Noname manuscript No.
(will be inserted by the editor)

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

Vishal Sharma · Subhashish Banerjee

Received: date / Accepted: date

Abstract Quantum Key Distribution (QKD) is a key exchange protocol which is implemented over free space optical links or optical fiber cable. When direct communication is not possible, QKD is performed over fiber cables, but the imperfections in detectors used at the receiver side and also the material properties of fiber cables limit the long-distance communication. Free-space based QKD is free from such limitations and can pave the 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. We assume two specific attacks, namely PNS (photon number splitting) and IRUD (intercept-resend with unambiguous discrimination), which could be main threats for future QKD based satellite applications. The key generation rates and the error rates of the considered QKD protocols are presented. Other parameters such as optimum signal and decoy states mean photon numbers are calculated for each protocol and distance. Further, in SARG04 QKD protocol with two decoy states, the optimum signal-state mean photon number is independent of the link distance and is valid for the attacks considered here. This is significant, highlighting its use in a realistic scenario of satellite quantum communication.

Keywords Free space optics · geometric losses · quantum key distribution · quantum teleportation · satellite applications · space technology · total attenuation · turbulence.

1 Introduction

Quantum key distribution [1, 61, 62, 67] 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

Vishal Sharma
IIT Jodhpur, Rajasthan, India.
E-mail: pg201383506@iitj.ac.in.

Subhashish Banerjee
IIT Jodhpur, Rajasthan, India.
E-mail: subhashish@iitj.ac.in.

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 [3, 5, 6]. 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 [7–9], 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 a 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 are the second 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 [36, 44, 50, 52, 63, 64, 89–92].

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 straight forward model would posses 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 a diameter not less than 0.5 m can be used. In satellite quantum communication, losses are due to diffraction, which scales 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 [11–15, 17–21, 72]. These satellite based quantum communication schemes are designed for FSO communications [22]. For successful implementation of satellite based quantum communication, it is necessary to consider free-space QKD under atmospheric turbulence. In an earth-satellite link, only around 30 km of the path (depending on the satellite elevation) are inside the atmosphere. The link attenuation must be below 60 dB for earth to space quantum communication, above this value quantum communication is not feasible. Link distance (L) for various scenarios between earth to space are as follows: ground-LEO and LEO-ground links is 500 to 1400 Km; ground-GEO and GEO-ground is above 36, 0000 Km; for LEO-LEO (intersatellite link) is 2, 000 Km; LEO-GEO (intersatellite link) link distance is 35, 500 Km and link distance for GEO-GEO (intersatellite link) is 40, 000 Km. Although the technological advancement in commercial applications of QKD has met with enormous success, quantum communication still needs more investigations

to deal with issues related to security, data rate, and communication distance [23–25, 93, 118–120].

The Chinese quantum satellite Micius is one of the several Microsatellite missions launched in the year 2016 which consists of a big platform with a dedicated technology demonstration. This is a space-based quantum key distribution (QKD) system. For the commercial purpose, satellite-based QKD systems must be cost effective, small in size and reliable for real-field applications [60, 68].The cryptographic key for implementing QKD technology aboard the Chinese satellite Micius, part of the quantum experiments at space scale (QUESS) mission placed into orbit in August 2016 and a number of quantum-optical experiments have been developed and conducted in recent times [60, 68, 94–97].

There are a number of projects running, ranging from QKD technology verification within orbit to setting up fully automatic links and key exchange with many ground stations based on optical setup. Some of the relevant examples in this regard are the Japanese SOTA (small optical transponder) laser communication terminal onboard the microsatellite SOCRATES (space optical communications research advanced technology satellite), a hot-air balloon and photon reflection experiment was performed between the LAGEOS satellite (laser geodynamics satellite or laser geometric environmental observation survey, using action of corner-cube reflectors) and the Italian Matera Laser-Ranging Observatory (MLRO) as well as a recent Chinese experiment with a small payload on Tiangong-2 Space Lab in the Chinese Micius satellite. Further, QKD links between ground stations and airplanes have been demonstrated by many academic groups in Canada, Germany, Waterloo and Munich [60, 68, 98].

Currently, most of the projects are aimed towards development of technology. National University of Singapore has investigated entangled-photon on nanosatellite. QUTEGA is a German national quantum technologies funding scheme, which will build a nanosatellite to carry a quantum payload with numerous sources embedded in photonic chip technique. The Canadian government is funding an important project known as QEYSSat. The aim of the project is to establish a microsatellite into orbit to carry a single photon detection system. Thus, this is different from other projects, in which a receiver is used in the setup placed in space. This is an important mission which is developed for radiation-hard single-photon detection systems, polarization-mapping assembly and a fine-pointing system. Other countries are also performing quantum-based satellite communication projects. Some of them are CubeSat Quantum Communications Mission started by U.K. and NanoBob project started by France and Austria [60, 68].

The SpaceQuest experiment, which was jointly developed by the University of Waterloo and the German aerospace company OHB System, is mainly used for the testing of quantum-physical effect known as gravitationally induced decoherence. The subsystem was mainly developed by University of Waterloo, in which quantum key distribution is a secondary mission [60, 68]. In addition to the successful Chinese experiments, several satellite based quantum communication schemes [17, 34, 35, 55, 69–73, 75–84, 86–88, 113] have also been proposed.

In this paper, we have analyzed the performance of Quantum Key Distribution (QKD), in satellite-earth down and up, and in intersatellite links, with two QKD protocols: SARG04 and BB84, with and without decoy states. In real field applications, we have considered real telescope dimensions and usual atmospheric conditions before sunset, 5 dB and 11 dB, in clear summer

day. In addition to this, we have considered two specific attacks the photon number splitting, and the intercept-resend with unambiguous discrimination attacks. We have not included losses due to pointing errors or misalignment of the optics. These effects can be included in the term δ_{diff}, as an additional diffraction (geometric loss). These losses if taken into account, would only shift, slightly, the communication distance axis to the right. Various results related to secure key generation rate and communication distance are calculated with and without decoy states for each protocol. In addition to these, effect of mean photon number on secure key generation rate as well as on communication distance is investigated. The results shown that, it is feasible to establish quantum key distribution with LEO (Low Earth Orbit) satellites, but not possible with GEO (Geostationary earth orbit satellites). The optimum mean photon number for SARG04 with two decoy states does not depend on distance between transmitter and receiver (link distance), which underscores its importance to perform well in a real scenario.

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

2 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.

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].

$$\begin{aligned} \delta_{diff} &= (e^{-2\gamma_t^2\alpha_t^2} - e^{-2\alpha_t^2})(e^{-2\gamma_r^2\alpha_r^2} - e^{-2\alpha_r^2}), \\ \gamma_t &= \frac{b_t}{R_t}, \gamma_r = \frac{b_r}{R_r}, \alpha_t = \frac{R_t}{\omega_t}, \alpha_r = \frac{R_r}{\omega_r}, \\ \omega_t &= R_t, \omega_r = \frac{\sqrt{2}\lambda L}{\pi R_t}, \end{aligned} \tag{1}$$

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), λ is the considered wavelength and $\omega_{t,r}$ is the beam radius at transceiver ends.

We are not considering losses due to pointing errors or misalignment of the optics. These effects can be included in the term δ_{diff}, as an additional diffraction (geometric losses). These losses if taken into account, would only shift, slightly, the communication distance axis to the right.

