Secure Two-Way Fiber-Optic Time Transfer Against Sub-ns Asymmetric Delay Attack With Clock Model-Based Detection and Mitigation Scheme

Yang Li, Jinlong Hu, Yan Pan, Wei Huang, Li Ma, Jie Yang, Shuai Zhang, Yujie Luo, Chuang Zhou, Chenlin Zhang, Heng Wang, Yun Shao, Yichen Zhang, *Associate Member, IEEE*, Xing Chen, Ziyang Chen, Song Yu, Hong Guo, *Member, IEEE*, and Bingjie Xu

***Abstract*— Two-way fiber-optic time transfer (TWFTT) is a promising precise time synchronization technique with subnanosecond stability. However, the asymmetric delay attack is a severe threat, which can deteriorate the performance of the TWFTT system. In this article, a clock model-based scheme is used to defend the subnanosecond asymmetric delay attack. For the scheme, a security threshold is set according to a two-state clock model, and the estimated frequency difference is excluded from the measured time difference to detect the subnanosecond asymmetric delay attack. Systematic detection and mitigation scheme for asymmetric delay attack is developed in this article. Theoretical simulation and experimental demonstration are implemented to explore the feasibility of the method. A TWFTT system of time stability with 24.5, 3.98, and 2.95 ps at average times of 1, 10, and 100 s is shown under subnanosecond asymmetric time delay attack experimentally for the first time. The proposed method provides a promising secure subnanosecond precise time synchronization technique against asymmetric delay attacks.**

***Index Terms*— Delay attack, security, synchronization.**

Manuscript received 31 December 2022; revised 24 February 2023; accepted 3 April 2023. Date of publication 18 May 2023; date of current version 19 June 2023. This work was supported in part by China NSF under Grant 61901425, Grant U19A2076, Grant 61771081, Grant 62101516, Grant 61771439, and Grant 61702469; in part by the Fundamental Research Funds for the Central Universities under Grant 2019CDXYJSJ0021; in part by the Sichuan Youth Science and Technology Foundation under Grant 2019JDJ0060; in part by the Chengdu Major Science and Technology Innovation Program under Grant 2021-YF08-00040-GX; in part by the Sichuan Application and Basic Research Funds under Grant 2021YJ0313; in part by the Sichuan Science and Technology Program under Grant 2019JDJ0060, Grant 2020YFG0289, Grant 2022YFG0330, Grant 2022ZYD0118, Grant 2023JDRC0017, Grant 2023YFG0143, Grant 2022ZDZX0009, and Grant 2021YJ0313; in part by the Equipment Advance Research Field Foundation under Grant 315067206; in part by the National Key Research and Development Program of China under Grant 2020YFA0309704; in part by the National Natural Science Foundation of China under Grant U19A2076, Grant 62101516, Grant 62171418, and Grant 62201530; in part by the Natural Science Foundation of Sichuan Province under Grant 2023NSFSC1387 and Grant 2023NSFSC0449; in part by the Basic Research Program of China under Grant JCKY2021210B059; in part by the Chengdu Key Research and Development Support Program under Grant 2021-YF05-02430-GX and Grant 2021-YF09-00116-GX; and in part by the Foundation of Science and Technology on Communication Security Laboratory under Grant 61421030402012111. The Associate Editor coordinating the review process was Dr. Valentina Cosentino. *(Corresponding authors: Bingjie Xu; Hong Guo.)*

Yang Li, Jinlong Hu, Yan Pan, Wei Huang, Li Ma, Jie Yang, Shuai Zhang, Yujie Luo, Chuang Zhou, Chenlin Zhang, Heng Wang, Yun Shao, and Bingjie Xu are with the Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China (e-mail: xbjpku@pku.edu.cn).

Yichen Zhang, Xing Chen, and Song Yu are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Ziyang Chen and Hong Guo are with the State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, and the Center for Quantum Information Technology, Peking University, Beijing 100871, China (e-mail: hongguo@pku.edu.cn).

Digital Object Identifier 10.1109/TIM.2023.3268476

I. Introduction

PRECISE time synchronization has become increasingly important for transportation [1], smart grid [2], contemporary space geodesy [3], high-resolution radio astronomy [4], and modern particle physics [5]. Among various kinds of time transfer techniques, the two-way time transfer technique is a promising one that transmits time signals symmetrically in both directions to cancel the time jitter for one-way transfer [6].

Two-way satellite time transfer has achieved nanosecond accuracy [7] and a time stability of 200 ps [8]. Due to widely installed optical fiber infrastructure, two-way fiber-optic time transfer (TWFTT) [3], [9] has attracted much attention in recent years with the advantage of low cost. Based on directly measuring arrival times of pulses, a time stability as low as picosecond level has been reported [9], [10], [11], [12], [13], [14], [15], [16], [17], [18]. Recently, in order to improve the performance of the time transfer, some technologies are developed, such as joint time and frequency transfer [15], [16], phase modulation technique [15], [17], λ-swapping technique [18]. Although the performance of the time transfer is improved by these technologies, there are security threads for TWFTT, which can deteriorate the performance significantly. Security strategy based on encryption is proposed in [19]. However, there is a threat called asymmetric delay attack which can not be protected by encryption.

For TWFTT technology, there are two kinds of asymmetric time delay, intrinsic and extra. The intrinsic asymmetric time delay is caused by the nature of the fiber. In order to gain subnanosecond accuracy for TWFTT, the bidirectional signals are transferred in the same fiber to restrict the intrinsic asymmetric time delay. However, the residual asymmetric delay induced by the fiber characteristic, such as the fiber chromatic dispersion with unequal wavelength and the polarization mode dispersion (PMD) [9], is inevitable, which is related to the

TABLE I
COMPARISON TABLE

	Method	Protocol	Performance	Condition	Restriction
[22]	RTT, multiple paths, multiple clocks	PTP, NTP	/	Theory	/
[23]	RTT	PTP	μs level	Simulation	/
[24]	Game Theory	PTP, NTP	/	Theory	Multiple paths
[25]	EM algorithm	PTP	μs level	Simulation	Multiple paths
[26]	SAGE algorithm	PTP	μs level	Simulation	Multiple paths
[27]	Network clocks	PTP	ms level	Simulation	Multiple clocks
[28]	NTR	PTP, NTP	ms level	Simulation	External reference clock
[29]	TSN	PTP	μs level	Experiment	Multiple slave devices
[30]	Model-based and data-driven detector	PTP	μs level	simulation	Extra information from PMU, without mitigation
[31]	Polar coding	NTP	ms level	Simulation	Limited performance
[32]	Probabilistic model checker	PTP	μs range	Simulation and experiment	Limited performance
[33]	Observation task	PTP	μs level	Experiment	Limited performance
This paper	Clock model-based method	TWFTT	ps level	Simulation and experiment	/

lower bound of the performance of the TWFTT system. Except for the intrinsic asymmetric delay, the adversary can introduce extra asymmetric time delay, and it is unknown to the synchronization parties. So, if there is no secure measure, the extra asymmetric delay can deteriorate the performance of the TWFTT system significantly, which have been shown experimentally [20], [21]. However, to the best of our knowledge, the method to detect and mitigate the asymmetric delay attack of TWFTT has not been studied experimentally.

Similar asymmetric delay attacks and solutions have been studied for other time synchronization protocols like NTP and PTP [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]. In [22], several security methods are proposed, such as round-trip time (RTT) monitor, multiple clocks, and multiple paths. However, no quantitative analysis on the countermeasure is provided. In [23], requirements for secure two-way protocol, such as PTP, are proposed, and RTT is proposed to detect the delay attack. However, the influence of fixed frequency difference between the two parties is not excluded from the adversary detection. In [24], a game theoretic analysis of delay attacks is studied, and a multiple paths strategy is proposed to mitigate delay attacks. However, this method needs multiple paths between the master and slave clocks. By using the information of multiple paths, different lower bounds on the best achievable performance are derived in the presence of asymmetric delay by using expectation-maximization (EM) algorithm [25] or space alternating generalized-maximization (SAGE) algorithm [26]. In [27], a new delay attack detection method is proposed by comparing the network clocks with each other. However, multiple clocks are needed for this method. In [28], an external reference clock called network time reference (NTR) with very high accuracy is used to detect cyber-attacks. However, external reference clock with very high accuracy is needed. In [29], the proposed model relies on a monitor unit called the trust supervisor node (TSN), which is able to compare clock offsets/delay measurements provided by a large number of slave devices. In [30], model-based and data-based methods are proposed as a countermeasure for time attacks. However, extra information from phase measurement unit (PMU) is needed and mitigation is not included in the method. In [31], polar coding is proposed as a security strategy. The channel polarization caused by polar coding is utilized to construct secure channel for timestamps. In [32], a detection and mitigation method based on probabilistic model checker for delay attack is studied theoretically and experimentally. However, only 100-μs level synchronization error is achieved by the method. In [33], an improved method is proposed by introducing an observation task and analytically deriving attack parameters of the time delay attack. However, only μs level synchronization error is achieved by the method. A comparison is given in Table I.

In all, due to the high precision for TWFTT which can provide sub-ns level time synchronization, sub-ns delay attack can still influence the performance significantly. However, a real-time detection and mitigation method for subnanosecond asymmetric delay attacks is still an open question for TWFTT system.

