IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 8, 2020, accepted May 22, 2020, date of publication May 27, 2020, date of current version June 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2998036

Physical Layer Authentication Based on BER Measurement of Optical Fiber Channel

XIANGQING WANG, YAJIE LI, YONGLI ZHAO, (Senior Member, IEEE), CHAO LEI, HUIBIN ZHANG, AND JIE ZHANG

State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Jie Zhang (jie.zhang@bupt.edu.cn)

This work was supported in part by the NSFC under Grant 61831003 and Grant 61901053, in part by the Joint Foundation of Ministry of Education of China and Department of Equipment Pre-Research, in part by the University Natural Science Research Project of Anhui Province under Grant KJ2019A0616, and in part by the Key Projects in Natural Science of West Anhui University under Grant WXZR201719.

ABSTRACT Physical layer authentication is an important way to ensure the security of optical communication network. We hereby propose a scheme to realize it by measuring the variation of the bit error rate (BER) on both sides of communication. In this scheme, the legitimacy of the receiver is identified by analyzing the BER variation of the optical fiber loop based on the short-term correlation of the channels. We then simulate a 16 PSK optical transmission system with intensity modulation direct detection-orthogonal frequency division multiplexing (IMDD-OFDM). The authentication effect is analyzed in the case of disturbance and beam split, as well as replacement of optical fiber channels caused by eavesdropper (Eve). The results show that this scheme is sensitive to the three kinds of attacks. A high probability of detection (PD) and a low false alarm rate (FAR) can be obtained. The experimental results show that with the increase of the frequency test, PD and FAR tend to be stable, and the authentication effect is better with the accuracy rate 100%.

INDEX TERMS Physical layer authentication, bit error rate, intensity modulation direct detection orthogonal frequency division multiplexing, false alarm rate.

I. INTRODUCTION

Optical communication networks transmit all kinds of sensitive and private information, so the security of optical transmission is increasingly important. In order to ensure the security of optical fiber communication, it is necessary to verify the identity of both parties. At the same time, security authentication is also an important prerequisite for other security approaches like key distribution and data encryption [1]–[3].

The traditional authentication is realized by the mathematical algorithm of the application layer [4]–[6]. Nevertheless, it will make the application layer more complex and consume a lot of computing resources. In quantum communication, the physical quantum (PUF) cannot be cloned and predicted, which has made it possible to design the authentication or anti-counterfeiting protocols based on PUF devices [7], [8]. However, the security analysis based on PUF quantum authentication protocols is immature and unintegrated.

In wireless communication, more focuses have been put on the research of physical layer authentication based on the wireless channels which are ephemerally reciprocal and location-dependent [9]–[13]. It was also put forward the authentication realized by multi-carrier transmission and fingerprint embedding [14], [15]. However, there is a lack of present research involved in authentication based on the physic layer in optical fiber channel. Unlike wireless channels, the optical fiber channels are relatively stable and it is convenient to extract the physical features [16]–[18]. Additionally, the unidirectional transmission of optical signals makes the authentication method of physical layer security in optical fiber channel different from that in wireless channel. Therefore, it is necessary to further study the physical layer authentication technology suitable for optical fiber communication.

In this paper, a physical layer authentication mechanism based on BER variation of optical fiber loop is proposed. We simulate a 16 PSK intensity modulation direct detection

The associate editor coordinating the review of this manuscript and approving it for publication was San-Liang Lee.

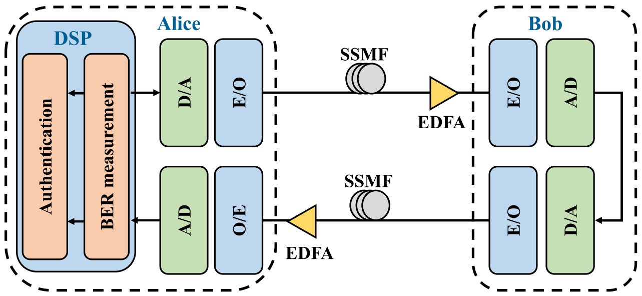

FIGURE 1. The process of Alice authenticating the legitimate receiver Bob.

orthogonal frequency division multiplexing (IMDD-OFDM) optical transmission system, where the demonstrated three attacks by Eve are carried out. In the first case, Eve interferes with the optical signal by introducing extra noise, which decreases the optical signal to noise ratio (OSNR) of the system. In the second case, Eve uses an optical splitter to eavesdrop on the optical signal, which increases the optical power loss. In the third case, Eve replaces the legitimate receiver (Bob), which causes the actual transmission distance to be shortened. The FAR and the PD are analyzed respectively in the three cases. The results show that this scheme is sensitive to the three kinds of attacks. A high PD and a low FAR can be obtained. In this paper, we conducted experimental frequency test and further verified the authentication effect in the scenario of the attack by Eve. We perform DSP processing on the signals collected by the oscilloscope (OSC), which include demapping, judgment and so on. Finally, the BER is calculated and the authentication test is carried out. The experimental results show that Alice can correctly distinguish the legitimate receivers from the illegal ones. Therefore, Alice can authenticate correctly.

II. THE PHYSICAL LAYERAUTHENTICATION SCHEME BASED ON MEASUREMENT

Wireless communication is bidirectional in transmission. However, optical fiber communication is unidirectional in transmission, even though there is not only single bidirectional but also single unidirectional fiber. Unlike wireless communication, the actual optical fiber network is unidirectional. The easily measured BER of the fiber loop between Alice and Bob reflects the change of the fiber channel and the transmission performance. Under normal circumstances, the fiber channel is relatively stable and the measured BER does not fluctuate much. However, when Eve attacks or interferes with the optical fiber channel, the measured BER will inevitably fluctuate. We take the change of BER as an important index of physical layer authentication. When the variation of BER is greater than the threshold value, the system is considered to be attacked by Eve. When the variation of BER is less than the threshold value, the receiver is considered legitimate.

Fig. 1 shows the process in which Alice authenticates the legitimate receiver Bob. DSP in transmitter at Alice side generates a series of random bit stream D^A. After the bit stream is mapped into 16 PSK data, it is modulated with IMDD OFDM. The OFDM data is sent in the form of a data frame. The data length of each frame is N bits. After digital-to-analog converter (DAC) and electro-optical modulator, the OFDM signal reaches the Bob side through the optical fiber. The direct detection receiver converts the optical signal into electrical signal, and the analog-to-digital converter (ADC) samples the signal. The collected signal is sent directly through DAC and electro-optical modulator. Passing through the optical fiber, the signal is transmitted to Alice side. After the signal goes through the direct detection receiver and ADC, Alice demodulates the signal into binary bit stream D^{ABA}. The BER of the fiber loop is calculated by comparing D^A and D^{ABA}.