The atmospheric attenuation δ_{atm} is due to various phenomena such as turbulence, scattering and absorption. Hence it can be written as $\delta_{atm} = \delta_{scatt}\delta_{abs}\delta_{turb}$, where each quantity represents the attenuation of the corresponding phenomena. Here absorption and scattering depend on elevation angle and direction of transmission. The effects due to atmospheric turbulence are enlarged beam divergence, results in less amount of signal power collected by the receive telescope. Other effects generated due to turbulence are decoherence, beam-wander, scintillation and pulse distortion and

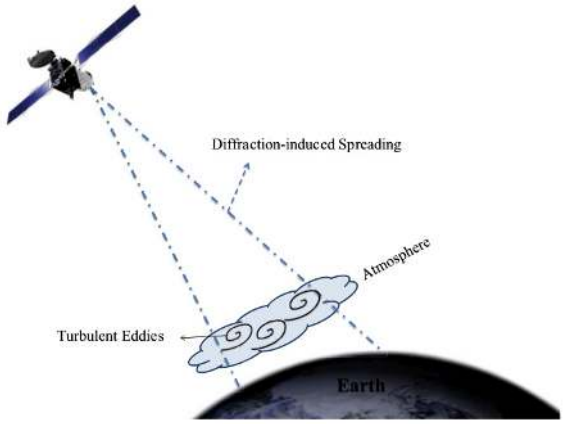

Fig. 1 Beam-spreading in downlink scenario [117].

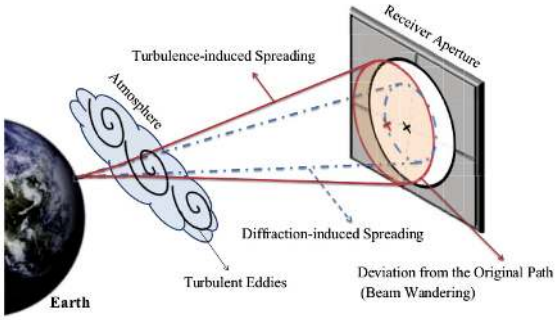

Fig. 2 Beam-wandering and beam-spreading in uplink scenario [117].

broadening. The turbulence effects are different for ground to space and space to ground scenarios. In a space to earth scenario light first propagates through vacuum for larger distances before being affected by the atmospheric turbulence, whereas in earth to space scenario, beam spreading effects due to turbulence occur at the beginning of the photon propagation, which causes a high value of divergence. These generic scenarios are depicted in Figures 1 and 2. More detailed description of free space optics and turbulence effects can be obtained from [30–32, 34, 69]. Gas molecules and aerosols absorb the light when it passes through the atmosphere. Turbulence is the main factor which contributes in atmospheric attenuation. This is because of thermal fluctuation which produce refractive index variations. The main factors which determine turbulence are the atmospheric conditions and the position of the ground station [69]. Turbulence effects are calculated by increasing the divergence angle of the beam. In uplink, attenuation caused by turbulence is calculated as [34]

$$\delta_{turb} = \frac{\left(\frac{\lambda}{R_t}\right)^2}{\left(\frac{\lambda}{R_t}\right)^2 + \theta_{turb}^2}, \tag{2}$$

where θ_{turb} is the additional divergence, in radians, produced by turbulence. The expression for θ_{turb} is, $\theta_{turb} = \frac{\lambda}{r_0}$, where r_0 is Fried parameter. $r_0 \approx (\lambda)^{\frac{6}{5}}$. Total channel attenuation is written as

$$\delta = \delta_{diff}\delta_{atm}\delta_{rec}. \tag{3}$$

The above equation for total attenuation (δ) is represented in dB (dB is calculated as $10log_{10}(\delta)$ $= 10log_{10}(\delta_{diff}) + 10log_{10}(\delta_{atm}) + 10log_{10}(\delta_{rec})$). In above equation δ_{diff}, δ_{atm} and δ_{rec} represent attenuation due to geometrical losses, atmospheric losses and losses due to receiver inefficiency, respectively. In our current work, we are using Eq. 3 for calculating total attenuation (δ) which also includes attenuation due to detector inefficiency. In case of uplink (ground to space links), the total attenuation (δ), excluding attenuation due to detector efficiencies, can also be written as

$$\delta = \frac{L^2\left(\theta_T^2 + \theta_{atm}^2\right)}{D_R^2}\frac{1}{T_T\left(1 - L_P\right)T_R}10^{A_{atm}/10}, \tag{4}$$

where A_{atm} is the attenuation of the atmosphere in dB. $A_{atm} = 1$ dB for excellent sight conditions (no haze, fog, or clouds) and is valid only in certain wavelength region. $\theta_T = \frac{\lambda}{D_T}$, here θ_T is the divergence angle resulting from the transmit telescope. D_T is the diameter of the transmit telescope. L_P represents pointing loss. T_T and T_R are the telescope transmission factors. We consider $T_T = T_R = 0.8$. Here we are considering $L_P = 0$. r_0 is 9 cm for 800 nm. In above equation, $\delta_{rec} = 3$ to 3.5 dB attenuation must be added which is due to detector efficiency operating in the wavelength range of 650 nm to 1550 nm. The satellite telescopes radius of the primary and secondary mirrors are 15 cm and 1 cm, respectively. The ground telescope radius of the primary and secondary mirrors are 50 cm and 5 cm, respectively. The values of telescope radii have been obtained from the SILEX Experiment [56] and the Tenerife's telescope [55]. The scattering and absorption attenuation is evaluated using a model of clear standard atmosphere [58] which results in $\eta_{scatt} = 1\ dB$.

For calculating total channel attenuation, the considered parameters are shown in Table 1. We have considered $\lambda = 650nm$, it seems reasonable because suitable avalanche photo detector (silicon avalanche photo detector) for single photon detection is available. At telecom wavelength, $\lambda = 1550\ nm$, link attenuation increases due to high beam divergence at large wavelength and due to higher absorption in the atmosphere. At $\lambda = 1550\ nm$, due to longer wavelength, the photon becomes weaker, hence detection of single photon particularly at this telecom wavelength becomes difficult to detect. The present quantum technology exists between 700-800 nm wavelength range, which is close to visible light and effect of natural light pollution starts dominating. In addition to this, sunlight intensity at 1550 nm is five times weaker than at 800 nm, this is the reason that background noise has to reduce at a very low level, hence it is another difficult task to perform at this telecom wavelength.

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.

3 THE SECURE KEY RATE ANALYSIS WITH DIFFERENT PROTOCOLS

Here we study BB84 and SARG04 QKD protocols, with and without decoy states, under two specific attacks, namely PNS (photon number splitting) and IRUD (intercept-resend with unambiguous discrimination) attacks.

3.1 The BB84 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].

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{5}$$

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

$$P_n(\mu) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} = e^{-|\mu|} \frac{|\mu|^n}{n!} \tag{6}$$

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 μ (mean photon number) which ranges from 0.1 to 0.5. Here 0.1 indicates 1 photon every 10 pulses [13,17,72]. For bit encoding in QKD system, the polarization 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 [43, 61]. Here,

$$I(A:B) = \sum_{n=0}^{\infty} \Big(1 - (1-\delta)^n\Big) P_n(\mu) \approx \mu\delta, \tag{7}$$

$$I(B:E) = \sum_{n\geq 2}^{\infty} P_n(\mu). \tag{8}$$

Eve's Information, I_{Eve}, is defined as

$$I_{Eve} \approx \frac{I(B:E)}{I(A:B)}. \tag{9}$$

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

$$R \geq q\bigg(- Q_\mu f(E_\mu) H_2 E_\mu + \Omega Q_\mu \Big(1 - H_2\Big(\frac{E_\mu}{\Omega}\Big)\Big)\bigg), \tag{10}$$

where Ω ($\Omega = 1 - I_{Eve}$)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].The yield of the n-photon pulses is represented as Y_n [44].

The expected raw key rate can be written as [50]

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_n(\mu). \tag{11}$$

Quantum Bit Error Ratio (QBER), E_μ, is [50]

$$E_\mu = \frac{\sum_{n=0}^{\infty} Y_n P_n(\mu) e_n}{Q_\mu} = \frac{Y_0}{2Q_\mu}. \tag{12}$$

Here, Y_0 represents dark counts.The above expression is due to the bit error ratio of n-photon signals being $e_n = \frac{Y_0}{2Y_n}$, given that the dark counts, Y_0, are the only effect causing QBER. Also, for binomial probability distribution, $\sum_{n=0}^{\infty} P_n(\mu) = 1$.

