Controllable Asymmetric Attack Against Practical Round-Trip Fiber Time Synchronization System

Xuesong Xu[1], Yiming Bian[1], Jinlong Hu[2], Jiayi Dou[1], Yang Li[2], Bingjie Xu[2], Yichen Zhang[1*], Song Yu[1], Hong Guo[3]

[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

[3] State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China

E-mail: *zhangyc@bupt.edu.cn

***Abstract*—Using optical fiber links to transmit time information is widely regarded as an accurate and secure time synchronization scheme. However, the accuracy of the round-trip time synchronization system can be manipulated arbitrarily by attack schemes. In this paper, a controllable asymmetric attack scheme against round-trip time synchronization system is proposed and experimentally demonstrated. By adjusting the asymmetry of the link, the time synchronization accuracy can be controlled down from 23 ps to 0.91 ns, 2.13 ns and 5.20 ns. Our work reveals system vulnerability caused by asymmetry, and points out that current systems can be attacked unwittingly by adversaries.**

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

I. INTRODUCTION

Precise clock synchronization is increasingly required in both scientific measurements and daily applications, such as metrology, navigation, and communication networks. In recent years, new time synchronization schemes prove that fiber time transmission systems can achieve high time synchronization precision [1-3], which are widely regarded as accurate and secure time synchronization schemes. However, fiber transmission systems are implemented based on the assumption of symmetrical links, which can be exploited maliciously [4], allowing the synchronization accuracy to be artificially manipulated [5, 6].

Here, we propose a controllable asymmetric attack scheme against round-trip time synchronization system, which is carried out by introducing asymmetry to the fiber link. This attack can cause significant time asynchrony in the system and it is difficult to be detected in realistic scenarios, since the round-trip time remains constant, and it is the only time delay monitored in time transmission systems. Moreover, such attacks are controllable, as their effectiveness can be controlled by accessing various attack modules.

In this paper, we theoretically analyze and experimentally demonstrate this attack. The experimental results show that the original system accuracy of 23 ps can be reduced to 0.91 ns, 2.13 ns and 5.20 ns. The work in this paper reveals that this attack scheme breaks the assumption of channel symmetry in practical applications.

II. THE CONTROLLABLE ATTACK IN PRACTICAL SYSTEM

The round-trip fiber time synchronization system is shown in Fig. 1. The light output from the laser enters the amplitude modulator. DG645 outputs pulse per second (PPS) signal to the

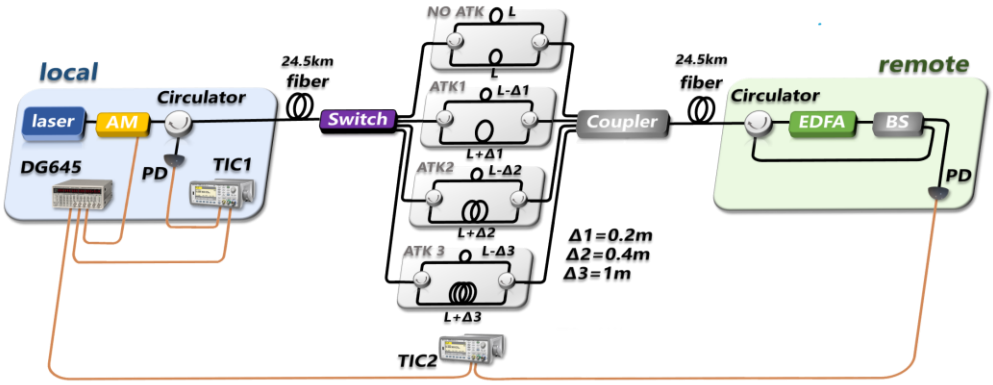

Fig. 1. Practical round-trip fiber time synchronization system. AM: amplitude modulator; EDFA: erbium doped fiber amplifier; PD: photo detector; BS: beam splitter; TIC: time interval counter. Four modules are connected between the optical switch and the BS, allowing the link to access different attack modules through the optical switch, where No ATK refers to the symmetric module without attack effect. In the asymmetric attack module, two circulators are used to change the length of the fiber link, where the length of the forward link of the nth attack module is $L-\Delta n$, and the length of the backward link is $L+\Delta n$, while the total length of the fiber link is always $2L$.

