SlimWiFi: Ultra-Low-Power IoT Radio Architecture Enabled by Asymmetric Communication

Renjie Zhao, *University of California San Diego;* Kejia Wang, *Baylor University;* Kai Zheng and Xinyu Zhang, *University of California San Diego;* Vincent Leung, *Baylor University*

https://www.usenix.org/conference/nsdi23/presentation/zhao-renjie

This paper is included in the
Proceedings of the 20th USENIX Symposium on
Networked Systems Design and Implementation.

April 17–19, 2023 • Boston, MA, USA

978-1-939133-33-5

SlimWiFi: Ultra-Low-Power IoT Radio Architecture Enabled by Asymmetric Communication

Renjie Zhao[1], Kejia Wang[2], Kai Zheng[1], Xinyu Zhang[1], Vincent Leung[2]
[1]*University of California San Diego,* [2]*Baylor University*
[1]*{r2zhao, kazheng, xyzhang}@ucsd.edu,* [2]*{kejia_wang1, vincent_leung}@baylor.edu*

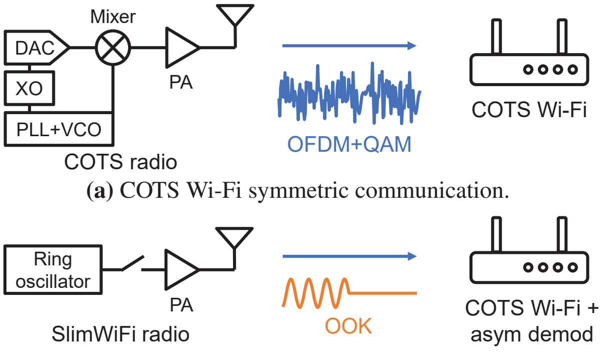
Abstract

To communicate with existing wireless infrastructures such as Wi-Fi, an Internet of Things (IoT) radio device needs to adopt a compatible PHY layer which entails sophisticated hardware and high power consumption. This paper breaks the tension for the first time through a system called SlimWiFi. A SlimWiFi radio actively transmits on-off keying (OOK) modulated signals. But through a novel *asymmetric communication* scheme, it can be directly decoded by off-the-shelf Wi-Fi devices. With this measure, SlimWiFi radically simplifies the radio architecture, evading power hungry components such as data converters and high-stability carrier generators. In addition, it can cut the transmit power by around 18 dB, while keeping a similar link budget as standard Wi-Fi. We have implemented SlimWiFi through PCB prototype and IC tape-out. Our experiments demonstrate that SlimWiFi can reach around 100 kbps goodput at up to 60 m, while reducing power consumption by around 3 orders of magnitude compared to a standard Wi-Fi transmitter.

1 Introduction

The Internet of Things (IoT) is playing a key role in bridging the physical and digital worlds. IoT will act as the workhorse to fully automate human life, through a new wave of applications in environment/behavior sensing, asset tracking, ambient human-computer interaction, *etc.* As of 2021, the population of active IoT endpoints already reached 12.2 billion, and will surge towards 27 billion in 2025 [27]. Maintaining the connectivity between the IoT fabric and the existing Internet infrastructure entails non-trivial human efforts, and will ultimately be feasible only if the IoT devices can sustain themselves, *e.g.*, through RF energy harvesting. In practice, RF energy harvesting can usually reach at most tens of μW [75] for IoT devices, so any self-sustainable communication paradigm has to adhere to this limit. RFID represents one such paradigm, which is truly battery-free and communicates by merely harvesting and remodulating the RF power from an interrogator (reader). Yet to date, RFID has witnessed limited adoption in consumer applications, due to its limited communication range, relatively high cost of the reader, and limited functionality (mostly restricted to reading preprogrammed information on passive tags).

Ideally, we would prefer to reuse the existing wireless infrastructures (*e.g.*, the pervasive Wi-Fi) as gateways to connect the ultra-low-power (ULP) IoT radios to the Internet. Unfortunately, mainstream wireless communication standards cannot support battery-free operations due to their high *peak power*. For example, the commercial off-the-shelf (COTS) Wi-Fi, BLE, ZigBee, NB-IoT, and LoRa devices all require tens to hundreds of mW of peak power [34, 60, 61, 70], orders of magnitude higher than that available from RF energy harvesting. Their self-sustained operations are feasible only under an extremely low duty cycle (a few dozen bytes per day) while supported by a bulky power source (*e.g.*, a solar panel).



(a) COTS Wi-Fi symmetric communication.

(b) SlimWiFi asymmetric communication.

Figure 1: Comparison between COTS Wi-Fi and SlimWiFi.

We argue that the root cause of the high power consumption of such systems lies in the requirement of *symmetric communication*, *i.e.*, the IoT radios must adopt the same high-profile modulation/demodulation hardware as the existing wireless infrastructures. As illustrated in Fig. 1a, to be compatible with existing Wi-Fi access points (APs), an IoT radio needs to support OFDM and QAM, which entails stringent hardware requirements, such as accurate and stable carrier frequency, low phase noise, wideband and high-resolution ADC/DAC, and a high-gain high-linearity (but often low-efficiency) power amplifier, all of which translate into power hungry components. We thus pose an important question: *Is it possible to relax such requirements and make the communication hardware and modulation asymmetric?*

We explore the answers through a novel system design called *SlimWiFi*. SlimWiFi adopts a novel *asymmetric communication* scheme to realize Wi-Fi-compatible ULP radio. Specifically, the SlimWiFi ULP radio builds on a highly simplified architecture as shown in Fig. 1b, capable of only modulating/demodulating on-off keying (OOK) waveforms. But it can directly communicate with existing Wi-Fi APs that are designed to modulate/demodulate sophisticated OFDM waveforms. Essentially, SlimWiFi shifts the PHY layer complexity to the high-power infrastructure side, and by doing so, it can improve the energy efficiency of the IoT radio by orders of magnitude. Unlike the backscatter-based systems [29, 35, 42, 79] that rely on additional helper devices to generate external carrier signals, SlimWiFi is an active, standalone radio transceiver. To materialize the design principles behind SlimWiFi, we need to address two key challenges.

(a) How to enable direct communication between asymmetric hardware, i.e., the OFDM-based Wi-Fi device and the OOK based SlimWiFi device? The uplink communication, *i.e.*, demodulating the OOK signal with an unmodified Wi-Fi OFDM device, is very challenging due to the highly incompatible waveforms and demodulation hardware. Note, however, that any demodulation process is essentially sampling and mapping analog waveforms into a binary sequence. The SlimWiFi Wi-Fi receiver thus reverses its OFDM demodulation steps, as well as the Forward-Error-Correction (FEC) decoder, and descrambler, and then reconstruct the incoming OOK symbols merely based on the payload bits reported by the Wi-Fi driver. With this measure, an ordinary Wi-Fi AP can decode the OOK signals from the ULP SlimWiFi transmitter, *without any hardware modifications*. On the other hand, the downlink modulation is straightforward, as recent work [35, 78, 79] has well-explored ways of mapping a sequence of bits into a pseudo-OOK waveform using a WiFi transmitter. To achieve MAC layer compatibility, SlimWiFi delegates the carrier sensing task to the Wi-Fi AP, which uses the CTS-to-self packets to virtually reserve the channel, and then informs the SlimWiFi node to start its transmission.

(b) How to optimize the SlimWiFi radio hardware to minimize power consumption while maintaining Wi-Fi compatibility? In commensurate with the complicated modulation, the typical hardware architecture of a COTS Wi-Fi radio necessarily consists of a power amplifier (PA) for a high transmit power, high precision and wideband digital-to-analog converter (DAC) for high-order modulation, and phase-locked loop (PLL) and voltage-controlled oscillator (VCO) for accurate carrier generation. The power consumption of these components is fundamentally governed by physical laws, and almost impossible to fall below several mW [9, 16, 55, 63]. SlimWiFi circumvents the fundamental limitation with a highly simplified radio architecture that leverages asymmetric communication. The SlimWiFi ULP radio eliminates the power hungry DAC/ADC and PLL and affords a more efficient PA owing to the lower power and linearity requirements. As for carrier generation, we adopt a free-running ring oscillator [82], which bears a low frequency stability, but suffices for SlimWiFi as its narrowband OOK signal can be asymmetrically demodulated as long as the carrier falls within the 2.4 GHz ISM band.

To verify the effectiveness of our design, we implement asymmetric communication with a COTS Wi-Fi device and a prototype SlimWiFi device. Our experiments demonstrate that the OOK based SlimWiFi signals can be decoded from the payload bits of the Wi-Fi device over a range of 60 m, with a goodput of around 100 kbps. We have also designed and taped out a SlimWiFi IC based on the aforementioned SlimWiFi radio architecture. Our measurement shows that the SlimWiFi only consumes around 90 µW of power, approximately 3 orders of magnitude lower compared with COTS WiFi radios.

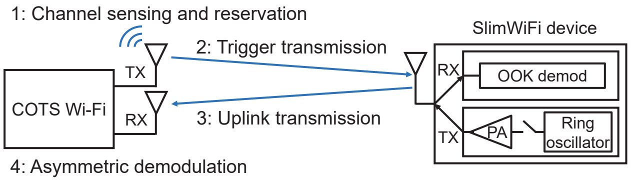


Figure 2: Workflow of a SlimWiFi uplink transmission.

To summarize, we make the following contributions through the SlimWiFi design and implementation.

- We propose SlimWiFi, a novel asymmetric communication paradigm that enables COTS Wi-Fi devices to decode OOK signals from ULP radios. The design enables such ULP radios to reuse the existing Wi-Fi as the IoT infrastructure, which can substantially reduce the deployment cost for attaining ubiquitous connectivity.
- We introduce a new SlimWiFi ULP radio architecture, which leverages the asymmetric communication to enable the first *active* Wi-Fi-compatible transmitter at a peak power of tens of µW.
- We implement the asymmetric communication system through a PCB prototype and IC tape-out. Our experiments verify the potential of SlimWiFi in supporting self-sustained IoT communication.

2 System Workflow

The SlimWiFi design mainly focuses on the IoT uplink, consisting of the SlimWiFi device and the COTS Wi-Fi radio. The former transmits OOK modulated data, through a highly simplified ULP radio architecture. The latter acts as the demodulator and gateway to connect the SlimWiFi device to the Internet. As illustrated in Fig. 2, a typical uplink transmission attempt involves the following workflow.

(1) The Wi-Fi device first runs standard carrier sensing to acquire the channel and reserves access by transmitting the CTS-to-self frame.

(2) The Wi-Fi device emulates an OOK modulated trigger frame by manipulating the Wi-Fi bit sequence. The SlimWiFi device's ULP OOK receiver decodes the information and synchronizes with the trigger frame.

(3) Following step (2) immediately, the Wi-Fi device initiates the demodulation procedure of its receiver chain, and meanwhile, the SlimWiFi device sends an OOK modulated uplink signal to the Wi-Fi device.

(4) The Wi-Fi device decodes the OOK modulated signal

by applying asymmetric demodulation.

In what follows, we introduce the SlimWiFi asymmetric communication design (Sec. 3) and the SlimWiFi ULP radio hardware (Sec. 4). Our exposition mainly focuses on the novel uplink design (steps 3 and 4). The ULP downlink design (step 2) follows the same asymmetric modulation + simplified hardware principle. It builds on recent cross-technology communication (CTC) and backscatter techniques [20, 35, 45, 67, 78], and will be discussed briefly in Sec. 4.4.

3 Asymmetric Demodulation for SlimWiFi

In this section, we first provide a quick primer on the standard Wi-Fi receiver. Then we introduce the Wi-Fi compatible asymmetric communication in SlimWiFi.

