Investigating Wireless Quantum Key Distribution for Advanced Reactor Communications

Metcalf Internship Program Report

Nuclear Science and Engineering Division
About Argonne National Laboratory
Argonne is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC under contract DE-AC02-06CH11357. The Laboratory’s main facility is outside Chicago, at 9700 South Cass Avenue, Argonne, Illinois 60439. For information about Argonne and its pioneering science and technology programs, see www.anl.gov.

Document availability

Reports not in digital format may be purchased by the public from the National Technical Information Service (NTIS):
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312
www.ntis.gov
Phone: (800) 553-NTIS (6847) or (703) 605-6000
Fax: (703) 605-6900
Email: orders@ntis.gov

Reports not in digital format are available to DOE and DOE contractors from the Office of Scientific and Technical Information (OSTI):
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831-0062
www.osti.gov
Phone: (865) 576-8401
Fax: (865) 576-5728
Email: reports@osti.gov

Disclaimer
This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor UChicago Argonne, LLC, nor any of their employees or officers, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of document authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, Argonne National Laboratory, or UChicago Argonne, LLC.
Investigating Wireless Quantum Key Distribution for Advanced Reactor Communications

Metcalf Internship Program Report

prepared by
Madeleine Roberts$^{1,2}$ and Alexander Heifetz$^1$

$^1$Nuclear Science & Engineering Division, Argonne National Laboratory
$^2$University of Chicago, Chicago IL

August 20, 2021
# Table of Contents

Table of Contents ............................................................................................................. 1  
List of Figures .................................................................................................................. 2  
List of Tables .................................................................................................................... 2  
Abstract ............................................................................................................................. 3  
1. Introduction .................................................................................................................... 3  
2. Quantum Key Distribution Overview .......................................................................... 4  
2.1. Protocol basics .......................................................................................................... 4  
2.2. Wireless configuration with SMR ............................................................................. 5  
3. Atmospheric Attenuation Model .................................................................................. 6  
3.1. Clear weather attenuation ......................................................................................... 6  
3.2. Cloud and fog attenuation ......................................................................................... 7  
3.3. Rain attenuation ........................................................................................................ 7  
4. Results ........................................................................................................................... 8  
4.1. Attenuation model ..................................................................................................... 8  
4.2. SeQUeNCe simulation .............................................................................................. 9  
5. Conclusions .................................................................................................................. 10  
References ....................................................................................................................... 11
List of Figures

Figure 1 – Reactor-remote user communication channels. Secure keys are distributed along a quantum channel via QKD then used to encrypt reactor state data via AES for transmission along a classical channel……………………………………………………………………………………………………5

Figure 2 – Ground-satellite quantum channel schematics. The microwave signal is relayed from sender (the reactor facility) to receiver (the remote user) via satellite, removing the need for a line of sight between communication parties…………………………………………………………6

Figure 3 – Attenuation per km altitude gain for various weather conditions. (a) Signal path through clear sky. (b) Signal path through light rain conditions (rain rate of 0.5 mm/hr). (c) Signal path through moderate rain conditions (rain rate of 4.0 mm/hr). (d) Signal path through heavy rain conditions (rain rate of 8.0 mm/hr) ……………………………………………………………………………………………………………8

List of Tables

Table 1 – Average attenuation for 500 km signal pathlength in various weather conditions……9
Table 2 – Average SeQUeNCe protocol duration for a sample of 256-bit keys transmitted in various weather conditions…………………………………………………………………………………………………………9
Table 3 – Average SeQUeNCe protocol duration for a sample of 256-bit keys transmitted in heavy rain (8 mm/hr) with various depolarization rates…………………………………………………………10
Abstract

Remote operation of small modular reactor (SMR) facilities is an appealing prospect for streamlined operation costs, safety concerns, and user convenience. The ability to guarantee security of communication channels between offsite users and nuclear reactor facilities is critical to enabling remote operations, given the sensitive nature of reactor state data. This report proposes a configuration implementing quantum key distribution (QKD) and advanced encryption standard (AES) protocols to establish secure reactor data feeds. The model outlined, which utilizes the Argonne-developed SeQUeNCe software package and custom MATLAB code, determines free-space channel losses for microwave-band communications in a variety of weather conditions and simulates QKD via ground-satellite links. This report demonstrates the feasibility of repeatable, real-time key generation and distribution for this configuration towards enabling secure wireless reactor communications.

