KEY DETECTION RATE MODELING AND ANALYSIS FOR SATELLITE-BASED QUANTUM KEY DISTRIBUTION

THESIS

Jonathan C. Denton, Captain, USAF

AFIT-ENY-MS-16-M-206

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENY-16-M-206

KEY DETECTION RATE MODELING AND ANALYSIS FOR SATELLITE-BASED QUANTUM KEY DISTRIBUTION

THESIS

Presented to the Faculty

Department of Aeronautics and Astronautics

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Space Systems

Jonathan C. Denton, BS

Captain, USAF

March 2016

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT-ENY-16-M-206

KEY DETECTION RATE MODELING AND ANALYSIS FOR SATELLITE-BASED QUANTUM KEY DISTRIBUTION

Jonathan C. Denton, BS

Captain, USAF

Committee Membership:

Richard. G. Cobb, PhD
Chair

Douglas D. Hodson, PhD
Member

Michael. R. Grimaila, PhD CISM, CISSP
Member

Abstract

A satellite QKD model was developed and validated, that allows a user to determine the optimum wavelength for use in a satellite-based QKD link considering the location of ground sites, selected orbit and hardware performance. This thesis explains how the model was developed, validated and presents results from a simulated year-long study of satellite-based quantum key distribution. It was found that diffractive losses and atmospheric losses define a fundamental trade space that drives both orbit and wavelength selection. The optimal orbit is one which generates the highest detection rates while providing equal pass elevation angles and durations to multiple ground sites to maximize the frequency of rekeying. Longer wavelengths perform better for low Earth orbit satellites while shorter wavelengths are needed as orbital altitude is increased. For a 500km Sun-synchronous orbit, a 1060nm wavelength resulted in the best performance due to the large number of low elevation angle passes. On average, raw key rates of 170kbit/s per pass were calculated for a year-long orbit. This work provides the user with the capability to identify the optimal design with respect to wavelength and orbit selection as well as determine the performance of a QKD satellite-based link.

Acknowledgments

First and foremost I would like to thank my wife and daughter for their incredible support throughout my time at AFIT. Without them, I would not have been able to complete my studies. Second, I would like to thank all my friends from the EN departments, especially those from section ENY4. The comradery built over the many late nights studying and finishing homework assignments will be a memory I cherish. Lastly I'd like to thank the faculty, research team and our sponsor for the encouragement, insight and education they have provided me.

Jonathan C. Denton

Table of Contents

Page

List of Figures

Page

List of Tables

Page

KEY DETECTION RATE MODELING AND ANALYSIS FOR SATELLITE-BASED QUANTUM KEY DISTRIBUTION

I. Introduction

General Issue

Quantum Key Distribution (QKD) allows users to securely generate shared cryptographic key [1]. Ideal implementations of QKD, leveraging the use of physical properties of quantum particles, have been shown to create an unconditionally secure method for the exchange of cryptographic keys. This unconditional security has motivated the development of real-world systems. The distance limits of these real-world terrestrial systems have been reached due to hardware inefficiencies and the birefringent nature of optical fiber [2]. In order to extend the range of QKD systems, a transition to free-space including satellite platforms is the next step in the evolutionary development of this technology. The Air Force Institute of Technology (AFIT) QKD research team has developed a discrete event computer model for QKD systems that captures the limitations of real systems [3]. The current model does not incorporate the free-space channel effects to implement the quantum transmitter on a satellite platform. Including free-space effects is a critical next step in order to continue to maintain modeling accuracy and currency in the evolving field. The development of a validated model that accurately characterizes the orbital dynamics and space-based optical link budgets will continue the cutting edge research of the AFIT QKD team.

Problem Statement

The essential factors that influence QKD space-based key detection rates (i.e., model) needs to be developed to understand the role each factor plays in a space-based link. The effect of the atmospheric channel on the identified factors also needs to be characterized, to understand the additional variation introduced in the transition to a space-based platform. The significance of each factor and the resulting atmospheric effects are expected to identify the design space for optimization allowing researchers to select the best orbit and wavelength for a given scenario.

Research Objectives/Questions/Hypotheses

The main research questions investigated are: 1. What are the factors that directly determine the detection rate of a LEO QKD space-based system? 2. Of the factors identified in question 1, which are orbit dependent and in what way do they define the design space for optimization? and 3. For the specific case of a 500km Sun-synchronous orbit with equal detector efficiencies, what is the best wavelength for a space-based QKD system acting as a trusted node between the Air Force Institute of Technology (AFIT) and the Naval Postgraduate School (NPS)?

Two known factors that directly influence optical links include the transmittance and refraction in the atmosphere [4]. It is believed that the Laser Environmental Effects Definition and Reference (LEEDR) toolset developed at AFIT can be leveraged to create a model that lines up very well with current transmittance estimates for atmospheric conditions anywhere in the world [5]. LEEDR is traditionally used to capture optical properties of lasers propagated within the atmosphere. The transmittance estimates are

only one of the many key parts of the optical link equation. Another important part captured by LEEDR is the refracted path through the atmosphere. Lt Jeremiah Specht, another member of the QKD team, is pursuing the modeling of refractive bending of the laser paths in question [6]. Other parts of the link equation include hardware properties, choice of wavelength and total energy in the beam. All of these portions of the link equation provide various design choices, dependent on the research scenario.

Research Focus

The focus of this research is to first understand the factors that determine satellite QKD detection rates and then develop and validate a model for satellite QKD implementation. Detection rates, or raw key rates, are defined as the expected number of detections averaged over a given time interval. The model is intended to provide descriptive performance of a space-based QKD link and provide insight into orbit optimization. The model highlights the most useful wavelengths for satellite QKD based on the optical losses experienced during typical orbital passes. The optimal wavelength is the one that provides the least amount of channel loss and the highest detection rate, averaged over all satellite passes. The optimal orbit is defined as the one that ensures the greatest amount of raw key material is exchanged at both ground sites.

Methodology

This thesis first identifies and presents the factors that influence satellite QKD. Secondly, the factors are incorporated into a model that characterizes the quantum bit (qubit) exchange between a space-based platform and a ground site. Finally, the model is used to conduct a year-long study of a specific scenario. The model developed provides

an end-to-end architecture that incorporates orbital mechanics, atmospheric physics and QKD principles. The model first develops the satellite position, then characterizes the ground site atmosphere and lastly applies an optical communication link between the orbiting satellite and the fixed ground station. The satellite modeling component determines azimuth, elevation angle, range and the corresponding time based on a user selected TLE file. The atmospheric modeling component determines the atmospheric properties above the ground site depending on the season and time of day. Finally, the model characterizes the link budget, calculates the usable quantum bit rate as a function of time and estimates the quantum bit error rate (QBER). Averaging the detection rate over the year-long passes provides the final metric to describe the overall quality of the system's performance.

Assumptions/Limitations

This section outlines the assumptions made throughout this thesis. The main assumptions in this thesis are: equivalent detector efficiencies, negligible weather effects, atmospheric reciprocity up to 100km [7, p. 202], and that the parameters describing the optical link are approximately constant over the bandpass[1] [8]. Real single photon detectors vary in efficiency for photon detection, mainly due to different responses of materials to incident photons of different wavelength. This thesis assumes that all photon detectors provide the same level of detection efficiency. This assumption reduces the variability across hardware and studies more directly the channel effects on space-based QKD. The ability to vary the detection efficiencies is still included, to allow the

[1] Bandpass – the frequency spectrum of electromagnetic energy that passes through a given medium e.g. a channel or filter, this identifies the range of wavelengths to which a device is sensitive

validation of the model against other sources and modeling of real-world systems. The weather effects of fog and clouds prevent QKD from taking place due to excessive attenuation of the optical beam. An assumption of clear skies is used to capture unhindered year-long system performance as cloud coverage is ground site dependent. The calculated total detections measured should be scaled by the fraction of nights that clear skies actually exists over a given ground site for the best representation of real-world performance. Atmospheric reciprocity refers to the properties describing the atmosphere along a defined path. These properties are defined for each point along a path and do not change for that given path, regardless of moving forward or backwards along that path. This means that the uplink path and downlink paths have the same atmospheric properties for density, transmittance, temperature and constituents [7]. This does not mean that the lens effect of the atmosphere is the same for an uplink as it is for a downlink. The final assumption of constant properties across the bandpass describes two conditions. The optical beam does not have sufficient energy to change the properties of the atmosphere along its path (thermal blooming) and the pulse moves along the path faster (~10E-5 sec) than changes due to wind, turbulence and other atmospheric transitions (~10E-3 sec) [9].

Additional Assumptions are listed below:

- Propagation of Two-Line Element (TLE) sets provide sufficient orbital accuracy to allow insight into key rate generation
- The ground telescope can track the orientation of the satellite and properly align to the orientation of the transmission frame so that there is no loss due to misalignment in the reference frame defining polarization

- Doppler effects on optical frequencies are incorporated without issue in the available optical bandwidth of the receiver

Known limitations of the developed model include: a line of sight approximation for pointing error, no loss due to rotational misalignment, and an assumption that the diffraction pattern of the receiving optic completely fills the detection area of the single photon detector. The line of sight approximation for pointing error was required in order to validate the model against the approaches from Specht [6] and Bourgoin [10].

Implications

The implications of this research help determine the utility and feasibility of space-based platforms for incorporation into QKD systems. This research allows decision makers to argue for or against funding a LEO satellite platform to act as a technology demonstration for unconditionally secure key distribution. The model developed during this research provides the framework to allow additional study for any desired orbit, wavelength and hardware combination to identify the optimal implementation of a QKD space-based system.

This model proves the feasibility of key rates on the order of tens of thousands of bits per day. This results in the ability to securely pass significant amounts of encrypted data from AFIT to NPS over 2500 miles via traditional communication infrastructure. This extends the current range from 250km [2] to any site in the world a ground station can be established. The model should be used to generate technical requirements for a low Earth orbit technology demonstration satellite. It should also be used to identify the

ideal locations for ground sites. The model will be used in the existing framework to expand the realm of possible simulation scenarios.

Preview

This thesis explains the development of the model, validates it against two sources from academia and conducts a simulated year-long experiment for a satellite in a 500km Sun-synchronous orbit. The model lines up within 25% of other computer simulations and within 7% of experimental data. The experiment showed that the 1060 nm wavelength generated the highest average detection rate during the year due to its balance of loss from diffraction and transmittance at low elevation angles. The Sun-synchronous orbit was not optimal as it did not evenly generate key between the selected AFIT and NPS each night.

Chapter II discusses QKD and the protocol used in this study. It also familiarizes the reader with the SGP4 orbital mechanics routine, Gaussian laser beams and atmospheric transmission. Chapter II also reviews relevant work performed in academia to include modeling and experimental results within the field.

Chapter III outlines the three components of the model and how they were used. Chapter III begins with the implementation of the atmospheric characterization. It then describes the orbital propagator and the link basics. Finally Chapter III defines the entire optical link. The methodology section also provides justification for the design choices made during the model development.

Chapter IV presents the validation of the model against two similar computer simulations and experimental data. It then presents the results for the 500km orbit year-

long study. Due to similarity, only the results for AFIT passes are shown in Chapter IV while the results for the NPS high and low elevation angle passes can be found in Appendix A.

Chapter V highlights the findings of this research. It also identifies major lessons learned during the effort and outlines future work that should leverage the model developed. Chapter V concludes with a review of the important themes from this thesis.

II. Background

Chapter Overview

This chapter provides background information required to understand the multidisciplinary aspects of an integrated QKD satellite model. It begins by providing the reader a high-level understanding of QKD systems and the workings of the BB84 methodology - references to appropriate security proofs are provided. Once QKD is understood, qkdX is presented to provide a top level summary of the framework. After qdkX, the frame of references used and the physical setup of the problem are developed in the satellite dynamics section. Next, the reader is provided with sufficient familiarity governing LEEDR as to understand its contributions to the work accomplished. The final background developed is an explanation of the optical properties of the link and the propagation of the electromagnetic energy used in the communication. Lastly, current work completed by other members of academia is examined to provide the reader with an understanding of relevant work in the field.

Quantum Key Distribution

Overview

Quantum key distribution is a form of key distribution that leverages the laws of physics to provide a secure source of key distribution. Using quantum communication, photons that have specific properties are transmitted from a source (Alice) to a receiver (Bob). The purpose of this transmission is to generate a unique key shared by both Alice and Bob so that they may exchange encrypted information over an open channel without the concern of security compromise.

Quantum Computations

Quantum particles used to represent ones and zeros are referred to as quantum mechanical bits, or *qubits* as shorthand [11]. These qubits are denoted in the Dirac notation, signifying states that exist in a two-dimensional state space. The traditional state space is defined by the computational basis $|0\rangle$ and $|1\rangle$. The specific qubit state may then be generally represented as the state ψ shown in equation (1).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

The qubit ψ represents a polarization vector with the probability of detection in a chosen basis. The probability of measuring the given vector along the associated component is proportional to the square of the α or β term. Choosing to measure ψ from the $|0\rangle, |1\rangle$ basis will return a successful measurement with a probability$|\langle 0|\psi\rangle| = |\alpha|^2$ and a probability $|\langle 1|\psi\rangle| = |\beta|^2$. The dimension of the basis, either $|0\rangle$ or $|1\rangle$, is then associated with a digital bit of information. The information transferred via the qubit can be encoded in the qubit's polarization, and then received in the correct state as either $|0\rangle$ or $|1\rangle$. Finally the receiver assigns a digital value appropriately and the information is transferred. Orthogonal states define the computational basis of the qubit state and can be arbitrarily defined in orientation. Traditional choices of bases reference the eigenvectors of the x and z Pauli matrices shown below [12].

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2}$$

The Z basis defined by $(|0\rangle, |1\rangle)$ corresponds to a horizontal $|H\rangle$ vector and vertical $|V\rangle$ vector.

$$|H\rangle = 1|0\rangle + 0|1\rangle$$
$$|V\rangle = 0|0\rangle + 1|1\rangle \tag{3}$$

An X-basis defined $(|D\rangle, |A\rangle)$ can be visualized as a forty five degree right handed rotation of the Z basis, such that the diagonal vector, D, and anti-diagonal vector, A, are defined as below. [13, pp. 61-93]

$$|D\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle \tag{4}$$
$$|A\rangle = \frac{1}{\sqrt{2}}|V\rangle - \frac{1}{\sqrt{2}}|H\rangle$$

Orthogonality of the diagonal and anti-diagonal vectors above can be confirmed by examining the inner product space.

$$|\langle D|A\rangle|^2 = \left\langle \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle \middle| \frac{1}{\sqrt{2}}|V\rangle - \frac{1}{\sqrt{2}}|H\rangle \right\rangle \tag{5}$$
$$= \left| \frac{1}{\sqrt{2}} \cdot \frac{-1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \right|^2 = 0$$

Note that attempting to measure in the X basis, a quantum particle that was defined in the Z basis with an H or V polarization vector has equal probability of resulting in a polarization vector of D or A.

$$|\langle D|A\rangle|^2 = \left\langle 0|H\rangle + 1|V\rangle \middle| \frac{1}{\sqrt{2}}|V\rangle - \frac{1}{\sqrt{2}}|H\rangle \right\rangle \tag{6}$$

$$= \left| 0 \cdot \frac{-1}{\sqrt{2}} + 1 \cdot \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

This is similar for any of the possible combinations, so that anytime a state is measured in the correct basis it will provide the correct polarization, and anytime that a polarization state is measured in the incorrect basis it will have an equally random chance of appearing as either a 1 or 0 in either of the orthogonal parts of the wrong basis.

These bases are the fundamental encoding used to convey information in satellite QKD. The satellite payload will be responsible for random selection of both the basis and the value of the bit transmitted to the receiver, so that the final key may be implemented in the BB84 protocol outlined below.

BB84 Protocol

The BB84 Protocol was developed by Charles Bennet and Giles Brassard in 1984 [1]. The fundamental idea was to use quantum particles to generate a secret random key at a distance. The transmitter, Alice, could send random bits encoded on a quantum particle to a distant party, Bob, in order to generate a secret key shared by both parties. An eavesdropper, Eve, would not be able to measure the particles in any way, without disturbing them. If the particles were received without disturbance, the truly random nature of their generation would allow a secure key to be based fundamentally in the laws of physics. This key could then be applied to a traditional encryption algorithm such as the Advanced Encryption Standard in order to create an unconditionally secure key.

Van Der Wiel [11] very clearly outlines the protocol, excepting changes to match the reference vectors used in this thesis.

BB84 protocol:

1. Alice generates $4m+\varepsilon$ random classical bits, and for each bit she randomly chooses the X or the Z basis. For each bit she generates a qubit and sends it to Bob. If the bit is 0 she sends $|H\rangle$ or $|D\rangle$, and if the bit is 1 she sends $|V\rangle$ or $|A\rangle$.

2. Bob measures the $4m + \varepsilon$ qubits in a random basis; either the X or the Z basis. … Bob's measurement result will be equal to Alice bit if they used the same basis. Otherwise the measurement result will be random. This initial key is often called the *raw key*.

3. Alice and Bob publicly announce their basis choices on the classical channel, and they discard the bits where they used different bases. With a high probability they have $2m$ bits left, commonly called the *sifted key*.

4. Alice randomly selects half of the remaining bits and publicly announces the bit values. Bob compares Alice's bit values with his measurement results to probe for Eve's presence. From this set they can estimate the quantum bit error rate (QBER), and if it is sufficiently low they continue the protocol with the remaining m bit key. Otherwise they discard the key and start over again.

5. This step is called *reconciliation*. Using the QBER estimate Alice sends Bob error correcting data to obtain equal keys. Further Alice and Bob calculate an upper bound on Eve's information about the key. They then perform privacy amplification to fully remove Eve's information about the key. In this step the m bit erroneous, partly secure key is reduced to an n bit identical, unconditionally secure key. [11]

This explains the principles of the QKD information transfer. Next, a general overview of the qkdX framework is presented to illustrate how qkdX is used.

qkdX Framework

"The qkdX framework was designed with the goal of enabling efficient modeling of QKD systems for performance analysis and characterization. This capability allows users to more efficiently (i.e., without significant re-programming) model and analyze variations in QKD system hardware configurations, software processes, or communication protocols in order to more fully understand the system design trade space and practical implementation limitations. More specifically, the qkdX enables the detailed study of relationships between physical (e.g., quantum phenomenon, temperature, and disturbances) and system-level interactions (e.g., hardware designs, software implementations, and protocols).

Initially, the framework was used to model a notional polarization-based, prepare and measure BB84 terrestrial fiber QKD system. However, the framework was designed with considerations to support all forms of qubit encoding schemes (i.e., polarization, phase, and entanglement), multiple protocols (e.g., BB84, SARG04, E91, etc.), and various QKD implementations (e.g., aerial fiber, terrestrial free space, satellite free space, and multiplexed transmissions)" [3, p. 16].

"The qkdX Framework defines models (e.g., optical, electro-optical, and electrical components), modules (i.e., subsystems or "smart" components), and communication channels (e.g., fiber or free space) common to many different architectures. Each model, module, and channel can be reused in multiple QKD system representations" [3, p. 17]. Currently, the only defined communication channel is a polarization maintaining fiber [3, p. 95]. A space-based free space channel is the next modular component that needs to be

added to qkdX . In order to understand the descriptions of the space-based platform and associated reference frames, satellite dynamics is examined in the next section.

Modeling Satellite Dynamics

Overview

Standard General Perturbations 4 (SGP4) is an openly available set of algorithms that provides the building blocks for comprehensive modeling of satellites, ground stations, spatial vector representations and temporal resolution for all points within the relevant three dimensional space. SGP4 also has the functionality to identify points on the Earth based on their geodetic longitude and latitude, transform vectors between multiple frames of reference and acts as the industry standard for orbital modeling.

SGP4

The SGP4 initialization routine uses a position and a velocity in the Earth centered inertial (ECI) coordinate frame, along with properties of the central body (in this case the Earth), to initialize and define orbital characteristics of a satellite. Once the satellite is initialized, the SGP4 routine will propagate the satellite position either forward or backward in time to determine the new position and velocity vectors. SGP4 incorporates disturbances due to resonances, third body forces, atmospheric drag and other perturbations [14, p. 697].

In order to initialize the SGP4 routine, specific orbital characteristics from a supplied Two Line Element (TLE) file are used to identify the position and velocity of the satellite to be modeled. This TLE is based on the format used by Air Force Space Command, and TLEs of current orbiting satellites are readily available to the public. The

TLE format includes information on the unique identifier for the satellite, and its international designator. It also includes ten fields that uniquely identify the satellite orbit, including the classical orbit elements. The first six are required for calculations, and the remaining four variables are necessary to describe the effect of perturbations on the satellite motion. The first six fields include the inclination, right ascension of the angular node, eccentricity, argument of perigee, the mean anomaly and the mean motion. For TLE formatting, all angle measurements are in degrees. Mean motion and its associated derivatives are calculated from units of revolutions/day. The four inputs to perturbation calculations include B*, the epoch, the derivative of mean motion and the second derivative of mean motion. B* is a drag-like parameter that can be used to determine the ballistic coefficient of the satellite [14, p. 106].

The coordinate system for TLEs is a true-equator, mean equinox system [14, p. 106]. The overall error in a TLE can be more than a kilometer due to errors in the mathematical approximations used to generate the TLE. As acquisition is not the purpose of this research, it is assumed that the TLE is sufficiently accurate as to allow insight into the problem being studied.

Frames of Reference

The frames of reference used in this work include the Earth centered inertial (ECI) frame, the Earth centered Earth fixed frame (ECEF) and the topocentric horizon coordinate system (SEZ). The ECI frame is defined with the principal axis pointing along the vernal equinox's direction in January of 2000. The third axis is along the axis of rotation of the Earth, matching a vector pointing toward the average geographic North

Pole. The second axis is formed as the right handed cross product of the third axis with the principal axis. Figure 1 [15] below shows an illustration of this coordinate system.

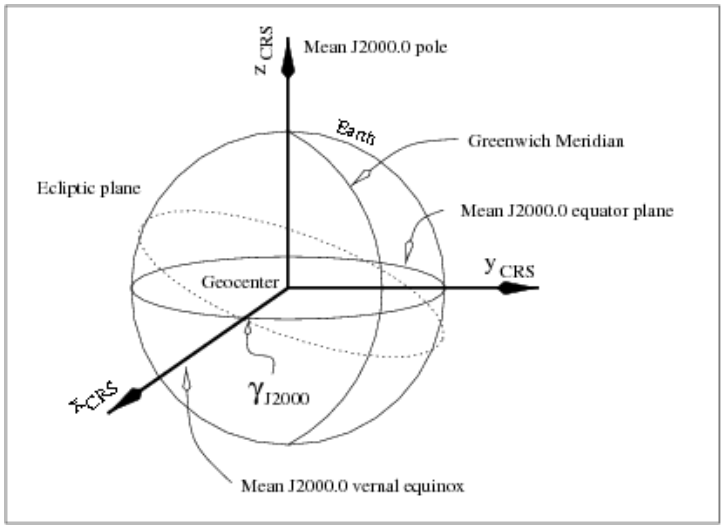


Figure 1: Earth Centered Inertial Frame [15]

The properties of the ECI frame are not truly constant and must reference an epoch to ensure accuracy over long periods of time. The standard referenced epoch for this thesis is the J2000 epoch, corresponding to the IAU-2000 definitions of the Earth's orientation, equator, precession and nutation.

The Earth centered Earth fixed frame is similar to the ECI frame except it accounts for the rotation of the Earth due to the Earth fixed nature of the axes. The Earth does not only rotate around its polar axis, but it also undergoes nutation and precession.

$$\vec{r}_{ECEF} = [\boldsymbol{P}(t)][\boldsymbol{N}(t)][\boldsymbol{R}(t)][\boldsymbol{W}(t)]\vec{r}_{ECI} \tag{7}$$

where:

$\boldsymbol{P}(t) = rotation\ due\ to\ precession$
$\boldsymbol{N}(t) = rotation\ due\ to\ nutation$
$\boldsymbol{R}(t) = rotation\ of\ the\ earth$
$\boldsymbol{W}(t) = rotation\ due\ to\ polar\ motion$

Equation (7) is used to rotate vectors from the Earth centered inertial coordinate frame to the Earth centered Earth fixed coordinate frame. It is important to note that the position of the Earth fixed frame is dependent on any point in time whereas the Earth fixed inertial frame is tied only to a specific reference time.

The final reference framed used in this thesis is a polar version of the topocentric horizon coordinate system. The SEZ frame refers to a three dimensional Cartesian frame with origin aligned on the surface of the World Geodetic Survey ellipsoid approximating the surface of the Earth. The principal axis points toward the south, the secondary axis points towards the east and the third axis is the right-handed cross product of the principal and secondary axes. The SEZ frame can be related back to the ECEF frame through the site's geodetic latitude, ϕ_{gd}, and the longitude, θ. First rotate about the secondary axis by $-(90 - \phi_{gd})$ degrees and then about the tertiary axis by $-\theta$. A common reference from a ground site to define the look angle towards a satellite as it passes overhead is the azimuth and elevation angle. These values define the orientation of a unit vector pointing toward the satellite in the SEZ frame, with azimuth typically referenced from the negative of the principal axis (local geographic North). Figure 2 [14, p. 161] shows the respective orientation of the SEZ frame as related to the ECEF frame.

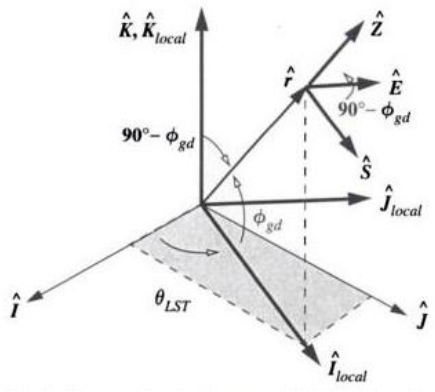


Figure 2: Topocentric to Geocentric Rotation [14, p. 161]

The satellite position vectors, ground site position vectors and multiple frames of reference are used together to describe the overall geometry of the satellite to ground station link. This geometry can be distilled to a single elevation angle and range used to define the specific properties of the satellite optical link.

Satellite Optical Downlinks

Overview

This section provides the building blocks of the optical link used in this work. The laser path describes the possible paths a single photon could travel along from satellite to receiver. The beam model used was the standard Gaussian laser beam defined by Andrews and Phillips [16]. The majority of loss is due to diffraction by the beam spreading out from the aperture at the source to the plane of the receiver. The atmosphere is a multilayer spherical lens that refracts the downlink without significant expansion. As the beam propagates through the atmosphere it is not significantly changed as to alter the beam properties other than reducing the amplitude of the electromagnetic field. Optical

hardware is characterized as a system, so that the total system efficiency is fifty percent, which is the standard assumption for optical hardware [17].

