Hydra: Attacking OFDM-base Communication System via Metasurfaces Generated Frequency Harmonics

Yangfan Zhang[†‡§], Yaxiong Xie[♯], Zhihao Hui[†♭], Hao Jia[†♮], Xiaojiang Chen[†‡♭⋄]

[†] Northwest University, China [♯]University at Buffalo SUNY, USA
[‡]Shaanxi International Joint Research Centre for the Battery-Free Internet of Things, China
[§]Xi'an Key Laboratory of Advanced Computing and System Security, China
[♭]Xi'an Advanced Battery-Free Sensing and Computing Technology International Science and Technology Cooperation Base, China [♮]Internet of Things Research Center, Northwest University, China
[†]{zhangyangfan1,zhihaoh,haoj}@stumail.nwu.edu.cn, [†]xjchen@nwu.edu.cn [♯]yaxiongx@buffalo.edu

ABSTRACT

While Reconfigurable Intelligent Surfaces (RIS) have been shown to enhance OFDM communication performance, this paper unveils a potential security concern arising from widespread RIS deployment. Malicious actors could exploit vulnerabilities to hijack or deploy rogue RIS, transforming them from communication boosters into attackers. We present a novel attack that disrupts the critical orthogonality property of OFDM subcarriers, severely degrading communication performance. This attack is achieved by manipulating the RIS to generate frequency-shifted reflections/harmonics of the original OFDM signal. We also propose algorithms to simultaneously beamform the multiple RIS-generated frequency-shifted reflections towards selected targets. Extensive experiments conducted in indoor, outdoor, 3D, and office settings demonstrate that Hydra can achieve a 90% throughput reduction in targeted attack scenarios and a 43% throughput reduction in indiscriminate attack scenarios. Furthermore, we validated the effectiveness of our attacks on both the 802.11 protocol and the 5G NR protocol.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**;

KEYWORDS

Reconfigurable intelligent surfaces, Wireless communication

ACM Reference Format:
Yangfan Zhang[†‡§], Yaxiong Xie[♯], Zhihao Hui[†♭], Hao Jia[†♮], Xiaojiang Chen[†‡♭⋄]. 2024. Hydra: Attacking OFDM-base Communication System via Metasurfaces Generated Frequency Harmonics. In *International Conference On Mobile Computing And Networking (ACM MobiCom '24), Nov. 18-22, 2024, Washington, D.C., USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3636534.3690670

⋄ Corresponding author.

ACM MobiCom'24, Nov. 18-22, 2024

ACM ISBN 979-8-4007-0489-5/24/09…$15.00
https://doi.org/10.1145/3636534.3690670

1 INTRODUCTION

Orthogonal frequency-division multiplexing (OFDM) is a dominant force in wireless communication. OFDM divides the bandwidth into multiple narrowband subcarriers, each less susceptible to fading caused by obstacles or multipath propagation, allowing for robust data transmission across various challenging environments [32]. As a result, OFDM has become the cornerstone of numerous wireless systems that permeate our daily lives, from cellular networks enabling seamless mobile connectivity to Wi-Fi providing internet access in our homes and offices [40].

On the other hand, reconfigurable intelligent surfaces (RIS) are emerging as a powerful tool for manipulating wireless signals. Composed of numerous, equally spaced, and programmable meta-atoms, RIS can dynamically alter its reflective properties, offering the ability to enhance signal strength, mitigate interference, and even focus signals towards specific users [6, 30]. This technology unlocks exciting possibilities for overcoming limitations in existing wireless systems and enabling entirely new functionalities.

The integration of RIS with OFDM-based communication system has emerged as a transformative force in wireless communication [33, 46, 47]. This powerful combination unlocks significant performance enhancements for established

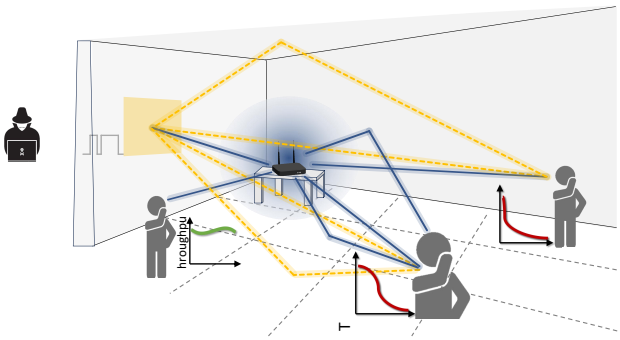


Figure 1: Malicious actors deploy or hijack the existing RIS to attack the communication.

systems like cellular and Wi-Fi and paves the way for the widespread deployment of RIS alongside OFDM systems.

However, a potential vulnerability could arise with widespread RIS deployment. Malicious actors might deploy rogue RIS or hijack existing ones to target communication within their coverage area, as shown in Figure 1. RIS-based attacks pose a unique threat due to their covert nature. By manipulating reflections of legitimate signals, these attacks require minimal effort from the attacker, making them difficult to detect. The very nature of the RIS—acting as a seemingly passive reflector—further complicates threat identification.

In this paper, we propose Hydra, a novel RIS-based attack that targets the inherent weaknesses of OFDM systems. The attack disrupts the critical orthogonality property of OFDM subcarriers, severely degrading communication performance. The core idea lies in manipulating the RIS to generate malicious reflections with slight frequency shifts compared to the original, legitimate OFDM signal. We theoretically and experimentally demonstrate that when these frequency-shifted replicas overlap with the original signal, the subcarrier orthogonality is destroyed, leading to significant Inter-Carrier Interference (ICI). This ICI renders the received signal unreadable by the receiver, resulting in an increased packet error rate (PER) and substantial throughput loss [26, 42].

To generate frequency-shifted reflections, we propose to implement *state transitions* within each meta-atom of the RIS. Each meta-atom typically possesses multiple states, each corresponding to a specific phase shift value, *e.g.*, a 2-bit meta-atom offers four phase shifts 0, $\pi/2$, π, or $3\pi/2$. Traditionally, all meta-atoms operate in a single state and only switch when the channel conditions change. We propose a paradigm shift by enabling each meta-atom to cycle through its states actively, forming a *state transition sequence*. We further demonstrate theoretically and experimentally that by carefully programming the parameters of the state transition sequence—including the duration, the number of states, and the state transitions themselves—we can not only *generate* frequency-shifted reflections but also *manipulate* the phase and amplitude of the resulting frequency-shifted reflections.

To successfully launch the attack, we also need to program the RIS to deliver the frequency-shifted reflections to the victim. We propose two types of attacks: *indiscriminate attacks* and *targeted attacks*. In indiscriminate attacks, any device within the RIS's coverage is susceptible. We achieve this by programming the RIS to distribute the reflected power as evenly as possible over a wide range of angles. Conversely, targeted attacks focus on specific victims. By leveraging the controllable amplitude and phase of the reflections, we propose an algorithm that can precisely beamform those RIS-generated frequency-shifted reflections towards the designated targets. This attack method significantly reduces interference with nearby devices while enhancing the attack's effectiveness and stealth.

We implement Hydra on a RIS consisting of 16×16 meta-atoms and spanning an area of $0.35 \times 0.35 m^2$. Its compact size enables discreet integration into everyday environments like walls, furniture, and billboards, facilitating inconspicuous attacks. The effectiveness and principles of Hydra were validated through extensive theoretical analysis and simulations. We demonstrated its capability to conduct both indiscriminate and targeted attacks on OFDM signals via practical experiments. Our research sheds light on the emerging security vulnerabilities that arise with the wide deployment of RIS. Extensive experiments conducted in indoor, outdoor, 3D, and office settings demonstrate that Hydra can achieve a 90% throughput reduction in targeted attack scenarios and a 43% throughput reduction in indiscriminate attack scenarios. Furthermore, we validated the effectiveness of our attacks on both the 802.11 protocol and the 5G NR protocol.

To our knowledge, Hydra is the first RIS-based attack system on commercial OFDM systems by introducing a comprehensive theoretical analysis and detailed attack strategies. Hydra implements the attack by manipulating meta-atoms' state transitions to generate small, hard-to-detect kHz-level frequency shifts, thereby disrupting subcarriers orthogonality. Our methods can deal with various real-world attack scenarios, including both indiscriminate and targeted attacks. Finally, we implement the Hydra hardware and validate its effectiveness in a wide range of practical scenarios.

2 RELATED WORK

Jamming Attack Based on Endpoints. Due to the broadcast and superposition nature of wireless channels, jamming attacks can deliberately damage wireless communication networks. The jammer attack based on the endpoints can be divided into three categories: brute suppression attack, channel-aware attack, and off-tone attack. For the brute suppression attack, the jammer can destroy packet reception by introducing high-power interference [19]. Or, it can

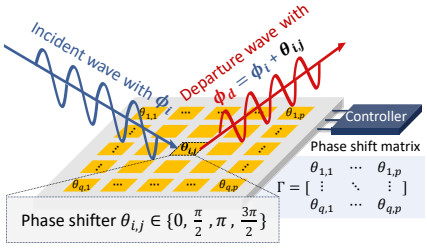


Figure 2: The basic principle of RIS.

