Channel Characteristics Based Adjustable Fingerprint for Identity Authentication in WDM-PON With Deep Neural Networks

Kun Wu, Hongxiang Wang, *Member, IEEE*, and Yuefeng Ji, *Senior Member, IEEE*

***Abstract*—Wavelength-division-multiplexed passive optical network (WDM-PON) has been widely deployed for the high-speed, reliable transmission and low-cost properties. The physical layer identity authentication in WDM-PON becomes increasingly prominent. Recently, many device fingerprint based identity authentication schemes are proposed. However, these schemes only realize constant fingerprint, which will be acquired by illegal ONU after optical spectrum analysis. Therefore, the higher-level security requirement cannot be satisfied. To solve the problem, we propose a physical layer identity authentication method in WDM-PON by exploiting the channel characteristics based adjustable fingerprint with deep neural networks (DNNs). By secretly negotiating with legal optical network units (ONUs) on the lengths of the local fibers applied by them, the optical line terminal (OLT) can acquire the unique channel characteristics fingerprint obtained by each legal ONU. It should be noted that the fingerprint can be adjusted by modifying the length of the local fiber. Moreover, the same number of DNNs as legal ONUs are trained for fingerprint identification. Simulation results show 100% identification accuracy for illegal ONU when the length deviation between two fibers applied by legal ONU and illegal ONU is greater than 1.5 km. Meanwhile, the identity of each legal ONU can be recognized with 100% accuracy.**

***Index Terms*—Deep learning, identity authentication, channel characteristics fingerprint, identity spoofing attack, wavelength-division-multiplexed passive optical network (WDM-PON).**

I. Introduction

IN ORDER to meet the ever-increasing demand of high-speed, reliable transmission with minimum cost and complexity of next generation optical network, the WDM-PON system has been widely deployed [1], [2]. In particular, the called 10-Gigabit PON (XG-PON) is considered as one of the essential technologies for future internet access [3]. However, there are many security threats in WDM-PON due to its point-to-multipoint topological structure and broadcasting nature, such as eavesdropping, jamming attack, interceptions, identity spoofing attacks and infrastructure attacks. For solving the above threats, many different types of secure schemes are investigated and proposed. In these schemes, the security of data transmission is mainly considered [4]–[9]. However, the security threats exist not only on the transmission link, but also on the access end. Jamming attack and identity spoofing attack, representing that the illegal individuals apply unauthorized ONUs to forge the legal ONUs and join the optical network, may significantly threaten the security of the optical network [10]. Specifically, the issue becomes more hazardous in WDM-PON because many different ONUs communicate with OLT by a shared fiber in the upstream direction [11]. Therefore, satisfactory identity authentication schemes in WDM-PON are extremely essential for identifying legal ONUs.

Existing authentication mechanisms in the upper layer are mainly based on encryption algorithm, such as digital certificate-based authentication and password authentication. By contrast, the password authentication is more widely applied [12]. Meanwhile, the most ideal passwords should be simply remembered, hard to guess and able to resist brute force attack. To further enhance the security, one-time password [13], [14] mechanisms based on hash function are proposed, such as challenge/response [15] and S/KEY [16]. However, because of the risk of modification, counterfeit and disclosure, the higher level security requirement of certain scenarios still cannot be satisfied by applying password authentication. On the other hand, although the digital certificate, which is based on mathematics, is more secure since its security is founded on public-key encryption algorithms, a reliable certificate agency (CA) is required to distribute the digital certification for each legal ONU. Moreover, the CA needs to be deployed in advance and certain protocols are required to be implemented during the authentication process, so the digital certificate-based authentication is more complex and expensive.

In order to provide more secure identity authentication in WDM-PON, the physical layer secure schemes have been studied. In [17], authors first mentioned the concept of device fingerprint in radio frequency communication by referring to the biometric identification technology [18]. Device fingerprint represents the unique and non-clonable physical layer characteristic. In [19], [20], the device fingerprint was employed to identify the legal ONUs and illegal ONU in OFDM-PON. By using the non-ideal devices of the legal ONUs as the device fingerprint of each legal ONU, the physical layer identity authentication

Manuscript received January 9, 2022; revised February 17, 2022; accepted March 8, 2022. Date of publication March 11, 2022; date of current version March 31, 2022. This work was supported by the National Natural Science Foundation of China under Grants 61871051 and 62021005. *(Corresponding author: Yuefeng Ji.)*

The authors are with the State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, Beijing 100876, China (e-mail: wkbupt@bupt.edu.cn; wanghx@bupt.edu.cn; jyf@bupt.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2022.3158622

schemes with constant fingerprint are realized. In WDM-PON, these schemes can still be applied for identity authentication. However, if we assume that the illegal ONU receives the signal sent by each legal ONU and conducts the optical spectrum analysis, the device fingerprint obtained by each legal ONU will be acquired by illegal ONU. Therefore, facing the changeable and unpredictable attack scenarios, these identity authentication schemes with constant fingerprint cannot meet the higher-level security requirement.

In this paper, a physical layer identity authentication method by applying the channel characteristics based adjustable fingerprint with DNNs in WDM-PON is proposed. The channel characteristics fingerprint represents the linear and nonlinear distortions experienced by the transmitted data. By secretly negotiating with legal ONUs about the lengths of the local fibers used by them [21], the channel characteristics fingerprint obtained by each legal ONU will be acquired by the legal OLT because the lengths of the local fiber applied by OLT and public fiber are obtainable to OLT. However, the lengths of the local fibers used by legal ONUs are unknown to illegal ONU, so the channel characteristics fingerprint of each legal ONU is dissimilar from that of illegal ONU. At the OLT end, the identity of each ONU is authenticated by recognizing these fingerprints with DNNs. Compared to the above secure schemes, our proposed method realizes adjustable fingerprint, which can be changed by modifying the length of the local fiber applied by each legal ONU. Meanwhile, the modified fingerprint will still be obtained by the OLT and is obscure to the illegal ONU, which can effectively resist the identity spoofing attack and guarantee the higher-level security requirement. Furthermore, the proposed method is fully compatible with current PON infrastructure, guaranteeing the lower cost compared with those methods with specially designed hardware structure [22].

II. System Model

The proposed physical layer identity authentication method in WDM-PON can be divided into the following four steps, as shown in Fig. 1.

1. *Information Negotiation:* The legal OLT negotiates with each legal ONU about the length of the local fiber, detection data and two optical signal wavelengths, which are used for modulation, applied by each legal ONU.
2. *DNN Training:* The legal OLT locally simulates the fiber path from it to each legal ONU, transmitting the pre-agreed detection data to acquire the corresponding received data. Then, the DNN is trained by the OLT with the detection data and the corresponding received data.
3. *Data Transmission:* Each legal ONU modulates the detection data and plaintext to two different optical signal wavelengths respectively, which have been negotiated in step 1. Then, the modulated signals are transmitted to the legal OLT through the SSMF.
4. *Identity Authentication:* After the transmission signals have been received by the legal OLT, the part of received data corresponding to the detection data is input into the corresponding trained DNN for fingerprint identification. If it comes from the legal ONU, the part of received data of the corresponding plaintext will be processed. Inversely, the received data will be discarded.

