This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

WASTON: Inferring Critical Information to Enable Spoofing Attacks using COTS mmWave Radar

Yanlong Qiu, Jiaxi Zhang, Tao Sun, Yanjiao Chen, *Senior Member, IEEE*, Jin Zhang, *Member, IEEE,* and Bo Ji, *Senior Member, IEEE*

Abstract—Radar spoofing attacks mislead victim radars by injecting false information. Successful attacks require prior knowledge of the victim radar's mode and parameters, and existing works obtain this critical information with expensive equipment, e.g., software-defined radio or spectrum analyzer. In this paper, we propose WASTON, a low-cost system for radar mode detection and parameter estimation using commercial off-the-shelf (COTS) mmWave radars. To overcome the disadvantage of low sampling frequency of COTS mmWave radars, we design two special local signals to detect frequency points and spectral shapes for radar mode detection. We propose a novel parameter estimation algorithm to estimate frequency- and time-domain parameters for spoofing different radars. We have implemented a prototype on the TI AWR1843 platform and conducted extensive experiments to evaluate the performance of WASTON. Our experimental results demonstrate that WASTON achieves an accuracy of 100% for mode detection and 99% for parameter estimation. Furthermore, we demonstrate that the estimated parameters can be used to launch a successful spoofing attack against the victim radar.

Index Terms—Spoofing Attack, mmWave Radar, Mode Detection, Parameter Estimation.

1 INTRODUCTION

Recent years have witnessed increasing applications of radars [1], [2]. For instance, Continuous Wave (CW) and Frequency Shift Keying (FSK) radars are commonly used for detecting vital signs and estimating traffic speeds. Frequency Modulated Continuous Wave (FMCW) radars are used in human tracking and autonomous driving. However, security issues regarding radar systems, especially spoofing attacks, have become a growing concern [3], [4], [5]. A spoofing attack injects false information into the victim radar, e.g., creating a "ghost object". This may pose severe threats for autonomous vehicles, e.g., lure the victim vehicle to mistakenly stall, brake, or change lanes [4], [6].

To launch a successful spoofing attack, the attacker must have prior knowledge of the mode and parameters of the victim radar. As shown in Fig. 1, a traffic light is equipped with a CW radar A, while vehicles are equipped with FMCW radars B and C. To spoof radar B, the attacker must know its mode and parameters to tailor the spoofing signal accordingly.

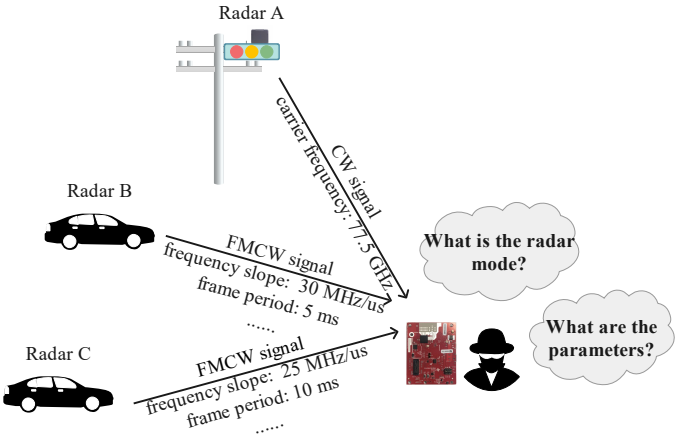


Fig. 1. To generate a spoofing signal, the attacker should have prior knowledge of the victim radars' mode and parameters.

Current spoofing attack systems usually assume that the attacker has prior knowledge of the default mode and parameters of the victim radar from public resources [3], [4], [5], [7]. However, these systems do not consider that users can change the mode and parameters rather than using the default setting [8]. When the user changes the mode and parameters, these system will not work any more. Therefore it is essential to detect the radar mode and parameters timely.

On the other hands, some spoofing systems could access the prior information by an expensive spectrogram or software define radio (SDR) [4], [9], [10], [11], [12], [13]. These

- *Yanlong Qiu is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China, and also with the Department of Computer and Information Science, Temple University, U.S. (email: qiuyl@mail.sustech.edu.cn).*
- *Jiaxi Zhang is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China, and also with the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology, China (email: jzhanghl@connect.ust.hk).*
- *Tao Sun is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China (email: 12232426@mail.sustech.edu.cn).*
- *Yanjiao Chen is with the College of Electrical Engineering, Zhejiang University, China (email: chenyanjiao@zju.edu.cn).*
- *Jin Zhang is with Shenzhen Key Laboratory of Safety and Security for Next Generation of Industrial Internet, Research Institute of Trustworthy Autonomous Systems, Department of Computer Science and Engineering, Southern University of Science and Technology, China (email: zhangj4@sustech.edu.cn).*
- *Bo Ji is with the Department of Computer Science at Virginia Tech, U.S. (email:boji@vt.edu).*

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

systems employ expensive devices to analyze the signal pattern in radio-frequency (RF), which increases the cost to launch a spoofing attack. To reduce the cost, we make the first attempt to use commercial off-the-shelf (COTS) radar, which is small-sized and low-priced, for critical information inference to enable spoofing attacks. However, we are facing a major challenge, since COTS radars only have a low sampling rate that is inadequate to obtain fine-grained spectrogram from RF signal for mode detection and parameter estimation of the victim radar. According to Nyquist's Theorem [14], to recover RF mmWave signals demodulated to the baseband with a bandwidth of 4 GHz at 77-81 GHz, a sampling rate of at least 8 GHz is required. However, the sampling rates of COTS radars are usually limited (around 25 MHz), which only enables us to sample the intermediate frequency (IF) signal rather than RF signal. Therefore, it is essential to design special IF signal for mode detection and parameter estimation. Besides, COTS radar has a limited detection range, which is limited by the low pass filter. The monostatic radar is not designed to detect other radars' signals. How to estimate other radars' information using COTS radar becomes a major challenge.

In this paper, we present WASTON, an effective system for critical information inference using low-cost COTS radars to enable spoofing attacks. A COTS radar processes the received signal by mixing it with a local signal (usually the transmitted signal) and passes the mixed signal through a low-pass filter. The information loss caused by the low-pass filter makes it difficult for accurate information inferences. To overcome the challenges of low sampling rate and signal filtering, we carefully design local signals for mode detection and parameter estimation of diverse victim radars. For mode detection, we estimate the frequency points and the spectral shape of the radar signal and feed them into a classifier. We design two different local signals to identify the frequency points and the spectral shape. The first local signal is a sweep-frequency signal, which is used to help calculate the frequency points in the IF signal. The other local signal is a single-frequency signal, which shifts the IF signal frequency to the baseband for analyzing the spectral shape. Finally, we feed the frequency points and the spectral shape to a neural network for mode detection. For parameter estimation, we leverage the two local signals to calculate the frequency and period of the radar signal. Specifically, we shift the signal to the baseband by mixing it with our designed local signals and propose a parameter estimation algorithm using the IF signal to estimate radar parameters in the frequency- and time- domain.

We summarize our contributions as follows.

- We propose a radar information inference system, named WASTON, using a COTS radar to detect the mode and estimate the parameter of a target radar, which facilitates spoofing attacks.
- We carefully design local signals of the COTS radar to achieve accurate mode detection and parameter estimation.
- We conduct various experiments to verify the effectiveness and robustness of WASTON. Our evaluation results show that the mode detection accuracy can reach 100%, and the relative error of parameter estimation is less than 1%.

2 PRELIMINARIES

In this section, we first introduce commonly-used radars. Then, we review radar spoofing attacks and state-of-the-art works on radar information inference. Finally, we present the threat model.

2.1 Radar Modes & Parameters

We focus on three commonly used radars, namely CW, FSK, and FMCW radars.

2.1.1 CW Radar

CW radar transmits a continuous wave signal of a single frequency $s(t)$ with carrier frequency f_0 and initial phase ϕ:

$$s(t) = e^{j2\pi f_0 t + \phi}. \tag{1}$$

The receiver demodulates the signal to the baseband and measures the velocity v based on the Doppler frequency shift as

$$v = \frac{f_d}{2f_0} \cdot c, \tag{2}$$

where f_d is the Doppler frequency estimated by the target radar, and c is the speed of light.

To spoof CW radars, the attacker should know the carrier frequency f_0 and generates a misleading Doppler frequency signal, which induces an incorrect velocity estimation according to Eq. (2).

2.1.2 FSK Radar

FSK radar transmits two single-frequency signals alternatively:

$$s(t) = \begin{cases} e^{2\pi f_a t + \theta_a} & 0 < t \leq \frac{T}{2} \\ e^{2\pi f_b t + \theta_b} & \frac{T}{2} < t \leq T \end{cases}, \tag{3}$$

where f_a, f_b are carrier frequencies, θ_a, θ_b are initial phases, and T is the period. FSK radar can estimate both velocity and range.

Suppose there is an object located at a distance d_0, the absolute distance between the target and the radar can be calculated as follows:

$$d_0 = \frac{c(\Delta\theta_a - \Delta\theta_b)}{4\pi(f_a - f_b)}, \tag{4}$$

where $\Delta\theta_a, \Delta\theta_b$ are the phase difference between the transmitted signal and received signals at each frequency.