In this article, we investigate the method to protect TWFTT from subnanosecond asymmetric time delay attacks. By analyzing the mechanism of asymmetric time delay attack, a defense scheme based on the clock dynamics is proposed. In this article, systematic method is proposed to detect and mitigate asymmetric delay attack, without extra information, such as multiple paths, multiple master clocks, or information from PMU. Then theoretical simulations and experimental demonstrations are implemented to explore the feasibility of this method. A TWFTT system of time stability with 26.4, 6.82, and 3.58 ps under subnanosecond equal interval asymmetric time delay attacks and with 24.5, 3.98, and 2.95 ps under subnanosecond random interval asymmetric time delay

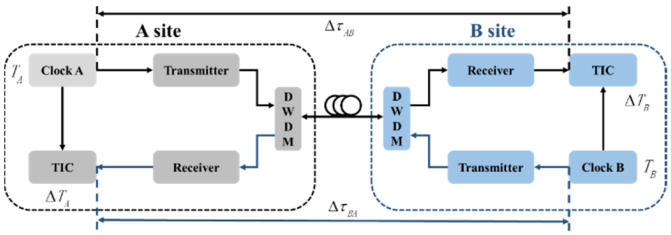


Fig. 1. Schematic of TWFTT system. DWDM: dense wavelength division multiplexing, TIC: time interval counter.

attacks at average times of 1, 10, and 100 s is shown. The experimental results show that almost all the asymmetric delay attacks with subnanosecond delay can be detected and mitigated by this scheme, no matter whether the attacks happen in an equal interval or randomly. To the best of our knowledge, it is the first time to demonstrate secure time transfer against sub-ns asymmetric delay attack for TWFTT. It provides an efficient method to protect TWFTT from the asymmetric time delay attack.

II. Schematic Description

A. TWFTT Scheme

We consider a general scheme of the TWFTT system (as shown in Fig. 1). It consists of two parties, A and B, interconnected by an optical fiber channel. At each of the parties, the time scales (one pulse per second, 1PPS) are transmitted to each other through a bidirectional optical fiber link. The 1PPS signals are detected by the receiver. The time difference between the received 1PPS and the sent 1PPS is measured by the time interval counter (TIC) at each part, named ΔT_A and ΔT_B. So

$$\Delta T_A = (T_B + \Delta\tau_{BA}) - T_A \tag{1}$$

$$\Delta T_B = (T_A + \Delta\tau_{AB}) - T_B \tag{2}$$

where $\Delta\tau_{BA}$ is the propagation time from B to A, and $\Delta\tau_{AB}$ in the other direction. According to (1) and (2), the time offset between A and B is derived by

$$\Delta T = T_A - T_B = \frac{1}{2}(\Delta T_B - \Delta T_A) + \frac{1}{2}(\Delta\tau_{BA} - \Delta\tau_{AB}). \tag{3}$$

Assuming a symmetrical propagation delay, $\Delta\tau_{BA} = \Delta\tau_{AB}$, the time offset between A and B is given by

$$\Delta T = \frac{1}{2}(\Delta T_B - \Delta T_A). \tag{4}$$

For TWFTT system, one party is called the remote site and the other is called the local site. The measured time offset is used by the local site to correct its clock to synchronize with the remote clock. In this article, B is used as the local site, and A is used as the remote site.

B. Asymmetric Delay Attack

Unknown asymmetric delay in the channel will lead to synchronization errors in TWFTT system. There are two kinds of asymmetric time delay, intrinsic and extra. The intrinsic asymmetric time delay is caused by the nature of the fiber. In order to gain subnanosecond accuracy for TWFTT, the bidirectional signals are transferred in the same fiber to restrict the intrinsic asymmetric time delay. However, an adversary can deteriorate the performance of TWFTT system by introducing extra asymmetric time delays which are unknown to the synchronization parties. This attack is called the asymmetric delay attack.

The impact of the asymmetric delay attack is analyzed quantitatively. Specifically, if the adversary delays the 1PPS from B to A by $\Delta\tau_{\text{attack}}$, the actual time offset between A and B is given by

$$\Delta T_{\text{actual}} = \frac{1}{2}(\Delta T_B - \Delta T_A) + \frac{1}{2}\Delta\tau_{\text{attack}}. \tag{5}$$

Comparing (4) and (5), if no secure method is adopted, the adversary introduces a time synchronization error with $\Delta\tau_{\text{error}} = (1/2)\Delta\tau_{\text{attack}}$.

C. Countermeasure

In order to detect the asymmetric delay attack, a clock dynamic model is built for the time offset between A and B. An adversary detector function with the measured time offset and the estimated time offset from the dynamic model as variables are built. By setting a security threshold, if the value of the detector exceeds the threshold, a potential attack is detected, and a special time offset correction scheme is chosen. And if the value of the detector does not exceed the threshold, a normal time offset correction scheme is chosen.

In this article, a two-state clock model is employed [31]. Equations describing the clock dynamics are

$$\begin{cases} d\theta(t) = \gamma(t)dt + d\omega_\theta(t) \\ d\gamma(t) = d\omega_\gamma(t) \end{cases} \tag{6}$$

where s and $\gamma(t) = f_{\text{local}} - f_{\text{remote}}$ are time offset and frequency difference between the local clock and the remote clock, $\omega_\theta(t)$ and $\omega_\gamma(t)$ relate to random-walk phase noise and random-walk frequency noise, respectively, which are independent 1-D zero-mean Wiener processes with variances equal to σ_θ^2 and σ_γ^2, respectively.

For TWFTT system, the local clock is updated periodically, and time offset correction, $u_\theta(t_n)$, is applied to the local clock to synchronize with the remote clock at the nth synchronization instant $t_n = n \cdot \tau$. So, (6) can be rewritten as difference equations [32]

$$\begin{cases} \theta(t_n) = \theta(t_{n-1}) + u_\theta(t_{n-1}) + \gamma(t_{n-1}) \cdot \tau + \omega_\theta(t_n) \\ \gamma(t_n) = \gamma(t_{n-1}) + \omega_\gamma(t_n). \end{cases} \tag{7}$$

For TWFTT system, the measured time offset, which is rewritten as $\theta_M(t_n) = \Delta T(t_n)$, can be used to correct the local clock. Correction strategy influences the performance of the TWFTT system and adversary detection effect. In this article, the direct correction strategy is chosen to compare with the attack detection strategy.

For direct correction strategy, the measured time offset is used to correct the local clock directly. That means, after the measurement of the time offset between the local clock

and the remote clock, the update value of the local clock is given by the measured time offset $u_\theta(t_n) = \theta_M(t_n)$. Then $u_\theta(t_n)$ is used to correct the local clock. For the TWFTT system, the measured time offset is given by $\theta_M(t_n) = \Delta T(t_n) = (1/2)(\Delta T_B(t_n) - \Delta T_A(t_n))$, where ΔT_B and ΔT_A are the measured time intervals at local site and remote site, as described in II-A.

Algorithm Direct Correction Strategy

1. Calculate measured time offset, $\theta_M(t_n) = \Delta T(t_n) = \frac{1}{2}(\Delta T_B(t_n) - \Delta T_A(t_n))$.
2. Calculate the update value of the local clock, $u_\theta(t_n) = \theta_M(t_n)$.

For the attack detection strategy, in order to detect the subnanosecond asymmetric delay attack, the frequency difference between the local clock and remote is supposed to be relatively stable, and excluded to construct the attack detector. Specifically, the frequency difference is estimated according to the clock model. And the attack index is defined as the absolute value of the measured time offset minus the time offset induced by the estimated frequency difference. A secure threshold is set for attack detection. If the attack index exceeds the threshold, a potential attack is detected, and a special time offset correction scheme is chosen. Otherwise, a normal time offset correction scheme is chosen. More details are shown below.

Algorithm Asymmetric Time Delay Attack Detection

1. Calculate the measured time offset, $\theta_M(t_n) = \Delta T(t_n) = \frac{1}{2}(\Delta T_B(t_n) - \Delta T_A(t_n))$.
2. Calculate the estimated frequency difference.

   If no attack is detected at t_{n-1}, then the measured frequency difference at t_n is given by $\gamma_M(t_n) = (\theta_M(t_n) - \theta_M(t_{n-1}) + u_\theta(t_{n-1}))/\tau$, and the estimated frequency difference is given by $\hat{\gamma}_E(t_n) = \gamma_M(t_n)$.

   Else, the estimated frequency difference is given by $\hat{\gamma}_E(t_n) = \gamma_{best}(t_{n-1})$.
3. Calculate the fixed time offset induced by frequency difference, $offsetF(t_n) = \gamma_{best}(t_{n-1}) \cdot \tau$.
4. Calculate the attack index, $I_{attack} = |\theta_M(t_n) - offsetF(t_n)|$, where $\theta_M(t_n)$ is the measured time offset at t_n.
5. Make a judgment whether an attack happens at t_n, and calculate the update value of the local clock and the best frequency difference estimation.

   If $I_{attack} > I_{threhold}$, then $u_\theta(t_n) = offsetF(t_n)$, and $\gamma_{best}(t_n) = \gamma_{best}(t_{n-1})$.

   Else, $u_\theta(t_n) = \theta_M(t_n)$, $\gamma_{best}(t_n) = w \cdot \gamma_M(t_n) + (1-w) \cdot \gamma_{best}(t_n)$, $0 \le w \le 1$.

The estimated frequency difference is very important for the proposed algorithm. The measured frequency difference $\gamma_M(t_n) = (\theta_M(t_n) - \theta_M(t_{n-1}) + u_\theta(t_{n-1}))/\tau$ fluctuates due to the measurement noise. In order to reduce the influence of the measurement noise, a smoothing method is introduced with a smoothing factor as w, as shown in step 5 of the algorithm.