3.1 A Primer on Standard Wi-Fi Receiver

Without loss of generality, we focus on 802.11n, a standard adopted by most modern COTS Wi-Fi devices, running on a 20 MHz channel and single antenna [43]. The upper part of Fig. 3 shows the 802.11n demodulation procedure, which is hard coded into the receiver's IC. The incoming analog signals are first captured by the RF front end and converted into baseband samples. The receiver searches across the samples to identify a standard 802.11 preamble–a predefined OFDM modulated training sequence. If no valid preamble is detected, the samples will be discarded. Otherwise, the receiver will proceed to additional demodulation steps.

The samples are first sliced into *OFDM symbols*, each consisting of 16 samples of cyclic prefix (CP) and 64 samples of data. The CP is redundant samples used to overcome intersymbol interference due to the multi-path effect. The Wi-Fi demodulator needs to remove the CP and apply a 64-point FFT to convert the 64 data samples into frequency-domain, which essentially slices the entire 20 MHz band into 64 *subcarriers*. Only 52 of the subcarriers are extracted as valid data. The remaining are either null subcarriers to mitigate adjacent channel interference or pilots for calibrating the residual offsets of the channel estimation.

Afterwards, a QAM block demaps the complex sample on each subcarrier into one or more bits, depending on the baseband modulation method, *i.e.*, BPSK, QPSK, 16-QAM, and 64-QAM. The resulting bit sequence X contains redundant bits due to forward-error-control (FEC) and needs to be decoded into a sequence Y. The ratio between the length of Y and X is called *coding rate* and can be 1/2, 2/3, 3/4, or 5/6.

The decoded bits Y need to be further reordered to recover the original transmitted bits. This so-called *descrambling* is performed by an XOR operation with a repeatedly generated 127-bit sequence whose initial state is determined by a *scrambler seed*. The PHY layer processing ends here and the output bits will be reported to the upper layer as a MAC frame. We emphasize that *the entire PHY-layer demodulation is implemented in the Wi-Fi IC and thus cannot be bypassed without hardware modification*.

On the other hand, the MAC layer control, management, and frame processing are usually implemented in software (Soft MAC) or firmware (Full MAC) [31, 47]. The MAC frames will be passed to the Wi-Fi driver and can be post-processed in software.

3.2 Overview and Challenges in Asymmetric Demodulation

The asymmetric demodulation design is grounded on a key observation: *The Wi-Fi OFDM demodulation procedure is deterministic and at least partially reversible.* An OFDM receiver essentially converts the incoming time domain samples into frequency domain through FFT, and then "quantizes" the samples through QAM demapping. Theoretically, any signals within the 20 MHz bandwidth can be *reconstructed from the OFDM receiver's bit sequence output*, by reversing the Wi-Fi demodulation procedure. *The SlimWiFi asymmetric demodulator essentially performs such reconstruction in software at the Wi-Fi receiver to recover the incoming OOK waveforms and subsequently demodulate them*, as illustrated in the bottom part of Fig. 3.

Unfortunately, the standard Wi-Fi receiver blocks, such as CP removal, QAM, and FEC, inevitably induce information loss or ambiguities. As a result, SlimWiFi must address the following key challenges.

(1) How to design the OOK signal in order to avoid the impact of information loss while enabling asymmetric demodulation? The hard-coded OFDM demodulation procedure does eliminate certain incoming samples. For example, CP removal erases part of the signal in the time domain, and data subcarrier extraction removes all information in the non-data subcarriers (*i.e.*, null and pilot subcarriers). If the removed segments contain useful data symbols from the SlimWiFi device, it would be hard to reconstruct them. We thus need to carefully design the SlimWiFi OOK waveform to avoid the impact of information loss (Sec. 3.3).

(2) How to deal with the reconstruction errors introduced by the COTS receiver? Besides the information loss from the OFDM block, the QAM and FEC blocks also cause two types of reconstruction errors: *Quantization error*, *i.e.*, the difference between the SlimWiFi signal and the closest point in Wi-Fi's QAM constellation; and *coding error*, *i.e.* the mismatch between the Wi-Fi demodulated bit sequence X and the regenerated bit sequence X' after reversing the FEC, as shown in Fig. 3. SlimWiFi addresses the reconstruction errors by (i) judiciously configuring the receiver parameters and (ii) performing additional channel coding on top of the SlimWiFi signals, as to be described in Sec. 3.4.

(3) How to integrate SlimWiFi with standard Wi-Fi protocols? To make SlimWiFi fully compatible with standard Wi-Fi, several PHY/MAC layer primitives are needed, *e.g.*, generating PHY preamble, PHY/MAC headers, and triggering the Wi-Fi receiver to start demodulation. We address these practical challenges in Sec. 3.5.

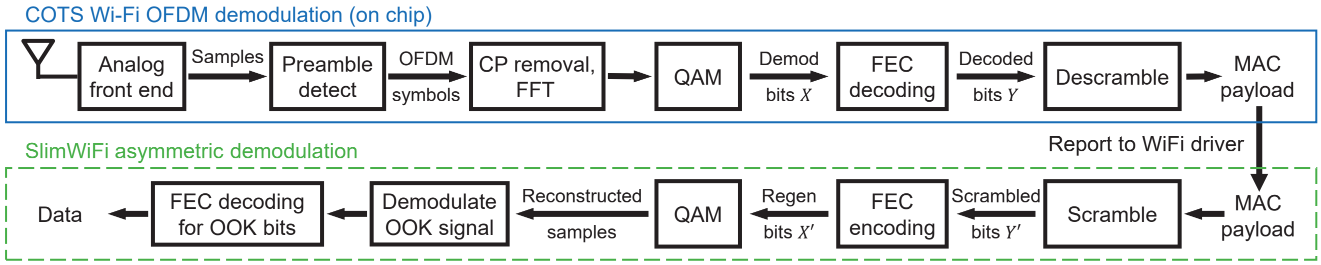
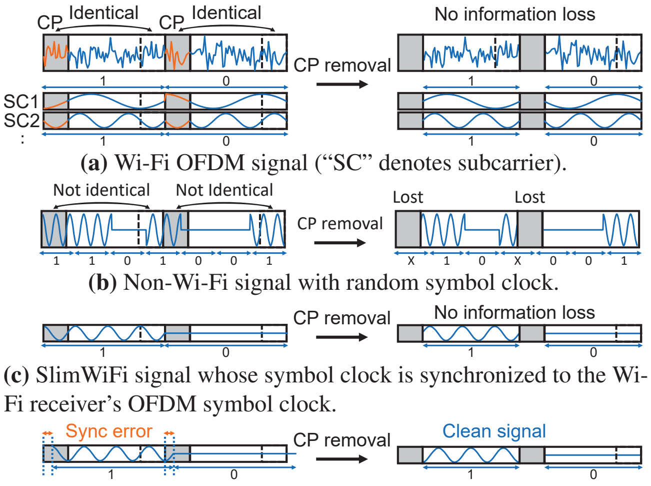


Figure 3: Receiving procedure of a SlimWiFi uplink receiver, *i.e.*, the COTS Wi-Fi device.



(a) Wi-Fi OFDM signal ("SC" denotes subcarrier).

(b) Non-Wi-Fi signal with random symbol clock.

(c) SlimWiFi signal whose symbol clock is synchronized to the Wi-Fi receiver's OFDM symbol clock.

(d) SlimWiFi signal with synchronization error.

Figure 4: Symbol clock sync to counteract CP removal.

3.3 SlimWiFi Signal Design

3.3.1 Overcoming signal erasures on the COTS Wi-Fi demodulator

In this section, we introduce the transmission waveform of the SlimWiFi device which are designed to circumvent the signal erasures on the COTS Wi-Fi demodulator.

As shown in Fig. 4a, the standard Wi-Fi waveform inside a CP is a replica of the last 0.8 µs of the OFDM symbol (4 µs in total) hosting the CP. Therefore, removing the CP does not cause any information loss for the Wi-Fi demodulator. In contrast, for a non-Wi-Fi signal with an arbitrary symbol clock (Fig. 4b), this operation may inadvertently erase 20% of the original signal which makes the demodulation unreliable. To overcome this issue, we choose to synchronize the OOK symbol clock of the SlimWiFi device with the OFDM symbol clock of the Wi-Fi receiver, *i.e.*, 250 kHz for 802.11n. Fig. 4c shows that, with such symbol-level clock synchronization, the SlimWiFi signal acts the same as the signal of one Wi-Fi subcarrier (in Fig. 4a). Therefore, the signal erasure caused by CP removal can be avoided. To realize the symbol level clock synchronization, the SlimWiFi device simply generates a 250 kHz clock and aligns its transmission time to the aforementioned trigger frame (Sec. 2). Such synchronization relies on symbol energy detection and may not be precise. However, as shown in Fig. 4d, the redundant CP part can be utilized to tolerate the synchronization errors, which we will further verify in Sec. 6.2.

Recall that 12 out of the 64 subcarriers within the 20 MHz Wi-Fi channel are null or pilot subcarriers, eventually discarded by the Wi-Fi demodulator. Therefore, to prevent information loss, the SlimWiFi device should avoid modulating its OOK waveform at the same frequencies as the non-data subcarriers. This in turn imposes more constraints on its signal bandwidth and carrier frequency, which we address below.

3.3.2 Relaxing the hardware requirements on the SlimWiFi radio device

Range, TX power, and bandwidth. The communication range of the SlimWiFi uplink can be estimated based on the classical link budget equation [85]:

$$k_bT_aB+NF+SNR_o=P_{TX}+G_{TX}+G_{RX}-20log_{10}(4\pi d f_c/c)$$

where k_b is the Boltzmann constant, and T_a is the equivalent noise temperature in [K]. B, NF, and SNR_o denote the signal bandwidth, RX noise figure, and SNR threshold for robust decoding, respectively. P_{TX}, G_{TX}, and G_{RX} are TX power, TX, and RX antenna gain, respectively. d is the operating range, f_c is the carrier frequency and c is the light speed.

To achieve a target range d while keeping the SlimWiFi device at ULP, we propose to reduce B, which can in turn lower the total transmit power P_{TX}. This design choice hinges on the observation that we can treat each subcarrier of the OFDM receiver as an individual narrow-band (312.5 kHz) channel. As long as the SlimWiFi signal falls within one of the subcarriers, it can be captured and demodulated by the OFDM receiver. Therefore, even if its P_{TX} is reduced by $10log_{10}(20000/312.5)$ = 18 dB, the total power of a SlimWiFi symbol can still be equivalent to that of a Wi-Fi subcarrier, and SlimWiFi can still keep the same transmission range as a normal Wi-Fi! The operating range can be further traded off for even lower transmit power. In fact, with the 250 kHz OOK symbol rate the SlimWiFi signal bandwidth is 250 kHz which can already fit within one Wi-Fi subcarrier.

Carrier frequency requirement. Most existing communication standards require an accurate carrier frequency. In particular, a highly stable carrier is crucial for synchronizing OFDM TX and RX, and reducing leakage between subcarriers. However, this usually entails a high-profile carrier generator,

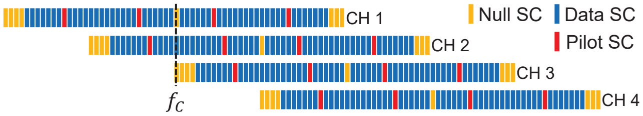


Figure 5: Subcarrier mapping between different channels of Wi-Fi on the 2.4 GHz band. Only 4 channels are illustrated.

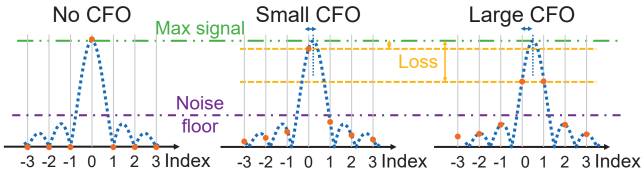


Figure 6: Amplitude of different subcarriers with or without the CFO, when receiving a single tone OOK signal.

consisting of a VCO and PLL which consumes several mW power [54, 66, 71]. The SlimWiFi asymmetric demodulation circumvents this requirement for the first time. As long as the OOK signal's carrier frequency f_C is located within the 20 MHz Wi-Fi band, it can be captured and recovered by demodulating the Wi-Fi receiver's subcarrier that covers f_C. However, two issues need to be solved to accommodate the inaccurate carrier frequency.

