Controllable Asymmetry Attack on Two-Way Fiber Time Synchronization System

Chenlin Zhang, Yang Li, Xing Chen, Yichen Zhang, Lifeng Fu, Yuan Gong, Heng Wang, Wei Huang, and Bingjie Xu

***Abstract*—Precise and secure time synchronization between two remote sites is necessary in many practical scenarios. Recently, the two-way fiber time transfer (TWFTT) system has become an attractive option for high-precision time synchronization. However, TWFTT is implemented based on symmetric link assumption, and such assumption may be maliciously utilized to cause significant time asynchronization to TWFTT. In this paper, we propose two novel controllable asymmetry attack schemes for TWFTT, namely, the link asymmetry attack and the attenuation asymmetry attack. We theoretically analyze the controllability and the effectiveness of these two attacks. Experimental results show that our link asymmetry attack can introduce 2.49 ns time offset per asymmetric link length (in meters), and our attenuation asymmetry attack can introduce at most 36.6 times time offset (compared to normal situation) when the attenuation is 45.3%. Our work can provide instructive insights for future studies of protecting TWFTT from delay asymmetry attacks.**

***Index Terms*—Real-time systems, time measurement, communication system security.**

I. Introduction

PRECISE and secure time synchronization is widely used in many fields. For instance, in smart grid systems including transmission, distribution, controlling, and metering require time accuracy from 100ms to 1μs [1], [2]. In Internet of Things (IOT) and industrial applications, algorithms must have the precise sequence of the events [3], [4]. In energy sector, the time synchronization is needed to integrate various types of management techniques to achieve collaboration [5]. In submarine, time synchronization is the basis of sensor node cooperation [6]. In Vehicular Ad-hoc Networks (VANETs), network nodes must be synchronized to exchange time-critical vehicle locations and warning messages for various road safety applications [7].

Traditionally, the precision time protocol (PTP) and the network time protocol (NTP) achieve time synchronization through exchanging time messages between two nodes [8]–[10]. With the advances in modern atomic timekeeping technology [11]–[13], some new time synchronization schemes achieve ultra-high time synchronization precision through measuring optical signal intervals [14], [15]. Among them, Two-Way Fiber Time Transfer (TWFTT) has the highest time synchronization precision because it transmits time information with optical signals from two directions [15]. As a result, the synchronization precision of TWFTT can reach picoseconds, whereas the precision of NTP is milliseconds [8], and the precision of PTP is microseconds [9], [10].

Notably, most time synchronization protocols, including NTP, PTP, and TWFTT, rely on the assumption of symmetric propagation delay in both directions of the synchronization channel, i.e., they estimate the one-way packet transmission time as half of the round-trip time. However, the forward and backward delays of a transmission channel can be asymmetric due to deliberate attacks [16]–[18]. For NTP and PTP, attacks causing delay asymmetry have been intensively studied [18]–[20], and many solutions have been proposed [21]–[23]. But for TWFTT, how to perform delay asymmetry attack is still unclear, and thus no security method for delay asymmetry is ever proposed. This makes TWFTT highly vulnerable for delay attacks.

In this paper, we innovatively propose two delay asymmetry attacks against TWFTT, namely, link asymmetry attack and attenuation asymmetry attack, which can cause significant time asynchronization to TWFTT. More importantly, these two attacks are controllable, i.e., their attack effects can be controlled by adjusting variable optical delay line or variable optical attenuator. In addition, they are feasible in real-world scenarios, because they can be easily conducted through extracting, manipulating, and injecting of the optical signals of the transmission fiber link, which are consistent with the security issues of modern optical fiber communication networks [24]–[26]. The goal of this paper is to reveal the vulnerabilities of TWFTT under delay asymmetry attacks, and thereby to provide instructive insights for future studies of protecting TWFTT from delay asymmetry attacks.

The contributions of this paper are two-folds. First, we analyze the principle of the asymmetry attack, and give the quantitative

Manuscript received September 15, 2021; accepted October 18, 2021. Date of publication October 20, 2021; date of current version November 2, 2021. This work was supported in part by the National Natural Science Foundation of China under Grants U19A2076, 61771439, 61702469 and 61901425, in part by the Sichuan Application and Basic Research Funds under Grants 2021YJ0313, 2020YJ0482, and in part by the Sichuan Science and Technology Program under Grant 2019JDJQ0060. *(Corresponding author: Bingjie Xu.)*

Chenlin Zhang, Yang Li, Lifeng Fu, Heng Wang, Wei Huang, and Bingjie Xu are with the Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China (e-mail: charlene99@126.com; yishuihanly@pku.edu.cn; 1479815881@qq.com; wanghg1991@163.com; huangwei096505@aliyun.com; xbjpku@163.com).

Xing Chen and Yichen Zhang are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: starchengirl@163.com; zhangyc@bupt.edu.cn).

