Fair and Secure 5G and Wi-Fi Coexistence Using Robust Implicit Channel Coordination

Siddharth Dongre and Hanif Rahbari
Rochester Institute of Technology, Rochester, NY
Email: {sd4767, hanif.rahbari}@rit.edu

***Abstract*—5G and Wi-Fi systems are embracing coexistence in the unlicensed portions of the 5–7 GHz bands recently allocated by FCC to support the increasing data rate demands for the growing number of wireless users. To achieve fair and effective spectrum sharing, both 5G and Wi-Fi rely on carrier sensing for medium access. However, differences in sensing thresholds create an unfair advantage for 5G nodes, as they access the medium more aggressively and degrade the data rate and latency of Wi-Fi users. We first demonstrate how an adversary can stealthily exploit this unfairness to further reduce the spectrum occupancy of Wi-Fi nodes, effectively denying Wi-Fi services. Accordingly, in this paper, we propose a novel implicit channel coordination (ICC) approach to both mitigate starvation attacks and improve spectrum access fairness under practical considerations like noise and strong adversaries who try to circumvent our technique. In ICC, Wi-Fi access points (APs) influence 5G gNBs into choosing a precoding matrix that nearly nullifies 5G downlink signals at the APs, enabling concurrent gNB and AP transmissions while accounting for a hidden terminal problem this creates. We theoretically analyze and show that our ICC mitigates novel attacks we have identified, and experimentally demonstrate on a USRP testbed its resilience against starvation attacks. Our design outperforms prior work by achieving an overall 30% higher data rate of the 5G and Wi-Fi coexistence system, 3x improvement in spectrum access fairness, and 1.5x in system capacity, all while conforming with the latency requirements of 5G.**

***Index Terms*—spectrum sharing security, 5G NR-U, Wi-Fi 6E, channel coordination, nullification.**

I. Introduction

Emerging applications of 5G and Wi-Fi, such as augmented and virtual reality in mobile applications, are characterized by high data rate and low latency requirements [1]. Consequently, these technologies are embracing coexistence in the newly allocated 5–7 GHz unlicensed frequency bands through 5G New Radio Unlicensed (5G NR-U) and Wi-Fi 6E protocols, respectively, to acquire the needed additional bandwidth [2]. In the absence of fair *coexistence-aware* medium access control mechanisms, this coexistence may lead to chaos or monopoly.

In the most recent 5G specifications, coexistence with heterogeneous technologies is facilitated under NR-U by adopting the listen-before-talk (LBT) mechanism to avoid concurrent transmissions with other networks [3], [4]. On the Wi-Fi side, the carrier-sense multiple access with collision avoidance (CSMA/CA) mechanism has been used for decades for similar purposes. Both LBT and CSMA use energy detection (ED) to sense whether the medium is idle or busy, and defer and perform random backoff when it is busy. However, because the ED threshold used in NR-U is higher than the one used in Wi-Fi by default [5], NR-U devices access the shared medium more aggressively, causing Wi-Fi to defer its transmissions and enter a backoff state more frequently and for exponentially longer periods of time. Subsequently, an unfair situation is created where the spectrum occupancy of Wi-Fi degrades significantly, and its latency increases more than that of NR-U, as shown in recent studies [6]. This poses a challenge, especially for Wi-Fi networks that have multiple users demanding high data rates, as signals from a nearby 5G base station (gNB) are likely to repeatedly interrupt Wi-Fi transmissions.

The unfair coexistence problem can become more critical when an adversary tries to take advantage of the difference in ED thresholds to exacerbate the consequences, even leading to shutting down Wi-Fi data transmissions entirely—a denial of service attack we showed in our preliminary work [7]. We designed and demonstrated such a Wi-Fi *resource starvation attack* on a hardware testbed, where an attacker selectively and stealthily transmits during idle time slots between legitimate gNB transmissions to completely starve a Wi-Fi access point (AP); repeatedly forcing the AP into a backoff state while not affecting the gNB. This highlights the necessity for a robust coexistence system to not only (1) maintain fairness in spectrum access and (2) satisfy critical latency requirements of next-generation wireless networks but also (3) incorporate security by design to protect against likely adversaries.

Existing approaches address either fairness or latency challenges, but not both simultaneously. Considering fairness, existing works that use explicit channel coordination achieve adequate spectrum sharing fairness but at the cost of violating critical latency requirements. For instance, cross-technology communications involve the exchange of explicit messages between LTE and Wi-Fi nodes [8], [9], and coordinated beamforming techniques rely on the addition of dedicated devices [10], [11], both incurring a delay of about 1–2 ms due to the exchange of coordination messages. A delay of this magnitude is detrimental for NR-U applications with a 0.5 ms latency requirement [5]. On the contrary, implicit channel coordination approaches that satisfy latency requirements are limited or inadequate in improving sharing fairness due to the use of obsolete features [12] or unsatisfactory improvements (only 10%) in access fairness [13]. Increasing spectrum access efficiency using deep learning and game theoretic approaches, e.g., [14]–[17] and resource block optimization techniques such as [18]–[20] are also limited in achieving fairness because they rely on the unrealistic assumption of static traffic. Moreover, directly adjusting the ED thresholds would make them

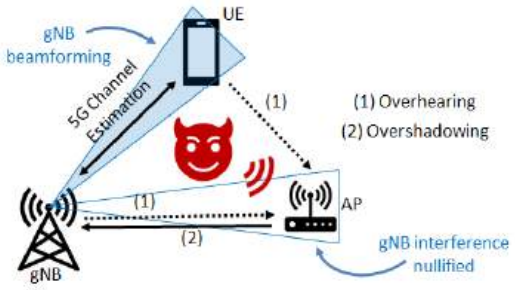


Fig. 1. Overview of the proposed technique. The AP influences the gNB to nullify its interference, providing reliable opportunities for the AP to transmit and receive. That removes the attacker's ability to interrupt the AP repeatedly.

depart from typical power levels in respective systems and increase carrier sensing inaccuracies [21]. Besides the above limitations on improving sharing fairness, which is the main motivation behind our work, none of these works consider the presence of adversaries, a unique aspect of our work.

Due to the drawbacks of existing approaches, we proposed in our preliminary work the first *implicit* channel coordination (ICC) scheme, the predecessor of the scheme proposed in this paper, that jointly addresses the benign and adversarial interference issues for NR-U and Wi-Fi coexistence without violating the latency requirements of NR-U [7]. The idea is to provide the AP with opportunities to transmit concurrently with the gNB, improving access fairness and limiting the attacker's ability to keep the AP from transmitting. As illustrated in Fig. 1, in step ①, the AP overhears unencrypted reference signals transmitted by NR-U nodes (gNB and UE) to estimate the channel between them and itself and to craft an optimum overshadowing signal, explained below. In step ②, the AP carefully overshadows (lightly superposes) this signal on the subsequent reference signals to influence, but not disrupt, the 5G channel estimation procedure. This is, therefore, unlikely to violate anti-jamming laws and regulations. ICC causes the gNB (assumed to have multiple antennas) to choose a precoding matrix that optimizes signal-to-interference-plus-noise ratio (SINR) at the UE for the 5G services and nearly nullifies the gNB signal at the AP, accomplishing our three objectives, except that it creates a new hidden-terminal problem.

In this paper, we propose direct extensions on the preliminary scheme and develop a critical, optimized technique to address its practical coexistence implications. More specifically, we improve its robustness under more practical considerations and a stronger attack model while effectively addressing a non-trivial hidden terminal problem the preliminary design introduced. The robustness and security of our enhanced ICC technique is supported by theoretical analysis and extensive experimental evaluations, as summarized below:

- We develop a novel technique to influence the gNB's channel estimation, addressing a weak assumption of the preliminary ICC that the gNB-to-UE channel capacity is not effectively reduced. As the AP would no longer detect the transmissions of the gNB and may inadvertently interfere at the UEs, in our technique the AP computes controlled noise perturbations within time constraints of the 5G channel estimation interval and adds them to its overshadowing signal. These optimized noise perturbations influence the gNB to adjust its transmission rate to accommodate concurrent Wi-Fi transmissions.
- We theoretically model and analyze the effectiveness of our enhanced ICC design under practical considerations, such as imperfect channel estimation and varying number of gNB antennas (2–10). Considering the quality of nullification, we demonstrate in our simulations that our enhanced ICC achieves at least $10\,\text{dB}$ attenuation in the gNB signal at the AP. Our time complexity analysis shows that ICC completes within $0.05\,\text{ms}$, proving its feasibility for delay-sensitive applications of NR-U.
- We justify the security of ICC under a stronger attack model that captures attempts to abuse or circumvent it, showing it is robust by design against likely attacks.
- We prototype and demonstrate ICC on software-defined radios, equipped with 2 antennas, in a 5G and Wi-Fi coexistence testbed. Our experiments show that the total data rate of the two systems increases by 30% with our technique, even under a Wi-Fi starvation attack. This increase is the result of nearly $3\times$ increase in the spectrum occupancy of Wi-Fi and only a slight decrease in that of 5G—a fair and robust system that improves the system capacity by $1.5\times$ and Jain's fairness index by at least $2.5\times$ over the state-of-the-art [13]. We experimentally verify the theoretical analysis of our enhanced ICC design and make our code and data available for reproducibility[1].