A. Information Negotiation

First, the legal OLT secretly negotiates with each legal ONU [21] about the length of the local fiber, the detection data and two different optical signal wavelengths applied by each legal ONU, as shown in ① of Fig. 2. It is obvious that two optical signal wavelengths used by ONU_1 are λ_1 and λ_2, and the length of the local fiber applied by ONU_1 is l_1. However, the optical signal wavelengths applied by different ONUs must be distinct, which is to guarantee that the OLT can distinguish the signals transmitted by different legal ONUs. Therefore, we assume that λ_{2n-1} and λ_{2n} are utilized by ONU_n for modulation. It should be noted that the lengths of the local fibers applied by different ONUs may be distinct, and the detection data is presented as $detection\ data$ in Fig. 2.

Although the illegal ONU can acquire the length of the local fiber applied by each legal ONU by cracking the key distribution scheme proposed in [21] to acquire the channel characteristics fingerprint obtained by each legal ONU, it should be noted that the fingerprint can be adjusted by modifying the length of the local fiber. Meanwhile, the related security assessments about the proposed key generation scheme are discussed. It is obvious that if the parameters of the proposed key generation scheme are properly designed, it is also very difficult for the illegal ONU to acquire the right final key, and it will consume a lot of time. Even if the illegal ONU has spent a period of time to acquire the length of the local fiber applied by each legal ONU, the corresponding length may have been changed. At this time, the fingerprint generated by the illegal ONU is still distinct with that of each legal ONU.

B. DNN Training

After the information negotiation, the legal OLT can locally simulate the fiber path from it to each legal ONU because the lengths of the public fiber and the local fibers applied by the OLT and each legal ONU are known to the OLT, as shown in ② of Fig. 2. Then, the pre-agreed detection data is transmitted through the simulated fiber. And the corresponding received data is acquired by the OLT after the transmission. It should be noted that the received data has experienced the simulated fiber path from the corresponding legal ONU to the legal OLT and is unavailable to the illegal ONU.

As shown in ② of Fig. 2, the optical transmitter is represented as the Tr, and its function is to convert digital signal into optical signal. Moreover, the Re is the optical receiver, which is used to convert optical signal into digital signal. At the transmission end, the 100 Gbps pulse-amplitude modulation-8 (PAM8) detection data is modulated through Mach-Zehnder Modulated (MZM), amplified via the optical amplifier. Then, the modulated signal is transmitted to the Re through the simulated fiber. After the transmission, the corresponding received data is acquired after Photo-Diode (PD) and digital signal process (DSP). Since the received data has suffered the linear and nonlinear distortions

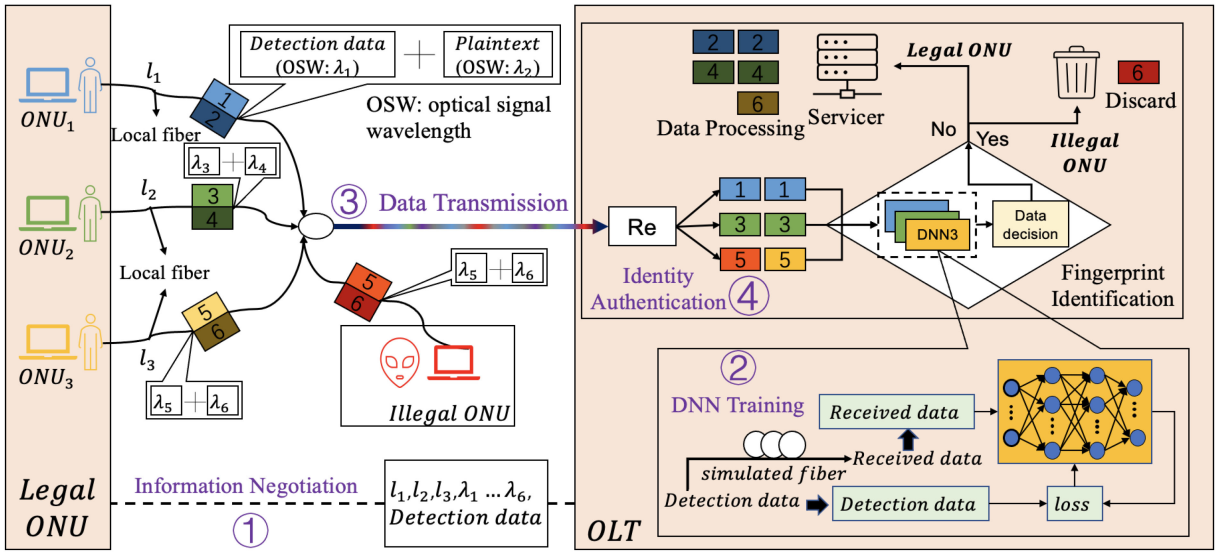

Fig. 1. The system chart of the proposed identity authentication method in WDM-PON. Re, optical receiver; DNN, deep neural network; OSW, optical signal wavelength; SSMF, standard single-mode fiber.

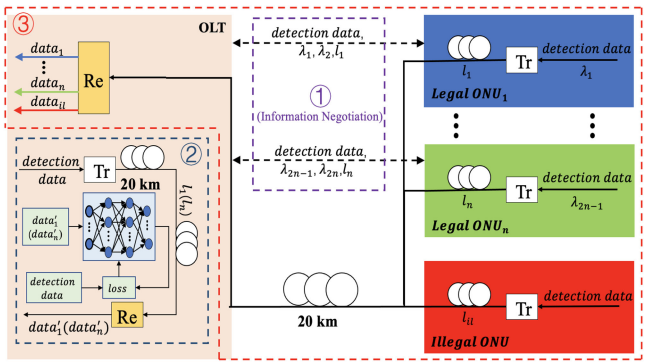

Fig. 2. The schematic diagram of fingerprint extraction.

caused by the fiber, the channel characteristics fingerprint is obtained in the received data. The fiber path from each legal ONU to the OLT is simulated by the OLT after the negotiation, so the channel characteristics fingerprint of each legal ONU will be acquired by the OLT. On the other hand, because the length of the local fiber applied by each legal ONU is confidential to the illegal ONU, the data sent by illegal ONU will experience different fiber path from that transmitted by each legal ONU. Hence, the channel characteristics fingerprint generated by the illegal ONU is dissimilar from that generated by each legal ONU. Furthermore, the channel characteristics fingerprint can be changed by modifying the length of the local fiber used by each legal ONU. Therefore, it is impracticable for illegal ONU to acquire the adjustable channel characteristics fingerprint generated by each legal ONU, while the legal OLT can always acquire the changed channel characteristics fingerprints.

In order to describe our principle more clearly, we assume that the OLT has completed the information negotiation with legal ONU_1. Therefore, the $data_1'$ will be acquired by OLT, as shown in ② of Fig. 2. Meanwhile, the $data_1'$ has experienced the simulated fiber path from OLT to legal ONU_1, so the channel characteristics fingerprint obtained by legal ONU_1 has been acquired by OLT. Subsequently, because of the powerful performance of deep learning in dealing with channel equalization problems [23]–[25], a DNN is trained with the pre-agreed detection data and the corresponding received data, which are indicated as $detection\ data$ and $data_1'$ in Fig. 2 respectively, to recognize the fingerprint of legal ONU_1. It should be noted that the same number of DNNs as legal ONUs should be trained for fingerprint identification since different legal ONUs may generate distinct channel characteristics fingerprints.

