electronics

MDPI

Article

Intelligent Security Authentication for Connected and Autonomous Vehicles: Attacks and Defenses

Xiaoying Qiu [1,*], Jinwei Yu [2], Wenbao Jiang [1] and Xuan Sun [1]

[1] School of Information and Management, Beijing Information Science & Technology University, Beijing 100192, China; 20051452@bistu.edu.cn (W.J.); sunxuan@bistu.edu.cn (X.S.)
[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; hahayuswag@bupt.cn
* Correspondence: 20192329@bistu.edu.cn

Abstract: The emergence of integrated positioning, communication, and sensing technologies has paved the way for a surge in connected and autonomous vehicles. The control system has been successful in reliable and fast transmission. However, practical applications face security risks, especially data tampering and spoofing attacks. To improve the resilience of the system against potential attacks, we attempt to leverage a generative adversarial network learning-assisted authentication framework (GAF). In addition to proposing a new method for validating vehicles, we also introduce a new architectural innovation in the generator–discriminator pair to achieve improved results. The generator sub-network is constructed using an advanced convolutional neural network, whereas the discriminator is designed to leverage global and local information to determine whether a signal is real or fake. On this basis, we propose a signal enhancement-based authentication method, a deep convolutional generative adversarial network (DCGAN). Experimental results using the National Institute of Standards and Technology (NIST) dataset show that the proposed method is effective in denoising and improving the detection performance.

Keywords: connected and autonomous vehicles; wireless communication; artificial intelligence; privacy security protection; generative adversarial networks

check for updates

Citation: Qiu, X.; Yu, J.; Jiang, W.; Sun, X. Intelligent Security Authentication for Connected and Autonomous Vehicles: Attacks and Defenses. *Electronics* **2024**, *13*, 1577. https://doi.org/10.3390/electronics13081577

Academic Editor: Daniel Gutiérrez Reina

Received: 8 March 2024
Revised: 8 April 2024
Accepted: 18 April 2024
Published: 20 April 2024

1. Introduction

Integrated positioning, communication, and sensing (IPCS) technologieshave garnered significant interest from both academia and industry for various applications such as connected and autonomous vehicles [1–3]. The communication methods in the control systems of connected and autonomous vehicles are essential to fulfill the requirements of these exciting applications, including high data rates, exceptional reliability, and intelligent solutions [4–6]. The movement of target vehicles in a wireless transmission signal coverage area leads to changes in signal reflection characteristics. These changes affect the properties of the received signal like the channel impulse response (CIR), carrier frequency offset (CFO), received signal strength index (RSSI), and angle of arrival (AoA). Then, 5G wireless networks are advantageous for sensing tasks due to their widespread deployment [7,8]. The proposed IPCS solution analyzes and processes sensed information from the control system. This extensive information needs access to the Vehicle-to-Everything (V2X) network through collaboration with other vehicles. Artificial intelligence disciplines like deep learning (DL) train models to provide intelligent applications by deriving insights from data collected by autonomous driving devices [9,10].

1.1. Prior Art and Motivation

Figure 1 illustrates a connected automated driving scenario using the IPCS system, where 5G signals provide positioning, communication, and sensing functions. The IPCS system serves as an intelligent platform with numerous connected and autonomous vehicles [11]. However, these devices and terminals in autonomous driving are vulnerable to malicious attacks exploiting security weaknesses in the wireless network [12–14]. Attackers can send harmful data to the control system, jeopardizing legitimate operations and vehicle communication. For instance, unauthorized devices can execute clone node attacks in unsupervised autonomous driving networks. The attacker seizes control of a vehicle, obtains its ID, key, and confidential data, and then deploys numerous cloned vehicles in the communication environment, posing security risks by gathering sensitive information. As the control center may struggle to differentiate these fraudulent vehicles, the compromised IPCS network could lead to severe safety incidents and financial losses.

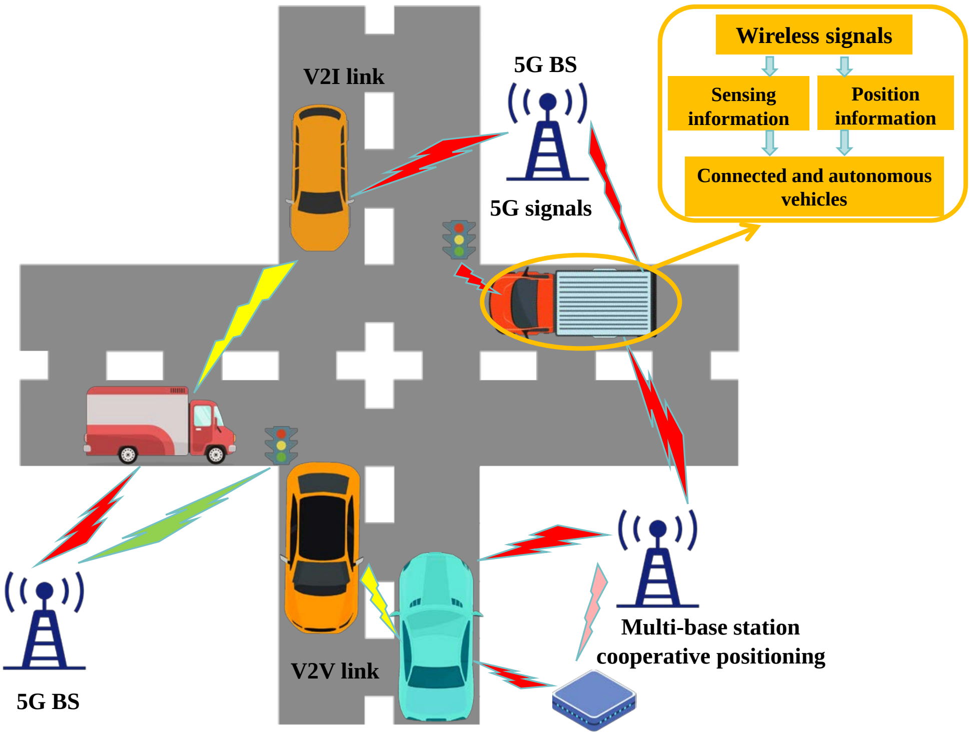

Figure 1. A scenario for autonomous driving application.

Traditional cryptographic methods suffer from delays and computational complexity unsuitable for connected and autonomous vehicles [15,16]. Given the dynamic wireless communication environment, ensuring the security authentication of autonomous vehicles is crucial. In [17,18], an identity authentication system using unique spatial and temporal fingerprints was developed. Although these systems offer benefits like quick and efficient authentication, models trained on real-world data may lack robustness. Furthermore, to enhance the detection performance, an adaptive trust management strategy was proposed in [18]. The adjustment algorithm is based on the difference between previous and new estimates. In control systems for connected and autonomous vehicles, channel attributes can change dynamically over time, making it challenging to predict time-varying characteristics.

Deep learning has proven to be effective in creating more precise models. Many research studies have focused on identity authentication using learning models, such as the Gaussian mixture model [19,20], long short-term memory [21], reinforcement learning [22], transfer learning [23], and convolutional neural networks. Moreover, an extreme machine learning-based method was proposed in [24], and a pseudo-adversary model was assumed to generate training data. A group of classifiers is used for security authentication between authorized and unauthorized devices in the IPCS network [25,26]. In [27,28], different learning-assisted authentication algorithms based on multiple features were used to offer various levels of authorization. The algorithms in [29] were designed to meet diverse security needs by incorporating a set of appropriate features. However, many studies on model learning frameworks have concentrated on combining multi-dimensional features [30]. Learning models for device certification offer improved security compared to statistical methods, but the quality of training data impacts their performance [31,32]. Another motivation for using machine learning is to handle large volumes of intricate data. The intricate IPCS network results in a high false alarm rate for security authentication [33]. Some research has utilized a linear first-order autoregression approach to model wireless channels [34,35]. Although they have obvious advantages including low overhead and low latency, most one-time authentication schemes are static in time [36]. Some efforts have been made to predict estimates for selecting channel attributes. An authenticator is used to monitor and save extracted features [37,38]. In previous research [39,40], a data-adaptive matrix in a deep learning structure was suggested for tracking changing attributes over time. This creates an adaptive authenticator that can choose smart devices automatically. However, security schemes may suffer from errors in channel estimation and noise interference, impacting their performance. Authentication accuracy may decrease significantly if channel estimation errors and Gaussian noise are included during classifier training [41,42]. Enhancing immunity against environmental noise is crucial for security authentication in connected and autonomous vehicle control systems. Signal enhancement technology is essential in complex IPCS networks to enhance security effectiveness.

