Mirror Mirror on the Wall: Wireless Environment Reconfiguration Attacks Based on Fast Software-Controlled Surfaces

Paul Staat
Max Planck Institute for Security and Privacy
Bochum, Germany

Harald Elders-Boll
TH Köln – University of Applied Sciences
Cologne, Germany

Markus Heinrichs
TH Köln – University of Applied Sciences
Cologne, Germany

Christian Zenger
PHYSEC GmbH
Bochum, Germany

Christof Paar
Max Planck Institute for Security and Privacy
Bochum, Germany

ABSTRACT
The intelligent reflecting surface (IRS) is a promising new paradigm in wireless communications for meeting the growing connectivity demands in next-generation mobile networks. IRS, also known as software-controlled metasurfaces, consist of an array of adjustable radio wave reflectors, enabling smart radio environments, e.g., for enhancing the signal-to-noise ratio (SNR) and spatial diversity of wireless channels. Research on IRS to date has been largely focused on constructive applications.

In this work, we demonstrate for the first time that the IRS provides a practical low-cost toolkit for attackers to easily perform complex signal manipulation attacks on the physical layer in real time. We introduce the environment reconfiguration attack (ERA) as a novel class of jamming attacks in wireless radio networks. Here, an adversary leverages the IRS to rapidly vary the electromagnetic propagation environment to disturb legitimate receivers. The IRS gives the adversary a key advantage over traditional jamming: It no longer has to actively emit jamming signals, instead the IRS reflects existing legitimate signals. In addition, the adversary doesn’t need any knowledge about the legitimate channel. We thoroughly investigate the ERA in wireless systems based on the widely employed orthogonal frequency division multiplexing (OFDM) modulation. We present insights into the attack through analytical analysis, simulations, as well as experiments. Our results show that the ERA allows to severely degrade the available data rates even with reasonably small IRS sizes. Finally, we implement an attacker setup and demonstrate a practical ERA to slow down an entire Wi-Fi network.

1 INTRODUCTION
Part of the ever-evolving digital landscape is growing demand for wireless connectivity at high data rates and low latency. In addressing this need, increasingly sophisticated mobile communication networks are being deployed. In particular, we are in the midst of the worldwide roll-out of 5G networks, which are the key-enablers for emerging applications such as, e.g., autonomous driving, smart cities, smart grids, and immersive entertainment [1, 2, 19]. Such applications will lead to an increased dependency on a wireless infrastructure with high availability and high attack resistance. Specific to wireless networks is jamming of radio signals, which leads to denial of service and can pose a serious threat to, e.g., cellular networks such as 4G and 5G [3, 15, 26].

Next-generation wireless networks make use of sophisticated communication technologies such as massive MIMO (massive multiple-input and multiple-output), which is now realized with 5G [6]. An even more recent example for a technological advance are intelligent reflecting surfaces (IRS) [43]. IRS consist of an array of electronically adjustable reflectors with respect to radio waves. IRS enable smart radio environments [25, 36] to, e.g., enhance the wireless radio channel quality in terms of signal-to-noise ratio (SNR) [24] or spatial diversity [13].

However, the IRS is also a novel attacker tool for malicious purposes — an issue that has received only little attention as of yet. In this work, we show that time-varying IRS allow to disrupt wireless communications by (smart) reflecting radio signals originating from the legitimate parties. We introduce the environment reconfiguration attack (ERA), which can be viewed as a novel class of practical, low-cost, and low-complexity jamming attacks. The essence of the ERA lies in high-speed IRS reconfigurations, which are digitally controlled by the attacker Eve. In effect, the wireless propagation environment, i.e., the wireless channel, between the communication parties Alice and Bob (cf. Fig. 1) exhibits exceptionally fast and instantaneous changes that otherwise do not occur in nature. In turn, severe variations are applied to signals coming from the legitimate transmitter which disturb the intended receiver. A key

![Figure 1: Illustration of the ERA setting where the attacker Eve uses an IRS to gain partial control over the wireless channel between legitimate parties Alice and Bob. $c_{i,k}$ and $g_{i,k}$ are the channels to (and from) the IRS, $d_k$ is the direct (non-IRS) channel, with the $k^{th}$ OFDM subcarrier and $i^{th}$ IRS element.](https://example.com/era_diagram.png)
difference to traditional jamming attacks is that the attacker does not actively emit a jamming signal but merely reflects signals generated by a victim party. Accordingly, the ERA leads to correlated interference and dramatically simplifies the implementation of such attacks [27], as the attacker neither needs an RF transmitter nor a receiver. Unlike previous work [29], the ERA does not require the attacker to have any channel knowledge and only rudimentary knowledge (such as the modulation scheme) about the communication system. This crucial relaxation allows us to demonstrate the first real-world jamming attack based on IRS.

In this paper, we show that the IRS is a practical and low-cost attacker tool, enabling the ERA. We investigate the attack using orthogonal frequency division multiplexing (OFDM) which is widely used in modern wireless networks, including 4G, 5G, and Wi-Fi. We perform a thorough theoretical analysis to explain the fundamental attack mechanisms. Furthermore, we show simulation results that allow us to characterize the attack requirements on signal power, distances and IRS dimensions. Finally, we implement an attacker setup and demonstrate a practical ERA, slowing down an entire wireless network. Our results show that the attack works with reasonably small IRS sizes, notably the used IRS has dimensions 40 cm × 16 cm. Moreover, we provide a practical IRS optimization algorithm to enhance the attack performance.

In summary, building upon the advent of IRS, we introduce a new class of practical jamming attacks which are low-cost and can easily be deployed in many wireless scenarios. The paper at hand contains the following key contributions:

- We propose the environment reconfiguration attack (ERA) as a novel class of jamming attacks, based on low-cost IRS.
- We present a theoretical analysis explaining how the ERA affects OFDM communications.
- We show comprehensive simulation results to determine the attacker requirements on signal power, distances and IRS dimensions.
- We demonstrate a practical ERA on commodity Wi-Fi using a low-cost IRS prototype, allowing to substantially reduce the wireless throughput in the entire network.
- We present an IRS optimization algorithm to further enhance the ERA jamming performance.

2 BACKGROUND

In this section, we provide technical background on the IRS, jamming attacks, and OFDM communications.

2.1 Intelligent Reflecting Surface

An IRS is a synthetic planar structure with digitally reconfigurable reflection properties of electromagnetic (EM) waves. In wireless communications, the IRS is a rather new concept that has evolved from physics research on metamaterials and metasurfaces [24] which are tailored to enable non-standard EM wave field manipulations. More recently, the evolutionary step from the metasurface to the IRS has been made: Metasurface designs have been drastically simplified and became digitally controllable. An IRS consists of many distributed identical unit cells, each of which reflects impinging EM waves. Most importantly, the complex reflection coefficient of each element across the surface is individually programmable, allowing to influence the wireless channel of communication parties (see Fig. 1). Practical IRS designs are often targeted to adjust only the signal phase with quantization as low as 1 bit [48]. Thus, the IRS provides a simple digital interface towards the physical layer of wireless communications and enables what is coined smart radio environments [25] with novel applications such as, e.g., optimization of the signal-to-noise ratio (SNR) [5] or spatial diversity [13]. Since only ambient signals are reflected, the IRS is inherently energy efficient and does not require active RF chains. Thus, IRS have low hardware complexity since manufacturing requires standard microstrip technology on low-cost printed circuit board (PCB) substrate. Currently, the IRS is in discussion to complement future wireless infrastructure on a large scale in wireless networks beyond 5G [49].