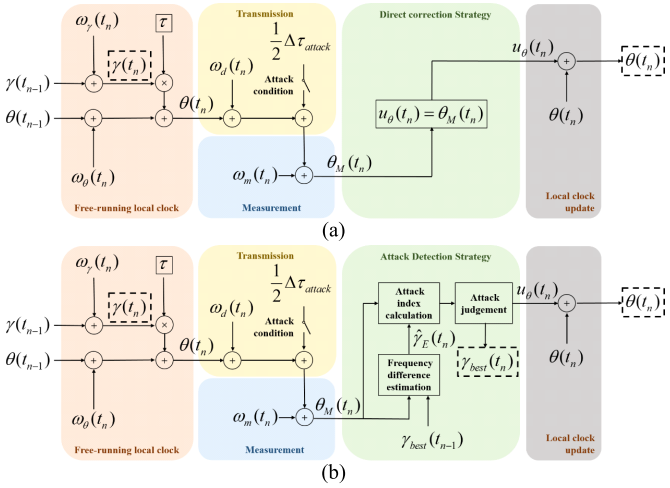


Fig. 2. Logical structure of the simulation. (a) Direct correction strategy. (b) Attack detection strategy.

D. Metric

On the one hand, in order to analyze the effect of the attack detection algorithm quantitatively, two performance metrics are introduced which are precision and recall. Precision is defined as the number of detected actual attack events over the total number of detected attack events, while recall is defined as the number of detected actual attack events over the total number of actual attack events.

On the other hand, in order to analyze the influence of the attack detection strategy on the performance of the time synchronization system, time deviation error variance (TDEV) and maximum time interval error (MTIE) are introduced as [33]

$$\mathrm{TDEV}(\tau = n * \tau_0) = \sqrt{\frac{1}{6n^2(N-3n+1)} \sum_{j=0}^{N-3n} \left[\sum_{i=j}^{n+j-1} (x_{i+2n} - 2x_{i+n} + x_i) \right]^2} \tag{8}$$

$$\mathrm{MTIE}(\tau = n * \tau_0) = \max_{i=0}^{N-n-1} \left\{ \max_{k=1}^{k=n} [|x(i+k) - x(i)|] \right\}. \tag{9}$$

III. Theoretical Simulation

In this section, theoretical simulation is implemented to explore the feasibility of the attack detection strategy proposed in this article.

Two strategies are compared in this article, which are direct correction strategy and attack detection strategy. First, as shown in Fig. 2, a free-running local clock module is applied to produce the time difference $\theta(t_n)$ at the nth synchronization instant $t_n = n \cdot \tau$. In this module, $\omega_\theta(t_n)$ and $\omega_\gamma(t_n)$ are the random-walk phase noise, random-walk frequency noise and transmission noise during the period between t_{n-1} and t_n, which are independent 1-D zero-mean Wiener processes with standard deviation equal to σ_θ and σ_γ, respectively. After the free-running local clock module, a transmission module

TABLE II
SIMULATION PARAMETERS

Parameter	Value	Description
σ_m	25 ps	Standard deviation of measurement noise
σ_d	10 ps	Standard deviation of transmission noise
σ_θ	10 ps	Standard deviation of random-walk phase noise of the clock
σ_γ	1 ps/s	Standard deviation of random-walk frequency noise of the clock

is applied, where $\omega_d(t_n)$ is the transmission noise, which is an independent 1-D zero-mean Wiener process with standard deviation equal to σ_d. A conditional delay attack is applied to modify the time difference with the value of $(1/2)\Delta\tau_{\text{attack}}$, as explained in (5). Then, a measurement noise $\omega_m(t_n)$ is added, which is an independent 1-D zero-mean Wiener process with standard deviation equal to σ_m. After the measurement module, the measured time offset $\theta_M(t_n)$ is produced.

For direct correction strategy, the update value of the local clock is calculated as $u_\theta(t_n) = \theta_M(t_n)$. For attack detection strategy, the frequency difference estimation unit is applied to calculate the estimated frequency difference $\hat{\gamma}_E(t_n)$, and the details are shown in step 3 of the algorithm. Then, the attack index is calculated, and the details are shown in step 4 of the algorithm. Attack judgment unit is applied to calculate the update value of the local clock $u_\theta(t_n)$ and the best estimation of the frequency difference $\gamma_{\text{best}}(t_n)$ according to whether an attack happens during the period between t_{n-1} and t_n, and the details are shown in step 5 of the algorithm.

After the strategies module, the calculated update value of the local clock $u_\theta(t_n)$ is added to the actual time difference $\theta(t_n)$ to get the final time difference after the nth synchronization.

First, the performance of TWFTT system under no attack events with a direct correction strategy and attack detection strategy is compared by simulation. In the simulation, two extra independent 1-D zero-mean Wiener processes with variances σ_m^2 and σ_d^2 are introduced for the measurement noise and transmission noise. Without loss of generality, all the values of the noises in the simulation are chosen as in Table II. As shown in Fig. 3, the time synchronization error (time offset) is just around zero for both cases where the fluctuation is caused by measurement noise, transmission noise, and random-walk noise.

Second, the influences of delay attacks on time synchronization are studied. In the simulation, a delay attack happens once every 50 s. Two cases are compared, where direct correction strategy is adopted for the first case and attack detection strategy is adopted for the second one.

In order to evaluate the influence of the attack detection algorithm on the performance of time synchronization quantitatively, we studied the TDEV and MTIE for both cases. As shown in Fig. 4, time stabilities with metrics TDEV and MTIE are almost the same for the two cases. The results show

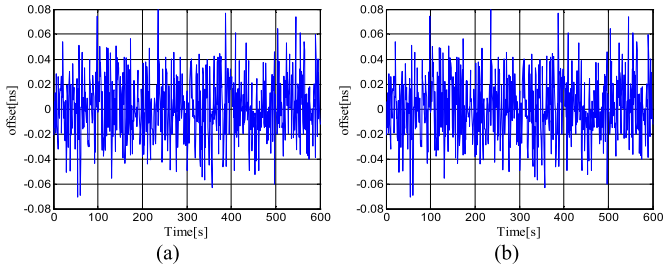


Fig. 3. Simulation of TWFTT's time difference without attack. (a) Direct correction strategy. (b) Attack detection strategy.

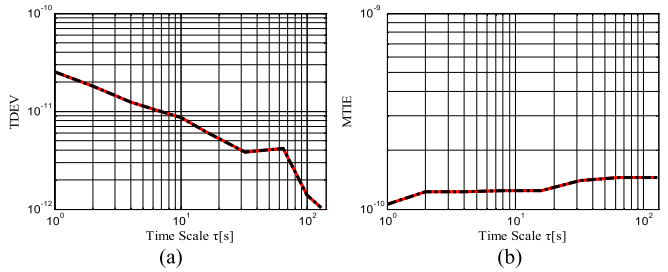


Fig. 4. Simulation of TWFTT's TDEV and MTIE without attack. (a) TDEV. (b) MTIE (red solid line: attack detection strategy; black dashed line: direct correction strategy).

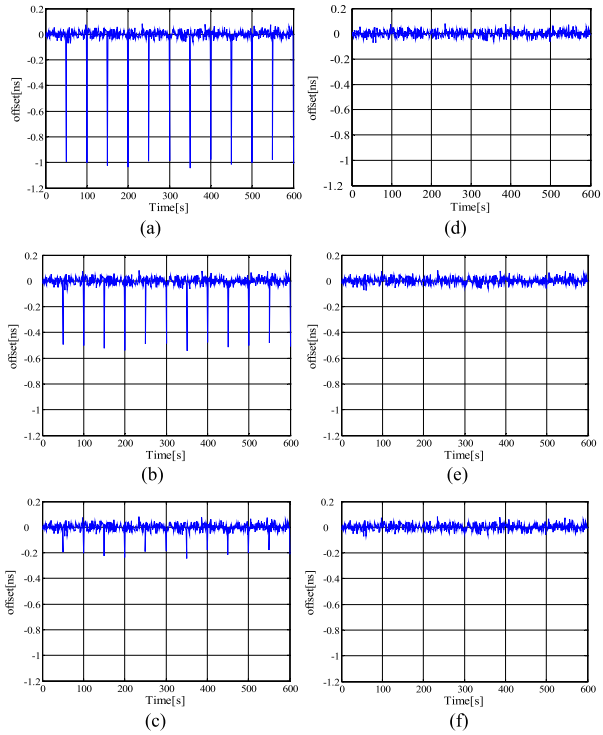


Fig. 5. Simulation of TWFTT's time difference under asymmetric time delay attack with time errors. (a) 1 ns with direct correction strategy. (b) 0.5 ns with direct correction strategy. (c) 0.2 ns with direct correction strategy. (d) 1 ns with attack detection strategy. (e) 0.5 ns with attack detection strategy. (f) 0.2 ns with attack detection strategy.

that the attack detection algorithm does not deteriorate the performance of the time synchronization if no attack exists.

