Implementation of a Wireless Time Distribution Testbed Protected with Quantum Key Distribution

Jason Bonior†, Philip Evans†, Greg Sheets†, John Paul Jones†, Toby Flynn†, Lori Ross O'Neil‡,
William Hutton‡, Richard Pratt‡, Thomas Carroll‡
†Oak Ridge National Laboratory
{boniorjd, evanspg, sheetsgs, jonesjpjr, flynnth}@ornl.gov
‡Pacific Northwest National Laboratory
{lro, william.hutton, rmpratt, thomas.carroll}@pnnl.gov

***Abstract*—Secure time transfer is critical for many time-sensitive applications. The Global Positioning System (GPS) which is often used for this purpose has been shown to be susceptible to spoofing attacks. Quantum Key Distribution (QKD) offers a way to securely generate encryption keys at two locations. Through careful use of this information it is possible to create a system that is more resistant to spoofing attacks. In this paper we describe our work to create a testbed which utilizes QKD to distribute secure one-time pad keys for traditional RF links. This testbed will be used for the development of more secure and spoofing resistant time distribution protocols.**

***Index Terms*—Time Services, Quantum Key Distribution, Wireless Testbed, Global Positioning System**

I. Introduction

Accurate and reliable timing is increasingly important to a variety of applications. Office and financial networks require accurate timing to track trading and business [1]. Cyber-physical systems such as Connected Vehicle Technology [2], Advanced Grid Integration [3], and sensor networks require accurate timing sources to maintain the quality of their services. Many of these devices and services rely on the Global Positioning System (GPS) to provide the current time and discipline their clocks. However, GPS is vulnerable to spoofing attacks wherein an adversary transmits false GPS signals to introduce timing and localization errors [4], [5]. Such attacks can compromise the quality of the timing information provided to the aforementioned services causing significant disruptions and rendering sensor data useless due to improper time stamps. More advanced adversaries can even force false reporting of data by more subtle shifts in timing [6].

One proposed solution for providing reliable timing that is resistant to spoofing attacks is to secure the communications using Quantum Key Distribution (QKD). Traditionally QKD is used to distribute secure keys for cryptographic algorithms and protocols even in the presence of eavesdroppers [7], [8]. Here, we pursue a different system model by instead using QKD to make a system more resistant to spoofing. Time distribution over traditional QKD systems would be cumbersome and costly since each device would require expensive QKD hardware and dedicated optical fiber links to the timing source. We instead propose a system which uses two or more QKD-connected trusted beacons to send the time: one (e.g., Alice) which sends the time encrypted with QKD-generated keys; and the other (e.g., Bob) which sends the QKD keys necessary to decrypt and obtain the time following an appropriate delay. This, combined with a carefully crafted two-way protocol can create a system which is very difficult for an adversary to spoof.

In this paper we present our testbed for the development and testing of wireless time distribution protocols secured using QKD. In Section II we will provide an overview of what QKD is and why it is so secure. Section III will cover the capabilities of the testbed and the choices made in its design. Section IV describes the implementation of a basic two-way protocol for sharing timing and other data. We will present the results of performance measurements of the testbed in Section V and the future plans for continuing to improve it in Section VI.

II. Quantum Key Distribution

QKD is a broad technique for generating and distributing encryption keys amongst two or more parties even in the presence of an eavesdropper. QKD protocols, such as the famous BB84 [7] and Ekert91 [8] protocols, have been studied extensively from a security perspective and are known to be provably secure [9]. Two spatially separated parties, traditionally referred to as *Alice* and *Bob*, wish to communicate securely in the presence of a suspected eavesdropper, *Eve*. There exists a quantum channel (typically an unlit optical fiber) over which the quantum key is shared, and a classical channel over which the quantum-key secured information is exchanged using a standard symmetric encryption technique, e.g., AES-256. Eve is assumed to have access to both the quantum and classical channels.