Benefits of Satellite Dynamics on QKD Systems

There are two immediate benefits of moving QKD platforms to space-based platforms. First, the satellite position in space and time can only be occupied by a single vehicle. No eavesdropper, outside the atmosphere, could be present in the middle of the communication link for the entire duration of the communication. An eavesdropper's presence is possible with a terrestrial fiber as it can be spliced. Satellite QKD adds to the overall security of the system due to isolation of the channel from eavesdroppers. A traditional QKD assumption is that Eve is "all powerful" such that any error or loss is a function of her malevolent efforts. In satellite QKD, Eve could be imagined as an aerial platform that flies in and out of the laser link absorbing photons and re-emitting her received states and values to the ground site. Second, the satellite can propagate the quantum information via free space rather than some birefringent method that requires polarization correction. This reduces the total loss and the overall complexity of the channel. A channel with less loss can be used for longer distances promoting communication between geographically separated sites. In order to accurately model a satellite QKD link the channel, geometry and beam must be modeled correctly.

Gaussian Beams

A Gaussian laser beam is one that concentrates the majority of its electromagnetic energy in the center of the beam. As one moves radially out from the center, the energy decreases as the negative exponent of the radial distance squared over the beam radius

squared, as shown in Figure 3 [18]. In addition to this concentration of energy, the Gaussian beam has a parabolic phase front and the axial propagation is much greater than the off-axis beam spreading.

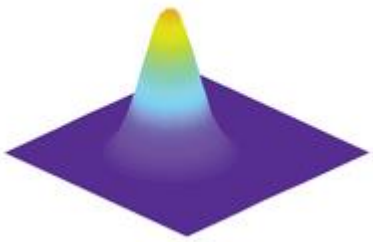


Figure 3: Gaussian Beam Planar Energy Distribution [18]

The Gaussian laser beam consists of an amplitude and phase. The amplitude is a function of the transverse distance the beam has propagated. The phase is also a function of the transverse distance the beam has propagated, but is not a significant factor in the BB84 implementation of satellite QKD. For this study, the optical beam information is carried in the polarization of the photon being transmitted rather than in its phase, and as such the second exponential term of Equation (8) will be carried forward as unity. The final Gaussian beam equation used to characterize the energy in the field, as developed in [16] is shown in Equation (8).

$$U_o(r,z) = \frac{a_o}{\sqrt{\Theta_0^2 + \Lambda_0^2}} \exp(-\frac{r^2}{W^2}) \exp[i(kz - \phi - \frac{kr^2}{2F})] \quad (8)$$

The propagation parameter defines the wave based on input plane beam parameters. Starting with the real and complex parts of the propagation parameter

$$p(z) = \Theta_0 + i\Lambda_0 \tag{9}$$

$$\Theta_0 = 1 - \frac{z}{F_o}; \Lambda_0 = \frac{2z}{kW_0^2} \tag{10}$$

where:

$a_o = Max\ amplitude\ of\ the\ field$
$z = propagation\ distance\ in\ meters$
$F_0 = radius\ of\ curvature\ in\ meters$
$W_0 = beam\ waist$
$k = \frac{2\pi}{\lambda}\ is\ the\ optical\ wave\ number$
$\lambda = wavelength\ in\ meters$

Equation (8) shows the spatial dependency of the beam's energy field. The a_o term is the peak value, and the field drops off radially from the center of the beam. The $-\frac{r^2}{W^2}$ term accounts for the drop off in energy as a function of radial distance. The spot size *W*, must also be calculated to determine the size of the laser at the plane of the receiver.

$$W = W_0\sqrt{\Theta_0^2 + \Lambda_0^2} \tag{11}$$

The large distance over which a laser propagates from a satellite to the ground causes the beam to spread to a much larger size on the ground. Only a portion of this beam is actually incident on the receiving telescope and this additional loss is accounted for by integrating the irradiance at the receiver, the square of the field at the receiver, over the area of the receiving aperture. Assuming the same initial field amplitude, the total irradiance and spot size are a function of both transvers distance and vary with wavelength.

Optical Wavelengths

Transmission through the atmosphere at optical frequencies is not uniform for all wavelengths. Transmission, on average, is much higher for frequencies on the infrared side of the electromagnetic spectrum with greater scattering reducing transmission for frequencies on the blue side of the electromagnetic spectrum. The principal wavelengths of interest were chosen as a point of comparison with Bourgoin [10]. They include 405nm, 532nm, 670nm, 785nm, 830nm, 1060nm and 1555nm. Each of these wavelengths will experience different amounts of diffraction and attenuation along a defined space-based optical link.

Atmospheric Effects

The atmosphere directly affects electromagnetic radiation passing through it. Attenuation and scatter are the major influences that were considered in this study, captured by the transmittance values. While the atmosphere does not influence the polarization of the laser passing through it, it will readily attenuate certain wavelengths of light due to the atmospheric constituents. This attenuation is a lump sum of the absorption, Mie scattering and Rayleigh scattering that the light experiences. Weather effects create additional attenuation. The large number of spherical droplets in clouds and fog act as spherical lenses readily scattering light passing through them. This scattering disrupts the ability to leverage optical paths for laser communication. For this reason, a "clear sky" is assumed when developing the optical transmission of the atmosphere. Clear sky refers only to the absence of large scattering pockets along the transmission path. It still allows the presence of atmosphere, aerosols, humidity and turbulence. These

assumptions feed directly into the Laser Environmental Effects Definition and Reference (LEEDR) platform that was used to generate the selected transmittance curves.

LEEDR

LEEDR is a software package implemented in MATLAB 2013a that was developed by the Center for Directed Energy at AFIT. It is comparable to other forms of atmospheric radiative transfer codes, such as the commercial MODTRAN [19], but is readily available to DOD entities. The user guide quotes Jaclyn Schmidt describing LEEDR as:

"The LEEDR model is a fast-calculating, first-principles, worldwide surface-to-100km, ultraviolet-to-radio-frequency (UV to RF) wavelength, atmospheric characterization package. In general, LEEDR defines the well-mixed atmospheric boundary layer (BL) with a worldwide, probabilistic surface climatology that is based on season and time of day and, then computes the radiative transfer and propagation effects from the vertical profile of meteorological variables. The LEEDR user can also directly input surface observations or use numerical weather prediction (NWP) data to create a near real-time atmospheric profile. (JAMC, 2014)." [5]

LEEDR allows a user to select any site worldwide and calculate the radiative transfer through the atmosphere above that location. Multiple inputs are required to properly characterize the atmosphere for the given area of study. The user can define the atmospheric model used or import their own, the level of aerosols in the atmosphere and the number of layers to calculate along the path. Weather can also be incorporated with the addition of clouds at user defined altitudes, models for wind and turbulence and

selection of the typical level of humidity that is being experienced. Once all of these inputs have been defined, LEEDR allows the user to define a laser wavelength and the line of sight geometry from the transmitter to the receiver [5].

Based on the user defined laser, LEEDR will calculate the refractive bending of the laser beam. This laser can be transmitted from any altitude to a receiver at any appropriate altitude. The software is designed to properly characterize atmospheric effects within 100km of the Earth's surface [5], and by assuming that any additional impacts above 100km in height are negligible, it can be programmed to calculate laser paths for orbital altitudes. The path can be defined in many ways to include slant path, refractive bending or a point to point solution that accounts for refractive bending and provides a corrected zenith angle for aiming. Specific details regarding the implementation of the laser path calculations are discussed in Chapter III.

Figure 4: Laser Environmental Effects Definition and Reference Location Tab

Figure 4 shows the location selection tab of the LEEDR interface. This is provided to help the reader visualize additional discussion in the methodology section.

Relevant Research

Overview

Quantum key distribution is a subject that has been studied since its advent in the 1980s. It has been extensively reviewed at a terrestrial level for both fiber channels and atmospheric channels. Overtime longer and longer free space transmissions were realized and the practical application of QKD to satellite platforms is now completely feasible. This section presents some of the recent publications on the subject of applying quantum key distribution to orbital platforms. Various computational models have been developed

in the last twenty years, as well as a comprehensive QKD model and a proof of concept experiment that validated the feasibility of the BB84 protocol.

Rarity et al [20] provide a definition for the detection rates that can be expected for a satellite QKD link. The link is a combination of the pulse rate, mean photon number per pulse, transmittance of the atmosphere, geometric loss and system efficiencies. The total key rate is divided by two due to the random nature of basis selection in BB84 protocol that reduces the correct number of properly oriented receptions by half.

$$K = \frac{RMTL_g\eta}{2} \tag{12}$$

While Equation (12) provides some insight into the optical link, a better understanding of the appropriate components can be found from Villoresi [21]. They represent the number of photons received more similarly to a traditional optical link as shown in Equation (13) by separating out all the different contributions of each component along the optical link. This equation is for a reflected photon propagating from the ground to the satellite and back, which must be modified appropriately for a single propagation path.

$$N_{ph} = \eta_q E_t \left(\frac{\lambda}{hc}\right) \eta_t G_t \sigma_{sat} \left(\frac{1}{4\pi R^2}\right)^2 A_r \eta_R T_A^2 T_c^2 \quad (13)$$

where

$\eta_q = detector\ quantum\ efficiency$
$E_t = laser\ energy\ in\ the\ pulse$
$h = planck's\ constant$
$c = the\ speed\ of\ light$
$\lambda = wavelength\ in\ meters$
$\eta_t = tranmitter\ path\ efficiency$
$G_t = transmitter\ gain$
$\sigma_{sat} = satellite\ backscattering\ cross\ section$
$R = distance\ between\ the\ satellite\ and\ receiver$
$A_r = receiving\ aperture\ area$
$\eta_R = receiver\ path\ efficiency$
$T_A = atmospheric\ transmission$
$T_c = cloud\ transmission$

Equation (13) should be modified by removing the squared term for propagation loss and converting it to a scaling factor reflecting the fractional power received, removing the G_t term, and removing the σ_{sat} as the satellite is the transmitter, not a reflector, resulting in [8]

$$N_{ph} = \eta_q E_t \left(\frac{\lambda}{hc}\right) \eta_t P_{frac} A_r \eta_R T_A T_c \quad (14)$$

This result can then be related to the detection rate of the system by dividing the number of photons received by the time step over which the photons arrived, such that the quantum bit rate is defined by Equation (15) [8].

$$Q = \frac{N_{ph}}{\Delta t} \quad (15)$$

One of the additional complications to QKD is the presence of additional photons in the atmosphere, due to light emissions from the Earth's surface, reflected light from

either the Sun or the Moon or starlight refracted into the receiving telescope. These photons can show up as detections in a QKD system and are referred to as background noise, which adds to the total loss of the system. Er-long [22] describes a number of configurations for a telescope receiving system. Based on [22], an average background noise of 5 $x10^{-6}$ counts per pulse will be assumed for this simulation.

A comprehensive analysis of the performance of a space-based QKD system was developed by Bourgoin [10]. Using MODTRAN and seven select wavelengths representing optical atmospheric transmission passbands, Bourgoin created simulations for detection rates during orbital passes and exchanged secure key. Bourgoin calculated the average number of secure key bits received for an upper percentile satellite pass between 68.5kbit to 465.6kbit, varying by wavelength. Bourgoin also provided graphs of the results for raw key rate and QBER generated for a 600km overhead pass operating on a 670nm wavelength. Bourgoin's paper is the main simulation comparison to help validate the results of the simulation developed in this thesis.

Vallone was able to use a reflecting satellite to prove the feasibility of the BB84 protocol [23]. Using the Matera Laser Ranging Observatory, a laser was aimed at a retroreflective satellite covered in corner cubes. The laser was used to provide range data with ranging pulses and reflect qubits off of the satellite. The 100MHz laser pulses were attenuated to approximate a mean photon number of 1.6. The quantum bit error was then measured over an eighty-five second pass and resulted in an average value of 5.7% [23]. The experimental raw key rate measurements are provided for a portion of the satellite pass. This experimental data is also a source of comparison for validation purposes.

Summary

The necessary fundamental concepts of quantum key distribution have been developed to help the reader better comprehend the research performed as a part of this thesis. Current research is still ongoing in the field. This thesis will enhance the capability of the current QKD framework at AFIT. It also provides academia insight into the practical applications of satellite-based QKD from an orbit design perspective.

III. Methodology

Chapter Overview

This chapter presents the methodology used in this thesis. It also provides supporting arguments for the assumptions and choices made throughout the research effort. The model development and implementation is presented in a building block method illustrating the components of the model that were first developed and then the link calculation from integrating the model pieces.

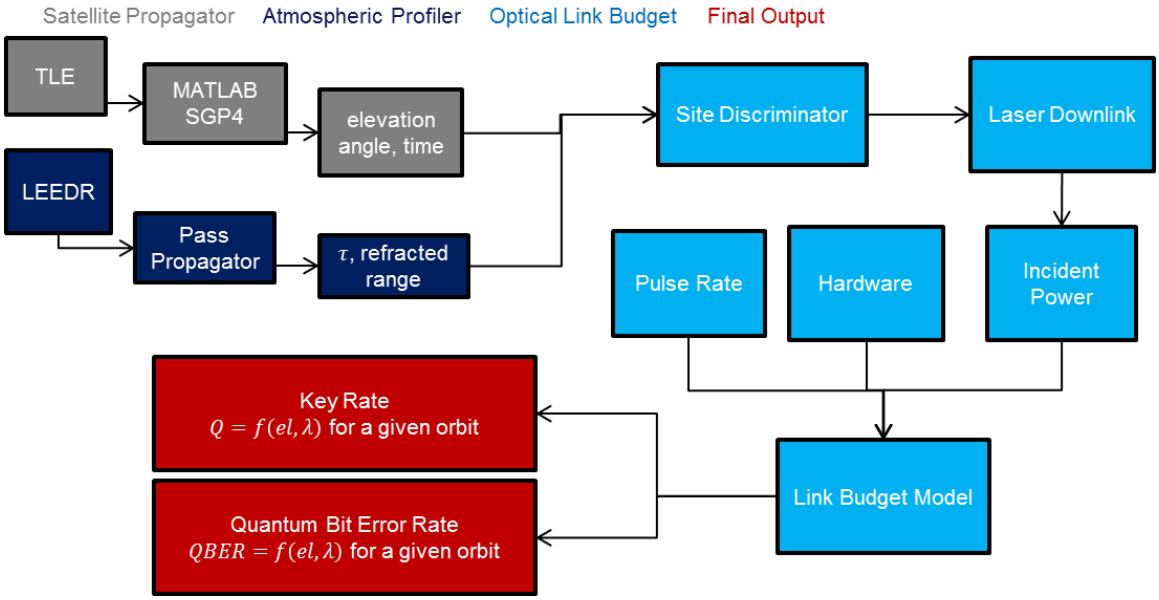


Figure 5: Model Components Color Coded by Functionality

As shown in Figure 5, the three components include an atmospheric pass propagator, a satellite orbit propagator and an optical link budget. The first component developed was the atmospheric pass propagator that generated the transmittance values and refracted paths for every satellite elevation angle greater than zero degrees. The second component developed was the satellite orbit propagator, which determined

satellite position as a function of time and related the range and elevation angle to a specific ground station. The final component contains the optical link budget calculations that connected the satellite to the ground station. The refraction of the optical path and the atmospheric characteristics of the path are functions of both wavelength and satellite elevation angle. Each of the seven selected wavelengths required its own inputs for path calculations, starting with the atmospheric profile.

Atmospheric Profile

The atmospheric profile is defined by user parameters input into LEEDR. The possible inputs include ground site, time of day, relative humidity percentile, aerosols, number of layers, wind models, turbulence models, cloud formation and height, and the laser geometry used. The ground sites modeled include the Air Force Institute of Technology (AFIT) and the Naval Postgraduate School (NPS) for simulations. Matera, Italy is also used, but only as the ground site for validation against Vallone. As developed, LEEDR characterizes the latitude and longitude of NPS as an ocean location rather than land. Due to the coastal proximity of NPS to the Pacific Ocean this approximation is assumed to provide sufficient accuracy for the atmospheric characteristics that will be modeled.

First, the atmospheric profile parameters were selected. The atmosphere was defined by the ExPERT profile present in LEEDR. This definition leverages the average of historical conditions for a given site, based on time of day, summer or winter and relative humidity (RH) percentile. Note that the RH percentile does not mean the actual

relative humidity, but instead an estimate of the relative humidity based on how similar it is to the historical average value experienced at the chosen location.

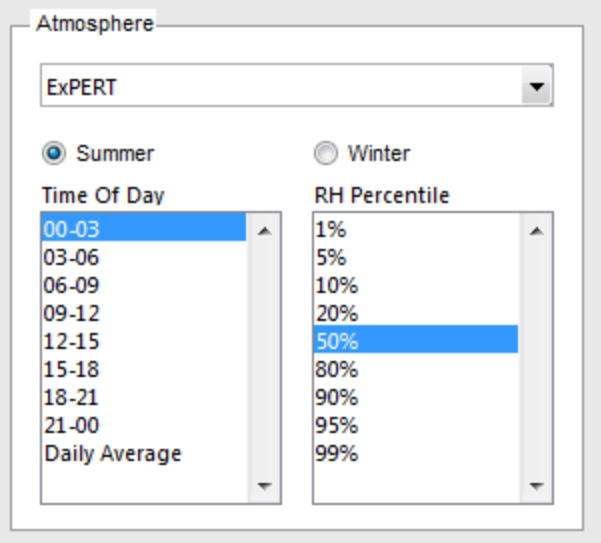


Figure 6: LEEDR Atmospheric Input Parameter Selection

Next, the aerosols present in the atmosphere were characterized. In order to maintain an accurate comparison to the Bourgoin study discussed earlier [10], the aerosol model used was a standard model for moderate aerosols in the appropriate season, based on the MODTRAN model in urban conditions. Urban conditions are necessary due to the location of AFIT and NPS in urban environments. The selected parameters for the summer profiles are shown in Figure 7.

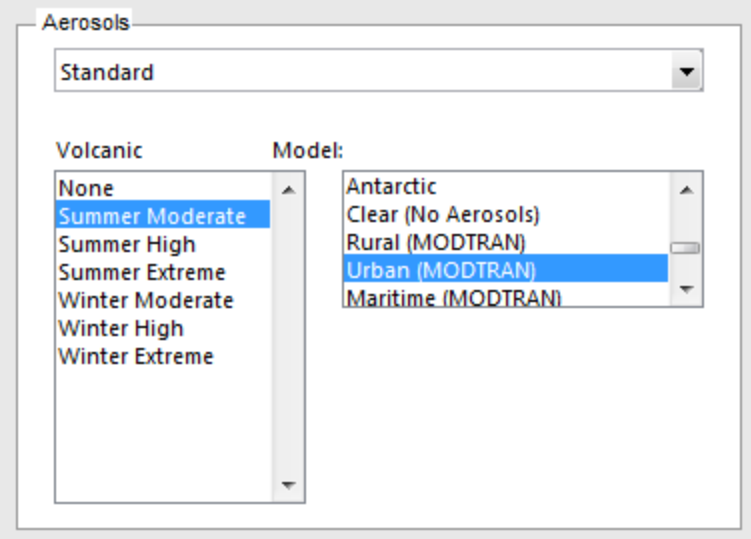


Figure 7: LEEDR Aerosols Input Parameter Selections

Lastly, the wind and turbulence models were characterized. Based on the recommendations of Fiorino [24], the Tatarski model for turbulence was selected. This model is similar to a traditional Kolmogorov power law spectrum, but it uses a Gaussian distribution to truncate the Kolmogorov model when high wave numbers are used [16, p. 67]. There is an available Clouds/Rain input section for LEEDR modeling, but the clear sky assumption enforces a condition without clouds or fog of any kind.

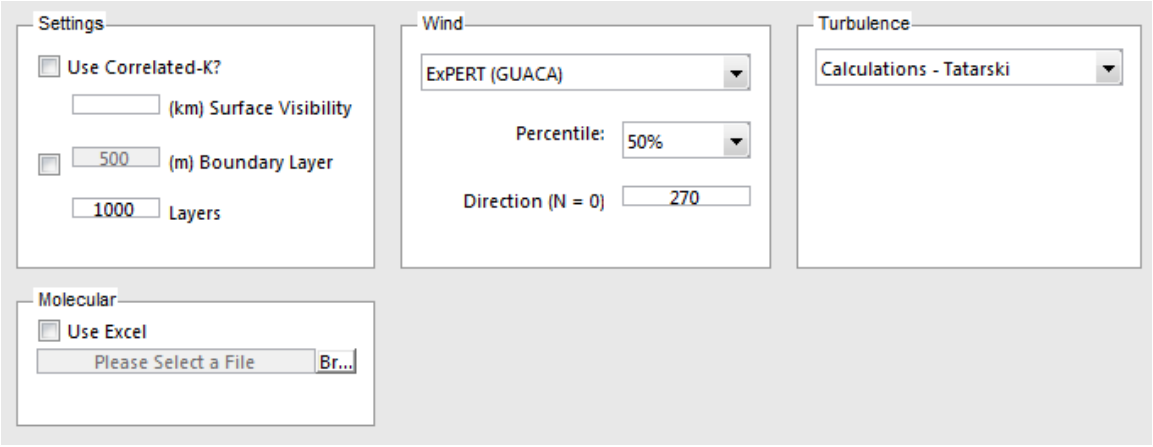


Figure 8: Wind and Turbulence Parameter Selections

The defined atmospheric profile allows the path transmittance to be characterized for both a variety of wavelengths and a variety of transmission paths. The Laser/Geometry tab of the LEEDR interface allows the user to input a single laser path for study. While useful, this would become exceptionally tedious to perform by hand for every path that could be modeled during a satellite orbit. Instead, an assumption that transmittance as a function of satellite elevation angle would accurately represent the characteristics for multiple satellite passes was used. A script was developed in order to automate the geometry calculations. To ensure the accuracy of the developed script the atmospheric transmittance for the range of 400nm – 1555nm wavelengths was calculated along the Zenith for a satellite passing over WPAFB at an altitude of 500 kilometers. The output of the LEEDR Zenith calculation for transmittance is shown in Figure 9.

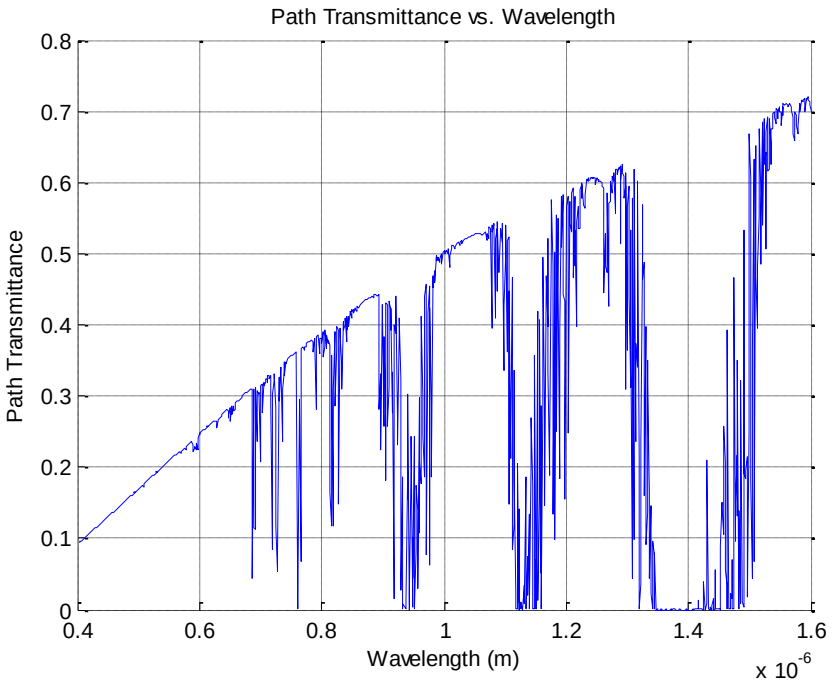


Figure 9: Zenith Transmittance as a Function of Wavelength

The transmittance is a combination of the transmittance for aerosol and the transmittance for atmospheric constituents. Aerosols in the atmosphere will scatter and absorb electromagnetic energy, and the molecules normally present in the atmosphere will also do the same [4, pp. 122-132]. The amount of scattering and absorption is a function of wavelength. By looking at the smooth curve of Figure 10 combined with the output given in Figure 11 it becomes clear the reason for the erratic shape of Figure 9.

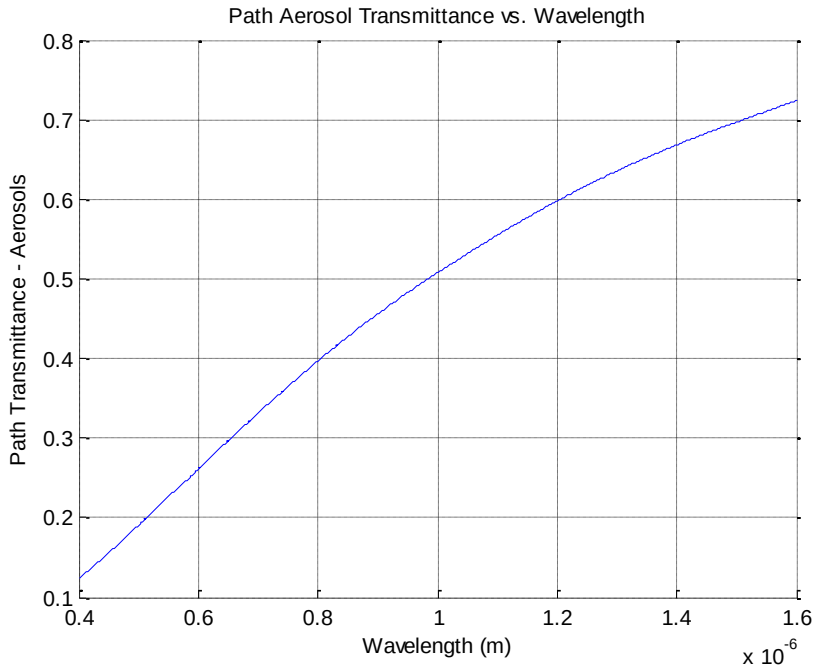


Figure 10: Aerosol Only Transmittance as a Function of Wavelength

The effect of aerosols is to provide the majority of scattering that occurs during atmospheric transmission, and results in a smooth curve as a function of wavelength. The molecular constituents within the atmosphere provide the majority of absorption at specific wavelengths and create the seemingly sporadic drop outs shown in Figure 11.