The previous fingerprints classification method is based on convolution neural network (CNN) [19], [20], the number of neurons in the output layer is identical to the number of legal ONUs in their schemes. When the number of legal ONUs changes, the CNN is required to be restructured and retrained, which will consume a lot of time. Moreover, the CNN is not applicable to intensity modulation direct detection (IM-DD) system because the amplitude information is one-dimensional data. Therefore, we adopt a new fingerprints classification method by applying DNNs and the structure of DNN is presented in Fig. 3(a). It is obvious that the DNN contains two hidden layers. The circles in the figure indicate the neurons, and the number of the neurons in the input layer is 51, which represents that 51 consecutive sampled symbols are required as input for a judged symbol. Moreover, each hidden layer has 128 neurons, while the output layer has 8 neurons, representing the probability of eight amplitudes of the PAM8 signal.

We input the corresponding received data into the DNN, applying the pre-agreed detection data as the target data and the output data of DNN is represented as $data_{out}$ in Fig. 3(a). Each neuron of hidden layer and output layer is identical to a computing unit, which consists of nonlinear operation and linear operation and can be expressed as follows:

$$y = f\left(\sum_{i=1}^{n} w_i x_i + b\right) \tag{1}$$

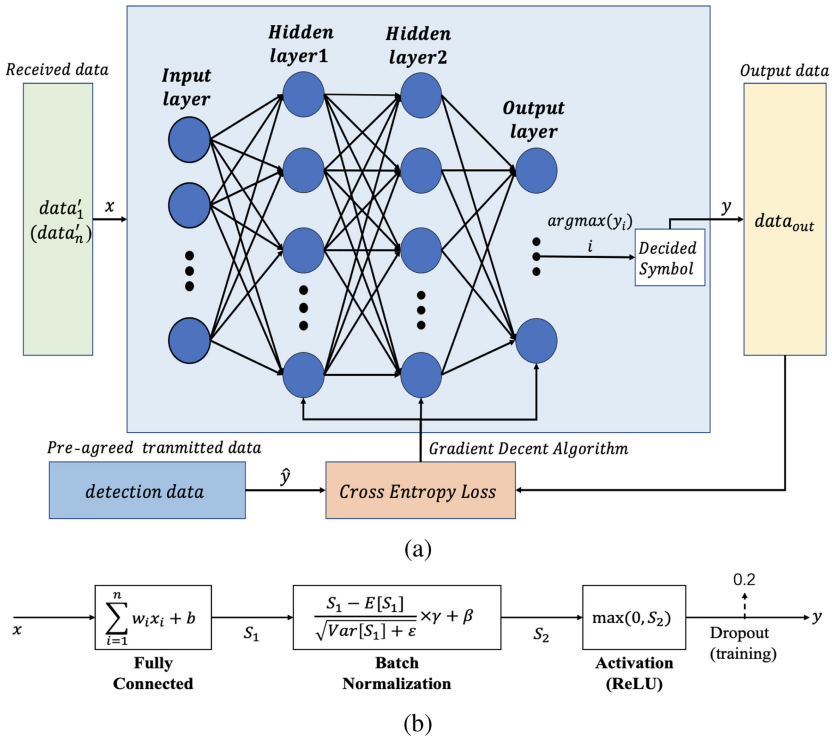

Fig. 3. (a) The DNN structure, (b) The flow chart of hidden layer.

where y represents the output data of the neuron, x_i is not only the input data of the neuron but also the output data of the previous neuron, w_i represents the weight and b is the bias. Furthermore, $f(*)$ indicates a nonlinear function, which can also be called the activation function. The activation function of the hidden layer is $ReLU$, while $Softmax$ is employed in the output layer, as simply expressed below:

$$ReLU(x) = max(0, x), Softmax(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{8} e^{x_j}} \tag{2}$$

The output data of the DNN $y_i = Softmax(x_i)$ is composed of

$$y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \tag{3}$$

where each element indicates the probability of eight amplitudes of PAM8. Meanwhile, the max value y_i of this vector represents that the detected symbol is the $i-th$ symbol of PAM8. Therefore, the formation of target data is

$$\hat{y} = \begin{cases} 0, & i \neq k \\ 1, & i = k \end{cases} \tag{4}$$

where $k \in \{1, 2, 3, 4, 5, 6, 7, 8\}$. Moreover, we select the cross-entropy loss as the loss function, calculating it in accordance with the output data of the DNN and the corresponding target data. It can be recognized from [26] that the cross-entropy loss is a conception accustomed to evaluate the similarity between two probabilities in information theory and can be expressed as follows:

$$CrossEntropyLoss = -\sum_{j=1}^{8} \hat{y}_i log(y_i) \tag{5}$$

where y is the output data, while $\hat{y}$ represents the corresponding target data. With the training, the cross-entropy loss slowly decreases and eventually converges to a small constant value. At the same time, the probability distribution of output data closes to the corresponding target data. The batch size, epoch, learning rate and the length of training data are set as 200, 120, 0.001, 28672, respectively. Moreover, the lengths of cross validation data and test data are 1024 and 7072, respectively. Simultaneously, Adam is applied as the optimizer to carry out back propagation and gradient descent [27]. To prevent overfitting, we employ the dropout strategy [28] with the rate of 0.2, which will be active during the training. For better training performance, we implement the batch normalization [29], which can be expressed as

$$y = \frac{x - E[x]}{\sqrt{Var[x] + \varepsilon}} \gamma + \beta \tag{6}$$

where x represents the input data, y is the normalized output data, γ and β represent the trainable vectors of the same size as x, and the flow chart of hidden layer is shown in Fig. 3(b).

As shown in ③ of Fig. 2, even if different legal ONUs transmit the same detection data, the OLT may receive dissimilar data because the lengths of the local fibers applied by different legal ONUs may be distinct. Therefore, the OLT needs to independently train a DNN for each of the different legal ONUs. When

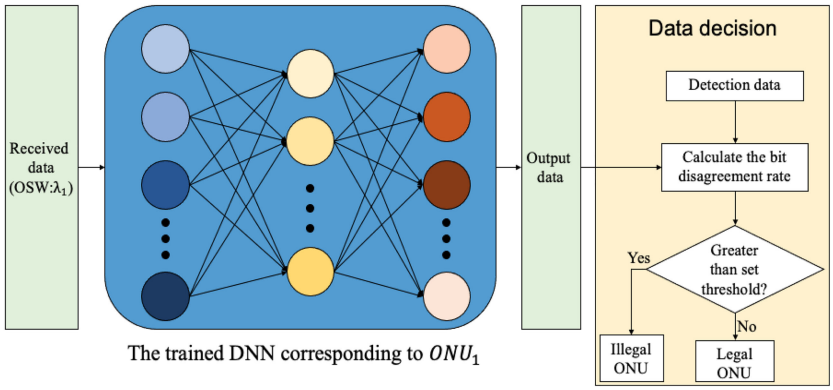

Fig. 4. The principle diagram of fingerprint identification.

the number of legal ONUs increases, the OLT only needs to train a DNN with the corresponding training data to identify the increased legal ONU. Inversely, when the number of legal ONUs decreases, the OLT is not required to train a new DNN, but just discard the trained DNN corresponding to the decreased legal ONU. Consequently, the consumed time is less when the number of legal ONUs changes compared with employing CNN for fingerprints classification. Moreover, the DNN is more suitable in IM-DD system.