For the case of the direct correction strategy, since no attack detection is adopted, the time delay attack brings in synchronization errors [see Fig. 5(a)–(c)]. By the theoretical

TABLE III
PERFORMANCE METRIC UNDER ASYMMETRIC TIME DELAY ATTACK

	Recall	Precision	TDEV @ 1 s	TDEV @ 10 s	TDEV @ 100 s	MTIE @ 1 s	MTIE @ 10 s	MTIE @ 100 s
Attack Detection strategy without attack	/	/	2.5174 E-11	8.6769 E-12	1.3905 E-12	1.0647 E-10	1.2489 E-10	1.4537 E-10
Attack Detection strategy with 1 ns attack	100%	100%	2.5012 E-11	8.7183 E-12	1.4889 E-12	1.0647 E-10	1.2489 E-10	1.4537 E-10
Direct correction strategy with 1 ns attack	/	/	1.3820 E-10	4.4448 E-10	4.0823 E-12	1.0462 E-09	1.0688 E-09	1.0962 E-09
Attack Detection strategy with 0.5 ns attack	100%	100%	2.5012 E-11	8.7183 E-12	1.4889 E-12	1.0647 E-10	1.2489 E-10	1.4537 E-10
Direct correction strategy with 0.5 ns attack	/	/	7.2929 E-11	2.4092 E-11	1.3905 E-12	5.6548 E-10	5.8463 E-10	2.6192 E-10
Attack Detection strategy with 0.2 ns attack	100%	100%	2.5012 E-11	8.7183 E-12	1.4889 E-12	1.0647 E-10	1.2489 E-10	1.4537 E-10
Direct correction strategy with 0.2 ns attack	/	/	3.7248 E-11	1.2712 E-11	1.3904 E-12	1.6549 E-10	2.8467 E-10	3.2196 E-10

analysis, as explained in (4) and (5), the direct correction algorithm does not recognize the time delay introduced by the adversary, the update value of the local clock is given by $u_\theta(t_n) = \theta_M(t_n) = \theta(t_n) + \omega_d + \omega_m + (1/2)\Delta\tau_{\text{attack}}$, where $\theta(t_n)$ is the actual time offset of the local clock and the remote clock, ω_d and ω_m is the noise introduced by the transmission and measurement, and $(1/2)\Delta\tau_{\text{attack}}$ is introduced by the delay attack. That means a time synchronization error with $(1/2)\Delta\tau_{\text{attack}}$ is included in the update value. In the simulation, three cases are studied, where the values of delay attack $\Delta\tau_{\text{attack}}$ are given by 2, 1, and 0.4 ns every 50 s. The theoretical analysis shows the time synchronization error introduced by the delay attack should be 1, 0.5, and 0.2 ns. As shown in Fig. 5(a)–(c), the actual synchronization error is around 1, 0.5, and 0.2 ns every 50 s. The fluctuation is caused by noises, such as measurement noise, transmission noise, and random-walk noise. So, the simulation results match with the theoretical analysis.

For the case of attack detection strategy, all the actual attack events are detected by the algorithm, and no event which is not attack event is recognized as an attack event. So, precision and recall for the simulation are both 100%. From Fig. 5(d)–(f), we can see that the actual time offset is around zero, and the influence of the delay attack is eliminated by the attack detection algorithm. In order to evaluate the influence quantitatively, TDEV and MTIE curves are drawn (see Fig. 6). By comparing the direct strategy without attack and with attack, the results show that the delay attack brings a serious influence on the performance of the time synchronization. By comparing the attack detection strategy without attack and with attack, the results show that the influence of the delay attack can be effectively eliminated by the attack detection strategy. As shown in Table III, TDEVs and MTIEs at average

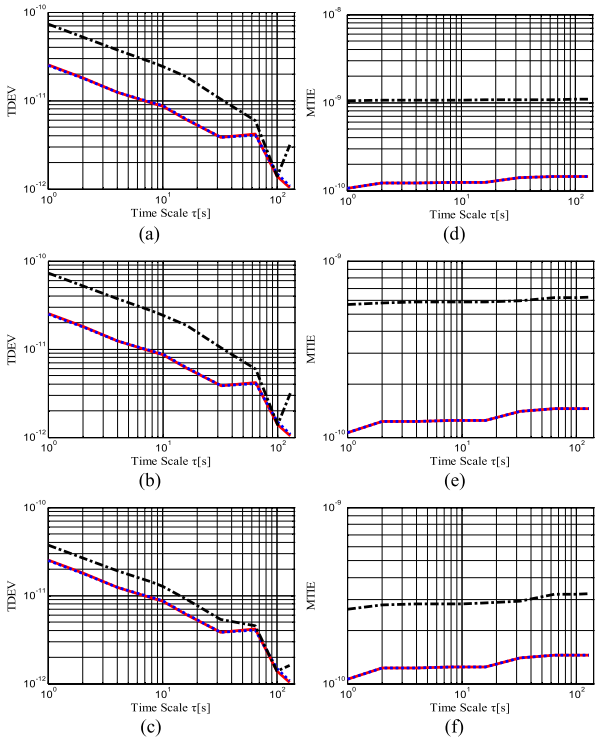


Fig. 6. Simulation of TWFTT's TDEV and MTIE under asymmetric time delay attack. (a) TDEV under 1-ns attack. (b) TDEV under 0.5-ns attack. (c) TDEV under 0.2-ns attack. (d) MTIE under 1-ns attack. (e) MTIE under 0.5-ns attack. (f) MTIE under 0.2-ns attack (red solid line: direct correction strategy without attack; blue dashed line: attack detection strategy with attack; black dotted line: direct correction strategy with attack).

TABLE IV
PERFORMANCE METRIC WITHOUT ATTACK

	TDEV @ 1 s	TDEV @ 10 s	TDEV @ 100 s	MTIE @ 1 s	MTIE @ 10 s	MTIE @ 100 s
Attack Detection strategy without attack-1	2.6534 E-11	7.6253 E-12	4.4366 E-12	1.1230 E-10	1.2207 E-10	1.5625 E-10
Attack Detection strategy without attack -2	2.7624 E-11	6.0616 E-12	1.7291 E-12	1.3672 E-10	1.3672 E-10	1.3672 E-10
Attack Detection strategy without attack -3	2.7947 E-11	6.5088 E-12	2.5012 E-12	1.1719 E-10	1.1719 E-10	1.5137 E-10
Direct correction strategy without attack-1	2.6096 E-11	5.9026 E-12	2.5161 E-12	1.2207 E-10	1.2695 E-10	1.6113 E-10
Direct correction strategy without attack -2	2.5843 E-11	7.4686 E-12	1.1633 E-11	1.0254 E-10	1.3184 E-10	1.5137 E-10
Direct correction strategy without attack -3	2.6754 E-11	7.2747 E-12	6.0021 E-12	1.2207 E-10	1.3184 E-10	1.5625 E-10

times of 1, 10, and 100 s are compared. By comparing cases of attack detection strategy without attack, and with 1-, 0.5-, and 0.2-ns attacks, respectively, it shows that the proposed attack detection algorithm can distinguish effectively the attack events and the normal events. That means the values of precision and recall are all 100% for attack detection strategy. And all the TDEVs and MTIEs at different average times are almost the same. For TDEV@1 s, TDEV@10 s, TDEV@100 s, MTIE@1 s, MTIE@10 s, and MTIE@100 s, all the cases are around 25, 8.7, 1.3, 106, 125, and 145 ps, respectively. By comparing cases of direct correction strategy and cases of attack detection strategy with 1, 0.5, and 0.2 ns attacks, it shows that the asymmetric time delay attack brings a serious influence on the performance of the time synchronization. Counter-intuitively, TDEV@100 s is seemed to not be influenced by the attack. It is caused by the definition of TDEV. According to (8), when $\tau = 100$, $x_{i+2n} - 2x_{i+n} + x_i$ equals to $x_{i+200} - 2x_{i+100} + x_i$. Since the interval of attack event in the simulation is 50 s, when i is an integral multiple of 50, the same time error is induced by the attack for x_{i+200}, x_{i+100}, and x_i, so the effects are counteracted, and when i is not an integral multiple of 50, no time error is induced by the attack for x_{i+200}, x_{i+100}, and x_i. So, the TDEV curve of the direct correction strategy and the TDEV curve of no attack case meet when $\tau = 100$, as shown in Fig. 5, and the TDEVs@100 s are almost the same for the cases of attack detection strategy and the cases of direct correction strategy as shown in Table III. In this article, scientific notation is adapted in Tables III–VI, where nEm presents $n \times 10^m$.

IV. EXPERIMENTAL DEMONSTRATION

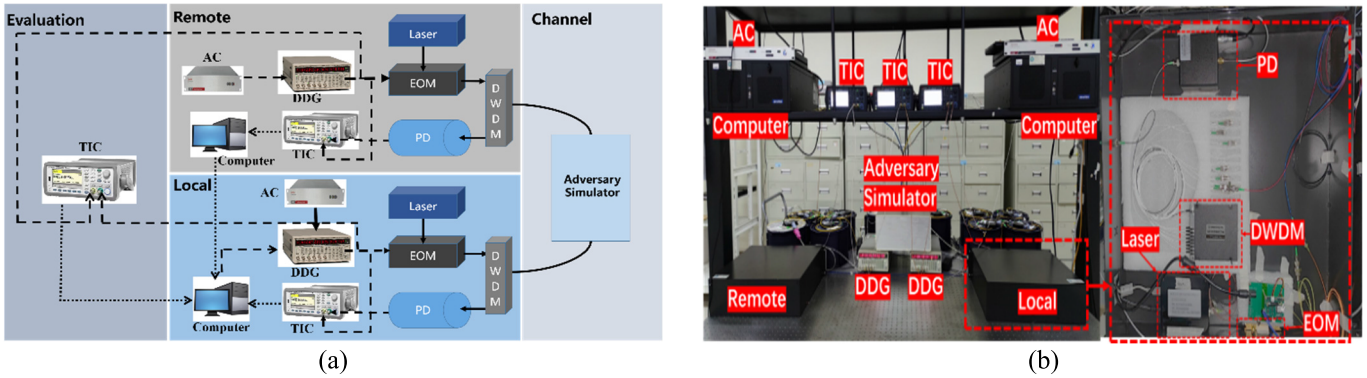
In this section, an experimental TWFTT system is set up in the laboratory, and demonstrations are implemented to explore the feasibility of the attack detection strategy proposed in this article.

