Enabling Integrated Circuit-Based Full-Duplex Wireless in GNU Radio

Alon S. Levin[1] ALON.S.LEVIN@COLUMBIA.EDU
Manav Kohli[1] MANAV.KOHLI@COLUMBIA.EDU
Igor Kadota[2] KADOTA@NORTHWESTERN.EDU
Tingjun Chen[3] TINGJUN.CHEN@DUKE.EDU
Sasank Garikapati[1] SG3734@COLUMBIA.EDU
Aravind Nagulu[4] NAGULU@WUSTL.EDU
Mahmood Baraani Dastjerdi[1] MB4038@COLUMBIA.EDU
Jin Zhou[5] JINZHOU@ILLINOIS.EDU
Ivan Seskar[6] SESKAR@WINLAB.RUTGERS.EDU
Harish Krishnaswamy[1] HARISH@EE.COLUMBIA.EDU
Gil Zussman[1] GIL.ZUSSMAN@COLUMBIA.EDU

[1]Columbia University, 530 West 120th Street, New York, NY 10027
[2]Northwestern University, 2145 Sheridan Rd, Tech M309, Evanston, IL 60208
[3]Duke University, 534 Research Dr, Durham, NC 27705
[4]Washington University in St. Louis, 1 Brookings Drive, St. Louis, MO 63130
[5]University of Illinois Urbana-Champaign, 306 N. Wright St. MC 702, Urbana, IL 61801
[6]WINLAB, Rutgers University, 671 Route 1 South, North Brunswick, N.J. 08902

Abstract

Full-duplex (FD) wireless communication, the simultaneous transmission and reception of wireless signals on the same frequency channel, has garnered significant attention from the research community over the past decade. Software-defined radio (SDR) has become instrumental in bridging the gap from theory to implementation, providing the flexibility necessary to design and deploy FD radio nodes, links, and networks. As part of the Full-Duplex Wireless: From Integrated Circuits to Networks (FlexICoN) project, we have developed three generations of IC-based FD radios that utilize GNU Radio as the primary control and signal processing platform. This paper presents an overview of the design considerations and techniques for implementing FD in GNU Radio, from the transmit and receive signal processing chains to broader testbed integration.

1. Introduction

The exponential growth of wireless internet traffic in recent decades demands significantly enhanced network capacity and spectral efficiency. Every new generation of wireless technology attempts to provide novel solutions to these problems, such as massive multiple-input–multiple-output (MIMO) and millimeter-wave (mmWave) systems in 5G. However, every single wireless communication system today, from amateur radio to licensed cellular networks, operates on the fundamental assumption that wireless devices cannot transmit and receive simultaneously on the same frequency band, instead operating in *half-duplex* (HD) mode in which the transmit and receive signals are processed either in separate time slots, known as

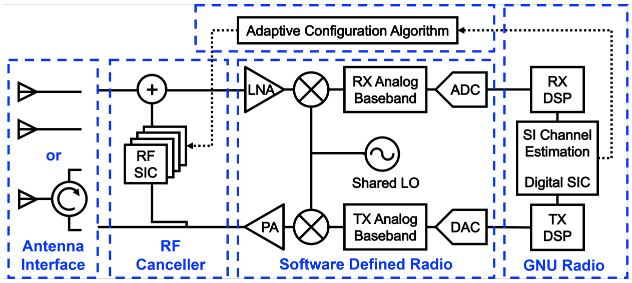


Figure 1. Block diagram of a typical full-duplex (FD) transceiver employing multi-domain SIC, including antenna interface isolation, adaptive analog RF cancellation, and digital cancellation.

Proceedings of the 14th GNU Radio Conference, Copyright 2024 by the author(s).

time-division duplexing (TDD), or in different frequency bands, known as frequency-division duplexing (FDD).

Over the past decade, however, significant attention has been given to *full-duplex* (FD) wireless communication, an emerging paradigm that enables the simultaneous transmission and reception (STAR) of radio signals on the same frequency, thereby providing many potential benefits including improved spectrum efficiency, higher data rates, and reduced communication latency (Duarte et al., 2012; Bharadia et al., 2013; Sabharwal et al., 2014; Zhang et al., 2015; Kim et al., 2015; Krishnaswamy & Zussman, 2016; Kolodziej et al., 2019; Chen et al., 2021; Smida et al., 2023; Nagulu et al., 2024).

The main challenge in realizing FD communication systems is the presence of the strong *self-interference* (SI) signal leaking from the radio's transmitter (Tx) to its receiver (Rx), which can often be $70 - 110\,\text{dB}$ more powerful than the desired signal from a different, more distant transmitter. This problem is further compounded by long delay spreads in the SI channel, resulting in substantial frequency dispersion, as well as shifts in the SI channel response due to changes in the electromagnetic environment. To address these challenges, multi-domain SI cancellation (SIC) techniques have been proposed that include antenna interface isolation, analog RF cancellation, and digital domain algorithms, as depicted in Figure 1.

Recently, particular attention has been given to benchtop implementations using both commercial off-the-shelf (COTS) components and custom hardware (Nagulu et al., 2024), including the use of software-defined radios (SDR) and GNU Radio for control and signal processing (Kohli et al., 2021). This paper aims to provide an overview of the design considerations and techniques for implementing FD using GNU Radio and SDRs in conjunction with FD frontends based on integrated circuit (IC) implementations, using experience gained over three generations of FD radio design as part of the Full-Duplex Wireless: From Integrated Circuits to Networks (FlexICoN) project at Columbia University (FlexICoN, 2024). The motivations and outcomes of the FlexICoN project, including the three generations of FD radios, will be discussed in Section 2. We build on this over the next several sections with analyses and discussions of individual functions within the FD transceiver architecture. Section 3 describes the transmit and receive signal chains, focusing on the encapsulation and unwrapping, respectively, of the data packets to allow for FD communication. Section 4 follows up by discussing how the SI channel can be estimated from received packets and the application of digital SIC to the received stream. Section 5 then describes the mechanism for controlling and communicating across these functions, including between GNU Radio and the FD frontend hardware, to ensure that the system functions properly across different system states including initialization and canceller optimization. Section 6 discusses the integration of FD hardware in the ORBIT and NSF PAWR COSMOS testbeds. Finally, Section 7 concludes this article.

