This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

Scarecrow: Forging Human Presence within mmWave Radar Signal Stream

Hankai Liu, Jiaqi Zhang, Xiulong Liu, *Senior Member, IEEE*, Xin Xie, Heng Qi, *Senior Member, IEEE*, Jiancheng Chen, Junzhao Du, Keqiu Li, *Fellow, IEEE*

***Abstract*—The mmWave radar technology empowers a privacy-friendly and non-contact human-computer interaction experience. However, data leakage from the domestic mmWave radar can expose the house occupancy, which may lead to threats like burglaries. Protecting against this leakage is challenging, as physical-layer spoofing struggles to imitate the fine-grained signatures captured by high-resolution mmWave radars, while existing signal synthesis approaches rarely model both human-related signatures and propagation factors for occupancy spoofing. This paper presents Scarecrow, the pioneering system that forges human presence into the radar signal stream at the data layer. Scarecrow aims to synthesize a signal stream that is indistinguishable from a genuine radar stream. In doing so, Scarecrow addresses three critical challenges. First, it makes the forged target exhibit human-like behaviors, including natural trajectories, walking motions, and breathing signatures. Second, it makes the forged radar signals match the propagation effects and hardware responses of a real radar system. Third, it enables trusted terminals to distinguish forged targets from real ones and thus avoid erroneous sensing decisions. We develop a software prototype of Scarecrow and conduct extensive experiments to evaluate its fidelity, verisimilitude, and identifiability, in which the anomaly detection AUCs for spatial, velocity, and vital sign signatures are 0.639, 0.634, and 0.601, respectively, demonstrating that Scarecrow's synthesis is highly authentic and effective in preserving house occupancy privacy.**

***Index Terms*—mmWave radar, sensing privacy, signal synthesis, RF computing.**

I. Introduction

A. Motivation & Threat Statement

Advancements in human sensing technology have significantly contributed to the progress of human-computer interaction. As human-sensing devices enter smart homes, privacy leakage has become a key concern for consumers [1]. The risk is intuitive for privacy-sensitive sensors such as cameras, where leaked video data can directly expose home privacy.

This work was supported in part by the National Natural Science Foundation of China under Grant 62372324 and Grant 62002259. *(Corresponding author: Xiulong Liu.)*

Hankai Liu is with the College of Cryptology and Cyber Science, Nankai University, Tianjin 300350, China (e-mail: lhk@nankai.edu.cn).

Jiaqi Zhang, Xiulong Liu, Xin Xie, and Keqiu Li are with the College of Intelligence and Computing, Tianjin University, Tianjin 300350, China (e-mail: jqzhang0731@tju.edu.cn; xiulong_liu@tju.edu.cn; xinxie@tju.edu.cn; keqiu@tju.edu.cn).

Heng Qi is with the School of Computer Science and Technology, Dalian University of Technology, Dalian 116023, China (e-mail: hengqi@dlut.edu.cn).

Jiancheng Chen is with the Xiamen Peiyang BCI & Smart Health Innovation Research Institute, Xiamen 361006, China (e-mail: mikexm@qq.com).

Junzhao Du is with the School of Computer Science and Technology, Xidian University, Xi'an 710126, China (e-mail: dujz@xidian.edu.cn).

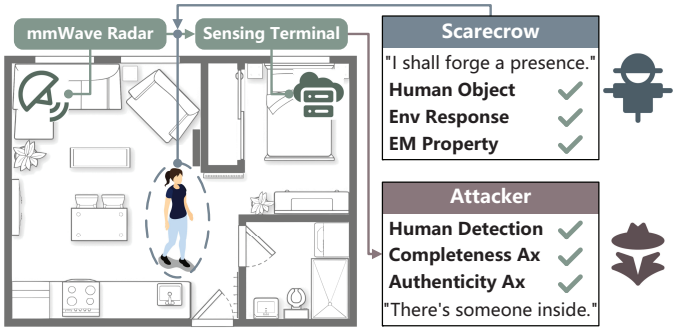


Fig. 1: Deployment scenario of Scarecrow.

The emerging millimeter-wave (mmWave) radar is considered a privacy-friendly sensor for non-contact sensing [2], and it is viewed as a key component of future integrated sensing and communication technologies. However, this privacy advantage is not absolute because RF sensing streams may expose sensitive information if they are obtained by attackers [3], and mmWave radar has even been shown to support video reconstruction [4]. Motivated by this threat landscape, this paper focuses on an immediate and safety-critical leakage in domestic scenarios: house occupancy exposure. Specifically, the attacker may compromise the networked sensing terminal through malware or a backdoor. Since the terminal needs plaintext radar streams for legitimate sensing services, the compromised terminal can expose the plaintext radar stream from memory, local files, or logs. The attacker can then perform signal processing on the leaked stream to infer house occupancy. The exposure of this critical information can cause dangerous events such as burglaries [5]. This risk parallels the situation with home cameras—if video data is stolen, home privacy will be seriously threatened. Encryption can protect radar data during transmission or storage, but it cannot prevent leakage after a compromised terminal legitimately obtains the plaintext stream for sensing. Therefore, the main purpose of this paper is to *modify or interfere with the radar signal stream to spoof attackers about the house occupancy.*

B. Limitations of Prior Art

Physical layer spoofing: Protecting location privacy at the physical layer is a key focus of wireless signal privacy security [6], [7]. Several studies have been conducted to spoof radar detection at the physical layer by emitting signals [8], [9] or backscattering [5], [10], [11]. While effective against external malicious radar detection, these methods are limited

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

in addressing user-side radar data leakage. For one thing, the richness of human activity, along with the large reflection area, makes it *challenging to achieve fine-grained human construction through deceptive signals or reflectors.* For another, the multiple-input multiple-output (MIMO) antenna array of radar relies on signal differences among channels for spatial spectrum estimation, and such differences are *difficult to be introduced and fine-tuned by external signals.* Therefore, compared to the physical layer interference, we consider spoofing at the data layer a more reliable approach.

Signal synthesis: By inserting synthetic signals into the real signal stream, the occupancy can be forged at sensing terminals. Previous signal synthesis techniques tend to be aimed at specific sensing applications and view the synthesis as a means of training data generation [12], [13], [14], [15], which have significantly enhanced the practicality of mmWave applications. For occupancy spoofing, however, the forged signal stream should go beyond a single sensing signature and *comprehensively model human-related signatures, including motion trajectories, micro-Doppler patterns, and vital signs, together with propagation factors such as multipath effects and MIMO channel mismatch.* Moreover, existing techniques sometimes *rely on domain transformation to enhance the authenticity of sensing signatures* [16], [17], [18], [19]. This post-editing does not affect the original signatures obtained by attackers, therefore we need to ensure the authenticity of the synthesized signal itself.

C. Scarecrow in a Nutshell

To overcome the limitations of existing solutions, this paper presents Scarecrow, a system for forging a human presence within a mmWave radar signal, as shown in Fig. 1. It uses the skinned multi-person linear (SMPL) model [20] from motion capture (MoCap) datasets to construct human activities and environmental responses, along with a propagation model to synthesize radar signals. The analog-to-digital converter (ADC) sampled real signal stream exists in the form of complex vectors or matrices, while the signal synthesis system generates a forged stream in the same format. When superimposed, the resulting stream contains both the environmental information from the real signal and the forged target from synthesis. Scarecrow is not an additional sensing radar, but a data-layer preprocessing module. This solution can be deployed, either in software or hardware, at any place between signal sampling and data uploading. Once an attacker accesses the uploaded data for occupancy detection, the forgery will appear authentic across various sensing signatures, making the room seem occupied and avoiding potential invasion threats.

D. Novelties & Advantages

Assuming the attacker has advanced radar signal processing and human sensing capabilities, they can perform target detection and various sensing applications, including anomaly detection to assess the authenticity of targets. Our Scarecrow system aims to mislead such attackers, addressing three key challenges to demonstrate its innovations.

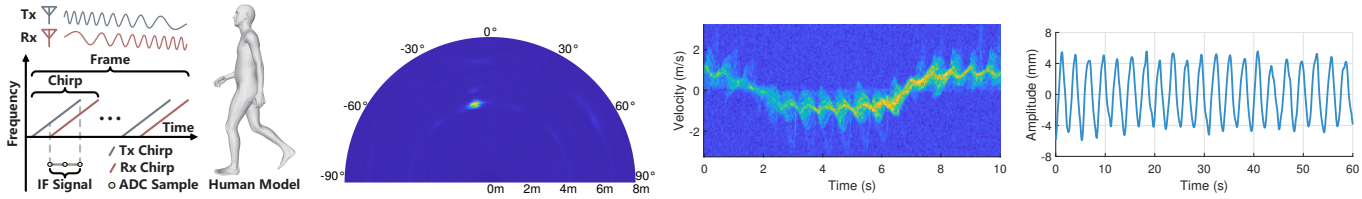
- *How to achieve high authenticity of the forgery's human activities.* We design our approach focusing on trajectory, velocity, and vital signs to create realistic virtual human objects. First, we replicate and modify historical trajectories to produce distinct paths aligned with users' behavioral patterns. Next, we apply displacement correction to ensure accurate gait information. Additionally, we propose a time expansion method for MoCap data. Finally, we simulate respiration-induced torso movement by manipulating mesh vertices. As a result, the forgery possesses authentic and rational activities across multiple dimensions.
- *How to achieve high authenticity of the synthesized signal's electromagnetic properties.* This requires in-depth and comprehensive research in ray tracing techniques involving reflection modeling and signal synthesis. For human reflections, we extract visible mesh faces and propose a stable downsampling method that minimizes fluctuations and instability in the downsampled reflection object. Next, we develop a multipath propagation model using ray tracing and Rician fading to incorporate environmental responses to the forgery into the signal. In signal computation, we simulate channel mismatches so that the synthesized signal's spatial spectrum exhibits energy leakage similar to real signals. The antenna gain and amplitude fading are also considered. Consequently, the electromagnetic properties of the synthesized signal are complete and self-consistent.
- *How to prevent trusted terminals from being interfered with by the forgery.* Scarecrow skillfully embeds identity within the forged respiration curve by assigning codes `1` and `0` to different respiration frequencies. By employing a frequency modulation variant that alters the duration of each respiration cycle, the identity code is incorporated into the respiration curve. To reduce the repetitiveness and detectability of the identity code, we implement two measures. First, the identity code occupies only a small portion with a randomized position in each broadcast period. Second, redundant bits are randomly inserted into the gaps of the identity bits, ensuring that the code varies in each broadcast. In this way, the forgery covertly informs trusted terminals of its identity, allowing the terminals to ignore its presence.

The Scarecrow system has three main advantages over previous works. (1) Compared with physical layer spoofing methods, Scarecrow enables fine-grained human object construction and provides unique signals to each channel of the MIMO array. (2) Compared with other signal synthesis methods, Scarecrow undergoes a comprehensive technical design that provides authentic sensing signatures, thereby achieving high levels of spoofing effectiveness. (3) Benefiting from the proposed identification mechanism, Scarecrow's forgeries do not interfere with trusted terminals.

The rest of this paper is structured as follows. Section II provides fundamental knowledge and the threat model of this work. Section III details the design of Scarecrow, and Section IV presents the experimental evaluation. We discuss the related work in Section VI, and conclude this paper in Section VII.

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



(a) FMCW signal (b) RAM (c) MDS (d) Respiration curve

Fig. 2: FMCW signal and typical representations of the sensing signatures.

II. Preliminaries

This section introduces the background of this work, including the principle of mmWave signal synthesis, the signatures of human sensing, and the threat model.