When the BER of optical communication signals is calculated, the influence of channel noise and phase noise on the signal must be fully considered. The specific analysis is as follows.

$$s(\mathrm{t}) = e^{j(2\pi f_0+\varphi(\mathrm{t}))} + \beta e^{j(2\pi\Delta f+\varphi(\mathrm{t}))}\sum_{k=1}^{N} a_k e^{j(2\pi f_k)} + n(\mathrm{t}) \quad (1)$$

At the transmitting end, a signal with frequency and phase noise can be represented by Eq. (1). Among them, s(t) is the optical signal, β is the proportionality factor, f_0 is the main frequency signal, Δf is the frequency offset, φ(t) is the phase noise, and n(t) is the additive white Gaussian noise (AWGN). a_k and f_k are the sign and frequency of the signal of the k subcarrier, respectively. After the signal passes through the fiber link, it can be expressed by Eq. (2).

$$s(\mathrm{t}) = e^{j(2\pi f_0+\phi_D(-\Delta f)+\varphi(\mathrm{t}))}+\beta e^{j(2\pi\,\Delta f+\varphi(\mathrm{t}))}s_B(\mathrm{t})+n(\mathrm{t}) \quad (2)$$

$$s_B(\mathrm{t}) = \sum_{k=1}^{N} a_k e^{j(2\pi f_k+\phi_D(\Delta f))} \quad (3)$$

Among them $\phi_D(f_k)$ is the phase delay caused by the dispersion coefficient. At the receiving end, the photocurrent is expressed by Eq. (4).

$$I(\mathrm{t}) = |s(\mathrm{t})|^2 = 1+\beta\mathrm{Re}\left\{e^{j(2\pi\,\Delta f+\varphi(\mathrm{t}))}\sum_{k=1}^{N} s_B(\mathrm{t})+n(\mathrm{t})\right\} \quad (4)$$

When the photocurrent is detected to be converted by the ADC, it is demodulated and restored to the original signal after being processed by the DSP. When the BER of the signals modulated by MPSK is calculated, the influence of factors such as phase noise must be fully considered too.

Alice denotes the BER of three consecutive frames as BER_{k-2}, BER_{k-1} and BER_k. In order to accurately record the dynamic change of channel, the BER variation of three consecutive frames is calculated and normalized, as is shown in Eq. (5).

$$T = \left|\frac{BER_k - BER_{k-1}}{BER_{k-1} - BER_{k-2}} - 1\right| \quad (5)$$

At k-1 and k-2, there is no attack. At this time, Alice measures the BER_{k-1} and BER_{k-2}. When attacked, Alice measures the BER_k. By bringing BER_{k-1}, BER_{k-2} and BER_k

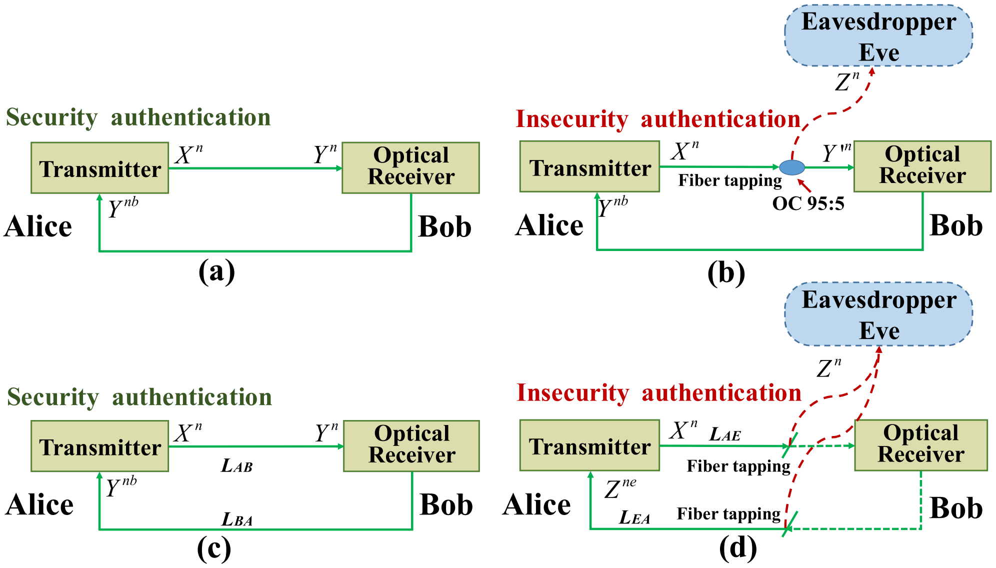

FIGURE 2. Different ways of authentication in different situations.

into Eq. (5), T increases. Therefore, the increase of T is the important indicator of whether the system is attacked. By setting the threshold, we can get $T > \eta$, so we can detect the attack. Whether BER becomes larger or smaller, T will increase. When Eve splits eavesdropping, the loopback BER measured by Alice becomes larger. When Eve eavesdrops between Alice and Bob, the loopback BER measured by Alice becomes smaller. Therefore, as the loopback link BER increases or decreases, there is a risk of eavesdropping. The BER fluctuation of a normal optical fiber transmission system is within a certain range, and the BER variation is relatively small at this time. When Eve eavesdrops, it will increase the range of the BER fluctuation of the optical fiber link. At this time, the BER fluctuation is relatively large, and T increases. By setting a threshold, when the BER change T is greater than the threshold, it is considered that the system has eavesdropping and the authentication fails. When the BER change T is less than the threshold, it is considered that there is no eavesdropping and the authentication succeeds.

When Alice communicates with the legitimate receiver Bob, the BER variation T obtained by Alice is small and the channel is relatively stable. When Eve attacks the fiber channel, it will cause the fluctuation of BER and the BER variation T is greater than normal.

Physical layer authentication is usually considered as a hypothesis-testing problem, which is developed to verify the performance of the proposed authentication scheme. The binary hypothesis-testing problem is correspondingly expressed in Eq. (6).

$$\begin{cases} H0 : T \leq \eta \\ H1 : T > \eta \end{cases} \tag{6}$$

In Eq. (6) *H0* is the null hypothesis, indicating that the receiver is legitimate. H1 indicates that Eve participates in the communication. The BER variation T is compared with the threshold η. When $T \leq \eta$, the receiver is considered legitimate and the system is not under attack. When $T > \eta$, the system is considered to be attacked by Eve.

This system refers to the literature [19] for threshold selection, with the actual situation taken into account. We use the method of traversing the threshold to find the best threshold, thereby improving the authentication effect. By traversing the threshold $\eta > 0$, the PD and the FAR corresponding to different thresholds are calculated. Through simulation, it is found that when the threshold value $\eta > 30$, the PD and the FAR tend to zero. The change range of T is mostly in the range of 0~50, so the threshold is also selected in the range of 0~50. Therefore, there is no need to increase the measurement interval of the threshold. So we choose the threshold η to traverse between (0-50).

Generally, the changes of PMD noises, EDFA noises, detector noises and other factors are slight, and there is no obvious fluctuation in a short time. The authentication scheme proposed in this paper is applicable in the situation where the BER fluctuates greatly in a short period of time. The threshold value is related to the FAR and the PD. With the increase of the threshold value, the FAR and the PD decrease. In order to get a lower FAR and a higher detection probability, it is necessary to set a threshold for a better effect of authentication. In order to improve the PD, the threshold can be reduced but the FAR will improve, so there is a balance between PD and FAR.