1. Introduction

The ability to communicate with small modular reactor (SMR) facilities offsite is key to enabling remote operations, which is an appealing prospect for streamlining operation costs, increasing workplace safety, and ensuring user convenience. Fully remote control requires a two-way transmission exchange between the reactor and user, in which the facility sends reactor state data, and the user responds with a command signal. To implement this exchange, the communication channel must have a high level of security to prevent compromising potentially sensitive reactor state information. Pairing quantum key distribution (QKD) and advanced encryption standard (AES) protocols to generate a communication cipher could achieve the necessary level of security for these communications.

The security of QKD results from its utilization of a quantum communication channel to share a secret key between sender and receiver, which offers a reliable way to detect any eavesdropping on the channel [1,2]. However, fiber-based quantum channels are currently limited to tens of kilometers due to high signal loss and a lack of functional quantum repeater technology [3,4]. A viable alternative is establishing a free-space quantum channel between the reactor and remote user. To avoid limiting communication distance by requiring a line of sight, a satellite can be used to relay the signal transmitted in the form of polarized microwave photons. Nevertheless, the effects of atmospheric channel losses on quantum signal transmission are not well studied and may present an impediment to establishing a reliable, real-time link between reactor and user. Since reactor power can function as a backup for other energy sources that are handicapped in certain weather conditions, such as solar energy, it is important that key distribution be possible even in inclement weather [5].
To investigate these factors, this report utilizes the Argonne-developed SeQUeNCe software package to model a wireless quantum channel and custom MATLAB code to determine channel losses resulting from transmission through the atmosphere in various weather conditions [6]. These results will indicate whether the proposed wireless configuration is feasible for experimental implementation.

2. Quantum Key Distribution Overview

2.1. Protocol basics

Applications of quantum technology to cryptography were first theorized in the 1980s, and since then two primary QKD protocols have emerged: BB84, developed by Charles Bennett and Gilles Brassard, and E91, developed by Arthur Ekert [7]. BB84, a discrete-variable protocol utilizing single-photon detection, is the more common of the two and is thus the focus of this research.

A communication party initiates BB84 by encoding a random string of qubits via polarization of weak coherent photon pulses according to two distinct basis orientations. The four possible states are given by:

\[\begin{align*}
\text{Base A (rectilinear)}: & \quad \psi_0 = |0\rangle \\
& \quad \psi_1 = |1\rangle \\
\text{Base B (diagonal)}: & \quad \psi_{0'} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
& \quad \psi_{1'} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{align*}\]  

Each basis forms a complete quantum system, such that \(\langle \psi_0 | \psi_1 \rangle = \langle \psi_{0'} | \psi_{1'} \rangle = 0\). Since the bases overlap but are not orthogonal relative to each other, there is no way for the receiver to determine the base used to encode a transmitted photon with complete certainty [8]. Thus, the receiver selects a basis at random for each pulse and records the results of the measurements. If the receiver by chance does not select the basis used for qubit encoding, he is not guaranteed to measure the correct bit value. To remove resulting discrepancies, both parties perform a key sifting procedure on the raw key, in which they publicly reveal via an unsecure classical channel which basis was used to encode and measure each pulse. Instances where basis selections do not align are thrown out. Since the receiver has a 50% probability of choosing the correct basis for measurement, the initial key size is reduced by approximately half. The two parties now possess secret keys that, barring channel interference, are identical [2].

The unique security component of QKD arises from the no-cloning theorem of quantum physics, which asserts that an unknown quantum state cannot be copied without modifying the original state. Thus, any attempt to eavesdrop on the communication channel will introduce key discrepancies between the sender and intended receiver. By estimating the error rate in the key transmission, accomplished by publicly revealing and comparing a sample bit string, the
communication parties can determine if their channel is secure. If the error rate is statistically significant, the protocol is abandoned and reinitiated as necessary [1]. When a secure key is generated and verified, it can be used with an advanced encryption standard (AES) protocol to encrypt reactor state data before transmission along a classical channel. Upon reception, the message is decrypted by a remote user possessing the key. The schematics of this procedure are depicted below.

Fig. 1: Reactor-remote user communication channels. Secure keys are distributed along a quantum channel via QKD then used to encrypt reactor state data via AES for transmission along a classical channel.

