# Attacking mmWave-enabled Chest Vibration Sensing via Actuator-induced Mimicry

Xiaonan Guo[†], Yi Wei[†], Yuan Ge[†], Yucheng Xie[‡], Yan Wang[§], Jerry Cheng[¶], Yingying Chen[||]
[†] George Mason University, USA
[‡] Yeshiva University, USA
[§] Temple University, USA
[¶] New York Institute of Technology, USA
[||] Rutgers University, USA
Email: xguo8@gmu.edu, ywei8@gmu.edu, yge3@gmu.edu,
yucheng.xie@yu.edu, y.wang@temple.edu, jcheng18@nyit.edu,
yingche@scarletmail.rutgers.edu

*Abstract*—**Millimeter-wave (mmWave) technology has enabled emerging applications such as vital-sign-based healthcare monitoring, user authentication, and emotion-aware human-computer interaction. By capturing subtle chest displacements induced by heartbeat and respiration, mmWave systems provide high-resolution, contactless chest-vibration sensing. However, the mmWave signals that power these applications are vulnerable to spoofing attacks, posing serious risks such as identity impersonation and falsified health assessments. While prior studies have demonstrated the feasibility of spoofing mmWave sensing, existing methods often require access to raw mmWave data or rely on expensive, specialized RF equipment, limiting their real-world applicability. In this work, we present a real-time, low-cost spoofing attack using a programmable actuator concealed under clothing to physically mimic a target user's chest vibrations. Our attack allows adversaries to bypass authentication systems or falsify health data, potentially granting unauthorized access, or concealing critical medical conditions and triggering false emergency responses. To ensure high-fidelity spoofing, we introduce a mitigation strategy that integrates IMU-assisted compensation and quaternion-based alignment to mitigate interference from the attacker's own chest motion. We further employ deep learning to dynamically adjust actuator behavior in real time. Experiments with eight participants over six months validate the attack's effectiveness, revealing a critical security vulnerability in emerging mmWave-based sensing systems.**

## I. Introduction

Millimeter-wave (mmWave) technology has gained increasing attention due to its high-resolution sensing capabilities and extensive applications in the domain of mobile sensing [1]–[5] and security [6]–[9]. With mm-level wavelengths, mmWave signals can capture fine-grained mechanical displacement arising from chest vibrations caused by cardiac and respiratory activities. These capabilities facilitate many applications in chest vibration sensing, including non-contact vital sign monitoring (e.g, within healthcare and smart home environments ) [3], [10]–[13], as well as biometric-based user authentication (e.g., in secure access control systems) [14]–[16].

Despite the growing adoption of mmWave-based chest-vibration sensing in applications such as authentication and health monitoring, the security implications of these systems remain largely underexplored. Since mmWave signals capture subtle, user-specific physiological patterns, successful spoofing could lead to serious consequences, including unauthorized access to secure devices or services, identity impersonation, and falsified vital signs that obscure medical conditions or trigger incorrect responses. These risks highlight the urgent need to understand how such systems can be manipulated in practice. Previous research has demonstrated that mmWave sensing systems are vulnerable to attacks on their digital representations as range-Doppler maps and point clouds [17]–[19]. In parallel, physical-layer efforts have shown that RF signal manipulation using mixers or frequency shifters can alter reflected waveforms, enabling spoofing of sensing outputs [20], [21]. However, these approaches often rely on strong assumptions, such as adversaries having access to internal digital data or requiring expensive, specialized RF equipment.

**Actuator-Induced Vibration Mimicry Spoofing Attack**. Motivated by the insufficient exploration of security vulnerabilities in mmWave-based chest vibration sensing systems, we present a stealthy and low-cost physical-layer spoofing attack that leverages an actuator to mimic a target user's chest movements in real time. This actuator-induced vibration mimicry manipulates the reflected mmWave signals such that the sensing system misidentifies the adversary as the target user, thereby enabling unauthorized access or falsified physiological readings. To execute the attack, the adversary first acquires the target's chest vibration patterns (e.g., by using a mmWave device to discreetly record the target's chest movements in shared spaces), and then employs a programmable actuator to reproduce these patterns with high fidelity. Moreover, in healthcare monitoring scenarios, public datasets of normal vital signs can be leveraged to spoof plausible physiological patterns and deceive health monitoring systems regarding the user's physical condition. The compact actuator can be concealed beneath clothing, allowing real-time spoofing in practical scenarios.

**Challenges in Mimicking Chest Vibration using Actuator.** There are major design and technical challenges to realize the aforementioned spoofing attack: *1) Aligning Measurements with mmWave Radar's Coordinate System.* The target user

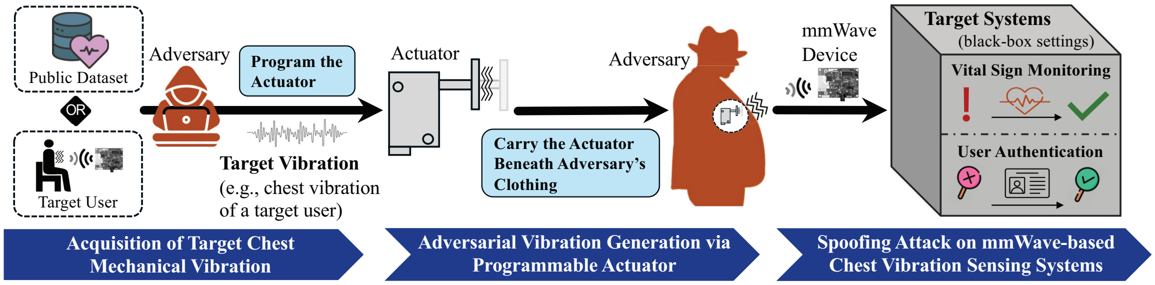

Public Dataset
OR
Target User
Adversary
Program the Actuator
Target Vibration
(e.g., chest vibration of a target user)
Actuator
Carry the Actuator Beneath Adversary's Clothing
Adversary
mmWave Device
Target Systems
(black-box settings)
Vital Sign Monitoring
User Authentication
Acquisition of Target Chest Mechanical Vibration
Adversarial Vibration Generation via Programmable Actuator
Spoofing Attack on mmWave-based Chest Vibration Sensing Systems

Fig. 1: Illustration of the proposed stealthy spoofing attack on mmWave-based chest vibration sensing systems via actuator-induced chest vibration mimicry.

usually maintains a specific relative position with respect to the mmWave radar during chest sensing. To launch an effective attack, the adversary needs to ensure the actuator-generated vibrations are adjusted to resemble those of the target user. This requires the generated vibrations to be aligned with the radar's orientation. *2) Generating Precise Actuator Vibration with Interference Mitigation.* When the actuator is concealed under the adversary's clothes, the adversary's chest movement will interfere with the actuator's output. Thus, simply generating the target user's vibration signal based on public datasets or secret observation is not sufficient for launch an effective attack. To perform an effective spoofing, such interference must be mitigated through appropriate compensation techniques. *3) Achieving Real-time Attack Execution.* To launch the attack in real time, the system is required to rapidly identify the adversary's chest vibration, calculate the necessary compensatory movements, and apply these adjustments on the actuator to effectively spoofing the target user's chest vibration.