The experimental setup of TWFTT system with adversary simulator is shown in Fig. 7. On the remote/local site, the digital delay generator (DDG, SRS DG645) generates 1PPS electric signal. 1PPS from one output port of DDG drives an electrooptic modulator (EOM, AX-0S5-10-PFA-PFA-UL) to modulate the CW laser to generate 1PPS optic signal. The same 1PPS from another output port of DDG is sent to the start trigger port of a TIC. The 1PPS optic signal is coupled to channel 35 of DWDM, and transmitted to the local site through the fiber channel. The photodetector on the local/remote site detects the 1PPS optical signal and the generated electric signal is sent to the stop trigger port of the TIC on the local/remote site. The time difference recorded by

TIC on the remote site is sent to the local site. By (4), the measured time offset is calculated on the local site. According to the adversary detection strategy and correction strategy, the delay correction value is calculated on the computer of the

TABLE V
PERFORMANCE METRIC UNDER EQUAL INTERVAL ATTACK

	Recall	Precision	TDEV @ 1 s	TDEV @ 10 s	TDEV @ 100 s	MTIE @ 1 s	MTIE @ 10 s	MTIE @ 100 s
Attack Detection strategy without attack	/	/	2.6534 E-11	7.6253 E-12	4.4366 E-12	1.1230 E-10	1.2207 E-10	1.5625 E-10
Attack Detection strategy with 1.25 ns attack	100%	100%	2.7675 E-11	6.8526 E-12	5.6365 E-12	1.2695 E-10	1.3672 E-10	1.6113 E-10
Direct correction strategy with 1.25 ns attack	/	/	1.8109 E-10	5.9854 E-11	8.0417 E-12	1.3818 E-09	1.4063 E-09	1.4795 E-09
Attack Detection strategy with 0.83 ns attack	100%	100%	2.7934 E-11	6.8546 E-12	V3.5781 E-12	1.3672 E-10	1.3672 E-10	1.5625 E-10
Direct correction strategy with 0.83 ns attack	/	/	1.1770 E-10	3.8755 E-11	3.5045 E-12	9.1797 E-10	9.3262 E-10	9.4727 E-10
Attack Detection strategy with 0.296 ns attack	100%	100%	2.6409 E-11	6.8165 E-12	6.7124 E-12	1.4160 E-10	1.4160 E-10	1.6602 E-10
Direct correction strategy with 0.296 ns attack	/	/	4.8687 E-11	1.4371 E-11	3.8927 E-12	3.6621 E-10	3.6621 E-10	4.0527 E-10



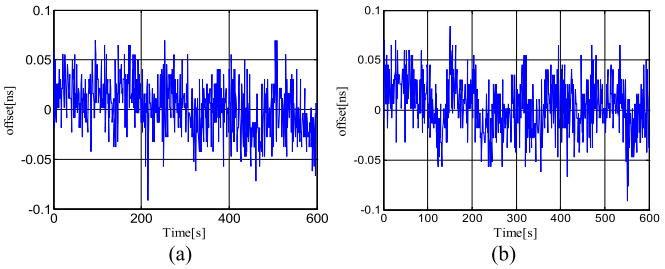
(a) (b)

Fig. 7. Experimental setup of TWFTT system with adversary simulator. AC: atomic clock, TIC: time interval counter, DDG: digital delay generator, EOM: electrooptic modulator, PD: photodetector, DWDM: dense wavelength division multiplexing.

local site and sent to DDG on the local site to modify the time delay. In order to evaluate the strategy, an extra TIC is added to measure the actual time errors between the remote clock and the local clock.

An adversary simulator is installed in the fiber channel, which can simulate the asymmetry delay attack launched by the adversary. Similar to [21], the adversary simulator consists of a 1 × 4 optical switch. When the optical switch is set to path 1, no asymmetry delay is added to the channel. When the optical switch is set to path 2–4, 0.296, 0.83 s, and 1.25-ns asymmetry delay is added to the channel, respectively.

Before studying the influence of the attack on the TWFTT system, we first compare the attack detection strategy and direct correction strategy without attack. For each strategy, 600-s data of evaluation TIC are recorded, and the TDEV and MTIE are calculated, as shown in Figs. 8 and 9. Different from the simulation case, the values of TDEV and MTIE between

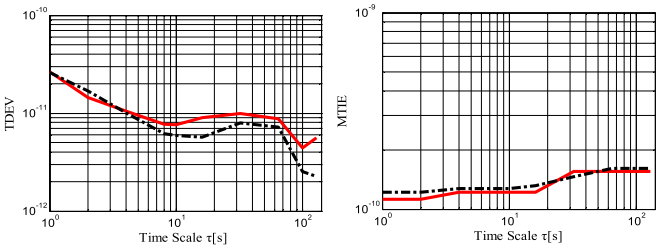


(a) (b)

Fig. 8. TWFTT's time difference without attack. (a) Direct correction strategy. (b) Attack detection strategy.

TABLE VI
PERFORMANCE METRIC UNDER RANDOM INTERVAL ATTACK

	Recall	Precision	TDEV @ 1 s	TDEV @ 10 s	TDEV @ 100 s	MTIE @ 1 s	MTIE @ 10 s	MTIE @ 100 s
Attack Detection strategy without attack	/	/	2.6534 E-11	7.6253 E-12	4.4366 E-12	1.1230 E-10	1.2207 E-10	1.5625 E-10
Attack Detection strategy with 0.83 ns attack	100%	100%	2.8298 E-11	3.9795 E-12	2.9450 E-12	1.2695 E-10	1.5905 E-10	1.6113 E-10
Direct correction strategy with 0.83 ns attack	/	/	3.3061 E-10	1.2786 E-10	3.3645 E-11	9.6680 E-10	9.6680 E-10	1.0596 E-09
Attack Detection strategy with 0.296 ns attack	100%	100%	2.4511 E-11	7.9209 E-12	6.7849 E-12	1.2207 E-10	1.4160 E-10	1.5137 E-10
Direct correction strategy with 0.296 ns attack	/	/	1.1571 E-10	4.3600 E-11	1.4957 E-11	3.8086 E-10	4.0039 E-10	4.5410 E-10
Attack Detection strategy with 0.83 ns & 0.296 ns mixed attack	100%	100%	2.5856 E-11	9.9418 E-12	5.1802 E-12	1.2207 E-10	1.3672 E-10	1.6602 E-10
Direct correction strategy with 0.83 ns & 0.296 ns mixed attack	/	/	4.9180 E-10	1.8902 E-10	4.2464 E-11	1.3818 E-09	1.3818 E-09	1.4014 E-09



(a) (b)

Fig. 9. TWFTT's TDEV and MTIE without attack (red solid line: attack detection strategy; black dashed line: direct correction strategy). (a) TDEV. (b) MTIE.

the attack detection strategy and direction correction strategy are not the same. Because in the simulation, the measurement noise, transmission noise, and process noise are the same for the two strategies, and in the experiment, these noises are different for the two strategies. However, although the values of TDEV and MITE are not exactly the same for the two strategies, the values are very close. Many experiments are done to confirm that the differences between the two strategies are induced by random noises.

As shown in Table IV, TDEVs and MTIEs at average times of 1, 10, and 100 s are compared for attack detection strategy and direct correction strategy without attack. Different from the simulation results, the TDEVs and MTIEs are not the same for the two strategies, which are due to the random factors, such as the measurement noise, transmission noise, random-walk phase noise, and frequency noise, in the experiment.

On the one hand, theoretically, the attack detection strategy is degraded to a simple form which is the same as the direct correction strategy. So, the difference between the two strategies in the experimental demonstration without attack is due to the random factors.

On the other hand, it is impossible to compare the direct correction strategy and the attack correction strategy in the same experiment with identical noise. So, in order to compare the direct correction strategy and the attack detection strategy, experiments are done with the same experimental parameters for the two strategies. However, the noise in the experiment is random process. Although the noises follow the same probability distribution, the actual noises are different for the experiment of the direction strategy and the experiment of the attack correction. So, although the two algorithms are the same when there is no attack, the calculated TDEVs and MTIEs are not the same. The experiments are implemented three times for each strategy, as shown in Table IV.

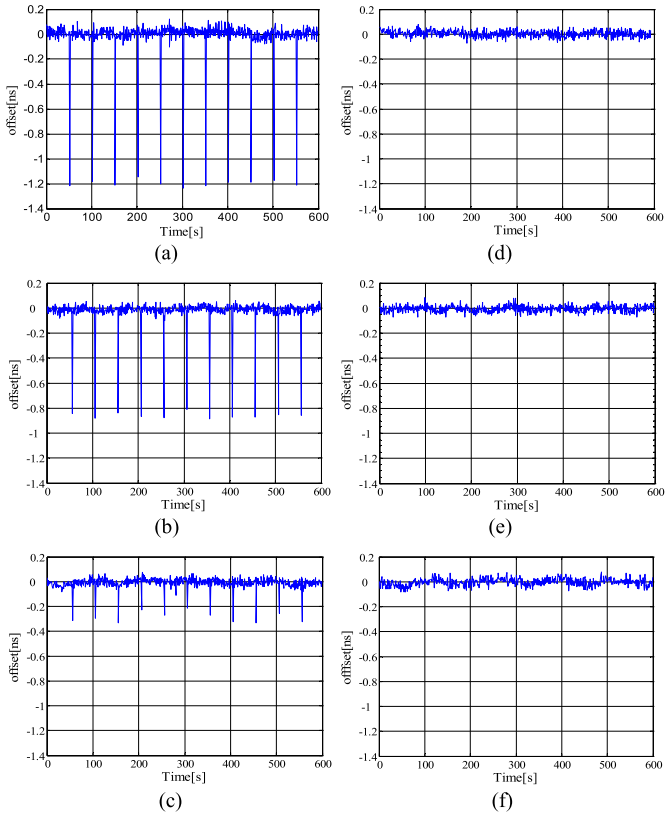


Fig. 10. TWFTT's time difference under asymmetric time delay attack with time errors. (a) 1.25 ns with direct correction strategy. (b) 0.83 ns with direct correction strategy. (c) 0. 296 ns with direct correction strategy. (d) 1.25 ns with attack detection strategy. (e) 0.83 ns with attack detection strategy. (f) 0. 296 ns with attack detection strategy.

