Security Enhancement of CSI-based Wireless Sensing via Generative AI

Jiacheng Wang[1], Chenyuan Feng[2], Geng Sun[3], Hongyang Du[4], Dusit Niyato[1], Tony Q. S. Quek[5,6], and Victor C. M. Leung[7]
[1]College of Computing and Data Science, Nanyang Technological University, Singapore
[2]Eurecom, France
[3]College of Computer Science and Technology, Jilin University, China
[4]Department of Electrical and Electronic Engineering, University of Hong Kong, China
[5]Singapore University of Technology and Design, Singapore
[6]Yonsei Frontier Lab, Yonsei University, South Korea
[7]Department of Electrical and Computer Engineering, The University of British Columbia, Canada
Emails: {jiacheng.wang, dniyato}@ntu.edu.sg, Chenyuan.Feng@eurecom.fr, sungeng@jlu.edu.cn, duhy@eee.hku.hk, tonyquek@sutd.edu.sg, vleung@ieee.org

***Abstract*—Integrated Sensing and Communication (ISAC) is becoming a key technology in 6G networks, where sensing based on channel state information (CSI) plays an essential role. Present research primarily focuses on enhancing sensing performance, yet often overlooks security issue, especially the threat of unauthorized sensing that tends to receive little attention. In response to the above threat, this paper proposes to use generative AI to enhance the security of CSI-based sensing systems. Specifically, we design the guarding signal according to the characteristics of CSI fluctuations caused by user activities and build the corresponding database based on the measurements collected by software-defined radio. Utilizing the constructed dataset, we train the conditional generative diffusion model, which can produce guarding signals that are similar yet distinct from the original training samples. Then, these guarding signals are modulated onto pilot signals, effectively masking the user-induced fluctuations, thereby preventing unauthorized devices from performing illegitimate sensing. Taking the user activity recognition as the example, experimental evaluations illustrate that the proposed method reduces the recognition accuracy of unauthorized devices by about 75%, significantly enhancing user privacy protection against unauthorized sensing.**

***Index Terms*—Channel state information, wireless sensing security, generative AI.**

I. Introduction

As a promising technology, integrated sensing and communication (ISAC) combines communication and sensing within one system, fully leveraging network resources for concurrent data transmission and environmental sensing [1]. A typical example of ISAC is channel state information (CSI) based sensing [2]. CSI based sensing involves analyzing CSI extracted from wireless communication signals to perceive users. From large scale to small scale, it includes users' spatial position, activities, and even physiological signs such as breath. While these efforts are comprehensive and thorough, they overlook the sensing security. Specifically, these sensing systems rely on CSI extracted from pilot signals, making them easy to deploy. Nonetheless, this accessibility also means that typical device in the open space can intercept wireless communication signals and employ pre-defined pilot signals to obtain CSI. On this basis, unauthorized devices can exploit these CSI measurements to sense users' daily activities. For example, rogue access points (APs) can catch wireless signals and estimated CSI to monitor user activities, as shown in Fig. 1, causing privacy risks [3].

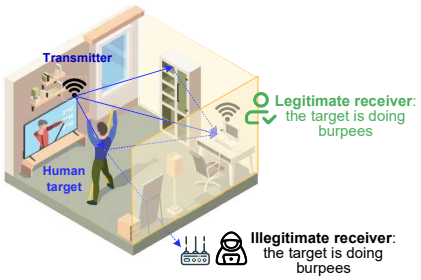


Fig. 1: An unauthorized access point(AP) conducts illegitimate sensing without disrupting legitimate sensing and communication activities.

An promising approach to safeguard users against illegitimate sensing is to generate a guarding signal and modulate it onto standard pilot signals, so as to cancel the CSI variations induced by activities of the user [4]. In this process, it is crucial to ensure that the guarding signal cannot be reconstructed by unauthorized devices. Furthermore, another issue is to make sure the signal generation can dynamically adjust according to variations in transmission contexts, which is challenging. Fortunately, recent developments in AI-generated content (AIGC) have facilitated the evolution of generative AI (GAI) models [5] that can be used to produce the guarding signals. Within AIGC domain, diffusion models are capable of creating text, images, and videos based on user prompts, demonstrating strong capability and adaptability in data generation. In fact, beside digital content generation, diffusion models are proficient in both signal denoising and generation [6], providing multiple distinct benefits [7]. Firstly,

they demonstrate creativity in data generation by producing outputs that are similar to the training data but not identical, thereby ensuring diversity in the generated samples. Secondly, they rely on specific network parameters and random seeds for data generation through denoising processes, which leads to unpredictable results. Moreover, they are flexible, enabling adjustments to the signal generation process to better align with user prompts. Such attributes render diffusion models an ideal choice for the creation of guarding signals.

