MetaWave: Attacking mmWave Sensing with Meta-material-enhanced Tags

Xingyu Chen*, Zhengxiong Li*, Baicheng Chen†, Yi Zhu‡, Chris Xiaoxuan Lu§, Zhengyu Peng¶, Feng Lin‖, Wenyao Xu‡, Kui Ren‖ and Chunming Qiao‡
* University of Colorado Denver, Denver, Colorado, USA
Email: {xingyu.chen,zhengxiong.li}@ucdenver.edu
† University of California San Diego, California, USA
Email: {b3chen}@ucsd.edu
‡ University at Buffalo, the State University of New York, Buffalo, New York, USA
Email: {yzhu39,wenyaoxu,qiao}@buffalo.edu
§ University of Edinburgh, Edinburgh, Scotland, United Kingdom
Email: {xiaoxuan.lu}@ed.ac.uk
¶ Aptiv, USA
Email: {zpeng.me}@gmail.com
‖ Zhejiang University, Hangzhou, Zhejiang, China
Email: {flin, kuiren}@zju.edu.cn

***Abstract*—Millimeter-wave (mmWave) sensing has been applied in many critical applications, serving millions of thousands of people around the world. However, it is vulnerable to attacks in the real world. These attacks are based on expensive and professional radio frequency (RF) modulator-based instruments and can be prevented by conventional practice (e.g., RF fingerprint). In this paper, we propose and design a novel passive mmWave attack, called MetaWave, with low-cost and easily obtainable meta-material tags for both vanish and ghost attack types. These meta-material tags are made of commercial off-the-shelf (COTS) materials with customized tag designs to attack various goals, which considerably low the attack bar on mmWave sensing. Specifically, we demonstrate that tags made of ordinal material (e.g., C-RAM LF) can be leveraged to precisely tamper the mmWave echo signal and spoof the range, angle, and speed sensing measurements. Besides, to optimize the attack, a general simulator-based MetaWave attack framework is proposed and designed to simulate the tag modulation effects on the mmWave signal with advanced tag and scene parameters. We evaluate, MetaWave, the meta-material tag attack in both simulation and real-world experiments (i.e., 20 different environments) with various attack settings. Experimental results demonstrate that MetaWave can achieve up to 97% Top-1 attack accuracy on range estimation, 96% on angle estimation, and 91% on speed estimation in actual practice, 10-100X cheaper than existing mmWave attack methods. We also evaluate the usability and robustness of MetaWave under different real-world scenarios. Moreover, we conduct in-depth analysis and discussion on countermeasures for MetaWave mmWave attacks to improve wireless sensing and cyber-infrastructure security.**

Zhengxiong Li (zhengxiong.li@ucdenver.edu) is the corresponding author.
Xingyu Chen, Zhengxiong Li, and Baicheng Chen are co-primary authors.

Network and Distributed System Security (NDSS) Symposium 2023
27 February - 3 March 2023, San Diego, CA, USA
ISBN 1-891562-83-5
https://dx.doi.org/10.14722/ndss.2023.24348
www.ndss-symposium.org

I. Introduction

Millimeter-wave (mmWave) sensing has been employed extensively in many critical applications (e.g., automotive vehicle [61], [59], security [20], and robot [91]) due to its exceptional ability to determine the targets' range, angle, and velocity, and works in harsh weather and climate conditions (e.g., lighting, smoke, and fog [84], [76]). These radars have been used for obstacle detection, speed measurement, localization, invasion detection, blind-spot detection, collision avoidance, and surveillance. Due to their widespread use, particular emphasis was laid on investigating the various attacks on mmWave sensing (hereafter mmWave attack) and identifying solutions to mitigate these attacks. These attacks on mmWave sensing can interfere with the sensing measurements to disappear the ahead object or create the ghost object, which can directly or indirectly cause serious consequences such as crash accidents, malicious invasion, and sudden braking. Thus, these radar sensing units are prone to wireless sensing errors that can lead to severe consequences. For example, there is the infamous ghosting effect from perimeter security, robots, and automotive vehicles where it either detects something in front that does not exist (e.g., false alarm and phantom braking) [19], or it misses something that should have been detected [18], [13], causing undetected intrusion and accident collision. Such errorsome sensing mechanisms can further be designed for meticulously targeted attacks (i.e., attack on mmWave sensing).

Given the unique properties of the mmWave signal (loosely recognized from 24GHz-300GHz), current attack vectors to mmWave devices all rely on active electronic-based approaches (e.g., active jamming of electromagnetic waves and injecting malicious signals). However, such attack signals are generated from high-cost, and proprietary equipment, lending these attack vectors are highly expensive, easily detectable track provenience, and even preventable [79], [57]. On the other side, researchers have explored that non-electronic meta-

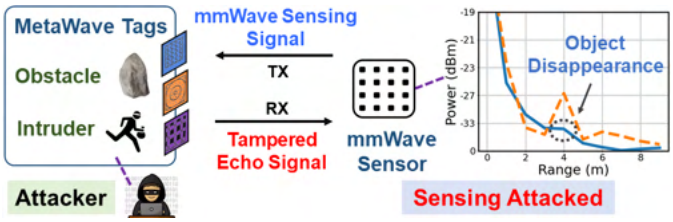


Fig. 1: MetaWave is a novel mmWave sensing attack with meta-material-enhanced tags. The tags can attach to the objects as paper tags and then hide the obstacle or intruder and mislead the mmWave sensing measurements to produce lethal consequences. Note: the dashed line in sensor reading (right side) is natural, and the solid line represents tampered.

material tags can passively modulate RF signals for communication and networking applications [30], [31], [29]. Meta-material is a new class of functional materials designed around unique patterns or structures, which cause them to interact with RF signals and other forms of energy in ways not found in nature [92], [90]. Given these tag materials' low cost and ubiquity, one can easily customize a meta-material tag that tampers the modulation of mmWave signals to launch more practical and pervasive attacks on a range of mmWave sensing applications. Motivated by the above, we ask the following question - *is it possible to use low-cost meta-material tags to incur high-consequence attacks on mmWave sensing?*

In this work, we present the design and implementation of a novel meta-material-enhanced tag attack on mmWave sensing as shown in Figure 1&2, namely MetaWave. The MetaWave system comprises two main modules as shown in Figure 3: (i) **MetaWave Tag** uses the characteristics of the meta-material to modulate the mmWave signal passively. Specially designed tag patterns, meta-materials, and deployment methods make it possible to manipulate echo mmWave signal and attack radar measurement results toward the attack goal; (ii) **MetaWave Attack Framework** further advances the MetaWave tag via an RF simulator to optimize the attack. The MetaWave tag optimizer module iteratively fine-tunes and optimizes the tag design and deployment parameters in a simulated attack scenario to achieve optimal attack performance. In particular, MetaWave features (1) **Stealthy**: unlike existing radio frequency (RF) attacks that reply using RF modulators to perform active attacks, MetaWave produces fully passive meta-material tags for stealthy on-site deployment, which exposes little information regarding the attacker; (2) **Viable**: MetaWave embodiment is to use low-cost and easily obtainable commercial off-the-shelf (COTS) materials with customized tag designs to attack mmWave sensing systems, which has a considerably low bar to launch attacks (simple as paper tags); (3) **Versatile**: MetaWave offers multi-function attacks through a united design framework (as shown in Figure 2). Specifically, MetaWave utilizes three common COTS materials: C-RAM LF, tin foil, and copper parallel wire grid to modulate and affect the victim's mmWave sensing system passively. In addition, the MetaWave tag is optimized via a simulator to achieve optimal robustness and practicality.

To realize MetaWave, two technical challenges need to be addressed: *(a) Design and implement easy-obtainable meta-material tags for the mmWave sensing attack.* The foundation of the MetaWave attack rests on the tag modulating signals from victims' mmWave sensing systems. When the incidental mmWave signal meets the tag, the designated modulation effect will be triggered, and the victim will now receive our modified echo signal. Inspired by such modulation mechanisms, we recruit three different materials (see Section III-B) to attain three typical mmWave modulations (e.g., absorption, reflection, and polarization). With these tags, the attackers can realize ghost attack (GA) and vanish attack (VA), even on multiple objects simultaneously against the RF fingerprint protection. *(b) Simulation model and optimization of the tag attack for robustness and practicality.* Since the diffraction phenomenon of RF is more complex than that of light, the RF simulation is more demanding than the simulation of other sensing modalities (e.g., camera and lidar). Mainstream RF simulators are not practical in this work due to their high computational overhead. Moreover, the material types, patterns, and deployment parameters (e.g., height, orientation) of the MetaWave tags jointly lead to a high-dimensional parameter space of the design. Finding the optimal parameters in this high-dimensional space that satisfies the demanding attack requirement is also a non-trivial challenge. To make the problem tractable, we first utilize a specially designed simulator to create a digital replica of the physical world using the inversible simulations of mmWave signals. Compared to mainstream simulators, our simulator is capable of calculating the mmWave echo signal of arbitrary objects in an accurate and efficient manner. Then, we leverage a gradient descent approach to find the optimal attack parameter solution iteratively. That is, the system automatically outputs the MetaWave tag's optimal material type, pattern, size, and location. Our extensive real-world experiments show that MetaWave can achieve an average attack success rate of 97% on range estimation, 96% on angle estimation, and 91% on speed estimation.

Our contributions can be summarized in the following four points:

- We propose a new passive attack type with meta-material-enhanced tags on mmWave sensing and investigate the feasibility of these security threats.
- We design and develop the first low-cost and easily obtainable meta-material-enhanced tags with specific designs for mmWave ghost and vanish attacks.
- We then design and implement a simulator-based mmWave attack framework to optimize the attack. It can enable stealthy and viable attacks that rapidly analyze the physical environment and generate MetaWave tag design for a trap setup. We will open-source this work.
- We extensively evaluate the system performance and robustness in representative mmWave sensing scenarios in both simulation and real-world. We further examine the system in actual practice scenarios and present countermeasures against these meta-material-enhanced tag attacks.

II. Threat Model

We consider an adversary Eve (Attacker) attempts to spoof Bob (Victim), a victim that leverages mmWave sensing for measurement and detection, such as adaptive vehicle cruising and motion surveillance monitoring.

We identify two targeted attack cases: **(1)** Vanish Attack (VA), which either hides an obstacle that Bob should avoid

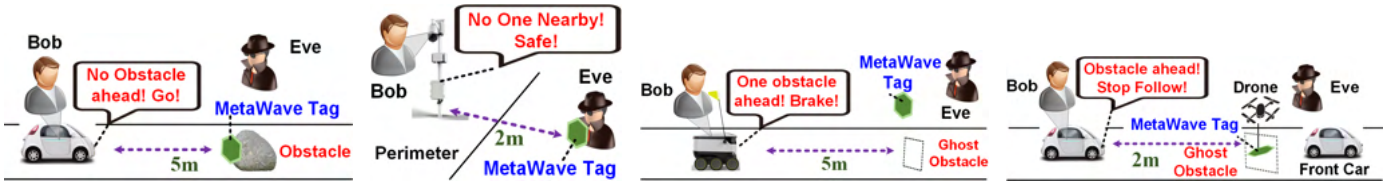


Fig. 2: Four typical MetaWave attack scenarios: (a) VA example where Eve places a MetaWave tag to hide a hard obstacle that Bob should avoid for personal safety, (b) VA example where Eve uses a MetaWave tag to evade detection, (c) GA example where Eve uses MetaWave tag to trigger Bob's vehicle's auto-braking safety feature which may lead to rear-end collision from cars behind, and (d) GA example where Eve utilizes an intermediate RF relay to perform the multi-path attack.