At the heart of QKD are the generation, transmission, and detection of quantum states of light. Typically, the light is

prepared and measured in either of two complementary bases. In single-photon QKD, Alice randomly chooses a bit value and a preparation basis, i.e., a specific set of non-orthogonal polarization or phase states, while Bob randomly chooses a measurement basis. If Bob's basis choice is the same as Alice's, then he will be able to measure the value of the bit prepared by Alice. However, if they choose different bases, then Bob's measurement result will be completely uncorrelated with Alice's bit value. As an example, the information might be carried in the polarization of a single photon: the rectilinear basis comprises orthogonal states of horizontal (H) and vertical (V) polarization, while the complementary diagonal basis has orthogonal states of 45 (+) and -45 (-) polarization. Suppose Alice prepares a V photon. If Bob measures in the H/V basis, then his measurement result will be V. However, if he measures in the +/- basis, then he will record either + or - each with 50% probability. Once Alice and Bob have prepared and measured a suitable number of photons, they publicly compare their basis choices (but not the bit values) and discard all of the cases (roughly 50%) for which they chose complementary bases. Barring errors, the remaining data are perfectly correlated: Bob knows what Alice sent, and she knows what he measured.

Alice and Bob assume Eve has access to both the classical and quantum communication channels. There are a number of attacks Eve can deploy in an attempt to gain information of the secret key passed between Alice and Bob. One of the most straightforward is the classic intercept-resend spoofing attack, in which Eve intercepts Alice's photon destined for Bob, applies her own measurement, and then attempts to recreate the same state that she measured to retransmit to Bob. However, this is in direct violation of the no-cloning theorem, which states that it is impossible to create identical copies of an arbitrary quantum state [10]. In essence, Eve's strategy works only when she guesses the same basis as Alice and Bob. When she guesses incorrectly, she ends up sending an uncorrelated state to Bob, leading to a detectable increase in the number of errors in the raw key. The presence of, and any information leakage to Eve, can be detected by comparing a certain subset of their remaining bit string and analyzing errors. Eve has at her disposal any number and variety of attacks in an attempt to gain more information about the secret key shared by Alice and Bob. However, any attempt by Eve to gain any sizable amount of information is revealed by an increase in the quantum bit error rate detected by Alice and Bob.

Any information leakage due to Eve's eavesdropping can be minimized by performing reconciliation and privacy amplification steps on the shared bit string. Reconciliation is a form of error correction performed over the classical channel to ensure the shared key is identical. The cascade protocol, one method of performing reconciliation, breaks the shared bit string into smaller blocks and performs recursive parity checks of increasingly smaller blocks of the bit string [11]. The result is that Alice's and Bob's keys can be made identical with high probability, but at the expense of an increase in information captured by Eve due to their continued bit comparisons over a compromised channel. Finally, privacy amplification is performed in order to eliminate the partial information gained by Eve. This is accomplished by using the shared key between Alice and Bob to produce a new, shorter key having less mutual information with Eve [12].

After the QKD process is the encryption of information with the shared secret key, ideally using a standard such as Advanced Encryption Standard (AES), for secure information transfer between Alice and Bob. For maximum security, the secret key is used only once in a one-time pad scheme.

TABLE I
DISTANCE BETWEEN TESTBED NODES

Link	Distance (miles)
Alice to Bob	1.23
Alice to RX1	0.98
Bob to RX1	2.21

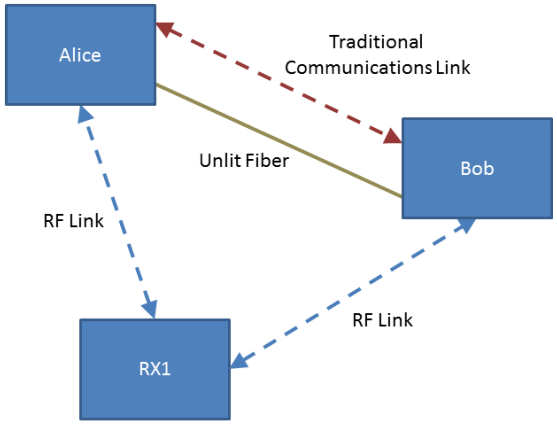

Fig. 1. System overview and communications links

III. SYSTEM IMPLEMENTATION

Our testbed is located at the Pacific Northwest National Laboratory (PNNL) in Richland WA and includes three sites across the campus. The distances between the nodes is given in Table I. Figure 2 shows the locations of the radio nodes and their names. Alice and Bob are each equipped with a QKD system and Software-Defined Radio (SDR) based RF system. The QKD consists of a pair of optoelectronic units comprising the single photon source and detectors, connected together over unlit fiber. Computers at each end station are responsible for controlling the QKD units, and the necessary communications over the classical channel to generate the secret key data from the raw key data. The RF system is made up of a Universal Software Radio Peripheral B210 (USRP-B210) and another laptop. The third location, RX1, is equipped with an RF system identical to those at Alice and Bob. Figure 1 shows the interconnection of the devices in the system.