**Addressing the Challenges.** To realize the proposed stealthy spoofing attack in practical settings, we design an attack system that addresses those major challenges: 1) We employ a quaternion-based rotation method to dynamically rectify orientation discrepancies. This approach ensures that actuator displacements are accurately projected onto the mmWave radar's sensing axis, thereby preventing measurement error due to coordinate misalignment. 2) We design a compact interference compensation module by integrating an Inertial Measurement Unit (IMU) with the actuator to capture the adversary's chest vibrations. We then employ a Convolutional Neural Network (CNN) to learn the mapping between IMU-recorded signals and mmWave-derived displacement features. This model enables real-time correction of the actuator output, ensuring that the spoofed signal remains aligned with the target's vibration pattern. 3) We develop a Long Short-Term Memory (LSTM) model to predict future IMU readings based on recent chest movement history. This forward-looking design enables the system to preemptively compute compensation values, allowing real-time adjustment of actuator output with minimal delay. By incorporating predicted IMU data into control decisions, the system ensures timely and accurate spoofing performance.In summary, our work makes the following contribution:

- We design and implement a practical real-time attack system that leverages a programmable actuator, discreetly concealed under clothing, to accurately reproduce a target user's chest vibrations. To the best of our knowledge, this is the first work to demonstrate that fine-grained actuator control can reliably spoof mmWave-based chest vibration sensing, enabling a stealthy and effective physical-layer attack.
- We propose an IMU-assisted compensation framework with quaternion-based coordinate alignment to address interference caused by the adversary's own chest vibrations. This mechanism enables high-fidelity vibration reproduction, which is critical for maintaining spoofing stealth and accuracy.
- We incorporate CNN and LSTM models to adaptively correct for motion-induced perturbations. The CNN model learns the mapping between IMU-recorded self-vibrations and mmWave displacement signals, enabling real-time compensation. The LSTM model anticipates future IMU signals to proactively adjust actuator output, ensuring stable and precisely timed spoofing under dynamic conditions.
- We validate our proposed spoofing attack through extensive experiments involving eight participants under various attack settings over a six-month period. The attack achieves an average success rate of 88% in a simulated platform deployment and 83% in concealed deployment beneath clothing. Our results reveal the feasibility of real-time actuator-induced chest vibration mimicry, highlighting a critical security vulnerability inherent in chest vibration sensing.

## II. Background and Attack Feasibility

### A. FMCW-Based Chest Motion Sensing

Chest vibration sensing systems using mmWave technology have been widely adopted in critical applications such as vital sign monitoring and continuous user authentication. These systems usually use mmWave Frequency-Modulated Continuous Wave (FMCW) radars to capture small chest vibrations induced by physiological activities, such as respiration and heartbeat.

Specifically, for a chirp with carrier frequency $f_c$, bandwidth $B$, and duration $T_c$, the received signal reflected from the chest exhibits a phase:

$$\phi_H(t) \approx 4\pi \frac{Bd(t)}{T_c c} t + 4\pi \frac{f_c}{c} d(t), \quad (1)$$

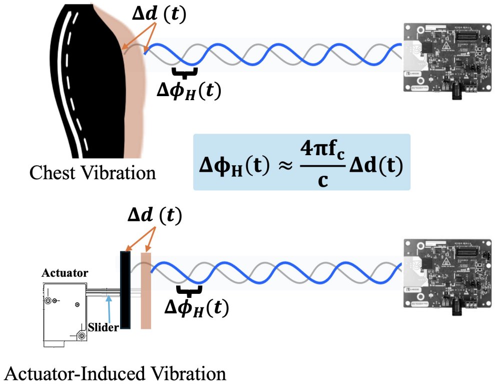


Fig. 2: Illustration of the principle of chest vibration sensing using mmWave signals and the rationale for actuator-based spoofing attack.

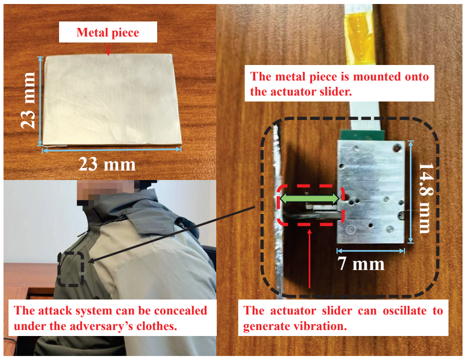

Metal piece
23 mm
23 mm
The metal piece is mounted onto the actuator slider.
14.8 mm
7 mm
The attack system can be concealed under the adversary's clothes.
The actuator slider can oscillate to generate vibration.

Fig. 3: The prototype of the proposed attack system using a programmable actuator and a metal plate. The compact design allows the device to be concealed under clothing.

where $d(t)$ is the time-varying chest-to-radar distance. By comparing two consecutive chirps spaced by $T_c$, the phase difference becomes:

$$\Delta\phi_H(t_i) \approx 4\pi f_c \frac{\Delta d(t_i)}{c}. \quad (2)$$

This clearly shows that phase changes $(\Delta\phi_H(t_i))$ are strongly linked to chest displacements $\Delta d(t_i)$ induced by physiological motions. As illustrated in Figure 2, our attack drives a programmable actuator to impose a small, time-varying displacement $\Delta d_{\text{act}}(t)$ on the chest surface. According to Eq. (2), this displacement produces a controlled phase shift $\Delta\phi_H(t_i)$, which makes the receiver recover a target user's vibration pattern, enabling spoofing attack.

### *B. Attack Feasibility*

To assess the feasibility of mimicking human chest movements and spoofing chest vibration sensing systems, we prototyped our attacking system using an Xeryon XLA-1-70-312 actuator [22]. As shown in Figure 3, the actuator features a precisely controlled slider that can move bidirectionally via its dedicated controller. Through tailored voltage pulses (i.e., actuation commands), we can generate displacements up to 55mm within the 0Hz to 20Hz frequency range. To guarantee detection by mmWave devices, we developed an enhanced reflective surface. This surface, a paperboard covered with aluminum foil, increases the effective reflection area for the mimicked chest vibrations.

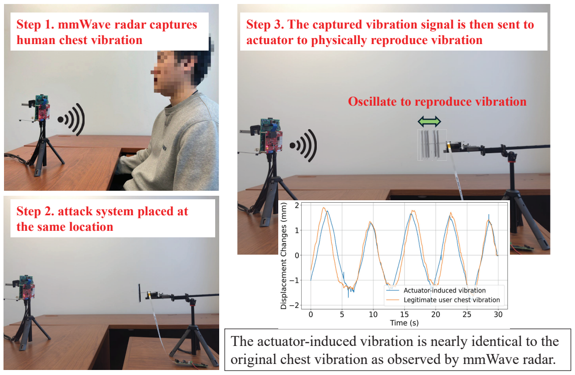


Fig. 4: Demonstration of attack feasibility using a tripod-mounted actuator.

To motivate our approach, we first verify that a stationary actuator mounted on a tripod can replicate chest vibrations with high fidelity as shown in Figure 4. However, in a practical scenario where the actuator is worn by the adversary, their own physiological movements (e.g., respiration) will introduce significant interference, distorting the spoofing signal and rendering simple replay attacks ineffective. This core challenge necessitates the real-time interference mitigation system detailed in Section IV.