1.2. Novelty and Contribution

To overcome these challenges, using adversarial networks for signal enhancement is helpful for improving communication security in IPCS networks. We aimed to leverage the generative modeling capabilities of adversarial networks. Generative adversarial network (GAN) algorithms have been successful in visual tasks such as image generation and image super-resolution [43]. The generator acts as a mapping function to transform the input channel estimation into an enhanced signal. However, traditional GAN approaches are not stable to train, and doing so may introduce artifacts [44,45]. To address this issue, we introduced a new generator–discriminator pair to assist the proposed network. The generative adversarial network learning-assisted authentication framework (GAF) provides a practical security approach without the use of any additional preprocessing. Incorporating noisy wireless signals enhances the strength of the generator and discriminator, improving the denoising effect of the GAF model. In summary, the GAF algorithm enhances signals and authentication decisions in IPCS networks. The contributions of this paper are outlined as follows:

- An authentication framework using generative adversarial networks is introduced for IPCS systems, featuring a verification mechanism to identify potential pseudo-attack devices.
- An improved signal enhancement network is constructed using an advanced convolutional neural network, which is designed for denoising tasks.
- Extensive experiments were conducted on publicly available datasets to demonstrate the effectiveness of the proposed method in terms of denoising quality and authentication performance.
- Lastly, the effectiveness of the proposed method was demonstrated on the National Institute of Standards and Technology (NIST) dataset [46]. The superiority of the GAF scheme over existing methods was demonstrated.

1.3. Organization

The remainder of this paper is organized as follows. Section 2 elaborates on the system model, with a focus on the attack model. We present the design of the GAF framework for the IPCS system in Section 3. This is followed by presenting the experimental verification in Section 4. Finally, Section 5 concludes this work.

2. Attack Model

Figure 1 illustrates the IPCS system, comprising N_D independent vehicle devices, 5G base stations, and collaborative intelligent transportation infrastructures. Each IPCS device includes a wireless intelligent sensor for transmitting and receiving radio signals, used for positioning, sensing, and communication. In each IPCS network, there is a control center, and autonomous vehicles handle local data collection and upload tasks. Each vehicle device is linked to an authentication node, and the central system must identify all connected devices to facilitate communication and data updates with local nodes. In Figure 1, we consider a potential spoofing attack scenario. The security performance of the control system depends on the trusted identity of the connected vehicle. However, several factors affect the control system in real-world wireless environments, which may stem from connected vehicles involved in authentication or external spoofing attack sources. These factors, through eavesdropping and disguising legitimate vehicles, prevent the authentication model from correctly fulfilling the purpose of the classification and identification tasks [24,40].

For connected and autonomous vehicles, the wireless signal is affected by the dynamic activity of the vehicle, resulting in multipath signal superposition, and these dynamic changes can be used for identity authentication. The dynamic wireless communication link between the transmitter and control system can be described using channel state information. However, in some cases, there may be malicious or damaged vehicles, especially when the number of participants increases, and potentially malicious and damaged vehicles are more likely to be present. These connected and autonomous cars generate false labels or insert false data, affecting the authentication model. In taking the neural network algorithm [47] as a reference, its weight update can be expressed as

$$W_{global} = \sum_{i=1}^{I} \alpha_i w_{i,local} \tag{1}$$

where α_i is the proportion of the local training set of vehicle i to the total dataset, and w_i denotes the weight of the unattacked vehicle. The effect of the fake dataset on the authentication model mainly depends on the number of malicious vehicles k involved in the aggregation and the proportion of the respective amount of tampered data α_i. According to Equation (1), when the amount of tampered data α_i is small, the spoofing attack has the least impact on the authentication model, but with an increase in the number of pseudo-attack vehicles, the pollution degree of the authentication model will be greatly increased. Therefore, security authentication is essential for IPCS systems.

3. Materials and Methods

3.1. Overall Design

Figure 2 shows the structure of the GAF method. The proposed network consists of two sub-networks serving different purposes. The generator sub-network is shown in the top part in Figure 2. Its main goal is to synthesize a denoised signal. The discriminator sub-network shown in the bottom part in Figure 2 serves to distinguish “fake” channel information from the “real” channel information. The GAF algorithm involves inputting NIST data samples into the generator, which produces pseudo signals resembling the original signal. The discriminator then compares the generated signal with the real wireless signal and provides feedback to the generator. Through this feedback loop, the generator adjusts its network structure and parameters to enhance the signal. The GAF scheme uses the model output to identify devices with different identities, completing identity verification tasks and detecting potential attacks.

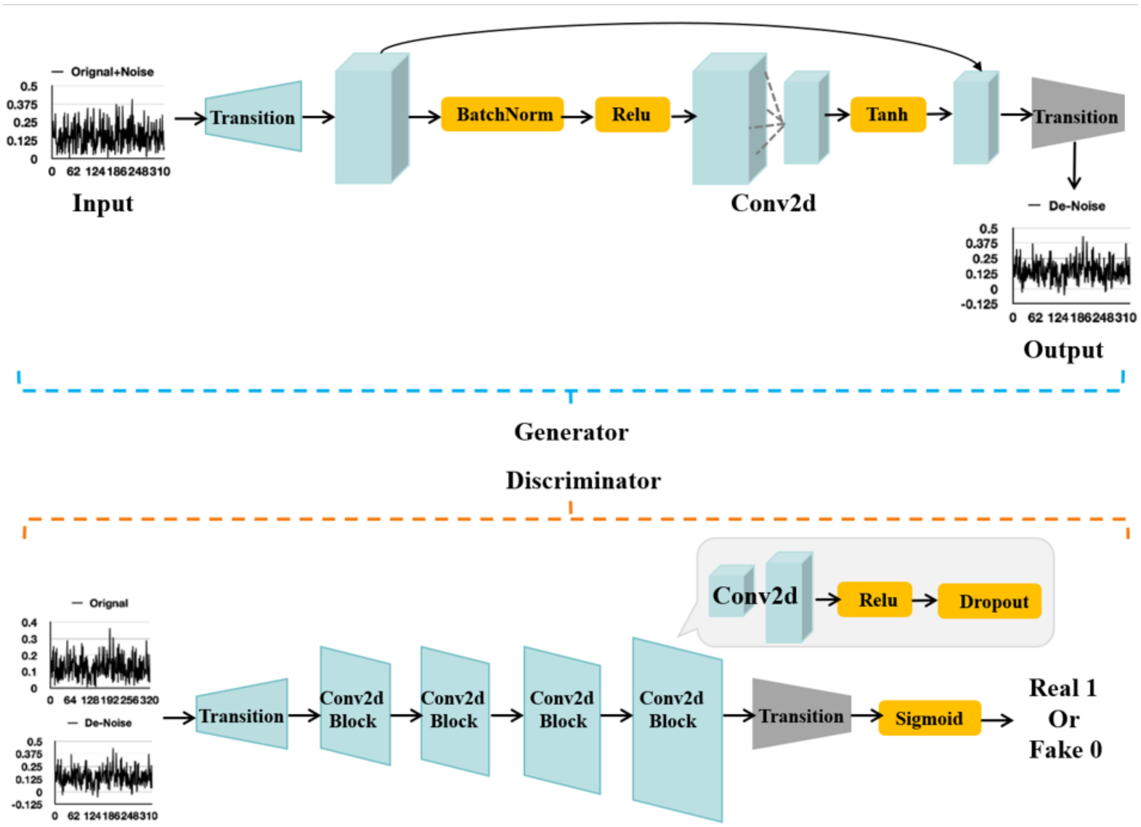

Figure 2. The structure of proposed GAF algorithm.

