

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

Xuesong Xu¹, Yichen Zhang^{1*}, Hailong Xu¹, Yiming Bian¹, Yang Li², Bingjie Xu², Song Yu¹

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

Email: zhangyc@bupt.edu.cn

In the round-trip fiber time synchronization system, asymmetric channel attacks will affect the synchronization accuracy of the system, but the synchronization accuracy is only monitored by the round-trip time of the local end, so the existence of asymmetric attacks cannot be detected¹. Considering the large impact of asymmetric attacks on system synchronization accuracy, attack detection is crucial for fiber time synchronization system. To address the above problem, we find a method to sense attacks on the round-trip system, which can detect the existence of asymmetric channel attacks by setting up a monitoring module at the remote end.

In our experiments, as shown in Fig. 1(a), we connect a 40-kilometer-long optical fiber to the system, and the synchronization accuracy can be stabilized at several tens of ps on average. The monitoring module is set at the remote end of the system to measure the time difference between the rising edges of two adjacent pulses, and the monitored time difference is stable at about 1 s. It can be found that the time difference of remote monitoring will suddenly change in the order of ns after accessing the attack module. The results are shown in Fig. 1(b).

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.

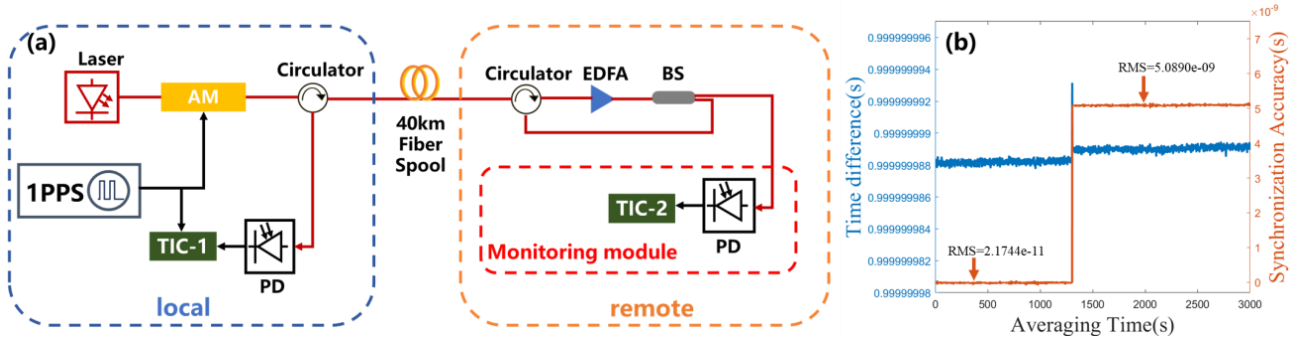


Fig. 1: (a) Experimental setup of practical system. AM: amplitude modulation; EDFA: erbium doped fiber amplifier; BS: beam splitter; PD: photo detector; TIC: time interval counter. (b) Measured monitoring time difference and synchronization accuracy. The attack module can reduce the system synchronization accuracy to 5.09 ns, and after accessing it, the remote monitoring time difference will suddenly change by 4.77 ns.

¹ X. Xu et al., "Controllable Asymmetric Attack Against Practical Round-Trip Fiber Time Synchronization Systems", J. IEEE Photon. Technol. Lett., vol. 35, no. 23, pp. 1263-1266, 1 Dec.1, 2023.