RISENSE: Long-Range In-Band Wireless Control of Passive Reconfigurable Intelligent Surfaces

Sai Pavan Deram[*§], Marco Rossanese[†], Andres Garcia-Saavedra[†]
Syed Waqas Haider Shah[*], Vincenzo Sciancalepore[†], Joerg Widmer[*], Xavier Costa-Perez[†‡¶]
[*]IMDEA Networks Institute, [†]NEC Laboratories Europe, [‡]i2CAT, [§]Universidad Carlos III de Madrid, [¶]ICREA

ABSTRACT

Reconfigurable Intelligent Surfaces (RIS) are a promising technology for creating smart radio environments by controlling wireless propagation. However, several factors hinder the integration of RIS technology into existing cellular networks, including the incompatibility of RIS control interfaces with 5G PHY/MAC procedures for synchronizing radio scheduling decisions and RIS operation, and the cost and energy limitations of passive RIS technology. This paper presents RISENSE, a system for practical RIS integration in cellular networks. First, we propose a novel, low-cost, and low-power RIS design capable of decoding control messages without complex baseband operations or additional RF chains, utilizing a power sensor and a network of microstrip lines and couplers. Second, we design an effective in-band wireless RIS control interface, compatible with 5G PHY/MAC procedures, that embeds amplitude-modulated (AM) RIS control commands directly into standard OFDM-modulated 5G data channels. Finally, we propose a low-overhead protocol that supports swift on-demand RIS re-configurability, making it adaptable to varying channel conditions and user mobility, while minimizing the wastage of 5G OFDM symbols. Our experiments validate the design of RISENSE and our evaluation shows that our system can re-configure a RIS at the same pace as users move, boosting 5G coverage where static or slow RIS controllers cannot.

CCS CONCEPTS

• **Networks** → **Mobile networks**; **Wireless access points, base stations and infrastructure**; **Network reliability**.

ACM Reference Format:
Sai Pavan Deram[*§], Marco Rossanese[†], Andres Garcia-Saavedra[†], Syed Waqas Haider Shah[*], Vincenzo Sciancalepore[†], Joerg Widmer[*], Xavier Costa-Perez[†‡¶]. 2025. RISENSE: Long-Range In-Band Wireless Control of Passive Reconfigurable Intelligent Surfaces. In *The 23rd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '25), June 23–27, 2025, Anaheim, CA, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3711875.3729154

1 INTRODUCTION

Reconfigurable Intelligent Surfaces (RIS) are artificially designed structures that transform traditionally passive radio channels into programmable actuators, enabling the creation of smart environments. Their potential to introduce novel applications, such as coverage extension [1], localization [2], and security [3], has attracted the attention of both academia and industry [4], positioning RIS as a key enabler for 6G [5]. A RIS is, sensu lato, a planar structure populated with a large number of small, controllable *passive* reflecting cells that can adjust their electromagnetic response. By collectively tuning these elements, a RIS can programmatically alter the propagation behavior of impinging radio waves, e.g., to perform passive beamforming on reflected signals [6].

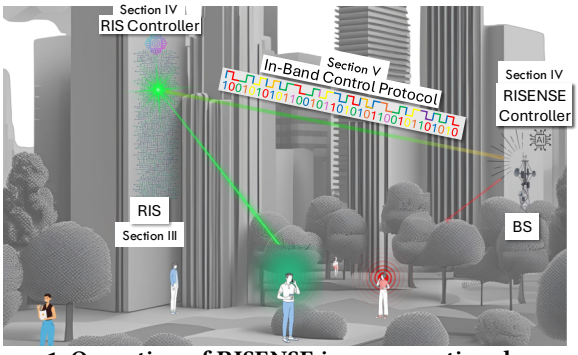


Figure 1: Operation of RISENSE in a conventional scenario. References to paper sections are embedded in the figure.

The advantages of a RIS over active alternatives such as pico-cells, relays, or the so-called active RIS [7] are significant. First, passive signal reflection eliminates the need for radio-frequency (RF) chains and baseband processors, resulting in drastically reduced hardware and energy costs, enabling off-grid deployments [8] and massive outdoor structures [9]. In contrast, active RIS uses baseband processors and RF chains [7]. Second, since a (passive) RIS does not involve active signal processing, it inherently supports full-duplex operation. Third, the absence of complex electronics makes the RIS lightweight and geometrically flexible, simplifying and reducing the cost of deployment and maintenance.

RISs can be designed on PCB using metamaterial or patch antennas [10]. Varactor diodes and liquid crystals offer continuous-range electromagnetic responses, but varactor diodes may introduce nonlinearities, and liquid crystals are temperature-sensitive and slow-responsive. PIN diodes and RF switches, in contrast, are more cost- and energy-efficient and can support high-resolution phase shifters [9], making the latter our baseline choice.

The problem. To date, the RIS literature has primarily focused on the reflective metasurface design [11–14] and on the optimization of the RIS configuration (e.g., via beam sweeping methods) [6, 15–18]. While such research demonstrates that RIS technology can enhance wireless coverage, *its integration into mobile systems has not been sufficiently studied.* Although 5G offers base stations (BS) significant flexibility to schedule radio resources, different users

MobiSys '25, June 23–27, 2025, Anaheim, CA, USA

ACM ISBN 979-8-4007-1453-5/25/06
https://doi.org/10.1145/3711875.3729154

Table 1: Technology candidates for wireless RIS control.

Technology$^{(i)}$	Power Consumption$^{(ii)}$	Range$^{(iii)}$	5G Integration$^{(iv)}$
LoRaWAN [22]	>18.6 mW	2 km	No
WiFi [21]	>5.15 mW	30 m	No
Bluetooth LE [21]	>4.25 mW	5 m	No
ZigBee [21]	>2.95 mW	11 m	No
Backscattering [23]	>100 μW	1 m	No
RISENSE	370 μW	>100 m*	Yes

$^{(i)}$ Typical technologies considered for low-power embedded systems.
$^{(ii)}$ Assuming a highly dynamic environment (see model in §6).
$^{(iii)}$ Maximum distance at which it provides a robust signal in real environments.
$^{(iv)}$ 5G integration enables synchronization between 5G MAC layer decisions and RIS state, which is required to preserve the optimum RIS configuration in dynamic settings.
*For a 10x10 RIS (see §3); range can be extended with larger surfaces.

require distinct RIS configurations for optimal performance. Consequently, *the RIS state must be synchronized with the BS's MAC/PHY scheduling decisions, which requires tight 5G/RIS integration.*

Most existing RIS designs employ wired control interfaces (typically via USB [11, 12]) to achieve fast RIS control. However, this approach has two major drawbacks: (*i*) they are hard to integrate into real-time MAC/PHY procedures in the BS, and (*ii*) cabling costs can be prohibitive for outdoor deployments. These limitations make wireless control a prerequisite for practical RIS deployments.

Current wireless RIS control solutions rely on out-of-band technologies, such as visible light communication [19], modulated infrared signals [20], Bluetooth [12], or even WiFi [21]. However, like its wired counterpart, this approach lacks integration with 3GPP-compliant BSs and introduces additional problems: (*i*) they need additional hardware, increasing cost, (*ii*) they need additional baseband processing, increasing latency and energy consumption to process RIS control messages, and (*iii*) most are not suitable for long-range control in outdoor scenarios. Table 1 compares different technologies that can be used for wireless RIS control.

Our solution. Our objective is to *design a system that enables a long-range, real-time, wireless RIS control interface*[1] *while (i) maintaining the cost- and energy-efficiency of passive RIS technology, i.e., with no baseband processors or full RF chains, and (ii) ensuring seamless integration with 5G's MAC/PHY procedures in the BS*, as depicted in Fig. 1. Achieving such a goal involves a number of challenges.

Challenge 1 (Passive control receiver). The first challenge is enabling a RIS to decode wireless control messages without sacrificing its passive nature. We address this challenge with a novel design, introduced in §3, which extends basic RF switch-based RIS approaches with two innovations.

First, we integrate a low-cost, energy-efficient power sensor to decode simple amplitude-modulated (AM) signals. This eliminates the need for complex baseband processors or RF chains. Second, we design a network of microstrips and couplers that merge and route RF signals from individual RIS cells to the power sensor. This network is engineered to introduce specific phase shifts in each unit cell, ensuring that signals combine constructively at the power sensor to maximize the RISENSE's signal-to-noise ratio (SNR).

Although the power sensor employs active electronic components (in line with the related literature [24]), these elements have minimal energy consumption, and enable the RIS to decode AM-modulated control messages without requiring full RF chains or complex baseband operations — a key requirement of passive RIS [7]. These claims are experimentally demonstrated in §6.

[1]Finding optimal RIS configurations (e.g., via beam sweeping) is out of the scope of this paper as is covered by abundant literature (see §7). In this paper, we focus on the much less studied problem of the RIS' control interface used to communicate and enforce such configurations, and its integration into 5G systems. We discuss RISENSE's support for beam sweeping/tracking mechanisms in §8.

Table 2: 5G NR Numerology

Numerology μ	Subcarrier spacing (KHz)	Symbol duration (μs)	CP duration (μs)	Max BW (MHz)
0	15	66.7	4.7	50$^{(1)}$
1	30	33.3	2.3	100$^{(1)}$
2	60	16.7	1.2/4.13	100$^{(1)}$/200$^{(2)}$
3	120	8.33	0.59	400$^{(2)}$
4	240	4.17	0.29	400$^{(2)}$

$^{(1)}$ sub-6GHz bands. $^{(2)}$ mmWave bands.

Challenge 2 (Long-range in-band control channel). The second challenge is to unlock a 3GPP-compliant 5G BS to emit RIS control messages *in-band*, exploiting its own 3GPP New Radio (NR) wireless interface. An in-band RIS control mechanism offers two advantages: (*i*) seamless integration with the BS's MAC/PHY scheduling procedures, which allows tight synchronization between RIS and BS, and (*ii*) long-range RIS control by leveraging the transmission power of standard 5G NR data channels.

To achieve this, we draw inspiration from cross-technology communication (CTC), which facilitates interoperability across technologies [25]. We propose embedding AM RIS control commands directly into standard orthogonal frequency division multiplexing (OFDM)-modulated 5G NR data channels, making them decodable with the RIS power sensor. This technique, detailed in §4, allows a 5G BS to exert agile wireless RIS control without major modifications to its data processing architecture.

Challenge 3 (RIS control protocol). Finally, to ensure the aforementioned system's effectiveness, we address the challenge of designing a BS-to-RIS control protocol that minimizes overhead (caused by OFDM NR symbols used for RIS control instead of data) while maximizing RIS control reliability (minimizing losses in RIS control messages). This is particularly challenging due to the lack of strict time synchronization between the RIS and the 5G BS.

To address this, we develop a protocol, detailed in §5, that achieves soft synchronization by exploiting three RIS operating modes: (*i*) full reflection mode, maximizing end-user performance; (*ii*) full sensing mode, maximizing RIS control reliability; and (*iii*) a hybrid mode, using a subset of cells for sensing while the rest remain in reflection mode. This hybrid mode enables soft synchronization and schedules RIS control messages without fully sacrificing user capacity, thereby minimizing overhead.