To spoof an FSK radar, the attacker should know the radar's two frequency points f_a, f_b, and the period T. The attacker can spoof the velocity measurement by adding Doppler frequency shift to these two frequency points f_a and f_b. Because the range is calculated from the phase difference, the attacker must also know the period T to synchronize with the signal.

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

2.1.3 FMCW Radar

FMCW radar can measure the absolute distance and velocity of a target with high resolution, so it is extensively used in autonomous vehicles [15]. In the frequency domain, the lowest and the highest frequencies in a chirp are designated as f_L and f_H, respectively, and their difference is the bandwidth $B = f_H - f_L$. In the time domain, the *Sweep Time* T_S indicates how long the radar will take to sweep from f_L to f_H, while the *Chirp Idle Time* T_I indicates how long the radar will be idle while waiting for the received signal. The *chirp period* T_C is composed of the *Sweep Time* T_S and the *Chirp Idle Time* T_I, $T_C = T_S + T_I$. The transmitted signal of an FMCW radar is

$$s(t) = \begin{cases} e^{j(2\pi f_L t + \frac{\pi B}{T_S} t^2)}, & 0 < t \leq T_S, \\ 0, & T_S < t \leq T_C. \end{cases} \tag{5}$$

Suppose that there is an object at distance d_i from the radar. Once the receiver receives the signal, it dechirps the received signal with the transmitted signal to obtain the IF signal $y(t)$:

$$y(t) = r(t) \cdot \overline{s(t)} = \sum_i \alpha_i e^{j(ft+\phi)}, \tag{6}$$

where frequency f is related to the time delay τ_i, $f = -2\pi S\tau_i$. Fast Fourier Transform (FFT) of the IF signal can be used to get the spectrum and calculate the frequency. We can estimate the distance by $\hat{d}_i = c\tau_i/2$.

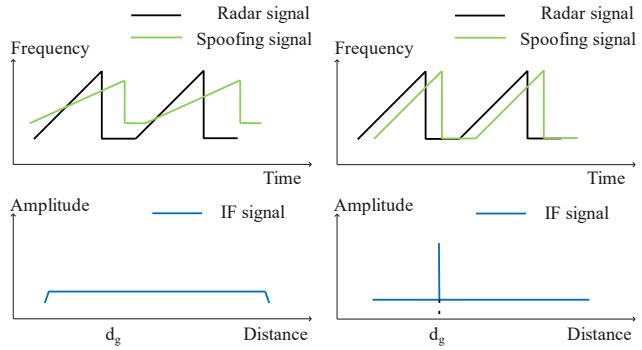
In FMCW radars, a frame is composed of a certain number of continuous chirps and a frame idle. We should estimate the frame period T_F and the frame idle time T_{FI} [15].

It is necessary to estimate the frequencies f_L, f_H, the chirp period T_C, the sweep time T_S, the frame period T_F and the frame idle time T_{FI} of an FMCW radar to spoof it.

As shown in Fig. 2(a), if the spoofing signal uses different parameters from victim radar, its frequency components will spread to all distances in the range profile, so such an attack exhibits an increase in the noise floor rather than spoofing attack. To stably and accurately spoof the victim radar, the attack must transmit a spoofing signal with the same parameters as the victim radar, and introduce the "ghost" target by time delay, as is shown in Fig. 2(b). This study emphasizes the importance of parameter estimation in spoofing attacks.

2.2 Radar Spoofing Attacks

Recent studies have demonstrated various spoofing attacks targeting CW and FMCW radars, which can pose serious threats. We summarize and compare these attacks in Table 1. Rodriguez et al. [3] demonstrated the ability to mimic a user by adding a "vital Doppler" to a Doppler radar. Sun et al. [4] implemented a wireless FMCW radar spoofing system using an SDR. Nallabolu et al. [5] designed a frequency shift mixer to launch a spoofing attack. Nashimoto et al. [7] used a cable to connect the attacker and the victim radar to launch a spoofing attack. However, they assume that the attacker has prior knowledge on the type of mmWave radar and parameters including the waveform parameters (frequency sweep bandwidth and slope), the number of chirp signals used in a frame, and the duty cycle of the radar frame. Chen et.al. [16] proposed to use a passive tag to spoof a radar. However, this method requires the attack to get the sensing signal information of the victim mmWave sensor from open public sources.



(a) Different parameters: invalid spoofing (b) Same parameters: valid spoofing

Fig. 2. Parameter estimation necessity: only when the spoofing signal has the same parameters as the radar signal, can the attacker create an "ghost" object and launch a spoofing attack successfully.

It is worth noting that all existing spoofing attacks assume that certain critical information, in particular, the mode and parameters of the victim radar, are known. However, the attacker may not have access to the critical information or the user may change the parameters of radar from time to time. To address this issue, we design WASTON to estimate the important information required for radar spoofing attacks.

2.3 Radar Information Inference

We focus on mode detection and parameter estimation of radar systems, which are critical for radar spoofing attacks.

2.3.1 Mode Detection

Previous works mainly utilized spectrum analyzers or SDR to detect radar modes based on handcrafted features of radar waveforms, e.g., complex envelope [17], spectral correlation density [18], and auto-correlation function [19]. Time-frequency features of radar signals can be extracted via short-time Fourier transform (STFT) [20], Wigner-Ville distribution (WVD) [21], and Choi Williams distribution (CWD) [22] for radar detection. However, existing methods require high sampling rates for feature extraction, which cannot be achieved by COTS mmWave radars.

2.3.2 Parameter Estimation

Previous research on radar parameter estimation was mostly verified by simulation but not on COTS radars. The maximum likelihood method [23] performs the best for estimating parameters of chirp signal, but needs time-consuming two-dimensional search in both frequency and time domain. Liu et al. [24] proposed QPF-FRFT to estimate radar parameters with one-dimensional search to reduce time complexity. Liu et al. [13] adopted Otsu-ratio to estimate parameters with higher accuracy. Nonetheless, their performance has not been validated on COTS radars.

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

TABLE 1
A comparison of existing mmWave attack approaches.

Work	Attack Method	Cost	Wireless	Stealthiness	Deployment
Nashimoto et al. [7]	RF modulator-based	Medium (> $100)	No (Cable-connected)	No	Difficult
Sun et al. [4]	RF modulator-based	High (> $800)	Yes	No	Difficult
Nallabolu et al. [5]	RF modulator-based	High (> $1300)	Yes	No	Difficult
Chen et.al. [16]	Meta-material-based	Low ($10)	Yes	Yes	Easy

2.4 Threat Model

We define the objective, knowledge, and capability of the attacker.

Attacker's objective. The attacker aims to infer the mode (CW/FSK/FMCW) of the victim radar and the critical parameters for spoofing attacks. For CW radar, we need to estimate its frequency information. For FSK radar, we need to estimate its frequency and period information. For FMCW radar, we need to estimate its chirp and frame parameter information. With this critical information, the attack can spoof the range and speed sensing measurements of the victim radar.

Attacker's knowledge. The attacker does not have access to any prior knowledge of the mode or parameters of the victim radar.

Attacker's capability. The attacker can place a mmWave radar with the field-of-view (FoV) of the victim radar, but not any large equipment (e.g., SDR, spectrum analyzer).

Attack Scenario. Autonomous vehicles are equipped with FMCW radars to detect the range and velocity of multiple targets. Given the parameters estimated by WASTON, we can create a "ghost" object with arbitrary range and speed for the victim radar. Then the autonomous vehicles will stall and even cause traffic jams.

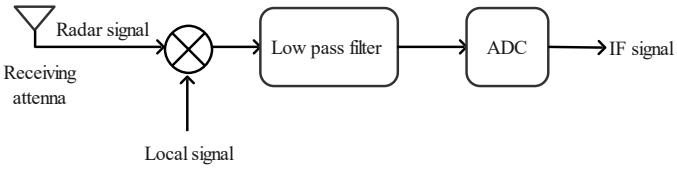


Fig. 3. COTS radar processing flow.

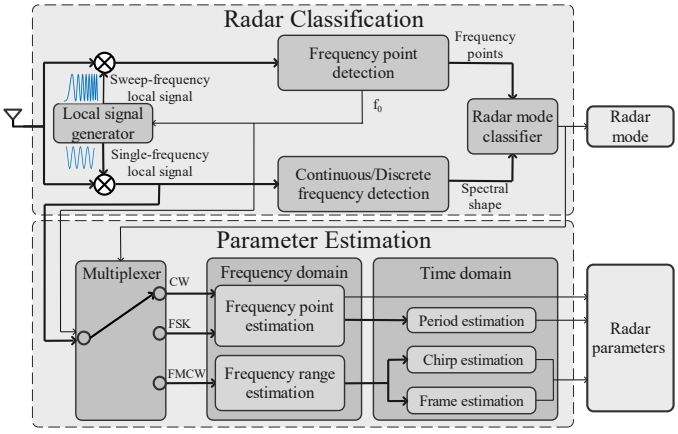


Fig. 4. System architecture. The bold lines refer to the processed signal, and the fine lines refer to the detection results.

3 WASTON: DETAILED DESIGN

We propose WASTON to infer critical information of the victim radar using COTS radars to enable spoofing attacks. The main challenge is that COTS radars have a low sampling rate, typically 25 MHz, which is not enough to sample the RF signal directly to get the information. Besides, the COTS radars are designed primarily for transmission but not infering information of a certain radar.