3.2 The SARG04 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 [61]. 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 ω, $\omega' \in \{+,-\}$ and $|\pm x\rangle = 0, |\pm z\rangle = 1$, [46–48].

Comparison between SARG04 and BB84 QKD protocols

The SARG04 protocol protects against the PNS attack, without extra resources. In the BB84 protocol, Alice and Bob use two non-orthogonal polarization bases Z($|V\rangle$, $|H\rangle$) and X($|45^\circ\rangle$, $|-45^\circ\rangle$). Alice randomly sends one of the four non-orthogonal polarization states ($|V\rangle$, $|H\rangle$, $|45^\circ\rangle$, and $|-45^\circ\rangle$). After quantum communication is completed, Alice and Bob each disclose their basis. However, the SARG04 protocol uses four sets: $s_1 = (|V\rangle, |45^\circ\rangle)$, $s_2 = (|V\rangle, |-45^\circ\rangle)$, $s_3 = (|H\rangle, |45^\circ\rangle)$, and $s_4 = (|H\rangle, |-45^\circ\rangle)$. Alice randomly sends one of the two non-orthogonal polarization states in the randomly selected set; Bob uses either the Z basis or the X basis to measure the photon. After quantum communication is finished, Alice and Bob exchange the information of Alice's selected set and Bob's measuring basis. Thus, quantum communication in SARG04 is identical to the BB84 protocol; only the classical key sifting procedure is modified. At that time, SARG04 is secure for two photon pulses. For example, if Alice sends $|V\rangle$ with two-photon pulses and discloses $s_1 = (|V\rangle, |45^\circ\rangle)$, then Eve obtains $|V\rangle$ by the Z basis and measures $|45^\circ\rangle$ or $|-45^\circ\rangle$ with 50 % probability by the X basis. Eve cannot differentiate the state from her measurement in two-photon pulses. Hence, SARG04 produces a secret key from one-photon and two-photon pulses, whereas BB84 produces a secret key from one-photon pulses. The SARG04 protocol can generate the secret key even when a pulse contains two photons, because Eve cannot get full information of Alice's key from the two-photon pulse [114].

At first, a photon number non-demolition quantum measurement is performed during IRUD attack; if a pulse has one or two photons, Eve blocks it, otherwise she performs a generalized quantum measurement. If the measurement is conclusive, she uses a transparent quantum channel to send a copy of the state to Bob.

In IRUD attack, Eve introduces some attenuation. If the channel attenuation is less than that introduced by the IRUD attack, Eve should apply a different strategy, otherwise her presence would be immediately detected. In such circumstances, she blocks a fraction t of the single-photon pulses, keeps one photon from each two-photon pulse, and performs the IRUD attack on the rest of the multi-photon pulses. Then, the attenuation can be written as

$$\delta = \frac{(1-t)P_1 + P_2(\mu) + \chi}{\mu}, \quad t \in [0,1]. \tag{13}$$

Here χ is expressed as

$$\chi = \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n), \tag{14}$$

where P_{ok} represents the probability of acceptance. For BB84 protocol, this value is 0.5 [45,48]. The value of P_{ok} depends on the number (n) of photons of the state and the overlap of the basis, but it is not less than $\frac{1}{2}$ [46–48]. Using this attack, Eve does not obtain information from single-photon pulses.

In general, $P_n(\mu)$ is the Poisson probability distribution of photons for every weak laser pulse of the transmitter, taking into account the assumption that there are n photons in a pulse. In the same context, P_1 and P_2 represent probability of 1 and 2 photon(s) attenuation.

In PNS attack, Eve first performs a photon number non-demolition measurement to identify Alice's multi-photon signals. Eve blocks all single photon pulses, while for multi-photon pulses she stores one photon in a quantum memory, and resends to Bob the remaining photons by a transparent quantum channel. When Eve performs the PNS attack, she introduces some attenuation. If this attenuation is lower than the channel attenuation, Alice and Bob can not notice the presence of Eve, and thus Eve can obtain full information. *If the attenuation introduced by PNS attack is more than the allowed channel attenuation, Eve has to apply different strategy to hide her presence.*

In SARG04 QKD protocol information is encoded in four nonorthogonal states, when a generalized measure is performed, it is necessary to have at least three copies of the state to obtain a conclusive result with probability $P_{ok}(n)$ [21,47]. Therefore, in order to obtain full information, Eve must carry out an IRUD attack (Intercept-Resend with Unambiguous Discrimination).

If the attenuation introduced during IRUD attack carried out by Eve, is more than the channel attenuation, her presence can easily be detected by the authenticate users (Alice and Bob). In a high-attenuation channel, Eve may extract full information about the key. This is the reason that Eve does not apply PNS attack in such conditions. Hence, she applies a different strategy to hide her presence, depicted in Eq. 13.

The attenuation introduced by Eve in Eq. 13 is defined as the ratio between the mean number of photons that are received and the mean number that would be received in the absence of attenuation (i.e. μ). According to Eve's planning, discussed above, the mean number of photons obtained can be calculated as the sum of a fraction (1 - t) of the single-photon pulses, plus one photon for each two-photon pulse, plus one photon for the pulses with three or more photons that lead to conclusive measurements. This last term is denoted by χ.

Similarly, Eve blocks a fraction s of the two photon pulses and apply IRUD attack on the remaining multi-photon pulses, to hide herself, as represented by Eq. 15. The attenuation in this case can be written as

$$\delta = \frac{(1-s)P_2(\mu)+\chi}{\mu}, \quad s \in [0,1]. \tag{15}$$

Fig. 3 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 the BB84 protocol as compared to SARG04 protocol. Hence, it can be concluded that SARG04 protocol outperforms the BB84 protocol under such specific conditions.

In SARG04 protocol, the secret key can be generated with both single photon and two-photon states. The SARG04 protocol can generate the secret key even when a pulse contains two photons, because Eve cannot get full information of Alice's key from the two-photon pulse [114], as shown in Fig. 3.

3.3 Protocols with the decoy-states: An effective approach to counter 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 [63, 64, 89]. The shared mutual information is

$$I(A:B) = P_1(\mu)(1-t) + P_2(\mu)(1-s) + \sum_{n\geq 3}^{\infty} P_n(\mu)P_{ok}(n), \tag{16}$$

$$I(B:E) = P_2(\mu)(1-s)I_2 + \sum_{n\geq 3}^{\infty} P_n(\mu)P_{ok}(n), \tag{17}$$

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 protocol: Vacuum + weak decoy state:

A lower bound on the key generation rate [50, 99], based on entanglement distillation described in [53] which in turn use the concept of decoy-state, is

$$R_{BB84} \geq q\Bigg(- Q_\mu f(E_\mu) H_2(E_\mu) + Q_1\Big(1 - H_2(e_1)\Big)\Bigg), \tag{18}$$

where Q_μ represents the gain of the signal state, E_μ 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]

$$Q_1 = Y_1 e^{-\mu}\mu. \tag{19}$$

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

$$Y_1^L = \frac{\mu}{(\mu\nu - \nu^2)}\left(Q_\nu e^\nu - Q_\mu e^\mu\Big(\frac{\nu^2}{\mu^2}\Big) - \frac{(\mu^2 - \nu^2)}{\mu^2}Y_0\right) \leq Y_1, \tag{20}$$

$$Q_1^L = \mu e^{-\mu} Y_1^L \leq Q_1, \tag{21}$$

$$e_1^U = \frac{e_0 Y_0}{Y_1^L} \geq e_1. \tag{22}$$

2) The SARG04 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 the SARG04 protocol [54]. Taking this into account with the approach developed in [53], the gain in case of two-photon pulses is [43,54]

$$Q_2 = Y_2 e^{-\mu}\frac{\mu^2}{2}. \tag{23}$$

The SARG04 protocol uses three decoy states, ν_0, ν_1 and ν_2, assuming that ν_0 is the vacuum (i.e. $\nu_0 = 0$), and the two weak decoy states are ν_1 and ν_2. For these decoy states, gain and quantum bit error rate are [50]

$$Q_{\nu_i} = \sum_{n=0}^{\infty} Y_n P_n(\nu_i), \tag{24}$$

$$E_{\nu_i} = \sum_{n=0}^{\infty} \frac{Y_n P_n(\nu_i) e_n}{Q_{\nu_i}}. \tag{25}$$

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 ν_1 and ν_2 which satisfy [50]

$$0 < \nu_1 < \nu_2, \;\; \nu_1 + \nu_2 < \mu. \tag{26}$$

Now the key generation can be shown to be [50]

$$R_{SARG04} \geq q\Bigg(- Q_\mu f(E_\mu) H_2(E_\mu) + Q_1\Big(1 - H\Big(\tfrac{Z_1}{X_1}\Big)\Big) + Q_2\Big(1 - H(Z_2)\Big)\Bigg), \tag{27}$$

where X_n and Z_n represents the binary random variables. $H_2(.)$ is the Shannon's binary entropy function [43].