We name our solution to these challenges RISENSE. We follow an experimental-driven design principle that empirically validates our choices. Specifically, in §6, we validate the feasibility of implementing RISENSE using low-cost, low-energy components integrated into the RIS. Furthermore, §6 also demonstrates RISENSE's ability to re-configure an RIS at the same pace as users move, with negligible overhead, even at vehicular speeds.

2 BACKGROUND

We begin by presenting the requisite background on RIS technology (§2.1) and 5G New Radio (§2.2) for the development of RISENSE.

2.1 An overview of RISs

RISs are engineered structures designed to manipulate the behavior of impinging radio waves. By adjusting its configuration, an RIS can

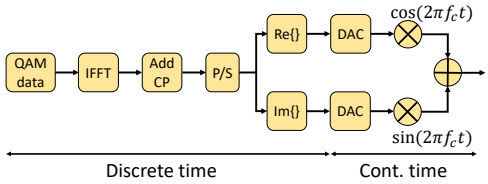


Figure 2: OFDM Transmitter

control the direction and other properties of the reflected waves. RISs are typically passive in terms of signal processing, i.e. they do not involve RF chains, amplification, or digital signal processors. Although often referred to as "passive" in the literature because they do not amplify or regenerate the signal before retransmission [7], they do require a small amount of power for control [11]. In contrast, an active RIS can amplify the signal before retransmission, perform complex baseband operations or include full RF chains, but at the cost of increased energy consumption [26].

RISs can be implemented using various types of surface, ranging from highly sophisticated metasurfaces to arrays of antennas used as reflectors. A metasurface is composed of metamaterials, a type of material engineered to exhibit properties not found in natural materials. They typically consist of arrays of small metallic or dielectric elements whose behavior can be externally controlled. Although complex to construct, they can unlock numerous features [27].

Alternatively, an array of passive reflecting elements, such as small metallic patches, can be used to reflect incoming radio waves in a specific direction. This property is usually achieved by adapting conventional beamforming techniques, where individual reflecting elements passively apply appropriate phase shifts to the reflected signals. More precisely, each *unit cell* includes a reflecting antenna and a phase shifter, the key component responsible for applying the desired phase delay. Different technologies, such as RF-switch, PIN-diodes, varactors, etc., can be employed to perform this task and each of them has its strengths and weaknesses, as discussed in [28]. Hence, by correctly configuring each unit cell, the reflection contribution from each of them can constructively interfere in the desired direction while canceling each other out in other directions, creating a phenomenon called *passive beamforming*.

2.2 A primer on 5G New Radio (NR)

New Radio (NR) is the PHY/MAC interface for 5G BSs. It employs OFDM with cyclic prefix (CP) with a flexible *numerology* μ [29]. The basic spectrum unit is the resource block (RB), consisting of 12 subcarriers with $15 \cdot 2^{\mu}$ KHz spacing. Time is divided into 1-ms subframes, each carrying 2^{μ} slots with, usually, 14 $66.7 \cdot 2^{-\mu} - \mu$s OFDM symbols. Some examples are depicted in Table 2. Every transmission time interval (TTI), often one slot, the BS's MAC schedules one transport block (TB) for/from every active user. The amount of bits carried in a TB depends on the numerology, the BS' bandwidth, the amount of buffered data, the BS' policy to schedule available RBs, and their modulation and coding scheme (MCS) that, in turn, depend on the channel SNR.

The transmission chain of an OFDM signal is illustrated in Fig. 2. An OFDM signal is composed of K sinusoids, also known as bins, with a spacing denoted as f_k. These sinusoids are modulated by data symbols that have a duration of T_s, which is equal to the reciprocal of the subcarrier spacing. Data is modulated into a complex data symbol block $\mathbf{S} = \left[s_0, s_1, \ldots, s_{K-1}\right]^T$. Each element s_k represents

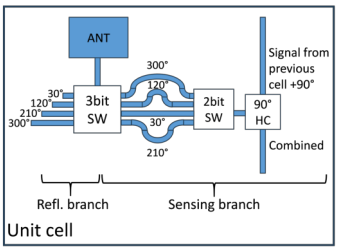


Figure 3: RISENSE unit cell.

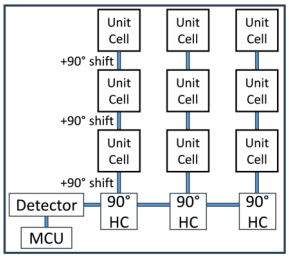


Figure 4: RISENSE board.

a quadrature amplitude modulated (QAM) symbol, where $s_k = a_k + jb_k$, with a_k and b_k being the real and imaginary parts of the symbol, respectively. This data symbol block $\mathbf{S}$ is then fed into an K-point inverse fast Fourier transform (IFFT) operation, resulting in discrete time-domain samples represented as

$$x[q] = \sum_{k=0}^{K-1} s_k \cdot \mathrm{e}^{j \cdot \frac{2\pi}{K} \cdot q \cdot k}, \; q = 0, 1, \ldots, Q-1. \tag{1}$$

The samples to be transmitted are passed through a parallel-to-serial (P/S) converter, and then a CP of duration T_{cp} is inserted, i.e., the last L samples in $\boldsymbol{x}$ are copied and placed as the first L samples:

$$\boldsymbol{u} = \left[x[Q-L-1], \ldots, x[q-1], \ldots, x[0], \ldots, x[Q-1].\right]$$

The baseband samples with the cyclic prefix are then divided into phase and quadrature components and fed to the digital-to-analog converter (DAC) to generate continuous-time waveforms $s_I(t)$ and $s_Q(t)$, respectively. Finally, these waveforms are up-converted to the carrier RF (f_{rc}) and added to generate the passband signal:

$$s(t) = \text{Re}\left\{s(t)\mathrm{e}^{j2\pi f_{\text{rc}} t}\right\} = s_{\text{I}}(t)\cos(2\pi f_{\text{rc}} t) + s_{\text{Q}}(t)\sin(2\pi f_{\text{rc}} t). \tag{2}$$

3 PASSIVE RIS CONTROL RECEIVER

Our goal is to augment conventional RIS capabilities with the ability to estimate incident power. This sensing capability is essential for decoding AM signals carrying RISENSE messages as shown in §4.

MARISA [24] and ARES [8] have a similar requirement to locate users. However, they both assume that the received power can be split between reflection and sensing. While this enables concurrent RIS operation and sensing, it significantly reduces SNR (see more details in §7). Instead, we propose a time-switching approach between RIS operation and sensing, which trades off a small number of radio resources for increased SNR (see §5).

3.1 Design

We extend a basic RF switch-based RIS design [11] by incorporating a mechanism that enables each unit cell to transition between *reflection* and *sensing* modes. As depicted in Fig. 3, each unit cell comprises a patch antenna, 3-bit and 2-bit RF switches, and an RF combiner. The patch antenna is designed for maximum gain within a 100 MHz bandwidth centered at 5.3 GHz. The 3-bit RF switch controls two sets of output ports, used to set each unit cell to either:

- **Reflection mode:** This is the conventional mode of a unit cell in an RIS. In the reflection branch, the first set of output ports of the 3-bit RF switch connects to four open-ended delay lines of varying lengths, enabling the reflection of impinging waves with four distinct phase shifts, enabling 2-bit phase shifting. This resolution could be easily raised with a higher-resolution RF switch.

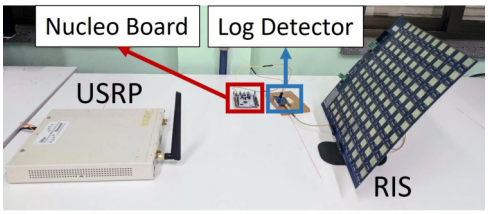


Figure 5: Experimental testbed components.

- **Sensing Mode:** This mode is used to retrieve RIS configuration commands wirelessly. In the sensing branch, the second set of output ports of the 3-bit switch uses four additional delay lines to connect to the 2-bit RF switch. Each unit cell's sensing branch terminates in a 90° hybrid coupler (90HC), enabling the merging of signals from all unit cells. As depicted in Fig. 4, this combined signal is then fed into a log detector, which measures its envelope, and subsequently to an analog-to-digital converter (ADC) sampling at 5.3×10^6 samples per second (Msps). The microcontroller unit (MCU), already responsible for configuring each RF switch, can readily process these samples for AM demodulation concurrently, as described in §4. Each delay line in the sensing branch introduces a different phase shift, which, when optimized, maximizes SNR at the log detector, similar to how beamforming maximizes SNR for end users in reflection mode.

This approach allows each RIS unit cell to be configured for either reflective beamforming (the conventional operation of a RIS) or power sensing (for RISENSE operation), and preserves the passive nature of the RIS as the only active electronic components are used for RIS control with minimal footprint (see §6). However, unit cells in sensing mode compromise communication capacity, as fewer antennas contribute to beamforming. To mitigate this overhead, §5 presents a time-switching protocol designed to maximize network capacity while ensuring a high rate of RIS reconfiguration.

3.2 Testbed

Our testbed is depicted in Fig. 5. For reflection mode, we replicate the prototype of [11], with individual boards of 10x10 patch antenna elements that can be connected to create larger reflective surfaces, and 3-bit phase shifters. To implement RISENSE's sensing branch, we employ an STM32 Nucleo Board equipped with STM32L476RG, a low-power MCU (Arm Cortex-M4 with FPU, 1 MB flash, 128 KB SRAM, up to 80 MHz) and an AD8318 low-power RF logarithmic detector [30]. The AD8318 functions as an envelope detector, producing a DC output voltage that linearly decreases with the amplitude of the RF input signal. We also use a USRP X310, generating 5G NR-compliant OFDM symbols using GNU Radio and a dipole antenna to radiate the signals.

No RF chains or baseband processors have been added to the RIS. To validate RISENSE's capability to decode incoming RIS control signals, we use the USRP to generate AM-within-OFDM signals as explained in §4 via GNU Radio, while the AD8318 log detector, mounted on an ad-hoc PCB board for RIS control, samples the signals. The detector's output is wired directly into the Nucleo Board's successive approximation register (SAR) ADC, which offers fast conversion times (12-bit resolution at 5.3 Msps with an 80 MHz board clock). This setup enables the acquisition of a high-fidelity digital representation of the envelope transmitted by a 5G BS' data channel, while requiring very low energy (see §6).

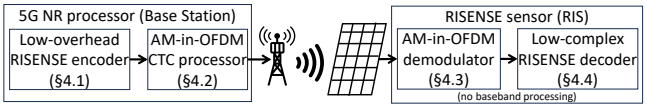


Figure 6: RISENSE's in-band wireless control interface.

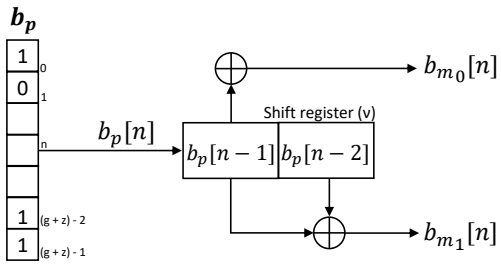


Figure 7: RISENSE encoding for $v = 2$ and $r = 1/2$.

