yuan. Key to the quantum industry. *Physics World*, 20(3):24, 2007.
[12] Christian Kurtsiefer, P Zarda, M Halder, Ph M Gorman, Paul R Tapster, JG Rarity, and Harald Weinfurter. Long-distance free-space quantum cryptography. In *Photons Asia 2002*, pages 25–31. International Society for Optics and Photonics, 2002.
[13] Vishal Sharma and Richa Sharma. Analysis of spread spectrum in matlab. *International Journal of Scientific & Engineering Research*, 5(1), 2014.
[14] Malvin Carl Teich and B Saleh. Fundamentals of photonics. *Canada, Wiley Interscience*, 3, 1991.
[15] Javier Alda. Laser and gaussian beam propagation and transformation. *Encyclopedia of optical engineering*, 2(6):178–200, 2003.
[31] Shlomi Arnon. Effects of atmospheric turbulence and building sway on optical wireless-communication systems. *Optics Letters*, 28(2):129–131, 2003.

[32] Motti Gabay and Shlomi Arnon. Quantum key distribution by a free-space mimo system. *Journal of Lightwave Technology*, 24(8):3114–3120, 2006.

[33] JG Rarity, PR Tapster, PM Gorman, and P Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4(1):82, 2002.

[34] Markus Aspelmeyer, Thomas Jennewein, Martin Pfennigbauer, Walter R Leeb, and Anton Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551, 2003.

[35] William T Butlter, Richard J Hughes, Steve K Lamoreaux, George L Morgan, Jane E Nordholt, and C Glen Peterson. Daylight quantum key distribution over 1.6 km. *Physical Review Letters*, 84(24):5652, 2000.

[36] Tobias Schmitt-Manderbach, Henning Weier, Martin Furst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[37] Attila Pereszlenyi. Simulation of quantum key distribution with noisy channels. In *Telecommunications, 2005. ConTEL 2005. Proceedings of the 8th International Conference on*, volume 1, pages 203–210, IEEE, 2005.

[38] Christopher A Fuchs, Nicolas Gisin, Robert B Griffiths, Chi-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Physical Review A*, 56(2):1163, 1997.

[39] Dagmar Bruss and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. *Applicable Algebra in Engineering, Communication and Computing*, 10(4):383–399, 2000.

[40] Rodney Loudon. *The quantum theory of light*. OUP Oxford, 2000.

[41] Vishal Sharma, Chitra Shukla, Subhashish Banerjee, and Anirban Pathak. Controlled bidirectional remote state preparation in noisy environment: a generalized view. *Quantum Information Processing*, 14(9):3441–3464, 2015.

[42] Vishal Sharma, Kishore Thapliyal, Anirban Pathak, and Subhashish Banerjee. A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. *Quantum Information Processing*, 15(11):4681–4710, 2016.

[43] Thomas M Cover and Joy A Thomas. Elements of information theory 2nd edition (wiley series in telecommunications and signal processing). 2006.