To address these challenges, we exploit the potential of COTS radar by designing different local signals. As shown in Fig. 3, the COTS mmWave radar mixes the radar signal with a local signal, typically the transmitted signal, to shift the frequency in the RF band to the baseband. To ensure non-destructive sampling of the IF signal after mixing, a low pass filter with a cutoff frequency of $f_s/2$ is often utilized [14]. However, the filtering process limits the bandwidth of the IF signal, leading to frequency loss if the radar signal frequency deviates significantly from that of the local signal. We design different local signals to mix with the radar signal, facilitating the recovery of critical information from the IF signal.

We illustrate our system architecture in Fig. 4, which comprises two fundamental components:

Mode detection. WASTON detects radar modes based on their frequency points and spectral shape. To obtain this critical information, we have designed two distinct local signals, one to acquire the frequency points and the other to detect the spectral shape. Subsequently, we feed the obtained frequency points and spectral shape into a neural network for accurate radar mode classification.

Parameter estimation. WASTON estimates radar parameters based on the frequency and period of IF signals. We devise a customized parameter estimation algorithm for different radar modes. In the frequency domain, we estimate fine-grained frequency points for CW/FSK radar and the frequency range for FMCW radar. In the time domain, we estimate the period for FSK radar and chirp parameters and frame parameters for FMCW radar. Note that CW radar transmits signals continuously, thus, no time domain parameter estimation is necessary.

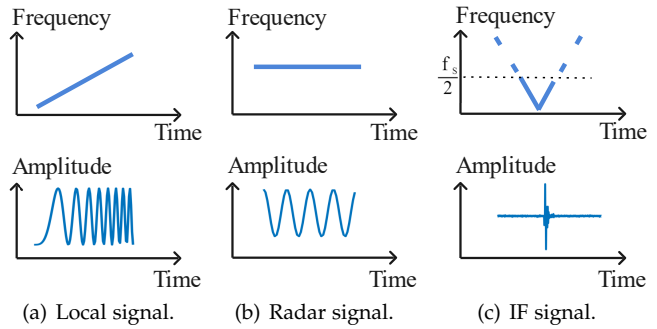
3.1 Local Signal Design

The most important thing in our system is to design local signals facilitating the recovery of critical information from the IF signal. We should detect the frequency, period, and spectral shape of the radar signal.

To detect the frequency of the radar signal, we design a sweep-frequency local signal whose frequency f_t covers the full bandwidth, $f_t = S \cdot t + f_k$, where S is the frequency slope, and f_k is the start frequency. As illustrated in Fig. 5, if the radar signal is a single-frequency signal with frequency

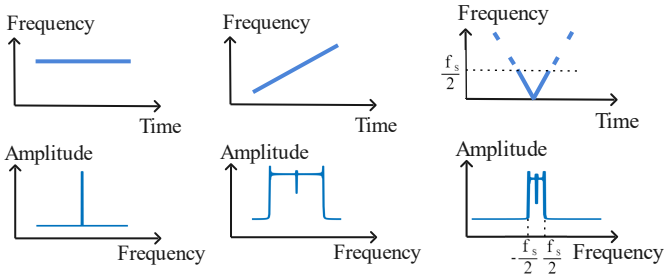
Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038



(a) Local signal. (b) Radar signal. (c) IF signal.

Fig. 5. We use a sweep-frequency signal as the local signal to detect the frequency point of the received radar signal.



(a) Local signal. (b) Radar signal. (c) IF signal.

Fig. 6. We use a single-frequency signal as the local signal to detect the spectral shape of the received radar signal.

f_0, we can mix the radar signal with the sweep-frequency signal as the local signal. If $|f_t - f_0| \geq f_s/2$, the low pass filter will filter out the frequency component, and we cannot observe it in the IF signal. Since f_s is typically a small value, we can detect a peak in the time domain of the IF signal, which signifies that at that particular time, $|f_t - f_0| < f_s/2$. By determining the peak location t_p, we can estimate the frequency point $\hat{f}_0 = S \cdot t_p + f_k$.

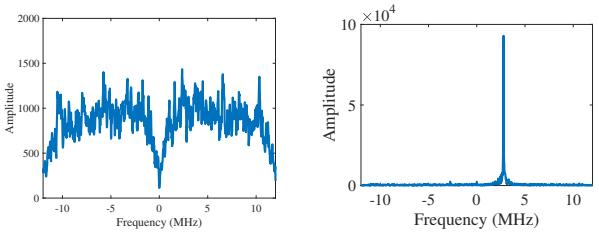
While the sweep-frequency local signal helps rapidly detect the frequency component of the radar signal, it can also obscure the spectral shape. Hence, it can be challenging to determine whether the frequency is continuous or discrete.

To detect the spectral shape, we design a single-frequency local signal whose frequency lies within the bandwidth of the radar signal. As depicted in Fig. 6, if the radar signal has continuous frequencies f_t, we can use the single-frequency local signal with frequency f_0 to shift the frequency from the RF band to the baseband. The resulting IF signal can be represented as

$$IF(t) = e^{j(2\pi(f_t - f_0)t)}. \tag{7}$$

In the frequency domain, all frequency components are reduced by f_0, thereby preserving the spectral shape. Although the low pass filter limits the bandwidth, we can still observe the spectral shape and whether it is continuous or discrete. Mixing with the single-frequency local signal, the IF signal preserves the period of the radar signal, enabling parameter estimation in the time domain.

As a result, COTS radar could sample and analyze the victim radar's signal using these two local signals.



(a) Spectrum of a continuous frequency radar (FMCW) signal (b) Spectrum of a discrete frequency radar (CW/FSK) signal

Fig. 7. Spectral shape detection.

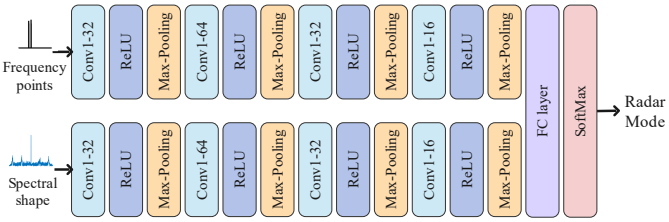


Fig. 8. CNN-based radar mode classifier.

3.2 Mode Detection

Radar mode is detected according to frequency points and spectral shape.

3.2.1 *Frequency Point Detection*

Frequency points are a crucial differentiating factor among various radar modes. For instance, CW radar transmits a single-frequency signal, and therefore, we can detect only one frequency point in the IF signal. FSK radar transmits a switched-frequency signal. By dechirping the radar signal with our designed sweep-frequency local signal, we can detect two discrete frequency points in the IF signal.

In contrast, FMCW radar transmits a continuous frequency-modulated signal, with the frequency varying with time. Hence, we need to detect the spectral shape to differentiate between a continuous frequency (FMCW) signal and a discrete frequency (CW/FSK) signal.

3.2.2 *Continuous/Discrete Frequency Detection*

To differentiate between a continuous and a discrete frequency signal, we should detect the spectral shape of the signal. We use a sweep-frequency local signal to detect at least one frequency point within the bandwidth of the radar signal. Then, using this frequency point, we design a single-frequency local signal to shift the frequency band from the mmWave band to the baseband. The IF signal preserves the spectral shape of the radar signal.

As illustrated in Fig. 7, an FMCW signal has a continuous frequency, which results in a wideband spectrum in the IF signal. In contrast, a CW or FSK signal has discrete frequencies, resulting in a narrowband spectrum in the IF signal. Based on the spectral shape of the IF signal, we can differentiate between a continuous and a discrete frequency signal.

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

3.2.3 Mode Detection

To achieve accurate mode detection, we use a conventional neural network (CNN) for the following considerations: CNNs automatically learn relevant features from the data, leveraging their ability to capture temporal patterns through convolutional operations, leading to more effective feature extraction. Additionally, CNNs exhibit parameter sharing and translational invariance properties, enabling efficient processing of temporal data while reducing overfitting risks. The model architecture is depicted in Fig. 8. The detected frequency points and spectral shape are used as inputs to the CNN. The classifier comprises four convolutional layers, each followed by a Rectified Linear Unit (ReLU) and a max pooling layer. The fully-connected layer computes the probability of the radar mode. The SoftMax function is applied to predict the radar mode.

3.3 Parameter Estimation

We estimate frequency-domain and time-domain parameters.

3.3.1 Frequency-Domain Parameter Estimation

CW radars and FSK radars both transmit a discrete-frequency signal, while FMCW radars transmits a continuous-frequency signal. Therefore, for CW and FSK radars, we should estimate its frequency points. For FMCW radars, we should estimate a working frequency range instead of a specific frequency point.

Frequency point estimation. To estimate the carrier frequency f_0 for CW radar, the coarse estimation provided by the sweep-frequency local signal is not sufficient, since a peak in an IF signal indicates only $|f_t - f_0| < f_s/2$ but not $f_t = f_0$. Therefore, a fine-grained frequency estimation is necessary.