3.2. *Internal Structure of Neural Network Based on NRCT-4CRD*

In current neural network structures, both the maximum pooling layer and the uniform pooling layer present distinct issues [37]. For instance, in enhancing wireless signal denoising, the maximum pooling layer filters the signal to retain valuable features but may lose most signal details irreversibly. On the other hand, the uniform pooling layer can lead to the loss of signal differences during processing, potentially causing distortion in signal restoration and reducing the quality of wireless signals [40,48].

To address these challenges, it is essential to preserve various features and key points in wireless signals. The proposed deep convolutional structure reduces the number of pooling layers in the neural network model and maintains performance through a new hierarchical combination structure. We introduced two special constructions. A generator sub-network consisting of a normalization module, ReLU activation, a convolutional layer, and Tanh activation is defined as an NRCT. A discriminator sub-network consisting of four convolutional layers, ReLU activation, and dropout layers is defined as 4CRD. The functionality of the pooling layer is replaced by the convolutional layer, reducing performance loss. This substitution is actually achieved through a convolutional pooling operation, where each input signal in the receptive field of each unit in the convolutional layer receives all the information from the previous neural unit, and the weight of each input feature signal is trained through the learning process, resulting in a more effective feature filtering scheme compared to the pooling layer. The difference between convolutional pooling layers and general convolutional layers is that the dimensions of the output features and input features are consistent. The internal structure of a neural network based on the NRCT-4CRD structure alleviates the impact of pooling layers on wireless signals in convolutional neural networks.

3.3. Improved DCGAN-Based Signal Enhancement Process

The signal enhancement algorithm based on traditional generative adversarial networks has problems such as unstable training process and the easy collapse of generation modes. In order to improve the security performance and stability of identity authentication schemes, a deep convolutional (DC) network based on the NRCT-4CRD structure is introduced into the GAF algorithm. Compared with traditional networks, the NRCT-4CRD structure has the advantage of higher information utilization and improves the denoising effect of channel estimation values.

Figure 3 shows the process of signal enhancement technology based on an improved DC-based generative adversarial network algorithm (DCGAN). The reconstructed NRCT-4CRD structure can be used to enhance the feature dimension of channel estimation collected in real wireless scenes, so as to ensure that the GAN can obtain the signal feature information well. As shown in Figure 3, the improved DCGAN algorithm consists of two stages: training and enhancement. G is the abbreviation for "Generator", indicating a signal generation network. D is the abbreviation for "Discriminator", representing a signal discriminator network. Note that the plus sign "+" is not a mathematical addition. In the GAF scheme, the plus sign "+" indicates a connection. Consistent with traditional adversarial generative networks, the training process of the improved DCGAN algorithm greatly reduces the losses of the generator and discriminator, thereby achieving accurate updates of model parameters. After the model training is completed, the improved DCGAN algorithm completes the signal enhancement process based on the generator (i.e., enhancement stage). For the discriminator network, the mathematical expression of the objective function is as follows:

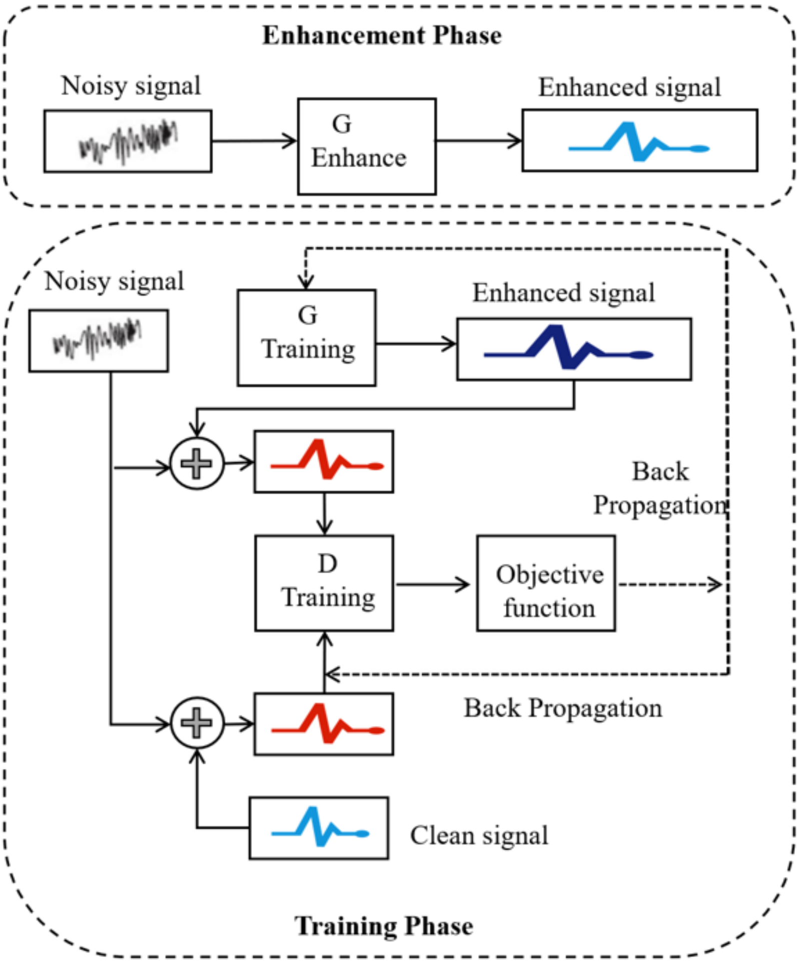

Figure 3. The process of improved CNN-GAN-based signal enhancement.

$$minV(D) = \frac{1}{2}E_{x,x_c - Pdata(x,x_c)}[(D(x,x_c)-1)^2] + \frac{1}{2}E_{z-p_z(z),x_c-Pdata(x_c)}[D(G(z,x_c),x_c)^2] \tag{2}$$

For the generator network, the mathematical expression of the objective function can be denoted as

$$\min V(G) = \frac{1}{2}E_{z-p_z(z),x_c\sim Pdata(x_c)}[(D(G(z,x_c),x_c)-1)^2] + \lambda\|G(z,x_c)-x\|_1 \tag{3}$$

where x indicates the clean wireless signal, z represents noise, x_c denotes a noisy wireless signal, λ is a hyperparameter that controls the weight of the generated loss, E stands for expectation, and $\|.\|_1$represents the 1-norm.

4. Numerical Results and Discussion

4.1. Experiment Setup

As shown in Figure 4, a typical multi-acre transmission assembly factory of the automotive industry was selected for radio frequency propagation measurements. To create a security authentication dataset and simulate malicious attack scenarios, we used the channel information dataset provided by the NIST in the automotive factory [46]. The floor size of the automotive factory is more than 167.4 m × 122.8 m. The ceiling is about 12 m high. In this scenario, we assume that the attacker captures and impersonates a legitimate vehicle, deploying multiple cloned nodes in different locations. The receiver in the automotive industry aims to identify malicious nodes. The parameter configuration of the channel measurement system includes the center frequency, antenna, and power.

