6
Analysis of atmospheric effects on satellite based quantum communication: A comparative study

6.1 Introduction

Quantum Key Distribution (QKD) is a key exchange protocol [Long and Liu, 2002] 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[Brassard et al., 2000]. 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. The results obtained indicate that SARG04 protocol is an effective approach for satellite-based quantum communication.

Moore's law performed well for classical devices used in classical communication. From a quantum communication point of view, Moore's law will not work and is now saturated. This is one of the major motivations for quantum computation at the atomic level, for which, for example, nano-technology would be needed to speed up quantum operations for handling quantum parallelism [Hanzo et al., 2012; Botsinis et al., 2013].

Quantum-based satellite communication is an effective technique, as shown in the Fig. 6.1, which overcomes the limitations of classical wireless communication systems [Hanzo et al., 2012]. Quantum entanglement and superposition of various quantum states are the main features which provide unconditional security and these effects are absent in its classical counterpart. Quantum communication can be achieved by the following steps: (a) quantum state preparation- here classical information is encoded into quantum state; (b) quantum state transmission through a quantum channel such as free-space optical channel (FSO) or an optical fiber – here encoded quantum states are transmitted from transmitter (Alice) to receiver (Bob) (c) detection – here the classical information is extracted from the received quantum states via measurement operations. All these operations are demonstrated in Fig. 6.2.

Quantum information using photon polarization is more secure as compared to classical schemes. Quantum key distribution (QKD) is a well-known example of this and its security is proved [Bennett and Brassard, 2014]. Einstein's spooky action at a distance establishes a relation between quantum entanglement and quantum communication, which