Yuan Gong is with the Key Lab of Optical Sensing and Communications (Ministry of Education), University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: ygong@uestc.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2021.3121569

TABLE I
DEFINITION OF VARIABLES

Variables	Definition
δ	The time offset of Bob relative to Alice.
δ_c	The time delay compensation adjusted by pulse delay control module on the Bob site.
$\Delta t_{A\to B}$ ($\Delta t_{B\to A}$)	The systematic delay of the 1 PPS signal from Alice (Bob) to Bob (Alice) including optical to electrical conversion delay, electrical to optical conversion delay, as well as electronics processing delay.
$\Delta \tau_{A\to B}$ ($\Delta \tau_{B\to A}$)	The propagation delay over the optical fiber from Alice (Bob) to Bob (Alice).
$\Delta\tau$	The asymmetric delay.
P	The period of time signal transfer.
T_A (T_B)	The time that the 1 PPS signal in Alice (Bob) triggers the TIC to start timing.
M_A (M_B)	The measurement of the TIC on the Alice (Bob) site.

description of the attack effect. Second, we design controllable asymmetry attack scheme, and examine the attack by introduce link asymmetry and attenuation asymmetry on the fiber of the TWFTT in experiment. The experimental results show that, the link asymmetry linearly controls the time offset of Bob relative to Alice with the coefficient of 0.51, and attenuation asymmetry introduces nanoseconds time offset when the attenuation is larger than 43.2% .

II. Analysis of Two-Way Fiber Time Synchronization System and Asymmetry Attack Scheme

A. Background of TWFTT

We briefly review the time synchronization protocol based on the two-way fiber time transfer (TWFTT) system [15]. The definition of variables is shown in Table 1. The protocol supposes that the clock frequency has been synchronous during the process of time synchronization. Alice has a precise atomic clock, and Bob tries to synchronize its clock to Alice's. They are connected by a single mode optical fiber. Periodically, Alice transfers a precise 1 PPS (Pulse Per Second) signal to Bob, and meanwhile, Bob transfers a local 1 PPS signal to Alice. The period of such signal exchange is P = 1 s. The time intervals of the two counter-propagated 1 PPS signals, namely, MA and MB, are measured by two time-interval counters (TIC, Agilent 53230 A) at both sides.

Consider that during the *i*-th period of time synchronization, The TIC on the Alice site gets the time interval $M_A(i)$, and the TIC on the Bob site gets the time interval $M_B(i)$. In addition, Alice sends the value of $M_A(i)$ to Bob after updating $M_A(i)$. The values of $M_A(i)$ and $M_B(i)$ can be described by

$$M_A(i) = [T_B(i) + \Delta t_{B\to A}(i) + \Delta\tau_{B\to A}(i)] - T_A(i) \quad (1)$$

$$M_B(i) = [T_A(i) + \Delta t_{A\to B}(i) + \Delta\tau_{A\to B}(i)] - T_B(i) \quad (2)$$

where $T_A(i)$ is the time that the 1 PPS signal on Alice triggers the TIC to start timing, $\Delta t_{A\to B}(i)$ is the inherent delay of the 1 PPS signal from Alice to Bob (including optical to electrical conversion delay, electrical to optical conversion delay, electronics processing delay, etc.), $\Delta\tau_{A\to B}(i)$ is the propagation delay over the optical fiber from Alice to Bob. $T_B(i)$, $\Delta t_{B\to A}(i)$ and $\Delta\tau_{B\to A}(i)$ are in reverse. Thus, the time offset between Alice and Bob, $\delta(i)$, can be expressed as

$$\begin{aligned}\delta(i) &= T_B(i) - T_A(i)\\ &= \frac{M_A(i) - M_B(i)}{2} + \frac{\Delta t_{A\to B}(i) - \Delta t_{B\to A}(i)}{2}\\ &\quad + \frac{\Delta\tau_{A\to B}(i) - \Delta\tau_{B\to A}(i)}{2}\end{aligned} \quad (3)$$

The first part $M_A(i)$ –$M_B(i)$ is the difference between the measured values of TIC on the Alice and Bob, which is variable due to the fluctuation of the unstable clock on the Bob site. The second part $\Delta t_{A\to B}(i)$ and $\Delta t_{B\to A}(i)$ represent the systematic delay between Alice and Bob including optical to electrical conversion delay, electrical to optical conversion delay, as well as electronics processing delay, which are constant and known. The third part $\Delta\tau_{A\to B}(i) - \Delta\tau_{B\to A}(i)$ is the delay gap between the forward propagation delay $\Delta\tau_{A\to B}(i)$ and the backward propagation delay $\Delta\tau_{B\to A}(i)$. In normal situations, the delay gap is constant which is introduced by the dispersion for different wavelength channels. As a result, the second part and third part are threat as constant (*C*), and Bob computes the delay compensation $\delta_c(i+1)$ as follows:

$$\delta_c(i+1) = \frac{M_B(i) - M_A(i)}{2} - C \quad (4)$$

Afterwards, Bob will set $\delta_c(i+1)$ to the Pulse Delay Control Module (PDCM) for the $(i+1)$-th period:

$$\begin{aligned}T_B(i+1) &= T_B(i) + \delta_c(i+1) + P\\ &= T_A(i) + \delta(i) + \delta_c(i+1) + P\\ &= T_A(i+1) + \delta_c(i+1) + \delta(i)\end{aligned} \quad (5)$$

B. Asymmetry Attack Scheme

If there is no attack during the *i*-th period, the delay compensation $\delta_c(i+1) = \delta(i)$. Henceforth, Eq. (5) becomes

$$\begin{aligned}T_B(i+1) &= T_A(i+1) + \delta_c(i+1) + \delta(i)\\ &= T_A(i+1)\end{aligned} \quad (6a)$$

which means the time between Alice and Bob is synchronized at the $(i+1)$-th repetition.