2. The FlexICoN Project

Despite the recent progress in the development of benchtop FD radios, the use of COTS components results in large transceivers that are not suitable for small-form-factor mobile and handheld applications. As a result, the FlexICoN project was started at Columbia University to address both the need to design compact IC-based analog RF cancellers and the cross-layer challenges (PHY and MAC) that stem from such implementations (FlexICoN, 2024).

The analog cancellation stage is necessary as the initial antenna interface isolation alone is insufficient to avoid saturation and signal desensitization at the Rx (Nagulu et al., 2024). In general, there are three classes of analog RF cancellers: *phase- and amplitude*-based (P&A) cancellers, *time-domain equalization*-based (TDE) cancellers, and *frequency-domain equalization*-based (FDE) cancellers (Chen et al., 2021). Three "generations" of FD radios were designed around these three classes, with each being implemented as a configurable RFIC to serve as the frontend of the radio. The three generations of FD radios, shown in Figure 2, are described in the remainder of this section; their characteristics are summarized in Table 1.

2.1. Gen-1 FD Radio

The Gen-1 FD radio was developed around a P&A RFIC canceller consisting of a single filter tap with configurable attenuation and phase parameters (Zhou et al., 2014). The canceller's ideal transfer function is given by

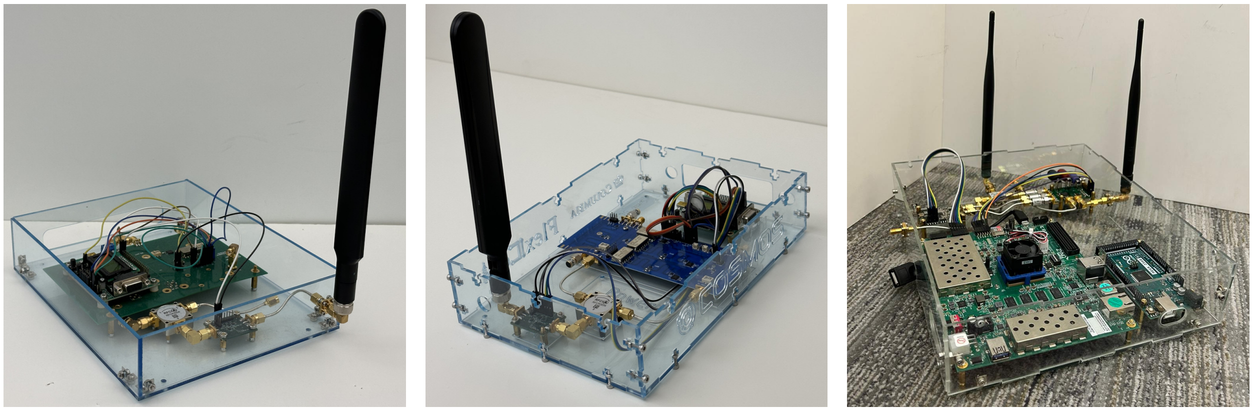
$$H_{\text{Gen-1}}^{\text{P\&A}}(f) = \alpha e^{-j\phi}, \tag{1}$$

in which α and ϕ are the configurable, frequency-independent amplitude and phase parameters, respectively. The amplitude can be tuned from a range of $0 - 37.5\,\text{dB}$ in intervals of $0.25\,\text{dB}$ (four-bit resolution); the phase can be tuned across the full $360°$ range in intervals of approximately $1.5°$ (eight-bit resolution) (Chen et al., 2016).

The implemented Gen-1 FD radio, shown in Figure 2a,

	Category	# Taps	Bandwidth
Gen-1 FD Radio	P&A	1	5 MHz
Gen-2 FD Radio	FDE	2	20 MHz
Gen-3 FD Radio	TDE	16	>50 MHz

Table 1. Summary and comparison of three generations of FD radios developed as part of the Columbia FlexICoN project.



(a) Gen-1 P&A FD radio

(b) Gen-2 FDE FD radio

(c) Gen-3 TDE FD radio

Figure 2. Three generations of FD radios using hardware developed as part of the Columbia FlexICoN project.

uses a custom PCB-based RF SI canceller that emulates the RFIC canceller using discrete components. The canceller PCB is paired with a circulator-based shared-antenna interface to make up the FD frontend, which is connected to a National Instruments (NI) Universal Software Radio Peripheral (USRP) controlled from a computer running GNU Radio. A SUB-20 multi-interface USB adapter (DIMAX) is used to control the FD frontend from the computer; through a GNU Radio GUI, a user has control over all the configuration parameters needed to program the canceller PCB and an antenna tuner[1] over SPI. When optimally configured, the P&A-based PCB canceller can achieve $43\,\mathrm{dB}$ of RF SIC across a $5\,\mathrm{MHz}$ bandwidth. The integration of the Gen-1 FD radio in the open-access ORBIT and COSMOS testbed is discussed in Section 6.1.