The rest of the paper is organized as follows. In Section II, we describe our system model and a brief overview of how the 5G and Wi-Fi channel estimation and access mechanisms can lead to unfair coexistence. We present our threat model in Section III and our ICC scheme in Section IV, including our novel technique to optimally influence the 5G channel estimation procedure. Our detailed theoretical analysis is presented in Section V, followed by simulation results that support the analysis. Next, we experimentally show the effectiveness of our starvation attack and the performance of ICC in Section VI. We present a summary of related work and conclude the paper in Sections VII and VIII, respectively.

II. System Model and Background

We start with an overview of the 5G NR-U and Wi-Fi coexistence system and their channel models, and how the channel is estimated in 5G. We also briefly review the differences between LBT and CSMA/CA and how they can lead to unfair channel access for Wi-Fi. A list of important abbreviations used in this paper is provided in TABLE I.

A. System Model

We assume dense urban environments, such as crowded indoor public spaces, where gNBs can create up to $-45\,\text{dBm}$ interference on Wi-Fi devices due to being within $50\,\text{m}$ of them [22]. Consider the simplified Wi-Fi and 5G NR-U coexistence system illustrated in Fig. 2. It consists of an NR-U network with one gNB and, for simplicity, one UE. We will

[1] https://github.com/nanosid/Implicit-Channel-Coordination

TABLE I
LIST OF IMPORTANT ABBREVIATIONS.

Abbreviation	Definition
CDL	Clustered Delay Line
CQI	Channel Quality Index
CSI	Channel State Information
CSI-RS	CSI Reference Signal
ED	Energy Detection
LBT	Listen-Before-Talk
MCS	Modulation Coding Scheme
MSE	Mean Square Error
PSS	Primary Synchronization Signal
RSSI	Received Signal Strength Indicator
SINR	Signal-to-Interference-and-Noise Ratio
SRS	Sounding Reference Signal
SSS	Secondary Synchronization Signal

show in Section IV that our scheme can be easily extended to support multiple UEs. The gNB has M antennas while the UE has only one, creating a multiple-input-single-output (MISO) system that allows the gNB to use beamforming. We also have a Wi-Fi AP close to the UE and we consider the worst-case scenario where the AP has only one antenna, meaning that it cannot apply interference cancellation. We consider only one AP, even though multiple APs may be nearby, because adjacent APs are usually configured to operate on different channels and hence will not coexist with the same gNB. Similarly, we consider only one gNB because other gNBs within range either use different channels or time-based scheduling to prevent simultaneous transmission on the same band.

We assume the default ED threshold of -59 dBm for the gNB, which is higher than the default -79 dBm ED threshold used by the AP (see Section II-C). The transmission duration of 5G subframes is 1 ms while the duration of Wi-Fi frames is variable depending on the size of data being sent. We further consider a nearby attacker who performs various attacks against the AP. A detailed threat model will be discussed in Section III. While we only consider interference on the AP, the pivotal Wi-Fi device, the attack and mitigation presented in this paper can also be applied to Wi-Fi clients.

Channel Models: We mainly consider two types of channel models. (1) For all transmissions involving the gNB (and attacker), we consider the Clustered Delay Line (CDL) channel model defined in 3GPP specifications [23]. CDL models are suited for MISO/MIMO systems with frequencies ranging from 0.5 GHz to 100 GHz and a maximum bandwidth of 2 GHz, making them a reasonable choice for our analysis in this paper. CDL supports five delay profiles, CDL-A to CDL-E. The CDL-C channel model is resilient to Doppler spread due to velocities of up to 30 kmph and delay spreads of up to 30 ns. Hence, given the environment of our system, we assume the CDL-C delay profile to represent non-LOS (NLOS) scenarios. (2) Although the AP does not communicate with the UE, it will inevitably create interference on the UE. Hence, we model the channel for these interference signals based on the TGax indoor NLOS channel model [24].

B. 5G Channel Estimation Procedure

Reviewing the channel estimation procedure of the gNB and UE is necessary to show how an AP can influence it, which

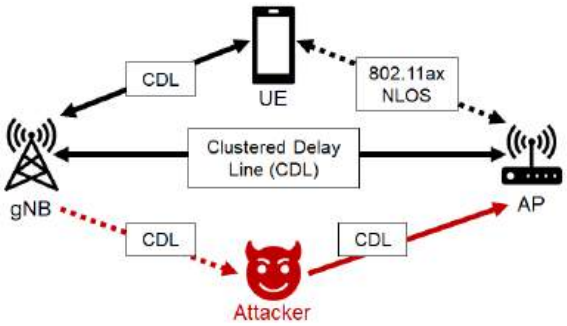


Fig. 2. Simplified 5G NR-U and Wi-Fi coexistence security model showing the channel models between the gNB, UE, AP, and an attacker.

is the basis of our implicit channel coordination technique to achieve fair spectrum sharing. The goal is to estimate the channel state information (CSI) between the gNB and the UE to determine the optimum precoding matrix that maximizes the downlink and uplink SINRs at the UE and gNB, respectively. Note that in 5G, downlink and uplink signals are sent in alternate time slots scheduled by the gNB [5].

The CSI reporting procedure is illustrated in Fig. 3. The CSI Reference Signal (CSI-RS) of the gNB contains pilot symbols located in predetermined locations as specified in [5]. The CSI-RS is used by the UE to estimate CSI parameters, such as channel quality index (CQI), that are then sent to the gNB in the unencrypted CSI Feedback message. Accordingly, the gNB calculates an optimum precoding matrix for its M antennas to transmit the downlink data. Note that in the case of multiple UEs, the gNB estimates a separate CSI for each UE and combines them to derive the precoding matrix. Next, the UE sends a Sounding Reference Signal (SRS) containing known pilot symbols similar to CSI-RS. The gNB then estimates similar CSI parameters for the uplink channel based on the received SRS and then applies a separate precoding matrix on the received uplink signal. This entire procedure is repeated every 10 ms by default, i.e., for each 5G frame structure.

C. Unfairness Problem Statement

The key difference between LBT and CSMA/CA is their ED threshold values. Wi-Fi devices tend to select the *lower* ED value of -79 dBm since most Wi-Fi devices are intended for indoor applications and do not operate at a high transmit power [24]. The gNB, on the other hand, operates at high transmit powers to support longer transmission ranges, subsequently choosing higher ED values of -69 or -59 dBm [25]. Due to a lower ED threshold, Wi-Fi devices are more sensitive to surrounding signals and so are better at detecting NR-U signals even when those signals are weaker than -59 dBm. In contrast, the gNB sometimes incorrectly detects the medium as idle even if a Wi-Fi signal is present as long as its received power is less than -59 dBm at the gNB. As a result, the gNB may schedule downlink transmissions that collide with the Wi-Fi ones. Without multiple antennas for interference cancellation, the AP is unlikely to recover the received Wi-Fi signals in such cases, and hence, a collision occurs which doubles its backoff window. The gNB, however, accesses the medium more aggressively (higher ED threshold, smaller

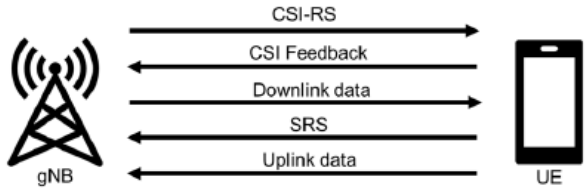


Fig. 3. Steps of the 5G CSI reporting procedure used by the gNB and UE to estimate uplink and downlink channels, in order from top to bottom.