On the other hand, if an attacker can increase an asymmetric delay $\Delta\tau$ whose plus or minus represents the delay applying on the forward propagation or the backward propagation during the *i*-th period, the delay gap $\Delta\tau_{A\to B}(i) - \Delta\tau_{B\to A}(i)$ can no longer be ignored. As a result, Eq. (5) becomes

$$\begin{aligned}T_B(i+1) &= T_A(i+1) + \delta(i) + \delta_c(i+1)\\ &= T_A(i+1) + \frac{\Delta\tau_{A\to B} - \Delta\tau_{B\to A}}{2}\\ &= T_A(i+1) + \frac{\Delta\tau}{2}\end{aligned} \quad (6b)$$

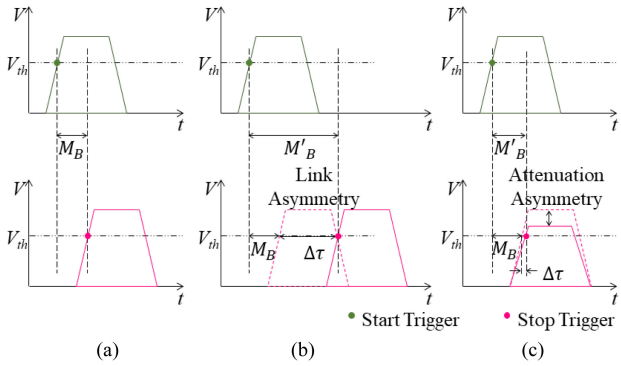

Fig. 1. The principle of controllable asymmetry attack by increasing the link asymmetry or the attenuation asymmetry. The green line and pink line are two 1PPS signals which arrive at TIC as the start trigger and stop trigger of TIC, respectively. (a) No attack; (b) Link asymmetry; (c) Attenuation asymmetry. V_{th}: the threshold voltage of TIC; M_B: the measurement of TIC without attack; M'_B: the measurement of TIC with attack; $\Delta\tau$: the asymmetric delay introduced by link asymmetry or attenuation asymmetry.

Note that there is a time offset between Alice and Bob at the $(i+1)$-th period, which can be derived from Eq.(6b) as

$$\delta(i+1) = T_B(i+1) - T_A(i+1) = \frac{\Delta\tau}{2} \tag{7}$$

Therefore, the asymmetric delay $\Delta\tau$ caused by the attacker during the i-th period will cause direct influences to the time offset $\delta(i+1)$ during the $(i+1)$-th period.

Based on (6b) and (7), we propose a controllable asymmetry attack scheme against TWFTT system. Specifically, by imposing asymmetric delay $\Delta\tau$ on the fiber link, an attacker can increase time offset δ by $\Delta\tau/2$ between Alice and Bob, i.e., time asynchronization between Alice and Bob. Moreover, the attacker can precisely control such time offset δ through changing the forward propagation delay $\Delta\tau_{A\to B}$ or the backward propagation delay $\Delta\tau_{B\to A}$.

In practice, the asymmetric delay can be achieved by increasing the link asymmetry or the attenuation asymmetry on the fiber channel. In Fig. 1, we take the direction Alice to Bob as an example to illustrate the principle. In Fig. 1(a), when there is no attack, the measurement of TIC on the Bob site is M_B. In Fig. 1(b), when there is link asymmetry, the time that the stop trigger arrives at the TIC on the Bob site is prolonged, which directly increases the measurement of TIC from M_B to M'_B. In Fig. 1(c), when there is attenuation asymmetry,1PPS has a smoother rising edge and thus requires more time to reach the measurement threshold V_{th}, which indirectly increases the measurement of TIC from M_B to M'_B. More details about these two attacks will be studied in the next section.