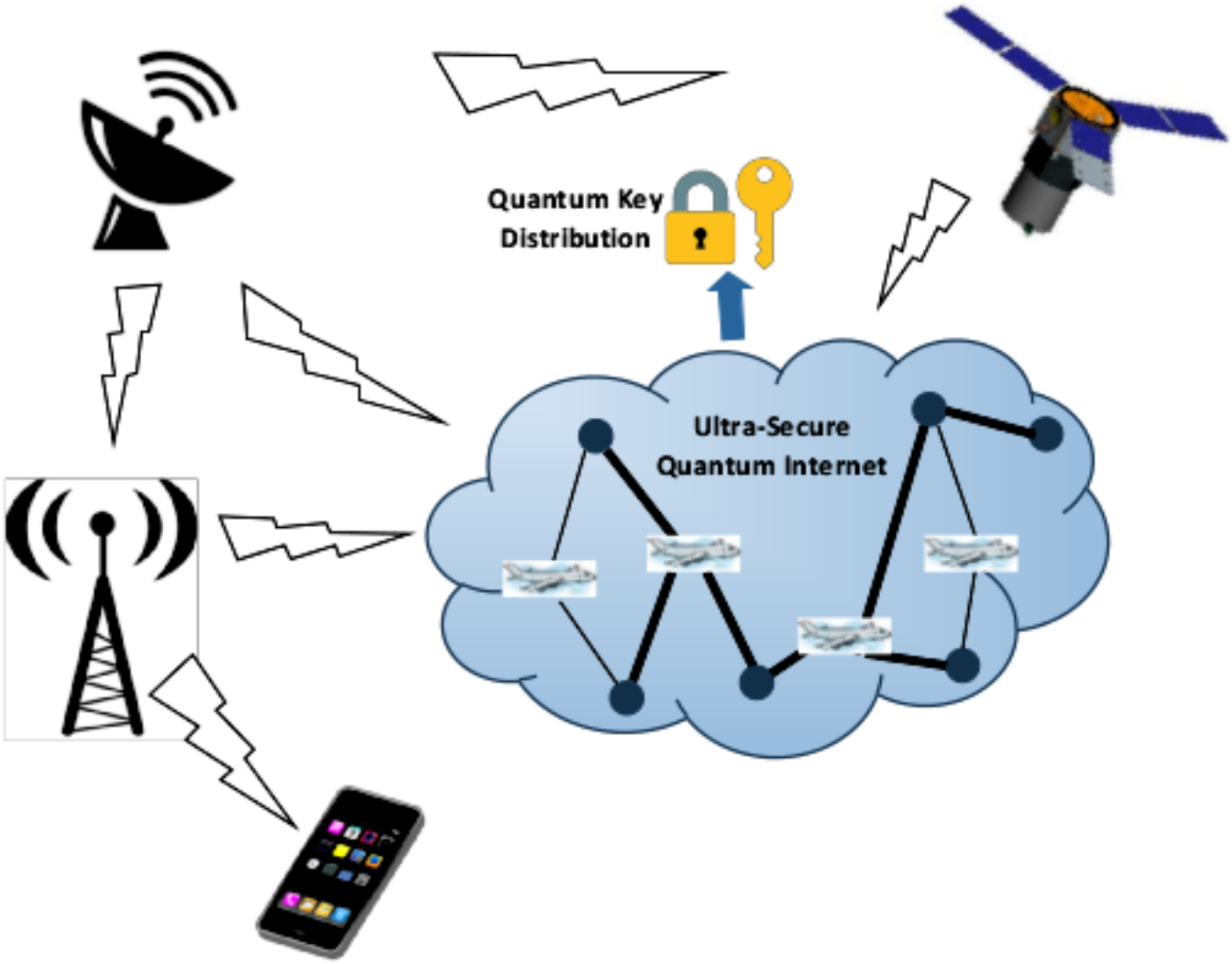

Figure 6.1: Global quantum communication system [Hosseinidehaj et al., 2017].

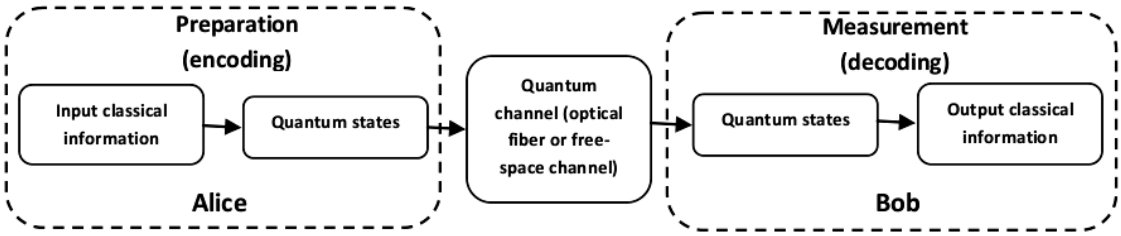

Figure 6.2: Basic quantum communication system [Hosseinidehaj et al., 2017].

means changes in polarization of a photon alters the instantaneous change in the photon polarization for its corresponding entangled pair [Bennett et al., 1993b; Furusawa et al., 1998; Vaidman, 1994; Furusawa et al., 1998; Van Loock and Braunstein, 1999].

Quantum states are represented in the form of discrete-variable (DV) or continuous-variable (CV) [Nielsen and Chuang, 2010; Braunstein and Van Loock, 2005]. In discrete-variable (DV) form, quantum states are represented by, for example, polarization of single photons [Bennett and Brassard, 2014]. These are detected by single photon detectors. In DV form, quantum information is encoded in 'qubit'. Laser light as information carrier is used in continuous variable (CV) approach [Bennett, 1992; Ralph, 1999]. In this, information is encoded on the quadrature variables of the optical field [Bennett, 1992; Ralph, 1999; Cerf et al., 2001; Grosshans and Grangier, 2002; Grosshans et al., 2003b,a], which form an infinite-dimensional Hilbert space. These variables are detected by heterodyne or homodyne detectors of high efficiency. Such detectors operate at faster transmission rate as compared to single-photon detectors [Hosseinidehaj et al., 2017; Semenov et al., 2012; Croal et al., 2016]. The quadrature components of the field are related to phase and amplitude of the laser light, which represents a quantum state.