A. mmWave Signal Synthesis

1) FMCW Chirp Signal: The mmWave radar employs frequency modulated continuous wave (FMCW) chirp signals, as depicted in Fig. 2a. Let the transmitted (Tx) signal be $s_t(t) = A_t \exp(j2\pi(f_c + kt/2)t)$, where t, A_t, f_c, and k are the time, amplitude, start frequency, and slope, respectively. Given a reflector at distance $D(t) = R + d(t)$ from the radar, where R represents the distance between this range bin and the radar and $d(t)$ is the reflector's displacement at time t, the propagation delay is $\tau = 2D(t)/c$, and the received (Rx) signal is $s_r(t) = \alpha s_t(t - \tau)$, where α is the amplitude coefficient and c is the light speed. Passing Rx and Tx signals into the mixer, we get the intermediate-frequency (IF) signal

$$s(t) = s_t^*(t)\, s_r(t) \approx \alpha A_t \exp(j2\pi\tau(f_c + kt)). \quad (1)$$

Multiple chirps form a frame, a time unit of signal processing.

2) Signal Synthesis using MoCap Data: With human model estimation from MoCap technology, various methods have been developed to synthesize radio frequency (RF) signals. The process begins by modeling the human body to determine reflection points and radar cross sections (RCS) [19]. Then, the IF signal corresponding to each reflection point is calculated by Eq. 1. Thus, summing up the signals from all reflection points yields the final synthesized signal

$$s(t) = \sum_{n=1}^{N} s_n(t), \quad (2)$$

where N represents the number of reflection points.

B. Human Sensing Signatures

Radar sensing applications operate based on specific sensing signatures, which can be generally categorized as spatial and velocity [18]. For human targets, the vital signs should also be regarded as a class of signature [5]. Fig. 2 showcases the typical representations of these signatures.

1) Spatial Signature: Depending on the sensing task, the spatial information is typically transformed into the range-azimuth map (RAM) or elevation-azimuth map. Additionally, point clouds can be extracted by detecting points with high reflection strength. Among these, the RAM provides fine-grained spatial information about both the human body and the environment, thus serving as the representative of the spatial signature in this paper.

2) Velocity Signature: By applying the short-time Fourier transform (STFT) to the signal frame by frame, we can obtain the velocities of reflectors at each instant. This velocity-time map is known as the micro-Doppler spectrum (MDS), which describes the motion information of the target and is the foundation of several motion sensing applications such as gait measurement and activity recognition.

3) Vital Sign Signature: Vital signs like respiration and heartbeat are key signatures of a living organism. In this paper, we focus on the respiration curve as it is widely applicable and robust. During respiration, the chest and abdomen expand and contract, causing surface displacements, from which the respiration curve can be obtained by radar.

C. Threat Model

1) Scenario: We consider scenarios where mmWave radar is deployed for non-contact interaction and health monitoring, as shown in Fig. 1. The radar front-end collects raw digital IF signal and transmits it to a networked sensing terminal, which analyzes the signal stream to derive the sensing results. The attacker is assumed to obtain the uploaded or stored radar stream from the compromised sensing terminal, rather than deploy an additional radar to sense the room.

2) Attacker Capability: We consider a terminal-side data leakage threat, where the attacker obtains radar streams from a compromised sensing terminal or its storage. Such leakage may result from malware, a backdoor, or unauthorized data access. Terminal compromise itself is outside the scope of this work, which instead focuses on protecting occupancy privacy after radar stream leakage. The attacker is assumed to know the radar parameters and the building structure as prior knowledge for occupancy inference. Scarecrow is placed before the compromised terminal in the radar data pipeline, so the stream accessible to the attacker has already been modified. The attacker cannot access or tamper with the radar front-end or the Scarecrow module.

3) Attacker Strategy: We consider the following three levels of strategies employed by the attacker.

Naive detection: The attacker obtains spatial point clouds through signal processing and determines the human presence based on the clustering results.

Completeness assessment: The attacker performs multi-dimensional sensing computations on the detected target, including tracking for the spatial dimension, MDS analysis for the velocity dimension, and respiration measurements, to assess the completeness of the target.

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

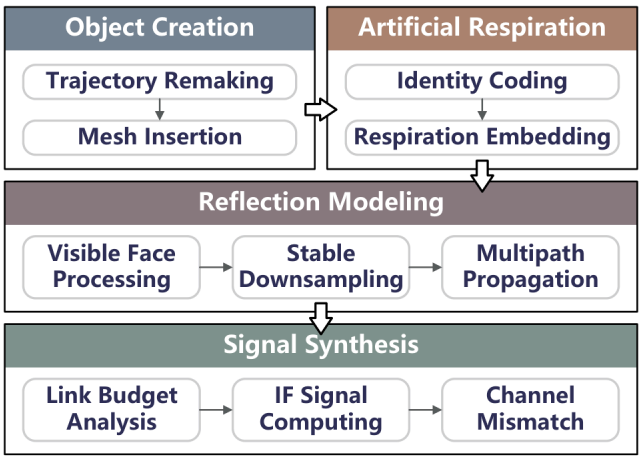


Fig. 3: Primary framework of Scarecrow.

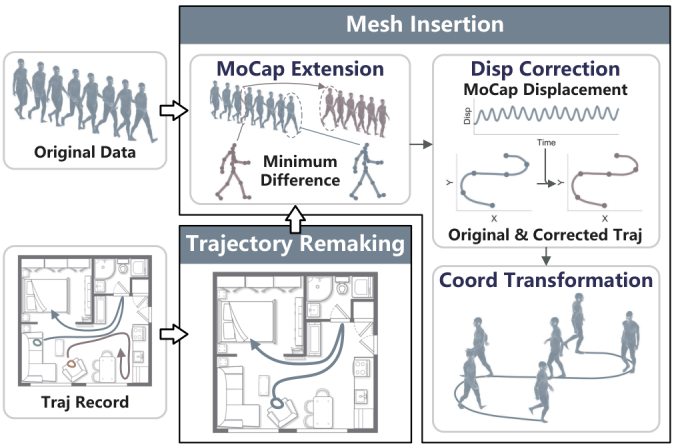


Fig. 4: Overview of object creation.

Authenticity assessment: Furthermore, the attacker extracts features from the sensing signatures RAM, MDS, and respiration curve, and performs anomaly detection to assess the authenticity of the sensing target.

III. Design of Scarecrow

This section introduces the design of Scarecrow, a forgery-embedding mmWave radar signal synthesis system for data layer occupancy spoofing.

A. System Overview

The primary framework of the Scarecrow system is shown in Fig. 3, which consists of the following four modules.

1) Forgery Object Creation: Scarecrow utilizes the users' location history to generate moving trajectories, based on which the human meshes are integrated into the environment to initially create the forgery object.

2) Artificial Respiration Embedding: Then, we generate respiration curves and covertly embed identity codes into them, and incorporate them into the human mesh by manipulating the displacement of the torso vertices.

3) Reflection Modeling: Next, we refine the human body mesh from the radar's perspective and model the multipath reflection to obtain all reflection points for signal synthesis.

4) Signal Synthesis: Finally, we incorporate the link budget and channel mismatches, and compute the IF signals from the established reflection points.

B. Forgery Object Creation

In this section, we generate moving trajectories and subsequently insert the human model to preliminarily create the virtual human object, as illustrated in Fig. 4.

1) Trajectory Remaking: The forgery's trajectory should bear a resemblance to historical trajectories while maintaining its uniqueness. First, the forged trajectories should not simply be a replay of historical trajectories since human actions cannot be entirely replicated. Next, the trajectories must conform to the room structure. Furthermore, the person's behavior adheres to certain patterns, such as extended periods of sitting on a sofa, a single round trip between the bedroom and restroom, and frequent short-distance movements within the kitchen. Considering the above requirements, we propose trajectory remaking, which is a limited replay and modification of historical trajectories. In implementation, Scarecrow first randomly selects one historical trajectory and copies its frames sequentially. Every k frames, it decides whether to jump with probability $(n_{rep}/N_{rep})^2$, where n_{rep} is the current number of consecutively copied frames and N_{rep} controls the upper limit of consecutive copying. If a jump is triggered or the selected historical trajectory reaches its end, Scarecrow treats frames in other historical trajectories as candidate connection points, selects the one closest to the current endpoint, and continues copying from that frame. Here, k determines how often Scarecrow evaluates a trajectory switch, while N_{rep} controls how long a historical segment can be continuously reused. The quadratic probability keeps the jump chance low at the beginning of a segment and increases it as repeated frames accumulate, preserving short-term motion continuity while preventing long consecutive reuse of the same historical segment. In this way, we have the forged trajectories that are consistent in both appearance and behavior with the real ones.

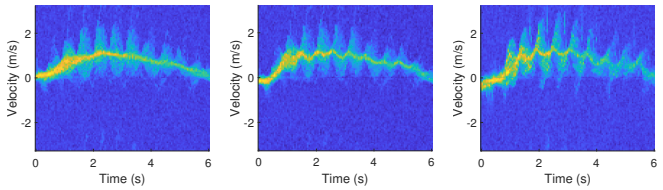
2) Mesh Insertion: With a forged trajectory, we can insert human meshes with various actions. In this study, we consider two actions, walking for RAM and MDS measurement and sitting for respiration measurement.

MoCap data extension: The MoCap data may have a short duration and need to be extended to cover a trajectory segment. When the data reaches its end, we extract the joint coordinates $\mathbf{J}_{end}$ in the body coordinate system. Then, we calculate the Euclidean distance $\sum_{n_{jt}=1}^{N_{jt}} \left\|\mathbf{J}_{i,n_{jt}} - \mathbf{J}_{end,n_{jt}}\right\|_2$ between $\mathbf{J}_{end}$ and the joint coordinates $\mathbf{J}_i$ from the frames in the beginning part of the data, where i, n_{jt}, and N_{jt} are the frame index, joint index and number of joints, respectively. The frame with the smallest Euclidean distance will be selected as the new start. The global translations and orientations of the new data will be connected to the old data by coordinate transformation. This extension can be performed in advance on the MoCap dataset to prepare sufficient data for forging.

Displacement correction: The human velocity has inherent

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



(a) w/o correction (b) w/ correction (c) Genuine reference

Fig. 5: Effect of displacement correction on velocity signature.

characteristics. Taking the MDS shown in Fig. 5c as an example, the highlighted line represents the velocity of the torso, exhibiting a fast-slow periodicity according to the gait. The secondary highlighted shadow represents the motion of the limbs, which also matches the gait. However, when the human model is placed on another trajectory, its inter-frame displacement is modified, resulting in the disruption of torso velocity. Depending on the degree of smoothing applied to the trajectory, the body's gait is either eliminated or replaced with the gait of the trajectory. In either case, it fails to form an authentic velocity signature along with the limbs' motions. For example, in Fig. 5a, we can see the swinging of the limbs, but the torso does not show a corresponding movement—it is more like the target is "sliding" rather than walking, which is obviously weird. To solve this, we propose displacement correction. The velocity changes of the torso can be accurately reflected in the cumulative displacement record. Therefore, we first calculate the cumulative displacements of the MoCap trajectory and the forged trajectory. Then, the two cumulative displacement sequences are normalized into progress sequences from 0 to 100%. Using the normalized MoCap displacement sequence as the progress reference, Scarecrow interpolates the positions on the forged trajectory at the corresponding progress values. In this way, the forged path keeps its spatial shape, while its frame-by-frame displacement follows the gait-related displacement pattern of the MoCap data. Consequently, the MoCap mesh walks along the forged trajectory while retaining its inherent gait, as showcased in Fig. 5b. Then, we calculate the trajectory's orientation and perform a coordinate transformation to complete the creation of the human object.

C. Artificial Respiration Embedding

This section endows the human object with the respiration signature and proposes an identity coding mechanism based on the respiration cycle duration, as shown in Fig. 6.

1) Respiration Embedding: The addition of the respiration signature requires designs in two aspects: generating a respiration curve and embedding this curve into the human mesh.