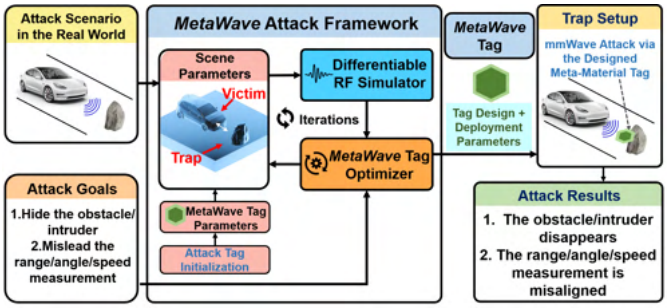


Fig. 3: MetaWave is a passive mmWave sensing attack paradigm using meta-material-enhanced tags. For instance, MetaWave tags are designed, manufactured, and deployed in our scouted physical environment (i.e., trap) to affect mmWave sensing. For instance, they can trick the mmWave sensing system on the victim's automotive vehicle into believing there is no obstacle in front of the vehicle, which may cause intentional catastrophes.

or hide Eve from being detected while trespassing, and **(2)** Ghost Attack (GA), which makes objects appear out of thin air, which triggers false alerts for obstacle detection or trespassing security alerts. Attack examples are shown in Figure 2.

In contrast to prior work, we envision the following desirable features when Eve practically launches an attack:

Passive Tag: The active electromagnetic attack signal or electronic device can be detected by forensic tools or prevented by the security check (e.g., RF fingerprint), and the electromagnetic wave generation equipment is expensive, requiring professional operating knowledge. Therefore, it is hard for Eve to launch an attack using an active electromagnetic wave generator to interfere or jam with Eve's wireless sensing system.

Practical: Assuming Bob puts the mmWave radar and computing devices in a well-controlled environment (e.g., a locked garage or security check routinely). Therefore, it is difficult for Eve to access and modify the devices imperceptibly in advance.

Black Box: Assuming Bob's mmWave sensing system and the computing platform is isolated/secured from the Internet or any other communication channels. Although Eve can have some knowledge about mmWave sensing signal information (e.g., signal frequency and bandwidth), Eve does not have access to the parameters/details of the sensing algorithms implemented, thus, attempting black-box attacks.

As far as we know, none of the prior mmWave sensing attacks can work under an application scenario with the constraints mentioned above (details in Section XII). In addition, tags can be flexibly attached to carrier devices for deployment in various attack scenarios: *(1) Sticker:* The tag can be disguised as a sticker by attaching it to the surface of the object. *(2) Sign:* The tag can be made into general common artifacts (e.g., traffic or roadside signs) to be placed near the target. *(3) Drone:* The tag can be hung under the drone to get close to the target. The weight of the drone can be less than 250g, and then the drone will not be regulated by the remote ID from Federal Aviation Administration [34]. The operating distance (i.e., the approximate distance from the attacker hidden to the victim) could be more than 200m. Therefore, *the challenge at Bob's hand is how to attack mmWave sensing with designed MetaWave tags without violating the constraints above.*

Considering the current mmWave sensors follow standards regulated by spectrum band licenses (e.g., 24GHz) and industrial mmWave sensor parameters are publicly accessible via administrative documents, patents, and media reports (e.g., Bosch [14], Continental [9]), it is practical for attackers to get the sensing signal information of the victim mmWave sensor from open public sources.

III. Rationale and Preliminaries

A. mmWave Sensing Measurements

There are multiple signal modulation technologies in mmWave sensing, such as Frequency-Modulated Continuous-Wave (FMCW), Continuous Wave (CW), and Frequency Modulated Shift Keying (FSK/FMSK). Considering FMCW is the most representative one in real practice and applied in prevailing sensing applications, we take FMCW as an example for illustration. A typical mmWave probe in FMCW mode has one transmitter and multiple receivers. The transmitter generates the chirp waveform as $s(t) = cos(2\pi f_{start} t + \frac{\pi B}{T_{chirp}} t^2)$, where f_{start} is the transmission start frequency, B is the sweep bandwidth ($f_{end} - f_{start}$), and T_{chirp} is the chirp duration. Then the chirp signal is reflected back by the object at the distance d and received by the receivers at the probe. The received signal is given by $r(t) = \alpha cos(2\pi f_{start}(t - t_{delay}) + \frac{\pi B}{T_{chirp}}(t - t_{delay})^2)$, where $t_{delay} = \frac{2(d+vt)}{c}$ is the time delay due to an object at distance d moving with velocity v with respect to the probe, c is the speed of mmWave signal in air. α represents the amplitude of the received signal. Thus, the received signal consists of three fundamental properties of the sensing target (i.e., range d, angle θ, and speed v) for

measurement, which are the basis of the mmWave sensing. Then the range estimation is derived by $d = \frac{T_c c f_b}{2}$, where T_c is the up-chirp time, and f_b is the beat frequency corresponding to the target. The angle estimation is $\theta = arcsin(\frac{\lambda \triangle \theta}{2\pi l})$, where $\triangle\theta$ is the phase difference at the receive antennas, l is the distance of the receive antennas, and λ is the wavelength of the sensing single. The speed estimation is $\upsilon = \frac{\triangle\theta\lambda}{4\pi T_{chirp}}$, where $\triangle\theta$ is the phase shift.

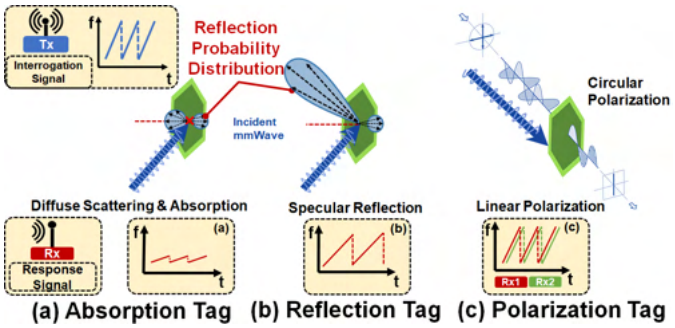


Fig. 4: Targeted absorption, reflection, and polarization of incident mmWave signal are essential characteristics of MetaWave tag design. Different combinations of MetaWave meta-material tags will enable pre-programmed mmWave modulation to be deployed for different attack applications.

B. Meta-material Tags

MetaWave tag includes negative refractive index (i.e., mmWave absorbing) meta-material, and RF modulations meta-material (i.e., specular reflection and polarization) as shown in Figure 4. Rather than directly attacking the computing parts of a mmWave sensing system, MetaWave tag aims at directly modulating the sensing echo signal while physically present in the environment. We select proper attack materials that can achieve low-cost and high-precision attacks while being harmless to the human body and environment. It is worth noting that most of the meta-materials can cover a wide range of RF frequencies, enabling high robustness and scalability in real practices. For example, the refection tag (e.g., metal foil-based) can create a strong reflection for RF signal from a wide frequency band supporting Sub-6GHz and Terahertz bands [12], [62], [78].

Absorption Tag is to largely attenuate the amplitude of the echo signal, which can make the probe believe there is no object detected and make the obstacle/intruder ahead *disappear*. We find that the C-RAM LF material [16] is the most suitable for attacking mmWave. C-RAM LF is layers of lossy open-cell plastic foam It is lightweight, flexible, and can be bonded to many metals, plastic, or wooden surfaces using a polychloroprene contact adhesive. The frequency range of use is 18–40 GHz with -20dB. It has high service temperature of a maximum of 120° C. Its thermal conductivity is 6.5×10^{-5} cal-cm/sec-cm^2-° C and density is 0.07g/cm^3. We consider C-RAM LF as a meta-material because it was not the materials (e.g., metal wires, silicon chips, etc.) traditionally utilized in RF circuit and system designs.

Reflection Tag is to rebound the transmission signal and spoof the object detection by overwhelming the object signal and utilizing the range resolution limitation (round 0.75-0.9m in 24GHz probe) [57]. It can create *ghost* objects to the radar and affect the position and speed measurements. The tin foil is the most suitable for the reflection tag since it is malleable and can create a strong electromagnetic reflection. The high-frequency RF energy is strongly reflected when the frequency is higher than 100 MHz (e.g., 24-300GHz). The density of tin foil is 2.7g/cm^2, but it only has a thickness of 0.016 mm, making it ultra low-weight in practice.

Polarization Tag is to restrict the specific fields in the mmWave signal movement since the mmWave signal is the transverse wave, which can tamper with the echo signal. The polarization tag is mainly used for performing GA for speed and angle measurements. We use specific designed parallel grid made of fine copper wires as polarization tags [15]. The polarization tag can attenuate EM waves in the parallel wire direction by more than 90% while having almost no effect on EM waves in the perpendicular wire direction. It is a combination of cardboard and copper wire, with a thickness of 3mm and a density of around 8g/cm^3.

C. Simulator to Optimize Attack Designs

Different from the adversarial examples aiming for deep neural networks [77], the physical attack prefers manipulating the physical environment to spoof and mislead the sensing measurements leading to disaster aftermath (e.g., a crash) [24]. Compared to other active attacks, this physical attack works passively and is harder to discover and trace with existing forensic tools (e.g., RF fingerprint and false alarm detection). Then, we propose this MetaWave attack. In this work, the designed simulator can provide a digital replica of the corresponding attack scenario (i.e., the physical object or process) and simulate the tag modulation effects on the mmWave signal. Besides, we also utilize the optimization concept in the simulator [28] to optimize the tag design and deployment parameters (i.e., the physical manipulation) to achieve a practical and robust mmWave attack.

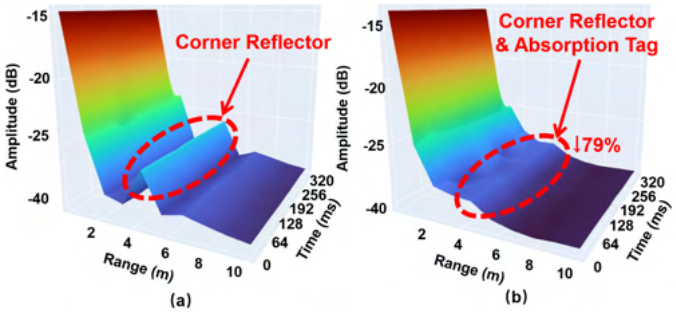


Fig. 5: Ranged amplitude analysis using Fast Fourier Transform (a) radar RX in line of sight with the corner reflector, and (b) absorption tag placed in front of the corner reflector.

D. Feasibility Study

To examine the feasibility of MetaWave attack using the meta-material tag, we perform a real-world VA feasibility study using a mmWave sensing probe and a corner reflector in the real world. We first place a trihedral corner reflector (30 cm height and width), four meters in front of the mmWave sensing probe, and record its original mmWave response. As

shown in Figure 5(a), a peak that represents the corner reflector is detected at four meters range using Fast Fourier transform (FFT). Then, we apply a real mmWave absorbing meta-material-enhanced tag on the corner reflector and record the attacked mmWave response. As shown in Figure 5, the meta-material absorbing tag is effectively erasing the response wave from the corner reflector. Making radar receivers disabled to sense the object fundamentally. So far, such fundamental attacks are undetectable using mmWave sensing systems alone.

IV. System Overview

A. MetaWave Tag Design

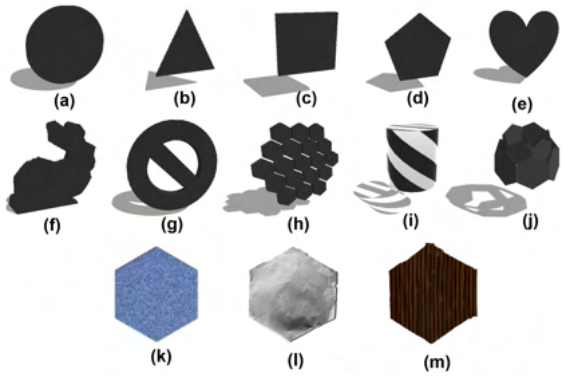


Fig. 6: MetaWave tags can be designed into both 2D and 3D patterns to blend in the environment. Representative tag patterns, (a)-(e) are basic 2D pattern, (f)-(h) are advanced 2D pattern, and (i)-(j) are 3D pattern. (k)-(m) are the real-world prototypes of absorption, reflection, and polarization tags.