Quantum key distribution [Bennett and Brassard, 1984; Shenoy-Hejamadi et al., 2017; Scarani et al., 2009; Srinatha et al., 2014] 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 [Sangouard et al., 2011; Bussières et al., 2013; Guha et al., 2015]. 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 [Munro et al., 2012; Azuma et al., 2015; Muralidharan et al., 2014], 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 [Boone et al., 2015].

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 [Thapliyal and Pathak, 2015; Pathak, 2013; Shukla et al., 2014; Schmitt-Manderbach et al., 2007; Lo et al., 2005b; Wang, 2005; Ma et al., 2005; Liu et al., 2010; Pugh et al., 2017; Liao et al., 2017b].

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 [Gisin et al., 2002; Carbonneau and Wisely, 1998; Bennett et al., 1992; Zbinden et al., 2000; Owens et al., 1994; Hughes et al., 2002b; Resch et al., 2005; Mayers, 2001; Shields and Yuan, 2007; Sharbaf, 2011; Buttler et al., 1998]. These satellite-based quantum communication schemes are designed for FSO communications [Kurtsiefer et al., 2002a]. 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 [Sharma, 2016; Omkar et al., 2013; Sharma and Sharma, 2014; Bedington et al., 2017].

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 [Khan et al., 2018; Calderaro et al., 2018].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 [Khan et al., 2018; Calderaro et al., 2018; Yin et al., 2017; Ren et al., 2017; Liao et al.,

2017a, 2018].

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 [Khan et al., 2018; Calderaro et al., 2018; Qi et al., 2015].

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 [Khan et al., 2018; Calderaro et al., 2018].

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 [Khan et al., 2018; Calderaro et al., 2018]. In addition to the successful Chinese experiments, several satellite-based quantum communication schemes [Rarity et al., 2002; Aspelmeyer et al., 2003; Nordholt et al., 2002; Kurtsiefer et al., 2002b; Hughes et al., 2002b,a; Pfennigbauer et al., 2005; Buttler et al., 2000; Lindenthal et al.; Fung et al., 2008; Resch et al., 2005; Ursin et al., 2007; Villoresi et al., 2008; Wang et al., 2013; Peloso et al., 2009; Toyoshima et al., 2009; Nelson and O'meara, 2004; Toyoshima et al., 2008a,b; Hughes et al., 2000, 2004; Bourgoin et al., 2013; Hughes et al., 1999] have also been proposed.

We have performed QKD protocols with and without decoy states for uplink, downlink, and intersatellite links. 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. We have not included losses due to misalignment in experimental setup. These can be considered 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 satellites, but not possible with GEO.

[1]This chapter is organized as follows: Section 6.2 sketches the methodology for an FSO communication link under various atmospheric conditions. In section 6.3, secure key rate for different QKD protocols are briefly discussed. We discuss our results in section 6.4 and conclude in section 6.5 .

6.2 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 [Teich and Saleh, 1991; Alda, 2003], obscuration and beam diffraction generate attenuation and shown to be [Klein and Degnan, 1974; Degnan and Klein, 1974].

$$\begin{aligned} \delta_{diff} &= (e^{-2\gamma_t^2\alpha_t^2} - e^{-2\alpha_t^2})(e^{-2\gamma_r^2\alpha_r^2} - e^{-2\alpha_r^2}), \\ \gamma_t = \frac{b_t}{R_t}, \gamma_r = \frac{b_r}{R_r}, \alpha_t &= \frac{R_t}{\omega_t}, \alpha_r = \frac{R_r}{\omega_r}, \\ \omega_t = R_t, \omega_r &= \frac{\sqrt{2}\lambda L}{\pi R_t}, \end{aligned} \tag{6.1}$$

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.

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 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.

[1]This chapter is based on Sharma and Banerjee [2017, 2019] .