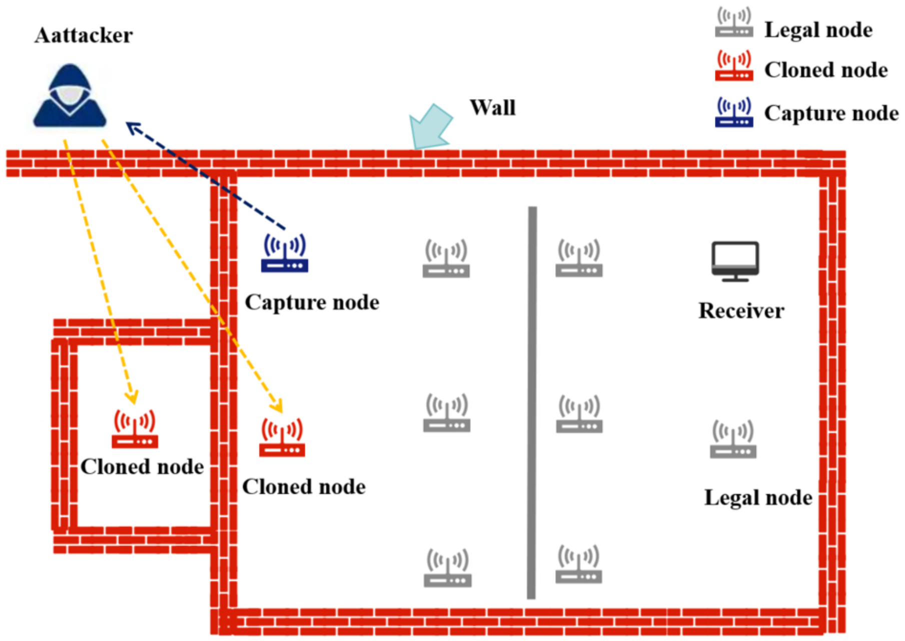

Figure 4. The layout of NIST data collection experimental scene.

4.2. Parameter Setting

To evaluate the performance of our proposed framework in enhancing authentication, we applied it to the NIST dataset [46], which is constructed based on a real industrial wireless environment, including dynamic and static scenarios. The parameters for generating the dataset that used in this work are presented in Table 1.

Table 1. The details of the experimental dataset.

Parameters	Assignment
Size of the automotive factory	400 m × 400 m
Frequency	5.4 GHz
Location	aa plant day 2 at automotive assembly plant
Path loss exponent	3.6
Delay	644.4 ns
Delay spread	177.4 ns
K-factor	4.7 dB
TX antenna gain	3.6
RX antenna gain	−3.5
PN oversample factor	4.0
Sample rate	80 MHz

We divided the experiment data into two parts: 30,000 samples for training and 3000 samples for testing. Since the dataset contains a large number of characteristic parameters, such as position, angle, gain, etc., we chose channel state information as the input data of the security model in order to facilitate model training. In this section, Run1-r-one-005.csv [46] was used as a training set, and Run1-r-one-006.csv [46] was used as a test set. The main simulation parameters for training and testing of the proposed framework are listed in Table 2.

Table 2. Parameters in the proposed approach for the training and testing.

Parameters	Assignment
Dataset scenarios	6
Total number of training data samples	30,000
Total number of test data samples	3000
Epoch	1000
Batch size	16
Kernel size	1× 322
Learning rate	1.00×10^{-4}
Optimizer	Adam
Generator layers	3
Discriminator layers	6

To describe the enhanced performance of the GAF algorithm, we used several performance metrics to describe the model. The R2-score represents the coefficient of determination, and the higher the R2-score, the higher the accuracy of the prediction. In addition, the total sum of squares (TSS), explained as the sum of squares (ESS), and residual sum of squares (RSS) were used, and were calculated as follows:

$$TSS = \sum_{i=1}^{n} (y_i - \bar{y})^2 \tag{4}$$

$$ESS = \sum_{i=1}^{n} (\hat{y}_i - \bar{y}_i)^2 \tag{5}$$

$$RSS = \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \tag{6}$$

where y_i represents real value, $\bar{y}_i$ denotes the average value, and $\hat{y}_i$ is an estimate of the network output.

In addition, a segmented signal-to-noise ratio (SNRseg) is a wireless signal enhancement evaluation index based on the time domain, which is the average of all wireless frame signal-to-noise ratios used to measure the early degree of the overall system. The

Quality Perception Evaluation (PESQ) is a complex evaluation index, and is one of the most common indicators in signal enhancement techniques, which has been standardized for evaluating the difference between a reference signal and a measured signal. Short-term objective comprehension (STOI) is an evaluation index for the correlation between the reference signal and the measured signal in a wireless signal estimate.

4.3. Denoising Performance

We first evaluated the performance of the GAF under the background of output data visualization, and the visualized images clearly displayed the estimated values of different types of wireless channels. Figure 5 shows two different representations of three different signals (i.e., original wireless channel estimation, original wireless channel estimation with added noise, and denoised wireless channel estimation). The three wireless data line graphs in the left image are very similar and difficult to classify directly with the naked eye. However, the data for image conversion is easily distinguishable, and there are significant differences in the details of the images. Figure 5 shows that the amplitude variation range of noisy waveforms is larger than that of clean signals, with more blurs and redundant details, which is not conducive to the later training of learning models and may lead to overfitting problems. Therefore, the denoising enhancement of channel estimation datasets is essential for the training of later models.

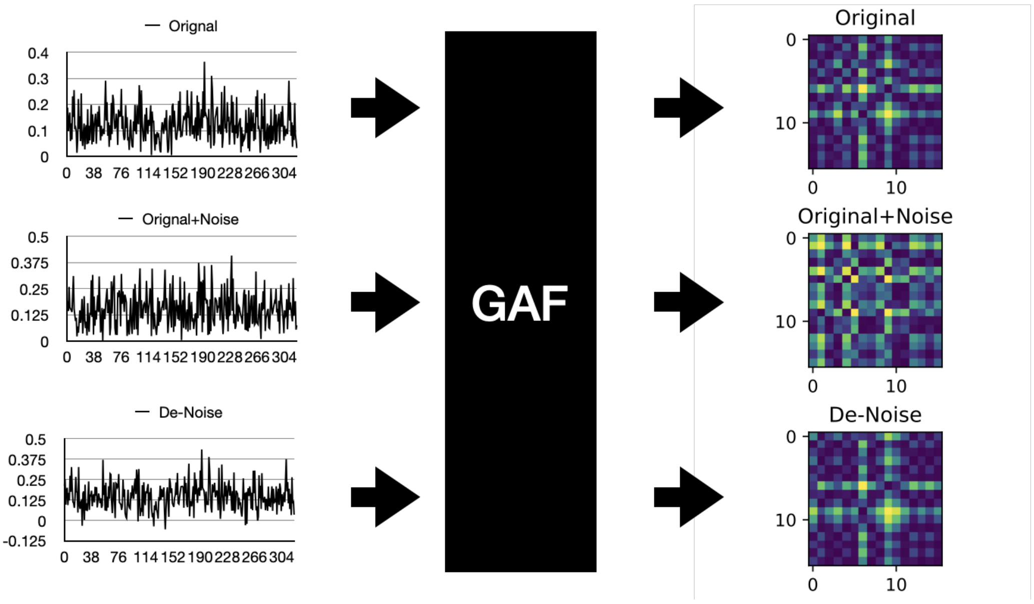

Figure 5. Signal denoising performance based on the proposed GAF algorithm.

Figure 5 is a schematic of the signal denoising performance based on the GAF algorithm. Figure 5 shows that the GAF algorithm can effectively transform the input noisy channel estimation into a denoised signal. Figure 5 shows the estimated signal sequence in the real wireless industrial network environment, that is, the first frame signal. This frame signal, after 256 samplings per frame, is observed in the formation of the signal style diagram. In the experimental verification, the model input was 20 frames each time. Figure 5 shows a schematic of the noisy signal. On the basis of the original wireless channel information signal, the signal-to-noise ratio was changed to 10 dB by artificially adding Gaussian white noise. It can be seen that the noisy signal reduces the received signal strength value of the signal as a whole, and the amplitude of the wireless channel information is reduced because of the cover of noise, which greatly increases the difficulty of identity authentication. By introducing a DCGAN-based network, the GAF model reduces the loss rate of useful wireless signals as much as possible, thus retaining more high-frequency feature components, and further improving the perception quality and intelligibility of enhanced wireless. Therefore, the wireless signal denoising and identity authentication joint optimization scheme can achieve a better signal enhancement effect.