## III. Threat Model and Attack Overview

### *A. Attacker's Capability*

Our spoofing attack targets two critical application domains of mmWave-based chest vibration sensing: user authentication and healthcare monitoring via vital sign. By replicating a target user's unique chest vibration patterns induced by respiration or heartbeat, an adversary can bypass biometric authentication systems, gaining unauthorized access to secure facilities, financial accounts, or personal devices. Moreover, the attack can be used to falsify physiological data, deceiving health monitoring systems with spoofed vital signs. Such manipulation could obscure serious medical conditions, leading to reduced insurance premiums, regulatory violations, or erroneous emergency responses, ultimately posing significant risks to both individual privacy and public safety.

To execute this attack, an adversary must first obtain the target individual's chest vibration data. In user authentication scenario, the adversary can secretly deploy a commercial off-the-shelf (COTS) mmWave radar device in public or shared spaces to measure the target individual's chest vibrations while they remain stationary (e.g., reading, using a phone, or working). For vital sign monitoring scenario, the monitored user can themselves act as the adversary. Instead of collecting user-specific data, the adversary user leverages publicly available datasets of respiration and heartbeat signals (e.g., [23]–[25]) to select a representative "healthy" template, enabling the user to manipulate the health-monitoring system (e.g., to mask abnormalities as normal). In both attack scenarios, we assume

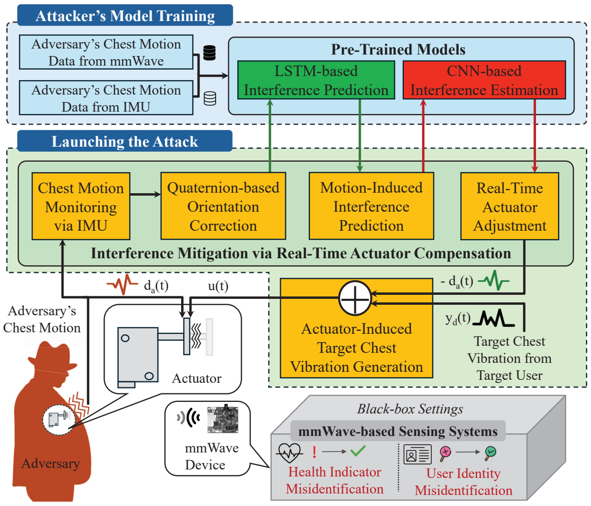

Attacker's Model Training
Adversary's Chest Motion Data from mmWave
Adversary's Chest Motion Data from IMU
Pre-Trained Models
LSTM-based Interference Prediction
CNN-based Interference Estimation
Launching the Attack
Chest Motion Monitoring via IMU
Quaternion-based Orientation Correction
Motion-Induced Interference Prediction
Real-Time Actuator Adjustment
Interference Mitigation via Real-Time Actuator Compensation
$d_a(t)$
$u(t)$
$- d_a(t)$
$y_d(t)$
Adversary's Chest Motion
Actuator
Actuator-Induced Target Chest Vibration Generation
Target Chest Vibration from Target User
Black-box Settings
mmWave-based Sensing Systems
Health Indicator Misidentification
User Identity Misidentification
mmWave Device
Adversary

Fig. 5: Flow of our physical spoofing attack targeting mmWave-based chest vibration sensing systems.

the adversary has prior knowledge of the target's posture and orientation relative to the radar, which is easily observable. The adversary could conceal the actuator-based attack system underneath clothing, making it less noticeable and enabling a stealthy attack in practice. Note that our attack is a black-box attack, as it operates independently of the target's sensing system and requires no access to or modification of its internal components.

## B. Overview of Attack System

We design an attack system to enable the practical spoofing attack on mmWave-based chest vibration sensing systems in black-box settings as shown in Figure 5. The attack begins by acquiring a target user's chest vibration data, which is later replayed in real time using a concealed programmable actuator.

**Attacker's Model Training.** Note that concealing the programmable actuator beneath clothing inevitably results in interference from the adversary's own chest vibrations, which distorts the actuator-induced mimicry. To address this, our attack system employs a learning-based method during an offline phase to compensate for this interference in real time. This ensures the target mmWave sensing system captures only the reproduced chest vibrations from the target user. To achieve this, the adversary first collects a dataset of their own chest vibrations using an IMU sensor and an mmWave radar. This dataset is then used to train two deep learning models: The *LSTM-based Interference Prediction* model predicts the IMU readings of the adversary's current chest vibrations based on their previous chest vibrations. This model allows our attack system to continuously track the interference (i.e., the adversary's own chest vibration) without introducing any time delays caused by measuring the adversary's real-time chest vibrations. Furthermore, the *CNN-based Interference Estimation* model maps the predicted IMU readings to the mmWave signals that capture the adversary's chest vibrations. This enables the adversary to generate their chest vibrations for real-time interference mitigation when launching the attack.

**Launching the Attack.** When launching our spoofing attack in the online phase, our attack system continuously monitors the adversary's chest vibrations using an IMU sensor attached to the actuator. We designed a *Quaternion-based Orientation Correction* algorithm to convert these IMU readings to the world coordinate system. This step aligns the adversary's chest vibrations with the direction of the target user's chest vibration, ensuring our attack system accurately reproduces the target user's movements for the mmWave sensing system. After coordinate correction, the IMU readings are fed into the pre-trained LSTM and CNN models, which predict the adversary's chest vibrations. Next, our attack system combines these predicted adversary's chest vibrations with the target user's chest vibrations. This combined signal then controls the programmable actuator. The combined chest vibrations effectively cancel out the adversary's own chest vibrations on the actuator, allowing only the target user's chest vibrations to be presented and thus spoofing the mmWave-based chest vibration sensing systems.

# IV. Attack Design and Implementation

## A. Attack Problem Formulation

The adversary aims to spoof a mmWave-based chest vibration sensing system by accurately reproducing the target user's chest vibrations using a programmable actuator. The effectiveness of this spoofing depends primarily on two factors: (1) *Actuator-generated vibration*, denoted as $u(t)$, representing the intentionally controlled displacement, and (2) *Adversary's own chest motion*, denoted as $d_a(t)$, capturing the unintended displacement caused by natural physiological movements. For successful spoofing, the adversary must precisely control the actuator-generated displacement while simultaneously compensating for interference from their own chest vibrations. Thus, the optimal actuator displacement control $u^*(t)$ can be formulated as a function of the desired target chest vibration $y_d(t)$ and the adversary's chest motion $d_a(t)$:

$$u^*(t) = f(y_d(t), d_a(t)), \tag{3}$$

where $y_d(t)$ is the target user's chest vibration pattern acquired beforehand, and $d_a(t)$ is the adversary's chest motion. Accurately estimating $d_a(t)$ in real time is the primary technical challenge of this spoofing approach.