More detailed description of free space optics and turbulence effects can be obtained from [Bloom et al., 2003; Arnon, 2003; Gabay and Arnon, 2006; Rarity et al., 2002; Aspelmeyer et al., 2003]. Turbulence is the main factor which contributes in atmospheric attenuation. This is because of thermal fluctuation which produce refractive index variations. Turbulence effects are calculated by increasing the divergence angle of the beam. In uplink, attenuation caused by turbulence is calculated as [Rarity et al., 2002; Aspelmeyer et al., 2003]

$$\delta_{turb} = \frac{\left(\frac{\lambda}{R_t}\right)^2}{\left(\frac{\lambda}{R_t}\right)^2 + \theta_{turb}^2}, \tag{6.2}$$

where θ_{turb} is the turbulence generated divergence in radians. 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

$$\delta = \delta_{diff}\delta_{atm}\delta_{rec}. \tag{6.3}$$

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. 6.3 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

$$\delta = \frac{L^2\left(\theta_T^2 + \theta_{atm}^2\right)}{D_R^2}\frac{1}{T_T\left(1 - L_P\right)T_R}10^{A_{atm}/10}, \tag{6.4}$$

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 [Gatenby and Grant, 1991] and the Tenerife's telescope [Ursin et al., 2007]. The scattering and absorption attenuation is evaluated using a model of clear standard atmosphere [Elterman, 1964] which results in $\eta_{scatt} = 1$ dB.

For calculating total channel attenuation, the considered parameters are shown in Table 6.1. 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.

6.3 THE SECURE KEY RATE ANALYSIS WITH DIFFERENT PROTOCOLS

6.3.1 The BB84 protocol

The BB84 protocol was proposed in [Bennett and Brassard, 1984], see [Fuchs et al., 1997; Bruß and Lütkenhaus, 2000] 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 [Teich and Saleh, 1991; Loudon, 2000].

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{6.5}$$

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

$$p_n = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}. \tag{6.6}$$

In QKD, the transmitter transmits the bit stream in the form of optical pulses via a quantum channel [Sharma et al., 2015, 2016b]. 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 [Bennett et al., 1992; Hughes et al., 2002b; Resch et al., 2005]. 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 [Bennett et al., 1992; Mayers, 2001; Shields and Yuan, 2007]. 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 [Scarani et al., 2009; Cover and Thomas, 2006]. Here,

$$I(A:B) = \sum_{n=0}^{\infty} \Big(1 - (1-\delta)^n\Big) P_n(\mu) \approx \mu\delta, \tag{6.7}$$

$$I(B:E) = \sum_{n\geq 2}^{\infty} P_n(\mu). \tag{6.8}$$

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

$$I_{Eve} \approx \frac{I(B:E)}{I(A:B)}. \tag{6.9}$$

The lowest value for the key generation rate R (in bits/pulse) is expressed in [Fuchs et al., 1997; Cover and Thomas, 2006; Lo et al., 2005b]

$$R \geq q\bigg(- Q_\mu f(E_\mu) H_2 E_\mu + \Omega Q_\mu \Big(1 - H_2\Big(\frac{E_\mu}{\Omega}\Big)\Big)\bigg), \tag{6.10}$$

where Ω ($\Omega = 1 - I_{Eve}$)denotes those photons, from which Eve cannot extract any information, also known as untagged photons [Lo et al., 2005b]. 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 [Brassard and Crépeau, 2005; Sharma and Banerjee, 2018].The yield of the n-photon pulses is represented as Y_n [Lo et al., 2005b].