Leveraging above mentioned observations, we propose using conditional diffusion models to generate guarding signals, thereby enhancing the security of CSI-based sensing systems. Specifically, we first conduct a detailed analysis of the CSI fluctuation characteristics caused by human activities and design guarding signals based on the analysis. Using software-defined radios (SDR), we collect extensive CSI data to construct a dataset of guarding signals, and then train a conditional diffusion model with this dataset. After that, the model is used to produce guarding signals, which are modulated onto pilot at the transmitter (Tx) to mask the CSI variations. At the receiver (Rx), the replication of the modulated guarding signals are conducted by the authorized sensing devices through running the same conditional diffusion model and random seed. This allows authorized devices to obtain the actual CSI for effective sensing and communication. In contrast, unauthorized devices cannot generate guarding signals, so they are blocked from accessing the real CSI and are unable to carry out illegal surveillance. In summary, the contributions of this paper are outlined as follows.

- We conduct a thorough analysis of signal fluctuations caused by various human activities in indoor scenarios and design guarding signals based on the characteristics identified through this analysis.
- We use an SDR platform to collect CSI data under various conditions and built a dataset of guarding signals. Based on this dataset, we trained a generative conditional diffusion model, which can then generate guarding signals tailored to specific input conditions.
- Using activity recognition as an example, the proposed method is evaluated. Experimental results indicate that the activity recognition accuracy of unauthorized devices can be declined by about 75% by using our method, validating its effectiveness in protecting users from illegitimate monitoring.

II. System Design

This section describes the proposed method in detail, including the guarding signal design, dataset construction, conditional diffusion model training, and how the generated signals are utilized to protect users from illegitimate sensing.

A. Signal Model

Consider a pair of transceivers that sense users in the environment by using orthogonal frequency-division multiplexing signals. The Rx receives signals and then uses the predefined pilot signal for both the Tx and rX to estimate the CSI for human activities recognition. Assuming no inter-carrier interference (ICI), then the CSI is obtained via

$$\hat{\mathbf{H}} = \left(\mathbf{X}^{\mathrm{H}}\mathbf{X}\right)^{-1}\mathbf{X}^{\mathrm{H}}\mathbf{Y} = \mathbf{X}^{-1}\mathbf{Y}, \tag{1}$$

where $\mathbf{X}$ is the transmitted training symbols, $\mathbf{Y}$ is the received training symbols, and the superscript H is the conjugate transpose operator. At time t, the CSI of the n-th subcarrier can be denoted as

$$\begin{aligned} H\left(f_n,t\right) = e^{-j\varepsilon}\sum_{l\in P_d}\alpha_l\left(f_n,t\right)e^{-j2\pi f_n d_l(t)/c} + n_{f_n,t} \\ + e^{-j\varepsilon}H_s\left(f_n,t\right), \end{aligned} \tag{2}$$

where $e^{-j\varepsilon}$ represents the phase shift caused by synchronization, $H_s\left(f_n,t\right)$ denotes sum of the CSI corresponding to all static propagation paths, P_d contains dynamic propagation paths induced by the moving user, $\alpha_l\left(f_n,t\right)$ indicates the initial signal phase and attenuation of the path l, $e^{-j2\pi f_n d_l(t)/c}$ is the accumulated phase due to the propagation length change of the path l, and $n_{f_n,t}$ is noise. On this basis, the power of CSI can be expressed as

$$\begin{aligned} \left|H\left(f_n,t\right)\right|^2 &= \sum_{l\in P_d}\left|\alpha\left(f_n,t\right)\right|^2 + \left|H_s\left(f_n,t\right)\right|^2 \\ &+ \sum_{l\in P_d} 2H_s\alpha \times \cos\left[\frac{2\pi f_n\left(v_l t + d_l\left(0\right)\right)}{c} + \theta_{sl}\right] \\ &+ \sum_{l,l'\in P_d} 2\alpha_{ll'}\cos\left[\frac{2\pi f_n\left(t\Delta v_{ll'} + \Delta d_{ll'}\left(0\right)\right)}{c} + \theta_{ll'}\right] \\ &+ \Psi\left(n_{f_n,t}\right), \end{aligned} \tag{3}$$