4 IN-BAND RIS CONTROL INTERFACE

As shown in Fig. 6, RISENSE's in-band control interface comprises:
(*i*) A low-overhead encoder of RIS configurations (§4.1);
(*ii*) An AM-within-OFDM cross-technology-communication (CTC) scheme that embeds AM signals into 5G NR's data channel for seamless *in-band* RIS control of *passive* RISs (§4.2);
(*iii*) An AM-in-OFDM demodulator that leverages the sensing capabilities of RISENSE (§4.3); and
(*iv*) A low-complex decoder of RISENSE messages at the RIS (§4.4).

4.1 Encoding RIS control messages

The duration of every RISENSE message is 72 μs, corresponding to one 5G OFDM symbol plus a 4.7 μs cyclic prefix (CP), during which we can encode M_{ctrl} bits. Note that, due to the CP, one bit from the end of the symbol appears at the beginning of the AM waveform.

To minimize control signaling overhead, we employ a codebook approach. The RIS and the BS maintain an identical lookup table, C, which contains a predefined set of C RIS configurations. This codebook serves as a reference for both the RIS controller and the BS. Whenever the BS needs to reconfigure the RIS, it transmits a message encoding the corresponding codebook index, uniquely identified by a z-bit word $\boldsymbol{b}_s$.

To increase reliability, we employ two methods: CRC for error detection, and a convolutional code for forward error correction. To this end, we segment the bit stream $\boldsymbol{b}_s$ of each RISENSE control message into g equally-sized chunks, each followed by 1-bit CRC for error detection. This results in a $(g + z)$-bit sequence $\boldsymbol{b}_p$. A convolutional encoder then processes this sequence for forward error correction, producing a stream $\boldsymbol{b}_m$ of $M_{\text{ctrl}} = (g + z)/r$ parity bits that are encoded onto the carrier's envelope, where r is the code rate. This approach increases reliability without compromising the computing requirements of RISENSE decoder at the RIS.

In convolutional encoding, illustrated in Fig. 7, each input bit is convolved with generator polynomials to produce multiple output bits, enhancing communication reliability. The convolutional code is characterized by its code rate $r = (g + z)/M_{\text{ctrl}}$ (ratio of input bits $g + z$ to output bits M_{ctrl}) and constraint length v (memory of the encoder). A larger v generally leads to better error correction but increased complexity. The input bit stream is shifted into a length-v shift register, and its contents are convolved with generator polynomials to produce the output bit stream [31]. The output of the encoder $\boldsymbol{b}_m$ is then modulated for transmission.

4.2 AM-within-OFDM CTC processor

As mentioned before, our goal is to leverage the 5G NR data channel processing pipeline to subtly embed AM signals encoding RIS control messages. This cross-technology-communication (CTC) approach capitalizes on the fact that the 5G BS's PHY already manipulates the amplitude characteristics of each OFDM symbol. Thus, RISENSE's modulation-within-modulation technique can be achieved by strategically configuring the data bits within each sub-carrier of the 5G OFDM symbol, eliminating the need for additional hardware-based power control mechanisms, at the cost of 5G NR overhead that we strive to minimize in §5.

In AM modulation, the amplitude of a sinusoidal carrier signal is varied according to the instantaneous values of a modulating message signal. Mathematically, an AM signal is represented as:

$$a_{AM}(t) = A_c \cdot [1 + \psi(t)] \cdot \cos(2\pi f_{\text{rc}} t) \tag{3}$$

Here, $a_{AM}(t)$ represents the passband signal, and A_c denotes the amplitude of the carrier signal. Comparing Eqs. (2) and (3) reveals that, for our purposes, the key is to manipulate the baseband OFDM signal, i.e., $s_I(t) \cong \psi(t)$. The quadrature component can take a constant value, which only affects the signal's DC component and thus becomes irrelevant.

In this context, the choice of a modulation scheme $a_{AM}(t)$ is crucial to ensure efficient decoding at the RIS, which lacks a baseband processor. In this case, On-Off Keying (OOK) is an ideal choice due to its energy efficiency at the receiver. OOK enables non-coherent demodulation, eliminating the need for strict phase coherence, and places minimal demands on the receiver gain control and resolution. Therefore, we adopt the OOK modulation for RISENSE messages:

$$\psi(t) = \sum_{m=0}^{M-1} b_m \cdot p(t - mT_p).$$

In this equation, b_m represents message bits, $p(t)$ characterizes the shape of the transmitted pulse, T_p is the pulse width, and M denotes the total number of bits or symbols (we have 1 bit per symbol).

The discrete representation of the OOK signal becomes:

$$\psi[k] = \psi(t)|_{t=kT_s}, \ -\infty < k < \infty, \tag{4}$$

where T_s coincides with the sampling frequency of the 5G OFDM system, ensuring that the number of discrete samples matches that of the OFDM baseband signal in Eq. (1). Thus, to generate an AM signal within a 5G OFDM symbol with maximum demodulation performance, we seek to find optimal frequency-domain OFDM symbol that minimizes the mean square error between Eqs. (1) and (4), i.e.,

$$\min_{s_k} \quad \|\psi[k] - x[k]\|_2^2 . \tag{5}$$

This problem involves minimizing the difference between the OFDM and target OOK waveforms using a least-squares approach, which can be efficiently solved with standard tools. The resulting values are then quantized to the nearest element in the set $\mathcal{F}$, which represents a 1024-QAM constellation, to obtain an optimal feasible solution. This quantization process can be mathematically expressed as:

$$\hat{s}_k = f_q(s_k)$$

where $f_q(\cdot)$ projects s_k onto the closest element of $\mathcal{F}$.

Algorithm 1: Codebook Q generation (offline)

1. **Pulse design:** Select $p(t)$ s.t. $T_p \cdot M = T_s$
   (T_p: pulse width, M_{ctrl}: bits, T_s: OFDM symbol duration).
2. **foreach** $\boldsymbol{b}$ *in* C **do**
   a. **Ideal time domain signal:**
   $\psi(t) = \sum_{m=0}^{M-1} b_m \cdot p(t - mT_p)$
   b. **Sample** $\psi(t)$ **and take** K**-point DFT**:
   $\psi[k] = \frac{1}{K} \sum_{k=1}^{K} C_n e^{-j \cdot 2\pi \cdot k \cdot \frac{n}{N}}$
   c. **Solve** $\min_{s_k} \|\psi[k] - x[k]\|_2^2$
   d. **Save to codebook** $Q \leftarrow f_q(s)$

end

Now, instead of solving this problem online for every RISENSE RIS configuration command, which would incur additional computational burden at the BS, we exploit the fact that the entries of the codebook C and their associated identifiers are pre-determined to establish an additional codebook Q. Q is pre-computed offline with sub-carrier entries $\boldsymbol{s}$ that modulate each configuration in C. These entries consist of complex constellation symbols that are loaded during modulation to embed $\boldsymbol{b}_p$ onto the signal's envelope in a simple manner, as outlined in Algorithm 1.

Hence, during online operation, the BS simply needs to select an entry in C (RIS configuration) and then an entry in Q (pre-computed sub-carrier entries to modulate the RIS configuration), which can be implemented with low-complex look-up tables. Note that BS requires both codebooks C (RIS configurations) and Q (info to modulate each configuration), while the RIS only requires C, so memory requirements are also negligible.

4.3 AM-in-OFDM demodulation

At the RIS, the AM-within-OFDM signal can be sensed by the sensing branch of RISENSE described in §3 as

$$\mathbf{y} = \text{Re}\left\{ ab \sum_{l} \gamma_l \mathbf{x} + \mathbf{w} \right\},$$

where a and b denote the power gains provided by the BS and the RIS' sensing infrastructure, respectively. The term γ_l represents the complex path loss coefficient associated with the l^{th} path, and $\mathbf{w}$ is additive white Gaussian noise. The real part of the equation arises from the RIS envelope detector (see §4.2), which tracks the inherently real shape of the passband signal, where the RIS control information resides (see §4.2).

This has two advantages. First, the RIS does not need to shift the signal to the baseband, and no baseband processing is required. Second, this envelope is sampled by the ADC on the RIS MCU. Although 5G OFDM signals are typically sampled at 61.44 Msps, because the RIS control data reside on the envelope of the carrier signal, the RIS can demodulate the embedded AM signal at a much lower rate. Specifically, with a sampling rate of 5.3 Msps (see §3.2), we obtain $Q_{\text{RISENSE}} = \frac{5.3 \cdot 66.7}{M_{\text{ctrl}}}$ samples per RISENSE symbol (e.g., $Q_{\text{RISENSE}} \approx 22$ samples when $M_{\text{ctrl}} = 16$ RISENSE symbols), sufficient for demodulation. This low sampling rate allows us to avoid power-hungry electronics for demodulation.

4.4 Decoding RIS control messages

Then, to decode RISENSE messages, the sampled signal $y[q], \ \forall q \in \{1, \ldots, Q\}$, is divided into $M_{\text{ctrl}} + 1$ bins, and the values within each

Algorithm 2: RISENSE message receiver

a. Collect the samples from ADC represented as $y[q]$.
b. Divide $y[q]$ into $M_{\text{ctrl}}+1$ bins with $\bar{M}$ samples.
c. $\bar{y}^q = \sum_{m=1}^{\bar{M}} y[m],\ \forall q \in \{1,\ldots,M_{\text{ctrl}}+1\}$
d. thr $\leftarrow \frac{1}{Q}\sum_{\forall q} y[q]$
e. $\hat{b}_m = \begin{cases} 0, & \text{if } \ |\bar{y}^m - \text{thr}| < 0 \\ 1, & \text{otherwise} \end{cases}$
f. $\hat{b}_m \rightarrow$ Viterbi decoding
g. CRC check

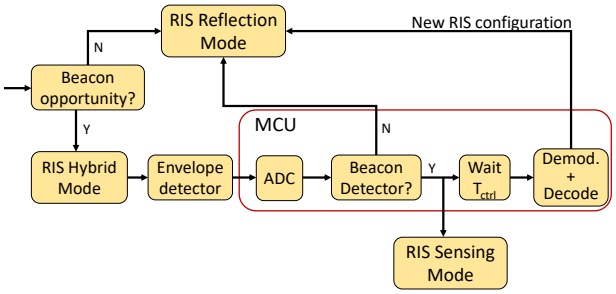


Figure 8: RIS workflow during beacon opportunities.

bin are averaged as $\bar{y}^m,\ \forall m \in 1,\ldots,M_{\text{ctrl}}+1$. The mean values $\bar{y}^m$ close to the noise floor are interpreted as 0, while those close to 1 are interpreted as 1. These bits, $\hat{b}_m$, obtained by hard thresholding, are an estimation of the encoded word and they are then decoded into a message sequence using the Viterbi algorithm [32].

In summary, the Viterbi algorithm is a dynamic programming method for convolutional codes that exhibits strong performance for small codewords, which is our case. By systematically evaluating all possible paths through the code trellis, the algorithm determines the most probable sequence of transmitted symbols. The computational time is primarily determined by the size of the trellis, $2^{(g+z)\nu}$, but the algorithm's recursive approach minimizes redundant calculations, making it well suited for resource-constrained environments like our RIS, as we empirically demonstrate in §6.

Finally, a CRC check verifies the decoded codeword. Algorithm 2 summarizes the steps described in §4.3 and in §4.4 so the RIS can retrieve the control information $\boldsymbol{b}$s.