C. Data Transmission

After the legal ONU has completed the information negotiation with the OLT, the legal ONU modulates the pre-agreed detection data and the plaintext to two different optical signal wavelengths, which have been negotiated in Section II. A. Furthermore, if multiple legal ONUs communicate with the OLT, the optical signal wavelengths applied by different ONUs must be distinct, which is to ensure that the OLT can distinguish the data transmitted by different legal ONUs. As shown in Fig. 2, the optical signal wavelengths applied by ONU_1 are λ_1 and λ_2, while the optical signal wavelengths applied by ONU_n are λ_{2n-1} and λ_{2n}. Afterwards, the OLT can not only distinguish the data transmitted by different legal ONUs, but also recognize which part of the received data corresponding to the detection data, and which part of the received data refers to the plaintext. Finally, these two modulated optical signals are transmitted to the OLT.

D. Identity Authentication

After the modulated signals have been acquired by OLT, the OLT will first judge which legal ONU the signals come from according to optical signal wavelengths. For the sake of convenience, we assume that the signals are transmitted by legal ONU_1. It can be seen from Fig. 1 that the wavelengths applied by legal ONU_1 are λ_1 and λ_2. Then, the part of received data corresponding to the detection data is input into the trained DNN corresponding to ONU_1, as shown in Fig. 4. Obviously, the wavelength of the optical signal that modulates this part of received data is λ_1. Meanwhile, it is worth noting that we ought to employ different DNNs to identify the data transmitted by diverse legal ONUs because distinct channel characteristics fingerprints are obtained by different legal ONUs. Moreover, it is obvious that the input data of DNN and the corresponding target data are the received data and the pre-greed detection data, respectively, so the DNN is essentially a channel equalizer. Then, we calculate the bit disagreement rate (BDR) between the output data of DNN and pre-agreed detection data. As shown in ③ of Fig. 2, if the identity of legal ONU_1 is not forged by illegal ONU, the part of received data corresponding to the detection data, which is also the input data of DNN, will go through the fiber path from the legal ONU_1 to OLT. Therefore, the calculated BDR will approximately equal to zero if the transmitter is the legal ONU_1. Inversely, because the length of the local fiber applied by legal ONU_1 is confidential to illegal ONU, the calculated BDR will be greater if the transmitter is the illegal ONU.

Hence, we need to set a threshold in advance to determine the identity of legal ONUs and illegal ONU. However, because the changes in the environment around the fiber will lead to the changes of optical fiber parameters, the channel characteristics fingerprint and the corresponding calculated BDR of each legal ONU will change too. Therefore, different thresholds should be set according to dissimilar environments. The ideal threshold should be slightly greater than the maximum value of calculated BDRs corresponding to the legal ONUs. Of course, a small error space needs to be reserved for legal ONUs. After the threshold has been set, the identity of legal ONUs and illegal ONU can be ascertained according to the calculated BDRs and the set threshold. If the calculated BDR is greater than the threshold we set according to the actual environment, the received data will be judged to be sent by the illegal ONU, and the OLT will discard the corresponding received data. On the contrary, the received data will be judged to be transmitted by the legal ONU, and then the OLT will process the corresponding received data. During the data processing, the part of received data corresponding to the plaintext is processed by channel compensation algorithm. Obviously, the wavelength of the optical signal that modulates this part of received data is λ_2, After the channel compensation, the OLT will acquire the error-free plaintext sent by each legal ONU. Therefore, by applying the proposed method, the identity spoofing attacks in WDM-PON are recognized and resisted. Moreover, the channel characteristics fingerprint can be adjusted

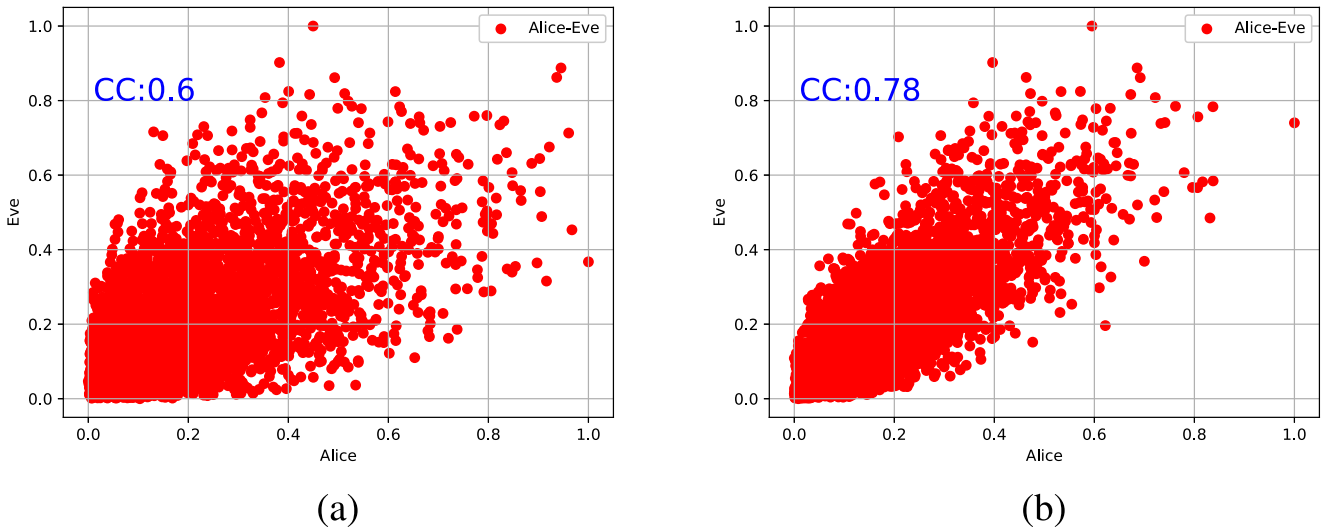

Fig. 5. The scatter diagrams and correlation coefficients of the two sets of received data corresponding to the local fibers with different lengths applied by Eve. (a) 10 km, (b) 25 km.

TABLE I
STANDARD SINGLE-MODE FIBER PARAMETERS

Parameter	Value(Unit)
Dispersion	$16e^{-6}(\frac{s}{m^2})$
Group Refraction	1.47
Nonlinear Refractive	$2.6e^{-20}(\frac{m^2}{W})$
Polarization Mode Dispersion	$\frac{0.1e^{-12}}{31.62}(\frac{s}{\sqrt{m}})$
Dispersion Slope	$0.08e^{3}(\frac{s}{m^3})$

by changing the length of the local fiber, ensuring the higher-level security and controllability of the proposed method.

III. SIMULATION RESULTS AND ANALYSE

A. Simulation Tools

The system signal transmission is simulated by a combination of simulation tools including VPI transmission Maker and Python. The VPI transmission Maker is used to generate the detection data and plaintext, to acquire the modulated PAM8 optical signals and to receive data. The lengths of the local fibers applied by each legal ONUs are set to 35 km, while the length of the local fiber used by the OLT is 0 km. Moreover, the length of public fiber, the bit rate, and the gain of optical amplifier are set as 20 km, 100 Gbps and 20 dB, respectively. The input powers of all lasers are 2 mW, and the other optical fiber parameters are shown in Table I.