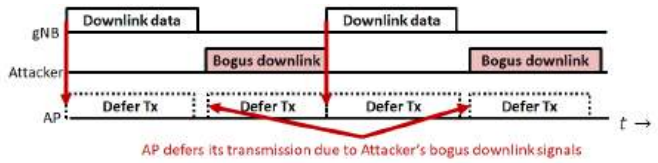


Fig. 4. Wi-Fi Starvation Attack: The attacker detects gaps between gNB transmissions to inject bogus 5G signals that keep the AP from transmitting.

backoff window) and keeps transmitting since the UE often successfully receives the signal thanks to beamforming. This causes the AP to defer its transmission and stay in the backoff state for longer periods, degrading its data rate and increasing its latency, undermining the AP's capability to serve its clients.

In effect, 5G devices occupying the shared medium more frequently than Wi-Fi create a coexistence biased towards 5G. Note that uplink transmissions from UEs, which typically have much lower power due to being battery-powered, do not cause significant interference on the AP. Hence, we consider downlink transmissions to be the dominant cause of unfairness.

III. Threat Model

We assume that the attacker emulates a gNB, without joining the NR-U network, using low-cost software-defined radios such as USRP B210. The attacker overhears the gNB's transmissions and transmits low-power falsified downlink signals, assuming the CDL-C channel model, while located within 15 m of the UE and the victim AP, a plausible scenario in a public indoor environment, such as a coffee shop. The attacker's goal is to exploit the unfairness issue to almost completely deny the AP access to the shared medium by launching a "starvation attack", explained below. We further assume that the attacker knows the ICC technique and may attempt to circumvent or abuse it by either (1) jamming 5G reference signals at the AP to reduce its effectiveness in leveraging them for estimating the gNB-AP and AP-UE channels, or (2) interfering with overshadowing signals sent by the AP aimed to influence the 5G channel estimation procedure and nullify gNB interference at the AP—two novel attacks we devise in this paper. In each attack, the attacker aims to remain stealthy by limiting the power and duration of its signals.

Wi-Fi Starvation Attack

As illustrated in Fig. 4, our stealthy Wi-Fi starvation attack is performed by transmitting bogus 5G signals only when the gNB is not transmitting (the AP already avoids transmitting during gNB transmissions). The attacker first synchronizes with the NR-U transmissions using the gNB's plaintext Primary and Secondary Synchronization Signals (PSS/SSS) sent in downlink slots. By performing PSS/SSS correlation, it identifies the signal as a 5G NR-U transmission and synchronizes with the gNB to accurately predict the time offsets of the future downlink slots in the frame structure. We tested in our experiments (see Section VI) that the attacker can detect gNB transmissions even when the gNB uses beamforming. This is because the precoding matrix is not designed to completely nullify the beamforming signal at any point around the gNB.

TABLE II
List of Important Mathematical Notations.

Notation	Description
$\mathbf{w}$	Downlink precoding matrix of gNB
$\mathbf{h_{g<D>}}$	Channel between gNB and AP ($D = W$) or UE ($D = U$)
h_{WU}	Channel between AP and one UE
$\gamma(w)$	SINR as a function of the gNB precoding matrix
ρ_S	Power of the gNB downlink signal
ρ_{RI}	Power of the AP interference plus noise
$\mathbf{w_{opt}}$	Optimal gNB precoding matrix before applying ICC
$\mathbf{Q}$	Orthonormal basis on the null space of $\mathbf{h_{gW}}$
$\mathbf{w_{copt}}$	Optimal gNB precoding matrix after applying ICC
$\mathbf{b_{CRS}}$	CSI-RS symbols received by AP
b_{SRS}	SRS symbol received by AP
$\mathbf{b_{INT}}$	Optimum overshadowing symbol (excluding synthetic noise)
μ_{opt}	Optimum synthetic AWGN noise added to $\mathbf{b_{INT}}$
γ_1	SNR reported by UE in CSI Feedback during ICC Phase 1
γ_2	SNR reported by UE after addition of μ_{opt}
$A1$	Constraint ensuring UE can recover gNB transmissions
$A2$	Constraint to ensure minimum gNB nullification at AP

From the time slots of successive downlink transmissions, the attacker determines the transmission schedule of the gNB. If no PSS/SSS signal is detected in a slot, the attacker senses if the medium is idle and if there is a gap in NR-U transmissions, in which case it triggers transmitting bogus signals immediately. To the victim AP, however, it appears as if the NR-U transmissions never stopped, so it continues to defer its transmissions after performing CSMA/CA. This reduces the AP's data rate to nearly zero (see Section VI).

If the coexistence were fair, the AP would have more opportunities to transmit, forcing the attacker to either transmit more often to keep starving the AP but risk exposure, or remain stealthy and reduce its effectiveness. In the following, we describe our ICC approach that mitigates this attack by directly addressing the challenge of unfair coexistence.

IV. Implicit Channel Coordination

We start by first explaining why we need channel coordination to address the unfairness problem. We then describe how the gNB normally calculates an optimum precoding matrix followed by the two phases of our ICC approach, including our novel two-step optimization technique to facilitate concurrent gNB and AP transmissions. A reference list for the important notations used in the following sections is given in TABLE II.

A. Significance of Implicit Channel Coordination

As we alluded to earlier, raising the current -79 dBm ED threshold of Wi-Fi would increase collisions between Wi-Fi transmissions due to the typically low power level of Wi-Fi devices (the received signal strength of a Wi-Fi signal

is usually between -85 to -65 dBm [22]) and CSMA/CA might incorrectly detect the channel as idle even during active Wi-Fi transmissions, leading to packet collisions [21]. Wi-Fi can potentially raise its ED threshold to protect itself from starvation, albeit at the cost of increased collisions. Conversely, lowering the ED threshold of the gNB would unnecessarily prevent concurrent gNB transmissions, such as during UE handovers, or needlessly defer transmissions because of noise. These naive solutions are inferior to ICC because it can mitigate the starvation attack, and improve fairness, without causing any collisions or violating latency requirements.

A possible solution might involve using preamble detection schemes for protocol identification and adaptive interference avoidance, but ED threshold-based detection is simpler and effective [21]. However, a hybrid technique combining ED threshold and preamble detection could potentially mitigate the unfairness problem. In such a system, a gNB might lower its ED threshold to -79 dBm to detect weak Wi-Fi transmissions. It would then perform preamble detection and subsequently defer transmission to avoid interference if it detects a Wi-Fi signal, and revert to its default behavior otherwise. Such a system would likely address the consequences of the ED threshold differences between NR-U and Wi-Fi systems. However, it will not have the advantage of ICC, which allows NR-U and Wi-Fi to transmit concurrently for higher spectrum utilization while the hypothetical system we described here causes NR-U to defer its transmissions. Moreover, this hypothetical system would still be susceptible to our starvation attack, as Wi-Fi would still not have sufficient opportunities to transmit that are otherwise provided by our proposed scheme. Note that attempting a similar enhancement at the AP also has the drawback of creating collisions at the UE, reducing reliability in recovering gNB transmissions.

B. Problem Formulation

We first consider a general 5G NR-U system with multiple UEs, then simplify it to our system model with one UE. We assume the gNB is sending a downlink signal to K UEs over an NLOS channel represented by the CDL-C delay profile. For now, we also assume that nearby devices (e.g., APs) are not creating any interference at the UEs. The received signal vector $\mathbf{r} \in \mathbb{C}^{1\times K}$ at the K UEs is defined in the time domain as

$$\mathbf{r} = m\mathbf{w}^{\mathbf{H}}\mathbf{h} + \mathbf{n} \tag{1}$$

where m is the orthogonal frequency-division multiplexing access (OFDMA) signal containing K messages, $\mathbf{h} \in \mathbb{C}^{M\times K}$ is the channel matrix containing the coefficients[2] that the gNB has estimated via the CSI reporting procedure described in Section II-B, $\mathbf{w} \in \mathbb{C}^{M\times 1}$ is the precoding matrix chosen by the gNB to maximize the downlink SINR at the UEs, the superscript $(.)^{\mathbf{H}}$ denotes the matrix Hermitian operation, and $\mathbf{n} \in \mathbb{C}^{1\times K}$ is the additive white Gaussian noise vector.

