https://doi.org/10.7840/kics.2025.50.11.1660

Physical Layer Authentication for Mobile Devices in WLAN Systems: An Autoencoder-Based Approach

Ralph Kumah Assan◆, Jihwan Moon*, Taehoon Kim**, Inkyu Bang°

ABSTRACT

Physical layer authentication (PLA) enhances wireless security by using wireless channel features like channel state information (CSI) to authenticate transmitters and detect adversaries. While machine learning (ML) has been applied to improve PLA, most methods require adversary data or assume a stationary environment, limiting real-world practicality. This paper proposes an autoencoder-based PLA framework that relies solely on legitimate users' CSI to distinguish them from adversaries in dynamic wireless environments. Using a wireless local area network (WLAN) testbed (e.g., Wi-Fi) with mobile and stationary devices in both line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios, experimental results show that the proposed method outperforms existing schemes in authentication accuracy under mobility conditions.

Key Words : Physical layer authentication, autoencoder, mobility, channel state information, anomaly detection

Ⅰ. Introduction

The rapid advancement of the fifth-generation (5G) and next-generation wireless networks has unraveled a new era of global connectivity. The evolution of wireless communication systems is expected to provide diverse services and applications through seamless connectivity with various Internet of Things (IoT) devices[1]. The number of IoT devices in wireless networks has increased steadily but they are also exposed to unexpected security threats due to diverse attack vectors in IoT networks. Traditional security protocols in wireless networks primarily depend on cryptographic techniques, which are often inadequate for resource-constrained IoT applications such as sensing and smart home applications[2]. Accordingly, alternative security techniques such as physical layer security and physical layer authentication (PLA) have been recently studied to compensate for limitations in directly applying the existing security protocols to IoT devices[3].

Physical layer authentication (PLA) is one of the promising techniques for enhancing wireless security, which exploits features of wireless channels, such as channel state information (CSI), to authenticate legitimate transmitters and identify malicious users (i.e., adversaries)[4]. Recent studies have shown that machine learning (ML)-based PLA schemes can improve authentication accuracy[5]. For example, Liu *et al.* applied support vector machine (SVM) algorithms to PLA, using CSI to build user-specific profiles in stationary scenarios[6]. However, most of the existing ML-based PLA techniques are required to collect both legitimate users' and adversaries' CSI data for

※ This research was supported by the HBNU 2024 KNUDP(Korea National University Development Project) funded by the Ministry of Educa- tion(MOE, Korea) and National Research Foundation of Korea(NRF).

◆ First Author : Portland State University, Department of Electrical and Computer Engineering, rassan@pdx.edu, 학생회원
* Hanbat National University, Department of Mobile Convergence Engineering, anschino@staff.hanbat.ac.kr, 정회원
** Hanbat National University, Department of Computer Engineering, thkim@hanbat.ac.kr(co-corresponding author), 종신회원
° Corresponding Author : Hanbat National University, Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 종신회원

논문번호 : 202504-096-A-RU, Received April 28, 2025; Revised May 23, 2025; Accepted May 23, 2025

training.

In fact, it is difficult to measure adversaries' CSI data in practical scenarios, and thus there have been studies to tackle this issue. In [7], this problem is investigated by focusing on a stationary environment. This study employs the one-class SVM (OSVM) model which is trained exclusively on legitimate users' data. The OSVM model shows high accuracy in detecting anomalies considering static conditions.

In addition, the use of generative adversarial networks (GAN) was employed in [8]-[10] to detect adversaries while also identifying legitimate radio frequency transmitters in stationary environments. In [11], a dual-input convolution neural network (CNN) model is proposed to learn the temporal and spatial similarity scores between two input CSIs limited by the need for both legitimate user and adversary CSI data, making them less suitable for real-world use. Despite the growing body of work on ML-based PLA schemes, most existing studies focus on stationary environments or require adversary data, which makes them unsuitable for mobile settings.

