On Physical-Layer Authentication via Triple Pool Convolutional Neural Network

Yi Chen[1,2], Shahriar Real[2], Hong Wen[1], Boyang Cheng[2], Wei Wang[2], Pin-Han Ho[2] and Shih Yu Chang[3]
[1]*National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China*
[2]*Department of Electrical and Computer Engineering, University of Waterloo,Waterloo, Canada*
[3]*Department of Computer Engineering, San Jose State University, San Jose, USA*
Email:{yi.chen1, shahriar.real, b9cheng, w345wang, p4ho}@uwaterloo.ca, sunlike@uestc.edu.cn, shihyu.chang@sjsu.edu

***Abstract*—This paper introduces a novel physical-layer authentication scheme, called Triple Pool Convolutional Neural Network physical-layer authentication (TP-CNN-PHA), aiming to enable a light-weight user authentication mechanism based on physical-layer channel state information (CSI). We first introduce the TP-Net, which is characterized by jointly utilizing maximum pooling, average pooling, and global pooling on a globally connected CNN architecture. To assess its performance, we conduct two sets of experiments, including the one using simulated channel data, and the other one utilizing real experiment data generated from our wireless testbed. The result demonstrates the superiority of the proposed TP-CNN-PHA in terms of authentication accuracy and significant complexity reduction compared with all the considered counterparts, including the threshold-based authentication method.**

***Index Terms*—Edge computing, convolutional neural network (CNN), physical-layer authentication, channel state information (CSI).**

I. Introduction

Security is of vital importance for wireless communication systems due to the open transmission media that could be subject to various security threats. Regarding all network security procedures, user authentication serves as a critical role to ensure legitimate usage of the network resources. The traditional approach for user authentication is via cryptography-based security measurements, where arithmetic operations are performed at the sender and receiver. Such computations may lead to high hardware complexity and power consumption at the battery-powered Internet of thing (IoT) devices, which is nonetheless not suitable for the resource-constrained wireless terminals with limited storage and computing power.

The rich characteristics of physical-layer (PHY-layer) channel state information (CSI) of wireless links have been taken as a signature to authenticate the senders. PHY-layer authentication is lightweight in nature due to the much less consumed computation resources than that by the conventional cryptography based approaches. Besides, PHY-layer authentication can achieve a graceful trade-off between the level of security and latency requirements [1].

This work is supported by China Scholarship Council, and National Major R&D Program, China (2018YFB0904900, 2018YFB0904905).

In the literature, the spatial decorrelation property of the PHY-layer characteristics are exploited and applied in a stochastic model. These PHY-layer characteristics include received signal strength (RSS) [2], CSI [3], channel phase response [4], channel impulse response [5], and hardware fingerprints. The stochastic model, generally referred to as a binary hypothesis test, is used to make decisions based on the sensed PHY-layer characteristics and a predefined threshold, for the user/message authentication purpose. Nevertheless, the accuracy of these approaches is highly rely on the test threshold values that are hard to obtain in practical environment.

Instead of statistic models, machine learning (ML) based decision processes have recently been employed by numerous research initiatives for the PHY-layer authentication scenarios [6]–[8]. L. Xiao et al. [6] introduced a spoofing detection scheme that leverages a reinforcement learning process to accomplish the PHY-layer authentication. X. Wang et al. [7] used a deep neural network to accomplish the indoor positioning via CSI, which showed a remarkable effect compared with some other existing methods in two representative indoor environments. N. Wang et al. [8] proposed a PHY-layer authentication scheme based on ML to detect spoofing attack.

The above schemes, although being claimed effective in the considered scenarios, used conventional ML models with a large number of layers and parameters, leading to significant computation time and power consumption. They are not suitable for edge computing where some nodes are subject to stringent limitation on power consumption, computation, and storage. For a ML model to be applied under the scenario of edge computing, the efficiency of such ML model can not be just measured by ML metric, we should also consider the required resources to perform model training and prediction simultaneously. It is clear that an efficient ML model with resources consideration for the PHY-layer authentication mechanism in edge computing systems is of great importance.