2.2. Gen-2 FD Radio

The Gen-2 FD radio was developed around a FDE RFIC canceller consisting of two configurable, parallel bandpass filter (BPF) taps (Zhou et al., 2015). The canceller's ideal transfer function is given by

$$H_{\text{Gen-2}}^{\text{FDE}}(f) = \sum_{n=1}^{2} \frac{A_n e^{-j\phi_n}}{1 - jQ_n \left(\frac{f_{c,n}}{f} - \frac{f}{f_{c,n}} \right)}, \tag{2}$$

where A_n and ϕ_n are the configurable amplitude and phase parameters applied to the n^{th} BPF tap with center frequency $f_{c,n}$ and quality factor Q_n, both of which are likewise configurable. Each tap, therefore, has four degrees of freedom, allowing one to shape the canceller response not only in amplitude and phase but also in the slopes of the amplitude and phase (i.e., group delay), providing a significant advancement over the P&A canceller (Chen et al., 2019).

The Gen-2 system, shown in Figure 2b, builds on the implementation of the Gen-1 system, using a PCB equivalent to the Gen-2 canceller IC as part of the FD frontend. The system uses a circulator-based shared-antenna interface and is connected to an NI USRP, controlled from a computer running GNU Radio and interfacing with both the canceller PCB and the antenna tuner using a SUB-20 device. When optimally configured, the FDE-based PCB canceller can achieve $50\,\mathrm{dB}$ of RF SIC across a $20\,\mathrm{MHz}$ bandwidth. The integration of the Gen-2 FD radio in the open-access COSMOS testbed is discussed in Section 6.2.

2.3. Gen-3 FD Radio

The Gen-3 FD radio was developed around a TDE RFIC canceller, featuring sixteen parallel time-domain RF filter taps with configurable gain and delay (Nagulu et al., 2021).[2] The canceller's ideal transfer function is given by

$$H_{\text{Gen-3}}^{\text{TDE}}(f) = \sum_{n=1}^{16} \alpha_n e^{-j2\pi f \tau_n}, \tag{3}$$

where α_n and τ_n are the configurable gain and delay parameters for tap n. It should be noted that this is effectively a multi-tap generalization of the P&A canceller response described in Section 2.1, in which the phase parameter is determined by a configurable delay and is therefore no longer frequency-independent.

The sixteen filter taps are comprised of one zero-delay tap, five low-delay taps with eight possible delay values ranging from $0\,\mathrm{ps}$ to $1.75\,\mathrm{ns}$, and ten high-delay taps with thirty-two possible delay values ranging from $0\,\mathrm{ps}$ to $7.75\,\mathrm{ns}$, all in increments of $250\,\mathrm{ps}$ (Nagulu et al., 2021). Selecting the

[1] Positioned between the circulator and the antenna to improve impedance matching.

[2] The RFIC canceller also features a secondary cancellation stage with eight configurable, complex-weighted baseband filter taps; however, this is bypassed in the Gen-3 radio implementation and will not be discussed herein.

appropriate delays for each tap is, therefore, a challenge, as the configuration space for delay selection is on the order of 10^{19}; this is further compounded by the fact that each tap has a six-bit adjustable gain which likewise needs to be configured optimally. As a result, whereas the Gen-1 and Gen-2 FD radios can be manually configured with relatively high assurance of finding a sufficient analog canceller configuration, this is not the case with the Gen-3 FD radio, which requires an intelligent algorithm to find the optimal solution.

The Gen-3 system (Levin et al., 2024), shown in Figure 2c, deviates from the previous two generations in that it utilizes a bistatic simultaneous transmit and receive antenna interface instead of a circulator-based antenna interface in order to support a wider operational bandwidth, enabled by the high complexity of the RFIC canceller. The canceller is controlled by a Zynq UltraScale+ MPSoC ZCU104 Evaluation Board (Xilinx, 2018), which computes and updates the optimal configuration in parallel to the radio's standard operation, performed by an NI USRP controlled from a computer running GNU Radio (Levin et al., 2023). When optimally configured, the TDE-based RFIC canceller can achieve $50\,\mathrm{dB}$ of RF SIC across a bandwidth of at least $50\,\mathrm{MHz}$.

3. Transmission and Reception

Although the transmission and reception of baseband data to and from the USRP are handled directly by pre-existing USRP Hardware Driver (UHD) Sink and Source blocks (Ettus Research), additional control and signal processing is necessary before and after these stages.

3.1. Encapsulation

Each transmission consists of two components: the payload and the prepended pilot symbols. The payload can be generated to any standard using GNU Radio OOT modules, such as the IEEE 802.11 Wi-Fi standard (Bloessl et al., 2013), and is outside the scope of this work. The payload is then prepended with unique identifying pilot symbols in an assigned pilot slot, as shown in Figure 3. The goal of the pilot symbols is twofold: to enable robust synchronization using a known pattern and to measure the SI channel during a dedicated "quiet" period. The pilot symbols should be designed to cover the same instantaneous bandwidth as the payload in order to achieve an accurate representation of the SI channel's effects on the payload, and can be repeated over multiple symbols to increase the accuracy of the instantaneous SI measurement at the cost of additional overhead. We implemented a customized OOT block to prepend the pilot symbols and to add zero padding between packets, thereby explicitly defining timeslot lengths in a slotted transmission system.

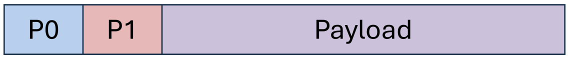


Figure 3. Packets are transmitted simultaneously by both radios such that only the payloads overlap. Each radio prepends its payload with its unique identifying pilot symbol in its assigned pilot slot (P0 or P1), thereby providing a brief "quiet" period that would allow for high-fidelity SI measurement.