where

$$\begin{cases} H_s\alpha = \left|H_s\left(f_n,t\right)\alpha_l\left(f_n,t\right)\right| \\ \alpha_{ll'} = \left|\alpha_l\left(f_n,t\right)\alpha_{l'}\left(f_n,t\right)\right| \\ \Delta v_{ll'} = v_l - v_{l'} \\ \Delta d_{ll'}\left(0\right) = d_l\left(0\right) - d_{l'}\left(0\right) \end{cases}, \tag{4}$$

v_l and $d_l\left(0\right)$ are the length change rate and initial length of the l-th dynamic propagation path, θ_{sl} and $\theta_{ll'}$ are the initial phases, and $\Psi\left(n_{f_n,t}\right)$ is the power of the noise multiplied by cross terms. As can be seen from (3) that CSI power consists of a combination of sinusoids and constants, with the total intensity influenced by $\left|H_s\left(f_n,t\right)\right|$. Moreover, we can see the main fluctuations in the CSI are caused by the term in second raw, whose intensity is lower than $\left|H_s\left(f_n,t\right)\right|^2$. Given that distinct human activities produce different v_l values, activity recognition can be achieved by identifying and analyzing the patterns of these fluctuations.

To mask the variations in CSI induced by human activities, we propose to generate the guarding signal and then multiply them with pilots that are used for CSI estimation at the Rx. Concretely, let the training symbols with N subcarriers be

$$\mathbf{X} = \mathrm{diag}\left(X\left[0\right],\ \ldots,\ X\left[N-1\right]\right), \tag{5}$$

where $X\left[n\right]$ denotes the pilot signal of the n-th subcarrier.

Then the training symbol with the guarding signal can be expressed as

$$\mathbf{X}' = \mathrm{diag}\left(s\left(f_0,t\right)X\left[0\right],\ldots,s\left(f_{N-1},t\right)X\left[N-1\right]\right), \quad (6)$$

where $s\left(f_n,t\right)$ is the guarding signal corresponding to the n-th subcarrier. In this case, the authorized device, which has guarding signal, can extract real CSI via $\hat{\mathbf{H}} = \left(\mathbf{X}'\right)^{-1}\mathbf{Y}'$, where $\mathbf{Y}'$ is the captured signal as $\mathbf{X}'$ is sent out. On the other hand, for the unauthorized device without guarding signal can obtain $\hat{\mathbf{H}}' = \mathbf{X}^{-1}\mathbf{Y}'$. Therefore, according to (2) and (3), we have

$$\left|H'\left(f_n,t\right)\right|^2 = \left|s\left(f_n,t\right)\right|^2\left|H\left(f_n,t\right)\right|^2, \quad (7)$$

where

$$\begin{aligned} H'\left(f_n,t\right) &= e^{-j\varepsilon}s\left(f_n,t\right)H_s\left(f_n,t\right) + {n'}_{f_n,t} \\ &\quad + e^{-j\varepsilon}\sum_{l\in P_d} s\left(f_n,t\right)\alpha_l\left(f_n,t\right)e^{-j2\pi f_n d_l(t)/c}. \end{aligned} \quad (8)$$

From (7) and (8), it is clear that the fluctuation of CSI power in unauthorized devices is influenced by both the channel and the guarding signal, hence allowing effective masking of fluctuations due to user activities via guarding signal adjustments. For instance, let $\left|H_{wk}\left(f_n,t\right)\right|^2$ be the CSI power when a user is walking. The fluctuation characteristics of $\left|H_{wk}\left(f_n,t\right)\right|^2$ are defined by many parameters, including $d_l\left(0\right)$, v_l, and P_d, primarily governed by the static path components, which depend on the positions of the transmitter and receiver. Then, we can set $s\left(f_n,t\right) = 1/\left|H_{wk}\left(f_n,t\right)\right|$, which can makes the CSI power obtained by the unauthorized Rx close to 1. Hence, the CSI variations induced by the user's activity can be masked by the guarding signal. However, in practice, the activity of the human user is unknown, and aforementioned parameters are difficult to obtain, making it challenging to calculate $1/\left|H_{wk}\left(f_n,t\right)\right|$ directly.

