SIGNiPHY: Reconciling Random Access with Directional Reception for Efficient mmWave WLANs

Nina Grosheva*
nina.grosheva@imdea.org
IMDEA Networks Institute and
Universidad Carlos III de Madrid
Madrid, Spain

Sai Pavan Deram*
sai.deram@imdea.org
IMDEA Networks Institute and
Universidad Carlos III de Madrid
Madrid, Spain

Jesus O. Lacruz
jesusomar.lacruz@imdea.org
IMDEA Networks Institute
Madrid, Spain

Joerg Widmer
joerg.widmer@imdea.org
IMDEA Networks Institute
Madrid, Spain

ABSTRACT

Millimeter-Wave (mmWave) WiFi can provide very low latency and multi-Gbps throughput, but real-world deployments usually do not achieve the theoretically feasible performance. One main source of inefficiency is the contention-based random channel access, as it requires omni-directional reception which limits performance. Additionally, carrier sensing at mmWave frequencies is highly unreliable, leading to reduced channel usage. In this paper, we present SIGNalling in the PHY Preamble (SIGNiPHY) for efficient directional communications, a solution that allows to embed user identity in the preamble of data packets. It allows for *true* early user identification and then immediately steering the beam towards the transmitter while receiving the physical layer preamble. SIGNiPHY enables directional reception in random access mmWave networks, and additionally helps to quickly filter unwanted packets. It does not affect any preamble functions and is backward-compatible with legacy stations. We implement SIGNiPHY on an FPGA-based mmWave testbed and show that it achieves 99.6% decoding accuracy even under very low SINR conditions. We also implement SIGNiPHY in ns-3 to evaluate large networks and show that it achieves throughput gains between 13% and 230% compared to different baseline schemes, due to the lower packet loss rate and improved spatial sharing.

CCS CONCEPTS

• **Networks** → **Wireless local area networks**; **Network simulations**; • **Hardware** → **Reconfigurable logic and FPGAs**.

KEYWORDS

mmWave, PHY Signaling, IEEE 802.11ad/ay, directional MAC

ACM Reference Format:
Nina Grosheva, Sai Pavan Deram, Jesus O. Lacruz, and Joerg Widmer. 2023. SIGNiPHY: Reconciling Random Access with Directional Reception for Efficient mmWave WLANs. https://doi.org/10.1145/3581791.3596860

1 INTRODUCTION

Wireless networks are rapidly evolving to support advanced applications like Augmented Reality (AR)/Virtual Reality (VR), remote surgery, vehicular connectivity, connected homes, and factory automation. These applications require extremely high data rates and low latencies and Millimeter-Wave (mmWave) networks are a key enabling technology to meet these requirements. The IEEE 802.11ad standard [20] introduced WiFi operation in the 60 GHz band, supporting transmission rates of up to 8 Gbps over a single 2.16 GHz channel. The IEEE 802.11ay amendment [21] further pushed the performance to peak rates of up to 100 Gbps [16] by introducing advanced physical (PHY) layer technologies like Multiple-Input and Multiple-Output (MIMO) and channel aggregation.

However, transmissions in the 60 GHz band suffer from increased path loss, oxygen absorption and sensitivity to blockage [30]. To provide reliable communication at longer link ranges, IEEE 802.11ad/ay devices use directional communication by means of phased antenna arrays. Having narrow directional beams not only increases the link Signal-to-Noise Ratio (SNR) to enable high data rates, but also reduces interference, creating the potential for high spatial reuse and thus high network throughput. Beam training provides devices with information about which Beam Pattern (BP) to use for each device it communicates with, stored in the form of a table.

Unfortunately, while highly beneficial, directional reception is incompatible with the random medium access mechanisms of mmWave WiFi devices. All current WiFi devices implement legacy Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [4, 41], a contention-based random access scheme without a fixed transmission schedule. Instead, *any* user in the network can communicate with the Access Point (AP) at any time, as long as it determines that the channel is free, which is done by carrier sensing the medium. Since the AP does not know which user will be transmitting next, it needs to be able to listen to *every* direction users can be located in. To allow this, current Commercial Off-the-Shelf (COTS) devices [31, 41] only support directional transmission but use omni-directional BPs for the reception. While Stations (STAs) usually only communicate with a single AP, the same issue may arise at STAs in case of multi-hop or device-to-device communication.

We identify two main problems stemming from the use of quasi-omnidirectional reception. i) Omni-directional reception limits single-link performance by reducing the coverage range and data rates due to the lower antenna gain. ii) It negatively affects spatial reuse, as it leaves devices vulnerable to interference coming from any direction. This makes it more difficult to successfully establish

*Both authors contributed equally to this work.

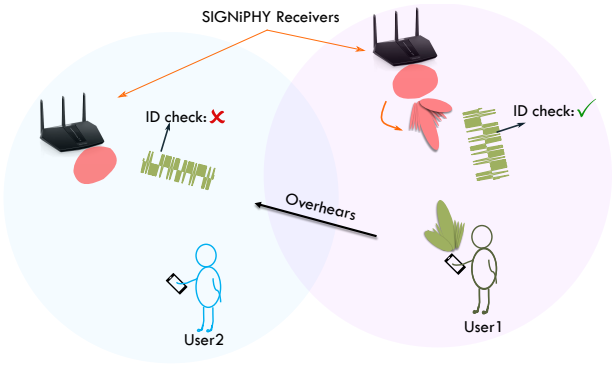


Figure 1: SIGNiPHY utilizes an embedded ID to enable (i) directional reception (ii) PHY filtering

concurrent transmissions in a given area. In particular, it significantly increases the probability that a device will overhear packets that are not meant for it. In turn, while it is busy attempting to decode unwanted packets, it may fail to detect a concurrent packet actually meant for it. This overhearing of unwanted packets is a well-known problem in random-access networks, where the lack of a transmission schedule imposes the need to attempt to decode any packet that stations detect. In sub-6 GHz it leads to decreased energy efficiency since the receiver is wasting energy decoding useless packets. In mmWave networks, however, the impact is much more harmful since it limits spatial sharing, one of the key benefits of mmWave that is critical for high network performance.

Existing solutions fall short in solving these problems efficiently. Directional reception can be implemented through standard mechanisms like Ready-to-Send (RTS)-Clear-to-Send (CTS) and CTS-to-self. While these control packets would be received with a quasi-omnidirectional BP, they announce the identity of the transmitter at the receiver, which can then use the correct directional receive BP for the data packet. However, these mechanisms add non-negligible overhead due to the additional control message exchanges, which translates into sub-optimal channel usage and low Medium Access Control (MAC) layer efficiency [1, 41]. Control packets are also particularly robust and thus likely to be overheard even by far-away nodes, further reducing the spatial re-use in the network.

Instead, in this paper we design a mechanism to tackle these problems at the PHY layer without introducing *any* additional control overhead, and in a manner that is backward compatible with legacy devices. Our solution of SIGNaling in the PHY Preamble (SIGNiPHY) for efficient directional communications, embeds a device identifier in the PHY packet preamble for early transmitter identification at the receiver, which allows directional reception of the packet payload. Critically, the packet preamble is the *only* part of the packet where such an identifier can be embedded. The preamble is followed by the Channel Estimation Field (CEF), and the receiver has to use the same BP for CEF and packet payload reception, otherwise packet decoding fails since a change of BP implies a change of the channel. In contrast, the packet preamble can be received with a different (i.e., omni-directional) beam pattern without impacting its functionality.

This design imposes very stringent timing requirements, since preamble detection, identifier decoding, and BP switching have to be carried out while the preamble is being received, and they need to finish on time before the CEF starts to be received. To meet these timing constraints, we implement a highly efficient identifier decoder and a fast beam-switching mechanism to quickly change from quasi-omni-directional reception to directional mode once the user is identified. SIGNiPHY identifier embedding retains the same correlation properties of the original preamble, which allows to use the same receiver processing blocks without *any* modification, ensuring not only backward compatibility but also interoperability between SIGNiPHY devices and legacy stations. Legacy stations not aware of the identifier embedding will simply receive such packets with their quasi-omnidirectional BP as before, and preamble functionalities like packet detection, Carrier Frequency Offset (CFO) estimation, and synchronization are not affected.

SIGNiPHY also allows to early on abort the reception of packets for which the device is not the intended recipient. While such filtering could be done once the MAC address of the sender is decoded [5, 13], doing it during the PHY preamble saves precious time and is more efficient.Fig. 1 illustrates the concept of SIGNiPHY.

We implement and integrate SIGNiPHY for real-time operation in an FPGA-based mmWave testbed with 60 GHz phased antenna arrays. We show that our implementation is able to correctly identify the user identity just 160 ns after packet detection, ensuring 100% accuracy for Signal-to-Interference-plus-Noise Ratios (SINRs) higher than 7 dB and 99.5% for SINRs above -6 dB. We further demonstrate that SIGNiPHY ensures that none of the preamble functionalities are affected and, in fact, the decoding benefits from the SNR boost due to the quick antenna reconfiguration. Finally, we implement SIGNiPHY and several baseline solutions (RTS-CTS, CTS-to-Self, MAC filtering) in the IEEE 802.11ad/ay module of ns-3 [3] to evaluate its performance in dense scenarios with accurate modeling of the MAC layer and PHY channel of mmWave WiFi. The results show that SIGNiPHY outperforms the other solutions and improves up-link network throughput by up to 230%, depending on the scenario and baseline against which it is compared.

To sum up, in this paper we make the following contributions:

- SIGNiPHY is the first system enabling early user identification for directional mmWave reception in 802.11ad/ay WiFi networks, which does not incur *any* additional overhead.
- We manage to embed the user identity in the packet preamble while retaining the characteristics of legacy systems which ensures backward compatibility and interoperability.
- We design a low-complexity hardware architecture for SIGNiPHY, that only requires a few adders and comparators. This allow us to implement and validate SIGNiPHY in real scenarios using an FPGA-based mmWave testbed.
- We integrate SIGNiPHY in a network-level simulation that allows validation in dense scenarios, comparing its performance against different baseline solutions.