The expected raw key rate can be written as [Ma et al., 2005]

$$Q_\mu = \sum_{n=0}^{\infty} Y_n P_n(\mu). \tag{6.11}$$

Quantum Bit Error Ratio (QBER), E_μ, is [Ma et al., 2005]

$$E_\mu = \frac{\sum_{n=0}^{\infty} Y_n P_n(\mu) e_n}{Q_\mu} = \frac{Y_0}{2Q_\mu}. \tag{6.12}$$

6.3.2 The SARG04 Protocol

The SARG04 protocol was proposed in [Scarani et al., 2004] 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 [Scarani et al., 2009]. 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, [Scarani et al., 2004; Chefles, 1998; Acin et al., 2004]. While performing attacks, Eve introduces attenuation which is expressed as

$$\delta = \frac{(1-t)P_1 + P_2(\mu) + \chi}{\mu}, \;\; t \in [0,1]. \tag{6.13}$$

Here χ is expressed as

$$\chi = \sum_{n\geq 3}^{\infty} P_n(\mu) P_{ok}(n), \tag{6.14}$$

where P_{ok} represents the probability of acceptance. For BB84 protocol, this value is 0.5 [Brassard and Crépeau, 2005; Acin et al., 2004].

In SARG04 protocol three copies of the quantum state is needed to extract a conclusive result with probability P_{ok} [Chefles, 1998]. In addition to this, four nonorthogonal states are used to encode the information.

In eavesdropping attempts, some attenuation is introduced. If the attenuation generated by IRUD attack is greater as compared to channel attenuation, Eves presence will be detected. Eve performs two operations represented by Eqs. 6.13 and 6.15, to hide her presence.

The attenuation in this case can be written as

$$\delta = \frac{(1-s)P_2(\mu) + \chi}{\mu}, \;\; s \in [0,1]. \tag{6.15}$$

Fig. 6.3 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 conditions.

6.3.3 Protocols with the decoy-states: An effective approach to counter Eavesdropping

The decoy-state method was proposed in [Hwang, 2003], and further studied in [Ma et al., 2005; Horikiri and Kobayashi, 2006; Wang, 2005]. 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 [Wang et al., 2008; Thapliyal and Pathak, 2015;

Pathak, 2013; Shukla et al., 2014]. The shared mutual information is

$$I(A:B) = P_1(\mu)(1-t) + P_2(\mu)(1-s) + \sum_{n\geq 3}^{\infty} P_n(\mu)P_{ok}(n), \tag{6.16}$$

$$I(B:E) = P_2(\mu)(1-s)I_2 + \sum_{n\geq 3}^{\infty} P_n(\mu)P_{ok}(n), \tag{6.17}$$

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 [Scarani et al., 2004]. 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 [Ma et al., 2005; Meyer-Scott et al., 2011], based on entanglement distillation described in [Gottesman et al., 2004] which in turn use the concept of decoy-state, is

$$R_{BB84} \geq q\bigg(- Q_\mu f(E_\mu)H_2(E_\mu) + Q_1\Big(1 - H_2(e_1)\Big)\bigg), \tag{6.18}$$

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 [Fung et al., 2006]

$$Q_1 = Y_1 e^{-\mu}\mu. \tag{6.19}$$

The lower bound for Q_1 and upper bound for e_1 with the vacuum and a weak decoy state (ν) is [Ma et al., 2005]

$$Y_1^L = \frac{\mu}{(\mu\nu - \nu^2)}\left(Q_\nu e^\nu - Q_\mu e^\mu\Big(\frac{\nu^2}{\mu^2}\Big) - \frac{(\mu^2-\nu^2)}{\mu^2}Y_0\right) \leq Y_1, \tag{6.20}$$

$$Q_1^L = \mu e^{-\mu} Y_1^L \leq Q_1, \tag{6.21}$$

$$e_1^U = \frac{e_0 Y_0}{Y_1^L} \geq e_1. \tag{6.22}$$

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 [Fung et al., 2006]. Taking this into account with the approach developed in [Gottesman et al., 2004], the gain in case of two-photon pulses is [Cover and Thomas, 2006; Fung et al., 2006]

$$Q_2 = Y_2 e^{-\mu} \frac{\mu^2}{2}. \tag{6.23}$$

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 [Ma et al., 2005]

$$Q_{\nu_i} = \sum_{n=0}^{\infty} Y_n P_n(\nu_i), \tag{6.24}$$

$$E_{\nu_i} = \sum_{n=0}^{\infty} \frac{Y_n P_n(\nu_i) e_n}{Q_{\nu_i}}. \tag{6.25}$$