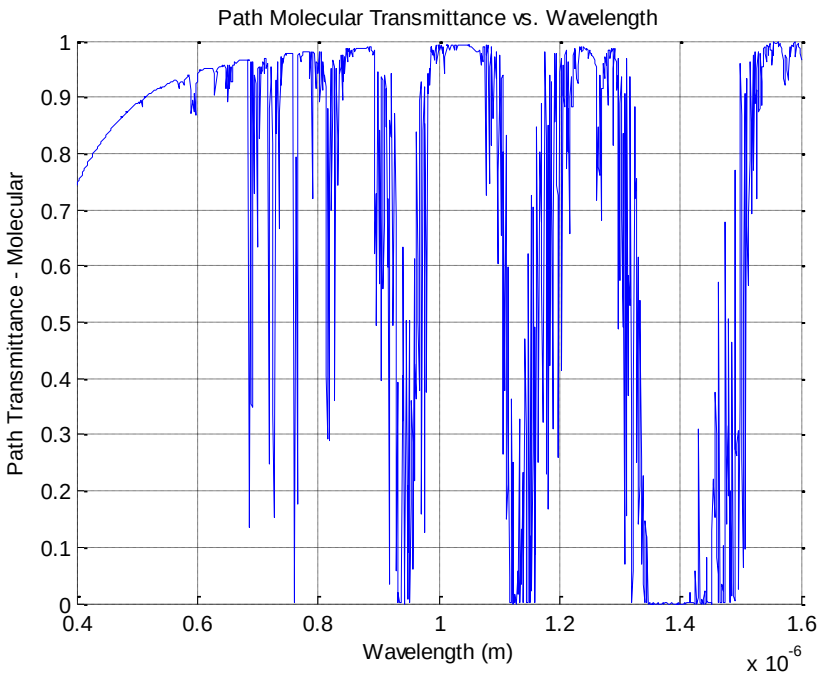


Figure 11: Molecular Only Transmittance as a Function of Wavelength

The zenith transmittances for each of the wavelengths identified for study are shown in Table 1. These served as baseline indicators to ensure that the automated calculations used in the development of the varying elevation angle model were accurate. Transmittance is lower for AFIT during the winter than the summer. NPS has an order of magnitude smaller change in loss than AFIT during the winter. This is due to its coastal proximity.

Table 1: Wavelength Transmittance at Zenith for Studied Wavelengths

Wavelength	AFIT Summer Transmittance	NPS Summer Transmittance	AFIT Winter Transmittance	NPS Winter Transmittance
405 nm	0.095	0.084	0.080	0.090
532 nm	0.194	0.182	0.172	0.185
670 nm	0.299	0.290	0.274	0.287
785 nm	0.397	0.373	0.354	0.366
830 nm	0.403	0.397	0.382	0.393
1060 nm	0.527	0.523	0.504	0.513
1555 nm	0.702	0.699	0.693	0.699

The model used to calculate transmittance as a function of elevation angle consists of a loop that calculates multiple laser geometries along a satellite pass. Figure 12 shows a sample calculation of a single point during an orbital pass. Note that the geometry shown defines the path from the ground to the satellite. This is acceptable due to the assumption of atmospheric reciprocity. The properties of the atmosphere along the defined path are invariant whether light is moving from the ground to the satellite or from the satellite to the ground. This is assumed to still be true for individual photons propagating along the same path.

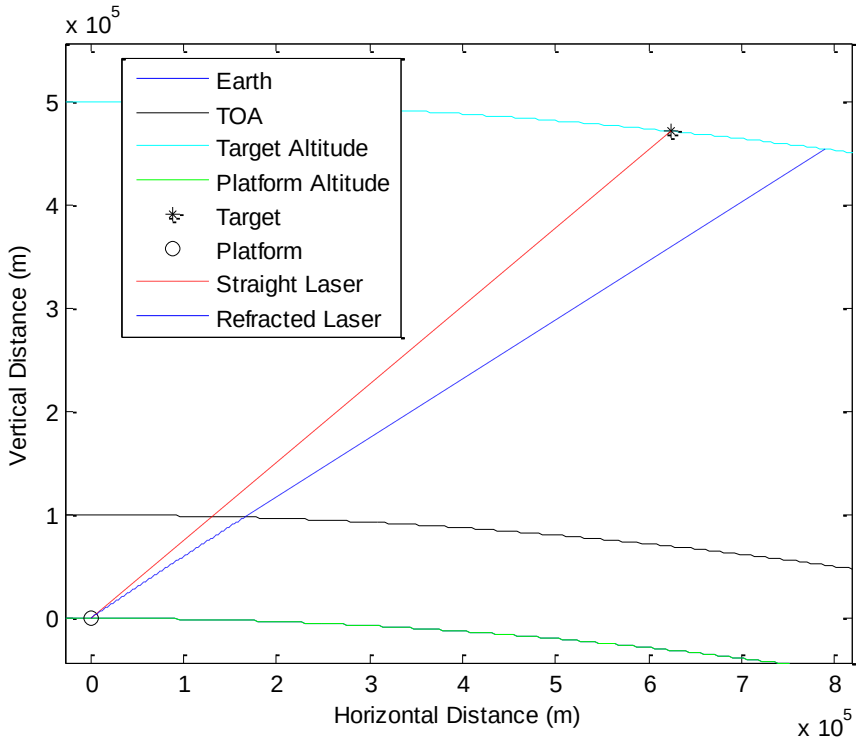


Figure 12: Refracted Laser for 1000km Target Distance

The surface of the Earth is hidden by the platform altitude plot in green. The blue line shows the refracted path that the laser takes, representative of the actual optical path a photon would propagate along during QKD. The optical properties of the atmosphere characterizing the entire pass are assumed to be similar regardless of azimuth. This allows the model to only calculate one side of the orbital pass, for angles from zenith down to the horizon. Due to landmarks, buildings and surface variations a conservative minimum elevation angle of fifteen degrees is used as the lower bound.

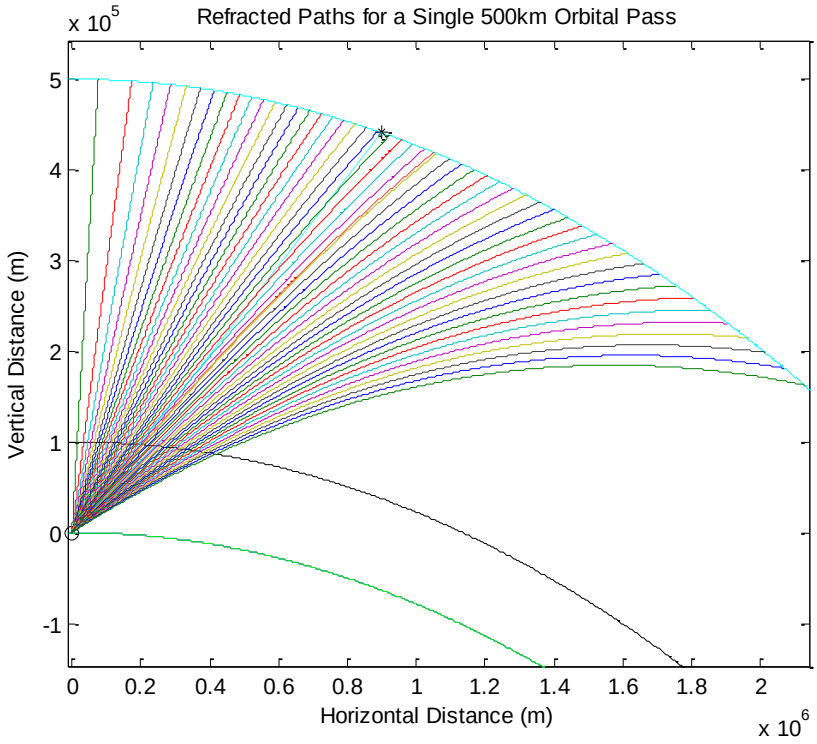


Figure 13: Refracted Paths for 500km Pass Showing Excessive Refraction

Figure 13 shows the multiple refracted paths for a 500km pass, based on the original geometry calculated by LEEDR. Each of these paths has a specific path length and transmittance that can be modeled as a function of the elevation angle at the ground station. Orbital passes that do not pass directly overhead of a ground site will still have a defined elevation angle anytime the satellite is in view, the apex elevation angle will be lower than the maximum of a directly overhead pass and the pass duration will be shorter. One of the significant errors visible in Figure 13 is continued refraction outside of the top of the atmosphere. Light should only be diffracting, not refracting, in the vacuum of space. This highlights that a geometry correction must be applied in order to use LEEDR to accurately characterize the refractive bending for an optical communication pass outside of the atmosphere.

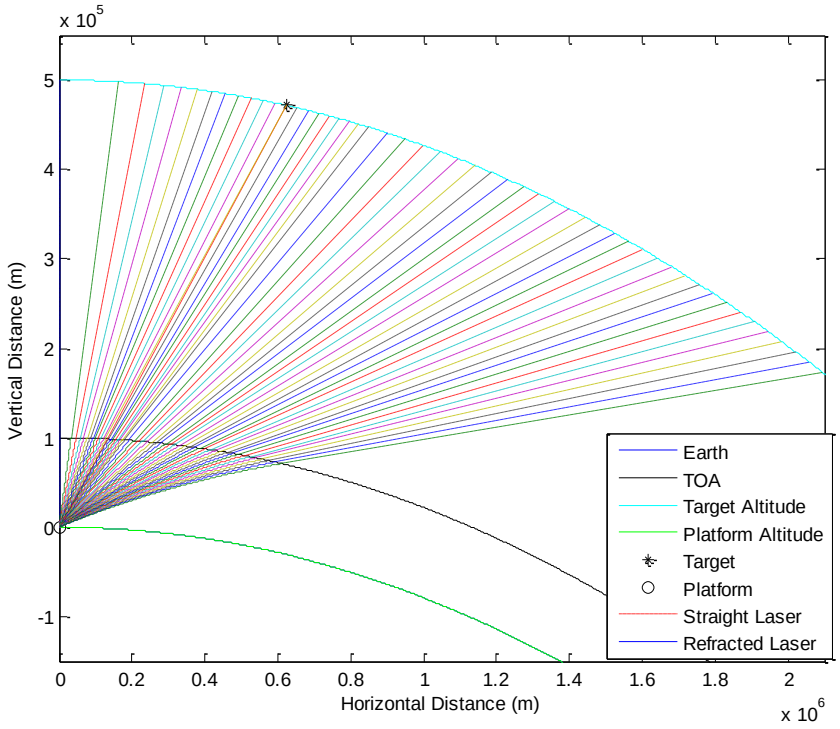


Figure 14: Refracted Paths for 500km Pass Showing Corrected Refraction

In order to address the geometry correction, the target height was adjusted down from 500km to 100km, the top of the atmosphere for LEEDR calculations. The refracted path was then recalculated. The last piece of the refracted path was used to define the direction vector of the optical path outside of the atmosphere. This direction vector defined a linear curve that intersects the circular 500km orbit. These two equations were solved by substituting the linear equation into the equation of the circle and solving for the roots. The solution resulted in the two possible x-axis points of intersection. Taking the positive x value, and solving the equation of the circle for y yields the Cartesian points used to define the final point of the refracted path. These final points were used to calculate the corrected line of sight distances and elevation angles. This resulted in the straight line paths above the atmosphere visible in Figure 14.

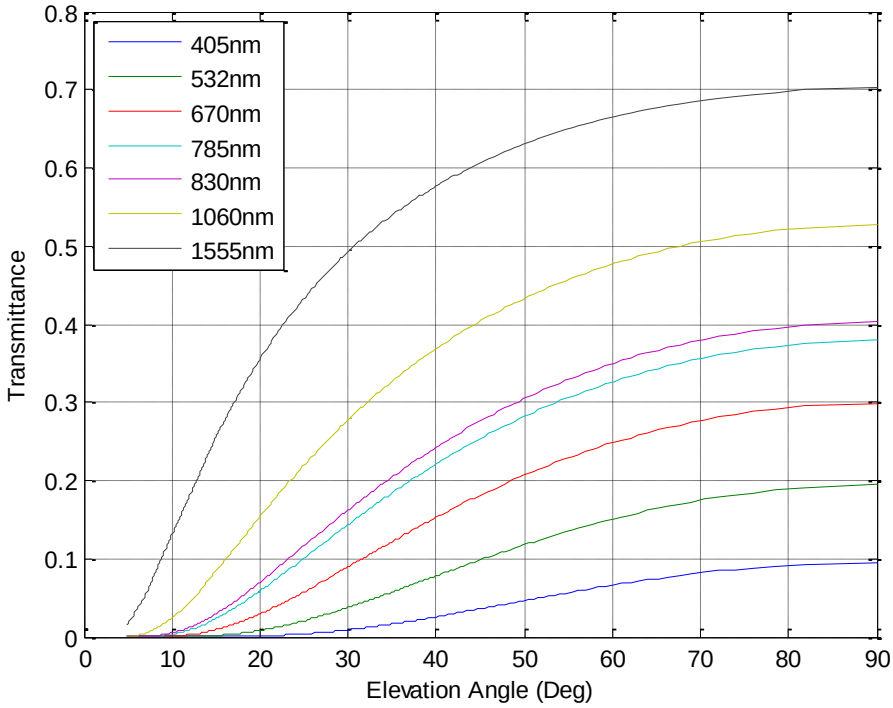


Figure 15: Atmospheric Transmittance as a Function of Elevation Angle

Figure 15 presents the summer atmospheric transmittance as a function of elevation angle, as modeled for a 500km Sun-synchronous orbit. A 405nm wavelength has the least amount of transmittance through the atmosphere and a 1555nm wavelength has the greatest amount of transmittance through the atmosphere. The drop off at low elevation angles for a 1555nm wavelength appears to be greater than for shorter wavelengths, however this is misleading. The transmittance directly scales the energy/power/number of photons that pass through the atmosphere. For this reason a calculation of the atmospheric loss better displays the wavelength dependent behavior for electro-magnetic energy propagating through the atmosphere.

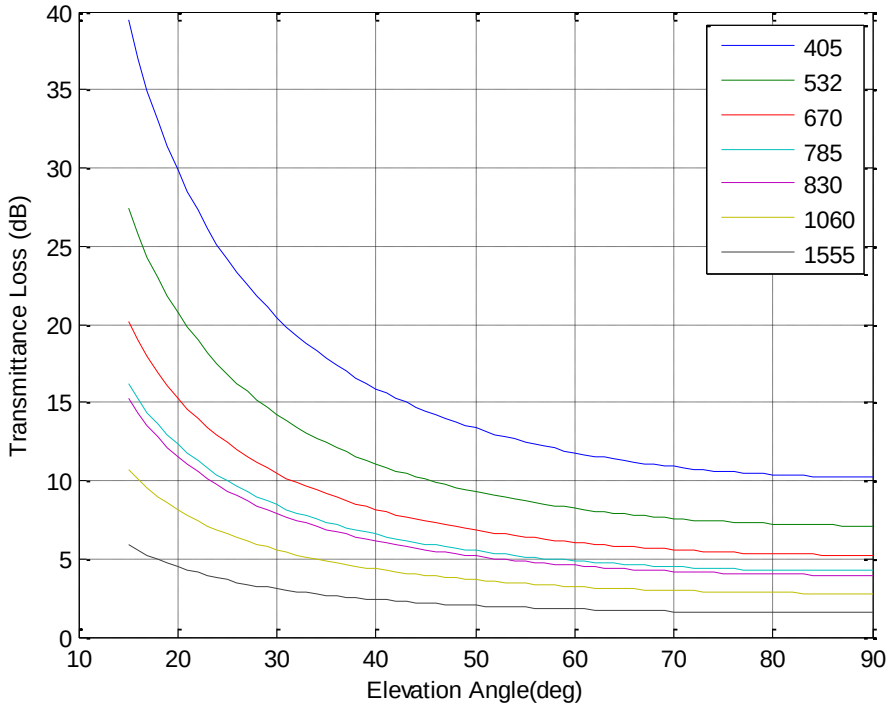


Figure 16: Atmospheric Loss as a Function of Elevation Angle

Figure 16 presents the atmospheric loss for an optical link as a function of elevation angle for seven wavelengths. The longest wavelength, 1555nm, has a difference of less than 4dB of loss between an elevation angle of 15 degrees and zenith. The shortest wavelength, 405nm, undergoes 29.22dB of loss at 15 degrees compared to zenith.

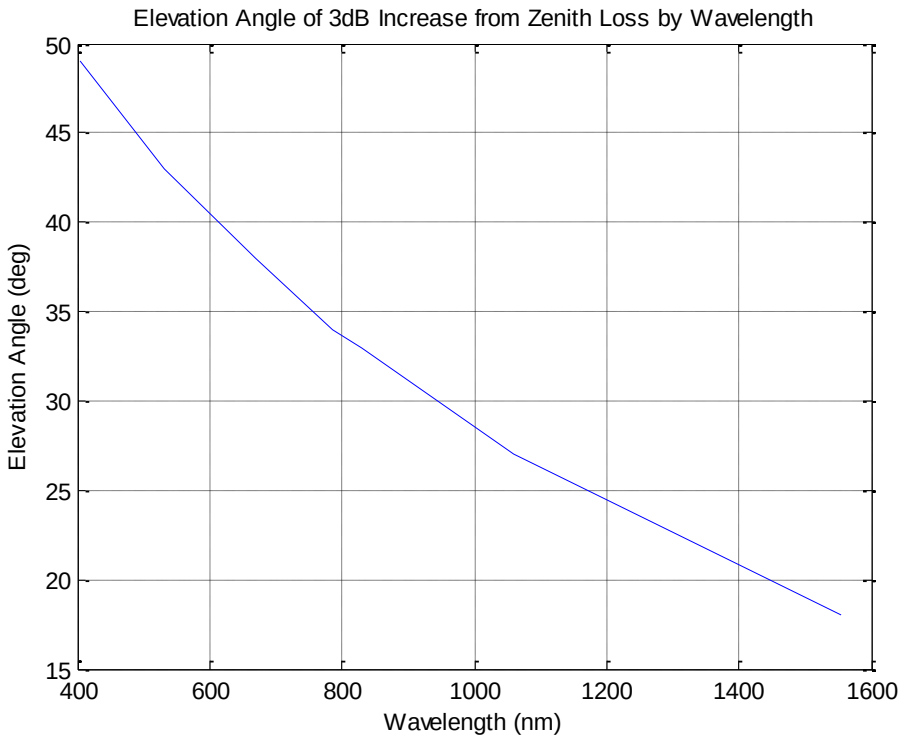


Figure 17: Elevation Angle for 3dB Increase from Zenith Loss by Wavelength

Figure 17 presents the 3dB increase from zenith. This is the point at which the transmittance value from Figure 15 is half of the zenith value for each wavelength. This line shows the cutoff where LEEDR begins to provide the needed additional fidelity for modeling transmittance as a function of elevation angle, rather than simply assuming transmittance is a constant or linear function of elevation angle.

LEEDR geometry calculations define the original elevation angle as a direct line of sight between the platform and the initial target position. The refractive bending that occurs serves to further push the laser path end point away from the initial target position described by the non-refracted line of sight elevation angle, as was shown in Figure 12. The LEEDR transmittance and refracted paths are output as a function of this straight line

elevation angle. This uncorrected elevation angle corresponds to the arrival angle of the laser beam wave front at the ground site, and defines the look angle of the receiving telescope. The corrected line of sight elevation angle for the satellite position is calculated from the refracted path end point. Using the final horizontal and vertical position of the laser path, the total range to the satellite is computed. This provides the hypotenuse and the horizontal displacement for use in determining the satellite position elevation angle. The receiving telescope pointing elevation angle and the satellite position line of sight elevation angles are then used to map the satellite's elevation angle based on line of sight (true elevation angle) to the elevation angle used to point towards the incoming optical beam (refracted elevation angle).

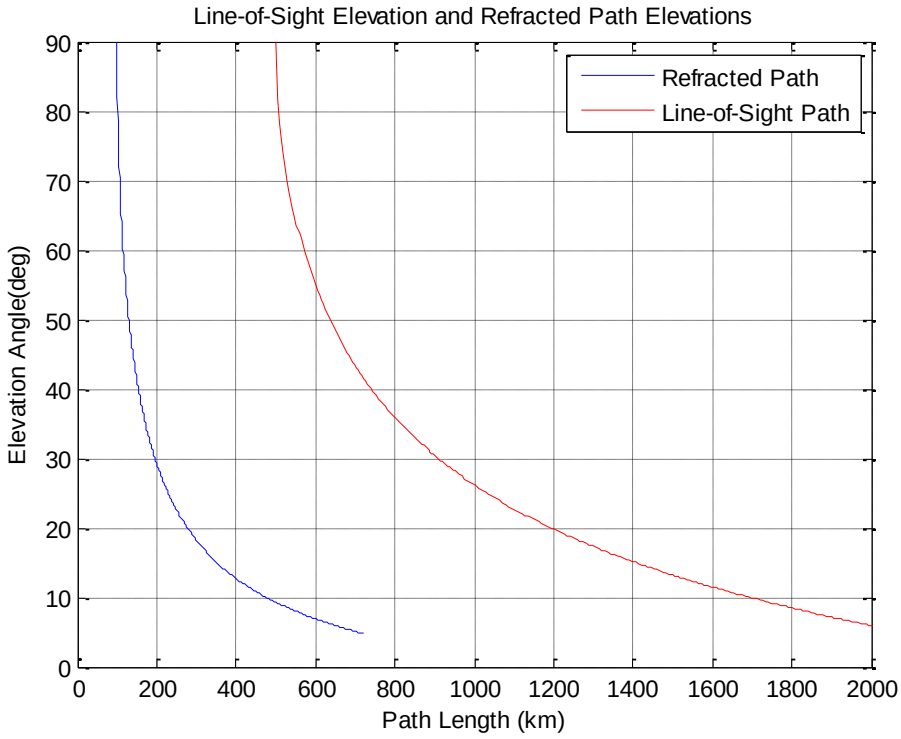


Figure 18: Correlation of Path Lengths and Elevations for Mapping Refracted Properties

Figure 18 shows the difference between the uncorrected elevation angle and the true elevation angle based on line of sight as a function of path length. The model accounts for the longer refracted path by mapping the line of sight path to the properties of the shorter refracted path, while still accounting for the longer path length. Any values that don't match specific points in the model are interpolated via the method of cubic splines. The steps in the graph (most noticeable at 22^{o} and 1125km) that occur throughout the curve are a result of changes in the thickness of the modeled atmospheric layers as the line of sight distance continues to increase. This results in step changes for the total refraction of the beam. The curves reflect identical step behavior because the line of sight elevation angle is determined from the end points of the refracted data.

The atmospheric profile for both AFIT and NPS are both dependent on the time of night that the satellite passes over head. The best balance of atmospheric characteristics occur for a midnight to 3am pass as the temperature gradients in the atmosphere provide a negative temperature gradient that bends light towards the Earth [16, p. 14]. This midnight to 3am window provides additional viewing range without introducing additional background noise from the Sun. A Sun synchronous orbit ensures that the satellite passes over ground sites at similar local times within the midnight to 3am window. The pass times were verified against the orbital simulator that was created, correcting UTCG to local times based on a 5 hour difference at AFIT and an 8 hour time difference at NPS.

Orbital Simulator

David Vallado's book *Fundamentals of Astrodynamics and Applications* [14] provides the instructions to implement the SGP4 algorithm and an additional amount of functionality, to include coordinate transformations. The code available from Celestrak's online software repository [25] serves as the backbone of this orbital propagator. The need for development of an orbital propagator was driven by licensing requirements from the research sponsor. The code created can readily be executed in any scripting computer language that has a working Octave interpreter. This software may be used freely for any purpose, to include academic, military or commercial studies.

The foundation of the orbital model is developing a TLE file and feeding it into the SGP4 initialization subroutine. This routine reads in the parameters used to describe the orbit of the satellite, as well as the approximations of the perturbations affecting the satellite. This defines all the relevant properties of the satellite that are used by the SGP4 propagator to determine the satellite position at any point in time. The satellite structure and the desired time step for propagation are then passed into the SGP4 propagation routine. This routing calculates all of the forces acting on the satellite, to include perturbations due to third bodies, drag and other factors. The routine then numerically integrates the acting forces to define the acceleration, velocity and position vectors of the satellite, for a give point in time. The time period for study was chosen as 1 Jan 15 to 1 Jan 16. This was an arbitrary choice, tied to the center period for which the author was attending school. Shifting the time period either forward or backward in time would not change the properties of the orbital passes over the ground sites due to the Sun-synchronous orbit selected. One short-coming with this year-long period of propagation

is that the atmospheric properties were defined for summer and winter conditions and the two other seasons experienced in a year are not accurately characterized. The initial time step chosen was a one minute interval to limit the total amount of data that was output by the orbital propagator. The reason for this choice was to speed up simulations so that the model could be evaluated for functionality without excessive wait times. The one minute step size resulted in 525,600 data points that output a specific ECI position, velocity, range to each ground site and elevation angle for each ground site.

The ECI position and velocity output vectors were then used to calculate the initial Doppler shift experienced. They were also fundamental to convert satellite elevation angles seen by the ground sites at AFIT and at NPS via implementation of Vallado's *rv2razel* routine [25]. Initially there was difficultly implementing the routine due to neglecting leap seconds for time transformations between the Julian day calendar and the J2000 epoch used as a time reference. The *rv2razel* routine calculates the elevation angle for every time step, as referenced in the SEZ frame. Any elevation angle less than zero indicate that the satellite is below the horizon and can be immediately discarded. From the remaining elevation angle data, the range to ground site information was used to as the logical switch to determine which ground site in view would provide a higher key rate for an optical downlink. NPS was given priority over AFIT in order to provide additional pass time to transfer the key generated at AFIT. This approach did not provide the expected utility as a satellite could use classical communication to provide the AFIT key to NPS as an encrypted message. The logical prioritization of NPS proved useful in that NPS averaged lower average detection rates than AFIT as will be addressed in Chapter IV.

Laser Downlink

The laser downlink is a single function composed of three outputs. The power received, the fractional power received and the spot size are calculated based on Equations (8) and (10) depending on the total refracted path length, telescope properties and the wavelength used. The spot size information allows calculation of the percentage of the beam that the receiving aperture captures, which is directly dependent on receiving aperture size. The received power defines the link losses as a function of wavelength and propagated distance. The model for spot size and power was verified by performing calculations similar to those in [16].