2.2 Jamming

Wireless communication relies on a broadcast medium that must be shared between many users. In principle, each user is free to transmit at any time and thus, signals are by definition subject to interference. Instead of just the desired signal, a receiver then additionally picks up an unwanted signal, disrupting the intended communication. Despite regularly occurring interference from other user’s communications, malicious parties can also launch jamming attacks. Here, an attacker deliberately produces interference to disable the communication of targeted users. Jamming attacks can be classified into a variety of different categories, including the type of interference and the strategy to trigger emission of the interfering signal [18]. A jammer may use noise signals, constant tones, or even valid waveforms. Attackers can apply constant jamming or act reactively in order to disable only selected parts of the victim communication, such as physical control channels [15].

2.3 Orthogonal frequency division multiplexing (OFDM)

Due to its unique properties, OFDM has become one of the most important and widely used modulation techniques in wireless networks [9, 16]. Most importantly, OFDM can cope with multipath signal propagation easily. In order to push data rates, wide channel bandwidths need to be used. However, when transmitting a widebandwidth signal over a wireless link, it will most likely experience some form of frequency selective attenuation due to fading from multipath signal propagation. OFDM divides a wide bandwidth into numerous independent (say, orthogonal) narrowband channels, i.e., subcarriers, and can thus handle frequency selective channels at low computational complexity. Taking the concept to the next level, OFDM based multiple access (OFDMA) schemes assign different subcarriers to different users. Finally, the modulation and demodulation of OFDM are elegantly handled using an efficient (inverse) fast Fourier transform (FFT). Today, OFDM has become the definitive transmission scheme for broadcasting, e.g., DAB and DVB, cellular systems, e.g., 4G and 5G, and personal networks, e.g., Wi-Fi.
3 RELATED WORK

In this section, we summarize the relevant literature on IRS and jamming attacks, and also describe how our work differs from previous proposals.

Intelligent reflecting surface. The IRS has been widely recognized as a potential major innovation in wireless communications and has stimulated much research activity recently. Hence, there is a manifold literature now. Regarding key concepts and literature reviews, we refer to numerous overview works [5, 25, 43, 44].

To the best of our knowledge, previous works on IRS in a security context focus on theoretical aspects. Most notably, Lyu et al. [29] proposed the IRS for minimizing the signal power received by a victim party for jamming. We further elaborate the similarities and differences to our work towards the end of this section. Several works, e.g., [12] and [7], provide analytical and simulation results in the context of physical layer security assisted by an IRS. Huang and Wang [21] discuss a pilot contamination attack using an IRS to increase signal leakage by reflecting pilot signals. In [47], the authors pursue IRS to be used as a mitigation for active jamming attacks.

In the following we give examples for studies including practical IRS demonstrations with a focus on improving wireless communication. An early work from 2014 is [24], where the authors demonstrate wave field shaping. Work from 2019 [13] has shown that IRS are capable of enhancing spatial diversity. Arun and Balakrishnan in 2020 [4] demonstrated a large prototype IRS with 3200 elements for passive beamforming applications. In recent work of Pei et al. [33], an IRS is used to achieve substantial channel improvements, enabling a long-range communication field trial over 500 m. Several works report practical IRS designs, e.g., [22, 46, 48].

Jamming attacks. The literature widely recognizes jamming attacks as a risk to the reliability of wireless communications. Several works have pointed out the threat of jamming against 4G [15, 26] and 5G [3] networks. Grover et al. [18] provide an overview on different jamming strategies, localization and detection techniques, and countermeasures. However, the ERA does not fit any of the reported categories properly. Poisel gives a highly comprehensive overview on all classes of jamming in his book [34]. Lichtman et al. [27] provide a taxonomy for jamming attacks by defining four attacker capabilities time correlation, protocol awareness, ability to learn, and signal spoofing. Following their categories, the ERA may be labeled as a partially time-correlated jammer. However, unlike the author’s category-based conjecture, the ERA is a low-complexity attack. Hang et al. [20] investigate repeater jamming against direct sequence spread spectrum (DSSS). The ERA may indeed be seen as a special case of repeater jamming, as a reflection of the signal in fact is a time-varying copy of the legitimate signal. Thus, the ERA is conceptually related. In the ERA, however, the attacker eliminates RF receiver and transmitter chains and processing delays. Pöpper et al. [35] report a method to achieve jamming-resistant broadcast communications without shared keys. The authors comment on the repeater jammer which could circumvent their security assumptions in some cases and also point to processing delays. For our IRS-based approach, however, processing delays vanish. Clancy [10] has pointed out that OFDM communications can be efficiently disrupted by jamming or nulling of pilot signals for channel estimation. The ERA now provides a simple method to realize the manipulation of the OFDM equalizer. Also, many works pursue detection of jamming, examples include [8, 28, 39]. A different body of work examines helpful aspects of jamming, e.g., to provide confidentiality [42]. However, Tippenhauer et al. [40] have shown that jamming for confidentiality has fundamental security limitations.

Differentiation from previous work. The general idea of maliciously using an IRS for jamming was first proposed by Lyu et al. [29] in 2020, albeit in a very different manner that we believe results in a much lower practicality than the ERA. The approach of [29] is based on an IRS to minimize the signal power received by a victim party – a method opposite to the classical IRS-based SNR improvement. Here, the superposition of the direct signal and the malicious IRS signal shall result in destructive interference, i.e., the IRS signal is to be a phase-exact cancellation signal. However, finding a specific IRS configuration to meet this goal is non-trivial. Addressing this issue, the authors formulate an optimization scheme to obtain a corresponding IRS configuration from the channel states $c_{i,k}$, $g_{i,k}$, and $d_k$, cf. Fig. 1. Thus in this approach the attacker needs to have full knowledge of all involved channel states. Unfortunately for an attacker, $d_k$ can only be found by the victim parties and obtaining $c_{i,k}$ and $g_{i,k}$ is infeasible (without a large number of additional RF receivers at the attacker’s IRS), as recognized in the literature [5, 43, 44].

In contrast, the ERA approach presented in this paper works entirely different, thereby eliminating the unrealistic requirement of channel knowledge for the attacker. Crucially, the attack leverages the IRS to rapidly toggle between (two) effective wireless channels. In particular, we address OFDM receivers which get disturbed by the unnatural switching between channel states, e.g., partly due to adaptive behavior. Our goal is not the minimization of the signal reception of one or both of the ERA channels. Rather, the ERA exploits signal changes from the difference between the two ERA channels as a source of interference. Thus, the attack neither requires synchronization or phase-exact knowledge of all channels, and thereby avoids a location-dependent attack performance (signal phase changes by movement), as our experimental results show.

In order to compare the two attack strategies, we would like to point out that a cancellation approach [29] is equivalent to reducing the SNR – an aspect that we readily cover in our simulations in Section 6.1, showing that the ERA can achieve substantially increased jamming performance.