Typically, the gNB tries to maximize SINR at UEs while constrained by quality-of-service (QoS) criteria (e.g., data rate). This criterion can be modeled as $\mathbf{w}^{\mathbf{H}}\mathbf{h} = \mathbf{e}$, where $\mathbf{e} \in \mathbb{C}^{1\times K}, 0 < |e_i| < 1, i = 1, \ldots, K$ is the vector containing values associated with QoS of each of the K UEs. Without loss of generality, we assume $\mathbf{e} = \mathbf{1}_{K\times 1}$, i.e., the QoS is the same for all UEs.

Now we add one AP to the system and create an adjusted channel matrix $\mathbf{h}_a \in \mathbb{C}^{M\times(K+1)}$ such that $\mathbf{h}_a = [\mathbf{h}\ \mathbf{h}_{gW}]$, where the vector $\mathbf{h}_{gW} \in \mathbb{C}^{M\times 1}$ contains the coefficients of the channel between the gNB and the AP. At this point, we assume that the attacker may actively perform its starvation attack on the AP. However, the attack would not foil the design of ICC. This is because the starvation attack succeeds mainly when the AP could be repeatedly forced into a backoff state, but our solution will prevent that. For our ICC scheme to work, the downlink signal needs to be nullified at the AP. Hence, we want to achieve $\mathbf{w}^{\mathbf{H}}\mathbf{h}_a = \mathbf{e}_a$, where $\mathbf{e}_a = [\mathbf{e}\ 0]$ is the adjusted QoS criterion vector. Given the null space $null(\mathbf{h}_{gW})$ of the channel between the gNB and AP, then $\forall \mathbf{w} \in null(\mathbf{h}_{gW}), \mathbf{w}^{\mathbf{H}}\mathbf{h}_{gW} = 0$. This means the precoding matrix $\mathbf{w}$ can nullify the downlink signal at the AP. The challenge is to find a way to influence the gNB into choosing a precoding matrix $\mathbf{w}$ that belongs to the null space of $\mathbf{h}_{gW}$.

Without loss of generality, we simplify this NR-U system and assume $K = 1$, as shown in Fig. 5. Let us rewrite the received signal at this UE considering the interference coming from the AP as

$$r = m\mathbf{w}^{\mathbf{H}}\mathbf{h}_{gU} + ih_{WU} + n \tag{2}$$

where $\mathbf{h}_{gU} \in \mathbb{C}^{M\times 1}$ contains the channel between the gNB and that single UE, h_{WU} represents the channel between the AP and the UE, while i is the interference from the AP. The SINR, denoted by γ, as a function of $\mathbf{w}$ is defined as,

$$\gamma(\mathbf{w}) = \frac{\mathbb{E}\{|m\mathbf{w}^{\mathbf{H}}\mathbf{h}_{gU}|^2\}}{\mathbb{E}\{|ih_{WU} + n|^2\}} \tag{3}$$

$$\Rightarrow \gamma(\mathbf{w}) = \frac{\rho_S}{\rho_{RI}}|\mathbf{w}^{\mathbf{H}}\mathbf{h}_{gU}|^2 \leq \frac{\rho_S}{\rho_{RI}}\|\mathbf{w}\|^2\|\mathbf{h}_{gU}\|^2 \tag{4}$$

where ρ_S and ρ_{RI} denote the power of the downlink signal, and interference plus noise, respectively. To maximize $\gamma(\mathbf{w})$, the Cauchy-Schwartz inequality in (4) would be an equality if and only if $\mathbf{w} = \mathbf{w}_{opt} = c\,\mathbf{h}_{gU}$, where c is any scalar.

We now apply a constraint on $\mathbf{w}$ such that it causes minimal interference on the AP. Let $\mathbf{w}_c = \mathbf{Q}\mathbf{y}$ represent this constraint, where $\mathbf{Q} \in \mathbb{C}^{M\times M-1}$ is the orthonormal basis for the null space of $\mathbf{h}_{gW}$, and $y \in \mathbb{C}^{M\times 1}$ is any vector. Thus, the constrained optimized precoding matrix, $\mathbf{w}_{copt}$, is defined as

$$\mathbf{w}_{copt} = \underset{\mathbf{w}_c=\mathbf{Q}\mathbf{y}}{\arg\max}\,\gamma(\mathbf{w}_c) = \underset{\mathbf{w}_c=\mathbf{Q}\mathbf{y}}{\arg\max}\,|\mathbf{w}_c^{\mathbf{H}}\mathbf{h}_{gU}|^2. \tag{5}$$

By rewriting the problem above in terms of $\mathbf{y}$ to find $\mathbf{y}_{copt}$ that solves for a constrained optimal precoding matrix $\mathbf{w}_{copt}$, we obtain the following problem formulation and solution:

$$\mathbf{y}_{copt} = \underset{y\in\mathbb{C}^M}{\arg\max}\,|\mathbf{y}^{\mathbf{H}}\mathbf{Q}^{\mathbf{H}}\mathbf{h}_{gU}|^2 = c\,\mathbf{Q}^{\mathbf{H}}\mathbf{h}_{gU} \tag{6}$$

$$\Rightarrow \mathbf{w}_{copt} = \mathbf{Q}\mathbf{y}_{copt} = c\,\mathbf{Q}\mathbf{Q}^{\mathbf{H}}\mathbf{h}_{gU}. \tag{7}$$

The precoding matrix $\mathbf{w}_{copt}$ can maximize the downlink SINR at the UE while nullifying interference at the AP.

[2] $\mathbb{C}^{a\times b}$ denotes the set of all complex-valued matrices of size $a \times b$.

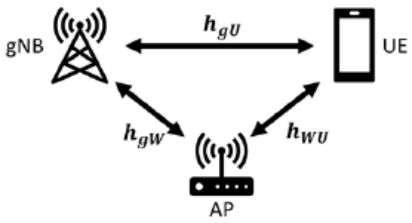


Fig. 5. Simplified channel model of a 5G NR-U and Wi-Fi coexistence system with one gNB, one UE, and one AP.

However, the gNB will not choose $\mathbf{w}_{copt}$ on its own since it is not concerned with the performance of the AP. Hence, the AP will need to influence the gNB into choosing $\mathbf{w}_{copt}$.

C. Influencing the CSI Reporting Procedure

In a nutshell, our idea is that the AP carefully overshadows (superposes a signal on) the CSI-RS signals sent by the gNB to influence it into choosing a desirable precoding matrix that nullifies the NR-U downlink signal at the AP. It must also influence the gNB into reducing its transmission rate to allow the AP, which no longer detects the gNB transmissions, to transmit concurrently with the gNB (see Section IV-F). This process is illustrated in Fig. 6, which consists of two phases.

1) Phase 1: The AP will start by estimating the channels $\mathbf{h}_{gU}, \mathbf{h}_{gW}$, and h_{WU}. Let us again consider the simplified channel model in Fig. 5. In the CSI reporting procedure, the symbols used in channel estimation are present at known locations within *unencrypted* CSI-RS and SRS reference signals. The AP uses those reference signals to estimate the channels $\mathbf{h}_{gW}$ and h_{WU}. When the gNB sends the CSI-RS containing pilot symbols $\mathbf{b}_{CRS}$ in the downlink transmission, the AP estimates $\mathbf{h}_{gW}$ in the frequency domain as

$$\mathbf{h}_{gW} = \frac{\mathbf{r}_{gW}}{\mathbf{b}_{CRS}} \tag{8}$$

where $\mathbf{r}_{gW}$ is the CSI-RS symbols received at the AP. Here, we perform element-wise division between $\mathbf{r}_{gW}$ and $\mathbf{b}_{CRS}$. Similarly, by overhearing the SRS symbol b_{SRS} sent by the UE, the AP estimates h_{WU} using received signal r_{UW} as

$$h_{WU} = \frac{r_{UW}}{b_{SRS}}. \tag{9}$$

Finally, the channel estimate $\mathbf{h}_{gU}$ is obtained by overhearing the CSI Feedback $\mathbf{CSI}_{FEED}$ sent by the UE. By the time the first CSI reporting procedure is completed, the AP has estimated the coefficients of all the channels. Now, assuming the channels do not vary within a 10 ms frame, the AP sends a signal that overshadows the CSI-RS signal used in the *next* channel estimation procedure at the UE to influence the gNB to choose the desired precoding matrix $\mathbf{w}_{copt}$.