The paper investigates a ML-based PHY-layer authentication scheme, called TP-CNN-PHA, for lightweight message authentication in edge computing systems. The proposed TP-CNN-PHA scheme incorporates with a ML model containing a novel CNN architecture, namely Triple Pool Network (TP-Net), which is uniquely featured by using three pooling

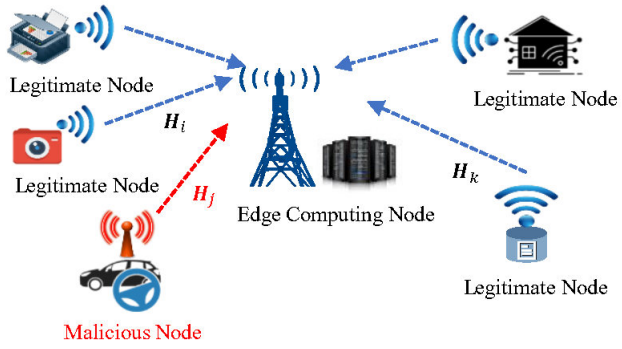


Fig. 1. PHY-layer authentication in edge computing scenario.

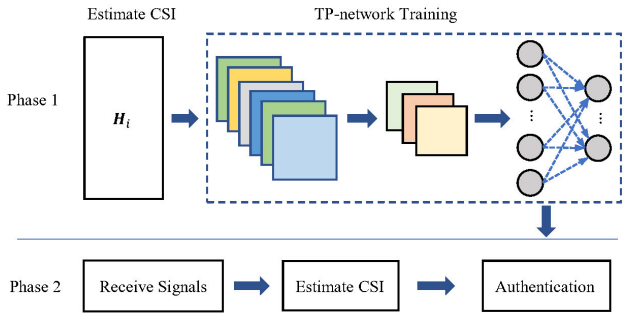


Fig. 2. The overall framework of TP-Net based PHY-layer authentication scheme.

schemes, i.e., max pooling, average pooling, and global average pooling (GAP). We train the TP-Net by using the channel data from a Rayleigh model as well as our testbed built on Universal Software Radio Peripheral (USRP) [9]–[11], respectively, where extensive simulation is conducted to verify the proposed TP-CNN-PHA scheme and compare with its counterparts.

The main contributions of this paper are summarized as follows.

(1) Develop a novel CNN architecture, namely TP-Net, aiming to achieve an efficient decision making process at the edge nodes in terms of required power consumption and computation.

(2) Integrate the proposed CNN architecture into PHY-layer authentication mechanism, namely TP-CNN-PHA, for lightweight user/message authentication in edge computing systems.

(3) Launch extensive simulation to examine the proposed TP-CNN-PHA and compare with a number of representative counterparts under multiple-input multiple-output orthogonal frequency-division multiplexing (MIMO-OFDM), where the experiments are conducted by using the data obtained from computer simulation and our USRP testbed, respectively.

The rest of the paper is organized as follows. Section II introduces the proposed TP-CNN-PHA scheme, including how its PHY-layer authentication mechanism is integrated to a TP-Net model. Section III presents the detailed explanations of the proposed TP-Net. Section IV shows the experimental results obtained from simulation and wireless testbed, and comparison with the counterparts. The paper is concluded in Section V.

II. Proposed TP-CNN-PHA

Fig. 1 illustrates the application scenario considered in this study, where an edge computing node (ECN) is associated with multiple client devices (CDs) for broadband access. Authentication is needed when any message is delivered in between the edge node and each CD, while any malicious node attempting to access the ECN should be rejected. Instead of cryptography based numeric approach, the channel matrix of each CD is used for the authentication purpose.

Fig.2 demonstrates the overall framework of the proposed system functions. In the training phase, the ECN measures the CSI of each CD $\boldsymbol{H}_i$ according to the received signal. The ECN uses the CSI to generate channel training vector specific to each CD. We assume that the ECN can verify the validity of the CSI through the conventional cryptography based approach implemented by the upper layer. The ECN then transfers the parameters of the TP-Net to each of the CDs.