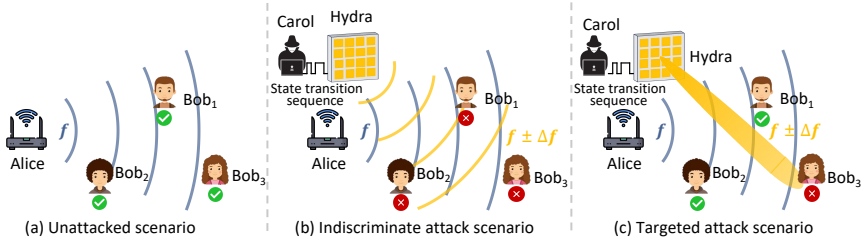


Figure 3: Threat model under different attack scenarios.

prevent the legitimate receiver from accessing the channel by continuously occupying [34]. While these methods can achieve good attack performance, they are low-efficient attacks [7, 37, 39]. Channel-aware jamming attack is also known as reactive jamming attack, in which a malicious jammer sends an interfering radio signal when it detects legitimate packets transmitted over the air [9, 14, 24]. However, these methods require detailed prior network knowledge and channel information, making them challenging to implement in real wireless networks. Off-tone attack aims to destroy the orthogonality of OFDM signals by injecting frequency offset signals [25, 38, 51]. Although the attack principle is similar to Hydra, these systems are required to continually identify and track frequently changing communication channels. In addition, the presence of malicious signals reduces the stealthiness of the attack, making it more detectable [52, 53]. In contrast, Hydra can overcome the abovementioned issues by achieving attack during the legitimate signal propagation. Hydra does not require active signal transmission and solely relies on the energy of reflected legitimate signals for executing attacks, significantly enhancing the stealth and efficiency of the operation. Hydra can work well without depending on the prior channel information or frame knowledge.

RIS-aided Wireless Communication. RIS equipped with electronic components [8, 20–22, 44, 45, 48, 49] can manipulate the phase of impinging electromagnetic waves and beamform or resteer the signals toward an intended direction, to extend the network coverage [12, 13, 16, 17]. For instance, RFocus [5] includes thousands of RF switches to control whether Wi-Fi signals are reflected or passed through to realize beamforming. These methods focus on leveraging RIS to enhance the wireless radio channel quality in terms of signal-to-noise ratio (SNR) [23] or spatial diversity [15] through redirection and reshaping of RF signals. However, the RIS as a novel attacking tool for malicious purposes has yet to receive attention. In contrast, Hydra reveals and discusses the serious threat of RIS regulation in radio space.

RIS-based Over-the-air Attack. Unlike traditional methods where leveraging RIS to enhance signal SNR, a few state-of-the-art works reveal the threat of programming radio environment. One approach leverages RIS to generate frequency deviation paths for eavesdropping [11], while another disrupts wireless communication. Specifically, Lyu et al. [31] employs RIS to minimize the signal power received by the attack target. RIS-Jamming [27] utilizes RIS to affect rapid changes in the channel and reduce the signal-to-noise ratio of legitimate links. However, these systems require RIS configuration based on obtaining the channel state information, which can hardly be implemented in reality. Staat et al. [41] demonstrated that by rapidly alternating between configurations of RIS, it induces swift changes in the wireless channel, subsequently impacting the channel equalization process of the receiver. However, the attack strategy can only achieve the "one-size-fits-all", decreasing the throughput for all potential receivers within the manipulation region, rather than recognizing whether attack targets or not. In contrast, Hydra utilizes harmonics to generate frequency shifts as a breakthrough to destroy the orthogonality of OFDM signals. Hydra bypasses the requirement for channel information and offers various attack strategies for real-life attack scenarios, including indiscriminate and targeted attacks.

3 PRIMER

OFDM and Subcarrier Orthogonality. Orthogonal frequency division multiplexing (OFDM) leverages orthogonality to divide a wideband channel into multiple closely spaced subcarriers. The time domain subcarrier signal $x(t)$ is:

$$x(t) = \sum_{k=0}^{N-1} a_k e^{j2\pi k f_k t} \tag{1}$$

where a_k is the data symbol on the k^{th} subcarrier, N is the number of subcarriers, and f_k is the frequency of the k^{th} subcarrier [35]. After going through the wireless channel, the received signal $y(t)$ becomes:

$$y(t) = h(t) * x(t) + z(t) \tag{2}$$

where $h(t)$ is the channel impulse response and $z(t)$ is the Gaussian noise. The receiver demodulates the transmitted data symbol by performing a FFT on the received signal $y(t)$:

$$Y(f_k) = H(f_k) \cdot a_k + Z \tag{3}$$

where $H(f_k)$ represents the channel frequency response of the k-th subcarrier. As indicated in Eqn 3, due to the orthogonality, all data symbols modulated on each subcarrier

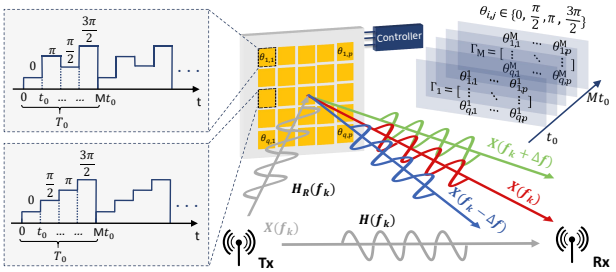


Figure 4: RIS induces frequency shifts within the signal. Each meta-atom performs a sequence of state transitions.

can be cleanly recovered, even though the spectrum spacing between subcarriers is small. Therefore, the receiver could easily demodulate the a_k, by simply estimating $H(f_k)$.

Reconfigurable Intelligent Surface (RIS). A RIS is composed of multiple identical *meta-atoms*, as shown in Figure 2. Upon the signal's arrival at a meta-atom, it introduces a phase shift θ before reflecting the signal. Practical meta-atoms are realized using microelectronic components like PIN diodes or switches, often providing a limited set of discrete phase shift states. In general, an N-bit meta-atom provides 2^N states. For example, for a 2-bit RIS, each meta-atom effectively functions as a 2-bit phase shifter with four possible phase shifts. During operation, each meta-atom *maintains its state throughout the wireless transmission period* and only changes its state when there are fluctuations in the channel conditions.

The *RIS controller*, typically a microcontroller or FPGA, serves as the brain of the RIS, dynamically manipulating the incident wave. It calculates the optimal phase shifts θ for each meta-atom, stored in a phase shift matrix θ:

$$\Gamma = \begin{bmatrix} \theta_{1,1} & \cdots & \theta_{1,p} \\ \vdots & \ddots & \vdots \\ \theta_{q,1} & \cdots & \theta_{q,p} \end{bmatrix} \tag{4}$$

This matrix, $\Gamma \in \mathbb{R}^{p \times q}$, dictates how the RIS, with its p rows and q columns of meta-atoms, alters the incoming wavefront. By strategically adjusting Γ, the controller instructs the RIS to perform specific signal manipulations, such as beamforming.

4 ATTACK DESIGN

4.1 Threat Model

We consider a generic wireless link between Alice and Bob, as shown in Figure 3. By default, we focus on the forward link, i.e., Alice is the default transmitter. Alice can be a base station, Wi-Fi router, surveillance camera, etc. Bob is the victim system that can be the commercial IoT device, sever, or smart traffic indicator, among others, and can be in either a stationary or mobile state. Alice and Bob can use arbitrary types of antennas, i.e., omni-directional or directional antennas. There are n desired victim systems (i.e., Bob_1, ..., Bob_n) who are transmitting information with Alice. The wireless communication between Alice and Bob can be SISO or MIMO links. Carol is the attacker who attempts to utilize the RIS to disrupt Alice's transmission. The Hydra RIS is placed near Alice, and the RIS does not require the line-of-sight of Bob and Alice, which means Carol can achieve an imperceptibility attack behind the wall. There is no synchronization or other run-time coordination between the Hydra RIS and Alice. In other words, the RIS configures meta-atoms independent of the packet/symbol timing of the transmitter.

4.2 Attack Model

OFDM relies on subcarrier orthogonality for optimal performance, rendering it susceptible to frequency disturbances. Our proposed attack referred to as Hydra, harnesses RIS to generate one or multiple frequency-shifted versions of the original OFDM signal, as depicted in Figure 4. Upon reception, the victim, exemplified by Bob, encounters a superimposition of the original OFDM signal and frequency-shifted reflections from the RIS. Such superimposed signals destroy subcarrier orthogonality, leading to inter-carrier interference (ICI) and subsequent decoding failures.

Hydra focuses on two types of attack scenarios: *indiscriminate attacks* and *targeted attacks*. In indiscriminate attacks, Hydra aims at disrupting all receivers within the propagation environment, causing interference in communication between any pair of transceivers. In this operational mode, Hydra autonomously operates without prior knowledge of the number of devices or their spatial distribution within the environment. Additionally, it operates independently of feedback from devices to adjust its attacks, thereby eliminating the necessity for specific information about the target system or external conditions beforehand.

Conversely, targeted attacks involve selectively disrupting specific receivers within the environment, such as Bob_1 in Figure 3, while maintaining communication performance for non-targeted receivers like Bob_2 and Bob_3. To execute targeted attacks, Hydra relies on feedback from devices to fine-tune its attack parameters, including beamforming directions. Importantly, Hydra obtains this feedback without necessitating cooperation from the victim or receivers within the system. Instead, Hydra equips the RIS with a network card supporting monitor mode. Leveraging this configuration, it captures throughput quality indicators of designated users and utilizes beam scanning techniques to precisely identify the intended victim.

4.3 Theoretical Analysis

In this section, we present the theoretical analysis of how the frequency-shifted signal reflections destroy the destroy subcarrier orthogonality, leading to inter-carrier interference (ICI) and subsequent decoding failures.

Modeling the Malicious Frequency-shifted Signal. The signal, after being reflected by the RIS, is modeled as a legitimate signal with a frequency offset:

$$x_s(t) = x(t)e^{j2\pi\Delta f t} \tag{5}$$

where Δf is the frequency offset.

Superposition of Original and Malicious Signal. The received superposed signal, including both the original OFDM signal and the frequency-shifted reflection is given as:

$$y(t) = h(t) * x(t) + h_R(t) * x_s(t) + z(t) \tag{6}$$

where $h_R(t)$ represents the channel that the frequency-shifted reflection experiences, as shown in Figure 4.