MetaWave's meta-material tags are malleable. As shown in Figure 6, tags can be made into various shapes and structures to blend with the environment to improve stealthiness. Moreover, these meta-materials are COTS, making the tags easy to make.

After extensive evaluation, we find that the hexagon is the most suitable candidate for the basic tag element. Since the hexagon is densely paved and has reflection symmetry, the hexagon shape has less overlap than other shapes (e.g., circle) and can be composed into honeycomb patterns, as shown in Figure 6(h). In addition, each honeycomb hexagon's material and orientation can be individually adjusted and reused. Therefore, the honeycomb pattern has the best overall robustness with ultra-low-cost.

As shown in Figure 6(i) and (j), the MetaWave supports 3D patterns as well. The 3D patterns have the unique advantage of multi-directional attack, capable of attacking in multiple directions with no impact of orientation. Moreover, the 3D patterns can be rotated to generate micro-motion for attacking the Doppler effect-based measurement algorithms, thus further improving the attack performance.

B. MetaWave Attack Framework Design

1) Scene Parameters : As shown in Figure 7 and Table I, we need two types of parameters at the initial beginning to define an attack scenario. The first one is the victim parameters , including the victim's radar sensor frequency, bandwidth, polarization mode, and sensing distance. These parameters are

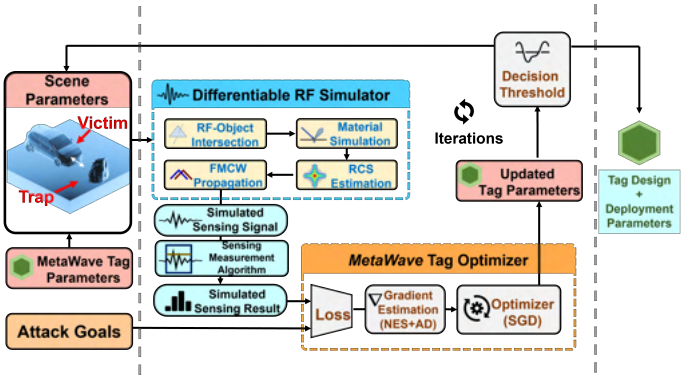


Fig. 7: MetaWave attack framework contains two parts: the Differentiable RF simulator and the MetaWave Tag Optimizer. It takes scene parameters including the victim and the trap setup as input, and outputs an optimized tag design with specific tag deployment parameters such as location.

usually publicly open or can be obtained from the target product's manual or even through social engineering, alternatively, by using an RF signal receiver to sample the target radar's parameters (details see Section II). It is worth mentioning that existing RF modulator-based attack approaches also need these parameters to launch attacks (details see Section XII and Table III). The second type is the trap parameters that include the geometry and material of the objects (e.g., walls, vehicles) and the trap environment. These objects usually have a consistent geometry, or their crucial descriptors are easily obtainable due to the manufacture standards and marketing or user needs, so common pre-defined geometries can be used. Also, the characterization of the scenario environment can be observable via remote measurements (e.g., telescope, augmented reality) or extracted through public navigation maps (e.g., Google Maps). The total number of scene parameters is about 1000, most of which define the object geometry.

2) Differentiable RF Simulator: To find the optimal design of MetaWave tags for a given scenario, we need a specially designed RF simulator that can both output the simulated sensing signal and provide guidance for optimizing the tag design in the gradient estimation. To achieve this, we need a simulation technique that is (1) Differentiable: The differentiability of the simulator can dramatically increase the optimization speed of the gradient-based optimizer; (2) Efficient: the highly efficient simulator can enable fast iteration for finding optimal tag design. However, existing Computational Electromagnetics methods such as FEM [43] and MoM [35] have huge computational costs and are therefore unable for fast iteration and hence are not suitable for this work. Ray tracing is a method of computer graphics that simulates the physical behavior of light. Since RF and light are both electromagnetic radiations. The ray-tracing method can also be applied to RF. MetaWave's simulation is based on the Shooting and Bouncing Rays (SBR)[53]. The ray tracing-based method is much faster than other RF simulation methods (e.g., FEM [43] and MoM [35]).

RF-Object Intersection: To simulate the interaction of RF

TABLE I: Scene parameter examples in the proposed simulator

	Parameter Categories	Example Value	Description
Victim	mmWave Frequency	24 GHz	Frequency of target radar
	mmWave Polarization	Circular	Polarization method of mmWave
	mmWave Bandwidth	500 MHz	Bandwidth of mmWave
	mmWave Carrier	FMCW	Waveform modulation method
	Sensing Algorithm	Range FFT	Function mapping raw signal to sensing results
	Sensing Distance	10m	Function distance of victim's radar
	Victim/Radar Rotation	(1,0.5,0.5,1)	Quaternion (x,y,z,w)
	Victim/Radar Position	(0,2,0)	3D vector (x,y,z)
Trap	Ghost/Target Rotation	(0,1,0,0)	Quaternion (x,y,z,w)
	Ghost/Target Position	(0,1,5)	3D vector (x,y,z)
	Ghost/Target Geometry	Car	List of Points defines the mesh
	Ghost/Target Material	Metal	BSDF of surface properties
	Environment	Road	List of environment meshs

signals with the object geometry, we need to find the specific location where RF intersects the object. And because of the wave-particle duality of EM and to reduce the computational complexity, we only consider the particle properties of the RF at this stage and emit it as a ray. The geometry of the object in the digital world is usually represented by thousands to millions of triangles (i.e., mesh). Since direct intersection computation of mesh is challenging, we split the intersection detection with mesh into intersection detection with each triangle within its mesh and calculate the integral of all intersected rays to get approximate solutions. The whole process is called ray tracing.

We utilized the Bounding Volume Hierarchy (BVH) [81] structure to store the triangles, which is an optimization structure-based binary search tree that has the logarithmic time complexity of finding the nearest triangle at a given location. The Möller-Trumbore intersection algorithm [56] is used for the fast ray-triangle intersection calculation. The Monte Carlo method is used to calculate the approximation of all rays emitted and received by the radar. However, the classic random sampler in ray tracing and SBR is considered indifferentiable. Therefore, we applied a new edge sampler [48] in MetaWave's sampling state, which is continuous and can be differentiated.

Material Simulation: Material simulation and definition are essential for the attack system because of the need to simulate MetaWave tags with different RF modulation methods. However, the native SBR method does not support the simulation of materials. Therefore, we enhance SBR by introducing an extension of the Bidirectional Scattering Distribution Function (BSDF) in the ray-tracing stage.

BSDF is a universal function that defines an arbitrary surface's reflection and refraction properties [22], as shown in Figure 4. The BSDF takes incident ray and reflection ray direction as input and returns the probability of the reflection happening. In addition, it can also change the characteristics of the rays (e.g., polarization).

RCS Estimation: The Radar Cross-section (RCS) of simulated objects is estimated via the number of ray hits and the distance of the ray. RCS is then used to calculate the voltage level of the radar echo signal. The voltage level of each ray is denoted as [72]:

$$V = \sqrt{\frac{G_T G_R \sigma}{4\pi}} \frac{\lambda}{d}, \tag{1}$$

where σ is the RCS, G_T and G_R is the gains of transmitter and receiver, d is the ray distance, λ is the wavelength.

FMCW Propagation: It is worth mentioning that MetaWave simulator can work for various signal modulation technologies (e.g., FMCW, CW) in signal propagation. As discussed in Section III-A, we use FMCW as an example for illustration. The FMCW Propagation module first generates an FMCW waveform from digital radar. Then manipulate the transmitted signal according to the response of the objects. The echo signal is denoted as [73]:

$$S_{IF_s}(t) = \sum_{i=0}^{N} A(\alpha, \gamma) exp(2\pi j(\mu t \tau + f_c \tau)), \tag{2}$$

where N is the number of the rays. $A(\alpha, \gamma)$ is the attenuation at given α (azimuth) and γ (elevation) angle, f_c is the carrier frequency, μ is the frequncy slope. The signal delay τ is denoted by $\tau = \frac{d}{c}$. It is worth noting that f_c and μ can be configured to simulate RF with different frequencies.

The simulator takes the scene parameters as input. A digital copy of the attack trap is created based on the parameters of environmental, objects, and radar specifications. The digital radar then emits an RF signal, which is received by the radar and approximated by a number of ray samples. Each ray is passed through the **RF-Object Intersection** module to calculate the ray exposure point, and then the reflected/refracted rays are calculated based on the surface properties of the **Material Simulation** module. The RCS values are then fed into the **FMCW Propagation** module to calculate the echo signal for FMCW. The simulator outputs the time-domain RF signal.

To illustrate the fidelity and effectiveness of this simulator, we compare our simulated signal with other commercial simulator products (see Section VII). To reduce the effect of noise in the time domain signals, we convert the signals to the frequency domain via an FFT heatmap. We use Structural similarity (SSIM) [82] to measure the similarity. SSIM is a full reference method (FR) [75] that considers both structural information and perceptual phenomena of the data. It is better at handling two-dimensional signal data than metrics such as PSNR [74]. The SSIM outputs a value range from 0 to 1. The higher the SSIM, the better the similarity.

3) MetaWave Tag Optimizer: Given a scenario δ, the attacker aims to design a MetaWave tag such that when deployed in this scenario, the mmWave measurement results are manipulated according to the attack goal. The MetaWave attack on mmWave sensing via MetaWave tag can be formulated as:

$$L(x, y) = \|y - f(S(\delta + x))\|^2, \tag{3}$$

where x is the tag parameters, y is the attack goal value, f is a mmWave measurement algorithm. It is worth noting that MetaWave only requires querying these measurement algorithms and does not need implementation details. S is the RF simulator, $S(\delta+x)$ is the simulated mmWave signal of the scenario with MetaWave tag, σ is the attack success criterion threshold. The attack goal is realized when the loss function $L < \sigma$ is achieved.

The attack goal value y is the mmWave measurement results of the ideal successful attack scenario. y for disappearing attack is set to 0 since the attack excepted the target disappeared on the radar. y for the creation attack is set to the detection threshold of the target measurement algorithm. To minimize the $L2\ norm$ in Equation 3, we employ the natural evolution strategy (NES) [39] and automatic differentiation (AD) for gradient estimation and use Stochastic Gradient Descent (SGD) [45], [71] as an optimizer to fine-tune the MetaWave tags.

V. Attack System Integration

Algorithm 1 MetaWave Attack Framework

Input: $sceneParam$: Attack scenario parameters
$radar$: Radar setting
$RFmeasure$: RF measurement Algorithm
$goal$: Attack Goal Value
Output: $tagParam$: MetaWave tag parameter.

```
tarParam = TagParam.randomInit()
sceneGen = SceneGenerator.create(sceneParam)
simulator = DiffRFSim.create()
optimizer = Optimizer.create()
for _ in range(MAX_ITER) do:
    scene = sceneGen.generate(scene,tagParam)
    simSignal = simulator.sim(scene)
    simValue = RFmeasure(simSignal)
    loss = Loss(simValue, goal)
    if loss ≤ threshold then
        return tagParam
    end if
    optimizer.zeroGrad()
    loss.backward()
    optimizer.step()
end for
return tagParam
```

A. MetaWave Tag Advancement

In this section, we further advance the MetaWave tag design and deployment parameters using the simulator. The simulator can automatically optimize the MetaWave tag design for different attack scenarios. To simulate the meta-materials, we define BSDF for each material according to its characteristics.

1) Absorption Tag in MetaWave Simulator: The C-RAM LF material has a -20db attenuation for mmWave signals, meaning that it is able to reduce energy reflections by 90%. Therefore, for the BSDF of absorbing material, we set a 90% probability of absorbing rays and a 10% probability of Lambertian reflection. The BSDF of C-RAM LF material is denoted as: $BSDF(\theta_i, \phi_i; \theta_r, \phi_r) = \frac{\rho_s}{\pi}$, where (θ_i, ϕ_i) is direction of incident rays, (θ_r, ϕ_r) is direction of reflection rays. ρ_s is the albedo of the material. in this work, $\rho_s = 0.1$.

