

PrivyWave: Privacy-Aware Wireless Sensing of Heart Beat

YIXUAN GAO*, Cornell Tech, USA

TANVIR AHMED*, Cornell Tech, USA

ZEKUN CHANG, Cornell Tech, USA

THIJS ROUMEN, Cornell Tech, USA

RAJALAKSHMI NANDAKUMAR, Cornell Tech, USA

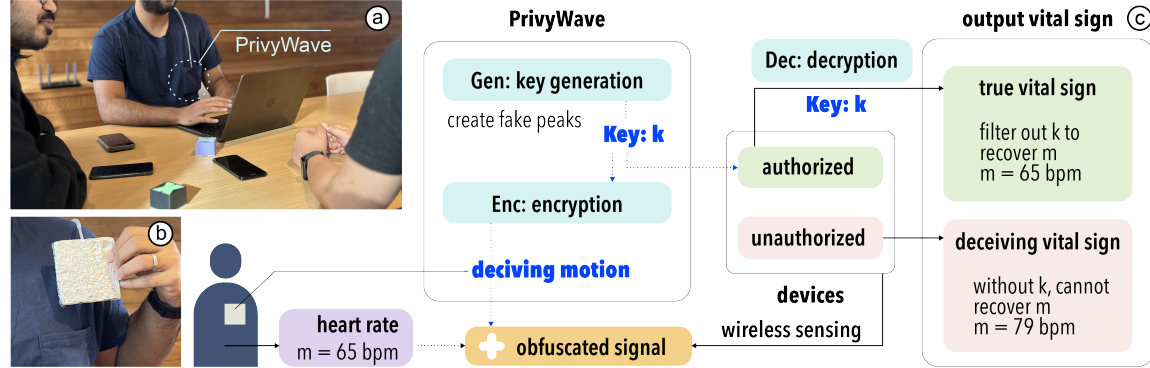


Fig. 1. PrivyWave system overview. (a) A person wearing PrivyWave in office, surrounded by ubiquitous devices (e.g., mobile phones, laptops, speakers, Wi-Fi router) that could potentially function as wireless sensors to pick up vital signal from people without them noticing. (b) PrivyWave pneumatic actuator device. (c) System workflow: key generation creates decoy signal frequencies k , encryption superimposes decoy motion on true vital sign m using the actuator, and authorized devices use k to decrypt and recover the true signal while unauthorized devices observe one of the decoy signals.

Wireless sensing technologies can now detect heartbeats using radio frequency and acoustic signals, raising significant privacy concerns. Existing privacy solutions either protect from all sensing systems indiscriminately preventing any utility or operate post-data collection, failing to enable selective access where authorized devices can monitor while unauthorized ones cannot. We present a key-based physical obfuscation system, PrivyWave, that addresses this challenge by generating controlled decoy heartbeat signals at cryptographically-determined frequencies. Unauthorized sensors receive a mixture of real and decoy signals that are indistinguishable without the secret key, while authorized sensors use the key to filter out decoys and recover accurate measurements. Our evaluation with 13 participants demonstrates effective protection across both sensing modalities: for mmWave radar, unauthorized sensors show 21.3 BPM mean absolute error while authorized sensors maintain a much smaller 5.8 BPM; for acoustic sensing, unauthorized error increases to 42.0 BPM while authorized sensors achieve 9.7 BPM. The system operates across multiple sensing modalities without per-modality customization and provides cryptographic obfuscation guarantees. Performance benchmarks show robust protection across different distances (30-150 cm), orientations (120° field of view), and diverse indoor environments, establishing physical-layer obfuscation as a viable approach for selective privacy in pervasive health monitoring.

CCS Concepts: • **Security and privacy** → **Privacy protections**.

*Both authors contributed equally to this research.

Authors' Contact Information: Yixuan Gao, yixuan@cs.cornell.edu, Cornell Tech, New York, New York, USA; Tanvir Ahmed, tanvir@infosci.cornell.edu, Cornell Tech, New York, New York, USA; Zekun Chang, zekunchang@infosci.cornell.edu, Cornell Tech, New York, New York, USA; Thijs Roumen, thijs.roumen@cornell.edu, Cornell Tech, New York, New York, USA; Rajalakshmi Nandakumar, rajalakshmi.nandakumar@cornell.edu, Cornell Tech, New York, New York, USA.

Additional Key Words and Phrases: Privacy, Wireless Sensing, Smart Textile

1 Introduction

Wireless sensing technologies have advanced rapidly in recent years. Systems using acoustic [18], WiFi [1], and millimeter-wave (mmWave) [32] sensors can now monitor vital signs without any physical contact, detecting chest movements as small as few millimeters to measure breathing and heartbeat. These capabilities enable critical healthcare applications, such as detecting sleep apnea [18], identifying opioid overdoses [17], even detecting cardiac arrest and calling emergency services [5] all without requiring users to wear sensors.

However, these same technological capabilities that promise healthcare benefits also create privacy risks. Any ambient device such as a WiFi router, smart speaker, home assistant or someone’s smartphone, can potentially become a covert physiological signal monitor, silently extracting vital signs without user awareness or consent. This threat is particularly concerning because vital signs reveal far more than basic metrics, they could expose emotional states [34], or stress levels [9] that may even indicate mental health conditions. In addition, some wireless signals are invisible and penetrate walls and clothing, creating an omnipresent surveillance risk which is hard for users to detect or avoid. So as wireless sensing becomes ubiquitous, developing solutions that maintain its practical benefits while preventing unauthorized surveillance is a necessity.

Existing privacy protection approaches for wireless signals fall into two categories: post-collection data processing and real-time protection. Post-collection approaches [10, 14, 24] protect data after acquisition through techniques such as data aggregation [24], differential privacy [10], and signal tampering [14]. However, these methods cannot prevent unauthorized sensing in the first place, as adversaries can collect raw signals in real-time before any post-collection protection is applied. For real-time protection, jamming methods [6, 22, 33] inject noise to degrade signal quality, but they are modality-specific—protecting against one type of sensor (e.g., acoustic) but not others (e.g., radio-frequency or RF). Anti-Sensing [19] uses wearable oscillators to mislead radar-based heartbeat detection, but blocks all sensors indiscriminately. VitalHide [7] presented the first approach for selective protection using vibration-based obfuscation. However, this work remained conceptual, lacking theoretical foundations, formal privacy analysis, and systematic validation.

We present *PrivyWave*, a combined software and hardware solution that protects users from unauthorized wireless monitoring while preserving the full utility of authorized sensing. Our central idea is to enable private wireless sensing using decodable physical-layer obfuscation technique. We generate controlled, physical actuation co-located with the user’s body, which mimics the periodic motion of vital signs (e.g., a heartbeat) to create plausible decoy signals. Since wireless sensing systems operate by detecting such periodic motions, an unauthorized sensor observing the user perceives a composite *obfuscated* signal and is unable to distinguish the user’s true vital sign from the decoys. Conversely, an authorized system, possessing a shared cryptographic key, can computationally identify and filter out these decoy signals, thereby recovering the user’s true signal with high fidelity. Our system overview is given in Fig. 1.

This method has two main advantages i) The obfuscation is done by generating fake motions and hence this method is agnostic to different wireless modalities and frequencies such as acoustic, RF (WiFi, mmWave). ii) The generated decoy signals are similar to legitimate physiological signals which the unauthorized devices cannot distinguish.

In this work, first, we design a cryptographic framework for physical-layer obfuscation that provides a privacy guarantee. We define (1) a key generation procedure for creating valid decoy signal frequencies to obfuscate the true signal, (2) an encryption algorithm that physically generates these decoys through actuation and obfuscates true vital signal, and finally (3) a decryption algorithm that enables authorized devices to recover the true signal by filtering

out known decoy frequencies with they key. We mathematically show that unauthorized attackers gain negligible distinguishing advantage from random guessing among the decoy frequencies. Second, we implement this framework through a compact silicone-based pneumatic prototype design that generates heartbeat-like actuation patterns while fitting inside the user’s pocket. Third, we experimentally validate that our system works across multiple sensing modalities: frequency-modulated continuous wave (FMCW) mmWave radars and acoustic sonars, demonstrating modality-agnostic protection.

We validate *PrivyWave* for mmWave and acoustic systems through a user study with 13 participants. The results show that detection error and standard deviation for unauthorized sensor is significantly higher ($p < .001$) than for authorized devices. For heart rate detection, the average mean absolute error (MAE) for mmWave unauthorized and authorized devices are 21.3 and 5.8 BPM, while for acoustic are 42 and 9.7 BPM respectively. We also show the effectiveness of *PrivyWave* in different environments as well as different radar range and orientation. These results demonstrate that *PrivyWave* enables a new paradigm for wireless vital sign sensing, one where users can benefit from continuous wireless health monitoring while not having to worry about unwanted surveillance.

In this work, we explore the possibility of preserving the utility of wireless sensing while giving users agency over their privacy. From developing a cryptographic obfuscation framework for physical signals to building actual hardware systems, this work demonstrates that functionality and strong privacy protection can coexist in wireless sensing systems. To summarize, our key contributions are:

- We design and build the first motion-based, modality-agnostic, and privacy-preserving physical layer obfuscation wireless sensing system for vital sign monitoring called *PrivyWave* that protects against unauthorized monitoring while keeping the full utility of authorized devices.
- We provide a mathematical bound for the unauthorized attacker’s distinguishing advantage for the designed physical layer obfuscation system.
- We demonstrate the effectiveness of *PrivyWave* through a comprehensive user study and micro-benchmarks, which shows a significantly higher detection error for unauthorized devices.