Combing Eqn. 6 and Eqn. 3, we derive the received frequency domain data symbol $Y(f_k)$ on the k-th subcarrier [43]:

$$\begin{aligned} Y(f_k) =& H(f_k) \cdot a_k + H_R(f_k)\text{sinc}(\varepsilon) \cdot a_k \\ &+ H(f_k) \sum_{m=0,m\neq k}^{N-1} \text{sinc}(m-k+\varepsilon) \cdot a_m + Z(f_k) \end{aligned} \tag{7}$$

where $\varepsilon = \frac{\Delta f}{f_{sc}}$ is the normalized carrier frequency offset, and f_{sc} is subcarrier spacing. Ideally, without interference and ICI, the received data symbol should preserve orthogonality:

$$Y(f_k) = H(f_k) \cdot a_k \tag{8}$$

so that we can demodulate the data symbol a_k by simply estimating the channel $H(f_k)$. However, according to Eqn. 7, the data symbol contains two extra components. Specifically, the first component $P_1(f_k)$:

$$P_1(f_k) = H_R(f_k)\text{sinc}(\varepsilon) \cdot a_k \tag{9}$$

represents the interference of the frequency-shifted reflection. And the second component $P_2(f_k)$:

$$P_2(f_k) = H(f_k) \sum_{m=0,m\neq k}^{N-1} \text{sinc}((m-k+\varepsilon)) \cdot a_m \tag{10}$$

characterizes the ICI from m-th subcarriers where $m \neq k$. According to Eqn. 7, it is evident that injecting frequency-shifted malicious signal reflections through RIS destroys orthogonality and thus introduces significant interference.

4.4 Experimental Verification

In this section, we conduct simulations to verify the effectiveness and implementation requirements of the attack strategy.

4.4.1 Simulation Setup. Our simulations are conducted using the MATLAB WLAN Toolbox [2]. The foundational simulation parameters of the Wi-Fi system are set to the IEEE 802.11n wireless standard with HT Mixed mode, employing a 40 MHz bandwidth, 2×2 MIMO channels, 30 SNR, 7 MCS, and Channel Model-D. To assess the impact of the frequency-shifted malicious signal, we observe the packet error rate (PER) as a key metric for evaluating communication quality.

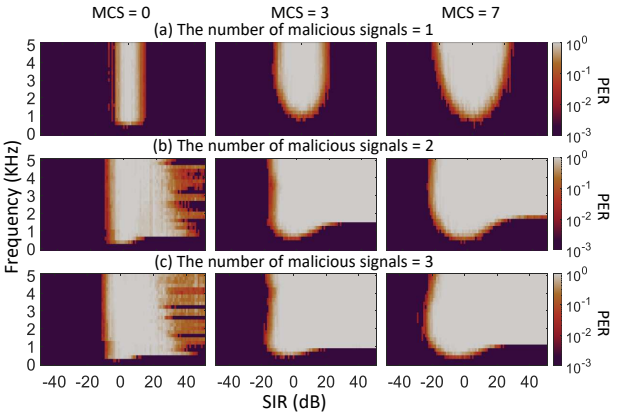


Figure 5: The PER when decoding the OFDM signal superposed with frequency-shifted copies.

4.4.2 Simulation Results. Figure 5 illustrates the simulated results. Each row shows the results under different numbers of malicious signals, with combinations of signals having one, two, and three times the frequency shift, while maintaining equal energy. Each column corresponds to the legitimate signal using different Modulation and Coding Schemes (MCS), with examples including MCS levels 0, 3, and 7. The horizontal axis of each subplot denotes the signal-to-interference ratio (SIR), indicating the power ratio between the original legitimate Wi-Fi signal and the frequency-shifted malicious signal. Zero SIR signifies equal power, positive SIR values denote a stronger malicious signal, and negative SIR values indicate a stronger legitimate signal. The vertical axis of each subplot showcases the incremental frequency shifts of the malicious signal, starting from zero frequency shifts. The color gradient represents the calculated PER.

Impact of SIR. We take the results in Figure 5(a) *right*, as an example to illustrate the impact of SIR. We observe that when the SIR equals zero, indicating equal power between the original and malicious signals, even small frequency shifts (*e.g.*, 900 Hz) in the malicious signal can significantly degrade communication performance, resulting in a 100% PER. As the SIR deviates from zero, the malicious signal requires larger frequency shifts compared to the original signal to achieve a 100% PER. Furthermore, we note that as the SIR reaches a certain threshold where one signal, either the malicious or the original, dominates the other, the PER decreases to zero due to the capture effect[1] The receiver effectively deciphers correct data from either the original or malicious signal since they serve as frequency-shifted mirrors of each other, thus carrying identical data payloads.

Impact of Frequency Shifts. We observe larger frequency shifts correspond to an increased likelihood of communication being attacked, resulting in a 100% PER. However,

[1]The capture effect occurs when one signal significantly outweighs the other, leading the decoder to decode the stronger signal.

the ultimate PER is profoundly influenced by the SIR value. Once the SIR surpasses the threshold necessary to induce the capture effect, the PER stabilizes at 0%, irrespective of the magnitude of frequency shifts.

Impact of MCS. Our findings indicate that attacking OFDM signals with lower MCS is more challenging due to the reduced attack success area. Low-order modulation schemes exhibit greater tolerance for signal degradation, so in high packet loss environments, devices typically reduce the MCS to maintain reliable data transmission [18, 36].

Impact of Number of Malicious Signals. Increasing the number of malicious frequency-shifted signals intensifies communication disruption. When exceeding one signal, even with a large positive SIR (malicious dominance), interference among these signals themselves eliminates the capture effect, leading to 100% PER at significant frequency shifts. Additionally, more malicious signals decrease the minimum effective frequency shift for inducing packet errors and broaden the SIR range susceptible to errors. This empowers attacks with weaker signals and smaller frequency shifts.

5 RIS-BASED ATTACK IMPLEMENTATION

In this section, we explain how to utilize RIS to generate effective frequency-shifted attack signals, including theoretical analysis (Sec 5.1), parameter selection (Sec 5.2), and attack strategies tailored for different scenarios (Sec 5.3).

5.1 Generating Frequency-Shifted Signal

In this section, we introduce the principle we proposed to generate frequency-shifted signal reflections using RIS.

5.1.1 Solution: State Transitions. We propose to configure the meta-atom to perform a sequence of deliberate state transitions aimed at inducing frequency shifts within the signal. As shown in Figure 4, our approach involves setting the meta-atom to remain in a specific state for a duration of t_0 before transitioning to another state. The state transitions follow a predefined sequence that consists of M shifts, with an aggregate sequence duration of T_0=$M \cdot t_0$. We repeat the predefined state transition sequence in time.

Signal Model for RIS-Reflected Signal. We model the phase shifts the meta-atom introduces to the signal during each period of T_0 as:

$$\Theta(t) = \sum_{m=0}^{M-1} e^{j\theta_m} g(t - mt_0), 0 < t < T_0 \tag{11}$$

where θ_m represents the phase shifts the meta-atom introduces in the m-th state interval. The signal $g(t)$ is a pulse signal that maintains high for one state interval t_0:

$$g(t) = \begin{cases} 1, & 0 \le t \le t_0 \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

Given the incident wireless signal $S_i(t)$, we model the signal reflected by each meta-atom $S_r(t)$ as:

$$S_r(t) = S_i(t) \cdot \Theta(t) \tag{13}$$

We now conduct a detailed analysis of the reflected signal.

Frequency Analysis of Reflected Signal. To examine the frequency characteristics of the signal reflected by the meta-atom, we perform a Fourier series expansion on Eqn. 11 and then conduct a frequency domain transformation of the signal $S_r(t)$. This transformation yields the following [50]:

$$S_r(f) = \sum_{k=-\infty}^{+\infty} \alpha_k S_i(f - kf_\Delta) \tag{14}$$

where f_Δ=$1/T_0$ is a constant frequency derived from T_0, and k represents the k-th frequency component which we also denote as the harmonic order. In Eqn. 14, it becomes evident that the reflected signal comprises an infinite series of frequency components. Each component is a weakened rendition of the incident signal $S_i(t)$ with a frequency shift kf_0 and an associated complex attenuation factor of α_k.

Takeaway. This analysis reveals that, by introducing state transitions to the meta-atoms, we successfully generate frequency shifted reflections of the original signal using RIS.

5.2 Programming the Reflections

In this section, we introduce the algorithm for programming the frequency-shifted reflection, involving adjustment of state transition sequence parameters: the time duration of the sequence T_0, the total number of states denoted by M, and the precise phase shifts θ_m at each stage of the sequence.

5.2.1 Programming The Frequency Shift. The value of the frequency shift f_Δ, between two harmonics depends on the time duration T_0 of the entire transition sequence:

$$f_\Delta = 1/T_0 \tag{15}$$

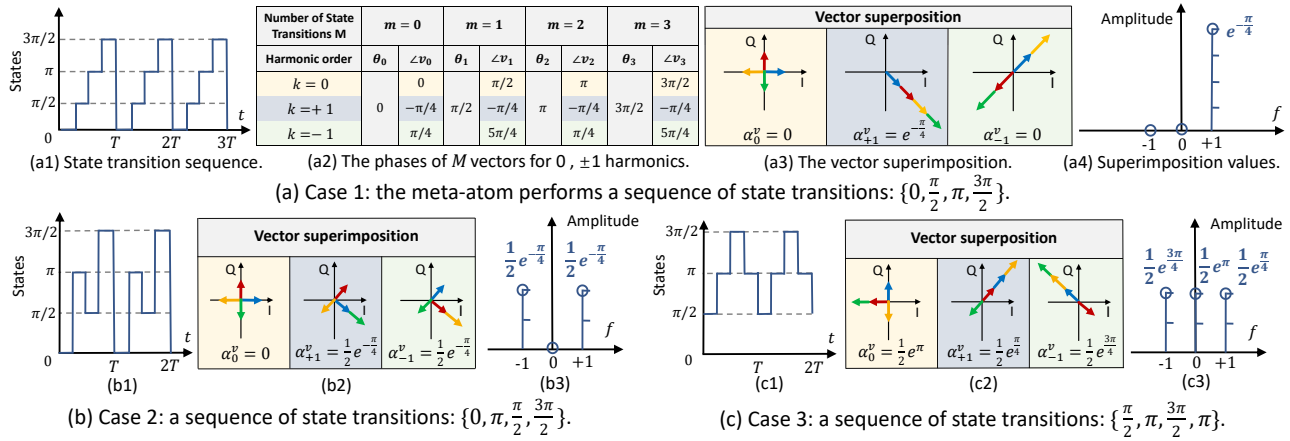
as shown in Eqn. 14. Consequently, we can regulate the frequency of the generated harmonics by adjusting the duration of the transition sequence.