As is shown in Fig. 2(a), under normal circumstances, Alice sends the information n-bit, Bob receives it as Y^n and then resends it to Alice. Finally, Alice receives the information as Y^{nb}. The physical channel characteristic such as the BER is calculated and a secure authentication mode is constructed. As is shown in Fig. 2(b), the fiber link is

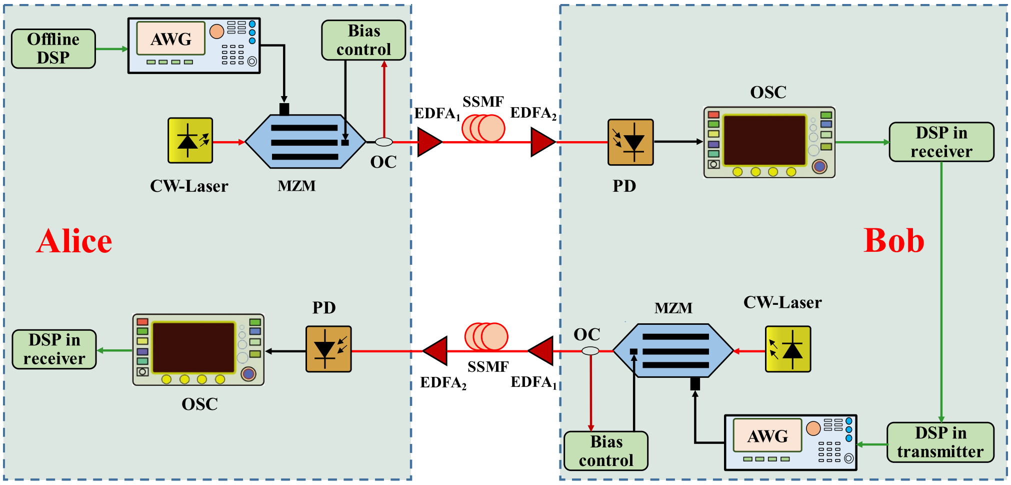

FIGURE 3. Simulation setup for authenticating system.

eavesdropped by Eve and the stolen optical information capacity is Z^n Bob receives the data Y'^n sent by Alice, and then sends Y^{nb} to Alice. Because the optical link is broken by Eve, the characteristics of the measured channel will change. Through calculation and analysis, the channel is changed to an untrusted one, so non-secure authentication is achieved. As is shown in Fig. 2(c), when there is a certain distance, Alice sends information to Bob and the distance of loop measurement is $L_{AB} + L_{BA}$. As is shown in Fig. 2(d), in the case where Eve cuts the fiber link, Eves forges Bob to send information to Alice. Since the cut position changes, the loop distance changes even if the signal information is not lost. In this way, the distance measured by the loopback is $L_{AE} + L_{EA}$. The physical characteristics of the fiber link are changed due to the change of the distance. The untrusted channel is determined and the non-secure certification is then achieved.

In order to evaluate the performance of the proposed authentication scheme, the FAR and the PD are calculated. The FAR refers to the fact that the system is wrongly judged to be under attack when there is no attack. The calculation of the FAR is shown in Eq. (7), where F and M are the frequency of false reports and experiments respectively. The PD refers to the probability that the system is correctly detected to be attacked by Eve. The calculation of PD is shown in Eq. (8), where A and C are the number of Eve's attack and correct detection of the attacks respectively. Similarly, Bob can authenticate Alice in the same way.

$$FAR = \frac{F}{M} \tag{7}$$

$$PD = \frac{A}{C} \tag{8}$$

Optical fiber channel is relatively stable since natural interference such as the change of temperature, humidity and pressure has little influence on its characteristics as well as the authentication. In order to continuously monitor the authenticated party, a separate monitoring channel is adopted. Setting up a single monitoring channel can lead to a large bandwidth overhead, but it can improve the success rate of authentication. The authentication scheme mentioned in this paper can be applied to the existing WDM optical network. A wavelength channel of WDM system is used as the authentication channel, so some additional equipment on the basis of WDM such as transmitters, receivers, modulators and so on is really needed. Because different wavelengths are isolated from each other, the transmission performance of other channels will not be affected. Generally speaking, fiber aging is a very slow process, and there is no obvious fluctuation in a short time. The scheme mentioned in this paper is sensitive to the large fluctuation of BER in a short period of time, but insensitive to the slow change of BER. Besides the existing WDM optical network, the authentication can also be applied to PON and bidirectional networks. PON uses time-division multiplexing for communication. At one time, it can be considered that the optical fiber communication is unidirectional, and this scheme can be extended to bidirectional networks. Each wavelength of WDM is equivalent to an independent channel, so the authentication scheme is also applicable. We will carry on the detailed simulation and experimental demonstration in the later paper.

III. SIMULATION PRINCIPLE AND SYSTEM CONFIGURATION

A. SIMULATION SETUP

Fig. 3 shows that at the transmitter end, Alice sends the original data to AWG after offline processing by DSP module at a rate of 20Ga/s. Then, it is loaded onto the optical carrier by IM-DD modulator. The red line is the optical path while the black line is the electric signal. The optical signal is amplified by erbium-doped fiber amplifier (EDFA), and then enters the 200km optical fiber link. At the receiving end, the optical signal is amplified by EDFA, and then enters the photoelectric detector. Finally, the DSP module recovers the

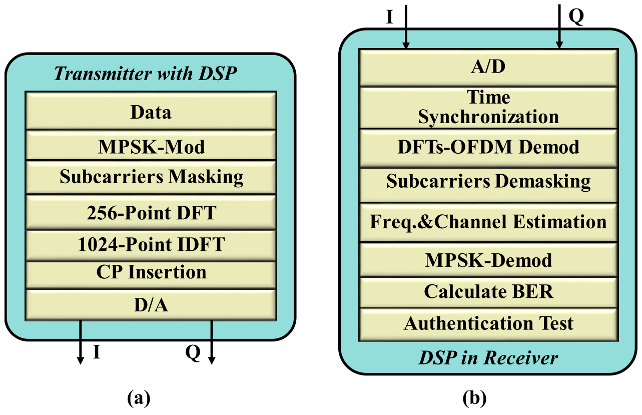

FIGURE 4. Digital signal processing for the authenticating at the transmitter and receiver.

original data. After signal recovery processing, Bob sends it to Alice in the same way. In this way, Alice determines the fingerprint parameter index of trusted channel by returning the measurement and calculating the error rate of data. In this scheme, Monte Carlo model is used to simulate and verify by MATLAB.

The authentication process in this article is divided into six steps, step1, step2 $\cdots$ step6, to complete a test authentication process. The specific authentication steps are as follows:

Step 1: Alice generates a data stream D^A through a pseudo-random number generator PRBS, maps the bit stream to 16PSK, and modulates it through IM-DD for transmission.

Step 2: The data received by Bob are $D^{AB} + N_{AB}$, and N_{AB} is the noise that Alice sends to Bob. Then the data received by Bob are sent to Alice.

Step 3: Alice receives the data $D^{ABA} + N_{ABA}$ from Bob, and N_{ABA} is the noise that Bob sends to Alice.

Step 4: Alice compares the signal D^A with the signal $D^{ABA} + N_{ABA}$ through loopback measurement, and calculates the BER.

Step 5: The normalized BER T is calculated by Eq (5). When the value of T is relatively small, it is a legitimate receiving end. By comparing the value of T, Bob is authenticated.

Step 6: A BER threshold η is set. When $T \leq \eta$ Bob is authenticated successfully to a legitimate receiver, that is, the authentication status is *H0*. When $T > \eta$, Eve is authenticated unsuccessfully for the illegal receiving end, that is, the authentication status is *H1*.

Fig. 4 shows the processing flow of the DSP module at the transmitter and receiver. At the transmitter, firstly the binary sequence of the original data is mapped to MPSK format. Then the subcarriers are loaded and it is modulated as DFT-OFDM signal. Finally, with the CP signal inserted and analog-to-digital conversion performed, it enters into the IM-DD modulator. At the receiving end, firstly the analog-to-digital conversion is carried out and the data signal is synchronized in time. Then the DFT-OFDM demodulation is carried out and the signal in MPSK format is generated by inverse mapping of the demodulated signal. Finally, the BER of the data at the transmitter and receiver is calculated, and the authentication test is carried out. Through testing the trusted channel, the fingerprint features can be extracted. The trusted and the untrusted channel are distinguished by the parameters of fingerprint characteristics.

