Drone-based Quantum Key Distribution

Alexander D. Hill[1], Joseph Chapman[1], Kyle Herndon[1], Christopher Chopp[1],
Daniel J. Gauthier[2], Paul Kwiat[1]

[1]The University of Illinois at Urbana-Champaign
Department of Physics
1110 West Green Street
Urbana, IL 61801-3003

[2]The Ohio State University
Department of Physics
191 West Woodruff Ave
Columbus OH, 43210

Current best-in-class QKD protocols and implementations are limited to point-to-point key exchange. A future quantum-secure network will require a set of reconfigurable local nodes that can exchange keys individually with other nodes and mediate connections between two or more actors as a trusted cryptographic third party. Free-space quantum cryptographic platforms naturally lend themselves to reconfiguration, as nodes may be moved and reoriented to target new nodes with relative ease.

Free-space quantum communication over any significant distance, however, will inevitably encounter signal degradation due to weather events (such as fog) and turbulence. These effects are significantly mitigated by launching the quantum signal from a higher altitude -- in the case of turbulence, even an increase of tens of meters in launch height may reduce the effects of scintillation by orders of magnitude [1]. Having access to an agile, reconfigurable QKD networking system will enable quantum cryptography to reach applications prohibited by current approaches, such as temporary networks in seaborne, urban, or battlefield situations.

Recent advances in Lithium battery technology and control theory have made multicopter drones (or Unmanned Aircraft System(s) - UAS) stable and reliable enough to be a viable candidate for an agile QKD node. In this work, we present progress toward demonstrating a two-node quantum cryptographic network using multicopter UAS [2]. Because even enterprise-level, non-military UAS have maximum payloads on the order of 10 kg, developing lightweight yet robust hardware for free-space QKD is a prerequisite for a UAS-based approach. Our current progress is focused on developing a functioning optical payload for QKD capable of maintaining pointing between a transmitter node and receiver node while both are in flight. Research in this area is separated into several sub areas: fast, high-resolution optical stabilization; compact, independent, and identically distributed sources; and compact, lightweight single-photon detection.

Experimental Design: The DJI S1000+ Octocopter is a suitable airframe for airborne optical applications due to its high payload capacity (approximately 11 kg total). Control over basic functions of each of the transmitter and receiver UAS is designed to be semi-autonomous; the onboard flight controller (DJI A3) allows for serial interfacing with external sensor hardware via an onboard Linux computer (or onboard embedded system - OES). The OES is responsible for implementing the QKD protocol and for maintaining alignment of the transmitter/receiver nodes by interfacing with the flight controller and with the fast stabilization system in the optical payload (Fig. 1)

The transmitter/receiver optical payloads are sketched in Fig. 2. Our approach to signal acquisition and stabilization is adapted from the approach demonstrated in Ref. [3]. Initial acquisition is performed by rotating each UAS autonomously until each side "sees"' their alignment laser returned from the other side's corner-cube array. This ensures that the UAS themselves are approximately properly situated. Fine pointing is achieved by using steering mirrors to keep each drone's quadrant detector locked on the partner drone's alignment laser.

To avoid opening any side channel attacks due to system alignment, we have restricted our alignment corrections to local operations. As a result, our correction system loses some sensitivity and cannot correct any arbitrary translation/rotation. Because the channel lengths will be much larger than the input clear aperture on the receiver, however, only a small range of input angles need to be corrected by the optical payloads themselves. Additionally, small displacements of the UAS are irrelevant if complete angular control is possible.

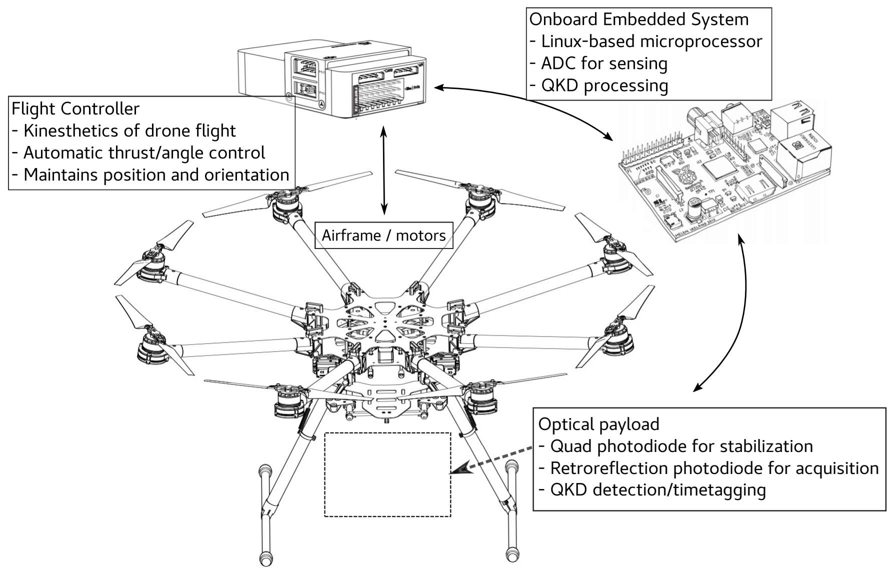

Figure 1: Node system design. Several subsystems align the multicopter UAS in our node model. The flight controller is responsible for maintaining proper position of the UAS on a kinesthetic level. An onboard microprocessor (in this case, an inexpensive Raspberry PI) instructs the flight controller on how to correct its position at a high level (*e.g., rotate 45 degrees*, or *translate 3 m horizontally*). The microprocessor also interprets sensor data from the optical payloads (such as quadrant-cell photodiode signals) and instructs the payload steering mirrors how to respond. In the final implementation, the onboard microprocessor will implement the entirely of the QKD protocol as well. (composite sources: DJI and Helen Ireland (CC))