Respiration curve generation: The forged respiration curve must conform to the real respiration pattern, therefore the ideal way would be to directly replicate the real respiration curves. However, due to the limited amount of real data, forged curves are inevitably subject to repetition. Therefore, Scarecrow first divides real respiration curves at adjacent troughs and stores the resulting single-cycle segments in a

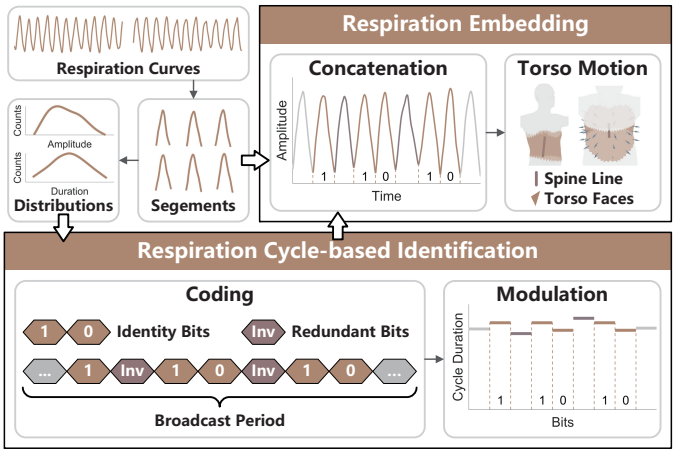


Fig. 6: Overview of artificial respiration.

segment library. Each segment is normalized as a reusable displacement profile, while its original amplitude and duration are recorded. For a respiration recording, the amplitudes and durations of its constituent cycles form empirical distributions $\mathcal{D}_A$ and $\mathcal{D}_T$, respectively. These distributions are then used to determine the amplitude and duration of each forged cycle. Scarecrow first selects a normalized segment from the library, then samples an amplitude $A \sim \mathcal{D}_A$ and a duration $T \sim \mathcal{D}_T$, and rescales the segment in amplitude and time to match A and T, respectively. Adjacent segments are concatenated by sharing endpoints to keep the curve continuous. Finally, we compute a local baseline for the concatenated curve using a 3s moving-average window and subtract it from the curve to remove the low-frequency drift introduced by segment concatenation.

Torso vertex expansion and contraction: Next, we simulate the respiration-induced expansion and contraction of the torso, especially the chest and abdomen, in the human mesh. We choose the body parts "spine" and "spine1" [21] of the SMPL model to represent the torso, and use the line passing through skeleton joints "spine1" and "spine3" as the torso axis. For each torso vertex, Scarecrow projects the vertex onto the torso axis and uses the vector from the projected point to the vertex as its expansion direction. At each frame, the forged respiration curve determines the displacement along this direction, so the torso vertices move inward and outward with respiration. However, on the one hand, there are differences between the movement directions of the vertices and the incident direction of the radar signal. On the other hand, radar reflection signals are the vector superposition of reflection signals from multiple vertices. Therefore, the respiration amplitude measured by radar is usually smaller than the input amplitude. To solve this problem, we multiply the input amplitude by a coefficient to make the radar measured amplitude close to the original value, and experimentally set the coefficient to $1.1\times$. As a result, performing respiration measurements on the synthesized signal yields a respiration curve that is faithful to the forged curve, as shown in Fig. 7.

2) Respiration Cycle-based Identification: The interference caused by forgery affects not only attackers but also trusted

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

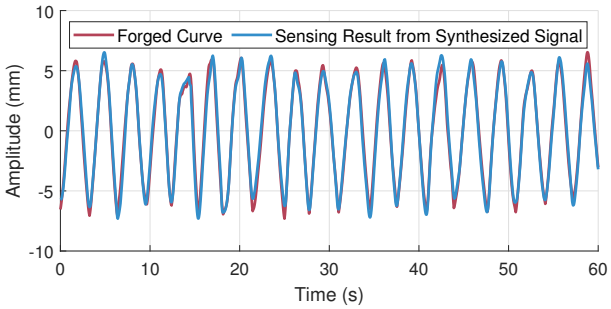


Fig. 7: Forged curve and sensing result.

sensing terminals. If trusted terminals cannot distinguish forged targets from real targets, they may make sensing and control decisions based on forgeries, leading to resource wastage or even risks in smart-home systems. For example, a terminal may adjust the air conditioner based on a forged location or activate kitchen devices according to forged gestures. Thus, a covert and effective identification mechanism would be highly beneficial. We find that the periodic respiration curve is well suited for information modulation.

Modulation: As a signal waveform, the respiration curve's frequency is low, making it unsuitable as a carrier and better suited for direct digital modulations. Among them, amplitude modulation is unreliable because the measured amplitude is affected by body fluctuation, signal superposition, and noise. Phase modulation disrupts the continuity of the respiration profile. In contrast, the measurement of respiration frequency is generally accurate, and the frequency modulation preserves the continuity of the profile. Moreover, as the actual respiration frequency of a human is continuously changing, modulation in frequency is less perceptible. Therefore, we adopt frequency modulation as the modulation manner. Specifically, each respiration cycle corresponds to one bit, and the cycle duration represents the frequency. Using troughs as triggers, this modulation naturally supports time synchronization. Trusted terminals can then perform respiration sensing and decode cycle durations into identity codes according to the pre-informed settings. In this way, accurate identity code detection allows trusted terminals to ignore forged targets and avoid interference with legitimate sensing services.

Coding & identification: In the choice of coding manner, we consider the following facts: (1) Given the low respiration frequency, it is desirable to minimize the bit requirements. (2) Considering the need to reduce detectability, the identity code should occupy only a small portion with a random position in a broadcast period, hence the channel coding is of little help. (3) The identity code is short and does not require source coding compression. Therefore, we adopt the simple non-return-to-zero (NRZ) scheme, whose signal level does not change when transmitting each information bit. Therefore, each bit of the identity code can be directly modulated to the corresponding frequency. Our identity code scheme consists of three types of bits/levels. Based on a time tolerance, specific cycle durations represent `0` or `1`, while other durations are considered `invalid`. To reduce the repetitiveness of the identity code and counter attackers' attempts to infer it by recording respiration cycles, we have implemented two measures. First, the identity code sequence appears infrequently and unpredictably. With an N_{id}-bit length, it appears at a random position within each broadcast period, and occupies only a small portion of each broadcasting period. The duration of non-identity bits in a broadcast period obeys the preset respiration frequency distribution. Second, the identity code is embedded with redundant bits so that the sequence of cycles is different for each occurrence. In each occurrence, we insert $N_{rdn} = \lceil N_{id}/3 \rceil$ bits of `invalid` at its random gaps, so that the code differs in its frequency sequence at each occurrence. The trusted terminal clips the decoding result with a sliding window of $(N_{id} + N_{rdn})$-bit length and 1-bit step, retains the `0` and `1` bits, and then compares it with the pre-informed identity code to distinguish between real and forged targets. Respiration decoding during walking is indeed challenging, but the identity code does not need to be decoded continuously from moving targets. The goal of the identity code scheme is to recognize forged targets and prevent them from affecting the sensing system. It is not used to authenticate real users. Therefore, even if a real user has no sufficiently long stationary period for respiration decoding, normal sensing applications can still proceed. For forged targets, Scarecrow can ensure sufficiently long stationary segments in their trajectories. Since radar sensing systems can continuously track a target, once a trusted terminal identifies a forgery during such a segment, this identification result can persist as the target moves. Therefore, the identity code scheme can work over a long period as long as the forged trajectory contains such stationary segments.

D. Reflection Modeling

After completing all the modifications to the human mesh, we improve the mesh from the perspective of radar detection and model the environmental reflection to obtain all reflection points for signal synthesis, as illustrated in Fig. 8.

1) Visible Face Processing: Based on the radar viewpoint, the occluded triangular faces in corresponding human body meshes can be removed. We use the hidden point removal algorithm [22] to obtain visible points and consider faces containing at least two visible points as visible faces. The larger the area of a face, and the closer the normal vector is to the direction of viewpoint, the stronger the reflection strength, therefore the RCS coefficient for each visible face is calculated by $\sigma = \varsigma \cos^2 \gamma$, where ς is the face's area and γ is the angle between the vector from the face's centroid to the viewpoint and the face's normal vector.

2) Stable Downsampling: The human mesh model contains thousands of faces, and performing calculations for all faces would be computationally burdensome and unnecessary. Therefore, downsampling is required. Signal synthesis is the process of simulating the reflection of an infinite number of real "points" with a finite number of reflection points. Therefore, the reflection points must be relatively fixed to ensure that the time-domain signals have a correct and stable continuity relationship on long-time signatures such as the MDS and respiration curve. This requires that the number of downsampled reflection points and their positions on the

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

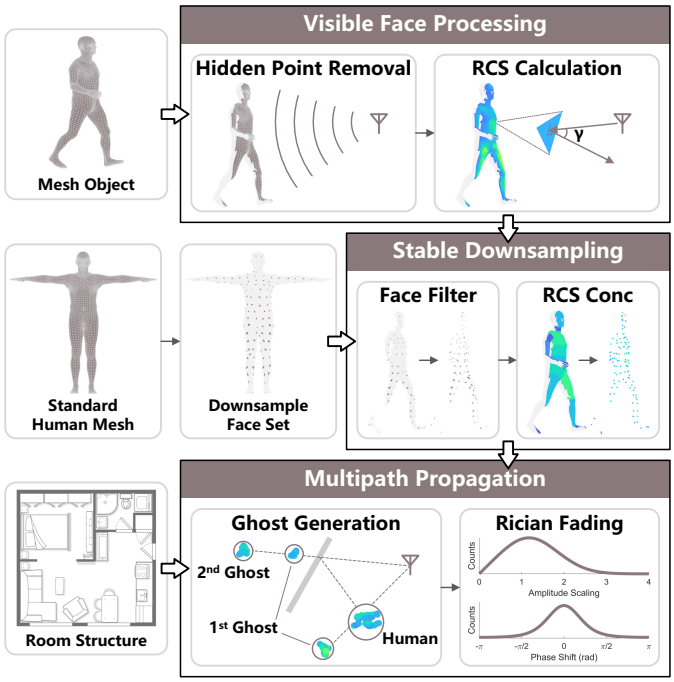


Fig. 8: Overview of reflection modeling.

body should be as stable as possible. To achieve this, we first perform box grid-based downsampling on the standard SMPL mesh, which provides a more spatially uniform description of the human body. Next, each downsampled coordinate is mapped to the nearest triangular face, and the index set of the latter is called downsample indices. The downsample indices generated from the standard SMPL mesh guarantee that regardless of the location and posture of the forged human object, its downsampled reflection surfaces are in the same set, ensuring the stability of the reflection points used for signal synthesis in terms of position and quantity. For each visible mesh, we keep only the faces that belong to the downsample indices. Meanwhile, we perform RCS concentration. The RCS of visible faces is transferred to the corresponding downsampled faces based on body parts by $\sigma' = \sigma\left(\sum_{n_{raw}=1}^{N_{raw}}\sigma_{n_{raw}}/\sum_{n_{ds}=1}^{N_{ds}}\sigma_{n_{ds}}\right)$, where σ and σ' represent the RCS of the downsampled face before and after concentration, and N_{raw} and N_{ds} are the number of visible faces and visible downsampled faces for that body part. This concentration preserves the total visible RCS of each body part after downsampling. In other words, downsampling reduces the number of reflection faces, while the RCS contribution of discarded faces is redistributed to retained faces of the same body part. In this way, the fluctuation and instability of the reflection object can be avoided while downsampling.

