A physical-layer Rogue ONU identification method based on hardware fingerprint technology

Kaiyu Liu[1, 2], Danming Huang[1, 2], Chengzhe Tang[1, 2], Lei Deng[1, 2], Qi Yang[1, 2], Xiaoxiao Dai[1, 2], Deming Liu[1, 2], Mengfan Cheng[1, 2]*

1. National Engineering Research Center for Next Generation Internet Access System, School of Optical and Electronic Information, Huazhong University of Science and Technology (HUST), Wuhan, 430074, China
2. Jinyinhu Laboratory, Wuhan, 430040, China
Author e-mail address: chengmf@mail.hust.edu.cn

Abstract: We propose a method for identifying rogue ONUs based on hardware fingerprint technology. By directly detecting waveform fingerprints, the experimental results show that the average identification accuracy within 16 ONUs can reach 96.74%. © 2024 The Author(s)

1. Introduction

In the TDM-PON (Time Division Multiplied Passive optical network) system, Time-Division-Multiple-Access (TDMA) is used to achieve uplink channel sharing between optical network units (ONUs) (Fig1.a). Normal ONUs may become rogue ONUs due to hardware failures, software program errors, or malicious attacks. The transmission of Rogue ONU is uncontrollable, causing bandwidth allocations to other ONUs' upstream transmission in multipoint-to-point (MP2P) networks. [1]. Rogue ONU transmits signals outside its assigned time slots, occupying too many bandwidth resources, and even causing network paralysis in severe cases.

There are three main manifestations of rogue ONUs in the upstream direction of TDM-PON (Fig1.bcd): 1) Continuous emission; 2) Occupy the identity document (ID) or logical link identifier (LLID) of other ONUs; 3) Irregularly emitting light with no compliance with protocol-assigned time slots. In the troubleshooting of rogue ONU, situation 1 can be identified by detecting the changes in optical power; Situation 2 affects several ONUs and the detection is more difficult. While situation 3 irregularly influences the other ONUs, even breaking the time slot. It is the most difficult to be identified. How to accurately identify the rogue ONUs and replace them efficiently, reducing interference to users is the key concern in the industry.

Researchers have proposed many methods to detect rogue ONU attacks, such as strengthening bandwidth control at OLT [2] or establishing authentication mechanisms between OLT and ONUs. [3] But for operators, it is still difficult to identify rogue ONU IDs and replace them in time. The existing commercial identification requires controlling each ONU to be turned on or off through an upper-layer protocol from the OLT. [4] The method is time-consuming and difficult to identify rogue ONUs that emit irregularly. (Fig1.d) Communication will meet interruption as well.

Hardware fingerprint technology can distinguish features through machine learning (ML), being a worth-trying solution. For single ONU waveforms, we have implemented identity authentication in OFDM-PON based on wavelet transform [3] and in TDM-PON based on the eye diagram [5]. But whether the overlapped waveform suits the way is still unknown. In 2019, Li et al. proposed the use of overlapping spectrum analysis to detect rogue ONUs. [6] However, the implementation cost of the optical spectrum analyzer is high, and exhaustive classification of the combinations between any two ONUs leads to an extremely huge neural network in multi-user scenarios.

In this article, we propose a physical-layer rogue ONU identification method based on hardware fingerprint technology. We use only one PD for direct detection, making the method compatible with existing TDM-PON networks. We also propose parallel Neural Network library to deal with multi-user scenarios. The experimental results show that the average identification accuracy of the tested waveform in time domain is above 95%.

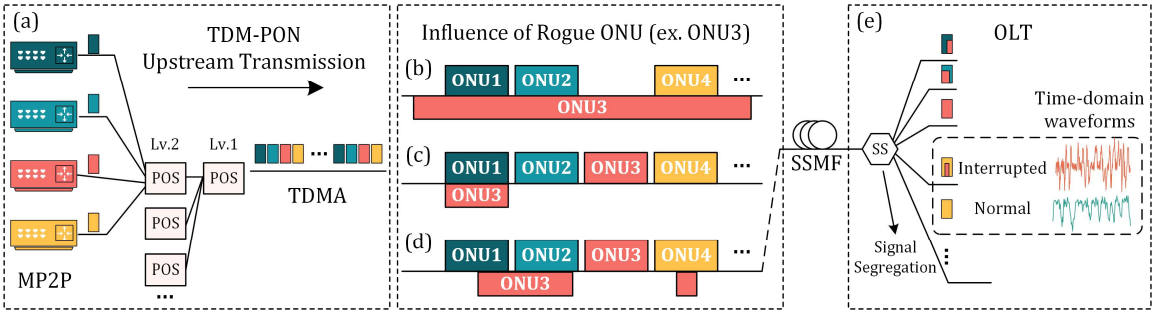


Fig. 1. Rogue ONU attacks in TDM-PON

2. Principle and methodology

We attempt to implement the identification problem of rogue ONUs using an eye-diagram-based CNN classification algorithm. It is a kind of application of fingerprint technology in the physical layer of PON. From the perspective of transmission, the eye diagram reflects the impact of inter-symbol crosstalk and noise levels. From the perspective of feature extraction (FE), an eye diagram contains feature information such as hardware parameter tolerances for different transmitter waveforms, strength differences in signal caused by different channel lengths, and relative delay between two ONUs. The work in reference [7] demonstrates the feasibility of an eye diagram in monitoring signal characteristics, such as modulation formats, optical signal-to-noise ratio (OSNR), and roll-off factor (ROF). We collect eye diagrams of the overlapped waveform from 4 ONUs' C_4^2= 6 groups, which exhibit significant differences in shape. It also shows a certain degree of stability over several hours. (Judged by naked eyes)