2) Reflection Tag in MetaWave Simulator: We use tin foil tape as the reflection material. The reflection of metal for millimeter wave follows the same specular reflection as visible light. The probability of ray reflection is related to the angle of incidence and the angle of the normal plus fuzziness. The BSDF of specular reflection is denoted as: $BSDF(\theta_i, \phi_i; \theta_r, \phi_r) = \rho_s\delta(\theta_i - \theta_v)\delta(\phi_i + \pi - \phi_v)$, where (θ_i, ϕ_i) is direction of incident rays, (θ_r, ϕ_r) is direction of reflection rays. ρ_s is the specular albedo of the material, δ is the dirac delta function.

3) Polarization Tag in MetaWave Simulator: mmWaves waves pass directly through linearly polarizing materials and are not reflected or scattered. However, the material changes the way mmWave is polarized. The material retains the polarization in the tag's tangent direction and rejects the polarization in the bitangent direction. As shown in Figure 4. A circularly polarized mmWave will transform to linearly polarization after passing through.

TABLE II: Tag parameter examples for mmWave attack

Parameter Categories	Example Value	Description
Tag Design Parameters		
Tag Material	Absorb	BSDF of MetaWave tag
Tag Pattern	Honeycomb	Texture, Geometry, or Presets
Tag Deployment Parameters		
Relative Size	(0.1,0.1,0.1)	3D vector (x,y,z)
Relative Position	(0,0,-0.5)	3D vector (x,y,z)
Relative Rotation	(0,0,0,0)	Quaternion (x,y,z,w)
Position Tolerance	(0,0,-0.5)	3D vector (x,y,z)
Rotation Tolerance	(0,0,0,0)	Quaternion (x,y,z,w)

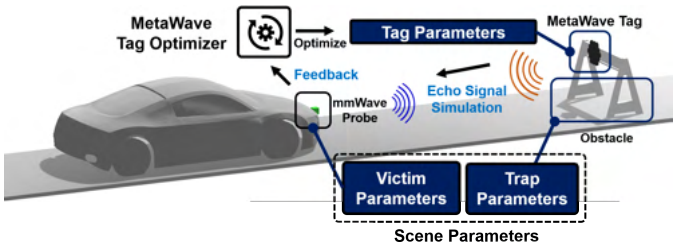


Fig. 8: In MetaWave simulator, scene parameters are defined in three parts to characterize the attack scenario: tag parameters, victim parameters, and trap parameters. The MetaWave Tag optimizer tunes tag parameters until it makes the victim's mmWave sensor makes a mistake. For instance, the MetaWave tag vanishing the roadblock can lead to a severe collision on highways with roadworks.

B. Simulator-based MetaWave attack on mmWave sensing

Different from most adversarial attacks that are focusing on the computing module (e.g., the target recognition/classification algorithms), MetaWave targets the physical characteristic of RF via a differentiable RF simulator. MetaWave's simulator-based attack system utilizes an iterative approach to find the optimal tag design and deployment parameters, as shown in Figure 8. The integrated end-to-end attack

workflow is illustrated in Algorithm 1 and can be described as follow:

The attacker first defines an attack scenario using scene parameters (described in Section IV-B1). MetaWave creates an MetaWave tag in the simulator with randomly initialized tag parameters as shown in Table II. Then, the MetaWave framework iteratively fine-tunes and optimizes the tag parameters to achieve the best attack performance and robustness. When the attacking loss is less than a predefined threshold or the maximum iterations count is reached, MetaWave outputs the tag design and deployment parameters. The attacker creates an actual MetaWave tag and deploys it following these parameters. The tag parameters are designed to have fault tolerance for real-world deployments to improve feasibility.

In this work, we define three meta-materials as mentioned in Section V-A. These meta-material tags can also be optimized to work for different frequencies simultaneously. Besides, it is worth noting that MetaWave is a general mmWave attack framework since the target algorithm, tag materials, etc., are configurable. In other words, it is highly scalable and supports wide range of RF frequencies and various sensing measurement algorithms and meta-materials.

VI. Evaluation Setup

We evaluate MetaWave in the simulation in Section VII and its real-world attack performance in Section VIII&IX.

mmWave Probe: We use a representative and commercial off-the-shelf radar with 24Ghz carrier frequency and FMCW modulation [41]. The supply voltage varies from 3.3V to 5.5V, the size of the probe is 5.0cm × 4.5cm and the weight of the probe is 250g, and the cost of the probe is less than $300. Thus, this probe is suitable as a testbed to be spoofed.

Computing Device: MetaWave's system is completed on an ordinary PC equipped with an Intel Core i7-8700K 3.70GHz CPU and one NVIDIA GTX1080 8 GB GPU.

Environments: As shown in Figure 10, we evaluate MetaWave in 20 different environments including indoor and outdoor parking lots, roads, and traffic intersections. at different times of days (8:00 - 22:00) with different weather conditions (e.g., fog, snow, and wind).

Objects Preparation: We recruit 17 different objects that most often appear in sensing scenarios, including roadblocks, humans, rocks, garbage cans, trees, and cars. All procedures follow the institutional IRB protocol.

Data Acquisition: As shown in Figure 9, we first collect COTS mmWave radar's sensing signal from the victim's perspective. For each trial, we collected a 60s raw signal from Vitim's radar to evaluate if the success rate that sensing result is spoofed. The obstacle is deployed at a four-meter range from the mmWave radar by default. The tags' deployment varies by application and will be specified for each experiment (e.g., on the obstacle, non-contact, hung on a drone, etc.). The tags are hexagon-shaped, and the size is according to the attack system's optimal output. The tag size ranges from 6cm to 50cm in edge length. In addition, we test square shaped tags with 100cm edge length.

Evaluation Metrics: To measure the effectiveness, pervasiveness, and adaptability of MetaWave attack in the real world, we employ Top-k for attack success rate. In this study, $k = 1, 3,$ and 5, which means we attack 1, 3, and 5 times for the same attack scenario. If there is any successful attack, we consider the whole trial attack successful. Top-k inference accuracy is defined as the percentage of successful trials. As discussed in Section III-A, the range, angle, and speed are the three fundamental properties of the sensing target. To prove MetaWave attack is not due to victim sensors' hardware measurement error-tolerance, we define a stricter and more reasonable **attack success criterion** that should be larger than the tolerance range [40]: (1) Range Measurement: the attack is considered a success if the sensing algorithm output no detection while a real object is presented, or vice versa (or more than ±0.9m from the actual range). (2) Angle Measurement: attack success if the sensing output is more than ±10° from the actual angle. (3) Speed Measurement: attack success if the sensing output is larger than ±0.19m/s from the actual speed. We quantify the attack result by calculating the Average Misalignment (AM) of the victim's measurement. Each Misalignment is calculated by $\frac{|x-y|}{\sigma} * 100\%$, where x is the sensing measurement result, y is the ground truth, and σ is the normal measurement tolerance. If AM is larger than 100%, it implies we attack successfully. Standard deviation (STD) is also adopted on top of AM to show case the attack robustness. With larger AM and STD, victim sensor experiences higher deviation from correct reading, leading to more severe consequences.

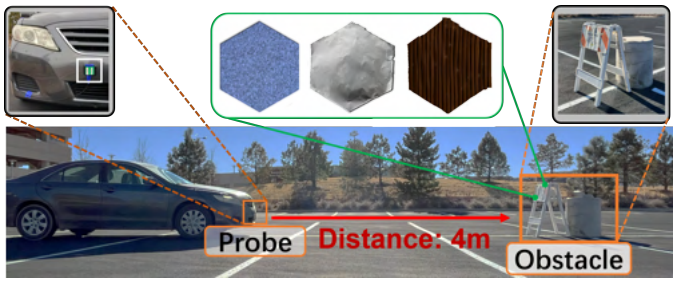


Fig. 9: System Setup implementation: the designed meta-material tags (from left to right: absorption, reflection, and polarization) with a mmWave sensing probe mounted on the vehicle/stand and the obstacle, imitating the mmWave sensor working in the real world.

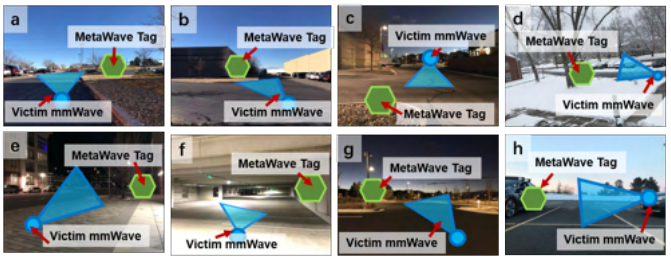


Fig. 10: Various environments at different times are utilized in the Evaluations. (a,b,e,d,g) are Roadsides, (c, f, h) are parking lots. (a,b,d,h) are during daytime, (c,e,f,g) are during nighttime. (d,h) are during snowy weather.

VII. Simulator-Based Attack System Evaluation

In this section, we evaluate MetaWave's attack performance in the simulation.

A. System Simulation Performance

We evaluate MetaWave simulator's capability and effectiveness of RF propagation with meta-material tag. We compare our simulator's result with the real-world echo signal. As shown in Figure 11, we test the MetaWave system with the three most common objects in the attack scenarios (e.g., human, car, and roadblock) with and without attacks. The results are shown in range-FFT. The X axis is the range, and the Y axis is the amplitude of the spectral signal. The average similarity between our simulator result and the corresponding real signal is 75.2%. For all scenarios, our simulator fully reflects the echo signal change and outputs the same attack performance as the real-world one. Thereby, our simulator in MetaWave has an excellent ability to help us explore the meta-materials effect on RF signals in this work.

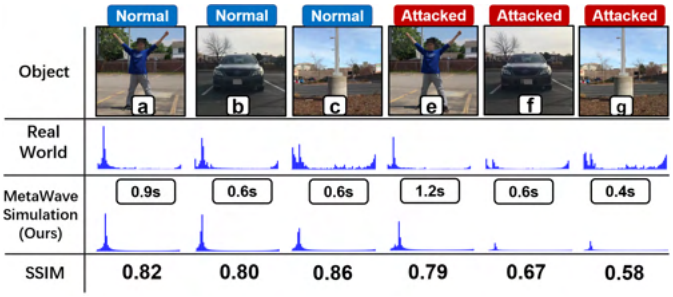


Fig. 11: The comparison between the real-world echo signal and our designed RF simulator with three representative mmWave sensing objects under without (a)-(c) and with (e)-(g) tag attacks.

Computational Overhead: The complexity of MetaWave simulator is approximately $O(nlogn)$ where n is the number of triangles representing scene geometries. It is much faster than other simulation methods such as FEM [43] and MoM [35], which complexity is $O(n^2)$. We evaluate the working time of three representative objects with six configurations in Figure 11. The average time cost for MetaWave to simulate mmWave echo signal for one scene is about 1s, 80-100X faster than the representative and professional product, FeKO [17].

B. Attack Robustness in the Simulator

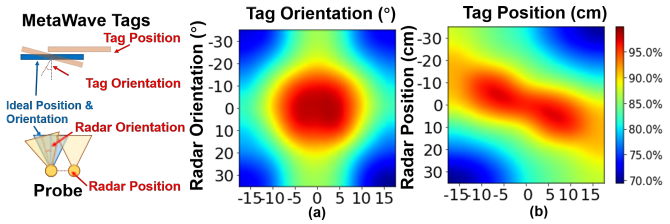


Fig. 12: Robustness Evaluation with the deployment condition in the simulator on the tag orientation and position.