We design a single-frequency signal whose frequency $\hat{f}_0$ is the estimated result using the sweep-frequency local signal. By mixing this signal with the radar signal, the difference in frequency Δf between f_0 and $\hat{f}_0$ can be determined, allowing for a more accurate estimation of the carrier frequency, $f_0 = \hat{f}_0 + \Delta f$. Similarly, for FSK radar, fine-grained frequency points f_a and f_b can be calculated. We need two iterations to achieve fine-grained frequency estimation for each frequency point. Therefore the time cost for frequency point estimation is approximately two chirp periods.

Frequency range estimation. To estimate the frequency range of an FMCW radar, we propose a binary search algorithm to approximate the low frequency f_L and the high frequency f_H. We present our binary search algorithm in Algorithm 1. Using a single frequency local signal of frequency f_c, we can detect whether a frequency component f_c exists in the bandwidth of the victim radar. The whole bandwidth f_{min} and f_{max} are known according to spectrum regulations. For example, automotive radars works from 76GHz to 81GHz according to Federal Communications Commission (FCC) regulation. Therefore, we can set f_{min} and f_{max} as the upper and lower bounds specified by FCC. We define the expected frequency resolution as Δf_{res}.

We first set both the lower frequency f_L and higher frequency f_H to the frequency component f_c firstly (line 1). Then binary search algorithm is performed for lower frequency estimation (lines 2-9) and higher frequency estimation (lines 10-16), respectively. Take lower frequency estimation as an example. If the frequency resolution $|f_L - f_{min}|$ does not reach the required value Δf_{res} (line 2), we iteratively calculate the middle frequency $f_m = \frac{f_L + f_{min}}{2}$ (line 3). We check whether the middle frequency f_m is within or outside the frequency range of the victim radar by detecting whether peaks can be found in the IF signal (line 4). If the middle frequency is within the frequency range, we assign it to the upper bound f_L (line 5); otherwise, we assign it to the lower band f_{min} (line 7). The higher frequency is estimated in the way. The search terminates if the error is within a specified frequency resolution. We need about $\log_2(\frac{f_{max} - f_{min}}{\Delta f_{res}})$ iterations to achieve fine-grained frequency range estimation with resolution Δf_{res}. Therefore the time cost for frequency range estimation is dozens of chirp duration, which is around several ms.

Algorithm 1 Binary Search Algorithm

Input: Frequency found using a sweep local signal: f_c; Frequency bound of the bandwidth: f_{min} and f_{max}; The expected frequency resolution: Δf_{res}
Output: The frequency bound of the target: f_L, f_H;

1: $f_L \leftarrow f_c$, $f_H \leftarrow f_c$
2: **while** $|f_L - f_{min}| > \Delta f_{res}$ **do**
3: $f_m \leftarrow \frac{f_L + f_{min}}{2}$
4: **if** Peak detected at frequency f_{temp} **then**
5: $f_L \leftarrow f_m$
6: **else**
7: $f_{min} \leftarrow f_m$
8: **end if**
9: **end while**
10: **while** $|f_{max} - f_H| > \Delta f_{res}$ **do**
11: $f_n \leftarrow \frac{f_H + f_{max}}{2}$
12: **if** Peak detected at frequency f_{temp} **then**
13: $f_H \leftarrow f_n$
14: **else**
15: $f_{max} \leftarrow f_n$
16: **end if**
17: **end while**
18: **return** f_L, f_H

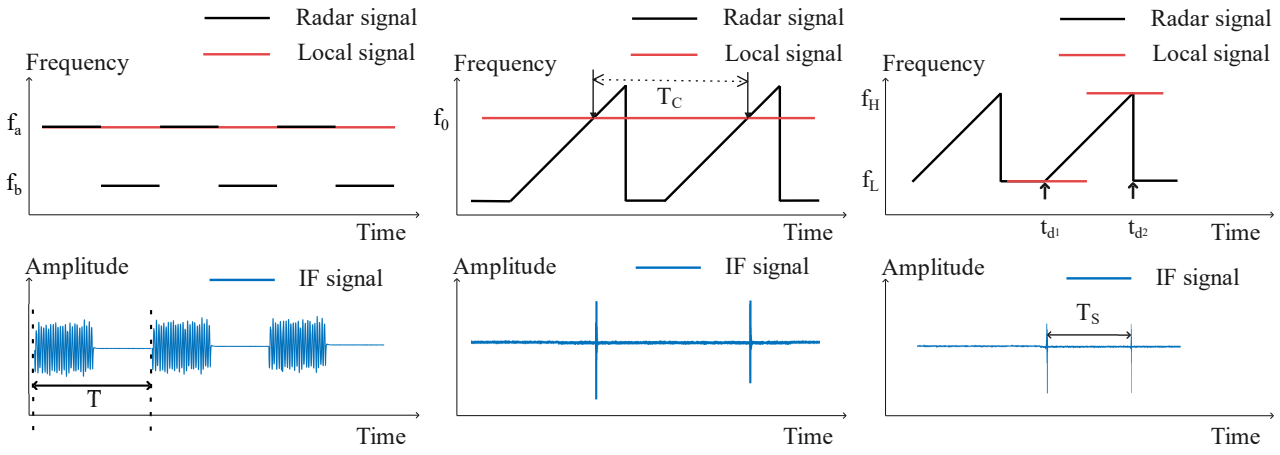
3.3.2 Time-domain Parameter Estimation

CW radar transmits signals continuously, so no time-domain parameters need to be estimated for CW radar. FSK radar transmits two discrete frequencies alternatively, and we should estimate the period T for FSK radar. For FMCW radar, we need to estimate the chirp parameters, including the chirp period T_C, the sweep time T_S, and the frame parameters T_F and T_{FI}. For time-domain parameter estimation, the iteration depends on the time-domain parameter of the victim radar. Generally, the time cost for time-domain parameter estimation is around dozens of ms.

Period estimation. To estimate the period T for FSK radar, we leverage the periodicity of the FSK signal. We set the local signal as a single-frequency signal of frequency $\hat{f}_a$, which is the estimated result of f_a using frequency point estimation in Section 3.3.1, we mix the local signal

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038



(a) Period estimation in FSK radar (b) Chirp period estimation in FMCW radar (c) Sweep time estimation in FMCW radar

Fig. 9. Time domain parameter estimation.

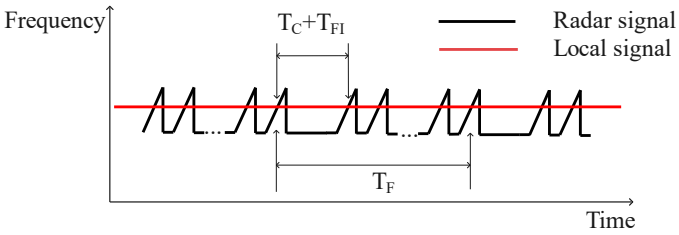


Fig. 10. Frame idle time and frame period estimation.

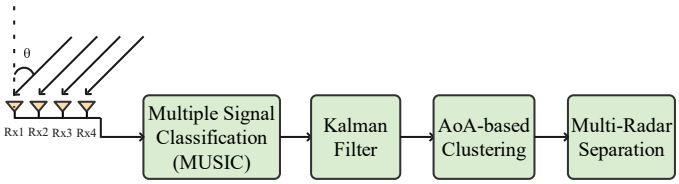


Fig. 11. Multi-radar separation.

with the radar signal, and the mixed signal can reflect the period information of the FSK. Specifically, as shown in Fig. 9(a), when the FSK radar works at f_a, due to the frequency estimation inaccuracy and the frequency offset caused by the difference between the detecting radar and victim radar's oscillators, we can observe a sine wave in the mixed signal. When the FSK radar works at f_b, considering the difference between f_a and f_b is usually larger than $f_s/2$, the mixed signal will be filtered by the anti-alias low-pass filter, therefore no frequency components are left in the baseband. This enables us to estimate the period T of the FSK signal as the interval between two baseband signals in the IF signal.

Chirp estimation. A chirp is composed of a sweep-frequency signal of sweep time T_S and an idle time T_I. We should estimate the chirp period T_C and the sweep time T_S.

T_C estimation. To estimate the chirp period T_C, we use a single-frequency local signal whose frequency f_0 is estimated using a sweep-frequency signal, and observe multiple peaks in the IF signal after mixing with the single-frequency signal, as shown in Fig. 9(b). The interval between two adjacent peaks in the IF signal indicates the chirp period T_C.

T_S estimation. Given the f_L and f_H estimated in Section 3.3.1, we generate a local switched-frequency signal with the low frequency f_L and the high frequency f_H to estimate the sweep time T_S. As shown in Fig. 9(c), the interval between two timestamps t_{d1} and t_{d2} in the IF signal is the sweep time T_S, and the frequency slope S can be calculated as $S = \frac{f_H - f_L}{T_S}$.

Frame estimation. For FMCW radar, we also need to estimate the frame structure, including the frame period T_F and the frame idle time T_{FI}. As shown in Fig. 10, we use a single-frequency local signal to observe the intervals between two adjacent peaks in the IF signal, which can be either the chirp period T_C or $T_m = T_C + T_{FI}$. We can easily differentiate them as T_m should be larger than T_C. The frame idle time T_{FI} can be calculated as $T_{FI} = T_m - T_C$. By segmenting the time domain IF signal into frames, the detector can estimate the frame period T_F by calculating the interval between two adjacent frames.