III. Experimental Demonstration of Asymmetry Attacks

The experimental setup of controllable asymmetry attack based on TWFTT system is shown in Fig. 2. The time synchronization mechanism of TWFTT is set according to Ref. [15]. On the Alice site, the 1 PPS signal generated from the atomic clock (Quartzlock A1000) is used as the trigger to the synchronization

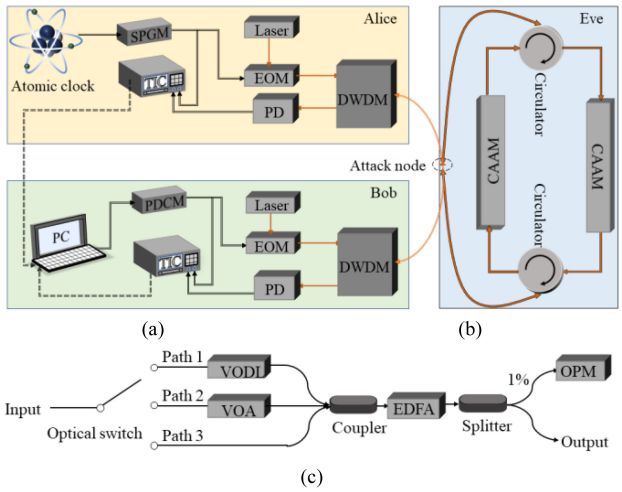

Fig. 2. Experimental setup of controllable asymmetry attack based on TWFTT system. (a) Experimental setup of TWFTT. (b) Experimental setup of the Eve site. SPGM: synchronization pulse generation module; (c) The internal structure of CAAM; TIC: time interval counter; EOM: electro-optic modulator; TIC: time interval counter; PD: photo detector; PDCM: pulse delay control module; DWDM: dense wavelength division multiplexing; PC: personal computer; CAAM: controllable asymmetry attack module; VODL: variable optical delay line; VOA: variable optical attenuator; EDFA: erbium doped optical fiber amplifier; OPM: optical power meter.

pulse generation module (SPGM) which is digital delay/pulse generator (SRS DG645) in the experiment. A part of the output of SPGM drives an electro-optic modulator (EOM) to modulate a CW laser, and the other part drives a time interval counter (TIC) as the start trigger. The output of EOM is coupled to one of the channels of the DWDM, and transfers to photo detector on the Bob site. The detected signal drives Bob's TIC as the stop trigger. On the Bob site, the 1 PPS signal generated from pulse delay control module (PDCM) transfers to Alice through the process as the description above. The time offset is obtained by comparing the time intervals of the two TICs, and is sent to PDCM for resetting the time delay. After that, the time is synchronous between Alice site and Bob site. Eve may introduce the controllable asymmetry attack module by separating the two propagation directions in the optical fiber with a pair of circulators.

As shown in Fig. 2(b), a pair of controllable asymmetry attack modules (CAAM) is used to change the symmetry of the transmission channel. The internal structure of CAAM is shown in Fig. 2(c). The CAAM is composed of three parallel paths with a 1*3 optical switch. Path 1 is composed of a variable optical delay line (VODL), which is used to control the link asymmetry. Path 2 is composed of variable optical attenuator (VOA), which is used to control the attenuation asymmetry. Path 3 is vacant. The optical laser is coupled with a 3*1 coupler, amplified by an erbium doped optical fiber amplifier (EDFA), and 1% of the amplified laser is detected by optical power meter with the help of a 1:99 splitter. We can separately study the link asymmetry and attenuation asymmetry by switching the path. The EDFA is used to compensate the attenuation caused by CAAM, including inherent attenuation caused by device and variable attenuation caused by VODL. The compensation of EDFA is determined by OPM. In CAAM, because the length

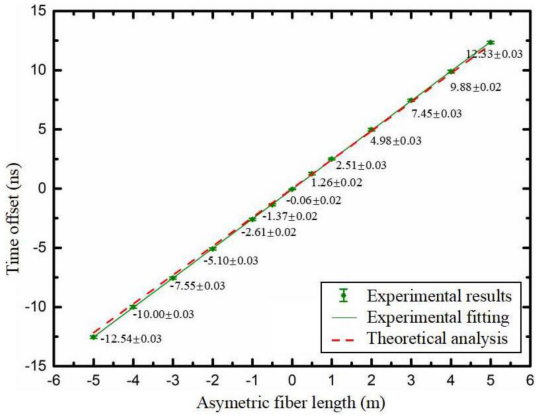

Fig. 3. Experimental results of asymmetric delay attack by setting the asymmetric fiber length as -5 m $\sim$ 5 m. The green point and bar are the average and the fluctuation range of different asymmetric delay, respectively. The green line is the linear fitting of the experimental results with the slope of 2.49. The red dot line is the theoretical analysis with the slope of 2.42.

variation of the variable optical delay line is less than 10m, and the difference of wavelength in DWDM is only 0.8nm, the delay of dispersion on different wavelength is less than 0.01ps (much less than the accuracy of detection equipment in TWFTT, which is around 0.1 ns).

A. Link Asymmetry

For link asymmetry attack, the asymmetry delay $\Delta\tau$ is controlled based on $\Delta\tau = (\Delta L_{A\to B}$ - $\Delta L_{B\to A})$ / v, where $\Delta L_{A\to B}$ and $\Delta L_{B\to A}$ are the directional attack induced by VODL, and v is the speed of light in fiber. We test the asymmetric delay attack results by setting the asymmetric fiber length ($\Delta L = \Delta L_{AB}$ - ΔL_{BA}) as $\pm$0.5 m, $\pm$1 m, $\pm$2 m, $\pm$3 m, $\pm$4 m, and $\pm$5 m. The experimental result is shown in Fig. 3. The green point and bar are the average and the fluctuation range of experimental $\Delta\tau$ for each attack. The red dot line is the theoretical results based on Eq. (7) with the slope of 2.42 ns/m. According to the experimental results, the link asymmetry attack can linearly introduce time offset with asymmetric link length. Specifically, the time offset increases linearly with the asymmetric fiber length, and the fitting curve can be described by $\delta = 2.49^{*}\Delta L$ or $\delta = 0.51^{*}\Delta\tau$.