Figure 6 shows the output result of the signal enhancement module of the GAF model. Figure 6 shows the signal enhancement effect of the GAF network noise reduction model after 10, 210, and 560 runs of model training, respectively. Figure 6 shows that as the number of training iterations increases, the denoised image becomes closer and closer to the original image. The GAF is used as a signal enhancer. The latent variables are input into the GAF generator and mapped to the wireless signal according to certain rules, so the latent variables are characteristics of the wireless signal. These rules can be mined through GAF adversarial training. The results indicate that the CNN-GAN model can effectively eliminate the noise interference in the wireless channel estimation samples. The enhancement effect means that the generated signal is not a simple copy of the existing data. In summary, the denoising algorithm based on the CNN-GAN model can reduce the interference generated in the process of wireless channel information estimation, and it is conducive to the training of the authentication model.

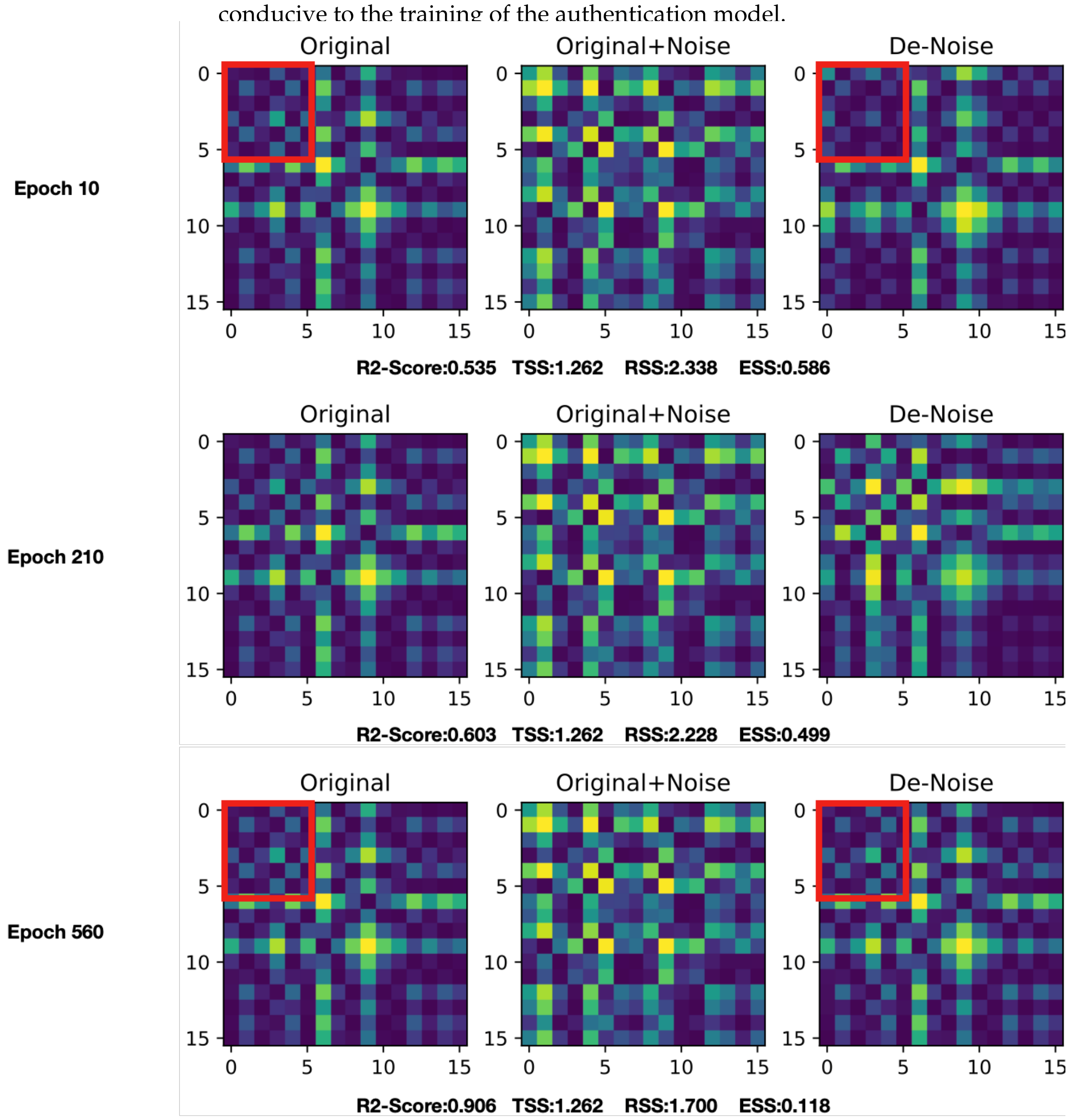

Figure 6. Denoising performance over epochs.

4.4. Superiority Evaluation

Table 3 provides a performance comparison of the MMSE-SPZC [49], SEGAN [49], and GAF algorithms. The main evaluation performance indicators include the average PESQ value, average STOI value, and SNRseg value. Table 3 shows that compared with MMSE-SPZC, the GAF model performs well in terms of the PESQ and STOI values under various conditions. Compared with SEGAN, except under a −2 dB to −3 dB environment, the GAF model performs slightly worse on STOI. Under other signal-to-noise ratio conditions, the GAF algorithm performs better on the corresponding index values. Compared with directly collected noisy wireless signal data, the GAF algorithm improved the PESQ value by an average of about 20% and the STOI value by an average of nearly 10%. Further analysis shows that compared with the traditional MMSE-SPZC scheme, the overall average PESQ value of the GAF algorithm has increased by about 4%, and the average STOI value has increased by about 8%. In summary, the GAF algorithm is superior to the MMSE-SPZC algorithm and SEGAN algorithm in almost all aspects. In addition, in observing Table 3, the GAF algorithm can effectively reduce the noise when the signal-to-noise ratio is −2.5 dB, thus improving the quality of the wireless signal and the classification performance in the later stage. This section further validates the signal enhancement problem through this objective indicator.

Table 3. Performance comparison with different algorithms.

Algorithm	Parameters	−2.5 dB	2.5 dB	7.5 dB	12.5 dB	17.5 dB
MMSE-SPZC	PESQ	1.0	1.5	1.9	2.6	4.7
	STOI	0.13	0.15	0.17	0.18	0.19
	SNRseg	−5.4	−4.4	0.5	4.6	7.8
SEGAN	PESQ	2.0	2.6	2.5	3.7	4.1
	STOI	0.15	0.18	0.18	0.19	0.19
	SNRseg	0.3	1.4	4.8	7.5	11.0
GAF	PESQ	2.0	2.1	2.8	4.1	4.3
	STOI	0.14	0.18	0.19	0.19	0.22
	SNRseg	1.3	1.5	1.7	1.9	2.7

4.5. Accuracy Evaluation

Figure 7 shows the convergence of the GAF algorithm. The results indicate that the R2-score, TSS, RSS, and ESS functions of the GAF algorithm converge with increasing iteration times. With the increase in training data, although the R2-score, TSS, RSS, and ESS function values fluctuate, they remain stable after 520 iterations. For example, after 520 iterations, the RSS value is fixed at 1.9, the TSS value is 1.9, the R2-score is 0.99, and the ESS value is 0. The results indicate that the generated GAF model can effectively achieve the expected results. The proposed GAF system incorporates a DCGAN architecture, augmented by convolutional pooling operations, to enhance the feature representation of wireless channel estimates. By utilizing the NRCT-4CRD-based internal structure as both the generator and discriminator in the adversarial generation network, we present an effective data enhancement scheme through adversarial training using clean signals and noisy signals to diminish noise in estimated values. Figure 7 shows that the GAF method effectively improves the detection and recognition rates of the model, thus providing an efficient approach for enhancing security capabilities.