3.4 Multi-Radar Separation

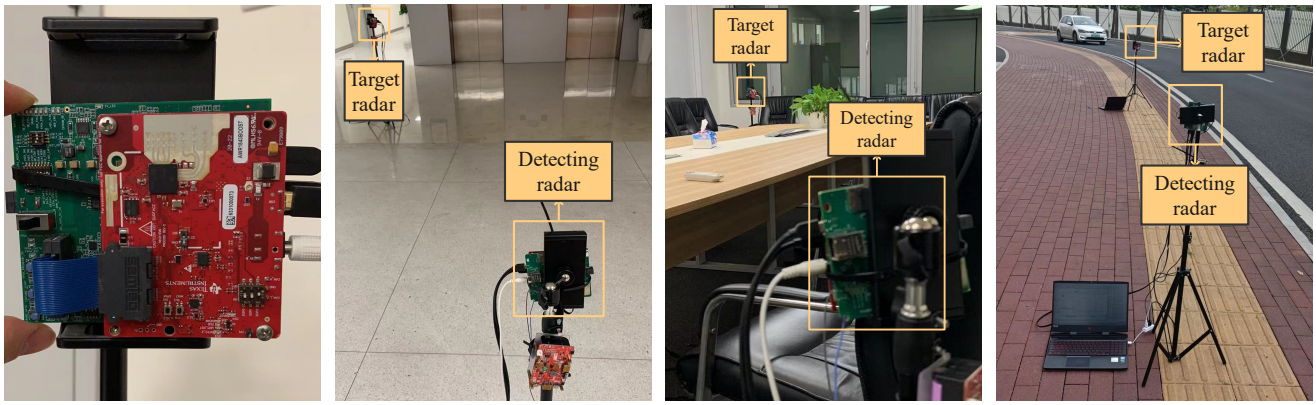
Multiple radars pose a challenge for identifying radar modes and estimating parameters. Signals from different sources are mixed. As a result, it is necessary to separate each signal.

To separate each signal comes from different sources, the observation is that these signal usually comes from a different angle of arrival (AoA). Multiple radar signals can be differentiated by their unique AoA, which allows these radars to be separated.

Specifically, we measure AoA using a MIMO radar. Four antennas can receive each path simultaneously, and their phase difference indicates the AoA. Multiple Signal Classification (MUSIC) is used to estimate the AoA for each peak [25]. To provide a more accurate AoA when the radar is moving, we use the Kalman Filter [26]. We further cluster each peak based on its AoA for multi-radar separation. Radar mode detection and parameter estimation are carried out separately.

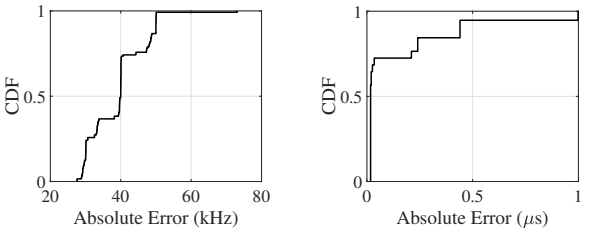
Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038



(a) The TI AWR1843 testbed (b) Scenario 1: open area (c) Scenario 2: conference room (d) Scenario 3: sidewalk

Fig. 12. Testbed and experimental scenario.



(a) Frequency point error of CW/FSK radar. (b) Period error of FSK radar.

Fig. 13. Cumulative distribution function of errors for CW and FSK radar.

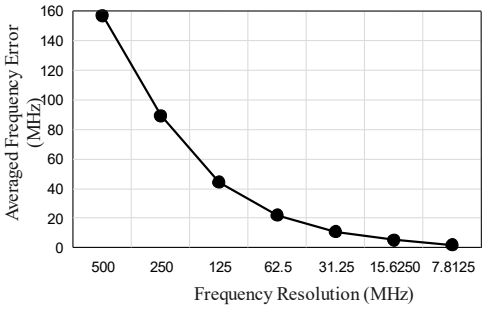


Fig. 14. Frequency range error of FMCW radar: Frequency error vs. Resolution requirement.

4 Evaluation

In this section, we report the results of the experimental evaluation of WASTON. In particular, we present the detailed setup, the overall performance, the robustness, and a case study to launch a spoofing attack using our estimated parameters.

4.1 Experimental Setup

Hardware. We use the TI AWR1843 [27] (Fig. 12(a)) as the detector for radar classification and parameter estimation, and another TI AWR1843 demo board is used as the target radar. Only one receiving antenna on the detector is enabled. **To ensure that the target radar is unaware of the detecting radar, we disable all transmission antennas on the detector.** This can be accomplished using the mmWave Studio software. The target radar is set to be in three different modes: CW/FSK/FMCW by setting the frequency slope to be zero/switched/continuous respectively. The parameters of our detecting radar are listed in Table 2.

Software. We use mmWave Studio and mmWave SDK to configure mmWave sensor modules. We implement our signal processing and parameter estimation algorithm using MATLAB. To classify the radar mode, our CNN-based classifier is implemented in PyTorch 1.10.0 using CUDA 11.2. The CNN is trained on a dataset consisting of 2400 samples collected from different environments. The training dataset consists of a total of 54 minutes of data.

TABLE 2
Configuration of the detecting mmWave radar.

Parameter	Single frequency	Sweep frequency
Sweep time (μs)	420	200
Chirp idle time (μs)	10	10
Sampling rate (ksps)	10,000	20,000
ADC samples	4,096	3,900
Frame period (ms)	57	5
Number of chirps in a frame	128	23

4.2 Performance of Radar Classification

We place the target radar (victim radar) within the field-of-view (FoV) of the detecting radar (attacker). The transmission power of the target radar is set to 12 dBm. The classification accuracy holds at 100% when the detecting radar is within 60 meters of the target radar. The classification accuracy drops with increasing distance since the received power decreases when the distance increases.

4.3 Performance of Parameter Estimation

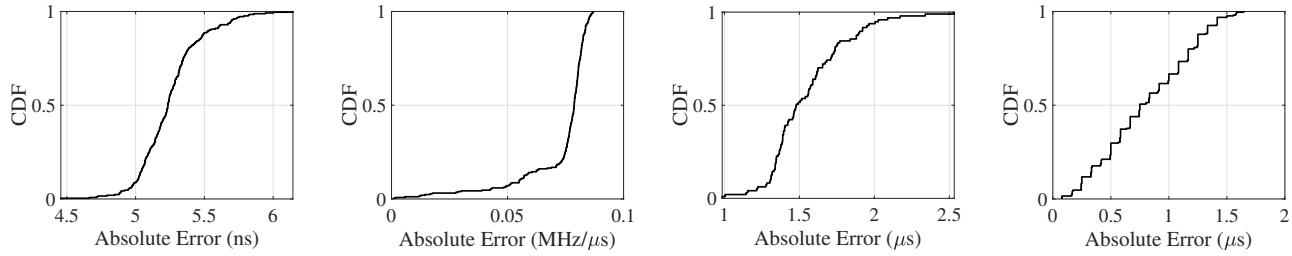
We use *absolute error* and *relative error* as metrics for evaluating parameter estimation. The detector is deployed at a distance of 8 m from the target radar. The transmission power of the target radar is set to 12 dBm.

4.3.1 Frequency Domain Parameter Estimation

In the frequency domain, we evaluate the performance of frequency point calculation for CW/FSK radar and frequency range calculation for FMCW radar.

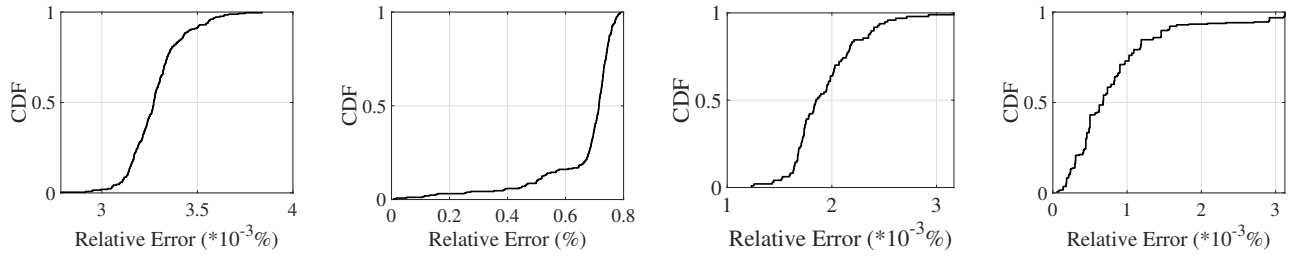
Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038



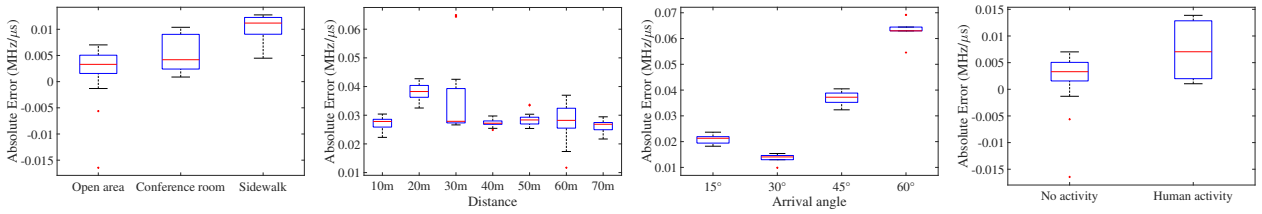
(a) Chirp period T_C (b) Frequency slope S (c) Frame idle T_{FI} (d) Frame period T_F

Fig. 15. Cumulative distribution function of absolute errors for chirp and frame period estimation of FMCW radar.