5 RISENSE PROTOCOL DESIGN

The effectiveness of RIS technology is contingent on efficient and timely reconfiguration of their unit cells to adapt to changing channel conditions and user mobility. Since our control channel is in-band, as explained above, we need a low-overhead RIS control plane protocol that minimizes the use of 5G OFDM symbols and RIS unit cells that are not devoted to carry actual user data.

Naive methods, such as periodic polling, incur significant overhead, especially when frequent reconfigurations are unnecessary. Therefore, we propose a novel protocol designed to minimize overhead while maintaining the flexibility to reconfigure RIS *on demand*.

5.1 RISENSE protocol

RISENSE protocol employs two types of messages:

- **RIS control messages:** Messages encoding RIS configuration information as explained in §4.1.

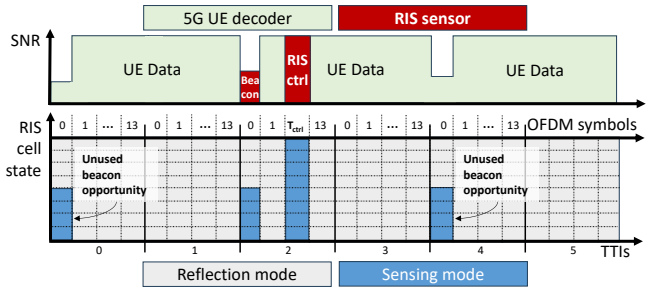


Figure 9: Example of RISENSE protocol for $T_{\text{bcn}} = 28$ OFDM symbol periods and $\alpha = 0.5$. Toy RIS example with 8 unit cells.

- **Beacon messages:** These predefined signals, transmitted by the BS, serve to schedule the arrival of RIS control messages and enable time synchronization. As detailed in §5.2, unlike RIS control messages, beacons require only detection at the RIS, not decoding, which reduces overhead.

We define T_{bcn} as the time interval between *beacon opportunities*, during which the BS can transmit a beacon. Fig. 8 illustrates the workflow triggered at the start of a beacon opportunity (time synchronization issues are discussed in §5.2). To minimize overhead, the RIS operates in a *hybrid mode* during beacon opportunities, where only a fraction α of its unit cells are set to *sensing mode* for beacon messages (which require only detection, not decoding). The remaining cells continue to operate in reflection mode, contributing to network capacity. These modes were introduced in §3.

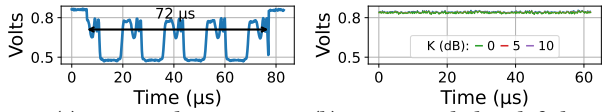
Since beacon opportunities are fixed over time, the BS can emit RISENSE commands at time $nT_{\text{bcn}} + T_{\text{ctrl}}$, where n denotes the beacon opportunity index and T_{ctrl} is the time required by the RIS to process the beacon (see §5.2). This includes the time required by the detector (§5.2) and switch all the unit cells to *sensing mode* to *reliably* receive and decode the subsequent RIS control message. Once an RIS configuration message is decoded, the RIS re-configures all its phase shifters accordingly and switches all unit cells back to *reflection mode*. If no beacon is detected, the RIS reverts to full reflection mode immediately, using the last received configuration.

Fig. 9 illustrates the protocol's operation using a toy 8-unit-cell RIS with $T_{\text{bcn}} = 28$ OFDM symbol periods and $\alpha = 0.5$. During unused beacon opportunities (the first symbol in TTIs 0 and 4), a fraction $1-\alpha$ remains in reflection mode, minimizing the impact on end-user SNR compared to polling mechanisms that would sacrifice all cells for sensing. Conversely, in TTI 2, the BS uses the first symbol (beacon opportunity) to schedule a RIS control message T_{ctrl} OFDM symbol periods later, prompting the RIS to switch all antennas to sensing mode for optimal RIS control message decoding.

This protocol offers two key advantages:

- With the hybrid mode, the impact of RISENSE beacon opportunities on network capacity is minimized, leading to a significant reduction in overhead compared to traditional polling methods.
- The protocol allows 5G BSs to trigger RIS reconfigurations *on demand* and at OFDM symbol granularity, making the RIS adaptable to varying channel conditions and user mobility.

Naturally, the effectiveness of RISENSE's protocol hinges on careful optimization of the parameters T_{bcn} and α, which we study in §6, but also on the RIS ability to detect beacons and synchronize in time with the BS, which we address next.



(a) RISENSE beacon. (b) OFDM symbol with fading.

Figure 10: RISENSE power sensor output.

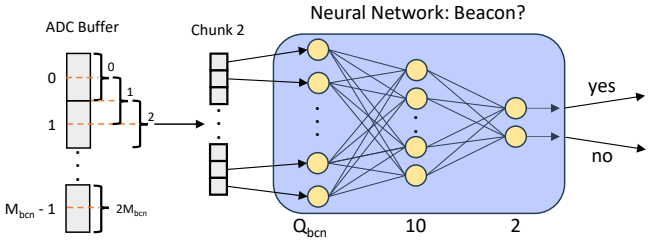


Figure 11: RISENSE beacon detection workflow.

5.2 RIS control beacons

As explained above, we employ beacons for both scheduling RIS control commands and synchronization. Beacon messages are transmitted by the BS using a similar AM-within-OFDM modulation approach as for RIS control messages (§4.2), i.e., we embed M_{bcn} AM-within-OFDM symbols within one 5G OFDM symbol.

5.2.1 Beacon detection. As shown in Fig. 10a, we employ an alternating stream of 1s and 0s as the beacon bit stream to facilitate detection. However, unlike control messages, *beacon messages only need to be detected as they do not carry actual information.* This allows us to use a smaller number of AM-within-OFDM symbols per 5G OFDM symbol, i.e., $M_{\text{bcn}} < M_{\text{ctrl}}$, increasing the number of samples per beacon and, thus, reliability. Moreover, AM-within-OFDM's longer symbol duration provides the envelope detector ample time to accurately track the envelope, aiding in differentiating the beacon from noise-like samples.

Conventional approaches for beacon detection, using convolutional filters or FFTs are impractical for two reasons. First, the RIS envelope detector produces only positive values, which makes convolution a monotonically increasing weighted sum, making beacon differentiation threshold-dependent. Second, they are computationally intensive ($O(M_{\text{bcn}}^2)$ and $O(M_{\text{bcn}} \log M_{\text{bcn}})$ complexity, respectively), requiring significant processing time on the RIS resource-constrained microcontroller unit (MCU).

Therefore, we need to resort to lower-complexity methods. Specifically, we exploit the fact that the low sampling rate of the envelope detector in our RIS design (see §3) effectively treats carrier-modulated signals as noise. This can be observed by comparing Fig. 10a (a RISENSE beacon) and Fig. 10b (a regular 5G NR symbol) when they are filtered by RISENSE's power sensor. Fig. 10b depicts results for channels with different levels of fading. To this end, we applied a Rician channel model with varying K factors: High K values indicate a low amount of fading, while $K = 0$ indicates Rayleigh fading; see [33]. More specifically, we used 3GPP's Pedestrian A (PED A) channel model [34, 35], with each tap parameterized with delays and average power equal to $\{0, 110, 190, 410\}$ ns and $\{0, -9.7, -19.2, -22.8\}$ dB, respectively. The low sampling rate of RISENSE's power sensor essentially acts as a filter that attenuates power variations caused by fading at carrier frequencies and removes information carried by OFDM symbols, resulting in a noise-like signal that is clearly distinct from RISENSE beacons.

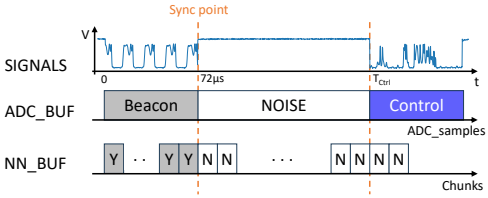


Figure 12: RIS synchronization and drift correction.

This observation motivates the use of low-complex functions for classification. Therefore, we utilize a tiny neural network (NN) illustrated in Fig. 11, trained offline for *beacon chunk detection* as follows. As explained in §4.3, our RIS sensor provides $Q_{\text{RISENSE}} = \frac{5.3 \cdot 66.7}{M_{\text{bcn}}}$ samples per RISENSE symbol (e.g., $Q_{\text{RISENSE}} \approx 22$ samples when a beacon contains $M_{\text{bcn}} = 16$ RISENSE symbols). Assuming time synchronization between RIS and BS (see §5.2.2), every OFDM symbol that potentially contains a beacon, we generate a chunk with $2 \cdot M_{\text{bcn}}$ overlapping symbols as described in Fig.11. Then, each chunk feeds an NN with a Q_{bcn}-neurons input layer (chunk size), followed by a 10-neuron fully connected layer with ReLu activation function, and a 2-neuron softmax layer to approximate the chunk detection distribution. Finally, to detect a beacon (with M_{bcn} symbols), we establish a simple rule: *a beacon is detected only if* $\frac{M_{bcn}}{4}$ *consecutive beacon chunks are detected.* This increases the reliability of our detector. This approach, based on a tiny NN requiring a few simple arithmetic operations ($10Q_{\text{bcn}} + 20$ multiplications and $10(Q_{\text{bcn}} - 1) + 18$ additions), proved to be effective and computationally inexpensive as we demonstrate in §6.

We train the NN offline, with a set of pre-generated beacons and 5G OFDM symbols with a wide range of SNR conditions, and using the Weighted Binary Cross-Entropy Loss functions

$$\mathcal{L}_{wBCE} = -\mathbb{E}[w_1 \cdot t_i \cdot \log(p_i) + w_2 \cdot (1 - t_i) \cdot \log(1 - p_i)],$$

a standard approach to train binary classifiers, where $\mathbb{E}$ is the expectation operator, w_1 and w_2 are weights, p_i is the softmax probability for the i^{th} class, and t_i is the truth value (0 or 1).

5.2.2 Time synchronization. Once a beacon is detected, the RIS shall prepare to receive a RIS control message in a time T_{ctrl}, as explained in §5.1. This requires time synchronization, as the MCU needs to initiate a countdown from the end of the beacon.

The design of the beacons and the architecture of RISENSE's RIS simplify this problem significantly. As shown in Fig. 10b, any signal other than beacons or RIS control messages is detected as *noise* by RISENSE (even 5G modulated data). This is because the sampling rate of RISENSE's detector is much lower than that of 5G. Therefore, measuring noise after a beacon detection indicates the beacon time boundary (and thus a 5G OFDM symbol boundary), which is used to correct the MCU's internal clock drift.

This is illustrated in Fig. 12. The outputs of the NN employed by RISENSE for beacon detection (§5.2.1) are stored in a binary buffer to record beacon occurrences. The MCU periodically analyzes the noise level within the ADC buffer to identify discontinuities, indicative of a signal of interest. Upon detecting a discontinuity, the MCU records the corresponding buffer index. This index enables the system to query the NN buffer, distinguishing between signals originating from RISENSE messages and other sources (e.g., 5G user data), as detailed in §5.2.1, and facilitates time synchronization. Given that each sample in the ADC buffer represents a fixed time

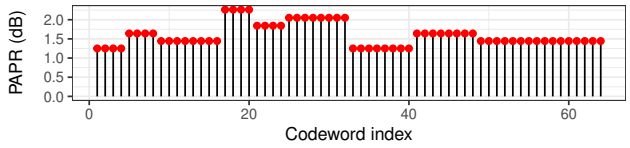


Figure 13: PAPR of each RISENSE codeword.