2 MOTIVATION

Although mmWave WiFi networks show great promise, multi-AP deployments where interference and collisions lead to reduced throughput and inefficient channel usage prove challenging for current COTS devices [1, 4, 31, 35, 36, 39]. The mismatch between what is envisioned by mmWave standards and what is achieved in practice lies in the fact that multi-Gbps data rates are only possible

under the assumptions of 1) narrow directional beams with high gains on both sides of the link and 2) high spatial reuse with multiple concurrent data transmissions. Currently, mmWave networks can not fully implement either, leading to losses in performance. As discussed in Section 1 omni-directional reception and the attempted decoding of all detected packets are the main problems fundamentally limiting current networks. We now investigate them in more detail in Section 2.1 and analyze existing solutions in Section 2.2.

2.1 Performance analysis of directionality and unwanted packet overhearing

To validate our analysis of the key mmWave WiFi deficiencies we perform simulations using the ns-3 IEEE 802.11ad/ay module [3]. This is meant to complement previous conclusions drawn by performance evaluations of COTS WiFi networks such as [1, 4, 31, 35, 36, 39] by studying a dense deployment under idealized conditions, removing the effects of hardware imperfections and device-specific implementation details. In this way, we ensure that our insights are generalized and connected to essential mmWave behaviors. We use a simple indoor scenario with a dense deployment of 16 APs. Each AP has only one associated STA and can thus use directional reception. STAs transmit UDP traffic with a data rate of 300 Mbps, resulting in an aggregate load of 4.8 Gbps.

First, we evaluate the possible benefits of enabling directional reception. Fig. 2 shows the aggregate throughput with omnidirectional and directional reception, revealing a dramatic increase of 150% in median throughput when directional reception is used. Moreover, we find that directional reception practically eliminates packet failures due to low SNR, reducing them from 10% to only 0.4%.

Next, we demonstrate the harmful effects of unwanted packet reception. For this purpose we implement a filter on the PHY layer that cuts reception of all packets not intended for device, immediately after preamble detection, leaving it free to receive its own packets. In Fig. 3 we show how this benefits network throughput, using both quasi-omni (blue) and directional (red) reception. We observe that in both cases performance is increased with throughput gains above 40%. Additionally, we see how directional reception and packet filtering complement each other. The directional reception enhances the spatial sharing potential and packet filtering helps realize this potential by reducing packet failures.

2.2 Existing solutions

The cause of both problems we study can be traced back to the usage of CSMA/CA, a random-access scheme without a fixed schedule. APs can not use a directional BP to receive packets because they are not aware *which* STAs is transmitting the packet, preventing them from steering towards them. Similarly, since they do not know *when* they will receive packets intended for themselves, they attempt to decode every packet they detect.

While one solution would be to use another channel access mechanisms such as a Time-Division Multiple Access (TDMA) scheme with a pre-defined transmission schedule, in practice, proposed alternatives have been proven to be too complex, inefficient and inflexible for implementation. Despite the fact that IEEE 802.11ad and IEEE 802,11ay allow for channel access with both a polling-based scheme and TDMA-like scheduled access, they are not implemented in any current COTS devices. The main issue with TDMA lies in its unsuitability for bursty or low latency traffic and the complexity of designing a schedule that implements spatial sharing. Poliing, on the other hand, suffers from significant overheard. Finally, CSMA/CA is very simple and easy to implement and highly robust. These are desirable properties that are valuable for WiFi protocols and are worth retaining. Therefore, we looked for approaches that are designed for random-access networks and can address CSMA/CA deficiencies, such as the ones discussed below.
RTS-CTS and CTS-to-self in mmWave WiFi: RTS-CTS and CTS-to-self were designed to reduce WiFi collisions and as they enable user identification ahead of the transmitted data packet they can be used to enable directional reception in mmWave WiFi. Studies of COTS devices [1, 41] have found that RTS-CTS is in fact commonly used in mmWave WiFi, although not for directional reception. As they address both directional reception and MAC efficiency and they are standard compliant, we consider them as the closest baseline schemes for comparison with our work. Fig. 4 shows RTS-CTS and CTS-to-self operation in the context of directional reception. The transmission of the RTS or CTS-to-self frame announces the intent to transmit, protecting the data by reserving the channel. By signaling the identity ahead of the data, it allows the receiver to select the receive BP before data reception.

Both mechanisms, however, have been found to limit performance due to the high overhead and inefficient airtime usage by control packets. Consequently, they can increase network latency, which might be critical for applications such as AR/VR. Analysis of RTS-CTS in mmWave WiFi has also found that it can have a negative effect on spatial sharing [1, 41]. Finally, from Section 2.1, we note that packet filtering based on identification from RTS or CTS-to-self packets is not fully reliable, since there is no guarantee that the next packet received is from the same source as the announcement packet and can thus lead to discarding useful packets.
MAC filtering: several methods allow to filter unwanted packets based on the MAC address. However, filtering at the MAC layer incurs a delay until the filter can be applied which reduces its usefulness. We use the simulation scenario from Section 2.1 to demonstrate this by comparing the performance of the optimal PHY filter, applied directly after preamble detection with a MAC filter that is applied after the reception and decoding of the MAC header. Fig. 3 shows the comparison of the throughput results with both omnidirectional and directional reception. We can see that cutting reception early on at the PHY layer makes a difference, due to the high number of short control packets exchanged where the MAC header is a significant portion of the packet.

We find that existing solutions are inefficient as they rely on MAC identification to control PHY layer behavior such as BP selection and packet reception, which imposes either overhead or delay. To eliminate these drawbacks, the obvious solution is to instead introduce PHY layer identifiers (IDs), which allows to address both directional reception and unwanted packet reception without any additional overhead. This is the core motivation for the design of SIGNiPHY, explained in more detail in the following sections.

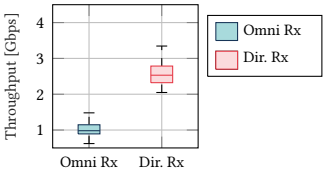


Figure 2: Throughput with omni and directional reception

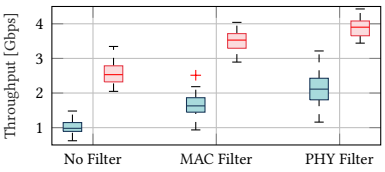


Figure 3: Throughput with filtering of unwanted packets

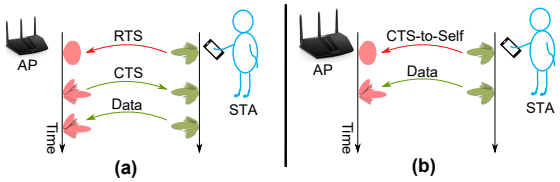


Figure 4: Directional reception through (a) RTS-CTS or (b) CTS-to-self

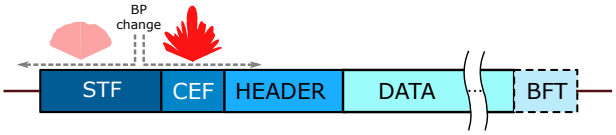


Figure 5: IEEE 802.11ad frame format

3 SIGNiPHY DESIGN

As we highlight in Section 2, PHY layer IDs are the only approach to enabling directional reception without high control packet overhead. MAC layer signaling is simply not sufficient as it identifies the user too late in packet reception. The key limitation is that any changes to the receive BP have to finish before channel estimation starts in order to not destroy the packet decoding due to failed equalization. Fig. 5 shows IEEE 802.11ad packet structure. In mmWave WiFi, channel estimation is done in the CEF field, immediately after packet detection. Therefore by the time that the MAC header, located in the packet payload has been decoded, it is already too late to make any changes to the BP. This implies that the PHY ID we introduce has to be embedded in the packet preamble, or more specifically in the Short Training Field (STF).

This makes the design of the PHY identification quite challenging for three reasons: 1) The packet preamble enables fundamental receive functionalities like packet detection, CFO estimation and synchronization which must not be altered. Therefore, when modifying the preamble design we have to ensure that these functionalities are preserved. 2) The modified preamble has to have the same inherent structure and auto-correlation properties in order to ensure backward-compatibility and interoperability with legacy devices. 3) The embedded IDs must be decoded fast enough to allow for a BP switch before the end of the STF field.

SIGNiPHY's preamble embedding mechanism manages to accomplish all three goals and provide extremely robust ID decoding as we will demonstrate in Section 5. The details of how we accomplish that are given in Section 4, while below we elaborate on how SIGNiPHY utilizes the early PHY identification to solve key sources of mmWave WiFi inefficiency.

3.1 Enabling directional reception

It is clear that the AP benefits from using omnidirectional reception when it is in idle mode, since it allows it to receive packets from different STAs. However, a directional BP would be optimal for the packet decoding itself. SIGNiPHY enables seamless transition from omnidirectional to directional reception with zero overhead. This is done by early identification of the user identity, as soon as the preamble of the packet starts being received. If the decoded ID corresponds to an associated STA, the AP performs fast switching from omnidirectional to directional reception, steering the antenna towards the identified STA. This allows the packet payload to be received with a higher antenna gain, increasing the decoding probability. If no user ID is embedded, it remains in omnidirectional reception, thus ensuring interoperability between SIGNiPHY and legacy IEEE 802.11ad/ay devices within the same network.

Interestingly, we note that this mechanism can also be used at the STA side, although this is not necessary. Since STAs only communicate with their AP, they can simply always steer towards the AP. This reduces the carrier sensing accuracy outside the BP main lobe and could increase collisions. However, carrier sensing is enhanced in the area towards the AP, which can be beneficial. Additionally, packet detection is improved by the higher antenna gain, enabling reception of low SNR packets that would be lost with an omnidirectional BP. We found that the benefits of continuous directional reception at the STA outweigh the drawbacks and thus only use SIGNiPHY for directional reception at the AP side. However, this is an implementation choice.

Lastly, we highlight that SIGNiPHY operates independently from the beamforming training and simply utilizes the identifier to BP mapping table already provided by the beam training.

3.2 PHY Packet Filtering

An extra benefit of the SIGNiPHY user ID embedding capability is the possibility of true early PHY filtering of unwanted packets. When an AP receives a packet carrying an ID that is not registered in the network, it is able to quickly react by dropping the packet and returning to idle mode to wait for the next packet. This is different from MAC filtering (as discussed in Section 2), since SIGNiPHY does not have to fully decode the MAC header to decide whether the packet needs to be dropped or not.