First, f_C might be in the non-data subcarriers which are discarded by the Wi-Fi receiver. We overcome this problem by making use of the partially overlapped Wi-Fi channel designated in the 2.4 GHz band, where the non-data subcarriers of one channel are the data subcarriers of an adjacent channel, as shown in Fig. 5. With this mechanism, the carrier frequency requirement can be further relaxed from 20 MHz (a single Wi-Fi channel) to 80 MHz (the entire 2.4 GHz ISM band covering 13 Wi-Fi channels). Note that, the Wi-Fi receiver can identify the subcarrier where the SlimWiFi signal is located by simply checking the subcarrier energy level. If the Wi-Fi receiver does not observe any uplink signal after the trigger frame (Sec. 2), then the signal may fall on a non-data subcarrier, and the receiver should switch to an adjacent channel instead.

The second issue is that the OOK carrier frequency f_C may not be aligned exactly with an OFDM subcarrier. Although OOK can be demodulated non-coherently, the carrier frequency offset (CFO) leads to non-orthogonality in the Wi-Fi receiver's FFT processing, which may in turn affect the asymmetric demodulation. Fig. 6 illustrates a case where a single tone signal (OOK with ON state) spreads to multiple subcarriers due to CFO. Demodulating the OOK signal on a single subcarrier will result in a low SNR. Combining the signal energy across subcarriers does not necessarily help either because it increases the noise bandwidth. Nonetheless, the worst-case SNR loss due to CFO is only 3 dB (signal spreads evenly between two adjacent subcarriers), which will be verified in Sec. 6.2.

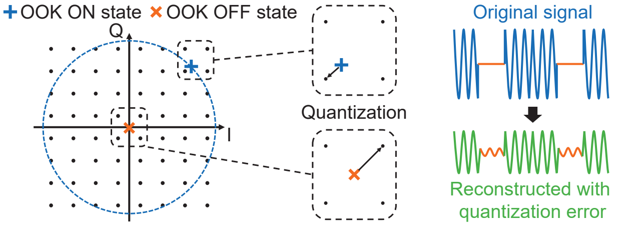


Figure 7: OOK modulated signal with QAM demodulation.

3.4 Resolving Quantization and Coding Errors

3.4.1 QAM and quantization error

The Wi-Fi receiver's QAM demapping block quantizes the phase and amplitude of the signal on each subcarrier. Fig. 7 illustrates the case when a SlimWiFi OOK signal is demapped on a 64-QAM constellation diagram. For the ON state of OOK, the signal sample will have a non-zero amplitude with an arbitrary phase, hence falling at the outer circle. For the OFF state, the sample will have a near-zero amplitude, falling at the origin point. For other subcarriers where no active signals are located, the demapped sample will be the same as the OFF state.

Essentially, the QAM demapping is performing quantization in the complex domain. Thus the original OOK signal on the active subcarrier can be easily reconstructed through the reverse operation, *i.e.*, QAM mapping which converts bits to a complex number. However, this process will introduce quantization errors, which compromises the SNR of the reconstructed signal. The quantization error depends on the precision of quantization which is determined by QAM modulation order. We thus configure the Wi-Fi receiver to the highest modulation order 64-QAM, leading to the lowest quantization error.

3.4.2 FEC and coding error

When receiving the non-OFDM SlimWiFi signal, the FEC block causes a mismatch between the demodulated bit sequence X and regenerated bit sequence X' shown in Fig. 3. The fundamental reasons are two-fold: (i) The demodulated bit sequence can be treated as an arbitrary bit sequence instead of a valid codeword of FEC; (ii) The standard Wi-Fi FEC decoding is a many-to-one mapping, whereas the reverse operation (*i.e.*, FEC encoding in Fig. 3) is a one-to-one mapping. So there is no guarantee that the reconstructed X' can match the original X by simply reversing the FEC.

Fortunately, we found that the number of mismatched bits is limited and can be mitigated with a careful design. The coding errors induced by the two standard FEC schemes in Wi-Fi, *i.e.*, binary convolutional coding (BCC) and low-density parity check (LDPC), are different. Here we only summarize their properties. The detailed proofs are in Appendix A.

(1) Both BCC and LDPC incur fewer coding errors at a higher coding rate. Therefore, we configure the Wi-Fi receiver to the highest available coding rate (*i.e.*, 5/6) when performing the asymmetric demodulation. With this measure, the fraction

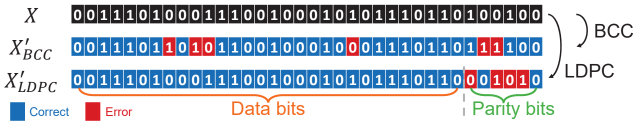


Figure 8: Distribution of coding errors (mismatch between X and X'), for BCC and LDPC, respectively.

of FEC-induced errors can be reduced to around 1/6 and can be further reduced if we apply a separate FEC coding on the SlimWiFi OOK transmitter.

(2) When the Wi-Fi receiver runs the LDPC decoder, the locations of the FEC errors are known a priori on the time-frequency domain. Fig. 8 shows an example of the error distributions when using BCC and LDPC with 5/6 coding rate. X'_{BCC} and X'_{LDPC} are the regenerated bit sequence under BCC and LDPC, respectively. The mismatched bits of the BCC scheme are spread randomly all over the bit sequence X'_{BCC} due to the BCC decoding and interleaving. In contrast, the mismatched bits of the LDPC scheme is always located at the parity bits block (also proven in Appendix A.2).

Based on this observation, we configure the Wi-Fi receiver to LDPC mode in the asymmetric demodulation, which brings two advantages: (i) The error bits are distributed in a periodic way across the reconstructed sequence X' (more details in Sec. 3.6). Therefore, they can be easily corrected by applying a convolutional encoding on the data from SlimWiFi device and using a convolutional decoder on the asymmetric demodulator. (ii) The receiver knows which bits are parity bits (*i.e.*, where the coding errors are clustered). The convolutional decoder can adopt a soft decision decoder which sets those bits with a low log-likelihood ratio, thus improving the decoding performance.

3.5 Practical Challenges

3.5.1 MAC layer configuration

To ensure the MAC payload bits can be used to reconstruct the SlimWiFi signal, we need to resolve two issues: (i) incorrect frame check sequence (FCS), and (ii) limited MAC frame length.

Incorrect FCS. As shown in Fig. 9, the FCS, a 32-bit cyclic redundancy check (CRC) located at the end of the whole frame, is adopted for error protection. Since the received signal is an OOK modulated instead of a valid Wi-Fi signal, it is nearly impossible that the FCS is correct. But we need to capture the data frames through the Wi-Fi driver, even if they fail the FCS check. This is supported by many COTS Wi-Fi devices [2, 21]. A simple software/firmware update can enable the same capability on other Wi-Fi devices.

Data frame length. The length of the payload in a normal Wi-Fi frame is limited by the 2,304 bytes maximum size of the MAC Service Data Unit (MSDU). Recall that SlimWiFi needs to configure the Wi-Fi receiver to the highest data rate (64-QAM, 5/6 code rate, Sec. 3.4). Under this configuration, the maximum number of OFDM symbols is less than 70, corresponding to only 70 OOK symbols as illustrated in Fig. 9. To create a longer frame, we choose to use the aggregate MAC service data unit (A-MSDU) with a quality of service (QoS) data frame, whose maximum size is 7,935 bytes, which extends the frame length to about 240.

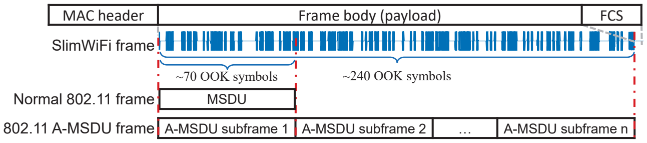


Figure 9: Mapping between the standard Wi-Fi MAC frame and SlimWiFi signal waveform.

3.5.2 Scrambler seed

Since the descrambling is a one-to-one mapping operation on the Wi-Fi receiver, it can be easily reversed by applying a scrambling block with the same scrambler seed. Although the scrambler seed is not reported to the driver, it is set by the PHY header which triggers the receiver's demodulation process (Sec. 3.5.3). Therefore, we can just set a fixed scrambler seed, which can be used to reverse the descrambling block.

3.5.3 Initiating the receiving procedure on Wi-Fi

The final practical challenge lies in generating a valid Wi-Fi preamble and PHY/MAC header. The preamble is needed for triggering the Wi-Fi receiver to start the receiving procedure (packet detection), and is also used for auto gain control, synchronization, and channel estimation. The PHY/MAC header is needed for specifying demodulation parameters such as QAM order, coding rate, scrambling seed, and packet length. Unfortunately, the Wi-Fi preamble and PHY/MAC header are complex OFDM modulated signals, and cannot be directly generated by the SlimWiFi ULP transmitter.

Note that many Wi-Fi devices have separate but co-located transmitter and receiver modules. For example, many Wi-Fi APs [7, 8, 59] usually have multiple transceiver chips (to support concurrent multi-band and multi-antenna operation) which can be configured as co-located TX and RX modules. Therefore, we repurpose the co-located Wi-Fi TX module as an *initiator* to emit a self-initiation frame, comprised of the legitimate preamble and PHY/MAC header but without any payload. Such zero-payload frames are supported by Wi-Fi drivers such as Nexmon [69], or through Wi-Fi frame emulation methods [37]. Upon receiving the initiation frame, the receiver starts its Wi-Fi demodulation workflow followed by the asymmetric demodulation (Fig. 3). Notably, since the transmission of the initiation frame and the reception of OOK data occur consecutively, there is no self-interference between the co-located transmitter and receiver. Therefore, unlike backscatter communication systems, the link budget and receiving sensitivity is not affected by direct Tx leakage or near-far problems [40]. For those Wi-Fi devices with integrated transceivers, a firmware update is needed to enable the receiver to start its demodulation workflow immediately after the transmitter sends out the trigger frame.

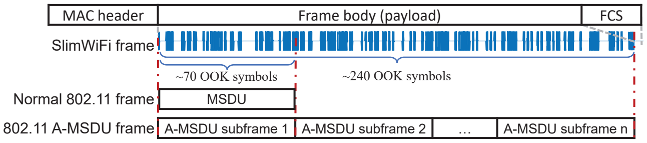


Figure 10: Demodulating the SlimWiFi OOK symbols directly in the frequency domain. The subcarrier with non-zero signal power contains the OOK symbols.

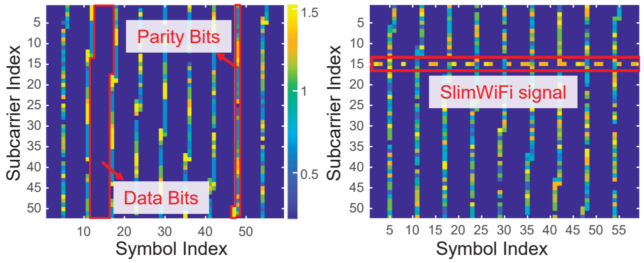
Optimizing receiver gain and sensitivity. A standard Wi-Fi receiver performs automatic gain control (AGC) based on the signal strength of the preamble from the transmitter. For SlimWiFi, since the preamble is from the co-located initiator instead of the actual transmitter, the AGC may be misconfigured. If the initiation frame is too strong, the receiver will set a low gain, leading to insufficient amplification of the incoming SlimWiFi signals. In this situation, the demodulation performance will be bottlenecked by the quantization error (Sec. 3.4.1). Therefore, to achieve the best receiver sensitivity, we would prefer to reduce the power of the initiation frame. This may risk forcing the receiver to tune to a high gain, resulting in the clipping of high amplitude signals. Fortunately, for OOK signals, the clipping effect will not impact demodulation, since clipped signals are recognized as “1” regardless of their amplitude. We will evaluate the effects of the receiver gain in Sec. 6.2.