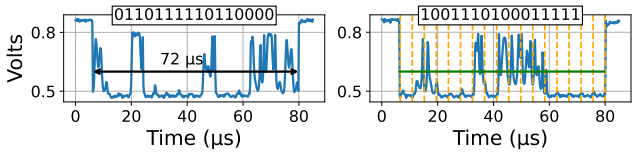


Figure 14: Examples of signal demodulation.

interval, the precise timing of the detected signal is determined by its buffer position. This synchronization point is used to predict the arrival of the next RISENSE message as the timings are known and to compensate for clock drifts relative to the base station clock, ensuring system-wide timing accuracy.

6 VALIDATION AND EVALUATION

The effectiveness of RISENSE hinges on careful optimization of several system parameters, indicated in Table 3, which we analyze in this section using the testbed introduced in §3. Without loss of generality, we employ 5G numerology $\mu = 0$, where each OFDM symbol spans $T_s = 66.7$ μs.

6.1 RISENSE control messages

We begin by evaluating the Peak-to-Average Power Ratio (PAPR) of RISENSE messages, as high PAPR can lead to signal distortion. Fig. 13 presents the measured PAPR of the signals modulating and encoding each RISENSE codeword. The results demonstrate that the PAPR is upper-bounded by 2.5 dB, indicating a sufficiently low value and validating our design [36].

Now, since our envelope detector's sampling rate is fixed at 5.3 Msps and $T_s = 66.7$ μs, the codeword length M influences the demodulator's performance. For instance, $M = 8$ yields 44 samples per RISENSE symbol, while $M = 36$ yields only 9 samples, potentially hindering detection. Using our testbed, we assess in Fig. 16 the soft-bit error rate (after demodulation, before decoding) as a function of SNR for a range of M values. To emulate different SNR conditions, we adapt the USRP's transmission power accordingly.

Excessively low SNR regimes result in a 0.5 soft bit error probability (equivalent to random guessing) regardless of M. Furthermore, even at higher SNRs, the demodulator exhibits non-negligible error probabilities when $M \geq 20$. Therefore, we consider $M_{\text{ctrl}} = 16$ a suitable trade-off between performance and RIS control data rate. Since $T_s = M \cdot T_p = 71.4$ μs, then $T_p \approx 4.17$ μs, i.e., 24 MHz of bandwidth. Fig. 14 shows two AM-within-OFDM signals with $M = 16$, demodulated in our testbed, with their corresponding codeword.

Table 3: RISENSE system parameters

Parameter	Details	Section
M_{ctrl}	RISENSE symbols per control msg. (§4.2, §4.3)	§6.1
ν	Parameter of RISENSE's encoder (§4.1, §4.4)	§6.1
z	RIS codebook C resolution (§4.1)	§6.1
g	CRC bits in control messages (§4.1)	§6.1
r	Conv. code's rate for control msg. (§4.1)	§6.1
M_{bcn}	RISENSE symbols per beacons (§4.2, §5.2)	§6.2
α	Sensing cells during beacon opps. (§5.1)	§6.2
T_{bcn}	Period of beacon opportunities (§5.1)	§6.3

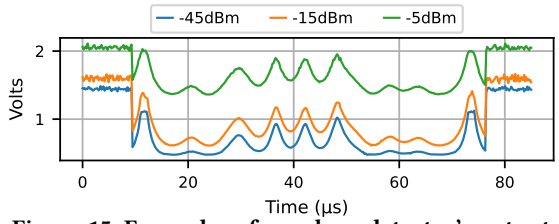


Figure 15: Examples of envelope detector's output.

Table 4: RISENSE empirical characterization for demodulation and decoding (§4.4), and for beacon detection (§5.2).

	Comput. time (μs)	Power consumption (mW)	Flash (kB)	RAM (KB)
Demod. ($M = 16$)	196 ± 0.1	49.76	19	14
Decoding	351 ± 0.8	50.16	24.5	2.5
Beacon detection	94 ± 0.5	47.87	35	5
Data reflection/idle	0	0.03	0	0

Although these signals appear below the noise floor, this is an artifact of the log detector's output, which is a decreasing linear-in-dB function of the RF input amplitude. Lower transmitted power at the detector results in a higher DC output noise floor, obscuring the signal. This effect is visualized in Fig. 15.

We now evaluate the MCU resource usage of both the demodulator and decoder, as summarized in Table 4. Our tests indicate that the demodulation process takes approximately 196 μs with minimal power consumption of (~49.8 mW), given $M_{\text{ctrl}} = 16$. In contrast, the decoder's processing time depends primarily on the constraint length ν, which determines the trellis size (see §4.1 and §4.4). Fig. 17 shows that this processing time scales exponentially with ν, exceeding 100 ms for $\nu = 5$ on our MCU. Given the limited size of RISENSE control messages ($M_{\text{ctrl}} = 16$) and these observations, we adopt $\nu = 2$, which, as shown in Table 4, requires approximately 351 μs and ~ 50 mW to process, allowing a maximum rate of approximately one RISENSE message every 550 μs. We analyze the overall system power consumption in §6.3.3.

Additionally, the decoder's error correction performance depends on the ratio r of information bits $(z + g)$ to message bits (M_{ctrl}). Since $g > 0$ (CRC bits) and $M_{\text{ctrl}} = 16$, the only feasible coding rate is $r = \frac{1}{2}$. However, the ratio between g and z (resolution of the RIS codebook C) remains to be determined. Fig. 18 depicts the empirical success rate of message decoding for $\nu = 2$ across a range of SNRs. The results indicate that $(z, g) = (6, 2)$ represents a suitable trade-off between error protection and information length, allowing for a codebook with up to $|C| = 2^6$ RIS configurations.

6.2 RISENSE beacons

Next, we analyze the impact of the number of RISENSE symbols per beacon on beacon detection performance. As explained in §5.2, beacon messages only require detection (no information is carried), allowing $M_{\text{bcn}} < M_{\text{ctrl}}$ to increase the number of samples per beacon symbol and improve detection reliability. Based on our earlier results (Fig. 16), we set $M_{\text{bcn}} = 8$, resulting in a RISENSE symbol duration of 8.325 μs and $Q_{\text{bcn}} = 41$ samples per symbol.

Beacons sent during beacon opportunities are detected at the RIS using the NN-based solution introduced in §5.2, trained on a 15k-beacon dataset with varying noise levels. 70% of the dataset is used for training (Fig. 19), and the remaining is used for evaluation (Fig. 21). Fig. 19 shows the training loss evolution, with a rapid initial decrease followed by a plateau as the model reaches 84%

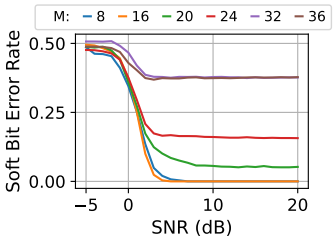


Figure 16: Design of RISENSE M_{ctrl}.

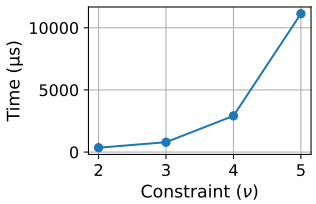


Figure 17: Viterbi decoding time as a function of ν.

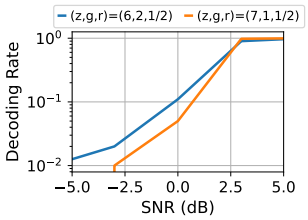


Figure 18: RISENSE control message decoding rate.

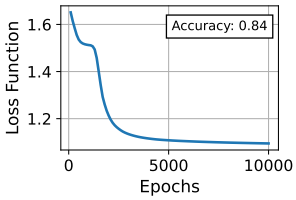


Figure 19: NN training reaching 84% accuracy.

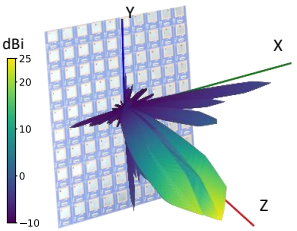


Figure 20: Empirical beam of our RIS prototype achieving 24.93 dBi gain in $(0°, 0°)$ (azimuth, elevation). Our empirical dataset is available in [37].

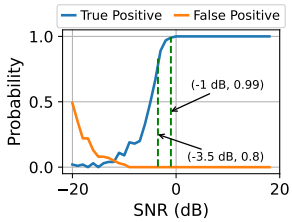


Figure 21: Beacon detection performance of the NN for different SNRs.

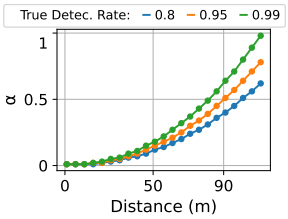


Figure 22: α required for our 10x10 RIS as a function of a macro-cell BS distance.

accuracy. Fig. 21 plots the ratio of true positive (blue) and false positive (orange) detections against SNR. These results characterize the minimum SNR required for beacon detection given target true/false positive ratios. Specifically, 0.8/0, 0.95/0 and 0.99/0 true/false detection probabilities require SNRs of −3.5, −2, and −1 dB, respectively.

The SNR experienced by RISENSE's beacons depends on two factors: the proportion of RIS cells dedicated to sensing during beaconing opportunities α and the BS-RIS channel conditions. However, higher values of α reduce the 5G network capacity for end-users. Therefore, for fixed BS and RIS locations (and thus a static BS-RIS channel), which is a reasonable assumption in cellular systems, a target SNR for beacons can be achieved by optimizing α.

To this end, we investigate the impact of the BS-RIS distance. We first empirically characterize the RIS reflection using our testbed (see Fig. 5). The resulting reflection pattern is illustrated in Fig. 20. We are interested in outdoor scenarios. Unfortunately, the 5G NR transmitter in our testbed (an USRP X310, see §3.2) only supports one antenna and a maximum transmission power of 20 dBm, which are much lower than conventional macro-cell BSs. Therefore, we emulate the presence of a macro-cell as follows. The received power at the RIS, expressed in decibels, can be approximated by $P_{\text{RIS}}^{[\text{dBm}]} = P_{\text{BS}}^{[\text{dBm}]} + G_{\text{BS}}^{[\text{dBi}]} + G_{\text{RIS}}^{[\text{dBi}]} - \beta^{[\text{dB}]}$ where G_{RIS} is the RIS gains (fitted with our experimental data), and $\beta^{[\text{dB}]} = -37.5 - 22\log_{10}(\frac{d}{1\text{m}})$ is the path-loss coefficient, calculated as in [38], where d is the BS-RIS distance. We assume a BS transmission power and antenna gain of $P_{\text{BS}} = 43$ dBm [39] and $G_{\text{BS}} = 15$ dBi [40], respectively.