5.2.2 Programming the Complex Attenuation Factor. The complex attenuation factor α_k of the k-th frequency component is calculated as:

$$\alpha_k = sinc(\frac{\pi k}{M}) \cdot \frac{1}{M} \cdot \sum_{m=0}^{M-1} e^{j(\theta_m - \frac{k\pi(2m+1)}{M})} \tag{16}$$

We see from Eqn. 16 that, the complex factor α_k can be divided into two components: the α_k^s, represented as:

$$\alpha_k^s = sinc(\pi k/M) \tag{17}$$



Number of State Transitions M	$m=0$		$m=1$		$m=2$		$m=3$	
Harmonic order	θ_0	$\angle v_0$	θ_1	$\angle v_1$	θ_2	$\angle v_2$	θ_3	$\angle v_3$
$k=0$	0	0	$\pi/2$	$\pi/2$	π	π	$3\pi/2$	$3\pi/2$
$k=+1$		$-\pi/4$		$-\pi/4$		$-\pi/4$		$-\pi/4$
$k=-1$		$\pi/4$		$5\pi/4$		$\pi/4$		$5\pi/4$

Figure 6: Cases of frequency-shifted signal generation.

is a scalar component that only affects the amplitude; and the vector component α_k^v:

$$\alpha_k^v = \frac{1}{M}\sum_{m=0}^{M-1} v_m = \frac{1}{M}\sum_{m=0}^{M-1} e^{j(\theta_m - \frac{k\pi(2m+1)}{M})} \tag{18}$$

is the superposition of M unit vectors and thus affects both the final amplitude and phase of the complex factor α_k.

Unit Vector Superposition. The superposition of M unit vectors highly depend on the phase of each vector:

$$\angle v_m = \theta_m - k\pi(2m+1)/M \tag{19}$$

We use the example in Figure 6 to illustrate how the state transition sequence affects the vector superposition. In the first example, we set $M=4$ and configure the meta-atom to iterate all four states, resulting in the state transition sequence in Figure 6(a1). The phases of all M vectors for $k=0$ and ±1 harmonics are listed in Figure 6(a2), while the vector superposition results are illustrated in Figure 6(a3), and the final superposition values α_k^v of M vectors are depicted in Figure 6(a4). Combining Figures 6(a3) and 6(a4), we observe that under such a configuration, the superposition of M vectors is zero for the $k=0$ and -1 harmonics, as these vectors cancel each other out. Consequently, the RIS cannot generate these two harmonics. However, the α_k^v for $k=1$ harmonics is non-zero. Thus, the RIS is capable of generating such a frequency-shifted reflection, with the phase reflection of $-\frac{\pi}{4}$, as α_k^s is a scalar and therefore has no impact on the phase.

We also demonstrate the superposition results with the state transition sequence shown in Figure 6(b1). Such a sequence iterates all four states, similar to the sequence in Figure 6(a1) but in a different order. Combining the superposition results in Figure 6(b2) and the value of α_k^s for $k=0$ and ±1 in Figure 6(b3), we observe that the RIS generates two harmonics, namely $k=-1$ and $k=1$, each with phase $-\frac{\pi}{4}$ and $-\frac{\pi}{4}$, respectively. The $k=0$ harmonic remains inactive. It is noteworthy that when the state transition sequence iterates only three out of the four possible states that each meta-atom has, as shown in Figure 6(c), the RIS successfully generates the $k=0$ harmonics.

Takeaway. By controlling the total number of states M in the state transition sequence and the exact state θ_m within each state of the sequence, we can program the number of harmonics the RIS generates and the phase of each harmonic.

Phase and Amplitude Controllability. To demonstrate the controllability of phase and amplitude by adjusting the vector superposition, we exhaustively iterate all possible state transition sequences for $M=4$ (yielding 256 sequences), $M=6$ (yielding 4096 sequences), and $M=8$ (resulting in 65536 possible sequences). The superposition results α_v^k for $k=1$ harmonics are plotted in Figure 7. We observe that the number of states within a transition sequence increases, finer control over both phase and amplitude is achieved. However, larger values of M also lead to a larger search space for possible sequences. To strike a balance between search space and controllability, we opt to fix $M=6$ in our design.

Scalar Component α_k^s. The scalar component α_k^s solely affects the amplitude, as indicated by Eqn. 17. We plot the value of α_k^s under various M and harmonic order k in Figure 8. We can observe that α_k^s effectively works as a scalar energy attenuation coefficient. The further away the harmonic order k from zero, the larger the attenuation. For example, as shown in Figure 8(b), we can clearly see that when the order of harmonics exceeds ±4, the attenuation is reduced by more than 59%. The inappreciable energy significantly reduces their impact. Therefore, in Hydra, we overlook the attack performance of higher-order harmonics and instead focus on the scalar component α_k^s of the lower-order harmonics.

Overall Amplitude. The overall amplitude depends on both the α_k^s and the result of the vector superposition: $|\alpha_k| =$

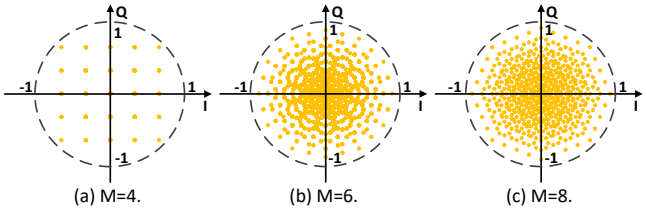


Figure 7: The vector superposition results α_k^v for ±1 harmonics obtained by iterating all transition sequences.

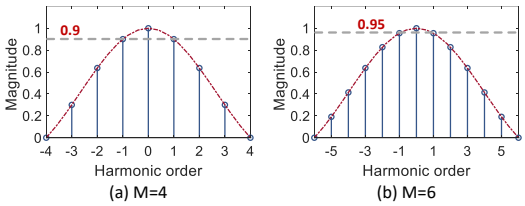


Figure 8: Influence of state account M and harmonic order k on energy attenuation coefficient $\alpha_{\mathrm{k}}^{\mathrm{s}}$.

$\alpha_k^s \cdot |\alpha_k^v|$. We emphasize that the vector superposition primarily governs the amplitude since the amplitude of the superposition $|\alpha_{\mathrm{k}}^{\mathrm{v}}|$ may approach zero when the vectors cancel each other out. In contrast, $\alpha_{\mathrm{k}}^{\mathrm{s}}$ only attenuates the amplitude.

5.3 Programming RIS for Attack

In this section, we introduce our algorithm to program the RIS for attacking wireless communication.

5.3.1 Indiscriminate attack. In indiscriminate attacks, we configure the RIS to generate diffuse reflection. This means reflecting incoming signals, regardless of their incident angle, towards a wide range of outgoing directions. More specifically, we aim for the RIS to generate multiple frequency-shifted versions of the signal upon reflection and distribute all these shifted signals across a broad angular range within the targeted attack zone. Consequently, any receiver within the attack zone will receive multiple reflections from the RIS, each with a distinct frequency shift, and thus gets attacked.

Problem Definition. To realize an indiscriminate attack, we must identify the optimal RIS configuration—the specific sequence of phase shifts for each meta-atom—that effectively generates diffuse reflection. Fortunately, this search only needs to be conducted once, offline. We can then fix the configuration for the RIS throughout the actual attack. However, a brute-force search algorithm is impractical due to the vast search space. For instance, given the fixed M = 6, there are 4096 potential state transition sequences for each of the 256 meta-atoms. This translates to a search space of 4096^{256}, which is computationally infeasible.

To reduce the search space, we propose a strategy to eliminate state transition sequences that generate weak frequency-shifted signals. We focus on finding sequences that produce strong first-order harmonics (k = 1 and k = −1). Specifically, we only retain sequences where the sum of the absolute amplitudes of these harmonics, $|\alpha_1| + |\alpha_1|$, exceeds a predefined threshold. Figure 9 illustrates the reduction in the number of candidate sequences under different threshold values. Based on this analysis, we set the threshold to 1 and only search with the selected sequences.

Figure 10 presents the optimal configuration we identified, where each of the 4096 possible transition sequences is assigned a unique color for easy visualization. We plot

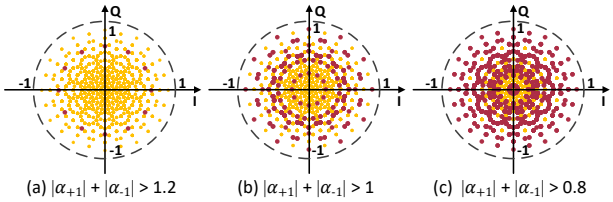


Figure 9: Candidate sequence count at different thresholds.

the theoretical and measured power distribution of the first-order harmonics, given the incident signal from 0° elevation and 30° azimuth in Figure 10(a1) and (a2), respectively. As a comparison, we also plot the results for the signal from 30° elevation and 30° azimuth in Figure 10(b). We see that both of the first-order harmonics indeed spread out in a wide range regardless of the angle of the incident signal.