3.6 Putting Everything Together

Overall, the Wi-Fi receiver follows the processing blocks shown in Fig. 3 to perform the asymmetric demodulation. At a high level, the incoming OOK samples go through the hard-coded normal Wi-Fi demodulation steps which result in a MAC frame. Our asymmetric demodulator reconstructs the complex samples from the MAC frame, by reversing the Wi-Fi demodulation steps, and then decodes the desired bit sequence from the reconstructed samples.

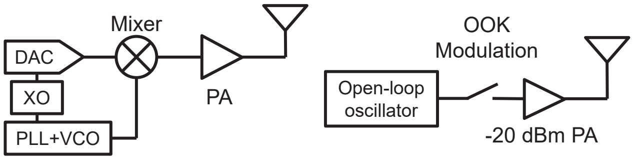
Note that the reverse processing skips the IFFT. Since the OOK signal is narrowband and only occupies one subcarrier, we can directly process the complex samples on that subcarrier, without IFFT-converting them to the time domain, as shown in Fig. 10. The amplitude of the complex sample is used directly to decode the OOK modulated symbol.

To visualize the samples in the time-frequency domain, we collect an example trace with the following configurations: 802.11n with 20 MHz bandwidth, 64-QAM modulation, 5/6 coding rate, LDPC code, and frame length of 2,000 bytes. The waterfall plot in Fig. 11a shows the case without any active transmission. The x and y axis are the symbol index in the time domain, and the subcarrier index in the frequency domain, respectively. The color represents the amplitude of the samples. It can be seen that the samples corresponding to the data bits of the LDPC coded sequence always have a low amplitude (since no coding errors occur there), while the ones corresponding to the parity bits have uncertain results. If we pick the time domain symbols within one subcarrier, the symbols with coding errors (*i.e.* contain parity bits) appear once every 6 symbols. The result corroborates our observations in Sec. 3.4.2.



(a) Without active transmission. **(b)** With OOK signal.

Figure 11: Waterfall plots of reconstructed time-frequency domain samples.



(a) Traditional active transmitter. **(b)** SlimWiFi active transmitter.

Figure 12: Transmitter radio hardware architecture.

Fig. 11b shows the case when a SlimWiFi device is transmitting signals, causing a high amplitude to appear at subcarrier 15 of the Wi-Fi demodulator. The other subcarriers remain the same as the idle case. The OOK signals can thus be demodulated using the samples on subcarrier 15.

4 SlimWiFi ULP Radio Hardware Design

In this section, we focus on the SlimWiFi transmitter hardware, which is designed for asymmetric demodulation. We also provide a brief discussion on the ULP OOK receiver which explains how SlimWiFi device interacts with the COTS Wi-Fi device on the downlink.

4.1 High Power Consumption in Traditional IoT Radios

Modern IoT radio designs need to make challenging trade-offs between power consumption and other competing requirements, including range, bit rate, spectrum efficiency, *etc.* Regardless of how they bias the trade-offs, the IoT radio architecture invariantly comprises 3 key components (Fig. 12a): a high power PA to ensure sufficiently high transmit power; a crystal oscillator (XO) reference and carrier generator consisting of a PLL and VCO, to ensure a stable carrier frequency; a high-resolution DAC to support complex modulation schemes. These high-profile hardware components are the main culprit behind the high power consumption [10].

For example, the industry’s most power efficient Wi-Fi radio consumes around 300 mW for TX and 100 mW for RX [34]. BLE consumes 5.1 mW at -20 dBm transmit power and 8.1 mW for RX [61]. ZigBee chip consumes 6.9 mW for transmission and 6 mW receiving [60]. LoRa takes 32.4 mW

Table 1: Power break down of IC implementation

	BLE [63]	SlimWiFi (Simulated)
Power amplifier	2.5 mW	43 µW
Carrier generation	0.7 mW	30 µW
Modulation	0.5 mW	∼0 µW
Rest	0.2 mW	N/A
Sum	3.9 mW	73 µW

and 14.8 mW for TX and RX, respectively [70]. Even the most advanced low power BLE IC [63] which adopts many aggressive optimizations consumes more than 3.9 mW. Table. 1 shows a breakdown of the power consumption of each component. All in all, to achieve extremely low power and open the pathways for battery-free operations, a fundamentally different architecture is needed that evades all the power hungry components.

4.2 SlimWiFi Transmitter Architecture

Owing to the asymmetric communication design (Sec. 3), the SlimWiFi device only needs to generate signals with low transmit power, low-accuracy carrier frequency, and simple OOK waveforms. Therefore, we propose the SlimWiFi active transmitter architecture shown in Fig. 12b. Compared to the traditional active transmitters, the SlimWiFi transmitter: (i) replaces the high-power PA with a low-power PA optimized for constant-amplitude signals at -20 dBm output power; (ii) replaces the closed-loop PLL+VCO with a simple open-loop oscillator; (iii) removes the DAC and uses an RF switch for OOK modulation. With such optimizations, SlimWiFi can bring the power consumption down to 73 µW in simulation. Table. 1 provides the power breakdown of SlimWiFi in comparison with the aforementioned BLE IC. Now we explain how the extremely low power is achieved.

4.2.1 Transmit power

Existing IoT radio designs aim for long-range, high throughput, and robust communication, which in turn requires a high transmit power. For example, Wi-Fi devices usually transmit at more than 20 dBm (*i.e.*, 100 mW). BLE, ZigBee, or LoRa devices are at around 0 dBm (*i.e.*, 1 mW). The transmit power, and the associated PA hardware, dominates the power consumption of the entire transmitter.

For SlimWiFi, recall it can reduce the transmit power by 18 dB while keeping the same link budget, owing to the narrower bandwidth (250 kHz) (Sec. 3). This comes at the cost of a lower bit-rate, but is a much preferred trade-off for most IoT applications, especially considering the existing Wi-Fi infrastructure can be reused. Since the Wi-Fi preamble is generated by the initiator instead of the SlimWiFi device, the PA only needs to support a narrow bandwidth and can be optimized for high efficiency. Our actual on-chip PA is optimized for -20 dBm, whose power consumption can be as low as 43 µW with 24 % drain efficiency. This would be equivalent to a Wi-Fi transmitter at $18-20=-2$ dBm, and comparable to the emission power of BLE, LoRa, and ZigBee radios.

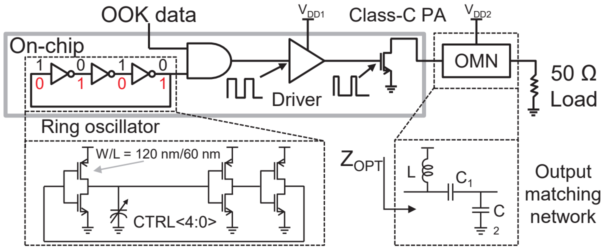


Figure 13: Circuit diagram of the SlimWiFi chip.

However, reducing the transmit power alone cannot bring the peak power to tens of µW. For example, a BLE IC [61] still consumes 4.5 mW when transmitting at -40 dBm (1 μW), and [63] still consumes 1.4 mW even without a PA (Table. 1). At an extremely low transmit power, the carrier generator and modulation blocks will become the bottleneck.

4.2.2 Open-loop carrier generation

Traditional closed-loop carrier generators are based on PLL, which can generate a highly accurate carrier frequency but consumes high power due to the requirement of phase detection. For example, typical analog PLLs for IoT consume power in the mW level [54, 71]. All digital PLLs can potentially bring down the power consumption to several hundred µW [9, 49, 63], but still around one order of magnitude higher than our target power consumption. The asymmetric demodulation design enables SlimWiFi to drastically relax the requirements of frequency stability. Instead of tolerating around 48 kHz (± 20 ppm) of carrier frequency offset as in COTS Wi-Fi devices [43], SlimWiFi works as long as its carrier falls within the 80 MHz range of the entire 2.4 GHz Wi-Fi band! Therefore, SlimWiFi can use an open-loop oscillator with low frequency accuracy as the carrier generator. More specifically, we chose an open-loop ring oscillator for the 2.4 GHz carrier generation which consumes only around 30 µW when implemented on an IC (more details in Sec. 4.3.1).

4.2.3 Low power modulation

To synchronize with the symbol clock of the Wi-Fi receiver (Sec. 3.3.1), the SlimWiFi transmitter uses an RF switch at 250 kHz switching rate to generate the OOK symbols. In fact, our IC implementation realizes OOK by simply powering on and off the PA, without the need of an additional RF switch. Since the open-loop ring oscillator's start-up time (ns level) is much shorter than the symbol period, it can also be power-cycled with the PA, which together can reduce the modulation power consumption to nearly zero.

4.3 IC design

Fig. 13 shows the circuit diagram of our SlimWiFi IC, consisting of an open-loop ring oscillator and a PA optimized for OOK signal at -20 dBm.

4.3.1 Ring oscillator

The ring oscillator consists of an odd number (3-stage in our design) of inverters cascaded into a ring, as illustrated in Fig. 13. The logic input is inverted after passing through the inverters, which causes oscillation between two voltage levels. The open-loop design circumvents the requirement of an external reference clock (*e.g.*, crystal oscillator), thus further reducing the radio cost and form-factor.

The zoom-in plot in Fig. 13 shows the detailed on-chip design of the ring oscillator. It is composed of minimum size transistors (W/ L = 120 nm/ 60 nm) for the minimum area and lowest power consumption. The ring oscillator's actual carrier frequency output is affected by the process, voltage and temperature (PVT) variations. We introduce a 5-bit binary weighted capacitor bank (CTRL$\langle 4:0 \rangle$) loading the first stage of the inverter to tune the propagation delay across different stages of the circuit. This in turn allows us to empirically adjust the oscillation frequency at design time, so it falls within the 2.4 GHz band under typical PVT conditions.

4.3.2 Class-C PA

The carrier is directly modulated by a 250 kHz data sequence and then fed to the inverter-based driver to drive a PA. We choose a Class-C PA for its easy implementation in terms of harmonic terminations and better efficiency at low output power [36]. This comes at the cost of low linearity but is acceptable for SlimWiFi since its OOK waveform is insensitive to clipping distortion (Sec 3.5.3). For a Class-C PA, the relationship between the output power P_{out}, optimal load impedance Z_{OPT} and supply voltage V_{DD} follows [36]:

$$P_{out} = V_{DD}^2/(2 \cdot Z_{OPT})$$

For the target of -20 dBm output power, the optimal load impedance can be 18 kΩ, which would be impractical to match to the standard 50 Ω. To alleviate this problem, a dual-supply voltage scheme [32] is applied for efficiency enhancement. Specifically, we use a 0.9 V V_{DD1} to supply the VCO and driver stage, and 0.3 V V_{DD2} to supply the final PA stage. Off-chip high-Q components [77] are utilized in the tapped-capacitor output matching network to achieve the impedance transformation.

Table. 2 compares the simulated IC performance with and without the PCB parasitic S-parameter (SP) model (extracted using ADS Momentum). Both simulation results are obtained with chip post-layout parasitic extraction (LPE). The table shows that, when co-simulated with the PCB SP model, the output power and efficiency are degraded, indicating that the PCB parasites can have a detrimental effect on the IC performance. This problem can be solved by integrating the capacitors on-chip to ensure a good match and carefully modeling the inductor on PCB to co-optimize the performance.