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 [Ma et al., 2005]

$$0 < \nu_1 < \nu_2, \;\; \nu_1 + \nu_2 < \mu. \tag{6.26}$$

Now the key generation can be shown to be [Ma et al., 2005]

$$\begin{aligned} R_{SARG04} \geq q\Bigg(& -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1\Big(1 - H\Big(\tfrac{Z_1}{X_1}\Big)\Big) + \\ & Q_2\Big(1 - H(Z_2)\Big)\Bigg), \end{aligned} \tag{6.27}$$

where X_n and Z_n represents the binary random variables. $H_2(.)$ is the Shannon's binary entropy function [Cover and Thomas, 2006].

The lower limit of the two photon gain is [Ma et al., 2005]

$$Q_2^L = \frac{Y_2^L \mu^2 e^{-\mu}}{2} \leq Q_2. \tag{6.28}$$

The upper limit of e_2 can be manipulated by considering quantum bit error rate of weak decoy states [Ma et al., 2005].

$$E_{\nu_i} Q_{\nu_i} e^{\nu_i} = e_0 Y_0 + e_i \nu_i Y_1 + e_2 \frac{\nu_i^2}{2} Y_2 + \sum_{n=3}^{\infty} e_n Y_n \frac{\nu_i^n}{n!}. \tag{6.29}$$

6.4 Results

The results shown here are based on three scenarios. The parameters for link establishment (shown in Table 6.1) 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) in counts/pulse, 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 [Ursin et al., 2007; Gatenby and Grant, 1991].

As compared to APDs, superconducting nanowire single-photon detectors (SNSPDs) possess 80 percent quantum efficiencies. To achieve, such a high quantum efficiency, SNSPDs, require liquid-helium cryogenics. These values are valid for near infrared (NIR) diodes in the range of 750 nm-950 nm. APDs suffer from increases in dark counts due to radiation, and the cooling requirements of SNSPDs make their use in space very challenging. Note that, in our current work, silicon APDs are the best candidate for the considered 650 nm wavelength, which suffer least losses for low considerable quantum efficiencies. However, SNSPDs have added advantages in terms of performance for long range quantum communication (> 1200

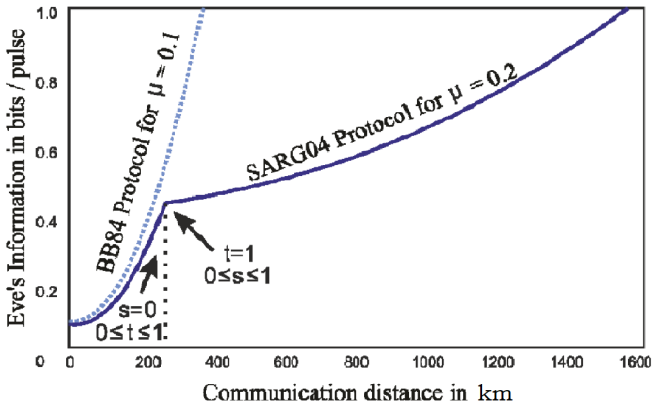

Figure 6.3: Variation in Eve's information with communication distance for each protocol under the uplink case ($\delta_{turb} = 5\ dB$) calculated using Eqs. 6.7, 6.8, 6.9, 6.13, 6.14, and 6.15.

km), space communication (239000 miles or 384633.216 km), high data rate (1.3 Gb s^{-1}), less losses, and higher quantum efficiency for detecting single photons Xue et al. [2016]; Holzman and Ivry.

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) [Aviv, 2006]. Effect of turbulence on the downlink is almost negligible [Rarity et al., 2002]. A value of $\delta_{scatt} = 1$ dB is achieved for the scattering plus absorption attenuation with the help of Clear Standard Atmosphere model [Elterman, 1964]; these values are similar to those discussed in [Rarity et al., 2002; Aspelmeyer et al., 2003]. In Fig. 6.3 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) [Scarani et al., 2004].