Given the above, we analyze in Fig. 22 the fraction of RIS elements required for beacon detection, α, given d and different target true-positive detection probabilities (0.8, 0.95, 0.99). As expected, longer distances and higher true-positive ratios require higher values of α. For example, for our 10x10 RIS placed 80 m from the BS, $\alpha = 0.5$ is sufficient to guarantee a 0.99 beacon detection probability.

Finally, we validate the RIS MCU's capacity for RISENSE's beacon detection. We deploy the trained NN on the Nucleo Board's MCU using the STM32 X-CUBE-AI toolkit, a library for NNs optimized for computational efficiency and memory usage. This toolkit facilitates the conversion of pretrained NNs from popular frameworks like Keras and TensorFlow. As shown in Table 4, the MCU executes the beacon predictor in ∼94 μs with low energy consumption (∼4.5 mJ), validating the feasibility of our solution.

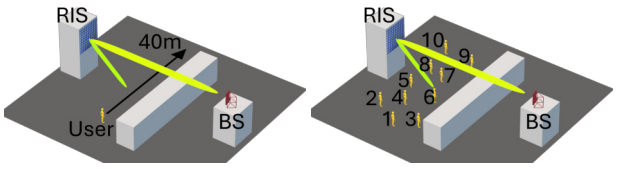
6.3 System evaluation

To evaluate RISENSE in real-world scenarios, we assess a mobility scenario (§6.3.1) and a multi-user scenario (§6.3.2). As in our previous analysis, we mix empirical RIS data from our prototype and a Rician model to model the BS-RIS and RIS-UE channels.

Specifically, the 5G NR data received by a user is given by $\boldsymbol{y} = \boldsymbol{hs} + \boldsymbol{w}$, where $\boldsymbol{h} = \boldsymbol{h}_d + \boldsymbol{h}_r \boldsymbol{\Gamma} \boldsymbol{H}_i$. Here, $\boldsymbol{h}_d$ corresponds to direct-path (BS to user) channel attenuated due to blockage, and $\boldsymbol{w} \in \mathcal{CN}(0, \sigma^2)$ is additive Gaussian noise. Importantly, the term $\boldsymbol{\Gamma}$, representing the RIS phase-dependent gains, is modeled directly using experimental data obtained from characterizing our physical RIS prototype testbed (see §3.2). These measurements capture the actual radiation patterns and gains for different phase configurations, including real-world hardware imperfections (see Fig. 20 for an illustrative example), forming a key component of our data-driven approach. The terms $\boldsymbol{H}_i$ and $\boldsymbol{h}_r$ represent the channel between the BS and the RIS and the RIS and the UE, respectively. We assume a realistic channel model comprising of line-of-sight (LOS) and non-line-of-sight (nLOS) paths characterized by a collection of channel scattering objects each generating a number of channel paths that are closely spaced in the angular domain [33, 38, 41].

We consider a macro-cell BS equipped with a 4×4 UPA antenna whose center is at coordinates $\pi_{\text{bs}} = [10, 10, 9]$ m, with a transmission power of $p_t = 43$ dBm [40], and our RIS positioned at coordinates $\pi_{\text{RIS}} = [60, 10, 9]$ m (50 meters away from the BS). The users are equipped with a single antenna and, when scheduled by the BS, we estimate their instantaneous capacity as:

$$C = P_{t/f} \log_2(1 + \frac{p_t}{\sigma^2} \tilde{\boldsymbol{h}}^{\text{H}} \tilde{\boldsymbol{h}}) + (1 - P_{t/f}) \log_2(1 + \frac{p_t}{\sigma^2} \boldsymbol{h}^{\text{H}} \boldsymbol{h}), \quad (6)$$



(a) Moving user. **(b) Multiple users.**

Figure 23: RIS-aided scenarios for evaluation.

where $P_{t/f} \in (0, 1)$ denotes whether RISENSE's RIS reconfiguration has been successful (i.e., whether RISENSE messages are successfully processed, see Fig. 21). If RIS reconfiguration is successful, then $\tilde{\boldsymbol{h}} = (\boldsymbol{h}_d + \boldsymbol{h}_r \tilde{\boldsymbol{\Gamma}} \boldsymbol{H}_i)$ becomes the effective channel after a delay incurred by the RIS to demodulate and decode the control message (see Table 4), where $\tilde{\boldsymbol{\Gamma}}$ corresponds to the updated RIS phase shifts. In case of beacon detection failure, the RIS continues using an outdated phase shift configuration $\boldsymbol{\Gamma}$. To minimize beacon detection failures, we select $\alpha = 0.25$ according to our earlier results in Fig. 22.

This data-driven approach provides credibility, as it is based on experimental data (i.e., it includes imperfect RIS reflection patterns, RISENSE overheads, and RISENSE processing delays) yet it is flexible enough to assess realistic scenarios. Finally, RISENSE and all benchmarks assume perfect BS knowledge of the user's location.[2] We consider three benchmarks:

- "No-RIS" represents a scenario without an RIS, where the users are served solely by the BS's direct link.
- "Static-RIS" emulates an RIS unable to reconfigure dynamically. Therefore, it uses a wide beam (120° in azimuth and 40° in elevation) to cover the user's entire trajectory.
- MARISA [24] or ARES [8], RISENSE's closest competitor, which, as explained in §7, enables RIS reconfiguration at only a second-level granularity (i.e., much slower than RISENSE).

All the results correspond to the average over 1000 independent monte-carlo realizations.

6.3.1 Mobile scenario. First, we study the 5G network capacity of a mobile user in a common scenario aided by RIS. The scenario we consider, illustrated in Fig. 23a, involves an obstacle that obstructs the direct link between a macro-cell BS and the user, with the user moving a distance of 40 meters.

In more detail, the user moves along a 40-meters linear track starting from coordinates $\pi_{\text{ue}} = [50, -10, 2]$ m to $\pi_{\text{ue}} = [50, 30, 2]$ m. We simulate different user velocities ranging from $v = 1.2$ m/s (walking speed) to $v = 15$ m/s (urban vehicle speed) and consider different obstacle attenuation levels corresponding to materials such as glass, wood, brick, and concrete [42]. Moreover, we assume that RISENSE uses every beacon opportunity (worst-case in terms of overhead), which means that two OFDM symbols every T_{bcn} are devoted for RISENSE's protocol and not for 5G NR data delivery.

Fig. 24 depicts the end-user 5G capacity as a function of the blockage attenuation. As expected, RISENSE with T_{bcn}=10 ms (the highest reconfiguration rate) maximizes network capacity, followed closely by RISENSE with T_{bcn}=100 ms. This performance is achieved because the RIS is reconfigured at the same pace as the user moves,

[2]Locating users or finding optimal beamforming configurations are classical problems with a vast amount of literature and are out of the scope of this paper.

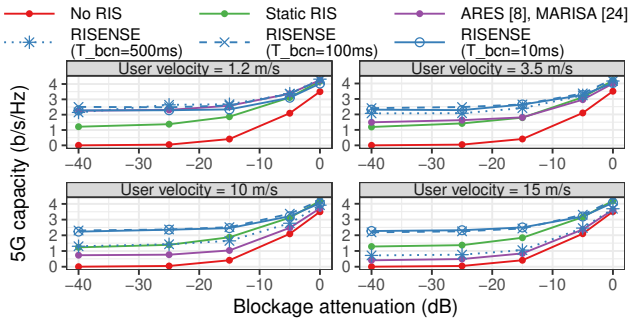


Figure 24: End-user 5G network capacity for a mobile user with different velocities in a RIS-aided scenario.

with narrow ~10° reflection beams, which provides a capacity boost that compensates the overhead RISENSE introduces to this end.

Reducing the reconfiguration rate with RISENSE (with $T_{\text{bcn}} =$ 500 ms), and especially with MARISA/ARES (second-level reconfigurability), leads to increased capacity loss as user velocity increases. This loss occurs because the RIS controller cannot reconfigure the RIS quickly enough to keep up with user movement. "Static-RIS" provides even lower capacity, as it must resort to a wide beam to cover all user locations during the user's trip. Finally, "No-RIS", which is served only by the BS's direct link, sacrifices network capacity when the attenuation caused by the blockage increases, as it is not aided by a reflecting surface. Notably, when the blockage attenuation diminishes, the BS' direct link dominates and all of the mechanisms achieve the same capacity.

6.3.2 Multi-user scenario. We now study a multi-user scenario as illustrated in Fig. 23b. The BS, RIS, and -40 dB blockage are positioned as before. Without loss of generality, we assume that the BS employs a round-robin radio scheduling policy, where NR symbols are granted to a distinct user every T_{sch} slots. It is important to note that RISENSE is agnostic to the BS's scheduling policy as, in contrast to alternative approaches, its in-band nature allows the RIS configuration to be synchronized with any policy. Fig. 25 depicts the overall 5G system capacity over 250000 slots as a function of the number of active users randomly placed as in Fig. 23b.

As expected, "No-RIS" underperforms, consistent with previous results. In contrast, RISENSE provides maximum capacity regardless of the number of active users in the system and the BS's scheduling policy (illustrated by T_{sch} in this case), as RISENSE can reconfigure the RIS in synchronization with the BS's scheduling decisions. Note, however, that as T_{sch} decreases, more frequent RIS reconfigurations are required, and RISENSE incurs a small capacity toll due to its in-band overhead, approximately 14% with $T_{\text{sch}} = 1$ slot (the worst case), which quickly diminishes as T_{sch} increases. As noticed by [43], today's mobile networks process data every ~10 slots in the median. With $T_{\text{sch}} = 10$ slots, RISENSE's overhead drops to a negligible 1.4%. Despite this overhead, RISENSE provides between 87% and 144% more capacity than a "static RIS," which offers a wide reflection beam and does not require dynamic reconfiguration.

MARISA and ARES' slow reconfigurability performs close to RISENSE only when there is a single user (i.e., no need for RIS reconfigurations) or when users are scheduled at least every $T_{\text{sch}} > 1000$ slots (every 1 second), which represents a rather static environment. With 10 active users and $T_{\text{sch}} = 1$ slot, RISENSE achieves 3x

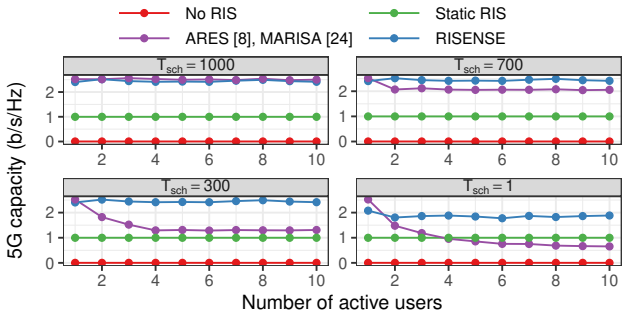


Figure 25: 5G network capacity in a RIS-aided scenario with multiple users and 5G scheduling periods T_{sch}.

more capacity than these benchmarks. In fact, their poor adaptation to dynamic scheduling decisions (any $T_{sch} < 300$ slots) causes MARISA and ARES to underperform even compared to a static wide reflection beam ("static RIS"), as the RIS' narrow reflection beams are frequently outdated and pointing to the wrong user.