5.3.2 Targeted attack. Unlike indiscriminate attacks, targeted attacks require the RIS to focus (beamform) the signal towards a specific victim. While conventional RIS beamforming is a well-established area [17, 28], our challenge here is to simultaneously beamform multiple frequency-shifted signals toward targeted directions. To address this, our algorithm adopts a two-step approach:

- **Individual Harmonic Beamforming.** We first solve the beamforming problem for each harmonic ($k = \pm 1$) independently. This step determines the optimal phase shifts each meta-atom should introduce to achieve the desired beamforming pattern for each harmonic.
- **State Transition Sequence Matching.** We search for the state transition sequence that realizes the phase shifts $\angle\alpha_k^v$ for each harmonic ($k = \pm 1$) that matches the individual harmonic beamforming solutions. We note that, during this process, we also eliminate those sequences that introduce significant attenuation to the harmonics.

This approach allows us to efficiently achieve targeted manipulation of multiple frequency-shifted signals.

Single-Target and Multi-Target Attack. We use the two examples in Figure 11 to illustrate how our beamforming algorithm works for single-target and multi-target attacks.

In Figure 11(a), we beamform two harmonics in the same direction, *i.e.* the direction of the single target. Given the phase ϕ_{i} of the incident signal, solving the beamforming problem derives the departure signal phase $\phi_{\mathrm{d}}^{\mathrm{k}}$ for the k-th

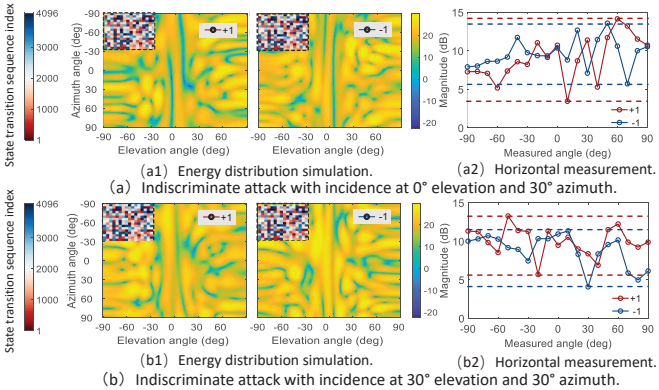


Figure 10: RIS configuration and the power distribution of the frequency-shift signals under indiscriminate attacks.

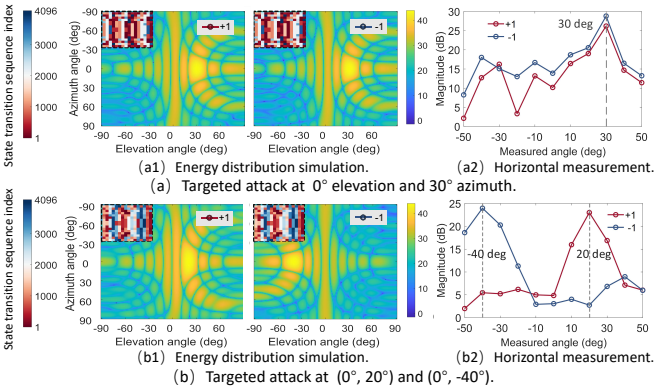


Figure 11: RIS configuration and the power distribution of the frequency-shift signals under targeted attack scenario.

harmonic, and thus the desired phase shifts $\gamma_k = \phi_d^k - \phi_i$ that the meta-atom should introduce. Since we target the same direction, two harmonics have the same desired phase shifts, *i.e.*, $\gamma_{+1} = \gamma_{-1}$. Figure 11(a1) shows the state sequences that achieve the desired phase shifts. Similarly, Figures 11(a1) and (a2) plot the theoretical and measured power distribution when the RIS implements this solution. The results confirm that both harmonics are indeed beamformed towards the desired direction. In Figure 11(b), we beamform two harmonics in two different directions. The algorithm works similarly to the single-target scenario, except that the desired phase shifts differ for the two harmonics, i.e., $\gamma_{+1} \neq \gamma_{-1}$. The theoretical and measured power distributions in Figures 11(b1) and (b2) further demonstrate that the two harmonics are indeed beamformed in different directions. In addition, we can also use the same method to precisely guide the beam direction of the ±2 and ±3 harmonics, thereby reducing their interference in non-target directions, focusing more effectively in the target direction, or adding new attack directions.

Adapting the Beamforming Directions. Hydra leverages the interaction between users and access points (APs) to address the challenges of adapting the beamforming directions given unknown user locations and moving targets. Specifically, users periodically send Block Acknowledgment (BA) frames to the AP. BA is a mechanism in the Wi-Fi protocol for confirming the successful reception of a sequence of data packets, reflecting data loss situations. With the target user's MAC address known, we can install Wi-Fi receivers on RIS to intercept these BA frames. Using the network protocol analysis tool, we filter packets containing the specific MAC address and statistically analyze the Bitmap within the BA frames. The Bitmap marks unaccepted and accepted packet sequences with "0" and "1," respectively. Calculating the percentage of zeros allows us to ascertain the user's packet loss rate. Therefore, by adjusting the direction of the harmonic beams, Hydra can know the direction of the victim by calculating the packet loss rate. To expedite the search process, we employ +1 and -1 order harmonics for beam scanning across various directions and initiate the search with a larger step size, like 20°, for a rough directional estimate. Subsequently, we refine our approach by adopting smaller step sizes, such as 5°, to precisely adjust and pinpoint the results. Additionally, the beam codebook of the RIS is pre-stored in the controller and can be directly accessed.

6 IMPLEMENTATION

Hydra uses two prototype RISs respectively for 5 GHz and 3.5 GHz to verify system performance under Wi-Fi and 5G NR protocols, as shown in Figure 12. Each meta-atom on the RIS uses two SMP1340-040LF PIN diodes as tunable electronic elements. Activate or deactivate the PIN diodes by using different DC voltages (5 V or 0 V), each meta-atom can provide four phase shifts, i.e., 0 ("00" state), $\pi/2$ ("01" state), π ("10" state), and $3\pi/2$ ("11" state). To independently control each meta-atom, we employ a XILINX XC7K325T FPGA and 64 SN74LV595 shift registers to provide a bias voltage to PIN diodes. FPGA can be powered by a laptop's USB port, which outputs DC 5V with a current not exceeding 500mA [4]. Note that the power can be easily replaced by batteries, solar energy, or wireless charging technologies [10, 29]. Specifically, we divide the RIS into two areas, each segmented into 8 channels. Each channel uses four sequentially connected SN74LV595 shift registers to transmit a 32-bit data flow, controlling 32 PIN diodes (16 meta-atoms).

The circuit design enables the controller to independently manipulate the state of each meta-atom. To prevent various delays, the state switching of all meta-atoms can be synchronized using a common clock signal. For example, a frequency shift of 5 kHz can be generated by leveraging RIS, which can switch six states within 0.2 ms, corresponding to a state switching frequency of 30 kHz. This hardware requirement can be easily satisfied using low-cost commercial devices equipped with MHz-range clock oscillators. The power consumption of Hydra at the mW level since the RIS

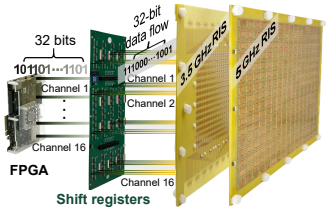
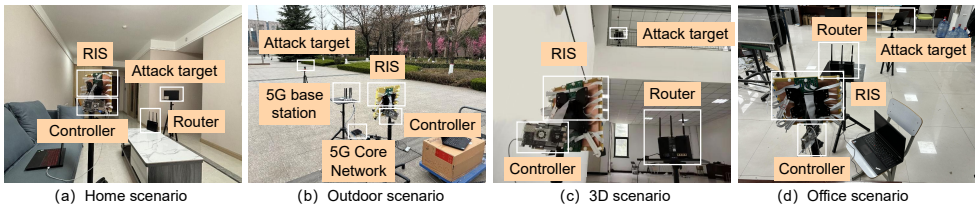


Figure 12: RIS prototypes.



(a) Home scenario (b) Outdoor scenario (c) 3D scenario (d) Office scenario

Figure 13: Experimental scenarios.

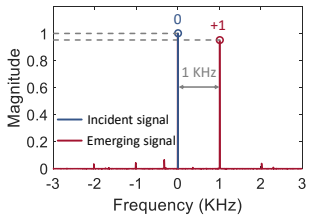


Figure 14: Spectrum of state transition sequence.

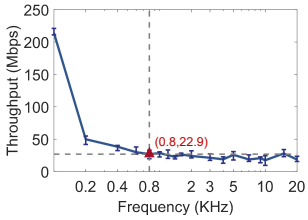


Figure 15: Results at different frequency shifts.

only reflects rather than receives and regenerates existing signals. As shown in Figure 13, we have conducted experimental verification in multiple scenarios such as furniture, outdoor, 3D, and office.

7 EVALUATION

Experimental setup. For controlled experiments, the transmitter (Tx) is a commercial WLAN router Asus RT-AC68U with 2 antennas (MIMO channel count of 2). The router operates in 802.11n/ac mixed at a frequency band of 5.825 GHz with a 40MHz bandwidth. The receiver is a laptop with an Intel Wireless-AC 8265 network card and 2 antenna (MIMO channel count of 2). We use the iperf3 toolbox to collect throughput measurements. In the default setup, the Tx is deployed in the normal direction of the RIS, and the Tx-RIS distance stays at 1m. The Rx moves along a semicircle (5 m radius) from $-90°$ to $90°$ with a step of $10°$, while the Tx stays in the center. All devices are held up at a height of 1 m. Hydra uses 6 state transitions during a time-variant period of 0.2 ms to generate ± 1 order harmonic with a frequency shift of 5 kHz. We use throughput and throughput decrease percentage (TDP) as metrics to evaluate the effectiveness of the Hydra attack on the victim communication systems.

7.1 Benchmark Performance

Harmonic generation. To evaluate the effectiveness of harmonic generation, we use a USRP N210 software-defined radio with a UBX-40 daughterboard as the radio transceiver, operating at a default center frequency of 5.25 GHz. Hydra uses 4 state transitions (i., 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$) during a time-variant period of 1 ms to generate +1 order harmonic with 1 KHz frequency shift. Figure 14 shows the frequency spectrum. We can clearly see that the +1 order harmonic is efficiently generated when rapidly state transition sequences, compared with the without RIS. The results demonstrated the effectiveness of Hydra principle.