2) Phase 2: Now that the AP has all the required channels, it proceeds with calculating the optimum overshadowing symbols $\mathbf{b}_{INT}$ due to which the UE would estimate an *influenced* version of $\mathbf{h}_{gU}$ once it divides the frequency-domain symbols of the received signal superposed by the CSI-RS ones. From (7) we see that this influenced channel should have the form $\mathbf{h}_{os} = \mathbf{Q}\mathbf{Q}^{\mathbf{H}}\mathbf{h}_{gU}$. Let $\mathbf{r}_{UE}$ be the superposition signal received by the UE, as defined below.

$$\mathbf{r}_{UE} = \mathbf{h}_{gU}.\mathbf{b}_{CRS} + h_{WU}.\mathbf{b}_{INT}. \tag{10}$$

We want $\mathbf{r}_{UE}$ to have the form $\mathbf{r}_{UE} = \mathbf{h}_{os}.\mathbf{b}_{CRS}$ so that $\mathbf{h}_{os}$ is estimated as the *actual* channel[3]. Thus, to influence the UE into estimating $\mathbf{h}_{os}$, the AP calculates the optimum overshadowing symbols (before adding perturbations) as

$$\mathbf{b}_{INT} = \frac{(\mathbf{Q}\mathbf{Q}^{\mathbf{H}} - \mathbf{I}_M)\mathbf{h}_{gU}.\mathbf{b}_{CRS}}{h_{WU}} \tag{11}$$

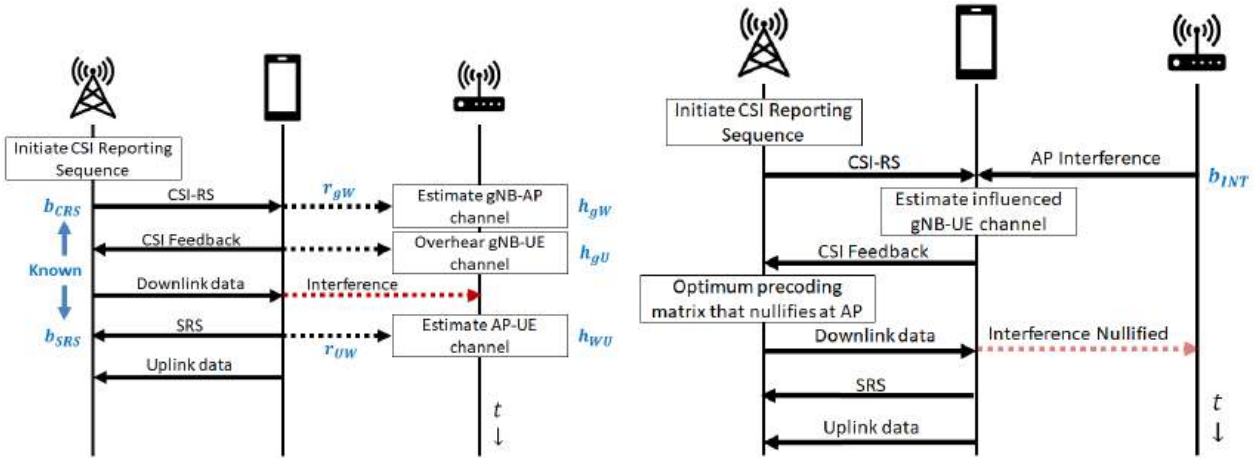
where $\mathbf{I}_M$ is the identity matrix of order M.

The AP then adds optimally calculated noise perturbations to $\mathbf{b}_{INT}$ (see Section IV-F), converts it into a time-domain signal, and transmits it such that it superposes on the CSI-RS signal of the gNB. The AP uses PSS/SSS signals (see Section III), that precede the CSI-RS, for synchronizing the transmission of $\mathbf{b}_{INT}$. As a result, the UE estimates $\mathbf{Q}\mathbf{Q}^{\mathbf{H}}\mathbf{h}_{gU}$ as the gNB-UE channel, which it then reports to the gNB in the CSI Feedback message. Subsequently, the gNB will choose the precoding matrix $\mathbf{w}_{copt}$ that not only optimizes the downlink SINR at the UE but also nullifies the signal at the AP. Hence, the AP has achieved its goal of creating a more favorable environment for coexistence by reducing the received signal strength of the gNB to much lower than -79 dBm. Now, when the AP needs to transmit a signal, it will no longer detect the medium as busy during CSMA/CA, and when it receives a signal from its clients, it will not be severely interfered by the gNB. Furthermore, the AP gets more reliable opportunities outside the idle slots to transmit and receive, which removes the attacker's ability in the starvation attack to keep interrupting the AP. However, the attacker may react to ICC and attempt to circumvent it under a white-box model. It might try to jam the 5G channel estimation reference signals at the AP to reduce the AP's effectiveness at estimating channels, or it might interfere with b_{INT} sent by the AP. In Section V-C, we show how ICC is resilient against both attempts.

D. Unique Hidden Terminal Problem

Similar to our preliminary work [7], the design above without adding noise perturbations to $\mathbf{b}_{INT}$ would work only under a weak assumption that the concurrent transmissions of the gNB and AP will not exceed their respective channel capacity. This creates an unintended consequence of ICC which was later discovered when performing experiments in our testbed (see Section VI) where both the gNB and the AP choose transmission rates as if the other one is idle and the channel capacity of the UE is reduced. In fact, in Section V-B, we see that the received signal strength of the gNB signal at the AP is below -79 dBm when ICC is active, which is now lower than the Wi-Fi ED threshold. As a result, the gNB is now hidden from the AP and it inadvertently interferes with ongoing gNB transmissions. This causes the gNB transmissions with high data rates to fail due to irrecoverable collisions with the AP's transmissions. We propose to further influence the gNB to adjust its transmission

[3](.) represents element-wise multiplication



(a) Phase 1: Estimating channels $\mathbf{h}_{gU}, \mathbf{h}_{gW}$, and h_{WU}.

(b) Phase 2: Calculating $\mathbf{b}_{INT}$ and superposing it on the CSI-RS.

Fig. 6. Illustration of our Implicit Channel Coordination approach for fair coexistence of 5G NR-U and Wi-Fi. In Phase 1, the AP overhears the CSI reports to estimate channel parameters between the gNB, UE, and AP. In Phase 2, the AP overshadows the gNB downlink signal in the subsequent iterations of CSI reporting to influence CSI estimation at the UE.

rate to account for the reduced channel capacity at the UE and mitigate the hidden terminal problem.

E. Influencing gNB Transmission Rate

In our experiments, we observed that when the AP is transmitting after ICC is active, it reduces the SINR at the UE. We argue that one way to account for AP transmission interference is to distort the CSI estimation at the gNB so that it estimates a lower CQI and proactively reduces its modulation coding scheme (MCS). Although this reduces the data rate for the 5G NR-U network, we prove in Section VI that this technique achieves a higher total system data rate and is more fair towards Wi-Fi networks. The AP can do this by transmitting the b_{INT} signal at the same transmit power as normal data transmission. This is because although the b_{INT} signal that AP overshadows on CSI-RS only contains symbols at specific locations (coinciding with CSI-RS), it still occupies the same bandwidth as the gNB downlink transmission and will reduce the SINR at the UE. However, there is one drawback to this approach - if we inject some noise onto b_{INT}, then it will also reduce the quality of nullification at AP (Section V-B). We note here that noise creates a desired effect, reducing the transmission rate of the gNB, and an undesired effect, a reduction in the quality of nullification. If the nullification is reduced but enough to force the gNB to reduce the transmission rate, then ICC achieves its goal.