B. guarding Signal Design and Dataset Construction

Although user activities are unpredictable and related signal parameters are difficult to acquire, the types of activities performed in indoor environments are limited and the research shows corresponding signal parameters values fall within a certain range [4]. We carried out experiments in the indoor scenario using the method described in [4] to analyze the v_l for four common user activities. The findings presented in Fig. 2 demonstrate that the v_l for sitting down varies from approximately 0.1 to 2.5 m/s, whereas for falling, it spans from about 2 to 5.5 m/s. This is notably higher than those of the rest activities. Based on these observations and the aim of the guarding signal, which is to mask user movements induced signal variations, the guarding signal is designed as follows

$$\begin{aligned} s\left(f_n,t\right) &= 1/\left|H_1\left(f_n,t\right)\right| + 1/\left|H_2\left(f_n,t\right)\right| \\ &\quad + 1/\left|H_3\left(f_n,t\right)\right| + 1/\left|H_4\left(f_n,t\right)\right|, \end{aligned} \quad (9)$$

where $H_1\left(f_n,t\right)$, $H_2\left(f_n,t\right)$, $H_3\left(f_n,t\right)$, and $H_4\left(f_n,t\right)$ are CSI measurements corresponding to falling, running, walking, and siting down, respectively. The reason for such design is

Fig. 2: Distribution of v_l corresponding to four common indoor activities.

that the v_l associated with these activities spans from 0 m/s to approximately 6 m/s, nearly covering all potential values of v_l [4]. Hence, it provides two significant benefits. First, the signal fluctuations induced by various indoor user activities can be effectively canceled by $s\left(f_n,t\right)$ to certain degrees. Second, it also introduces new interference to further mask the signal fluctuation characteristics. For instance, when a user waves hand, components $H_1\left(f_n,t\right)$ and $H_2\left(f_n,t\right)$ in $s\left(f_n,t\right)$ can help cancel the signal fluctuations. Meanwhile, components $H_3\left(f_n,t\right)$ and $H_4\left(f_n,t\right)$ contribute additional new interference, which further masks the signal features introduced by waving hands.

To ensure the $s\left(f_n,t\right)$ possesses the aforementioned characteristics while preventing unauthorized devices from replicating it, a generative diffusion is trained to produce the guarding signal. To guarantee the quality of $s\left(f_n,t\right)$, a dataset containing real-world CSI measurements is built to train the diffusion model. Specifically, the universal software radio peripheral (USRP) is used to collect CSI data under various conditions for four types of activities. Then, $H_1\left(f_n,t\right)$, $H_2\left(f_n,t\right)$, $H_3\left(f_n,t\right)$, and $H_4\left(f_n,t\right)$ are calculated and combined to obtain the guarding signal, thereby building the training dataset. Figure 3 displays the general process of the dataset construction.

C. Guarding Signal Generation

Based on the constructed dataset, the conditional diffusion model is trained to generate guarding signals. During this process, the distance between the signal transmitter and receiver is used as a generation condition since it directly impacts the CSI power according to (3), which in turn affects the guarding signal. The generative diffusion model consists of a forward process and a reverse process. Specifically, given a noise scale schedule denoted as $0 < \beta_1,\ldots,\beta_T < 1$, for a given guarding training signal $\mathbf{x}_0 \sim q_g\left(\mathbf{x}\right)$, the forward process of the diffusion model involves adding noise over T steps to perturb the training sample, therefore

$$q\left(\mathbf{x}_t\left|\mathbf{x}_{t-1}\right.\right) = \mathcal{N}\left(\mathbf{x}_t;\sqrt{1-\beta_t}\mathbf{x}_{t-1},\beta_t\mathbf{I}\right), \quad (10)$$

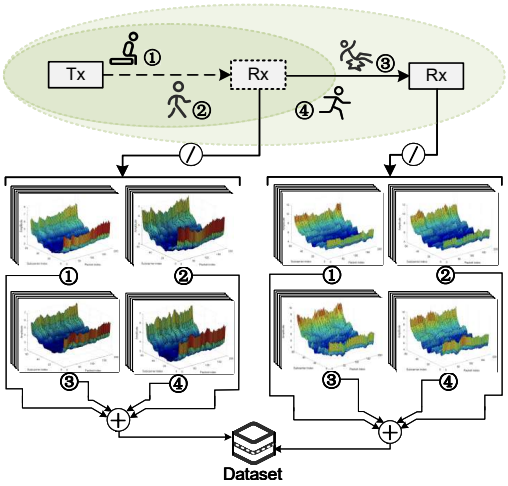


Fig. 3: The process of constructing the dataset. It involves calculating and accumulating $s(f_n, t)$ by using the CSI of different activities gathered in varying cases to assemble the training dataset.