B. Simulation Results

Since the length of the local fiber applied by each legal ONU is identical, which indicates that the channel characteristics fingerprint generated by each legal ONU is equivalent, so we only consider a legal ONU and an illegal ONU. In order to simplify the analysis of the simulation results, we assume that the legal ONU is represented as Alice, while the illegal ONU is indicated as Eve. First of all, we assume that the transmitter is the legal OLT, plotting the corresponding scatter diagrams and calculating the corresponding correlation coefficients (CCs) of the two sets of data received by Alice and Eve corresponding to the local fibers with different lengths applied by Eve, as shown in Fig. 5. It is obvious from the figure that the two sets of data received by Alice and Eve are divergent whether the length of the local fiber used by Eve is 10 km or 25 km. Moreover, the CCs between the two sets of data received by Alice and Eve are 0.6 and 0.78, respectively. Therefore, the channel characteristics fingerprints generated by Alice and Eve are dissimilar when the length of the local fiber applied by Alice is distinct from that applied by Eve.

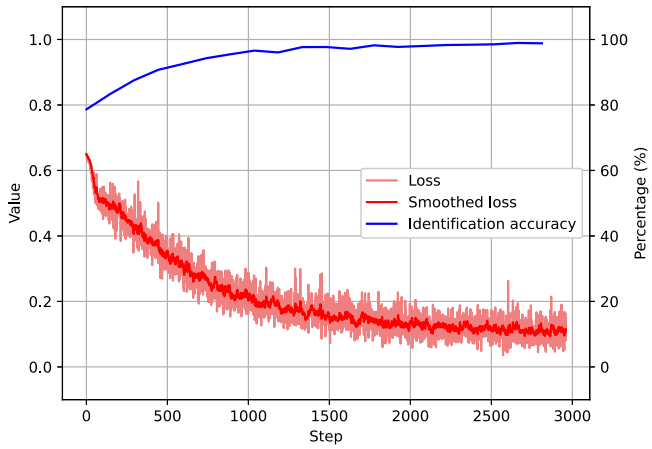

Fig. 6. The loss function and identification accuracy.

Then, the loss function and the identification accuracy of the DNN, which is trained in Section II. B, are presented, as shown in Fig. 6. It can be seen from the figure that the loss function appears a sharp decline in the beginning of training. As the weights

TABLE II
PARAMETERS AND RESULTS OF TRAINING/TEST

DNN	Training	Test
Length	28672	7072
Time	15.36s	0.51s
Loss	0.1085	–
Base Learning Rate	0.01	
Accuracy	100%	

and biases are continuously updated by the gradient descent algorithm, the loss function of the trained DNN slowly and stably decreases and finally converges to a very small constant value. In the meantime, the identification accuracy of the trained DNN increasingly rises, which is for the reason that the weights and biases of the trained DNN are constantly approaching the corresponding target values with the progressively training.

The computational complexity of the proposed method can be roughly analyzed by the consumed time during the training and testing. Therefore, we summarize the used parameters and corresponding results of training/test, as shown in Table II. It is noteworthy that the consumed time is influenced not only the dataset size, but also by the computer performance and other factors. If the base learning rate is 0.01, the training time for 28672 bits is 15.36 s with 120 epochs and the loss which is an evaluation indicator of the DNN is 0.1085 of the last epoch. In the meantime, the consumed time is 0.51 s when the trained DNN is applied to identify a sample with 7072 bits and the identification accuracy of all the test samples is 100%.

Considering that the length of the local fiber applied by each legal ONU is obscure to the illegal ONU, so we simulate the relationship between the identification accuracy of DNN for legal ONU and illegal ONU and the length deviation of two local fibers applied by legal ONU and illegal ONU. At the same time, we assume that the transmitter is the legal OLT and plot the relationship curve between the length deviation between two local fibers applied by legal ONU and illegal ONU and the corresponding BDR between two sets of data received by legal ONU and illegal ONU. It should be noted that the BDR between the two sets of data received by legal ONU and illegal ONU here is not the same meaning with the BDR between the output data of DNN and the pre-agreed detection data, which has been mentioned in Section II. D. And the following BDR represents the BDR between the two sets of data received by legal ONU and illegal ONU. It can be seen from Fig. 7 that the identification accuracy for legal ONU is 100% in any case. This is due to the fact that the linear and nonlinear distortions, which are represented as channel characteristics fingerprint in this paper, experienced by the data transmitted by the legal ONU does not change because the length of the local fiber applied by legal ONU has not been modified. On the other hand, the accuracy to identify the illegal ONU is 100% when the length deviation between the two local fibers applied by legal ONU and illegal ONU is greater than 1.5 km, while the identification accuracy for illegal ONU is not 100% in other cases. It is worth

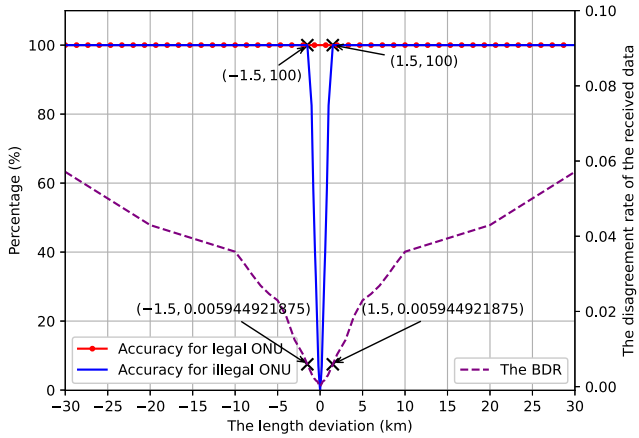

Fig. 7. The identification accuracy and BDR corresponding to different length deviation of two local fibers applied by legal ONU and illegal ONU.

noting that the length of the local fiber applied by legal ONU is 35 km. Therefore, the accuracy to identify illegal ONU is 100% when the length of the local fiber applied by illegal ONU is not within 33.5 km to 36.5 km, while the identification accuracy is not 100% in other cases. Moreover, it is obvious that when the length deviation between the two local fibers applied by legal ONU and illegal ONU is 1.5 km, the corresponding BDR is about 0.5945%. Nevertheless, compared with huge length options, 3 km is an absolutely small space, so it is strenuous for illegal ONU to spoof the identity of legal ONU.

Furthermore, the training data of DNN, which is employed for fingerprint identification, and the channel characteristics are related to the gain of optical amplifier, so we simulate the security level of the proposed method under different gains of optical amplifier. It should be noted that the gain of the optical amplifier is 20 dB in Fig. 7. As shown in Fig. 7 and Fig. 8(a), if we decrease the gain of optical amplifier, the BDR under the same length deviation will be greater, which is for the reason that the optical signal to noise ratio (OSNR) will diminish as we decrease the gain of optical amplifier. At this time, the fiber will cause stronger linear and nonlinear distortions on the transmitted data. On the contrary, since the OSNR will rise with the increasing of gain of optical amplifier, there are smaller nonlinear and linear distortions on the transmission data in the channel. Consequently, the corresponding BDR under equivalent length deviation is lower, as shown in Fig. 7 and Fig. 8(b). Moreover, it should be noted that the received data relates to the channel characteristics, so the corresponding training data of DNN under different gains of optical amplifier are also distinct. Therefore, the performance of DNN will change with the variation of gain. However, since the received data will change with the variation of gain of optical amplifier, so we cannot determinate the change of DNN performance according to the BDR between the two sets of data received by legal ONU and illegal ONU. Obviously, the security level of the proposed method can be evaluated by the length deviation between the two local fibers applied by legal ONU and illegal ONU. Hence, we do not discuss the relationship between the performance of DNN and the BDR between the two sets of data received by legal ONU and illegal ONU in this part.