When the TP-Net model is trained properly, the ECN and each CD can perform the desired PHY-layer authentication. Firstly, the ECN estimates the most updated CSI from the received signals sent by each CD and obtain the channel response matrix $\boldsymbol{H}_{i+1}$, which is fed into the TP-Net for authentication. The CSI used for the authentication purpose should be assumed same within the channel coherent time [12], otherwise, the authentication would expire and the proposed authentication system returns to the training phase. Finally, the TP-Net parameters will be updated after the next round of training.

III. Proposed TP-Net

The CNN-based neural network has been well recognized as a powerful tool for intelligent decision making in presence of big data sets [13]–[16]. Mostly, CNN has problem of overfitting and its mostly computationally expensive because it has to take a large amount of data for training. These problems, however, limit the applicability of CNN to edge computing systems. Although significant research has been conducted to explore more efficient CNN architectures, such as VGG-16, Resnet, and Inception, most of them require numerous layers consisting of a huge number of parameters to achieve desired accuracy.

Global-Connected Net (GC-Net) [13] is a recently introduced CNN architecture that is reported to achieve similar performance to that by its predecessors while taking much less parameters, thus requiring much less computation resources. The unique features of GC-Net include a globally connected interconnection architecture and a piecewise activation function between the convolution layers that can successfully mitigate the notorious gradient-vanishing problem.

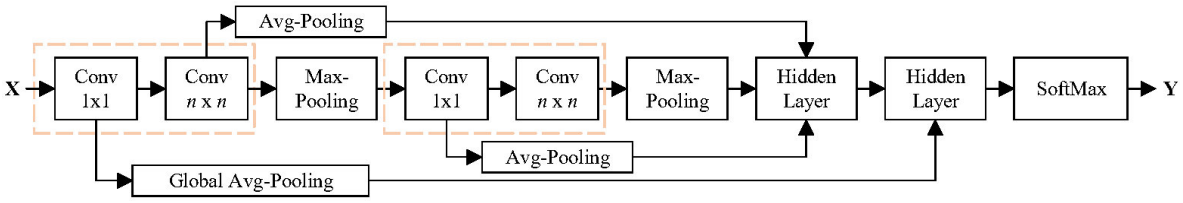


Fig. 3. Proposed Triple Pool Convolutional Neural Network (TP-Net).

Inspired by the GC-Net, we propose a new CNN architecture, namely TP-Net, whose interconnection architecture is shown in Fig.3. With n convolutional blocks in total, each block has two filters, followed by batch normalization and activation. The proposed TP-Net is distinguished from the conventional cascaded structure in a sense that any convolutional block is allowed to connect with a hidden layer that feeds into the last hidden layer and output (SoftMax) layer.

A unique design of the proposed TP-Net is that it consists of three types of pooling: max, average and global. The max-pooling is applied between two convolutional blocks to reduce the feature map sizes. The average pooling aims to tune the variance in the data set for possibly dimensional reduction. The global average pooling decreases the dimension rapidly to possibly save computation cost. The main reason behind using the triple pools is that the cons of a specific pooling type could be made up by the pros of the others.

The proposed TP-Net employs an exponential linear unit (ELU) and a standard unit SoftMax function as its activation functions, where the ELU is defined as a nonlinear function as presented in formula (1), and the SoftMax is defined by the formula (2), where, $i = 1, 2, \cdots, N$, and $\mathbf{z} = (z_1, z_2, \cdots, z_N) \in \mathbb{R}^N$.

$$f(x) = \begin{cases} x, & if\ x \geq 0; \\ \alpha\left(e^x - 1\right), & if\ x < 0; \end{cases} \tag{1}$$

$$SoftMax(\mathbf{z})_i = \frac{e^{z_i}}{\sum_{j=1}^{N} e_j^z}. \tag{2}$$

IV. Experimental Results

In this section, we will present our experimental results based on simulated data and practical channel data collected from our wireless testbed.