Note that even with the continuing background interference caused by the unwanted packet, it is usually possible to successfully identify incoming packets from registered STAs thanks to the high robustness of the preamble (as will be shown in Section 5). Once the preamble has been decoded, the directional reception enabled by SIGNiPHY reduces the gain outside the main lobe which helps to minimize the interference from the filtered packets and increases the probability of successful packet reception. In this way, SIGNiPHY improves spatial reuse and prevents nearby networks from interfering with each other. Importantly, SIGNiPHY does not increase intra-network interference, as devices still use standard carrier sensing to determine whether they are allowed to transmit. Therefore, devices do not transmit more than in standard operation, but instead the probability of successful transmission is increased.

3.3 Protocol implementation

We have two main design considerations for SIGNiPHY: 1) ease of implementation and 2) avoiding unintended negative behavior. We ensure 1) by avoiding global optimizations and using simple distributed mechanisms that do not need coordination. In fact, the only required information is the user IDs which can be obtained with no overhead in several ways. One option is to re-purpose the Association Identifier (AID). This only requires randomizing the AID allocation and ensuring that assigned AIDs are within the SIGNiPHY ID space. Another option is to apply a known hash function to the MAC address that maps it to our ID space. In addition, backward compatibility at the protocol level is ensured, as devices always default to standard behavior in case no ID has been embedded in the preamble by legacy STAs.

Finally, handling duplicate IDs among STA of different networks is feasible by monitoring the SNR change after the switch to a directional BP and the match between the decoded ID and the MAC address. Once an AP has detected duplicate IDs, it can assign a new one to the STA in its own network, ensuring that duplicate IDs are only transient. During this transition, the AP simply uses the BP for the associated STA, rather than discarding the unwanted packet, which is no worse than receiving it omnidirectionally.

We accomplish 2) by designing SIGNiPHY to not increase transmission probabilities and instead we focus on optimizing packet reception, in order to increase spatial reuse without adding interference. Additionally, we ensure that even in the case of incorrect ID decoding, SIGNiPHY does not cause harm to network operation. For this purpose SIGNiPHY monitors the SNR change after the switch to a directional BP, as well as the match between the decoded ID and the MAC address. This allows SIGNiPHY to estimate the probability of correct decoding and default to standard omnidirectional reception when the SNR is too low for reliable ID decoding. We also note, that our evaluation in Section 5 shows that SIGNiPHY ID decoding failures only happen at very low SINR at which very few packets are detected and successful packet decoding is not possible. Therefore, due to SIGNiPHY's high robustness, we find that ID decoding errors have a negligible effect in our testbed.

3.4 Initial Setup Procedure

SIGNiPHY is designed to be an enhancement to the mmWave WiFi protocols, with only minor modifications to the operation of devices. When a new STA joins the network, the only change to the initial access procedure is that the STA is assigned a SIGNiPHY ID by the AP. As discussed in Section 3.3, this can be done in the association process by re-using the AID or through a hash function. IEEE 802.11ad/ay specify that before any data transmission can take place, new STAs need to perform beamforming training to determine the optimal BPs for communication and support several protocols to perform the training. SIGNiPHY does not modify the beam training procedure in any way and is compatible with all beamforming training protocols. It is only activated afterwards, during the transmission and reception of data packets between the AP and the new STA. The STA embeds the SIGNiPHY ID it was assigned in the preamble of all data packets it sends and the AP extracts the embedded ID and uses it to enable directional reception and PHY packet filtering.

3.5 Optional support for Dynamic Sensitivity Control (DSC)

SIGNiPHY early user identification can be beneficial beyond its core functionalities. Therefore, we envision that SIGNiPHY PHY signaling can be extended to support further mmWave WiFi enhancements. As an example, we use it to implement the IEEE 802.11ax DSC mechanism, as conceptually it requires SIGNiPHY functionalities. This new feature allows 802.11ax STAs to dynamically adjust their carrier sensing level for enhanced spatial reuse. For optimal performance it is combined with the Basic Service Set (BSS) color feature that inserts an identification field for the originating BSS in the PHY header. Together, they enable STAs to use different carrier sensing thresholds for transmissions from their own and other overlapping BSS [25]. Such a mechanism can be particularly beneficial for mmWave networks as it can allow to reduce collisions within a BSS without disturbing the spatial sharing in the network. Neither BSS color nor DSC are currently supported in mmWave WiFi, but SIGNiPHY allows us to easily implement a dynamic threshold approach by relying on SIGNiPHY IDs instead of BSS color.

4 SIGNiPHY PREAMBLE EMBEDDING MECHANISM

The role of the preamble in communication systems is to *announce* the start of a packet transmission, i.e. it goes in front of the signal being transmitted. The structure of the preamble must ensure robustness, even under severe adverse conditions, since proper detection, synchronization and impairments correction depends on how well the preamble is identified. Thus, a preamble has to have very good correlation properties.

Specifically, the IEEE 802.11ad/ay standards, include an STF (or L-STF in IEEE 802.11ay) as the first part of a packet. For data packets, the STF is composed of 16 repetitions of Ga_{128} Golay sequences, followed by a $-Ga_{128}$ to identify the end of the STF. Control packets (C-PHY) have 48 repetitions of Gb_{128} Golay sequences instead of 16, which makes them even more robust. The STF is modulated using $\frac{\pi}{2}$ Binary Phase Shift Keying (BPSK), which greatly simplifies the processing. Note that this is independent of the packet payload modulation schemes, which can be of higher-order.

The STF is used for packet detection, symbol synchronization, CFO estimation and correction, as well as coarse synchronization (boundary detection). The repeated structure of the STF is used by the receiver to detect the start of a packet, usually by implementing a normalized autocorrelation (NAC) method [23, 26]. The CFO estimation is computed by averaging phase difference measurements across identical sequences that are sent periodically. Boundary detection identifies the end of the STF, to start processing the rest of the packet. The simplest implementation only requires to identify the phase inversion caused by the switch from Ga_{128} to $-Ga_{128}$, to obtain a coarse synchronization point [19].

A key observation is that *none of these STF tasks require explicit knowledge of the preamble sequences* as long as they have the same autocorrelation properties as the original one, which we exploit to implement SIGNiPHY.

4.1 Redesigning the preamble

From the above discussion, it follows that the main STF requirement is to have multiple repetitions of sequences with good correlation properties, with a phase-inverted sequence at the end for boundary detection. For backward compatibility with legacy devices, we have the additional constraints of keeping the fixed duration of the STF and the length of the periodic sequence used to build the STF.

Intuitively, to embed user identities in the preamble of communication packets, it is necessary that each user have its own preamble, such that they can be distinguished from each other. SIGNiPHY relies on the properties of Golay sequences [38] that state that it is possible to build Golay sequences by concatenating shorter sequences. Then, by exploiting the different combination of such shorter sequences, we are able to assign a different preamble for each user, without incurrin in any penalty since preamble processing functionalities operates with the longer sequence.

Let $\boldsymbol{\psi}_{a_i}$ be the autocorrelation of a sequence $\boldsymbol{a}_i$ and $\mathcal{A} = \{\boldsymbol{a}_i \mid 1 \leq i \leq p\}$ is a set of bipolar $(+1/-1)$ sequences which satisfy

$$\sum_{i=1}^{p} \boldsymbol{\psi}_{a_i}(k) = 0, \ \forall k \neq 0. \tag{1}$$

Such binary sequences are called Golay complementary sequences and the set is called a Golay complementary set [17, 38]. These sequences find application in system identification and also form an integral part of the preamble (STF, CEF) of IEEE 802.11ad/ay packets [20, 21]. Golay sequences are generated using either recursive or non-recursive methods. To design our preamble structure, we rely on the following non-recursive method.

Complementary set synthesis: Consider a set of Golay sequences $\boldsymbol{a}_k, \forall k \in \{1, \ldots, K\}$ of length N and $\boldsymbol{u} = \left[u_1, \ldots, u_K\right]$ be any column of orthogonal matrix $\boldsymbol{H}$ of size $K \times K$ with only $\{+1, -1\}$ as entries, then set $\boldsymbol{\mathcal{S}}$ comprising of sequences $\boldsymbol{s}_k$ of length NK is a complementary set that satisfies Eq. (1) [38] and $\boldsymbol{s}_k$ is defined as

$$\boldsymbol{s}_k = \left[\boldsymbol{a}_i^{u_1}, \ldots, \boldsymbol{a}_K^{u_K}\right] \tag{2}$$

As an example, let $(\boldsymbol{x}, \boldsymbol{y}, \bar{\boldsymbol{x}}, \bar{\boldsymbol{y}})$ be complementary sequences and

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

be an Hadamard matrix. Then

$$\{[\boldsymbol{x}, \boldsymbol{y}, \bar{\boldsymbol{x}}, \bar{\boldsymbol{y}}], [\boldsymbol{x}, \bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}, \boldsymbol{y}], [\boldsymbol{x}, \bar{\boldsymbol{y}}, \boldsymbol{x}, \bar{\boldsymbol{y}}], [\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}, \boldsymbol{y}]\} \tag{3}$$

are Golay sequences and form a complementary set. Here, $\bar{\boldsymbol{x}}$ represents the complement of $\boldsymbol{x}$.

Non-recursive Golay sequence synthesis: Consider a set of Golay sequences $\boldsymbol{a}_k, \forall k \in \{1, \ldots, K\}$ of length N, then,

$$\boldsymbol{s}_j = \left[\boldsymbol{a}_i, \ldots, \boldsymbol{a}_K\right] \tag{4}$$

is a new Golay sequence. $\mathcal{F}$ contains all combinations of $\boldsymbol{a}_i, \forall i \in \{1, \ldots K\}$. While the complete set $\mathcal{F}$ does not satisfy the property (1) [17], each sequence in $\mathcal{F}$ and its complement do, and can be used as a complementary pair for system identification purposes.