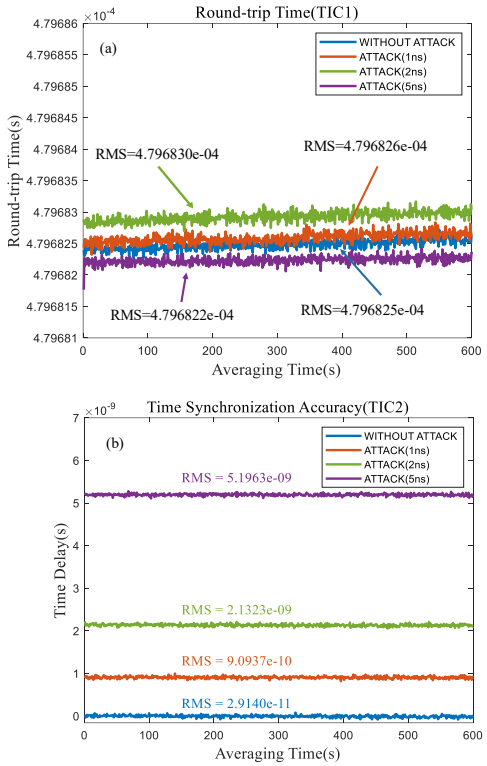

Fig. 2. Measured transfer delay and round-trip time of 49 km round-trip fiber time synchronization system. The blue line represents the system with no attack. The orange, green and purple lines represent the attack modules with transmission delays of 1 ns, 2 ns and 5 ns respectively connected to the system. (a) Round-trip time. (b) System accuracy.

modulator to apply time information to the light. Then the modulated signal enters the fiber and travels to the remote end. The signal received at the remote end enters the beam splitter, where the beam splitter splits the signal into two paths. 10 % of the output optical power is converted into an electrical signal on the photo detector (PD), while the other optical signal is sent back to the local end.

In a practical system, the round-trip time (TIC1) is obtained by comparing the PPS signal between the DG645 and the local PD. To show the effect of the attack well, we also measure the time difference between the local end and the remote end, known as synchronization accuracy, and it is denoted by TIC2.

$$TIC2 = \frac{TIC1}{2} + \frac{T_{L1} - T_{L2}}{2} + T_{asy} \quad (1)$$

Here, T_{L1} (T_{L2}) is the transmission delay from the local (remote) end to the remote (local) end, and T_{asy} is the delay of the devices in the system, which can be offset by pre-compensation.

In general, the optical fiber link of the system is symmetrical ($T_{L1} = T_{L2}$). In this case, if the local signal is delayed by (1-TIC2), time synchronization between the local end and the remote end will be achieved.

However, if the length of forward link decreases by Δ, and the length of backward link increases by Δ, the measured transfer delay changes ($T_{L1} \neq T_{L2}$), where the amount of change in TIC2 is $\tau = \Delta/(3 \times 10^8/1.5)$. The attack module uses two circulators to insert a piece of optical fiber in each forward and backward links, resulting in the length of the two links changing by Δ. The value of Δ differs for different attack modules.

We use the 1 × 4 optical switch to divide the optical fiber into four paths, which are connected to four modules respectively, and the ends of the four modules are connected with a beam splitter, so that they converge into one path. Thus, controlling the optical switch can achieve different effects on the optical fiber link attack.

III. EXPERIMENTAL RESULTS AND CONCLUSIONS

The round-trip time is shown in Fig. 2 (a). When the optical fibers are switched between different attack modules, the round-trip time hardly changes, indicating that the round-trip time cannot be used to determine whether an attack is occurring or not, so in actual scenarios, asymmetric attacks will not be detected.

Fig. 2 (b) shows the time delay between the remote ends and the local ends. Without asymmetric attack, the time synchronization accuracy is 23 ps, when we control the optical switch so that the fiber link is connected to a different attack module, the synchronization accuracy is reduced to 0.91 ns, 2.13 ns and 5.20 ns respectively, proving that even if the asymmetry of the transmission link changes slightly, the accuracy will be greatly reduced.

In conclusion, with the controllable asymmetric attack, the transmission accuracy of the system is greatly reduced. At the same time, the value of TIC1 remains unchanged, achieving a spoofing attack on the time synchronization system of the optical fiber link. Our work demonstrates the effectiveness of asymmetric attacks and provides a reference for future improvements in the security of time synchronization.

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] D. Piester et al., "Time transfer with nanosecond accuracy for the realization of International Atomic Time," Metrologia, vol. 45, no. 2, pp. 185-198, (2008).

[2] B. Wang et al., "Precise and continuous time and frequency synchronisation at the 5×10^{-19} accuracy level," Scientific Reports, vol. 2, pp. 556–560, (2012).

[3] J. Lin et al., "Michelson interferometer based phase demodulation for stable time transfer over 1556 km fiber links," Optics Express, vol. 29, no. 10, pp. 14505-14512, (2021).

[4] C. Zhang et al., "Controllable Asymmetry Attack on Two-Way Fiber Time Synchronization System," IEEE Photonics Journal, vol. 13, no. 6, pp. 1-6, (2021).

[5] Z. Liu et al., "Asymmetric Channel Attack Against Practical Round-Trip Fiber Time Synchronization System," 2022 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), pp. 1-3, (2022).

[6] Y Li et al., "Secure two-way fiber-optic time transfer against sub-ns asymmetric delay attack," arXiv. 2203. 03803, (2022).