3) Multipath Propagation: In the signal propagation, apart from the line-of-sight (LoS) path, reflective objects such as walls and floors give rise to the non-line-of-sight (NLoS) paths [23], [24], leading to the so-called ghosts as depicted in Fig. 9d. A synthesized signal lacking this component is spatially inconsistent, as shown in Fig. 9a. For each main planar reflector, such as a wall or floor, Scarecrow uses specular reflection geometry to find the reflection point for the radar-body path. Treating this reflection point as the NLoS viewpoint, Scarecrow performs visible-face extraction and downsampling on the human mesh to obtain ghost reflection faces. The centers and RCS values of these faces are then used to derive first-order and second-order ghost reflection points and amplitudes. In addition, the real propagation environment includes scattering, diffraction, and high-order reflections from various reflectors. When a LoS path is unoccluded, its propagation undergoes Rician fading. We now refer to reflections from main surfaces such as walls as main NLoS reflections, which in reality exhibit strong instability, and face a more complex reflection environment, thus being significantly affected by the Rician fading. In other words, the main NLoS paths undergo Rician fading, with their amplitude scaling and phase shifting following a Rician distribution and an approximate Gaussian distribution, respectively. We enhance the realism of multipath propagation by applying Rician fading to ghost points during signal synthesis. In the Rician fading model, the K-factor is used to describe the ratio of the signal strengths of the main path to the scattering paths [25]. We record the signal strength ratio between the human body and the ghost in the real signal. Based on this ratio, we adjust the K-factor until the ratio in the generated signal matches that of the real signal, and finally conclude that a K-factor of 3dB can make the ghost conform to the real attenuation. Therefore, this K-factor is a site-specific calibration value, and it can be re-tuned when the environment changes. As a result, a self-consistent multipath effect is added to the synthesized signal, as shown in Fig. 9c.

E. Signal Synthesis

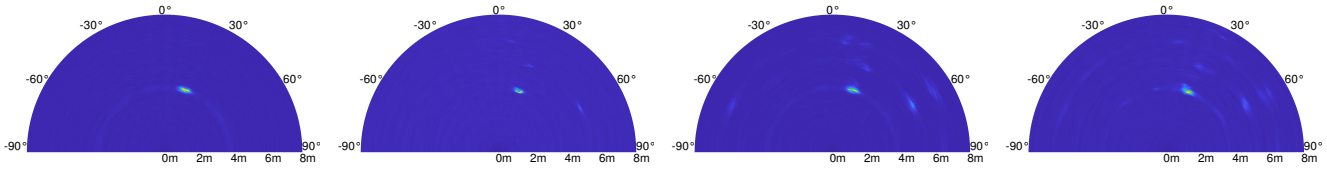
This section simulates the propagation of signal waves and the electromagnetic characteristics of the device to finally obtain the synthesized signal.

1) Link Budget Analysis: The signal is transmitted from the Tx antenna with a preset transmit power, reflected by the object, and received by the Rx antenna. The amplitude coefficient can be expressed by $\alpha = \sqrt{LG\sigma}$, where L and G represent the attenuation factor and antenna gain, respectively. In free space, L covers only the path loss [26], then $L = \left(\frac{\lambda}{(4\pi)^{1.5}D^2}\right)^2$ [27]. When considering the absorption, diffraction, and scattering of electromagnetic waves by the human body, we need to add the shadow fading. In this case, L is rewritten as $L = \left(\frac{\lambda}{(4\pi)^{1.5}D^2}\right)^{\mu}$, and we empirically set the fading factor $\mu = 3.2$. The antenna gain $G = G_tG_r$, where G_t and G_r denote the gains of the Tx and Rx antennas, which can be obtained by referring to datasheets [28]. Since the link budget changes very little within a frame, we calculate it once per frame and apply it to all chirps and channels.

2) Signal Computing: With the positions and amplitude coefficients of reflection points, we can now proceed with the signal computation. Given a Tx-Rx channel and a reflection point, the propagation delay is calculated as $\tau = (D_t + D_r)/c$, where D_t and D_r are the distances from the Tx and Rx to the reflection point. Given the ADC start time t_s, sampling index n_s, and sampling rate f_s, the ADC sampling time slots can be calculated by $t = t_s + n_s/f_s$. Then, the IF signal can be calculated using Eqs. 1 and 2. Eventually, through matrix

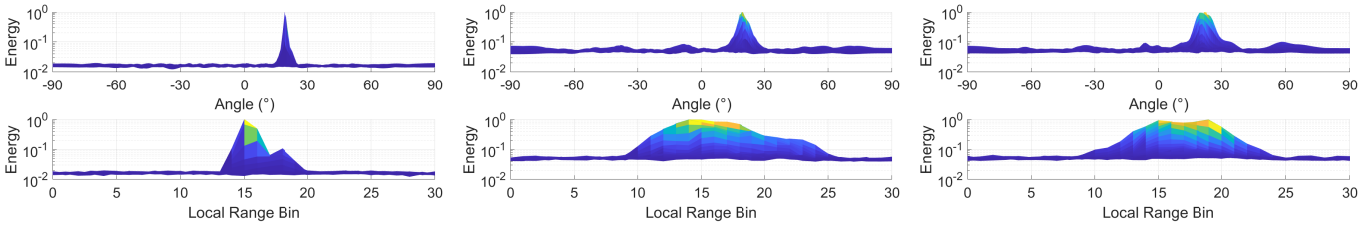
Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



(a) w/o multipath propagation (b) w/o channel mismatch (c) w/ both (d) Genuine reference

Fig. 9: Influence of multipath propagation and channel mismatch on RAM.



(a) w/o channel mismatch (b) w/ channel mismatch (c) Genuine reference

Fig. 10: Simulating the spatial energy leakage caused by channel mismatch.

operations and parallel computation, the IF signals for each chirp of each channel are obtained, which can be directly superimposed into the ADC data stream of the real signal.

3) Channel Mismatch: It is necessary to simulate the measurement errors caused by the electromagnetic characteristics of the radar device, particularly the channel mismatch in the MIMO array. Channel mismatch refers to the difference in frequency response between Tx-Rx channels, which will cause the actual behavior of the array to deviate from the theoretical model, resulting in a reduction in overall array performance. The mismatches can arise from various reasons, such as path length mismatch, chip-to-chip variation, antenna coupling, and phase center deviation [29], [30]. As a result of these mismatches, we encounter amplitude differences ε_a and phase offsets ε_p between channels. Besides, variations in mixing and ADC sampling can introduce frequency mismatches, which can be modeled as ranging errors. One significant consequence of channel mismatch is spatial energy leakage, which can be observed in Figs. 9d and 10c. Without accounting for this effect, energy tends to become overly concentrated around the reflection object, as demonstrated in Figs. 9b and 10a. Scarecrow simulates this energy leakage by introducing amplitude, phase, and frequency mismatches in the signal synthesis, resulting in a more realistic spatial spectrum, as shown in Figs. 9c and 10b. Let the ranging error be ϵ_r, then the frequency error is given by $\varepsilon_{f,n_s} = 2\pi\varepsilon_r n_s/N_s$, where n_s and N_s represent the sampling index and the number of samples. Following these hardware sources, Scarecrow models channel mismatch as a per-channel complex gain together with a range-dependent phase term. The complex gain represents the amplitude imbalance and static phase offset across channels, while the range-dependent phase term represents the effective ranging error caused by frequency-related offsets. The empirical distributions specify the magnitude of these hardware-related errors, so that the synthesized spatial spectrum exhibits energy leakage similar to real radar measurements. In our evaluation, the default channel mismatch terms are independently sampled as $\varepsilon_a \sim \mathcal{N}(1, 0.1^2)$, $\varepsilon_p \sim \mathcal{N}(0, 0.15^2)$ radians, and $\varepsilon_r \sim \mathcal{N}(0, 0.2^2)$ bins. For a different radar platform, these magnitudes can be re-tuned from calibration measurements without changing the mismatch model. For each Tx-Rx channel, Scarecrow combines the corresponding Tx-side and Rx-side error terms to obtain the channel-specific mismatch. Then, for the synthesized IF signal $\mathbf{s} = [s_1, \cdots, s_{N_s}]$ of a channel, the channel mismatch is introduced by $\mathbf{s}' = \left(\varepsilon_a \exp\left(j\left(\varepsilon_p + 2\pi\varepsilon_r\left[1, \cdots, N_s\right]/N_s\right)\right)\right) \odot \mathbf{s}$, where $\odot$ denotes element-wise multiplication.

IV. Performance Evaluation

In this section, we conduct extensive experiments to comprehensively evaluate the Scarecrow system. Each participant is fully informed about the experimental content and purpose.

A. Experimental Setup

The evaluation contains three parts, respectively verifying the fidelity, verisimilitude, and identifiability of the Scarecrow system.

Fidelity: Refers to the extent to which the synthesized signal accurately reproduces the desired content. This part is to verify whether the signatures of the synthesized signal align with the expectations, and whether the correct human sensing results can be obtained from the synthesized signal.

Verisimilitude: Refers to the degree of similarity between synthesized signals and real signals. This part aims to evaluate the camouflage effectiveness of forgeries when facing anomaly detection performed by attackers.

Identifiability: This part evaluates whether trusted terminals can distinguish forgeries and whether they may mistakenly identify real targets as forgeries.

To make the evaluation criteria and references explicit, Table I summarizes the evaluation part, task, metric, and ground

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

TABLE I: Summary of Evaluation Metrics and References

Part	Task	Metric	Ground Truth/Reference Source
Fidelity	Tracking	Position/Range/Angle Errors	Preset trajectories used for human-model placement
	MDS Analysis	Spectrum SSIM/IoU Velocity RMSE Cadence Error	MDSs computed directly from inserted human meshes, with velocity and cadence extracted from the MDSs
	Respiration Measurement	Curve RMSE/DTW/CS Trough Error	Generated respiration curves and their trough times
	Trajectory Remaking	Normalized FID	Self-collected real trajectories used as the reference distribution for normalized FID
Verisimilitude	Anomaly Detection	Recall/Precision AUC	Labels assigned by data source, including real data, Scarecrow forgeries, and baseline forgeries (True: forged, False: real)
Identifiability	Bit Decoding	BSR	Preset identity codes embedded before respiration synthesis
	Forgery Identification	TPR/TNR	Labels of respiration signals observed from forged and real targets (True: forged, False: real)

TABLE II: Grouped Definitions of Evaluation Metrics

Category	Definitions (hatted and unhatted quantities denote estimates and references, respectively)
Error	Range, angle, cadence, and trough errors follow $e_i = \lvert\hat{z}_i - z_i\rvert$. Position error $e_i^{\text{pos}} = \lVert\hat{\mathbf{p}}_i - \mathbf{p}_i\rVert_2$. Velocity and curve RMSE follow $\text{RMSE} = \sqrt{\sum_{i=1}^{N}(\hat{z}_i - z_i)^2/N}$.
Similarity	Spectrum SSIM follows [31]. $\text{IoU} = \lvert A \cap \hat{A}\rvert / \lvert A \cup \hat{A}\rvert$. Curve DTW follows [32]. $\text{CS} = \mathbf{x}^T\hat{\mathbf{x}}/(\lVert\mathbf{x}\rVert_2\lVert\hat{\mathbf{x}}\rVert_2)$.
Distribution	Normalized FID $= \text{FID}/\text{FID}_{\text{real}}$, where FID follows [33] and FID_{real} is the real-trajectory FID baseline.
Classification	Recall, precision, AUC, TPR, and TNR follow [34]. $\text{BSR} = N_{\text{correct}}/N_{\text{bits}}$.

truth/reference source for each evaluation item. The corresponding mathematical definitions are grouped by computation form in Table II.