Moreover, deep learning-based classifiers such as CNNs, LSTMs, or transformers, though effective, typically depend on supervised learning involving both classes of data, including adversarial samples, which are often unavailable in real-time deployment scenarios. In contrast, autoencoder architectures offer a powerful solution for one-class learning by learning compact representations of legitimate users' CSI only, and identifying deviations as anomalies. This makes them naturally aligned with practical PLA systems where only legitimate channel profiles can be reliably acquired. Furthermore, the autoencoder can flexibly capture complex spatio-temporal patterns without explicit attacker labels, thus eliminating the dependency on a complete adversarial dataset and improving robustness under mobility.

To fill this gap, we propose an autoencoder-based PLA framework that only exploits legitimate users' CSI data to efficiently learn the temporal and spatial differences between legitimate users and adversaries in dynamic wireless environments.While our experiments are limited to a controlled indoor Wi-Fi 6 testbed using the 2.4 GHz band, the methodology is generalizable and can be extended to other configurations including outdoor, 5 GHz Wi-Fi, or mmWave systems in future work.

The main contributions of this work are summarized as follows: (1) We propose an autoencoder-based anomaly detection algorithm to authenticate legitimate users against adversaries in mobile environments; (2) We set up our testbed considering mobile and stationary devices in the wireless local area network (WLAN) environment (e.g., Wi-Fi) and collect extensive CSI data for training and evaluation in both line-of-sight (LoS) and non line-of-sight (NLoS) scenarios; (3) The experiment results demonstrate that the proposed PLA scheme outperforms the OSVM-based method, particularly in dynamic wireless environments, highlighting its potential for real-world IoT security applications. A comparison with the OSVM serves as a meaningful baseline aligned with the constraint of unsupervised learning, and further evaluations with other deep models are suggested as future extensions.

Ⅱ. System and Threat Model

In this section, we introduce our system and threat model, including some basics for the IEEE 802.11 physical layer and assumptions for an adversary.

2.1 System Model

We consider two legitimate devices (Alice and Bob) and a single adversary as illustrated in Fig. 1, where H_B and H_A indicate channel state information in the frequency domain at Bob and adversary,

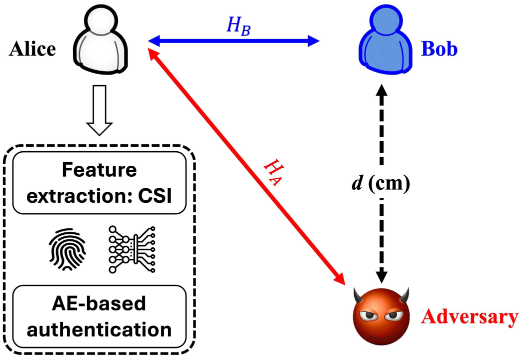


Fig. 1. System model

respectively. Alice (e.g., access point) is responsible for authenticating legitimate users (i.e., Bob) considering CSI as a feature for a one-class classifier. We assume that both Bob and an adversary are mobile and apart from each other at least d cm. We consider that every node (including an adversary) adopts orthogonal frequency division multiplexing (OFDM) for physical layer transmission with the IEEE 802.11ax standard[12].

Alice receives OFDM signals from Bob or the adversary and estimates the CSI of them. The received signal at Alice in the frequency domain is given by

$$Y(k)=H(k)X(k)+N(k), \tag{1}$$

where k denotes a subcarrier index, $H(k)$, $X(k)$, and $N(k)$ indicates channel response in the frequency domain, transmitted symbol, and additive white Gaussian noise (AWGN), respectively, on subcarrier k.

Although our setup considers only one legitimate transmitter-receiver pair and one adversary, this model can be extended to multi-user scenarios involving concurrent transmissions and interference sources. In such environments, the classifier may need to be adapted to operate over segmented or aggregated CSI streams from multiple users, and future work will explore such scalability. The IEEE 802.11ax standard adopts the high-efficiency long training field (HE-LTF) to precisely estimate CSI over wideband. If we consider $X(k)$ as the pilot symbol in the frequency domain, the channel estimation on subcarrier k is calculated as