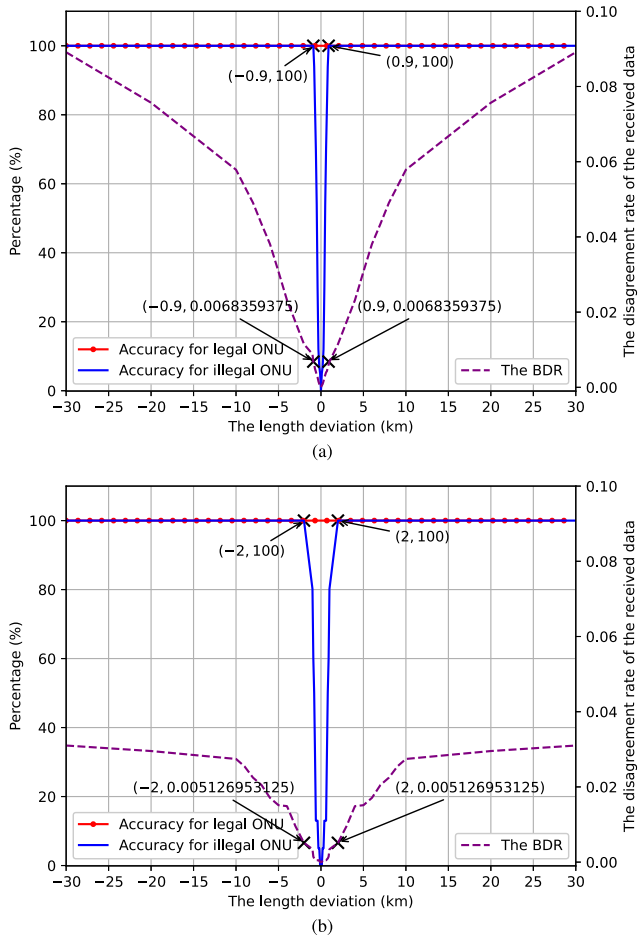

Fig. 8. The relationship between length deviation and identification accuracy, BDR corresponding to different gains of optical amplifier. (a) 15 dB, (b) 25 dB.

Since the length deviation of 0.9 km in Fig. 8(a) is smaller than the length deviation of 1.5 km in Fig. 7, the security level has been improved when the gain decreases from 20 dB to 15 dB. On the other hand, the length deviation of 2 km in Fig. 8(b) is greater than the length deviation of 1.5 km in Fig. 7, so the security level has been reduced when the gain increases from 20 dB to 25 dB. Meanwhile, it should be noted that the OSNR will affect quality of telecommunication (QoT). Therefore, the appropriate gain of optical amplifier should be selected according to the actual requirements of the specific scenarios for security level, QoT and power consumption.

Finally, because the performance of DNN will also affect the security level of the proposed method, we simulate the relationship between the performance of DNN and the security level. For keeping the two sets of data received by legal ONU and illegal ONU unchanged, we only adjust the structure of DNN to simulate the change of DNN performance. As shown in Fig. 10(a), when we employ a DNN, containing 3 hidden layers and 128 neurons in each layer, for fingerprint identification, the identification accuracy for illegal ONU will decrease if the length deviation between the two local fibers is smarter than 0.95 km, which is lower than the length deviation of 1.5 km in Fig. 7. Therefore, compared with the DNN, which contains 2 hidden layers and 128 neurons of each layer, the security level of the proposed method has been improved.

However, how does the performance of DNN change? For the sake of convenience, we assume that the legal OLT is represented as Alice. Meanwhile, the legal ONU is Bob, while the illegal ONU is Eve. Therefore, Alice can receive $data_{Bob}$ when Bob transmits the pre-agreed detection data, which can be represented as $data$, to Alice. Similarly, when Eve transmits the $data$ to Alice, Alice can receive $data_{Eve}$. As shown in Fig. 3(a), the input data of the DNN is $data_{Bob}$, while the corresponding target data is $data$. Then the trained DNN is applied for fingerprint identification. Here, we assume that if we input the $data_{Bob}$ into the trained DNN, the corresponding output data is $Data$, which can be represented as $data + \triangle B$. However, if we input the $data_{Eve}$ into the trained DNN, the corresponding output data is $Data'$, which can be represented as $data + \triangle B + \triangle E$. It is obvious that the BDR between the output data of DNN and the pre-agreed detection data is $\triangle B$ for Bob, while the corresponding BDR is $\triangle B + \triangle E$ for Eve. At this time, the threshold is set to T. If the performance of the DNN changes, it can be divided into two cases:

1) The Performance of DNN is Downgraded: Then, when we input the $data_{Bob}$ into the trained DNN, the corresponding output data is $data + \triangle B + BB$. Similarly, the corresponding output data is $data + \triangle B + \triangle E + EE$ when we input the $data_{Eve}$ into the trained DNN. It is obvious that the BDR between the output data of DNN and the pre-agreed detection data is $\triangle B + BB$ for Bob, and increases BB than before. Similarly, the BDR is $\triangle B + \triangle E + EE$ for Eve, increasing EE than before. However, since the input data of DNN is $data_{Bob}$ and the corresponding target data is $data$, the trained DNN has a greater correlation with $data_{Bob}$ than $data_{Eve}$. Consequently, the change of equalized bit error rate caused by the deterioration of the DNN is more obvious for Bob. That is, $BB > EE$. Meanwhile, it should be noted that the corresponding threshold should be changed too. Because the BDR is $\triangle B + BB$ for Bob, increasing BB than before, the corresponding threshold is increased to $T + BB$ now. However, $BB > EE$ and the calculated BDR of Eve is $\triangle B + \triangle E + EE$, increasing EE than before, so some samples of illegal ONU will be judged as legal ONU, as shown in Fig. 9(a) and (b). Consequently, only when the BDR between the two sets of data received by legal ONU and illegal ONU is greater, all samples of illegal ONU can be correctly identified.

Then we consider a more extreme situation, that is, the performance of DNN is particularly poor. Therefore, the two BDRs between the output data of DNN and the pre-agreed detection data for Bob and Eve are equivalent. At this point, no matter how big the difference between two channel characteristics fingerprints generated by Bob and Eve, the identity of Bob and Eve cannot be distinguished by employing this DNN. In other words, $BB = EE + \triangle E$. Therefore, the security level of the proposed method is extremely low.

2) The Performance of DNN is Improved: Then, when we input the $data_{Bob}$ into the trained DNN, the corresponding output data is $data + \triangle B - BB$. Similarly, the corresponding output data is $data + \triangle B + \triangle E - EE$ when we input the

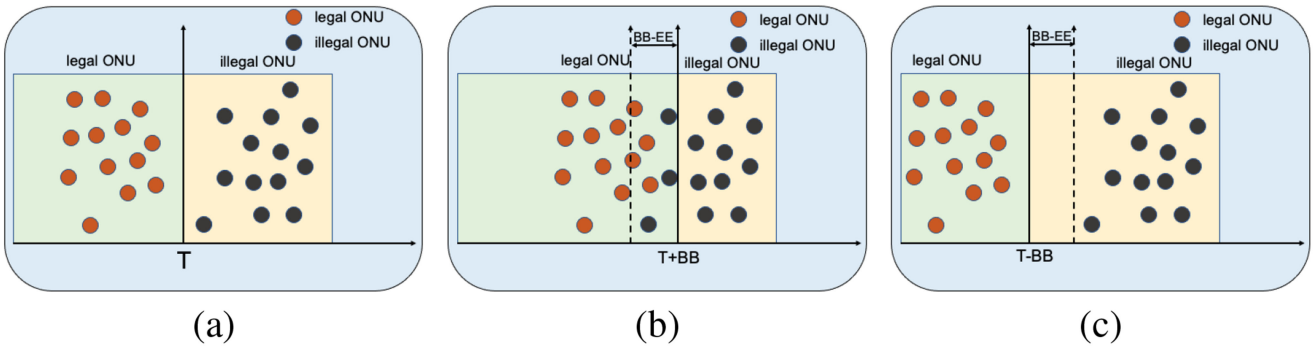

Fig. 9. The performance of DNN is (a) unchanged, (b) downgraded, (c) improved.