We rely on the two properties (2,4) stated above, to design our proposed STF structure that embeds the user identity. Based on property 1 (2), we can decompose the standard Golay sequence of STF as Ga_{128} = [Gb_{32} Ga_{32} -Gb_{32} Ga_{32}]. Then, according to (4), by considering all possible combinations of $\pm\mathrm{Ga}_{32}$ and $\pm\mathrm{Gb}_{32}$ sequences, it results in 256 different 128-length sequences.[1]

However, some limitations prevent us from using all possible sequence combinations. While packet detection is extremely robust (see Section 5), the packet *detection point* depends on the SNR and on the confidence value added to the detection [23]. Although it is possible to estimate the exact start of the sequence, this would require at least to perform channel estimation and then back-propagate to a posteriori determine the start of the sequence. This would incur too high latency and high complexity due to the required buffering of samples. We therefore remove sequences that are cyclically shifted versions of other sequences from the set, aiming to keep the design as simple as possible to facilitate integration in real systems.

Furthermore, due to CFO and the relative phase of the local oscillator used in STAs and APs, it is not straightforward to distinguish positive sequences from negative ones. We thus also remove sequences that are 180^o phase shifts of others. The remaining dictionary $\mathcal{D}$ contains 38 different sequences.

4.2 Extracting the embedded information

Let us consider a fundamental sequence $\boldsymbol{x} \in \mathbb{C}^{128}$, that is composed of combinations of $\pm\mathrm{Ga}_{32}$ and $\pm\mathrm{Gb}_{32}$ sequences (from here on: $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively), that are $\frac{\pi}{2}$-BPSK modulated. The STF is composed of multiple repetitions of $\boldsymbol{x}$. The received signal $\boldsymbol{y}$ at the receiver can be expressed as

$$\boldsymbol{y}[i] = \sum_{l=0}^{L} \boldsymbol{h}[l] \cdot \boldsymbol{x}[i-l] + v[i]. \tag{5}$$

Here, $\boldsymbol{v}[\cdot]$ is the additive noise at the receiver and $\boldsymbol{h}[\cdot]$ is the time-domain CIR with L taps represented as

$$\boldsymbol{h} = \sum_{l=1}^{L} \alpha_l \cdot \delta(\tau - \tau_l),$$

where α_l, τ_l represent path loss and propagation delay, respectively. We rely on a cross-correlation-based decoding algorithm, whose inputs are the noisy baseband signal $\boldsymbol{y}$ and the sequences $\boldsymbol{a}$ and $\boldsymbol{b}$.

$$\boldsymbol{R}_g[i] = \frac{1}{32} \sum_{n=0}^{31} \boldsymbol{y}[i+n] \cdot \boldsymbol{g}[n]^* \text{ where } \ g \in \{\boldsymbol{a}, \boldsymbol{b}\} \tag{6}$$

where $[\cdot]^*$ is the conjugate operator. $\boldsymbol{R}_g$ contains peaks that correspond to the waveform used in the STF as well as delayed and attenuated copies of it, depending on the path-delay profile of $\boldsymbol{h}$. $\boldsymbol{R}_g$ captures the similarity between the received sequence and candidate sequences in $\mathcal{D}$, which we use to decode the ID.

A naive decoding approach would be brute-force parallel correlation. However, this requires a bank of 38 128-bit correlators which is costly. Instead, SIGNiPHY relies on the observation that a sequence in $\mathcal{D}$ can be uniquely identified by estimating its key features. That is, since we embed the user information in four length-32 sequences, we only need to estimate whether each individual sequence corresponds to $\boldsymbol{a}$ or $\boldsymbol{b}$ and the phase difference between those sequences.

[1] The main reasons for using length-32 sequences instead of length-16 are i) that the robustness of Golay sequences against noise increases with their length and ii) the delay spread of the channel could introduce aliasing between adjacent Golay sequences, which would impose additional challenges to the decoding.

We map this information to a 7-bit code c as shown in Eq. 7, which we then map to a unique entry in the dictionary $\mathcal{D}$.

$$\underbrace{c[0]\ c[1]\ c[2]\ c[3]}_{\text{Classification bits}}\quad\underbrace{c[4]\ c[5]\ c[6]}_{\text{Phase Difference bits}} \tag{7}$$

To compute the classification bits, first we compute the index I using Eq. 8 that returns the position of the maximum across the concatenation of $\boldsymbol{R}_a$ and $\boldsymbol{R}_b$

$$I = \arg\max_n \Big(\boldsymbol{R}_a[m+n], \boldsymbol{R}_b[m+n]\Big) \bmod 32\,, \tag{8}$$

where m is a random shift in the correlation $\boldsymbol{R}_g$, that depends on the packet detection point. Then we collect the peaks from the correlator output in an array for all $g \in \{\boldsymbol{a}, \boldsymbol{b}\}$ as

$$\boldsymbol{P}_g[i] = \boldsymbol{R}_g[m + 32i + I]\ \forall i \in \{0 \dots 3\}\,. \tag{9}$$

Given the set $\boldsymbol{P}_g$, we identify if the peak belongs to $\boldsymbol{a}$ or $\boldsymbol{b}$ by comparing their absolute values and then getting the classification bits $\boldsymbol{c}$ and the final correlation peaks $\boldsymbol{R}$ as shown in Eq. 10 and Eq. 11.

$$\boldsymbol{c}[i] = \begin{cases} 1, & \text{if } |\boldsymbol{P}_a[i]| > |\boldsymbol{P}_b[i]| \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

$$\boldsymbol{R}[i] = \max(\boldsymbol{P}_a[i], \boldsymbol{P}_b[i]) \tag{11}$$

Step 2 computes the Phase Difference bits from Eq. 7 by computing the relative phases of $\boldsymbol{R}$. Note that although absolute phases of the peaks may be corrupted, their relative phases are intact and the easiest way to find the relative phase is by addition, where in-phase leads to a maximum.

$$\boldsymbol{c}[i+4] = \begin{cases} 1, & \text{if } |\boldsymbol{R}[i] + \boldsymbol{R}[i+1]| > |\boldsymbol{R}[i] - \boldsymbol{R}[i+1]| \\ 0, & \text{otherwise,} \end{cases} \tag{12}$$

where $i = \{0, 1, 2\}$. From Eq. 12, we see that the phase difference depends on the sign of the first sequence used to build the entries in $\mathcal{D}$. As we avoid 180° phase shifted codes, both codes point to the same entry in $\mathcal{D}$. Finally, we map c to one of the 38 entries of $\mathcal{D}$ by means of a Look-Up Table (LUT) with 128 entries (7-bits), considering the possible 180^o phase changes and cyclic shifts. LUTs map well to FPGA architectures and require few logic elements.

4.3 Implementation

In this section, we address the implementation of SIGNiPHY in hardware. Fig. 6a shows a diagram with the necessary hardware blocks to decode the STF of IEEE 802.11ad/ay packets, highlighting the ID decoding block. After the down converter and Analog-to-Digital Converters (ADCs), the ID block takes the I/Q samples from the packet detector block, computes the ID and then *enables* the operation of the CFO estimation and correction and boundary detection. If the ID corresponds to a known user, it sends a command to the antenna controller block to change the receiver BP from quasi-omnidirectional to the corresponding directional one. This is done by sending GPIO pulses from the antenna controller to the mmWave front-end. The BP change has to finish before receiving the part of the preamble intended for channel estimation, to not corrupt the subsequent payload decoding.

The architecture chosen for the ID decoding block is shown in Fig. 6b. Considering an FPGA clock frequency of f_{clk} = 440 MHz, we choose a Super Sampling Rate factor (SSR) of four (SSR=4), ensuring a proper balance between area and latency. The I/Q samples coming from the packet detector block pass through a $\pi/2$ derotation block which reverses the effect of the $\pi/2$-BPSK modulator. This allows to implement the correlation as two real-valued correlators and avoids complex-valued multiplications. For the correlators, we choose an architecture similar to the one from [26], which we modify to implement a fast architecture for length-32 Golay sequences. Using the same logic elements, the block computes correlation against both Ga_{32} and Gb_{32} sequences. The outputs of the correlators are fed to the blocks surrounded by dashed lines in Fig. 6b, which implement Eq. 8, to obtain I. At the same time, the outputs of the correlators pass through shift registers that match the latency incurred by the I computation blocks.

The classification block implements Eq. 9 to Eq. 11 by sequentially sampling the $\boldsymbol{P}_a$ and $\boldsymbol{P}_b$ values from $\boldsymbol{R}_a$ and $\boldsymbol{R}_b$, then selecting the ones with higher amplitude. The Phase Diff. block computes the phase differences between the $\boldsymbol{R}$ values by implementing Eq. 12. Once we build c, a LUT searches for the unique 6-bit code that matches the User ID, as explained in Section 4.2.

We implement the architecture in Fig. 6b on a Xilinx XCZU28DR FPGA, which only requires 0.6% of the available logic elements and computes the ID in just 160 ns, corresponding to 10% of the duration of the STF for data packets. We use an AXI-stream interface which makes it easy to use the block in different hardware architectures.

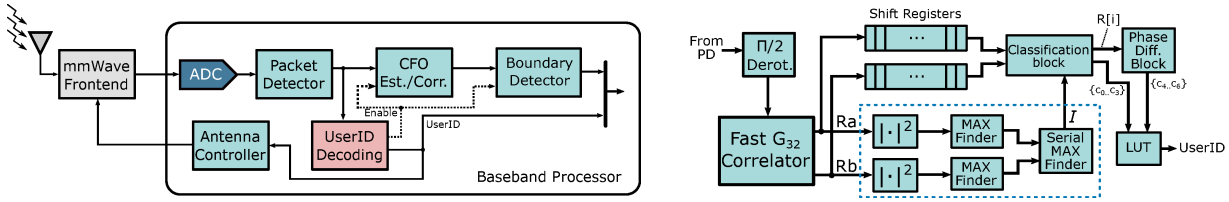
As can be seen in Figure 6a, SIGNiPHY has been designed to need minimal modifications with very low implementation complexity. For APs, none of the preamble processing blocks are modified, and only the ID-decoding block is added, requiring 10% extra hardware resources in the already minor preamble processing block. The additional power consumption is also negligible compared to components like ADCs and amplifiers. For STAs, 32-bit Golay sequences are already included in IEEE 802.11ay, and therefore, only a very simple logic is required to select the successive sequences when building the preamble. Finally, fast BP switching is already required in the standards for beam refinement and group beamforming.