The BER of the authentication system can be measured using single-carrier or multi-carrier signals. IM/DD-OFDM transmission has the advantages of high spectral efficiency [20], [21], simple realization and fine anti-fading performance. Therefore, we use the IM/DD-OFDM signal to measure the BER of the system.

The BERs of each three consecutive data frames can be used to calculate a normalized BER variation T. Then the binary hypothesis test is used to determine whether the system has been attacked by Eve. Furthermore, the FAR and the PD are calculated. The length of each data frame is set to 2^{15} bits. When T is less than η, the receiver is considered legitimate. When T is larger than η, the system is considered to be attacked by Eve. In the case that the receiver is legitimate, we conduct Monte Carlo simulations for 1000 times to calculate the probability of T greater than η as the false alarm rate. Similarly, in the case of Eve attack, 1,000 times Monte Carlo simulations are performed to calculate the probability of T less than η as the detection rate.

The authentication scheme is analyzed in the case of high-order PSK, but not limited to the PSK signal. The high-order QAM signal is also applicable. The key of this scheme is to measure the change of BER. In order to make BER change obviously, it is necessary to reduce the SNR of the system and improve BER. The higher-order modulation format signal and the method of reducing the optical power of the transmitted signal can be used.

B. RESULTS AND DISCUSSION

BER is the key index of the authentication scheme. In order to accurately reflect the change of fiber channels, the value range of BER should be limited. However, too small BER value means large fluctuation and randomness, which will reduce the authentication accuracy. If the BER is too high, it will be insensitive to fiber channel change. Therefore, it is necessary to control the BER value within an appropriate range. Fig. 5 shows the received constellations of 8 PSK, 16 PSK and 32 PSK signals after passing through 200 km optical fiber loop. The calculated BERs of these three signals are 5.65×10^{-3}, 3.36×10^{-2} and 1.91×10^{-1}, respectively.

As is shown in Table 1, it is the simulation specific parameters. The BER of 8 PSK signal is too small and random to accurately reflect the fiber channel change. The BER of 32 PSK signal is too large and not sensitive to reflect the fiber channel change. Therefore, the 16 PSK signal is selected for this authentication scheme. We simulate three types of Eve attacks. In the first case, Eve interferes with the normal fiber channel by introducing additional noise, which will reduce the channel OSNR and increase the BER. We set the OSNR of

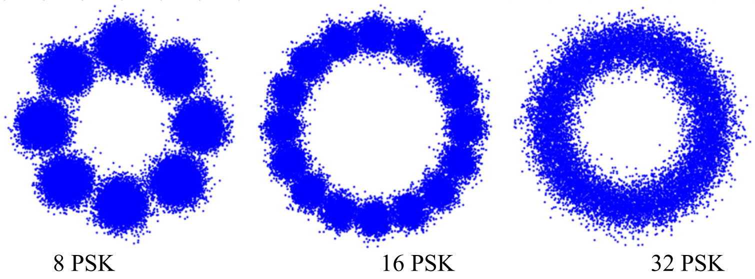

FIGURE 5. Received constellations of 8 PSK, 16 PSK and 32 PSK signals.

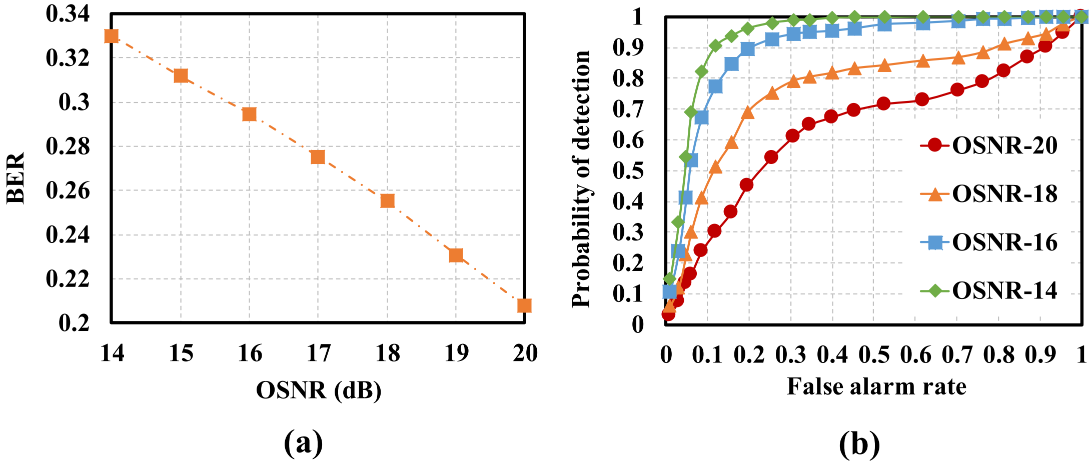

FIGURE 6. (a) The BER variation of optical fiber loop as a function of OSNR. (b) The relationship between false alarm rate and probability of detection with different OSNRs.

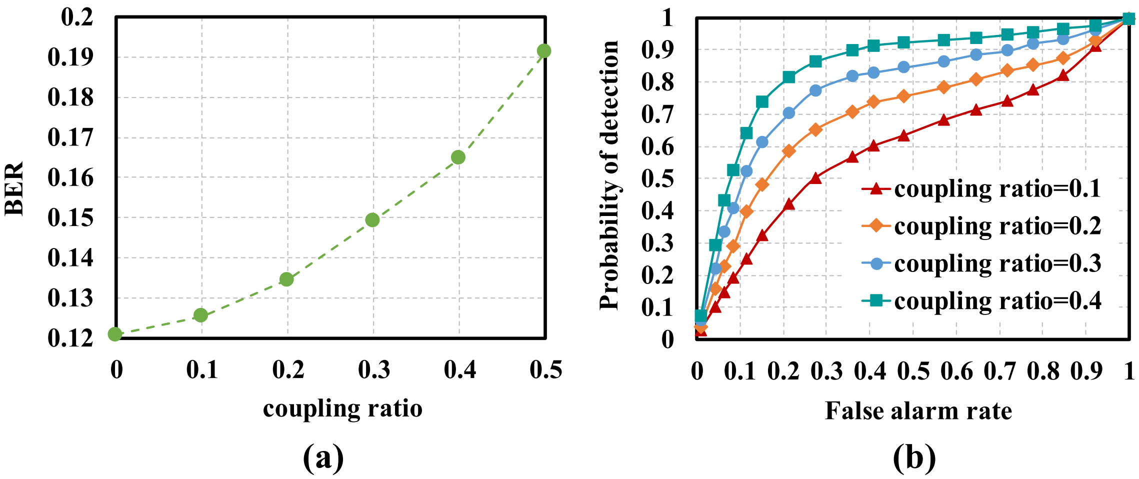

FIGURE 7. (a) The BER variation of the optical fiber communication system with different coupling coefficient. (b) The relationship between false alarm rate and probability of detection with different coupling coefficient of Eve.

the fiber channel without Eve's attack to 20. By reducing the OSNR, we simulate different degrees of Eve's interference with the fiber channel.

In the process of simulation, the loss of the system in 16PSK is as follows. Alice sends the signal. EDFA$_1$ output is 0dBm, the link loss is 40dB together with others losses such as noise losses and the gain of EDFA$_2$ is 10dB, so the final received power is worse than −30dBm. Bob receives the signal and performs DSP processing. Similarly, Bob sends the signal to Alice according to the same parameter settings to complete the loopback measurement data. It is also true of that in 8 PSK and 32PSK.