In Eq. 27, we can replace $H(Z_1/X_1)$ with $H_2(e_1)$, and $H(Z_2)$ with $H_2(e_2)$, because Eve's attacks (i.e. IRUD attack) does not introduce phase error or bit errors, and we assume that the only source of errors, i.e. the dark counts, is independent of the signal, phase and bit errors which are independent from each other and have the same distribution.

The lower limit of the two photon gain is [50]

$$Q_2^L = \frac{Y_2^L \mu^2 e^{-\mu}}{2} \leq Q_2. \tag{28}$$

The upper limit of e_2 can be manipulated by considering quantum bit error rate of weak decoy states [50].

$$E_{\nu_i} Q_{\nu_i} e^{\nu_i} = e_0 Y_0 + e_i \nu_i Y_1 + e_2 \frac{\nu_i^2}{2} Y_2 + \sum_{n=3}^{\infty} e_n Y_n \frac{\nu_i^n}{n!}. \tag{29}$$

4 Results

The results shown here are based on three scenarios: uplink, downlink, and intersatellite links. The parameters for link establishment (shown in Table 1) are detector efficiency (δ_{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) [112, 113] and wavelength (λ) whose values are 65%, 15 cm, 1 cm, 50 cm, 5 cm, 50×10^{-6} counts/pulse and 650 nm, respectively. $\lambda = 650\ nm$ represents an absorption window with a commercial detector made of silicon avalanche photo diode with high detection efficiency. Silicon avalanche photo diode with internal gain can work with high data rate. The optical efficiency in the receiver $(f) = \frac{c}{\lambda}$; for 650 nm wavelength, frequency will be 4.61538×10^8 MHz, which is 461.538 THz. The 650 nm region is close to the highest efficiency detection region (65%). The optical frequency (for example of a quasi-monochromatic laser beam) is the oscillation frequency of the corresponding electromagnetic wave. For visible light, optical frequencies are roughly between 400 THz (terahertz = 10^{12} Hz) and 700 THz, corresponding to vacuum wavelengths between 700 nm and 400 nm. We assume a wavelength in the 650 nm region because the diffraction spread is the smallest. Silicon avalanche photo diodes are deployed to detect the wavelengths in between 250 nm and 1100 nm. These photo diodes detect even the very weak light intensities and very fast optical signals because of their avalanche effect. The absorption spectrum of silicon is quite broad. Visible wavelengths (400-1100 nm) are serviced by silicon avalanche photodiode which has > 50 % detection efficiency with maximum count rates in MHz range and low

dark counts. InGaAs avalanche photo diodes and superconducting single photon detectors detect infrared wavelengths (950 - 1650 nm). The major drawbacks of InGaAs avalanche photo diodes (APD) are higher dark count rates, lower detection efficiencies and low repetition rates. These are the reasons that InGaAs APDs are not used for satellite mission. Telescope radius values are taken from [55, 56].

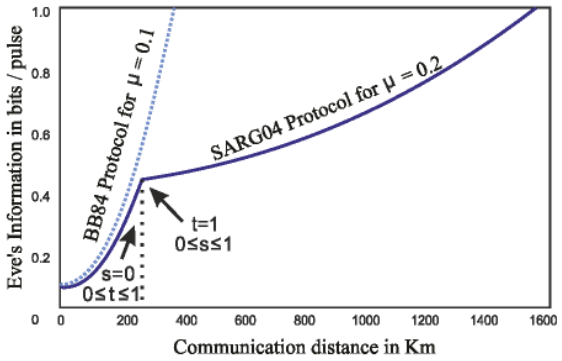

Fig. 3 Variation in Eve's information with communication distance for each protocol under the uplink case ($\delta_{turb} = 5\ dB$) calculated using Eqs. 7, 8, 9, 13, 14, and 15.

The attenuation caused by turbulence in the uplink scenario is computed considering two usual atmospheric scenarios, one for $\delta_{turb} = 5$ dB (before sunset) and other for $\delta_{turb} = 11$ dB (in a clear summer day) [57]. Effect of turbulence on the downlink is almost negligible [69], as shown in Tables 2 and 3. A value of $\delta_{scatt} = 1$ dB is achieved for the scattering plus absorption attenuation with the help of Clear Standard Atmosphere model [58]; these values are similar to those discussed in [34, 69]. In Fig. 3 we simulated the considered system parameters to interrelate the attenuation with distance and the condition $I_{Eve} = 1$ is achieved for the optimum parameters (attenuation = 13 dB, $\mu = 0.1$ for BB84 protocol and attenuation = 25.6 dB, $\mu = 0.2$ for SARG04 protocol) [46].

In Fig. 4 we have shown the dependency of key generation rates on the communication distance for the considered protocols. The pulses emitted from the laser source can be converted from bits/pulse to bits/second [36]. We take the values of μ and ν which are mean photon numbers of signal state and decoy states, respectively, in the range of $[0, 1]$ with a step 0.001. The number of pulses used as the signal state and the vacuum state are $N_\mu = 0.95N$, and $N_0 = 0.05\ N$ (sent by Alice), where $N = 100\ Mbit$. In Fig. 5, we have optimized μ and $\nu_i^{'s}$ in each protocol for both the states to obtain the highest key rate.

In Fig. 4, it is observed that critical distance obtained for SARG04 is comparatively higher than BB84, both with and without decoy states. Also in Fig. 4, 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

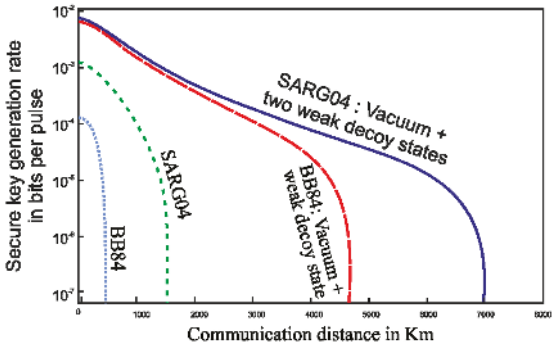

Fig. 4 In uplink ($\delta_{turb} = 5\ dB$), secure key generation rate for all protocols under investigation calculated using Eqs. 10, 18, and 27.

helps in reducing the chance of attacks performed by Eve (in this case μ must be decreased) as shown in Fig. 5. At the higher value of μ, 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 the satellite along its orbit, its distance with the ground station varies. The value of μ has to be adjusted to achieve the maximum secure rate, which is the challenging part of the problem.

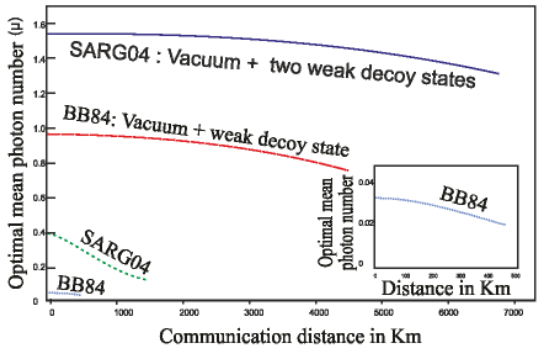

Fig. 5 Variation in optimum mean photon number with communication distance for all protocols under the uplink case ($\delta_{turb} = 5\ dB$). These variations in μ correspond to the highest achievable secure rates, as shown in Fig. 4.

