An asymmetric channel attack monitoring method for round-trip fiber time synchronization system

Xuesong Xu[1], Yichen Zhang[1*], Hailong Xu[1], Yiming Bian[1], Yang Li[2], Bingjie Xu[2], Song Yu[1]
[1] State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China
E-mail: *zhangyc@bupt.edu.cn

***Abstract*—We present a method for monitoring potential asymmetric channel attacks within a round-trip fiber time synchronization system. This is achieved by observing and tracking the time difference at the remote end. Experimental results show that the attacking operation causes unavoidably obvious fluctuations in time difference, with the time difference measured by our monitoring module changing by nanoseconds when an attack occurs, which can be used for attack recognition. Our work provides a reference for further improving the security of fiber time synchronization systems and lays the foundation for the development of more advanced time synchronization attack identification techniques.**

Keywords—round-trip time synchronization; asymmetric channel attack; attack monitoring

I. INTRODUCTION

With the development of high-precision time comparison technology, the accuracy of atomic clocks can reach 10^{-18} orders of magnitude [1-5]. However, high-performance atomic clocks are complex in structure and large in size, and mainly serve scientific research institutions, which is not conducive to wide-scale use. With the rapid development of fiber communication networks in recent years, fiber transmission has the advantages of low signal loss, better stability and long transmission distance, so it has a broad prospect in high-precision time and frequency transmission technology. In view of the potential of optical fiber time synchronization technology in realizing high-precision time-frequency transmission, in-depth study and strengthening of its security measures are of great significance in guaranteeing the reliability and stability of the relevant system [6-8].

Recently, there has been an asymmetric time delay attack scheme that is capable of massively degrading the synchronization accuracy of the system, which is based on the symmetry assumption of fiber time synchronization systems, where the attacker introduces additional asymmetric time delays that cannot be detected by the synchronization system. Therefore, without security measures, the additional asymmetric delay can significantly degrade the performance of round-trip fiber time synchronization systems, as has been experimentally demonstrated [9,10].

In this paper, we propose a method that can detect asymmetric delay attacks and design a corresponding monitoring module. Experimental results show that the time difference measured by this monitoring module changes by ns magnitude when accessing an attack. Our work can further improve the security of the round-trip fiber time synchronization system.

II. SYSTEM CONFIGURATION

The classical round-trip fiber time synchronization system is shown in Fig. 1. A digital pulse generator (DG645) loads pulse-per-second (PPS) signals onto the light by means of an amplitude modulator, which is then transmitted to the remote end via 40 km optical fiber spool. In this case, a part of the signal received at the remote end is sent back to the local end through the beam splitter and circulator for round-trip time, and the other part goes to the monitoring module. The monitoring module we designed consists of a photodetector (PD), which converts the optical signal into an electrical signal, and a time

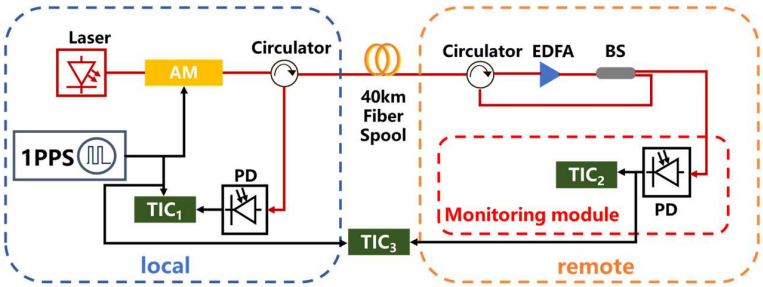

Fig. 1. Experimental setup of practical system. AM: amplitude modulation; EDFA: erbium doped fiber amplifier; BS: beam splitter; PD: photo detector; TIC: time interval counter. Where TIC_1 is the round-trip time of the system, TIC_2 refers to the time difference measured by the monitoring module, and TIC_3 indicates the synchronization accuracy of the system.

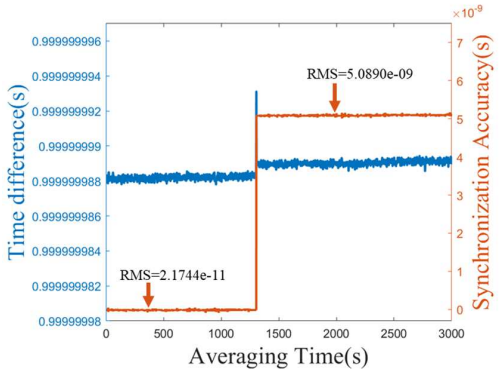

Fig. 2. Measured monitoring time difference and synchronization accuracy. The attack module can reduce the system synchronization accuracy to 5.09 ns, and after accessing it, the remote monitoring time difference will suddenly change by 4.77 ns.

interval counter (TIC), which measures and stores the received time signal.