4 ATTACK OVERVIEW

Parties. In this work, we consider a physical layer attacker Eve trying to disrupt the wireless radio communication of two legitimate parties Alice and Bob who deploy a conventional OFDM-based wireless communication system. Thus, Alice and Bob may use Wi-Fi, 4G, or 5G and could represent a base-station and an end-user, respectively. The attacker Eve has full control over an IRS which is part of the wireless propagation channel between Alice and Bob. Eve is capable of applying custom configurations to the IRS at update rates comparable to the symbol rate used by Alice and Bob. Apart from that, we grant the attacker basic wireless eavesdropping capabilities, i.e., the attacker possesses a wireless receiver and can
receive and demodulate signals of Alice and Bob. However, Eve does not have a wireless transmitter and thus cannot transmit any signals on itself.

Finally, our system and attacker model is illustrated in Fig. 1. Note that the attacker operates at the physical layer and therefore we do not need to take the cryptography applied at the upper layer of the user’s communication into account.

**Attack and overview of investigation.** In the ERA, the attacker Eve uses a software-controlled surface, i.e., an IRS, to rapidly vary the wireless radio channel between Alice and Bob. This yields fast and instantaneous variations in the legitimate signals that normally would not occur in nature. Disturbed by the anomalous signal behavior, the intended receiver fails to correctly demodulate the incoming signals, leading to a denial of service. In this work, we design an ERA against OFDM communications by rapidly toggling between two distinct IRS configurations. An illustration of the corresponding attacker action is shown in Fig. 2. Compared to classical jamming attacks, the ERA allows attackers to silently disable the wireless communications of victim parties, i.e., the attacker does not actively generate a jamming signal. Instead, it manipulates signals transmitted by Alice and Bob during propagation.

We begin our investigations by examining the fundamental attack mechanisms in an analytical analysis (Section 5). Here, we lay the foundations of the attack and show that ERA-induced fast channel variations are harmful for wireless OFDM communication. We then turn to a simulation model (Section 6) of an end-to-end wireless OFDM link. From the simulation, we deduce several key factors of the attack, such as, e.g., signal power and attacker distances. For both theoretical analysis and simulations, we abstract the effect of the adversarial IRS as a time-varying signal component and omit the impact of specific IRS patterns. Finally, we use a practical IRS implementation to design and evaluate real-world ERAs to demonstrate successful jamming attacks (Section 7). In the first and simplest variant, we rapidly toggle the IRS patterns by either setting all elements to ’0’ or ’1’. This attack is of remarkably low complexity and requires nothing more than a certain proximity between the attacker and a victim party. The second attack variant is more advanced and includes an optional setup phase where the attacker optimizes the two IRS patterns to increase the jamming efficiency. This procedure incorporates the channel state information (CSI) from Alice and Bob, as provided by CSI feedback signals in existing wireless standards.

### 5 THEORETICAL ANALYSIS

In this section, we present a theoretical analysis of the mechanisms underlying the ERA against OFDM communications. We outline that the ERA affects channel equalization from outdated channel estimations and subcarrier orthogonality.

#### 5.1 Modelling Preliminaries

We begin our considerations by introducing the models for the legitimate OFDM communications and the IRS attacker.

##### 5.1.1 OFDM

We assume that Alice and Bob generate their RF transmit signals using a modulator fed by conventional complex-valued in-phase and quadrature (IQ) baseband signals [16]. The baseband signals for OFDM are generated by taking the inverse discrete Fourier transform of a block of $K$ complex modulated data symbols $X_k[n]$ for all $k = 0, \ldots, K - 1$ subcarriers, yielding the $n^{th}$ OFDM symbol. For instance, the data symbols contained in $X_k[n]$ may be modulated using, e.g., binary phase shift keying (BPSK) or quadrature amplitude modulation (QAM) of arbitrary order. Then, in the time domain, a cyclic prefix is prepended to each OFDM symbol. At the receiver side (see Fig. 3), after time- and frequency synchronization, removal of the cyclic prefix, and discrete Fourier transform, the received baseband signal on the $k^{th}$ subcarrier of the $n^{th}$ OFDM symbol in the frequency domain is given by:

$$Y_k[n] = H_k[n] X_k[n] + Z_k[n],$$

where $H_k[n]$ is the complex channel gain of the link between Alice and Bob for the $k^{th}$ subcarrier, and $Z_k[n] \sim CN(0, \sigma^2)$ is additive white Gaussian noise (AWGN). Following the implementation of practical systems, we assume that (known) pilot symbols are transmitted with a preamble to allow channel estimation at the receiver side. The pilot symbols are populated on each of the $K$ subcarriers of the $n^{th}$ OFDM symbol (i.e., block-type pilot arrangement [11]) and allow Alice and Bob to obtain CSI using, e.g., a standard Least-Squares (LS) channel estimator:

$$\hat{H}_k[n] = \frac{Y_k[n]}{\overline{X}_k[n]} - H_k[n] = H_k[n] + Z_k[n] - H_k[n] = H_k[n] + Z_k[n].$$

The channel estimate then is used to equalize the subsequently received OFDM symbols:

$$\hat{X}_k[n] = \frac{Y_k[n]}{\hat{H}_k[n]}.$$  

##### 5.1.2 Intelligent Reflecting Surface

We now establish the model for OFDM wireless communication in the presence of an IRS. We assume an IRS consisting of $N$ identical sub-wavelength-sized elements, arranged in an array on a planar surface to reflect impinging waves with a programmable phase shift. The generalized reflection coefficient for the $i^{th}$ IRS element can be expressed as:

$$r_i = \alpha_i e^{j\phi_i} \quad i = 1, \ldots, N,$$

where we assume $\alpha_i = 1$ and $\phi_i \in [0, 2\pi)$. Note that the IRS used in the experiments in Section 7 is a binary phase-tunable IRS, i.e., then $\phi_i \in \{0, \pi\}$ and $r_i \in \{-1, 1\}$ which correspond to ’0’ and ’1’ states of the IRS control signal. Next, following the illustration in Fig. 1, we find an expression for the channel between Alice and Bob, taking the IRS contribution into account. Here we assume that
We now proceed to show how the fast channel variations invoked at subcarrier (cf. Fig. 1) leading to a symbol error of the link between Alice and the receiver (cf. Fig. 3) is the channel estimation that is mandatory between two IRS configurations changing the direct link between Alice and Bob which will likewise affect the channel equalization. A fundamental part of every OFDM system, we now strive to further explore the affects of channel variation depending on the source of channel variation depending on \( \theta \).

### 5.2 Analytical Analysis

We now proceed to show how the fast channel variations invoked by the ERA will impact OFDM wireless communication.

#### 5.2.1 Channel Equalization

A fundamental part of every OFDM receiver (cf. Fig. 3) is the channel estimation that is mandatory to equalize the received data symbols [9]. As previously outlined, operating an IRS allows the attacker to alter the wireless channel between Alice and Bob which will thus likewise affect the channel equalization.