To improve the MetaWave tags' deployment error tolerance and robustness, we include the location variation in the simulator-based optimization. Specifically, for each iteration, the MetaWave tag is placed at a distance of $\pm$ 15 cm and an angle of $\pm$ 10 degrees from the target location. The simulated VA attack results are shown in Figure 12. We observe that the simulated attack success rate remains high (above 99%) when radar orientation and tag orientation variation is less than 10 degrees. The average attack success rate in the simulator is 91.2%. The results are close to the performance in actual practice (see Section VIII-D). Thereby, MetaWave can simulate the variation of the tag parameters in the simulator and then support multi-directional attacks.

VIII. Practicality and Generalization Evaluation

In this section, we evaluate MetaWave's attack performance for different attack goals and tasks in the real world. Especially, for range, angle, and speed measurement attacks, the most representative and essential corresponding measurements in real practice are employed.

A. Overall Performance

We evaluate the ability of MetaWave to attack range, angle, and speed measurements with Top-1/3/5 inference accuracy. As shown in Figure 13, the Top-1 attack success rate for three measurements are all above 90% (i.e., Range: 97%, Angle: 96%, Speed: 91%), achieving equivalent performance as other state-of-the-art mmWave attack approaches in a more low-cost way [79]. Besides, the attacks can cause far greater errors in measurement results than the typical measurement tolerance. When attacking the mmWave system's range sensing, MetaWave can spoof the system and cause an average absolute error of 1.3m (STD: 1.27m) on sensing results (AM 144%, STD 141%). When attacking angle measurements, MetaWave can cause an average absolute error of 38 degrees (STD: 14 degrees) on sensing results (AM 384%, STD 194%). For speed measurements, MetaWave can cause an maximum absolute error of 5.4 m/s (50 percentile: 2.5m/s) on sensing results (AM 1570%, STD 7368%).

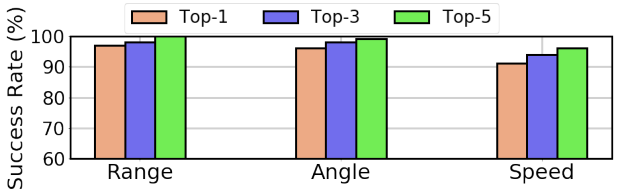


Fig. 13: Overall Performance of attacking range, angle, and speed sensing measurements.

B. MetaWave Tag Optimizer Analysis

To reflect our simulator optimization improving the MetaWave attack performance, we test the attacks with and without the guidance in the simulator-based optimization. When deploying without the tag optimization, we set up the tags based on our manual experience and understanding of the attack mechanism (i.e., estimate the mmWave sensor positions and the mmWave signal propagation physically present in the environment shown in Section III-B). For range and angle manual attacks, we place the tag at locations that would

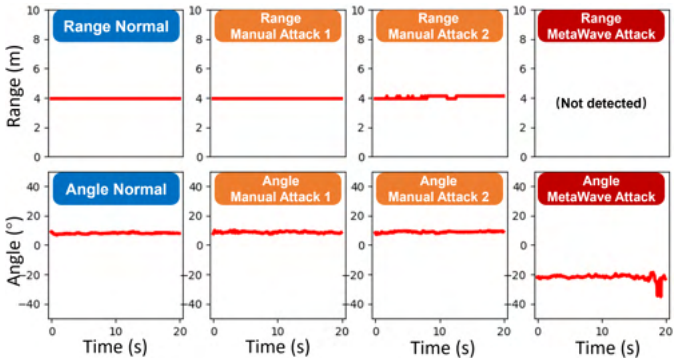


Fig. 14: The impact of the MetaWave Tag Optimizer on attack performance on range and angle measurements. The first column is the normal range reading without attack, the second and third columns are tag attacks without the optimizer, and the forth column is the tag attacks with the optimizer. The tag attacks with the optimization achieve over 99% attack success rate, while others fail.

intuitively trick the mmWave system, such as placing it in front of the obstacle for VA and placing on the road side for GA. To avoid personal preference, we conduct the attacks without the tag optimization twice for each setting. The attacks on the range and angle measurements results are shown in Figure 14. Both manual attacks without the optimization on both range and angle measurements lead to minute deviation from the normal one (the Top-1 attack success rates are all below 5%). In contrast, the attacks with the optimization lead to significant advancements (the Top-1 attack success rates are both over 99%). Overall, the tag optimizer enables attacks on the range and angle measurements and significantly improves their attack performance.

C. Trap Variation Analysis

Environmental Dynamic: To reflect the system performance withstanding environmental inferences in actual practice, we consider four common environmental dynamic factors in daily life for tests: (1) Temperature, range from -1$^{\circ}C$ to 20 $^{\circ}C$; (2) Humidity controlled from 20% to 70% (3) Lighting, the light intensity is controlled from 0Lux to 1000Lux; (4) Magnetic field strength is controlled from 100T to 400T. As shown in Figure 15(a), the results demonstrate that the attack success rate is all above 95%. Thereby, MetaWave presents a solid tolerance to different environmental dynamics.

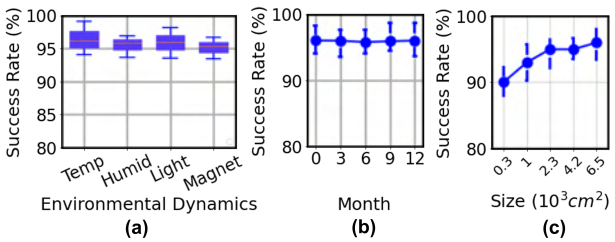


Fig. 15: (a) The performance under different environmental dynamics, including temperature, humidity, lighting, and magnetism respectively. (b) The longitude evaluation of a span of 12 months. (c) The performance under different tag size.

Longitude: To illustrate the reliability of the MetaWave tag, we evaluate the longitude test in 12 months. The MetaWave tags are stored in a normal environment with no special protective treatment. As shown in Figure 15(b), MetaWave can maintain a consistent and high attack success rate ($>$ 95%) for an extended period.

Tag Size: To illustrate the system performance under the impact of tag size, we evaluate the system effectiveness in the same application with difference tag size. In order to achieve the attacks, the tag size can be minimized to 20%-40% of the sensing cross-sectional area of the target objects. As shown in Figure 15(c), MetaWave attack size has better performance on larger tag, but still keep success rate even on smallest tags ($>$90% on 10cm length).

D. Attack Range Measurement

In this section, we evaluate MetaWave's attack success rate based on tag distance. We use range FFT [38] as the target distance measurement algorithm.

Impact of Tag Position: In a real attack, the position of the tag relative to the radar may not exactly match our ideal deployment in our simulation. Therefore, we evaluate MetaWave's tolerance on the tag's position. As shown in Figure 16(a), The attack results reach a high (above 94%) success rate when the position variation is less than 15cm, and it remains above 90% when larger than 10cm. The results show MetaWave has strong tolerance on tag deploy position when attacking distance measurement.

Impact of Tag Orientation: In a real attack, the orientation of the tag toward the radar may not exactly match our ideal deployment in our simulation. Therefore, we evaluate MetaWave's tolerance on the tag's orientation. As shown in Figure 16(a), we evaluate MetaWave's performance at different tag orientations. MetaWave gets a high (above 94%) attack success rate when the rotation variation is less than 7°, and it remains above 90% when the rotation variation is at 12°. Figure 16(a) manifests that the impact of the orientation is higher than the range since the mmWave signal has narrow beamforming. The results show MetaWave has strong tolerance on tag deploy orientation when attacking range measurement.

Impact of Tag Attack Duration: The stability of MetaWave's attack is crucial for the feasibility of real attacks. Therefore, we test the system with time duration from 0.3s to 1.5s. The average success rate is 97%, and all kept above 92%, which proves the reliability of MetaWave in the attack. The results show MetaWave is capable of attacking distance measurement with long-term stability.

E. Attack Angle Measurement

In this section, we evaluate MetaWave's performance when attacking angle measurement in real practice. We use Angle of Arrival (AoA) [44] as the target angle measurement algorithm. The results are shown in Figure 16(b).

Impact of Tag Position: As shown in Figure 16(b), the attack results reach a high (above 95%) success rate when the position variation is less than 10cm, and it remains above 90% when larger than 10cm. Thereby, MetaWave has strong tolerance on tag deploy position when attacking angle measurement.

Impact of Tag Orientation: MetaWave get a high (above 94%) attack success rate when the rotation variation is less than 7°, and it remains above 90% when the rotation variation is at 12°. It also shows the same phenomenon mentioned in Section VIII-D due to the narrow beamforming of the mmWave signal. The results show when attacking angle measurement, MetaWave can keep high performance when tag deploy orientation is slightly different from ideal deployment.

Impact of Tag Attack Duration: We test the system with time duration from 0.3s to 1.5s. The average success rate is 96%, and all kept above 88%, which proves MetaWave attack system is capable of attacking angle measurement with long-term stability.

F. Attack Speed Measurement

mmWave sensing senses the velocity of the target object via the Doppler effect. In this work, we use the Range-doppler algorithm [85] as the target algorithm. The results are shown in Figure 16(c). Unlike the distance and angle measurements, the attacks on speed measurement show irregular results because the doppler algorithm is susceptible to micro-motion.

Impact of Tag Position: As shown in Figure 16(c), the attack results reach a high (above 92%) success rate when the position variation is less than 10cm, and it remains above 88% when larger than 10cm. The results show MetaWave has a strong tolerance on tag deploy position when attacking speed measurement in real practice.

Impact of Tag Orientation: MetaWave get a high (above 94%) attack success rate when the rotation variation is less than 7°, and it remains above 90% when the rotation variation is at 12°. The minimum is 84% when the rotation error is larger than 20°. Thus, MetaWave shows a strong tolerance on tag deploy orientation when attacking speed measurement in real practice.

Impact of Tag Attack Duration: We test the system with time duration from 0.3s to 1.5s. The average success rate is 91%, and all kept above 85%. The average success rate is 97% while 5 frames have the best performance. At all time intervals, it still kept above 73%, which proves MetaWave attack system can attack the speed measurement with long-term stability.

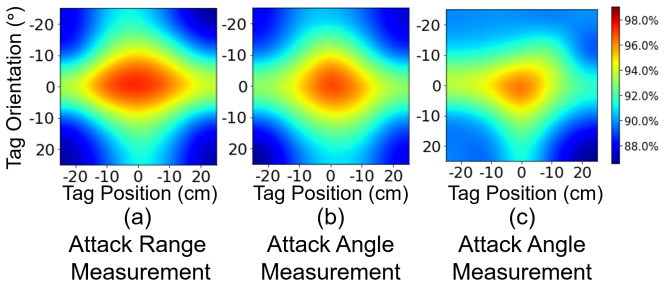
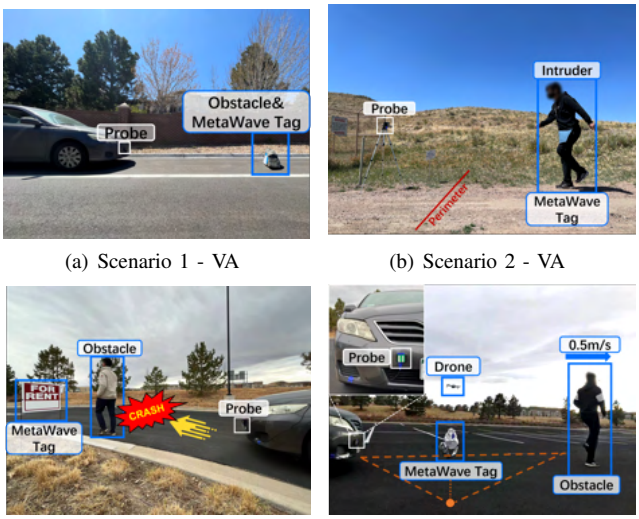


Fig. 16: The generalization evaluation of attacks on the range, angle, and speed measurements. The X axis is the variance of tag position, the Y axis is the variance of tag orientation, the color illustrates the attack success rate.