3.2. Synchronization

Two forms of synchronization need to be achieved: intra-node synchronization between the FD node's internal transmit stream and the received SI, and inter-node synchronization between the two nodes in order to align the transmissions within each timeslot.

Intra-node Synchronization

Intra-node synchronization is necessary in order to properly align the radio's received SI signal and extract the transceiver's pilot symbols and shared payload. As the SI is sufficiently powerful and easily detectable, the start of the SI packet can be coarsely identified using a simple energy threshold algorithm. Cross-correlation with one's known unique pilot symbol can then be used to fine-tune the synchronization to sample-level resolution. Once the start time of the packet is identified within the timeslot, it is consistent for the remainder of the experiment's runtime so long as no UHD errors take place. The pseudocode is presented in Algorithm 1; additional logic can be added to check for spurious in-band emissions in case energy detection is falsely activated and to trigger resynchronization after UHD errors. In cases where the delay through the SI

Algorithm 1 Intra-Node Synchronization

```
Require: Received Timeslot $R_i = \{r_0, \dots, r_n\}$, delay $d$
if SYNCED then
    return Packet $\{r_d, \dots, r_{d+\text{length(pkt)}}\}$
end if
while UNSYNCED do
    $d \leftarrow \text{EnergyDetect}(R_i)$                ▷ Coarse search
    if $d = \varnothing$ then                            ▷ Empty timeslot
        $R_i \leftarrow R_{i+1}$
        continue
    else
        $d \leftarrow \text{xcorr}(R, d)$                ▷ Fine search
        set SYNCED
        return Packet $\{r_d, \dots, r_{d+\text{length(pkt)}}\}$
    end if
end while
```

channel is greater than the length of a timeslot, buffering the transmitted packets is necessary to ensure proper data alignment for digital SIC.

INTER-NODE SYNCHRONIZATION

Once both FD radios in a link have synchronized their internal transmit and receive streams, they need to synchronize their transmissions with each other so that the packets overlap appropriately (i.e., with non-overlapping pilot slots and overlapping payloads, as shown in Figure 3). This requires one of the two nodes to act as a primary node, to which the other node will synchronize. The primary transmits an initial packet, and the secondary (which remains silent) determines at what point in the timeslot the packet is received. The secondary then adjusts its zero padding allocation such that its transmitted packets will coincide with the primary's transmitted packets.

This baseline algorithm is presented in Algorithm 2; additional control mechanisms, such as acknowledgment of synchronization, can be introduced to improve the reliability of the synchronization. This process can scale for networks consisting of multiple FD nodes in the same manner, with the primary node broadcasting the initial packet to all nodes; in situations where certain FD nodes are outside of the primary node's range, nodes can take turns as the primary to ensure full coverage.

Algorithm 2 Inter-Node Synchronization

```
Require: Intra-node synchronization complete
if Primary node then
    Transmit packet at $\tau_{T1}$
end if
if Secondary node then
    Receive packet at $\tau_{R1}$
    Update padding to transmit at $\tau_{R1}$
end if
```

4. SI Channel Processing

As stated in Section 3.1, one of the primary tasks of the pilot symbols and assigned pilot slots is to ensure that the SI channel can be measured and estimated with high fidelity. The channel measurements are used as inputs to algorithms for configuring the FD frontend hardware and for digital SIC. As each packet is received, new channel measurements are obtained, thereby allowing a system to dynamically track and adapt to the SI channel as it changes due to fluctuations in the electromagnetic environment.

4.1. SI Channel Estimation

Once extracted from the received packet, the users' pilot symbols are a product of the residual SI channel after the isolation and analog cancellation stages; as such, traditional signal processing methods can estimate the SI channel response from the received symbols. One low-complexity approach employs the least-squares (LS) algorithm to estimate the SI channel in the frequency domain (Jain et al., 2011). This method is particularly well-suited for OFDM-based transmission schemes, such as the IEEE 802.11 Wi-Fi standard (Bloessl et al., 2013), as individual subcarriers are encoded with predefined training symbols that are known to the device at transmission time.

Specifically, let $\mathbf{X} = (X[0], \ldots, X[N-1])$ be a single pilot symbol, defined as a frequency-domain vector across N subcarriers, and assume that the symbol is repeated M times within the FD radio's allocated pilot slot.[3] Let $\mathbf{Y}^{(m)}, m = 1, \ldots, M$ be the corresponding received signal consisting of the same pilot symbols after the SI channel. Then, the frequency-domain LS estimate of the SI channel $\hat{H}_{\text{SI}}$ at subcarrier k is

$$\hat{H}_{\text{SI}}[k] = \frac{1}{M}\left[\frac{1}{X[k]}\left(\sum_{m=1}^{M} Y^{(m)}[k]\right)\right]. \qquad (4)$$

An important factor that must be taken into account when performing channel estimation is the effect of sub-sample delay between the Tx and Rx signal processing chains' clocks in the USRP. As the Tx and Rx clocks, operating at the sampling frequency set in GNU Radio, do not necessarily start up on the same master clock cycle, there is a random phase offset between the transmitted and received streams which inhibits consistent measurements of the SI channel across different GNU Radio runs and must be corrected for consistent behavior and performance.