.

In Fig. 6, for each protocol in uplink scenario, secure key generation rate decreases at constant value of μ, which is independent of the distance. This is the maximum value at maximum distance for the protocols under analysis. In this figure, for the protocols based on decoy states, we get comparatively low decrease (less than 3%), which clarify that the dependency of μ on distance is not required. In case of other protocols, keeping μ constant, secure key rate decreases by 25% and 50% from their maximum values at short distances. The results depicted in Fig. 6, for each protocol indicates the maximum key generation rates, keeping μ constant to that of optimal μ for maximum distance. It is clearly observed that in case of protocols based on decoy states the

Table 1 Link Parameters for uplink, downlink and intersatellite links

Considered Parameters	Numerical Values
Detector efficiency (δ_{rec})	65%
Wavelength (λ)	650 nm
Dark Counts (Y_0) [112, 113]	50×10^{-6} counts/pulse
Ground secondary mirror radius ($b_{t,r}$)	5 cm
Satellite secondary mirror radius ($b_{t,r}$)	1 cm
Ground telescope radius ($R_{t,r}$)	50 cm
Satellite telescope radius ($R_{t,r}$)	15 cm

Table 2 Critical distance for different protocols under consideration [Km]

Scenarios	BB84	SARG04	BB84:Vacuum + weak decoy state	SARG04:Vacuum + two weak decoy state
Downlink	1540	3290	9450	14100
Intersatellite	430	920	2660	3900
Uplink(δ = 5 dB)	460	1520	4650	6980
Uplink(δ= 11 dB)	-	500	2200	3460

Table 3 Maximum possible secure rate for different protocols under consideration [Bits/Pulse]

Scenarios	BB84	SARG04	BB84:Vacuum + weak decoy state	SARG04:Vacuum + two weak decoy state
Downlink	$1.7.10^{-2}$	$2.4.10^{-2}$	$4.4.10^{-2}$	$4.6.10^{-2}$
Intersatellite	$2.0.10^{-2}$	$2.6.10^{-2}$	$4.8.10^{-2}$	$5.0.10^{-2}$
Uplink(δ = 5 dB)	$1.4.10^{-4}$	$1.2.10^{-3}$	$5.8.10^{-3}$	$6.5.10^{-3}$
Uplink(δ= 11 dB)	-	$7.5.10^{-5}$	$1.4.10^{-3}$	$1.6.10^{-3}$

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 in clear weather conditions and inter satellite links) follows the same steps.

It would be appropriate, at this juncture, to make a comparison between the results obtained here and the pertinent literature:

1. The total channel attenuation is the result of three effects, it is given by

$$\delta = \delta_{diff}\delta_{atm}\delta_{rec}.$$

.

The total channel attenuation is represented by δ. In above equation δ_{diff} , δ_{atm} and, δ_{rec} represent attenuation due to geometrical losses, atmospheric losses and losses due to receiver inefficiency, respectively. We have taken into account this total channel attenuation in our current work, *whereas*

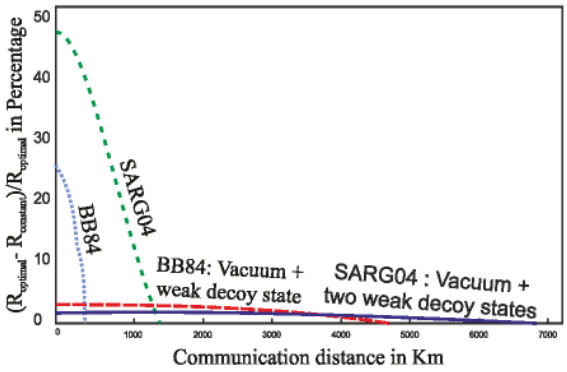

Fig. 6 (Color online) Blue (dotted) :- BB84; Green (small dashed):- SARG04; Red (large dashed):- BB84: Vacuum+weak decoy state; Purple (continuous dark line):- SARG04: Vacuum+two weak decoy states. In the uplink scenario ($\delta_{turb} = 5\ dB$), for each protocol, variation in secure key rate (R) with communication distance at constant value of mean photon number calculated using Eqs. 10, 18, and 27.

such type of channel attenuation is not used in [54, 114, 116].

2. This work is focused on realistic scenarios of satellite uplink, downlink and intersatellite quantum communication. We are considering two specific type of attacks; PNS (photon number splitting) attack and *IRUD (intercept-resend with unambiguous discrimination) attacks* [21, 47]. The results shown are *valid for these specific attacks*, and hence, our tabulated values differ from that in [115, 116], *where IRUD attack was not considered.*

When Eve performs the PNS attack, she introduces some attenuation. If this attenuation is less than the channel attenuation, Alice and Bob can not notice the presence of Eve, and thus Eve can obtain full information. Eve introduces no errors when performing the PNS attack.

3. We assume that the dark counts of the detector are the only source of quantum bit errors, which are quantified by the quantum bit error ratio (QBER). In addition to this, we considered dark count $(Y_0) = 50 \times 10^{-6}$ [112, 113], which comes in the detection range of the considered detector, i.e., Si-APD (silicon avalanche detector); whereas value of dark count (Y_0) is 1.7×10^{-6}, in [115, 116]. We have considered values of the parameters given in Table 1.

4. The lower bound of the key generation rate for SARG04 is given in Eq. 27 [54], where X_n and Z_n represent the bit error and the phase error events, respectively, for n-photon pulses. X_n and Z_n are binary random variables, they take a value equal to one when there is a bit or phase error, and zero othersiwe. H(.) is the Shannon entropy of a random variable [43]. *The specific class of Eve's attacks we are considering (i.e., IRUD attack) does not introduce phase error or bit errors, and the only source of errors, i.e., the dark counts, is independent of the signal, phase and bit errors which are independent from each other and have the same distribution. Hence, we can replace* $H(\frac{Z_1}{X_1})$ *with* $H_2(e_1)$*, and* $H(Z_2)$ *with* $H_2(e_2)$*. Here* e_1 *is the error rate of single-photon states.*

Tables 2 and 3 exhibit the critical distance and secure key generation rate for both BB84 and SARG04 protocols, with and without decoy states. The critical distances and secure key generation rates in the downlink are significantly larger as compared to uplink scenario, due to lack of turbulence induced attenuation in downlink scenario. In addition to this, in MEO satellite downlink quantum communication with decoy states quantum key distribution protocols are possible. These optimum results are not possible in case of intersatellite quantum communication links, due to reduced telescope dimensions. The most challenging and difficult part in such realistic scenarios are turbulence generated attenuation and telescope dimensions. Comparing all these tabulated results in such realistic scenarios and specific attacks considered here, we conclude that SARG04 QKD protocol with decoy states outperforms the BB84 protocol in terms of both a higher secret key rate and greater secure communication distance.

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 μ.

In the uplink scenario, secure key generation is low because of high attenuation [93,100,113]. At the same time, the value of μ cannot be increased due to PNS (photon number splitting) attack. To minimize the effects of PNS attack and to increase the secure key generation rate WCP (weak coherent pulse) is preferred over entangled photon source [99,113]. The background count rate for uplink is higher than downlink because of artificial light pollution emitted upward [113]. Our results show significant design considerations, e.g., type and features of detectors and sources, operating wavelength, ground station locations, specific orbits and telescope design.

Power needed at ground station is more as compared to the power needed at the satellite. The main reason for this is that uplink frequency is set high as compared to downlink frequency. In uplink, attenuation is more because of turbulence effects. Hence we need powerful devices to send signals. In addition to this, it is much easier to compensate losses due to attenuation on earth due to no weight limitation. On the other hand, weight and space limitations are predominant on the satellite, hence the need to minimize attenuation [101,102].