(a) Chirp period T_C (b) Frequency slope S (c) Frame idle T_{FI} (d) Frame period T_F

Fig. 16. Cumulative distribution function of relative errors for chirp and frame period estimation of FMCW radar.



(a) Impact of environments. (b) Impact of distances. (c) Impact of arrival angles. (d) Impact of human activity.

Fig. 17. Absolute error of frequency slope S for robustness evaluation.

Frequency point evaluation result. This experiment aims to assess the accuracy of frequency point estimation. We configure eight frequency points in CW modes and FSK modes to be 77 GHz, 77.2 GHz, 77.5 GHz, 77.8 GHz, 78 GHz, 78.5 GHz, 79 GHz, and 80 GHz. The cumulative distribution function (CDF) of the absolute error for frequency point calculation is shown in Fig. 13(a). Based on our experiment, 90% of absolute errors are within 52.8 kHz, and its corresponding relative errors are within 0.0065%. The Hamming window and sampling rate limit the theoretical frequency resolution [28]. Our setting has a theoretical frequency resolution of approximately 40 kHz.

Frequency range evaluation result. We set the f_L ranged from 77 GHz to 80 GHz, and f_H ranged from 78 GHz to 81 GHz. As shown in Fig. 14, when we set the required resolution to be 7.8 MHz, the average frequency error is 2.09 MHz, which is about 0.0026% relative error. About seven iterations are performed in the Algorithm 1.

4.3.2 Time Domain Parameter Estimation

In the time domain, we evaluate the performance of period calculation for FSK radar, the chirp parameter, and the frame parameter calculation for FMCW radar.

Period evaluation result. To estimate the period T of FSK radar, we fix the frequency points and change the period T from 100 µs to 2100 µs, stepping by 500 µs. The CDF of absolute error for period estimation is shown in Fig. 13(b): 90% of absolute errors are within 0.44 µs and its corresponding relative errors are within 0.11%.

Chirp parameter evaluation result. We set the chirp period T_C to be ranged from 350 µs to 1000 µs, separated by 50 µs. As shown in Fig. 15(a) and Fig. 16(a), 90% of the absolute errors of T_C are within 0.0055 µs, and its corresponding relative errors are within 0.00345%. We set T_S ranging from 50 µs to 300 µs. As shown in Fig. 15(b) and Fig. 16(b), 90% of the absolute errors of the frequency slope S are within 0.083 MHz/µs, and its corresponding relative errors are within 0.76%. The estimation is accurate enough to spoof the target radar, which we will show in the case study.

Frame parameter evaluation result. We set the frame period of the target radar from 40 ms to 200 ms with a 10 ms step and set the chirp number to 64, 96, and 128 respectively. Fig. 15(c) and Fig. 16(c) indicates that 90% of the absolute

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

errors of the frame idle time T_{FI} are within 1.92 µs and its corresponding relative errors are within 0.0024%. Fig. 15(d) and Fig. 16(d) shows that 90% of the absolute errors of the frame period T_F are within 1.33 µs and its corresponding relative errors are within 0.0015%.

4.4 Robustness

To evaluate the robustness of WASTON, we conduct various experiments under different conditions. We choose the frequency slope S as a representative parameter.

Impact of environment. To evaluate the robustness of WASTON under different environments, we conduct experiments in three different scenarios: an open space, a conference room, and a sidewalk environment, as shown in Fig. 12. WASTON achieves 100% accuracy in radar classification under all three environments. In terms of parameter estimation, the results show that errors remained within 1% for all three environments (Fig. 17(a)), demonstrating its robustness against a variety of circumstances.

Impact of distance. With increasing distance between target radar and detecting radar, the received signal strength and SNR decrease, which affects the performance of WASTON. In this experiment, we assess the robustness of WASTON across various distances between the detecting radar and a target radar. In particular, we adjust the distance from 10 m to 70 m at a fixed angle of 0°. The result shows that the radar classification accuracy is 100% when the distance is within 50 meters. The accuracy decreases to 96.875% at 60 meters and 92.766% at 70 meters. The error in frequency slope estimation does not exceed 0.07 MHz/µs within 70 meters (Fig. 17(b)), which is sufficient to spoof another FMCW radar, demonstrating that WASTON is highly resistant to distance.

Impact of direction. To evaluate the robustness of WASTON under various arrival angles, we adjust the target radar at 15°, 30°, 45°, and 60°of detecting radar. In all cases, the classification accuracy holds at 100 %. Fig. 17(c) shows that the error in frequency slope estimation increases slightly with the angle, from 0.02 MHz/µs to 0.07 MHz/µs, with a relative error of 0.7% sufficient for spoofing. Therefore, we conclude that the parameter estimation of WASTON is robust in various directions.

Impact of human activity. We ask a person to walk around the room to evaluate the robustness of human activity. With human activity, classification accuracy remains 100%. Fig. 17(d) illustrates that parameter estimation errors with human activity are comparable with errors when there is no human activity.

Impact of radar type. To evaluate the robustness of WASTON under different combinations of attack radars and victim radars, we conduct extensive experiments with another COST radar uRAD Automotive [29] with frequency range 76 to 81 GHz. We use AWR1843 as the attack radar and uRAD Automotive as the victim radar. WASTON achieves 100% accuracy in radar classification. In terms of parameter estimation, the results show a relative error of 0.5%. The results demonstrate its robustness against different combinations of radars targeted and attacking.

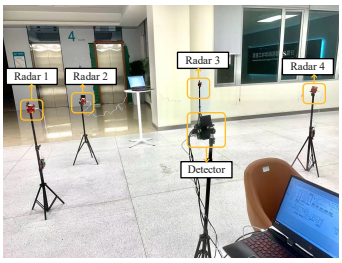


Fig. 18. Multi-radar detection scenario.

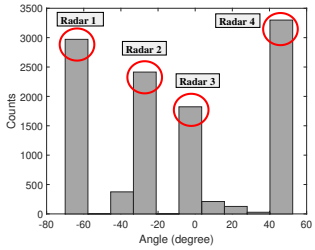


Fig. 19. Angle distribution for multi-radar separation.

4.5 Multiple Radars

As shown in Fig. 18, in this experiment, we placed four radars randomly in an open area, each transmitting a unique signal pattern. A detector is placed to classify their radar mode and estimate their parameters.

Fig. 19 illustrates an example of the AoA estimation result. Based on their unique AoAs, their signal is separated and radar modes and parameters are estimated separately. The overall result is shown in Table 3. The result shows that with the increasing number of radars, the performance of parameter estimation will drop a little (e.g. the error of frequency slope estimation will increase from 0.066 MHz/µs to 0.103 MHz/µs). However, it still provides us with accurate parameter measurements to launch a spoofing attack. We will use the maximum error measured in our evaluation to show a case study.

4.6 Moving Scenario

We examine the performance of WASTON in a dynamic scenario when the victim radar is moving toward the attacker. We deploy radars on two moving cars, as shown in Fig. 20, to evaluate the performance of radar classification and parameter estimation when cars are moving.

Table 4 summarizes the performance comparison under the moving scenario and static scenario. The results indicate the robustness of WASTON under the moving scenario. Because the Doppler frequency introduced by the movement is only approximately $v/c \cdot f_c \approx 5.1kHz$ at a speed of 20 m/s, which is negligible for parameter estimation. The results prove WASTON has the capability to achieve radar classification and parameter estimation when the radar is moving.

5 Case Study

To verify the effectiveness of the estimated parameters in a spoofing attack, **we spoof the target radar by generating a**

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

TABLE 3
Performance for multiple radars working simultaneously.

Number of radars	2	3	4
T_c error (ns)	4.31	5.75	8.03
T_F error (µs)	0.49	0.52	0.81
S error (MHz/µs)	0.066	0.071	0.103

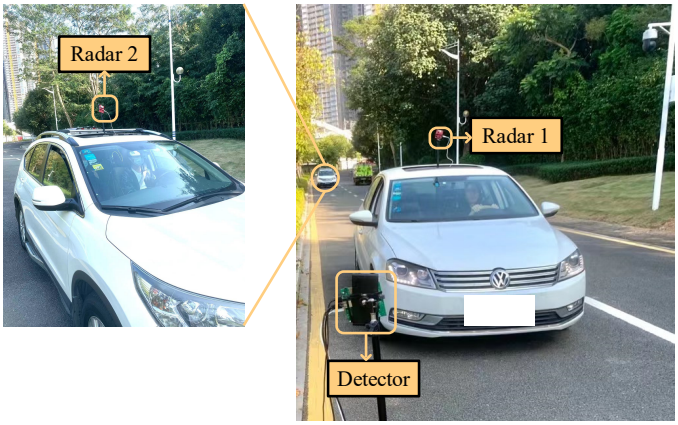


Fig. 20. Moving radar scenario.

spoofing signal based on the estimated parameters with maximum error in the evaluation. To ensure synchronization between the attacker and the victim radar, we set the detecting radar (AWR1843) to the hardware trigger mode and use a RIGOL DG952 signal generator as an external clock for synchronization, which is usually deployed in the existing spoofing system [7].