where $\mathbf{I}$ is the identity matrix. From $t-1$ to t, based on above transition relationship, we can have

$$q(\mathbf{x}_t|\mathbf{x}_0) = \mathcal{N}(\mathbf{x}_t; \sqrt{\alpha_t}\mathbf{x}_0, (1-\alpha_t)\mathbf{I}), \tag{11}$$

where $\alpha_t = \prod_{t'=1}^{t}(1-\beta_{t'})$. After adding noise over T steps, the distribution of the perturbed training sample is

$$\begin{aligned} q(\mathbf{x}_{1:T}|\mathbf{x}_0) &= \prod_{t=1}^{T} q(\mathbf{x}_t|\mathbf{x}_{t-1}) \\ &= \prod_{t=1}^{T} \mathcal{N}\left(\mathbf{x}_t; \sqrt{1-\beta_t}\mathbf{x}_{t-1}, \beta_t\mathbf{I}\right). \end{aligned} \tag{12}$$

The diffusion model fundamentally operates as a Markov chain, therefore, by incorporating the generation condition $\mathbf{u}'$ into the forward process, (9) can be transformed to

$$q'(\mathbf{x}_t|\mathbf{x}_{t-1}, \mathbf{u}') = q(\mathbf{x}_t|\mathbf{x}_{t-1}). \tag{13}$$

On this basis, we can obtain

$$\begin{aligned} q'(\mathbf{x}_t|\mathbf{x}_{t-1}) &= \int_u q'(\mathbf{x}_t, \mathbf{u}|\mathbf{x}_{t-1})\, d\mathbf{u} \\ &= \int_u q(\mathbf{x}_t|\mathbf{x}_{t-1})\, q'(\mathbf{u}|\mathbf{x}_{t-1})\, d\mathbf{u} \\ &= q(\mathbf{x}_t|\mathbf{x}_{t-1}) = q'(\mathbf{x}_t|\mathbf{x}_{t-1}, \mathbf{u}), \end{aligned} \tag{14}$$

and

$$\begin{aligned} q'(\mathbf{x}_{1:T}|\mathbf{x}_0) &= \int_u q'(\mathbf{x}_{1:T}, \mathbf{u}|\mathbf{x}_0)\, d\mathbf{u} \\ &= \int_u q'(\mathbf{u}|\mathbf{x}_0) \prod_{t=1}^{T} q'(\mathbf{x}_t|\mathbf{x}_{t-1}, \mathbf{u}) d\mathbf{u} \\ &= \prod_{t=1}^{T} q'(\mathbf{x}_t|\mathbf{x}_{t-1}) = q(\mathbf{x}_{1:T}|\mathbf{x}_0). \end{aligned} \tag{15}$$

As can be seen, the noise $\beta_1, \ldots, \beta_T$ is predefined, allowing $\mathbf{x}_T$ to approximate $\mathcal{N}(\mathbf{0}, \mathbf{I})$ in the forward process. Meanwhile, incorporating the generation condition in the forward process has no significant effect on the noise addition.

In the reverse process, the diffusion model begins with Gaussian noise and generates samples through T steps of denoising. If $q(\mathbf{x}_{t-1}|\mathbf{x}_t)$ is accessible, the reverse diffusion process can be effectively executed to obtain samples from $q(\mathbf{x}_0)$. However, determining $q(\mathbf{x}_{t-1}|\mathbf{x}_t)$ requires calculating the data distribution, which is practically intractable. Hence, $q(\mathbf{x}_{t-1}|\mathbf{x}_t)$ is parameterized, which is denoted as

$$p_\theta(\mathbf{x}_{t-1}|\mathbf{x}_t) = \mathcal{N}(\mathbf{x}_{t-1}; \boldsymbol{\mu}_\theta(\mathbf{x}_t, t), \boldsymbol{\Sigma}_\theta(\mathbf{x}_t, t)). \tag{16}$$

Through this, the process from x_T to x_0 can be obtained

$$p_\theta(\mathbf{x}_{0:T}) = p_\theta(\mathbf{x}_T) \prod_{t=1}^{T} p_\theta(\mathbf{x}_{t-1}|\mathbf{x}_t), \tag{17}$$

and the loss function can be expressed as

$$L(\theta) = \mathbb{E}_{\mathbf{x}_0, \boldsymbol{\varepsilon}\sim N(0,\mathbf{I}), t}\left[\left\|\boldsymbol{\varepsilon}_\theta\left(\begin{array}{c}\sqrt{\alpha_t}\mathbf{x}_0 \\ +\sqrt{1-\sqrt{\alpha_t}}\boldsymbol{\varepsilon}, t\end{array}\right) - \boldsymbol{\varepsilon}, t\right\|^2\right], \tag{18}$$