Table 2: Simulated IC performance

	LPE	LPE +PCB SP
Frequency (MHz)	2451	2438
Pout (dBm)	-19.9	-21.3
Pdrain (µW)	42.9	43.4
Pvco+driver (µW)	29.2	29.3
Drain efficiency (%)	23.7	16.9
Global efficiency (%)	14.1	10.1

Another potential solution is to replace the 50 Ω termination with a non-50 Ω antenna. For example, a patch antenna can have an input impedance of 100-400 Ω at resonance [11], which can effectively lower the impedance transformation ratio, thus reducing loss in the matching network.

4.4 Downlink ULP Receiver

To enable downlink communication for SlimWiFi, the COTS Wi-Fi transmitter needs to emulate OOK waveforms using OFDM. Such emulation has been well explored in recent cross-technology communication and backscatter systems [20, 35, 45, 67], and can be directly adopted by SlimWiFi. The resulting OOK receiver does not need a carrier generator or PA, and thus consumes even less power than the transmitter.

Considering that the TX power of the COTS Wi-Fi device can be 30 dBm, 50 dB higher than the SlimWiFi device's transmit power, a similar uplink and downlink range can be achieved even if the downlink OOK receiver's sensitivity is 50 dB worse than the uplink Wi-Fi receiver. To achieve a 100 m target range, the required receiver sensitivity is 30 dBm + 6 dBi + 2 dBi - 80 dB (FSPL) = -42 dB, which has been achieved in many existing systems. For example, [78] achieves -42.6 dBm sensitivity at 2.8 µW power; [15] achieves -50 dBm sensitivity at 4.5 µW. Much better sensitivity (smaller than -70 dBm) can be achieved with wake-up radio designs [3, 17, 30] at tens of µW power consumption.

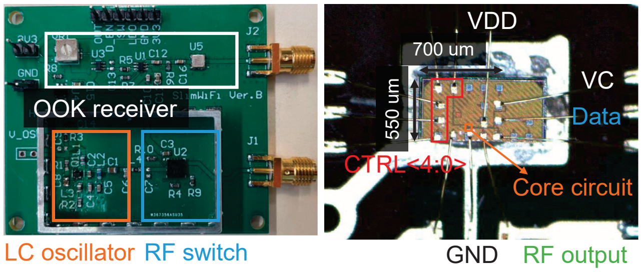
Other than the 2.4 GHz carrier, the SlimWiFi device also requires a 250 kHz symbol clock. Such low frequency clock can be generated with a ULP oscillator (*e.g.*, 0.3 µW [14]) or extracted from the 2.4 GHz carrier through a ULP fraction counting clock as proposed in [84]. The symbol clock can also be calibrated based on the downlink trigger frame which has a 250 kHz OFDM symbol rate.

5 Implementation

5.1 SlimWiFi Device

We have implemented three versions of the SlimWiFi device for different evaluation purposes.

Emulation. To benchmark the performance of the asymmetric demodulation, we need to flexibly control SlimWiFi's signal transmission, such as carrier frequency, symbol time, transmit power, *etc.* Therefore, we use the WARP software radio [56] to emulate the SlimWiFi signals. To faithfully represent the performance of a real SlimWiFi device, we carefully tune the amplitude of the samples and the RF gain of the WARP board, so that the emulated signal has a calibrated transmission power of -20 dBm, consistent with other versions of implementation.



(a) Prototype version. **(b)** IC version.

Figure 14: Two versions of the SlimWiFi device implementation.

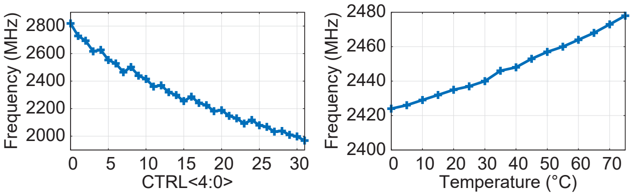
Discrete circuit prototype. The prototype version thoroughly implements both the SlimWiFi TX and RX on a PCB (Fig. 14a), and is used for end-to-end functional validation of the SlimWiFi design. Following the hardware architecture in Sec. 4.2, the TX device consists of an open-loop LC oscillator BFP720 [33] and an RF switch HMC8038 [5] for OOK modulation. The RLC components of the oscillator are carefully designed to tune the oscillation frequency to the 2.4 GHz ISM band. The OOK RX is implemented by a power detector LT5534 [6] and the sensitivity is tuned to -45 dBm. A Cmod A7 [24] FPGA evaluation board is used to process the trigger frame, synchronize the symbol clock, and generate TX data.

IC fabrication. We also tape out a SlimWiFi transmitter following Sec. 4.3 in TSMC 65 nm RF LP process [74] to evaluate its functionality and power consumption. Die photo of the fabricated chip is shown in Fig. 14b, whose core size is 30×25 µm^2. The die is directly bonded to a PCB for testing. More advanced process nodes can be utilized to further scale down the chip size and power consumption.

5.2 COTS Wi-Fi Device

We use DWA-192 [21], a Wi-Fi dongle that supports LDPC code and A-MSDU, to communicate with the SlimWiFi device. To calibrate the antenna gain, we replace the original antennas of unknown gain with two 8 dBi antennas [4]. To implement the asymmetric demodulation on this Wi-Fi receiver, we capture the data frames with CommView [73] on the user space of the PC host and implement the signal processing workflow in Matlab. No additional software, firmware, or hardware modification is needed for receiving.

For the initiation procedure discussed in 3.5.3, the DWA-192 firmware does not support the generation of a zero-payload initiation frame. As a workaround, we verified that a COTS Nexus 5 smartphone with Nexmon Wi-Fi driver [57, 69] can be used as the initiator to send the CTS-to-self, trigger frame and initiation frame, thus triggering the demodulation procedure on DWA-192. However, the signal strength of the COTS devices cannot be well calibrated and controlled which hinders us from benchmarking the impact of the power difference between the initiation frame and the SlimWiFi's signal. Therefore, we use the WARP software radio [56] to send the initiation frame for emulation-based evaluation (Sec. 6.2).



(a) Frequency v.s. CTRL$\langle 4:0 \rangle$. **(b)** Frequency v.s. temperature.

Figure 15: SlimWiFi IC carrier frequency drift corresponding to CTRL$\langle 4:0 \rangle$ and temperature.

Table 3: SlimWiFi prototype and chip performance

	Frequency (Drift)	Power Consumption @ TX Power
Emulation	Tunable	N/A @ -20 dBm
Prototype	2460 (± 5) MHz	1 mW @ -20 dBm
Simulated IC	2438 (± 10) MHz	73 µW @ -21 dBm
Fabricated IC	2465 (± 10) MHz	90 µW @ -24 dBm

6 System Evaluation

Our evaluation mainly focuses on the SlimWiFi uplink, since the OFDM-to-OOK downlink has been studied in prior research (Sec. 4.4).

6.1 SlimWiFi Device Microbenchmark

We first benchmark the different implementations of the SlimWiFi device. Table. 3 summarizes some important parameters of the SlimWiFi device.

Carrier frequency. We first profile the frequency stability of the SlimWiFi IC with the open-loop ring oscillator. Fig. 15a illustrates the measured carrier frequency when varying the CTRL$\langle 4:0 \rangle$ from 0 to 31 with 0.95 V supply voltage at room temperature (25 $^\circ C$). We see that the ring oscillator design achieves a wide tuning range (around 1 GHz) and fine steps (30 MHz) compared to the 80 MHz frequency tolerance. In addition, as shown in Fig. 15b, the frequency variance is within 54 MHz even when considering a very wide temperature range of 0 to 75 $^\circ C$. Therefore, it suffices to perform a one-time calibration to tune the oscillator to the center of the the 2.4 GHz band and let it run freely.

We found that the emulated and prototype version of SlimWiFi show consistent behavior compared with the IC version. The prototype board also has an inaccurate carrier frequency, though a relatively lower drift (around 5 MHz). The WARP setup can emulate arbitrary carrier frequencies for evaluation purposes.

Power consumption and transmit power. The discrete prototype version of the SlimWiFi transmitter consumes around 1 mW power when transmitting at -20 dBm. This is already superior to state-of-the-art IoT ICs (Sec. 4). The chip version further cuts the power consumption by an order of magnitude owing to the highly optimized oscillator and PA. Sub-100 µW of power consumption is achieved, for both the simulated and fabricated SlimWiFi chips. The measured

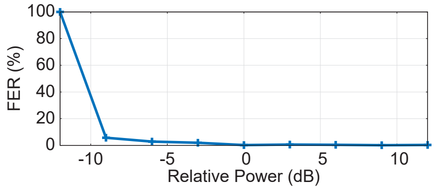


Figure 16: Frame error rate with different relative power between the SlimWiFi signal and the initiation signal.

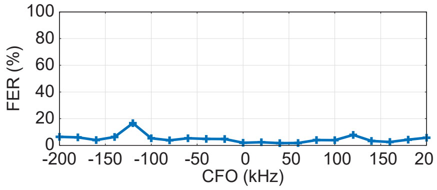


Figure 17: Frame error rate under different carrier frequency offset.

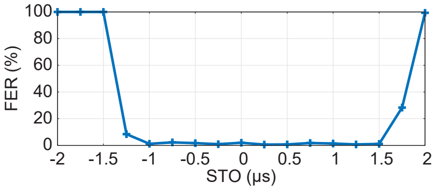


Figure 18: Frame error rate under different symbol time offset.

output power is -24 dBm, which is 3 dB lower than the simulated results. We suspect this is due to the tolerance of the inductor and capacitors used for the high-Q output matching and/or the PCB parasitics (*e.g.* bond wire inductance) not fully captured by the EM simulation. We expect much lower power consumption and a higher PA efficiency is feasible by optimizing the PCB peripherals and by using advanced fabrication processes (lower than 65 nm).

6.2 Microbenchmark for Asymmetric Demodulation

The demodulation performance depends on various parameters, including CFO, symbol time offset (STO), receiver gain, *etc.* Since SlimWiFi uses an open-loop carrier generator that keeps drifting, it is impossible to manually fix these parameters for controlled experiments. We thus calibrated the signal strength and used WARP to decouple and benchmark the impact of each parameter individually.

We conduct link-level experiments in an outdoor parking space, with the following default configurations of the Wi-Fi receiver: 20 MHz 802.11n OFDM, 64-QAM modulation, LDPC coding with 5/6 coding rate and 7935 bytes frame length. Meanwhile, we use WARP to emulate the SlimWiFi device transmitting OOK modulated signals with a frame length of 240 bits and 1/2 BCC coding rate. By default, the link distance is 20 m.

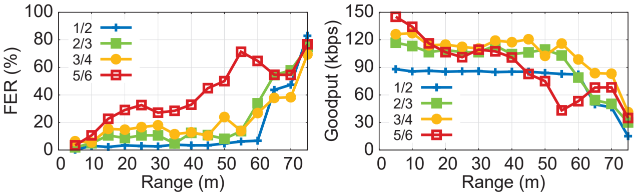
Impact of receiver gain. Recall that the mismatch of signal strength between the initiation signal and the SlimWiFi signal may mislead the Wi-Fi receiver towards a suboptimal gain setting (Sec. 3.5.3). To evaluate its impact, we use the WARP board to transmit the initiation frame along with the emulated signal, so that the strength difference can be intentionally controlled. We consider the relative power of the emulated SlimWiFi signal as 0 dB when the signal strength is the same as that of one subcarrier in the initiation frame. Fig. 16 shows that the receiver performance does not degrade significantly until the relative power is lower than -9 dB, when the receiver gain is too low for robust demodulation. This corroborates our explanation in Sec. 3.5.3. Therefore, instead of adjusting the power of the initiation frame which will lead to complicated management overhead, we can just transmit an initiation frame at a fixed low power. By default, our experiments control the relative power to -6 dB to prevent degrading the demodulation performance.