## B. Chest Motion Monitoring and Orientation Correction via IMU

To accurately estimate the adversary's natural chest motion $d_a(t)$, we attach an IMU sensor to the actuator. The IMU continuously measures the acceleration induced by the adversary's chest movements, denoted as $\mathbf{a}_{IMU}(t)$, in its local coordinate frame. To ensure effective spoofing from the perspective of the target mmWave radar, we must precisely align these measured accelerations with the radar's measurement direction. To accomplish this, we first project the measured acceleration onto the known actuator slider direction $\mathbf{v}_s^{IMU}$ in the IMU frame as follows:

$$a_s^{IMU}(t) = \mathbf{a}_{IMU}(t) \cdot \mathbf{v}_s^{IMU}. \tag{4}$$

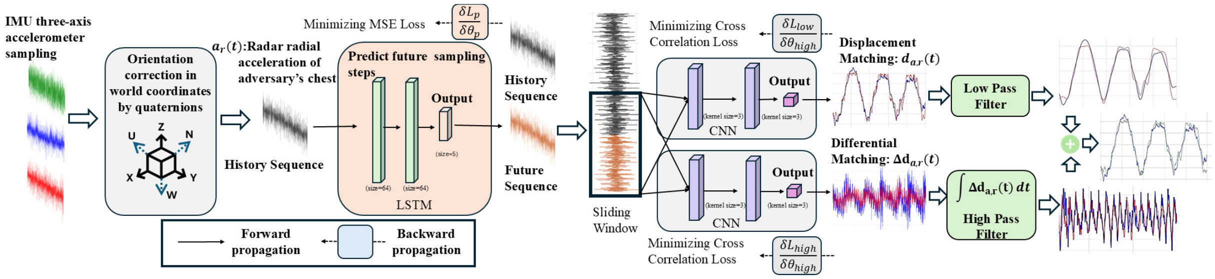

IMU three-axis accelerometer sampling
Orientation correction in world coordinates by quaternions
U
Z
N
X
Y
W
$a_r(t)$:Radar radial acceleration of adversary's chest
History Sequence
Minimizing MSE Loss
$\frac{\delta L_p}{\delta \theta_p}$
Predict future sampling steps
(size=64)
(size=64)
Output
(size=5)
LSTM
History Sequence
Future Sequence
Forward propagation
Backward propagation
Sliding Window
Minimizing Cross Correlation Loss
$\frac{\delta L_{low}}{\delta \theta_{high}}$
(kernel size=3)
(kernel size=3)
Output
CNN
(kernel size=3)
(kernel size=3)
Output
CNN
Minimizing Cross Correlation Loss
$\frac{\delta L_{high}}{\delta \theta_{high}}$
Displacement Matching: $d_{a,r}(t)$
Differential Matching: $\Delta d_{a,r}(t)$
Low Pass Filter
$\int \Delta d_{a,r}(t)\, dt$
High Pass Filter

Fig. 6: The proposed LSTM-CNN architecture for motion-induced interference prediction and real-time actuator adjustment.

Next, using the IMU's orientation quaternion $q(t)$, we transform this acceleration into the global coordinate frame:

$$a_s^{World}(t) = R(q(t)) \cdot a_s^{IMU}(t), \tag{5}$$

where $R(q(t))$ is the rotation matrix derived from the quaternion. Finally, to extract the specific component of the adversary's chest motion affecting the victim mmWave radar, we project the global-frame acceleration onto the radar's radial measurement direction $\mathbf{v}_r$:

$$a_r(t) = a_s^{World}(t) \cdot \mathbf{v}_r, \tag{6}$$

where $\mathbf{v}_r$ is determined based on the relative positions and orientations between the adversary and the mmWave device. This combined formulation enables accurate estimation and alignment of chest motion for effective spoofing attacks.

### C. Motion-Induced Interference Prediction

With the adversary's chest acceleration aligned to the mmWave radar's reference frame, the next challenge is accurately estimating and compensating for chest-induced interference in real time. A significant obstacle arises from inherent system latency, which may cause actuator adjustments to become outdated, reducing attack effectiveness. To address this latency, we propose an LSTM-based interference prediction model [26] to forecast future IMU acceleration samples from recent historical data. As illustrated in Figure 6, our model uses a sliding window $T_{hist}$ of past accelerations to predict acceleration values for the actuator's next control cycle $T_{pred}$. By predicting future chest motion, the actuator can proactively adjust its movements, aligning them precisely with real-time physiological signals. Formally, the prediction step is expressed as:

$$\hat{a}_r(T_{pred}) = f_{LSTM}(a_r(T_{hist})), \tag{7}$$

The predicted acceleration $\hat{a}_r(T_{pred})$ is subsequently passed to the CNN-based interference estimation module, enabling proactive rather than reactive actuator control.

### D. Real-Time Actuator Adjustment

Traditional displacement estimation methods based on double integration of acceleration measurements suffer from accumulated errors due to IMU sensor noise. To mitigate this, we propose a CNN-based mapping approach that directly estimates chest displacement $d_{a,r}(t)$ from IMU accelerations $a_r(t)$, as illustrated in Figure 6.

*1) CNN Model Design and Training:* We design a parallel CNN architecture comprising two independent branches, each focusing on distinct frequency ranges of chest vibrations. The CNN model is trained offline using synchronized datasets containing IMU acceleration measurements and corresponding ground-truth chest displacement data obtained from mmWave radar. Specifically, the *Low-Frequency CNN* estimates displacement components corresponding primarily to respiratory movements (below 0.8 Hz), whereas the *High-Frequency CNN* estimates velocity-related displacement changes associated with cardiac-induced vibrations (above 0.8 Hz).

Each CNN branch employs a composite loss function combining cross-correlation to maintain temporal alignment and amplitude regularization to prevent displacement overestimation. The loss for both branches is defined as:

$$\mathcal{L} = (1 - \text{Corr}(\hat{x}(t), x(t))) + \lambda \|\hat{x}(t)\|^2, \tag{8}$$

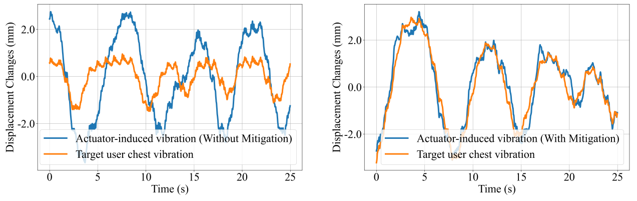
where $\text{Corr}(\hat{x}(t), x(t))$ denotes the normalized cross-correlation between predicted $\hat{x}(t)$ and ground-truth $x(t)$ signals, and $\lambda = 0.8$ is empirically selected through ablation studies. This parallel CNN design effectively separates and accurately estimates low- and high-frequency chest motion components for real-time actuator control.

*2) Interference Estimation and Mitigation:* The outputs from the two CNN branches capture complementary frequency components of chest displacement but may overlap if combined directly. To prevent frequency redundancy and ensure accurate reconstruction, we apply spectral filtering before fusion. Specifically, the integrated output of the High-Frequency CNN is processed through a high-pass filter (HPF, cutoff at 0.8 Hz), while the Low-Frequency CNN output is filtered by a corresponding low-pass filter (LPF). The final displacement estimation is obtained by summing these filtered high- and low-frequency components, providing accurate and artifact-free interference estimation.

### E. Actuator-Induced Target Vibration Generation

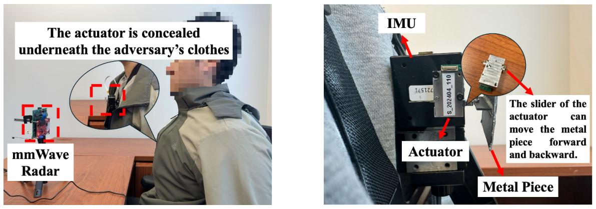
To ensure that the mmWave sensing system perceives the intended target chest vibration pattern $y_d(t)$, the actuator displacement must be dynamically controlled to compensate for the adversary's involuntary chest movements. This section formulates the final actuator control strategy by integrating orientation correction and interference estimation described in Sections IV-B to IV-D.