There are two difficulties in using ML to identify the ID of rogue ONU: 1) The time-domain waveforms received by the OLT are overlapped. It is impossible to separate signals from different ONUs due to the beat frequency effect. (Fig1.e) So, it is necessary to achieve the identification in an overlapped state, meaning to determine both the two ONUs' IDs. 2) In a multi-user scenario, there can be over 64 ONUs for one OLT in TDM-PON. So, it is necessary to provide a sufficiently large feature parameter space for ML classification.

We propose an optimization to reply to the issue: When detecting a rogue ONU attack, OLT returns the ONU ID that is being attacked. Taking the 16-user TDM-PON for example, the number of classified groups is $C_{16}^2 = 120$. By returning the ID of the attacked ONU, the number of classification groups decreases to 15. Thus, we transform the identification problem within $N(N-1)/2$ groups to the identification problem within $(N-1)$ groups in N parallel networks. In the identification procedure, OLT can select the network for classification based on the time slot under attack. It will greatly expand the parameter space available for classification, reducing the training consumption of time and sample size. It also benefits from improving the speed of identification.

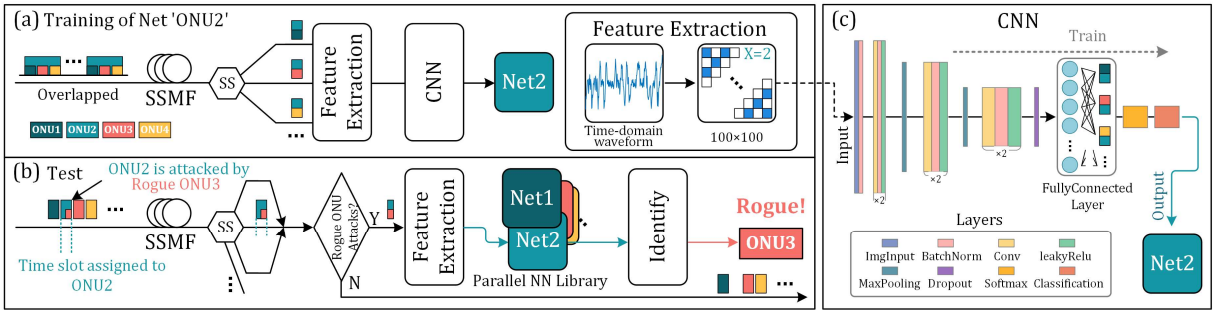


Fig. 2. The Training and Test process in our proposed identification method.

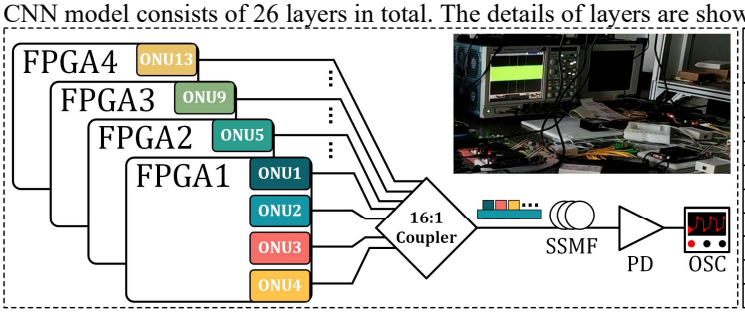
The working process is shown in Fig2.a b. In the classification stage, signals from each ONU are captured after signal segregation. In the feature extraction stage, we establish an eye-diagram-based feature matrix and a label X representing the assigned time slot. Then we input these feature matrices into CNN and complete the training process offline. In the identification stage, after detecting the ONU is suffering from attacks by a rogue ONU, the real-time feature matrix and the label X assigned to the time slot will be sent to the parallel NN library. In the parallel NN library, the network match to the overlapped time slot will be used to achieve identification.

3. Experiment and results

To evaluate the performance of the proposed identification method of rogue ONU, we use four field-programmable gate arrays (FPGA) development boards to control sixteen 1310nm commercial ONU modules. The transmitted signal is set as a pseudo-random binary sequence (PRBS31) in on-off keying (OOK) modulation format at a rate of 10 Gbit/s. This sequence is commonly used for performance analysis and testing in data transmission systems. After passing through a 16/1 coupler, the intensity distribution of the superimposed waveform is in the range of -18 to -15dBm. Then the light signal is converted to the electrical signal by the photoelectron detector (PD). The analog waveform is received by the oscilloscope (OSC) for sampling. (Fig.3) The oscilloscope is used to periodically collect overlapped time-domain waveforms from every two ONUs' combination, the sampling rate is set as 50GSa/s.