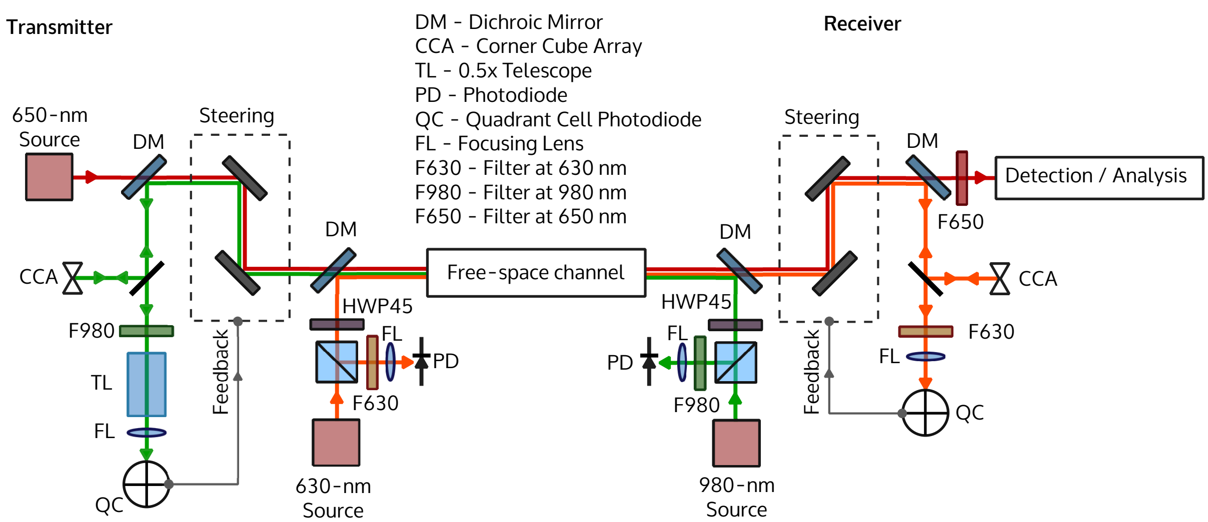

Figure 2: Optical payload design for transmitter/receiver. A rough initial alignment is performed by rotating the entire UAS until each side's respective alignment laser (980 nm and 630 nm) reflects from the opposing side's corner cube array and returns to the original side's bucket photodiode. After initial acquisition, each side centers the opposing side's alignment laser on a local quadrant-cell photodiode using its own steering mirrors. This orients each drone toward the other and establishes a robust link.

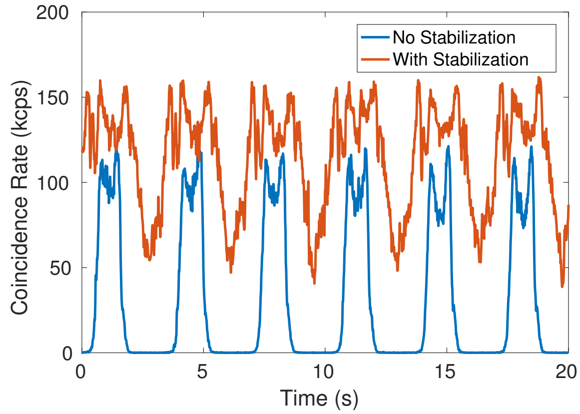

Figure 3: Stabilization performance for ±0.5° angular Tx deviations of a single-photon level signal, 500-kHz rep rate (4-m path on tabletop testbed). Stabilization eliminates dropouts and increases the mean count rate. Preliminary tests of UAS stability indicate an average uncorrected angular deflection of less than ±0.3°, which should be compensated completely. Optimization of the stabilization system resolution/bandwidth tradeoff should reduce the remaining oscillations, further improving the mean count rate.

Current Progress: Closing our QKD link requires a stabilization system that can compensate for the normal movements of the UAS during flight. Tabletop demonstrations of our stabilization scheme have shown that a single-photon signal can be reliably coupled into a multi-mode fiber on the receiver while transmitter rotations are applied externally (Fig 3). Our preliminary data shows that the stabilization system can handle slow oscillations up to ±0.5° which, according to our initial tests, is larger than the ±0.3° deflection introduced by the UAS while hovering.

Current work is focused on moving the stabilization hardware to the UAS platform to implement a complete BB84 protocol. Work on sources, analysis, and platform stabilization is ongoing. For the transmitter, we are developing a polarization-based BB84 protocol that uses R/L polarization for the information channel and only the H polarization for security checking. Spectrally filtered resonant-cavity light-emitting diodes operating at 650 nm will be used to generate the quantum photonic states as well as decoy states. These emitters can be modulated on the few nanosecond time scale and can be directly driven by a field-programmable gate array (FPGA). The receiver will use silicon avalanche photodiodes with custom-built, fast quench read-out and drive electronics. A FPGA will be used to time-tag the single-photon events and time synchronization across the platforms will be based on modulating the classical alignment and tracking beams.

This work is supported by the ONR MURI program on Wavelength-Agile Quantum Key Distribution in a Marine Environment, Grant #N00014-13-1-0627.

References

[1] S. Hammel. Turbulence effects on laser propagation in a marine environment. In Proc. SPIE 6708, Atmospheric Optics: Models, Measurements, and Target-in-the-Loop Propagation, 670804, volume 6708, pages 670804–670804–10, 2007.

[2] Kwiat, Paul G. and Gauthier, Daniel J., U.S. Patent Application No. 15/434,313 filed Feb. 16, 2017

[3] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, and D. Bitauld. Handheld free space quantum key distribution with dynamic motion compensation. Opt. Express, 25(6):6784–6795, Mar 2017.