The actuator moves along a fixed direction $\mathbf{v}_s^{IMU}$ in the IMU's local coordinate frame. Using the IMU's real-time



(a) (b)

Fig. 7: Comparison of actuator-induced and target user chest vibrations as measured by mmWave radar. (a) Without mitigation, the actuator-induced signal deviates significantly from the target pattern. (b) With mitigation, the reproduced vibrations closely match the target signal.


The actuator is concealed underneath the adversary's clothes
mmWave Radar
IMU
The slider of the actuator can move the metal piece forward and backward.
Actuator
Metal Piece

(a) (b)

Fig. 8: Demonstration of a stealthy attack setup with a concealed actuator. (a) The actuator is hidden beneath the adversary's clothing. (b) The actuator, IMU and metal piece are securely attached to the chest using straps.

orientation quaternion $q(t)$, this direction is transformed into the global coordinate frame as:

$$\mathbf{v}_s(t) = R(q(t)) \cdot \mathbf{v}_s^{IMU}. \tag{9}$$

Let $\mathbf{v}_r$ denote the radar's known radial sensing direction. The contribution of the actuator displacement $u(t)$ to the total displacement measured by the radar is then:

$$y(t) = u(t)\,(\mathbf{v}_s(t) \cdot \mathbf{v}_r) + d_{a,r}(t) + \epsilon(t), \tag{10}$$

where $d_{a,r}(t)$ is the adversary's chest interference estimated in Section IV-D, and $\epsilon(t)$ represents measurement noise.

To ensure the radar perceives exactly the desired target vibration $y_d(t)$, the actuator displacement $u^*(t)$ must be adjusted in real time to cancel out interference:

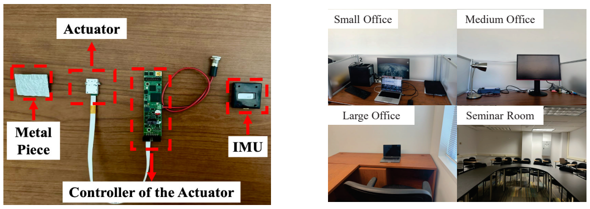
$$u^*(t) = \frac{y_d(t) - d_{a,r}(t)}{\mathbf{v}_s(t) \cdot \mathbf{v}_r}. \tag{11}$$

This control strategy directly addresses the initial problem formulation in Eq. (3), enabling the actuator to simultaneously inject spoofed chest vibrations and negate the adversary's involuntary movements. Figure 7 demonstrates the effectiveness of this approach, showing improved consistency between the actuator-generated vibration and the target user's chest signature under realistic interference conditions.

## V. Evaluation of Attack Performance

### A. Evaluation Setup and Attack Methodology

*1) Device Configuration:* We implement the proposed attack system using a Xeryon XLA-1-70-312 actuator and a PhidgetSpatial Precision 3/3/3 IMU [27], with the actuator concealed beneath clothing and securely fastened to the adversary's chest (see Figure 8). Our prototype uses a commercial off-the-shelf Texas Instruments AWR1642 mmWave radar [28] and a DCA1000EVM data-capture card [29], as shown in Figure 9a. The radar operates at 77 GHz with 598 ADC samples, providing a range resolution of 3.85 cm and a field of view of 120° in elevation and 30° in azimuth, typical for user authentication and vital-sign monitoring applications. Currently, our real-time CNN and LSTM models run on a PC equipped with an Intel i7-10700 CPU. Given their lightweight architecture, these models can be easily migrated to compact edge computing platforms, such as NVIDIA's Jetson Nano [30], for future practical deployments. The small form-factor of such devices (100 mm × 80 mm × 29 mm) further facilitates discreet concealment and portability for an adversary.



(a) (b)

Fig. 9: Experimental setup used for evaluation. (a) Hardware components of the attack system, including the actuator, metal piece, controller, and IMU. (b) Four representative indoor environments used for testing: small office, medium office, large office, and seminar room.

*2) Data Collection:* We evaluate the proposed attack using 8 volunteers (7 males, 1 female) across four different environments as shown in Figure 9b, to evaluate the system's performance under diverse conditions. In each session, one participant serves as the target user while another acts as the adversary, replaying the recorded chest vibrations using a concealed actuator. All participants rotate through both roles to ensure a comprehensive evaluation. Each participant contributes 20 sessions collected across multiple days, with each session lasting approximately 40 seconds and including varied breathing patterns to simulate realistic chest vibration scenarios. The radar-to-subject distance ranges from 0.4 to 1.2 meters, reflecting typical deployment settings for authentication and health monitoring. To minimize motion artifacts and simulate common usage contexts (e.g., desk work or mobile device use), all participants remain seated during data collection. This setup mirrors realistic adversarial conditions, where a target's upper body is likely to be stationary, allowing accurate capture and spoofing of chest vibrations.

*3) Evaluation Metrics:* We evaluate the performance of our spoofing system using waveform-level metrics that directly assess the fidelity of the reproduced chest vibrations. The **Success Rate (SR)** quantifies how often the spoofed signals bypass the mmWave-based authentication system. To evaluate temporal alignment and waveform similarity, we use **Dynamic Time Warping (DTW)** distance. Lower DTW values indicate closer morphological similarity to the target vibrations. To measure amplitude accuracy, we report the **Root Mean Squared Error (RMSE)** and **Mean Absolute Error (MAE)**,

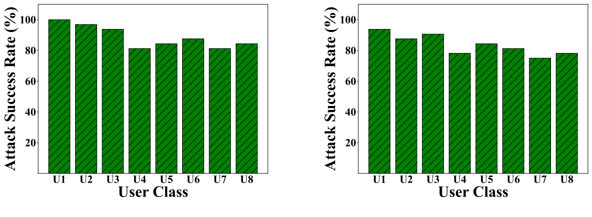


Fig. 10: Attack success rates against a mmWave-based heartbeat authentication system. (a) Simulated deployment with the actuator mounted on a tripod. (b) Real-world deployment with the actuator worn on the attacker's chest.

which reflect average and absolute displacement differences, respectively. For frequency-domain evaluation, we compute **STFT-based metrics**, including Euclidean distance and cross-correlation, to assess spectral alignment between spoofed and legitimate signals. All distance-based metrics are normalized to enable fair comparison across conditions. For module-level ablations, we additionally report the **coefficient of determination** ($R^2$) to quantify the regression quality of the interference-estimation module.

### B. *Effectiveness in Attacking*

We evaluate our spoofing attack against a state-of-the-art mmWave-based heartbeat authentication system that relies on unique cardiac-respiratory signatures for user identification [14]. Our experiments involve 8 participants to ensure the reliability and statistical robustness of results. Figure 10a and 10b summarize the attack success rates in two distinct scenarios. Figure 10a depicts the optimal scenario, with the actuator fixed on a tripod and unaffected by the adversary's own physiological motion. In this ideal configuration, success rates across participants range from 86% to 98%, with three participants (U1, U2, and U3) achieving over 95%. Figure 10b presents results under realistic concealed conditions, where the actuator is worn beneath clothing, requiring our proposed interference mitigation techniques to counteract adversary-induced vibrations. Despite the complexity introduced by interference, we still achieve success rates ranging from approximately 73% (participant U8) to 88% (participant U1). These findings confirm that the proposed actuator-induced mimicry can reliably bypass state-of-the-art heartbeat authentication systems, highlighting a significant vulnerability in real-world deployment scenarios.

| Metric | Simulated | Concealed Deployment | With Mitigation |
|---|---|---|---|
| *Time Domain* | | | |
| DTW Distance | 0.02 mm | 0.60 mm | 0.09 mm |
| RMSE | 0.03 mm | 0.61 mm | 0.12 mm |
| MAE | 0.01 mm | 0.34 mm | 0.06 mm |
| *Frequency Domain* | | | |
| STFT Euclidean Distance | 0.04 | 1.24 | 0.30 |
| STFT Cross-Correlation | 0.99 | 0.78 | 0.95 |

TABLE I: Replication performance under three deployment settings.