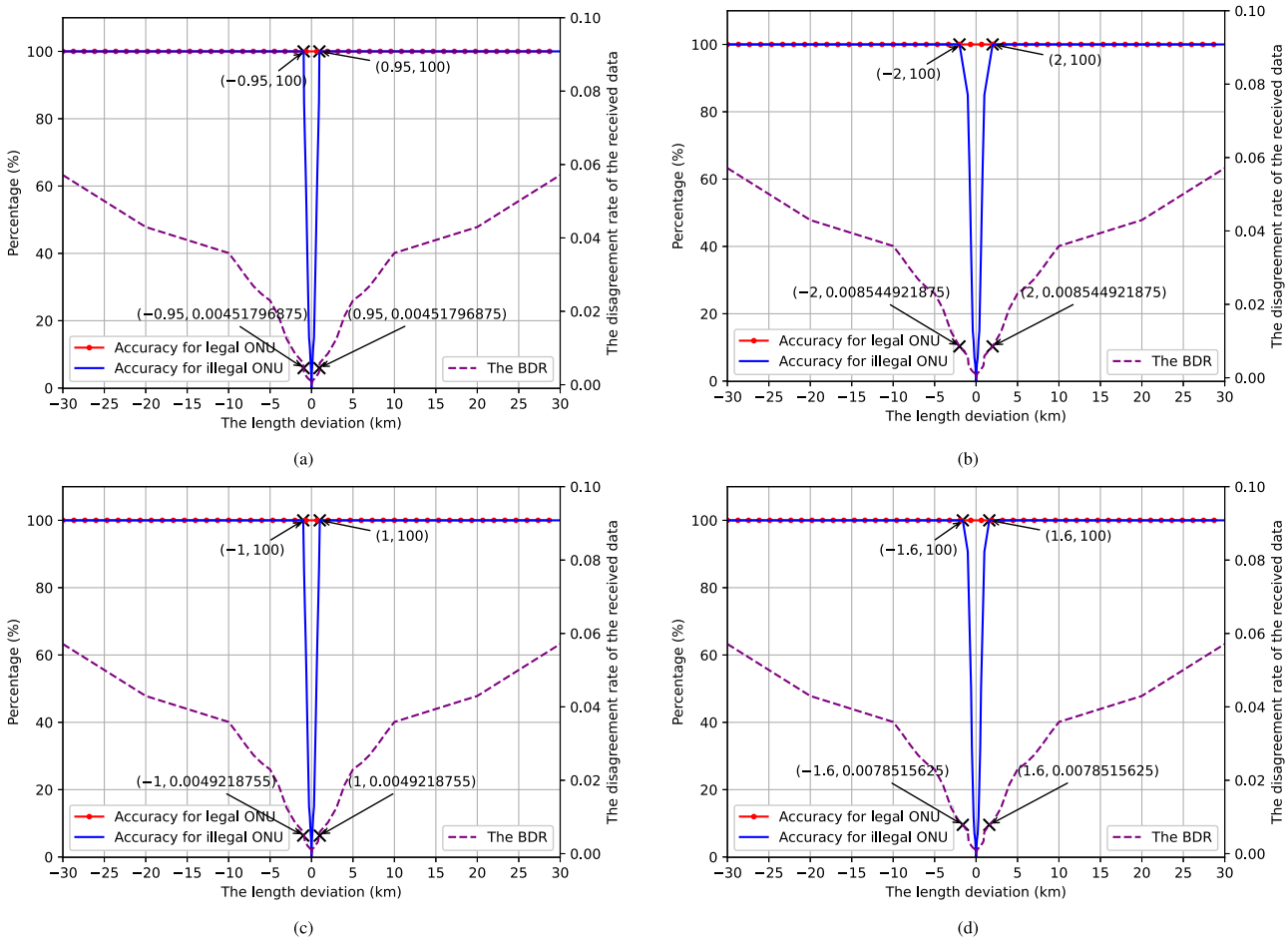

Fig. 10. The relationship between length deviation and identification accuracy, BDR corresponding to the DNNs with different structures. (a) 3 hidden layers, 128 neurons in each layer, (b) 1 hidden layer, 128 neurons of each layer, (c) 2 hidden layer, 256 neurons in each layer, (d) 2 hidden layer, 64 neurons of each layer.

$data_{Eve}$ into the trained DNN. It is obvious that the BDR between the output data of DNN and the pre-agreed detection data is $\triangle B - BB$ for Bob, and decreases BB than before. Similarly, the BDR is $\triangle B + \triangle E - EE$ for Eve, and decreasing EE than before. As discussed in the previous case, we can draw a conclusion that $BB > EE$. Similarly, because the BDR is $\triangle B - BB$ for Bob, the corresponding threshold is decreased to $T - BB$ now. However, the BDR is $\triangle B + \triangle E - EE$ for Eve, decreasing EE than before. Meanwhile, $BB > EE$. Hence, not only all samples of Eve can be judged correctly, but also the difference between the minimum value of calculated BDRs corresponding to Eve and the decreased threshold becomes larger, as shown in Fig. 9(a) and (c). In other words, even if the BDR between the two sets of data received by legal ONU and illegal ONU is smaller, all samples of illegal ONU can still be correctly identified.

Then, we consider a more extreme situation, that is, the performance of DNN is particularly good. At this time, if we

input the $data_{Bob}$ into the trained DNN, the corresponding output data will be $data$, which represents that $BB = \triangle B$ and the BDR between the output data of DNN and the pre-agreed detection data is 0 for Bob. Therefore, only when the two sets of data received by Bob and Eve are completely identical, the identity of Bob and Eve cannot be distinguished by employing this DNN. In other words, the security level of the proposed method is extremely high.

In summary, if the performance of DNN is improved, the corresponding BDR between the two sets of data received by legal ONU and illegal ONU will be smaller, and the security level of the proposed method will be improved. Therefore, the DNN applied in Fig. 10(a) has better performance than that applied in Fig. 7 because the BDR of 0.5945% and the length deviation of 1.5 km in Fig. 7 are greater than the BDR of 0.4518% and the length deviation of 0.95 km in Fig. 10(a). Similarly, it can be seen from the Fig. 10(c) that if we employ the DNN, which consists of 2 hidden layers and 256 neurons in each layer, for fingerprint identification, the performance of DNN and the security level will be enhanced compared with the DNN with 2 hidden layers and 128 neurons of each layer since the BDR of 0.4922% and the length deviation of 1 km in Fig. 10(c) are less than the BDR of 0.5945% and the length deviation of 1.5 km in Fig. 7. For this reason, we can improve the DNN performance by increasing the number of hidden layers or neurons in hidden layer appropriately, enhancing the security level of the proposed method. Nevertheless, the time of training and recognizing will be also prolonged because of the more complex DNN structure. Moreover, we also simulate the performance of DNNs with fewer hidden layers or neurons in hidden layer, as shown in Fig. 10(b) and (d). It is obvious from the figure that the performance of the DNN with fewer hidden layers or neurons of hidden layer to identify the legal ONU and illegal ONU is deteriorated. In other words, the security level of the proposed method is reduced. However, the corresponding time, which is used for training and identifying, will be shortened. Therefore, we ought to select the appropriate DNN structure according to the actual requirements of the specific scenarios for security level and time cost.