IX. Real-world Attack Evaluation

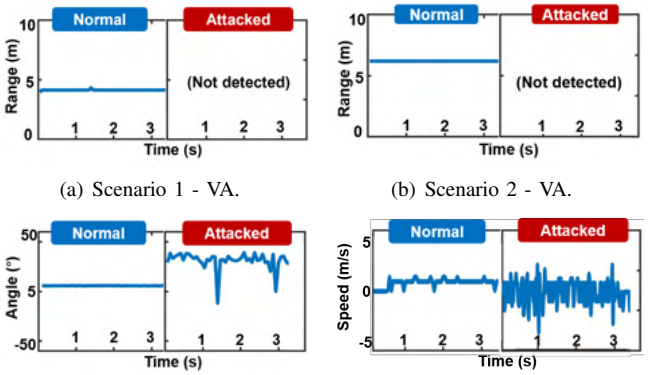
The attack system can be utilized in various public spaces since the high accessibility and portability of the setup. Thus, to evaluate MetaWave's attack performance in the real world, we conduct the MetaWave attacks on mmWave sensing in five scenarios. In Scenario 1, 3, and 4, we mount the mmWave sensor in front of a sedan car, and in Scenario 2, the mmWave sensor is deployed close to the security fence, imitating/hypothesizing the mmWave radar working on the vehicle/robot and the perimeter security, respectively, in the real world (but not on the real professional products).



(a) Scenario 1 - VA (b) Scenario 2 - VA

(c) Scenario 3 - VA (d) Scenario 4 - GA

Fig. 17: Attack scenarios for VA (a)-(c) and GA (d).



(a) Scenario 1 - VA. (b) Scenario 2 - VA.

(c) Scenario 3 - VA. (d) Scenario 4 - GA.

Fig. 18: Attacked sensing result compared with normal sensing result without MetaWave spoofing.

Scenario 1 (VA): We first test MetaWave tag's ability to hide potentially dangerous objects (e.g., rock on the road) from mmWave sensing systems. We place a rock in front of the mmWave probe at the 3m range and use the MetaWave tag to cover it, as shown in Figure 17(a). The average attack success rate is 88% (refer to Figure 18(a)), and the mmWave sensing system barely recognizes the obstacle continuously.

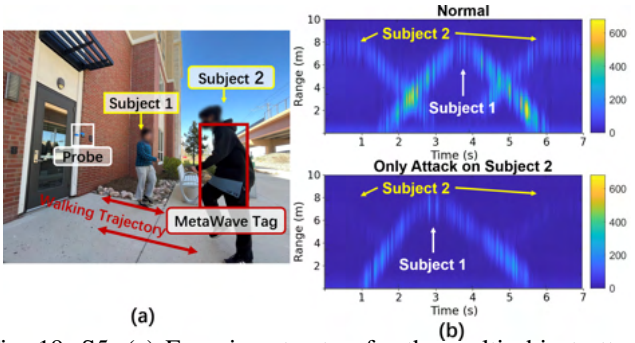
Scenario 2 (VA): MetaWave can also be used to hide trespassing intruders from being detected by mmWave sensing

systems. We place a mmWave surveillance probe at 2 m height on a light pole to cover a rectangular-shaped perimeter as shown in Figure 17(b). Figure 18(b) shows that MetaWave attack system successfully attacks the radar algorithm as it fails to detect the intruder with our attack success being 93 %.

Scenario 3 (VA): We then test MetaWave tag's ability to spoof mmWave sensing systems in obstacle detection. We place a MetaWave tag on the road side disguised as a normal house rental sign to make the pedestrian disappear in mmWave sensor sight, which can lead to vehicles hitting the pedestrian unexpectedly. The MetaWave tag is placed 0.5m away from the curb line, and a pedestrian walks in the vehicle's direction right in front of the vehicle, as shown in Figure 17(c). Figure 18(c) shows that the vehicle's mmWave sensing system only recognizes the road sign around 40 ° on the side and filters out the pedestrian's signal. The top-1 attack success rate is 89%, which proves MetaWave can be extremely dangerous when an adversary deploys such attacks in real-life.

Scenario 4 (GA): We then examine MetaWave tag's ability to create a ghost in front of mmWave sensing radar. We deploy a 3D tag hung under a drone that creates a ghost obstacle before the mmWave probe. The attacker can constantly control and maintain the distance (around 1.5m here) between the vehicle and the tag via the drone [32], as shown in Figure 17(d). As a comparison, an actual obstacle moves at a speed of 0.5 meters per second. The tag can spoof the vehicle that there is only one static large object ahead and make it sudden brake or force it to change the lane. As shown in Figure 18(d), the average success rate is 95%, proving MetaWave has the capability to create the ghost object remotely.

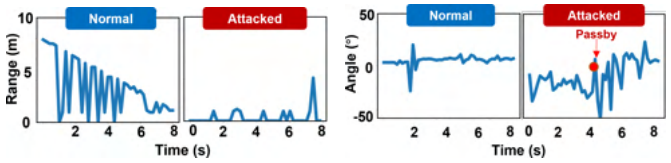
Scenario 5 (VA): Multi-object Attack under the Complex Scene. MetaWave is also capable of targeting specific attacks in multi-object scenarios. As shown in upper part of Figure 19, the range FFT heatmap can clearly distinguish two subjects. However, the echo signal from Subject 2 is significantly decreased to ground noise level if Subject 2 is carrying a MetaWave tag, as shown in the lower part. It is worth mentioning that vanishing Subject 2 does not affect Subject 1's sensor reading, making the attack stealthy and difficult to recognize. Thereby, MetaWave is capable of the precise and practical multi-object attack.



(a) (b)

Fig. 19: S5: (a) Experiment setup for the multi-object attack. (b) Range FFT heatmap showing the disappearance of subject-2's trajectory with the MetaWave tag.

Scenario 6 (VA&GA): Dynamic Attack of the Moving mmWave Sensor. We examine MetaWave tag's threat in a dynamic scenario when the radar is moving toward the target at a speed of 1m/s. As shown in Figure 20, MetaWave tag can alter the mmWave sensor's reading in terms of both range (e.g., from 9m distance to disappear) and angle (e.g., from straight ahead to on the side), which spoofs the victim's ability to detect forward collision. For attacking range measurement, the tag is attached to the target. For attacking angle measurement, the tag is placed in the middle of the vehicle and the object and at a 45-degree angle from the vehicle's initial position. As the vehicle moves forward, it passes the tag, so we only calculate the success rate of the attack before it passes by. The average success rate for range and angle (before pass by) is 92% and 93%, respectively. The results prove MetaWave has the capability to achieve GA and VA when the radar is moving.

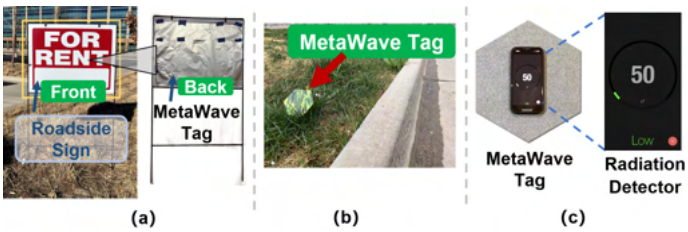


(a) S6-VA on Range. (b) S6-GA on Angle.

Fig. 20: Attack results when the victim carrying mmWave sensor is moving.

X. Countermeasure

In this section, we present defense mechanisms against MetaWave from both security check (i - ii) and victim awareness perspectives (iii - v).



(a) (b) (c)

Fig. 21: (a), (b), (c) show MetaWave tags can be disguised by a billboard to improve stealthiness, are hard to be detected by a radiation detector and can be camouflaged with paint to evade visual detection, respectively.

(i) Manual Check: Civilians can take precautions by calling attention to suspicious people or signs around them, or even acquire law enforcement teams for inspection. However, such method is rarely effective given MetaWave tag's ability to hide and camouflage as shown in Figure 21(a,b). Moreover, manual check is time-consuming (i.e., the forensics team can take minutes, hours to travel, while the mmWave sensing systems make decisions in real-time), and costly (i.e., giving up work duties and spending a long time on an object that only appears suspicious is not socially acceptable).

(ii) Radiation Detection: Another famous defense against RF attacks is to detect suspicious electromagnetic signals or radiation devices in the environment, similar to highway patrol officers detecting radar jammers [64]. However, the MetaWave tags work passively. We scan the MetaWave tags with an

TABLE III: A comparison of existing mmWave attack approaches. Note: these prior works do not provide the quantitative results with large trials, thus, high level comparison is showcased.

Work	Attack Method	Cost	Stealthiness	Multi-objects Attack	Against RF Fingerprint/False Alarm Detection	Obtainability
Nallabolu *et al.* [57]	RF Modulator-based (*bladeRF 2.0 boards*)	High (*>$1300*)	No (detectable with RF sensors)	Yes	No/Not Mentioned	Difficult
Sun *et al.* [79]	RF Modulator-based (*EV-RADAR-MMIC2*)	High (*>$800*)	No (short attack distance)	No	No/Not Mentioned	Difficult
Komissarov *et al.* [47]	RF Modulator-based (*60GHz mmwave RX/TX*)	High (*>$2000*)	No (need many attack devices)	No	No/Not Mentioned	Difficult
Nashimoto *et al.* [58]	RF Modulator-based (*Pasternack PE15A1010*)	Medium (*>$100*)	No (active attack)	No	No/Not Mentioned	Easily
MetaWave (ours)	**Meta-material-based (*Passive Tag*)**	**Low (*∼$10*)**	**Yes**	**Yes**	**Yes/Yes**	**Easily**

Electromagnetic Fields (EMF) Radiation Detector product [4], and the scan result is illustrated in Figure 21(c), showing the MetaWave tags have nearly no active radiation. Thus, this detection approach is hard to prevent our attack.

(iii) RF Fingerprint: Recently RF signal fingerprinting has gained attention in detecting sensing attacks, which utilizes the unique physical characteristics of the probe components to judge if the echo signal comes from the same electronic instruments. However, MetaWave directly attacks the sensing signal from the original mmWave probe instead of the computing part, making this countermeasure ineffective. We evaluate this protection with the approach in [79]. In the feature extraction, the statistical features of standard deviation, kurtosis, skewness of magnitude, and phase of the received signal are employed. Besides, the support vector machine is selected for one-class classification. As a result, the feature patterns between with/without attacks are similar, and the detection classification result is close to a random guess. Thus, this approach can not recognize the attack from MetaWave tags.

(iv) False Alarm Detection: In RF sensing practice, the Constant False-Alarm Rate (CFAR) technology [60] with the dynamic threshold is always used to rule out the active or passive noise and then resist the interference. However, we directly utilize meta-material tags to change the echo signal along with the environment (see Section III-D). We apply the classic CFAR detection [3], [70] on the range-FFT of the echo signal with the setup in Figure 9, and it is also undetected in the VA attack and falsely detected in the GA attack. Thus, such false alarm detection can not resist our attack.

(v) Multiply mmWave Sensors: It is possible that some devices may employ different mmWave sensors operating under different sensing frequency. However, MetaWave attacks are effective over a wide band of sensing frequencies simultaneously (e.g., multi-Ghz in Section III-B). Further, MetaWave tags can be inexpensively designated to specific ranges of frequencies and work together against redundant frequencies. Thus, this redundancy alone is unlikely to work.

XI. Discussion

Stealthy Analysis: The MetaWave tag works passively and can be camouflaged by plastic signs or billboards as common objects without causing visual vigilance. Such camouflaging material (e.g., plastic, wood) often exhibits little interference to attack performance, making it deceitful for human visual inspection.