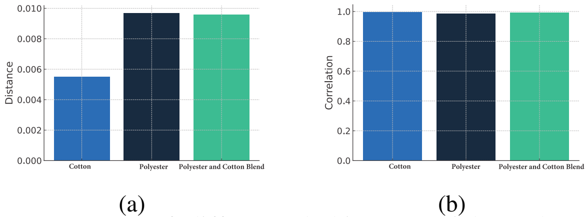


Fig. 11: Impact of different clothing material on the similarity between actuator-generated and reference signals. (a) DTW distance measured in the time domain. (b) STFT cross-correlation measured in the frequency domain.

### C. *Performance of Accurate Chest Vibration Replication*

We evaluate system performance under three deployment settings: simulated platform, concealed deployment without mitigation, and concealed deployment with mitigation. In the simulated setup where the actuator is mounted on a tripod, the system achieves high replication fidelity. The DTW distance is 0.02 mm, RMSE is 0.03 mm, and MAE is 0.01 mm. Frequency-domain similarity is also strong, with a STFT Euclidean distance of 0.04 and cross-correlation of 0.99, representing an upper bound for attack accuracy. When deployed beneath clothing without mitigation, replication quality drops significantly due to interference from the adversary's chest motion. The DTW distance increases to 0.60 mm, while RMSE and MAE rise to 0.61 mm and 0.34 mm. Frequency alignment also deteriorates, with cross-correlation falling to 0.78. Our mitigation approach restores much of the lost fidelity. The DTW distance improves to 0.0928 mm, RMSE to 0.11 mm, and MAE to 0.06 mm. In the frequency domain, STFT cross-correlation increases to 0.95. These results, summarized in Table I, confirm the effectiveness of our interference mitigation design under realistic attack conditions.

### D. *Impact of Clothing Material*

To evaluate whether clothing materials affect the detectability of actuator-induced vibrations, we conduct experiments with the actuator mounted on a tripod to ensure consistent output. Three typical clothing types (i.e., short sleeve cotton, a polyester jacket, and a thick polyester and cotton blend jacket) are individually placed between the actuator and the mmWave radar. In Figure 11a, the DTW distance remains consistently low across all clothing conditions, indicating minimal temporal distortion. As shown in Figure 11b, the STFT cross-correlation stays above 0.98, reflecting strong preservation of frequency-domain characteristics. Taken together, these results indicate that common clothing materials have negligible impact on the radar's ability to sense actuator-generated vibrations.

### E. *Ablation Study*

To understand the contribution of each component, we conduct an ablation study by comparing the full model against three reduced configurations: (i) removing the low-frequency CNN, (ii) removing the high-frequency CNN, and (iii) removing the LSTM while retaining both CNNs.

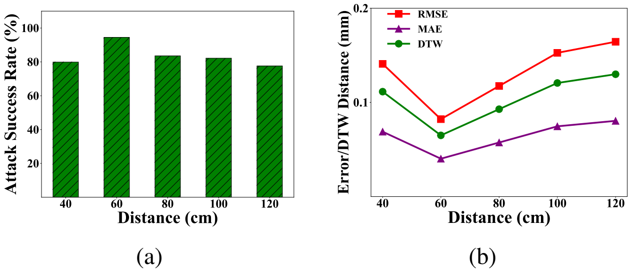
| Configuration | R² Score | Cross-Correlation | MAE (mm) |
|---|---|---|---|
| Complete System<br>(Low-Frequency CNN +<br>High-Frequency CNN + LSTM) | 0.92 | 0.96 | 0.31 |
| Complete System without<br>Low-Frequency CNN | -1.67 | 0.54 | 2.10 |
| Complete System without<br>High-Frequency CNN | 0.78 | 0.92 | 0.85 |
| Complete System without LSTM | 0.06 | 0.24 | 1.48 |

TABLE II: Ablation study.

As shown in Table II, the complete architecture achieves the highest accuracy, with an $R^2$ score of 0.92, a cross-correlation of 0.96, and a mean absolute error (MAE) of 0.31 mm. Removing the low-frequency CNN leads to a dramatic drop in performance ($R^2 = -1.68$, MAE = 2.10 mm, cross-correlation = 0.54), highlighting its critical role in capturing displacement features. In contrast, removing the high-frequency CNN results in a moderate degradation ($R^2 = 0.78$, MAE = 0.85 mm, cross-correlation = 0.92), suggesting that displacement estimation plays a more central role than velocity estimation. Omitting the LSTM leads to a significant loss in phase alignment and overall accuracy ($R^2 = 0.06$, MAE = 1.48 mm, cross-correlation = 0.24), emphasizing the importance of temporal modeling for robust interference estimation. These results indicate that while the low-frequency CNN contributes most significantly, the synergy among all three components is essential to achieve high-fidelity and phase-aligned vibration estimation.

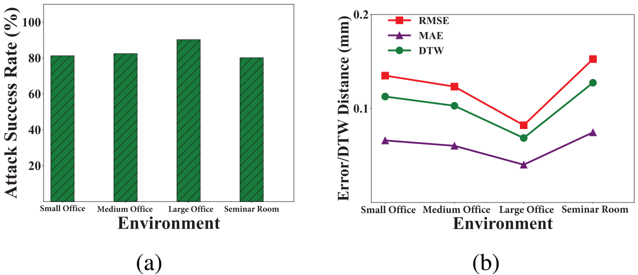
### F. Evaluation with Varied Conditions

*1) Impact of Distance Variation:* We conduct a series of experiments in which the adversary, equipped with the concealed actuator system, is positioned at different distances from the mmWave sensing device. The tested distances range from 40 cm to 120 cm, covering typical deployment scenarios for chest vibration sensing applications. For each distance setting, the adversary executes multiple attack trials where the actuator replicates the target user's chest vibrations while interference mitigation is applied in real time. Figure 12 shows that success rates were highest at shorter distances (i.e., 92% at 60cm) and gradually decline with increasing distance (i.e., 78% at 120cm) and error metrics further illustrate this trend. These results demonstrate that our attack performs optimally at typical usage distances for chest vibration sensing systems.



(a) (b)

Fig. 12: Impact of varying radar-to-human distance on attack success rate. (a) Attack success rate across five different distances. (b) Corresponding error metrics, including RMSE, MAE, and DTW distance.



(a) (b)

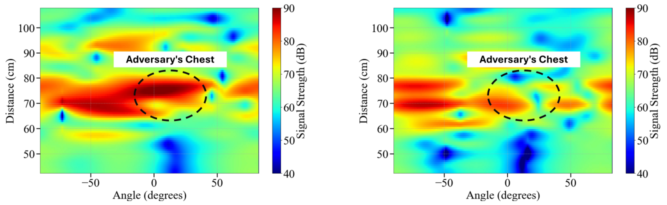
Fig. 13: Impact of different environments on attack success rate. (a) Attack success rate across four different environments. (b) Corresponding error metrics, including RMSE, MAE, and DTW distance.