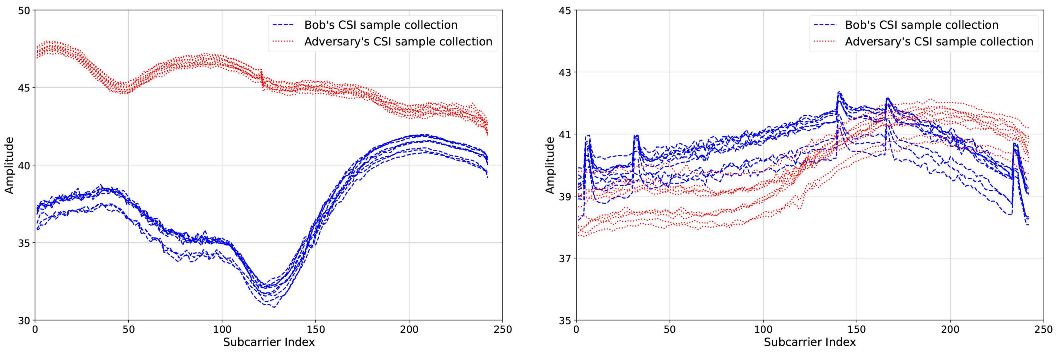
$$\hat{H}(k)=H(k)+\frac{N(k)}{X(k)},\quad k=0,1,\cdots,n_{\mathrm{sc}}-1, \tag{2}$$

where n_{sc} is the number of subcarriers, which is set to 242 for a 20 MHz bandwidth in the IEEE 802.11ax. Thus, Alice can estimate CSI from any received signals and also ask Bob to repeat transmission for CSI collection.

2.2 Threat Model

The adversary's primary objective is to bypass Alice's authentication, which could serve as an entry point for more sophisticated cyberattacks (e.g., malware injection into a router). It is assumed that conventional authentication protocols can be compromised, making physical layer authentication (PLA) the primary security measure. We also consider that an adversary is placed or moving close to Bob with short distance of d cm to increase the possibility of passing the authentication with similar channel properties to that of Bob. This model assumes a passive and nearby adversary who attempts to mimic the CSI profile of the legitimate user. This is a realistic and challenging case.

It is worth noting that more sophisticated attack models, such as replay attacks, signal amplification, coordinated adversarial nodes, or mobile relays, could be deployed in practice. However, these types of active and cooperative adversaries remain outside the scope of this study but are important directions for future investigation, particularly to evaluate the robustness of the proposed framework against high-



(a) Stationary scenario

(b) Mobile scenario

Fig. 2. 10 CSI samples collected from Bob and the adversary for $d=10$ cm: (a) stationary scenario and (b) mobile scenario er-layer attacks and physical-layer impersonation strategies.

Remark 1. *Fig. 2 shows CSI samples from Bob and the adversary in stationary and mobile scenarios (on the top of the next page). In the stationary scenario (Fig. 2a), a clear distinction is observed, whereas in the mobile scenario (Fig. 2b), the difference is less apparent due to CSI variations. While ML-based PLA schemes work well in stationary environments, they struggle in mobile settings, highlighting the need for more robust deep learning-based anomaly detection models for improved accuracy.*

Ⅲ. Autoencoder-based PLA

This section presents our proposed autoencoder-based PLA scheme, detailing the autoencoder architecture and the anomaly detection criterion.

The proposed scheme leverages only legitimate users' CSI data to effectively learn the temporal and spatial differences between legitimate users (i.e., Bob) and adversaries in mobile environments. The overall framework is illustrated in Fig. 3 with each step discussed in the following subsections. Unlike classification-based approaches that require labeled examples of both legitimate users and adversaries, the proposed autoencoder is trained solely on legitimate users' data, allowing it to learn the manifold of authorized CSI patterns. This design mitigates the practical limitation of requiring adversary CSI data and enables anomaly detection based on reconstruction errors, which reflect deviation from the legitimate distribution. Additionally, by capturing nonlinear temporal and spatial relationships in CSI, the autoencoder is more robust to mobility-induced channel variations.