2 Related Work

We discuss existing approaches for wireless vital sign privacy protection. We first review the capabilities of wireless vital sign sensing systems and their privacy implications. We then examine the current SOTA privacy protection solutions for wireless sensing, categorized into post-processing and real-time protection approaches. We then focus particularly on real-time protection systems, which can be further divided into jamming-based and obfuscation-based methods.

2.1 Wireless Vital Sign Sensing and Privacy Implications

Wireless vital sign sensing has evolved into reliable systems with high accuracy. Many smart devices have gained the ability to accurately detect vital signs without physical contact. Nandakumar et al. [18] demonstrated that smartphones can be turned into vital sign monitors by leveraging the acoustic sensors in the device. WiFi-based approaches extract breathing and heartbeat from the RF signals reflected by the subject [1, 15]. The mmWave sensors, commonly deployed for presence detection, can also measure breathing and heartbeat with high precision [8, 32]. These sensing capabilities have enabled beneficial applications in everyday life. Researchers have developed systems for sleep apnea detection [18], which can alert users to potentially dangerous breathing interruptions during sleep. Contactless vital sign monitoring has been proposed for overdose detection [17], enabling earlier intervention in emergency situations. Cardiac arrest

Table 1. Comparison of Privacy Protection Approaches

Approach	Target Domain	Real-Time Protect.	Selective Protect.	Multi-Modal	Security Guarantee	Auth. Access
<i>Post-Collection Processing</i>						
PriSense [24]	Sensor Data	✗	✗	✓	✓	N/A
Diff. Privacy [10]	Sensor Data	✗	✗	✓	✓	N/A
mmFilter [14]	mmWave Radar	✗	✓ [‡]	✗	✗	N/A
<i>Real-Time Jamming</i>						
Wearable Jammer [6]	Audio	✓	✗	✗	✗	✗
Dynamic Jamming [33]	Audio	✓	✗	✗	✗	✗
NUSGuard [22]	Voice	✓	✓ [†]	✗	✗	✓ [†]
<i>Real-Time Obfuscation</i>						
RF-Protect [23]	Human Tracking	✓	✗	✗	✗	✗
Radar Obfus. [3]	Activity	✓	✗	✗	✗	✗
Anti-Sensing [19]	Vital Signs	✓	✗	✓	✗	✗
VitalHide [7]	Vital Signs	✓	✓ [*]	✓ [*]	✗	✓ [*]
PrivyWave (Ours)	Vital Signs	✓	✓	✓	✓	✓

^{*}Proof-of-concept only; [†]Temporal selectivity only; [‡]Application-level, not device-level

✓: Supported; ✗: Not supported; N/A: Not applicable

detection systems [5] can automatically alert emergency services when abnormal vital signs are detected. However, vital signals carry far more information than just physiological measurements. Stress levels can be inferred from vital signals [9], emotional states can be detected from combined respiratory and cardiac patterns [34], and cognitive load during mental tasks can be assessed through cardiovascular responses [25]. As sensing accuracy continues to improve, the precision of these inferences also increases, making the privacy risks more severe.

This dual nature of wireless vital sign detection, which simultaneously allows beneficial health monitoring and creates unprecedented privacy risks, motivates the need for privacy protection mechanisms that can distinguish between authorized and unauthorized detection.

2.2 Privacy Protection for Wireless Sensing

We categorize existing privacy protection approaches for wireless signals into two main strategies: post-collection data processing and real-time signal protection.

2.2.1 Post-Collection Data Processing. There are a set of algorithms that focuses on protecting data after it has been collected by sensors. These approaches assume that sensing has already occurred and apply privacy-preserving techniques during subsequent processing, transmission, or storage stages. PriSense [24] introduced privacy-preserving data aggregation for sensor networks using data slicing, where each sensor splits its reading into multiple shares distributed to randomly selected cover nodes, protecting individual data unless the aggregation server colludes with all cover nodes. Differential privacy approaches [10] provide stronger theoretical guarantees by adding calibrated noise to sensor data datasets, ensuring that the presence or absence of any individual’s data cannot be reliably determined while preserving aggregate statistics. For mmWave radar-based sensing, mmFilter [14] applies signal reversion techniques that tamper with radar data after collection but before transmission to sensing processors. While these post-collection methods provide valuable privacy protections for captured data, they share a fundamental limitation: they cannot

prevent unauthorized sensing in the first place. An adversary can still collect the raw signals before any privacy protection is applied.

2.2.2 Real-Time Signal Protection. To enable protection against unauthorized sensing in real-time, researchers have developed technologies that mainly fall into two categories: jamming and obfuscation.

Jamming-Based Protection. Jamming approaches inject noise or interference to degrade signal quality (decrease SNR) for unauthorized receivers. For audio privacy, ultrasonic jamming exploits microphone nonlinearity: high-frequency ultrasonic signals cause microphones to produce audible-range noise, corrupting recordings. Chen et al. [6] developed a wearable bracelet with 24 ultrasonic transducers providing omnidirectional microphone jamming. Yu et al. [33] improved efficiency through adaptive jamming that analyzes speech characteristics in real-time and generates time-frequency interference patterns matched to audio content. NUSGuard [22] introduces temporal selectivity by detecting when users interact with authorized voice assistants, temporarily disabling jamming during those interactions. However, jamming approaches face fundamental limitations. Jamming is inherently modality-specific: it protects against one type of sensing signal, for example acoustic, but not RF or other sensing modalities, and vice versa, and we do not have control over what modality an unauthorized sensor uses.

Obfuscation-Based Protection. Obfuscation techniques inject plausible decoy information rather than noise, making it difficult to distinguish true signals from fake alternatives [4]. The core principle is to hide the real signal among believable decoys. For human tracking, RF-Protect [23] introduced a hardware reflector-based approach that injects phantom humans into device-free tracking systems. The system uses specially designed reflectors to modify radio waves and create reflections at arbitrary locations, combined with a generative model to create realistic human trajectories. For activity recognition, Argyriou [3] demonstrated that synthetic motion patterns can obfuscate human micro-Doppler signatures in passive radar. For vital sign protection, Anti-Sensing [19] uses wearable oscillators that generate motion patterns mimicking natural cardiac motion, creating decoy signals that mislead radar-based heartbeat detection. While the approach successfully generates realistic oscillatory patterns, it blocks all radar sensors indiscriminately without providing selective access for authorized monitoring. VitalHide [7] recently explored whether phone vibrators and smart textile actuators could generate physical obfuscation for vital signs, creating decoy heartbeat signals to confuse unauthorized sensors while potentially allowing authorized devices to filter them out. The proof-of-concept showed that vibration-based obfuscation could reduce unauthorized detection accuracy. However, this work remained at the conceptual demonstration stage, lacking theoretical foundations, formal security analysis, and systematic validation of the selective access mechanism across different sensing modalities.

Our work builds on the obfuscation approach but provides key advances: (1) a formal cryptographic framework for key-based selective access, including key generation, encoding, and decoding algorithms, (2) security analysis with provable guarantees for authorized and unauthorized scenarios, (3) wearable hardware designs that realize this framework on the human body, (4) systematic evaluation across multiple sensing modalities (mmWave and acoustic), and (5) performance benchmarks under varying physical conditions. Our system enables authorized monitoring while protecting against unauthorized sensing through cryptographic key-based decoy filtering.

3 background - FMCW radar

Frequency Modulated Continuous Wave (FMCW) [27] has emerged as the preferred technology for contactless vital sign monitoring due to its ability to detect sub-millimeter movements with high precision without the need for sampling

signal at carrier frequency. This capability enables FMCW radar to be implemented across a variety of signal modalities. In this section, we cover the FMCW radar theory and signal processing techniques used for extracting vital signs. We will then explain the design of *PrivyWave* that can protect the subjects from unauthorized sensors that run these algorithms to extract physiological signals.

3.1 FMCW Theory

The FMCW system transmits a chirp signal $s_{tx}(t)$, a sinusoid whose frequency increases linearly over time:

$$s_{tx}(t) = A_t \exp \left(j2\pi \left(f_c t + \frac{B}{2T_{chirp}} t^2 \right) \right) \quad (1)$$

where f_c is the carrier frequency, B is the bandwidth, and T_{chirp} is the chirp duration. When this chirp reflects off a target at distance $d(t) = d_0 + x(t)$, where $x(t)$ represents chest displacement from breathing and heartbeat, the received signal experiences a time delay $\tau = 2d(t)/c$:

$$s_{rx}(t) = A_r \exp \left(j2\pi \left(f_c (t - \tau) + \frac{B}{2T_{chirp}} (t - \tau)^2 \right) \right) \quad (2)$$

After dechirping (mixing transmitted and received signals), the intermediate frequency (IF) signal contains two critical phase components:

$$s_{IF}(t) = A_{IF} \exp \left(j \underbrace{\frac{4\pi B d(t)}{c T_{chirp}} t}_{\text{beat frequency}} + j \underbrace{\frac{4\pi f_c d(t)}{c}}_{\text{phase from displacement}} \right) \quad (3)$$

These two phase terms serve distinct purposes in vital sign sensing. The first term, $\frac{4\pi B d(t)}{c T_{chirp}} t$, represents a beat frequency that is proportional to the target distance $d(t)$. This term enables range separation: by applying FFT over samples within a single chirp (typically 50-100 microseconds), we obtain a range profile where echoes from different distances produce distinct frequency peaks. The range resolution is determined by the bandwidth: $\Delta R = c/(2B)$.