We assume the non-IRS channel \( d_k \) is static and Eve switches between two IRS configurations \( r_i^{(0)} \) and \( r_i^{(1)} \), corresponding to the channels \( H_k^{(0)} \) and \( H_k^{(1)} \). Now consider the pilot symbols for channel estimation have been transmitted with the malicious IRS configured as \( r_i^{(1)} \). Using (2), the victim receiver obtains the following channel estimate:

\[
\hat{H}_k[n] = H_k^{(1)} + d_k = \sum_{i=1}^{N} c_{i,k} r_i[n] g_{i,k} + d_k,
\]

where \( c_{i,k}, g_{i,k}, d_k \in \mathbb{C} \), respectively, are the complex channel gains of the link between Alice and the \( i \)th IRS element, the direct link between Alice and Bob for the \( k \)th subcarrier (cf. Fig. 1).

For high SNRs, which is a reasonable assumption when using LS channel estimation, the symbol error is approximated by

\[
\epsilon_k[n] \approx X_k[n] \frac{H_k^{(1)} - H_k^{(0)}}{H_k^{(0)}} = X_k[n] \frac{H_k^{IRS,(1)} - H_k^{IRS,(0)}}{H_k^{IRS,(0)} + d_k}.
\]

The resulting expression in (9) tells us that the IRS-induced symbol error is proportional to (i) the transmitted symbol, (ii) the difference between the two IRS channels, and (iii) is inversely proportional to the direct channel contribution. Thus, the attacker can maximize its chance of causing a false symbol decision by producing a pair of IRS channels, e.g., \( H_k^{IRS,(1)} = -H_k^{IRS,(0)} \).

### 5.2.2 Intercarrier Interference

OFDM systems in general are susceptible inter-carrier interference (ICI) which is caused by a degradation of subcarrier orthogonality. ICI usually results from imperfections such as Doppler shifts, frequency offsets, and channel variations during an OFDM symbol period [9, 16]. We emphasize that the time-varying IRS used in the ERA will deliberately introduce rapid and instantaneous channel variations at sub-symbol timing resulting in substantial ICI. To model the ICI, (1) is modified to account for the interference \( H_{k,k'} \) from other subcarriers \( k' \neq k \) to the received OFDM signal on the \( k \)th subcarrier [9]:

\[
\hat{Y}_k[n] = H_k[n] X_k[n] + \sum_{k' \neq k} H_{k,k'}[n] X_{k'}[n] + Z_k[n].
\]

In Appendix A we show that if the ERA-induced fast channel variations are zero-mean over one OFDM symbol, the signal-to-interference ratio (SIR) on the \( k \)th subcarrier is given by

\[
\text{SIR}_k = \frac{S_k}{4 \text{IRS}^2} = \frac{|d_k|^2}{P_{\text{IRS}}},
\]

which means that the IRS does not contribute to the direct signal power \( S_k \), but the total power received from the IRS, \( P_{\text{IRS}} \), completely translates into ICI, \( I_{\text{IRS}} \), only. Most importantly, this result is valid even without any optimization of the IRS elements with respect to the channels of the legitimate parties.

### 6 SIMULATION RESULTS

After having analytically outlined the key mechanisms of the ERA affecting an OFDM system, we now strive to further explore the attack through simulations. We give comprehensive results, identifying attack parameters, including signal power, attacker distance, and IRS dimensions. Further, we show that the ERA leads to significant packet error rates (PER) and is way more efficient when compared with a classical jamming attack using noise signals.

As an example for general OFDM-based radio systems, we consider Wi-Fi here, since our experimental investigation following in Section 7 also builds upon Wi-Fi devices. As the underlying simulation environment, we choose the MATLAB WLAN toolbox [30] due to the availability of end-to-end simulation capabilities for the entire IEEE 802.11n physical layer, including channel coding and standard-compliant channel models. We summarize the essential
We investigate the victim PER performance as a function of the JSR for various MCS settings. Therefore, we assume the attacker signal power arriving at the receiver from the attacker. Although in the ERA case, we assume a noise-free channel.

Like traditional jamming attacks, the ERA is subject to link budget constraints. Thus, the attack efficiency depends on the signal power arriving at the receiver from the attacker. Although in the ERA the attacker does not generate a jamming signal itself, we can still define a jamming-to-signal ratio (JSR) as the ratio of IRS signal to direct (non-IRS) signal powers

$$JSR = \frac{P_{IRS}}{S} = \frac{\sum_{k} S_k}{\sum_{k} S_k}.$$ (12)

For our simulations below, we use the JSR to assess the attacker strength. As an indication for the attacker’s success, we leverage the PER.

### Table 1: Summary of the simulation parameters

| Component         | Parameter               |
|-------------------|-------------------------|
| Wireless standard | IEEE 802.11n            |
| Mode              | HT Mixed                |
| Bandwidth         | 40 MHz                  |
| MIMO channels     | 1                       |
| MCS index         | 0 - 7                   |
| Total packet duration | 92 $\mu$s              |
| Data symbol duration | 64 $\mu$s             |
| Channel Model     | Model D                 |
| Equalizer         | Zero forcing            |

### 6.1 Attacker Signal Power

Table 1: Summary of the simulation parameters

We investigate the victim PER performance as a function of the JSR for various MCS settings. Therefore, we assume the attacker signal power originating from the IRS to have constant power while periodically toggling the phase between 0 and $\pi$ at a rate of 30 kHz, as is the case when inverting the sign of all IRS reflection coefficients $r_i$. The legitimate receiver has a high SNR of 50 dB. We plot the PER results for MCS 0 - 7 (covering BPSK, QPSK, 16-QAM, and 64-QAM modulations on the subcarriers [41]) as a function of the JSR in Fig. 4. As expected, higher order modulations are more prone to interference from an ERA. The results also highlight that the ERA indeed is capable of producing error rates which render reliable wireless communication impractical.

To relate the ERA performance to classical noise-based jamming or signal power reduction attacks [29], we compare the attack against an SNR reduction. For the ERA, we now consider the legitimate receiver to have an otherwise noise-free channel. For the SNR reduction, we consider the IRS to remain static while the attacker now deteriorates the SNR by adding noise with power equivalent to the IRS signal strength during the ERA. We plot the PER simulation results in Fig. 5, which indicates that the ERA achieves considerably better jamming performance when compared to a noise jammer at the same power.

### 6.2 Channel Modulation Frequency

To fully characterize the ERA, we vary the IRS modulation frequency. We conduct the simulation for MCS indices 0 - 7 at an SNR of 50 dB for the channel between Alice and Bob and a JSR of $-10$ dB. We plot the PER simulation results in Fig. 6 against the IRS update frequency. For the MCS indices 0 and 1, we observe particularly lower PERs due to the more robust modulation parameters. Despite that, the PER clearly increases as a function of the modulation frequency for all MCS values. The increasing PER at lower modulation frequencies can be explained by the increasing probability of an IRS reconfiguration taking place during packet transmission. That is, the packet error rate resulting from an ERA with IRS pattern durations $T_{IRS}$ longer than the packet duration $T_p$ is upper bounded by $T_p/T_{IRS}$. As the PER for modulation frequencies above approximately 16 kHz reaches a plateau, we conclude that at least one IRS reconfiguration during transmission of the

---

Paul Staat, Harald Elders-Boll, Markus Heinrichs, Christian Zenger, and Christof Paar
6.3 Surface Size