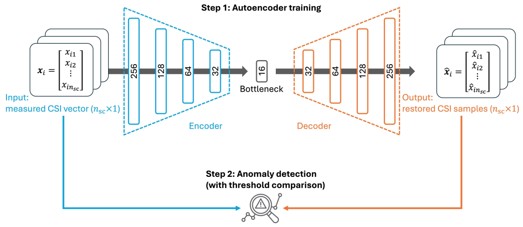

Step 1: Autoencoder training
$x_i = \begin{bmatrix} x_{i1} \\ x_{i2} \\ \vdots \\ x_{in_{sc}} \end{bmatrix}$
Input:
measured CSI vector (n_{sc}×1)
256
128
64
32
Encoder
16
Bottleneck
32
64
128
256
Decoder
$\hat{x}_i = \begin{bmatrix} \hat{x}_{i1} \\ \hat{x}_{i2} \\ \vdots \\ \hat{x}_{in_{sc}} \end{bmatrix}$
Output:
restored CSI samples (n_{sc}×1)
Step 2: Anomaly detection
(with threshold comparison)

Fig. 3. Overview of the proposed autoencoder-based anomaly detection procedure

3.1 Autoencoder Architecture

In Step 1 of Fig. 3, the proposed autoencoder network processes CSI samples from either a legitimate user or an adversary. The input consists of CSI values across multiple subcarriers, with a dimensionality of $n_{sc} \times M$, where M represents the number of features considered. In this study, $M = 1$ as only the absolute amplitude of CSI values is used. Previous studies, such as [11], have shown that magnitude-based features outperform complex CSI for authentication tasks, as magnitude is less influenced by phase variations due to carrier frequency offset, making it more robust in dynamic environments.

The autoencoder architecture consists of a symmetric encoder-decoder structure with a bottleneck layer for dimensionality reduction and feature extraction. The encoder reduces CSI data through fully connected layers, with neuron sizes 256 → 128 → 64 → 32 → 16, while the decoder reconstructs it symmetrically (16 → 32 → 64 → 128 → 256). The ReLU activation function is applied to all layers except the final output layer, which employs linear activation. The model is trained by minimizing the mean squared error (MSE) using the Adam optimizer with a learning rate of 10^{-4}, and early termination is implemented to prevent overfitting. The training process uses a batch size of 64 and is executed over a maximum of 100 epochs, with early stopping triggered if the validation loss does not improve for 10 consecutive epochs. These configurations ensure stable convergence while preserving generalization.

3.2 Anomaly Detection Criterion

Once the autoencoder is trained, it is used for anomaly detection. As described in step 2 of Fig. 3, the proposed autoencoder-based PLA scheme compares the input CSI data $\mathbf{x}_i = [x_{i1}, \cdots, x_{in_{\mathrm{sc}}}]^T$ and the reconstructed one $\hat{\mathbf{x}}_i = [\hat{x}_{i1}, \cdots, \hat{x}_{in_{\mathrm{sc}}}]^T$, where i indicates the data index.

We define the reconstruction error ε_i for the input CSI data i based on MSE between $\mathbf{x}_i$ and $\hat{\mathbf{x}}_i$ as follows:

$$\varepsilon_i = \frac{1}{n_{\mathrm{sc}}} \sum_{j=1}^{n_{\mathrm{sc}}} (x_{ij} - \hat{x}_{ij})^2. \tag{3}$$

Finally, we consider threshold-based comparison for anomaly detection, which is given by

$$r_i = \begin{cases} 1, & \text{if } \varepsilon_i > T_0, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where T_0 denotes a pre-determined threshold value and r_i represents a detection result for input data index i and it indicates anomaly CSI data for $r_i = 1$ (i.e., CSI data from adversary) and legitimate CSI data for $r_i = 0$, respectively.

Remark 2. *In scenarios where adversarial data is unavailable-such as during real-world deployment-the optimal threshold T0 cannot be computed using metrics that depend on both legitimate and adversarial labels. To address this limitation, we adopt an adaptive thresholding scheme that estimates the decision boundary based solely on the distribution of reconstruction errors from legitimate users during training. Specifically, the optimal threshold is selected based on the 90th quantile of the reconstruction error distribution, ensuring that the majority of legitimate samples fall below this boundary. This approach enables unsupervised deployment and preserves anomaly detection capabilities in the absence of ground-truth adversarial data, making it more suitable for practical implementation in dynamic wireless environments.*

Ⅳ. Performance Evaluation

This section investigates our experimental setup, scenarios, and results of the proposed PLA scheme compared to the existing OSVM-based approach.