IV. Conclusion

In this paper, we propose a channel characteristics based adjustable fingerprint physical layer identity authentication method with DNNs in WDM-PON. The proposed method can be divided into four steps — information negotiation, DNN training, data transmission and identity authentication. The OLT can acquire the unique channel characteristics fingerprint obtained by each legal ONU by secretly negotiating with legal ONUs on the lengths of the local fibers applied by them. Moreover, the channel characteristics fingerprint can be adjusted by modifying the length of the local fiber applied by each legal ONU, which can guarantee the higher-level security and controllability of the proposed method. At the OLT end, DNNs are applied to identify the illegal ONU and legal ONUs. The results show that the proposed method can realize 100% identification accuracy for illegal ONU when the length deviation between the two local fibers applied by legal ONU and illegal ONU is greater than 1.5 km. Meanwhile, the 100% identification accuracy for legal ONUs is achieved. The security level of the proposed method can be enhanced by modifying the structure of DNN and the gain of optical amplifier, but the QoT, time cost and power consumption will be influenced. Furthermore, the proposed method is fully compatible with current fiber infrastructure and provides a reference for realizing adjustable fingerprint. It should be noted that the proposed method can be combined with device fingerprint, DNN algorithm with better performance and a more secure key distribution scheme to enhance its security level. These tasks will be explored in our future work.

References

[1] N. Suzuki *et al.*, "100 Gb/s to 1 Tb/s based coherent passive optical network technology," *J. Lightw. Technol.* vol. 36, no. 8, pp. 1485–1491, 2018.

[2] R. Koma *et al.*, "Fast feed-forward optical and electrical gain control to extend the dynamic range of the burst-mode digital coherent receiver for high-speed TDM-PON systems," *J. Lightw. Technol.*, vol. 40, no. 3, pp. 647–654, 2021.

[3] C. Rodrigues *et al.*, "25 and 50G optical access network deployment forecasts using bi-logistic curves," in *Proc. Opt. Fiber Commun. Conf. Exhib.*, 2021, pp. 1–3.

[4] C. Zhang *et al.*, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.* vol. 36, no. 9, pp. 1706–1712, 2018.

[5] M. Bi *et al.*, "Chaotic arnold transform and chirp matrix encryption scheme for enhancing the performance and security of OFDM-PON," *Opt. Fiber Technol.* vol. 51, pp. 64–70, 2019.

[6] X. Gao, "Enhancing Ikeda time delay system by breaking the symmetry of sine nonlinearity," *Complexity*, vol. 2019, 2019, Art. no. 2941835.

[7] X. Gao *et al.*, "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Opt. Exp.* vol. 28, no. 8, pp. 10847–10858, 2020.

[8] Z. Zhang *et al.*, "Constellation shaping chaotic encryption scheme with controllable statistical distribution for OFDM-PON," *J. Lightw. Technol.* vol. 40, no. 1, pp. 14–23, 2021.

[9] Y. Wan *et al.*, "Chaotic power division multiplexing for secure optical multiple access," *J. Lightw. Technol.*, vol. 40, no. 4, pp. 968–978, 2022.

[10] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.* vol. 12, no. 1, pp. 160–167, Feb. 2018.

[11] M. Yang *et al.*, "Real-time verification of soft-decision LDPC coding for burst mode upstream reception in 50G-PON," *J. Lightw. Technol.* vol. 38, no. 7, pp. 1693–1701, 2019.

[12] W. Luo, Y. Hu, H. Jiang, and J. Wang, "Authentication by encrypted negative password," *IEEE Trans. Inf. Forensics Secur.* vol. 14, no. 1, pp. 114–128, Jan. 2019.

[13] E. Erdem and Mehmet Tahir Sandıkkaya, "OTPaaS—One time password as a service," *IEEE Trans. Inf. Forensics Secur.* vol. 14, no. 3, pp. 743–756, Mar. 2019.

[14] L. Wu, H. J. Cai, and H. Li, "SGX-UAM: A secure unified access management scheme with one time passwords via Intel SGX," *IEEE Access* vol. 9, pp. 38029–38042, 2021.

[15] W. Xu, J. Tian, Y. Cao, and S. Wang, "Challenge-response authentication using in-air handwriting style verification," *IEEE Trans. Dependable Secure Comput.* vol. 17, no. 1, pp. 51–64, Jan./Feb. 2020.

[16] N. M. Haller, "The S/key (TM) one-time password system," in *Proc. Symp. Netw. Distrib. Syst. Secur.*, 1994, pp. 151–157.

[17] J. Hall, M. Barbeau, and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," in *Proc. Conf. Wireless Opt. Commun.*, 2003, pp. 13–18.

[18] J. Daugman, "How IRIS recognition works," in *The Essential Guide to Image Processing*. New York, NY, USA: Academic, 2009, 715–739.

[19] S. Li *et al.*, "Enhancing the physical layer security of OFDM-PONs with hardware fingerprint authentication: A machine learning approach," *J. Lightw. Technol.* vol. 38, no. 12, pp. 3238–3245, 2020.
[20] C. Fan *et al.*, "Identify the device fingerprint of OFDM-PONs with a noise-model-assisted CNN for enhancing security," *IEEE Photon. J.*, vol. 13, no. 4, Aug. 2021, Art. no. 8600104.
[21] M. Baldi *et al.*, "Code-based physical layer secret key generation in passive optical networks," *Ad Hoc Netw.* vol. 89, pp. 1–8, 2019.
[22] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators," *J. Lightw. Technol.* vol. 34, no. 22, pp. 5325–5331, 2016.
[23] X. Ruan *et al.*, "High-speed PAM4 transmission with a GeSi electro-absorption modulator and dual-path neural-network-based equalization," *Opt. Lett.* vol. 45, no. 19, pp. 5344–5347, 2020.
[24] Y. Ji *et al.*, "Artificial intelligence-driven autonomous optical networks: 3S architecture and key technologies," *Sci. China Inf. Sci.*, vol. 63, no. 6, pp. 160301:1–160301:24, 2020.
[25] C. Häger and H. D. Pfister, "Nonlinear interference mitigation via deep neural networks," in *Proc. Opt. Fiber Commun. Conf. Expo.*, 2018, pp. 1–3.
[26] S. G. Zadeh and M. Schmid, "Bias in cross-entropy-based training of deep survival networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 9, pp. 3126–3137, Sep. 2021.
[27] M. Zhang, Y. Zhou, W. Quan, J. Zhu, R. Zheng, and Q. Wu, "Online learning for IoT optimization: A Frank-Wolfe Adam-based algorithm," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8228–8237, Sep. 2020.
[28] M. M. Kalayeh and M. Shah, "Training faster by separating modes of variation in batch-normalized models," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 42, no. 6, pp. 1483–1500, Jun. 2020.
[29] X. Shen, X. Tian, T. Liu, F. Xu, and D. Tao, "Continuous dropout," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 9, pp. 3926–3937, Sep. 2018.