As the sampling rate f_s of the USRP must be an integer divisor of the master clock rate f_c, assuming that the synchronization is correct to the nearest sample, the random phase offset takes the form

$$\varphi = 2\pi k(f_s/f_c),\ k \in \{0, 1, \ldots, (f_c/f_s) - 1\}. \qquad (5)$$

To correct for this phase offset, a "base state" where the SI channel is known to be consistent needs to be defined; in the case of configurable FD frontends, this can be the state when the analog RF canceller is disabled, ensuring a more powerful and consistent SI signal that is less affected by surrounding noise. The phase offset can be estimated as the group delay of the SI channel response at the base state, thereby achieving a maximally flat group delay after correction. This value is then used as a reference for correcting all subsequent SI channel response estimates in the same experimental run. Still, it must be recomputed when-

[3] Symbol repetition is not necessary, but rather presented as a simplification of the model, as different symbols can be employed in the same slot.

ever resynchronization is necessary, such as when restarting the flowgraph or when UHD errors arise.

4.2. Digital SIC

The estimated SI channel, obtained using Equation 4 after analog-to-digital conversion and phase-corrected, can be used to define an FIR filter that will then be used in the same fashion as the analog cancellers: the transmitted signal is fed through the filter and subtracted from the received signal to perform cancellation. These operations are performed on the frequency-domain signals, with the output ideally consisting solely of the desired received signal and no SI, and therefore ready for demodulation and processing.

Alternatively, digital SIC can be performed directly in the time domain by modeling the SI canceller as a truncated Volterra series in order to cancel both the main SI component and its intermodulation distortion (Krishnaswamy et al., 2016). Specifically, using a time-domain LS estimate of the SI channel $\hat{h}$ with i-th order digital cancellation coefficients $\hat{h}_i[k]$ up to order I, we can write the desired received signal $r[n]$ as

$$r[n] = y[n] - \sum_{i=1}^{I} \sum_{k=0}^{K} h_i[k] x[n-k]^i, \tag{6}$$

where $y[n]$ is the residual signal after the isolation and analog cancellation stages, and $x[n]$ is the corresponding known transmitted signal.

In practice, it was found that a third-order model was sufficient to achieve sufficient cancellation to obtain the desired receive signal, and, in most instances, a first-order (linear) model performs equivalently. In the latter case, the model can be represented as a Toeplitz matrix-based convolution, simplifying computation:

$$\mathbf{r} = \mathbf{y} - \mathbf{A}\hat{\mathbf{h}}, \tag{7}$$

where $\mathbf{A}$ is the Toeplitz matrix constructed from the known transmitted signal.

5. System Control

The functions described in Sections 3 and 4 cannot operate properly without the assurance that their inputs are properly formatted; a clear example of this is the channel estimation block, as when the system is unsynchronized, the system obtains corrupted measurements due to the misaligned of the pilot symbols. Therefore, it's instrumental that there be a centralized top-level controller orchestrating between the various blocks in the system and ensuring that all the functions are operating as they should be in various system states.

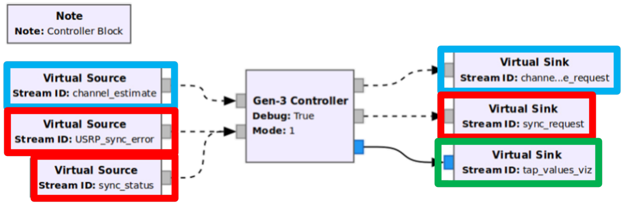


Figure 4. Controller block from the Gen-3 FD radio, utilizing a mix of message-passing and stream flow to control other blocks. Error detection and synchronization control paths are outlined in red; channel estimation control paths are outlined in blue; and visualization output is outlined in green.

In all three generations of FD radios, flow control between the signal processing blocks is achieved using stream tags to segment streams into timeslots, mark packet start times within timeslots, and indicate the pilot slots and payload within each packet. In addition to this, each block has input and output message ports that communicate with the top-level controller block, such as the Gen-3 controller block in Figure 4. Each block in the flowgraph maintains its own state machine and communicates with the controller to centralize system state information, including hardware errors, synchronization confirmation, SI channel measurements, and data for visualization. The controller uses this information to orchestrate the system, ensuring that broader tasks such as initialization and analog canceller optimization run as necessary.

5.1. FD Radio Initialization

As discussed in Section 3.2, it is imperative to have proper synchronization before any other operations, including the optimization of the analog canceller frontend, can function. The controller block tracks each stage of the initialization sequence, shown in Algorithm 3, requesting each block to perform its task when appropriate and receiving confirmation in return. Specifically, the startup sequence consists of the following three major steps:

1. the synchronizer block synchronizes the received SI packets with their corresponding transmitted packets;
2. the channel estimation block computes the channel estimation phase correction factor;
3. the encapsulation block adjusts the transmission padding for inter-node synchronization.

Algorithm 3 FD Radio Initialization

```
1: Perform intra-node synchronization      ▷ Algorithm 1
2: Compute phase correction factor          ▷ Equation 5
3: Perform inter-node synchronization      ▷ Algorithm 2
4: RFIC canceller optimization              ▷ Algorithm 4
```

Once all these tasks are achieved, only then can the FD radio begin its routine performance, including analog canceller optimization and digital SIC. It should be noted that this sequence must be repeated whenever UHD errors occur, as they result in random delays within the SDR's signal processing chain; the controller listens for such messages from the USRP Sink to retrigger the initialization sequence across the rest of the blocks in the flowgraph.

5.2. Canceller Optimization

Once the FD radio is in a state where all of the streams are synchronized properly, and the blocks are operating in a steady state mode, the canceller can begin to optimize the analog canceller to maximize RF SIC and enable reception while communicating in FD mode. Different algorithms for tuning the cancellers have been proposed and implemented for the three generations of FD radios (Krishnaswamy et al., 2016; Chen et al., 2019; Levin et al., 2024), and are outside the scope of this work. In each implementation, the controller iteratively receives an estimate of the SI channel from the channel estimation block, using it to compute and set a new configuration for the canceller, as shown in Algorithm 4.