The properties of the laser downlink change as a function of the wavelength used. For this reason it was important to determine if a Doppler shift would create effects that would influence the validity of the model. The Doppler shift was modeled based on Equation (16) [26, p. 121]. It was calculated in an ECI frame that was sufficiently inertial for the duration of the beam propagation, accounting for both motion of the satellite and the rotation of the Earth.

$$v_a = v_e * \frac{\left(1 - \frac{v}{c}\cos\left(\theta_{c,v}\right)\right)}{\left(1 - \frac{u}{c}\cos\left(\theta_{c,u}\right)\right)} \sqrt{\frac{\left(1 - \left(\frac{u}{c}\right)^2\right)}{\left(1 - \left(\frac{v}{c}\right)^2\right)}} \tag{16}$$

where:

$v_a = received\ frequency$
$v_e = emitted\ frequency$
$v = inertial\ velocity\ of\ the\ receiver$
$u = inertial\ velocity\ of\ the\ emitter$
$\theta = radial\ direction\ between\ v, u$
$c = the\ speed\ of\ light$

Table 2: Doppler Shift in GHz for Largest and Smallest Studied Wavelengths

Wavelength	**Shift (GHz)**
405 nm	34.385
1555 nm	8.956

The total Doppler shift experienced is the maximum frequency observed minus the minimum frequency observed.

Table 2 shows that the total expected Doppler shift for a 405nm wavelength would be on the order of 35 GHz. Similarly, the total expected Doppler shift for a 1555nm wavelength would be on the order of 9 GHz. Any wavelength longer than 405nm, but shorter than 1555nm, would have a Doppler shift between 35GHz and 9GHz. As long as the optical bandpass filters used for each wavelength can accommodate the Doppler shift, then the Doppler shift would not impact the optical link.

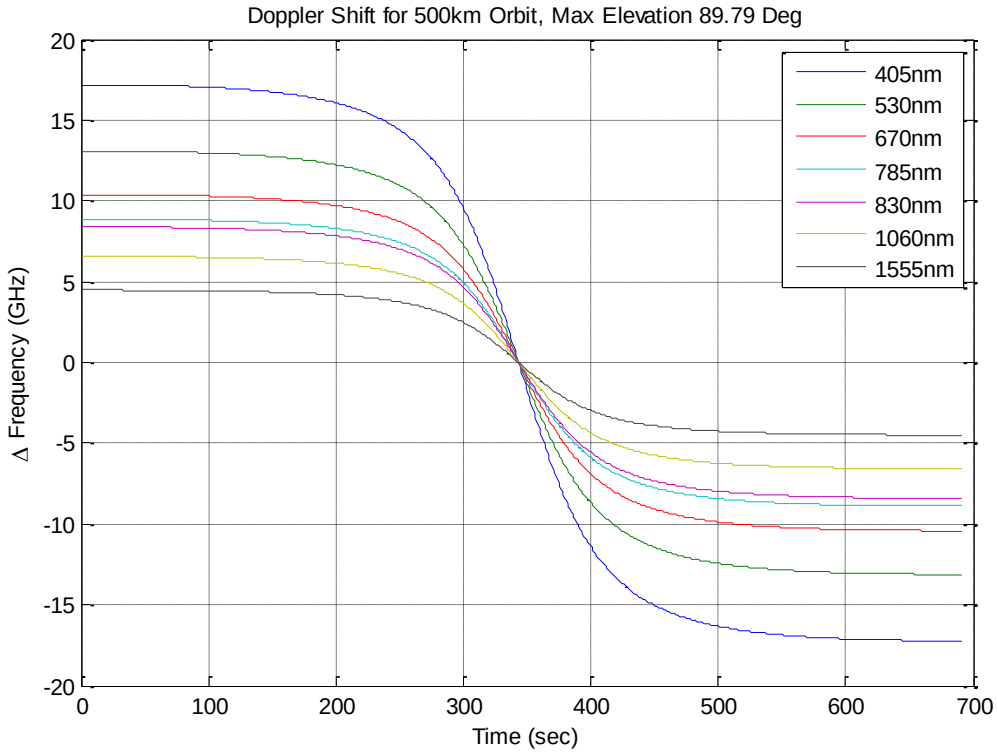


Figure 19: Doppler Shift for 89.79^{o} Elevation Angle Pass at 500km

Figure 19 shows the Doppler shift for the wavelengths of interest. They are approximately five orders of magnitude smaller than the center frequency. A survey of optical filters available from Newport Corporation [27] showed that most optical bandpass filters have 2nm of additional bandpass around the center wavelength. Shifts on the order of GHz correspond to at most a .03nm wavelength change for 1555nm wavelengths. These shifts are therefore assumed to be accommodated by the optical passband of the hardware and will be neglected. This assumption was confirmed by subject matter experts at the Starfire Optical Range (SOR) in Albuquerque, NM. An additional assumption is made that the wavelength's transmittance does not significantly differ due to Doppler shift. This is a valid assumption because the transmittance windows

shown in Figure 11 are tenths of nanometers wide which encompass the hundredths of nanometers wide Doppler shift.

The laser downlink is not only susceptible to losses from channel effects. Optical Hardware is not 100% efficient, and introduces additional losses. Quantum detectors are not perfect, and the illuminated area of receiving sensors can be limited by diffraction that occurs in the receiving telescope. Incorporation of these terms increases the complexity of the optical loss model from a single number to a large combination of every component's efficiency. Most optical models from academia have avoided specifying performance of individual components due to the greater variability in introduces into the model. Like others, this paper defines the optical hardware transmissivity as a single value of 50% efficiency, as the additional complexity will be included after integrating the model into qkdX [3]. SOR confirmed 50% optical system transmission as the standard assumption used for modeling optical hardware [17]. This corresponds to a 3db loss of the signal and matches the modeled losses of the Bourgoin study used as a validation comparison against the model.

Complete Optical Link

Detection Rate Equation

Equation (14) was rearranged to the format shown in Equation (17). The energy at the source is replaced by the irradiance profile at the receiver [8].

$$N = \int_{\lambda_1}^{\lambda_2} I_\lambda(\lambda, z, t)\, cos(\theta_R) T_a(\lambda, \theta_s) A_t \eta_R(\lambda) \left(\frac{\eta_q(\lambda)\mathcal{F}}{\frac{hc}{\lambda}} \right) d\lambda \Delta t \tag{17}$$

where

$\eta_q = detector\ quantum\ efficiency$
$I_\lambda = Irradiance\ at\ the\ receiver$
$h = Planck's\ constant$
$c = the\ speed\ of\ light$
$\lambda = wavelength\ in\ meters$
$R = distance\ between\ the\ satellite\ and\ receiver$
$A_r = receiving\ aperture\ area$
$\eta_R = receiver\ path\ efficiency$
$T_A = atmospheric\ transmission$
$\theta_R = incident\ wave\ front\ error\ angle$
$\theta_s = satellite\ elevation\ angle$
$\Delta t = time\ step$

Equation (17) is integrated with respect to the bandpass of the system. The assumption that values are approximately constant over the bandpass allows the integrand to be removed and the specific values for the link to become averages denoted by line accents [8].

$$N = \overline{I_\lambda(\lambda, z, t)}\, cos(\theta_R) \overline{T_a(\lambda, \theta_s)} A_t \overline{\eta_R(\lambda)} \left(\frac{\overline{\eta_q(\lambda)}\mathcal{F}}{\frac{hc}{\lambda}} \right) \Delta t \tag{18}$$

This irradiance is then integrated over the area of the receiver to equate to a power.

$$P = \bar{I}_\lambda A_r = \iint_0^r \bar{I}_\lambda(z, t) \delta^2 r = P_0[1 - \exp(-\frac{2r^2}{W})] \tag{19}$$

The power term is substituted into the equation, and all the terms are updated to match the assumptions made during this study. Equation (20) represents the final equation used to determine the detection rate measured at each second time step.

$$Q = \frac{N}{\Delta t} = P_0[1 - \exp(-\frac{2r^2}{W})]T_a(\lambda, \theta_s)\eta_R \left(\frac{\eta_q}{\frac{hc}{\lambda}}\right) \quad (20)$$

Equation (20) can be integrated with respect to time in order to measure the total number of qubits exchanged during a pass. Any additional inefficiency in the system simply scales Equation (20) as an additional factor. Specht determined that in order to account for an offset of the beam due to imperfect pointing, a calculation of the cumulative distribution function (CDF) of a Rician distribution should be used [6]. This distribution provides the same value as Equation (20) when no offset it used, and became necessary for the validation discussed in Section IV. The Rician CDF was implemented via *makedist* and *cdf* based on the available functionality in the MATLAB R2013a Statistics Toolbox v8.2, and replaced the Equation (19) bracketed terms in the final calculation.

Quantum Bit Error

The quantum bit error rate (QBER) was then calculated to better describe the quality of the link, and to ensure the required 11% threshold for QBER is not exceeded [23]. The formula for QBER is shown in Equation (21). This is the modeled error conditioned on random turbulence [28]. Shapiro [9] has shown that turbulence has a negligible effect on the error rate for BB84 implemented over a satellite link. This allows the QBER to be calculated based on the no turbulence condition rather than accounting for the random effect of turbulence during the simulation. The quantum bit error rate depends on the fraction of the power received, the noise in the link and the average photon number in each pulse. Each step of the satellite propagation was used to estimate a quantum bit error rate for that respective position.

$$QBER = \frac{\eta n_N e^{-\eta(n_s \mu \tau + 4n_N)}}{\eta(n_s \mu \tau/2 + 4n_N) e^{-\eta(n_s \mu \tau + 4n_N)}} \quad (21)$$

where $\eta = detector\ quantum\ efficiency$
$n_N = noise\ photon\ count\ per\ pulse$
$n_s = average\ photons\ per\ pulse$
$\mu =\ the\ optical\ link\ power\ fraction\ in\ vacuum$
$\tau = atmospheric\ transmittance$

The quantum bit error rate equation shows that the larger the fraction of received power (larger μ) the lower the overall error rate. The fraction of power received for a satellite link can be found from the Rician distribution cumulative distribution function [6]. The atmospheric transmittance also plays a role in the QBER estimate. The smaller the τ value the higher the QBER is going to be, as fewer of the signal photons are passed through the atmosphere.

Summary

This chapter has described all the pieces of the model that have been developed. The atmospheric parameters are derived from the functionality inherent in LEEDR, with a geometry correction for satellite application. The satellite's position is defined by propagating a TLE based on SGP4, which then feeds an elevation angle and range to the final optical link model. The optical link model calculates descriptive properties of the satellite QKD link based on the hardware choices and wavelengths selected. This model accounts for the telescope sizes, inefficiencies of optical hardware and limitations on single photon sources and detectors. The next critical step is to verify that the model accurately performs the way it is intended by validating it against other sources in academia.

IV. Analysis and Results

Chapter Overview

This section deals with the model validation and the experiment that was performed based on using the methodology described previously. The first part of this section describes validation against a computer model. While comparison to simulation results is useful, experimental data is a more accurate test of the quality of a model. The second validation step outlines the experimental data that was used and the validation process taken, as well as presenting the validation results. The final section of this chapter outlines the experiment conducted with the validated model and then presents the summary findings. Results are presented in tables and graphs to quantify best expected performance and to characterize how performance changes as a satellite passes overhead.

Validation Against Bourgoin

The model vas first validated against the simulation performed by Bourgoin [10]. The Bourgoin simulation calculated expected performance for a year-long 600km satellite conducting a QKD link at 670nm for a Sun-synchronous orbit implementing a decoy state protocol. The ground site was taken to be a location 20km outside of Ottawa, Canada. The detector efficiency for the single photon detection was identified as a thick avalanche photo diode from Excelitas Technologies. The exact detector is not identified and a representative efficiency of 0.62 was selected based on the products available in the cited catalog [29]. The optical hardware was assumed to be approximately 50% efficient, as identified by the described 3db loss. The transmitting telescope had a 10cm diameter, while the receiving telescope had a half meter diameter. The Bourgoin paper also made a

design choice of 300 million pulses per second to generate the beam used for their QKD link. QBER estimates and values for the raw key generation were presented in graphs so the maximum values for comparison are estimated. Bourgoin's simulation incorporated additional losses that were not originally included in the developed model. These additional losses were added for the validation calculations to ensure accuracy of the model and validity of comparing results.

Table 3: Bourgoin Validation Comparison, Best Pass at 670nm [10]

Property	**Bourgoin**	**Modeled**
Orbital Altitude	600km	600km
Site	Unknown	WPAFB
Aerosols	Rural (MODTRAN)	Urban (MODTRAN)
Pointing Error	2 μrad	2 μrad
MPN	.5	.5
Transmittance	~.38	.30
$\eta_{detector}$	Unknown	.62 [29]
η_{optics}	.5	.5
Telescope Radius	.25 m	.25 m
Zenith Detection Rate	~68k bit/s	85k bit/s
Minimum QBER	~1%	1%

The exact ground site is not identified within the Bourgoin study, only the location of the background light. The simulation describes a maximum elevation angle pass that is used from a noon/midnight Sun-synchronous orbit. WPAFB was used as the ground site because a similar elevation angle pass for a 600km orbit could be readily identified and the atmospheric differences were accounted for. The additional differences in detection rate can be attributed to the unknown detector efficiency, additional loss due to Bourgoin's incorporation of rotational misalignment between the satellite and the receiver, the slant range offset approximation used and the non-specific description of the decoy state protocol used.

Table 3 shows the input values used for the Bourgoin simulation and the developed model. The approximate 25% increase in zenith detection rate is most likely due to assumed values for the detector efficiency and the assumed implementation of mean photon number. The Bourgoin paper identifies the mean photon number as 0.5 and also states it is used with a decoy state protocol that randomly selects between sending a signal or a decoy state with a mean photon number of 0.1. The statement "randomly selects" was interpreted that fifty percent of the time the signal was sent and fifty percent of the time the decoy state was sent. The raw key rate is defined based on the signal photons only, and the power in the beam does not account for the additional photons from the decoy state. The total power in the beam was determined by taking the number of pulses per second and scaling it by both the percent of time the signal was being transmitted and the mean photon number which approximates the average number of photons in a pulse. The 25% error between models is acceptable for a first order model that is designed to study the general properties of a satellite link.

Validation Against Vallone

The second validation approach was to model the 2015 Vallone experiment and compare calculated bit rate and QBER to the experimental data collected, accounting for similar losses due to inefficiencies. The Vallone experiment took place in Matera, Italy at the Matera Laser Ranging Observatory. The experiment consisted of bouncing a 532nm beam of coupled 10Hz satellite laser ranging pulses and 100 Hz qubit pulses off of 5 satellites equipped with corner cube reflectors. Once the reflected beam was detected, the outgoing beam was attenuated to approximate a mean photon number of one leaving the

satellite. The purpose of the experiment was to measure a qubit sent with a known polarization in order to experimentally prove the feasibility of the BB84 protocol with satellite transmission. The experiment was very successful. The four satellites that had reflectors coated to maintain polarization had detectable qubits and measurable QBERs on the order of 5%. This is well within the 11% threshold to ensure eavesdropping is not present. The final satellite did not maintain polarization of the reflected qubit and had a measured QBER of 40%, close to the expected value of 50% and well above the 11% threshold used to detect Eve.

This experiment was the first of its kind to successfully demonstrate the BB84 protocol via satellite with an experimental demonstration. Of the four satellites, Jason2 was selected as the satellite for comparison because a TLE file to define the satellite's orbit was readily available. Modeling the downlink beam required a change in the implementation of the QKD model, in that a reflecting surface was used to define the beam incident at the receiver, rather than the collimated laser beam that was originally developed. The beam properties were calculated based on the mean photon number, the distance from the reflector to the receiver, the pulse rate, the downward gain derived in the article and the receiver area scaled by the loss due to energy spread along the surface of a sphere at a distance R from the satellite. The previous method of defining the total power in the beam based on the pulse rate and energy in a photon was used, however in order to accurately capture the new fraction of the beam incident on the receiver the approach shown in Equation (22) was used.

$$FRAC = \frac{G_{reflec} A_r}{4\pi R^2} \tag{22}$$

where $G_{reflec} = reflected\ downlink\ Gain$

This fraction was used in both the QBER estimate and scaled by the initial power in the beam to determine the total power in the beam at the receiver, and ultimately the total bit rate.

Table 4: Vallone Validation Comparison, Best Pass at 532nm [23]

Best Pass, 532nm	**Vallone**	**Modeled**
Orbital Altitude	1336km	1336km
Site	Matera, Italy	Matera, Italy
Aerosols	Unknown	Rural (MODTRAN)
Pointing Error	Unknown	None
MPN	1.6	1.6
Transmittance	.89	.65
$\eta_{detector}$	.10	.10
η_{optics}	.13	.13
Telescope Radius	.75 m	.75 m
Zenith Detection Rate	Unknown	200 counts/sec
Minimum QBER	~5% measured	5.7% calculated

Table 4 lists the properties used in the validation against the Vallone experiment. The rural aerosol definition used in LEEDR calculated a lower transmittance than the value provided in the article. No pointing error was used because the design of a CCR is such that incident light is returned in the direction it was received. Rotational misalignment is also unnecessary because of the polarization maintaining coating on the CCR. The mean photon number is a derived value based on the radar equation used in the article. The zenith detection rate calculated is approximately 200 counts per second (cps). The detected counts per second correlate very well between the experimental and modeled

values. The correlation is shown in Figure 20 as the green line overlaid on the Jason2 graph. The modeled QBER at a range of 1600km is higher than the experimental value by 2%. The error bars put a max on the QBER of 7.7% which is close to the modeled 8%.

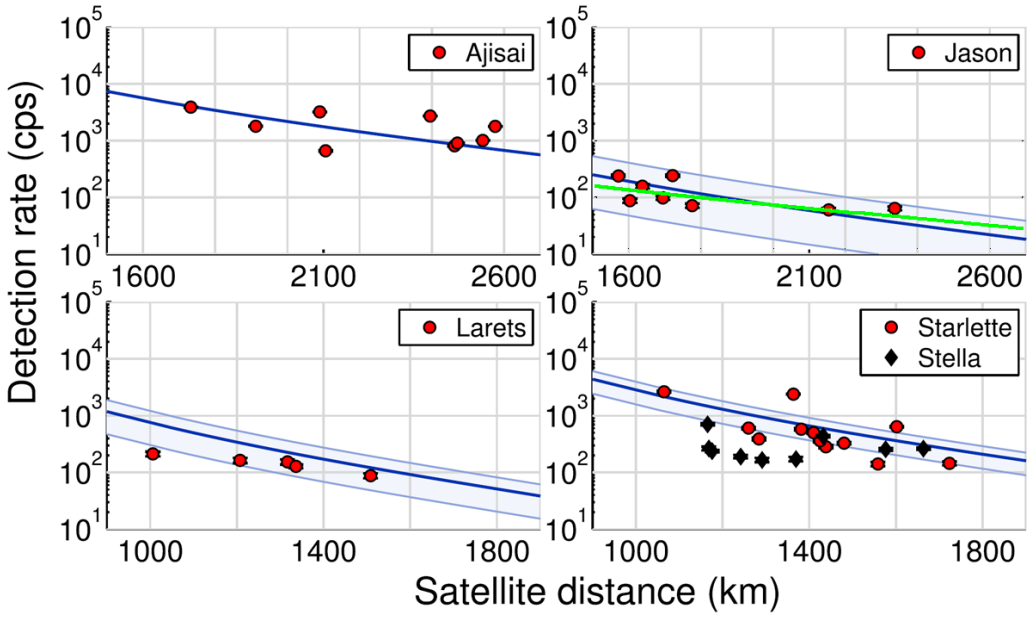


Figure 20: Detection Rates and Link Budgets with Modeled Overlay on Jason2 [23]

Specht Model Comparison

The developed model was also compared to the model developed by Specht [6]. The same values were used for any matching input parameters. Notable differences from Table 5 between the developed model and Specht are the atmospheric transmittance calculations and the pointing error approximations.

Table 5: Comparison of Specht's Approach and Modeled Approach by Model Property [6]

Model Property	**Specht**	**Modeled**
Wavelength	1 input, user defined	7 preselected values
Doppler	Not addressed	Addressed - negligible
QBER	Not addressed	Shapiro calculations
Refracted Path	User input number of layers	LEEDR defined, 1000 layers
Offset	Refracted Path	Line of sight approximation
Photon Reception	Probabilistic calculation	Fraction of diffracted beam
Atmosphere	1976 Standard Atmosphere	LEEDR ExPERT
Atmospheric Attenuation	Constant	Variable
Photon Source	Perfect Single Photon Source	MPN
Orbit Propagator	SGP4	SGP4
Language	Python 3.4	MatLab 2013a

Specht's model uses a constant transmittance for the entire pass. Specht's estimation of pointing error is improved over the approach used in this thesis. Specht calculates pointing error based on the refracted path used to define the satellite position. The model from this thesis approximates pointing error based on the line of sight distance from the satellite to the ground station plus the additional length of the refracted path. The line of sight approach provides similar estimates to the Specht model at directly overhead passes, however the approach underestimates the beam offset at low elevation angles. Compared values at approximately 35 degrees of elevation angle resulted in the model underestimating offset by over 2 meters compared to the Specht calculated value.

Table 6: Specht Validation Comparison, Best Pass at 670nm [6]

Best Pass, 670nm	**Specht**	**Modeled**
Orbital Altitude	600km	600km
Aerosols	None	Urban (MODTRAN)
Pointing Error	2 μrad (Refracted)	2 μrad (Line of Sight)
MPN	0.4	0.4
Transmittance	0.30 (Constant)	0.30 (Variable)
η_{rxr}	0.5	0.5
η_{optics}	0.5	0.5
Telescope Radius	0.5 m	0.5 m
Zenith Detection Rate	137.3k bit/s	141.5k bit/s
Difference	-4.2k bit/s	+4.2k bit/s

Table 6 highlights the values used for the comparison study. The method of MPN calculation was modified for the model to only capture the probability of a pulse having more than one photon, rather than accounting for the additional energy in the multi-photon pulses. This reduced the MPN from .5 to .3935. This change was necessary to enforce similarity between the models, by allowing the model to estimate perfect single photon sources rather than accounting for additional energy captured in the mean photon number. Table 7 presents the calculated values for the comparison at different elevation angles in the pass. As the elevation angle decreases the different approaches for modeling offset and transmittance become pronounced.

Table 7: Specht Comparison Calculated Differences for Several Elevation Angles [6]

Elevation (degrees)	**Approach**	**Spot Diameter (meters)**	**Offset (meters)**	τ_{atm}
88.9	Modeled	5.12	1.2	0.299
	Specht	5.25	1.23	0.3
35.1	Modeled	8.24	1.93	0.13
	Specht	8.43	3.44	0.3
15	Modeled	13.88	3.25	0.018
	Specht	14.1	12.78	0.3

The approximate magnitude due to the difference in offset approaches is similar to the approximate magnitude due to the differences in transmittance calculations. For this reason the models match more closely than would be expected.

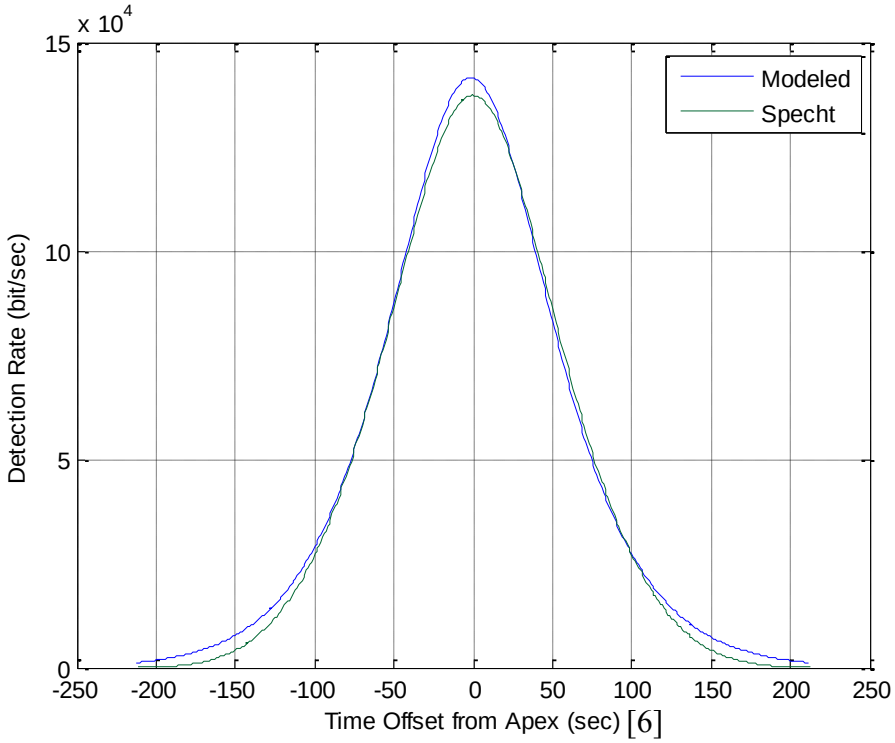


Figure 21: Detection Rate for Comparison to Specht Model, 600km Best Pass

Figure 21 shows the best pass comparison between the model and the Specht model. The model provides slightly higher estimates, especially at low elevation angles due to the non-refracted estimate for pointing error offset. At apex, the line of sight approximation is most accurate, and the atmospheric transmittance is identical. Again, the model does match more closely to the Specht comparison at low elevation angles than would be expected from the differing approaches to modeling offset. This is due to the additional transmittance losses that are not captured in the Specht model. From this comparison, the difference between line of sight and refracted error calculations for a 2

μradian bias matches closely to the difference between using a variable transmittance and a constant transmittance.

Based on the correlation between the model and both real-world data and an existing QKD simulation, the model is considered validated. The model lines up within the error bars of the experimental data curve fit and is within 25% of the simulated data while neglecting some additional error sources. The model is flexible enough to handle any satellite orbit and can be used for any latitude and longitude. The results of the validation support the use of the model to describe the performance of a real-world scenario. The chosen scenario and results are described in the next section.

Multi-Site Trusted Node

A simulation was conducted with the validated model to determine the expected raw key generated by a satellite acting as a trusted node between AFIT and NPS. This choice of ground stations is due to their geographic separation. The installation of an optical network linking these two sites is currently prohibitively expensive. AFIT and NPS were chosen as academic institutions that may have an interest in the secure communication offered by QKD. As a trusted node, the satellite in question passes over the first ground site and develops a secure key through the traditional BB84 protocol. The satellite then repeats the operation at the second ground site, and passes the first secure key as the contents of an encrypted message to the second ground site. The satellite passes the raw key material to the ground site at AFIT first because of the direction of the Earth's rotation. The AFIT ground station is the first one to come into the satellite's field of view during the night. Once the shared encrypted key is passed to the NPS, the satellite

can repeat the process each night to allow for one-time pads or frequent rekeying ensuring secure encrypted communications between AFIT and NPS.