Impact on frequency shift. We measure the throughput to verify how frequency shift affects the attack. From Figure 15, we can see that as the frequency shift increases, the throughput decreases. When the frequency shift is 0.8 KHz, the throughput drops from 214 Mbps to 22.9 Mbps. After that, throughput remains relatively stable even further increasing the frequency shift. This is because the attack has reached optimal effectiveness when the frequency shift is large enough (based on Sec. 4.4.1). This resilience is due to the adaptability of current communication protocols, which can automatically downgrade the MCS to a lower, more robust scheme. Overall, Hydra can effectively leverage frequency shift to degrade signal link throughput for attacks.

Effectiveness of different attack strategies. For single-target attacks, the victim receiver is located at $30°$. The RIS employs ± 1 harmonic beamforming simultaneously towards the receiver to disrupt communications. Figure 16(a) shows a dramatic drop of about 192 Mbps, indicating a significant 90% reduction compared to the baseline scenario of normal communication (the average throughput of 214 Mbps).

For multi-target attacks, Hydra uses the +1 and -1 order harmonic beamforming towards the $20°$ and $-40°$ respectively, corresponding to the azimuth angle of desired victims. Figure 16(b) shows the attack results. When compared to the baseline, there is a noticeable reduction in throughput of about 161 Mbps at $20°$ (75% reduction) and about 170 Mbps at $-40°$ (79% reduction). The similarity in amplitude between the ± 1 order harmonics leads to comparable reductions in throughput in both directions. Furthermore, compared to Figure 16(a), the multi-target attack exhibits a smaller throughput decrease percentage. This is because the amplitude of the attack signal is dispersed to dual attack directions.

For the indiscriminate attack, Hydra aims to decrease the throughput within the coverage area of the RIS. As illustrated in Figure 16(c), we can clearly see that the throughput shrinks significantly across all directions, spanning from $-90°$ to $90°$. Specifically, the throughput dramatically falls to 121 Mbps upon the implementation of the RIS's attack strategy. The average TDP is 43%. As the amplitude of the attack signal is dispersed across the entire attack region, the throughput

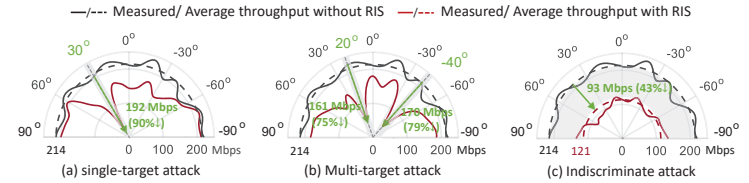


Figure 16: Different attack scenarios, such as single-target, multi-target, and indiscriminate attack.

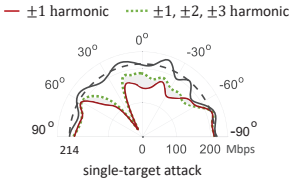


Figure 17: High-order harmonic suppression.

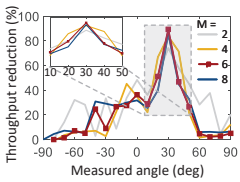


Figure 18: Effect of state transition count.

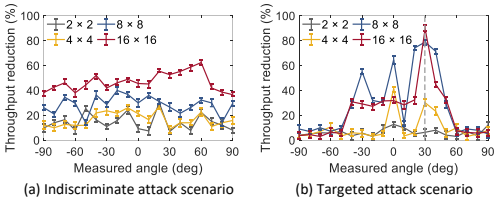


Figure 19: The impact of the number of RIS meta-atoms.

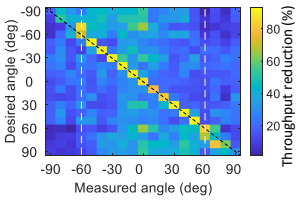


Figure 20: The filed-of-view of target attack.

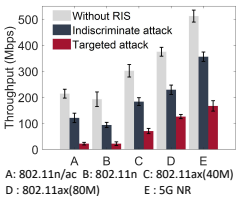


Figure 21: The attack of different protocols.

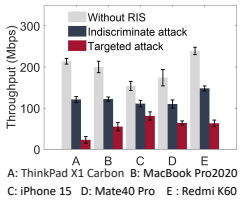


Figure 22: The attack of different devices.

decrease percentage of indiscriminate attacks is evidently smaller than that observed in targeted attacks.

Overall, these results demonstrate that Hydra can perform precisely attack strategies for different attack scenarios.

High-order harmonic suppression. To evaluate that Hydra reduces the energy leakage of high-order harmonics by controlling their direction, we compared the attack effects of using ±1 harmonics and using ±1 to ±3 harmonics for beamforming in a single-target scenario. The victim receiver is located at 30°, and Figure 17 shows the attack results. The results indicate that Hydra can effectively control the energy direction of high-order harmonics, significantly reduce interference in non-target directions, and improve the stealth of the attack. However, it should be noted that the throughput in the non-target direction is still slightly affected even compared to no RIS, mainly because the sidelobes of the beam also produce low-amplitude harmonics.

7.2 Parameters Evaluation

The impact of state transition numbers. To evaluate how the cycle encoding number M impacts attack effectiveness, we take a 30° single-target scenario as a case study. We keep the hardware switching frequency constant, set the number of router MIMO channels to 2, and vary M from 2 to 8 with a step of 2. We calculate the average TDP for each direction, ranging from −90° to 90°, for each value of M. Figure 18 illustrates that as M increases, the precision and effectiveness of the targeted attack improve. This enhancement is due to the ability of a higher number of cyclic codings to surpass the phase limitations inherent in RIS prototypes, allowing for nearly complete 360° phase compensation. Consequently, it facilitates more effective harmonic beamforming characterized by a narrower, more high gain mainlobe and reduced sidelobe levels. In addition, the results reveal that the attack performance for $M = 6$ and $M = 8$ are similar, which is attributed to the fact that $M = 6$ almost achieves the optimal phase compensation.

The impact of meta-atoms numbers. To evaluate the effect of varying meta-atom quantities on attack performance, we conducted evaluations of throughput and calculated TDP across indiscriminate and targeted attack scenarios, utilizing meta-atom configurations of 2×2, 4×4, 8×8, and 16×16.

In indiscriminate attacks, significant differences in TDP are observed across configurations under different numbers of meta-atoms. For instance, an average TDP of 43% and 13% for RIS equipped with 16×16 and 2×2 meta-atoms, respectively (Figure 19(a)). The results indicate that the number of meta-atoms directly influences the energy of the malicious signal, thereby impacting attack effectiveness.

In targeted attack, the direction of the victim is 30°. Figure 19(b) depicts that the 2×2 RIS lacks effective beamforming capabilities. Conversely, configurations employing 4×4 and 8×8 meta-atoms generate higher sidelobe energy during beamforming, resulting in negative effects communication in other directions. In contrast, the 16×16 RIS can perform an effective target attack by generating a "pencil beam" to focus on the desired target while suppressing sidelobe energy, thereby mitigating negative impacts on adjacent users.

Overall, larger RIS with more meta-atoms demonstrated enhanced capabilities in meeting the demands of both indiscriminate and targeted attack scenarios.

7.3 Attack Performance

The filed-of-view of target attack. To evaluate the effective attack filed-of-view (FoV) of Hydra, we measure the throughput and calculate the TDP for each attack direction within the range of −90° to 90°, at intervals of ±10°. Figure 20 presents the confusion matrix of TDP results. The TDP exceeds 80% across a wide range of 120° (i.e, [−60°, 60°]), clearly demonstrating Hydra's capability to conduct

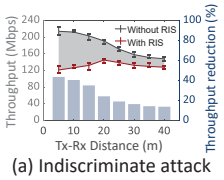


Figure 23: Performance of distance between Tx and Rx.

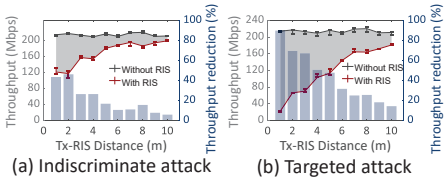


Figure 24: Performance of distance between Tx and RIS.

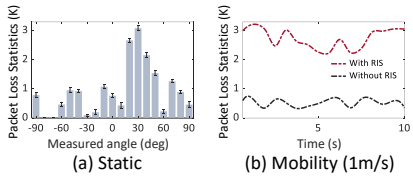


Figure 25: Effectiveness of BA frames for receiver direction identification.

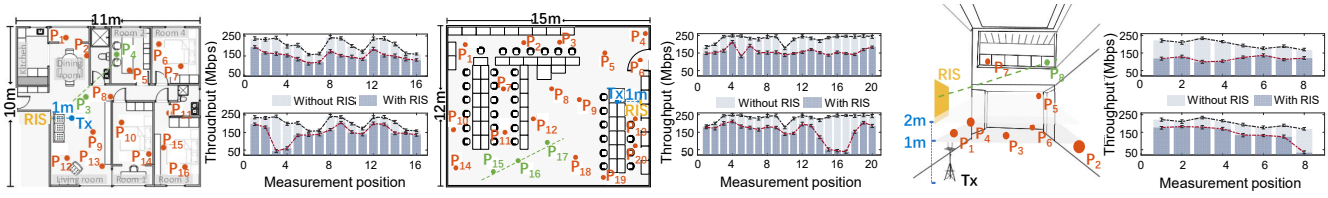


Figure 26: Attack performance under different physical environments.

highly destructive targeted attacks. For victim directions falling outside the effective attack FoV, we can readjust to the position/orientation of RIS or deploy multiple RISs to extend the attack coverage.