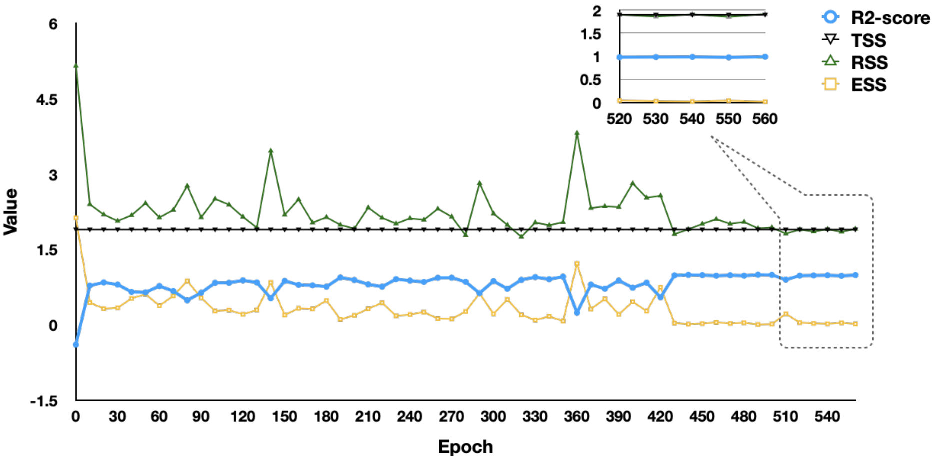

Figure 7. The convergence of the GAF algorithm.

To further evaluate the proposed GAF algorithm and provide an intuitive understanding of its feasibility, we used RSS metrics. Figure 8 shows that after 500 epochs, the RSS value is below 2, indicating that the GAF algorithm has achieved the correct accuracy. Specifically, as the signal-to-noise ratio increases, the RSS value gradually decreases and tends to stabilize. Meanwhile, as the number of iterations increases, the RSS value gradually decreases and tends to 2, remaining unchanged. We further discuss the GAF method, especially the NRCT-4CRD-based internal structure, which indeed demonstrated potential reasons for advanced results. As mentioned in Section 1, signal enhancement in wireless estimation is an important factor. The performance of the GAF model depends on the quality of channel estimation data. Adversarial learning models may perform better and be more powerful in high-complexity situations. In addition, when the signal-to-noise ratio is low, the GAF method may achieve better results than traditional authentication methods. These results demonstrate the advantage of the GAF model in improving task security by enhancing signals.

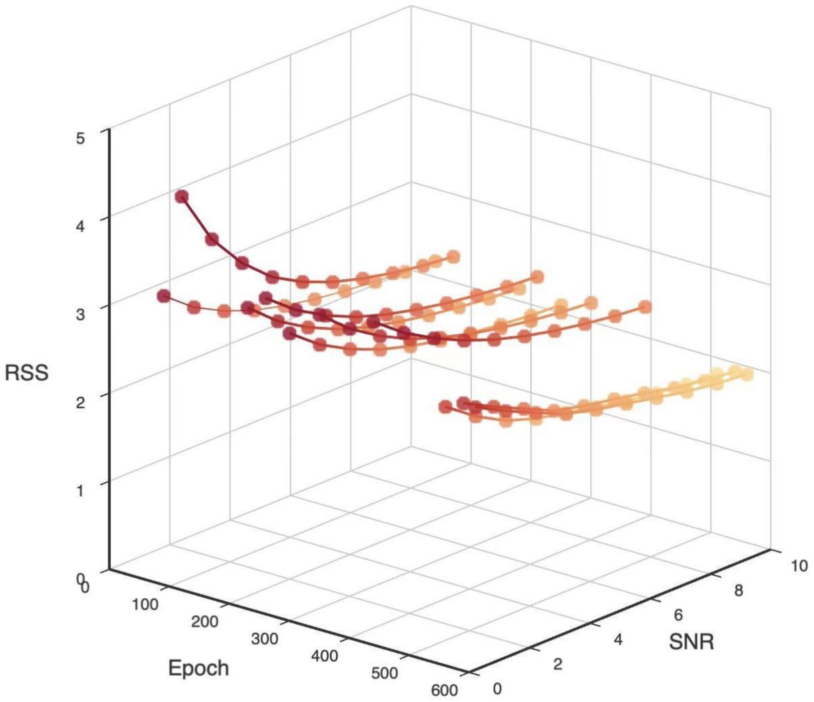

Figure 8. RSS Performance of the proposed GAF algorithm.

As shown in Figure 9, the number of epochs and signal-to-noise ratio impact the R2-score. The R2-score increases rapidly with an increasing number of iterations and signal-to-noise ratio. In order to observe the accuracy of the GAF model in identifying legitimate sending devices in the later stage, this experiment specially processed legitimate signals and simulated the recognition process of devices in different noise environments, with a signal-to-noise ratio between 0 dB and 10 dB. To compare the accuracy of the recognition results, we calculated the R2-score for each step of prediction. As can be seen from Figure 9, with the increase in the signal-to-noise ratio, the R2-score value reached above 0.9. This means that the signals generated by the network are not simple copies of the existing channel information data. The identity authentication scheme based on the GAF algorithm can effectively eliminate redundant information in wireless signals, which is beneficial for the GAF training process. From the results, the use of GAF can effectively reduce the impact of signal noise on the authentication results and improve the quality of wireless signals. The GAF network can effectively improve the accuracy of identity authentication. Even under the condition of high artificial noise interference, it still has a high detection and recognition rate.

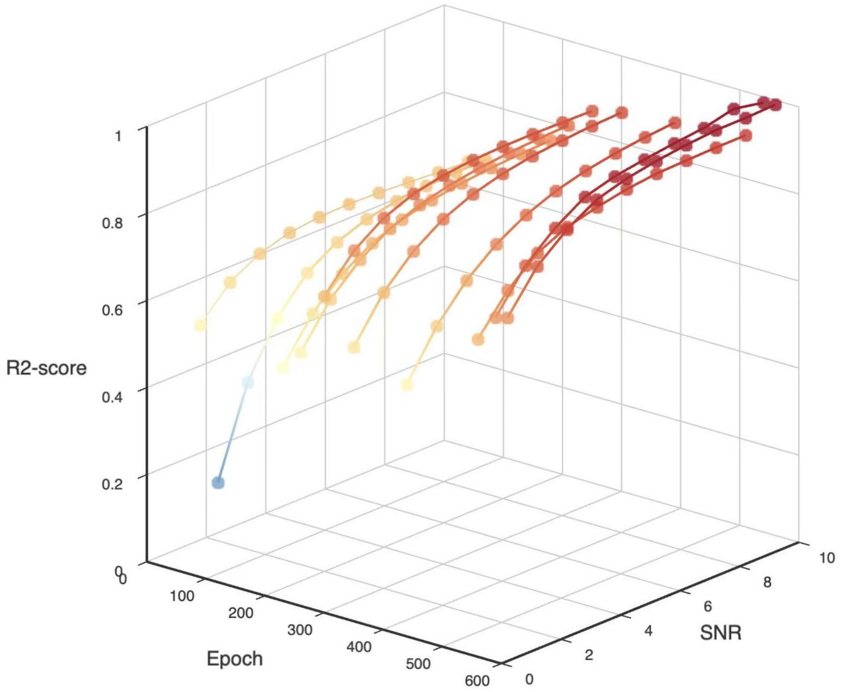

Figure 9. R2-score performance of the proposed GAF algorithm.