Attenuation and frequency are directly related to each other. Signal losses are higher for higher frequencies, hence more power is required for efficient transmission. The beam of lower frequency is broad whereas a beam of higher frequency is narrow. Earth station has to focus the signal to a small point on satellite in space, which is performed by deploying a narrow beam generated by higher frequency [103,104].

Satellite covers a large area on the ground by providing service to many earth stations, using broad beam generated by lower frequency [105,106]. For visible wavelengths, turbulence effects come into picture when using a transmitter telescope of more than 25-50 cm diameter [107,108]. Turbulence effects can be minimized by selecting a good ground station [69]. In addition to this, an adaptive optics system can be used to minimize the turbulence effects [109,110].

5 Conclusion

We have used realistic scenarios for investigating the feasibility of quantum key distribution, in satellite quantum communication; uplink, downlink and intersatellite links, with BB84 and SARG04 QKD protocols. We have implemented these protocols with and without decoy states for supporting future satellite quantum communication systems. For this reason, we have used practical values of optical hardware and used normal atmospheric conditions. In addition to this, we assumed two specific attacks, namely PNS (photon number splitting) and IRUD (intercept-resend with unambiguous discrimination), which could be main threats for future QKD based satellite applications. The key generation rates and the error rates of the considered QKD protocols are presented. Other parameters such as optimum signal and decoy states mean photon numbers are calculated for each protocol and distance. Our results indicate that, it is possible to establish LEO (Low Earth Orbit) and, MEO (Medium Earth Orbit) satellites. Further, in SARG04 QKD protocol with two decoy states, the optimum signal-state mean photon number is independent of the link distance. This could enhance its significance in a realistic scenario of satellite quantum communication. These results are valid for the specific attacks considered here.

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 photon 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.

Downlink performance is better than uplink scenario, the reason being that we can place heavy receiving telescopes on earth as compared to space. Also most of the time the beam propagates in vacuum with small diffraction spreading and comes under the effect of atmospheric turbulence in the final stage of propagation.

In this work low earth orbits (altitude upto 1000 km) are considered. They provide advantages of lower optical loss, less costly to attain and easy to operate than higher orbits, making them feasible in near future. To reduce background noise, quantum key distribution link can be performed at nighttime. Hence, one can aim to achieve a global scale quantum key distribution.

Acknowledgements

VS would like to thank the Ministery 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.

References

1. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and con tos5. (1984).
2. N Srinatha, S Omkar, R Srikanth, Subhashish Banerjee, and Anirban Pathak. The quantum cryptographic switch. *Quantum information processing*, pages 1–12, (2014).
3. Nicolas 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).
4. Pathak, Anirban and Srikanth, R and others Quantum cryptography: key distribution and beyond. *arXiv preprint arXiv:1802.05517*, (2018)
5. Félix Bussières, Nicolas Sangouard, Mikael Afzelius, Hugues de Riedmatten, Christoph Simon, and Wolfgang Tittel. Prospective applications of optical quantum memories. *Journal of Modern Optics*, **60**(18):1519–1537, (2013).
6. 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).
7. 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).
8. Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature communications*, **6**, (2015).
9. Sreraman Muralidharan, 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).
10. K Boone, J-P Bourgoin, E Meyer-Scott, K Heshami, T Jennewein, and C Simon. Entanglement over global distances via quantum repeaters with satellite links. *Physical Review A*, **91**(5):052325, (2015).
11. Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, **74**(1):145, (2002).
12. Theresa H Carbonneau and David R Wisely. Opportunities and challenges for optical wireless: the competitive advantage of free space telecommunications links in today's crowded marketplace. In *Voice, Video, and Data Communications*, pages 119–128. International Society for Optics and Photonics, (1998).
13. Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, **5**(1):3–28, (1992).
14. Hugo Zbinden, Nicolas Gisin, Bruno Huttner, Antoine Muller, and Wolfgang Tittel. Practical aspects of quantum cryptographic key distribution. *Journal of Cryptology*, **13**(2):207–220, (2000).
15. PCM Owens, JG Rarity, PR Tapster, D Knight, and PD Townsend. Photon counting with passively quenched germanium avalanche. *Applied Optics*, **33**(30):6895–6901, (1994).
16. 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).
17. KJ Resch, M Lindenthal, B Blauensteiner, HR Böhm, A Fedrizzi, C Kurtsiefer, A Poppe, T Schmitt-Manderbach, M Taraba, R Ursin, et al. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Optics Express*, **13**(1):202–209, (2005).
18. Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, **48**(3):351–406, (2001).
19. Andrew Shields and Zhiliang Yuan. Key to the quantum industry. *Physics World*, 20(3):**24**, (2007).
20. Mehrdad S Sharbaf. Quantum cryptography: An emerging technology in network security. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pages 13–19. IEEE, (2011).
21. Practical free-space quantum key distribution over 1 km. Buttler, WT and Hughes, RJ and Kwiat, PG and Lamoreaux, SK and Luther, GG and Morgan, GL and Nordholt, JE and Peterson, CG and Simmons, CM, *Physical Review Letters*, **81**(15):3283, (1998).
22. Christian Kurtsiefer, P Zarda, M Halder, Ph M Gorman, Paul R Tapster, JG Rarity, and Harald Weinfurter. Long-distance free-space quantum cryptography. In *Photonics Asia 2002*, pages 25–31. International Society for Optics and Photonics, (2002).
23. Vishal Sharma. Effect of noise on practical quantum communication systems. *Defence Science Journal*, **66**(2):186–192, (2016).
24. S Omkar, R Srikanth, and Subhashish Banerjee. Dissipative and non-dissipative single-qubit channels: dynamics and geometry. *Quantum information processing*, **12**(12):3725–3744, (2013).
25. Vishal Sharma and Richa Sharma. Analysis of spread spectrum in matlab. *International Journal of Scientific & Engineering Research*, **5**(1), (2014).
26. Malvin Carl Teich and B Saleh. Fundamentals of photonics. *Canada, Wiley Interscience*, **3**, (1991).
27. Javier Alda. Laser and gaussian beam propagation and transformation. *Encyclopedia of optical engineering*, 2013:999–1013, (2003).

28. Bernard J Klein and John J Degnan. Optical antenna gain. 1: Transmitting antennas. *Applied optics*, **13**(9):2134–2141, (1974).
29. John J Degnan and Bernard J Klein. Optical antenna gain. 2: Receiving antennas. *Applied optics*, **13**(10):2397–2401, (1974).
30. Scott Bloom, Eric Korevaar, John Schuster, and Heinz Willebrand. Understanding the performance of free-space optics. *Journal of optical Networking*, **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 Buttler, 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 Fürst, 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).
44. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, **94**(23):230504, (2005).
45. Gilles Brassard and Claude Crépeau. Quantum cryptography. In *Encyclopedia of Cryptography and Security*, pages 495–500. Springer, (2005).
46. Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, **92**(5):057901, (2004).
47. Anthony Chefles. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, **239**(6):339–347, (1998).
48. Antonio Acin, Nicolas Gisin, and Valerio Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Physical Review A*, **69**(1):012309, (2004).
49. Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, **91**(5):057901, (2003).
50. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, **72**(1):012326, (2005).
51. Tomoyuki Horikiri and Takayoshi Kobayashi. Decoy state quantum key distribution with a photon number resolved heralded single photon source. *Physical Review A*, **73**(3):032331, (2006).
52. Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, **94**(23):230503, (2005).
53. Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, (2004).
54. Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo. Performance of two quantum-key-distribution protocols. *Physical Review A*, **73**(1):012337, (2006).

55. Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, **3**(7):481–486, (2007).
56. PV Gatenby and MA Grant. Optical intersatellite links. *Electronics & communication engineering journal*, **3**(6):280–288, (1991).
57. David G Aviv. *Laser Space Communications*. Artech House Publishers, (2006).
58. Louis Elterman. Parameters for attenuation in the atmospheric windows for fifteen wavelengths. *Applied optics*, **3**(6):745–749, (1964).
59. Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, **76**(1):012307, (2007).
60. Satellite-Based QKD Khan, Imran and Heim, Bettina and Neuzner, Andreas and Marquardt, Christoph, *Optics and Photonics News, Optical Society of America*, **29**(2), 26–33, (2018).
61. The security of practical quantum key distribution, Scarani, Valerio and Bechmann-Pasquinucci, Helle and Cerf, Nicolas J and Dušek, Miloslav and Lütkenhaus, Norbert and Peev, Momtchil, *Reviews of modern physics*, **81**(3), 1301, (2009).
62. Srinatha, N and Omkar, S and Srikanth, R and Banerjee, Subhashish and Pathak, Anirban, The quantum cryptographic switch, *Quantum information processing*, 1–12, (2014).
63. Elements of quantum computation and quantum communication, Pathak, Anirban, *Taylor & Francis*, (2013).
64. Protocols of quantum key agreement solely using Bell states and Bell measurement, Shukla, Chitra and Alam, Nasir and Pathak, Anirban, *Quantum information processing*, **13**(11), 2391–2405, (2014).
65. Optical wireless communications: system and channel modelling with Matlab, Ghassemlooy, Zabih and Popoola, Wasiu and Rajbhandari, Sujan, *CRC press*, (2012).
66. Physics of semiconductor devices, Hoboken, Sze, Simon M and Ng, Kwok K, *New Jersey: John Wiley*, **163**, 8–5, (2007).
67. Quantum Cryptography: Key Distribution and Beyond, Akshata Shenoy and Anirban Pathak and R. Srikanth, *Quanta*, **6**, 1-47, (2017).
68. Towards Quantum Communication from Global Navigation Satellite System, Calderaro, Luca and Agnesi, Costatino and Dequal, Daniele and Vedovato, Francesco and Schiavon, Matteo and Santamato, Alberto and Luceri, Vincenza and Bianco, Giuseppe and Vallone, Giuseppe and Villoresi, Paolo, *arXiv preprint arXiv:1804.05022*, (2018).
69. Ground to satellite secure key exchange using quantum cryptography, Rarity, JG and Tapster, PR and Gorman, PM and Knight, P, *New Journal of Physics*, **4**(1), 82, (2002).
70. Present and future free-space quantum key distribution, Nordholt, Jane E and Hughes, Richard J and Morgan, George L and Peterson, C Glen and Wipf, Christopher C, Free-Space Laser Communication Technologies XIV, *International Society for Optics and Photonics*, 4635, 116–127, (2002).
71. Quantum cryptography: A step towards global key distribution, Kurtsiefer, Christian and Zarda, P and Halder, Matthus and Weinfurter, H and Gorman, PM and Tapster, PR and Rarity, JG, *Nature*, **419**(6906), 450, (2002).
72. Practical free-space quantum key distribution over 10 km in daylight and at night, Hughes, Richard J and Nordholt, Jane E and Derkacs, Derek and Peterson, Charles G, *New journal of physics*, **4**(1), 43, (2002).
73. Free space quantum key distribution over 10km in daylight and at night, Hughes, Richard and Nordholt, Jane E and Morgan, George L and Peterson, Charles G, Nonlinear Optics: Materials, Fundamentals and Applications, *Optical Society of America*, FA2, (2002).
74. Satellite-based quantum communication terminal employing state-of-the-art technology, Pfennigbauer, Martin and Aspelmeyer, Markus and Leeb, Walter and Baister, Guy and Dreischer, Thomas and Jennewein, Thomas and Neckamm, Gregor and Perdigues, Josep and Weinfurter, Harald and Zeilinger, Anton, *Journal of Optical Networking*, **4**(9), 549–560, (2005).
75. Long-distance free-space distribution of quantum entanglement over Vienna, Lindenthal, M and Resch, KJ and Blauensteiner, B and Boehm, HR and Fedrizzi, A and Poppe, A and Taraba, M and Ursin, R and Walther, P and Kurtsiefer, C and others.
76. Satellite-based quantum communication terminal employing state-of-the-art technology, Pfennigbauer, Martin and Aspelmeyer, Markus and Leeb, Walter and Baister, Guy and Dreischer, Thomas and Jennewein, Thomas and Neckamm, Gregor and Perdigues, Josep and Weinfurter, Harald and Zeilinger, Anton, *Journal of Optical Networking*, **4**(9), 549–560, (2005).
77. Security proof of quantum key distribution with detection efficiency mismatch, Fung, Chi-hang Fred and Tamaki, Kiyoshi and Qi, Bing and Lo, Hoi-Kwong and Ma, Xiongfeng, *arXiv preprint arXiv:0802.3788*, (2008).
78. Free-space quantum cryptography with quantum and telecom communication channels, Toyoshima, Morio and Takayama, Yoshihisa and Klaus, Werner and Kunimori, Hiroo and Fujiwara, Mikio and Sasaki, Masahide, *Acta Astronautica*, **63**(1-4), 179–184, (2008).