1) Hardware & Software: The evaluation follows the deployment pipeline of radar front-end, Scarecrow, and sensing terminal. The TI MMWCAS-RF-EVM [28] serves as the radar front-end, with chips #1 and #4 enabled, providing 6Tx and 8Rx channels. The radar parameters are listed in Table III. This physical radar is used to collect real radar streams, including walking, respiration, and empty-room signals. Scarecrow is implemented as a software prototype in MATLAB 2024b and synthesizes forged streams with the same format and radar parameters as the collected ADC stream. It then superimposes the forged stream with the collected empty-room stream, producing the radar stream that would be delivered to the sensing terminal after Scarecrow processing. The sensing-terminal processing is also implemented in MATLAB 2024b, taking the resulting stream as input for tracking, MDS analysis, respiration measurement, anomaly detection, and identity decoding. In our prototype evaluation, the Scarecrow module and the sensing-terminal processing run on the same workstation. In practical deployment, Scarecrow can run as a separate module between signal sampling and data uploading.

2) Real Data Collection: We collect real signals of walking and respiration scenarios, with the former used for evaluation in spatial and velocity dimensions, and the latter for respiration-related evaluation. In the prototype implementation of the Scarecrow system, the utilized data elements can be classified into two categories. (1) Open-source dataset: We obtain walking MoCap data, the corresponding SMPL parameters, and the standard SMPL mesh, from [35]. Some of the respiration-related experiments use respiration curves obtained from [36]. (2) Self-collected/historical data: We collect users' historical trajectories and respiration curves through experiments, which are employed for trajectory remaking and artificial respiration embedding, respectively. Additionally, signals of the unoccupied room are also collected to superimpose with the synthesized signals.

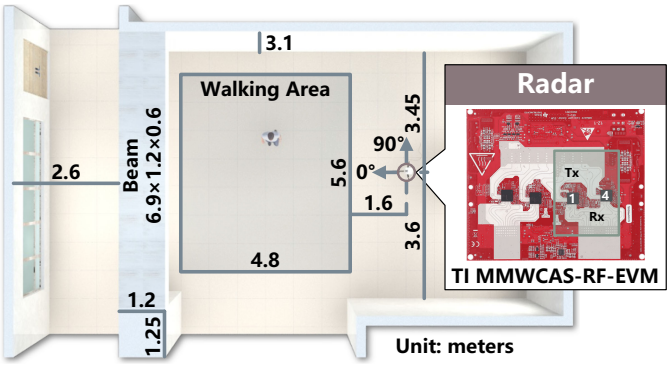


Fig. 11: Environment of the real data collection.

Walking: The experiment is conducted in an indoor environment, the room structure of which is shown in Fig. 11.

3) Evaluation Strategy: The participants walk freely within an area of 4.8m×5.6m. Ten participants are involved, each

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

TABLE III: mmWave Radar Parameters

Start Freq	Slope	Smp Rate	Smp Num	Chirp Period	Chirp Num	Frm Period
77GHz	99MHz/us	7.04MHz	256	50us×6Tx	128×6Tx	50ms

TABLE IV: Fidelity Evaluation on Tracking

Metric	Position Error (m)	Range Error (m)	Angle Error (°)
Mean	0.0609	0.0413	0.5127
Std	0.0300	0.0298	0.4228

TABLE V: Fidelity Evaluation on MDS Analysis

Metric	Spectrum SSIM	Spectrum IoU	Velocity RMSE (m/s)	Cadence Error (Hz)
Mean	0.8861	0.8898	0.0451	0.0497
Std	0.0324	0.0180	0.0090	0.0620

collecting 20 times for 10s (*i.e.* 200 frames), resulting in a dataset of 200×10s.

Respiration: The signals are collected from 10 participants while sitting, each collecting 20 times for 60s (*i.e.* 1200 frames). Among them, 10 collections are of normal respiration, 5 of deep respiration, and 5 of pant respiration.

B. Fidelity Evaluation

This section evaluates the consistency between sensing signatures of synthesized signals and the expectations, and verifies whether accurate human sensing results can be obtained from the synthesized signal. We employ tracking, MDS analysis, and respiration measurement as typical applications of mmWave signals in the spatial dimension, velocity dimension, and vital sign detection.

1) Fidelity in Tracking: In Scarecrow, a human body model is placed on a predefined trajectory. Here, we evaluate whether the synthesized signals adhere to the predetermined positions. We synthesize signals using 200 trajectories of real data as a preset, and then perform a standard tracking process [23] on the synthesized signal. We count the differences between the tracking results and the preset trajectories in terms of position, range, and angle in Table IV. The centimeter-level range error and the sub-1° angle error are negligible in human localization.

2) Fidelity in MDS Analysis: The analysis of MDS is crucial for motion sensing such as gait measurement and activity recognition. We generate 200 MDSs from the signals synthesized in the tracking evaluation. Additionally, we directly compute MDSs using the human meshes [17] for comparison purposes. We compare the structural similarity (SSIM) between the two spectrums and then evaluate their intersection over union (IoU) after performing adaptive binarization. Meanwhile, we measure the velocity and cadence from the two spectrums and obtain the velocity root mean square error (RMSE) and cadence error. The results, as shown in Table V, demonstrate the high fidelity of the forgery's velocity signature.

3) Fidelity in Respiration Measurement: We conduct respiration measurements on 1000 synthesized signals, each lasting 60s, to verify their fidelity to the forged respiration curves. Since the radial fluctuation may differ from the actual fluctuation, both curves are normalized before comparison. Table VI counts the RMSE, dynamic time warping (DTW) distance, and cosine similarity (CS) of the curves, which indicates a remarkably high level of consistency. In addition, we calculate the time error of the curve trough, which has a mean value of 0.0267s. Such a small error not only guarantees the fidelity of the respiration signature, but more importantly ensures the decoding accuracy in our proposed respiration cycle-based identification mechanism.

TABLE VI: Fidelity Evaluation on Respiration Measurement

Metric	Curve RMSE	Curve DTW	Curve CS	Trough Error (s)
Mean	0.0609	0.0213	0.9931	0.0267
Std	0.0163	0.0056	0.0043	0.0066

4) Performance of Trajectory Remaking: Scarecrow remakes the historical trajectories to generate the trajectories of forged targets. Fig. 12a shows an example. We employ the Fréchet inception distance (FID) used by RF-Protect [5] to evaluate the generated trajectories and compare it with the results from the literature. In the experiment, N_{rep} is set to 500, and Scarecrow makes a jump determination every 10 frames. During the 200 frames, the minimum, maximum, and average jump counts are 1, 4, and 1.41, respectively. The FID results are normalized based on the results of the real trajectories, thus the closer the FID is to 1, the more realistic the generated trajectory is. As shown in Fig. 12b, Scarecrow achieves an FID of 1.14, which not only significantly outperforms the random movement score of 3.44 but also surpasses the 1.23 of RF-Protect that employs a conditional generative adversarial network (cGAN). This is because the essence of trajectory remaking is replay with randomness. The approaches that incorporate repetition are more reasonable, as user behavior habits result in a high degree of similarity between their natural trajectories and historical ones. The advantage of trajectory remaking is that it allows the generated trajectories to be more aligned with user habits while avoiding monotonous repetition.

C. Verisimilitude Evaluation

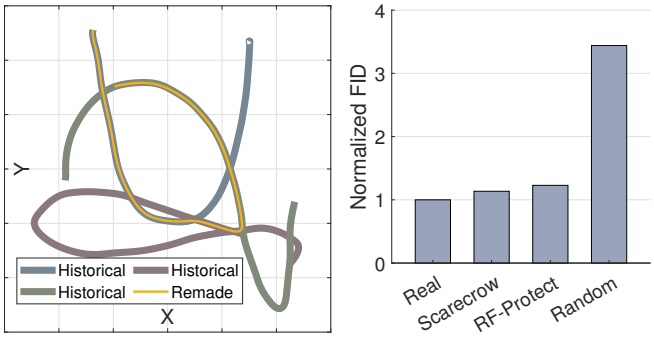
This section evaluates the forgery's ability to evade anomaly detection. We employ the RAM, MDS, and respiration curve as sensing signatures to be evaluated.

1) Discriminators: We use three anomaly detection algorithms, including isolation forest (iForest), local outlier factor (LOF), and one-class support vector machine (OCSVM), as discriminators of real and forged targets. In each evaluation, we first compare the performance of the discriminators and then select the optimal one for the remaining sub-evaluations.

2) Metrics: In this evaluation, we prioritize the following three metrics. Note that the positive and negative classes refer to forged and real targets, respectively. From the attacker's view, classifying a forged target as forged means that the camouflage is detected, while classifying it as real means that the forgery evades the discriminator. (1) Recall: the rate of

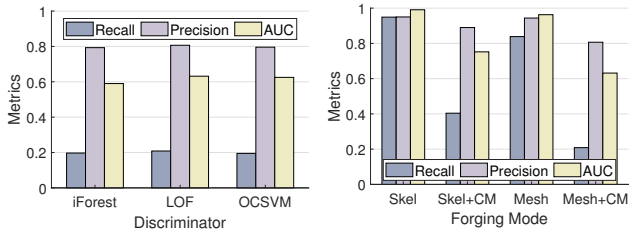
Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



(a) Remade trajectory. (b) FID results.

Fig. 12: Performance of trajectory remaking.



(a) (b)

Fig. 13: Verisimilitude evaluation on local RAM.

forged targets being classified as forged. This metric reflects the ability of the discriminator to identify forged targets. A lower recall therefore means that more forged targets evade detection, but recall alone is insufficient because the discriminator can raise recall by labeling more samples as forged. (2) Precision: the ratio of forged targets among all the targets classified as forged. Precision checks this trade-off by measuring whether the samples predicted as forged are truly forged. The recall and precision range from 0 to 1. When comparing two discriminators, if the recall and precision of one discriminator are both closer to 1, then its discriminative ability is often stronger. However, if one of recall and precision is higher and the other is lower, we cannot directly judge the discriminator performance. Therefore, we introduce a comprehensive metric for evaluating the performance of a discriminator. (3) Area under the receiver operating characteristic curve (AUC): the AUC comprehensively assesses the discriminators' ability to distinguish between positive and negative classes, ranging from 0.5 to 1. Values closer to 1 indicate better discrimination performance, while 0.5 corresponds to the random-guessing level. For the same discriminator, an AUC closer to 0.5 suggests stronger camouflage of the forged data. Since Scarecrow aims to make forged signatures hard to distinguish from real ones, we interpret AUC from the attacker's discrimination capability rather than from the defender's classification accuracy. A common rule of thumb regards AUC values below 0.7 as poor discrimination [37], which means that such an attacker-side discriminator cannot reliably distinguish forged signatures from real ones. In this paper, the discrimination and forging performance are evaluated with AUC as the core metric, and recall and precision as references.

3) Comparative Methods: To our knowledge, there is a lack of signal synthesis research that focuses on occupancy spoofing. Existing mmWave signal synthesis studies are mainly designed for sensing-data augmentation. Therefore, their original pipelines cannot be directly used as occupancy-spoofing baselines, because they do not generate a complete forged stream with trajectory remaking, vital signs, multipath propagation, and channel mismatch. Instead, we adapt two representative human modeling strategies for controlled comparison: the mesh-based modeling in mmGPE [16] and the skeleton-based modeling in SynMotion [18]. The *Mesh* baseline follows the mesh-based modeling of mmGPE by using the same SMPL-based human object as Scarecrow and the basic signal synthesis pipeline. It is the main ablation reference for evaluating Scarecrow-specific modules such as channel mismatch, multipath propagation, and displacement correction. The *Skel* baseline replaces the mesh object with skeleton-based modeling following SynMotion's reflection point interpolation and RCS calculation. It provides a comparison for human reflection modeling under the same evaluation protocol. For fairness, all compared variants use the same radar configuration, walking trajectories, sample construction, feature extraction, train-test split, and anomaly discriminators whenever applicable.