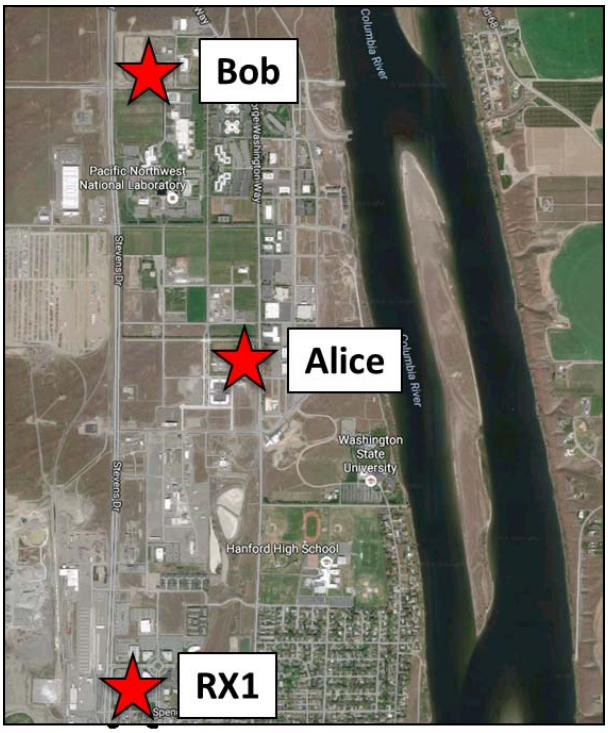

Fig. 2. Positions of the RF Nodes on the PNNL Campus

A. QKD Backbone & Key Servers

A 'plug and play' QKD system (IDQuantique Clavis2) was installed at the *Alice* and *Bob* stations to form the quantum backbone. An unlit SMF28 fiber strand was required for the quantum channel; a standard TCP/IP network comprised the classical channel. Burn-in tests were performed to confirm the QKD system was functioning correctly. During all other tests, the QKD system ran in the background. The typical performance statistics of any QKD system are: (1) the secret key rate (SKR) - a measure of how much key material is generated between *Alice* and *Bob* per second on average, and thus how often one can use one-time pad messages; and (2) the quantum bit-error rate (QBER) - a measure of the errors encountered during the error-correction phase of the BB84 protocol - either due to system noise or the presence of an eavesdropper.

keyTrans, a custom developed server-client application, was used to take the arbitrarily sized secret key file generated from the Clavis2 QKD system and provide 256-bit sized individual keys. These keys were then served to the radio hardware for one-time pad use. Following use by the radio hardware, the keys were discarded and refreshed with a new key.

B. RF System Implementation

This testbed was designed to operate in the 902-928 MHz ISM band. Direct Sequence Spread Spectrum is employed to increase the link margin of the system. The modulation used for this communication system is Binary Phase Shift Keying. Each location is fitted with omnidirectional antennas (Kathrein Scala OGB9-915N) on the roof. Low-Noise Amplifiers (LNAs), which provide about 30 dB of gain, were used in the receive chain, and Power Amplifiers (PA), which provide about 30dB of gain, were used for the transmitters. The current system is half-duplex. Separate channels are used for transmit and receive on the USRPs and each has its own antenna on the roof. The USRP-B210 is connected to a laptop which is connected to the PNNL network. The RF computers communicate with the QKD systems via this network. Because of the wideband front end of the USRP and the desire to avoid noise from adjacent bands, a hardware bandpass filter (Pasternack PE8700) was added to avoid potential issues with saturation of the analog-to-digital converter device and to reduce the digital filtering requirements.

The USRP-B210 was selected to be the basis of our radio platform because of the device's flexible nature, compatibility with widely used open source software (GNURadio), and similarity to the USRP-E310 which will be utilized in future revisions of the testbed. The USRP-B210 utilizes an RF front end which matches the USRP-E310 embedded system which will make development of software which is compatible with future improvements to the testbed easier.