Sensing Modalities: The scope of this paper focuses on the mmWave sensing attack by modulating the physical echo signal under representative attack scenarios where the mmWave sensor has been widely used for years in practice. For example, some perimeter surveillance systems are based on mmWave sensing [6], [7]. And some driver assistance systems' adaptive cruise control functionality on automotive vehicles often solely rely on a front-facing mmWave radar [8], [5]. Besides, vehicles or robots can employ a variety of sensors (e.g., Lidar, Camera, mmWave) to detect the surrounding environment by making decisions together in real practice. However, due to the mmWave sensing system's innate spatial perception advantages, applications' high-level decisions rely heavily on mmWave for range, angle, and velocity measurements or under undesirable ambient conditions (e.g., lighting, smoke, and fog) where other sensors do not work well [66], [76]. Moreover, since the mmWave sensing result is fused in the final decision, the final decision is inevitably influenced if the mmWave sensing is impacted [84].

Attack Cost Analysis: The average cost is $10-30 for the absorbing tag, $9-16 for the polarizing tag, and about two cents for the reflecting tag. Comparing to existing mmWave attack solutions as referenced in Table III, MetaWave is 10-100 times cheaper [58].

Practicality Analysis: MetaWave can achieve a practical mmWave sensing attack with minimal cost. Overall, MetaWave can stealthily achieve a high attack success rate and withstand harsh weather. Besides, MetaWave's tag can be integrated with mobile robots (e.g., drones, robot arms) for more complex attacks that involve motion for timely evasion and camouflage. Additionally, although we imitate real-world environments with our mmWave radars in evaluations without justifying

this attack on professional products, this work arouses public attention and provides in-depth explorations on this new attack type.

Attack Distance: The mmWave radar in practical applications usually cannot precisely sense within around 0.2-1m because of the physical limitations. Therefore, for VA, the MetaWave tag can work when the distance is larger than 0.2m. The maximum sensing distance of the vehicle mmWave radar is usually 160m [10], while the response distance to make the vehicle brake automatically depends on the speed of the vehicle (e.g., 73m stopping distance for a speed of 96km per hour [11]). By optimizing the MetaWave tag, we can vanish the obstacle or generate a ghost at the location of the maximum sensing distance to achieve the attack.

Signal Modulation Technology: As mentioned in Section IV-B, besides FMCW, MetaWave can also work on other popular types of signal modulation technology, such as CW, FSK/FMSK, and Digital Code Modulation (DCM). MetaWave can integrate different signal modulation technologies into the physical law-based calculation. Besides, the MetaWave attack mechanism is primarily based on the fundamental properties of the sensing signal.

Future Applications: (i) Since MetaWave modulates fundamental properties (e.g., amplitude, phase) of the sensing echo signal physically (mechanism see Section III-B), MetaWave can also work on other developing and emerging mmWave applications or products (e.g., object recognition, vital signal measurement, human activity monitoring, object classification/identification, and simultaneous mapping and localization [21], [1], [2]). (ii) MetaWave simulator can be utilized for advancing a general and scalable RF sensing framework and for attacking other frequencies (e.g., Sub-6, 60/77-81 GHz, Terahertz), since the physical laws utilized can also be applied to these frequency bands as long as the size of the target is not smaller than the sensing signal wavelength [46]. (iii) Besides, the MetaWave attack framework can promote exploring physical attacks on other sensing modalities (e.g., Lidar and infrared camera) in a more comprehensive and explainable way.

Material Healthiness: Material healthiness is considered in the attack. In order to ensure the stealthiness and practicality of the attack, the attacker needs to wear the material in a regular suit without causing any alert or notice. If the attacker needs extra protection against the harmful material, it will significantly affect stealthiness and fail the attack.

XII. Related work

Attack on mmWave Sensing: As shown in Table III, existing mmWave sensing system attacks utilizing professional electronic transmission devices to spoof location/velocity measurement [79], [57], [47], [58], however, such systems are high cost and can be easily traced by RF sensors on-site. Unlike the previous approaches, MetaWave proposes and designs a new attack type towards mmWave sensing based on low-cost meta-material tags and the simulator. It is also the first work of this attack type.

Physical Attacks on Sensing: Existing physical attack methods can be mainly summarized into three categories based on their sensing modality: (1) *Camera:* Many attacks on cameras use physical patterns to spoof recognition or classification, such as special stickers [37], [33], [77], T-shirts [88], or posters [86]. (2) *Lidar:* Most approaches are achieved by placing objects with special geometric shapes [69], [26], [25], [80], [63] to spoof the segmentation or recognition models. (3) *Microphone:* Most approaches use speakers to play unusual noises over-the-air to make the Automatic Speech Recognition unable to distinguish or misunderstand voice commands [68], [28], [87], [23]. Most of these works weigh on the shortcoming of the computing modules. Oppositely, in MetaWave, we explore the fundamental characteristics of mmWave signals and provide a novel explainable and practical attack approach on the signal side.

mmWave Sensing with Meta-material Tags: mmWave sensing has been growing popularity in a variety of domains, such as hand gesture monitoring [51], human activity [89], vital sign monitoring [52], [55], vibration measurement [42], material types and object status [93], [27], [55], [65], [50], localization and mapping [54], [83], and object imaging [36], [94], [67]. Besides, mmWave sensing is also applied to interact with meta-material tags enabling new paradigms and applications, such as tagging infrastructure [49], wireless temperature monitoring [27], and through-wall communication [30], [29]. To our best knowledge, MetaWave is the first work to utilize the meta-material-enhanced tags to attack mmWave sensing passively.

XIII. Conclusion

This paper designed and implemented a novel passive attack on mmWave sensing with meta-material-enhanced tags. We started with the mmWave signal's properties and passive modulation capabilities on RF signals of different meta-material tags. Then, to optimize the attack, we proposed a general attack framework that includes a simulator of RF and methods that utilize gradient descent to find the optimal parameters of the MetaWave tag. Furthermore, extensive real-world experiments indicated that our MetaWave can achieve an average attack success rate of 97% on range measurement, 96% on angle measurement, and 91% on speed measurement. Various levels of evaluation proved the stealthiness, robustness, and reliability of our proposed system in actual practice. MetaWave has the potential to bring a new research vision about the meta-material for wireless sensing and cyber-infrastructure security in the 5G/6G era.

References

[1] "Ai sensing." [Online]. Available: https://matrixspace.com/ai-sensing/

[2] "Amazon astro." [Online]. Available: https://www.amazon.com/dp/B078NSDFSB

[3] "Constant false alarm rate (cfar) detection." [Online]. Available: https://www.mathworks.com/help/phased/ug/constant-false-alarm-rate-cfar-detection.html

[4] "Emf radiation detector." [Online]. Available: https://apps.apple.com/us/app/emf-radiation-detector/id1046907307

[5] "Kia safety technology." [Online]. Available: https://www.kia.com/us/en/adas

[6] "Psrs perimeter surveillance radar system." [Online]. Available: https://www.security.honeywell.com/product-repository/psrs-perimeter-surveillance-radar-system

[7] "Shenzhen security exhibition: radar security application of the new engine." [Online]. Available: http://en.nanoradar.cn/Article/detail/id/409.html

[8] "What is honda sensing® suite? features amp; more: Honda." [Online]. Available: https://automobiles.honda.com/sensing

[9] "Continental automotive - radars," April 2022. [Online]. Available: https://www.continental-automotive.com/en-gl/Passenger-Cars/Autonomous-Mobility/Enablers/Radars

[10] "Honda civic teardown: Adas (advanced driver-assistance system)," Jan 2022. [Online]. Available: https://www.marklines.com/en/report_all/rep1740_201808

[11] "How speed affects braking distance," April 2022. [Online]. Available: https://www.aceable.com/safe-driving/how-speed-affects-braking-distance/

[12] "Selection of pcb materials for 5g," April 2022. [Online]. Available: https://rogerscorp.com/-/media/project/rogerscorp/documents/articles/english/advanced-connectivity-solutions/selection-of-pcb-materials-for-5g.pdf

[13] "A tesla vehicle using 'smart summon' appears to crash into a $3.5 million private jet," April 2022. [Online]. Available: https://www.theverge.com/2022/4/22/23037654/tesla-crash-private-jet-reddit-video-smart-summon

[14] ""front-radar-sensor." bosch mobility solutions," April 2022. [Online]. Available: https://www.bosch-mobility-solutions.com/en/solutions/sensors/front-radar-sensor/

[15] "The basics of polarization animated guides," 2022-04-15. [Online]. Available: https://www.specac.com/en/news/calendar/2018/04/polarization-basics

[16] "C-ram lf-72," 2022-04-15. [Online]. Available: https://stores.cumingmicrowave-online-store.com/c-ram-lf-72/

[17] "Simulation for connectivity, compatibility, and radar altair feko," 2022-04-15. [Online]. Available: https://www.altair.com/feko/

[18] "Tesla autopilot crashes and causes," 2022-04-15. [Online]. Available: https://www.autopilotreview.com/tesla-autopilot-accidents-causes

[19] "Tesla drivers report a surge in phantom braking," 2022-04-15. [Online]. Available: https://www.washingtonpost.com/technology/2022/02/02/tesla-phantom-braking

[20] R. Appleby and R. N. Anderton, "Millimeter-wave and submillimeter-wave imaging for security and surveillance," *Proceedings of the IEEE*, vol. 95, no. 8, pp. 1683–1690, 2007.

[21] D. Barnes, M. Gadd, P. Murcutt, P. Newman, and I. Posner, "The oxford radar robotcar dataset: A radar extension to the oxford robotcar dataset," in *2020 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2020, pp. 6433–6438.

[22] F. O. Bartell, E. L. Dereniak, and W. L. Wolfe, "The theory and measurement of bidirectional reflectance distribution function (brdf) and bidirectional transmittance distribution function (btdf)," in *Radiation scattering in optical systems*, vol. 257. SPIE, 1981, pp. 154–160.

[23] S. Bhattacharya, D. Manousakas, A. G. C. Ramos, S. I. Venieris, N. D. Lane, and C. Mascolo, "Countering acoustic adversarial attacks in microphone-equipped smart home devices," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 2, pp. 1–24, 2020.

[24] A. Boloor, X. He, C. Gill, Y. Vorobeychik, and X. Zhang, "Simple physical adversarial examples against end-to-end autonomous driving models," in *2019 IEEE International Conference on Embedded Software and Systems (ICESS)*. IEEE, 2019, pp. 1–7.

[25] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, "Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 176–194.

[26] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2267–2281.

[27] B. Chen, H. Li, Z. Li, X. Chen, C. Xu, and W. Xu, "Thermowave: a new paradigm of wireless passive temperature monitoring via mmwave sensing," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020, pp. 1–14.

[28] G. Chen, S. Chenb, L. Fan, X. Du, Z. Zhao, F. Song, and Y. Liu, "Who is real bob? adversarial attacks on speaker recognition systems," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 694–711.

[29] L. Chen, W. Hu, K. Jamieson, X. Chen, D. Fang, and J. Gummeson, "Pushing the physical limits of iot devices with programmable metasurfaces," in *18th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 21)*, 2021, pp. 425–438.

[30] K. W. Cho, M. H. Mazaheri, J. Gummeson, O. Abari, and K. Jamieson, "mmwall: A reconfigurable metamaterial surface for mmwave networks," in *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*, 2021, pp. 119–125.

[31] M. Di Renzo, K. Ntontin, J. Song, F. H. Danufane, X. Qian, F. Lazarakis, J. De Rosny, D.-T. Phan-Huy, O. Simeone, R. Zhang *et al.*, "Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 798–807, 2020.

[32] DJI, "Dji mini se," 2021. [Online]. Available: https://www.dji.com/mini-se

[33] I. Evtimov, K. Eykholt, E. Fernandes, T. Kohno, B. Li, A. Prakash, A. Rahmati, and D. Song, "Robust physical-world attacks on machine learning models," *arXiv preprint arXiv:1707.08945*, vol. 2, no. 3, p. 4, 2017.

[34] FAA, "How to register your drone," 2021. [Online]. Available: https://www.faa.gov/uas/getting$_$started/register$_$drone/

[35] W. C. Gibson, *The method of moments in electromagnetics*. Chapman and Hall/CRC, 2007.