5 EXPERIMENTAL EVALUATION

To validate the system, we integrate the ID decoding block in an IEEE 802.11ay-compatible FPGA-based testbed that is based on an open-source platform [24] with 60 GHz RF-frontends with analog beamforming capabilities [33]. First, we quantify the effects of modifying the STF structure, to ensure the backward compatibility. Next, we evaluate the ID decoding accuracy and the timing required to change BPs to not compromise the rest of the processing.

5.1 Ensuring preamble functionality

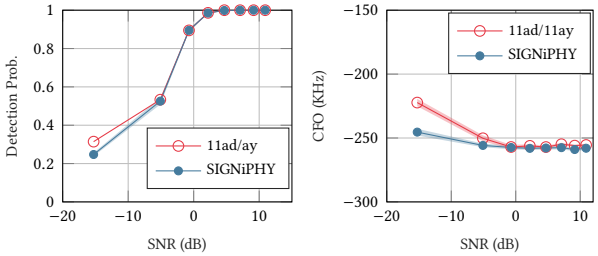
To validate that the modified preamble does not compromise STF functionality, we connect Tx/Rx mmWave RF front-ends to the same FPGA baseband processor. This allows to account for packets not detected by the packet detector block and estimate the CFO and boundary detection accuracy for detected packets. We set transmitter and receiver antennas 4 m apart and adjust the transmit power to set different SNR values. For each SNR, we analyze 2000 packets and compare SIGNiPHY to the standard IEEE 802.11ad/ay STF.



(a) STF hardware processing blocks

(b) Preamble ID decoder architecture

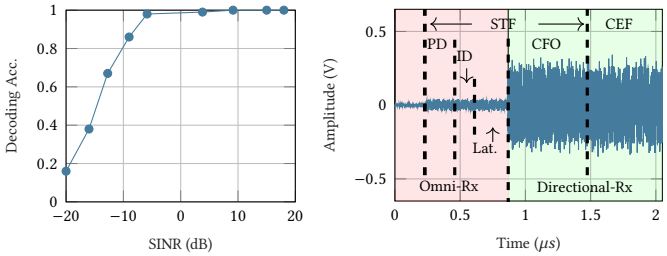
Figure 6: Hardware implementation of SIGNiPHY



(a) Packet Detection

(b) CFO Estimation

Figure 7: Backward Compatibility



(a) ID decoding accuracy

(b) SIGNiPHY timing

Figure 8: SIGNiPHY performance

Fig. 7a shows that SIGNiPHY preambles have the same packet detection probability for SNR values higher than -5 dB. For an average SNR of -15 dB, SIGNiPHY introduces a minor reduction of 6 % in the detection probability. However, in such noisy environments, data communication is impossible even for the lowest Modulation and Coding Scheme (MCS). In Fig. 7b, we show SIGNiPHY's CFO accuracy compared to that of IEEE 802.11ad/ay preambles. Similar to the packet detection accuracy, for SNRs higher than -5 dB the difference in the estimated CFO is lower than 2%, while for lower SNR values the difference increases to ~10%. As pointed out in [15], such small variations in the CFO estimation do not impact the performance of the receiver, since minor residual CFO can be corrected later in the processing pipeline.

Additionally, we also evaluate the boundary detection performance. In this case, the boundary detection probability is 100% for both, the IEEE 802.11ad/ay and the SIGNiPHY preambles, for all the SNR values from Fig. 7.

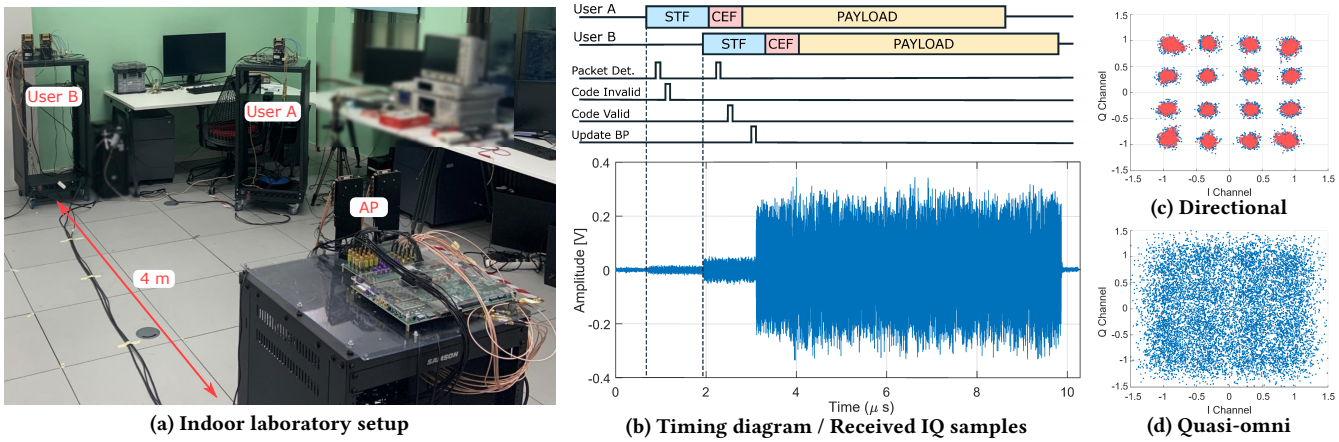
5.2 SIGNiPHY performance

After validating that SIGNiPHY has no significant impact on the preamble processing, we evaluate the performance of the ID decoding block. First, we analyze the probability of correctly decoding the ID under noise plus interference conditions. Note that the ID block from Section 4.3 *always* computes an ID from $\mathcal{D}$ when triggered by the packet detector. For this experiment, we send data packets from another transmitter with carrier sensing disabled, which constantly collide with the SIGNiPHY preambles. This is a highly challenging scenario, since the payloads of the interfering data packets use Golay sequences as guard intervals between data blocks [20, 21], which could confuse the ID decoding block. We use an additional mmWave front-end with fixed interference power and change the power of the mmWave front-end transmitting the SIGNiPHY packets to obtain different SINR values. As can be seen in Fig. 8a, we get 100 % decoding accuracy for SINRs higher than 5 dB, 99.5 % for SINR>-5 dB and for lower values it starts decreasing until 16 % for extremely low SINRs around -20 dB. As can be seen, the ID decoding is extremely robust, offering close to 100 % decoding accuracy for SNRs where packet detection is possible.

Finally, we must ensure that after decoding the ID of a valid user, there is enough time to change from quasi-omni to a directional BP. In Fig. 8b we show the received samples from the testbed and the time intervals required by STF tasks and SIGNiPHY to operate. The packet starts at time 0.22 μs and is detected 0.21 μs later. Then, the ID block requires 0.16 μs to decode the ID. The latency required to change from quasi-omni to directional reception and the delay incurred by the ADCs to deliver the samples to the FPGA logic is denoted by "Lat". The latter is entirely ADC-FPGA architecture dependant, and for our specific hardware takes 0.25 μs. As shown in the figure, both CFO and channel estimation with the CEF are performed already with the directional BP to augment packet decoding probability. This leaves 0.5 μs to perform CFO estimation which is more than enough to get a good estimate over several Golay sequences [26].

5.3 Real-time operation

We test the *early* packet filtering of SIGNiPHY in a real indoor scenario, as shown in Fig. 9a. We deploy three nodes, one acting as an AP while the other two are configured as users (`User A` and `User B`). For this experiment, the ID of `User B` is registered in the AP, while the one of `User A` is *not registered*. Both users transmit uplink frames using directional BPs to the AP, with similar transmit power, while the latter is listening using a quasi-omnidirectional BP. Both users are transmitting standard compliant MCS12 IEEE 802.11ad single carrier packets (LDPC rate = 3/4 and 16-QAM modulation) with different payloads.



(a) Indoor laboratory setup

(b) Timing diagram / Received IQ samples

(c) Directional

(d) Quasi-omni

Figure 9: Real-time operation of SIGNiPHY

In Fig. 9b we present the tough case where a packet from `User A` arrives first at the AP. In this scenario, as soon as the packet is detected, the Preamble ID decoding block (Fig. 6b) starts decoding the ID and compares its value with the registered list in the AP. Then, after comparison, the AP detects that `User A` is not a *valid* user and thus raises a `Code Invalid` flag, which causes the packet to be dropped. The AP returns to idle mode to continue listening to the channel. At $t = 2\mu s$, a packet from `User B` is received and detected by the AP, despite the interference caused by the ongoing packet from `User A`. After running the ID decoding block and identifying that `User B` is a *valid* user, a `Code Valid` is raised and then the antenna reconfiguration block is instructed to update the receive BP to steer in the direction of `User B`. It is worth noting that the rest of packet decoding (CEF and payload), are processed with the directional BP, i.e., at a higher SNR regime. Furthermore, the packet from `User A` is overlapping almost completely with the packet from `User B`. In Fig. 9c we show the IQ constellation of the equalized symbols (blue dots), which incurs an EVM of 10.2% compared with an ideal 16-QAM constellation, and incurs in zero bit errors after LDPC decoding, despite the interference caused by the packet of `User A`. As a reference, in Fig. 9c, we included the IQ constellation (red dots) in the case of no interference from other users. The EVM in this case is 8.6%, and it can be easily seen that both constellations almost completely overlap to each other. This demonstrates that despite the multiple packets overlapping in the receiver and the BP changes during the reception of the preamble, none of the processing functions are negatively affected by the implementation of SIGNiPHY.

To highlight the benefit of quick antenna reconfiguration based on user identification, we *force* the packet detection for `User B` (which is very unlikely, because the receiver locks to the first packet arriving to the receiver), and run the decoder without performing user identification (i.e., no change from omnidirectional to directional mode). In Fig. 9d we show the IQ constellation plot, which corresponds to a diffuse cloud of points and which cannot be successfully decoded.