The second term, $\phi(t) = 4\pi f_c d(t)/c = 4\pi d(t)/\lambda$, is the phase component that encodes fine-grained displacement information. Within a single chirp duration, this phase remains approximately constant since the chest displacement $x(t)$ changes negligibly over microseconds. However, across multiple chirps (frame period typically 20-50 milliseconds), this phase evolves as the chest moves due to breathing and heartbeat. By tracking this phase evolution across consecutive chirps, we extract the time-varying displacement signal:

$$x(t) = \frac{\lambda}{4\pi} \phi(t) \quad (4)$$

3.2 Signal Processing Methods for Vital Sign Extraction

Once displacement $x(t)$ is extracted, various methods process it to isolate vital signs.

Non-Learning-Based signal processing Methods. Peak detection algorithms [2] identify local maxima and minima in $x(t)$ corresponding to breathing cycles or cardiac phases, determining instantaneous rates from time intervals between peaks. FFT-based methods apply bandpass filtering to isolate specific frequency ranges (0.1–0.5 Hz for breathing, 0.8–2.0 Hz for heart rate), identifying peak frequencies as vital sign rates [2, 13]. Time-frequency decomposition techniques EMD/EEMD [31], VMD [35], and wavelet transforms [30] decompose the displacement signal into simpler signal components for analysis.

Learning-Based Methods. Deep learning approaches train neural networks on the features that include the displacement $x(t)$ [12, 29] to estimate vital signs. These methods handle complex scenarios including multi-person environments [28] and low SNR conditions, but require substantial labeled data and may not generalize across deployment environments.

3.3 Different modalities of wireless sensing

While both RF and acoustic systems apply identical FMCW principles and similar signal processing methods described above, they operate at different ranges with distinct trade-offs. Millimeter-wave radar transmits and receives RF signal of frequency range 60–77 GHz that travel at the speed of light. They achieve a millimeter level range resolution and a range of 3 to 5 meters and can penetrate clothes. However they require specialized hardware. WiFi based RF radars operate at 2.4 and 5 GHz and has similar properties where they can penetrate even through walls. However they also require specialized hardware such as expensive USRP. Acoustic FMCW (18–22 kHz) achieves millimeter level range resolution on commodity smartphones as the speed of sound is much lower than RF ($c_{sound} \approx 343$ m/s), but the range of the system is limited to 0.5–1.5 meters with poor penetration and high noise susceptibility. The choice reflects deployment context: acoustic systems democratize sensing through ubiquitous devices for close-proximity applications, while RF based systems such as WiFi and mmWave enables through-clothing monitoring at larger distances essential for privacy-sensitive scenarios.

In order to build a system that can hide from unauthorized sensors without depending on what modality they use and what algorithms they used, we need to build physical obfuscation: co-located fake heartbeat signals on the human body.

Despite the differences in the algorithmic diversity, all these systems record the reflections of custom frequency signals and analyze the variations caused by sub-centimeter motion generated from the human body. Hence, a co-located heartbeat generator with the human would obfuscate all sensing algorithms. For example, peak-detection algorithms will be confused by the peaks induced by the fake heartbeat, while frequency-dependent algorithms will be confused by the new frequency components added by the fake heart rate.

4 System Design

4.1 System Overview

To guarantee privacy against different sensing modality (e.g., acoustic and mmWave) that could run any signal processing algorithm, we designed *PrivyWave*, which operates by generating controlled heartbeat-like motions using a pneumatic-based device prototype. We carefully design the obfuscation mechanism so that a single device can generate multiple different-frequency heartbeat-like signals in real time. From an unauthorized sensor’s perspective, it will detect multiple heartbeat signals with the real one immersed among them, while authorized sensors that possess the cryptographic key can recover the true signal from the obfuscated composite signal.

We introduce our system by first formally formulating the problem and defining the threat model. We then present the obfuscation algorithm that describes how we generate the obfuscation signals, how these signals are encoded, and how authorized sensors can decode them. This is followed by a formal privacy bound analysis. Finally, we show how we implement the obfuscation scheme on a hardware prototype.

4.2 Problem Formulation

Our goal is to design a system that could enable provable secure wireless vital sign monitoring where authorized devices can accurately monitor within a negligible error, while unauthorized devices are prevented from extracting meaningful information in real-time.

From the lens of cryptography theory, the task of privacy-preserving wireless vital sign sensing system can be seen as a "secure communication" event. The user ($\mathcal{U}$) whose vital signs is to be protected becomes the *sender* (aka Alice), the vital sign is the *private message* (m) that the user is trying to send to an authorized wireless sensing system (aka Bob), who becomes the *receiver* ($\mathcal{V}$). The unauthorized wireless sensing systems, who try to intercept the *private message* becomes the *adversary* ($\mathcal{A}$) (aka Eve). In this work, we take a physical layer obfuscation approach, which *obfuscates* m into a ciphertext c , to provide privacy to the user.

4.3 Threat Model

We model the adversary $\mathcal{A}$ as a passive eavesdropper seeking to measure the user's vital signs through wireless sensing. We assume $\mathcal{A}$ is computationally bounded (a probabilistic polynomial-time adversary) and operates under the following conditions:

- **System Knowledge:** $\mathcal{A}$ has complete knowledge of the system design, algorithms, and probability distributions (per Kerckhoffs's Principle). Security relies solely on the secrecy of the session-specific cryptographic key (k), which defines the decoy signal frequencies.
- **Sensing Capabilities:** $\mathcal{A}$ can deploy arbitrary wireless sensing equipment (e.g., mmWave radar, acoustic FMCW sensors) with any number of antennas and apply any signal processing algorithm to extract vital signs.
- **Spatial Resolution Limit:** $\mathcal{A}$ cannot spatially separate the user's true vital sign motion from the co-located decoy motion generated by *PrivyWave*. Both signals originate from the same location on the user's body and are perceived by the sensor as a single, superimposed signal with multiple frequency components.
- **Passive Attack Constraint:** $\mathcal{A}$ is restricted to passive observation only. The model excludes active attacks such as stimulus-response probing (e.g., inducing a physical startle to identify reactive vs. non-reactive signals). Defending against such active attacks is left for future work.

Under this threat model, our goal is to prevent adversary $\mathcal{A}$ from distinguishing the true vital sign frequency from obfuscation frequencies with probability better than random guessing.

4.4 Obfuscation Scheme design

In this section, we design our obfuscation scheme, which consists of three core algorithms that set the theoretical foundation for *PrivyWave*: (1) **Gen** (key generation), which creates cryptographic keys containing decoy frequencies; (2) **Enc** (encryption), which physically generates obfuscation by actuating decoy signals; and (3) **Dec** (decryption), which enables authorized sensors to recover the true vital sign by filtering out known decoys. We then show the correctness of the framework and analyze the privacy guarantees of the scheme.

4.4.1 Key Generation. The key generation algorithm *Gen* produces a set of decoy signal frequencies that will be used to obfuscate the user's true vital signs. The algorithm samples p frequencies from a physiologically plausible range S (e.g., 60-100 BPM for heart rate), ensuring that the generated decoy frequencies are indistinguishable from actual

vital signs. These frequencies are stored in a cryptographic key $k = (f_1, \dots, f_p)$ that is shared between the user and authorized sensors.

Algorithm 1 Key Generation

```

1: procedure GEN( $p, S$ )
2:   Input: Number of decoys  $p$ , Physiological range  $S$  (e.g., 60-100 BPM)
3:   Output: Key  $k = (f_1, \dots, f_p)$ 
4:   for  $i = 1$  to  $p$  do
5:     Sample frequency  $f_i$  from range  $S$ 
6:     Add  $f_i$  to key  $k$ 
7:   end for
8:   return  $k$ 
9: end procedure

```

By sampling decoys from the plausible heart rate range S , we prevent statistical attacks where adversaries might identify outliers based on physiological implausibility. All generated frequencies appear as valid vital signs, making them indistinguishable from the user's actual heartbeat without knowledge of the key k .

4.4.2 Physical Obfuscation (Encryption). The encryption algorithm Enc physically generates the obfuscation by actuating a pneumatic device at the decoy frequencies specified in the key k . This process creates real physical motion co-located with the user's body that wireless sensors detect alongside the user's natural vital signs. The input to Enc is the key k containing the decoy frequencies and the user's true vital sign signal m . The output is an obfuscated signal c that represents the composite physical motion observed by any wireless sensor. Critically, this is not a digital encryption, it is a physical process where the actuator generates periodic motions at frequencies $f_1, \dots, f_p$, which superimpose with the user's natural heartbeat motion at frequency m .