In a conventional round-trip time synchronization system, the round-trip time of the system, TIC_1, is the pulse time difference between the digital pulse generator and the PD at the local end. A monitoring module is set up at the remote end of the system to measure the time difference between the rising edges of the Nth and (N+1)th PPS signal, which is recorded as TIC_2. In the link, there is a time difference of μ between the DG645 and the PPS signal received at the remote end, and the system at the local end digitally compensates for this time difference, so that the transmitted signals are delayed by 1-μ, and the Nth PPS signal at the sending end will be aligned with the (N+1)th PPS signal at the remote end, thus achieving time synchronization between the round-trip systems. At the same time, the monitoring module at the remote end measures the time difference between the rising edges of two neighboring arriving PPSs and stores it. Since the transmitter sends pulses every 1 s, TIC_2 is maintained at a relatively stable value around 1 s when the link is not under attack, and the error of the long-time measurements fluctuates in the sub-nanosecond order of magnitude.

The asymmetric time delay attack is an intrusive attack, which is achieved by accessing the corresponding attack module in the fiber link of the system. The attack module causes the length of the forward and backward fiber links to change by an amount of $\pm\Delta$ respectively, but the total round-trip length remains unchanged, resulting in an error in the compensated time delay μ at the local end, which leads to a degradation of the synchronization accuracy. For intuitive understanding, we additionally measure the synchronization accuracy between the local end and the remote end, denoted as TIC_3, where the amount of change under attack in TIC_3 is as follows:

$$\tau = \frac{\Delta}{3\times10^8/1.5} = \frac{\Delta}{2\times10^8}$$

When an asymmetric delay attack on the order of nanoseconds and above is introduced in the fiber link, the time transfer in the forward fiber link introduces an additional delay τ. At this point, the time difference between adjacent pulses arriving at the remote end becomes $1+\tau$, and therefore the time difference detected by the monitoring module before and after the attack will have a jump.

III. EXPERIMENTAL RESULTS AND CONCLUSIONS

The monitored time difference and the synchronization accuracy of the system are shown in Fig. 2. Here we have used an optical switch and a beam splitter to control the access of the attack module to the link. When there is no attack, the value measured by the monitoring module stays around 1 s (with a difference of 11.4 ps from 1 s), and the synchronization accuracy is maintained at 21.74 ps. When we access an attack module with Δ = 1 m, the synchronization accuracy drops to 5.09 ns, and the time difference measured by the monitoring module suddenly change by approximately 4.77 ns.

The proposed method emphasizes the detection of abnormal changes at the beginning of the attack. Experimental results have shown that this method can find the changes caused by asymmetric attacks, further improving the security of the round-trip fiber time synchronization system.

ACKNOWLEDGEMENTS

This research was supported by the Equipment Advance Research Field Foundation (315067206), the National Natural Science Foundation of China (62001044), the Basic Research Program of China (JCKY2021210B059), and the Fund of State Key Laboratory of Information Photonics and Optical Communications (IPOC2021ZT02).

REFERENCES

[1] N. Hinkley, J. A. Sherman, N. B. Phillips, M. Schioppo, N. D. Lemke, K. Beloy, M. Pizzocaro, C. W. Oates, and A. D. Ludlow, "An atomic clock with 10^{-18} instability," Science, vol. 341, no. 6151, pp. 1215–1218, 2013.

[2] T. L. Nicholson, S. Campbell, R. Hutson, G. E. Marti, B. Bloom, R. L. McNally, W. Zhang, M. Barrett, M. S. Safronova, G. Strouse, et al., "Systematic evaluation of an atomic clock at 2×10^{-18} total uncertainty," Nature communications, vol. 6, no. 1, pp. 1–8, 2015.

[3] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik, and P. O. Schmidt, "Optical atomic clocks," Reviews of Modern Physics, vol. 87, no. 2, p. 637, 2015.

[4] F. Riehle, "Optical clock networks," Nature Photonics, vol. 11, no. 1, pp. 25–31, 2017.

[5] W. McGrew, X. Zhang, R. Fasano, S. Schäffer, K. Beloy, D. Nicolodi, R. Brown, N. Hinkley, G. Milani, M. Schioppo, et al., "Atomic clock performance enabling geodesy below the centimetre level," Nature, vol. 564, no. 7734, pp. 87–90, 2018.

[6] D. Marcuse, "Principles of optical fiber measurements." 2012.

[7] M. Rost, D. Piester, W. Yang, T. Feldmann, T. Wübbena, and A. Bauch, "Time transfer through optical fibres over a distance of 73 km with an uncertainty below 100 ps," Metrologia, vol. 49, no. 6, p. 772, 2012.

[8] H. Zhang, G. Wu, L. Hu, X. Li, and J. Chen, "High-precision time transfer over 2000-km fiber link," IEEE Photonics Journal, vol. 7, no. 6, pp. 1–9, 2015.

[9] Z. Liu, Y. Bian, Y. Zhang, B. Xu, Y. Li, and S. Yu, "Asymmetric channel attack against practical round-trip fiber time synchronization system," in 2022 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), pp. 1–3, IEEE, 2022.

[10] X. Xu, Y. Zhang, Y. Bian, J. Hu, J. Dou, Y. Li, B. Xu, S. Yu, and H. Guo, "Controllable asymmetric attack against practical round-trip fiber time synchronization systems," IEEE Photonics Technology Letters, vol. 35, no. 23, pp. 1263–1266, 2023.