4) Verisimilitude of Local RAM: **Data and features:** We evenly extract 10 frames from each walking recording and obtain 200×10=2000 real RAMs, of which 80% are used for training and 20% for testing. Meanwhile, each real trajectory is used for one signal synthesis, from which 10 frames are extracted to form a total of 2000 forged RAMs. Since human sensing often first extracts signals from the user's spatial surroundings, and to better evaluate the reflection simulation of humans and environments separately, the RAMs are divided into two forms: local and global. We focus the RAM on the ranges where the target is located as the local RAM, which contains 31 range bins (≈1.29m) and 181 angle bins (-90°:1°:90°). The data features are the local binary pattern (LBP) features, and the contrast, correlation, energy, and homogeneity of the gray-level co-occurrence matrix (GLCM).

Discriminator selection: According to the results in Fig. 13a, the three algorithms perform similarly, and we choose the LOF with the highest AUC of 0.6316 as the optimal discriminator for the local RAM.

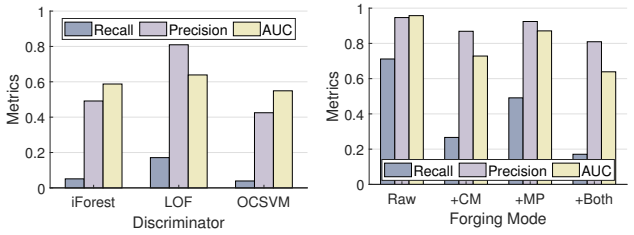
Effectiveness of channel mismatch: We now disable the channel mismatch module, and do the same for the skeleton model. The results are shown in Fig. 13b. When it is disabled, the forged RAM has poor verisimilitude, and the AUCs of the skeleton and mesh models are as high as 0.9908 and 0.9628, respectively. After enabling it, the AUCs are reduced to 0.7520 and 0.6316, respectively, which demonstrates the effectiveness and criticality of channel mismatch.

5) Verisimilitude of Global RAM: **Data and features:** The global RAM contains the full 241 effective range bins (≈10m), capturing comprehensive spatial information including environmental reflections. The features used are also LBP and GLCM properties.

Discriminator selection: As shown in Fig. 14a, the preci-

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



(a) (b)

Fig. 14: Verisimilitude evaluation on global RAM.

sion values of iForest and OCSVM are below 0.5, indicating that these methods are nearly incapable of discrimination. LOF, sensitive to density variations, demonstrates some availability and is chosen as the discriminator for global RAM.

Effectiveness of multipath propagation: To validate the effectiveness of multipath propagation (*MP*), we disable this module and observe the changes. We also control the channel mismatch to separately evaluate these two modules. Fig. 14b shows the results. Both channel mismatch and multipath propagation yield positive effects, as they reduce the raw mesh's AUC of 0.9574 to 0.7282 and 0.8709, respectively. When they are enabled together, the AUC is only 0.6388.

6) Verisimilitude of MDS: **Data and features:** From the above real and synthesized data of walking, we obtain 200×10s MDSs for each set. We slide with a window of 5s and a step of 2s to obtain 600×5s spectrums. 80% of the real spectrums are for training, and the remaining 20% for testing. In addition to using texture features LBP and GLCM, we incorporate gait features including mean cadence spectrum (mCS) [38] and its skewness, kurtosis, RMS, shape factor, and impulse factor.

Discriminator selection: The discrimination results are shown in Fig. 15a. iForest has higher recall, and OCSVM has higher precision. They have different focuses and advantages, but iForest shows higher comprehensive discrimination ability from a higher AUC and is therefore selected.

Effectiveness of displacement correction: To adapt the MoCap data with forged trajectories, we propose displacement correction (*DC*). In Fig. 15b, we disable this module on the skeleton and mesh models. The displacement-based insertion enhances the realism of both models since it preserves the inherent gait information of the MoCap data. This strategy resulted in a low AUC of 0.6338 for Scarecrow.

Influence of feature type: Fig. 15c shows the discrimination results when using texture or gait features alone, from which it can be seen that these two types of features possess similar discrimination performance. Compared to texture only, using both improves recall, precision, and AUC. Compared to gait only, using both has lower precision but higher recall and especially higher AUC. Therefore, using both performs better according to the experimental criteria. Such results prove that both Scarecrow's signal synthesis and human object creation achieve high authenticity.

Influence of MDS time span: In Fig. 15d, we vary the observation time of the MDS. The AUC of 5s is evidently higher than that of 2s, but the improvement of 8s over 5s is not significant, with an AUC of only 0.6566, which proves the reasonableness of our default experimental parameters, as well as the fact that Scarecrow achieves good verisimilitude across different time spans.

7) Verisimilitude of Respiration Curve: **Data and features:** Among the real respiration curves, 60% of the curves from 8 participants are used for training and the remaining 40%, as well as all curves from the other 2 participants, are used for testing. Scarecrow generates a respiration segment library from real curves, and synthesizes 160 signals of 60s. In addition, a segment library is obtained from the open-source dataset and 40 signals are synthesized. We follow [39] and perform sliding cropping with a 5-cycle window and a 2-cycle step. For each cropped sample, we perform 2-level wavelet packet decomposition (WPD) and extract skewness, kurtosis, RMS, shape factor, and impulse factor from each subspace and the original curve, resulting in 35 features per sample.

Discriminator selection: The performance of each discriminator is poor, as shown in Fig. 16a. Their precision values are all below 0.6, indicating that the features of forged respiration curves closely resemble the real ones. The OCSVM, which has relatively better performance with an AUC of 0.6005, is chosen as the discriminator of the respiration curve.

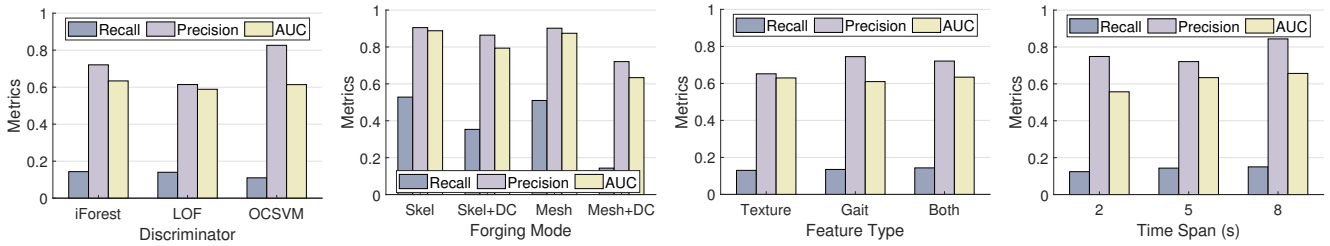
Influence of respiration segment source: The data source of the respiration segment needs to be carefully considered as it directly affects the quality and feasibility of artificial respiration. We categorize the sources into the following three groups. "Seen" means that the training data contains these segments. "Semi-seen" means that the training data contains the respiring people but not these segments. "Unseen" means that the respiring people are not in the training data, and it includes the data of 2 participants in our experiment, as well as the data of 4 people in the open-source dataset. The results are shown in Fig. 16b. For the "seen" case, since the segments are derived from training data, their AUC is only 0.5671. However, such reproduction may be perceptible to the attacker. Therefore, users have the option to measure their own offline respiration data to generate a segment library, and the AUC for this "semi-seen" case is 0.6047. In addition, Scarecrow can directly utilize third-party respiration data as a library, and the AUC for this "unseen" case is only 0.6283.

Influence of cycle number: In Fig. 16c, we test the effect of the number of cycles of a data sample. Benefiting from the excellent fidelity of artificial respiration, when the cycle number is low, the forged curve is almost equivalent to the real respiration segments, resulting in an AUC of 0.5427 at 2 cycles. When the number of cycles increases, the artificial frequency and amplitude imprints cause differences from the real respiration, but even so, the AUC at 10 cycles is only 0.6210, which further demonstrates the verisimilitude of Scarecrow's artificial respiration.

Influence of feature number: To evaluate the effect of the data processing depth and the feature amount, we increase the WPD level from 1 to 3, which corresponds to an increase in the number of features from 15 to 75, and the discrimination results are shown in Fig. 16d. 15 features do not provide enough information for discrimination. The recall with 75

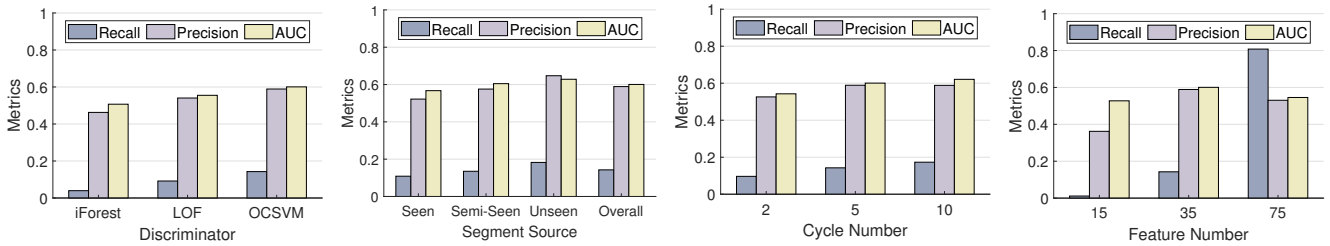
Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



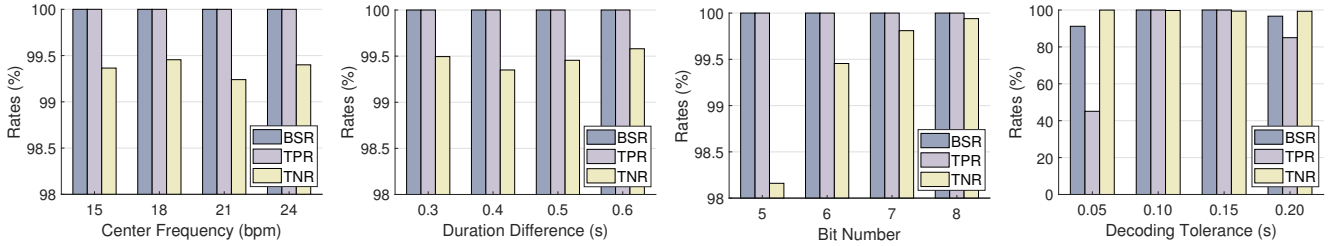
(a) (b) (c) (d)

Fig. 15: Verisimilitude evaluation on MDS.



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

Fig. 16: Verisimilitude evaluation on respiration curve.



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

Fig. 17: Identifiability evaluation results.

features is very high while the precision is close to 0.5, which suggests that the 75-feature setting is highly inclined to recognize a target as a forgery, regardless of whether the target is real or forged. Such high bias results in very poor discriminative ability. In contrast, the results for 35 features show certain usability, which reflects the rationality of the default experimental parameter.

D. Identifiability Evaluation

Under each set of parameters in this evaluation, we generate 100 identity codes and corresponding respiration curves to synthesize signals. Meanwhile, with each parameter setting and identity code, the same signal processing and identification flow is performed on all 200 real respiration samples.

1) Metrics: We employ the following three metrics. (1) Bit success rate (BSR): the rate at which the identity bits are decoded correctly. (2) True positive rate (TPR): the rate of forged targets being identified as forged. (3) True negative rate (TNR): the rate of real targets being identified as real.

2) Evaluation Results: The respiration coding configuration contains four key parameters: the center frequency of respiration, the difference in cycle duration of codes `1` and `0`, the bit number of identity codes, and the time tolerance of decoding. We vary these parameters to observe the changes in identifiability. The default parameter combination is [21bpm, 0.5s, 6, 0.15s].

Influence of center frequency: A higher respiration frequency leads to shorter cycles, which may increase measurement errors in detecting troughs and result in bit errors. We increase the center frequency from 15bpm to 24bpm, and the identification results are shown in Fig. 17a. Within the normal range of respiration frequencies, Scarecrow ensures 100% BSR and TPR, with a TNR of over 99%.