Algorithm 2 Physical Signal Obfuscation

```

1: procedure ENC( $k, m$ )
2:   Input: Key  $k = (f_1, \dots, f_p)$ , True signal  $m$ 
3:   Output: Obfuscated signal  $c$ 
4:   Activate pneumatic actuator at frequencies  $f_1, \dots, f_p$ 
5:   Physically superimpose actuated frequencies on  $m$  to create  $c$ 
6:   return  $c$                                       $\triangleright c$  contains dominant frequencies:  $\{m, f_1, \dots, f_p\}$ 
7: end procedure

```

The resulting obfuscated signal c contains $p + 1$ dominant frequency components: the true vital sign m plus p decoy frequencies. Both authorized and unauthorized sensors observe the same physical phenomenon, a composite motion signal with multiple periodic components. The critical difference is that unauthorized sensors cannot determine which of these $p + 1$ frequencies represents the true vital sign, while authorized sensors possess the key k that identifies the decoy frequencies. We discuss the physical implementation details of the pneumatic actuator in Section 4.6.

4.4.3 Signal Recovery (Decryption). The decryption algorithm Dec enables authorized devices to recover the user's true vital sign from the obfuscated signal c . Given the key k that specifies the decoy frequencies, Dec applies a series of notch filters and band-stop filters centered at each decoy frequency $f_1, \dots, f_p$. This filtering process removes the known

Algorithm 3 Authorized Signal Recovery

```

1: procedure DEC( $k, c$ )
2:   Input: Key  $k = (f_1, \dots, f_p)$ , Obfuscated signal  $c$ 
3:   Output: True signal  $m$ 
4:   Apply band-stop filters at frequencies  $f_1, \dots, f_p$ 
5:    $m \leftarrow c \setminus k$  ▷ Remove decoy frequencies
6:   return  $m$ 
7: end procedure

```

decoy components from the composite signal, leaving only the true vital sign m . The algorithm takes as input the key k and the obfuscated signal c observed by the sensor, and outputs the recovered true signal m .

In practice, this is implemented through cascaded notch or band-stop filtering in the frequency domain. Each filter is designed with a narrow bandwidth centered at a decoy frequency, ensuring that it removes the decoy component while preserving the true vital sign and minimizing distortion. This filtering approach is general and works regardless of what signal processing algorithm the sensor uses for vital sign extraction, as the decoy removal happens at the fundamental signal level before any algorithm-specific processing.

4.4.4 Correctness of the Scheme. A scheme is correct if an authorized user $\mathcal{V}$ (who possesses the key k) can always recover the original message m from the observed obfuscated ciphertext c . Formally, we must show that for any message $m \in S$ and any key k generated by $\text{Gen}(p, S)$, the following holds:

$$\text{Dec}(k, \text{Enc}(k, m)) = m \quad (5)$$

PROOF. The proof follows directly from the definitions of the algorithms. The encryption process $\text{Enc}(k, m)$ is a physical process that produces the observed multiset c of frequencies. As defined in Algorithm 2, this multiset is $c := \{m\} \cup k$. The decryption process $\text{Dec}(k, c)$ takes c and k as input and, as defined in Algorithm 3, computes the multiset difference $m' := c \setminus k$.

By substituting the definition of c into the decryption operation, we obtain:

$$m' = (\{m\} \cup k) \setminus k$$

By the definition of multiset difference, this operation removes all p elements of k from the multiset, leaving only the single element m , thus $m' = m$.

This correctness holds even in the negligible-probability collision case where $m = p_i$ for some $p_i \in k$. In such cases, the multiset c would contain two instances of the same value, and the decryption operation $c \setminus k$ correctly removes one instance (the decoy) while preserving the other (the message). Therefore, the scheme is correct. $\square$

4.5 Privacy Guarantee

Our security objective is to ensure that an adversary cannot distinguish the user's true signal m from the p decoy signals. We prove that the adversary gains no meaningful advantage in identifying which of the $p + 1$ observed signals represents the true message.

4.5.1 Defining Privacy. We formalize the adversary's task as follows: after observing the obfuscated signal c containing $p + 1$ frequency components, the adversary $\mathcal{A}$ must guess which one corresponds to the true vital sign. The adversary outputs an index $j \in \{1, \dots, p + 1\}$ representing their guess.

Definition 1 (Adversary's Advantage). A random guess succeeds with probability $1/(p+1)$. We measure the adversary's capability by their *advantage*—how much better they perform compared to random guessing:

$$\epsilon_{\text{adv}} := P(\mathcal{A}'\text{'s guess is correct}) - \frac{1}{p+1} \quad (6)$$

An obfuscation scheme is considered secure if ϵ_{adv} is bounded by a negligible value. Our goal is to prove that ϵ_{adv} is negligibly small.

4.5.2 Analysis Framework. To analyze the adversary's advantage, we partition all possible ciphertexts into two categories based on whether frequency collisions occur. A *collision* happens when the true signal frequency m coincidentally equals one of the decoy frequencies in the key k .

Non-colliding ("Good") Ciphertexts C_{good} . In this case, all $p+1$ signals (the true signal m and p decoys) have distinct frequencies. This is the typical operational scenario. For example, if the true heart rate is 75 bpm and we generate 3 decoys at 68, 82, and 91 bpm, the observed ciphertext is $c = \{68, 75, 82, 91\}$ with 4 distinct values. An adversary cannot determine which frequency corresponds to the true signal without the key.

Colliding ("Bad") Ciphertexts C_{bad} . In this rare case, at least two signals have the same frequency—a collision between the true signal and a decoy. For example, if the true heart rate is 75 bpm and by chance a decoy is also generated at 75 bpm, the observed ciphertext is $c = \{68, 75, 75, 91\}$. The repeated value could potentially leak information: an adversary might reason that "75 appears twice, so it's more likely that one is real and one is a decoy," potentially gaining an advantage.

The key insight of our analysis is that collisions are extremely rare. For typical parameters, the collision probability δ is approximately 10^{-4} . Therefore, we only need to bound the adversary's advantage in this unlikely case to prove overall security.

4.5.3 Privacy in the Good Case. We first analyze the standard operational case where all $p+1$ signals in c are distinct. This occurs with overwhelming probability $1 - \delta$.

LEMMA 4.1. *For any non-colliding ciphertext $c \in C_{\text{good}}$, the adversary's advantage is exactly zero.*

PROOF. An optimal adversary will use Bayesian inference to find the signal $s_j \in c$ that maximizes the posterior probability $P(M = s_j | c)$, where M denotes the true message. By Bayes' rule:

$$\begin{aligned} P(M = s_j | c) &\propto P(c | M = s_j) \cdot P(M = s_j) \\ &\propto P(\text{key is } c \setminus \{s_j\}) \cdot P(\text{message is } s_j) \end{aligned}$$

Let $f_S(x)$ denote the probability density $P(X = x)$ for a signal X sampled from the physiological distribution $\mathcal{D}_H(\cdot | S)$. Since both the true message and all decoys are independently sampled from the same distribution over S , we have:

$$\begin{aligned} P(M = s_j | c) &\propto \left(\prod_{i \neq j} f_S(s_i) \right) \cdot f_S(s_j) \\ &\propto \prod_{k=1}^{p+1} f_S(s_k) \end{aligned}$$

The final product $\prod_{k=1}^{p+1} f_S(s_k)$ is a constant for any given ciphertext c , regardless of which signal s_j is hypothesized as the true message. Therefore, the posterior probability $P(M = s_j | c)$ is identical for all $j \in \{1, \dots, p+1\}$.

Since all signals are equally likely to be the true message, the adversary's optimal strategy is to guess uniformly at random. Their success probability is exactly $1/(p+1)$, yielding zero advantage over random guessing. $\square$

4.5.4 Bounding the Collision Probability. We now bound the probability of the pathological collision case where at least two signals in c share the same frequency. This is the only scenario where information leakage is possible.

LEMMA 4.2. *The collision probability is bounded by $\frac{p(p+1)}{2N}$.*

PROOF. The $p+1$ signals (one true signal and p decoys) are sampled independently from a discrete frequency space S with $|S| \leq N$ possible values. We denote by δ the probability that any collision occurs. Using a union bound over all $\binom{p+1}{2}$ pairs of signals:

$$\delta = P(C_{\text{bad}}) \leq \binom{p+1}{2} \cdot P(\text{two signals collide}) \quad (7)$$

In the worst case, signals are uniformly distributed over S , giving $P(\text{two signals collide}) = 1/|S|$. When $|S| = N$:

$$\delta \leq \frac{p(p+1)}{2N} \quad (8)$$

$\square$

For any reasonably large frequency space (e.g., $N = 2^{16}$ representing heart rates at 0.12 bpm resolution over the [45, 180] bpm typical range) and practical number of decoys (e.g., $p = 3$), this collision probability is negligible: $\delta \approx 1.8 \times 10^{-4}$.

4.5.5 Main Privacy Theorem. We now combine the analyses of both cases to establish *PrivyWave*'s overall privacy guarantee.