79. Development of the polarization tracking scheme for free-space quantum cryptography, Toyoshima, Morio and Takayama, Yoshihisa and Kunimori, Hiroo and Takeoka, Masahiro and Fujiwara, Mikio and Sasaki, Masahide, Atmospheric Propagation V, *International Society for Optics and Photonics*, **6951**(695101), (2008).
80. Conceptual designs of onboard transceivers for ground-to-satellite quantum cryptography, Toyoshima, Morio and Shoji, Yozo and Takayama, Yoshihisa and Kunimori, Hiroo and Takeoka, Masahiro and Fujiwara, Mikio and Sasaki, Masahide, Atmospheric Propagation VI, *International Society for Optics and Photonics*, **7324**, 73240E, (2009).
81. Experimental verification of the feasibility of a quantum channel between space and Earth, Villoresi, Paolo and Jennewein, Thomas and Tamburini, Fabrizio and Aspelmeyer, Markus and Bonato, Cristian and Ursin, Rupert and Pernechele, Claudio and Luceri, Vincenza and Bianco, Giuseppe and Zeilinger, Anton and others, *New Journal of Physics*, **10**(3), 033038, (2008).
82. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution, Wang, Jian-Yu and Yang, Bin and Liao, Sheng-Kai and Zhang, Liang and Shen, Qi and Hu, Xiao-Fang and Wu, Jin-Cai and Yang, Shi-Ji and Jiang, Hao and Tang, Yan-Lin and others, *Nature Photonics*, **7**(5), 387, (2013).
83. Quantum cryptography for secure satellite communications, Hughes, Richard J and Buttler, William T and Kwiat, Paul G and Lamoreuax, SK and Morgan, GL and Nordholt, Jane E and Peterson, Charles G, *Aerospace Conference Proceedings, 2000 IEEE*, **1**, 191–200, (2000).
84. Method and apparatus for free-space quantum key distribution in daylight, Hughes, Richard J and Buttler, William T and Lamoreaux, Steve K and Morgan, George L and Nordholt, Jane E and Peterson, C Glen and Kwiat, Paul G, *US Patent* **6***,748,083,* Google Patents, (2004).
85. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, Bourgoin, JP and Meyer-Scott, E and Higgins, Brendon L and Helou, B and Erven, Chris and Huebel, Hannes and Kumar, B and Hudson, D and D'Souza, Ian and Girard, Ralph and others, *New Journal of Physics*, **15**(2), 023006, (2013).
86. Secure communications with low-orbit spacecraft using quantum cryptography, Hughes, Richard J and Buttler, William T and Kwiat, Paul G and Luther, Gabriel G and Morgan, George L and Nordholt, Jane E and Peterson, Charles G and Simmons, Charles M, *US Patent* **5***,966,224,* Google Patents, (1999).
87. System and method for communication between airborne and ground-based entities, Nelson, Eric A and O'meara, Michael B, *US Patent* **6***,760,778,* Google Patents, (2004).
88. Daylight operation of a free space, entanglement-based quantum key distribution system, Peloso, Matthew P and Gerhardt, Ilja and Ho, Caleb and Lamas-Linares, Antía and Kurtsiefer, Christian, *New Journal of Physics*, **11**(4), 045007, (2009).
89. Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles, Thapliyal, Kishore and Pathak, Anirban, *Quantum Information Processing*, **14**(7), 2599–2616, (2015).
90. Decoy-state quantum key distribution with polarized photons over 200 km, Liu, Yang and Chen, Teng-Yun and Wang, Jian and Cai, Wen-Qi and Wan, Xu and Chen, Luo-Kan and Wang, Jin-Hong and Liu, Shu-Bin and Liang, Hao and Yang, Lin and others, *Optics express*, **18**(8), 8587–8594, (2010).
91. Airborne demonstration of a quantum key distribution receiver payload, Pugh, Christopher J and Kaiser, Sarah and Bourgoin, Jean-Philippe and Jin, Jeongwan and Sultana, Nigar and Agne, Sascha and Anisimova, Elena and Makarov, Vadim and Choi, Eric and Higgins, Brendon L and others, *Quantum Science and Technology*, **2**(2), 024009, (2017).
92. Space-to-Ground Quantum Key Distribution Using a Small-Sized Payload on Tiangong-2 Space Lab, Liao, Sheng-Kai and Lin, Jin and Ren, Ji-Gang and Liu, Wei-Yue and Qiang, Jia and Yin, Juan and Li, Yang and Shen, Qi and Zhang, Liang and Liang, Xue-Feng and others, *Chinese Physics Letters*, **34**(9), 090302, (2017).
93. Progress in satellite quantum key distribution, Bedington, Robert and Arrazola, Juan Miguel and Ling, Alexander, *npj Quantum Information*, **3**(1), 30, (2017).
94. Satellite-based entanglement distribution over 1200 kilometers, Yin, Juan and Cao, Yuan and Li, Yu-Huai and Liao, Sheng-Kai and Zhang, Liang and Ren, Ji-Gang and Cai, Wen-Qi and Liu, Wei-Yue and Li, Bo and Dai, Hui and others, *Science*, **356**(6343), 1140–1144, (2017).
95. Ground-to-satellite quantum teleportation, Ren, Ji-Gang and Xu, Ping and Yong, Hai-Lin and Zhang, Liang and Liao, Sheng-Kai and Yin, Juan and Liu, Wei-Yue and Cai, Wen-Qi and Yang, Meng and Li, Li and others, *Nature*, **549**(7670), 70, (2017).
96. Satellite-to-ground quantum key distribution, Liao, Sheng-Kai and Cai, Wen-Qi and Liu, Wei-Yue and Zhang, Liang and Li, Yang and Ren, Ji-Gang and Yin, Juan and Shen, Qi and Cao, Yuan and Li, Zheng-Ping and others, *Nature*, **549**(7670), 43, (2017).
97. Satellite-relayed intercontinental quantum network, Liao, Sheng-Kai and Cai, Wen-Qi and Handsteiner, Johannes and Liu, Bo and Yin, Juan and Zhang, Liang and Rauch, Dominik and Fink, Matthias and Ren, Ji-Gang and Liu, Wei-Yue and others, *Physical Review Letters*, **120**(3), 030501, (2018).

98. A compact readout electronics for the ground station of a quantum communication satellite, author=Qi, Binxiang and Liu, Shubin and Shen, Qi and Liao, Shengkai and Cai, Wenqi and Lin, Zehong and Liu, Weiyue and Peng, Chengzhi and An, Qi, *IEEE Transactions on Nuclear Science*, **62**(3), 883–888, (2015).
99. How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss, Meyer-Scott, Evan and Yan, Zhizhong and MacDonald, Allison and Bourgoin, Jean-Philippe and Hübel, Hannes and Jennewein, Thomas, *Physical Review A*, **84**(6), 062326, (2011).
100. Secure key generation using an ultra-long fiber laser: transient analysis and experiment, Zadok, Avi and Scheuer, Jacob and Sendowski, Jacob and Yariv, Amnon, *Optics express*, **16**(21), 16680–16690, (2008).
101. The basics of satellite communications, Pelton, Joseph N, *Intl. Engineering Consortiu*, (2006).
102. Microwave radio transmission design guide, Manning, Trevor, *Artech House*, (2009).
103. Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design, Rappaport, Theodore S and MacCartney, George R and Samimi, Mathew K and Sun, Shu, *IEEE Transactions on Communications*, **63**(9), 3029–3056, (2015).
104. Satellite communications system employing frequency reuse, Rosen, Harold A, *Google Patents, US Patent*, **4**,879,711, (1989).
105. Spread spectrum multiple access communication system using satellite or terrestrial repeaters, Gilhousen, Klein S and Jacobs, Irwin M and Weaver Jr, Lindsay A, *Google Patents, US Patent*, **4**,901,307, (1990).
106. Method and apparatus for providing wideband services using medium and low earth orbit satellites, Wang, Arthur W, *Google Patents, US Patent*, **7**, 627, 284, (2009).
107. Atmospheric turbulence compensation using coherent optical adaptive techniques, Pearson, James E, *Applied optics*, **15**(3), 622–631, (1976).
108. Urban optical wireless communication networks: the main challenges and possible solutions, Kedar, Debbie and Arnon, Shlomi, *IEEE Communications Magazine*, **42**(5), S2–S7, (2004).
109. Atmospheric turbulence effects on a partially coherent Gaussian beam: implications for free-space laser communication, Ricklin, Jennifer C and Davidson, Frederic M, *JOSA A*, **19**(9), 1794–1802, (2002).
110. First-order performance evaluation of adaptive-optics systems for atmospheric-turbulence compensation in extended-field-of-view astronomical telescopes, Ellerbroek, Brent L, *JOSA A*, **11**(2), 783–805, (1994).
111. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, Kraus, Barbara and Branciard, Cyril and Renner, Renato, *Physical Review A*, **75**(1), 012316, (2007).
112. Background noise of satellite-to-ground quantum key distribution, Er-long, Miao and Zheng-fu, Han and Shun-sheng, Gong and Tao, Zhang and Da-Sheng, Diao and Guang-Can, Guo, New Journal of Physics, **7**(1), 215, (2005).
113. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, Bourgoin, JP and Meyer-Scott, E and Higgins, Brendon L and Helou, B and Erven, Chris and Huebel, Hannes and Kumar, B and Hudson, D and D'Souza, Ian and Girard, Ralph and others, New Journal of Physics, **15**(2), 023006, (2013).
114. Unconditionally secure key distillation from multiphotons, Tamaki, Kiyoshi and Lo, Hoi-Kwong, Physical Review A, **73**(1), 010302, (2006).
115. Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols, Ali, Sellami and Wahiddin, MRB, *The European Physical Journal D*, **60**(2), 405–410, (2010).
116. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols, Jeong, Y-C and Kim, Y-S and Kim, Y-H, *Laser Physics*, **21**(8), 1438–1442, (2011).
117. Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook, Hosseinidehaj, Nedasadat and Malaney, Robert and Ng, Soon Xin and Hanzo, Lajos, *arXiv preprint arXiv:1712.09722*, (2017).
118. Analysis of Quantum Key Distribution based Satellite Communication, Sharma, Vishal and Banerjee, Subhashish, *IEEE, 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–5, (2018).*
119. Principles and Applications of Free Space Optical Communication, Arockia Bazil Raj, Vishal Sharma, Subhashish Banerjee, *Chapter 19, ISBN: 978-1-78561-415-6, (2018) IET, UK.*
120. Decoherence can help quantum cryptographic security, Sharma, Vishal and Shrikant, U and Srikanth, R and Banerjee, Subhashish, *Quantum Information Processing*, **17**(8), 207, (2018).