A. Overall Setting

Experiments are conducted to examine the proposed TP-CNN-PHA and compare it with a number of reported CNN models, including conventional CNN [16], GC-Net [13], and VGG [15]. We also consider the threshold-based method reported in [17] for comparison. For this purpose, two suites of experiment are conducted. The first is that we use channels generated by Rayleigh simulation model for CNN training and testing. The second set of experiment adapts the channel data collected from our NI USRP testbed for CNN training and testing.

The TP-Net is implemented with 4 convolutions, two of which are composed of 2 convolution layers with 1×1 filter and only 16 and 32 feature maps, respectively; and the other two are composed of 2 convolution layers with 3×3 filters and only 32 feature maps. The 2×2 max pooling layer with a stride of 2×2 as applied after both of the two 3×3 convolution layers. Global average pooling is applied to the output of the first convolution layer and the collected parameters are fed as input to the SoftMax layer for classification.

In the experiments, the conventional CNN is modeled with 2 convolutions, named as CNN-2, one of which is composed of 4×4 filter and only 8 feature maps, and the other is composed of 2×2 filters and only 16 feature maps. The 4×4 average pooling layer with a stride of 4×4 as applied after the 4×4 convolution layers. The 2×2 average pooling layer with a stride of 2×2 as applied after the 2×2 convolution layers. CNN-2 employs ReLU as its activation function.

GC-Net is composed of 3 convolution layers with small 3×3 filters and only 64, 64 and 64 feature maps, respectively. The 2×2 max pooling layer with a stride of 2×2 is applied after both of the first two convolution layers. GAP is applied to the output of each convolution layer and the collected averaged features are fed as input to the softmax layer for classification. GC-Net employs GReLU [13] as its activation function.

VGG is composed of 7 convolution layers with small 3×3 filters and only 64, 64, 128, 128, 256, 256 and 256 feature maps, respectively, which is named as VGG-7. The 2×2 max pooling layer with a stride of 2×2 is applied after the first two, the first four and the last convolution layer, respectively. VGG-7 employs ELU as its activation function. It contains two fully connected layers, one with 512 neurons followed by an ELU activation function, while the other one has "classes" neurons accompanyed with the softmax activation function, where "classes" is the total number to be classified.

Moreover, the adaptive moment estimation (Adam) accelerated gradient algorithm was used for the acceleration of all CNN training. For the parameter α of ELU, the default value is $\alpha = 1$.

The performance metric focused in the experiment is the authentication rate, denoted as $AucRate$, which is defined as the probability of correctly distinguishing whether a wireless node is legitimate or not up receiving an authentication request, as described in (3). More specifically, $AucRate$ is the ratio of the number of correctly authenticated samples to

TABLE I
THE TIME DELAY OF THE FIFTH PATH OF EIGHT WIRELESS NODES.

wireless node 1	wireless node 2	wireless node 3	wireless node 4	wireless node 5	wireless node 6	wireless node 7	wireless node 8
$12 \times 10^{-6}s$	$11 \times 10^{-6}s$	$10 \times 10^{-6}s$	$9 \times 10^{-6}s$	$8 \times 10^{-6}s$	$7 \times 10^{-6}s$	$6 \times 10^{-6}s$	$5 \times 10^{-6}s$

that of the total launched ones.

$$AucRate = \frac{1}{\Psi} \sum_{\Psi} \left(\hat{\boldsymbol{Y}}_{Auc} \circ \boldsymbol{Y}_{Auc} \right), \tag{3}$$

where Ψ is the total number of CSI that needs to be verified, $\hat{\boldsymbol{Y}}_{Auc} \circ \boldsymbol{Y}_{Auc}$ denotes the Hadamard product of the matrices $\hat{\boldsymbol{Y}}_{Auc}$ and $\boldsymbol{Y}_{Auc}$. $\hat{\boldsymbol{Y}}_{Auc}$ is the label of output of TP-Net, while the real label of the output is $\boldsymbol{Y}_{Auc}$.