where $L(\theta)$ is a weighted form of the evidence lower bound. Based on the aforementioned reverse process, the generation condition $\mathbf{u}$, i.e., the distance between the signal transmitter and receiver, is incorporated to guide the diffusion model in producing the desired guarding signals. Hence, we have

$$p_\theta(\mathbf{x}_{0:T}|\mathbf{u}) = p_\theta(\mathbf{x}_T) \prod_{t=1}^{T} p_\theta(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{u}), \tag{19}$$

where

$$p_\theta(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{u}) = \mathcal{N}(\mathbf{x}_{t-1}; \boldsymbol{\mu}_\theta(\mathbf{x}_t, t, \mathbf{u}), \boldsymbol{\Sigma}_\theta(\mathbf{x}_t, t, \mathbf{u})). \tag{20}$$

The guarding signals generated in this manner resemble but differ from those in the training dataset. This similarity fosters randomness and diversity, which hinders unauthorized receivers from duplicating them. According to (5), the generated guarding signals are modulated onto the original pilot to mask fluctuations caused by user activity. Notably, the signal's fluctuation characteristics primarily manifest in the time domain. Therefore, the guard signal remains the same across different subcarriers, indicating that $s(f_0, t) = s(f_n, t)$.

III. IMPLEMENTATION AND EVALUATION

The proposed method is evaluated through the USRP from two aspects. Firstly, the guarding signal generation based on the trained conditional diffusion model is presented. Subsequently, the generated guarding signals are modulated onto the pilot signals and user activity classification is used as a case to evaluate the effectiveness in safeguarding users against unauthorized sensing.

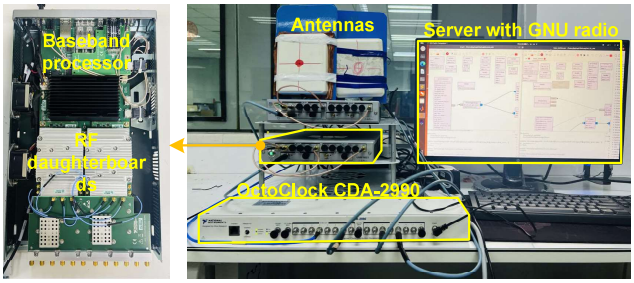


Fig. 4: The hardware devices, which include the USRP N321 along with its internal configuration, the server, external clock, and directional antenna.

A. Experimental Configurations

For hardware configuration, it involves USRP N321 devices and servers. The server for training and inference processes of the diffusion model are running Ubuntu 20.04 OS with an AMD Ryzen Threadripper PRO 3975WX 32-core processor and an NVIDIA RTX A6000 GPU. After generation, the guarding signals are transferred to the other server featuring 64 GB RAM and the GNU Radio 3, linked to the USRP N321 units through 10-gigabit Ethernet connections. Each USRP N321 device incorporates a processor for baseband along with a UBX-160 daughterboard. Synchronization across devices is ensured by an OctoClock-G CDA-29906. The test is conducted at 2.8 GHz with 100 MHz bandwidth spanning 64 subcarriers and a transmission rate of 100 packets per second. To improve the quality of both transmission and receiving, we employ a directional antenna with 12 dBi gain. Figure 4 provides a overview of the hardware used in the experiment, including the antennas, Xilinx baseband processor, daughterboard, etc.

B. Performance Evaluation

1) Guarding Signal Generation: The signal generation process under different conditions are shown in Figs. 5 and 6. As can be observed, with 460 denoising steps, the guarding signals are still noisy, indicating that denoising is inadequate. As the denoising continues, the noise further diminishes, making the guarding signals clearer. After 500 steps, a complete and distinct guarding signal is obtained, confirming the effectiveness of the generation process. On this basis, we can see that different conditions yield different guarding signals. For instance, the generated guarding signals are weaker when the transmitter and receiver are closer, and stronger when they are further apart. This occurs because when the transmitter and receiver are close, the signals received have higher amplitude and more pronounced fluctuations. Consequently, a weaker guarding signal is needed to effectively cancel the variation introduced by user activity. On the other hand, a greater separation needs stronger guarding signals. This demonstrates that the conditions can effectively guide the signal generation. Besides, while the generated signals mirror the training samples in terms of intensity and overall trends, they remain distinct. This underscores the variability and unpredictability, preventing unauthorized devices from replicating them.