The experiment itself is very similar to the Bourgoin model validation addressed in the previous section. The wavelengths at 405nm, 532nm, 670nm, 785nm, 830nm, 1060nm and 1555nm were all modeled in order to determine the best candidate for the payload design. Temporal constraints were placed on the satellite positions to only use passes that occurred between midnight and 3A.M. to correspond to the atmospheric profile defined in LEEDR. The satellite orbit used was a 500km Sun-synchronous orbit that maintained overhead passes between midnight and 3A.M. for ground stations on the night side of the Earth. Due to the need for NPS to both generate key, and exchange the secret key, additional time was allotted to the NPS passes by using a logical discriminator that prioritized NPS anytime it was in view concurrently with AFIT. Prioritizing NPS does not significantly change the results; however it does allocate a few more low elevation angle passes to NPS than AFIT, which provides additional time to transfer encrypted communications to ensure NPS receives the secure key generated between the satellite and AFIT. The transmittance profiles for both winter and summer were used to provide a more accurate year-long estimate. The winter profile was used for dates from 15 October to 14 April and the summer profile was used from 15 April to 14 October.

Results of Simulation Scenarios

The percentile passes are displayed in Figure 22. The values for AFIT were within 1% of those for NPS so only the AFIT percentiles are shown. The minimum elevation angle cutoff was fifteen degrees, which makes 50% of the total passes during a year

unusable for either AFIT or NPS. 75% of the total annual passes occur at very low elevation angles, below 35 degrees. Such low elevation angles increase path lengths through the atmosphere and drive transmission losses to dominate diffractive losses because of the lower altitude on a LEO satellite.

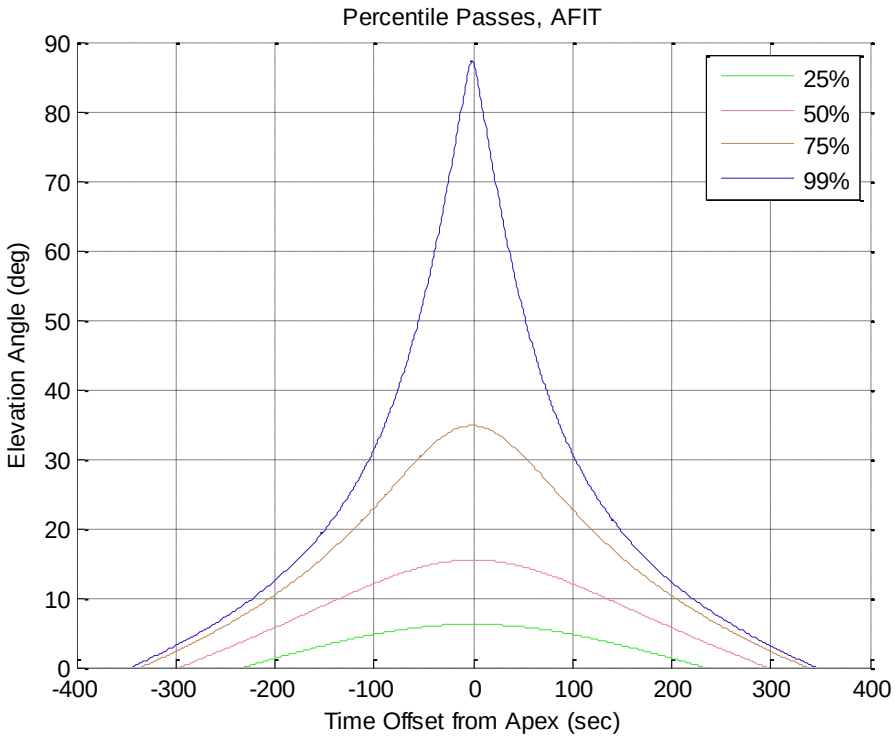


Figure 22: 500km Sun-Synchronous Orbit Percentile Passes

The best pass results for AFIT are shown in the following figures. The values for the AFIT passes are within 1% of the passes at NPS and the NPS graphs are located in Appendix A. The maximum elevation angle passes for both ground stations occur in winter near the beginning of the simulation runtime. The winter transmittance profiles reflect a more absorbing atmosphere at AFIT, while the NPS atmosphere does not vary significantly from summer due to its coastal proximity.

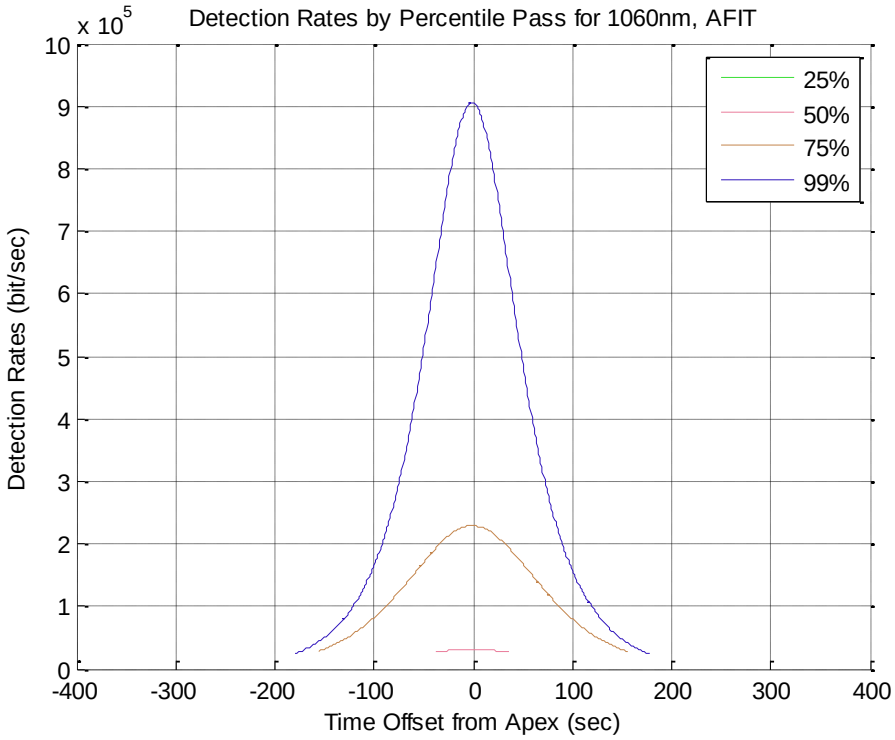


Figure 23: Detection Rates by Percentile Pass for 1060nm at AFIT

Figure 23 presents the associated detection rates for each percentile pass at the 106nm wavelength. The 99% percentile pass provides much higher detection rates as the line of sight distance between the satellite and ground station is the shortest of the percentile passes at apex. The majority of passes during the year are closer in performance to the 75% percentile pass. The 50% percentile pass barely contributes to the total number of qubits exchanged while the 25% percentile pass does not contribute to the modeled QKD scenario because the pass elevation angles are below the fifteen degree cutoff. The best-pass performance is slightly misleading in that it describes the closest possible approach the satellite makes to the ground stations. The majority of passes are much lower in elevation angle. Next, the performance for multiple wavelengths is presented. A low elevation angle pass is also presented, in order to highlight the

wavelength trends at low elevation angles which accounts for the majority of passes during the year. NPS graphs can be found in Appendix A.

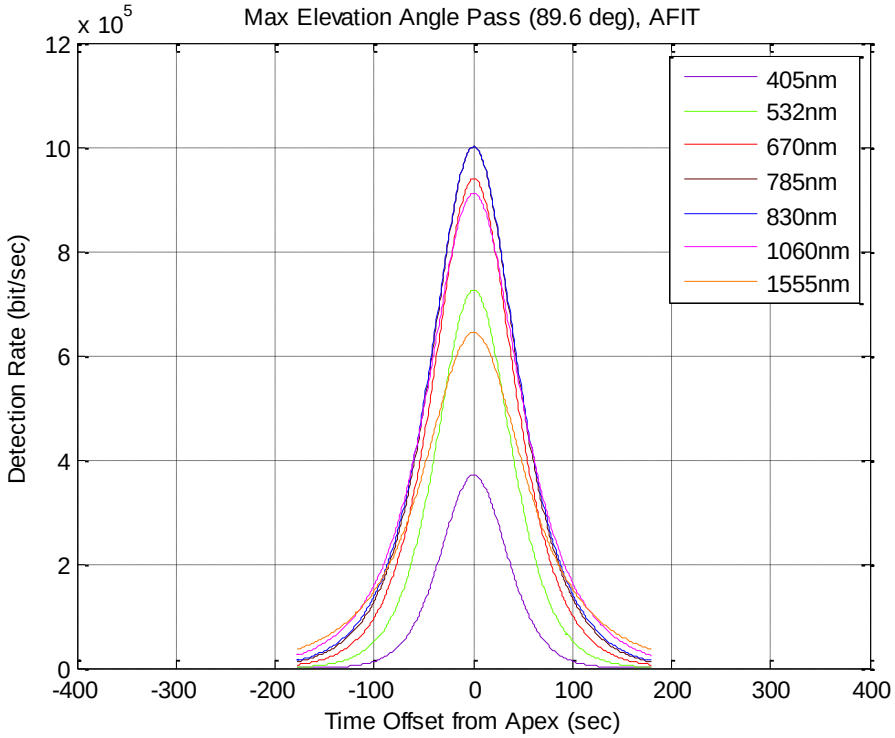


Figure 24: AFIT Detection Rate for Best Pass, 500km Sun-Synchronous Orbit

Figure 24 shows the 7 wavelengths studied and their detection rates from the satellite coming into view at 15 degrees of elevation angle, passing overhead at 89.6 degrees of elevation angle and moving away back down to 15 degrees of elevation angle. At the lowest elevation angles the 1555nm wavelength performs the best due to its greater transmittance through the atmosphere. As the satellite approaches overhead the transmittance of all wavelengths increases and the diffractive losses continue to decrease. This pushes the shorter wavelength key rates up as more and more of the downlink beam is captured by the receiver. At the most overhead point, the 785nm wavelength just barely surpasses the 830nm wavelength for maximum key rate.

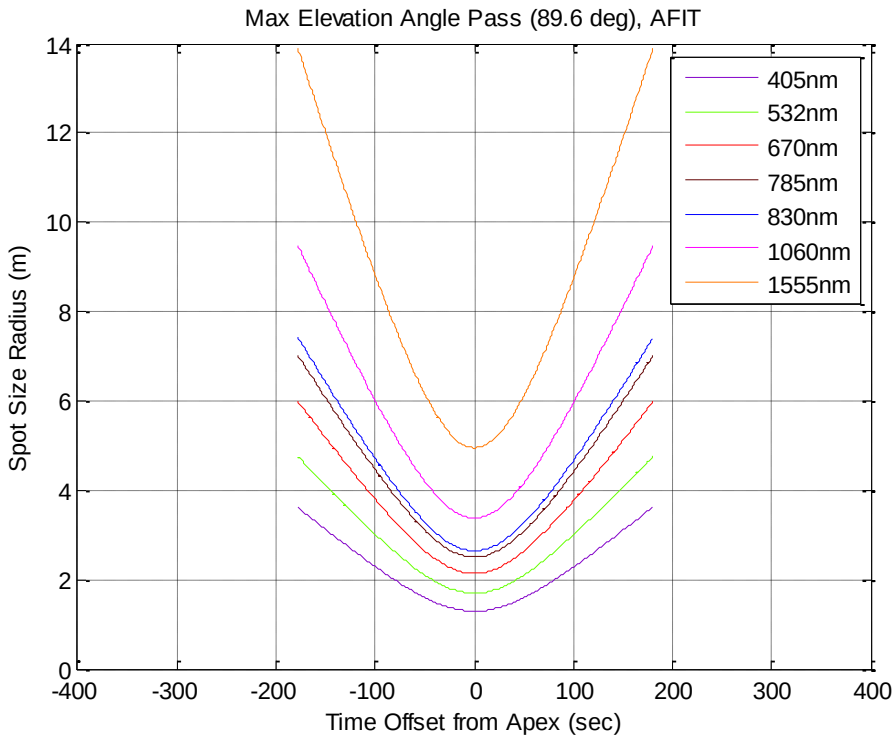


Figure 25: AFIT Spot Radius for Best Pass, 500km Sun-Synchronous Orbit

Figure 25 shows the radius of the spot size at the receiver. The spot size for any pass starts out at the same size and decreases as the satellite passes overhead. The smallest spot size is a function of the maximum elevation angle of the pass. Once the satellite is directly overhead the spot sizes are the smallest, relating to the increase in key rate as more of the energy in the beam is captured at the receiver.

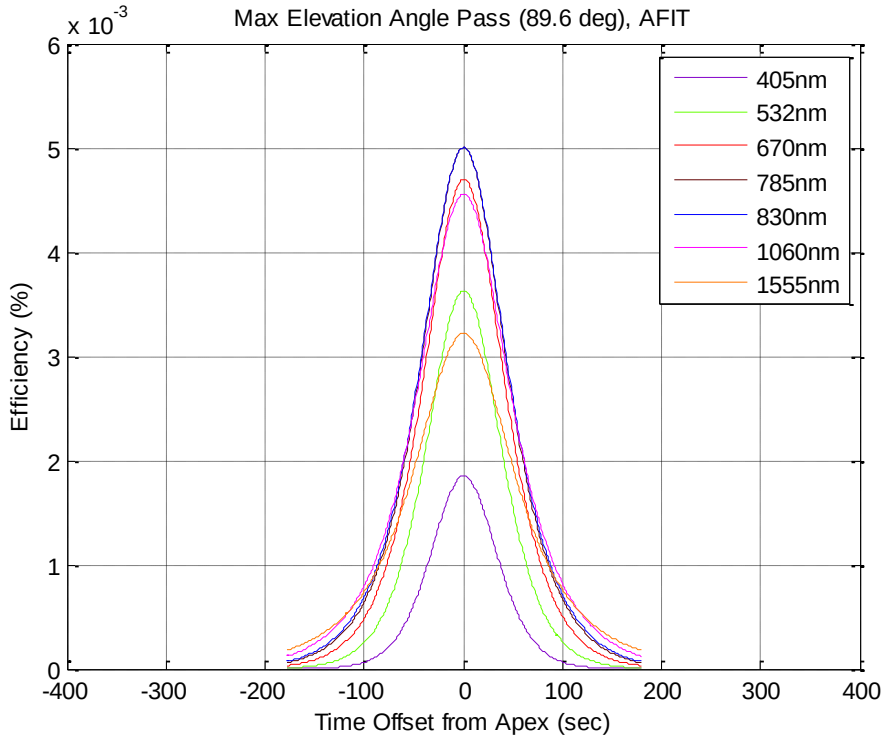


Figure 26: AFIT Efficiencies for Best Pass, 500km Sun-Synchronous Orbit

Figure 26 highlights a very important aspect of the QKD link. The link itself is highly inefficient. The large losses cannot be overcome by increasing the power in the beam, as that removes the security of QKD. The overall .001% efficiency indicates a high amount of loss from the transmitter to the receiver. The efficiency is driven by the losses in the receiving hardware, losses when the spot size is larger than the receiving telescope, losses due to absorption in the atmosphere and finally losses due to imperfections in the single photon source at the transmitter.

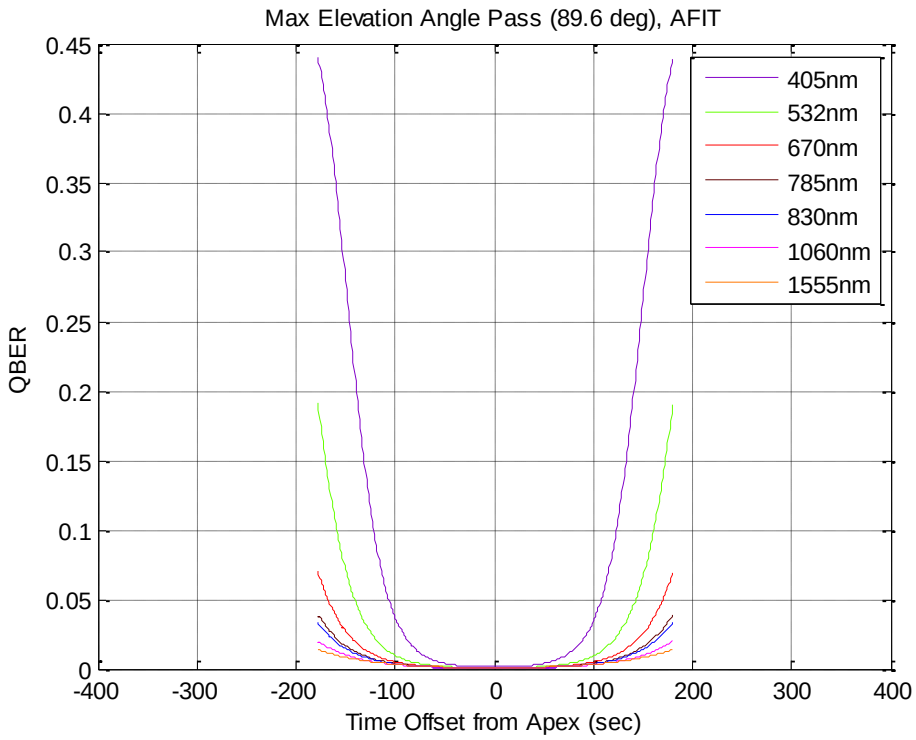


Figure 27: AFIT QBER for Best Pass, 500km Sun-Synchronous Orbit

Figure 27 shows the QBER as a function of time during the highest elevation angle pass. The scaling factor of the transmittance plays a larger role in the overall QBER than originally expected. At low elevation angles the low transmittance of short wavelengths decreases the total signal that arrives at the receiver. There is no lower bound on the QBER but all wavelengths approach values of 0.05% during the highest elevation angle of the pass. The 11% upper limit on QBER shows that 405nm and 532nm would not be usable for the entire pass, however all longer wavelengths would be usable during the entire pass.

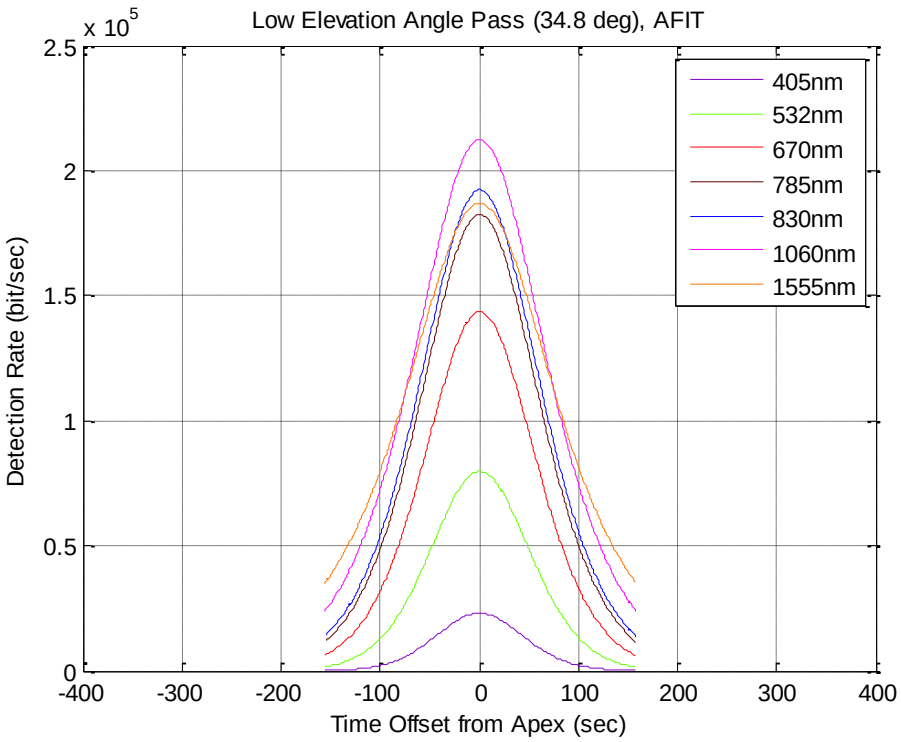


Figure 28: AFIT Detection Rate for 75% Percentile Pass, 500km Sun-Synchronous Orbit

The 75% percentile pass is now presented to provide a more realistic description of the satellite's performance throughout the year. This lower elevation angle pass corresponds to greater losses in the atmosphere, and transmittance becomes the dominant factor in performance by wavelength. The diffractive losses are still present, which causes the 1060nm wavelength to surpass the 1555nm wavelength in detection rate during the highest elevation angle of the pass. The low transmittance of the 405nm and 532nm wavelengths significantly decrease their performance compared to that of the 1060nm maximum bit rate. While the 1555nm wavelength performs better during the low elevation angles, the higher peak on the 1060nm wavelength allows for more raw key material to be delivered during the entire pass at a 1060nm wavelength than at the 1555nm wavelength.

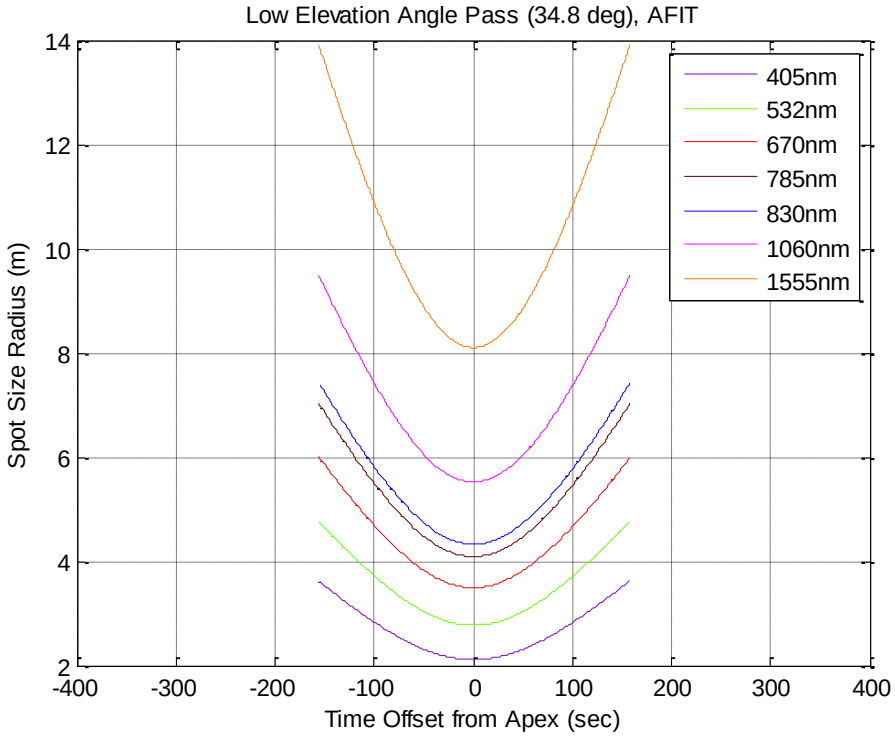


Figure 29: AFIT Spot Radius for 75% Percentile Pass, 500km Sun-Synchronous Orbit

Figure 29 shows the spot size radius for the 34.8 degree pass. The curves are shallower than the curves observed during the maximum elevation angle pass. This chart highlights that more diffraction is taking place during lower elevation angle passes, so there is more loss from the larger spot size arriving at the receiver, as compared to the maximum elevation angle case.

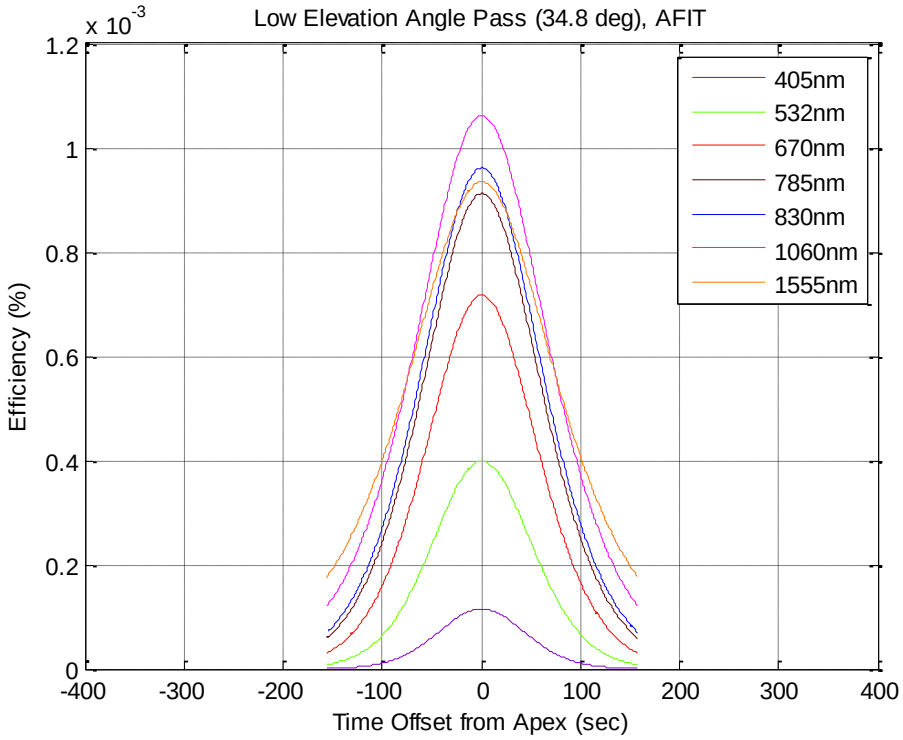


Figure 30: AFIT Efficiencies for 75% Percentile Pass, 500km Sun-Synchronous Orbit

Figure 30 presents the efficiencies for the multiple wavelengths during the 34.8 degree pass. This pass is even less efficient than the maximum elevation angle pass, due to the greater diffractive losses and absorption in the atmosphere associated with a lower elevation angle. The significant difference between the maximum elevation angle and the lower elevation angle pass is that the 1060nm wavelength now performs better than the 785nm wavelength. The 1060nm wavelength has a higher efficiency, for the entire duration of the link, than every wavelength except 1555nm. 1060nm again surpasses 1555nm for the middle of the pass.