Influence of duration difference: Codes `1` and `0` correspond to different cycle durations, and the difference may resemble the variations in the real respiration pattern, leading to the real respiration curves being frequently misidentified as forged. We increase the cycle difference from 0.3s to 0.6s, and the results are shown in Fig. 17b. The TNR does not exhibit a significant trend with the change in cycle difference.

Influence of bit number: The influence of the identity code's bit number is evident. A higher bit number will reduce

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

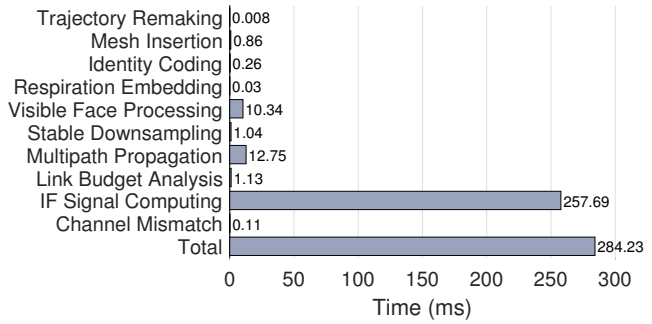


Fig. 18: Mean time costs per frame for 48 Tx-Rx channels.

the probability of misidentifying the real target, but it may increase the probability of misidentifying forged targets, and vice versa. We increase the bit number from 5 to 8, and the results are shown in Fig. 17c. As the bit number increases, the TNR improves from 99.41% at 5 bits to 99.99% at 8 bits. On the other hand, thanks to the high decoding accuracy, even at 8 bits, the TPR remains 100%.

Influence of decoding tolerance: The time tolerance for decoding requires careful consideration. If the tolerance is too strict, decoding is prone to failure due to trough measurement errors. If it is too loose, decoding may incorrectly treat non-identity cycles as identity codes. We increase the tolerance from 0.05s to 0.2s, and the results are shown in Fig. 17d. Both the strict tolerance of 0.05s and the loose tolerance of 0.2s lead to frequent bit errors, resulting in a drop in TPR, while the moderate tolerances of 0.1s and 0.15s achieve 100% BSR and TPR. Additionally, increasing the tolerance slightly reduces the TNR from 99.96% at 0.05s to 99.32% at 0.2s.

E. Time Cost

Fig. 18 shows the mean time cost of each module for one frame using an Intel i9-14900KF CPU. From the complexity perspective, all additional functionalities introduced by Scarecrow add less than 30ms, supporting a rate of over 30 frames per second. From the feasibility perspective, although the total time cost is 284.23ms, it is important to note that this includes a high sampling rate and a large MIMO array with 48 channels. The IF signal computing occupies 90% of the total time, costing 257.69ms under the 6Tx-8Rx configuration. This dominant cost roughly scales with the number of channels due to the channel-by-channel loop structure. Under the same settings, the IF computing cost is 5.47ms for 1Tx-1Rx and 64.75ms for 3Tx-4Rx. In practical applications, a lower sampling rate and fewer channels could significantly reduce the computational burden. Furthermore, IF signal computing can be naturally parallelized across channels and chirps, and is also well-suited to hardware acceleration. Thus, Scarecrow can meet real-time requirements in practice.

V. Limitations and Future Work

Scarecrow is designed as a privacy-enhancing defense against terminal-side radar stream leakage. However, signal-synthesis techniques are dual-use: while they can protect the radar owner's privacy, unauthorized use may also enable malicious spoofing by injecting forged human-presence signals into radar streams [3]. Therefore, Scarecrow should be deployed only in owner-authorized radar data pipelines. Beyond this broader-impact concern, we summarize the remaining issues and future directions for Scarecrow as follows:

(1) Multiple forged targets: While the current prototype focuses on one forged target, the signal superposition principle allows multiple synthetic targets to coexist in one forged stream. Extending Scarecrow to multi-target synthesis further requires avoiding overlaps among forged targets. (2) Compatibility with real users: Scarecrow mainly protects an unoccupied room by making the leaked radar stream appear occupied. Once a real user enters the room, Scarecrow can detect user presence and automatically stop forged-target insertion. For future enhanced spoofing systems where forged targets coexist with real users, collision-avoidance mechanisms should be developed to prevent spatial overlap between forged and real targets. (3) Generalization across environments and radar hardware: After significant environmental changes such as furniture rearrangement, Scarecrow can refresh the empty-room stream and trajectory library before generating new forged targets. The empty-room stream can be easily collected again, and the user trajectory library can be continuously updated during normal sensing in the new environment. Different radar hardware may introduce different channel responses. Future systems should develop automatic parameter tuning to make the synthesized stream better align with the real responses of each radar platform. (4) Reverse-engineering risk of identity codes: The current identity code uses randomized positions and redundant bits to reduce repetitiveness, making fixed patterns harder to identify from short-term observations. However, it should not be regarded as a cryptographic authentication mechanism. If an attacker records long-term streams and knows the coding rule or parameters, reverse-engineering may still be possible. Future systems can derive a shared secret through authenticated key exchange and use it to generate key-dependent coding schedules and periodic code updates.

VI. Related Work

A. RF Sensing Security

The privacy and security threats faced by RF sensing are as diverse as their applications. By measuring the sound-caused vibration [40], [41], spy radars [42] can eavesdrop on the victim's speech. User activities can also be eavesdropped through side-channel attacks [43], [44], [45]. Han *et al.* [4] demonstrate deep-learning-based surveillance video reconstruction from mmWave signals, showing that leaked mmWave data may expose fine-grained visual semantics. This sophisticated threat further motivates data-layer protection mechanisms such as Scarecrow, which injects realistic forged human signatures into the radar stream to mislead downstream sensing and inference. In data layer security, Xie *et al.* [46] conduct adversarial attacks on human activity recognition samples. Liu *et al.* [47], [48] perturb radar data in multiple dimensions to conceal users' activity information, but their methods are unable to generate targets out of thin air. One intuitive sensing

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

threat is the exposure of position information [49], [50]. Many physical-layer attack methods have been proposed to perform appearing and disappearing spoofing on the position detection of FMCW radar [11], [10], [5], ultra-wideband radar [8], WiFi [51], and LiDAR [52]. However, these methods have limitations in constructing human objects and face challenges with spoofing array antenna sensing. The mmWave radar's high spatial resolution and displacement sensitivity significantly enhance and expand the sensing performance and capabilities, making it easy to detect coarse-grained spoofing. This gives the motivation and significance of Scarecrow, which aims to holistically forge human presence in fine-grained mmWave human sensing.

B. Signal Synthesis

Researchers are increasingly paying attention to the training data collection burden for RF sensing, leading to significant interest in generating signals through synthesis. A typical RF signal synthesis system consists of three components. First, MoCap data are obtained from an open-source dataset [15] and through self-collection [17]. RFGen [12] exploits diffusion models to increase the diversity of MoCap data. Next, human reflection models are constructed, with a primary focus on skeleton models [14] and fine-grained mesh models [13]. Finally, the propagation is calculated by employing ray tracing techniques [19]. Additionally, some studies introduce domain transformation to make specific signatures of the synthesized signal more closely resemble real ones [18], [16]. Although the synthesized signals in existing works can help neural networks learn feature distributions, they are not designed to forge human-related signatures together with propagation factors for occupancy spoofing. Our Scarecrow system has undergone meticulous design in terms of human activities, reflection models, and signal propagation, enabling the synthesized signal to effectively spoof attackers from multiple perspectives and across multiple sensing dimensions.

VII. Conclusion

This paper studied the house occupancy threat of mmWave radar and presented Scarecrow, a forgery-embedding signal synthesis system for data layer occupancy spoofing. Scarecrow comprises a comprehensive design for human behavior, environmental response, and signal propagation, achieving high authenticity in both human construction and electromagnetic properties. A respiration cycle-based covert identification mechanism was proposed to protect trusted terminals from the forgery's interference. Extensive experiments demonstrated satisfactory fidelity, verisimilitude, and identifiability, in which the anomaly detection AUCs for spatial, velocity, and respiration signatures are 0.639, 0.634, and 0.601, respectively. The Scarecrow system has the potential to be applied in various privacy-sensitive scenarios.

References

[1] J. Haney, Y. Acar, and S. Furman, ""it's the company, the government, you and I": User perceptions of responsibility for smart home privacy and security," in *Proc. USENIX Security*, 2021, pp. 411–428.

[2] X. Liu, H. Liu, Y. Han, X. Xie, X. Tong, and K. Li, "MHTrack: mmwave-based mobile hand tracking," *IEEE Transactions on Mobile Computing*, vol. 24, no. 9, pp. 9168–9183, 2025.

[3] M. Han, H. Yang, W. Li, W. Xu, X. Cheng, P. Mohapatra, and P. Hu, "RF sensing security and malicious exploitation: A comprehensive survey," *arXiv preprint arXiv:2504.10969*, 2025.

[4] M. Han, H. Yang, M. Jia, W. Xu, Y. Yang, Z. Huang, J. Luo, X. Cheng, and P. Hu, "Seeing the invisible: Recovering surveillance video with COTS mmWave radar," *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 14 592–14 606, 2024.

[5] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht, "RF-Protect: Privacy against device-free human tracking," in *Proc. ACM SIGCOMM*, 2022, pp. 588–600.

[6] L. Jiao, Y. Ge, K. Zeng, and B. Hilburn, "Location privacy and spectrum efficiency enhancement in spectrum sharing systems," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 6, pp. 1472–1488, 2023.

[7] Y. Ge and P. C. Ching, "Energy efficiency for proactive eavesdropping in cooperative cognitive radio networks," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 443–13 457, 2022.

[8] P. Leu, G. Camurati, A. Heinrich, M. Roeschlin, C. Anliker, M. Hollick, S. Capkun, and J. Classen, "Ghost peak: Practical distance reduction attacks against HRP UWB ranging," in *Proc. USENIX Security*, 2022, pp. 1343–1359.

[9] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? Practical physical layer attack and defense for mmWave-based sensing in autonomous vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199–3214, 2021.

[10] R. Reddy Vennam, I. K. Jain, K. Bansal, J. Orozco, P. Shukla, A. Ranganathan, and D. Bharadia, "mmSpoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *Proc. IEEE S&P*, 2023, pp. 1807–1821.

[11] X. Chen, Z. Li, B. Chen, Y. Zhu, C. X. Lu, Z. Peng, F. Lin, W. Xu, K. Ren, and C. Qiao, "MetaWave: Attacking mmWave sensing with meta-material-enhanced tags," in *Proc. ISOC NDSS*, 2023, pp. 1–17.

[12] X. Chen and X. Zhang, "RF genesis: Zero-shot generalization of mmWave sensing through simulation-based data synthesis and generative diffusion models," in *Proc. ACM SenSys*, 2023, pp. 1–14.

[13] J. Li, D. Zhang, Z. Wu, C. Yu, Y. Li, Q. Chen, Y. Hu, Q. Sun, and Y. Chen, "SBRF: A fine-grained radar signal generator for human sensing," *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 13 114–13 130, 2024.

[14] S. Vishwakarma, W. Li, C. Tang, K. Woodbridge, R. Adve, and K. Chetty, "SimHumalator: An open-source end-to-end radar simulator for human activity recognition," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 3, pp. 6–22, 2022.

[15] H. Cai, B. Korany, C. R. Karanam, and Y. Mostofi, "Teaching RF to sense without RF training measurements," *Proc. ACM IMWUT*, vol. 4, no. 4, pp. 1–22, 2020.

[16] H. Xue, Q. Cao, C. Miao, Y. Ju, H. Hu, A. Zhang, and L. Su, "Towards generalized mmWave-based human pose estimation through signal augmentation," in *Proc. ACM MobiCom*, 2023, pp. 1–15.