We also analyzed the ESS performance of the GAF algorithm. As shown in Figure 10, the lowest ESS value is close to 0. This means that the performance of signal enhancement and recognition authentication remains stable under a high number of epochs and signal-to-noise ratio, and this indicates that the GAF algorithm is robust in IPCS systems. In summary, the performance of the GAF algorithm proposed in this paper was experimentally verified. The proposed network model effectively reduces the interference noise in the channel estimation and plays a supporting role in the construction of the later classification model. To address the movement of connected and autonomous vehicles, utilizing 5G location-aware communication could enhance security technology; 5G networks offer precise location data, aiding in control system design and optimization. Distinguishing transmitter positions can help reduce active attack risks by effectively identifying users through location information. Moreover, 5G technology features like beamforming in large-scale MIMO and high directionality in millimeter waves support position-aware communication. Integrating 5G location data while preserving personal privacy and developing efficient identity authentication solutions is a crucial research focus.

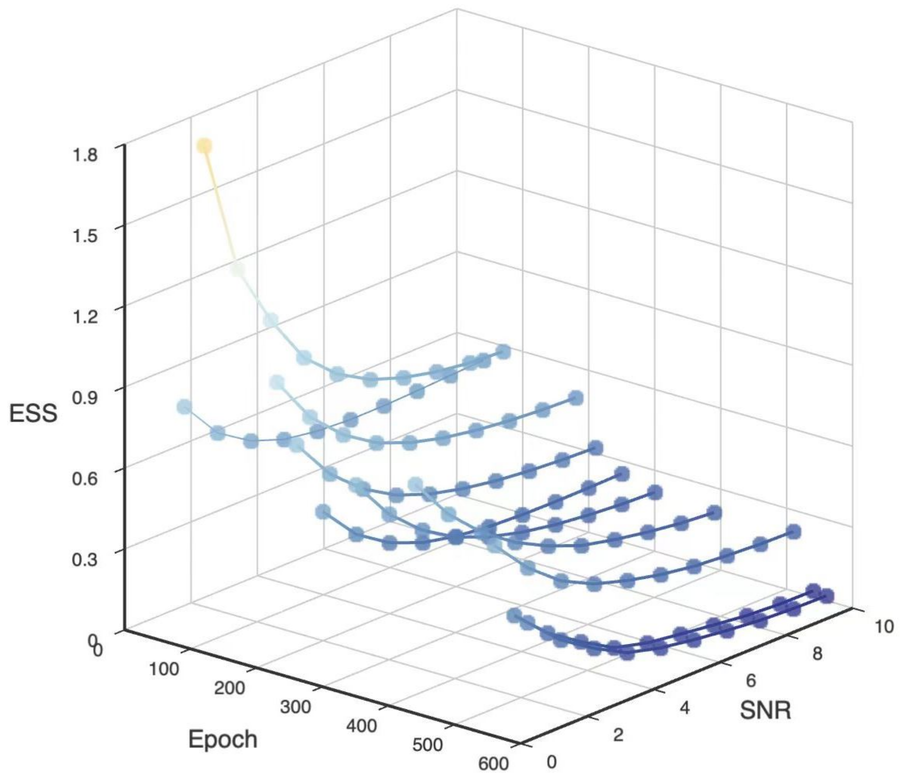

Figure 10. ESS performance of the proposed GAF algorithm.

5. Conclusions and Future Work

In this paper, we propose a highly secure and robust certification framework designed for connected and autonomous vehicles. In order to enhance the control system's resistance to phishing attacks, a GAF method for authenticating identities is proposed. Additionally, we propose an improved convolutional neural network design to enhance wireless channel estimation representation through convolutional pooling operations. By employing enhanced NRCT-4CRD-based internal structures as generators and discriminators in adversarial generation networks, we propose an efficient DCGAN-based signal enhancement approach to minimize noise interference during training. The experimental results demonstrate that the GAF algorithm effectively reduces noise in channel estimation data, enhances the model's detection and recognition rates, and offers a reliable method for authenticating device identities in connected and autonomous vehicles.

Author Contributions: Conceptualization, X.Q. and J.Y.; methodology, X.Q. and J.Y.; software, X.Q. and J.Y.; validation, X.Q. and J.Y.; formal analysis, X.Q.; investigation, X.Q.; resources, X.Q. and J.Y.; data curation, X.Q. and J.Y.; writing—original draft preparation, X.Q.; writing—review and editing, X.Q., J.Y., W.J. and X.S.; visualization, X.Q. and J.Y.; supervision, W.J. and X.S.; project administration, X.Q.; funding acquisition, X.Q. and W.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key R&D Program of China under Grant 2022YFB2703000 and in part by the R&D Program of Beijing Municipal Education Commission under Grant KM202211232012.

Data Availability Statement: NIST datasets are accessed on 1 January 2024 and available at http://doi.org/10.18434/T44S3N.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IPCS	Integrated positioning, communication, and sensing;
CIR	Channel impulse response;
CFO	Carrier frequency offset;
RSSI	Received signal strength index;
AoA	Angle of arrival;
DL	Deep learning;
GAF	Generative adversarial network learning-assisted authentication framework;
NIST	National Institute of Standards and Technology;
DC	Deep convolutional;
DCGAN	DC-based generative adversarial network.

References

1. Fang, H.; Wang, X.; Tomasin, S.; Al-Dhahir, N. Lightweight group authentication for decentralized edge collaboration. *IEEE Commun. Mag.* **2023**, *60*, 124–129. [CrossRef]
2. Song, F.; Li, L.; You, I.; Yu, S.; Zhang, H. Optimizing High-Speed Mobile Networks with Smart Collaborative Theory. *IEEE Wirel. Commun.* **2022**, *29*, 48–54. [CrossRef]
3. Im, J.H.; Jeon, S.Y.; Lee, M.K. Practical privacy-preserving face authentication for smartphones secure against malicious clients. *IEEE Trans. Inf. Forensics Secur.* **2023**, *15*, 2386–2401. [CrossRef]
4. Li, Z.; Zhou, Y.; Wu, D.; Tang, T.; Wang, R. Fairness-Aware Federated Learning with Unreliable Links in Resource-Constrained Internet of Things. *IEEE Internet Things J.* **2021**, *9*, 17359–17371. [CrossRef]
5. Li, Z.; Zhu, N.; Wu, D.; Wang, H.; Wang, R. Energy-Efficient Mobile Edge Computing Under Delay Constraints. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 776–786. [CrossRef]
6. Zhong, A.; Li, Z.; Wu, D.; Tang, T.; Wang, R. Stochastic Peak Age of Information Guarantee for Cooperative Sensing in Internet of Everything. *IEEE Internet Things J.* **2023**, *10*, 15186–15196. [CrossRef]
7. Illi, E.; Qaraqe, M.; Bouanani, F.E. A Novel Hybrid Physical-Layer Authentication Scheme for Multiuser Wireless Communication Systems. *IEEE Internet Things J.* **2023**, *10*, 22591–22610. [CrossRef]
8. Wang, Y.; Gao, Z.; Zheng, D.; Chen, S.; Gunduz, D.; Poor, H.V. Transformer-Empowered 6G Intelligent Networks: From Massive MIMO Processing to Semantic Communication. *IEEE Wirel. Commun.* **2023**, *30*, 127–135. [CrossRef]
9. Mahmood, N.; Berardinelli, G.; Khatib, E.J.; Hashemi, R.; Lima, C.; Latva-aho, M. A Functional Architecture for 6G Special Purpose Industrial IoT Networks. *IEEE Trans. Ind. Inform.* **2022**, *19*, 2530–2540. [CrossRef]
10. Li, Z.; Li, F.; Tang, T.; Zhang, H.; Yang, J. Video caching and scheduling with edge cooperation. *Digit. Commun. Netw.* **2022**, 2352–8648. [CrossRef]
11. Cao, B.; Zhang, L.; Li, Y.; Feng, D.; Cao, W. Intelligent Offloading in Multi-Access Edge Computing: A State-of-the-Art Review and Framework. *IEEE Commun. Mag.* **2019**, *57*, 56–62. [CrossRef]
12. He, W.; Xu, W.; Ge, X.; Han, Q.-L.; Du, W.; Qian, F. Secure Control of Multiagent Systems Against Malicious Attacks: A Brief Survey. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3595–3608. [CrossRef]
13. Zografopoulos, I.; Konstantinou, C. Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids. *IEEE Trans. Ind. Inform.* **2022**, *18*, 5815–5826. [CrossRef]
14. Gai, K.; Ding, Y.; Wang, A.; Zhu, L.; Choo, K.K.R.; Zhang, Q.; Wang, Z. Attacking the Edge-of-Things: A Physical Attack Perspective. *IEEE Internet Things J.* **2022**, *9*, 5240–5253. [CrossRef]
15. Song, F.; Li, L.; You, I.; Zhang, H. Enabling Heterogeneous Deterministic Networks with Smart Collaborative Theory. *IEEE Netw.* **2021**, *35*, 64–71. [CrossRef]
16. Xie, N.; Sha, M.; Hu, T.; Tan, H. Multi-User Physical-Layer Authentication and Classification. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 6171–6184. [CrossRef]
17. Xu, Y.; Zhang, J.; Zhang, Q.; Zhang, P.; Huang, L.; Xie, N.; Lu, J. Physical Layer Authentication in Spatial Modulation. *IEEE Trans. Commun.* **2023**, *71*, 2947–2962. [CrossRef]
18. Fang, H.; Wang, X.; Hanzo, L. Adaptive Trust Management for Soft Authentication and Progressive Authorization Relying on Physical Layer Attributes. *IEEE Trans. Commun.* **2020**, *68*, 2607–2620. [CrossRef]
19. Qiu, X.; Jiang, T.; Wu, S.; Hayes, M. Physical Layer Authentication Enhancement Using a Gaussian Mixture Model. *IEEE Access* **2018**, *6*, 53583–53592. [CrossRef]
20. Zhang, Y. Physical Layer Authentication Based on Gaussian Mixture Model Under Unknown Number of Attackers. In Proceedings of the 2021 IEEE/CIC International Conference on Communications in China (ICCC), Xiamen, China, 28–30 July 2021; pp. 70–74.
21. Zhu, Y.; Dong, X.; Lu, T. An Adaptive and Parameter-Free Recurrent Neural Structure for Wireless Channel Prediction. *IEEE Trans. Commun.* **2019**, *67*, 8086–8096. [CrossRef]
22. Wang, S.; Huang, K.; Xu, X.; Zhong, Z.; Zhou, Y. CSI-Based Physical Layer Authentication via Deep Learning. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 1748–1752. [CrossRef]