As a final experiment to validate SIGNiPHY under more challenging conditions, we deploy 4 STAs and 1 AP in an indoor scenario similar to the one from Fig. 9a. In this setup, only one STA is associated in the network (ID is registered at the AP) while the other STAs represent interferers from other networks. All STAs transmit packets with MCS12 (16QAM, 3/4 LDPC encoded) which carry 40 KB information bits (different for each of them) and have a duration of 12 μs. STAs directly transmit packets without carrier sensing, with a random uniform inter-frame spacing between 10 and 50 μs. Under this setup, it is very likely that multiple packets are being transmitted at the same time and collide with each other, thus making it very challenging to detect and decode packets from the single registered station. In Figure 10 we show SIGNiPHY throughput performance, varying the number of non-registered users (interferers) in the network between 1 and 3. The three unregistered stations have the same transmit power, while the transmit power of the registered station varies to produce the different SINR values. The SIGNiPHY AP operates similarly to the timing diagram of Figure 9b, i.e., dropping the detected packets from non-registered stations and switching to a directive beam pattern and decoding the packet for the registered station. We compare SIGNiPHY with the performance of an AP without packet filtering, i.e., operating as a standard first-see-first-decode device. To allow for a fair comparison, in this case, we allow the AP to change to a directive beam pattern when a wanted packet is detected by means of decoding its ID. For comparison, we also include the maximum possible throughput that can be obtained if *all* packets from the registered STA are successfully detected and decoded. We can see that while the first-see-first-decode method is fundamentally limited in terms of achievable throughput by the existence of even a single interferer, SIGNiPHY is able to successfully cope with multiple interferers and reach the maximum throughput even at an SINR of 0 dB and 80% of the maximum throughput at -5 dB.

6 SIMULATION RESULTS FOR LARGE NETWORKS

To study SIGNiPHY in dense scenarios with channel contention and spatial sharing, we use the open-source IEEE 802.11ad/ay ns-3 module [3]. The implementation includes all mandatory MAC procedures for mmWave WiFi, and a high fidelity PHY channel model.

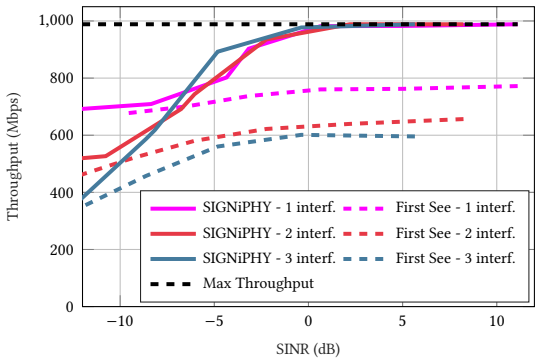


Figure 10: SIGNiPHY performance under multiple interferers

We modify [3] to support SIGNiPHY with all features described in Section 3. As ns-3 does not allow re-calculation of received power within a packet, to support directional reception, we split SIGNiPHY packets in two consecutive ns-3 events. The first event carries the ID, while the second contains the packet headers and payload. If the ID is known, the best receive BP (from prior beam training) is used to receive the second event. If the ID is not known, filtering is triggered in the `StartReceiveHeader` function and reception of the second SIGNiPHY event is canceled. SIGNiPHY can be activated in both AP and STA nodes and its functionalities can be turned on or off independently for a detailed performance analysis. Finally, we also modify the RTS-CTS and CTS-to-self mechanisms to switch to directional reception after an RTS or CTS-to-self packet, to compare SIGNiPHY with these two alternatives, as well as baseline 802.11ad/ay performance with quasi-omnidirectional reception.

6.1 Simulation scenarios

We study indoor scenarios, using a rectangular room (29.6 $m \times$ 54 $m \times$ 3 m) as the default scenario. Three AP deployments with 4, 8 and 16 APs are considered. APs are mounted on the ceiling at a height of 3 m. Between 8 and 64 STAs with a random location and orientation are placed at a height of 1.2 m. AP association is according to distance, using load balancing to have an equal number of STAs per AP. We use the IEEE 802.11ay protocol and study uplink data transmissions, to analyze channel contention. STAs transmit with data rates of 0.3, 0.5, 1, 2 and 4 Gbps, using two Aggregate MAC Protocol Data Unit (A-MPDU) aggregation sizes: the maximum aggregation supported by IEEE 802.11ay (4 MB) and a low aggregation of 16 KB. All devices use 8x32 element uniform rectangular antenna arrays, which generate narrow beams with high gain. We use IEEE 802.11ay-compliant beamforming training, taking into account both the training overhead and BP selection errors caused by interference. Each simulation has a duration of 50 s and the results are averaged over 50 simulation scenarios with different STA locations.

6.2 Evaluation Results

We first return to the scenario from Section 2.1 which has high spatial sharing potential, as 16 APs are deployed in a large room, and each AP only serves one STA. We study the two A-MPDU aggregation sizes since the aggregation affects the level of contention and the achievable throughput. The data rate is set to 0.3 Gbps per STA for the low aggregation and 2 Gbps for the high, to have similar channel saturation. Fig. 11 shows the Cumulative Distribution Function (CDF) of STA throughput measured over 2 s intervals, demonstrating the excellent SIGNiPHY performance. In the low aggregation mode, only SIGNiPHY can achieve the target data rate, with STAs having the maximum throughput approximately 40% of the time. CTS-to-self only manages this 6% of the time, while with RTS-CTS and the baseline, STAs barely get half of the target data rate. The high aggregation mode shows very similar results, with SIGNiPHY showing even more stable performance and achieving the maximum throughput 60% of the time. Moreover, throughput is below 500 Mbps only 5% of the time, compared to 25% for quasi-omni and 10% for the other schemes, showing that SIGNiPHY gains are not only focused on high performing STAs but that performance is boosted equally throughout the network. It is also evident from Fig. 11 that omnidirectional reception severely limits mmWave WiFi, leading to low achievable data rates. Additionally, the poor performance of RTS-CTS should be highlighted as even with directional reception it is not able to outperform quasi-omni IEEE 802.11ay. We found that this is not just due to the extra overhead, but also because it silenced large portions of the network, reducing the spatial sharing. STAs try to transmit a lot less often, which fundamentally limits the achievable throughput. While CTS-to-self is a better alternative, SIGNiPHY manages to have an extra gain of 50% in median throughput, since it incurs no overhead and quickly stops overhearing of unwanted packets.

Since low A-MPDU aggregation severely limits the achievable throughput and over-saturated the channel, in the following scenarios we focus on the high aggregation performance, which allows us to better explore the effect of the network density and traffic load.

To test SIGNiPHY in more challenging conditions, we design a smaller 8 AP deployment, where both spatial re-use and coverage are reduced. Additionally, we vary the number of clients per AP between 1 and 8 to create more realistic deployments, with more STAs sharing the medium. We keep the offered network load at 32 Gbps, reducing the per STA throughput from 4 Gbps to 0.5 Gbps as the number of STAs increases from 8 to 64. This allows us to study how well SIGNiPHY adjusts to different network configurations. Fig. 12 shows the median network throughput with 95% confidence intervals for the different network densities. We can see that SIGNiPHY handles density very well, with the median aggregate throughput remaining practically constant, regardless of the number of STAs. Although CTS-to-self also shows good performance, SIGNiPHY outperforms it by 20%. RTS-CTS and quasi-omni are both 50% below SIGNiPHY and furthermore they degrade as the density increases. Finally, we verify that even in dense deployments, SIGNiPHY maintains a high level of fairness. In the 64 STA deployment, STAs receive less than half of the offered throughput only 10% of the time, compared to 20% for CTS-to-self, 55% for quasi-omni and 76% for RTS-CTS.

Moreover, we demonstrate that SIGNiPHY improves another key network metric, latency. Fig. 13 shows the CDF of the application layer latency for the 8 STAs deployment including buffering delays in the MAC queue. We see that the latency gains are especially high towards the tail of the distribution. SIGNiPHY keeps packet latency below 76 *ms* 90% of time which is 43 *ms* lower than CTS-to-self, the closest baseline scheme, and more than twice as low as RTS-CTS

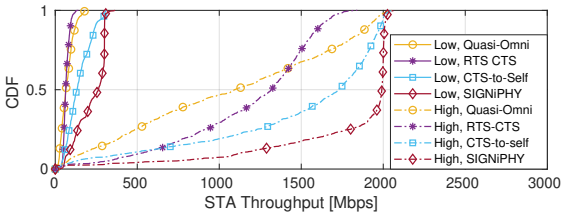


Figure 11: Throughput CDF for 16 APs, 16 STAs deployment

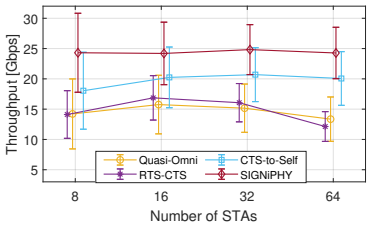


Figure 12: Median throughput for 8 APs deployments

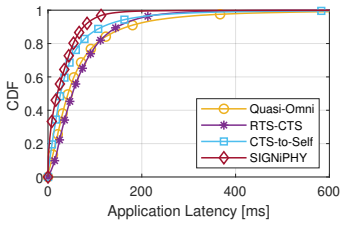
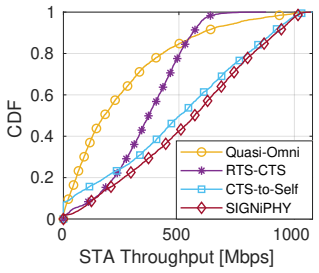
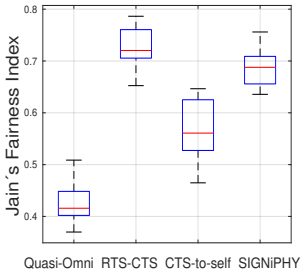


Figure 13: Application latency for 8 APs, 8 STAs deployment



(a) Throughput CDF



(b) Jain's Fairness Index

Figure 14: 8 APs, 64 STAs deployment, 1 Gbps data rate

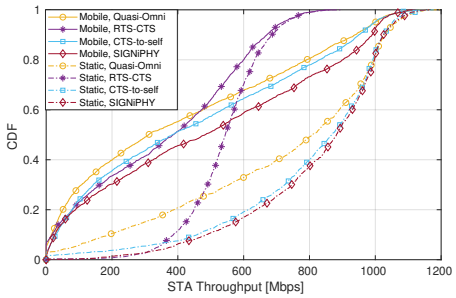


Figure 15: Throughput CDF in a mobility scenario

and quasi-omni. Finally, we observe that RTS-CTS overhead has the highest median latency, 32 *ms* higher than SIGNiPHY.