[36] J. Guan, S. Madani, S. Jog, S. Gupta, and H. Hassanieh, "Through fog high-resolution imaging using millimeter wave radar," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020.

[37] Y. Guo, X. Wei, G. Wang, and B. Zhang, "Meaningful adversarial stickers for face recognition in physical world," *arXiv preprint arXiv:2104.06728*, 2021.

[38] M. Z. Ikram, A. Ahmad, and D. Wang, "High-accuracy distance measurement using millimeter-wave radar," in *2018 IEEE Radar Conference (RadarConf18)*. IEEE, 2018, pp. 1296–1300.

[39] A. Ilyas, L. Engstrom, A. Athalye, and J. Lin, "Black-box adversarial attacks with limited queries and information," in *International Conference on Machine Learning*. PMLR, 2018, pp. 2137–2146.

[40] Infineon, "24ghz transceiver," 2021. [Online]. Available: https://www.infineon.com/dgdl/Infineon-AN553$_$BGT24MTR12$_$XMC4700$_$Position2Go$_$DemoBoard-ApplicationNotes-v01$_$02-EN.pdf?fileId=5546d4626cb27db2016d44631adb021f

[41] ——, "Demo position2go," 2021. [Online]. Available: https://www.infineon.com/cms/en/product/evaluation-boards/demo-position2go/

[42] C. Jiang, J. Guo, Y. He, M. Jin, S. Li, and Y. Liu, "mmvib: micrometer-level vibration measurement with mmwave radar," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020, pp. 1–13.

[43] J.-M. Jin, *The finite element method in electromagnetics*. John Wiley & Sons, 2015.

[44] C. R. Karanam, B. Korany, and Y. Mostofi, "Magnitude-based angle-of-arrival estimation, localization, and target tracking," in *2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2018, pp. 254–265.

[45] J. Kiefer and J. Wolfowitz, "Stochastic estimation of the maximum of a regression function," *The Annals of Mathematical Statistics*, pp. 462–466, 1952.

[46] R. E. Kleinman, "The rayleigh region," *Proceedings of the IEEE*, vol. 53, no. 8, pp. 848–856, 1965.

[47] R. Komissarov and A. Wool, "Spoofing attacks against vehicular fmcw radar," *arXiv preprint arXiv:2104.13318*, 2021.

[48] T.-M. Li, M. Aittala, F. Durand, and J. Lehtinen, "Differentiable monte carlo ray tracing through edge sampling," *ACM Transactions on Graphics (TOG)*, vol. 37, no. 6, pp. 1–11, 2018.

[49] Z. Li, B. Chen, Z. Yang, H. Li, C. Xu, X. Chen, K. Wang, and W. Xu, "Ferrotag: A paper-based mmwave-scannable tagging infrastructure," in *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*, 2019, pp. 324–337.

[50] Z. Li, F. Ma, A. S. Rathore, Z. Yang, B. Chen, L. Su, and W. Xu, "Wavespy: Remote and through-wall screen attack via mmwave sensing," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 217–232.

[51] J. Lien, N. Gillian, M. E. Karagozler, P. Amihood, C. Schwesig, E. Olson, H. Raja, and I. Poupyrev, "Soli: Ubiquitous gesture sensing with millimeter wave radar," *ACM Transactions on Graphics (TOG)*, vol. 35, no. 4, pp. 1–19, 2016.

[52] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '17. New York, NY, USA: ACM, 2017, pp. 315–328.

[53] H. Ling, R.-C. Chou, and S.-W. Lee, "Shooting and bouncing rays: Calculating the rcs of an arbitrarily shaped cavity," *IEEE Transactions on Antennas and propagation*, vol. 37, no. 2, pp. 194–205, 1989.

[54] C. X. Lu, S. Rosa, P. Zhao, B. Wang, C. Chen, J. A. Stankovic, N. Trigoni, and A. Markham, "See through smoke: robust indoor mapping with low-cost mmwave radar," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020, pp. 14–27.

[55] C. X. Lu, M. R. U. Saputra, P. Zhao, Y. Almalioglu, P. P. de Gusmao, C. Chen, K. Sun, N. Trigoni, and A. Markham, "milliego: single-chip mmwave radar aided egomotion estimation via deep sensor fusion," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys)*, 2020.

[56] T. Möller and B. Trumbore, "Fast, minimum storage ray-triangle intersection," *Journal of graphics tools*, vol. 2, no. 1, pp. 21–28, 1997.

[57] 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.

[58] S. Nashimoto, D. Suzuki, N. Miura, T. Machida, K. Matsuda, and M. Nagata, "Low-cost distance-spoofing attack on fmcw radar and its feasibility study on countermeasure," *Journal of Cryptographic Engineering*, pp. 1–10, 2021.

[59] P. Nguyen, V. Kakaraparthi, N. Bui, N. Umamahesh, N. Pham, H. Truong, Y. Guddeti, D. Bharadia, R. Han, E. Frew *et al.*, "Dronescale: drone load estimation via remote passive rf sensing," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 326–339.

[60] R. Nitzberg, "Constant-false-alarm-rate signal processors for several types of interference," *IEEE Transactions on Aerospace and Electronic Systems*, no. 1, pp. 27–34, 1972.

[61] J. Nolan, K. Qian, and X. Zhang, "Ros: passive smart surface for roadside-to-vehicle communication," in *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, 2021, pp. 165–178.

[62] H. W. Ott and H. W. Ott, *Noise reduction techniques in electronic systems*. Wiley New York, 1988, vol. 442.

[63] W. Park, N. Liu, Q. A. Chen, and Z. M. Mao, "Sensor adversarial traits: Analyzing robustness of 3d object detection sensor fusion models," in *2021 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2021, pp. 484–488.

[64] C. Peterson, "How police radar works, how to avoid it with the best radar detector," Jan 2021. [Online]. Available: https://radartest.com/how-radar-works.asp

[65] A. Prabhakara, V. Singh, S. Kumar, and A. Rowe, "Osprey: a mmwave approach to tire wear sensing," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020.

[66] K. Qian, Z. He, and X. Zhang, "3d point cloud generation with millimeter-wave radar," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 4, pp. 1–23, 2020.

[67] K. Qian, S. Zhu, X. Zhang, and L. E. Li, "Robust multimodal vehicle detection in foggy weather using complementary lidar and radar signals," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 444–453.

[68] Y. Qin, N. Carlini, G. Cottrell, I. Goodfellow, and C. Raffel, "Imperceptible, robust, and targeted adversarial examples for automatic speech recognition," in *International conference on machine learning*. PMLR, 2019, pp. 5231–5240.

[69] H. Ren and T. Huang, "Adversarial example attacks in the physical world," in *International Conference on Machine Learning for Cyber Security*. Springer, 2020, pp. 572–582.

[70] M. A. Richards, *Fundamentals of radar signal processing*. McGraw-Hill Education, 2014.

[71] H. Robbins and S. Monro, "A stochastic approximation method," *The annals of mathematical statistics*, pp. 400–407, 1951.

[72] C. Schöffmann, B. Ubezio, C. Böhm, S. Mühlbacher-Karrer, and H. Zangl, "Virtual radar: Real-time millimeter-wave radar sensor simulation for perception-driven robotics," *IEEE Robotics and Automation Letters*, vol. 6, no. 3, pp. 4704–4711, 2021.

[73] C. Schüßler, M. Hoffmann, J. Bräunig, I. Ullmann, R. Ebelt, and M. Vossiek, "A realistic radar ray tracing simulator for large mimo-arrays in automotive environments," *IEEE Journal of Microwaves*, vol. 1, no. 4, pp. 962–974, 2021.

[74] D. R. I. M. Setiadi, "Psnr vs ssim: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications*, vol. 80, pp. 8423–8444, 2021.

[75] M. Shahid, A. Rossholm, B. Lövström, and H.-J. Zepernick, "No-reference image and video quality assessment: a classification and review of recent approaches," *EURASIP Journal on image and Video Processing*, vol. 2014, no. 1, pp. 1–32, 2014.

[76] J. Shen, N. Wang, Z. Wan, Y. Luo, T. Sato, Z. Hu, X. Zhang, S. Guo, Z. Zhong, K. Li *et al.*, "Sok: On the semantic ai security in autonomous driving," *arXiv preprint arXiv:2203.05314*, 2022.

[77] D. Song, K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, F. Tramer, A. Prakash, and T. Kohno, "Physical adversarial examples for object detectors," in *12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18)*, 2018.

[78] P. Staat, H. Elders-Boll, M. Heinrichs, C. Zenger, and C. Paar, "Mirror mirror on the wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces," *arXiv preprint arXiv:2107.01709*, 2021.

[79] 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.

[80] J. Tu, M. Ren, S. Manivasagam, M. Liang, B. Yang, R. Du, F. Cheng, and R. Urtasun, "Physically realizable adversarial examples for lidar object detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 13 716–13 725.

[81] M. Vinkler, J. Bittner, and V. Havran, "Extended morton codes for high performance bounding volume hierarchy construction," in *Proceedings of High Performance Graphics*, 2017, pp. 1–8.

[82] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.

[83] T. Wei and X. Zhang, "mtrack: High-precision passive tracking using millimeter wave radios," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, 2015, pp. 117–129.

[84] Z. Wei, F. Zhang, S. Chang, Y. Liu, H. Wu, and Z. Feng, "Mmwave radar and vision fusion for object detection in autonomous driving: A review," *Sensors*, vol. 22, no. 7, p. 2542, 2022.

[85] V. Winkler, "Range doppler detection for automotive fmcw radars," in *2007 European Radar Conference*. IEEE, 2007, pp. 166–169.

[86] R. R. Wiyatno and A. Xu, "Physical adversarial textures that fool visual object tracking," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2019, pp. 4822–4831.

[87] Y. Xie, C. Shi, Z. Li, J. Liu, Y. Chen, and B. Yuan, "Real-time, universal, and robust adversarial attacks against speaker recognition systems," in *ICASSP 2020-2020 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 2020, pp. 1738–1742.

[88] K. Xu, G. Zhang, S. Liu, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, and X. Lin, "Adversarial t-shirt! evading person detectors in a physical world," in *European Conference on Computer Vision*. Springer, 2020, pp. 665–681.

[89] H. Xue, Y. Ju, C. Miao, Y. Wang, S. Wang, A. Zhang, and L. Su, "mmmesh: towards 3d real-time dynamic human mesh construction using millimeter-wave," in *Proceedings of the 19th Annual International*

Conference on Mobile Systems, Applications, and Services, 2021, pp. 269–282.

[90] H. Yang, X. Cao, F. Yang, J. Gao, S. Xu, M. Li, X. Chen, Y. Zhao, Y. Zheng, and S. Li, "A programmable metasurface with dynamic polarization, scattering and focusing control," *Scientific reports*, vol. 6, no. 1, pp. 1–11, 2016.

[91] P. Zhao, C. X. Lu, B. Wang, C. Chen, L. Xie, M. Wang, N. Trigoni, and A. Markham, "Heart rate sensing with a robot mounted mmwave radar," in *2020 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2020, pp. 2812–2818.

[92] Y. Zheng, Y. Zhou, J. Gao, X. Cao, H. Yang, S. Li, L. Xu, J. Lan, and L. Jidi, "Ultra-wideband polarization conversion metasurface and its application cases for antenna radiation enhancement and scattering suppression," *Scientific reports*, vol. 7, no. 1, pp. 1–12, 2017.

[93] Y. Zhu, Y. Zhu, B. Y. Zhao, and H. Zheng, "Reusing 60ghz radios for mobile radar imaging," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, 2015, pp. 103–116.

[94] Y. Zhu, Y. Zhu, Z. Zhang, B. Y. Zhao, and H. Zheng, "60ghz mobile imaging radar," in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, 2015, pp. 75–80.