Configuring the analog canceller requires a device to interface between the computer running GNU Radio and the canceller hardware, which is controlled over SPI. In the Gen-1 and Gen-2 FD radios, this is accomplished using a SUB-20 device (DIMAX) connected to the computer over USB. The Gen-3 FD radio can either use an FPGA (Xilinx, 2018) or an Arduino Mega 2560 (Arduino) as the interface, selected by a PCB-mounted switch; furthermore, the configuration computation is offloaded to the FPGA, with the controller block communicating the SI channel information to the controller and receiving the configuration state information back for logging. In all three radios, it is also possible to bypass the optimization stage entirely, with tools available to pre-load a known configuration directly onto the canceller if desired.

Digital SIC is performed in parallel to analog cancellation and can employ its own adaptive algorithms, as discussed in Section 4.2. Co-optimizing analog and digital SIC is an active field of research, and can be facilitated using the control systems described in this section.

Algorithm 4 Canceller Optimization

```
Estimate SI channel                          ▷ Equation 4
Compute initial configuration
loop
    Configure RFIC canceller
    Estimate SI channel                      ▷ Equation 4
    Compute configuration adjustment
    if UHD Error then
        Restart initialization               ▷ Algorithm 3
    end if
end loop
```

6. Testbed Integration

To aid the community's efforts in evaluating the higher-layer impacts of FD wireless, we integrated two generations of FD radios in the open-access ORBIT and COSMOS wireless testbeds (ORBIT, 2003; COSMOS, 2019; Kohli et al., 2021). The ORBIT and COSMOS testbeds are remotely accessible experimentation resources available to the broader research community, alleviating the need to develop or purchase FD-capable hardware and SDRs. The process for remotely accessing the FD radios is identical for the two testbeds: the user logs into the testbed console from their local machine using SSH, and X11 forwarding is used to interface with the GNU Radio GUI.

The FD nodes within the ORBIT and COSMOS testbeds are located in indoor laboratories, in which the temperature and interference levels are generally stable and the only major source of fluctuation in the electromagnetic environment due to the movement of people within. The experiments run in real-time on the testbed, allowing users to observe results visualized in GNU Radio without the need for offline processing. Several example experiments have been developed and are available for immediate use; a tutorial for interacting with the FD testbeds can be found at (COSMOS, 2024).

6.1. Gen-1 FD Radio Integration

A Gen-1 FD radio is integrated into the ORBIT main `grid`, labeled `node11-10`, as shown in Figure 5. The FD frontend is connected to a USRP N210 SDR, and uses

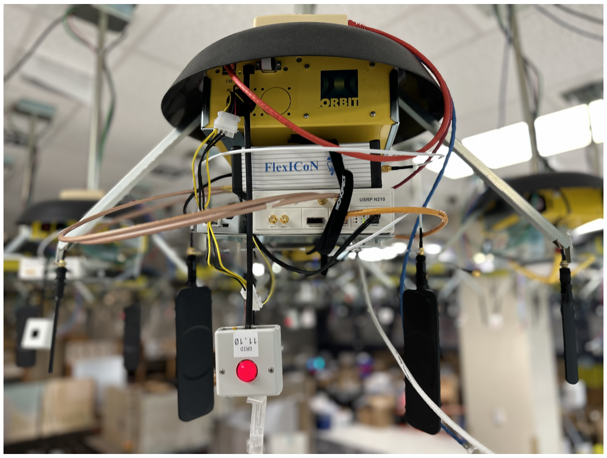
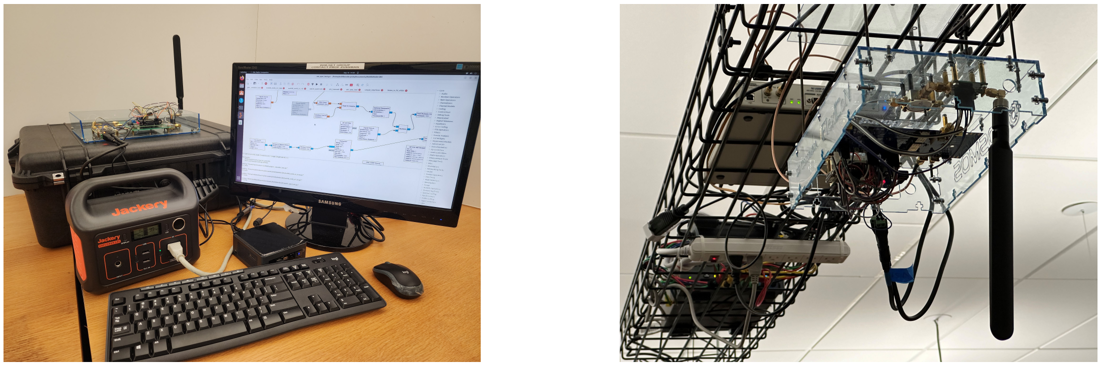


Figure 5. The Gen-1 FD radio integrated into the ORBIT testbed.



(a) The mobile Gen-1 FD radio.

(b) One of the four Gen-2 FD radios.

Figure 6. Two generations of FD radios integrated into the COSMOS wireless testbed.

an Apex II multi-band antenna. The USRP has a receiver noise floor of $-86\,\mathrm{dBm}$ at a $10\,\mathrm{MHz}$ bandwidth, operating at a center frequency of $900\,\mathrm{MHz}$. A node image is available with updated GNU Radio OOT modules and experiments. Other HD nodes in the testbed may be used in parallel to the Gen-1 FD radio to create a heterogeneous wireless link where one radio operates in FD mode.