5.1 CW Radar

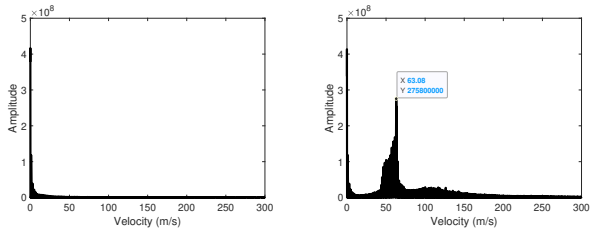
A CW radar can detect the velocity of the object. We can spoof the CW radar by transmitting another signal to generate a "false" speed. In our experiment, there are no moving objects. Initially, the velocity measured by the victim radar shows no moving objects, as shown in Fig. 21(a). We then transmit a spoofing signal with a certain carrier frequency shift. The victim radar then measures a speed of 63.08 m/s, as shown in Fig. 21(b). This speed has exceeded the vehicle's speed limit [30], and the victim radar would falsely indicate that the vehicle is speeding.

5.2 FSK Radar

FSK radars can detect the absolute distance. Given the parameters estimated by WASTON, we can launch a spoofing attack by manipulating the phase difference of the received signal to deceive the victim radar into detecting false absolute distances. In our experiment, a person is walking in front of the victim radar within a distance of 1.2 meters. As shown in Fig. 22(a), the FSK radar accurately detects the person's position. Then the attack radar generates a spoofing signal by adding a phase delay on the signal of detected frequency. As shown in Fig. 22(b), the spoofing signal successfully deceives the victim radar into detecting false distances.

TABLE 4
Performance comparison under static scenario and moving scenario.

Mean error	Static	Moving
Coarse frequency (MHz)	5.0	5.2
Fine frequency (kHz)	52.8	58.1
T_c (ns)	2.5	3.1
T_F (µs)	0.37	0.51
S (MHz/µs)	0.083	0.085



(a) Velocity measurement using CW radar without spoofing attack

(b) Velocity measurement using CW radar with spoofing attack

Fig. 21. Spoofing result of CW radar.

5.3 FMCW Radar

FMCW radars can detect the range and velocity of multiple targets. Given the parameters estimated by WASTON, we generate a spoofing signal by adding a time delay to launch a spoofing attack, which aims to create a "ghost" object for the victim radar.

The parameters of victim radar are listed in Table 5. A person is walking at 8 meters from the victim radar with a speed of 3 m/s. As shown in Fig. 23, both the person and a "ghost" obstacle are successfully detected. The "ghost" obstacle is detected at a distance of 18 meters from the victim radar.

Such a spoofing attack can introduce more severe attacks for autonomous vehicles, such as stalling attacks, hard braking attacks, and lane-changing attacks [4]. For example, there is no obstacle in front of the AV, but the mmWave radar detected a "ghost" object created by the spoofing signal. Then the AV will stall and even cause traffic jams.

6 COUNTERMEASURE

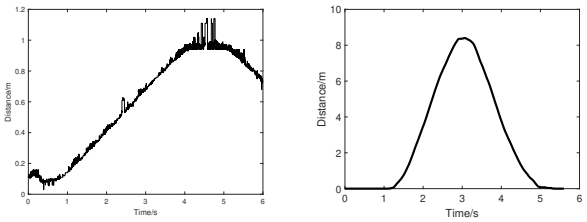
In this section, we present defense mechanisms against mode and parameter estimation from both radar coordination and victim awareness perspectives.

Existing spoofing attacks include active spoofing, which actively transmits a spoofing signal [4], [5] and passive spoofing, which passively leverages a tag to launch the attack [16]. All of them require knowing the victim radar's mode and parameters, so they can transmit a specific spoofing signal or design a specific tag to launch the attack.

Radar coordination: Active spoofing can be regarded as an radar-to-radar(R2R) interference. Thus the radar coordination system that mitigates R2R interference can be used as one of the defense strategies [31], [32]. In this case, even though WASTON provides a radar mode classification and parameter estimation system, the radar coordination system could coordinate the victim radar to adjust its parameter

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038



(a) Trajectory obtained using FSK radar without spoofing attack

(b) Trajectory obtained using FSK radar with spoofing attack

Fig. 22. Spoofing result of FSK radar.

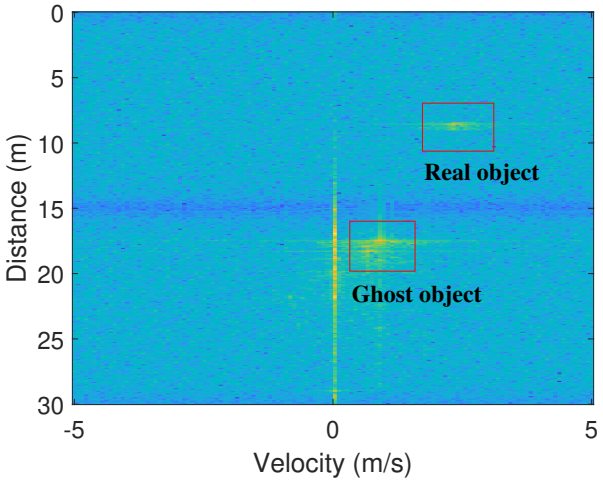


Fig. 23. Spoofing result of FMCW radar.

dynamically, which brings more challenges for launching a spoofing attack.

However, radar coordination is usually costly (i.e., requires additional hardware or bandwidth), and hard to deploy.

Random parameter adjustment: The victim radar can easily detect the spoofing signal by temporarily powering off its transmission. If a signal is received when the victim radar powers off the transmission, the spoofing signal can be detected. A famous defense against such an attack is frequency hopping or slot time adjustment [33], [34]. Specifically, the victim radar randomly adjusts its frequency bands or time slot to defend against the spoofing attack.

It should be noted that such a parameter adjustment strategy is powerful for previous static spoofing attacks [4], [5]. However, WASTON provides parameter estimation for the attacker, which could help the attacker to tune its spoofing signal timely in a challenge-response scheme.

Challenge-Response: Previous spoofing attack assumes mmWave radar uses a well-defined waveform designed to satisfy specific sensing capability. Some previous works propose to use a radar frame consisting of chirps with varying parameters to defend the attack [4]. Randomness can be introduced in the start frequency or the initial phase.

Moreover, WASTON provides a parameter estimation system for the attacker, which can measure the whole frame and replay it at a later time. If the parameter estimation can be achieved in microseconds (usually the length of the chirp period) in the future, the attacker could successfully launch a spoofing attack in theory. However, we only implement an offline parameter estimation system in this paper, so we didn't evaluate the online performance and time cost.

TABLE 5
Parameters of the victim radar.

Parameter	Value
Sweep time (μs)	20
Chirp idle time (μs)	10
Frequency slope (MHz/μs)	60
Frame period (ms)	20
Number of chirps in a frame	128

RF fingerprinting: RF signal fingerprinting has gained attention due to its ability to detect spoofing attacks, which leverages the unique physical characteristics of the probe components to assess if the echo signal comes from the same electronic instruments [4].

This technology is effective for active spoofing but is not feasible for passive spoofing. Besides, RF Fingerprinting can only detect the existence of a spoofing signal, and cannot mitigate its impact. On the other hand, RF Fingerprinting cannot defend against radar mode classification and parameter estimation by the attacker.

Security check: Passive spoofing requires knowing the prior information about the victim radar and even the trap, to design an appropriate passive tag for the spoofing attack. WASTON provided an affordable way to get the prior information. The only way to defend against passive spoofing attacks is a security check. However, a manual check is time-consuming and costly.

7 Conclusion

This paper presents WASTON, a radar classification and parameter estimation system using COTS radars. We conducted extensive experiments to evaluate the efficacy and robustness of the system for radar classification and parameter estimation. Furthermore, we demonstrate that the parameters estimated by WASTON are adequate for launching a spoofing attack. The attacker can gain knowledge about the mode and parameters of victim radar, enabling the practical spoofing attack.

References

[1] Y. Zeng, P. H. Pathak, Z. Yang, and P. Mohapatra, "Human tracking and activity monitoring using 60 ghz mmwave," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2016, pp. 1–2.

[2] Z. Yang, P. H. Pathak, Y. Zeng, X. Liran, and P. Mohapatra, "Vital sign and sleep monitoring using millimeter wave," *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 2, pp. 1–32, 2017.

[3] D. Rodriguez, J. Wang, and C. Li, "Spoofing attacks to radar motion sensors with portable rf devices," in *2021 IEEE Radio and Wireless Symposium (RWS)*. IEEE, 2021, pp. 73–75.

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

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

[5] 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*, vol. 69, no. 11, pp. 5086–5098, 2021.

[6] H.-L. Bloecher and J. Dickmann, "Automotive radar sensor interference–thread and probable countermeasures," in *2018 19th International Radar Symposium (IRS)*. IEEE, 2018, pp. 1–7.

[7] N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki, "A low-cost replica-based distance-spoofing attack on mmwave fmcw radar," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, 2019, pp. 95–100.