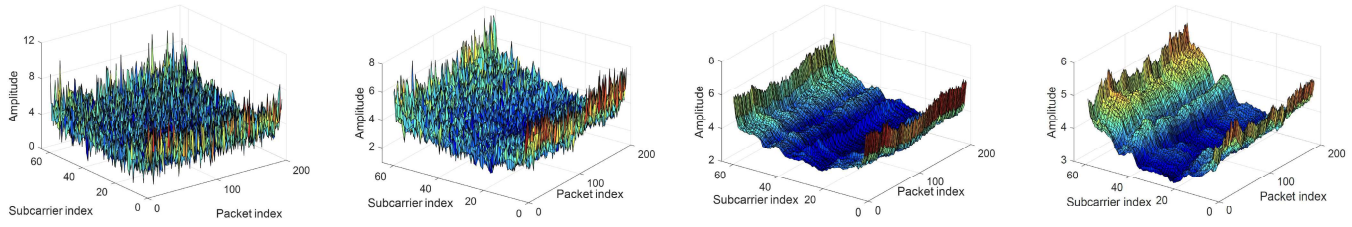
2) Protection Performance in Activity Recognition: The generated guarding signals are modulated onto pilot signals to evaluate the performance of protecting users from unauthorized activity recognition. The experiment is conducted based on AF-ACT [3], ABLSTM [8], and PhaseAnti [9], including five types of activities: waving (WH), walking (WK), squatting (SQ), sitting (ST), and falling (FL). The proposed method is compared with Secur-Fi [10] via recognition accuracy (RA) and accuracy degradation rate (ADR).The calculation of Recognition Accuracy (RA) involves dividing the number of accurate identifications by the total count of tests performed, and ADR is defined as $(RA_{org} - RA_{sf})/RA_{org}$, where RA_{org} is the RA without the guarding signal, and RA_{sf} is the RA of an unauthorized device when guarding signal is used. A higher ADR indicates better protection performance.

Figures 7(a) to 7(c) show that when the guarding signal is used, the average ADRs of AF-ACT, ABLSTM, and PhaseAnti are 0.78, 0.81, and 0.72, respectively. In contrast, when Secur-Fi is used, these systems achieve ADRs of 0.71, 0.68, and 0.58, respectively. These results indicate that our method holds better protection performance. This occurs because our method modulates the generated guarding signals onto the pilot signals. Compared to Secur-Fi, which introduces signal fluctuations by adjusting antennas, our method impacts the signal more directly and thoroughly, hence offering better protection.

Additionally, our method works well for different types of activities, demonstrated by the ADRs of ABLSTM for five different activities are 0.81, 0.82, 0.83, 0.81, and 0.77. However, its effectiveness varies between systems. For instance, it has a more pronounced effect on AF-ACT and ABLSTM than on PhaseAnti. This is because ABLSTM and AF-ACT depend solely on CSI amplitude to recognize user activity, while PhaseAnti uses both amplitude and phase, making it more robust. Finally, Fig. 7(d) presents the activity recognition confusion matrix of AF-ACT with RAs of five activities are 19%, 16%, 17%, 21%, and 27%. This demonstrates that our method prevents the systems from mistakenly classifying different activities as the same one. This outcome is due to the generated guarding signal's degree of randomness, which causes the CSI features captured by unauthorized devices to vary, leading to unpredictable recognition results.

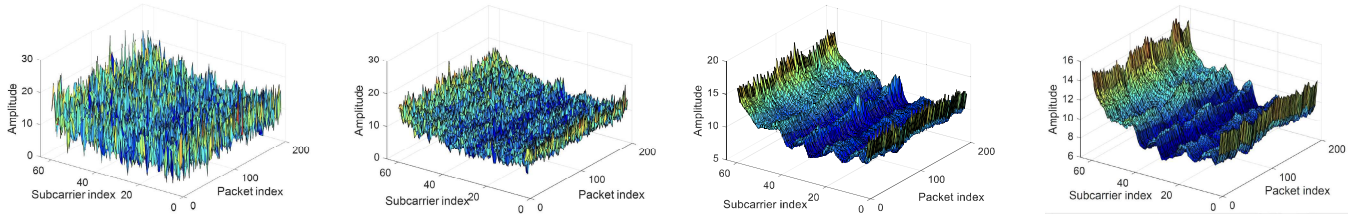
IV. Conclusion

This paper proposes to use the generative diffusion model to enhance the security of CSI-based sensing systems. It analyzes the signal fluctuation characteristics caused by user activities and designs guarding signals that can mask these fluctuations. On this basis, we construct a dataset and train a conditional diffusion model to generate the guarding signals. These signals are then modulated onto pilot signals to mask the signal fluctuations induced by the user, thereby, effectively preventing unauthorized devices from performing illicit sensing. Experimental evaluations demonstrate that the



