1 Reviewer 1

The authors have addressed some of my concerns, but there are still serious questions have not been clarified yet.

1. In the response letter, the authors briefly analyze the restrictions about symmetric delay attack. However, the revised manuscript doesn't discuss about this question, which might lead the audience to misunderstand the true meaning of the security defending symmetric delay attack.

Ans: We have included an analysis (Section 5, line 150) that clarifies the symmetric delay attack that has been demonstrated with the present setup involved abruptly changing the channel length. We have also calculated the maximum speed v_{max} that the channel length can change continuously to be upper bounded by $50\,\mathrm{mms}^{-1}$ ($1\,\mathrm{mms}^{-1}$) for the single (round)-trip time of the channel, so that the round-trip time can be measured to the desired precision of 14 ps (Section 3, line 100).

2. The authors also claim that this clock synchronization system has the potential to defend the intercept, delay and resend attacks due to the entanglement of photons. In my view, the feasibility of realizing this type of security has not been clearly verified due to lack of theoretical analysis or experimental verification.

Ans: A rigorous quantitative study on the degree of synchronization inaccuracy that an adversary can impose before being successfully detected by a Bell measurement, remains the subject of further work. Nonetheless, we maintain that the synchronization protocol has the potential to defend against intercept, delay and resend attacks as compared to classical protocols as the quantum no-cloning theorem precludes producing an exact copy of a detected photon, so that the copied photon can be resent with an arbitrary delay. To our knowledge, there is no theory in classical physics that provides the same protection to signal spoofing as the quantum no-cloning theorem. We updated the manuscript to highlight the relation of the quantum no-cloning theorem against intercept, delay and resend attacks in Section 6, line 169.

3. Moreover, this work seems to be a simplification of previous work in Ref. 6, which may be too specialized to appeal to the broad audience of Optics Express. Thus, suggesting that a more specialized journal could be a better avenue. In conclusion, I still cannot recommend the current version of the paper for publication in Optics Express.

Ans: While this work appears to achieve the same synchronization goals as Ref. 6 with less resources, it does so by implementing an optical time-domain reflectometry (OTDR) measurement for the round-trip time, achieved with a time-correlated pair source. To our knowledge, our work represents a novel application of OTDR at the single-photon level, and we believe that it will be interesting to an audience outside of the clock synchronization community, such as those who deploy similar techniques for quantum LIDAR applications [1-2].

2 Reviewer 2

I thank the authors for revising the manuscript, and I agree with the authors' point that the discrepancy between the measured offsets δ of different lengths in Fig. 5 (a) may come from the accuracy of the timestamp unit. Such interpretation or the specification of the timestamp unit related with the offset measurement given in the article would be more convincing. I recommend its publication.

Ans: We thank the reviewer for his recommendation. We have inserted at the end of Section 4 that provides the interpretation that the discrepancy between measured offsets might come from the accuracy of the timestamp units.

3 Summary of changes

1. Section 4: added:

As the mean offset values do not appear to correlate with L, we do not attribute the differences between the mean offset values to any length-dependent mechanism. We observe however, in Fig. 5(a), that the offsets measured changed continuously and gradually even when L was changed abruptly during the the symmetric delay attack. Given these observations, and given that both timestamp units were disciplined to the same Rubidium oscillator over the entire measurement duration in Fig. 5, it is plausible that the remaining continuous offset drift can be attributed to the long-term instability of the timestamp units; the timestamp unit accuracy fluctuates due to the non-uniformity of implementing timestamping bin-widths, and varies as a function of operation time and temperature.

2. Section 5: added:

The symmetric channel delay attack demonstrated in this work abruptly changed the channel length, and is similar to the attacks demonstrated in Refs.[6,7,19]. For scenarios where the channel delay is changing continuously in time, our protocol is robust against small length changes due to thermal fluctuations or mechanical vibrations. To extract the peak positions of the cross-correlation and auto-correlation distributions, we need to remain in the pseudo-stationary regime where we require that the peaks do not shift significantly compared to their widths. The upper bound to the rate v at which the channel length changes is determined by two inequalities: $\frac{vT_a^{AB}}{u} + \sqrt{2}d_0T_a^{AB} < \mathrm{FWHM}^{AB}$ and $2\frac{vT_a^{AA}}{u} < \mathrm{FWHM}^{AA}$, where T_a^{AB}, FWHM^{AB} and $\frac{vT_a^{AB}}{u}$ (T_a^{AA}, FWHM^{AA} and $2\frac{vT_a^{AA}}{u}$) is the acquisition time, width and timing-shift of the cross (auto)-correlation coincidence peak, $\sqrt{2}d_0T_a^{AB}$ the timing-shift due to the relative frequency inaccuracy between the clocks, and $u = 2.04 \times 10^8\,\mathrm{ms}^{-1}$ the speed of 1316 nm photons in the SMF28e fibre. Substituting the values of $\mathrm{FWHM}^{AB} = 905\,\mathrm{ps}$, $\mathrm{FWHM}^{AA} = 950\,\mathrm{ps}$, $T_a^{AB} = 3\,s$ and $T_a^{AA} = 90\,\mathrm{s}$, we obtain an upper bound of $v_{max} \approx 50\,\mathrm{mms}^{-1}$ and $1\,\mathrm{mms}^{-1}$ for measuring the single and round-trip times. We note that this upper bound increases with reduced acquisition times, at the expense of synchronization precision.

3. Section 6 line 172: removed: "However, due to the low coincidence to accidental

ratio..." and replaced it with "Due to the low coincidence to accidental ratio..." in line 176.

4. Section 6: added:

Presently, classical protocols are unable to authenticate a synchronization signal that has been delayed during an intercept, delay and resend attack when the resent signal has the same cryptographic characteristics as that of the genuine signal [5]. However, when entangled photons are used for synchronization, the same attack will, in-principle, degrade the distributed entanglement and alter the associated Bell measurement. This is a consequence of the quantum no-cloning theorem, which precludes an adversary from making an exact copy of the polarization state of the intercepted photon [20].

5. References: updated Ref. [7] from: Hou, R. Dong, R. Quan, X. Xiang, T. Liu, X. Yang, H. Li, L. You, Z. Wang, and S. Zhang, "Fiber-optic quantum two-way time transfer with frequency entangled pulses," arXiv preprint arXiv:1812.10077 (2018).

to: F. Hou, R. Quan, R. Dong, X. Xiang, B. Li, T. Liu, X. Yang, H. Li, L. You, Z. Wang et al., "Fiber-optic two-way quantum time transfer with frequency-entangled pulses," Phys. Rev. A 100, 023849 (2019).

6. References: added Ref. [20]: W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature 299, 802–803 (1982).

References

[1] Han Liu, Daniel Giovannini, Haoyu He, Duncan England, Benjamin J. Sussman, Bhashyam Balaji, and Amr S. Helmy, "Enhancing LIDAR performance metrics using continuous-wave photon-pair sources," Optica 6, 1349-1355 (2019)

[2] Peng Kian Tan, Xi Jie Yeo, Li Jiong Shen, Christian Kurtsiefer, "Quantum lidar using stationary broadband light," Proc. SPIE 11868, Emerging Imaging and Sensing Technologies for Security and Defence VI, 1186807 (2021)