23. Chen, Y.; Ho, P.-H.; Wen, H.; Chang, S.Y.; Real, S. On Physical-Layer Authentication via Online Transfer Learning. *IEEE Internet Things J.* **2022**, *9*, 1374–1385. [CrossRef]
24. Wang, N.; Jiang, T.; Lv, S.; Xiao, L. Physical-Layer Authentication Based on Extreme Learning Machine. *IEEE Commun. Lett.* **2017**, *21*, 1557–1560. [CrossRef]
25. Xie, N.; Chen, J.; Huang, L. Physical-Layer Authentication Using Multiple Channel-Based Features. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2356–2366. [CrossRef]
26. Senigagliesi, L.; Baldi, M.; Gambi, E. Comparison of Statistical and Machine Learning Techniques for Physical Layer Authentication. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1506–1521. [CrossRef]
27. Zhang, P.; Liu, J.; Shen, Y.; Jiang, X. Exploiting Channel Gain and Phase Noise for PHY-Layer Authentication in Massive MIMO Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4265–4279. [CrossRef]
28. Xia, S. Multiple Correlated Attributes Based Physical Layer Authentication in Wireless Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1673–1687. [CrossRef]
29. Fang, H.; Wang, X.; Xu, L. Fuzzy Learning for Multi-Dimensional Adaptive Physical Layer Authentication: A Compact and Robust Approach. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 5420–5432. [CrossRef]
30. Tushar, W.; Yuen, C.; Saha, T.K.; Nizami, S.; Alam, M.R.; Smith, D.B.; Poor, H.V. A Survey of Cyber-Physical Systems from a Game-Theoretic Perspective. *IEEE Access* **2023**, *11*, 9799–9834. [CrossRef]
31. Meng, R. Multiuser Physical-Layer Authentication Based on Latent Perturbed Neural Networks for Industrial Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 637–652. [CrossRef]
32. Lu, X.; Lei, J.; Shi, Y.; Li, W. Improved Physical Layer Authentication Scheme Based on Wireless Channel Phase. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 198–202. [CrossRef]
33. Zhang, Y. CV-3DCNN: Complex-Valued Deep Learning for CSI Prediction in FDD Massive MIMO Systems. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 266–270. [CrossRef]
34. Germain, K.S.; Kragh, F. Channel Prediction and Transmitter Authentication With Adversarially-Trained Recurrent Neural Networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 964–974. [CrossRef]
35. Liu, J.; Wang, X. Physical Layer Authentication Enhancement Using Two-Dimensional Channel Quantization. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 4171–4182. [CrossRef]
36. Xie, N. Physical Layer Authentication With High Compatibility Using an Encoding Approach. *IEEE Trans. Commun.* **2022**, *70*, 8270–8285. [CrossRef]
37. Yin, X.; Fang, X.; Zhang, N.; Yang, P.; Sha, X.; Qiu, J. Online Learning Aided Adaptive Multiple Attribute-Based Physical Layer Authentication in Dynamic Environments. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1106–1116. [CrossRef]
38. Wang, H.-M.; Fu, Q.-Y. Channel-Prediction-Based One-Class Mobile IoT Device Authentication. *IEEE Internet Things J.* **2022**, *9*, 7731–7745. [CrossRef]
39. Qiu, X.; Dai, J.; Hayes, M. A Learning Approach for Physical Layer Authentication Using Adaptive Neural Network. *IEEE Access* **2020**, *8*, 26139–26149. [CrossRef]
40. Qiu, X.; Sun, X.; Hayes, M. Enhanced Security Authentication Based on Convolutional-LSTM Networks. *Sensors* **2021**, *21*, 5379. [CrossRef] [PubMed]
41. Shawky, M.A.; Bottarelli, M.; Epiphaniou, G.; Karadimas, P. An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 8738–8754. [CrossRef]
42. Wu, Y.; Wei, D.; Guo, C.; Huang, W. Physical Layer Authentication Based on Channel Polarization Response in Dual-Polarized Antenna Communication Systems. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2144–2159. [CrossRef]
43. Zhang, H.; Sindagi, V.; Patel, V.M. Image De-Raining Using a Conditional Generative Adversarial Network. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 3943–3956. [CrossRef]
44. Wang, Q.; Jiang, K.; Wang, Z.; Ren, W.; Zhang, J.; Lin, C.-W. Multi-Scale Fusion and Decomposition Network for Single Image Deraining. *IEEE Trans. Image Process.* **2024**, *33*, 191–204. [CrossRef] [PubMed]
45. Li, W.; Chen, G.; Chang, Y. An Efficient Single Image De-Raining Model With Decoupled Deep Networks. *IEEE Trans. Image Process.* **2024**, *33*, 69–81. [CrossRef] [PubMed]
46. Cell, R.; Remley, K.A.; Moaveri, N. Radio frequency measurements for selected manufacturing and industrial environments. *NISTTech. Rep.* **2016**. [CrossRef]
47. Zhang, R.; Wu, S.; Jiang, C.; Gao, N.; Qiu, X.; Zhang, W. Trustworthy and Scalable Federated Edge Learning for Future Integrated Positioning, Communication and Computing System: Attacks and Defenses. *IEEE Internet Things J.* **2023**. [CrossRef]
48. Radford, A.; Metz, L.; Chintala, S. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks. *arXiv* **2015**, arXiv:1511.06434.
49. Arjovsky, M.; Bottou, L. Towards Principled Methods for Training Generative Adversarial Networks. *arXiv* **2017**, arXiv:1701.04862.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.