In addition, network training time is used to reflect the computational complexity of the network, which is described in (4),

$$Training\ time = \sum\nolimits_{i=1}^{N} t_i, \tag{4}$$

where, t_i denotes the training time of i-th epoch, i is the number of epoch, and $i = 1, 2, \ldots, N$.

B. Results Based on Simulated Rayleigh Channels

In the computer simulations, the tapped delay line (TDL) model was exploited to simulate the Rayleigh fading channel with multipath delay [12], [18]. The TDL model employs a set of non-frequency selective fading generators, such as the Filtered White Gaussian Noise (FWGN) model, where each generator is independent of others and has an average power of one. The channel state information, denoted as $y(n)$, of different transmitters can be generated by

$$y(n) = \sum_{d=0}^{N_D-1} h_d(n) x(n-d), \tag{5}$$

where N_D denotes the number of taps of the channel filters with filter weights h_d. Five paths with different power delays were selected to synthesize the channels of legitimate and malicious nodes. The time delay of the first four paths of the wireless nodes was the same, which was 0 second (s), $2 \times 10^{-6}s$, $4 \times 10^{-6}s$, $8 \times 10^{-6}s$, respectively. When there were eight wireless nodes, the time delay of the fifth path of each wireless node was shown in Table I.

The least squares (LS) algorithm is adopted to estimate CSI in the orthogonal frequency-division multiplexing (OFDM) system. We set the sampling interval $t_{sampling} = 1 \times 10^{-6}s$, the number of subcarriers $n_{subcarrier} = 128$, the maximum Doppler frequency shift $f_d = 15$ (Hz), the pilot interval $n_{pilot\_interval} = 3$, cyclic prefix length $l_{cp\_length} = 16$, and the digital modulation method is QPSK. The number of channel data frames collected for each node is 200, and the number of channel data frames for each node training CNN is 100.

The experimental environment for simulation is as follows: the host CPU is with Intel (R) Core (TM) i7-9750H with the main frequency as 2.59 Giga Hertz (GHz), the physical memory as 16 GB, the operating system as 64-bit Win10 Professional. The Keras library in Python is used to build the network.

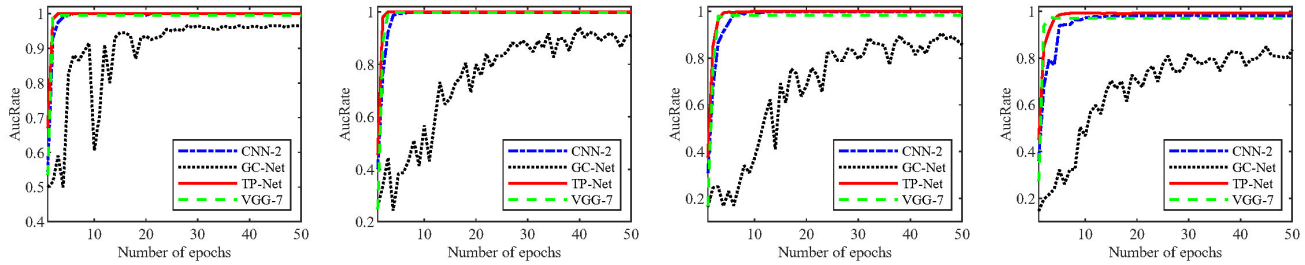
Fig.4 shows the results of authentication rate under different numbers of wireless nodes with channel signal-to-noise ratio (SNR) as 2dB, where the proposed TP-CNN-PHA scheme is compared with the case of using the conventional CNN (CNN-2), GC-Net, and VGG-7. It is clear that the TP-CNN-PHA using the proposed TP-Net can achieve the best performance, and such advantage remains when the number of wireless nodes increases.