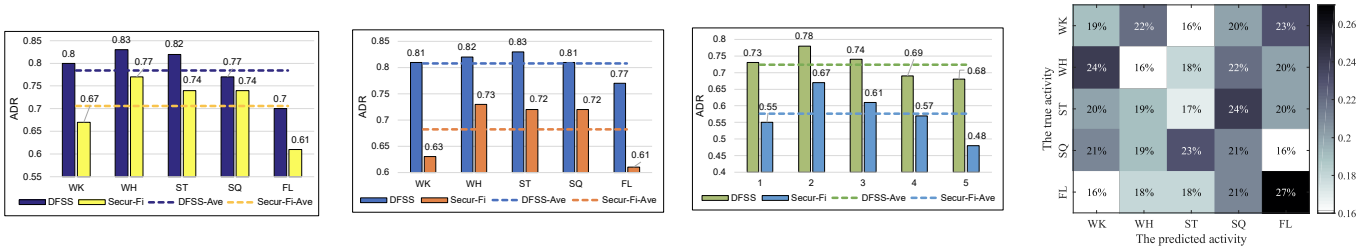
(a) (b) (c) (d)

Fig. 5: The guarding signal generation process when Tx and Rx are about 3 meters apart. (a) to (c) respectively show the guarding signals generated after 460, 480, and 500 denoising steps. (d) illustrates a sample from the training dataset.



(a) (b) (c) (d)

Fig. 6: The guarding signal generation process when Tx and Rx are about 6 meters apart. (a) to (c) respectively show the guarding signals generated after 460, 480, and 500 denoising steps. (d) illustrates a sample from the training dataset.



(a) ADR of AF-ACT. (b) ADR of ABLSTM. (c) ADR of PhaseAnti. (d) Confusion matrix of AF-ACT.

Fig. 7: The protection performance comparison.

proposed method reduces the activity recognition accuracy of unauthorized devices by about 75%. Given the widespread accessibility of CSI for wireless sensing applications, the proposed method offers an innovative approach to safeguard users against unauthorized sensing.

REFERENCES

[1] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6g and beyond," *IEEE journal on selected areas in communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[2] J. Wang, H. Du, D. Niyato, M. Zhou, J. Kang, and H. V. Poor, "Acceleration estimation of signal propagation path length changes for wireless sensing," *IEEE Transactions on Wireless Communications*, 2024.

[3] Y. Zhang, Q. Liu, Y. Wang, and G. Yu, "Csi-based location-independent human activity recognition using feature fusion," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–12, 2022.

[4] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Device-free human activity recognition using commercial wifi devices," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1118–1131, 2017.

[5] H. Du, R. Zhang, Y. Liu, J. Wang, Y. Lin, Z. Li, D. Niyato, J. Kang, Z. Xiong, S. Cui *et al.*, "Enhancing deep reinforcement learning: A tutorial on generative diffusion models in network optimization," *IEEE Communications Surveys & Tutorials*, 2024.

[6] J. Wang, H. Du, D. Niyato, Z. Xiong, J. Kang, B. Ai, Z. Han, and D. I. Kim, "Generative artificial intelligence assisted wireless sensing: Human flow detection in practical communication environments," *IEEE Journal on Selected Areas in Communications*, 2024.

[7] G. Chi, Z. Yang, C. Wu, J. Xu, Y. Gao, Y. Liu, and T. X. Han, "Rf-diffusion: Radio signal generation via time-frequency diffusion," in *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, 2024, pp. 77–92.

[8] Z. Chen, L. Zhang, C. Jiang, Z. Cao, and W. Cui, "Wifi csi based passive human activity recognition using attention based blstm," *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2714–2724, 2018.

[9] J. Huang, B. Liu, P. Liu, C. Chen, N. Xiao, Y. Wu, C. Zhang, and N. Yu, "Towards anti-interference wifi-based activity recognition system using interference-independent phase component," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 576–585.

[10] X. Meng, J. Zhou, X. Liu, X. Tong, W. Qu, and J. Wang, "Secur-fi: A secure wireless sensing system based on commercial wi-fi devices," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*. IEEE, 2023, pp. 1–10.