The attack performance under different protocols. The RIS of Hydra can be transparent to existing IoT communication standards. We verify this property through four kinds of protocols, i.e., 802.11n, 802.11n/ac, 802.11ax, and 5G NR, where 802.11ax has two modes with 40 MHz and 80 MHz bandwidth, respectively. Figure 21 shows the throughput when with attack modes are "ON" and "OFF" in target and indiscriminate attack scenarios. As we can see, with attacks "ON", there is a consistent and notable throughput decrease (up to 90%) for all protocols.

The attack performance under different devices. To evaluate the attack effectiveness on different devices, we conduct experiments using three commercial smartphones and two laptops to measure communication throughput, both with and without the attack strategy. The experimental results are shown in Figure 22. We can see a significant drop in throughput across all devices, indicating that Hydra can operate transparently across different devices.

The attack range. In outdoor settings, we evaluate the effectiveness of Hydra under both indiscriminate and targeted attack scenarios across various Tx-Rx distances.

For indiscriminate attack, the Tx-Rx distance varies from 1m to 40 m with a step of 5m. We measure the average throughput across $-90°$ to $90°$ under each Tx-Rx distance. As depicted in Figure 23(a), the attack remains effective up to a distance of 40m, albeit with a gradual decrease in the TDP. Specifically, the TDP drops from 43% at 5m to below 20% at 40m, illustrating the trade-off between attack range and distance in indiscriminate attacks due to the dispersion of attack signals across the entire region. This limitation can be easily mitigated by employing larger-sized RIS equipped with more meta-atoms.

For targeted attack, the victim receiver is located at a $30°$ direction from the RIS. Figure 23(b) reveals that the throughput decreases significantly, from 212 Mbps to 52.2 Mbps (75% reduction) at a distance of 10m, and from 45 Mbps to 21.4 Mbps (52% reduction) even at 150m. The TDP remains above 50% across distances ranging from 0 to 160m, demonstrating Hydra can conduct highly effective and precisely targeted attacks over distances spanning several hundred meters.

The impact of Tx-RIS distance. To evaluate the effect of the Tx-RIS distance on the efficacy of Hydra's attacks, we extend the Tx-RIS distance from 1m to 10m, measure throughput and calculate TDP in both indiscriminate and targeted attack scenarios. Figure 24 demonstrates that no matter what attack scenarios, while the attacks remain work with the Tx-RIS distance extended up to 10m, the TDP diminishes as the distance increases. This is because Hydra does not generate attack signals but rather reflects them from legitimate signals, the energy of attack signal decreases as the distance from the transmitter increases. We can increase the energy captured from the transmitter by using or hacking a larger RIS equipped with more meta-atoms. Overall, these results demonstrate Hydra's potential utility even when the RIS is positioned at greater distances from the Tx.

Effectiveness of BA frame. To evaluate the efficacy of the BA frame in pinpointing beamforming directions under conditions of unknown user locations and moving targets, we conducted tests measuring the packet loss statistic in both static and mobility scenarios(moving at 1m/s). The transmitter is located at a fixed location. Each beam scan listens to BA frames at 1 ms intervals, and each BA frame contains 64 ACK bits. First, ±1 harmonics are used to perform beam scans in $20°$ steps within the FoV of Hydra (i.e, $[-60°, 60°]$) to preliminarily estimate the direction, and then fine-tune with

5° steps. We shorten the preparation time by pre-storing the RIS beam codebook in the controller, and the entire attack initialization process does not exceed 12 ms. The results, depicted in Figure 25, compare real-time packet loss statistics with and without an RIS attack. The receiver is placed at a 30° angle in the static scenario and moves along a predefined trajectory. In Figure 25(a), we can see a spike in packet loss at specific directions, corroborating the capability of Hydra to leverage the BA frame in identifying the victim's location accurately. Furthermore, in Figure 25(b) packet loss rates remain consistently high proving that Hydra can execute harmonic beamforming targeted at the moving receiver. These results affirm that Hydra can utilize the BA frame to identify the direction of victims and maintain high performance in dynamic environments.

The attack performance under different environments. To assess the effectiveness of the attack across varied settings, we conduct experiments in three environments: a 110 m^2 residential space divided into four rooms representing a Non-Line-of-Sight (NLoS) scenario, a 180 m^2 open-plan office representing a Line-of-Sight (LoS) scenario, and a 3D complex spatial setup. Figure 26 shows the attack performance in different channel conditions. Figure 26(a1,b1,c1) display the scenario layout and measurement positions, with the directions of targeted attacks indicated by green dashed lines. Figure 26(a2,b2,c2) display the results of throughput measurements, where the upper charts show indiscriminate attacks and the lower charts show targeted attacks. The results highlight: firstly, in indiscriminate attack scenarios, the attack's effectiveness remains consistently high across all directions, irrespective of the environments. Secondly, when the receiver aligns with the beamforming direction, the attack consistently succeeds, regardless of the distance between the attacker and receiver and irrespective of whether the conditions are LoS or NLoS. This demonstrates the robustness and effectiveness of Hydra in both indiscriminate and targeted attack modes across a variety of physical environments.

8 DISCUSSION AND FUTURE WORK

Tx-RIS distance. RIS passively reflects energy from the Tx. Therefore, to ensure the effectiveness of the attack, the distance between Tx and RIS is affected by RIS size and Tx power. The smaller RIS and the lower Tx power necessitate closer deployment to the Tx. In our proof-of-concept prototype experiment, we used a small RIS (35 cm×35 cm), and this compact form factor allows us to deploy it discreetly in an inconspicuous location. Larger commercial-grade RISs [1, 3] are being developed, and attackers can manipulate these through their controllers. In addition, for higher-power or multi-antenna routers, or high-power base station facilities, the distance between Tx and RIS can also be increased.

Environmental conditions. Hydra offers flexible deployment of RIS to deal with various environmental conditions. One possible method in complex and large-scale environments with multiple targets is to use multiple small RIS for coordinated attacks, which can reduce the complexity and control burden, while enhancing stealth and fault tolerance. We will leave the environment-adaptive attack as a challenging yet interesting research direction for future work.

The victim parties. Hydra has tested the attack on 802.11 and 5G NR protocols, as well as on several commercial devices. Future work should investigate the susceptibility of attacks to new standards, different antenna configurations, various RF transceiver architectures, diverse signal processing algorithms, and specific chipsets.

Harmonic leakage. In the target attack scenario, the throughput in the sidelobe direction has slightly decreased due to weak harmonic leakage. Suppressing the harmonic leakage to achieve a highly directional target attack is future work.

Potential Defense Strategies. Hydra tampers with spatial-spectral attributes of reflected signal; hence, a potential Strategy is to exploit advanced signal processing techniques or deploy a high spectral resolution dedicated hardware to improve spectral resolution at the legitimate user and detect spectral anomaly patterns. However, it causes additional cost, complexity, and power consumption for legitimate users. We will explore defense strategies in future work.

9 CONCLUSION

This paper introduces a wireless link disruption system based on RIS by disrupting the critical orthogonality of OFDM subcarriers, Hydra. By carefully designing the attack strategies, the field study shows that Hydra can achieve a 90% throughput reduction in targeted attack scenarios and a 43% throughput reduction in indiscriminate attack scenarios. Furthermore, we validated the effectiveness of our attacks on both the 802.11 protocol and the 5G NR protocol.

ACKNOWLEDGMENT

This research was supported by the National Natural Science Foundation of China under Grant No. 62372374 and 62372372. This work is also supported by Shaanxi Science and Technology Innovation Team Program under Grant 2024RSCXTD05, and Shaanxi Qinchuangyuan Program under Grant QCYRCXM2023103. We thank our reviewers and shepherd for their insightful feedback which helped improve this paper.

REFERENCES

[1] [n. d.]. Greenerwave. http://greenerwave.com.
[2] [n. d.]. MathWorks WLAN Toolbox. https://www.mathworks.com/products/wlan.html.
[3] [n. d.]. Metawave Corporation. https://www.metawave.com.
[4] [n. d.]. USB. https://usb.org/document-library/usb-power-deliverys.

[5] Venkat Arun and Hari Balakrishnan. 2020. {RFocus}: Beamforming using thousands of passive antennas. In *17th USENIX symposium on networked systems design and implementation (NSDI 20)*. 1047–1061.

[6] Ertugrul Basar, Marco Di Renzo, Julien De Rosny, Merouane Debbah, Mohamed-Slim Alouini, and Rui Zhang. 2019. Wireless communications through reconfigurable intelligent surfaces. *IEEE access* 7 (2019), 116753–116773.

[7] Tamer Basar. 1983. The Gaussian test channel with an intelligent jammer. *IEEE Transactions on Information Theory* 29, 1 (1983), 152–157.

[8] Michael Boyarsky, Timothy Sleasman, Mohammadreza F Imani, Jonah N Gollub, and David R Smith. 2021. Electronically steered metasurface antenna. *Scientific reports* 11, 1 (2021), 1–10.

[9] Yifeng Cai, Konstantinos Pelechrinis, Xin Wang, Prashant Krishnamurthy, and Yijun Mo. 2013. Joint reactive jammer detection and localization in an enterprise WiFi network. *Computer Networks* 57, 18 (2013), 3799–3811.

[10] Mingyang Chang, Yajie Mu, Jiaqi Han, Guanxuan Li, Yicen Li, Haixia Liu, Long Li, and Tie Jun Cui. 2024. Tailless Information–Energy Metasurface. *Advanced Materials* (2024), 2313697.

[11] Haoze Chen and Yasaman Ghasempour. 2022. Malicious mmWave reconfigurable surface: Eavesdropping through harmonic steering. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*. 54–60.

[12] Kun Woo Cho, Yasaman Ghasempour, and Kyle Jamieson. 2022. Towards dual-band reconfigurable metasurfaces for satellite networking. In *Proceedings of the 21st ACM Workshop on Hot Topics in Networks*. 17–23.