THEOREM 4.3 (*PRIVYWAVE PRIVACY GUARANTEE*). *The PrivyWave obfuscation scheme provides strong privacy: the adversary's advantage ϵ_{adv} is bounded by the negligible collision probability δ :*

$$\epsilon_{\text{adv}} \leq \delta \leq \frac{p(p+1)}{2N} \quad (9)$$

PROOF. We express the adversary's total advantage using the law of total probability, partitioning over whether the ciphertext is good or bad:

$$\epsilon_{\text{adv}} = P(\text{Adv} | C_{\text{good}})P(C_{\text{good}}) + P(\text{Adv} | C_{\text{bad}})P(C_{\text{bad}}) \quad (10)$$

We bound each term individually. First, when the ciphertext is non-colliding ($c \in C_{\text{good}}$), the adversary's advantage is zero: $P(\text{Adv} | C_{\text{good}}) = 0$, by Lemma 4.1

Second, in the worst-case collision scenario, a collision could theoretically reveal the message's identity perfectly. The adversary's success probability would be at most 1, giving advantage at most $1 - 1/(p+1) < 1$. We conservatively bound this term by 1: $P(\text{Adv} | C_{\text{bad}}) \leq 1$.

Third, from Lemma 4.2, the probability of a collision is $P(C_{\text{bad}}) = \delta \leq \frac{p(p+1)}{2N}$.

Substituting these bounds into Equation 10:

$$\begin{aligned} \epsilon_{\text{adv}} &\leq (0 \cdot P(C_{\text{good}})) + (1 \cdot P(C_{\text{bad}})) \\ &\leq P(C_{\text{bad}}) \\ &\leq \delta \leq \frac{p(p+1)}{2N} \end{aligned}$$

Since δ is negligible for large N , the adversary's advantage ϵ_{adv} is also negligible, proving that *PrivyWave* is a strong obfuscation scheme. $\square$

4.6 PrivyWave Implementation

We implement *PrivyWave* using a pneumatic-based actuation system. The system consists of two main components: (1) a control unit (Arduino Uno) that generates the decoy electrical pulse signal based on the cryptographic key k , and (2) a pneumatic actuation device that converts the electrical pulse signal into a physical motion.

4.6.1 Decoy Signal Generation. A core requirement of our *PrivyWave* scheme is generating physical decoy signals (periodic signals of all frequencies f_i of the key $k = \{f_1, \dots, f_p\}$) that obfuscate the user's true heart-rate frequency (m). We generate a decoy signal using a binary pulse train that ultimately drives our pneumatic actuator (described in the next paragraph). We choose $p = 3$ number of decoy frequencies, which gives the adversary's probability:

$$P(\mathcal{A}'\text{'s guess is correct}) = \frac{1}{3 + 1} = 0.25.$$

The pulse signal is generated through a two-step process. First, we generate a 10-second base signal at 2000 Hz sampling rate, combining multiple sinusoids at the obfuscation frequencies (e.g., 53, 79, and 101 bpm) to create a complex composite signal, and copy 3 times to create a 30-second signal. Second, the base signal is converted to a binary pulse train using zero-crossing detection, where each positive-going zero-crossing triggers a fixed-duration pulse (25 ms). The pulse signal is used as an input to the air valve, which drives the pneumatic chamber *PrivyWave*. To visually understand the pulse signal in the frequency domain, we did a time-frequency analysis (spectrogram) with frequency resolution of 6 bpm. The spectrogram (Fig. 2a) shows that the generated pulse input indeed contains strong frequency components around 53, 79, and 101 bpms (labeled with dashed red lines).

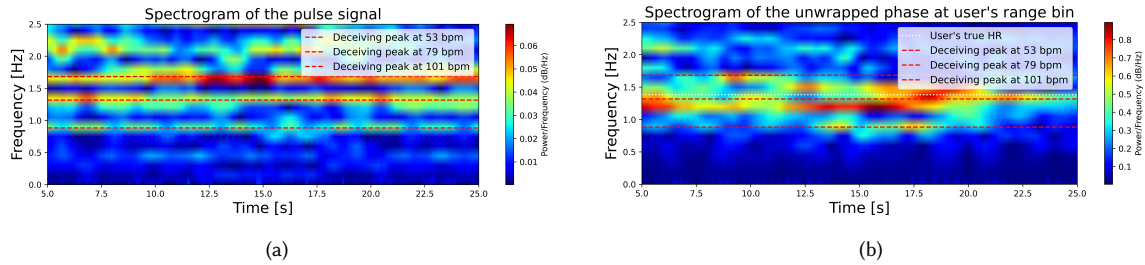


Fig. 2. Time-frequency analysis (spectrogram) of the theoretical decoy signal and the signal collected with mmWave for a person wearing *PrivyWave*. (a) Shows high frequency content around the fake frequencies from the key k . (b) mmWave collected data (User 4, trial 8) shows high frequency content around the same frequencies, with some minor distortions (which are expected because of the pulse conversion step).

4.6.2 Pneumatic Device. The pneumatic system employs a 12 V diaphragm pump with 6 L/min flow rate as the main air input. Using an Arduino and an nMOS transistor, the pulse signal from the previous step drives a normally-open air valve, enabling rapid inflation period (25 ms) and natural deflation period, creating the periodic expansion-contraction motion that mimics physiological patterns. The Arduino is interfaced using a MacBook Pro computer and the pump is powered-up using a DC power supply. The complete hardware is shown in Figure 3.

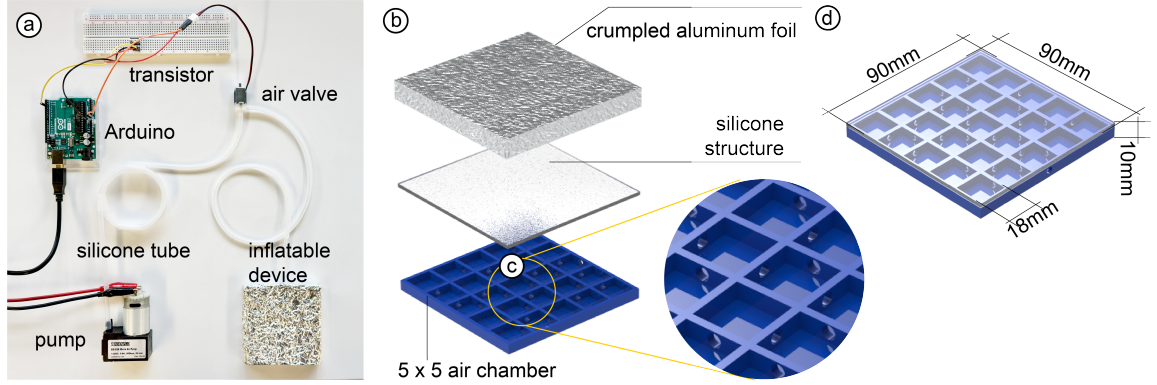


Fig. 3. (a) Complete hardware for *PrivyWave* (not powered-up). (b) Inflatable pneumatic device building blocks. (c) Interconnected airways inside the inflatable device. (d) Dimensions of the inflatable device.

The inflatable device generates obfuscation signals through controlled pneumatic actuation. The actuator transforms from a flat configuration (approximately 10mm thick) to an inflated state (30mm displacement), compact enough to fit in a chest pocket while providing sufficient radar cross-section for detection. The actuator consists of a multi-chamber silicone structure (Ecoflex 0050) with interconnected airways that enable uniform inflation (Fig. 3c). The outer surface is coated with aluminum foil to enhance radar reflectivity, ensuring strong signal returns for both mmWave and acoustic sensing modalities (Fig. 3b). The chamber design features a 5×5 grid of cells (each 18 mm $\times$ 18 mm) connected by 5 mm airways, allowing rapid pressure equalization while maintaining structural integrity during repeated inflation cycles (Fig. 3d). When activated, the coordinated pump and valve operation creates periodic expansion-contraction cycles at the programmed obfuscation frequencies. The inflation phase (pump on, valve closed) lasts 25 ms while deflation (pump off, valve open) occurs within 50ms, enabling operation across the full heart rate frequency range (0.8-3.0 Hz). This pneumatic approach generates physical motion detectable by all wireless sensing modalities while maintaining a simple, reliable design suitable for extended operation.

We validate the pneumatic system using our data collection mmWave device (radar configuration detailed in the next section). To visually understand the collected signal in the frequency domain, we again did a time-frequency analysis (spectrogram) with frequency resolution of 6 bpm. Data was collected from a user wearing *PrivyWave* at a 30 cm distance from the mmWave radar. The spectrogram (Fig. 2b) shows that the mmWave signal sustained the strong frequency components around 53, 79, and 101 bpm from earlier (also labeled with dashed red lines), thereby validating our implementation of *PrivyWave*.

5 Experimental Validation

We conduct comprehensive experiments to validate *PrivyWave*'s effectiveness across multiple scenarios: a user study with two sensing modalities (mmWave and acoustic), performance benchmarks across different environments, distances, and orientations.

5.1 Experiment Setup

Our experimental setup employs two wireless sensing systems to evaluate *PrivyWave*'s effectiveness. For mmWave radar sensing, we use the Texas Instruments IWR1443BOOST evaluation board operating at 77 GHz start frequency

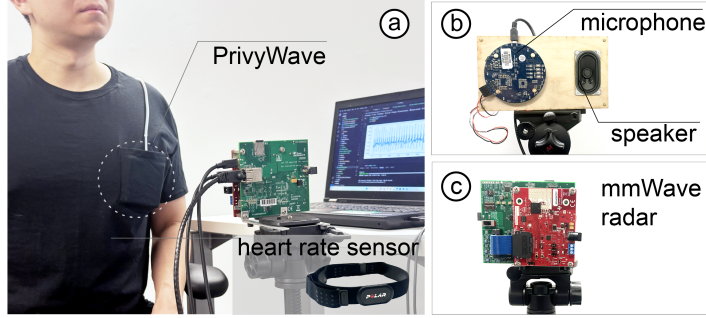


Fig. 4. (a) mmWave data collection setup. (b) Acoustic sensor board with microphone array and a speaker. (c) mmWave radar sensor with data collection board.