Since we have room for error in channel estimation and beamforming, we can add noise to proactively reduce the transmission rate of gNB so that its downlink transmission to the UE is always successful. In our enhanced ICC design, the AP initially adds noise to b_{INT} conservatively. In subsequent phases of ICC, the AP checks the reported CQI in the CSI Feedback message if it is enough to account for the interference due to AP transmission. At the same time, the AP checks if the nullification is at most $-10\,$dB residual signal power which we determined to be the threshold of nullification that is needed for AP to ensure that RSSI of gNB downlink signal at the AP is below $-79\,$dBm (see Section V-B). The AP then keeps adding noise to b_{INT} over subsequent phases of ICC until the gNB reaches the optimum transmission rate, while under the constraint of meeting the threshold of nullification. In Section VI, we show how these enhancements limit the negative effects on the data rate of 5G while allowing the 5G and Wi-Fi coexistence system to achieve an overall higher total system data rate, even in the presence of a starvation attack.

F. Determining Optimum Noise

Let μ_{opt} be the optimum additive white Gaussian noise that needs to be added to $\mathbf{b}_{INT}$ to influence the gNB to reduce its transmission rate. Hence, the expression for the optimum overshadowing symbols now becomes,

$$\mathbf{b}_{opt} = \mathbf{b}_{INT} + \mu_{opt} \tag{12}$$

We need to ensure that μ_{opt} satisfies two conditions: 1) UE can recover gNB data transmission even under interference from AP data transmissions; 2) gNB nullification at AP is at least $-10\,$dB. For this, we derive an expression for μ_{opt} such that the aforementioned constraints are satisfied

For the first constraint, we need to ensure that the UE can recover gNB data transmissions. Typically, the gNB will adjust its transmission rate based on the channel quality index (CQI) that is reported by the UE in the CSI Feedback message. Hence, if we reduce the perceived CQI at the gNB, it will proactively reduce its transmission rate so that the UE can recover the gNB downlink data transmission. We use the expression for channel capacity to represent CQI. For optimal fairness, we argue that both AP and gNB should use half of the available channel capacity, i.e., the perceived CQI (or channel capacity) at the gNB should be halved. We assume that when not using $\mathbf{b}_{opt}$, the SNR at the UE is γ_1 which is reported in the CSI Feedback message and overheard by the AP during Phase 1 of ICC. Let the channel capacity for γ_1 be C_1. During

Phase 2 of ICC, we use noisy $\mathbf{b}_{opt}$ such that it achieves SNR of γ_2 at the UE, given by,

$$\gamma_2 = \frac{\rho_s}{|\mu_{opt}|^2}|\mathbf{w^H h}_{gU}|^2 \tag{13}$$

where ρ_s is the gNB signal power. Since γ_2 reduces the channel capacity C_2 to not more than half of C_1, we get

$$B\log_2(1+\gamma_2) < (0.5)B\log_2(1+\gamma_1) \tag{14}$$

where B is the bandwidth of the channel. After simplifying and solving for μ_{opt}, we get the following expression for constraint $A1$,

$$A1 : |\mu_{opt}| > \frac{\rho_s}{\sqrt{1+\gamma_1}-1}|\mathbf{w^H h}_{gU}|^2 \tag{15}$$

Now, we observe that the inequality $\mathbf{w^H h}_{gU} < 0.1$ satisfies the second constraint, where $\mathbf{w} = c\,\mathbf{h}_{os} = c\,\frac{\mathbf{r}_{UE}}{\mathbf{b}_{CRS}}$. By combining (10) and (12) with this inequality and simplifying, we get the following expression for constraint $A2$,

$$A2 : |\mu_{opt}| < \left|(0.1 - \mathbf{QQ^H h}_{gU}).\frac{\mathbf{b}_{CRS}}{h_{WU}}\right| \tag{16}$$

Now that we have two constraints limiting μ_{opt}, we can form an optimization problem where we try to minimize the following,

$$\begin{aligned} \mu_{opt} &= \underset{\mu\in\mathbb{C}^{M\times 1}}{\arg\min}\,\|\mu\|^2 \\ &s.t. A1, A2. \end{aligned} \tag{17}$$

For brevity, we define α and β as shown below,

$$\begin{aligned} \alpha &= (\mathbf{QQ^H h}_{gU} - 0.1).\frac{\mathbf{b}_{CRS}}{h_{WU}} \\ \beta &= \frac{\rho_s}{\sqrt{1+\gamma_1}-1}|\mathbf{w^H h}_{gU}|^2. \end{aligned} \tag{18}$$

Using Lagrange multipliers method, we solve the optimization problem in (17) to yield the following combined expression for the optimum noise μ_{opt},

$$\mu_{opt} = -\frac{\beta(1 \pm \sqrt{1-\|\alpha\|^2})}{\|\alpha\|^2 + \beta(1 \pm \sqrt{1-\|\alpha\|^2})}\alpha \tag{19}$$

Time and Space Complexity Analysis: The algorithm for our ICC procedure is listed in **Algorithm 1**. When calculating the matrix α, multiplication operations are completed in $\mathcal{O}(M^2)$ time, while addition operations take $\mathcal{O}(M)$ time. Similarly, matrix β only takes $\mathcal{O}(M)$ time to complete its multiplication operations. When calculating the optimum noise symbols μ_{opt} in (19), multiplication and addition operations are completed in $\mathcal{O}(M^2)$ and $\mathcal{O}(M)$ time respectively. When performing these operations using MATLAB on a laptop with processing capabilities comparable to an AP (which has a quad-core processor [26]), it takes, on average, 0.05 ms to complete, which is significantly less than the 5G radio frame length of 10 ms [5]. This shows that our enhanced ICC technique with optimum noise estimation can be completed before one sequence of channel estimation messages, making it feasible in highly delay-sensitive applications of NR-U. Finally, all the parameters used in (19) take $\mathcal{O}(M)$ locations to store in memory, which makes our technique feasible on hardware that is used in most commercial APs, such as the Asus RT-AX88U wireless AP that we use in our experiments which supports 256 MB flash memory and 1 GB RAM [26].

Algorithm 1 Implicit Channel Coordination Procedure

PHASE_1 $(\mathbf{r}_{gW}, r_{UW}, \mathbf{CSI}_{FEED})$
- $\mathbf{h}_{gW} \leftarrow \frac{\mathbf{r}_{gW}}{\mathbf{b}_{CRS}}$
- $h_{WU} \leftarrow \frac{r_{UW}}{b_{SRS}}$
- $\mathbf{h}_{gU} \leftarrow \mathbf{CSI}_{FEED}$
- **return** $\mathbf{h}_{gW}, h_{WU}, \mathbf{h}_{gU}$

PHASE_2 $(\mathbf{h}_{gW}, h_{WU}, \mathbf{h}_{gU})$
- Calculate μ_{opt}
- $\mathbf{b}_{opt} \leftarrow \frac{(\mathbf{QQ^H}-\mathbf{I}_M)\mathbf{h}_{gU}.\mathbf{b}_{CRS}}{h_{WU}} + \mu_{opt}$
- $RSSI_{init} \leftarrow RSSI()$
- Overshadow $\mathbf{b}_{opt}$
- $RSSI_{null} \leftarrow RSSI()$
- $nullification \leftarrow RSSI_{null} - RSSI_{init}$
- **return** $nullification$

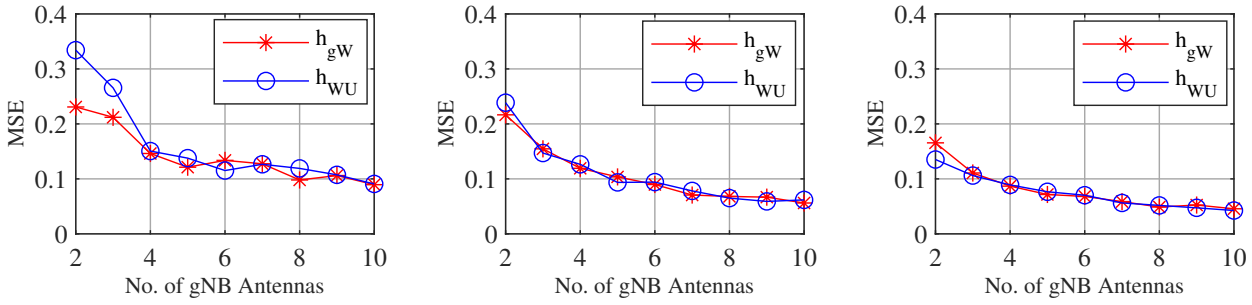
V. Theoretical Evaluation

In this section, we theoretically analyze the performance of our ICC technique. This analysis allows us to go beyond hardware experiments and their limitations in changing SNR and channel parameters as well as our limited access to software-defined radios with a large number of antennas. We first model the channel estimation mean square error (MSE) at the AP when it is using ICC, and study the effect of using multiple antennas at the gNB. We simulate ICC to verify our channel estimation MSE model, while also studying the effectiveness of ICC by measuring the nullification of the gNB downlink signal at the AP. Finally, we consider scenarios where an external attacker may use generic interference/jamming in an attempt to thwart ICC but still be unsuccessful.