Theoretically, the upper bound of the link asymmetry can reach to about 1s, and the lower bound is limited by the precision of the TWFTT. The link asymmetry can be boundless increased with the support of hardware (i.e., variable optical delay line, VODL). However, the TWFTT calculates the time delay compensation (i.e., δ_c) with a pair of measurements (M_A and M_B) for each period (i.e., 1s). If the link asymmetry exceeds 1s - max(M_A, M_B), where max(M_A, M_B) means the maximum of M_A and M_B, the TWFTT will crash due to the absence of M_A or M_B. As the precision of TWFTT is reach to 0.1 ns, and max(M_A, M_B) is about 50.572 μm, the boundary of link asymmetry ($\Delta\tau$) is

$$0.2ns < \Delta\tau < 1s - \max(M_A, M_B) \approx 1s \qquad (9)$$

We further analyze the variation of time interval counters (M_A and M_B) with the experimental results of the TWFTT system under the link asymmetry. Fig. 4 shows the variations of M_A and

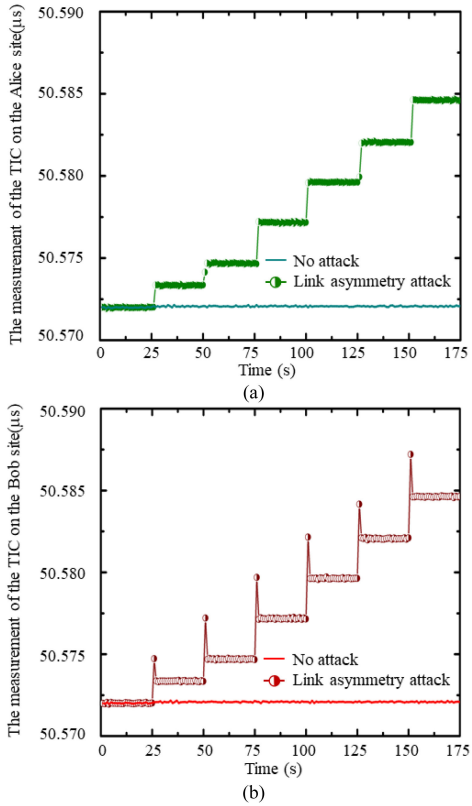

Fig. 4. The variations of time interval counters with link asymmetry when ΔL is 0, 0.5 m, 1.0 m, 2.0 m, 3.0 m, 4.0 m, and 5.0 m. The X axis is the time of measurement. The Y axis is the measurement of the TIC on each site. (a) The variations of M_A which is the reading of the time interval counter on the Alice site; (b) The variations of M_B which is the reading of the time interval counter on the Bob site.

M_B with ΔL of 0, 0.5 m, 1.0 m, 2.0 m, 3.0 m, 4.0 m, and 5.0 m by increasing ΔL every 25 s. When the link asymmetry introduces asymmetric delay $\Delta\tau$, M_A will increase $\Delta\tau$ /2 during the next period, and be stable with the same link asymmetry, as Fig. 4(a) illustrates. But for M_B, it will increase $\Delta\tau$ when the attack occurs, and will decrease $\Delta\tau$ /2 in the next period, causing the spikes of M_B in Fig. 4(b). More specifically, the measured TICs on both site (M_A and M_B) consists of two parts, i.e., the difference of the standard time ($T_B - T_A$ for M_A and $T_A - T_B$ for M_B), and the one-way delay (i.e., $\Delta t_{B\to A}(i) + \Delta\tau_{B\to A}(i)$ for M_A and $\Delta t_{A\to B}(i) + \Delta\tau_{A\to B}(i)$ for M_B). When link asymmetry introduces asymmetric delay $\Delta\tau$, M_B increases $\Delta\tau$ because of the increasing one-way delay from Alice to Bob, causing sudden rise of M_B to a spike. However, Bob believes the increased M_B is due to the increased difference of the standard time [15]. Hence, Bob will increase its local standard time (T_B) for recalibration, which not only decreases M_B by $\Delta\tau$ /2 from a spike, but also makes M_A increase by $\Delta\tau$ /2. We get similar experimental results for negative $\Delta\tau$, except that the spikes appear in M_A.