We collected 15 mixed-state signal samples from 16 ONUs at 20 time nodes within 5 hours, each with 720 samples. (15 groups represent the waveforms that overlapped between one normal ONU with another 15 virtual rogue ONU respectively.) The feature matrix size of each sample is 100×100. These samples are divided into three parts: train set, validation set, and test set. To match the practical scenario, the train set and validation set come from data collected during the first 70% period, with a ratio of 0.9 to 0.1. The data collected during the last 30% period is utilized as the

test set. The time span can characterize its stability and long-term performance in practical applications. The utilized CNN model consists of 26 layers in total. The details of layers are shown in Fig2.c.



Average Identification **Accuracy** (%) of 15 Groups by two FE methods

Eye Diagram		Wavelet Transform		Parameter settings
In Train	96.52	In Train	90.62	Training Samples =720*15*14
Test_AVG	96.74	Test_AVG	93.09	
Test_t1	95.15	Test_t1	91.09	Overlapped time slot for test = 200ns
Test_t2	97.51	Test_t2	93.90	
Test_t3	97.29	Test_t3	92.86	Sampling Rate =50Gsa/s
Test_t4	96.23	Test_t4	93.46	
Test_t5	97.12	Test_t5	93.95	Transmission Rate =10Gbit/s
Test_t6	97.12	Test_t6	93.25	

Fig. 3. Experimental schematic diagram, physical diagram, and experimental results.

Besides, we also conduct comparative experiments using the feature extraction method based on wavelet transform as reference [5], which maps to a 512 * 6 feature matrix. Except for matching the matrix dimension in the input layer, the other parameter settings of CNN are the same.

The identification accuracy in Fig.3 shows that for 15 different groups, the proposed method has an average recognition probability of 96.52%. For different test sets from 6-time nodes within one and a half hours later than the data of the train set, the identification accuracy remains above 95% and the average reaches 96.74%. For different test groups, we have not observed any significant deterioration trend in identification accuracy performance from all existing data (Fig.3). This proves the use of eye diagrams as a feature extraction method can continuously identify rogue ONUs from 15 classification groups. In contrast, the feature extraction method based on wavelet transform performs slightly worse. Due to time constraints, we only trained one network in the NN library. But the accuracy makes sense to other parallel networks. Therefore, we estimate that the final Rogue ONU identification accuracy would exceed 95%.

Furthermore, when it comes to multi-user TDM-PON, it is no longer feasible to use an NN to exhaustively list the IDs of all overlapped pairs of ONUs. For a 64-user TDM-PON, the number of classification groups will reach 2160. In the proposed method, the number of classification groups increases from 15 to 63, and the number of networks in the library increases from 16 to 64. This linear growth rate is acceptable for ML, and the current classification and identification results still have reference significance.

4. Conclusions

In this paper, we propose a physical-layer rogue ONU identification method based on hardware fingerprint technology. We use only one PD for direct detection, making the method compatible with existing TDM-PON networks. We also propose a parallel NN library to deal with multi-user scenarios. We use two FE methods to train the overlapped waveforms from 15 groups (1 normal ONU overlapped with 15 virtual rogue ONUs respectively). The experimental results show that the average identification accuracy of 200ns overlapped collected waveforms can reach 96.74% and 93.09% respectively for the two FE methods. In the future, the performance of the scheme may be improved by improving the signal-to-noise ratio of time-domain waveforms or optimizing FE and ML algorithms. We successfully demonstrate the feasibility of using hardware fingerprint technology in the physical layer to identify rogue ONU.

This work was supported by National Key Research and Development Program of China (2021YFB2900901); National Natural Science Foundation of China (62175077); Key Research and Development Program of Hubei province (2023BAB008).

5. References

[1] C. M, et al. Dynamic bandwidth allocation for quality-of-service over Ethernet PONs. JSAC. (2003).
[2] Elrasad A, et al. Virtual dynamic bandwidth allocation enabling true PON multi-tenancy. OFC. (2017).
[3] Li S, et al. Enhancing the physical layer security of OFDM-PONs with hardware fingerprint authentication: A machine learning approach. JLT. (2020).
[4] Oishi M, et al. Failed ONU detection technique applicable to commercially available passive optical networks. ECOC. (2010).
[5] Gong H, et al. Machine learning assisted hardware fingerprint identification for TDM-PON from eye-diagram. ACP. (2021).
[6] Li Y, et al. Real-time rogue ONU identification with 1D-CNN-based optical spectrum analysis for secure PON. OFC. (2019).
[7] Saif W S, et al. Machine learning techniques for optical performance monitoring and modulation format identification: A survey. IEEE Communications Surveys & Tutorials. (2020).