Through the BER variation T, the fiber channel can be judged whether it is attacked or not. Fig. 6(b) shows the

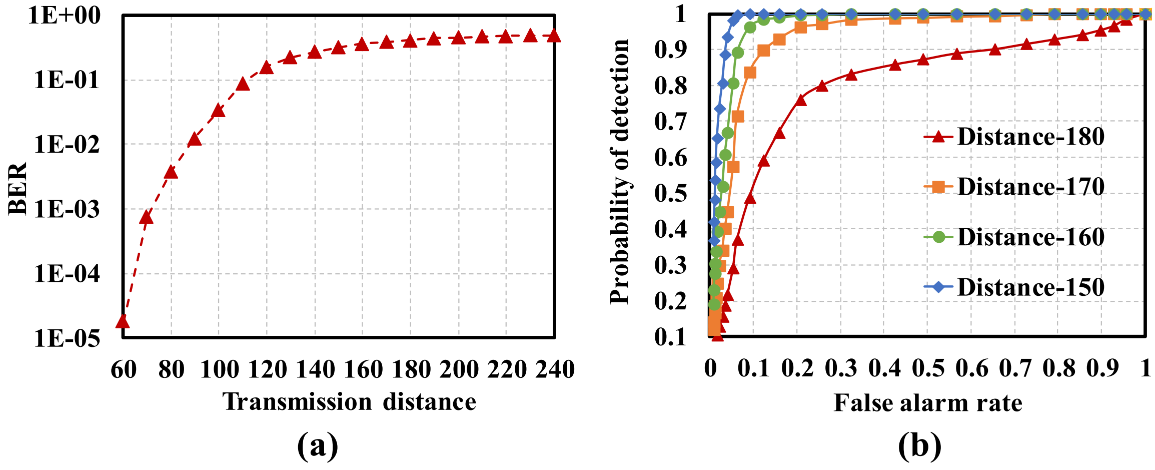

FIGURE 8. (a) The BER variation measured by Alice as a function of the distance from Alice to Eve. (b) The relationship between FAR and PD with different transmission distances from Alice to Eve.

TABLE 1. Simulation parameter list.

Equipment	Parameter Configuration
Detector noise	I_D=1e-9 A, Thermal noise=1e-11W/Hz
Detector responsivity	0.5A/W
Dispersion of the fiber	17ps/nm/km
$EDFA_1$	Output Power: 0dBm
Nonlinearity coefficients of the fiber	2.7e-20 m^2/W
$EDFA_2$ and noise parameters	Output Power: less than -30 dBm Noise parameters:5 dB
Losses in all the link components	200km,0.2dB/km, 40dB

relationship between the FAR and the PD with different OSNRs. With the increase of the FAR, the PD first increases rapidly and then slowly. The faster the PD increases, the better the performance of this authentication scheme is. It can be seen that the smaller the OSNR is, the faster the PD increases and the better the authentication performance is. This is because it is easier to detect Eve's attack in this case. In the second case, Eve uses an optical splitter to eavesdrop on the optical signal, which will affect the power of received signals and the BER of optical communication system. The coupling coefficient is used to represent the proportion of the optical power intercepted by Eve in the total power.

Figure 5 and figure 6 are generated by MATLAB simulation. The transmit power is set at 0dbm. The standard single-mode optical fiber is used. The optical fiber loss is 0.2dB/km, and the detector is intensity modulation detector.

The BER of the normal optical fiber transmission system is very small, so its BER fluctuation is very small and difficult to detect. We use the higher-order PSK signal and reduce the optical power to improve the BER. A wavelength channel of WDM system can be used as the detection channel to improve the BER through higher-order PSK and lower optical power. As the channels are independent of each other, other normal channels will not be affected.

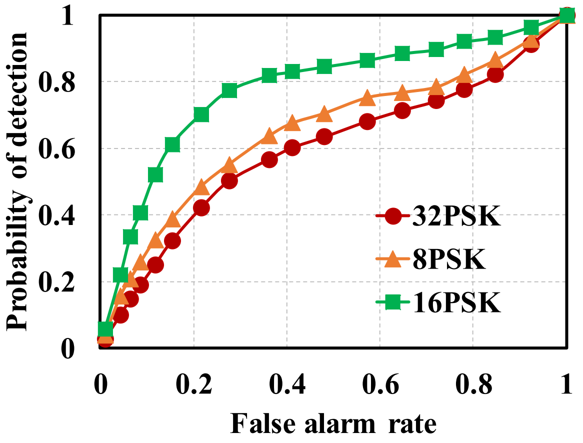

FIGURE 9. Comparison of authentication parameters under different modulation formats.

Fig. 7(a) shows the BER variation of the optical fiber communication system with different coupling coefficient. The coupling coefficient refers to the proportion of the optical power divided by Eve in the total optical power. As the coupling coefficient of Eve increases, the BER of the system increases gradually. Therefore, by detecting the BER variation T, the fiber channel can be judged if it is attacked. Fig. 7(b) shows the relationship between the FAR and the PD with different coupling coefficient of Eve. It can be seen that the greater the coupling coefficient is, the faster the PD increases and the better the authentication performance is. This is because as the coupling coefficient increases, the BER variation augments and Eve's attack is easier to be detected.

In the third case, Eve disguises as the legitimate receiver to carry out the substitution attack. For Alice, this is equivalent to a shorter transmission distance, which means the lower BER of the fiber loop. The distance between Alice and Bob is set at 200km. Eve conducts a substitution attack close to Bob. Fig. 8(a) shows the BER variation measured by Alice as a function of the distance from Alice to Eve.

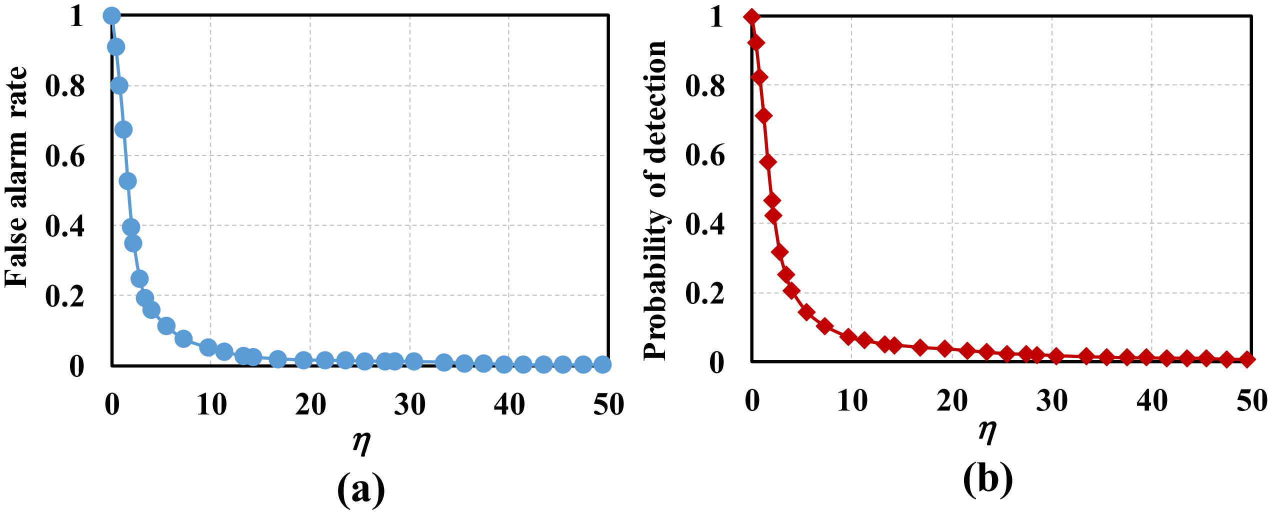

FIGURE 10. (a) FAR corresponding to different thresholds η. (b) PD corresponding to different thresholds η.