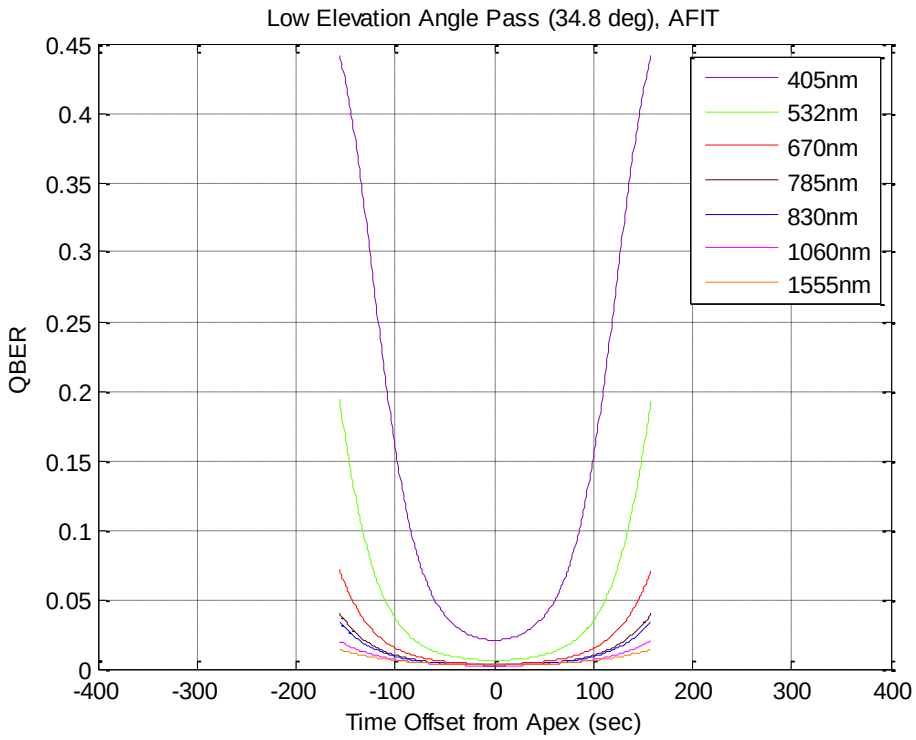


Figure 31: AFIT QBER for 75% Percentile Pass, 500km Sun-Synchronous Orbit

Figure 31 shows much higher QBER estimates for the duration of the pass, as compared to the 89.6 degree pass. This is explained by the increase in atmospheric losses for the lower elevation angle pass combined with a smaller fraction of received power collected by the receiver. Both 405nm and 532nm are only usable for a small portion of the pass, with both wavelengths being under 11% for a much smaller time than the maximum elevation angle pass, due to the shorter nature of a low elevation angle pass. All other wavelengths are still usable for the entire duration of the pass, with minimum QBERs of 0.3%±0.1%.

After looking at sample individual passes during the year it is insightful to look at the expected performance of the system for the entire duration of the year. One critical caveat to these values is that they don't account for limitations due to weather. This

means that the values presented are a conservative estimate of the system's maximum performance, given that every night of the year had clear sky conditions. Weather will further degrade the annual performance decreasing the total number of qubits that could be exchanged to generate secure keys.

Table 8: Year-long Performance Summary, 500km Sun-Synch Orbit

Annual	Avg Bit Rate (kbit/s)		Average QBER (%)		Total Bits (Gb)	
λ (nm)	AFIT	NPS	AFIT	NPS	AFIT	NPS
405	33.0	32.7	15.43	15.53	4.4	4.2
532	83.1	83.6	4.54	4.47	11.1	10.7
670	129.3	130.9	1.78	1.73	17.3	16.7
785	154.6	156.8	1.11	1.08	20.7	20.0
830	159.1	161.2	0.99	0.97	21.3	20.6
1060	169.7	171.6	0.69	0.68	22.7	21.9
1555	145.1	146.1	0.60	0.59	19.4	18.7

Table 8 presents the results of the study for the year-long duration, accounting for a seasonal change from summer transmittance profiles to winter profiles. The performance for each wavelength is presented in order to identify the best choice of wavelength for use with this particular orbit. The 1060nm wavelength generates the highest amount of raw key material due to its balance between diffractive losses and absorption in the atmosphere. AFIT is able to generate more raw key material than NPS because the transmittance for summer is higher at AFIT than at NPS. The winter transmittance drops for AFIT while staying relatively constants for NPS. This drop is not significantly lower than the NPS winter values. A similar study was performed for summer only conditions for Sun-synchronous orbits with orbital altitudes of 300km, 500km, 700km and 900km. The results are addressed in Appendix B. The main finding for differing orbit heights was that the majority of passes continued to be at low elevation

angles and 1060nm provided the greatest amount of raw key. As the altitude increases the ideal wavelength begins to shift toward 830nm however the altitude needs to increase above 900km before 830nm will provide better performance than 1060nm for a year-long Sun-synchronous orbit.

The 800M additional qubits exchanged at AFIT indicates that NPS is the limiting factor for the detection rates that can be leveraged for use with a one-time pad. One implementation issue that needs to be addressed in the building of a real system or an orbit optimization study is to balance the total bits passed between AFIT and NPS so that each ground site detects approximately the same number of qubits each pass. This would maximize the frequency of rekeying that could take place.

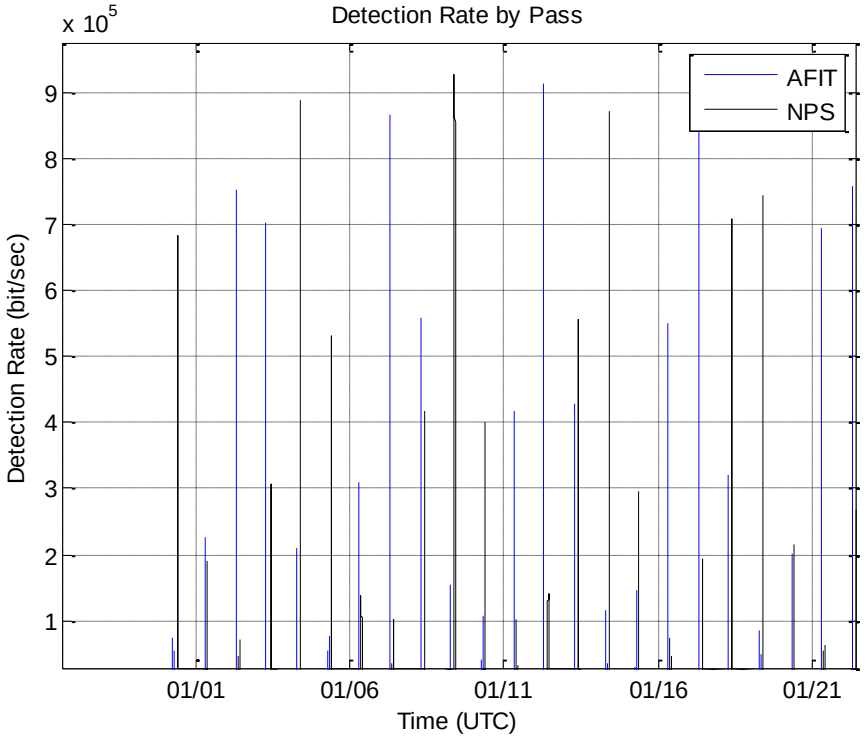


Figure 32: Detection Rate Comparison for First Three Weeks of Passes

Figure 32 shows the 1060nm detection rates for each pass during the start of the year. The very first pass highlights how a very small amount of key is generated at one site while a large amount of key is generated at the second site. The optimal orbit would balance these differences so that rekeying could be accomplished every night.

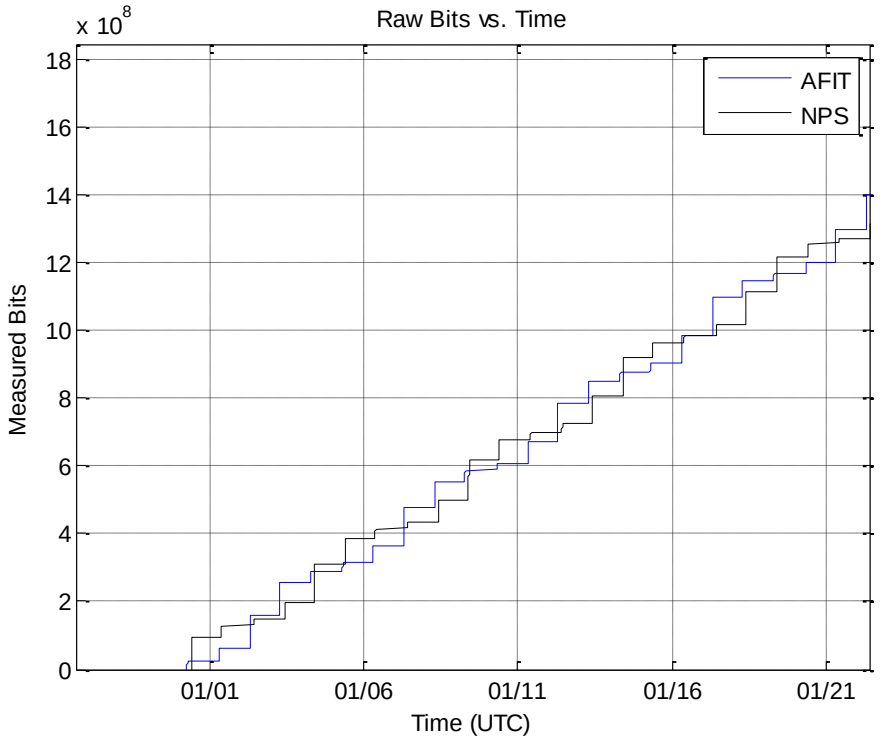


Figure 33: Total Detected Qubits for First Three Weeks of Passes

Figure 33 shows the integrated detection rates that determine the total number of qubits exchanged with each ground site. The optimal curve would be two identical step functions perfectly matching each other over time. In a real implementation this graph will drop back down to zero every time a secure key is exchanged to prevent excessive use of memory on the satellite, as well as to delete historical keys so that Eve could not obtain them. A similar study was performed for orbits at 300km, 700km and 900km altitudes. These results are presented with the year-long performance findings found in

Appendix B. The 700 km Sun-synchronous orbit resulted in the closest matching between key rates at AFIT and NPS.

Investigative Questions Answered

The factors that directly determine the detection rate of a LEO QKD space-based system are pulse rate, spot size, transmittance, wavelength, the transmitting optical hardware and the receiving optical hardware. The pulse rate directly scales the detection rate and should always be maximized. The spot size at the receiver is a function of the transmitting optical configuration, the wavelength selected and the distance between the transmitter and receiver. The spot size should always be minimized to focus the maximum amount of the energy in the optical link on the receiver. The transmittance is a function of both wavelength and elevation angle and varies as a function of elevation angle. Larger diameter transmitting optics can be used to reduce the total diffraction in the link to better focus the energy at the receiver. The receiving telescope's diameter determines how much of the beam and how much background noise is collected. The receiving telescope introduces losses in the link and further losses are introduced at the photon detector. A larger receiving telescope and higher detector efficiency will reduce losses in the link realizing higher detection rates.

For a given hardware configuration, elevation angle and range define the atmospheric and diffractive losses that limit the detection rate for each wavelength. Different orbits result in different combinations of loss and in view times which define the trade space used to optimize orbit selection. The goal of orbit optimization is to maximize the detection rate, maximize the in view time and minimize the channel loss.

The wavelength that provides the least loss over the entire collection of passes results in the highest average detection rate.

For the specific case studied the 1060nm wavelength provided the highest average detection rate. The 1060nm wavelength provides the highest average detection rate because the majority of satellite passes occur at these low elevation angles where the atmospheric loss due to transmittance exceeds 3dB for wavelengths longer than 1060nm. At these elevation angles the total losses for 1555nm are larger than the total losses for 1060nm due to the greater diffraction experienced by a 1555nm wavelength. The modeled scenario uses 50% detector efficiencies, 200 million pulses per second, 50% hardware losses in optical hardware and results in average key rates on the order of 170kbit/s.

Summary

This chapter has presented the model validation and the results for a modeled QKD satellite acting as a trusted node between AFIT and NPS. This model lines up well with other sources from academia and should be incorporated into the existing qkdX framework at AFIT. The peak performance of a real-world QKD satellite link for a 500km orbit is obtained by a 785nm wavelength on the maximum elevation angle pass. The maximum amount of qubits detected would be the result of a 1060nm wavelength link due to the amount of time the satellite spends at low elevation angles relative to both ground stations. The Sun-synchronous orbit is necessary to reduce background light that would increase the error rate, however it needs to be optimized to generate key at both ground sites in even steps to maximize the frequency of rekeying. This model can now be

used to further study satellite QKD implementations and develop the technical requirements to build a real system.

V. Conclusions and Recommendations

Chapter Overview

This chapter presents the conclusions of the research. It highlights the main ideas from the thesis and summarizes the importance of the research accomplished. The answers to the research questions are reiterated and the significance of the work is highlighted. Important lessons learned are presented and future areas of research are recommended.

Conclusions of Research

The main highlights from this thesis are: both diffraction and transmission vary as a function of elevation angle for satellite optical links, the optimal wavelength for satellite QKD depends on the scenario it is being used for and lastly the orbit parameters need to be optimized in order to deliver key evenly to maximize efficient use of the system at multiple ground sites.

Loss from diffraction is directly related to both the distance from the transmitter to the receiver and the optical configuration used. As expected for a given set of optics, the spot size at the receiver continues to increase in size as the transmitter moves away from the receiver and decrease in size as the transmitter approaches the receiver. This is no surprise, however for space-based QKD the distance between the transmitter and receiver varies as a function of elevation angle from the horizon which impacts diffraction. The distance is largest when the satellite comes into view, decreases until the satellite reaches the apex of the pass, then increases until out of view. The diffraction loss is constantly changing during this elevation angle sweep, and is smallest at the apex of

the pass. The transmittance of the atmosphere is a function of wavelength and the length of atmosphere the link passes through. Similar to diffraction, the length of the beam passing through the atmosphere starts large, reaches a minimum at apex and then increases until the satellite is out of sight. The minimum loss for each wavelength occurs at zenith but this does not identify the best wavelength to use for a given scenario. The best wavelength for a given scenario depends on the elevation angle of the majority of passes. The experimental scenario resulted in the majority of orbital passes occurring at low elevation angles rather than passing directly overhead. The wavelength that performed better at low elevation angles, 1060nm, outperformed the 785nm wavelength in terms of total qubits exchanged throughout the year. This performance could have been increased with a different orbit selection, but the focus of this research was to develop and validate the model. An exhaustive orbit optimization study should now be performed.

The orbit and ground site selection drives the design trade space for a satellite implementing QKD. A higher orbit results in more loss due to diffraction driving the optimal wavelength shorter and shorter. For the given ground sites, low Earth Sun-synchronous orbits from 300km to 900km are not sufficiently high in altitude to drive the optimal wavelength away from 1060nm. LEO satellites spend more time transmitting through additional atmosphere. This drives the optimal wavelength towards longer wavelengths, due to the higher atmospheric transmittance of longer wavelengths. The ground site selection affects the nightly elevation angle and the total qubits exchanged.

For a Sun-synchronous orbit the satellite passes the selected ground sites each night. The amount of time the satellite spends in view is not always evenly distributed between both ground sites. This means that the ground sites do not exchange the same

number of qubits with the satellite. The maximum frequency of re-keying for space-based QKD key generation occurs when the two ground sites receive the same number of qubits each night. Matching qubit exchange allows encrypted communication to be passed each day, in place of one ground site waiting while the other ground site receives additional passes to increase the amount of raw key received.

Significance of Research

This research has developed and validated an analytical satellite QKD model. The model provides the functionality needed for inclusion in the existing qkdX framework. This research has also provided the building blocks necessary to identify the optimal Satellite QKD orbit and begin developing technical requirements for a real-world system.

The creation of the model is significant because it expands the capability of AFIT's existing framework. Other models existed in academia, but the code developed was not available to the AFIT QKD research team. Without source code it was not possible to recreate the results of other academic studies. The development of the model and its ability to recreate the results of other studies augments the current capability of the qkdX framework. After integration, the model will also be able to leverage the functionality of the existing framework in order to provide statistically significant results for discrete event simulations. This meets the need of the research sponsor to address space-based QKD scenario's without a revolutionary change to the existing software or licensing concerns.

The need to optimize the orbit is significant because previous work in academia has looked at the expected performance for a single ground site. The incorporation of

multiple ground sites identifies additional complexity that must be addressed for increased fidelity of future modeled scenarios. This additional complexity has the potential to drive orbit selection away from the previously pursued method of minimizing background noise. The new optimal orbit may be a balance between increased background light, varying time of night passes and more directly overhead passes to increase the key rates from the space-based platform. This hypothetical optimal orbit would provide more exchanged key material than the studied scenario even with additional background light and worse atmospheric conditions. Once the optimal orbit is identified for a given scenario the modeled technical requirements (i.e. pointing error, wavelength and system efficiencies) can be passed to the designer to begin identifying the technical requirements of the real-world system.

Lessons Learned

There were two main lessons learned during the development of this thesis that were not the expected result prior to beginning the research effort. These included the utility of LEEDR and the role receiving hardware plays in the quality of the link.

The incorporation of LEEDR provided additional fidelity to the overall model. The comparison to Specht showed that the amount of error introduced by not including LEEDR (Specht's approach) is comparable to the amount of error introduced by using a slant range approximation for pointing offset (approach used in this thesis). A better model would incorporate both the variable transmittance and the refracted path offset, which would result in even narrower pass curves than those shown in Figure 21. The true benefit of incorporating LEEDR is the ability to integrate realistic weather effects into the

simulation. Transmittance profiles can be developed that reflect the cloud cover or fog at a given ground site and studies can be performed to determine whether there is a possibility of performing space-based QKD with weather effects included.

Originally the efficiencies of hardware were not intended to be modeled. After initial development it became clear that the additional losses due to hardware inefficiencies created a significant source of loss for the overall system, reducing the realizable key rates by two orders of magnitude. Further, the dark count of the receiving hardware had more effect on the total QBER than the Doppler shift or turbulence in the atmosphere. The Doppler shift is entirely encompassed in the passband of normal hardware. Turbulence less than $C_n^2 = 10^{-14}$ does not significantly affect the total error rate of the BB84 QKD link. Instead, the background noise and dark count contribute significantly to the number of errors in the link. This further highlights the impact of receiving hardware in a space-based QKD link.

Recommendations for Future Work

Future work should combine the Specht and Denton approaches and then integrate them into qkdX. First, the functionality of this model should be combined with the Specht implementation in order to capture a higher level of fidelity than each model provides. Second the combined model should be incorporated into the existing qkdX framework. Table 5 highlights the differences between the developed model and Specht's approach. The single user input for wavelength and number of refracted layers should be included from the Specht approach, as well as the calculated refracted path and the offset based on this calculation. The QBER estimates and the variable atmospheric

transmittance should be used from the model, as well as the MPN estimate to capture the true number of photons in the link. Incorporating the combined approach into the existing qkdX framework will expand its current capability. This will provide the functionality to implement a space-based channel in the qkdX framework and study additional research problems identified by the research sponsor.

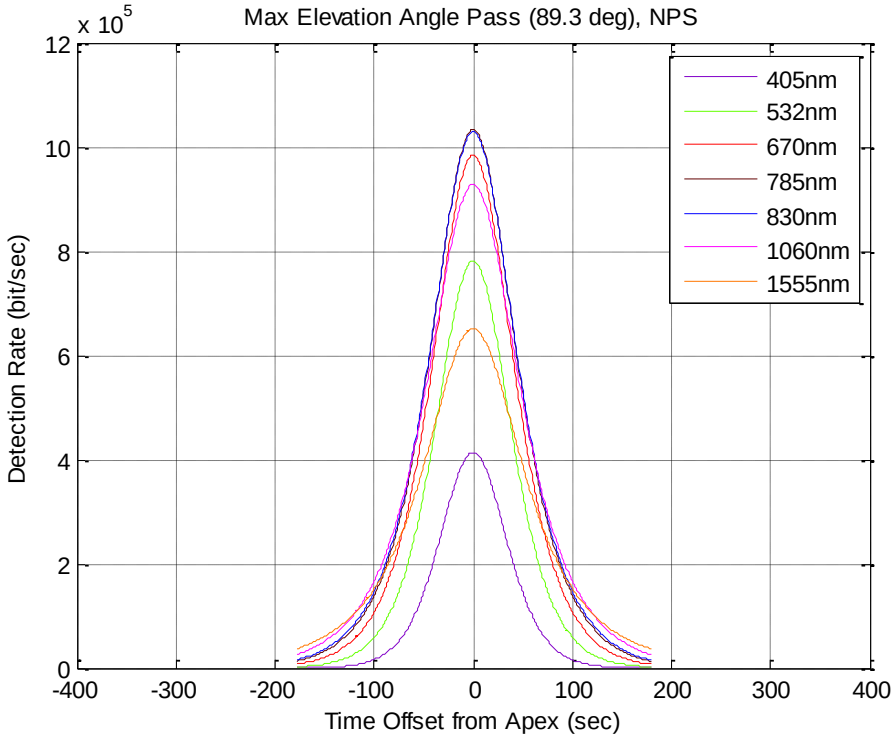
Once the two approaches are combined, an orbit optimization study should be performed. The goal of an optimization study is to identify the orbit that balances raw key generation at multiple ground sites while providing the highest usable detection rates at those ground sites. User defined TLEs or existing satellites should be leveraged in order to encompass the entire trade space of altitudes and inclinations. The study should not be limited to just LEO satellites, however the results of the 300-900km altitude study indicates that the closer the satellite is to the Earth the higher detection rates result in a larger amount of raw key material for secret key generation.

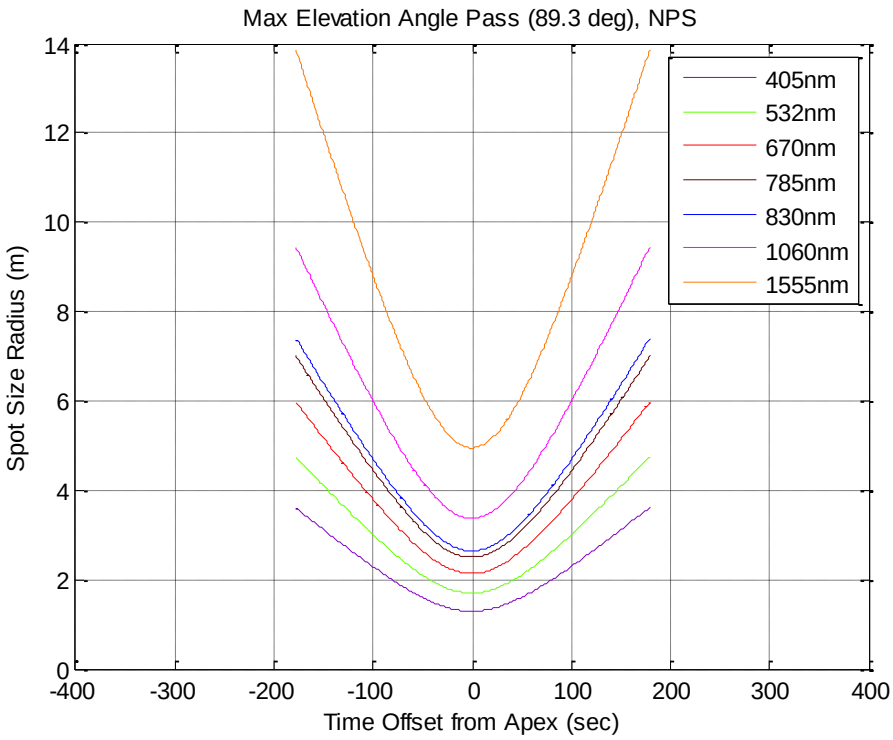
Summary

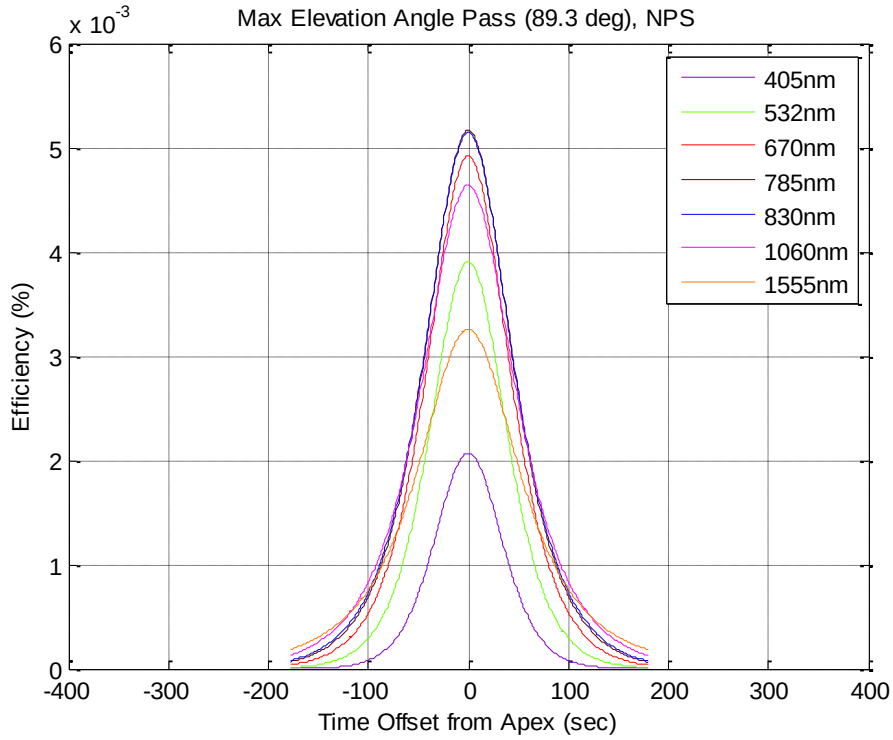
As CubeSat hardware continues to decrease in cost and improve in performance, a QKD technology demonstration is expected to be completed in the next few years. The model developed for this thesis accurately characterizes the expected performance of such a system and provides designers with the technical insight needed to define the technical requirements of such a system. The developed model should be leveraged to identify the best orbit and wavelength for demonstration of space-based QKD.