*2) Impact of Environmental Factors:* We conduct experiments across four distinct indoor environments: three office settings with different size and a seminar room, each with varying levels of background interference, furniture arrangements, and ambient conditions. In each environment, we maintain a consistent experimental setup, where the adversary, equipped with the concealed actuator system, attempts to spoof the mmWave-based chest vibration sensing system. As shown in Figure 13, our system maintains consistently high success rates (81%-89%) across four environments. Large office shows the highest performance at 89%, while the seminar room demonstrates the lowest performance at 81%. Performance metrics include DTW distances in a low range of 0.06-0.09, with minimal RMSE and consistent low MAE values across different environments.

## VI. Discussions

### A. Suppressing Self-Induced Reflections via RF-Absorbing Materials

To counter potential countermeasures that leverage beamforming to detect inconsistencies in chest vibrations, we explore the use of RF-absorbing materials to suppress unwanted reflections from the adversary's body. In some systems, mmWave radars may perform angular scans to localize chest motion signatures and detect impersonation by comparing signals across spatial directions. To remain stealthy under such detection schemes, an adversary can strategically deploy lightweight, concealable RF-absorbing sheets beneath their clothing [31], [32]. These materials are placed to cover the upper torso while intentionally leaving the area where the actuator-induced vibration is applied uncovered. We experimentally evaluate the effectiveness of this strategy by comparing the range-angle heatmaps with and without RF-absorbing materials as shown in Figure 14. Without absorption, the radar captures strong reflections from the adversary's chest, potentially revealing unintended vital signs. When the RF-absorbing sheet is applied, these reflections are significantly suppressed, making it more difficult for the radar to detect the adversary's chest region or distinguish real vibrations. This result demonstrates the feasibility of enhancing spoofing stealth using low-cost, passive materials.



(a) (b)

Fig. 14: Impact of RF-absorbing material on radar perception. (a) Range-angle heatmap without RF-absorbing material. (b) Heatmap with RF-absorbing material applied to the adversary's chest, showing reduced signal reflection.

### *B. Countermeasures*

To enhance system resilience against our proposed attack, we discuss two potential countermeasures. **(1) Multimodal consistency checking.** When an adversary uses RF-absorbing materials to suppress natural chest vibrations and expose only actuator output (Section VI-A), the target system can perform cross-region verification. The mmWave radar dynamically steers its beam to the face to capture subtle respiratory and vascular vibrations. Although facial and chest waveforms differ, prior work shows physiological coupling across body regions [33], [34]. Correlating chest and facial signatures over time enables authenticity checks and detection of actuator-only spoofing. **(2) User-centric privacy protection.** Users can employ physical obfuscation to disrupt the emission or propagation of their physiological vibrations. VitalHide [35] demonstrates masking vital signs to prevent unauthorized mmWave sensing. Such techniques reduce the risk of passive physiological surveillance and complement system-side defenses.

## VII. Related Work

**mmWave-based Chest Vibration Sensing.** Recently, mmWave-based chest vibration sensing has experienced significant growth, driven by the high resolution [36], [37] and large bandwidth [38] of mmWave signals. Numerous applications have emerged, such as user authentication [14], [15], [39] and vital sign monitoring [3], [10]–[12]. In user authentication, for example, M-Auth employs mmWave for user authentication by capturing the user's unique breathing pattern. It exploits the phenomenon that mmWave signals are affected by chest displacements due to breathing [15]. Similarly, in vital sign monitoring, mmHRV leverages mmWave signals to measure heart rates accurately by optimizing the decomposition of the signal phase modulated by chest movements [10].

**Digital Spoofing Attacks.** Researchers have uncovered the susceptibility of mmWave-based sensing systems to spoofing through direct manipulation of digital representations such as range-Doppler maps or point clouds [17]–[19]. For example, Ozbulak *et al.* examine how human activity recognition (HAR) systems based on mmWave radar can be misled by injecting perturbations into range-Doppler frames, causing incorrect activity classification [18]. Xie *et al.* further propose a universal spoofing method that precomputes perturbations and applies them to mmWave point cloud data, consistently inducing the model to output a target activity label [17]. However, such digital attacks usually assume that the adversary has access to users' sensing systems and can directly alter digital mmWave data, which are often impractical in real-world scenarios.

**Physical Spoofing Attacks.** Recent research has investigated physical spoofing attacks that manipulate mmWave signals at the physical layer [20], [21], [40]–[42]. For instance, Nallabolu *et al.* utilize radio frequency mixers (e.g., HMC525ALC4 SSB) to generate synthetic vital sign signatures, enabling spoofing attacks on Doppler and FMCW radars used for human monitoring [20]. Building on this direction, MadRadar [40] and mmSpoof [41] employ software-defined radios (e.g., USRP B210) to precisely manipulate signal characteristics such as frequency, phase, and amplitude, thereby altering the perceived radar scene. However, these methods rely on bulky and specialized hardware, limiting their portability and practicality in stealthy or real-time attack scenarios, as discussed in Section III. MetaWave [32] introduces metamaterial-enhanced tags that can modulate reflected mmWave signals to spoof sensing measurements such as range, angle, and velocity. Nonetheless, this approach does not capture the dynamic relationship between human chest motion and mmWave signal reflections. In contrast, our work develops a practical and low-cost spoofing method that uses a programmable actuator to physically replicate target chest vibrations. The actuator's compact form factor allows it to be concealed under clothing, enabling real-time, stealthy spoofing attacks against mmWave-based chest vibration sensing systems.

## VIII. Conclusion

In this work, we presented the first practical demonstration of a real-time physical-layer spoofing attack against mmWave-based chest vibration sensing systems. By leveraging a compact and programmable actuator concealed beneath clothing, an adversary can precisely reproduce a target user's chest vibration patterns, effectively deceiving systems designed for vital sign monitoring and authentication. To address challenges from the adversary's own chest motion, we integrate an IMU-assisted compensation framework with quaternion-based coordinate alignment, enabling stable and high-fidelity vibration control. In addition, we incorporate a hybrid LSTM-CNN architecture to predict and compensate motion interference in real time, ensuring temporal precision and robustness under dynamic conditions. Extensive experiments across diverse deployment scenarios confirm the feasibility and effectiveness of our attack. As mmWave vibration sensing gains adoption in healthcare monitoring and security-critical applications, our findings uncover a fundamental security vulnerability and call for urgent development of resilient sensing architectures and countermeasures against actuator-induced physical spoofing.

**Acknowledgment.** This work was partially supported by the National Science Foundation Grants CNS2304766, CNS2329280, CNS2329278, CNS2120396, CNS2120350, CNS2120276, CNS2329279, CNS2145389, III2311598, DGE2414365 and DGE2414367.

# References

[1] C. Wu, F. Zhang, B. Wang, and K. R. Liu, "msense: Towards mobile material sensing with a single millimeter-wave radio," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2020.

[2] Y. Wu, H. Ni, C. Mao, J. Han, and W. Xu, "Non-intrusive human vital sign detection using mmwave sensing technologies: A review," *ACM Transactions on Sensor Networks*, 2023.

[3] F. Wang, F. Zhang, C. Wu, B. Wang, and K. R. Liu, "Vimo: Multiperson vital sign monitoring using commodity millimeter-wave radio," *IEEE Internet of Things Journal*, 2020.