Fig.5 shows the training time of each scheme, in which the CNN-2 scheme has the shortest training time, mainly because it only has two convolution layers. The training time of TP-Net is less than that of GC-Net and VGG-7. Since two convolution layers of TP-Net are 1×1 filter, which can reduces the operation time of convolution process. VGG-7 has the largest number of convolution layers, so it takes the most training time than others. These results indicate that the computational complexity of TP-Net is lower than GC-Net and VGG-7, but higher than that of CNN-2.

Fig.6 shows the comparison result among all the ML based schemes and the threshold-based scheme. The threshold-based method corresponds to a channel SNR of 2dB and 8dB, respectively, and the authentication rate of the ML based schemes is on a channel SNR of 2dB. We can see that the ML based schemes provide much better performance than the threshold based one on the channel SNR of 2dB. For the threshold based scheme, the authentication performance of 8dB SNR is better than that of 2dB SNR. This shows that the authentication performance of the threshold-based method is greatly affected by SNR. It confirms again that our scheme based on TP-Net has all advantages against all the other counterparts.

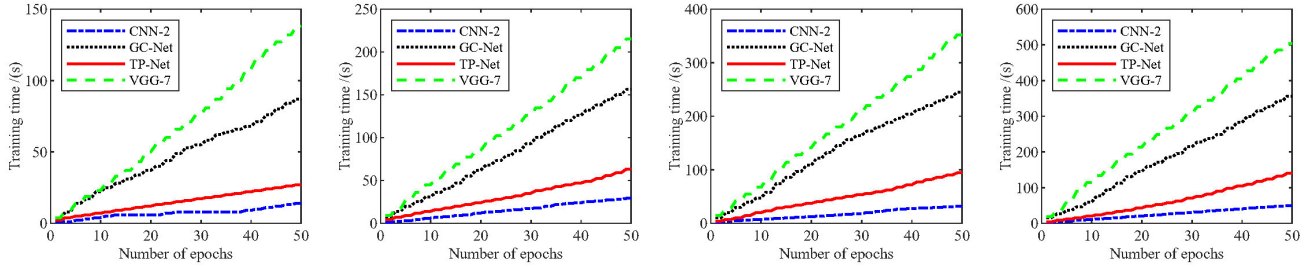
C. Experiments using Testbed Dataset

The proposed TP-CNN-PHA scheme is implemented over the NI USRP platforms. As shown in Fig.7, experiments were performed in an office room of 8 meters long, 7.5 meters wide, and 3 meters high. Edge computing device is simulated by four USRPs which configure 8 transmit and receive antennas, respectively. Four wireless client devices are simulated with different numbers of USRP. One node is equipped with 2 transmit and 2 receive antennas, respectively, while the other nodes are simulated by 2 USRPs which configure 4 transmit and 4 receive antennas, respectively. In the experiment, the communication solution is based on MIMO-OFDM and Improved-scaled Least Squares (ILS) is adopted to estimate CSI [19], [20]. We set the center frequency is $f_c = 3.5$ Giga



(a) 2 wireless nodes. (b) 4 wireless nodes. (c) 6 wireless nodes. (d) 8 wireless nodes.

Fig. 4. The authentication rate under different numbers of wireless nodes with channel SNR as 2dB. (a) The authentication rate of 2 wireless nodes. (b) The authentication rate of 4 wireless nodes. (c) The authentication rate of 6 wireless nodes. (d) The authentication rate of 8 wireless nodes.



(a) 2 wireless nodes. (b) 4 wireless nodes. (c) 6 wireless nodes. (d) 8 wireless nodes.

Fig. 5. The training time of each scheme under different numbers of wireless nodes. (a) The training time of 2 wireless nodes. (b) The training time of 4 wireless nodes. (c) The training time of 6 wireless nodes. (d) The training time of 8 wireless nodes.