We will now show that an ERA is feasible even for rather weak attacker configurations regarding the attacker distance and IRS dimensions. Previously, we have determined the JSRs necessary for the attacker to degrade the PER of Alice and Bob (see Fig. 4). Note that we define the JSR as the ratio of the signal power coming from the IRS and the direct (non-IRS) signal power. Thus, the attacker generally seeks to pick up sufficient power from the legitimate users. The attacker can either minimize the distance to one of the victim parties to minimize path loss or increase the IRS size. Although both strategies are suitable, we assume the attacker must maintain a minimum distance and also cannot increase the IRS size arbitrarily without raising suspicion. Hence, we derive a connection between JSR, attacker distance, and the surface size. For the parties, we assume the geometrical configuration shown in Fig. 7 (a). We start with the free-space path loss of the direct link between Alice and Bob [16], where the received power is proportional to

\[ L_d = \left( \frac{\lambda}{4\pi d_{AB}} \right)^2 \]

with the carrier frequency wavelength \( \lambda = c_0/f \). For an optimal surface configuration, the free-space path gain from Alice to Bob via the IRS is found by [32]:

\[ L_{IRS} = \left( \frac{A_{IRS}}{4\pi d_{AE}d_{EB}} \right)^2 \]

Assuming Alice and Bob use omni-directional antennas, the JSR becomes

\[ JSR = \frac{L_{IRS}}{L_d} = \left( \frac{A_{IRS} d_{AB}}{d_{AE}d_{EB}\lambda} \right)^2 \]

which allows us to link the surface area \( A_{IRS} \) to the JSR:

\[ A_{IRS} = \sqrt{JSR d_{AE}d_{EB}\lambda \over d_{AB}} \]

We use Equation (16) to plot the minimum IRS size required by an attacker to achieve a JSR of \(-10\) dB in Fig. 7 (b). We show the result as a function of the distance between Alice and Bob and for distances 1 m, 2 m, 10 m, and 20 m of Eve to Alice. Consider, for example, Alice and Bob are at a distance of 30 m and Eve is at a distance of 10 m to Alice. Then, an IRS size of only 0.19 m² is sufficient to achieve a JSR of \(-10\) dB, which results in a severe PER degradation for Alice and Bob.

7 EXPERIMENTAL EVALUATION

After having approached the ERA through theoretical analysis and simulations in the previous sections, we now proceed with a practical evaluation of the ERA. Therefore, we first describe our experimental setup comprising of a low-cost IRS prototype and commodity Wi-Fi devices. Furthermore, we demonstrate that the ERA is capable of severe link quality degradation, leading to a significant reduction in the effective wireless data throughput.
7.1 Experimental Attack Setup

In this section, we present our experimental attack setup consisting of a prototype IRS and two microcontrollers. We estimate the cost of the setup to be around 100 £.

7.1.1 IRS Prototype. As the essential part of a first exploration of the ERA in practical experiments, we use two low-cost IRS prototype modules (see Fig. 9 (a)) with 128 binary-phase tunable unit-cell elements in total, arranged in a 16 × 8 array on standard FR4 PCB substrate. The elements are rectangular patch reflectors on top of a ground plane. Attached to each element, there is a PIN diode which can switch a parasitic element to the reflector, allowing to shift its resonance frequency. Thereby, the reflection coefficient of each element can be individually switched between two states, i.e., a ‘0’ state and a ‘1’ state, by turning the control voltage to the reflector element either on or off. The unit cell circuitry and the reflector design are shown in Fig. 8 (a). The IRS prototype used in our experiments is optimized to achieve a 180° phase difference in the reflected wave for the ‘0’ and ‘1’ states (see Fig. 8 (b)), i.e., \( r_i \in \{-1, 1\} \) in (5).

7.1.2 IRS Modulation. As we strive for rather high IRS modulation frequencies, we drive the 128 IRS elements in parallel. Therefore, we connect each of the 128 control lines to a GPIO pin of two STM32F407 microcontrollers, allowing us to achieve IRS modulation frequencies of up to 1.6 MHz. The frequency and surface patterns used for the modulation are programmable from the host controller through an UART serial communication interface.

Like in the theoretical analysis and the simulations, cf. Section 6, we apply a simple binary surface modulation. That is, we periodically toggle between two IRS configurations and thereby maintain a low attack complexity. For instance, we switch between all 128 IRS elements either set to the ‘0’ or ‘1’ state. As discussed in Section 5, since \( r_i \in \{-1, 1\} \), this leads to switching between two channels \( H_{IRS, 0}(k) \) and \( H_{IRS, 1}(k) \), with \( H_{IRS, 0}(k) = -H_{IRS, 1}(k) \).

7.2 Wireless Throughput Measurement

We now demonstrate that the ERA is capable of significant throughput reduction in entire wireless networks. Therefore, we deploy a commercial off-the-shelf WLAN router to provide an IEEE 802.11ac network in an office space. We position the attacker setup strategically at the router with distances of 1 m and 2 m. We detail and summarize the setup in Table 2.

For the experiment, we use a laptop connected to the Internet via the Wi-Fi network to measure the effective end-to-end speed of
the connection [38]. We perform speed measurements without the ERA (the malicious IRS remains static) and with the ERA enabled (switching all IRS elements between ‘0’ or ‘1’ state). We repeat this procedure for a total of 37 positions distributed throughout the office space, as indicated in Fig. 10. We show the results of the throughput measurements in Fig. 11. Here we can see that the ERA leads to an average throughput reduction of 78 % and 40 % for the attacker at 1 m and 2 m distance to the router, respectively. Recall that the attacker does not actively emit any jamming signal to achieve this result. Furthermore, the attacker does not perform any kind of synchronization to the legitimate signals or optimization of the IRS configurations. Notably, the ERA also leads to substantial throughput reduction where the wireless channel between the client and the IRS is obstructed, i.e., in different rooms with walls in between. Thus, we conclude that the ERA is a scalable attack, allowing the attacker to slow down the wireless network at many different places.

| Table 2: Summary of the experimental setup |
|-------------------------------------------|
| Component | Parameter |
| Jammer | |
| Surface elements | 128 |
| Surface size | 40 cm × 16 cm, 0.064 m² |
| Operation frequency | 5.37 GHz |
| Modulation frequency | 5 kHz |
| Modulation type | All ‘0’ / all ‘1’ states |
| Wi-Fi | |
| Access point | Asus RT-AC59U V2 |
| Client | Dell Latitude 7490 Laptop, Intel Wireless-AC 8265 |
| Standard | IEEE 802.11n/ac |
| Frequency | Channel 64, 5.32 GHz |
| Bandwidth | 40 MHz |
| MIMO channels | 2 |

7.3 Systematic Packet Error Rate Measurement

We perform a second experiment to systematically assess the practical effectiveness of the ERA, aiming to obtain PER measurements similarly to our simulation result from Section 6.2. Therefore, we deploy single-board computers equipped with ath9k-based network interface cards (NICs) [45] for IEEE 802.11n Wi-Fi at the legitimate parties Alice and Bob. The NICs give us low level access to the Wi-Fi communication, i.e., we can transmit packets with defined length and MCS setting. Here, we use a 2x2 MIMO configuration with off-the-shelf Wi-Fi antennas. One of the parties provides a Wi-Fi network on channel 60 (at 5.300 MHz), allocating 40 MHz bandwidth. We place the attacker setup attacker at distance 2 m and 3 m in line-of-sight to Alice and Bob, respectively. The channel between Alice and Bob also has line-of-sight conditions. For the whole duration of the experiment, the propagation environment remains static apart from the adversarial IRS operation.