4.1 Experimental Setup

The experiment configures Alice as a Wi-Fi 6 access point (AP), as shown in Fig. 4. The AP is a NETGEAR AX1800 (RAX20) model, supporting the IEEE 802.11ax standard. We operate on a 20 MHz bandwidth within the 2.4 GHz frequency band, utilizing 242 subcarriers for CSI measurement. Bob and the adversary are high-performance laptops with Intel i7 (8-core CPU), 16GB RAM, and Intel AX201 NICs, running Ubuntu 20.04 LTS. This setup represents a controlled indoor environment with homogeneous device capabilities. While this provides reproducible results, future work will extend the evaluation to more diverse scenarios, such as 5 GHz band, outdoor line-of-sight and non-line-of-sight settings, and heterogeneous chipsets. These steps are essential to assess the method's robustness under more challenging wireless conditions.

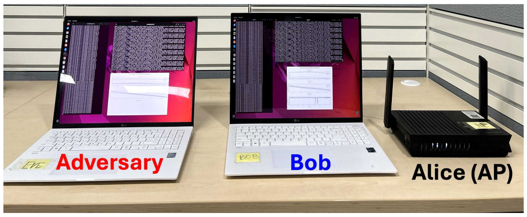


Fig. 4. Experiment setup: NETGEAR AX1800 (RAX20) model used as AP (Alice) and two laptops equipped with Intel AX201 NIC used for Bob and the adversary

To collect and analyze CSI data, we employ the PicoScenes open-source software[13], which enables fine-grained CSI extraction from commodity Wi-Fi devices, providing a flexible framework for wireless signal analysis research.

4.2 Experimental Scenarios

We conducted our experiment in our laboratory and near places located on the sixth floor of the N4 building at Hanbat National University, South Korea. Fig. 5 shows details of our experimental scenarios. We consider two experimental scenarios considering non lineof-sight (NLoS) and line-of-sight (LoS) environments.

For the NLoS scenario, the presence of obstacles and reflections within the laboratory introduces significant variability in the wireless channels. For the LoS scenario, a direct LoS is guaranteed and thus clearer signal propagation is expected, minimizing interference from obstacles and enhancing the reliability of CSI measurements. A total of 50,000 CSI frames were collected across all scenarios at a rate of 100 frames per second. The data was split 70% for training

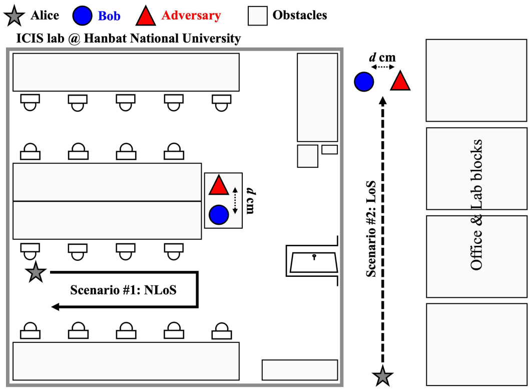


Fig. 5. Experimental scenarios: LoS and NLoS environments

and 30% for testing, with 10% of the training data used for validation. This evaluation assumes only one legitimate user and one adversary with dedicated channel access. However, realistic wireless environments often involve multiple users, devices, and interfering traffic. Future experiments will incorporate crowding effects and concurrent transmissions to investigate the scalability and interference resilience of the proposed scheme.

Bob and the adversary remain fixed at a distance *d* cm apart, while Alice moves to induce channel variations. This setup is equivalent to moving Bob and the adversary while keeping Alice stationary, allowing precise control over spatial separation. CSI samples were collected from both Bob and the adversary, but only Bob's samples were used to train the proposed autoencoder-based PLA scheme. Both devices continuously ping the AP at 0.01 second intervals. The experiments were conducted at three distances: 10 cm, 50 cm, and 100 cm, to assess how proximity influences the PLA system' s ability to detect adversarial presence.