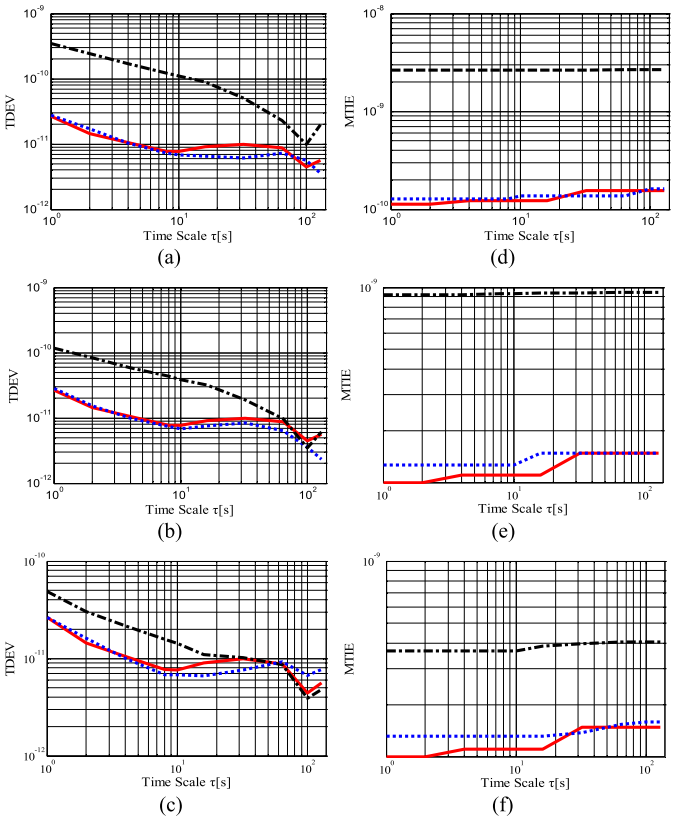


Fig. 11. TWFTT's TDEV and MTIE under asymmetric time delay attack. (a) TDEV under 1.25-ns attack. (b) TDEV under 0.83-ns attack. (c) TDEV under 0.296-ns attack. (d) MTIE under 1.25-ns attack. (e) MTIE under 0.83-ns attack. (f) MTIE under 0.296-ns attack (red solid line: direct correction strategy without attack; blue dashed line: attack detection strategy with attack; black dotted line: direct correction strategy with attack).

Then, two kinds of asymmetry delay attacks are studied, the equal interval attack and the random interval attack.

A. Equal Interval Attack

For equal interval attack, the adversary launched asymmetry delay attack once at set intervals. Without loss of generality, we set 50 s as the interval. Three kinds of asymmetry delay attacks with 0.296, 0.83, and 1.25 ns, respectively, are studied.

As shown in Fig. 10(a)–(c), when no attack detection strategy is applied, the TWFTT system can not recognize the attacks, and large synchronization errors are brought by the asymmetry delay attacks. In order to evaluate the influence quantitatively, TDEV and MTIE curves are drawn, as shown in Fig. 11. The results show that the equal interval attack brings a serious influence on the performance of the time synchronization, and the influence of the delay attacks is eliminated by the attack detection strategy.

As shown in Table V, TDEVs and MTIEs at average times of 1, 10, and 100 s are compared. By comparing cases of attack detection strategy without attack, with 1.25-ns attack, with 0.83-ns attack, and with 0.296-ns attack, it shows that the attack detection algorithm proposed in this article can distinguish the attack events and the normal events. That means the values of precision and recall are all 100% for attack detection strategy under equal interval attacks. The differences between TDEVs and MTIE are caused by the difference in the noises. The smallest TDEVs at average times of 1, 10, and 100 s are 26.4, 6.82, and 3.58 ps, and the smallest MTIEs at average times of 1, 10, and 100 s are 122.1, 136.7, and 151.4 ps, under nanosecond and subnanosecond equal interval attacks. By comparing cases of direct correction strategy and cases of attack detection strategy with 1.25-, 0.83-, and 0.296-ns attack, it shows that the asymmetric time delay attack brings a serious influence on the performance of the time synchronization. Counter-intuitively, TDEV@100 s is seemed to be not influenced by the attack. It is caused by the definition of TDEV. According to (8), when $\tau = 100$, $x_{i+2n} - 2x_{i+n} + x_i$ equals to $x_{i+200} - 2x_{i+100} + x_i$. Since the interval of attack event in the simulation is 50 s, when i is an integral multiple of 50, the same time error is induced by the attack for x_{i+200}, x_{i+100}, and x_i, so the effects are counteracted, and when i is not an integral multiple of 50, no time error is induced by the attack for x_{i+200}, x_{i+100}, and x_i. So, the TDEV value of the direct correction strategy approaches the TDEV value without attack, as shown in Fig. 11.

B. Random Interval Attack

For random interval attack, the adversary launched asymmetry delay attack randomly. So, the attack can happen consecutively. The probability of the attack is a key

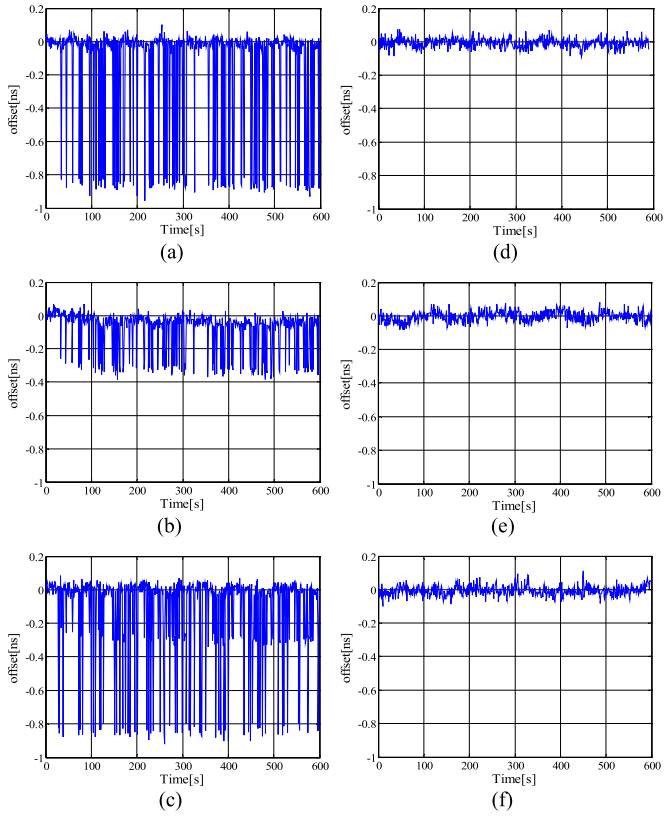


Fig. 12. TWFTT's time difference under asymmetric time delay attack with time errors. (a) $p_{\text{no}} = 0.8$, $p_{0.83\,\text{ns}} = 0.2$ with direct correction strategy. (b) $p_{\text{no}} = 0.8$, $p_{0.296\,\text{ns}} = 0.2$ with direct correction strategy. (c) $p_{\text{no}} = 0.7$, $p_{0.83\,\text{ns}} = 0.15$, $p_{0.296\,\text{ns}} = 0.15$ with direct correction strategy. (d) $p_{\text{no}} = 0.8$, $p_{0.83\,\text{ns}} = 0.2$ with attack detection strategy. (e) $p_{\text{no}} = 0.8$, $p_{0.296\,\text{ns}} = 0.2$ with attack detection strategy. (f) $p_{\text{no}} = 0.7$, $p_{0.83\,\text{ns}} = 0.15$, $p_{0.296\,\text{ns}} = 0.15$ with attack detection strategy.