[13] Kun Woo Cho, Mohammad H Mazaheri, Jeremy Gummeson, Omid Abari, and Kyle Jamieson. 2021. mmWall: A reconfigurable metamaterial surface for mmWave networks. In *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*. 119–125.

[14] T Charles Clancy. 2011. Efficient OFDM denial: Pilot jamming and pilot nulling. In *2011 IEEE International Conference on Communications (ICC)*. IEEE, 1–5.

[15] Philipp Del Hougne, Mathias Fink, and Geoffroy Lerosey. 2019. Optimally diverse communication channels in disordered environments with tuned randomness. *Nature Electronics* 2, 1 (2019), 36–41.

[16] Manideep Dunna, Chi Zhang, Daniel Sievenpiper, and Dinesh Bharadia. 2020. ScatterMIMO: Enabling virtual MIMO with smart surfaces. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom)*. 1–14.

[17] Chao Feng, Xinyi Li, Yangfan Zhang, Xiaojing Wang, Liqiong Chang, Fuwei Wang, Xinyu Zhang, and Xiaojiang Chen. 2021. RFlens: metasurface-enabled beamforming for IoT communication and sensing. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 587–600.

[18] Yuehong Gao, Changhao Sun, Xiaonan Zhang, and Xiao Hong. 2021. Study on MCS Selection and Spectrum Allocation for URLLC Traffic under Delay and Reliability Constraint in 5G Network. *arXiv preprint arXiv:2101.05215* (2021).

[19] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197–215.

[20] Kai Guo, Qun Zheng, Zhiping Yin, and Zhongyi Guo. 2020. Generation of mode-reconfigurable and frequency-adjustable OAM beams using dynamic reflective metasurface. *IEEE Access* 8 (2020), 75523–75529.

[21] Seyed Ehsan Hosseininejad, Kasra Rouhi, Mohammad Neshat, Albert Cabellos-Aparicio, Sergi Abadal, and Eduard Alarcón. 2019. Digital metasurface based on graphene: An application to beam steering in terahertz plasmonic antennas. *IEEE Transactions on Nanotechnology* 18 (2019), 734–746.

[22] Cheng Huang, Changlei Zhang, Jianing Yang, Bo Sun, Bo Zhao, and Xiangang Luo. 2017. Reconfigurable metasurface for multifunctional control of electromagnetic waves. *Advanced Optical Materials* 5, 22 (2017), 1700485.

[23] Nadège Kaina, Matthieu Dupré, Geoffroy Lerosey, and Mathias Fink. 2014. Shaping complex microwave fields in reverberating media with binary tunable metasurfaces. *Scientific reports* 4, 1 (2014), 6693.

[24] Matthew J La Pan, T Charles Clancy, and Robert W McGwier. 2012. Jamming attacks against OFDM timing synchronization and signal acquisition. In *MILCOM 2012-2012 IEEE Military Communications Conference*. IEEE, 1–7.

[25] Matthew J La Pan, T Charles Clancy, and Robert W McGwier. 2013. Phase warping and differential scrambling attacks against OFDM frequency synchronization. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2886–2890.

[26] Khoa N Le. 2008. Insights on ICI and its effects on performance of OFDM systems. *Digital Signal Processing* 18, 6 (2008), 876–884.

[27] Guyue Li, Paul Staat, Haoyu Li, Markus Heinrichs, Christian Zenger, Rainer Kronberger, Harald Elders-Boll, Christof Paar, and Aiqun Hu. 2023. RIS-Jamming: Breaking Key Consistency in Channel Reciprocity-based Key Generation. *arXiv preprint arXiv:2303.07015* (2023).

[28] Xinyi Li, Chao Feng, Xiaojing Wang, Yangfan Zhang, Yaxiong Xie, and Xiaojiang Chen. 2023. {RF-Bouncer}: A Programmable Dual-band Metasurface for Sub-6 Wireless Networks. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*. 389–404.

[29] Zhijian Liang and Guoliang Xing. 2024. SRIS: Self-powered Reconfigurable Intelligent Surfaces. In *Proceedings of the 25th International Workshop on Mobile Computing Systems and Applications*. 66–72.

[30] Yuanwei Liu, Xiao Liu, Xidong Mu, Tianwei Hou, Jiaqi Xu, Marco Di Renzo, and Naofal Al-Dhahir. 2021. Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE communications surveys & tutorials* 23, 3 (2021), 1546–1577.

[31] Bin Lyu, Dinh Thai Hoang, Shimin Gong, Dusit Niyato, and Dong In Kim. 2020. IRS-based wireless jamming attacks: When jammers can attack without power. *IEEE Wireless Communications Letters* 9, 10 (2020), 1663–1667.

[32] Richard van Nee and Ramjee Prasad. 2000. *OFDM for wireless multimedia communications*. Artech House, Inc.

[33] Mahyar Nemati, Behrouz Maham, Shiva Raj Pokhrel, and Jinho Choi. 2021. Modeling RIS empowered outdoor-to-indoor communication in mmWave cellular networks. *IEEE Transactions on Communications* 69, 11 (2021), 7837–7850.

[34] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. 2010. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials* 13, 2 (2010), 245–257.

[35] Thierry Pollet, Mark Van Bladel, and Marc Moeneclaey. 1995. BER sensitivity of OFDM systems to carrier frequency offset and Wiener phase noise. *IEEE Transactions on communications* 43, 2/3/4 (1995), 191–193.

[36] Rúben Queirós, Eduardo Nuno Almeida, Helder Fontes, José Ruela, and Rui Campos. 2022. Wi-Fi rate adaptation using a simple deep reinforcement learning approach. In *2022 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–3.

[37] Chowdhury Shahriar, Matt La Pan, Marc Lichtman, T Charles Clancy, Robert McGwier, Ravi Tandon, Shabnam Sodagari, and Jeffrey H Reed. 2014. PHY-layer resiliency in OFDM communications: A tutorial. *IEEE Communications Surveys & Tutorials* 17, 1 (2014), 292–314.

[38] Chowdhury Shahriar, Robert McGwier, and T Charles Clancy. 2013. Performance impact of pilot tone randomization to mitigate OFDM jamming attacks. In *2013 IEEE 10th Consumer Communications and*

Networking Conference (CCNC). IEEE, 813–816.

[39] Chowdhury Shahriar, Shabnam Sodagari, and T Charles Clancy. 2012. Performance of pilot jamming on MIMO channels with imperfect synchronization. In *2012 IEEE International Conference on Communications (ICC)*. IEEE, 898–902.

[40] W Pam Siriwongpairat and KJ Ray Liu. 2007. *Ultra-wideband communications systems: multiband OFDM approach*. John Wiley & Sons.

[41] Paul Staat, Harald Elders-Boll, Markus Heinrichs, Christian Zenger, and Christof Paar. 2022. Mirror, mirror on the wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. 208–221.

[42] Anastasios Stamoulis, Suhas N Diggavi, and Naofal Al-Dhahir. 2002. Intercarrier interference in MIMO OFDM. *IEEE Transactions on signal processing* 50, 10 (2002), 2451–2464.

[43] Peng Tan and Norman C Beaulieu. 2004. Reduced ICI in OFDM systems using the" better than" raised-cosine pulse. *IEEE Communications Letters* 8, 3 (2004), 135–137.

[44] Qian Wang, Edward TF Rogers, Behrad Gholipour, Chih-Ming Wang, Guanghui Yuan, Jinghua Teng, and Nikolay I Zheludev. 2016. Optically reconfigurable metasurfaces and photonic devices based on phase change materials. *Nature photonics* 10, 1 (2016), 60–65.

[45] Qingqing Wu and Rui Zhang. 2019. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. *IEEE Communications Magazine* 58, 1 (2019), 106–112.

[46] Gang Yang, Yating Liao, Ying-Chang Liang, Olav Tirkkonen, Gongpu Wang, and Xing Zhu. 2021. Reconfigurable intelligent surface empowered device-to-device communication underlaying cellular networks. *IEEE Transactions on Communications* 69, 11 (2021), 7790–7805.

[47] Fan Yi, Kun Woo Cho, Yaxiong Xie, and Kyle Jamieson. 2023. WaveFlex: A Smart Surface for Private CBRS Wireless Cellular Networks. *arXiv preprint arXiv:2310.11551* (2023).

[48] Lei Zhang, Ming Zheng Chen, Wankai Tang, Jun Yan Dai, Long Miao, Xiao Yang Zhou, Shi Jin, Qiang Cheng, and Tie Jun Cui. 2021. A wireless communication scheme based on space-and frequency-division multiplexing using digital metasurfaces. *Nature electronics* 4, 3 (2021), 218–227.

[49] Lei Zhang, Xiao Qing Chen, Shuo Liu, Qian Zhang, Jie Zhao, Jun Yan Dai, Guo Dong Bai, Xiang Wan, Qiang Cheng, Giuseppe Castaldi, et al. 2018. Space-time-coding digital metasurfaces. *Nature communications* 9, 1 (2018), 1–11.

[50] Jie Zhao, Xi Yang, Jun Yan Dai, Qiang Cheng, Xiang Li, Ning Hua Qi, Jun Chen Ke, Guo Dong Bai, Shuo Liu, Shi Jin, et al. 2019. Programmable time-domain digital-coding metasurface for non-linear harmonic manipulation and new wireless communication systems. *National science review* 6, 2 (2019), 231–238.

[51] Shangqing Zhao, Zhuo Lu, Zhengping Luo, and Yao Liu. 2019. Orthogonality-sabotaging attacks against OFDMA-based wireless networks. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 1603–1611.

[52] Yue Zheng, Chenshu Wu, Kun Qian, Zheng Yang, and Yunhao Liu. 2017. Detecting radio frequency interference for CSI measurements on COTS WiFi devices. In *2017 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[53] Yue Zheng, Zheng Yang, Junjie Yin, Chenshu Wu, Kun Qian, Fu Xiao, and Yunhao Liu. 2018. Combating cross-technology interference for robust wireless sensing with cots wifi. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 1–9.