C. Link Budget Calculations

During the design process, we calculated the expected path loss between each of the locations in this testbed. Based on this and the modulation schemes we had chosen, we calculated the link margin for all links in the testbed. Table II shows the results of these calculations.

All FCC transmit power limitation requirements were accounted for in the design and budgeting process and observed during the test execution. The transmit power limitation for the 900MHz ISM band is +36dBm with an omni-directional antenna. The antennas provided 11dBi of gain. Therefore, we assumed a back-off on power out of our power amplifier to overcome cabling losses, yet give us a 2dB margin to the FCC limit at the transmit antenna. The antennas were mounted at a height of approximately 10m, which gives a line-of-sight (LOS) channel.

Please note that a critical assumption, which results in a lot of calculated margin for the given hardware and distance, is the assumption of additive white Gaussian noise in the channel. This assumption will need to be updated based upon further site surveys. The propagation loss was derived by considering the channel to be free space LOS. The path loss component of the link budget came out to be 103dB for the Bob to RX1 link, 98dB for the Bob to Alice link, and 96dB for the Alice to RX1 link. In determining the thermal noise floor, we used 2.5MHz bandwidth, as the signal should be filtered to this bandwidth prior to the detector in the receiver. The roughly 18dB of coding gain associated with the spreading sequence length of 63 was also incorporated into the analysis. A receiver noise figure of 8dB was also factored into the calculations. Please note that the analysis assumes 5dB of cabling loss for every link from the radio to the antenna. The required ratio of energy per bit over noise power (Eb/No) for a probability of bit

TABLE II
SYSTEM LINK SIGNAL-TO-NOISE RATIOS

Link	LOS (dB)	Hata (dB)	Required (dB)
Alice to Bob	52.7	42.0	9.54
Alice to RX1	54.7	45.9	9.54
Bob to RX1	47.7	32.8	9.54

error of 10^{-5} is 9.54dB at the detector for the modulation type selected. As can be seen in Table II, given the assumptions and model chosen, we meet this requirement with margin from a calculation/theoretical perspective.

The accuracy of the free space LOS assumption may vary from season-to-season as foliage may obstruct the LOS path in summer and portions of spring and fall. Also, there are reflections and diffraction that will occur, because it is not really free space. To establish a worst-case scenario for the links in the presence of additive white Gaussian noise, a small urban Hata model was also utilized in the budget process. The margin in this case, as can be seen in Table II, was calculated to be 22.8 dB for the longest link, given the same bit error rate of 10^{-5}, which provided indication that the design was satisfactory.

IV. TIME DISTRIBUTION PROTOCOL

The goal of this testbed is to provide a platform for the testing and development of protocols like the one presented in [13]. As such, the final test for the completed system is to implement and demonstrate time transfer protocols. Two basic protocols were used in testing this system. It should be noted that these protocols are very basic and are intended only to test the functionality of the testbed. Secure protocols for time distribution will require additional safe guards such as the calculation of propagation delay, etc. Research into such techniques will be the subject of future efforts.

In these protocol descriptions Alice, Bob, and RX1 are made up of a computer and SDR. The QKD servers associated with Alice and Bob are referred to as QKD-Alice and QKD-Bob respectively.

A. Point-to-point Time Transfer

Two basic time transfer protocols were implemented in our testing. The first was a point-to-point synchronization between two devices which are also linked using the QKD system. In this case Alice is the master clock and Bob is a local master. We assume that Alice and Bob are in fixed locations and that the propagation delay (t_{prop}) between the two is known. In this scenario Bob would be used to distribute time locally and would be synchronized with Alice via this protocol:

1) Alice pulls a key from QKD-Alice and encrypts a packet containing the time.
2) Alice transmits the encrypted packet at the time given in the packet payload.
3) Bob receives the packet and applies a timestamp corresponding to when it was detected ($t_{detected}$).
4) Bob pulls the corresponding key from QKD-Bob and decrypts the time (t_{packet}).
5) The clock offset between Alice and Bob is given by: $\Delta t = t_{packet} + t_{prop} - t_{timestamp}$

This protocol in its current state is a simplified form of network timing protocols. Because Alice and Bob have access to a QKD system the RF channel between them can be considered very secure. However, this protocol still relies on local distribution of time which will not benefit from QKD and will require additional infrastructure.