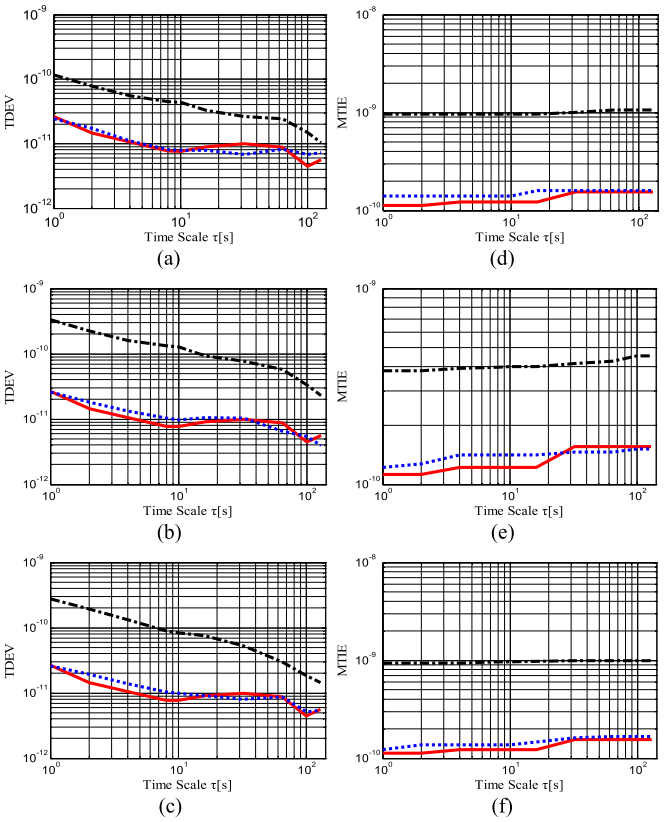


Fig. 13. TWFTT's TDEV and MTIE under asymmetric time delay attack. (a) TDEV under $p_{\text{no}} = 0.8$, $p_{0.83\,\text{ns}} = 0.2$. (b) TDEV under $p_{\text{no}} = 0.8$, $p_{0.296\,\text{ns}} = 0.2$. (c) TDEV under $p_{\text{no}} = 0.7$, $p_{0.83\,\text{ns}} = 0.15$, $p_{0.296\,\text{ns}} = 0.15$. (d) MTIE under $p_{\text{no}} = 0.8$, $p_{0.83\,\text{ns}} = 0.2$. (e) MTIE under $p_{\text{no}} = 0.8$, $p_{0.296\,\text{ns}} = 0.2$. (f) MTIE under $p_{\text{no}} = 0.7$, $p_{0.83\,\text{ns}} = 0.15$, $p_{0.296\,\text{ns}} = 0.15$ (red solid line: direct correction strategy without attack; blue dashed line: attack detection strategy with attack; black dotted line: direct correction strategy with attack).

parameter. Without loss of generality, three kinds of random interval attacks are studied. The first kind is a 0.83-ns delay random interval attack with probabilities $p_{\text{no}} = 0.8$, $p_{0.83\,\text{ns}} = 0.2$. The second kind is a 0.296-ns delay random interval attack with probabilities $p_{\text{no}} = 0.8$, $p_{0.296\,\text{ns}} = 0.2$. The third kind is mixed 0.83- and 0.296-ns delay random interval attack with probabilities $p_{\text{no}} = 0.7$, $p_{0.83\,\text{ns}} = 0.15$, $P_{0.296\,\text{ns}} = 0.15$.

As shown in Figs. 12 and 13, the attack detection strategy can detect and mitigate the random interval attacks. As shown in Table VI, TDEVs and MTIEs at average times of 1, 10, and 100 s are compared. By comparing cases of attack detection strategy without attack, with 0.83-ns attack, with 0.296-ns attack, and mixed attack, it shows that the attack detection algorithm proposed in this article can distinguish the attack events and the normal events. The differences between TDEVs and MTIE are caused by the difference in the noises. The smallest TDEVs at average times of 1, 10, and 100 s are 24.5, 3.98, and 2.95 ps, and the smallest MTIEs at average times of 1, 10, and 100 s are 122.1, 136.7, and 151.4 ps, under subnanosecond random interval attacks. By comparing cases of attack detection strategy with cases of direct correction strategy, it shows that, different from the equal interval attack, the TDEVs of the direct correction strategy does not approach the TDEV value without attack when $\tau = 100$ since the interval of the attack event is random.

V. Discussion and Conclusion

In this article, we propose a model-based method to protect the TWFTT system from subnanosecond asymmetric delay attacks. The theoretical simulation shows that the method is effective to protect the TWFTT system. Then, the method is tested under two kinds of attacks, equal interval attack and random interval attack for an experimental TWFTT system. The results show that the effect of the attack is eliminated by the method for the real TWFTT system. In order to measure the performance, TDEV and MTIE are calculated. With this method, an experimental TWFTT system of time stability with 26.4, 6.82, and 3.58 ps under subnanosecond equal interval asymmetric time delay attacks and with 24.5, 3.98, and 2.95 ps under subnanosecond random interval asymmetric time delay attacks at average times of 1, 10, and 100 s is shown. The proposed method can detect the attack in real time, and its computation complexity is low. So, this method can easily be integrated in the TWFTT system to provide secure sub-ns precise time synchronization under asymmetric delay attack.

Many interesting problems still remain. On the one hand, for longer transmission distances, such as 100-km fiber link, erbium-doped optical fiber amplifiers are integrated with the link as a repeater, which distorts the waveform. Part of

the distortion is fixed, and the other part is random. So, optimization of the delay attack detection method for longer transmission is an interesting problem. On the other hand, the network of TWFTT has attracted much attention in recent years. For the network, a node may be an intersection of multiple TWFTT paths. Except for the information from the suspected path, additional information can be provided from other paths for attack detection. So, the systematic delay attack detection method in networks is an interesting open question.

ACKNOWLEDGMENT

The authors would like to thank Dr. Giada Giorgi for the fruitful discussions.

REFERENCES

[1] 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, Oct. 2018, doi: 10.1016/j.vehcom.2018.09.001.

[2] J. Allnutt et al., "Timing challenges in the smart grid," NIST Special Publication 1500-08, 2017.

[3] J. Kodet, P. Pánek, and I. Procházka, "Two-way time transfer via optical fiber providing subpicosecond precision and high temperature stability," *Metrologia*, vol. 53, no. 1, pp. 18–26, Feb. 2016, doi: 10.1088/0026-1394/53/1/18.

[4] Y. Chen et al., "Integrated dissemination system of frequency, time and data for radio astronomy," *IEEE Photon. J.*, vol. 13, no. 1, pp. 1–7, Feb. 2021, doi: 10.1109/JPHOT.2021.3054432.

[5] M. Lipinski, T. Wlostowski, J. Serrano, and P. Alvarez, "White rabbit: A PTP application for robust sub-nanosecond synchronization," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas., Control Commun.*, Sep. 2011, pp. 25–30, doi: 10.1109/ISPCS.2011.6070148.

[6] Z. Jiang, H. Konaté, and W. Lewandowski, "Review and preview of two-way time transfer for UTC generation—From TWSTFT to TWOTFT," in *Proc. Joint Eur. Freq. Time Forum Int. Freq. Control Symp. (EFTF/IFC)*, 2013, pp. 501–504, doi: 10.1109/EFTF-IFC.2013.6702103.

[7] D. Piester, A. Bauch, L. Breakiron, D. Matsakis, B. Blanzano, and O. Koudelka, "Time transfer with nanosecond accuracy for the realization of international atomic time," *Metrologia*, vol. 45, no. 2, pp. 185–198, Mar. 2008, doi: 10.1088/0026-1394/45/2/008.

[8] Z. H. Jiang, Y. Huang, V. Zhang, and D. Piester, "BIPM 2017 TWSTFT SATRE/SDR calibrations for UTC and non-UTC links," BIPM Tech. Memorandum TM268 V2a, Tech. Rep., 2017.

[9] S. R. Jefferts, M. A. Weiss, J. Levine, S. Dilla, E. W. Bell, and T. E. Parker, "Two-way time and frequency transfer using optical fibers," *IEEE Trans. Instrum. Meas.*, vol. 46, no. 2, pp. 209–211, Apr. 1997, doi: 10.1109/19.571814.

[10] Ł. Śliwczyński, P. Krehlik, and M. Lipiński, "Optical fibers in time and frequency transfer," *Meas. Sci. Technol.*, vol. 21, no. 7, Jul. 2010, Art. no. 075302, doi: 10.1088/0957-0233/21/7/075302.

[11] P. Krehlik, Ł. Sliwczynski, Ł. Buczek, and M. Lipinski, "Fiber-optic joint time and frequency transfer with active stabilization of the propagation delay," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 10, pp. 2844–2851, Oct. 2012, doi: 10.1109/TIM.2012.2196396.

[12] B. Wang et al., "Precise and continuous time and frequency synchronisation at the 5×10-19 accuracy level," *Sci. Rep.*, vol. 2, no. 1, p. 556, Aug. 2012, doi: 10.1038/srep00556.

[13] C. Ci, Y.-X. Zhao, H. Wu, B. Liu, X.-S. Zhang, and Y. Zhang, "High-precision two-way time transfer system via long-distance commercial fiber link," *Optoelectron. Lett.*, vol. 13, no. 6, pp. 427–431, Nov. 2017, doi: 10.1007/s11801-017-7195-2.

[14] P. Krehlik, L. Sliwczynski, L. Buczek, H. Schnatz, and J. Kronjager, "Optical multiplexing of metrological time and frequency signals in a single 100-GHz-grid optical channel," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 6, pp. 2303–2310, Jun. 2021, doi: 10.1109/TUFFC.2021.3053430.

[15] J. Wang et al., "Fiber-optic joint time and frequency transfer with the same wavelength," *Opt. Lett.*, vol. 45, no. 1, pp. 208–211, Jan. 2020.

[16] F. Zuo, Q. Li, K. Xie, L. Hu, J. Chen, and G. Wu, "Fiber-optic joint time and frequency transmission with enhanced time precision," *Opt. Lett.*, vol. 47, pp. 1005–1008, Feb. 2022.

[17] J. P. Lin et al., "Michelson interferometer based phase demodulation for stable time transfer over 1556 km fiber links," *Opt. Exp.*, vol. 29, pp. 14505–14512, May 2021, doi: 10.1364/OE.420712.

[18] Ł. Sliwczynski, P. Krehlik, Ł. Buczek, and H. Schnatz, "Picoseconds-accurate fiber-optic time transfer with relative stabilization of lasers wavelengths," *J. Lightw. Technol.*, vol. 38, no. 18, pp. 5056–5063, Sep. 15, 2020, doi: 10.1109/JLT.2020.2999158.