2.2. Wireless configuration with SMR
Achieving practical security for communication with SMR facilities requires that this protocol be easily repeatable to generate a unique key for each transmission, reliable with minimal channel losses, and rapid enough to enable real-time communication feeds between reactors and remote users [9]. Because of significant channel losses through fiber transmission, most fiber optic QKD channels are currently limited to tens of kilometers [2,3]. The technology necessary to extend this range, a functional quantum repeater, has not yet been successfully developed. Thus, wireless transmission channels utilizing satellites in low earth orbit are the ideal configuration for achieving QKD along distances necessary for remote reactor communication [10]. The schematics of the proposed configuration are shown below.
The qubits are prepared at the reactor site using laser diodes to generate microwave pulses, which can be encoded with the desired polarization using a series of beamsplitters and waveplates. The pulses are then combined and filtered as necessary before being coupled into the atmosphere along the transmission path.

The satellite receives and directs the signal back down towards the remote user, who measures the qubits using an optical detector. The measurement basis is determined by a sequence of beamsplitter orientations applied to the pulses. After reading the bit values, the receiver initiates a key sifting procedure along a standard classical channel as described in section 2.1.

3. Atmospheric Attenuation Model

Attenuation resulting from atmospheric gases, cloud coverage, and rain was quantified utilizing MATLAB’s communications toolbox. The details of the model are outlined below.

3.1. Clear weather attenuation

In clear weather, attenuation for transmissions in the X-band (~7-10 GHz) is primarily caused by atmospheric oxygen, water vapor, and nitrogen. These effects were calculated using the following model, recommended by the ITU for transmission frequencies in the range 1-1000 GHz [11]:

![Ground-satellite quantum channel schematics. The microwave signal is relayed from sender (the reactor facility) to receiver (the remote user) via satellite, removing the need for a line of sight between communication parties.](image-url)
\[ \gamma = 0.1820f (N''_{oxy} + N''_{vap}) \]  \hspace{1cm} (2)

where \( \gamma \) is the specific attenuation in dB/km, \( f \) is the frequency in GHz, and \( N''_{oxy} \) and \( N''_{vap} \) are the imaginary parts of the frequency-dependent complex refractivities of oxygen and water vapor, respectively.

### 3.2. Cloud and fog attenuation

Cloud and fog attenuation was calculated according to the following model, recommended by the International Telecommunication Union (ITU) for transmission frequencies below 200 GHz [12]:

\[ \gamma_c = MK_i \]  \hspace{1cm} (3)

where \( \gamma_c \) is the specific attenuation in dB/km, \( M \) is the water density of the cloud or fog in g/m\(^3\), and \( K_i \) is the specific attenuation coefficient in (dB/km)/(g/m\(^3\)).

### 3.3. Rain attenuation

Rain attenuation was calculated according to the following model, recommended by the ITU for transmission frequencies in the range 1-1000 GHz [13]:

\[ \gamma_r = R^a \]  \hspace{1cm} (4)

where \( \gamma_r \) is the specific attenuation in dB/km, \( R \) is the rain rate in mm/hr, and \( k \) and \( \alpha \) are coefficients dependent on frequency.

Since attenuation drops off exponentially with altitude, special focus is given to the first 30 km of transmission pathlength, which encompasses the troposphere, lower stratosphere, and upper stratosphere. Adjustments to pressure and temperature inputs were calculated as a function of altitude, according to the following equations from NASA’s earth atmosphere model [14]:

\[
T(\degree C) = \begin{cases} 
15.04 - 0.00649h, & h < 11000m \\
-56.46, & 11000m < h < 25000m \\
-131.21 + 0.00299h, & h > 25000m 
\end{cases} \hspace{1cm} (5a)
\]

\[
P(kPA) = \begin{cases} 
101.29 \left( \frac{T+273.1}{288.08} \right)^{5.256}, & h < 11000m \\
22.65e^{1.73 - 0.000157h}, & 11000m < h < 25000m \\
2.488 \left( \frac{T+273.1}{216.6} \right)^{-11.388}, & h > 25000m 
\end{cases} \hspace{1cm} (5b)
\]

where \( h \) is the altitude in m, \( T \) is the temperature in degrees Celsius, and \( P \) is the pressure in kPa.
4. Results

4.1. Attenuation model

The MATLAB attenuation model was tested across a 500 km ground-satellite link for 10 GHz signal pulses, where a geosynchronous low earth orbit above the transmission site is assumed. Losses sustained per km altitude gained for the first 30 km of transmission in various weather conditions are shown below. “Light rain” corresponds to an average rain rate of 0.5 mm/hr, “moderate rain” to a rate of 4.0 mm/hr, and “heavy rain” to a rate of 8.0 mm/hr. Note that the average rainstorm height is about 13 km, hence the abrupt decrease in attenuation at that altitude.