B. Broadcast Time Transfer

The second protocol is an open broadcast protocol in which the time is sent encrypted by one device and the accompanying key is broadcast by another coordinated device. For this second protocol we make the following assumptions:

1) The information being sent from the infrastructure does not need to be private (the data (i.e. the time) can be shared throughout the coverage area without exemption).
2) The locations of the devices being shared freely over the air does not pose a security vulnerability.

The following is an outline of the protocol used in this testing:

1) Alice requests a key from QKD-Alice and uses it to encrypt the outgoing time packet.
2) The packet is tagged to be transmitted at a specific time in the future to match the timestamp in the packet.
3) Bob receives the packet from Alice, requests a key from QKD-Bob and decrypts the message. If the message is valid (i.e. the message can be successfully decrypted using the quantum generated key) Bob generates a data message that contains the key. This message is tagged to be sent out at a time matching the time stamp in the new message generated by Bob.
4) RX1 listens for and stores the most recent message from Alice. Upon reception of a message from Bob, RX1 will decrypt the message from Alice.
5) Upon successful receipt and decryption of a message from Alice, RX1 broadcasts an acknowledgement message back to Alice and Bob.
6) Alice and Bob confirm the authenticity of the receipt to ensure the correct time was distributed to RX1.

This protocol requires a greater degree of complexity to attack because it requires the spoofing of two broadcast signals. The required coordination of multiple infrastructure sites also facilitates the detection of spoofed Alice/Bob messages. However, this does not prevent the spoofing of both Alice and Bob at a client site (RX1). The response from RX1 is required to verify the receipt of a valid time message. Therefore, as stated before, this protocol cannot be considered secure in its current state. This protocol, and the previously described point-to-point protocol were employed only to test the functionality of the system.

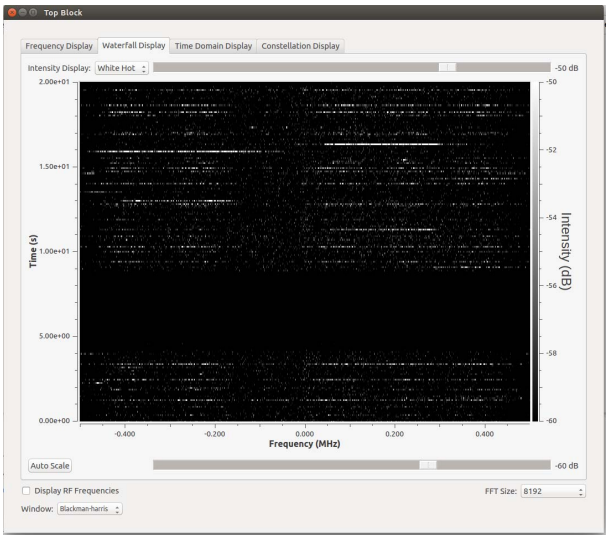

Fig. 3. Spectral capture taken at Bob. Center Frequency = 922.5 MHz, Sampling Rate = 1 Msps

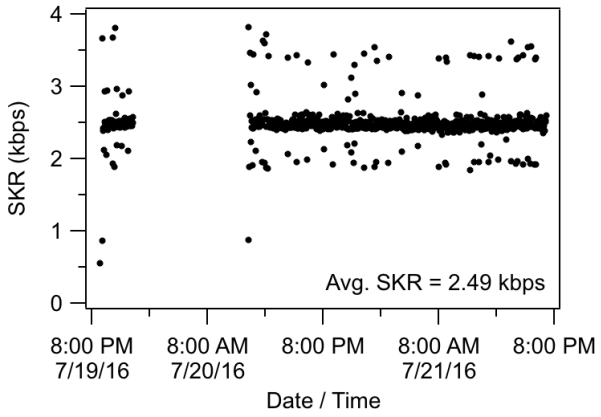

Fig. 4. QKD Secret Key Rate statistics over a 48 hour period. Average of 2.49 kbps.