[19] X. Guo et al., "A high-precision transfer of time and RF frequency via the fiber-optic link based on secure encryption," *Appl. Sci.*, vol. 12, no. 13, p. 6643, Jun. 2022, doi: 10.3390/app12136643.

[20] J. W. Lee, L. J. Shen, A. Cerè, J. Troupe, A. L.-Linares, and C. Kurtsiefer, "Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol," *Opt. Lett.*, vol. 45, no. 14, pp. 208–211, Sep. 2019, doi: 10.1063/1.5121489.

[21] C. Zhang et al., "Controllable asymmetry attack on two-way fiber time synchronization system," *IEEE Photon. J.*, vol. 13, no. 6, pp. 1–6, Dec. 2021, doi: 10.1109/JPHOT.2021.3121569.

[22] S. Barreto, A. Suresh, and J.-Y. Le Boudec, "Cyber-attack on packet-based time synchronization protocols: The undetectable delay box," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Taipei, Taiwan, May 2016, pp. 1–6, doi: 10.1109/I2MTC.2016.7520408.

[23] L. Narula and T. E. Humphreys, "Requirements for secure clock synchronization," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 749–762, Aug. 2018, doi: 10.1109/JSTSP.2018.2835772.

[24] T. Mizrahi, "A game theoretic analysis of delay attacks against time synchronization protocols," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas., Control Commun.*, Sep. 2012, pp. 1–6, doi: 10.1109/ISPCS.2012.6336612.

[25] A. K. Karthik and R. S. Blum, "Estimation theory-based robust phase offset determination in presence of possible path asymmetries," *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1624–1635, Apr. 2018, doi: 10.1109/TCOMM.2017.2761879.

[26] A. K. Karthik and R. S. Blum, "Robust clock skew and offset estimation for IEEE 1588 in the presence of unexpected deterministic path delay asymmetries," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5102–5119, Aug. 2020, doi: 10.1109/TCOMM.2020.2991212.

[27] M. Moradi and A. H. Jahangir, "A new delay attack detection algorithm for PTP network in power substation," *Int. J. Electr. Power Energy Syst.*, vol. 133, Dec. 2021, Art. no. 107226, doi: 10.1016/j.ijepes.2021.107226.

[28] B. Moussa, M. Kassouf, R. Hadjidj, M. Debbabi, and C. Assi, "An extension to the precision time protocol (PTP) to enable the detection of cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 18–27, Jan. 2020, doi: 10.1109/tii.2019.2943913.

[29] W. Alghamd and M. Schukat, "A detection model against precision time protocol attacks," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Riyadh, Saudi Arabia, 2020, pp. 1–3, doi: 10.1109/ICCAIS48893.2020.9096742.

[30] E. Shereen and G. Dán, "Model-based and data-driven detectors for time synchronization attacks against PMUs," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 169–179, Jan. 2020, doi: 10.1109/JSAC.2019.2952017.

[31] T. He, Y. Zheng, and Z. Ma, "Study of network time synchronisation security strategy based on polar coding," *Comput. Secur.*, vol. 104, May 2021, Art. no. 102214, doi: 10.1016/j.cose.2021.102214.

[32] 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, doi: 10.1109/TSG.2016.2644618.

[33] L. Schonberger, M. Hamad, J. V. Gomez, S. Steinhorst, and S. Saidi, "Towards an increased detection sensitivity of time-delay attacks on precision time protocol," *IEEE Access*, vol. 9, pp. 157398–157410, 2021, doi: 10.1109/ACCESS.2021.3127852.

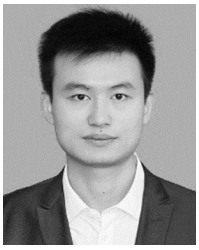
[34] L. Di Piro, E. Perone, and P. Tavella, "Random walk and first crossing time: Applications in metrology," in *Proc. 12th Eur. Freq. Time Forum*, 1998, pp. 388–391.

[35] G. Giorgi and C. Narduzzi, "Performance analysis of Kalman-filter-based clock synchronization in IEEE 1588 networks," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 8, pp. 2902–2909, Aug. 2011, doi: 10.1109/TIM.2011.2113120.

[36] W. J. Riley and D. Howe, "Handbook of frequency stability analysis," NIST Special Publication, Tech. Rep., 2008, vol. 1065.

Yang Li received the B.S. degree in physics and the Ph.D. degree in radio physics from Peking University, Beijing, China, in 2007 and 2012, respectively.

He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include secure time synchronization, quantum cryptography, and quantum information.



Jinlong Hu received the B.E. degree in mechanics and the M.A. degree in mechanical manufacturing and automation from Sichuan University, Chengdu, China, in 2018.

He is currently an Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu. His main research interest is secure time synchronization.

Yan Pan received the Ph.D. degree in information and communication engineering from Southwest Jiaotong University, Chengdu, China, in 2020.

He is currently an Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu. His research interests include quantum information, quantum cryptography, and secure time synchronization.

Wei Huang received the B.S. degree in mathematics and applied mathematics and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, in 2009 and 2015, respectively.

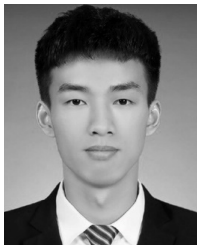
He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum secure communication, quantum information, and secure time synchronization.

Li Ma received the M.S. degree in physical electronics from the Taiyuan University of Technology (TYUT), Taiyuan, Shanxi, China, in 2017.

In 2017, she joined as an Engineer with the Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. Her research interests include quantum communication, quantum cryptography, and secure time synchronization.

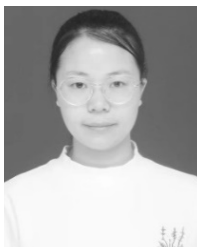
Jie Yang received the bachelor's degree in measuring instruments and controlling technology and the master's degree in communication and information systems from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011 and 2014, respectively.

He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum random number generation, quantum cryptography, quantum information, and secure time synchronization.



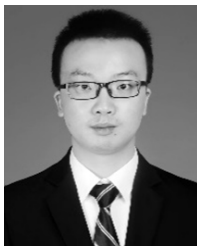
Shuai Zhang received the B.S. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2017. He is currently pursuing the M.S. degree in cryptography with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China.

His research interests include quantum information, quantum cryptography, and secure time synchronization.



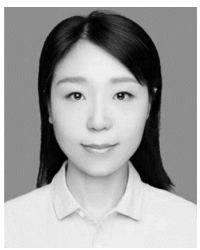
Yujie Luo received the B.S. degree in cryptography from the Institute of Southwestern Communication, Chengdu, China, in 2021.

She is currently an Assistant Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication. Her research interests include quantum information, quantum cryptography, and secure time synchronization.



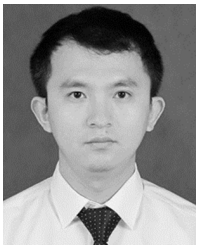
Chuang Zhou received the B.S. degree in communication engineering and the master's degree in information and communication engineering from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2018 and 2021, respectively.

He is currently an Assistant Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum information, quantum cryptography, and secure time synchronization.



Chenlin Zhang received the B.S. and Ph.D. degrees in optical engineering from the University of Electronic Science and Technology, Chengdu, China, in 2013 and 2018, respectively.

Her research interests include quantum information, quantum cryptography, and secure time synchronization.

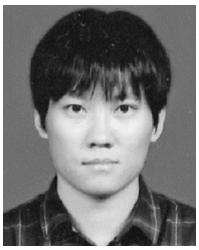


Heng Wang received the Ph.D. degree from the School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2018.

Since 2018, he has been a Senior Engineer with the Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu. His research interests include quantum secure communication, microwave photonics, and secure time synchronization.

Yun Shao received the B.S. degree in physics from Lanzhou University, Lanzhou, China, in 2013, and the Ph.D. degree in optics from Peking University, Beijing, China, in 2018.

He is currently a Senior Engineer with the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum information, quantum cryptography, and secure time synchronization.



Yichen Zhang (Associate Member, IEEE) is currently an Associate Professor with the State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China. Over the years, he has contributed to the development of the quantum key distribution using telecom components. His main research interests include quantum networks, quantum key distribution, quantum information theory, and quantum internet.

Xing Chen received the Ph.D. degree in radio physics from Peking University, Beijing, China, 2016.

She is currently an Associate Professor with the School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing. Her research interests include high-precision time–frequency transfer technology and network application, femtosecond laser, and measurement technology.

Ziyang Chen received the Ph.D. degree in quantum electronics from Peking University, Beijing, China, in 2020.

He is currently a Research Assistant Professor with the School of Electronics, Peking University. His current research interests include time and frequency transfer, quantum cryptography, quantum key distribution, and quantum random number generation.

Song Yu received the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2005.

He is currently a Professor with the School of Electronic Engineering, Beijing University of Posts and Telecommunications. His research interests include high-precision time–frequency transfer technology and quantum key distribution.

Hong Guo (Member, IEEE) received the B.S. degree from the National University of Defense Technology, Changsha, China, in 1991, and the M.S. and Ph.D. degrees from the Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, Shanghai, China, in 1993 and 1995, respectively.

He is currently a Professor with the School of Electronics, Peking University, Beijing, China. His research interests include quantum optics and quantum information.

Bingjie Xu received the B.S. degree in physics and the Ph.D. degree in radio physics from Peking University, Beijing, China, in 2007 and 2012, respectively.

He is currently the Chief Expert of the Department of Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, China. His research interests include quantum cryptography, quantum information, and secure time synchronization.