In Fig. 6.4 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 [Schmitt-Manderbach et al., 2007]. 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. 6.5, we have optimized μ and $\nu_i^{'s}$ in each protocol for both the states to obtain the highest key rate.

In Fig. 6.4, it is observed that critical distance obtained for SARG04 is comparatively higher than BB84, both with and without decoy states. Also in Fig. 6.4, 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 [Ma et al., 2007].

In case of increasing attenuation, the number of multi-photon pulses must be mini-

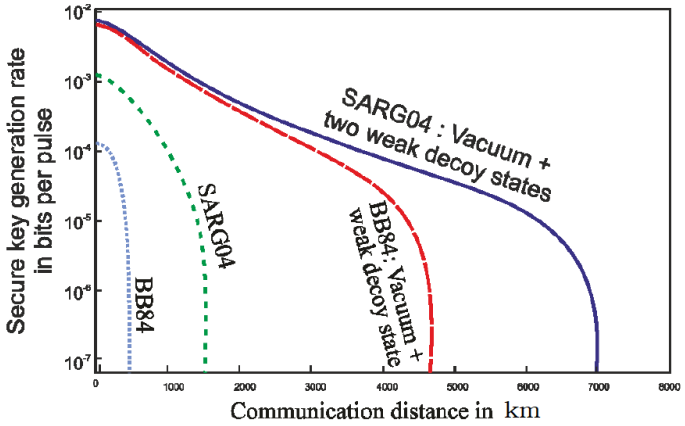

Figure 6.4: In uplink ($\delta_{turb} = 5\ dB$), secure key generation rate for all protocols under investigation calculated using Eqs. 6.10, 6.18, and 6.27.

mized which helps in reducing the chance of attacks performed by Eve (in this case μ must be decreased) as shown in Fig. 6.5. 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.

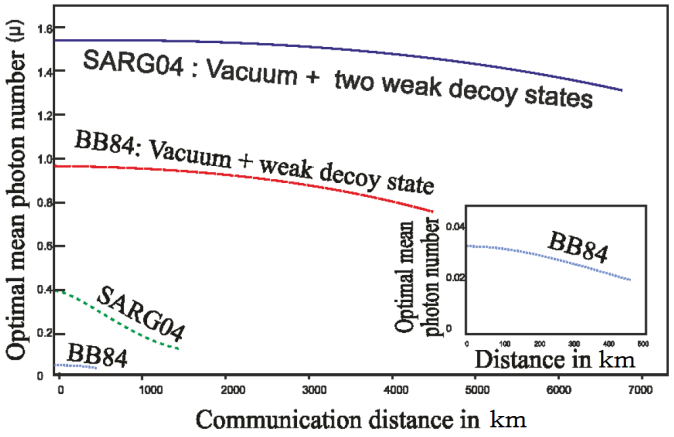

Figure 6.5: Variation in optimum mean photon number with communication distance for all protocols under the uplink case ($\delta_{turb} = 5\ dB$). These variations in μ correspond to the highest achievable secure rates, as shown in Fig. 6.4.

.

In Fig. 6.6, 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. 6.6, 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 secure rate decreases to a level below 3%,

Table 6.1: 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)	50×10^{-6}
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 6.2: 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