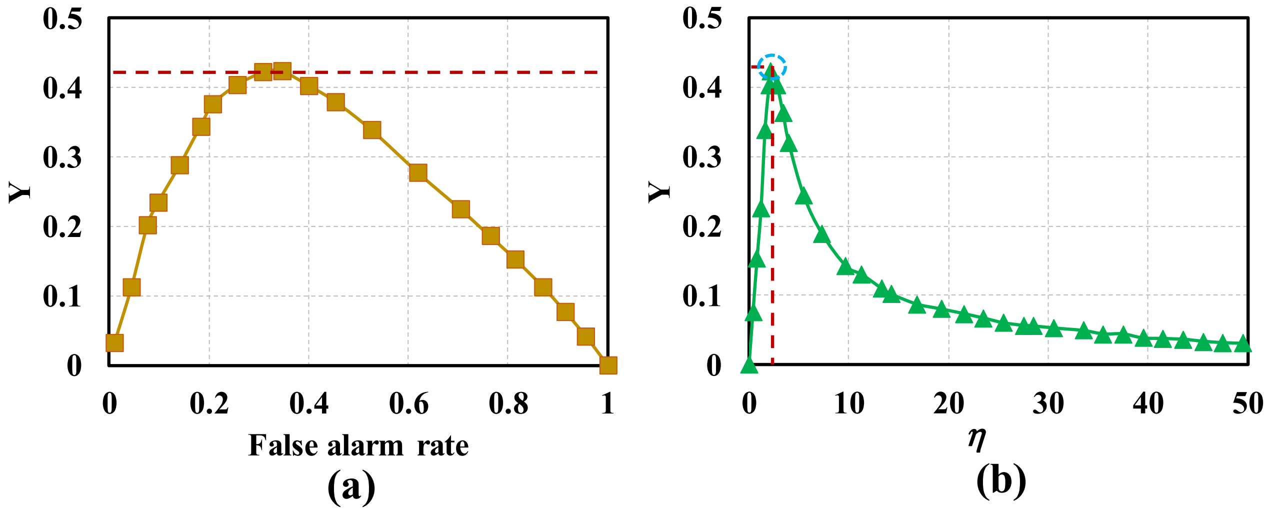

FIGURE 11. (a) Relationship between authentication coefficient Y and FAR. (b) Authentication coefficient Y corresponding to threshold η.

As the distance decreases, the BER of the system gradually decreases. Therefore, the fiber channel can detect whether it is attacked or not by calculating the BER variation. Fig. 8(b) shows the relationship between the FAR and the PD with different transmission distances from Alice to Eve. It can be seen that as the distance becomes shorter, the authentication performance becomes better. This is because the smaller the distance from Alice to Eve is, the larger the BER variation is, and the easier Eve's substitution attack is to be detected. As is shown in Fig. 8 (b), with the distance closer to 200km (Eve closer to Bob), the PD will decrease at the same the FAR. If Eve is very close to Bob, the authentication will fail.

We analyze theoretically why 16PSK is used instead and 32PSK. When the signal is in 8PSK modulation format, the BER is small and its change is not obvious, so the authentication performance is not good. During 32PSK modulation, the detected signal noise is too large, the BER fluctuates greatly, which cannot effectively distinguish legitimate channels from illegal ones, so the authentication performance is not good. Therefore, the BER of the system needs to be reasonably controlled. It cannot be too large or too small. When 16PSK is selected, the BER is appropriate and the authentication effect is good. As is shown in Fig. 9, the PD curve in the 16PSK modulation format is higher than that in the 32PSK, 16PSK modulation format.

The BER of the system is improved by using the method of higher-order PSK modulation and reducing the transmitted optical power. In the case of high BER, there is no effective communication. Our authentication scheme can be combined with WDM network. One wavelength channel is used for system authentication. Because different wavelengths are isolated from each other, communication can be carried out in other wavelength channels.

C. OPTIMAL AUTHENTICATION ANALYSIS

In this system a traversal method for the selection of thresholds is used. The threshold η is traversed between (0-50) to calculate the PD and the FAR corresponding to different

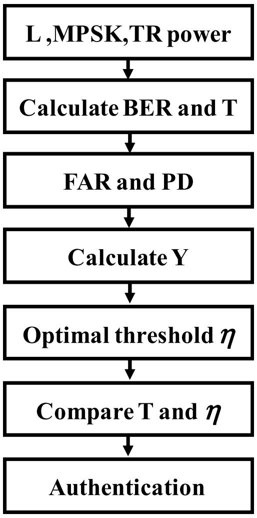

FIGURE 12. Authentication flow chart under different conditions.

TABLE 2. Deviece configuration model and parameters.

Equipment	Model Specifications	Parameter Configuration
AWG	M9505A	TR Rate: 10G/s TR Voltage: 200mv
Modulator	FTM7962EP	Baud Rate: 32GBaud
Light source	CoBrite-DX4	Wavelength: 1550nm , TR Power: 6dBm
$EDFA_1$	AmonicsAEDFA-IL-13B-FA	Output Power: 4dBm
Ultra-low loss fiber	ULL-G654-A130	200km,0.154dB/km
$EDFA_2$	AmonicsAEDFA-IL13B-FA	Output Power: 0dBm
Demodulator	TIM24706/303	Max Bandwidth: 28GHz Max Data Rate: 56Gbps
Oscilloscope	Wave Master 8Zi 4GHz-45GHz	Frequency Offset: 0 Sampling Rate: 20Gsa/s

thresholds. According to 10000 experiments, there are N Ts greater than the threshold, (10000-N) Ts less than the threshold to calculate the PD and the FAR. A set of PD and FAR values can be calculated for each threshold.

As is shown in Fig. 10(a) and Fig. 10(b), with the increase of threshold, the FAR and the PD decrease. Therefore, it is necessary to weigh the FAR and PD, and set a threshold.

$$Y = PD^{*}(1 - FAR) \tag{9}$$

For the authentication system, we want the PD to be as large as possible and the FAR to be as small as possible. Therefore, the variable Y is defined, as is shown in Eq. (9). When Y takes the maximum value, the authentication performance of the system is considered to be the best. Taking $Y = Y$ max, it can get the best authentication performance. Fig. 11(a) shows that when the curve reaches the peak, Y max $= 0.42$, FAR $= 0.34$, the authentication effect is the best. Fig. 11(b) shows that when the threshold η is traversed, the coefficient Y first increases and then decreases, and the peak position is the best authentication coefficient point. At this time, the corresponding threshold value, $\eta = 2.2$ is the optimal authentication threshold. 2.2 is a time-dependent variable. With the change of time, the average BER of the system will also change, but the change is limited, so the optimal threshold can be calculated every other day. Because the changing fiber changes slowly, it is calculated once a day. It is through traversing various modulation formats and all transmission powers to find the largest Y value. The corresponding threshold is the optimal threshold value. The larger the Y value is, the better the authentication effect as well as the modulation format and transmission power will be.