While the previous scenarios overloaded the other three schemes, SIGNiPHY never operated in fully saturated conditions, with STA always achieving a median throughput of 85% or higher of the offered load. Therefore, we set a higher data rate of 1 Gbps in the 64 STA deployment to observe SIGNiPHY in fully overloaded conditions. In Fig. 14a we see that SIGNiPHY maintains the performance gains over the three baseline schemes. Although CTS-to-self offers similar throughput for well-performing STAs, SIGNiPHY outperforms it by boosting low-performing STAs, leading to a median network throughput gain of 20%. Moreover, CTS-to-self has increased unfairness as the fraction of time STAs have 0 throughput increased to 8%, compared to 3% for quasi-omni IEEE 802.11ay. Conversely, SIGNiPHY is able to reduce it to 1%, the same as RTS-CTS. This is better illustrated in Fig. 14b which shows Jain's Fairness Index. Quasi-omnidirectional reception leads to very low fairness as STAs far from the AP have both few transmission opportunities and high packet loss due to the low link gain. RTS-CTS increases the fairness the most, but at a significant cost in terms of achievable throughput. CTS-to-self has high throughput but also high unfairness, in particular for low performing STAs. In contrast, SIGNiPHY further increases throughput and has much higher fairness, allowing low performing STAs to transmit more often even under fully overloaded conditions.

Lastly, we evaluate SIGNiPHY in a scenario with user mobility. SIGNiPHY is largely independent of mobility as it is not responsible for BP selection and simply relies on the underlying beam training mechanism to adapt to movement. To demonstrate this we design a scenario with 4 APs and 32 STAs, with a per-STA data rate of 1 Gbps. In the interest of simulation time and complexity, each AP has 2 mobile and 6 static clients. Fig. 15 shows the CDF of the per-STA throughput only for the mobile STAs, comparing the performance with a static scenario in which the STAs remain in their initial position for the duration of the simulation. We can see that while mobility has a negative effect on throughput, SIGNiPHY is not more affected than the other schemes and still outperforms them. In fact, the gain in performance compared to CTS-to-self is increased, as SIGNiPHY is more robust to interference. It is interesting to observe that quasi-omnidirectional reception, while still inefficient, is not as harmful in case of mobility as the wide BP can sometimes prevent link misalignment. Overall, SIGNiPHY increases the aggregate network throughout by 13%, 32% and 50%, as compared to CTS-to-self, RTS-CTS and quasi-omni, respectively.

7 DISCUSSION

We designed SIGNiPHY as a step towards practical mmWave deployments by enhancing packet reception. Our experimental results clearly demonstrate how SIGNiPHY increases resilience to interference and enables packet decoding under very challenging conditions. In turn, in the simulation results, we show how this translates into enhanced spatial sharing, allowing for higher throughput and lower latency, especially for STAs that get few transmission opportunities. This demonstrates the potential for use of SIGNiPHY in a variety of applications, from AR/VR due to the low-latency and high-throughput requirements to dense deployments like HD camera networks and Internet of Things (IoT) networks.

One challenge in very dense deployments might be scalability due to the limited ID space of SIGNiPHY. In most cases, 38 IDs should be sufficient to cover the full collision domain due to the short range of mmWave. However, for extremely dense scenarios it is also possible to significantly extend the number of IDs to 532 by additionally using $\pm Gc_{32}$ and $\pm Gd_{32}$ (already supported by IEEE 802.11ay) when building the preamble. This requires minor additional hardware resources, with an extra 32-bit correlator and

storage needed. Therefore, the ID space can be chosen depending on the trade-off between scalability and implementation cost. The increased ID space can also help to avoid duplicate IDs among STAs of different networks. As discussed in Section 3.3, duplicate IDs are only transient and do not disturb wanted packet reception. However, avoiding them can improve SIGNiPHY filtering.

Finally, although we have shown that mobility does not directly affect SIGNiPHY, very high mobility scenarios can still present a challenge. The issue in such scenarios is not any SIGNiPHY behavior, but rather that the use of directional receive BPs can often lead to beam misalignment caused by user mobility. Therefore, directional reception itself might lead to reduced performance. However, we plan to extend SIGNiPHY to address such scenarios with a link degradation detection mechanism. In this case, SIGNiPHY can measure the change in received power after the switch to directional reception. When this leads to a drop instead of the expected increase in power, SIGNiPHY would default back to omnidirectional reception and trigger link recovery procedures. As this check can be done on a per-packet basis and with simultaneous directional transmission and reception, SIGNiPHY has the potential to detect link misalignment very fast and prevent loss of service. Furthermore, we plan to extend SIGNiPHY to enable MIMO operation and to enhance the resilience to interferers by adapting the receive BP to create a null in the direction of known interferers.

8 RELATED WORK

PHY layer signaling: PHY signaling has been proposed for different applications [6, 11, 28, 29, 42–44]. [28] proposes replacing control packets with correlatable sequences for higher robustness and efficiency. However, this approach has significant implementation complexity due to the number of correlators needed at the receiver. Similarly, [6] does not take into account practical implementation aspects and rather focuses on security. Additionally, [6] along with [42] add an extra PHY preamble which adds overhead and prevents backward compatibility. In [11], the authors embed hidden bits in the STF by phase shift keying, which is, however, sensitive to CFO and phase noise. Time and phase shifts in the STF are used to encode bits in [44], with a decoding accuracy that depends on the estimated channel. Except for [28], all other works rely on channel estimation and equalization. This makes them unusable for our purposes since channel estimation and equalization have to be done already with the directional BP. In contrast, our approach enables quick ID decoding while having low complexity. To the best of our knowledge this is the first work to enable backward-compatible PHY signaling for mmWave WiFi.

Preventing overhearing in WiFi: Preventing overhearing of unwanted packets has mostly been considered in the context of energy efficiency for sub-6 GHz WiFi, where after stopping reception the device goes to sleep mode for the duration of the unwanted packet. This can be enabled after MAC header decoding [5, 13] or after the reception of an RTS or CTS [7, 12]. Finally, PHY signaling can enable identification and packet detection in low power mode [42] and prevent denial-of-service attacks [6]. Our approach differs from these works, both in the aim and the PHY signaling design.

mmWave WiFi optimization: Recent works [14, 22, 27, 39, 40] have considered optimizing mmWave performance in multi-AP deployments to cope with interference and increase spatial reuse. However, they approach the problem from the PHY layer perspective and attempt to optimize beam and AP selection [36, 39, 40], coordinate transmissions [14, 22] and reduce blockage [41] through global network optimization with a central controller. They are complementary to our work which focuses on improving the MAC functioning and can be jointly used with SIGNiPHY. For example, [27] mitigates interference by modifying the BP to create a null in the direction of the interferer. SIGNiPHY can provide fast interferer identification to simplify the steering of the BP null.

CSMA/CA for directional mmWave WiFi: Prior work on directional CSMA/CA mostly fails to take into account mmWave operation and assumes efficient communication is possible with omnidirectional antennas [9, 10, 37]. Works that are specifically targeted towards mmWave WiFi either assume the existence of a central controller [18, 34] to coordinate transmissions, require cooperation and relaying [8, 32] or introduce significant overhead [2]. Additionally, all these works propose new, modified MAC protocols with additional complexity and overhead which makes their deployment and evaluation in practical WiFi implementations difficult.

9 CONCLUSIONS

In this paper we present SIGNiPHY, a new approach for increased mmWave WiFi efficiency. SIGNiPHY uses preamble ID embedding for early PHY layer user identification, only 160 ns after packet detection, while maintaining backward compatibility and low implementation complexity. Fast switching from a quasi-omni to a directional reception BP allows to receive the packet payload with increased gain and lower interference. We further optimize packet reception by PHY filtering unwanted packets based on the embedded preamble ID for increased spatial re-use. We implement SIGNiPHY both on an FPGA-based mmWave testbed for a real-world validation, and in ns-3 to evaluate it in dense networks. The experimental evaluation demonstrates that SIGNiPHY is both backward compatible and highly robust, with a 99.5% decoding accuracy for SINR above -5 dB. The simulation results, meanwhile, show that SIGNiPHY boosts throughput between 13% and 230%, while ensuring high fairness.

10 ACKNOWLEDGMENTS

This work has been funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 861222 (MINTS) and the Spanish Ministry of Economic Affairs and Digital Transformation under European Union NextGeneration-EU projects TSI-063000-2021-59 RISC-6G and TSI-063000-2021-63 MAP-6G. We would also like to thank Tanguy Ropitault for his help with the simulation scenarios.

REFERENCES

[1] Shivang Aggarwal, Moinak Ghoshal, Piyali Banerjee, Dimitrios Koutsonikolas, and Joerg Widmer. 2021. 802.11ad in Smartphones: Energy Efficiency, Spatial Reuse, and Impact on Applications. *IEEE INFOCOM* (2021), 1–10.

[2] Anique Akhtar and Sinem Coleri Ergen. 2018. Directional MAC protocol for IEEE 802.11ad based wireless local area networks. *Ad Hoc Networks* 69 (2018), 49–64.

[3] Hany Assasa, Nina Grosheva, Tanguy Ropitault, Steve Blandino, Nada Golmie, and Joerg Widmer. 2021. Implementation and evaluation of a WLAN IEEE 802.11ay model in network simulator ns-3. *Workshop on ns-3* (2021), 9–16.

[4] Hany Assasa, Swetank Kumar Saha, Adrian Loch, Dimitrios Koutsonikolas, and Jörg Widmer. 2018. Medium Access and Transport Protocol Aspects in Practical 802.11 ad Networks. *IEEE WoWMoM* (2018), 1–11.

[5] Bharathan Balaji, Tamma Bheemarjuna Reddy, and B. S. Manoj. 2010. A Novel Power Saving Strategy for Greening IEEE 802.11 Based Wireless Networks. *IEEE GLOBECOM* (2010), 1–5.

[6] Andrea Bartoli, Juan Hernández-Serrano, Miguel Soriano, Mischa Dohler, Apostolos A. Kountouris, and Dominique Barthel. 2011. Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks. *IEEE Transactions on Smart Grid* 2, 4 (2011), 844–864.