In our setup, Alice transmits 20000 packets with randomized payload data to Bob. For each transmission, we configure the payload size and the MCS setting. Similarly to the simulation, we adjust the payload size to always result in 9 entire OFDM symbols (data symbol duration 3.6 µs, packet duration 6.8 µs). On Bob’s side, we count the number of successfully received packets to finally obtain the PER. We plot the PER results as a function of the adversarial IRS modulation frequency in Fig. 13 (a). Also, we indicate the previously discussed upper PER bound given by \( T_p / T_{IRS} > T_p \). Essentially, our measurement with standard Wi-Fi NICs confirms our previous simulation results, showing that higher-order modulations are more susceptible to the ERA. However, instead of reaching a plateau, we observe a drop in the PER when increasing the IRS modulation frequency beyond 30 kHz. We believe that this effect is due to hardware imperfections on the IRS prototype which initially was not designed to operate at high modulation speeds. As evident from the results, the upper PER bound based on the timing parameters holds. However, despite the fixed packet time duration, it appears that our bound seems to be too optimistic for MCS values below 12. We attribute this to reduced synchronization efforts, i.e., the receiver will barely be affected by an IRS change during the packet’s preamble portion, reducing the effective ERA-sensitive packet length.

7.3.1 Surface Pattern Optimization. Thus far, we have tested the simplest ERA strategy where the attacker switches all surface elements periodically between the ‘0’ or ‘1’ states. However, this strategy can be further improved by matching the used IRS configurations to the wireless link under attack. Thus, the attacker may prepend its jamming operation with a setup phase in order to optimize the IRS configurations used during the subsequent ERA. The attacker therefore can incorporate eavesdropped CSI feedback of the victim parties to further enhance the attack efficiency. For a first demonstration, we design and test an adaptive optimization algorithm to find IRS configurations well-suited for the ERA. The intuition of the algorithm is to use the adversarial IRS for maximizing a dissimilarity measure between the pair of IRS-induced channel responses of the victim wireless link. Following our analytical analysis in Section 5, we expect this to improve the attacker’s success. Algorithm 1 outlines the procedure. The result are two IRS configurations \( r_0^{(0)} \) and \( r_1^{(1)} \). Note that we here denote the binary surface control settings (‘0’ or ‘1’) as a proxy for reflection coefficients.

The randomly chosen initial IRS configurations in Algorithm 1 are given below:
The result of the algorithm are the updated IRS configurations: $r_i^{(0)}$, $r_i^{(1)}$ for ERA. Start with random $N$-bit IRS configurations $r_i^{(0)}$, $r_i^{(1)}$; dissimilarity metric $d$; algorithm rounds $R = 2$; for $j = 0$ to $R$ do
  configure IRS as $r_i^{(1)}$;
  $ref^{(1)}$ ← $H_k(r_i^{(1)})$;
  configure IRS as $r_i^{(0)}$;
  for $i ← 0$ to $N$ do
    $ref^{(0)}$ ← $H_k(r_i^{(0)})$;
    $r_i^{(0)} ← r_i^{(0)} ⊕ 1$;
    update IRS element $i$;
    $ref^{(0)}$ ← $H_k(r_i^{(0)})$;
    if $d(ref^{(1)}, ref^{(0)}) > d(ref^{1}, ref^{(0)})$ then
      $r_i^{(0)} ← r_i^{(0)} ⊕ 1$;
      update IRS element $i$;
    end
  end
end

The result is a vivid example for the combination of inherent simplicity and possibilities of the IRS for previously infeasible attacks. By Alice and Bob, before and after running the adversarial IRS optimization algorithm.

Using the presented algorithm with the Euclidean distance as a dissimilarity metric and magnitude CSI information on the link between Alice and Bob, we obtain the adapted IRS configurations $r_i^{(0)}$ and $r_i^{(1)}$, the pair of channel responses as observed by Alice and Bob before and after the optimization in Fig. 15. Here, we can see that our procedure indeed is highly effective in providing distinct channel responses designated to be used in the ERA. Note that even though the reception for $|H_k(r_i^{(0)})|$ has improved after running the algorithm, the difference between the two channel states is maximized. The result is a vivid example for the combination of inherent simplicity and possibilities of the IRS for previously infeasible attacks.

Using the presented algorithm with the Euclidean distance as a metric and magnitude CSI information on the link between Alice and Bob, we obtain the adapted IRS configurations $r_i^{(0)}$ and $r_i^{(1)}$,
which we now use to conduct the ERA. We repeat the PER measurement experiment from the previous section and plot the results in Fig. 13 (b). Here it is evident that the optimization was able to improve the attacker efficiency. Now, even the robust BPSK modulation for MCS 8 exhibits a significant PER induced by the ERA. Further, the optimization has also led to substantially increased PERs for the remaining MCS values.

8 DISCUSSION
In this section, we discuss (i) the real-world applicability, (ii) the attacker capabilities, and (iii) reason about countermeasures and mitigation. Also, we give directions for future work.

8.1 Real-world Applicability
We assess the costs and complexity of an ERA to be low. Our results show that a sub \(100\,\text{€}\) attacker setup can have significant impact on the effective wireless throughput. Once an attacker possesses a functional IRS, only basic microcontroller programming is required to rapidly vary a number of logic signals controlling the IRS. Thus, the attack can be easily carried out by non-specialists. While the commercial availability of IRS devices is currently still limited, several companies [17, 31] are working on product-grade IRS implementations. Besides that, many IRS designs are publicly available and can easily be reproduced by others using cheap PCB assemblies. Instead of using an own IRS, an attacker could also hijack existing IRS infrastructure which may be deployed in future wireless networks [49], most likely already at strategically advantageous positions.

8.2 Attacker Capabilities
To conduct an ERA, the attacker’s IRS must be within the wireless propagation environment between the victim nodes. As wireless communication is inherently supposed to bridge distances this will not be a hurdle for an attacker. As discussed, the JSR is an important parameter bounding the attack performance. In order to improve its JSR, the attacker can choose a favorable position or increase the IRS size. Therefore, to compensate the small size of our IRS prototype, we have used rather short attacker distances in our experiments, which still represents a valid attacker model. Our simulation results show that sufficient JSR values are, in principle, still possible for higher attacker distances and surface sizes. However, this also reveals a limitation of ERA: the attacker is passive and cannot amplify the signals it reflects. Hence, as it is generally the case for wireless communications (and jamming), the attack is limited by the available link budget.

Our simulation results show the underlying relationship between JSR and PER. For this purpose, we have simplified the attacker’s signal originating from the IRS to a time-varying signal component from alternating the sign of the IRS reflection coefficients. Although finding a corresponding IRS configuration to meet a certain JSR is non-trivial, our practical tests tests show that even with a binary-phase tunable IRS and without optimized surface configurations, the ERA significantly disrupts the victim communication.