As is shown in Fig.12, under different transmission distances, modulation formats, and transmit powers, the BER is measured by loopback. By traversing the distance L, the modulation format MPSK, and the transmission power TR Power, the best BER are found, and the T value is calculated. Then the FAR and the PD corresponding to different thresholds are calculated, we find the best threshold point through the Eq. (9). Finally, the best threshold point and T are compared to achieve system authentication. In the case of 200km, 16PSK is the best. Subsequent research will supplement other modulation formats and transmit power values.

By calculating Y, the FAR and the PD once a day, the best threshold can be calculated. By comparing T with the optimal threshold, when T is greater than the threshold, authentication fails, and when T is less than the threshold, authentication succeeds. By increasing the frequency of authentication as much as possible, the risk of Eve eavesdropping can be reduced

IV. EXPERIMENTAL SETUP

This experimental scheme mainly measures signals through loopback measurement. Firstly, at the transmitting end of Alice are a laser, a pseudo-random generator and an AWG as well as a modulator. As is shown in Fig. 13, the signals are the 10Gbit/s of 8PSK, 16PSK, 32PSK. After the EDFA signal is amplified at the transmitting end, it enters into the 200km optical fiber link. After it is amplified at the receiving end, Bob demodulates the signal through a demodulator and sends it to Alice based on the same transmission method. At the receiving end, Alice demodulates the recovered original signal through a demodulator, and collects data through the OSC for DSP processing. In the experimental scheme, Alice uses loopback measurement to finally input the signals collected by the OSC into the DSP processor, demaps the data, and calculates the BER through judgment. The generated BER is first processed by normalizing and then goes through safety certification tests. The distinction of the legitimate channel from the illegal one is realized by comparing their fingerprint characteristics. Then Alice's judgment on Bob's security authentication is reached. Similarly, based on the same method, Bob completes Alice's security authentication and the effect of two-way authentication is achieved.

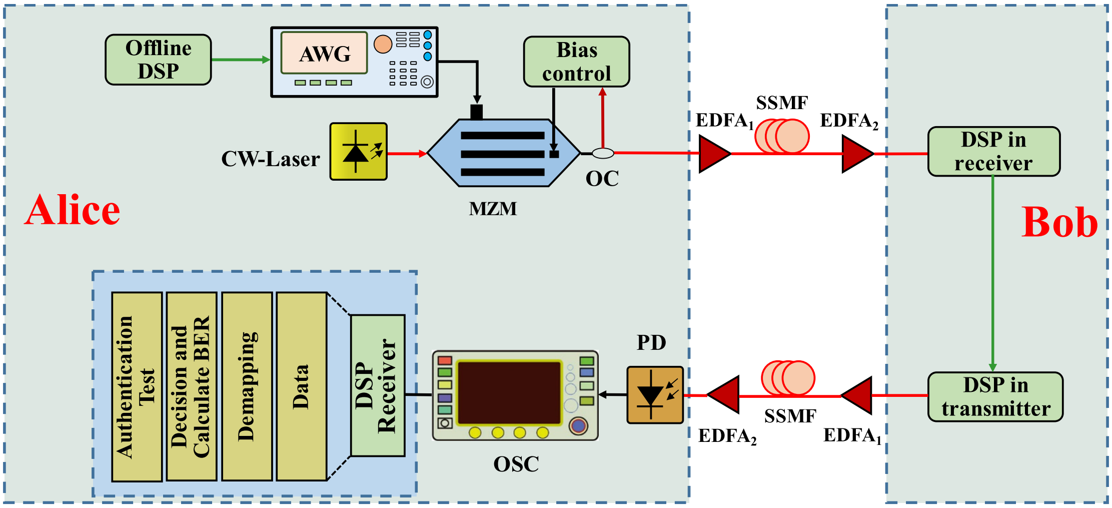

FIGURE 13. Diagram of security authentication principle in the experimental system. AWG: arbitrary waveform generator. MZM: Mach-Zehnder Modulator. SSMF: Standard Single Mode Fiber. OC: optical coupler. EDFA: erbium-doped fiber amplifier. PD: photodiode. OSC: oscilloscope.

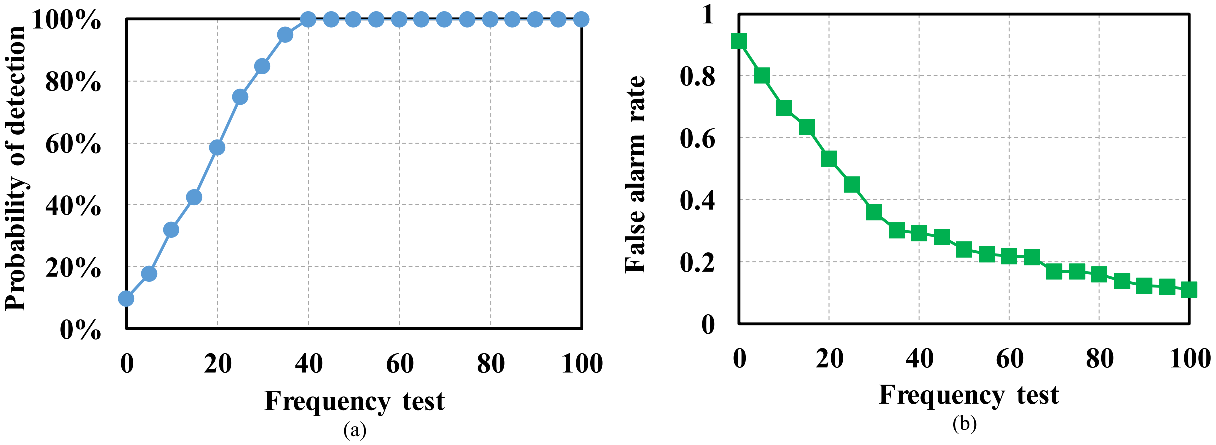

FIGURE 14. (a)Relationship between the test frequency and PD. (b) The effect of test frequency on FAR.

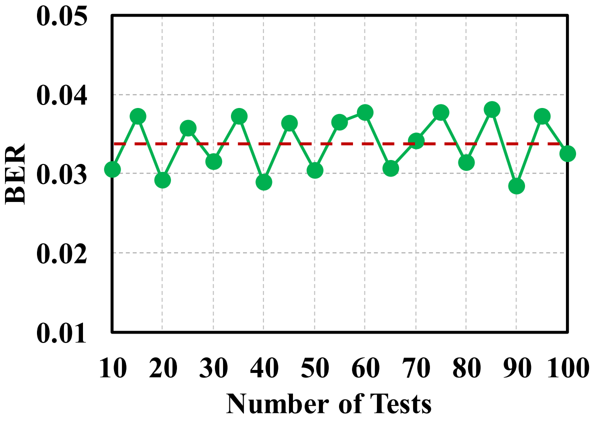

FIGURE 15. BER vs number of tests.

Experimental equipment and parameters are shown in TABLE 2. In DSP processing, the BER is mainly the extraction of the characteristics of the channel fingerprint in this experimental scheme. By comparing the size of the normalized BER T and the threshold coefficient η, it is determined whether the channel has been attacked by Eve. As shown in Fig. 14 (a), as the frequency test increases, the PD will increase accordingly. The frequency test is actually the number of experimental tests. The total number of frequency test is 100. When the frequency test is 0 to 40, the PD is consistently increasing. When it is greater than 40, the PD tends to stabilize, and the detection accuracy can reach 100%. The more the experimental tests are, the better the authentication effect is. Fig. 14 (b) shows the relationship between the total number of experiments and the FAR. As the experimental test increases, the FAR shows a decline. When the is number 100, the FAR is close to 0.1, which indicates that the system has a better false alarm effect. In the experiment, we can conclude that the higher the PD is, the better the effect of authentication is. And the relationship between PD and FAR is the opposite. When the frequency test increases, the authentication effect is better. When the frequency test reaches to a certain value, the two curves tend to stabilize. As is shown in Fig. 15, the result of measuring the BER shows random fluctuation under the same conditions, since the BER of the fiber channel is random. We calculate the threshold η between 0-0.42.