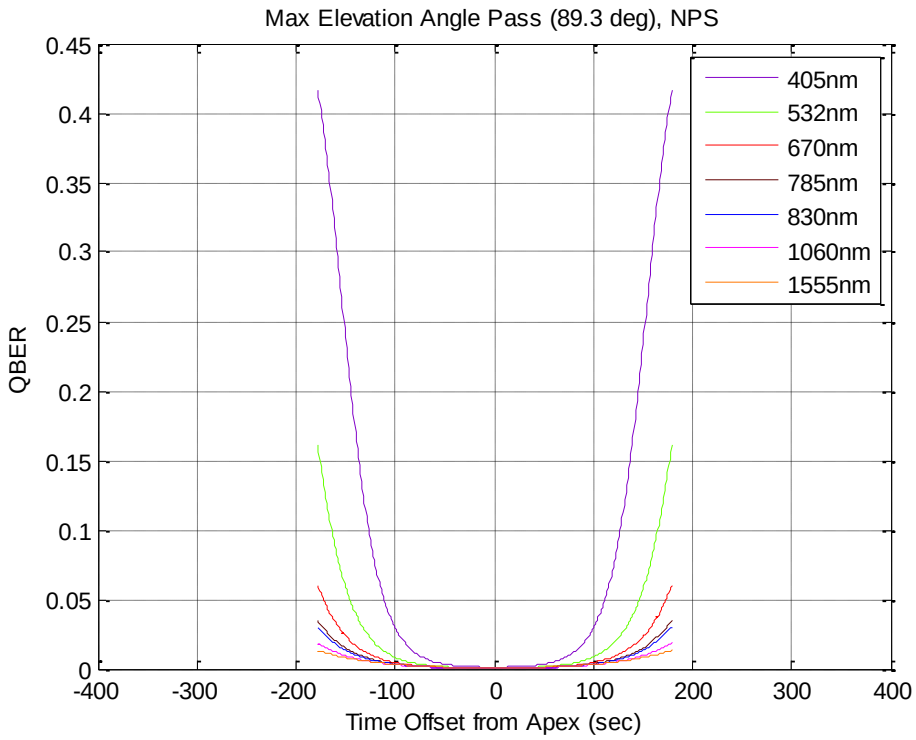
Appendix A: NPS High and Low Elevation Pass Results

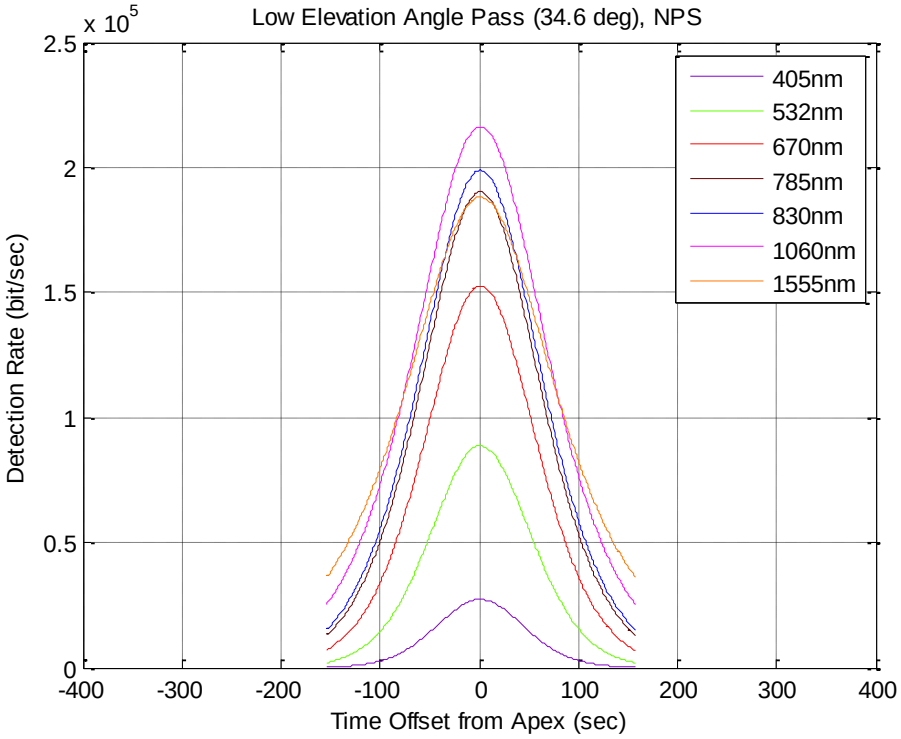
This Appendix presents the results of the high and low elevation angle passes over the Naval Postgraduate School. Due to the similarity of the passes to those over the Air Force Institute of Technology these charts were not presented in the body of the thesis. The key rates presented were used in the calculations shown in Table 8.

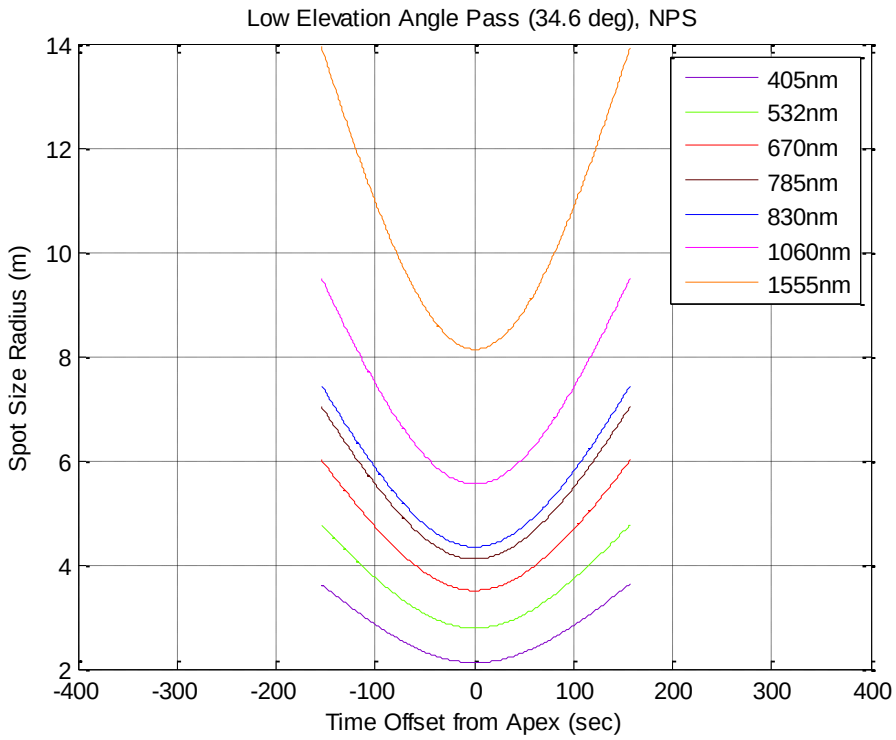


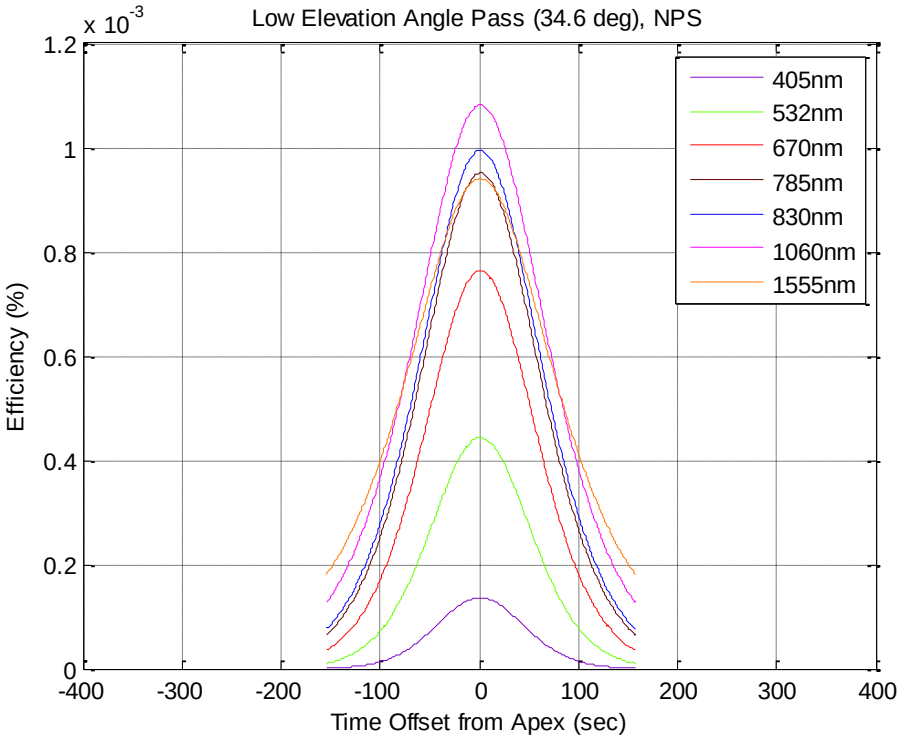

Max Elevation Angle Pass (89.3 deg), NPS
Spot Size Radius (m)
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
0
2
4
6
8
10
12
14
-400
-300
-200
-100
0
100
200
300
400

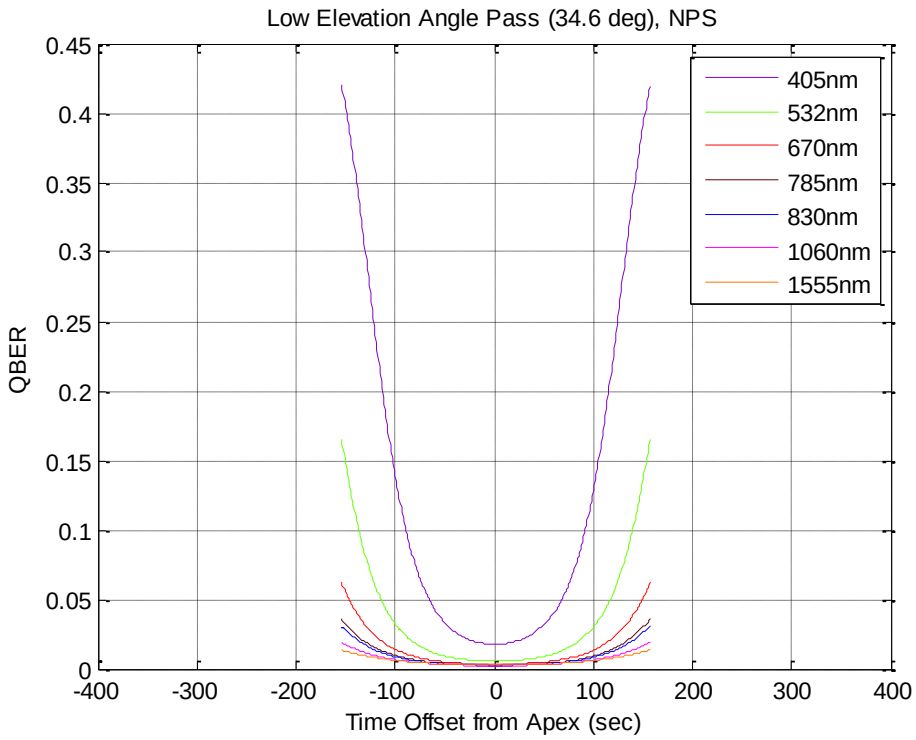

x 10-3
Max Elevation Angle Pass (89.3 deg), NPS
Efficiency (%)
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
0
1
2
3
4
5
6
-400
-300
-200
-100
0
100
200
300
400


Max Elevation Angle Pass (89.3 deg), NPS
QBER
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
-400
-300
-200
-100
0
100
200
300
400


Low Elevation Angle Pass (34.6 deg), NPS
x 10^5
Detection Rate (bit/sec)
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
2.5
2
1.5
1
0.5
0
-400
-300
-200
-100
0
100
200
300
400


Low Elevation Angle Pass (34.6 deg), NPS
Spot Size Radius (m)
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
14
12
10
8
6
4
2
-400
-300
-200
-100
0
100
200
300
400


x 10-3
Low Elevation Angle Pass (34.6 deg), NPS
Efficiency (%)
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
1.2
1
0.8
0.6
0.4
0.2
0
-400
-300
-200
-100
0
100
200
300
400

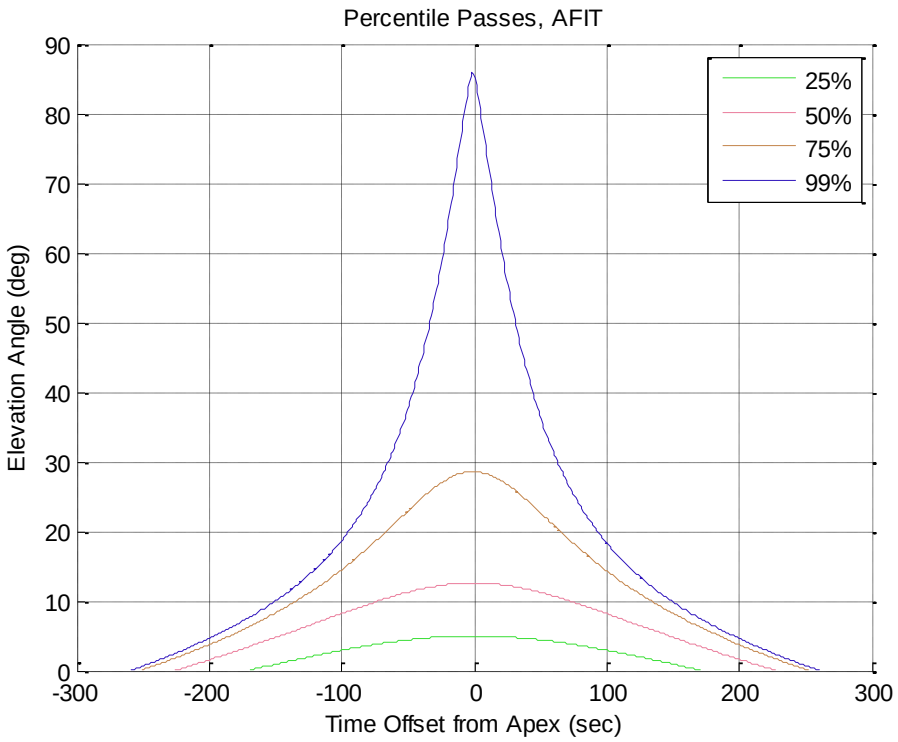

Low Elevation Angle Pass (34.6 deg), NPS
QBER
Time Offset from Apex (sec)
405nm
532nm
670nm
785nm
830nm
1060nm
1555nm
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
-400
-300
-200
-100
0
100
200
300
400

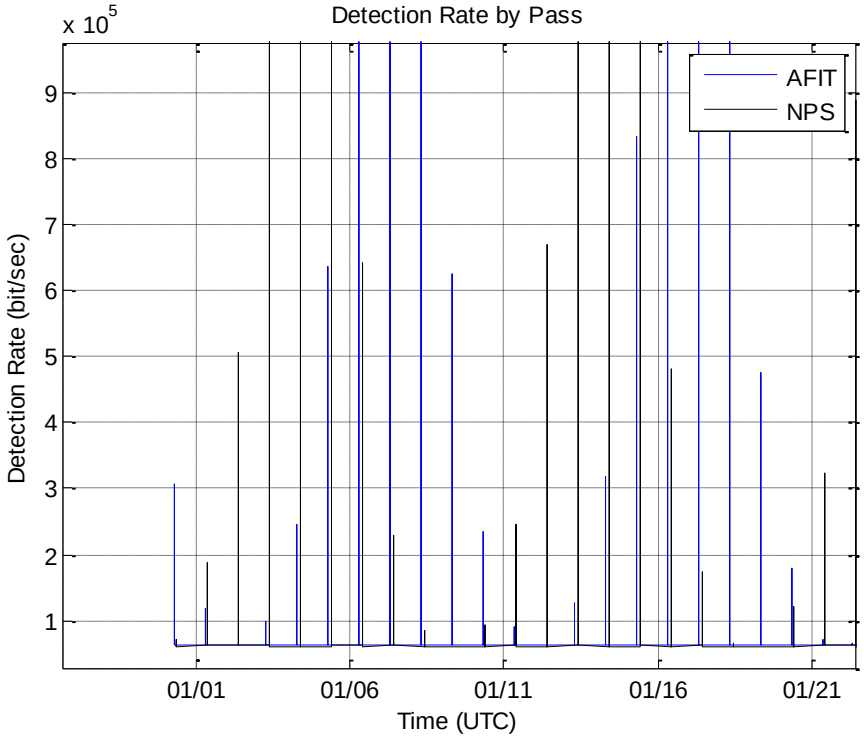
Appendix B: Orbital Study by Altitude

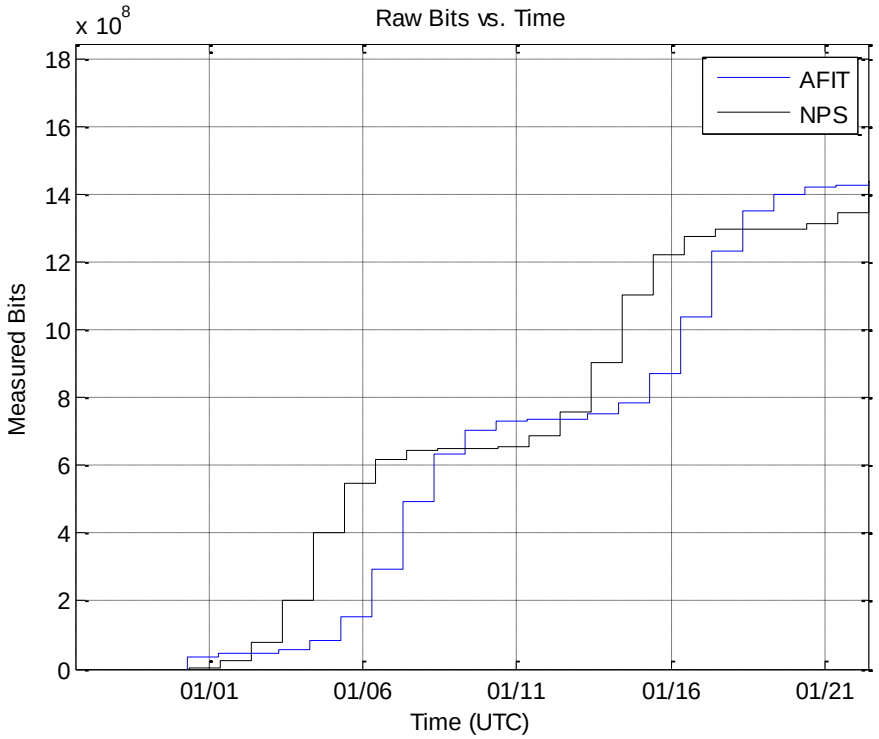
This Appendix presents the results of the year-long simulation for a Sun-synchronous orbit with a right-ascension of the angular node at 130 degrees. The inclination was calculated based on the selected orbital altitude, accounting for J2 perturbation effects and the orbit was propagated with SGP4 for a full year. The Sun-synchronous orbit RAAN selection ensured nighttime passes that stayed within the midnight to 3am window for the developed atmospheric profiles. The results in this appendix do not account for a seasonal variation as the desired study was to determine how wavelength performance changes based only on altitude changes.

300 km Sun-Synchronous Orbit

Alt. 300km	Avg Rate (kbit/sec)		Avg Error (%)		Total Key (Gbit)	
λ (nm)	AFIT	NPS	AFIT	NPS	AFIT	NPS
405	86.9	74.7	9.81	11.85	5.3	4.4
532	207.4	191.1	2.07	2.45	12.7	11.2
670	318.8	307.2	0.76	0.83	19.6	18.1
785	380.1	373.4	0.47	0.50	23.3	22.0
830	387.9	382.8	0.43	0.45	23.8	22.5
1060	416.8	415.5	0.30	0.30	25.6	24.4
1555	353.5	353.4	0.26	0.26	21.7	20.8

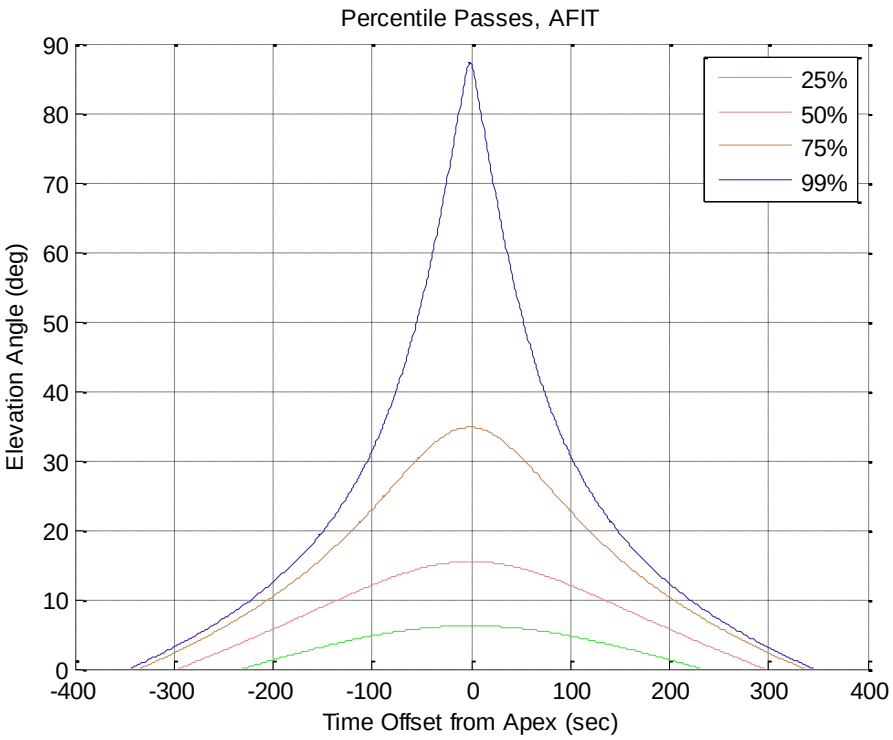

Percentile Passes, AFIT
25%
50%
75%
99%
Elevation Angle (deg)
Time Offset from Apex (sec)
0
10
20
30
40
50
60
70
80
90
-300
-200
-100
0
100
200
300

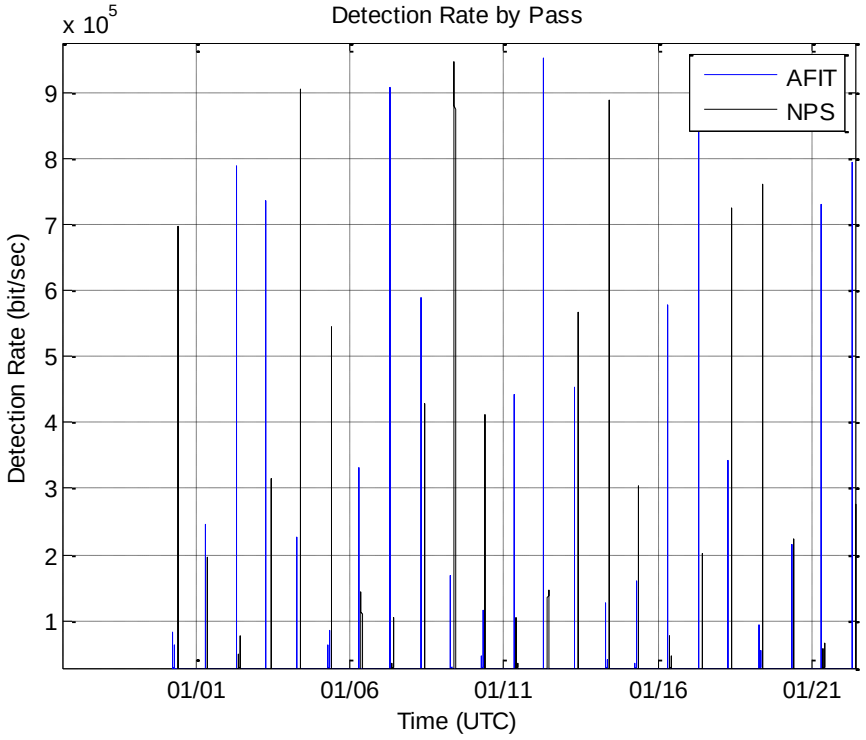

Detection Rate by Pass
x 10^5
AFIT
NPS
Detection Rate (bit/sec)
Time (UTC)
1
2
3
4
5
6
7
8
9
01/01
01/06
01/11
01/16
01/21

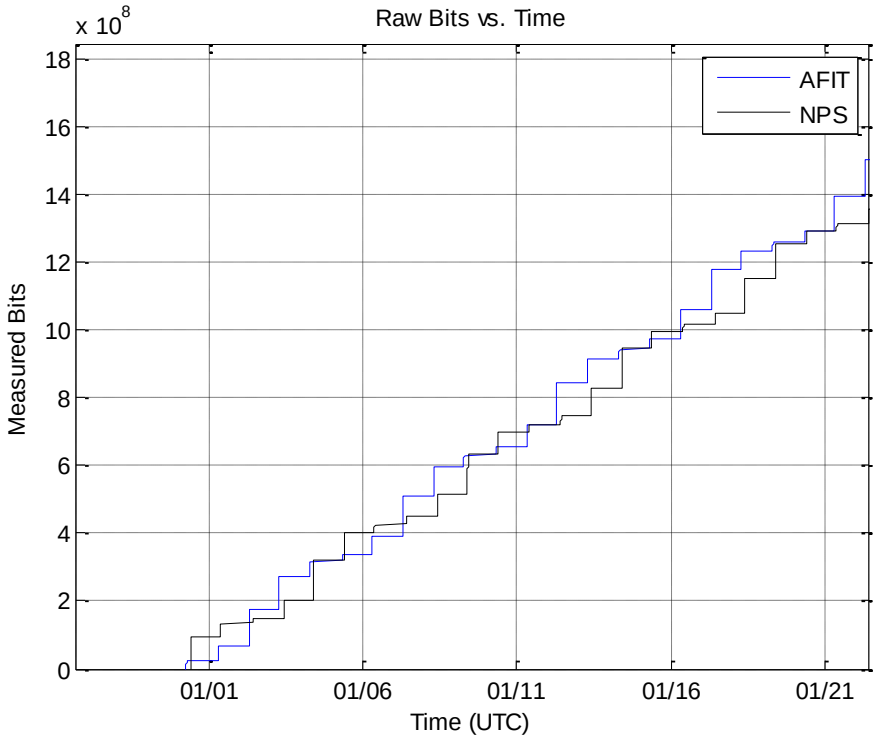


500 km Sun-Synchronous Orbit

Alt. 500km	Avg Rate (kbit/sec)		Avg Error (%)		Total Key (Gbit)	
λ (nm)	AFIT	NPS	AFIT	NPS	AFIT	NPS
405	36.6	31.2	13.99	16.13	4.9	4.0
532	90.2	82.5	3.92	4.57	12.1	10.5
670	137.8	132.0	1.57	1.71	18.5	16.9
785	162.9	159.0	1.01	1.06	21.8	20.3
830	165.8	162.6	0.92	0.96	22.2	20.8
1060	175.8	174.2	0.65	0.66	23.6	22.3
1555	146.8	146.1	0.59	0.59	19.7	18.7