As experimentation with mobile user equipment (UE) operating in FD mode is of interest, we have fabricated a prototype mobile Gen-1 FD radio consisting of the Gen-1 FD frontend, USRP B205mini-i SDR, and an Intel NUC 8i7BEH, as shown in Figure 6a. The entire mobile setup (including the radio, the computer, and peripheral equipment) can be powered by a portable battery, and can support real-time FD operation up to $5\,\mathrm{MHz}$ bandwidth.

6.2. Gen-2 FD Radio Integration

Four Gen-2 FD radios are integrated into the `Sandbox 2` domain in the COSMOS testbed, as shown in Figure 6b. They are mounted on the corners of a $4.5\,\mathrm{m} \times 3.5\,\mathrm{m}$ rectangle within a square laboratory room, where they are connected to two USRP X310 SDRs with SBX-120 RF daughterboards. The SDRs and Gen-2 FD radios are connected to two Dell R740 COSMOS servers via $10\,\mathrm{Gbit/s}$ network links. As with the ORBIT FD testbed, server node images are available with updated GNU Radio OOT modules and experiments.

Gen-2 SIC Dataset

We have published a dataset consisting of data packets transmitted using the Gen-2 FD radios and their corresponding residual SI after RF SIC, which can be accessed through the COSMOS dataset repository (COSMOS, 2023). The objective of this dataset is to provide ready-to-use data traces to support the development of FD-related algorithms, including digital SIC and other DSP applications. We provide an example MATLAB script that implements the linear digital SIC algorithm described in Equation 7.

Every experimental run is represented by two binary files, one each for the transmitted and received baseband data, with each run consisting of at least 100 data packets. There are a total of twelve experimental runs across three bandwidths (5 MHz, 10 MHz, and 20 MHz) using each of the four testbed radios. The transmitted data packets are QPSK 3/4-modulated 802.11a packets, and the received power after RF SIC is between -40 to $-50\,\mathrm{dBm}$ and the USRP noise floor is $-80\,\mathrm{dBm}$ at a $20\,\mathrm{MHz}$ bandwidth.

7. Conclusion

In conclusion, this work provides a discussion of the challenges and approaches to implementing IC-based FD wireless using GNU Radio, as was accomplished throughout the research conducted by the FlexICoN project. We presented three generations of FD radios, each utilizing a different class of configurable analog RF canceller. The remainder of the paper discussed the different functions and processes needed to enable FD wireless communication, including the transmission/reception signal chains, the processing of received packets in order to estimate the SI channel and perform digital SIC, the control mechanisms for ensuring proper operation within the GNU Radio flowgraph and communication with external hardware, and larger integration into open-access wireless testbeds for higher-layer experimentation.

Acknowledgements

This work was supported in part by the DARPA WARP program, NSF grants OAC-2029295, EEC-2133516, AST-2232455, CNS-2148128, CNS-2128638, and AST-2232458, and by funds from federal agency and industry partners as specified in the NSF Resilient & Intelligent NextG Systems (RINGS) program. A.S.L. was supported by the DoD through the NDSEG Fellowship Program. M.K. was supported by the NSF GRFP (DGE-2036197).

References

Arduino. Mega 2560 Rev3. URL https://docs.arduino.cc/hardware/mega-2560/.

Bharadia, Dinesh, McMilin, Emily, and Katti, Sachin. Full Duplex Radios. In *Proc. SIGCOMM'13*, 2013.

Bloessl, Bastian, Segata, Michele, Sommer, Christoph, and Dressler, Falko. An IEEE 802.11a/g/p OFDM Receiver for GNU Radio. In *Proc. SRIF'13*, 2013.

Chen, Tingjun, Zhou, Jin, Grimwood, Nicole, Fogel, Rel, Marašević, Jelena, Krishnaswamy, Harish, and Zussman, Gil. Demo: Full-duplex wireless based on a small-form-factor analog self-interference canceller. In *MobiHoc'16*, pp. 357–358, 2016.

Chen, Tingjun, Baraani Dastjerdi, Mahmood, Zhou, Jin, Krishnaswamy, Harish, and Zussman, Gil. Wideband full-duplex wireless via frequency-domain equalization: Design and experimentation. In *Proc. MobiCom'19*, 2019.

Chen, Tingjun, Garikapati, Sasank, Nagulu, Aravind, Gaonkar, Aditya, Kohli, Manav, Kadota, Igor, Krishnaswamy, Harish, and Zussman, Gil. A Survey and Quantitative Evaluation of Integrated Circuit-Based Antenna Interfaces and Self-Interference Cancellers for Full-Duplex. *IEEE Open Journal of the Communications Society*, 2:1753–1776, 2021.

COSMOS. Cloud enhanced open software defined mobile wireless testbed for city-scale deployment (COSMOS), 2019. URL http://cosmos-lab.org.

COSMOS. COSMOS Full-Duplex Dataset, 2023. URL https://wiki.cosmos-lab.org/wiki/Datasets/FD_Baseband_IQ.

COSMOS. Tutorial: Full-Duplex Wireless in the ORBIT and COSMOS Testbeds, 2024. URL https://wiki.cosmos-lab.org/wiki/Tutorials/Wireless/FullDuplex.

DIMAX. SUB-20 Multi Interface USB Adapter. URL http://www.xdimax.com/sub20/sub20.html.

Duarte, Melissa, Dick, Chris, and Sabharwal, Ashutosh. Experiment-Driven Characterization of Full-Duplex Wireless Systems. *IEEE Trans. Wireless Commun.*, 11 (12):4296–4307, 2012.