Note that for ICC to be effective, the gNB must have multiple antennas that use a precoding matrix. This requirement is satisfied in most 5G NR-U deployments in urban areas [11]. We also note that an attacker cannot exploit ICC to starve APs since it cannot estimate $\mathbf{h}_{gW}$ and h_{WU}, required to obtain the same $\mathbf{b}_{INT}$, and it also cannot use ICC to starve UEs since ICC requires SINR to be maximized at the UE.

A. Channel Estimation Error

In most mobile environments, channel estimation error can occur due to the highly dynamic nature of time-varying channels and noise. In ICC, as in the 5G channel estimation procedure, we assume that the channel is not highly dynamic and does not change in the time it takes for the CSI-RS or SRS signals to reach UE or gNB respectively. This leaves noise as the only contributor to channel estimation error. The AP estimates channels $\mathbf{h}_{gW}$ and h_{WU} by leveraging the CSI-RS and SRS signals respectively as seen in (8) and (9), We can simplify these equations to obtain a generalized channel $\mathbf{h}$ from a generalized received symbols $\mathbf{r}$ divided by a generalized reference symbols $\mathbf{b}$ in the frequency domain. Now we



(a) SNR=5 dB. (b) SNR=10 dB. (c) SNR=15 dB.

Fig. 7. Theoretical and simulation results of channel estimation MSE of the $\mathbf{h}_{gW}$ and h_{WU} channels at the AP.

assume that an estimation error occurs when AP estimates an inaccurate channel $\hat{\mathbf{h}}$ due to noisy received symbols $\hat{\mathbf{r}}$.

$$\hat{\mathbf{h}} = \frac{\hat{\mathbf{r}}}{\mathbf{b}}. \tag{20}$$

Hence, the channel estimation MSE can be modeled as,

$$MSE\colon \mathbb{E}\{|\hat{\mathbf{h}} - \mathbf{h}|^2\} = \mathbb{E}\left\{\left|\frac{\hat{\mathbf{r}}}{\mathbf{b}} - \frac{\mathbf{r}}{\mathbf{b}}\right|^2\right\} \tag{21}$$

where $\mathbb{E}$ denotes the Expectation operator. We can further expand this expression to get,

$$MSE\colon = \mathbb{E}\left\{\frac{\hat{\mathbf{r}}^{\mathbf{H}}\hat{\mathbf{r}} - \hat{\mathbf{r}}^{\mathbf{H}}\mathbf{r} - \mathbf{r}^{\mathbf{H}}\hat{\mathbf{r}} + \mathbf{r}^{\mathbf{H}}\mathbf{r}}{\|b\|_2^2}\right\} \tag{22}$$

$$= \frac{\mathbb{E}\{\hat{\mathbf{r}}^{\mathbf{H}}\hat{\mathbf{r}} - \hat{\mathbf{r}}^{\mathbf{H}}\mathbf{r} - \mathbf{r}^{\mathbf{H}}\hat{\mathbf{r}} + \mathbf{r}^{\mathbf{H}}\mathbf{r}\}}{\mathbb{E}\{\|b\|_2^2\}} \tag{23}$$

where we can split the Expectation operator since the distributions of the numerator and denominator are independent. Note that $\|.\|_2$ denotes the Frobenius norm operation. We make the following observations to simplify this expression.

$$\mathbb{E}\{\hat{\mathbf{r}}^{\mathbf{H}}\hat{\mathbf{r}}\} = \mathbb{R} + \mathbb{I}_M\sigma^2 \tag{24}$$

$$\mathbb{E}\{\mathbf{r}^{\mathbf{H}}\mathbf{r}\} = \mathbb{R} \tag{25}$$

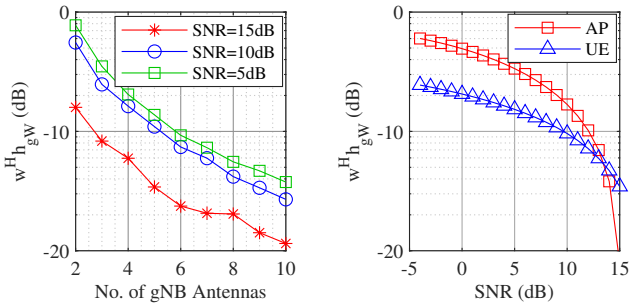
$$\mathbb{E}\{\hat{\mathbf{r}}^{\mathbf{H}}\mathbf{r}\} = \mathbb{E}\{\mathbf{r}^{\mathbf{H}}\hat{\mathbf{r}}\} = 0 \tag{26}$$

$$\mathbb{E}\{\|b\|_2^2\} = M.\rho \tag{27}$$

where $\mathbb{R}$ denotes the auto-correlation matrix of the received noisy signal, M is the number of gNB antennas, $\mathbb{I}_M$ denotes the identity matrix of order M, σ^2 is the noise variance, and ρ is the energy density of the reference symbols. Thus, the expression for MSE becomes,

$$MSE\colon \mathbf{e} = \frac{2\mathbb{R} + \mathbb{I}\sigma^2}{M.\rho}. \tag{28}$$

We model the auto-correlation matrix $\mathbb{R}$ such that it represents the channel impairments introduced in the received signal as a result of passing through the TDL-C propagation channel. The result $\mathbf{e}$ of this expression is a diagonal matrix where the value of each element $\mathbf{e}_{ij}\ \forall\ i,j \in \{1,\ldots,M\}, i = j$ is the channel estimation MSE when gNB is using i or j antennas. In Section V-B we see how using more antennas at the gNB helps reduce channel estimation MSE.



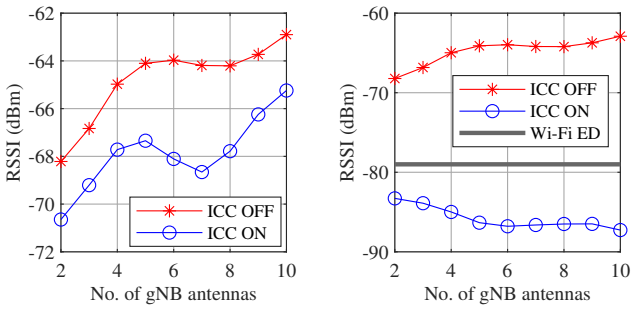
(a) Varying gNB antennas and SNR. (b) Varying SNR at the AP and UE.

Fig. 8. Residual power of the gNB downlink signal at the AP.

B. Simulation Results

1) Channel Estimation MSE: We now discuss how the AP's channel estimation MSE varies with an increasing number of gNB antennas from 2 to 10. We model the auto-correlation matrix $\mathbb{R}$ based on the TDL-C channel model and set the SNR at 5, 10, and 15 dB. We run simulations for $n = 5000$ iterations and then take an average of channel estimation MSE over all iterations. We maintain the same number of iterations for all the simulations discussed in this section. In Fig. 7, we plot the channel estimation MSE of $\mathbf{h}_{gW}$ and h_{WU} when evaluated at the AP, while comparing it to our theoretical model. First of all, we can see that our theoretical and simulation results are quite close to each other. Additionally, we observe that the channel estimation MSE tends to decrease as we increase SNR and the number of antennas. This indicates that the AP estimates a more accurate channel when used with most commercial gNBs that have $M = 10$ or more antennas [6].

2) Quality of Nullification: Now we see how the channel estimation MSE translates to ICC's effectiveness at nullifying gNB downlink signal at the AP. Recall that in (7), we derive the solution to the optimum precoding matrix that the gNB needs to maximize SNR at the UE while also minimizing interference at the AP. As seen in Section IV-B, as long as the optimum precoding matrix is a part of the null space of $\mathbf{h}_{gW}$, i.e., $\mathbf{w}_{copt} \in null(\mathbf{h}_{gW})$, then the gNB downlink signal is nullified at the AP and $\mathbf{w}^{\mathbf{H}}\mathbf{h}_{gW} = 0$. We independently change the noise at both the UE and the AP when estimating $\mathbf{h}_{gU}$ and h_{WU} respectively and see how it affects the quality



(a) At the UE. (b) At the AP.