4.3 Performance Metrics

The performance of the proposed PLA scheme is evaluated using the receiver operating characteristic (ROC) curve and the area under the curve (AUC). The ROC curve visually represents the trade-off between the true positive rate and the false positive rate across various decision thresholds, providing insight into the model's ability to distinguish between legitimate and adversarial users. The AUC quantifies the overall performance of the model by measuring the area beneath the ROC curve, where a higher AUC value signifies greater classification accuracy and improved adversary detection capabilities.

4.4 Experimental Results

The OSVM model-based PLA scheme (shortly, OSVM in this subsection) as the baseline scheme during the performance evaluation of our autoencoder-based PLA scheme (shortly, AE in this subsection).

Fig. 6 and Fig. 7 present the performance comparison between AE and OSVM across different distances in both NLoS and LoS scenarios. The AUC results confirm that AE consistently outperforms OSVM at all tested distances in both environments. Moreover, the findings indicate that increasing the distance *d* between Bob and the adversary enhances authentication accuracy. This improvement arises due to reduced spatial correlation in CSI, making it increasingly difficult for the adversary to replicate Bob's CSI characteristics. The AE model effectively leverages these differences, achieving superior anomaly detection and authentication accuracy. Although the current work compares only with OSVM as a baseline, which also adheres to a one-class learning framework, future research will incorporate additional deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformer-based architectures. These comparisons will

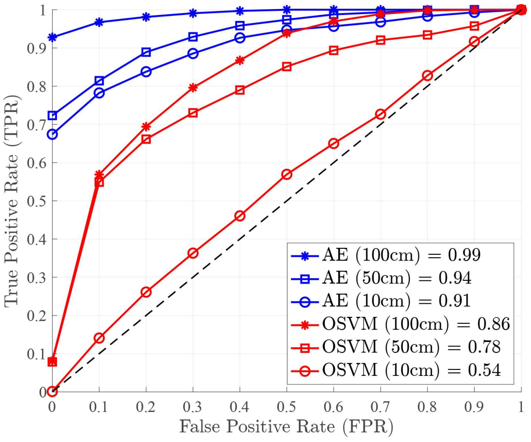


Fig. 6. ROC curve of OSVM versus the proposed one (i.e., AE) in NLoS for all distances

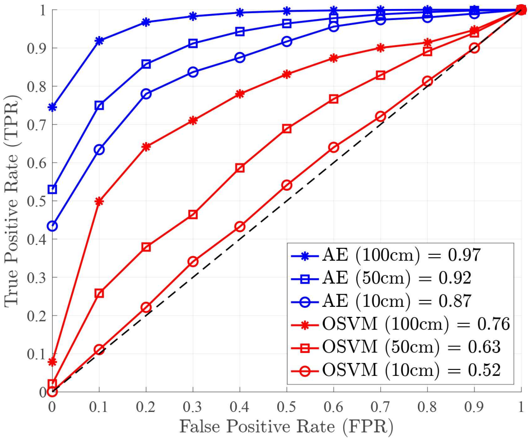


Fig. 7. ROC curve of OSVM versus the proposed one (i.e., AE) in LoS for all distances

help determine whether the unsupervised autoencoder remains superior when attacker labels are unavailable, or if supervised models can perform better under relaxed assumptions.

Fig. 8 illustrates that both AE and OSVM models achieve higher authentication accuracy in NLoS scenarios compared to LoS environments. Specifically, the AE model attains authentication accuracies of 0.84, 0.90, and 0.94 at distances of 10 cm, 50 cm, and 100 cm in NLoS, whereas in LoS, the accuracy slightly decreases to 0.81, 0.86, and 0.90, respectively. A similar pattern is observed for OSVM, where accuracy is lower in LoS than in NLoS. In particular, OSVM achieves 0.58, 0.72, and 0.80 in NLoS, whereas in LoS, it records 0.55, 0.70, and 0.78 at distances of 10 cm, 50 cm, and 100 cm, respectively. The observed performance gap between NLoS and LoS environments is attributed to the increased multipath effects in NLoS, which introduces more pronounced variations in CSI. These variations make it significantly more challenging for an adversary to imitate Bob' s CSI patterns, thereby strengthening the security of the proposed scheme.