6.3.3 Power Consumption. RISENSE enhances capacity in dynamic environments by enabling rapid RIS reconfigurations, though such an improvement comes with an associated energy overhead due to the increased frequency of control message processing. Nevertheless, RISENSE demonstrates superior energy efficiency compared to out-of-band transceivers commonly employed in low-power embedded systems, such as LoRaWAN, Bluetooth Low Energy (BLE), ZigBee, and WiFi, as shown in Table 5. To quantify this gain, we present a comparative analysis of the average power consumption of RISENSE and these out-of-band alternatives. For these transceivers, we rely on a simple model to estimate the average power consumption of these out-of-band transceivers: $P \geq \rho_{rx} \frac{1}{T_{\text{bcn}}} \frac{L}{R} + \rho_{sleep} \left(1 - \frac{1}{T_{\text{bcn}}} \frac{L}{R}\right)$, where L is the payload in bits of RIS reconfiguration messages, R the bitrate, and $\rho_{rx/sleep}$ are device-dependent coefficients while receiving a signal and sleeping, respectively (see Table 5. We assume $L = 400$ bits (50 bytes) for RIS reconfiguration messages, including all protocol headers, and the rate R that maximizes the range for each technology. This model is optimistic, as it does not account for the energy consumed by components such as DMA interfaces connected to the RIS or technology-specific control messages (e.g., WiFi beacons or acknowledgments). In contrast, RISENSE's are empirical measurements capturing all the components in our testbed, so its gains represent a lower bound.

Fig. 26 depicts the average power consumption of each technology (note the logarithmic scale in both axes), highlighting the significant advantage of RISENSE, particularly under conditions requiring frequent RIS reconfigurations. Table 1 in §1 presented the figures for $T_{\text{bcn}} = 100$ ms, e.g., ~370 μW for RISENSE, which proved sufficient for highly dynamic environments in our previous experiments. It is important to note that, while this analysis includes out-of-band transceivers, they do not provide native integration

Table 5: Power consumption profiles of alternative wireless transceivers for embedded devices.

	ρ_{rx} (mW)	ρ_{sleep} (mW)	R (kbps)
LoRa [22]	125	0.03	27
WiFi [21]	1240	0.15	1000
Bluetooth LE [21]	122	0.03	125
ZigBee [21]	178	0.03	250

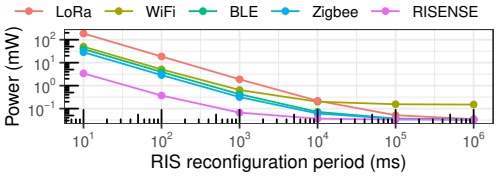


Figure 26: Power consumption of RIS control interface as a function of the RIS re-configuration period. Log scales.

into the 5G MAC layer, a key advantage of RISENSE. Furthermore, among these low-power out-of-band transceivers, only LoRa can support ranges acceptable for BS-RIS communication (see Table 1).

In conclusion, the results of §6.3.1-§6.3.3 highlight the advantages of a wireless RIS control solution capable of keeping pace with the BS's 3GPP-compliant procedures. RISENSE *not only provides such a feature but also preserves the passive, low-cost, and low-energy nature of the RIS, requiring no hardware modifications in the BS and seamlessly integrating into its 5G NR stack.*

7 RELATED WORK

To date, the RIS literature has focused on the reflective metasurface design [11–14, 44] and on the optimization of the RIS configuration [6, 15–18], including ideal continuous phase shifts [45], practical discrete shifts [46], phase quantization [6], and practical algorithms to find RIS configurations [15–18, 47]. However, the integration of RIS technology into mobile systems, where a BS dynamically serves distinct mobile users, has not been sufficiently studied. Different BS allocations require different RIS configurations to maximize capacity, rendering non-reconfigurable RIS solutions [48, 49] unsuitable. Consequently, *the RIS state must be synchronized with the BS's scheduling decisions, which requires tight 5G/RIS integration.*

Most studies assume ideal RIS control interfaces and most RIS implementations rely on out-of-band wired interfaces using USB [11], UART [13], or Ethernet [14], which are impractical for outdoor cellular networks. Some out-of-band wireless interfaces have been proposed. The most conventional methods are WiFi or Bluetooth Low Energy (BLE) [12]. Zhang et al. [19] propose a digital metasurface platform programmable with visible light, using photodiodes to convert light patterns into voltages to configure the metasurface elements. In [20], Sayanskiy et al. use modulated infrared. Kim et al. [50] use an NB-IoT interface. However, as shown in §6, out-of-band solutions incur higher costs and energy consumption. Other technologies such as backscattering [51] can solve the cost and energy problem. However, these solutions are limited by their short-range capabilities (see Table 1). LoRa [22] could be used for longer range at a moderate energy toll but, like all out-of-band solutions, its incompatibility with 3GPP 5G PHY/MAC procedures hinders seamless integration with BSs and real-time control, crucial for aligning RIS control with PHY/MAC scheduling decisions and, consequently, for maximizing network capacity.

Although Zappone et al. [52] and Saggese et al. [53] have theoretically studied the in-band RIS control overhead, we go further by proposing a practical implementation. MARISA [24] and its extension ARES [8], perhaps RISENSE's closest competitors, also utilize a power-sensing RIS architecture but for rough channel estimation and self-configuration. In more detail, both approaches assume the received power can be split between a reflecting branch (regular RIS operation) and a sensing branch, with the latter exploited to

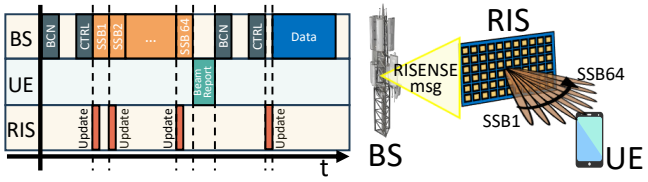


Figure 27: RISENSE support of beam sweeping.

localize users, so the burden of the beam-sweeping is translated to the RIS. In this case, the RIS has to sweep through all the configurations of a predefined codebook and measure which one provides the highest sensed power. This eliminates RIS control overhead, but is inefficient for mobile users due to its slow probing phase. Conversely, RISENSE's in-band nature seamlessly integrates the RIS control channel into the BS's PHY/MAC layer for real-time control, and its low-overhead protocol enables on-demand reconfiguration, adapting to varying channel conditions and user mobility.

8 DISCUSSION AND FUTURE WORK

We conclude discussing some practical aspects and future work.

8.1 Practical considerations

Beam sweeping support. Our results in §6.3 assume knowledge of each user's location to find optimal beamforming configurations at the BS and the RIS. The literature on this topic is extensive (see §7) and we do not cover them in this paper but typical methods rely on some form of beam sweeping by iterating through a predetermined codebook [54, 55]. To support these methods, instead of emitting a reconfiguration message for every item in the codebook, which would incur high overhead, RISENSE can transmit a predefined message to trigger a RIS configuration sweep, as illustrated in Fig. 27. RIS configurations can then be set over fixed time intervals, during which the BS can transmit Synchronization Signal Blocks (SSBs) to estimate the associated channels.

It is important to note, however, that RISENSE does not presuppose any specific RIS optimization method. RISENSE supports any method in the literature by providing an in-band control-plane communication interface that allows for quick and low-footprint RIS configuration, as demonstrated in §6.3.

RISENSE requirements. A first requirement to deploy RISENSE is the ability to embed amplitude-modulated OOK signals on top of 5G NR waveforms, a feature not natively supported by current commercial BSs. However, RISENSE has been designed for seamless integration. To this end, as explained in §4, 5G BSs are only required to store two precomputed codebooks, C and Q. No signal processing operations beyond the incumbent OFDM processing pipeline of 5G BSs are required. Whenever a radio scheduling decision warrants a RIS reconfiguration, the BS simply needs to select an entry in C (RIS configuration) and then an entry in Q (pre-computed subcarrier entries to modulate the RIS configuration), which can be implemented with low-complexity look-up tables.

A second requirement RIS-BS channel knowledge, e.g., to compute α (see §6). This is a reasonable assumption, as in typical deployments both the RIS and the BS are stationary, making the RIS-BS channel effectively quasi-static. Nonetheless, if long-term environmental dynamics lead to changes in this channel, a corresponding recalibration—using one of the established methods from the literature [56, 57]—can be triggered to update the channel estimate.

8.2 Future work

Evaluation in production systems. Although our evaluation is data-driven, incorporating empirically measured RIS gains from a physical prototype subject to hardware imperfections such as phase noise, mutual coupling, and limited tuning resolution, real-world deployments may introduce unforeseen artifacts. We defer the exploration of these artifacts, which requires trials in production systems, to future work. However, to ensure transparency and reproducibility, our empirical data is publicly available [37].

Time synchronization. As explained in §5, RISENSE relies on a low-overhead beaconing method for time synchronization. While this approach minimizes overhead and complexity, errors due to hardware imperfections or processing jitter may arise. Hence, future work is needed to develop a time synchronization method that mitigates potential synchronization errors.

RISENSE-aware radio scheduling. In this paper, we demonstrated how RISENSE facilitates synchronization between the RIS configuration and 5G BS scheduling decisions at a millisecond timescale. However, as illustrated in §6.3.2, the corresponding overhead increases with the BS's scheduling granularity, reaching up to 14% when $T_{\text{sch}} = 1$ ms. This overhead could potentially be reduced by employing a RIS-aware radio scheduler at the BS. Such a scheduler could minimize the frequency of RIS reconfigurations by, for instance, grouping users who can utilize the same RIS configuration or by encoding sequences of RIS configurations that can be initiated with a single RISENSE message. We leave this for future research.

9 CONCLUSIONS

In conclusion, this paper has presented RISENSE, a system that addresses the practical challenges of integrating Reconfigurable Intelligent Surfaces (RIS) into cellular networks. RISENSE's key innovations include: (*i*) a novel RIS design capable of decoding control messages without complex baseband operations or additional RF chains, utilizing a low-cost, low-energy power sensor and a network of microstrip lines and couplers; (*ii*) an in-band wireless control mechanism compatible with 5G New Radio (NR), which enables long-range, seamless, real-time RIS control; and (*iii*) a low-overhead RIS control protocol that minimizes 5G NR overhead while maintaining the flexibility of on-demand RIS reconfiguration. Our experimental validation of RISENSE, using low-cost, low-energy components, has demonstrated its feasibility. Our evaluation has showcased RISENSE's ability to swiftly reconfigure the RIS as users move, even at vehicular speeds, with negligible overhead. This capability opens up new possibilities for deploying RIS in dynamic environments and supporting high-mobility applications.

ACKNOWLEDGEMENTS

This work received funding from the EU's Horizon Europe program under Grant Agreements No. 101139270 (ORIGAMI) and 101192521 (MultiX), the Spanish Ministry of Economic Affairs and Digital Transformation through UNICO 5G I+D (OPEN6G), the CERCA Programme, the Spanish MCIN/AEI/FEDER, EU (PID2022-136769NB-I00), and the Madrid Regional Government through Project TUCAN6-CM (TEC-2024/COM-460). Syed Waqas Haider Shah is a Juan de la Cierva awardee (JDC2023-050996-I), funded by MCIU/AEI/10.13039/501100011033 and the EU (ESF+).

REFERENCES

[1] A. Albanese *et al.*, "RIS-Aware Indoor Network Planning: The Rennes Railway Station Case," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 2028–2034.