B. Attenuation Asymmetry

For attenuation asymmetry attack, the asymmetric attenuation $\Delta\alpha$ is controlled by VOA. We test the attenuation asymmetry attack results by setting $\Delta\alpha$ as 0, 11.9%, 23.4%, 31.3%, 38.1%, 43.2%, 44.2%, and 45.3%. The threshold voltage of TIC in Bob

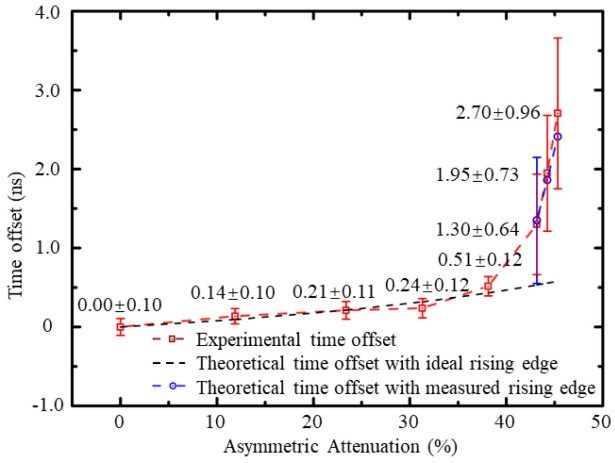

Fig. 5. Results of attenuation asymmetry by setting Asymmetric attenuation ($\Delta\alpha$) as 0, 11.9%, 23.4%, 31.3%, 38.1%, 43.2%, 44.2%, and 45.3%. The first red curve is the experimental results of the time offset δ, the second black curve is the theoretical δ with ideal rising edge, and the third blue curve is the theoretical δ with measured rising edge. The X axis is the value of attenuation asymmetry introduce to the TWFTT system. The Y axis is the time offset introduced by the attenuation asymmetry attack.

is 56 mV, which is about half of the peak value. The results are shown in Fig. 5.

The first red curve in Fig. 5 illustrates the experimental result. The point and bar are the average and fluctuation range of experimental results δ, for each asymmetric attenuation attack. Observe that the attenuation asymmetry attack can introduce nanoseconds time offset (compared to normal situation) when the attenuation is 45.3%. Specifically, when $\Delta\alpha$ is from 0 to 38.1%, δ increases modest (0, 0.14 ns, 0.21 ns, 0.24 ns, and 0.51 ns), and the fluctuation ranges for each attack are about 0.10∼0.12 ns. When $\Delta\alpha$ is from 43.2% to 45.3%, δ increases significantly (1.30 ns, 1.95 ns and 2.70 ns), and the fluctuation ranges is larger. When $\Delta\alpha$ is 50.0%, the peak value of 1PPS becomes even lower than the threshold voltage of TIC in Bob, making TWFTT stop synchronizing time.

The second black curve in Fig. 5 illustrates the theoretical result with ideal rise edge of the 1PPS signal. Specifically, here we assume that the 1PPS signal is a standard rectangular wave. When asymmetric attenuation $\Delta\alpha$ is introduced, it is equal to introduce an attack delay $\Delta\tau$, which can be expressed as

$$\Delta\tau = k_{\Delta\alpha} \cdot \frac{\Delta\alpha}{1-\Delta\alpha} \tag{10}$$

where $k_{\Delta\alpha} = V_{th}/k$, and V_{th} is the threshold voltage of TIC in Bob site, k is the rising edge slop of the 1PPS signal without attack. In our experiment, $V_{th} = 56$ mv, $k = 39.5$ mv/ns, so $k_{\Delta\alpha} \approx 1.4$. The theoretical relation between time offset (δ) and attenuation asymmetry ($\Delta\alpha$) can be derived by substituting Eq. (10) into Eq. (7), which is

$$\delta(i+1) = \frac{\Delta\tau}{2} = 0.7 \times \frac{\Delta\alpha}{1-\Delta\alpha} \tag{11}$$

The theoretical analysis result based on Eq. (11) is shown in Fig. 5 with the black dot line. It is in good agreement with the experimental results when $\Delta\alpha$ is less than 38.1%, but much smaller when $\Delta\alpha$ is larger than 38.1%.

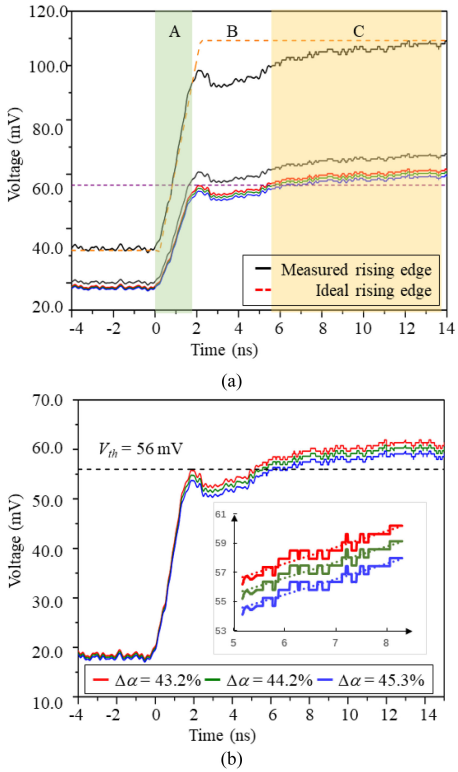

Fig. 6. The rising edge of the 1PPS signal in time domain at Bob site. The X axis is the time of measurement, where time = 0 ns is the arrival time of rising edge. The Y axis is the voltage measured by TIC. (a) The measured rising edge and the ideal rising edge (rising edge of rectangular wave) of the 1PPS signal; (b) Variations of the measured rising edge with different $\Delta\alpha$. Observe that when $\Delta\alpha$ is from 0 to 38.1%, the threshold voltage V_{th} is in area A. When $\Delta\alpha$ is 43.2%, V_{th} is just on the boundary of area B. When $\Delta\alpha$ is 44.2%, and 45.3%, V_{th} is in smooth area C.