Table 2. Comparison of Sensor System Parameters

(a) mmWave Sensor Parameters			(b) Acoustic Sonar Parameters		
Parameter	Value	Unit	Parameter	Value	Unit
<i>Sensor Configuration</i>			<i>Sensor Configuration</i>		
TX Antennas (N_{TX})	2		Transmitter (TX)	1	(Speaker)
RX Antennas (N_{RX})	4		Receivers (RX)	1	(Mic.)
Start Frequency (f_c)	77	GHz	Start Frequency (f_{start})	18	kHz
Frequency Slope (S)	60.012	MHz/ μ s	End Frequency (f_{end})	22	kHz
ADC Sample Rate (f_s)	5	Msp/s	Sample Rate (f_s)	48	kHz
ADC Samples (N_{ADC})	256	samples	ADC Samples (N_{ADC})	512	samples
Frame Periodicity (T_F)	0.5	ms	Range FFT Size (N_{FFT})	512	points
Range FFT Size (N_{FFT})	256	points	Chirp Duration (T_C)	10.67	ms
Chirp Duration (T_C)	98	μ s	<i>Calculated Performance</i>		
<i>Calculated Performance</i>			Bandwidth (B)	4	kHz
Bandwidth (B)	3.07	GHz	Range Resolution (ΔR)	4.29	cm
Range Resolution (ΔR)	4.88	cm			

with 3.07 GHz bandwidth, achieving 4.88 cm range resolution (Fig. 4c). The radar is equipped with 2 transmit and 4 receive antennas with 256-point range FFT processing. For acoustic sensing, we use a UMA-8-SP USB mic array with a speaker transmitter (Fig. 4b), operating with 18-22 kHz FMCW chirps (4 kHz bandwidth) that achieve 4.29 cm range resolution through 512-point FFT processing. Both sensors were interfaced using a Windows 10 laptop and Python scripts. The detailed configuration of both sensors is outlined in Table 2. For ground truth heart rate measurement, we used a Polar H10 chest strap worn under clothing, with data captured at 130 Hz sampling rate and synchronized with the wireless sensors through python scripts.

For unauthorized detection, we implement state-of-the-art heart rate measurement algorithms for mmWave [2] and acoustic sensing [21]. For authorized detection, we apply the same algorithms but first remove the known decoy frequencies using narrow band stop filters centered at $f_1, \dots, f_p$ as specified by the key k . Heart rate is computed from the displacement signal using the average RR interval over the 30-second recording period: Heart Rate (bpm) = $\frac{60}{\text{Average RR Interval}}$, and we evaluate performance using mean absolute error (MAE) between the measured heart rate and the Polar H10 ground truth.

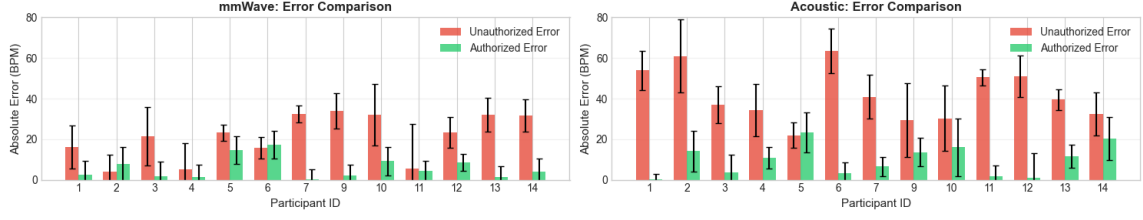


Fig. 5. Individual participant heart rate errors for mmWave (left) and Acoustic (right) sensing. Red bars show the high absolute error for unauthorized devices, which consistently selected decoy frequencies. Green bars show the significantly lower error for authorized devices after decryption. Error bars represent the standard deviation across recordings.

Table 3. Heart Rate Detection Accuracy Summary

Metric	mmWave		Acoustic	
	Unauthorized	Authorized	Unauthorized	Authorized
MAE (BPM)	21.3 ± 10.7	5.8 ± 5.2	42.0 ± 12.4	9.7 ± 7.3
Median Error	23.2	4.1	40.8	11.6
Error Range	[4.0, 33.8]	[0.2, 17.2]	[22.0, 63.4]	[0.3, 23.3]
Protection Ratio	$3.67\times (p < .001)$		$4.33\times (p < .001)$	

5.2 User Study

5.2.1 Participant recruitment and demographics. We recruited 14 participants aged 22-35 years from the university campus. All participants provided informed consent, and the study was approved by our institutional review board (Protocol #IRB0148510). One participant’s data was excluded due to ground truth sensor disconnection, resulting in 13 complete datasets for analysis.

5.2.2 Experimental Protocol. We conducted the user study in an open laboratory environment. After a brief explanation of the study and demographic data collection, each participant was asked to wear the Polar H10 strap under their clothes for ground truth heart rate measurement and place the *PrivyWave* device in their chest pocket. For all experiments, we positioned a sensor (mmWave or acoustic) approximately 30 cm in front of the participant. We initialized *PrivyWave* with $p = 3$ decoy frequencies. Two distinct key sets were generated and used across all experiments. For each sensing modality, we collected three 30-second recordings with each of the two key sets, totaling six recordings per modality. Participants rested for 10-15 seconds between recordings, resulting in 12 total recordings per participant across both modalities.

The same recorded data was then processed under two assumptions: the *authorized* case where the sensor possesses the key k and filters out known decoy frequencies before heart rate estimation, and the *unauthorized* case where the sensor processes the signal without the key. This controlled comparison, where both measurements are derived from identical sensor observations with access to the cryptographic key being the only variable, directly demonstrates *PrivyWave*’s selective protection capability.

5.2.3 Results. Figure 5 illustrates the per-participant heart rate errors for both mmWave (left) and acoustic (right) sensing. The mean and median bpm errors are reported for both unauthorized and authorized devices of all users. The

Table 4. Performance Benchmark Across Different Environments (mmWave Radar)

Environment	True HR (BPM)	Unauth MAE	Auth MAE
Lab (Open Space)	66.0 ± 3.0	6.0 ± 12.5	0.3 ± 1.5
Kitchen	57.2 ± 1.3	0.8 ± 4.5	1.0 ± 1.3
Office	60.2 ± 1.6	9.4 ± 6.7	3.6 ± 1.9

unauthorized errors (red bars) are consistently high, indicating successful obfuscation, while the authorized errors (green bars) remain low, demonstrating successful signal recovery for both sensing modality. A paired-samples t-test ($N=13$) was conducted with these error values, and the results showed that the authorized MAE is significantly lower than the unauthorized MAE ($p < .001$). Table 3 provides the summarized statistics for these findings. We analyze the performance for each modality:

For mmWave Sensing: The unauthorized devices were effectively deceived. These sensors exhibited a high MAE of 21.3 ± 10.7 BPM, which confirms they consistently influenced by the decoy frequencies instead of the true heart rate. In contrast, the authorized device, which used the cryptographic key to filter out the decoy signals, achieved a low MAE of 5.8 ± 5.2 BPM. To put these errors into context, the reported heart-rate error of [2] is 20%, while our errors converted into a percentage is 7.5% for the authorized and 26% for the unauthorized cases. So for mmWave, we are able to successfully preserve the utility of wireless heart-rate monitoring while providing obfuscation guarantee.

For Acoustic Sensing: The protection was even more robust, with unauthorized devices showing a very high MAE of 42.0 ± 12.4 BPM. The authorized device’s performance was slightly degraded compared to mmWave, with an MAE of 9.7 ± 7.3 BPM. The reported maximum heart-rate error of [21] is 3 BPM. This reduced accuracy for acoustic sensing (affecting both authorized and unauthorized measurements, as seen in the high error bars in Figure 5) is likely due to the physical properties of the modality. In our study, the users were just asked to sit in front of the system, but they did natural small movements while data collection, which also contributes to error while the reported method was more restricted during data collection. Acoustic signals have lower penetration through clothing and are more susceptible to environmental noise and multipath interference, resulting in a lower signal-to-noise ratio (SNR) compared to mmWave at the same range.

Protection Effectiveness: Despite the different baseline accuracies, *PrivyWave*’s effectiveness is confirmed across both modalities. The protection ratio, defined as the unauthorized MAE divided by the authorized MAE, was $3.67\times$ for mmWave and $4.33\times$ for acoustic sensing. This large and statistically significant difference (mmWave: $p = 0.0011$; acoustic: $p < 0.001$) validates that our physical-layer obfuscation approach is both highly effective and modality-agnostic.

5.3 Performance Benchmarks

To characterize *PrivyWave*’s robustness under varying physical conditions, we conducted systematic performance benchmarks using mmWave radar. We chose mmWave over acoustic sensing for these benchmarks because it demonstrated higher detection accuracy in our user study (5.8 BPM vs 9.7 BPM authorized error). Higher accuracy sensors present greater privacy risks to users, as they can more reliably extract heart rate. Therefore, mmWave represents the most challenging and critical case for validating *PrivyWave*’s protection effectiveness.