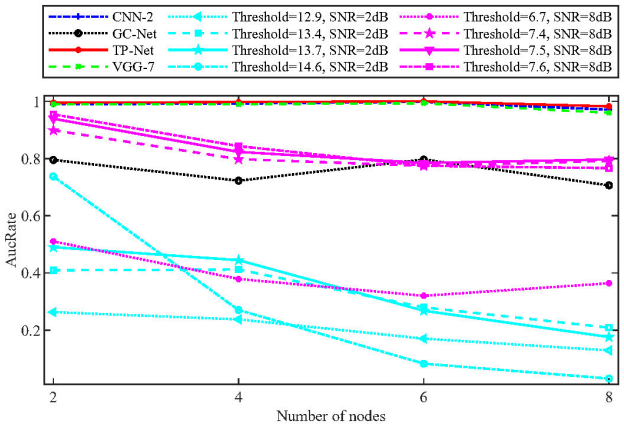


Fig. 6. The comparison of authentication rate under different numbers of wireless nodes among all the ML based schemes and a threshold-based scheme, where the authentication rate of ML based schemes is the result of the 50th epoch.

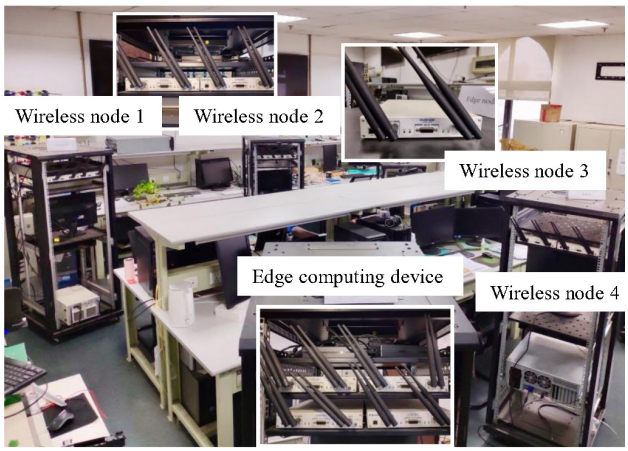
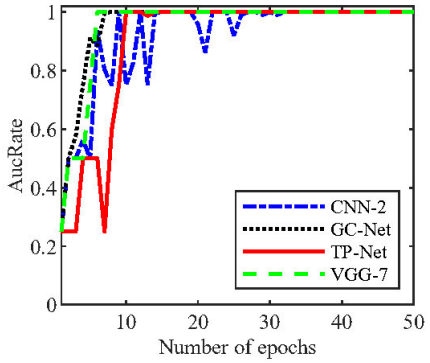


Fig. 7. Real experiment environment and test platforms.

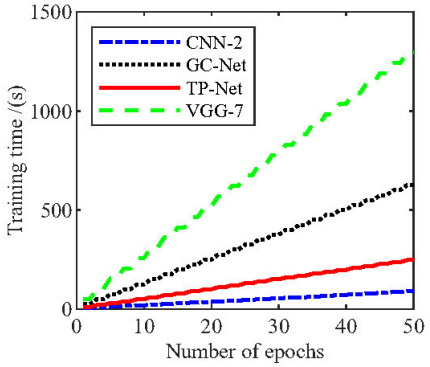
Hertz (GHz), the number of subcarriers is $n_{subcarrier} = 128$, the sampling interval $t_{sampling} = 5 \times 10^{-7} s$, the wavelength of the transmission signal is about $\lambda_{wave\_length} = 0.086$ meters, the digital modulation method is 4QAM, and the transmitting power was 15dBm and transmission gain 20 dB. The number of frames collected for each wireless node is 200 and the number of training frames per wireless node is 100.

The server parameters of the training CNN are as follows: the server CPU is with Intel(R) Xeon(R) Silver 4114 with the main frequency as 2.2 GHz, the physical memory as 15982940 kB, the operating system as Ubuntu 18.04.4 LTS.

Fig.8 demonstrates the authentication performance on the USRP testbed. Clearly, from the Fig.8(a), after many epochs, the authentication performance of all schemes converges and the authentication results are decent. From the Fig.8(b), the training time of TP-Net scheme is always slightly higher than CNN-2 but much lower than that of VGG-7 and GC-Net. This result is similar to the previous simulation result of Fig.5(b), proving that the computational complexity of TP-Net scheme is not high. The TP-Net is observed to facilitate the best performance and is proved of the best feasibility to the considered application scenarios.