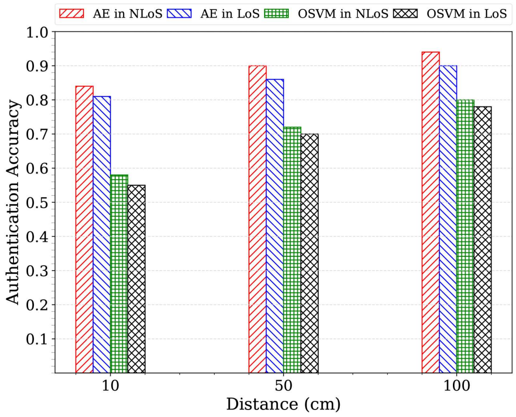


Fig. 8. Distance vs authentication accuracy between AE and OSVM for all distances

In Table 1, we assess the impact of threshold selection sensitivity, we consider three cases: a lower threshold T_L (corresponding to the 80th percentile), the adopted threshold T_0 at the 90th percentile, and a higher threshold T_H (corresponding to the 95th percentile) of the reconstruction error distribution. The authentication performance of the proposed AE model is evaluated across these thresholds. In the LoS scenario, all three threshold configurations yield relatively high accuracy, particularly at longer distances. However, in the NLoS scenario, only the 90th percentile threshold consistently achieves high authentication accuracy across all evaluated distances, whereas both the lower and higher percentile thresholds result in performance fluctuations due to the increased channel variability introduced by multipath effects. These results confirm the robustness and reliability of the adaptive thresholding strategy, demonstrating its suitability for unsupervised deployment in dynamic and complex wireless environments.

Table 1. Threshold comparison across distances

	Distance	T_L	T_0	T_H
LoS	10 cm	82.0%	87.0%	80.0%
	50 cm	88.0%	92.0%	87.0%
	100 cm	92.0%	97.0%	91.0%
NLoS	10 cm	72.0%	91.0%	83.0%
	50 cm	81.0%	94.0%	74.0%
	100 cm	69.0%	99.0%	88.0%

V. Conclusion

In this paper, we investigated the autoencoder-based physical layer authentication framework that only exploits legitimate users' channel state information (CSI) data to efficiently learn the temporal and spatial differences between legitimate users and adversaries in the mobile scenario. We performed extensive experiments by collecting many CSI data samples for training and evaluation in both non line-of-sight and line-of-sight scenarios. Our experimental results verified that the proposed autoencoder-based PLA scheme outperforms the existing one in terms of authentication accuracy in dynamic wireless environments. Future research aims to study additional physical layer features to enhance authentication accuracy and resilience against adversaries.

References

[1] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6G internet of things: A comprehensive survey," *IEEE Internet of Things J.*, vol. 9, no. 1, pp. 359-383, 2022. (https://doi.org/10.1109/JIOT.2021.3103320)

[2] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surv. & Tuts.*, vol. 23, no. 4, pp. 2384-2428, 2021. (https://doi.org/10.1109/COMST.2021.3108618)

[3] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things J.*, vol. 6, no. 5, pp. 8169-8181, 2019. (https://doi.org/10.1109/JIOT.2019.2927379)

[4] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics and Secur.*, vol. 3, no. 1, pp. 38-51, 2008. (https://doi.org/10.1109/TIFS.2007.916273)

[5] T. M. Hoang, A. Vahid, H. D. Tuan, and L. Hanzo, "Physical layer authentication and security design in the machine learning era," *IEEE Commun. Surv. & Tuts.*, vol. 26, no. 3, pp. 1830-1860, 2024. (https://doi.org/10.1109/COMST.2024.3363639)

[6] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 251-264, Feb. 2018. (https://doi.org/10.1109/TMC.2017.2718540)

[7] Q. Sun, X. Miao, Z. Guan, J. Wang, and D. Gao, "Spoofing attack detection using machine learning in cross-technology communication," *Secur. and Commun. Netw.*, vol. 2021, pp. 1-12, 2021. (https://doi.org/10.1155/2021/3314595)