V. CONCLUSION

We propose a physical layer authentication scheme by measuring the BER variation of the fiber loop channel. Alice authenticates the system and judges the authentication result. Alice needs to know the channel status of the entire system to determine whether the authentication is successful. Bob is the authenticated party. Therefore, Bob does not need to know the channel status. Bob only needs to loop back the signal sent by Alice. The normalized BER variation T is used to reflect the change of the fiber channel. We analyze three attack methods of Eve on optical fiber channel and the corresponding authentication performance. The results show that in these three attack cases, this scheme is sensitive to them. In the case of Eve's interference attack, the lower the OSNR is, the better the authentication performance becomes. In the case of Eve's wiretap attacks, the higher the coupling coefficient, the better the authentication performance becomes. In the case of Eve's substitution attack, the farther Eve is from Alice, the better the authentication performance becomes. By analyzing the change of the fingerprint of the extracted channel, the legitimate channel and the illegal one can be correctly distinguished. Through the analysis of the experimental results, the PD can reach 100% with the FAR is 0.1, thereby achieving the correct authentication of the legal party. This authentication scheme does not need additional physical equipment, but to upgrade the DSP. Therefore, it can be widely used in the existing optical fiber communication system.

REFERENCES

[1] M. Xiao, Y.-R. Cao, and X.-L. Song, "Efficient and secure authenticated quantum dialogue protocols over collective-noise channels," *Chin. Phys. Lett.*, vol. 34, no. 3, Mar. 2017, Art. no. 030302.

[2] H. Wang, Y. Zhang, G. Wu, and H. Ma, "Authenticated quantum dialogue without information leakage," *Chin. J. Electron.*, vol. 27, no. 2, pp. 270–275, Mar. 2018.

[3] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," *Opt. Express*, vol. 21, no. 20, pp. 23756–23771, Oct. 2013.

[4] M. Bunder, A. Nitaj, W. Susilo, and J. Tonien, "Cryptanalysis of RSA-type cryptosystems based on lucas sequences, Gaussian integers and elliptic curves," *J. Inf. Secur. Appl.*, vol. 40, pp. 193–198, Jun. 2018.

[5] T. Mefenza and D. Vergnaud, "Cryptanalysis of server-aided RSA protocols with private-key splitting," *Comput. J.*, vol. 62, no. 8, pp. 1194–1213, Aug. 2019.

[6] S. Jain and J. S. Baras, "Preventing wormhole attacks using physical layer authentication," in *Proc. WCNC*, Shanghai, China, Apr. 2012, pp. 2712–2717.

[7] B. Škorić, "Quantum readout of physical unclonable functions," *Int. J. Quantum Inf.*, vol. 10, no. 01, Feb. 2012, Art. no. 1250001.

[8] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. Pinkse, "Quantum-secure authentication of a physical unclonable key," *Optica*, vol. 1, no. 6, pp. 421–424, Dec. 2014.

[9] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[10] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[11] G. Wang, Q. Liu, R. He, F. Gao, and C. Tellambura, "Acquisition of channel state information in heterogeneous cloud radio access networks: Challenges and research directions," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 100–107, Jun. 2015.

[12] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[13] D. Wang, X. Tang, L. Xi, X. Zhang, and Y. Fan, "A filterless scheme of generating frequency 16-tupling millimeter-wave based on only two MZMs," *Opt. Laser Technol.*, vol. 116, pp. 7–12, Aug. 2019.

[14] X. Du, D. Shan, K. K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 1276–1284.

[15] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 151–157, Jun. 2016.

[16] X. Yang, Y. Li, G. Gao, Y. Zhao, H. Zhang, and J. Zhang, "Demonstration of key generation scheme based on feature extraction of optical fiber channel," in *Proc. Asia Commun. Photon. Conf. (ACP)*, Hangzhou, China, Oct. 2018, pp. 1–3.

[17] I. U. Zaman, A. B. Lopez, M. A. A. Faruque, and O. Boyraz, "Physical layer cryptographic key generation by exploiting PMD of an optical fiber link," *J. Lightw. Technol.*, vol. 36, no. 24, pp. 5903–5911, Dec. 15, 2018.

[18] X. Wang, J. Zhang, Y. Li, Y. Zhao, and X. Yang, "Secure key distribution system based on optical channel physical features," *IEEE Photon. J.*, vol. 11, no. 6, Dec. 2019, Art. no. 7205311.

[19] I. U. Zaman, A. B. Lopez, M. A. Al Faruque, and O. Boyraz, "A physical layer security key generation technique for inter-vehicular visible light communication," in *Proc. SPPCom*, New Orleans, LA, USA, 2017, Paper SpTu1F.3.

[20] F. B. Offiong, S. Sinanovic, and W. O. Popoola, "On PAPR reduction in pilot-assisted optical OFDM communication systems," *IEEE Access*, vol. 5, pp. 8916–8929, 2017.

[21] J. Zhao and L.-K. Chen, "Adaptively loaded IM/DD optical OFDM based on set-partitioned QAM formats," *Opt. Express*, vol. 25, no. 8, pp. 9368–9377, Apr. 2017.

XIANGQING WANG is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications (BUPT). His research interests include physical layer authentication of optical fiber, optical fiber communication signal process, and secure key distribution in optical fiber.

YAJIE LI received the Ph.D. degree in communication and information system from the Beijing University of Posts and Telecommunications (BUPT), in 2018. He was a Visiting Ph.D. Student with the KTH Royal Institute of Technology, from October 2016 to December 2017. He is currently working as a Postdoctoral Researcher with BUPT. His research interests include software defined optical networks, edge computing, and 5G optical transport networks.

YONGLI ZHAO (Senior Member, IEEE) received the B.S. degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT), in 2005 and 2010, respectively. He is currently a Professor with the Institute of Information Photonics and Optical Communications, BUPT. He has published more than 150 journal and conference papers. His research interests include software-defined optical networks, flexi-grid optical networks, and network virtualization.

CHAO LEI received the B.S. degree from the Xi'an University of Posts and Telecommunications (XUPT), in 2016. He is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications (BUPT). His research interests include secure optical communication at the physical layer, secure key distribution in optical fiber, and coherent optical communication.

HUIBIN ZHANG received the Ph.D. degree from BUPT, in 2011. He is currently a Lecturer with BUPT. His research focuses on a type of safe optical communication strategy which is completely provided by the communication system for the endogenous protection of information transmission.

JIE ZHANG received the bachelor's degree in communication engineering and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT), China. He is currently a Professor and the Dean of the Information Photonics and Optical Communications Institute, BUPT. He has published more than 300 technical articles. He has authored eight books, submitted 17 ITU-T recommendation contributions, and six IETF drafts. He holds 17 patents. His research interests include architecture, protocols, and standards of optical transport networks. He has served as a TPC Member of a number of conferences, such as ACP, OECC, PS, ONDM, COIN, and ChinaCom.