(a) Authentication rate.



(b) Training time.

Fig. 8. The authentication performance of four wireless nodes in the real scene. (a) Authentication rate. (b) Training time.

V. Conclusions

In this piece of work, we have proposed a new ML based PHY-layer authentication scheme, called TP-CNN-PHA, for light-weight user authentication in edge computing systems. We introduced TP-Net, that is a novel CNN architecture serving as the core of TP-CNN-PHA, and is designed by jointly employing max, global, and average pooling. We conducted extensive experiments by using both simulation and our USRP testbed. The results showed that the proposed scheme not only ranks up in terms of authentication accuracy compared with its counterparts, but also can reduce the computational complexity significantly at model training phase. The proposed scheme is much better than the traditional method based on threshold values in terms of authentication accuracy, and also avoids the trouble of finding proper threshold values. Because the proposed framework can achieve satisfactory authentication accuracy with low computational overhead, we expect this framework can more secure environment for users in the edge computing system.

References

[1] R. Liao, H. Wen, S. Chen, F. Xie, F. Pan, J. Tang, and H. Song, "Multiuser physical layer authentication in internet of things with data augmentation," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2077–2088, Mar. 2020.

[2] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[3] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[4] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Communications Letters*, vol. 19, no. 1, pp. 74–77, Jan. 2015.

[5] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4171–4182, June 2016.

[6] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 037–10 047, Dec. 2016.

[7] X. Wang, L. Gao, S. Mao, and S. Pandey, "Csi-based fingerprinting for indoor localization: A deep learning approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 763–776, Jan. 2017.

[8] N. Wang, T. Jiang, S. C. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1557–1560, Jul. 2017.

[9] K. M. Borle, B. Chen, and W. K. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2225–2235, Oct. 2015.

[10] M. S. Omar, S. A. R. Naqvi, S. H. Kabir, and S. A. Hassan, "An experimental evaluation of a cooperative communication-based smart metering data acquisition system," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 399–408, Feb. 2017.

[11] Y. Chen, H. Wen, J. Wu, H. Song, A. Xu, Y. Jiang, T. Zhang, and Z. Wang, "Clustering based physical-layer authentication in edge computing systems with asymmetric resources," *Sensors*, vol. 19, no. 8, p. 1926, Apr. 2019.

[12] R. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, and M. Cao, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116 390–116 401, Aug. 2019.

[13] Z. Chen and P. Ho, "Cloud based content classification with global-connected net (gc-net)," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, Feb. 2018, pp. 1–6.

[14] G. Huang, Y. Sun, Z. Liu, D. Sedra, and K. Q. Weinberger, "Deep networks with stochastic depth," in *European conference on computer vision*. Springer, 2016, pp. 646–661.

[15] G. Lou and H. Shi, "Face image recognition based on convolutional neural network," *China Communications*, vol. 17, no. 2, pp. 117–124, Feb. 2020.

[16] R. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, "Deep-learning-based physical layer authentication for industrial wireless sensor networks," *Sensors*, vol. 19, no. 11, p. 2440, May 2019.

[17] F. Pan, Z. Pang, M. Luvisotto, X. Jiang, R. N. Jansson, M. Xiao, and H. Wen, "Authentication based on channel state information for industrial wireless communications," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018, pp. 4125–4130.

[18] R. Clarke, "A statistical theory of mobile-radio reception," *Bell System Technical Journal*, vol. 47, no. 6, pp. 957–1000, 1968.

[19] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for ofdm systems with rapid dispersive fading channels," *IEEE Transactions on Communications*, vol. 46, no. 7, pp. 902–915, Jul. 1998.

[20] E. G. Larsson, G. Q. Liu, J. Li, and G. B. Giannakis, "Joint symbol timing and channel estimation for ofdm based wlans," *IEEE Communications Letters*, vol. 5, no. 8, pp. 325–327, Aug. 2001.