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) follows the same steps. The critical distance (in km), as shown in Table 6.2, for BB84 protocol is 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 the SARG04 protocol is seen to be: 3290 km in downlink case, 920 km in inter-satellite 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, 4650 km in uplink case ($\delta = 5dB$) and 2200 km in case of uplink with $\delta = 11dB$. The critical distance (in km), as shown in Table 6.2, for the SARG04 protocol with vacuum state and two weak decoy state are seen to be: 14100 km in downlink case, 3900 km in intersatellite case, 6980 km in uplink case ($\delta = 5dB$) and 3460 km in case of uplink with $\delta = 11dB$. The maximum possible secure rate (in Bits/Pulse) for BB84 protocol achieved from simulations are: 1.7×10^{-2} in downlink case, 2.0×10^{-2} in intersatellite case, 1.4×10^{-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), as shown in Table 6.3, for the SARG04 protocol are as follows: 2.4×10^{-2} in downlink case, 2.6×10^{-2} in intersatellite case, 1.2×10^{-3} in uplink case ($\delta = 5dB$) and 7.5×10^{-5} in case of uplink with $\delta = 11dB$. Following the same procedure, the maximum possible secure rate (in Bits/Pulse), as shown in Table 6.3, for BB84 protocol with vacuum state and weak decoy state are as follows: 4.4×10^{-2} in downlink case, 4.8×10^{-2} in intersatellite case, 5.8×10^{-3} in uplink case

Table 6.3: 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($\delta = 5$ dB)	$1.4.10^{-4}$	$1.2.10^{-3}$	$5.8.10^{-3}$	$6.5.10^{-3}$
Uplink(δ= 11 dB)	-	$7.5.10^{-5}$	$1.4.10^{-3}$	$1.6.10^{-3}$

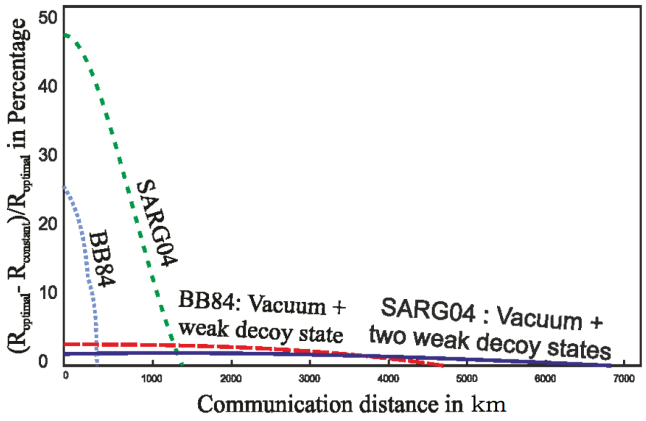

Figure 6.6: In the uplink scenario ($\delta_{turb} = 5\ dB$), for each protocol, variation in secure key rate (R) with communication distance at constant value of mean photon number calculated using Eqs. 6.10, 6.18, and 6.27.

($\delta = 5dB$) and 1.4×10^{-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: 4.6×10^{-2} in downlink case, 5.0×10^{-2} in intersatellite case, 6.5×10^{-3} in uplink case ($\delta = 5dB$) and 1.6×10^{-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 the 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 μ.

In the uplink scenario, secure key generation is low because of high attenuation [Bourgoin et al., 2013; Zadok et al., 2008; Bedington et al., 2017]. 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 [Meyer-Scott et al., 2011; Bourgoin et al., 2013]. The background count rate for uplink is higher than downlink because of artificial light pollution emitted upward [Bourgoin et al., 2013]. 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 [Pelton, 2006; Manning, 2009].

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 [Rappaport et al., 2015; Rosen, 1989].

Satellite covers a large area on the ground by providing service to many earth stations, using broad beam generated by lower frequency [Gilhousen et al., 1990; Wang, 2009]. For visible wavelengths, turbulence effects come into picture when using a transmitter telescope of more than 25-50 cm diameter [Pearson, 1976; Kedar and Arnon, 2004]. Turbulence effects can be minimized by selecting a good ground station [Rarity et al., 2002]. In addition to this, an adaptive optics system can be used to minimize the turbulence effects [Ricklin and Davidson, 2002; Ellerbroek, 1994].

6.5 Conclusion

In this work, we have analyzed two QKD protocols (BB84 and SARG04) with and without decoy states under normal atmospheric conditions (5 dB before sunset and 11 dB under clear summer day) and PNS attack for uplink and downlink scenarios. From the above results is borne out the point that the SARG04 protocol achieves the optimum result as compared to the BB84 protocol under the considered 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 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.