In Section 7.3.1, we have granted the attacker access to the CSI of Alice and Bob to demonstrate that an attacker can further optimize the IRS configurations used during the ERA. In an actual attack, the attacker would rely on eavesdropping CSI feedback, e.g., from the user to the base station. For instance, this is commonly used in IEEE 802.11 WLAN standards, 4G, and 5G to implement, e.g., transmit beamforming [14, 15, 23, 37]. Note that, in the standards mentioned, these signals are not encrypted.

8.3 Countermeasures
The ERA is based on an IRS within the channel between Alice and Bob. For the attack to work, a part of the transmitted signal must reach the receiver via the adversarial IRS. Due to the broadcast nature of wireless signal propagation, it is likely that an ERA cannot generally be prevented. The transmitter could use beamforming to diminish the attacker’s success, trying to minimize the signal power reaching the IRS. However, this requires a mechanism for attack detection and localization and an advanced attacker may even leverage beamforming to its favor by providing a preferred path via the IRS to the receiver. Since the interference signal produced in the ERA is correlated to the useful signal, it may also be possible to find signal processing-based countermeasures at the receiver side. However, we emphasize these considerations are speculative. Countermeasures, if they exist, cannot be implemented immediately in end-user equipment because the very low-level signal processing of radio transceivers is usually implemented in hardware or is not updatable.

Finally, to mitigate the attack, wireless communication systems could apply encryption of physical layer control channels, i.e., to prevent the attacker to obtain CSI feedback. However, this will not render the ERA infeasible, but would only impede an adversarial IRS optimization. Moreover, this requires drastic changes to protocols and such measures can likely only be implemented within future standards.

8.4 Future work
In this paper, we have presented a novel class of jamming attacks based on IRS-induced fast changes in the radio propagation environment of wireless communication parties. Naturally, this work only represents a very first exploration of the ERA and, more broadly, the IRS as a toolkit for practical wireless physical layer attacks. Therefore, our work may serve as a basis for future work studying, for example, the following aspects.

Improving the attack. We have provided first insights into the optimization of the IRS configuration for an ERA, demonstrating the potential for increased attack efficiency. The evaluation of improved optimization algorithms based on eavesdropping CSI feedback is left for future work. Also, future work should investigate non-binary surface modulation signals where the attacker uses more than two IRS configurations. Finally, there is room for hardware improvements to the attacker setup, perhaps through dedicated IRS designs for high modulation frequencies.

Attack detection and countermeasures. More work is needed to examine whether existing jamming attack detection and mitigation strategies, e.g., [18], can be adapted to the ERA. Also, we see a need to evaluate the possibility of signal processing based mitigation strategies that could be incorporated into future transmitter and receiver architectures.
Application to other modulations. We have outlined the ERA against OFDM communications, as it is the preferred modulation scheme for modern wireless communication systems, including Wi-Fi, 4G, 5G. Further studies should investigate the applicability of ERA to other modulation schemes.

9 CONCLUSION

In this paper, we have first used the IRS as a cost-effective attacker tool to accomplish physical layer attacks in wireless radio networks. Based on this observation, we introduce the Environment Reconfiguration Attack (ERA) as a novel wireless jamming attack primitive. Without actively emitting a jamming signal, the ERA allows an attacker to significantly reduce or even disable the wireless communication capabilities of victim parties. Our approach takes advantage of a time-varying IRS which we use to rapidly modulate the channel response of victim wireless communication parties. Using the widespread OFDM modulation as an example, we have shown that exceptionally fast and instantaneous changes in the radio propagation environment disturb radio receivers substantially. We have approached the ERA through analytical analysis, simulations, and experiments. Our work breaks down the fundamental attack mechanisms and determines important attacker requirements before demonstrating multiple experimental attacks on actual wireless networks.

Our work highlights that the IRS must be considered as a powerful attacker tool for physical layer attacks against wireless communications. The IRS is a striking example of how emerging technologies are causing attack taxonomies to shift as previously complex attacks become tractable.

ACKNOWLEDGEMENTS

This work was supported in part by the German Federal Ministry of Education and Research (BMBF) within the project MetaSEC (Grant 16KIS1234K) and by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States - EXC2092 CASA - 390781972.

REFERENCES

[1] Mamta Agwal, Abhinish Roy, and Navrati Saxena. 2016. Next Generation 5G Wireless Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 18, 3 (2016), 1617–1655.
[2] Jeffrey G. Andrews, Stefano Buzzi, Wan Choi, Stephen V. Hanly, Angel Lozano, Anthony C. K. Soong, and Jianzhong Charlie Zhang. 2014. What Will 5G Be? IEEE Journal on Selected Areas in Communications 32, 6 (2014), 1065–1082.
[3] Youness Arjoune and Saleh Faruque. 2020. Smart Jamming Attacks in 5G New Radio: A Review. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (Las Vegas, NV, USA). IEEE, 1010–1015.
[4] Venkat Arun and Hari Balakrishnan. 2020. EfoFocus: Beamforming Using Thous-

ands of Passive Antennas. In 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20) (San Francisco, CA). USENIX Association, 1047–1061.
[5] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini, and R. Zhang. 2019. Wireless Communications Through Reconfigurable Intelligent Surfaces. IEEE Access 7 (2019), 116753–116773.
[6] Emil Bjornson, Luca Sanguinetti, Henk Wymeersch, Jakob Hoydis, and Thomas L. Marzetta. 2019. Massive MIMO Is a Reality—What Is Next? Digital Signal Processing 94 (2019), 3–20.
[7] Jie Chen, Ying-Chang Liang, Yiyang Pei, and Huayan Guo. 2019. Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security. IEEE Access 7 (2019), 82599–82612.
[8] Jerry T. Chiang and Yih-Chun Hu. 2011. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. IEEE/ACM Transactions on Networking 19, 1 (2011), 286–298.
[9] Tzi-Dar Chiueh, Pei-Yun Tsai, Lai J.-Wei, and Tzi-Dar Chiueh. 2012. Baseband Receiver Design for Wireless MIMO-OFDM Communications (2nd ed). Wiley, Hoboken, N.J.
[10] T. Charles Clancy. 2011. Efficient OFDM Denial: Pilot Jamming and Pilot Nulling. In 2011 IEEE International Conference on Communications (ICC) (Kyoto, Japan). IEEE, 1–5.
[11] S. Coleri, M. Ergen, A. Puri, and A. Bahai. 2002. Channel Estimation Techniques Based on Pilot Arrangement in OFDM Systems. IEEE Transactions on Broadcasting 48, 3 (Sept. 2002), 223–229.
[12] Miao Cui, Guangchi Zhang, and Rui Zhang. 2019. Secure Wireless Communication via Intelligent Reflecting Surface. IEEE Wireless Communications Letters 8, 3 (2019), 1410–1414.
[13] Philipp del Hougne, Mathias Fink, and Geoffroy Lerosey. 2019. Optimaly Diverse Communication Channels in Disordered Environments with Tuned Randomness. Nature Electronics 2, 1 (2019), 36–41.
[14] ETSI. 2018. ETSI TS 138 214 V15.2.0. 5G; NR, Physical Layer Procedures for Data.
[15] Felix Girke, Fabian Kurtz, Nils Dorsch, and Christian Wietfeld. 2019. Towards Resilient 5G: Lessons Learned from Experimental Evaluations of LTE Uplink Jamming. In 2019 IEEE International Conference on Communications Workshops (ICC Workshops) (Shanghai, China). IEEE, 1–6.
[16] Andrea Goldsmith. 2005. Wireless Communications. Cambridge University Press, USA.
[17] Greenwave. [n.d.]. http://greenwave.com/ Accessed: July 30, 2021.
[18] 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.
[19] A. Gupta and R. K. Jha. 2015. A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access 3 (2015), 1206–1232.
[20] Wang Hang, Wang Zanji, and Guo Jingbo. 2006. Performance of DSSS against Repeater Jamming. In 2006 13th IEEE International Conference on Electronics, Circuits and Systems. IEEE, Nice, France, 858–861.
[21] Ke-Wei Huang and Hui-Ming Wang. 2021. Intelligent Reflecting Surface Aided Pi- lot Contamination Attack and Its Countermeasure. IEEE Transactions on Wireless Communications 20, 1 (2021), 345–359.
[22] Sean Victor Hur and Julien Perruisseau-Carrier. 2014. Reconfigurable Reflect- tarrays and Array Lenses for Dynamic Antenna Beam Control: A Review. IEEE Transactions on Antennas and Propagation 62, 1 (2014), 183–198.
[23] IEEE. 2013. Telecommunications and information exchange between systems Local and metropolitan area networks– Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Enhancements for Very HighThroughput for Operation in Bands below 6 GHz. Accessed: July 30, 2021.
[24] Nadjide Kaina, Matthieu Dupet, Geoffroy Lerosey, and Mathias Fink. 2015. Shap-