Impact of carrier frequency offset. Note that the 802.11n subcarrier spacing is 312.5 kHz, and asymmetric demodulation works as long as the SlimWiFi signals overlap with one of the subcarriers. We thus only evaluate the case when the SlimWiFi transmitter's carrier frequency deviates from a representative Wi-Fi subcarrier 15. To achieve higher SNR, we combine the samples of the two subcarriers that partially overlap with SlimWiFi's signals, only when the frequency offsets by 140 to 180 kHz (around half of the subcarrier width). Otherwise, the combination may induce more noise (Sec. 3.3.2). With this setting, the worst-case SNR loss is only 3 dB, *i.e.*, when nearly half of the signal power spills into an unusable adjacent subcarrier. To summarize, the asymmetric demodulator can tolerate arbitrary frequency offsets of the SlimWiFi signals in common cases.

Impact of synchronization. To evaluate how the symbol time offset (STO) influences the receiver performance, we manually introduced a delay between the emulated SlimWiFi signal and the initiation frame (both transmitted by the WARP board). The result in Fig. 18 shows that within an STO from -1 μs to 1.5 μs, the receiver performance is not affected in a noticeable manner. Therefore, the system performance should not be affected by the STO since a much better symbol level synchronization can be achieved by the OOK receiver [78,79]. Notably, the performance is not symmetric around 0 offset (*i.e.*, there is around 0.5 µs more tolerance on positive STO), because of the 0.8 µs redundancy introduced by the CP.

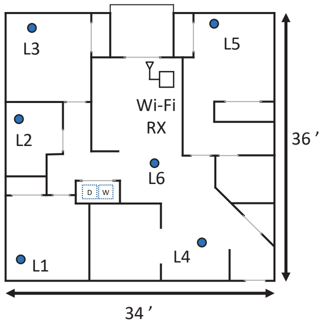
Range and coding rate on SlimWiFi device. Fig. 19a and Fig. 19b show the frame error rate (FER) and goodput with different link distances and BCC coding rate (applied on the data from SlimWiFi device to combat with the coding error discussed in Sec. 3.4.2). The goodput is calculated by only counting the frames with no bit error and including the overhead of channel access, initiation, and trigger frame as discussed in Sec. 2. It can be seen that SlimWiFi maintains a low FER of below 5% even at 60 m of communication range. A goodput of around 100 kbps can be achieved within the range of 60 m. A higher coding rate leads to higher goodput, with some sacrifice on the FER.

Non-line-of-sight (NLoS). We finally evaluate SlimWiFi in an indoor NLoS environment with rich multipath. Fig. 20 shows the deployment setup. We place the Wi-Fi receiver in the living room of a 3B2B apartment, and vary the location of the SlimWiFi transmitter (emulated by WARP). It can be



(a) Frame error rate. **(b)** Goodput.

Figure 19: Performance of the asymmetric demodulation receiver *w.r.t.* (a) frame error rate (FER) and (b) goodput at different range and coding rate.



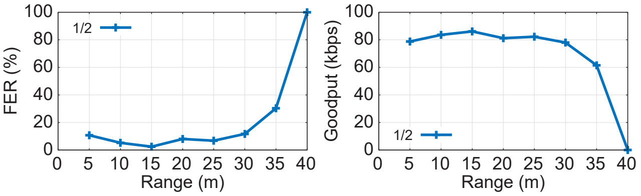
Location	FER
L1	1.382%
L2	0.311%
L3	0.340%
L4	0.218%
L5	0.411%
L6	0.043%

Figure 20: Experimental setup and result for NLoS deployment.

seen that a FER lower than 0.5% is achieved for all the locations except “L1”, despite the multipath and under NLoS. A FER of 1.3% can be achieved at “L1” even though the emulated transmitter is placed at the furthest end of the apartment with 2 concrete walls blocking the LoS. We note that the non-coherent demodulation of SlimWiFi is insensitive to the signals’ phase variations and naturally resilient to the multipath effects. In addition, as discussed in Sec. 4.2.1, although SlimWiFi bears a low transmit power, it still keeps an ample link budget owing to the high sensitivity of asymmetric demodulation, thereby easily achieving whole-home coverage even with NLoS links.

6.3 System Level Evaluation

We now put the workflow in Fig. 2 together and evaluate the SlimWiFi system end-to-end. We use the prototype SlimWiFi device to transmit an OOK signal with a 1/2 coding rate. The initiator’s output power is tuned for the highest receiving gain. The experiments are conducted in an outdoor parking lot. Fig. 21 shows that SlimWiFi can achieve a working range of around 30 m at a FER of 11% and goodput of 78.0 Kbps, and 35 m at a FER of 30% and goodput of 61.5 Kbps. Compared to the result in Fig. 19, the range is reduced by around 1/2. This is reasonable because the impacts of receiver gain, CFO, synchronization error, *etc.* are combined together. For example, unlike the emulated SlimWiFi device, the carrier frequency of the prototype device or IC is not strictly controlled. The resulting carrier frequency offset is unpredictable and will cause up to 3 db of SNR loss (Sec. 6.2) which translates into a range reduction. The result also indicates that the proposed symbol synchronization scheme based on a simple OOK receiver can satisfy the synchronization requirement.



(a) Frame error rate. **(b)** Goodput.

Figure 21: Performance of the SlimWiFi system *w.r.t.* (a) frame error rate (FER) and (b) goodput at different range.

7 Discussion

Other Wi-Fi standards. We use 802.11n Wi-Fi as the Internet gateway for SlimWiFi devices because the 802.11n standard is supported by mainstream Wi-Fi devices. Other OFDM-based Wi-Fi standards can also support asymmetric modulation, albeit with a few limitations: 802.11a/ac only resides in the 5 GHz band which is not ideal for ULP communication due to the larger path loss; 802.11g, the predecessor of 802.11n, does not support A-MSDU and hence can only accommodate 70 OOK symbols in one frame (Sec. 3.5.1); 802.11ax devices are still not widely deployed and the longer symbol period will lead to lower SlimWiFi throughput.

Initiating the Wi-Fi demodulation. The current SlimWiFi implementation requires an initiator as a workaround to trigger the standard Wi-Fi receiver’s demodulation procedure (Sec. 3.5.3). We expect a firmware update to the receiver can enable its self-triggering of the demodulation following the CTS-to-self, as discussed in Sec. 3.5.3. An alternative way to circumvent the initiator is to use the spectral scan function of certain Wi-Fi cards (*e.g.*, the Atheros Wi-Fi [48]), which can continuously report the samples before the QAM block without explicit triggering. We leave the implementation of these approaches for future work.

Ethical consideration. This paper does not involve human subjects and thus does not raise any ethical issues.

8 Related Work

Low-power communication hardware. ULP radio hardware design has been the holy grail of the IoT industry. Many RFIC techniques have been proposed for ULP radios, such as harmonic injection-locked carrier generator [28, 46, 64], crystal-free design [13, 65], power oscillator [58], *etc.* However, these radical radio designs are incompatible with existing IoT network infrastructures. In contrast, SlimWiFi demonstrates for the first time that signals from a ULP OOK radio can be demodulated by a COTS Wi-Fi device. The SlimWiFi ULP radio is extremely simple and can be easily mass-produced and embraced into the existing IoT ecosystem.

We note that most modern network standards have protocol-level power-saving mechanisms [1, 23, 43] based on sleep

Table 4: Comparing SlimWiFi with representative state-of-the-art low-power communication

	Radio architecture	Power	Data rate	Interference	Range	Infrastructure
Wi-Fi [34]	Active	100s mW	High	Low	Long	COTS Wi-Fi
BLE [62]	Active	$\sim$ 5 mW	Medium	Low	Medium	COTS BLE
Wi-Fi backscatter [41]	Direct backscatter	1s µW	Low	Low	Short	COTS Wi-Fi
Braidio [29]	Direct backscatter	10s µW	Medium	Low	Short	Customized device
PassiveWiFi [42]	FS backscatter	10s µW	Medium to high	High	Medium	Single tone generator + COTS Wi-Fi
HitchHike [79]	FS backscatter	10s µW	Medium	High	Medium	COTS Wi-Fi
SlimWiFi	Slim active	10s µW	Medium	Low	Long	COTS Wi-Fi

scheduling. These mechanisms cannot reduce the peak power consumption–a more essential metric for battery-free communication hardware. Nevertheless, they are complementary to the SlimWiFi design and can be used to further reduce its average power consumption.

Cross technology communication (CTC). The primary motivation behind CTC is to allow different communication standards to exchange messages, so as to reduce interference and enable sharing of data/control information. Recent work has explored both receiver-transparent CTC [18, 20, 39, 44, 45, 50] and transmitter-transparent CTC [26, 37, 38, 51]. However, CTC mainly sticks to the complex modulation adopted by the COTS IoT devices. In contrast, SlimWiFi aims to design the SlimWiFi signal so that it can be effectively decoded by high-profile OFDM demodulators while relaxing the hardware requirement of the transmitter. In addition, existing CTC systems can not be used in ULP settings due to two reasons. First, none of the existing CTC designs can reduce power consumption because they rely on standard transceivers such as Wi-Fi, BLE, ZigBee, and LoRa. Second, they have relatively low communication performance. For example, the recently proposed XFi [51] can only reach 10 m range at 3% FER. For such CTC systems, the majority of the energy is wasted to maintain an unreliable link between heterogeneous hardware, which is not desired in ULP IoT applications. In contrast, SlimWiFi is optimized to achieve a reasonable communication performance targeting IoT applications, with around 3 orders of magnitude lower power than standard transceivers.

Backscatter communication. Recent work has extended classical UHF RFID backscatter communication to realize ambient backscatter, which piggybacks on existing communication links to convey information. For example, Wi-Fi backscatter *et al.* [12, 29, 41, 52, 68] adopt direct backscatter where the tag data is directly modulated to the excitation signal. But due to the self-interference, they usually operate within a very short range and have a very low data rate. PassiveWiFi *et al.* [42, 72, 76, 81, 84] introduces frequency shifting backscattering to deal with the self-interference issues. A single-tone excitation signal is required as an RF carrier source for a low-power backscatter tag, and the tag can reflect and remodulate standard-compatible signals (Wi-Fi, BLE, LTE, ZigBee, *etc.*). HitchHike *et al.* [19, 25, 35, 44, 53, 78–80, 83] apply codeword translation, so that a COTS transmitter, instead of a dedicated single-tone generator, can be used as an excitation signal source.

Tab. 4 compares SlimWiFi with the representative communication schemes discussed above. Unlike these systems that backscatter signals from existing links, the SlimWiFi device is a *standalone active transmitter* and does not require an external RF carrier signal transmitter. Moreover, as verified in [22], Wi-Fi backscatter systems can cause interference to adjacent Wi-Fi channels, and may inadvertently remodulate and interfere with 5G NR links due to lack of frequency selectivity. Active transmitters like SlimWiFi do not have such out-of-band interference problems. On the other hand, the asymmetric demodulation design in SlimWiFi can also facilitate existing backscatter systems. Owing to the asymmetric demodulation design of SlimWiFi, the backscatter tag can generate a simple modulated signal instead of the sophisticated Wi-Fi compatible signal. Therefore, the tag can evade the need for an accurate and high frequency (tens of MHz) clock source for channel level frequency shifting, which can potentially cut its power consumption by multi-folds.

9 Conclusion

To our knowledge, SlimWiFi represents the first active OOK-modulated radio that can directly communicate with existing Wi-Fi infrastructures. Such asymmetric communication capabilities enable radical simplifications to the radio architecture, opening pathways towards standalone, battery-free Wi-Fi compatible IoT communication. Our SlimWiFi IC achieves a peak power consumption of 90 µW, but still leaves ample space for optimization, *e.g.*, through more advanced fabrication processes. The asymmetric communication paradigm can be similarly applied to other wireless standards, which we leave for future exploration.