[17] K. Ahuja, Y. Jiang, M. Goel, and C. Harrison, "Vid2Doppler: Synthesizing doppler radar data from videos for training privacy-preserving activity recognition," in *Proc. ACM CHI*, 2021, pp. 1–10.

[18] X. Zhang, Z. Li, and J. Zhang, "Synthesized millimeter-waves for human motion sensing," in *Proc. ACM SenSys*, 2022, pp. 377–390.

[19] K. Deng, D. Zhao, Q. Han, Z. Zhang, S. Wang, A. Zhou, and H. Ma, "Midas: Generating mmWave radar data from videos for training pervasive and privacy-preserving human sensing tasks," *Proc. ACM IMWUT*, vol. 7, no. 1, pp. 1–26, 2023.

[20] M. Loper, N. Mahmood, J. Romero, G. Pons-Moll, and M. J. Black, "SMPL: a skinned multi-person linear model," *ACM Transactions on Graphics*, vol. 34, no. 6, pp. 1–16, 2015.

[21] Meshcapade GmbH. (2021) A wiki on body-modelling technology. https://meshcapade.wiki/.

[22] S. Katz, A. Tal, and R. Basri, "Direct visibility of point sets," *ACM Transactions on Graphics*, vol. 26, no. 3, pp. 1–12, 2007.

[23] H. Liu, X. Liu, X. Xie, X. Tong, and K. Li, "Pmtrack: Enabling personalized mmWave-based human tracking," *Proc. ACM IMWUT*, vol. 7, no. 4, pp. 1–30, 2023.

[24] W. Chen, H. Yang, X. Bi, R. Zheng, F. Zhang, P. Bao, Z. Chang, X. Ma, and D. Zhang, "Environment-aware multi-person tracking in indoor environments with mmwave radars," *Proc. ACM IMWUT*, vol. 7, no. 3, pp. 1–29, 2023.

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820

[25] C. Tepedelenlioglu, A. Abdi, and G. Giannakis, "The ricean K factor: estimation and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 799–810, 2003.
[26] C. Tian, Y. Ma, and B. Wang, "Cooperative localization for passive RFID backscatter networks and theoretical analysis of performance limit," *IEEE Transactions on Wireless Communications*, vol. 22, no. 2, pp. 1388–1402, 2023.
[27] S. Rao. (2017) Texas Instruments: Introduction to mmwave sensing: FMCW radars.
[28] Texas Instruments. (2020) AWRx cascaded radar RF evaluation module (MMWCAS-RF-EVM). https://www.ti.com/lit/ug/swru553a/swru553a.pdf.
[29] ——. (2020) Imaging radar using cascaded mmwave sensor: Reference design. https://www.ti.com/lit/ug/tiduen5a/tiduen5a.pdf.
[30] J. Geiss, E. Sippel, M. Braunwarth, and M. Vossiek, "The impact of antenna array calibration errors on MIMO and multi-channel synthetic aperture radar imaging," *IEEE Journal of Microwaves*, vol. 3, no. 2, pp. 635–654, 2023.
[31] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.
[32] H. Sakoe and S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 26, no. 1, pp. 43–49, 1978.
[33] M. Heusel, H. Ramsauer, T. Unterthiner, B. Nessler, and S. Hochreiter, "GANs trained by a two time-scale update rule converge to a local nash equilibrium," in *Advances in Neural Information Processing Systems*, vol. 30, 2017, pp. 6626–6637.
[34] A. Tharwat, "Classification assessment methods," *Applied Computing and Informatics*, vol. 17, no. 1, pp. 168–192, 2021.
[35] Carnegie Mellon Graphics Lab. CMU graphics lab motion capture database. http://mocap.cs.cmu.edu/.
[36] M. A. García-González, A. Argelagós-Palau, M. Fernández-Chimeno, and J. Ramos-Castro. (2014) PhysioNet: Combined measurement of ECG, breathing and seismocardiograms. https://physionet.org/content/cebsdb/1.0.0/.
[37] D. W. Hosmer, S. Lemeshow, and R. X. Sturdivant, *Applied Logistic Regression*, 3rd ed. Wiley, 2013.
[38] A.-K. Seifert, M. G. Amin, and A. M. Zoubir, "Toward unobtrusive in-home gait analysis based on radar micro-doppler signatures," *IEEE Transactions on Biomedical Engineering*, vol. 66, no. 9, pp. 2629–2640, 2019.
[39] Y. Wang, T. Gu, T. H. Luan, and Y. Yu, "Your breath doesn't lie: Multi-user authentication by sensing respiration using mmWave radar," in *Proc. IEEE SECON*, 2022, pp. 64–72.
[40] C. Wang, F. Lin, T. Liu, K. Zheng, Z. Wang, Z. Li, M.-C. Huang, W. Xu, and K. Ren, "mmEve: Eavesdropping on smartphone's earpiece via COTS mmwave device," in *Proc. ACM MobiCom*, 2022, pp. 338–351.
[41] S. Basak and M. Gowda, "mmSpy: Spying phone calls using mmWave radars," in *Proc. IEEE S&P*, 2022, pp. 1211–1228.
[42] Y. Qiu, J. Zhang, Y. Chen, J. Zhang, and B. Ji, "Radar^2: Passive spy radar detection and localization using COTS mmWave radar," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2810–2825, 2023.
[43] Z. Li, F. Ma, A. S. Rathore, Z. Yang, B. Chen, L. Su, and W. Xu, "WaveSpy: Remote and through-wall screen attack via mmWave sensing," in *Proc. IEEE S&P*, 2020, pp. 217–232.
[44] J. Hu, H. Wang, T. Zheng, J. Hu, Z. Chen, H. Jiang, and J. Luo, "Password-stealing without hacking: Wi-Fi enabled practical keystroke eavesdropping," in *Proc. ACM CCS*, 2023, pp. 239–252.
[45] T. Ni, G. Lan, J. Wang, Q. Zhao, and W. Xu, "Eavesdropping mobile app activity via radio-frequency energy harvesting," in *Proc. USENIX Security*, 2023, pp. 3511–3528.
[46] Y. Xie, R. Jiang, X. Guo, Y. Wang, J. Cheng, and Y. Chen, "Universal targeted adversarial attacks against mmWave-based human activity recognition," in *Proc. IEEE INFOCOM*, 2023, pp. 1–10.
[47] H. Liu, X. Liu, X. Xie, X. Tong, T. Shi, and K. Li, "Application-oriented privacy filter for mmWave radar," *IEEE Communications Magazine*, vol. 61, no. 12, pp. 168–174, 2023.
[48] X. Liu, H. Liu, J. Zhang, X. Xie, and K. Li, "Multi-user behavioral privacy filtering for mmWave radar sensing," *IEEE Transactions on Mobile Computing*, vol. 24, no. 9, pp. 8347–8361, 2025.
[49] X. Xu, X. Meng, X. Tong, X. Liu, X. Xie, and W. Qu, "HyperTracking: Exploring the hyperbolic model for non-line-of-sight device-free Wi-Fi tracking," *Proc. ACM IMWUT*, vol. 7, no. 4, pp. 1–26, 2024.
[50] X. Tong, W. Ge, Y. Tian, Z. Liu, X. Liu, and W. Qu, "NNE-Tracking: A neural network enhanced framework for device-free Wi-Fi tracking," *IEEE Transactions on Mobile Computing*, vol. 23, no. 9, pp. 8981–8998, 2024.
[51] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar, "IRShield: A countermeasure against adversarial physical-layer wireless sensing," in *Proc. IEEE S&P*, 2022, pp. 1705–1721.
[52] Z. Jin, X. Ji, Y. Cheng, B. Yang, C. Yan, and W. Xu, "PLA-LiDAR: Physical laser attacks against LiDAR-based 3D object detection in autonomous vehicle," in *Proc. IEEE S&P*, 2023, pp. 1822–1839.



Hankai Liu is currently a lecturer in the College of Cryptology and Cyber Science, Nankai University, China. Before that, he received the B.E., M.S., and Ph.D. degrees from Tianjin University in 2018, 2021, and 2025, respectively. His current research interests include mmWave radar and RF security.



Jiaqi Zhang received her B.E. degree from Dalian University of Technology in 2022, and her M.S. degree from Tianjin University in 2025. Her research interests include wireless sensing and mmWave radar.



Xiulong Liu (Senior Member, IEEE) is currently a professor in the College of Intelligence and Computing, Tianjin University, China. Before that, he received the B.E. and Ph.D. degrees from Dalian University of Technology (China) in 2010 and 2016, respectively.

He also worked as a visiting researcher in Aizu University, Japan; a postdoctoral fellow in The Hong Kong Polytechnic University, Hong Kong; and a postdoctoral fellow in the School of Computing Science, Simon Fraser University, Canada. His research interests include wireless sensing and communication, indoor localization, and networking, etc. His research papers were published in many prestigious journals and conferences including SIGCOMM, NSDI, MOBICOM, UBICOMP, INFOCOM, TON, TMC, TC, TPDS, TCOM, etc. He received Best Paper Awards from ICA3PP 2014 and IEEE System Journal 2017. He is also the recipient of CCF Outstanding Doctoral Dissertation award 2017.

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2026.3747820



Heng Qi (Senior Member, IEEE) received the B.S. degree from Hunan University, Changsha, China, in 2004, and the M.E. and Ph.D. degrees from Dalian University of Technology, Dalian, China, in 2006 and 2012, respectively.

He was a JSPS Oversea Research Fellow with the Graduate School of Information Science, Nagoya University, Nagoya, Japan, from 2016 to 2017. He is currently a Professor with the School of Computer Science and Technology, Dalian University of Technology. He has published over 100 technical papers in journals and conferences such as the IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON MULTIMEDIA, and INFOCOM. His research interests include computer networking and multimedia computing.



Jiancheng Chen is the Chief Strategic and Technology Officer of Xiamen Intretech Inc. He has over 20 years of working experience in computing, smart manufacturing, and the Internet of Things. He held over five major R&D projects in IoT and personal computing for IntreTech and Lenovo in the past 20 years. He has won three provincial technology and innovation awards in the past ten years.



Junzhao Du received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1997, 2000, and 2008, respectively. He is currently a Professor and a Ph.D. Advisor with Xidian University. His research interests include edge AI, mobile computing, cloud computing, and IoT systems.

He is a member of ACM, a Distinguished Member of CCF, and an Executive Member of the council of ACM Xi'an Chapter.



Xin Xie received the B.E. and Ph.D. degrees from the School of Computer Science and Technology, Dalian University of Technology, China, in 2013 and 2019, respectively. He is currently a professor with the College of Intelligence and Computing, Tianjin University, China.

He also worked as a visiting scholar with the Department of Computer Sciences, Purdue University, USA, a postdoctoral fellow with the Department of Computing, The Hong Kong Polytechnic University, Hong Kong SAR, and a researcher with the Theory Lab of 2012 Labs, Huawei, Hong Kong SAR. His research interests include IoT, edge intelligence and network system.



Keqiu Li (Fellow, IEEE) is currently a full professor, the dean of the College of Intelligence and Computing, Tianjin University, China. Previously, he received his bachelor's and master's degrees from the Department of Applied Mathematics at the Dalian University of Technology in 1994 and 1997, respectively. He received the Ph.D. degree from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology in 2005.

He is the recipient of National Science Foundation for Distinguished Young Scholars of China. He keeps working on the topics of blockchain, mobile computing, datacenter, and cloud computing. He has more than 400 papers published on prestigious journals or conferences such as TON, TPDS, TC, TMC, INFOCOM, ICNP, etc.

Authorized licensed use limited to: NANKAI UNIVERSITY. Downloaded on October 31,2026 at 06:34:54 UTC from IEEE Xplore. Restrictions apply.
© 2026 IEEE. All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.