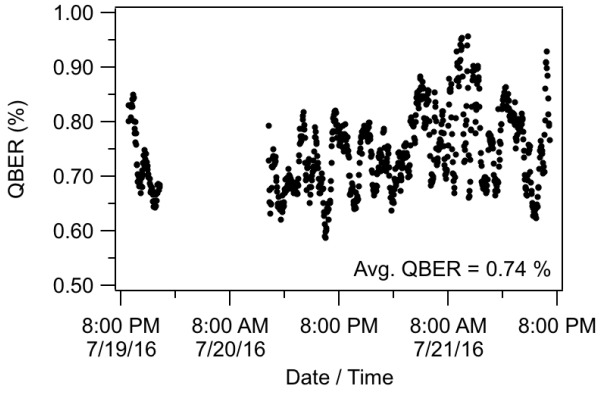

Fig. 5. QKD Quantum Bit-Error Rate statistics over a 49 hour period. Average of 0.74%

V. Results

A. Site Survey

As discussed in Section III, this testbed was designed to operate in the 902-928 MHz ISM band. Because this is a very popular band we had to be careful to avoid congested frequencies which would cause interference. A site survey was taken between each of the devices in the testbed. As is often the case in this band, the traffic is highly dependent on the time of day. Figure 3 shows a waterfall plot of a capture taken at Bob.

These results are not surprising given the popularity of this RF band, but it does highlight an important detail which must be addressed when using the testbed for future research and development. Ideally, bands specific to a target application will be utilized. Because the testbed is still in development, it is easier to work within this unlicensed band.

B. QKD System Measurements

Figures 4 and 5 show the sustained Secret Key Rate (SKR) and Quantum Bit-Error Rate (QBER) statistics of a sustained test run over 48 hours. The average SKR over this period is 2.49 kbps and the average QBER is 0.74%.

C. Implementation of a Time Distribution Protocol

Using the protocol described in Section IV we were able to send the time at a remote device. At the time this paper was written, we have only performed qualitative testing of the system, i.e. can we send and receive the time at a location? Further work is underway to test the performance of this system and the accuracy of the time transfer.

The use of two devices linked with QKD to send the time provides a tool that can be used to craft protocols that are very resistant to spoofing. The protocol presented in this work is very simplistic and has many vulnerabilities but effectively demonstrated the functionality of the system. This shows how the system can be utilized for the testing of more complex and secure protocols. The design and implementation of secure protocols which can take advantage of the tools provided in this testbed will be the subject of future efforts.

VI. Conclusions

We have presented a testbed for the development of time distribution protocols utilizing QKD and have shown the theoretical performance of the system. This system is unique in its application of QKD for secure time transfer. It is also unique due to the size of the testbed itself, spanning several miles in a light urban environment. To date, only preliminary data has been collected regarding the system performance. Qualitative tests of the links have been performed and we have shown that the basic protocol used for testing does in fact work. Future work will include the full characterization of the system including measured path loss and bit error rate figures.

Additional developmental work will include the transitioning from the laptop/USRP-B210 based RF system to one based on the USRP-E310 embedded platform. This will allow for stand alone systems which will give our testbed more

flexibility. We will also explore more complex and secure protocols for time transfer. Further work will include the integration of this system with a time dependent device such as a Phasor Measurement Unit (PMU) like those currently used for smart grid applications. This will allow us to demonstrate the setting of time on a device using the complete system and protocol.

ACKNOWLEDGEMENTS

This work was performed at Oak Ridge National Laboratory (ORNL), operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725. The authors acknowledge support from the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) program under contract M614000329.

REFERENCES

[1] GPS Applications: Timing. National Coordination Office for Space-Based Positioning, Navigation, and Timing. [Online]. Available: www.gps.gov

[2] Research and Innovative Technology Administration. Connected Vehicle Research, Intelligent Transportation Systems Joint Program Office. U.S. Department of Transportation. [Online]. Available: http://www.its.dot.gov/connected vehicle/connected vehicle.htm

[3] U.S. Department of Energy. Advanced grid integration. [Online]. Available: http://energy.gov/oe/mission/advanced-grid-integration-agi

[4] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," *Homeland Security Journal*, 2003.

[5] John A. Volpe National Transportation Center, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," Tech. Rep., 2001.

[6] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," *Power Systems, IEEE Transactions on*, vol. 28, no. 3, pp. 3253–3262, 2013.

[7] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[8] A. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, 1991.

[9] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

[10] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[11] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptography - EUROCRYPT '93*. Springer, 2001, pp. 410–423.

[12] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[13] L. Narula and T. E. Humphreys, "Requirements for secure wireless time transfer," in *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. IEEE, 2016, pp. 874–886.