Ettus Research. USRP Hardware Driver (UHD) software. URL https://github.com/EttusResearch/uhd.

FlexICoN. The Columbia FlexICoN Project, 2024. URL https://flexicon.ee.columbia.edu/.

Jain, Mayank, Choi, Jung Il, Kim, Taemin, Bharadia, Dinesh, Seth, Siddharth, Srinivasan, Kannan, Levis, Philip, Katti, Sachin, and Sinha, Prasun. Practical, Real-Time, Full Duplex Wireless. In *Proc. MobiCom'11*, 2011.

Kim, Dongkyu, Lee, Haesoon, and Hong, Daesik. A Survey of In-Band Full-Duplex Transmission: From the Perspective of PHY and MAC Layers. *IEEE Commun. Surveys Tuts.*, 17(4):2017–2046, 2015.

Kohli, Manav, Chen, Tingjun, Baraani Dastjerdi, Mahmood, Welles, Jackson, Seskar, Ivan, Krishnaswamy, Harish, and Zussman, Gil. Open-access full-duplex wireless in the orbit and cosmos testbeds. *Comput. Netw.*, 199, 2021.

Kolodziej, Kenneth E, Perry, Bradley T, and Herd, Jeffrey S. In-Band Full-Duplex Technology: Techniques and Systems Survey. *IEEE Trans. Microw. Theory Techn.*, 67(7):3025–3041, 2019.

Krishnaswamy, Harish and Zussman, Gil. 1 Chip 2x the Bandwidth. *IEEE Spectrum*, 53(7):38–54, 2016.

Krishnaswamy, Harish, Zussman, Gil, Zhou, Jin, Marašević, Jelena, Dinc, Tolga, Reiskarimian, Negar, and Chen, Tingjun. Full-Duplex in a Hand-Held Device — From Fundamental Physics to Complex Integrated Circuits, Systems and Networks: An Overview of the Columbia FlexICoN Project. In *Asilomar'16*, pp. 1563–1567, 2016.

Levin, Alon Simon, Kadota, Igor, Garikapati, Sasank, Zhang, Bo, Jolly, Aditya, Kohli, Manav, Seok, Mingoo, Krishnaswamy, Harish, and Zussman, Gil. Demo: Experimentation with wideband real-time adaptive full-duplex radios. In *Proc. SIGCOMM'23*, pp. 1170–1172, 2023.

Levin, Alon Simon, Flores Portillo, Eliot, Garikapati, Sasank, Bechhofer, Ahuva, Zhang, Bo, Kohli, Manav, Kadota, Igor, Krishnaswamy, Harish, Seok, Mingoo, and

Zussman, Gil. Demo: Achieving self-interference cancellation across different environments. In *Proc. MobiCom'24*, 2024.

Nagulu, Aravind, Garikapati, Sasank, Essawy, Mostafa, Kadota, Igor, Chen, Tingjun, Natarajan, Arun, Zussman, Gil, and Krishnaswamy, Harish. Full-Duplex Receiver with Wideband Multi-Domain FIR Cancellation Based on Stacked-Capacitor, N-Path Switched-Capacitor Delay Lines Achieving >54dB SIC Across 80MHz BW and >15dBm TX Power-Handling. In *Proc. IEEE ISSCC'21*, 2021.

Nagulu, Aravind, Reiskarimian, Negar, Chen, Tingjun, Garikapati, Sasank, Kadota, Igor, Dinc, Tolga, Garimella, Sastry Lakshmi, Kohli, Manav, Levin, Alon Simon, Zussman, Gil, and Krishnaswamy, Harish. Doubling Down on Wireless Capacity: A Review of Integrated Circuits, Systems, and Networks for Full Duplex. *Proceedings of the IEEE*, 112(5):405–432, 2024.

ORBIT. Open-access research testbed for next-generation wireless networks (ORBIT), 2003. URL http://www.orbit-lab.org.

Sabharwal, Ashutosh, Schniter, Philip, Guo, Dongning, Bliss, Daniel W., Rangarajan, Sampath, and Wichman, Risto. In-Band Full-Duplex Wireless: Challenges and Opportunities. *IEEE Journal on Selected Areas in Communications*, 32(9):1637–1652, 2014.

Smida, Besma, Sabharwal, Ashutosh, Fodor, Gabor, Alexandropoulos, George C., Suraweera, Himal A., and Chae, Chan-Byoung. Full-Duplex Wireless for 6G: Progress Brings New Opportunities and Challenges. *IEEE J. Sel. Areas Commun.*, 2023.

Xilinx. Zynq Ultrascale+ MPSoC ZCU104 Evaluation Kit, 2018. URL https://www.xilinx.com/products/boards-and-kits/zcu104.html.

Zhang, Zhongshan, Chai, Xiaomeng, Long, Keping, Vasilakos, Athanasios V, and Hanzo, Lajos. Full Duplex Techniques for 5G Networks: Self-Interference Cancellation, Protocol Design, and Relay Selection. *IEEE Commun. Mag.*, 53(5):128–137, 2015.

Zhou, Jin, Kinget, Peter R., and Krishnaswamy, Harish. 20.6 A blocker-resilient wideband receiver with low-noise active two-point cancellation of >0dBm TX leakage and TX noise in RX band for FDD/Co-existence. In *ISSCC'14*, pp. 352–353, 2014.

Zhou, Jin, Chuang, Tsung-Hao, Dinc, Tolga, and Krishnaswamy, Harish. 19.1 Receiver with >20MHz bandwidth self-interference cancellation suitable for FDD, co-existence and full-duplex applications. In *ISSCC'15*, pp. 1–3, 2015.