ing complex microwave fields in reverberating media with binary tunable meta-

surfaces. Scientific Reports 4, 1 (May 2015), 6693.
[25] Chrstos Laskos et al. 2019. A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems. Ad Hoc Networks 87 (May 2019), 1–16.
[26] Marc Lichtman, Roger Piqueras Jover, Mina Labih, Raghunandan Rao, Vuk Maro-

jevic, and Jeffrey H. Reed. 2016. LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. IEEE Communications Magazine 54, 4 (2016), 54–61.
[27] Marc Lichtman, Jeffrey D. Poston, Saiduhrar Amuru, Chowdhury Shabiriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed. 2016-01. A Commu-

nity Jamming Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks. In 2016 IEEE Security & Privacy. IEEE, Nice, France, 858–861.
[28] Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo. 2014. Real-

Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks. IEEE Communications Letters 18, 1 (2014), 110–113.
[29] 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 (Oct. 2020), 1663–1667.
[30] MathWorks. [n.d.]. WLAN Toolbox - MATLAB. https://www.mathworks.com/products/wlan.html Accessed: July 30, 2021.
[31] Metawave Corporation. [n.d.]. https://www.metawave.com/ Accessed: July 30, 2021.
[32] Ögecean Ozdogan, Emil Björnson, and Erik G. Larsson. 2020. Intelligent Reflec-
ting Surfaces: Physics, Propagation, and Pathloss Modeling. IEEE Wireless Communications Letters 9, 5 (May 2020), 581–585.
[33] Xilong Pei, Haifan Yin, Li Tan, Lin Cao, Dusit Niyato, and Dong In Kim. 2020. IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power. IEEE Wireless Communications Letters 9, 10 (Oct. 2020), 1663–1667.
[34] Richard Poiesi. 2011. Modern Communications Jamming: Principles and Techniques (2nd ed). Artech House.
[35] Christina Popper, Mario Strasser, and Srdjan Capkun. 2009. Jamming-Resistant Broadcast Communication without Shared Keys. In Proceedings of the 13th Con-ference on USENIX Security Symposium. USENIX Association, USA, 231–248.
We here derive the ICI arising from the ERA due to sub-symbol $k$ channel tap in time (sample) direction at the subcarrier offset $k - k'$.

While static channels do not result in any ICI, the frequency contents of the fluctuating channel response during the OFDM symbol yield crosstalk from offset subcarriers $k'$. Note that for the desired signal, i.e., $k' = k$, (17) yields the channel frequency response of the time-averaged CIR. During the ERA, the attacker switches between IRS surface configurations. Naturally, switching corresponds to abrupt changes within the channel response of Alice and Bob, and therefore we expect $H_I[k, n, k - k']$ to contain significant high-frequency terms. We now will continue showing that the ERA is capable of turning the complete signal power from the attacker to interference. We account for the attacker’s IRS by splitting the CIR into static direct (non-IRS) and IRS portions:

$$h_I[n, m] = h_{I,RS}[n, m].$$

Assuming that the attacker only affects a single channel tap $l = l_{IRS}$, the IRS-induced ICI is thus found from (17), omitting the non-IRS taps:

$$H_{I,RS}[n] = \frac{1}{K} H_{I,IRS}[n, k - k'] \cdot e^{-j2\pi l_{IRS} k'/K}$$

with squared magnitude given by

$$|H_{I,RS}[l, k']|^2 = \frac{1}{K^2} |H_{I,IRS}[n, k - k']|^2.$$  

For brevity and simplicity, we here consider the special case that the IRS is configured such that the sum of the IRS channel tap over one OFDM symbol is zero, namely

$$\sum_{m=0}^{K-1} h_{I,IRS}[n, m] = H_{I,IRS}[n, 0] = 0.$$  

Substituting this in (19) and setting $k' = k$ results in

$$H_{I,RS}[n] = H_{I,IRS}[n] = \frac{1}{K} H_{I,IRS}[n, 0] \cdot e^{-j2\pi l_{IRS} k'/K} = 0,$$

which means that the IRS channel tap does not contribute to the useful signal but to theICI only. Using (5), the signal power of the useful signal $S_k$ is thus given by:

$$S_k = |H_{I,RS}[n]|^2 = |H_{I,RS}[n] + d_k|^2 = |d_k|^2.$$  

Assuming that all data symbols $X_k[n]$ on different subcarriers and OFDM symbols are independent and using (20) and (22), the total ICI power due to the IRS is given by

$$I_{IRS} = \sum_{k=k'}^{K-1} |H_{I,RS}[n, k']|^2 = \sum_{k=0}^{K-1} |H_{I,IRS}[n, k']|^2 = \frac{1}{K} \sum_{m=0}^{K-1} |h_{I,IRS}[n, m]|^2,$$

where we used Parseval’s theorem for the DFT in the last step.

If the magnitude IRS channel tap is constant, i.e., the malicious IRS modulation results only in phase shifting, i.e., $|h_{I,IRS}[n, m]| = |h_{I,IRS}|$, this can be simplified further to:

$$I_{IRS} = \sum_{k=k'}^{K-1} |H_{I,RS}[n, k']|^2 = |h_{I,IRS}|^2 = P_{IRS},$$

which means that the total power received from the IRS, $P_{IRS}$, completely translates into ICI, only. Thus the signal-to-interference ratio (SIR) due to ICI on the $k_{th}$ subcarrier is given by

$$\text{SIR}_k = \frac{S_k}{I_{IRS}} = \frac{|d_k|^2}{|h_{I,IRS}|^2} = P_{IRS}.$$