[8] S. Karunaratne, E. Krijestorac, and D. Cabric, "Penetrating RF fingerprinting-based authentication with a generative adversarial attack," in *Proc. IEEE ICC*, pp. 1-6, Montreal, QC, Canada, 2021. (https://doi.org/10.1109/ICC42927.2021.9500893)

[9] H. Han, L. Cui, W. Li, L. Huang, Y. Cai, J. Cai, and Y. Zhang, "Radio frequency fingerprint based wireless transmitter identification against malicious attacker: An adversarial learning approach," in *Proc. Int. Conf. WCSP*, pp. 310-315, Wuhan, China, 2020. (https://doi.org/10.1109/WCSP49889.2020.9299859)

[10] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "RFAL: Adversarial learning for RF transmitter identification and classification," *IEEE Trans. Cognitive Commun. and Netw.*, vol. 6, no. 2, pp. 783-801, 2019. (https://doi.org/10.1109/TCCN.2019.2948919)

[11] Y. Guo, J. Zhang, and Y.-W. P. Hong, "Deep learning-enhanced physical layer authentication for mobile devices," in *Proc. IEEE GLOBECOM 2023*, pp. 826-831, Kuala Lumpur, Malaysia, 2023. (https://doi.org/10.1109/GLOBECOM54140.2023.10437299)

[12] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11ax high efficiency WLANs," *IEEE Commun. Surv. & Tuts.*, vol. 21, no. 1, pp. 197-216, 2018. (https://doi.org/10.1109/COMST.2018.2871099)

[13] Z. Jiang, T. H. Luan, X. Ren, D. Lv, H. Hao, J. Wang, K. Zhao, W. Xi, Y. Xu, and R. Li,

"Eliminating the barriers: Demystifying Wi-Fi baseband design and introducing the PicoScenes Wi-Fi sensing platform," *IEEE Internet of Things J.*, vol. 9, no. 6, pp. 4476-4496, Mar. 2022. (https://doi.org/10.1109/JIOT.2021.3104666)

Ralph Kumah Assan

2021 : B.Eng., Kwame Nkrumah University of Science and Technology (KNUST), Ghana

2025 : M.Eng., Hanbat National University, South Korea

2025~Current : Ph.D. Candidate Student, Departmnet of Electrical and Computer Engineering, Portland State University, USA

<Research Interest> Wireless network security, physical layer security, physical layer authentication.

[ORCID:0009-0007-3247-7443]

Jihwan Moon

2019 : Ph.D. Electrical Engineering, Korea University, South Korea

2019~2019 : Post-Doctoral Research Associate, Korea University, South Korea

2019~2020 : Senior Researcher, Affiliated Institute of ETRI, South Korea

2020~2022 : Assistant Professor, Department of Information and Communication Technology, Chosun University, South Korea

2022~Current : Assistant Professor, Department of Mobile Convergence Engineering, Hanbat National University, South Korea

<Research Interests> Optimization techniques, energy harvesting, physical-layer security, wireless surveillance, covert communications, and machine learning for wireless communications.

[ORCID:0000-0002-9812-7768]

Taehoon Kim

2017 : Ph.D. Electrical Engineering, KAIST, South Korea

2017~2020 : Senior Researcher, Agency for Defense Development, South Korea

2020~Current : Associate Professor/Assistant Professor, Department of Computer Engineering, Hanbat National University, South Korea

<Research Interests> Wireless communications, satellite communications, machine learning for wireless communications, and wireless network security.

[ORCID:0000-0002-9353-118X]

Inkyu Bang

2017 : Ph.D. Electrical Engineering, KAIST, South Korea

2017~2019 : Research Fellow, National University of Singapore, Singapore

2019~2019 : Senior Researcher, Agency for Defense Development, South Korea

2019~Current : Associate Professor/Assistant Professor, Department of Intelligence Media Engineering, Hanbat National University, South Korea

<Research Interests> Information-theoretic security (physical-layer security), mobile network security in 5G/6G, satellite communication, and AI applications in wireless communication systems.

[ORCID:0000-0001-7109-1999]