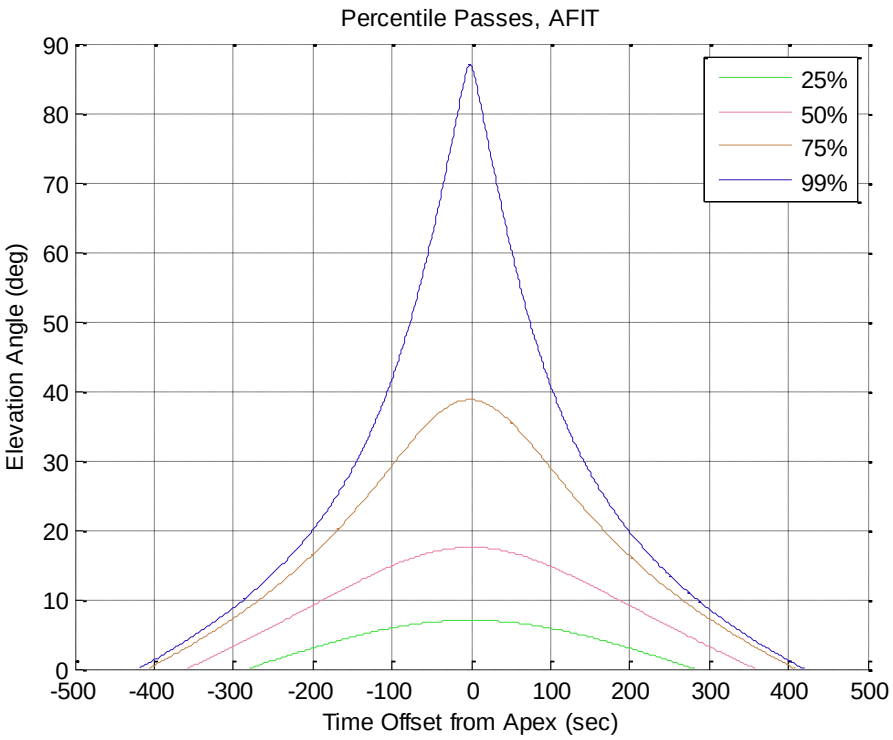

Percentile Passes, AFIT
25%
50%
75%
99%
Elevation Angle (deg)
Time Offset from Apex (sec)
0
10
20
30
40
50
60
70
80
90
-400
-300
-200
-100
0
100
200
300
400

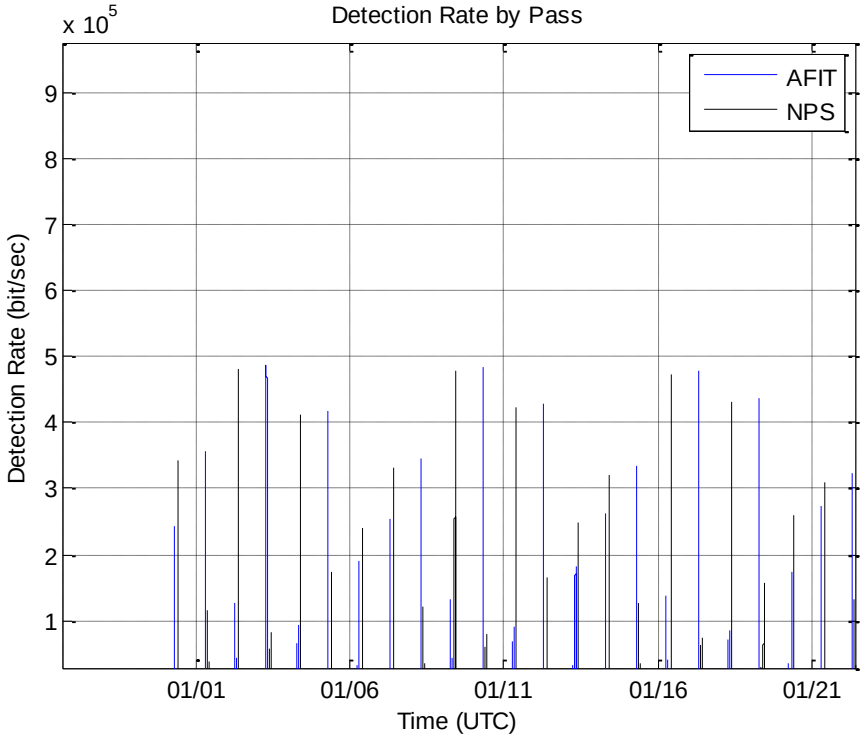

Detection Rate by Pass
x 10^5
AFIT
NPS
Detection Rate (bit/sec)
Time (UTC)
1
2
3
4
5
6
7
8
9
01/01
01/06
01/11
01/16
01/21

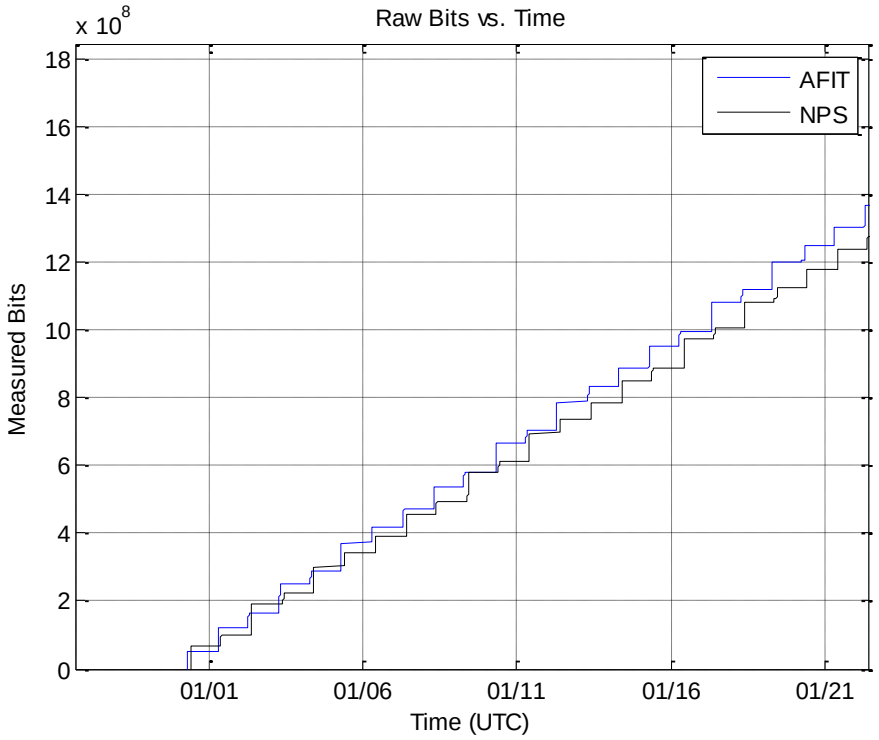


700 km Sun-Synchronous Orbit

Alt. 700km	Avg Rate (kbit/sec)		Avg Error (%)		Total Key (Gbit)	
λ (nm)	AFIT	NPS	AFIT	NPS	AFIT	NPS
405	21.0	17.8	16.80	18.89	4.5	3.7
532	52.2	47.6	5.70	6.53	11.3	9.8
670	79.5	75.8	2.47	2.67	17.2	15.7
785	93.5	91.0	1.62	1.69	20.3	18.8
830	95.0	92.9	1.49	1.55	20.6	19.2
1060	100.2	99.0	1.07	1.09	21.7	20.5
1555	83.0	82.4	0.99	1.00	18.0	17.0

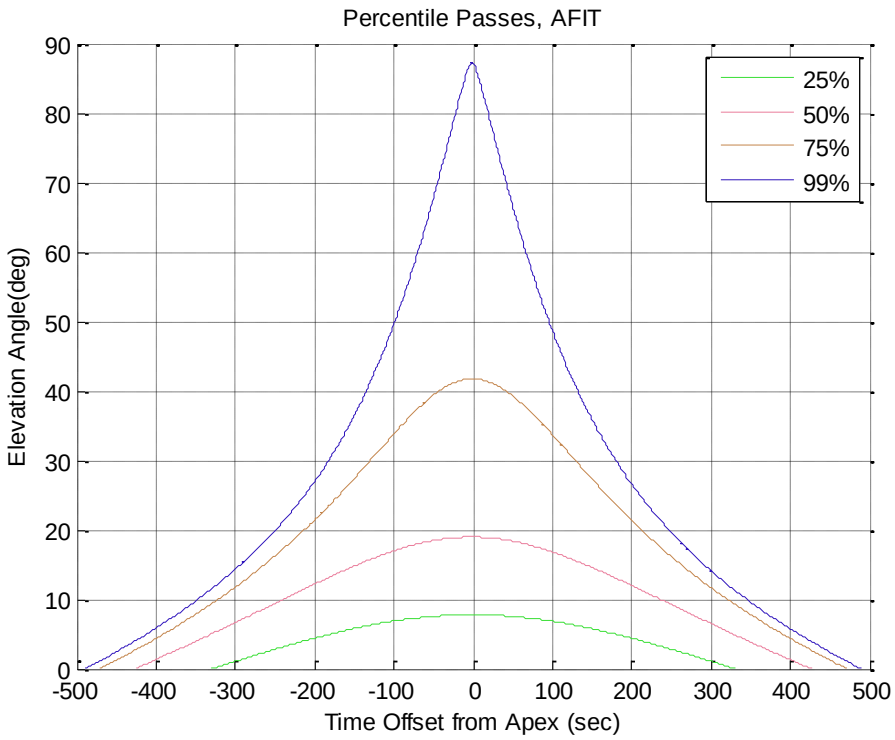

Percentile Passes, AFIT
25%
50%
75%
99%
Elevation Angle (deg)
Time Offset from Apex (sec)
0
10
20
30
40
50
60
70
80
90
-500
-400
-300
-200
-100
0
100
200
300
400
500

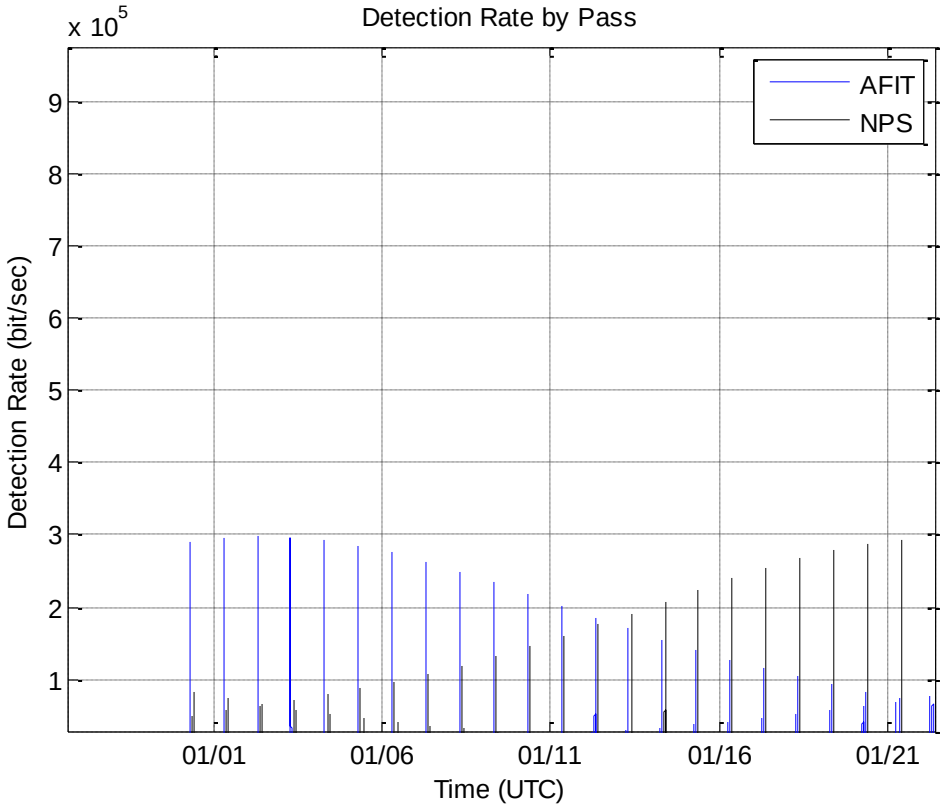

Detection Rate by Pass
x 10^5
AFIT
NPS
Detection Rate (bit/sec)
Time (UTC)
1
2
3
4
5
6
7
8
9
01/01
01/06
01/11
01/16
01/21

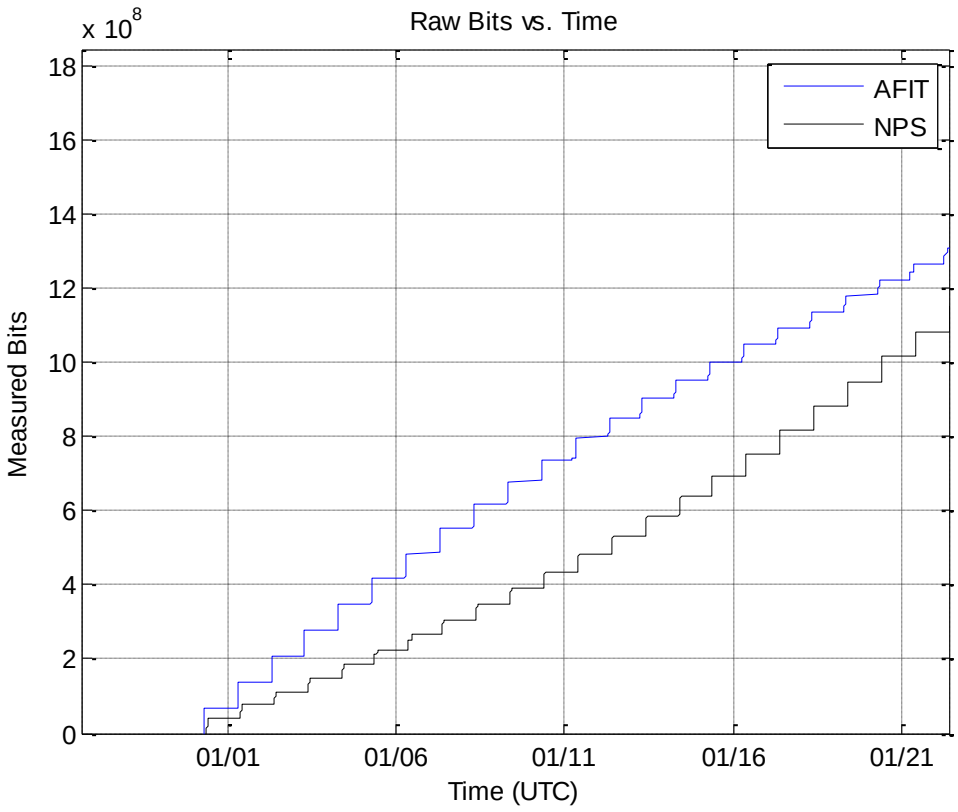


900 km Sun-Synchronous Orbit

Alt. 900km	Avg Rate (kbit/sec)		Avg Error (%)		Total Key (Gbit)	
λ (nm)	AFIT	NPS	AFIT	NPS	AFIT	NPS
405	14.2	11.5	18.86	20.97	4.3	3.4
532	35.2	30.9	7.33	8.30	10.7	9.1
670	53.3	49.3	3.38	3.65	16.3	14.5
785	62.5	59.2	2.27	2.38	19.1	17.3
830	63.4	60.4	2.10	2.18	19.3	17.7
1060	66.5	64.3	1.53	1.57	20.3	18.8
1555	54.8	53.5	1.43	1.45	16.7	15.7

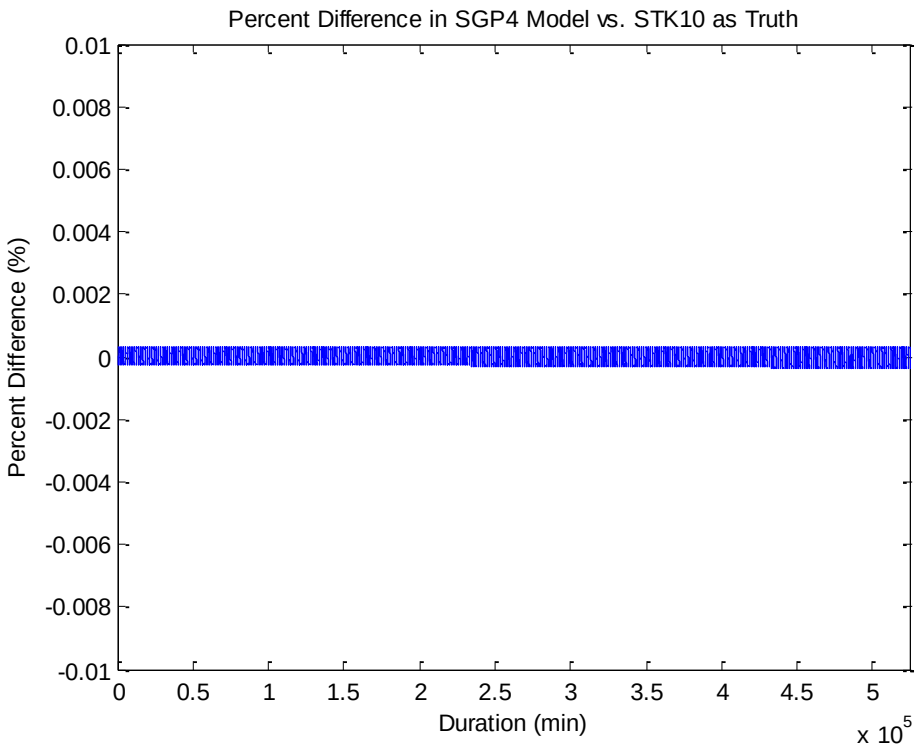

Percentile Passes, AFIT
Elevation Angle(deg)
Time Offset from Apex (sec)
25%
50%
75%
99%
90
80
70
60
50
40
30
20
10
0
-500
-400
-300
-200
-100
0
100
200
300
400
500


Detection Rate by Pass
x 10^5
Detection Rate (bit/sec)
Time (UTC)
AFIT
NPS
9
8
7
6
5
4
3
2
1
01/01
01/06
01/11
01/16
01/21


Raw Bits vs. Time
x 10^8
Measured Bits
Time (UTC)
AFIT
NPS
0
2
4
6
8
10
12
14
16
18
01/01
01/06
01/11
01/16
01/21

Appendix C: SGP4 Implementation Verification

In order to verify the accuracy of the SGP4 propagator implemented, Systems Toolkit 10© (STK) was used as a comparison. The same two line element set was propagated for a year within STK and the developed model at a one minute interval. The outputs for ECI position vectors were then compared for differences. As shown in the figure below the normalized difference with STK stays smaller than .001% for the entire year. Towards the end of the year the difference does begin to increase in magnitude. There is a cyclical nature to the difference, and this can be attributed to a lack of insight into the specific routines used by STK. Slight differences in math calculations across software platforms can attribute to rounding errors, and additional optimization in the STK code likely account for the overall difference.



The output elevation angles for NPS and AFIT ground sites were also compared between the orbital simulator and STK. This comparison is how the incorrect leap second implementation of the *rv2razel* algorithm was originally identified. Once the error was corrected, the elevation angles matched the STK values used as truth. The fractional degree differences are due to the differences in the defined position vectors.

The matching values between STK10 and the model developed provide sufficient orbital accuracy to develop insight into the problem of study. Due to the similar positions, velocities and elevation angles output as compared to the industry standard software, the orbital modeling component is considered verified.

Bibliography

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[2] D. Stuck, N. Walenta, F. Vannel, R. T. Thew and N. Gisin, "High Rate, Long Distance Quantum Key Distribution Over 250km of Ultra Low Loss Fibres," *New Journal of Physics,* vol. 11, no. 075003, p. 9, 2009.

[3] L. Mailloux and M. Grimaila, "Quantum Key Distribution Simulation Framework (qkdX)," Air Force Institute of Technology, Dayton, 2015.

[4] H. Evans, J. Lange and J. Schmitz, The Pheonmenology of Intelligence-focused Remote Sensing Vol 1, New York: Riverside Research, 2014.

[5] J. Schmidt, "LEEDR User Guide Version 4.0, Patch #16," Air Force Institute of Technology, Wright Patterson AFB, 2015.

[6] J. A. Specht, "Pointing Analysis and Design Drivers for Low Earth Orbit Satellite Quantum Key Distribution," Air Force Institute of Technology, Dayton, 2016.

[7] J. W. Strohbehn, Topics In Applied Physics vol. 25: Laser Beam Propagation in the Atmosphere, Berlin: Springer-Verlag Berlin Heidelberg, 1978.

[8] L. C. K. C. Walli, *Fundamental of Advanced Technical Intelligence Collection,* Dayton: AFIT, 2010.

[9] J. H. Shapiro, "Scintillation has Minimal Impact on Far-Field Bennett-Brassard 1984 Protocol Qunatum Key Distribution," *Physical Review A,* vol. 84, no. 3, p. 6, 2011.

[10] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgings, B. Helou, C. Erven, H. Hubel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflammes and T. Jennewein, "A Comprehesive Design and Performance Analysis of Low Earth Orbit Satellite Quantum Communication," *New Journal of Physics,* vol. 15, no. 023006, p. 25,

2013.

[11] L. V. van De Wiel Lydersen, Security of QKD-systems with Detector Efficiency Mismatch, Trondheim: Norwegian University of Science and Technology, 2008.

[12] M. Nielson and I. Chuang, Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, 2010.

[13] M. Nielson and I. Chuang, Quantum Computation and Quantum Information, Cambridge: Camrbidge University Press, 2001.

[14] D. A. Vallado, "Fundamentals of Astrodynamics and Applications," Madrid, 2010.

[15] J. Subirana, J. Zomoza and M. Hranandez-Pajares, "Conventional Celestial Reference System," European Space Agency, 23 February 2012. [Online]. Available: http://www.navipedia.net/index.php/Conventional_Celestial_Reference_System. [Accessed 9 November 2015].

[16] L. C. Andrews and R. L. Phillips, Laser Beam Propagation through Random Media, Washington: The International Society for Optical Engineering, 2005.

[17] M. Gruneisen, *Starfire Optical Range Technical Interchange Meeting,* Albuquerque, 2015.

[18] Newport Corporation, "Gaussian Beam Optics," Newport Coporation, 1996. [Online]. Available: http://www.newport.com/Gaussian-Beam-Optics/144899/1033/content.aspx. [Accessed 13 10 2015].

[19] Spectral Sciences Inc., "MODTRAN5: About Modtran," Spectral Sciences Inc., 2012. [Online]. Available: http://modtran5.com/about/index.html. [Accessed 12 February 2016].

[20] J. G. Rarity, P. R. Tapster, P. M. Gorman and P. Knight, "Ground to Satellite Secure Key Exchange Using Quantum Cryptography," *New Journal of Physics,* vol. 4, no. 82, p. 21, 2002.

[21] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger and C. Barbieri, "Space-to-Ground Quantum-

Communication Using an Optical Ground Station: A feasibility Study," Article Draft, Matera, 2004.

[22] M. Er-long, H. Zheng-fu, G. Shun-sheng, Z. Tao, D. Da-Sheng and G. Guang-can, "Background Noise of Satellite to Ground Quantum Key Distribution," *New Journal of Physics,* vol. 7, no. 215, p. 8, 2005.

[23] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco and P. Villoresi, "Experimental Satellite Quantum Communications," *Physical Review Letters,* vol. 115, no. 040502, p. 5, 2015.

[24] S. Fiorino, Interviewee, *LEEDR Usage and Applicability to Satellite Propagation.* [Interview]. 13 October 2015.

[25] T. S. Kelso, "Celestra: Astrodynamics Software," Center for Space Standards and Innovation, 30 September 2015. [Online]. Available: https://celestrak.com/software/vallado-sw.asp. [Accessed 6 October 2015].

[26] K. Brown, Reflections on Relativity, MathPages, 2015.

[27] Newport Corporation, "Bandpass Filters," Newport Corporation, 2015. [Online]. Available: http://search.newport.com/i/1/nav/1/q1/Optical%2520Filters/q2/Bandpass%2520Filters/q3/Bandpass%2520Filters/x1/section/x2/chapter/x3/family/x1/pageType/q1/Products/. [Accessed 13 January 2016].

[28] M. Cvijetic and Y. Takashima, "Beyond 1Mbs Free-Space Optical Quantum Key Distribution," in *Transparent Optical Networks (ITCON)*, Graz, 2014.

[29] Excelitas Technologies, "Photon Detection Solutions," 18 January 2016. [Online]. Available: http://www.excelitas.com/Downloads/CAT_PhotonDetection.pdf. [Accessed 6 January 2016].

Vita

Captain Jonathan Denton attended the University of California, Los Angeles for undergraduate education. He commissioned through AFROTC as a Distinguished Graduate with a degree in Aerospace Engineering. His first assignment was as a responsible engineer providing mission assurance during booster assembly supporting the OSP-2 contract. He then worked as the Launch Mission Manager at Vandenberg AFB for the first Falcon 9v1.1 launch from the Western Range. He concurrently led the 30 SW New Entrant Certification Team in their role certifying SpaceX to compete for EELV launches. Following his studies at the Air Force Institute of Technology, Captain Denton will be assigned to the National Reconnaissance Office.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
24-03-2016	Master's Thesis	August 2014 – March 2016

TITLE AND SUBTITLE
Key Detection Rate Modeling and Analysis for Satellite-Based Quantum Key Distribution

5a. CONTRACT NUMBER

5b. GRANT NUMBER
5713400-301-6448

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Denton, Jonathan C., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/ENY)
2950 Hobson Way, Building 640, WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENY-MS-16-M-206

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Laboratory for Telecommunication Sciences
Dr. Gerry Baumgartner
8080 Greenmead Drive, College Park MD 20740
gbaumgartner@ltsnet.net

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT
A satellite QKD model was developed and validated, that allows a user to determine the optimum wavelength for use in a satellite-based QKD link considering the location of ground sites, selected orbit and hardware performance. This thesis explains how the model was developed, validated and presents results from a simulated year-long study of satellite-based quantum key distribution. It was found that diffractive losses and atmospheric losses define a fundamental trade space that drives both orbit and wavelength selection. The optimal orbit is one which generates the highest detection rates while providing equal pass elevation angles and durations to multiple ground sites to maximize the frequency of rekeying. Longer wavelengths perform better for low Earth orbit satellites while shorter wavelengths are needed as orbital altitude is increased. For a 500km Sun-synchronous orbit, a 1060nm wavelength resulted in the best performance due to the large number of low elevation angle passes. On average, raw key rates of 170kbit/s per pass were calculated for a year-long orbit. This work provides the user with the capability to identify the optimal design with respect to wavelength and orbit selection as well as determine the performance of a QKD satellite-based link.

15. SUBJECT TERMS
Quantum Key Distribution, Detection Rate, Quantum Bit Error Rate, Satellite QKD

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Richard G. Cobb, AFIT/ENY
U	U	U	UU	120	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext 4559 (NOT DSN) (Richard.Cobb@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18