[7] S. Biswas and S. Datta. 2004. Reducing Overhearing Energy in 802.11 Networks by Low-power Interface Idling. In *IEEE IPCCC*. 695–700. https://doi.org/10.1109/PCCC.2004.1395157

[8] Qian Chen, Jiqiang Tang, David Tung Chong Wong, Xiaoming Peng, and Youguang Zhang. 2013. Directional Cooperative MAC Protocol Design and Performance Analysis for IEEE 802.11ad WLANs. *IEEE Transactions on Vehicular Technology* 62 (2013), 2667–2677.

[9] Romit Roy Choudhury and Nitin H. Vaidya. 2004. Deafness: a MAC Problem in Ad Hoc Networks When Using Directional Antennas. *IEEE ICNP* (2004), 283–292.

[10] Romit Roy Choudhury, Xue Yang, Nitin H. Vaidya, and Ram Ramanathan. 2002. Using Directional Antennas for Medium Access Control in Ad Hoc Networks. In *ACM MobiCom*. Association for Computing Machinery, 59–70.

[11] Jiska Classen, Matthias Schulz, and Matthias Hollick. 2015. Practical covert channels for WiFi systems. In *IEEE CNS*. 209–217. https://doi.org/10.1109/CNS.2015.7346830

[12] Mustafa Ergen and Pravin Varaiya. 2007. Decomposition of Energy Consumption in IEEE 802.11. *IEEE ICC* (2007), 403–408.

[13] Bing Feng, Chi Zhang, Haichuan Ding, and Yuguang Fang. 2018. PhyCast: Towards Energy Efficient Packet Overhearing in WiFi Networks. *IEEE ICC* (2018), 1–6.

[14] Wei Feng, Yanmin Wang, Dengsheng Lin, Ning Ge, Jianhua Lu, and Shaoqian Li. 2017. When mmWave Communications Meet Network Densification: A Scalable Interference Coordination Perspective. *IEEE Journal on Selected Areas in Communications* 35, 7 (2017), 1459–1471.

[15] Dolores Garcia Marti, Jesus Omar Lacruz, Pablo Jimenez Mateo, Joan Palacios, Rafael Ruiz, and Joerg Widmer. 2021. Scalable Phase-Coherent Beam-Training for Dense Millimeter-wave Networks. *IEEE Transactions on Mobile Computing* (2021), 1–1.

[16] Y. Ghasempour, C. R. C. M. da Silva, C. Cordeiro, and E. W. Knightly. 2017. IEEE 802.11ay: Next-Generation 60 GHz Communication for 100 Gb/s Wi-Fi. *IEEE Communications Magazine* 55, 12 (2017), 186–192.

[17] M. Golay. 1961. Complementary series. *IRE Transactions on Information Theory* 7, 2 (1961), 82–87. https://doi.org/10.1109/TIT.1961.1057620

[18] Michelle X. Gong, Robert Stacey, Dmitry Akhmetov, and Shiwen Mao. 2010. A Directional CSMA/CA Protocol for mmWave Wireless PANs. *IEEE WCNC* (2010), 1–6.

[19] Ya-Shiue Huang, Wei-Chang Liu, and Shyh-Jye Jou. 2011. Design and implementation of synchronization detection for IEEE 802.15.3c. In *2011 International Symposium on VLSI Design, Automation and Test*. 1–4. https://doi.org/10.1109/VDAT.2011.5783583

[20] IEEE 802.11 working group. 2012. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band. *IEEE Standard 802.11ad* (2012).

[21] IEEE 802.11 working group. 2021. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications-Amendment 2: Enhanced Throughput for Operation in License-Exempt Bands Above 45 GHz. *IEEE Standard 802.11ay* (2021).

[22] Suraj Jog, Jiaming Wang, Junfeng Guan, Thomas Moon, Haitham Hassanieh, and Romit Roy Choudhury. 2019. Many-to-Many Beam Alignment in Millimeter Wave Networks. In *NSDI*. 783–800.

[23] Jesus O. Lacruz, Dolores Garcia, Pablo Jiménez Mateo, Joan Palacios, and Joerg Widmer. 2020. mm-FLEX: An Open Platform for Millimeter-Wave Mobile Full-Bandwidth Experimentation. In *ACM MobiSys* (Toronto, Ontario, Canada). 1–13.

[24] Jesus O. Lacruz, Rafael Ruiz Ortiz, and Joerg Widmer. 2021. A Real-Time Experimentation Platform for Sub-6 GHz and Millimeter-Wave MIMO Systems *(in ACM MobiSys)*. 427–439.

[25] Leonardo Lanante and Sumit Roy. 2022. Performance Analysis of the IEEE 802.11ax OBSS_PD-Based Spatial Reuse. *IEEE/ACM Transactions on Networking* 30, 2 (2022), 616–628. https://doi.org/10.1109/TNET.2021.3117816

[26] Chun-Yi Liu, Meng-Siou Sie, Edmund W. J. Leong, Yu-Cheng Yao, Chih-Wei Jen, Wei-Chang Liu, Chih-Feng Wu, and Shyh-Jye Jou. 2017. Dual-Mode All-Digital Baseband Receiver With a Feed-Forward and Shared-Memory Architecture for Dual-Standard Over 60 GHz NLOS Channel. *IEEE Transactions on Circuits and Systems I: Regular Papers* 64, 3 (2017), 608–618.

[27] Sohrab Madani, Suraj Jog, Jesús Omar Lacruz, Joerg Widmer, and Haitham Hassanieh. 2021. Practical Null Steering in Millimeter Wave Networks. In *NSDI*. 903–921.

[28] Eugenio Magistretti, Omer Gurewitz, and Edward W. Knightly. 2014. 802.11ec: Collision Avoidance Without Control Messages. *IEEE/ACM Transactions on Networking* 22, 6 (2014), 1845–1858. https://doi.org/10.1109/TNET.2013.2288365

[29] Hanif Rahbari and Marwan Krunz. 2016. Full Frame Encryption and Modulation Obfuscation Using Channel-Independent Preamble Identifier. *IEEE Transactions on Information Forensics and Security* 11, 12 (2016), 2732–2747. https://doi.org/10.1109/TIFS.2016.2582560

[30] Sundeep Rangan, Theodore S. Rappaport, and Elza Erkip. 2014. Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges. *Proc. IEEE* 102, 3 (2014), 366–385.

[31] Swetank Kumar Saha, Hany Assasa, Adrian Loch, Naveen Muralidhar Prakash, Roshan Shyamsunder, Shivang Aggarwal, Daniel Steinmetzer, Dimitrios Koutsonikolas, Jörg Widmer, and Matthias Hollick. 2018. Fast and Infuriating: Performance and Pitfalls of 60 GHz WLANs Based on Consumer-Grade Hardware. *IEEE SECON* (2018), 1–9.

[32] Sumit Singh, Federico Ziliotto, Upamanyu Madhow, Elizabeth M. Belding-Royer, and Mark J. W. Rodwell. 2009. Blockage and directivity in 60 GHz wireless personal area networks: from cross-layer model to multihop MAC design. *IEEE Journal on Selected Areas in Communications* 27, 8 (2009), 1400–1413.

[33] Sivers Semiconductors. 2022. *EVK06002 Development Kit.* https://www.sivers-semiconductors.com/sivers-wireless/evaluation-kits/evaluation-kit-evk06002/.

[34] In Keun Son, Shiwen Mao, Michelle X. Gong, and Yihan Li. 2012. On frame-based scheduling for directional mmWave WPANs. *IEEE INFOCOM* (2012), 2149–2157.

[35] Sanjib Sur, Ioannis Pefkianakis, Xinyu Zhang, and Kyu-Han Kim. 2017. WiFi-Assisted 60 GHz Wireless Networks. *ACM MobiCom* (2017), 28–41.

[36] Sanjib Sur, Ioannis Pefkianakis, Xinyu Zhang, and Kyu-Han Kim. 2018. Towards Scalable and Ubiquitous Millimeter-Wave Wireless Networks. *ACM MobiCom* (2018), 257–271.

[37] Mineo Takai, Jay Martin, Rajive L. Bagrodia, and Aifeng Ren. 2002. Directional Virtual Carrier Sensing for Directional Antennas in Mobile Ad Hoc Networks. In *ACM MobiHoc*. 183–193.

[38] Chin-Chong Tseng and C. Liu. 1972. Complementary sets of sequences. *IEEE Transactions on Information Theory* 18, 5 (1972), 644–652. https://doi.org/10.1109/TIT.1972.1054860

[39] Teng Wei and Xinyu Zhang. 2017. Pose Information Assisted 60 GHz Networks: Towards Seamless Coverage and Mobility Support. *ACM MobiCom* (2017), 42–55.

[40] Yi Yang, Anfu Zhou, Dongzhu Xu, Shaoyuan Yang, Lele Wu, Huadong Ma, Teng Wei, and Jianhua Liu. 2020. mmMuxing: Pushing the Limit of Spatial Reuse in Directional Millimeter-wave Wireless Networks. In *IEEE SECON*. 1–9.

[41] Ding Zhang, Panneer Selvam Santhalingam, Parth H. Pathak, and Zizhan Zheng. 2019. Characterizing Interference Mitigation Techniques in Dense 60 GHz mmWave WLANs. *IEEE ICCCN* (2019), 1–9.

[42] Xinyu Zhang and Kang G. Shin. 2012. E-MiLi: Energy-Minimizing Idle Listening in Wireless Networks. *IEEE Transactions on Mobile Computing* 11, 9 (2012), 1441–1454.

[43] Zhengguang Zhang, Hanif Rahbari, and Marwan Krunz. 2020. Expanding the Role of Preambles to Support User-defined Functionality in MIMO-based WLANs. In *IEEE INFOCOM*. 1191–1200. https://doi.org/10.1109/INFOCOM41043.2020.9155507

[44] Zhengguang Zhang, Hanif Rahbari, and Marwan Krunz. 2021. Adaptive Preamble Embedding with MIMO to Support User-defined Functionalities in WLANs. *IEEE Transactions on Mobile Computing* (2021), 1–1. https://doi.org/10.1109/TMC.2021.3095459