[4] Z. Gao, L. Ali, C. Wang, R. Liu, C. Wang, C. Qian, H. Sung, and F. Meng, "Real-time non-contact millimeter wave radar-based vital sign detection," *Sensors*, 2022.

[5] L. Liu, J. Zhang, Y. Qu, S. Zhang, and W. Xiao, "mmrh: Noncontact vital sign detection with an fmcw mm-wave radar," *IEEE Sensors Journal*, 2023.

[6] 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 *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020.

[7] Y. Dong and Y.-D. Yao, "Secure mmwave-radar-based speaker verification for iot smart home," *IEEE Internet of Things Journal*, 2020.

[8] H. Dai, R. Zheng, X. Ma, Z. Lu, G. Sun, Z. Xu, C. Fan, and M. Wu, "Adaptive tracking strategy for the positioning of millimeter-wave radar security robots," *IEEE Sensors Journal*, 2024.

[9] P. Zhao, C. X. Lu, J. Wang, C. Chen, W. Wang, N. Trigoni, and A. Markham, "Human tracking and identification through a millimeter wave radar," *Ad Hoc Networks*, 2021.

[10] F. Wang, X. Zeng, C. Wu, B. Wang, and K. R. Liu, "mmhrv: Contactless heart rate variability monitoring using millimeter-wave radio," *IEEE Internet of Things Journal*, 2021.

[11] H. Wang, F. Du, H. Zhu, Z. Zhang, Y. Wang, Q. Cao, and X. Zhu, "Here: Heartbeat signal reconstruction for low-power millimeter-wave radar based on deep learning," *IEEE Transactions on Instrumentation and Measurement*, 2023.

[12] U. Ha, S. Assana, and F. Adib, "Contactless seismocardiography via deep learning radars," in *Proceedings of the 26th annual international conference on mobile computing and networking*, 2020.

[13] Z. Shi, T. Gu, Y. Zhang, and X. Zhang, "mmbp: Contact-free millimetre-wave radar based approach to blood pressure measurement," in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, 2022.

[14] Y. Wang, T. Gu, T. H. Luan, M. Lyu, and Y. Li, "Heartprint: Exploring a heartbeat-based multiuser authentication with single mmwave radar," *IEEE Internet of Things Journal*, 2022.

[15] 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 *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*.

[16] J. Peng, Z. Hao, Z. Zhang, R. Wang, M. Li, and X. Dang, "Utter innocence: Contactless authentication method based on physiological signals," *IEEE Sensors Journal*, 2024.

[17] Y. Xie, X. Guo, Y. Wang, J. Cheng, and Y. Chen, "Universal targeted adversarial attacks against mmwave-based human activity recognition," in *Network Security Empowered by Artificial Intelligence*.

[18] U. Ozbulak, B. Vandersmissen, A. Jalalvand, I. Couckuyt, A. Van Messem, and W. De Neve, "Investigating the significance of adversarial attacks and their relation to interpretability for radar-based human activity recognition systems," *Computer Vision and Image Understanding*, 2021.

[19] Z. Yang, Y. Zhao, and W. Yan, "Adversarial vulnerability in doppler-based human activity recognition," in *2020 international joint conference on neural networks (IJCNN)*. IEEE.

[20] P. Nallabolu, D. Rodriguez, and C. Li, "Emulation and malicious attacks to doppler and fmcw radars for human sensing applications," *IEEE Transactions on Microwave Theory and Techniques*, 2022.

[21] P. Nallabolu and C. Li, "A frequency-domain spoofing attack on fmcw radars and its mitigation technique based on a hybrid-chirp waveform," *IEEE Transactions on Microwave Theory and Techniques*, 2021.

[22] Xeryon, "Xla series - next generation of micro linear actuators," , 2025.

[23] E. Sadeghi, K. Skurule, A. Chiumento, and P. Havinga, "Comprehensive mm-wave fmcw radar dataset for vital sign monitoring: Embracing extreme physiological scenarios," *arXiv preprint arXiv:2405.12659*, 2024.

[24] M. Chan, L. Klein, J. Fan, and O. Inan, "Scg-rhc: Wearable seismocardiogram signal and right heart catheter database," 2023.

[25] S. Balocco, T. S. Lande, B. Zhou, F. d. Boer, and P. J. Havinga, "Mm-wave fmcw radar vital sign monitoring dataset: Diverse physiological and environmental scenarios," 2023. [Online]. Available:

[26] J. Peng, X. Zhang, and H. Li, "A lstm-based fall prediction method using imu," in *IFToMM Asian conference on Mechanism and Machine Science*. Springer, 2021.

[27] Phidgets Inc., "Phidgets - product page," 2025. [Online]. Available:

[28] Texas Instruments, "Awr1642 - single-chip 76-ghz to 81-ghz automotive radar sensor," 2025. [Online]. Available:

[29] ——, "DCA1000EVM: Data Capture Adapter for Radar Sensing Evaluation," , 2025, accessed: July 2025.

[30] S. Wei, Z. Hu, and L. Tan, "Res-eca-unet++: an automatic segmentation model for ovarian tumor ultrasound images based on residual networks and channel attention mechanism," *Frontiers in Medicine*, 2025.

[31] L. Technologies, "Eccosorb® hr - microwave absorbing foams," , 2023.

[32] 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 *The 30th Network and Distributed System Security (NDSS) Symposium 2023*. The Internet Society, 2023.

[33] N. Avilés-Rojas and D. E. Hurtado, "Whole-lung finite-element models for mechanical ventilation and respiratory research applications," *Frontiers in Physiology*, 2022.

[34] M. W. Mohiuddin, R. J. Rihani, G. A. Laine, and C. M. Quick, "Increasing pulse wave velocity in a realistic cardiovascular model does not increase pulse pressure with age," *American Journal of Physiology-Heart and Circulatory Physiology*, 2012.

[35] Y. Gao, T. Ahmed, Z. Chang, T. Roumen, and R. Nandakumar, "Vitalhide: Enabling privacy-aware wireless sensing of vital signs," in *Proceedings of the 26th International Workshop on Mobile Computing Systems and Applications*, 2025.

[36] Y. Ge, Y. Wei, X. Guo, Y. Xie, Y. Wang, J. Cheng, and Y. Chen, "Towards contactless human concentration monitoring using mmwave signals," in *2024 IEEE 10th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2024, pp. 19–28.

[37] Y. Xie, X. Guo, Y. Wang, J. Q. Cheng, T. Zhang, Y. Chen, Y. Wei, and Y. Ge, "mmpalm: Unlocking ubiquitous user authentication through palm recognition with mmwave signals," in *2024 IEEE Conference on Communications and Network Security (CNS)*.

[38] Y. Xie, T. Zhang, X. Guo, Y. Wang, J. Cheng, Y. Chen, Y. Wei, and Y. Ge, "Palm-based user authentication through mmwave," in *2024 IEEE 44th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2024, pp. 1472–1473.

[39] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017.

[40] D. Hunt, K. Angell, Z. Qi, T. Chen, and M. Pajic, "Madradar: A black-box physical layer attack framework on mmwave automotive fmcw radars," *arXiv preprint arXiv:2311.16024*, 2023.

[41] R. R. 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 *2023 IEEE Symposium on Security and Privacy (SP)*, 2023.

[42] 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*, 2021.