Acknowledgments

We thank our shepherd Rajalakshmi Nandakumar and the anonymous reviewers for their insightful comments and feedback. The work reported in this paper is supported in part by the NSF under Grant CNS-1901048, CNS-1925767, and CNS-2128588.

References

[1] 3GPP. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072.

[2] ALFA Network Inc. AWUS036ACM. https://www.alfa.com.tw/products/awus036acm.

[3] Erkan Alpman, Ahmad Khairi, Richard Dorrance, Minyoung Park, V. Srinivasa Somayazulu, Jeffrey R. Foerster, Ashoke Ravi, Jeyanandh Paramesh, and Stefano Pellerano. 802.11g/n compliant fully integrated wake-up receiver with -72-dbm sensitivity in 14-nm finfet cmos. *IEEE Journal of Solid-State Circuits*, 53(5):1411–1422, 2018.

[4] Amazon. 2 x 8dBi WiFi RP-SMA Male Antenna 2.4GHz 5.8GHz Dual Band. https://www.amazon.com/Antenna-Pigtail-Wireless-Routers-Repeater/dp/B07R21LN5P/ref=pd_lpo_1?pd_rd_i=B07R21LN5P&psc=1.

[5] Analog Devices. HMC8038. https://www.analog.com/en/products/hmc8038.html.

[6] Analog Devices. LT5534. https://www.analog.com/en/products/lt5534.html.

[7] ASUSTeK Computer Inc. RT-AC68U. https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RTAC68U/.

[8] ASUSTeK Computer Inc. RT-AX3000. https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-WiFi-Routers/RT-AX3000/.

[9] Masoud Babaie, Feng-Wei Kuo, Huan-Neng Ron Chen, Lan-Chou Cho, Chewn-Pu Jou, Fu-Lung Hsueh, Mina Shahmohammadi, and Robert Bogdan Staszewski. A fully integrated bluetooth low-energy transmitter in 28 nm cmos with 36% system efficiency at 3 dbm. *IEEE Journal of Solid-State Circuits*, 51(7):1547–1565, 2016.

[10] Torikul Islam Badal, Mamun Bin Ibne Reaz, Mohammad Arif Sobhan Bhuiyan, and Noorfazila Kamal. Cmos transmitters for 2.4-ghz rf devices: Design architectures of the 2.4-ghz cmos transmitter for rf devices. *IEEE Microwave Magazine*, 20(1), 2019.

[11] Constantine A Balanis. *Antenna Theory: Analysis and Design*. John Wiley & Sons, 2016.

[12] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. Backfi: High throughput wifi backscatter. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 283–296, New York, NY, USA, 2015. Association for Computing Machinery.

[13] Mengye Cai, Alireza Asoodeh, Yi Luo, and Shahriar Mirabbasi. An ultralow-power crystal-free batteryless tdd radio for medical implantable applications. *IEEE Transactions on Microwave Theory and Techniques*, 68(11):4875–4885, 2020.

[14] Sheng-Kai Chang, Zhi-Ting Tsai, and Kuang-Wei Cheng. A 250 khz resistive frequency-locked on-chip oscillator with 24.7 ppm/°c temperature stability and 2.73 ppm long-term stability. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–4, 2020.

[15] Shih-En Chen, Chin-Lung Yang, and Kuang-Wei Cheng. A 4.5 μw 2.4 ghz wake-up receiver based on complementary current-reuse rf detector. pages 1214–1217, 2015.

[16] Xing Chen, Jacob Breiholz, Farah B. Yahya, Christopher J. Lukas, Hun-Seok Kim, Benton H. Calhoun, and David D. Wentzloff. Analysis and design of an ultralow-power bluetooth low-energy transmitter with ring oscillator-based adpll and 4 × frequency edge combiner. *IEEE Journal of Solid-State Circuits*, 54(5):1339–1350, 2019.

[17] Kuang-Wei Cheng and Shih-En Chen. An ultralow-power ook/bfsk/dbpsk wake-up receiver based on injection-locked oscillator. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 29(7):1379–1391, 2021.

[18] Zicheng Chi, Yan Li, Yao Yao, and Ting Zhu. Pmc: Parallel multi-protocol communication to heterogeneous iot radios within a single wifi channel. In *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, pages 1–10, 2017.

[19] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. Leveraging ambient lte traffic for ubiquitous passive communication. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 172–185, New York, NY, USA, 2020. Association for Computing Machinery.

[20] Hsun-Wei Cho and Kang G. Shin. Bluefi: Bluetooth over wifi. In *Proceedings of the ACM SIGCOMM Conference*, 2021.

[21] D-Link. DWA-192. https://us.dlink.com/en/products/dwa-192-ac1900-ultra-wi-fi-usb-adapter.

[22] Farzan Dehbashi, Ali Abedi, Tim Brecht, and Omid Abari. Verification: Can wifi backscatter replace rfid? In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2021.

[23] Artem Dementyev, Steve Hodges, Stuart Taylor, and Joshua Smith. Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario. In *2013 IEEE International Wireless Symposium (IWS)*, pages 1–4, 2013.

[24] Digilent. Cmod A7. https://digilent.com/reference/programmable-logic/cmod-a7/start.

[25] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter communication. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2021.

[26] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Zihao Yu, and Yunhao Liu. Lego-fi: Transmitter-transparent ctc with cross-demapping. *IEEE Internet of Things Journal*, 8(8):6665–6676, 2021.

[27] Mohammad Hasan. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. https://iot-analytics.com/number-connected-iot-devices/.

[28] Huan Hu, Chung-Ching Lin, and Subhanshu Gupta. A 197.1-μw wireless sensor soc with an energy-efficient analog front-end and a harmonic injection-locked ook tx. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(6):2444–2456, 2021.

[29] Pan Hu, Pengyu Zhang, Mohammad Rostami, and Deepak Ganesan. Braidio: An integrated active-passive radio for mobile devices with asymmetric energy budgets. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, page 384–397, New York, NY, USA, 2016. Association for Computing Machinery.

[30] Xiongchuan Huang, Simonetta Rampu, Xiaoyan Wang, Guido Dolmans, and Harmke de Groot. A 2.4ghz/915mhz 51µw wake-up receiver with offset and noise suppression. In *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, pages 222–223, 2010.

[31] Hugues Anguelkov. Reverse-engineering Broadcom wireless chipsets. https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html.

[32] Shunta Iguchi, Akira Saito, Kazunori Watanabe, Takayasu Sakurai, and Makoto Takamiya. Design method of class-f power amplifier with output power of $-$ 20 dbm and efficient dual supply voltage transmitter. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(10):2978–2986, 2014.

[33] Infineon Technologies. BFP720. https://www.infineon.com/cms/en/product/rf/rf-transistor/low-noise-rf-transistors/bfp720/.

[34] InnoPhase. Talaria TWO Modules. https://innophaseinc.com/talaria-two-modules/.

[35] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *Proceedings of the 2016 ACM SIGCOMM Conference*, 2016.

[36] Daechul Jeong, Hankyu Lee, Taeyoung Chung, Seokwon Lee, Jaesup Lee, and Bumman Kim. Optimized ultralow-power amplifier for ook transmitter with shaped voltage drive. *IEEE Transactions on Microwave Theory and Techniques*, 64(8):2615–2622, 2016.

[37] Woojae Jeong, Jinhwan Jung, Yuanda Wang, Shuai Wang, Seokwon Yang, Qiben Yan, Yung Yi, and Song Min Kim. Sdr receiver using commodity wifi via physical-layer signal reconstruction. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2020.

[38] Wenchao Jiang, Song Min Kim, Zhijun Li, and Tian He. Achieving receiver-side cross-technology communication with cross-decoding. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, page 639–652, New York, NY, USA, 2018. Association for Computing Machinery.

[39] Wenchao Jiang, Zhimeng Yin, Ruofeng Liu, Zhijun Li, Song Min Kim, and Tian He. Bluebee: A 10,000x faster cross-technology communication via phy emulation. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2017.

[40] Mohamad Katanbaf, Anthony Weinand, and Vamsi Talla. Simplifying backscatter deployment: Full-Duplex LoRa backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2021.

[41] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R. Smith, and David Wetherall. Wi-fi backscatter: Internet connectivity for rf-powered devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, page 607–618, New York, NY, USA, 2014. Association for Computing Machinery.

[42] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. Passive Wi-Fi: Bringing low power to Wi-Fi transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016.

[43] LAN/MAN Standards Committee of the IEEE Computer Society. Ieee standard for information technology–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. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pages 1–4379, 2021.

[44] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2018.

[45] Zhijun Li and Tian He. Webee: Physical-layer cross-technology communication via emulation. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2017.

[46] Chung-Ching Lin, Huan Hu, and Subhanshu Gupta. Improved performance tradeoffs in harmonic injection-locked ulp tx for sub-ghz radios. *IEEE Transactions on Microwave Theory and Techniques*, 69(6):2885–2898, 2021.

[47] Linux Wireless. About mac80211. https://wireless.wiki.kernel.org/en/developers/documentation/mac80211.

[48] Linux Wireless. ath9k spectral scan. https://wireless.wiki.kernel.org/en/users/drivers/ath9k/spectral_scan.

[49] Hanli Liu, Dexian Tang, Zheng Sun, Wei Deng, Huy Cu Ngo, and Kenichi Okada. A sub-mw fractional- N adpll with fom of -246 db for iot applications. *IEEE Journal of Solid-State Circuits*, 53(12):3540–3552, 2018.

[50] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Lte2b: Time-domain cross-technology emulation under lte constraints. In *Proceedings of the 17th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2019.

[51] Ruofeng Liu, Zhimeng Yin, Wenchao Jiang, and Tian He. Xfi: Cross-technology iot data collection via commodity wifi. In *IEEE International Conference on Network Protocols (ICNP)*, 2020.

[52] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. Ambient backscatter: Wireless communication out of thin air. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 39–50, New York, NY, USA, 2013. Association for Computing Machinery.

[53] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. Verification and redesign of OFDM backscatter. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2021.

[54] Yao-Hong Liu, Johan Van Den Heuvel, Takashi Kuramochi, Benjamin Busze, Paul Mateman, Vamshi Krishna Chillara, Bindi Wang, Robert Bogdan Staszewski, and Kathleen Philips. An ultra-low power 1.7-2.7 ghz fractional-n sub-sampling digital frequency synthesizer and modulator for iot applications in 40 nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(5), 2017.

[55] Paolo Madoglio, Hongtao Xu, Kailash Chandrashekar, Luis Cuellar, Muhammad Faisal, William Yee Li, Hyung Seok Kim, Khoa Minh Nguyen, Yulin Tan, Brent Carlton, Vaibhav Vaidya, Yanjie Wang, Thomas Tetzlaff, Satoshi Suzuki, Amr Fahim, Parmoon Seddighrad, Jianyong Xie, Zhichao Zhang, Divya Shree Vemparala, Ashoke Ravi, Stefano Pellerano, and Yorgos Palaskas. 13.6 a 2.4ghz wlan digital polar transmitter with synthesized digital-to-time converter in 14nm trigate/finfet technology for iot and wearable applications. In *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 226–227, 2017.

[56] Mango Communications. Wireless Open-Access Research Platform (WARP), 2016.

[57] Matthias Schulz, Daniel Wegemer and Matthias Hollick. Nexmon: The C-based Firmware Patching Framework. https://nexmon.org/.

[58] Patrick P. Mercier, Saurav Bandyopadhyay, Andrew C. Lysaght, Konstantina M. Stankovic, and Anantha P. Chandrakasan. A sub-nw 2.4 ghz transmitter for low data-rate sensing applications. *IEEE Journal of Solid-State Circuits*, 49(7):1463–1474, 2014.

[59] NETGEAR. AX1800 WiFi Router (RAX20). https://www.netgear.com/home/wifi/routers/rax20/.