![Fig. 3: Attenuation per km altitude gain for various weather conditions. (a) Signal path through clear sky. (b) Signal path through light rain conditions (rain rate of 0.5 mm/hr). (c) Signal path through moderate rain conditions (rain rate of 4.0 mm/hr). (d) Signal path through heavy rain conditions (rain rate of 8.0 mm/hr).]
Average attenuation accumulated across the entire 500 km pathlength is summarized in the following table. For reference, typical attenuation for a 1550 nm QKD pulse in optical fiber is 0.2 dB/km [4].

**Table 1: Average attenuation for 500 km signal pathlength in various weather conditions.**

<table>
<thead>
<tr>
<th>Atmosphere conditions</th>
<th>Average attenuation (dB/km)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear sky</td>
<td>6.74e-5</td>
</tr>
<tr>
<td>Light rain</td>
<td>1.80e-3</td>
</tr>
<tr>
<td>Moderate rain</td>
<td>4.72e-3</td>
</tr>
<tr>
<td>Heavy rain</td>
<td>8.40e-3</td>
</tr>
</tbody>
</table>

**4.2. SeQUeNCe simulation**

SeQUeNCe, an open-source Python package developed at Argonne, was utilized to test the feasibility of a real-time, free-space quantum channel with signal losses [6]. The code models a two-node quantum channel for implementing QKD with pathlength and channel losses specified by the user, which can be used to estimate key generation and distribution time. Cascade is utilized as the primary error correction protocol, frequently paired with QKD for its consistently effective performance [15].

The 10 GHz pulse attenuation results outlined in section 4.1 were run with SeQUeNCe to simulate a ground-satellite link. For each weather condition, a sample of 100 256-bit keys was generated for use in AES encryption with 97% polarization fidelity. The results of the simulation are summarized below.

**Table 2: Average SeQUeNCe protocol duration for a sample of 256-bit keys transmitted in various weather conditions.**

<table>
<thead>
<tr>
<th>Atmosphere conditions</th>
<th>Average protocol duration (s)</th>
<th>Standard deviation (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear sky</td>
<td>0.48</td>
<td>0.06</td>
</tr>
<tr>
<td>Light rain</td>
<td>0.51</td>
<td>0.05</td>
</tr>
<tr>
<td>Moderate rain</td>
<td>0.52</td>
<td>0.09</td>
</tr>
<tr>
<td>Heavy rain</td>
<td>0.56</td>
<td>0.07</td>
</tr>
</tbody>
</table>

Signal depolarization, often caused by rain and ice particles in the atmosphere, is another major cause of transmission loss worth considering. Attenuation values plugged into SeQUeNCe were adjusted to reflect 10%, 20%, and 30% depolarization rates, based on the depolarization model.
recommended by the ICU [16,17]. The results of 100 256-bit key iterations are shown below for rainy conditions.

Table 3: Average SeQUeNCe protocol duration for a sample of 256-bit keys transmitted in heavy rain (8 mm/hr) with various depolarization rates.

<table>
<thead>
<tr>
<th>Polarization Fidelity</th>
<th>Average protocol duration (s)</th>
<th>Standard deviation (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>90%</td>
<td>0.64</td>
<td>0.04</td>
</tr>
<tr>
<td>80%</td>
<td>0.66</td>
<td>0.03</td>
</tr>
<tr>
<td>70%</td>
<td>0.70</td>
<td>0.04</td>
</tr>
</tbody>
</table>

5. Conclusions
Implementing QKD using a free-space quantum channel in place of fiber optics has the potential to significantly reduce transmission losses, resulting in a signal-to-noise ratio low enough to extend successful communication range considerably. The model outlined produces channel attenuation for transmission in clear sky smaller than 1% of typical losses sustained in commercial fiber, and up to only 4.2% of fiber losses in heavy rain. This indicates free-space QKD implementation is unconditionally attainable for communication involving satellites in geosynchronous low earth orbit. Additionally, QKD simulations with SeQUeNCe produced average protocol times consistently less than a second for attenuation caused by a variety of weather conditions, including rain-induced depolarization up to 30%, which suggests real-time key generation and distribution for encrypting reactor state data feeds is attainable for transmission across arbitrary distances. These results indicate experimental implementation of QKD is a worthwhile investment towards enabling real-time, unconditionally secure control of SMR facilities by remote users.
References