[8] "mmwave radar sensors – what is mmwave," https://www.ti.com/sensors/mmwave-radar/what-is-mmwave.html.

[9] 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)*. IEEE, 2023, pp. 1807–1821.

[10] J. Xue, L. Tang, X. Zhang, and L. Jin, "A novel method of radar emitter identification based on the coherent feature," *Applied Sciences*, vol. 10, no. 15, p. 5256, 2020.

[11] L. Liu and X. Li, "Radar signal recognition based on triplet convolutional neural network," *EURASIP Journal on Advances in Signal Processing*, vol. 2021, no. 1, pp. 1–16, 2021.

[12] A. Y. Erdogan, T. O. Gulum, L. Durak-Ata, T. Yildirim, and P. E. Pace, "Fmcw signal detection and parameter extraction by cross wigner–hough transform," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 1, pp. 334–344, 2017.

[13] X. Liu, B. Xiao, and C. Wang, "Frequency estimation of chirp signals based on fractional fourier transform combined with otsu's method," *Optik*, vol. 240, p. 166945, 2021.

[14] M. Gruber, "Proofs of the nyquist-shannon sampling theorem," *Konstanzer Online-Publikations-System (KOPS)*, pp. 1–70, 2013.

[15] S. Rao, "Introduction to mmwave sensing: Fmcw radars," https://training.ti.com/sites/default/files/docs/mmwaveSensing-FMCW-offlineviewing_4.pdf.

[16] X. Chen, Z. Li, B. Chen, Y. Zhu, C. Lu, Z. Peng, F. Lin, W. Xu, K. Ren, and C. Qiao, "Metawave: Attacking mmwave sensing with meta-material-enhanced tags," in *30th Annual Network and Distributed System Security Symposium*. The Internet Society, Mar. 2023, pp. 1–17.

[17] R. Mingqiu, C. Jinyan, Z. Yuanqing, and H. Jun, "Radar signal feature extraction based on wavelet ridge and high order spectra analysis," in *2009 IET International Radar Conference*, 2009, pp. 1–5.

[18] G. Vanhoy, T. Schucker, and T. Bose, "Classification of lpi radar signals using spectral correlation and support vector machines," *Analog integrated circuits and signal processing*, vol. 91, no. 2, pp. 305–313, 2017.

[19] C. Wang, H. Gao, and X. Zhang, "Radar signal classification based on auto-correlation function and directed graphical model," in *2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. IEEE, 2016, pp. 1–4.

[20] X.-W. Zhang, L. Zuo, D.-D. Yang, and J.-X. Guo, "Coherent-like integration for pd radar target detection based on short-time fourier transform," *IET Radar, Sonar & Navigation*, vol. 14, no. 1, pp. 156–166, 2020.

[21] C. Wang, J. Wang, and X. Zhang, "Automatic radar waveform recognition based on time-frequency analysis and convolutional neural network," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2017, pp. 2437–2441.

[22] M. Zhang, M. Diao, and L. Guo, "Convolutional neural networks for automatic cognitive radio waveform recognition," *IEEE access*, vol. 5, pp. 11 074–11 082, 2017.

[23] P. M. Djuric and S. M. Kay, "Parameter estimation of chirp signals," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 38, no. 12, pp. 2118–2126, 1990.

[24] X. Liu, J. Han, C. Wang, and B. Xiao, "Parameters estimation for chirp signal based on qpf-frft," *Optik*, vol. 182, pp. 529–537, 2019.

[25] M. Mohanna, M. L. Rabeh, E. M. Zieur, and S. Hekala, "Optimization of music algorithm for angle of arrival estimation in wireless communications," *NRIAG journal of Astronomy and Geophysics*, vol. 2, no. 1, pp. 116–124, 2013.

[26] G. Welch, G. Bishop *et al.*, "An introduction to the kalman filter," 1995.

[27] "Ti awr1843 evaluation board," https://www.ti.com/product/AWR1843.

[28] S. U. Rahman, Q. CAO, M. M. Ahmed, and H. Khalil, "Analysis of linear antenna array for minimum side lobe level, half power beamwidth, and nulls control using pso," *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, vol. 16, pp. 577–591, 2017.

[29] "urad radar automotive," https://urad.es/en/product/urad-radar-automotive.

[30] "Speeding and speed limits index and overview," https://trafficsafety.ny.gov/?utm_medium=301&utm_source=www.safeny.ny.gov#65.

[31] Y. Qiu, J. Zhang, K. Huang, J. Zhang, and B. Ji, "Poster: Radar-ca: Radar-sensing multiple access with collision avoidance," in *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, ser. MobiSys '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 581–582.

[32] C. Aydogdu, M. F. Keskin, N. Garcia, H. Wymeersch, and D. W. Bliss, "Radchat: Spectrum sharing for automotive radar interference mitigation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 1, pp. 416–429, 2021.

[33] T. Moon, J. Park, and S. Kim, "Bluefmcw: Random frequency hopping radar for mitigation of interference and spoofing," *EURASIP Journal on Advances in Signal Processing*, vol. 2022, no. 1, pp. 1–17, 2022.

[34] K. Haritha, V. B. Sukumaran, and C. K. Singh, "Slotted aloha and csma protocols for fmcw radar networks," *ArXiv*, vol. abs/2201.09030, 2022.

Yanlong Qiu received his B.E. degree in Department of Electrical and Electronic Engineering (EEE) from Southern University of Science and Technology in 2017. He is currently a joint Ph.D. in Computer and Information Science, at Temple University, USA, and in Department of Computer Science and Engineering, at Southern University of Science and Technology, China. His research interests include wireless sensing and security.

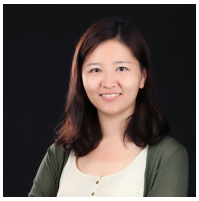
Jiaxi Zhang received his B.E. degree in Department of Computer Science and Engineering in 2022. He is currently a joint Ph.D. in Computer Science and Engineering, The Hong Kong University of Science and Technology, and Department of Computer Science and Engineering, at Southern University of Science and Technology. His research interests include rehabilitation using wearable devices.

Tao Sun received his B.E. degree in Department of Computer Science and Engineering in 2022. He is currently a master student in Computer Science and Engineering, at Southern University of Science and Technology. His research interests include acoustic sensing and wearable devices.

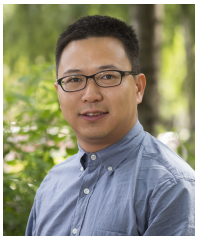
Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Dependable and Secure Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2024.3418038

Yanjiao Chen received her B.E. degree in Electronic Engineering from Tsinghua University in 2010 and Ph.D. degree in Computer Science and Engineering from Hong Kong University of Science and Technology in 2015. She is currently a Bairen researcher at the College of Electrical Engineering, Zhejiang University, China. Her research interests include computer networks, network security, and Internet of Things.



Jin Zhang is currently an associate professor with the Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen. She received her B.E. and M.E. degrees in electronic engineering from Tsinghua University, Beijing, in 2004 and 2006 respectively, and received her Ph.D. degree in computer science from Hong Kong University of Science and Technology, Hong Kong, in 2009. She was then employed in HKUST as a research assistant professor. Her research interests are mainly in mobile healthcare and wearable computing, wireless communication and networks, network economics, cognitive radio networks and dynamic spectrum management. She has published more than 70 papers in top-level journals and conferences. She is the Principle Investigator of several research projects funded by National Natural Science Foundation of China, Hong Kong Research Grants Council and Hong Kong Innovation and Technology Commission.



Bo Ji (S'11-M'12-SM'18) received his B.E. and M.E. degrees in Information Science and Electronic Engineering from Zhejiang University, Hangzhou, China, in 2004 and 2006, respectively, and his Ph.D. degree in Electrical and Computer Engineering from The Ohio State University, Columbus, OH, USA, in 2012. Dr. Ji is an Associate Professor of Computer Science and a College of Engineering Faculty Fellow at Virginia Tech, Blacksburg, VA, USA. Prior to joining Virginia Tech, he was an Associate/Assistant Professor in the Department of Computer and Information Sciences at Temple University from July 2014 to July 2020. He was also a Senior Member of the Technical Staff with AT&T Labs, San Ramon, CA, from January 2013 to June 2014. His research interests are in the modeling, analysis, control, and optimization of computer and network systems, such as wired and wireless networks, large-scale IoT systems, high performance computing systems and data centers, and cyber-physical systems. He has been the general co-chair of IEEE/IFIP WiOpt 2021 and the technical program co-chair of ACM MobiHoc 2023 and ITC 2021, and he has also served on the editorial boards of the IEEE/ACM Transactions on Networking, IEEE Transactions on Network Science and Engineering, IEEE Open Journal of the Communications Society, and IEEE Internet of Things Journal (2020-2022). Dr. Ji is a senior member of the IEEE and the ACM. He was a recipient of the National Science Foundation (NSF) CAREER Award in 2017, the NSF CISE Research Initiation Initiative Award in 2017, the IEEE INFOCOM 2019 Best Paper Award, the IEEE/IFIP WiOpt 2022 Best Student Paper Award, and the IEEE TNSE Excellent Editor Award in 2021 and 2022.

Authorized licensed use limited to: Southern University of Science and Technology. Downloaded on September 07,2024 at 03:16:31 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.