Note that there is a gap between the experimental result and the theoretical result for $\Delta\alpha > 38.1\%$. We find that the gap is actually caused by the imperfect waveform of 1PPS signal, instead of our theoretical model in Section II(B) being flawed. Specifically, we measure the waveform of 1PPS signal at Bob site by oscilloscope, and draw the rising edge in Fig. 6. The measured and the ideal rising edge of 1PPS signal are shown in Fig. 6(a) with black line and red dot line, respectively. In area A, the measured rising edge is nearly linear, which is in good agreement with the ideal one. As a result, the theoretical δ calculated with Eq. (10) is very close to the experimental δ. In area B, the measured rising edge is a parabolic curve, which may grow beyond the voltage threshold V_{th} for multiple times and trigger the TIC to stop timing at multiple time points. Particularly, in the case of $\Delta\alpha = 43.2\%$, there are two time points that may trigger the TIC to stop timing, namely, 1.1 ns and 4.3 ns. This increases the measurement error of the stop time because the TIC will randomly select one of the multiple points as the stop trigger. In area C, the measured rising edge is nearly a flat line. This also increases the measurement error of the stop time because it is difficult to accurately measure the exact stop time when the rising edge is nearly flat. The measurement errors in area B and area C explain why there is a large gap between the experimental results and the theoretical results based on ideal rising edge.

Based on the above analysis, we use the measured rise edge in Fig. 6(a) to improve our theoretical result of attenuation asymmetry attack, and obtain the third curve in Fig. 5. When $\Delta\alpha$ is from 0 to 38.1%, the theoretical value of δ is the same as the second black curve, which can be calculated with Eq. (11). When $\Delta\alpha$ is 43.2%, there are two possible values of $\Delta\tau$. The smaller one is about 1.1 ns which is calculated by Eq. (11), and the larger one is about 4.3 ns by adding the area B width of about 3.2 ns. The corresponding theoretical value of δ is 0.55 ns and 2.15 ns, which can be expressed as $\delta = 1.35 \pm 0.80$ ns. When $\Delta\alpha$ is 44.2%, and 45.3%, the rising edge near V_{th} can be linearly fitted with a slope of 1.1 mv/ns. The coefficient of the determination (R^2) is 0.90. Then, we can describe the relation between $\Delta\tau$ with different $\Delta\alpha$ as:

$$\Delta\tau(\Delta\alpha_2) - \Delta\tau(\Delta\alpha_1) = \frac{V_0(1-\Delta\alpha_1)}{k'} - \frac{V_0(1-\Delta\alpha_2)}{k'} = \frac{V_0}{k'}(\Delta\alpha_2 - \Delta\alpha_1) \quad (12)$$

where $\Delta\tau(\Delta\alpha_i)$ is the extra delay introduced by asymmetric attenuation of $\Delta\alpha_\iota$, V_0 is the peak voltage which is 110.8 mV in the experiment, and k' is the slope of the fitting curve, which is 1.1. So, we can calculate the $\Delta\tau(44.2\%) = 3.71$ ns and $\Delta\tau(45.3\%) = 4.82$ ns according to $\Delta\tau(43.2\%) = 2.70$ ns. The corresponding theoretical δ is 1.86 ns and 2.41 ns.

At last, the boundary of the attenuation asymmetry can be expressed by

$$0 < \Delta\alpha < 1 - \frac{V_{th}}{V_0} \quad (13)$$

Where V_0 is the peak voltage of the 1PPS without attack, and V_{th} is the threshold voltage of TIC.

To derive the upper bound $1 - V_{th} / V_0$, note that the peak voltage of the 1PPS under the attenuation asymmetry attack (i.e., $V_0(1-\Delta\alpha)$) must be larger than the threshold voltage of TIC (i.e., V_{th}), because otherwise the 1PPS signal will be too weak to be recognized as the stop trigger by the TIC and the time synchronization process will be terminated, which will substantially decrease the stealthiness of the attack.

In addition, the attenuation asymmetry, $\Delta\alpha$, is achieved by attenuator, which can only decrease the strength of the 1PPS signal. Therefore, $\Delta\alpha$ must be larger than 0, which explains the lower bound of (13).