[2] Z. Wang, Z. Liu, Y. Shen, A. Conti, and M. Z. Win, "Location Awareness in Beyond 5G Networks via Reconfigurable Intelligent Surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2011–2025, 2022.

[3] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep Reinforcement Learning-Based Intelligent Reflecting Surface for Secure Wireless Communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 375–388, 2021.

[4] R. Liu, Q. Wu, M. Di Renzo, and Y. Yuan, "A Path to Smart Radio Environments: An Industrial Viewpoint on Reconfigurable Intelligent Surfaces," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 202–208, 2022.

[5] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.

[6] P. Mursia *et al.*, "RISMA: Reconfigurable Intelligent Surfaces Enabling Beamforming for IoT Massive Access," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 4, pp. 1072–1085, 2021.

[7] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[8] A. Albanese *et al.*, "ARES: Autonomous RIS Solution With Energy Harvesting and Self-Configuration Towards 6G," *IEEE Transactions on Mobile Computing*, pp. 1–14, 2024.

[9] M. Rossanese *et al.*, "Data-driven Analysis of the Cost-Performance Trade-off of Reconfigurable Intelligent Surfaces in a Production Network," in *Proceedings of the 19th International Conference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT '23. New York, NY, USA: Association for Computing Machinery, 2023.

[10] B. Rana, S.-S. Cho, and I.-P. Hong, "Review Paper on Hardware of Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 11, pp. 29 614–29 634, 2023.

[11] M. Rossanese, P. Mursia, A. Garcia-Saavedra, V. Sciancalepore, A. Asadi, and X. Costa-Perez, "Design and validation of scalable reconfigurable intelligent surfaces," *Computer Networks*, vol. 241, p. 110208, 2024.

[12] M. Heinrichs, A. Sezgin, and R. Kronberger, "Open Source Reconfigurable Intelligent Surface for the Frequency Range of 5 GHz WiFi," *arXiv preprint arXiv:2307.06868*, 2023.

[13] C. Li, Q. Huang, Y. Zhou, Y. Huang, Q. Hu, H. Chen, and Q. Zhang, "RIScan: RIS-aided Multi-user Indoor Localization Using COTS Wi-Fi," in *Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems*, 2023, pp. 445–458.

[14] V. Popov, M. Odit, J.-B. Gros, V. Lenets, A. Kumagai, M. Fink, K. Enomoto, and G. Lerosey, "Experimental demonstration of a mmwave passive access point extender based on a binary reconfigurable intelligent surface," *Frontiers in Communications and Networks*, vol. 2, p. 733891, 2021.

[15] M.-M. Zhao, Q. Wu, M.-J. Zhao, and R. Zhang, "Intelligent reflecting surface enhanced wireless networks: Two-timescale beamforming optimization," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 2–17, 2020.

[16] A. Abrardo, D. Dardari, and M. Di Renzo, "Intelligent reflecting surfaces: Sum-rate optimization based on statistical position information," *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 7121–7136, 2021.

[17] K. Zhi, C. Pan, H. Ren, and K. Wang, "Statistical CSI-based design for reconfigurable intelligent surface-aided massive MIMO systems with direct links," *IEEE Wireless Communications Letters*, vol. 10, no. 5, pp. 1128–1132, 2021.

[18] S. W. H. Shah, S. P. Deram, and J. Widmer, "On the effective capacity of RIS-enabled mmWave networks with outdated CSI," in *Proc. IEEE INFOCOM 2023-IEEE Conference on Computer Communications*. IEEE, 2023, pp. 1–10.

[19] X. G. Zhang, W. X. Jiang, H. L. Jiang, Q. Wang, H. W. Tian, L. Bai, Z. J. Luo, S. Sun, Y. Luo, C.-W. Qiu *et al.*, "An optically driven digital metasurface for programming electromagnetic functions," *Nature Electronics*, vol. 3, no. 3, pp. 165–171, 2020.

[20] A. Sayanskiy, A. Belov, R. Yafasov, A. Lyulyakin, A. Sherstobitov, S. Glybovski, and V. Lyashev, "A 2D-Programmable and Scalable Reconfigurable Intelligent Surface Remotely Controlled via Digital Infrared Code," *IEEE Transactions on Antennas and Propagation*, vol. 71, no. 1, pp. 570–580, 2023.

[21] O. O. Kazeem, O. O. Akintade, and L. O. Kehinde, "Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things," *Int. J. Internet Things*, vol. 6, no. 1, pp. 9–13, 2017.

[22] R. Marini, K. Mikhaylov, G. Pasolini, and C. Buratti, "Low-power wide-area networks: Comparison of lorawan and nb-iot performance," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21 051–21 063, 2022.

[23] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, and T. Brecht, "Witag: Seamless wifi backscatter communication," ser. ACM SIGCOMM '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 240âĂŞ252.

[24] A. Albanese *et al.*, "MARISA: A Self-configuring Metasurfaces Absorption and Reflection Solution Towards 6G," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 250–259.

[25] Z. Li and T. He, "WEBee: Physical-Layer Cross-Technology Communication via Emulation," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 2âĂŞ14.

[26] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active RIS vs. passive RIS: Which will prevail in 6G?" *IEEE Transactions on Communications*, vol. 71, no. 3, pp. 1707–1725, 2022.

[27] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 162–169, 2018.

[28] M. Rossanese *et al.*, "Open Experimental Measurements of Sub-6GHz Reconfigurable Intelligent Surfaces," *IEEE Internet Computing*, 2024.

[29] E. Dahlman, S. Parkvall, and J. Skold, *5G NR: The next generation wireless access technology*. Academic Press, 2020.

[30] Analog Devices, "AD8318: 1 MHz to 8 GHz, 70 dB Logarithmic Detector/Controller," 10 2023. [Online]. Available: https://www.analog.com/en/products/ad8318.html

[31] N. Benvenuto and M. Zorzi, *Principles of communications Networks and Systems*. John Wiley & Sons, 2011.

[32] J. G. Proakis and M. Salehi, *Digital communications*. McGraw-Hill., 2008.

[33] V. Jamali, W. Ghanem, R. Schober, and H. V. Poor, "Impact of channel models on performance characterization of ris-assisted wireless systems," in *2023 17th European Conference on Antennas and Propagation (EuCAP)*. IEEE, 2023, pp. 1–5.

[34] International Telecommunication Union, "Guidelines for evaluation of radio interface technologies for imt-advanced," ITU-R, Report M.2135-1, 2009.

[35] R. Jain, "Channel models: A tutorial," Online Tutorial, February 2007. [Online]. Available: https://www.cse.wustl.edu/~jain/cse574-08/ftp/channel_model_tutorial.pdf

[36] A. M. Rateb and M. Labana, "An optimal low complexity papr reduction technique for next generation ofdm systems," *IEEE Access*, vol. 7, pp. 16 406–16 420, 2019.

[37] M. Rossanese *et al.*, "Open experimental measurements of sub-6ghz reconfigurable intelligent surfaces," *IEEE Internet Computing*, vol. 28, no. 2, pp. 19–28, 2024.

[38] E. BjÃűrnson, Ã. ÃŰzdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 244–248, 2020.

[39] A. Gupta and I. Jain, "Multiple smaller base stations are greener than a single powerful one: Densification of wireless cellular networks," *HotCarbon*, 2022.

[40] ETSI, "TR 136 942 V15.0.0 (2018-07)," European Telecommunications Standards Institute (ETSI), Technical Report, July 2018.

[41] S. Jaeckel, L. Raschkowski, K. Börner, L. Thiele, F. Burkhardt, and E. Eberlein, "Quadriga-quasi deterministic radio channel generator, user manual and documentation," *Fraunhofer Heinrich Hertz Institute, Tech. Rep. v2. 0.0*, 2017.

[42] W. Stone, "Electromagnetic signal attenuation in construction materials," *NIST Interagency/Internal Report (NISTIR) - 6055*, 1997-10-01 1997.

[43] L. L. Schiavo *et al.*, "CloudRIC: Open Radio Access Network (O-RAN) Virtualization with Shared HeterogeneousCcomputing," in *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, 2024, pp. 558–572.

[44] R. Ma, R. I. Zelaya, and W. Hu, "Softly, deftly, scrolls unfurl their splendor: Rolling flexible surfaces for wideband wireless," in *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, ser. ACM MobiCom '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3570361.3592520

[45] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE transactions on wireless communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[46] ——, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1838–1851, 2020.

[47] M. Yue, L. Liu, and X. Yuan, "RIS-Aided Multiuser MIMO-OFDM With Linear Precoding and Iterative Detection: Analysis and Optimization," *IEEE Transactions on Wireless Communications*, vol. 22, no. 11, pp. 7606–7619, 2023.

[48] K. Qian, L. Yao, X. Zhang, and T. N. Ng, "Millimirror: 3d printed reflecting surface for millimeter-wave coverage expansion," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, ser. MobiCom '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 15âĂŞ28. [Online]. Available: https://doi.org/10.1145/3495243.3517024

[49] R. Ma, S. Zheng, H. Pan, L. Qiu, X. Chen, L. Liu, Y. Liu, W. Hu, and J. Ren, "Automs: Automated service for mmwave coverage optimization using low-cost metasurfaces," in *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, ser. ACM MobiCom '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 62âĂŞ76. [Online]. Available: https://doi.org/10.1145/3636534.3649347

[50] M. Kim, N. Ahn, and S. M. Kim, "NR-Surface: NextG-ready μW-reconfigurable mmWave metasurface," in *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. Santa Clara, CA: USENIX Association, Apr. 2024, pp. 1641–1657. [Online]. Available: https://www.usenix.org/conference/nsdi24/

presentation/kim
[51] Y. Chae, Z. Lin, K. M. Bae, S. M. Kim, and P. Pathak, "mmComb: High-speed mmWave Commodity WiFi Backscatter," in *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*, 2024, pp. 1713–1729.
[52] A. Zappone, M. Di Renzo, F. Shams, X. Qian, and M. Debbah, "Overhead-aware design of reconfigurable intelligent surfaces in smart radio environments," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 126–141, 2021.
[53] F. Saggese *et al.*, "On the Impact of Control Signaling in RIS-Empowered Wireless Communications," *IEEE Open Journal of the Communications Society*, 2024.
[54] J. Wang, W. Tang, S. Jin, C.-K. Wen, X. Li, and X. Hou, "Hierarchical codebook-based beam training for ris-assisted mmwave communication systems," *IEEE Transactions on Communications*, vol. 71, no. 6, pp. 3650–3662, 2023.
[55] K. Chen-Hu, R. J. Williams, A. AlÃź, and P. Popovski, "Fast beam-sweeping in mmwave cellular network relying on frequency shifting-ris," in *ICC 2024 - IEEE International Conference on Communications*, 2024, pp. 2458–2463.
[56] S. Noh, J. Lee, G. Lee, K. Seo, Y. Sung, and H. Yu, "Channel estimation techniques for ris-assisted communication: Millimeter-wave and sub-thz systems," *IEEE Vehicular Technology Magazine*, vol. 17, no. 2, pp. 64–73, 2022.
[57] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning," *IEEE Access*, vol. 9, pp. 44 304–44 321, 2021.