[60] Nordic Semiconductor. NCS36510. https://www.onsemi.com/products/wireless-connectivity/wireless-rf-transceivers/ncs36510.

[61] Nordic Semiconductor. nRF5340. https://www.nordicsemi.com/Products/nRF5340.

[62] NXP Semiconductors. QN908x. https://www.nxp.com/products/wireless/bluetooth-low-energy/qn908x-ultra-low-power-bluetooth-low-energy-system-on-chip-solution:QN9080.

[63] SeongJin Oh, SungJin Kim, Imran Ali, Truong Thi Kim Nga, DongSoo Lee, YoungGun Pu, Sang-Sun Yoo, Minjae Lee, Keum Cheol Hwang, Youngoo Yang, and Kang-Yoon Lee. A 3.9 mw bluetooth low-energy transmitter using all-digital pll-based direct fsk modulation in 55 nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(9), 2018.

[64] Jagdish Pandey and Brian P. Otis. A sub-100 μ w mics/ism band transmitter based on injection-locking and frequency multiplication. *IEEE Journal of Solid-State Circuits*, 46(5):1049–1058, 2011.

[65] Giuseppe Papotto, Francesco Carrara, Alessandro Finocchiaro, and Giuseppe Palmisano. A 90-nm cmos 5-mbps crystal-less rf-powered transceiver for wireless sensor network nodes. *IEEE Journal of Solid-State Circuits*, 49(2):335–346, 2014.

[66] Naser Pourmousavian, Feng-Wei Kuo, Teerachot Siriburanon, Masoud Babaie, and Robert Bogdan Staszewski. A 0.5-v 1.6-mw 2.4-ghz fractional-n all-digital pll for bluetooth le with pvt-insensitive tdc using switched-capacitor doubler in 28-nm cmos. *IEEE Journal of Solid-State Circuits*, 53(9):2572–2583, 2018.

[67] Mohammad Rostami, Xingda Chen, Yuda Feng, Karthikeyan Sundaresan, and Deepak Ganesan. Mixiq: Re-thinking ultra-low power receiver design for next-generation on-body applications. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2021.

[68] Mohammad Rostami, Jeremy Gummeson, Ali Kiaghadi, and Deepak Ganesan. Polymorphic radios: A new design paradigm for ultra-low power communication. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, page 446–460, New York, NY, USA, 2018. Association for Computing Machinery.

[69] Matthias Schulz, Jakob Link, Francesco Gringoli, and Matthias Hollick. Shadow wi-fi: Teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over wi-fi. In *Proceedings of the 16th ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018.

[70] SEMTECH. SX1261. https://www.semtech.com/products/wireless-rf/lora-core/sx1261.

[71] Kuan-Yueh Shen, Syed Feruz Syed Farooq, Yongping Fan, Khoa Minh Nguyen, Qi Wang, Mark L. Neidengard, Nasser Kurd, and Amr Elshazly. A flexible, low-power analog pll for soc and processors in 14nm cmos. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(7), 2018.

[72] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), sep 2017.

[73] TamoSoft. CommView for WiFi. https://www.tamos.com/products/commwifi/.

[74] TSMC. 65nm RF LP Process. https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_65nm.

[75] Rudd J.M. Vullers, Rob van Schaijk, Hubregt J. Visser, Julien Penders, and Chris Van Hoof. Energy harvesting for autonomous wireless sensor networks. *IEEE Solid-State Circuits Magazine*, 2(2), 2010.

[76] Anran Wang, Vikram Iyer, Vamsi Talla, Joshua R. Smith, and Shyamnath Gollakota. FM backscatter: Enabling connected cities and smart fabrics. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2017.

[77] Kejia Wang, Sravya Alluri, Xinyu Zhang, and Vincent W. Leung. A sub-100μw 2ghz ook pa for iot applications. In *IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS)*, 2022.

[78] Po-Han Peter Wang, Chi Zhang, Hongsen Yang, Dinesh Bharadia, and Patrick P. Mercier. 20.1 a 28μw iot tag that can communicate with commodity wifi transceivers via a single-side-band qpsk backscatter communication technique. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 312–314, 2020.

[79] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. Hitchhike: Practical backscatter using commodity wifi. In *Proceedings of the ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2016.

[80] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. Freerider: Backscatter communication using commodity radios. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT)*, 2017.

[81] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. Enabling practical backscatter communication for on-body sensors. In *Proceedings of the*

2016 ACM SIGCOMM Conference, SIGCOMM '16, page 370–383, New York, NY, USA, 2016. Association for Computing Machinery.

[82] Xuan Zhang and Alyssa B. Apsel. A low-power, process-and- temperature- compensated ring oscillator with addition-based current source. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 58(5):868–878, 2011.

[83] Jia Zhao, Wei Gong, and Jiangchuan Liu. Spatial stream backscatter using commodity wifi. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018.

[84] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. Ofdma-enabled wi-fi backscatter. In *The 25th Annual International Conference on Mobile Computing and Networking*, MobiCom '19, New York, NY, USA, 2019. Association for Computing Machinery.

[85] Jim Zyren and Al Petrick. Tutorial on Basic Link Budget Analysis. http://www.sss-mag.com/pdf/an9804.pdf.

A FEC Errors in Asymmetric Demodulation

In this section, we discuss the behavior of BCC and LDPC when decoding a non-Wi-Fi frame which supports our design in Sec. 3.4.2

A.1 BCC

Viterbi algorithm is widely adopted for BCC decoding. To achieve the maximum likelihood decoding, the algorithm searches among all valid codewords $\{C\}$, to identify the codeword C^l which has the shortest Hamming distance with the input bit sequence. It then outputs the decoded bit sequence Y which can generate the codeword C^l by performing BCC encoding. This means that when we use the decoded bits Y to get the regenerated bits, the regenerated bits $X' = C^l$ will be the exact codeword that has the shortest hamming distance with the original bit sequence X. Since the demodulated bit sequence X has a very low chance to be the same as a valid codeword, the mismatch between X' and X is almost inevitable. However, we found that the number of mismatches between regenerated bit sequence X' and demodulated bit sequence X has an upper limit. Here we provide a quick proof.

For the BCC code with the basic coding rate 1/2, the codewords are generated by bitwise XOR in Eq. 1 where $d[k]$ is the k-th input data bit and $c_1[k]$ and $c_2[k]$ are the corresponding bits in the codeword.

$$\begin{aligned} c_1[k] &= d[k] \oplus d[k-2] \oplus d[k-3] \oplus d[k-5] \oplus d[k-6] \\ c_2[k] &= d[k] \oplus d[k-1] \oplus d[k-2] \oplus d[k-3] \oplus d[k-6] \end{aligned} \tag{1}$$

Consider a data sequence $D = \{d[1], d[2], \dots, d[K]\}$ where K is the length of the input sequence. The corresponding codeword will be $C = \{c_1[1], c_2[1], \cdot, c_1[K], c_2[K]\}$. For one valid codeword C^l generated by D^l, the bitwise inverted version (complementary codeword) $\bar{C}^l = C^l \oplus 1$ will also be a valid codeword whose corresponding data bits is $\bar{D}^l = D^l \oplus 1$. When we get the regenerated bit sequence $X' = C^l$, if the mismatch number between X' and X is more than 1/2 of the total bit number, the mismatch number between $\bar{C}^l$ and X will be smaller than 1/2 of the total bit number. Therefore, the hamming distance between X' and X will be higher than $\bar{C}^l$ and X, which is against the shortest hamming distance principle of the decoder. Therefore, the number of mismatches between regenerated bit sequence X' and demodulated bit sequence X should be lower than 1/2 of the total bit number. Fig. 22 gives an example that illustrates the proof.

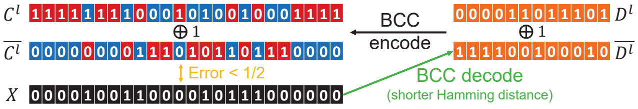


Figure 22: An example of the BCC decoding with complementary codewords at 1/2 coding rate.

For a higher coding rate, the codeword is generated by puncturing the codeword generated by the basic coding rate. Fig. 23 provides an example of how the puncturing is conducted with a 3/4 coding rate while processing the same sequence in Fig. 22. So the proof still holds, but only for the depunctured sequence. Therefore, to reduce the number of mismatches, we should choose the highest coding rate of 5/6.

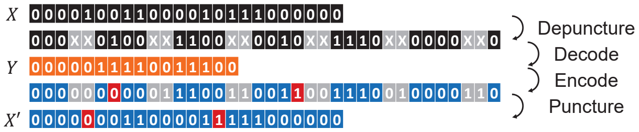


Figure 23: An example of the BCC decoding and regeneration at 3/4 coding rate.

In the previous proof, we only explained the BCC decoding with a hard decision and optimal maximum likelihood decoding. In practice, the error number might vary when considering the soft decision and imperfect maximum-likelihood decoder implementation. But the variation will not diverge the claim.

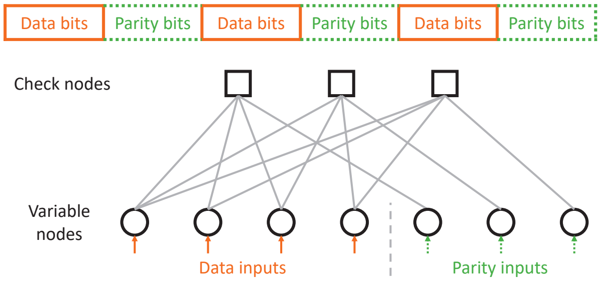


Figure 24: Bit sequence slicing of LDPC coding and an example connection between data bits and parity bits corresponding to one parity-check matrix.

A.2 LDPC

As illustrated in Fig. 24, an LDPC-coded bit sequence is organized into blocks. Each block consists of data bits and parity bits. A predefined parity-check matrix characterizes the connection between variable nodes and check nodes. For LDPC decoding, belief propagation decoders based on the message-passing algorithm are widely adopted. For a soft decision decoder, the inputs of the variable nodes are log-likelihood of the corresponding bits instead of quantized bits. The decoder iteratively updates the log-likelihood of the variable nodes and check nodes based on the inputs and the previous status of the nodes by using the sum-product or min-sum algorithm. After iteratively repeating the log-likelihood update, whether the data or parity bits should be flipped will be determined by the final bit log-likelihood of the variable nodes. The bit-flip of the variable nodes happens when the sum of the log-likelihood from the connected check nodes is larger than the input, which in exchange requires that the inputs have a predefined relation corresponding to the parity-check matrix.

Specific to the SlimWiFi asymmetric demodulation, the bit-flip ratio will be extremely low. This is mainly because the inputs are from the OOK signal which does not have the aforementioned relation. Under such conditions, the LDPC decoder is ineffective when decoding, and thus an extremely limited number of the demodulated bits will be falsely “corrected”. A theoretical proof of this conclusion can be found in [51]. Therefore, the data bits part of the regenerated bit sequence will be nearly the same as that of the demodulated bit sequence.

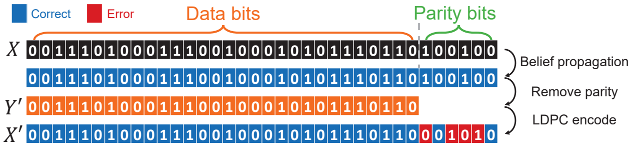


Figure 25: An example of LDPC decoding procedure and the regenerated bit sequence at 5/6 coding rate.

One thing to note is that even though the parity bits part will not be falsely corrected by the decoder, they will be removed after decoding. Since the original data bits do not have a high correlation with the parity bits, the parity bits part of the regenerate bits are not related to that of the demodulated bits. Thus the parity bits part should be treated as unreliable after the regeneration. Then, all bit errors introduced by decoding will be on the parity bits part as illustrated in Fig. 25. Therefore, it is preferable for SlimWiFi to reduce the ratio of parity bits which requires a higher coding rate.