5.3.1 Effect of Environment. We evaluated *PrivyWave*’s robustness across three diverse indoor environments using mmWave radar: an open laboratory space, a kitchen, and an office. We followed the same experimental procedure as

Table 5. Performance Benchmarks Across Distance and Viewing Angle (mmWave Radar)

(a) Range Benchmark				(b) Directional Benchmark			
Distance	True HR (BPM)	Unauth MAE	Auth MAE	Angle	True HR (BPM)	Unauth MAE	Auth MAE
30 cm	66.3 $\pm$ 0.6	11.3 $\pm$ 9.9	1.3 $\pm$ 1.4	-60°	59.7 $\pm$ 3.1	11.7 $\pm$ 2.8	8.8 $\pm$ 2.1
60 cm	67.3 $\pm$ 2.5	16.3 $\pm$ 4.2	0.7 $\pm$ 4.6	-30°	61.3 $\pm$ 0.6	13.3 $\pm$ 2.0	4.0 $\pm$ 2.3
90 cm	66.0 $\pm$ 3.0	6.0 $\pm$ 12.5	0.3 $\pm$ 1.5	0°	61.7 $\pm$ 2.5	10.7 $\pm$ 2.3	0.3 $\pm$ 2.1
120 cm	67.0 $\pm$ 5.0	7.7 $\pm$ 8.1	0.7 $\pm$ 2.5	+30°	60.0 $\pm$ 4.4	3.3 $\pm$ 5.8	5.0 $\pm$ 2.0
150 cm	69.0 $\pm$ 6.2	4.3 $\pm$ 20.0	2.7 $\pm$ 2.9	+60°	61.0 $\pm$ 1.0	7.7 $\pm$ 13.6	5.0 $\pm$ 3.0

the user study, with one participant collecting six 30-second recordings (three with each key set) in each environment. Table 4 presents the heart rate detection performance in each environment.

PrivyWave demonstrates effective protection in the lab and office environments. In the lab, unauthorized sensors show 6.0 BPM error while authorized sensors achieve 0.3 BPM accuracy. In the office, unauthorized error reaches 9.4 BPM compared to 3.6 BPM for authorized sensors, maintaining clear performance separation.

However, in the kitchen environment, protection is less effective: unauthorized sensors achieve 0.8 BPM error, comparable to authorized sensors’ 1.0 BPM error. The cause of this reduced effectiveness in this specific environment demonstrates that certain deployment scenarios may challenge the system’s obfuscation capability.

5.3.2 Effect of Range. We evaluated *PrivyWave*’s robustness across varying distances using mmWave radar. We followed the same experimental procedure as the user study with one participant, with the only variable being the sensor-to-participant distance. The participant was positioned at distances ranging from 30 cm to 150 cm at 30 cm intervals, and three 30-second recordings were collected at each distance. Table 5a shows the heart rate detection errors for both unauthorized and authorized sensors at each distance.

PrivyWave maintains effective protection across all tested distances (Table 5a). The system performs best at mid-range distances (60-90 cm), where unauthorized sensors show 6-16 BPM errors while authorized sensors maintain sub-1 BPM accuracy. At 60 cm—the optimal sensing range balancing signal strength and coverage—authorized error is only 0.7 BPM compared to 16.3 BPM for unauthorized sensors. At closer ranges (30 cm), near-field effects slightly degrade performance, while at extended distances (100 cm), both device experience signal attenuation, though authorized sensors (2.7 BPM) still significantly outperform unauthorized sensors (4.3 BPM).

5.3.3 Effect of Orientation. We evaluated *PrivyWave*’s performance across different orientations relative to the mmWave radar’s line of sight. We followed the same experimental procedure as the user study with one participant, with the only variable being the participant’s orientation relative to the radar. The participant was positioned at five angles spanning the radar’s 120° field of view at 30° intervals: -60°, -30°, 0°, +30°, and +60°, with three 30-second recordings collected at each angle. Table 5b presents the heart rate detection errors at each angle.

PrivyWave maintains protection across the radar’s 120° field of view. The system performs best at center position (0°), where authorized sensors achieve 0.3 BPM error while unauthorized sensors show 10.7 BPM error. At off-center angles ($\pm 30^\circ$ to $\pm 60^\circ$), signal quality degrades due to reduced radar cross-section. Notably, at +30°, the unauthorized sensor achieves a low mean error of 3.3 BPM, but with high variability (std: 5.8 BPM), while the authorized sensor shows 5.0 BPM error with stable performance (std: 2.0 BPM). At other angles, authorized sensors consistently outperform

unauthorized sensors (4.0-8.8 BPM vs 7.7-13.3 BPM). This demonstrates *PrivyWave*'s effectiveness across varying user orientations, with authorized sensors providing reliable measurements even when unauthorized sensors occasionally achieve low errors through chance alignment with decoy frequencies.

6 Discussion and Future Work

This work demonstrates that key-based obfuscation can effectively balance the utility of ubiquitous sensing with privacy protection. The key contribution is enabling selective privacy protection of wireless sensing: authorized devices can accurately monitor heart rate while unauthorized devices are effectively prevented from extracting meaningful information. As wireless sensing proliferates in everyday environments such as offices, public transit, cafes, proactive privacy mechanisms become essential. This work establishes the technical feasibility of key-based physical obfuscation and could potentially lead to future discussion on ethics, policy, and governance of pervasive sensing technologies which we will explore in future work. Below, we discuss a few limitations of the current work and outline directions for future research.

6.1 Motion Scenarios

Our evaluation focused on scenarios where participants remained stationary during measurements. This design choice reflects both the technical state of wireless heartbeat sensing and the most critical privacy threats in everyday life. Existing sensing algorithms achieve highest accuracy when subjects are stationary, as motion artifacts introduce significant noise that degrades detection [20]. Also, these stationary conditions align with privacy-sensitive environments where individuals are most vulnerable to unauthorized monitoring: public transportation (buses, trains, airplanes), workplaces (offices, meeting rooms), public spaces (waiting rooms, restaurants, cafes, bars). In these settings, people remain relatively stationary for extended periods, often unaware of their surroundings, while potential adversaries have stable sensing conditions and ample time to collect high-quality physiological data. For instance, a malicious actor in a coffee shop could continuously monitor customers' heart rates, or an unauthorized device in a shared office could track colleagues' stress levels throughout the workday. By demonstrating effective protection in stationary settings, we address the harder and more prevalent threat case. In the future we will verify the effectiveness of these algorithms when the subject is moving.

6.2 Active Side-Channel Attacks

Our threat model assumes passive adversaries who observe wireless signals without actively probing the system. However, *PrivyWave* remains vulnerable to active side-channel attacks [26] where an adversary could attempt to distinguish real vital signs from decoys through active stimulus-response probing. For example, an attacker might induce a sudden startle response and observe which signal components react, since the user's physiological response would change while mechanical decoys would not. Defending against such active attacks represents a fundamental challenge that requires different approaches beyond physical obfuscation, such as detecting and responding to active probing attempts. Exploring defenses against active attacks is an potential direction for future work.

6.3 Wearability and Form Factor

Our current prototype requires connection to an external power source due to the pneumatic actuators' power demands, limiting mobility to stationary monitoring scenarios. Future work should focus on miniaturization and power optimization to enable battery-powered operation. Beyond power considerations, seamless integration into everyday

clothing would significantly improve usability. Recent advances in smart textiles provide promising directions [11]: actuators and circuits could be embedded within fabric layers near the chest area, or shirt buttons could be redesigned as miniature pneumatic actuators. Such integration would eliminate the need for dedicated wearable devices while maintaining obfuscation effectiveness without compromising comfort or aesthetics.

6.4 Other Vital Signs

While this work focused on heartbeat protection, wireless sensing can detect other involuntary physiological signals with privacy implications. Breathing generates larger movements (millimeters vs. sub-millimeter) at lower frequencies (0.1-0.5 Hz), making it more detectable but potentially easier to obfuscate with larger-displacement actuators. Beyond cardiorespiratory signals, wireless sensors can detect other health related information such as tremors [16] (Parkinson's disease, 4-12 Hz). This will reveal private health conditions that could lead to discrimination. Future work could extend obfuscation techniques for breathing and other health related information leakage.

7 Conclusion

We presented *PrivyWave*, a key-based physical obfuscation system for selective privacy protection in wireless heartbeat sensing. By generating controlled decoy heartbeat signals at cryptographically-determined frequencies, our system enables authorized sensors to recover accurate measurements while unauthorized sensors cannot distinguish true signals from decoys. Our evaluation across mmWave radar and acoustic sensing demonstrates effective protection (average unauthorized error: 21.3-42.0 BPM) while maintaining high authorized accuracy (5.8-9.7 BPM). The authorized accuracy is comparable to typical wireless sensing heart rate measurement systems (ranging from 3-15 BPM) [2, 21], meaning *PrivyWave* does not hamper the utility of wireless sensing. The system operates across multiple sensing modalities without per-modality customization and provides formal security guarantees through cryptographic key-based decoding. This work establishes physical-layer obfuscation as a viable approach for balancing privacy and utility in pervasive health monitoring, opening new directions for privacy-preserving sensing systems.