IV. Conclusion

In summary, we have theoretically and experimentally demonstrated a novel controllable asymmetry attack against TWFTT. Our attacks are implemented by rerouting the signals with two circulators, and adjusting the link asymmetry or attenuation asymmetry with variable optical delay line or variable optical attenuator in the controllable asymmetry attack modules. The link asymmetry can linearly control the time offset with the coefficient of about 0.51, and the attenuation asymmetry can introduce nanoseconds time offset with the asymmetric attenuation larger than 43.2%. Our work systematically reveals the vulnerabilities of TWFTT under delay asymmetry attacks, therefore it is instructive for future studies of protecting TWFTT from delay asymmetry attacks.

References

[1] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 446–464, 2017.

[2] Y. Zhang, L. Wang, W. Sun, R. C. Green, II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE T. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[4] T. Qu, S. Lei, Z. Wang, D. Nie, X. Chen, and G. Q. Huang, "IoT-based real-time production logistics synchronization system under smart cloud manufacturing," *Int. J. Adv. Manuf. Tech.*, vol. 84, no. 1-4, pp. 147–164, 2016.

[5] J. A. Stankovic and T. He, "Energy management in sensor networks," *Philos. T. R. Soc. A*, vol. 370, no. 1958, pp. 52–67, 2012.

[6] O. P. Valls, P. J. Bouvet, and J. R, "Hybrid time synchronization for underwater sensor networks," *ACTA IMEKO*, vol. 4, no. 3, pp. 30–35, 2015.

[7] K. F. Hasan, C. Wang, Y. Feng, and Y. C. Tian, "Time synchronization in vehicular ad-hoc networks: A survey on theory and practice," *Veh. Commun.*, vol. 14, pp. 39–51, 2018.

[8] D. L. Mills, "Internet time synchronization: The network time protocol," *IEEE Trans. Commun.*, vol. 39, no. 10, pp. 1482–1493, Oct. 1991.

[9] J. C. Eidson, M. Fischer, and J. White, "IEEE-1588$^{\mathrm{TM}}$ standard for a precision clock synchronization protocol for networked measurement and control systems," in *Proc. 34th Annu. PTTI Syst. Appl. Meeting*, 2002, pp. 243–254.

[10] J. Han and D. K. Jeong, "A practical implementation of IEEE 1588-2008 transparent clock for distributed measurement and control systems," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 2, pp. 433–439, Feb. 2010.

[11] B. J. Bloom *et al.*, "An optical lattice clock with accuracy and stability at the 10− 18 level," *Nature*, vol. 506, no. 7486, pp. 71–75, 2014.

[12] T. L. Nicholson *et al.*, "Systematic evaluation of an atomic clock at 2 × 10-18 total uncertainty," *Nature Commun.*, vol. 6, no. 1, pp. 1–8, 2015.

[13] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik, and P. O. Schmidt, "Optical atomic clocks," *Rev. Mod. Phys.*, vol. 87, no. 2, 2015, Art. no. 637.

[14] B. Wang *et al.*, "Precise and continuous time and frequency synchronisation at the 5×10-19 accuracy level," *Sci. Rep.*, vol. 2, pp. 556–560, 2012.

[15] X. Chen *et al.*, "Simultaneously precise frequency transfer and time synchronization using feed-forward compensation technique via 120 km fiber link," *Sci. Rep.*, vol. 5, pp. 18343–18349, Dec. 2015.

[16] E. Itkin and A. Wool, "A security analysis and revised security extension for the precision time protocol," in *Proc. IEEE ISPCS*, 2016, pp. 1–6.

[17] S. Waldhauser, B. Jaeger, and M. Helm, "Time synchronization in time-sensitive networking," in *Proc. Netw. Architectures Serv.*, 2020, pp. 51–56.

[18] M. Ullmann and M. Vögeler, "Delay attacks—Implication on NTP and PTP time synchronization," in *Proc. IEEE ISPCS*, 2009, pp. 1–6.

[19] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *Proc. Energytech*, 2013, pp. 1–5.

[20] S. Barreto, A. Suresh, and J. Y. Boudec, "Cyber-attack on packet-based time synchronization protocols: The undetectable delay box," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. Proc.*, 2016, pp. 1–6.

[21] R. Exel, "Mitigation of asymmetric link delays in IEEE 1588 clock synchronization systems," *IEEE Commun. Lett.*, vol. 18, no. 3, pp. 507–510, Mar. 2014.

[22] M. Lévesque and D. Tipper, "Improving the PTP synchronization accuracy under asymmetric delay conditions," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization for Meas., Control, Commun.*, 2015, pp. 88–93.

[23] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3954–3965, Sep. 2018.

[24] M. Furdek *et al.*, "An overview of security challenges in communication networks," in *Proc. 8th Int. Workshop Resilient Netw. Des. Model.*, 2016, pp. 43–50.

[25] J. C. Garcia-Escartin and P. Chamorro-Posada, "Hidden probe attacks on ultralong fiber laser key distribution systems," *IEEE J. Sel. Top. Quant.*, vol. 24, no. 3, May/Jun. 2017, Art. no. 0902009.

[26] Y. Peng, K. Long, Z. Sun, and S. Du, "Propagation of all-optical crosstalk attack in transparent optical networks," *Opt. Eng.*, vol. 50, no. 8, 2011, Art. no. 085002.