References

- [1] Heba Abdelnasser, Khaled A Harras, and Moustafa Youssef. 2015. UbiBreathe: A ubiquitous non-invasive WiFi-based breathing estimator. In *Proceedings of the 16th ACM international symposium on mobile ad hoc networking and computing*. ACM, 277–286.
- [2] Mostafa Alizadeh, George Shaker, João Carlos Martins De Almeida, Plinio Pellegrini Morita, and Safeddin Safavi-Naeini. 2019. Remote monitoring of human vital signs using mm-wave FMCW radar. *IEEE Access* 7 (2019), 54958–54968.
- [3] Antonios Argyriou. 2023. Obfuscation of human micro-doppler signatures in passive wireless radar. *IEEE Access* 11 (2023), 40121–40127.
- [4] Finn Brunton and Helen Nissenbaum. 2015. *Obfuscation: A user's guide for privacy and protest*. MIT Press.
- [5] Justin Chan, Thomas Rea, Shyamnath Gollakota, and Jacob E Sunshine. 2019. Contactless cardiac arrest detection using smart devices. *NPJ digital medicine* 2, 1 (2019), 52.
- [6] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijiang Li, Pedro Lopes, Ben Y Zhao, and Haitao Zheng. 2020. Wearable microphone jamming. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–12.
- [7] Yixuan Gao, Tanvir Ahmed, Zekun Chang, Thijs Roumen, and Rajalakshmi Nandakumar. 2025. VitalHide: Enabling Privacy-Aware Wireless Sensing of Vital Signs. In *Proceedings of the 26th International Workshop on Mobile Computing Systems and Applications*. 37–42.
- [8] Jian Gong, Xinyu Zhang, Kaixin Lin, Ju Ren, Yaoxue Zhang, and Wenxun Qiu. 2021. RF vital sign sensing under free body movement. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 3 (2021), 1–22.
- [9] Unsoo Ha, Sohrab Madani, and Fadel Adib. 2021. WiStress: Contactless stress monitoring using wireless signals. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 3 (2021), 1–37.
- [10] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. 2019. Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials* 22, 1 (2019), 746–789.
- [11] Cedric Honnet, Wedyan Babatayin, Yiyue Luo, Ozgun Kilic Afsar, Chloe Bensahel, Sarah Nicita, Yunyi Zhu, Andreea Danielescu, Neil Gershenfeld, and Joseph Paradiso. 2025. FiberCircuits: A Miniaturization Framework To Manufacture Fibers That Embed Integrated Circuits. In *Proceedings of the*

- 38th Annual ACM Symposium on User Interface Software and Technology. 1–18.
- [12] Dongryul Kim, Jaeyoung Choi, Joonseok Yoon, Sungpil Cheon, and Byungkwan Kim. 2024. HeartBeatNet: Enhancing fast and accurate heart rate estimation with FMCW radar and lightweight deep learning. *IEEE Sensors Letters* 8, 4 (2024), 1–4.
 - [13] Hyunjae Lee, Byung-Hyun Kim, Jin-Kwan Park, and Jong-Gwan Yook. 2019. A novel vital-sign sensing algorithm for multiple subjects based on 24-GHz FMCW Doppler radar. *Remote Sensing* 11, 10 (2019), 1237.
 - [14] Hankai Liu, Xiulong Liu, Xin Xie, Xinyu Tong, Tuo Shi, and Keqiu Li. 2023. Application-oriented privacy filter for mmWave radar. *IEEE Communications Magazine* 61, 12 (2023), 168–174.
 - [15] Jian Liu, Yan Wang, Yingying Chen, Jie Yang, Xu Chen, and Jerry Cheng. 2015. Tracking vital signs during sleep leveraging off-the-shelf wifi. In *Proceedings of the 16th ACM international symposium on mobile ad hoc networking and computing*. 267–276.
 - [16] Geoffrey Lo, Ashwin Ram Suresh, Leo Stocco, Sergio González-Valenzuela, and Victor CM Leung. 2011. A wireless sensor system for motion analysis of Parkinson’s disease patients. In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 372–375.
 - [17] Rajalakshmi Nandakumar, Shyamnath Gollakota, and Jacob E Sunshine. 2019. Opioid overdose detection using smartphones. *Science translational medicine* 11, 474 (2019), eaau8914.
 - [18] Rajalakshmi Nandakumar, Shyamnath Gollakota, and Nathaniel Watson. 2015. Contactless sleep apnea detection on smartphones. In *Proceedings of the 13th annual international conference on mobile systems, applications, and services*. 45–57.
 - [19] Md Farhan Tasnim Oshim, Nigel Doering, Bashima Islam, Tsui-Wei Weng, and Tauhidur Rahman. 2025. Anti-Sensing: Defense against Unauthorized Radar-based Human Vital Sign Sensing with Physically Realizable Wearable Oscillators. *arXiv preprint arXiv:2505.10864* (2025).
 - [20] Felipe Parralejo, José A Paredes, Fernando J Álvarez, Khalid Z Rajab, and Elif Dogu. 2025. Challenges Behind Heart Rate Extraction Using mmWave Radar Due to External Factors. In *2025 IEEE Medical Measurements & Applications (MeMeA)*. IEEE, 1–6.
 - [21] Kun Qian, Chenshu Wu, Fu Xiao, Yue Zheng, Yi Zhang, Zheng Yang, and Yunhao Liu. 2018. Acousticcardiogram: Monitoring heartbeats using acoustic signals on smart devices. In *IEEE INFOCOM 2018-IEEE conference on computer communications*. IEEE, 1574–1582.
 - [22] Xiaoxiao Qiao, Man Zhou, Hongwei Li, Xiaojing Zhu, Zhihao Yao, Houzhen Wang, and Xiaojing Ma. 2025. NUSGuard: Smart Device Anti-Eavesdropping Protection Based on Near-Ultrasonic Interference. *IEEE Transactions on Information Forensics and Security* (2025).
 - [23] Jayanth Shenoy, Zikun Liu, Bill Tao, Zachary Kabelac, and Deepak Vasisht. 2022. Rf-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM 2022 Conference*. 588–600.
 - [24] Jing Shi, Rui Zhang, Yunzhong Liu, and Yanchao Zhang. 2010. Prisense: privacy-preserving data aggregation in people-centric urban sensing systems. In *2010 Proceedings IEEE INFOCOM*. IEEE, 1–9.
 - [25] Sorosh Solhjo, Mark C Haigney, Elexis McBee, Jeroen JG van Merriënboer, Lambert Schuwirth, Anthony R Artino Jr, Alexis Battista, Temple A Ratcliffe, Howard D Lee, and Steven J Durning. 2019. Heart rate and heart rate variability correlate with clinical reasoning performance and self-reported measures of cognitive load. *Scientific reports* 9, 1 (2019), 14668.
 - [26] François-Xavier Standaert. 2009. Introduction to side-channel attacks. In *Secure integrated circuits and systems*. Springer, 27–42.
 - [27] Andrew G Stove. 1992. Linear FMCW radar techniques. In *IEEE Proceedings F (Radar and Signal Processing)*, Vol. 139. IET, 343–350.
 - [28] Fengyu Wang, Feng Zhang, Chenshu Wu, Beibei Wang, and KJ Ray Liu. 2020. ViMo: Multiperson vital sign monitoring using commodity millimeter-wave radio. *IEEE Internet of Things Journal* 8, 3 (2020), 1294–1307.
 - [29] Haili Wang, Fuchuan Du, Hao Zhu, Zhuangzhuang Zhang, Yizhao Wang, Qixin Cao, and Xiaoxiao Zhu. 2023. HeRe: Heartbeat signal reconstruction for low-power millimeter-wave radar based on deep learning. *IEEE Transactions on Instrumentation and Measurement* 72 (2023), 1–15.
 - [30] Pei Wang, Xujun Ma, Rong Zheng, Luan Chen, Xiaolin Zhang, Djamal Zeghlache, and Daqing Zhang. 2023. SlpRoF: Improving the Temporal Coverage and Robustness of RF-based Vital Sign Monitoring during Sleep. *IEEE Transactions on Mobile Computing* (2023).
 - [31] Didi Xu, Weihua Yu, Changjiang Deng, and Zhongxia Simon He. 2022. Non-Contact detection of vital signs based on improved adaptive EEMD algorithm (July 2022). *Sensors* 22, 17 (2022), 6423.
 - [32] Zhicheng Yang, Parth H Pathak, Yunze Zeng, Xixi Liran, and Prasant Mohapatra. 2017. Vital sign and sleep monitoring using millimeter wave. *ACM Transactions on Sensor Networks (TOSN)* 13, 2 (2017), 1–32.
 - [33] Zichuan Yu, Lu Tang, Kai Wang, Xusheng Tang, and Hongyu Ge. 2025. Dynamic Ultrasonic Jamming via Time-Frequency Mosaic for Anti-Eavesdropping Systems. *Electronics* 14, 15 (2025), 2960.
 - [34] Mingmin Zhao, Fadel Adib, and Dina Katabi. 2016. Emotion recognition using wireless signals. In *Proceedings of the 22nd annual international conference on mobile computing and networking*. 95–108.
 - [35] Yuefeng Zhao, Kun Wang, and Jing Gao. 2023. Accurate 77-ghz millimeter-wave radar noncontact vital sign detection using the optimized variational mode decomposition algorithm. *Journal of Signal Processing Systems* 95, 11 (2023), 1297–1310.