Fig. 9. RSSI of gNB downlink signal with SNR=15 dB.

of nullification at the AP. Here we want to test the robustness of ICC in the presence of imperfect channel estimation. The amount of nullification is measured by tracking the percentage of residual signal power of the gNB's downlink transmission at the AP. The lower the residual signal power, the better the nullification. In Fig. 8(a), we plot the value of $\mathbf{w^H h}_{gW}$ on the *y-axis*, which represents the residual signal power of the gNB, against increasing number of gNB antennas and noise. We observe that the magnitude of $\mathbf{w^H h}_{gW}$ is less than 0.1 or -10 dB for SNR > 10 dB or when gNB is using 6 or more antennas. Also, in Fig. 8(b), we can see how noise at the AP and the UE can affect the quality of nullification at the AP. We assume the gNB has 4 antennas in this case. We observe that the nullification is more sensitive to noise at the AP. This is because the AP needs to estimate two channels $\mathbf{h}_{gW}$ and h_{WU} which are crucial in deriving the optimum b_{INT} signal and the presence of noise can create estimation errors in these channels. Again, the gNB residual signal power at the AP is under -10 dB for SNR > 10 dB, which is consistent with our results in Fig. 8(a). This shows that ICC is effective in most realistic cases of NR-U deployments.

3) RSSI of gNB: To further evaluate ICC's effectiveness, we measure the RSSI of gNB downlink signals at the AP. If the RSSI of the downlink signals is lower than the AP's ED threshold when ICC is active, then ICC is accomplishing its goal of limiting gNB interference. At the same time, we measure RSSI at the UE to see how much the UE is affected. ICC should not be disrupting the downlink signal so much that the UE is unable to recover it. As seen in Fig. 9, we have measured the RSSI at the AP and the UE both when ICC is ON and OFF. For this, we set the SNR at a constant 15 dB. It is observed that the gNB downlink signal gets nullified at the AP enough for the RSSI to go below -79 dBm. At the same time, the loss in RSSI is about 2–5 dB at the UE, meaning the UE is not affected too much.

C. Generic Interference from Attacker

The AP's capability to influence gNB relies on its ability to estimate the channels between gNB, UE, and AP. To do this, the AP overhears unencrypted CSI-RS and SRS reference signals sent in the CSI Reporting procedure. Since this procedure is unencrypted, an attacker smartly jams the CSI-RS and SRS signals received by the AP. The attacker only needs to jam the known locations where pilot symbols are sent, which can be determined from known 3GPP specifications. Due to jamming, the AP detects incorrect pilot symbols and subsequently estimates incorrect channel parameters, reducing the AP's effectiveness at influencing gNB. The AP cannot detect this jamming attempt by the attacker due to the random nature of the channels between the AP and gNB.

In another scenario, the attacker may interfere/jam the $\mathbf{b}_{INT}$ sent by the AP to UE when ICC is active. The attacker can potentially mimic the ICC approach and counter AP's signal carrying $\mathbf{b}_{INT}$ such that it negates AP's influence and circumvents ICC. This way, it may neutralize ICC's effect and make its starvation attack effective again. However, the attacker will need to estimate the same channel parameters that AP estimates. Otherwise, it will not be able to accurately mimic and negate the $\mathbf{b}_{INT}$ signal that AP uses. However, both attack approaches are not feasible against our enhanced ICC technique since it is not feasible for the attacker to estimate the same gNB-AP and AP-UE channels that the AP estimates unless the attacker is within half the wavelength of the 6 GHz frequency bands (≈ 25 mm) of the AP, at which point the attacker becomes very easy to detect and mitigate.

TABLE III
LIST OF IMPORTANT EXPERIMENTAL PARAMETERS.

Parameter	Value	Parameter	Value
No. of gNB antennas	2	gNB ED threshold	-59 dBm
gNB transmit power	12 dBm	AP ED threshold	-79 dBm
AP transmit power	5 dBm	gNB-UE distance	5 m
Center frequency	5.935 GHz	gNB-AP distance	5 m
Channel Bandwidth	20 MHz	AP-UE distance	1 m

VI. Experimental Evaluation

In this section, we discuss the performance of both our Wi-Fi Starvation attack and our ICC approach using real devices. First, we evaluate the performance of our attack with the help of experiments conducted on a 5G NR-U and Wi-Fi coexistence testbed deployed using USRPs. We then show the performance and effectiveness of ICC.

Our experimental setup is shown in Fig. 12. The NR-U network is deployed using srsRAN (based on srsLTE [27]), an open-source 5G software radio suite, on two separate laptops running an instance of gNB and UE, respectively, each connected to a USRP B210. The two NR-U B210s are separated by a wooden board to create an NLOS scenario. The Wi-Fi network consists of an Asus RT-AX88U 802.11ax capable commercial AP [26] with one of the laptops connected as a client. Later, we swap the ASUS AP with another B210 to run our ICC implementation via MATLAB. A third laptop running MATLAB is used to run an attacker on a USRP B210. All USRPs and AP are operating on the 5.935 GHz center frequency. The gNB uses two 2 dBi dipole antennas, at a transmit power of 12 dBm, while the UE uses one antenna.

In Fig. 10, we compare fairness in the context of airtime occupied by NR-U and Wi-Fi devices by measuring the average amount of time gNB, AP, and attacker nodes occupy the spectrum under different scenarios – (S1) attack and ICC

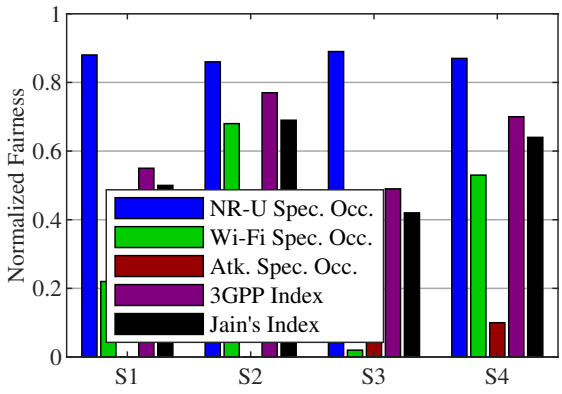
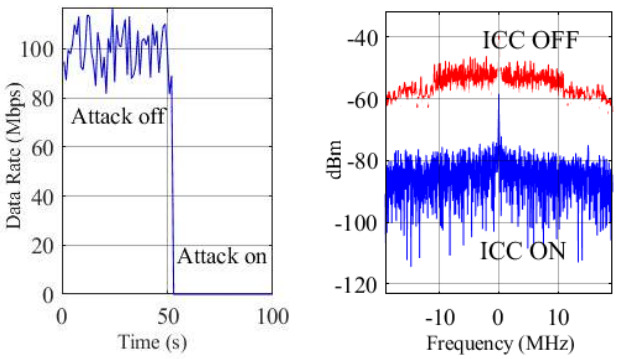


Fig. 10. Airtime fairness under ICC.



(a) Wi-Fi starvation attack. (b) Spectrum of gNB signal at AP.

Fig. 11. Performance evaluation of Wi-Fi starvation attack and ICC.

inactive; (S2) attack inactive, ICC active; (S3) attack active and ICC inactive; (S4) attack and ICC active. We also evaluate the sharing fairness using two additional metrics: (1) a metric described in 3GPP specifications [28] where the performance degradation of our coexistence scenario is compared with the degradation observed when two Wi-Fi networks operate together; (2) Jain's fairness index [29]. These two metrics provide a simple way to determine how equitably airtime is split between NR-U and Wi-Fi systems using values ranging from 0 to 1, with 1 indicating perfect fairness. For spectrum occupancy, we separately measure the amount of time the gNB, AP, and attacker occupy the spectrum, but for the remaining two fairness metrics we measure the airtime of each successful transmission only for the gNB and AP, but not the attacker. We observe that when the attack and ICC are inactive, NR-U occupies the shared medium nearly four times longer than Wi-Fi. This is because when ICC is inactive, AP data transmissions keep colliding with gNB downlink transmissions causing the AP to repeatedly enter backoff state. But after activating ICC, the Wi-Fi spectrum occupancy has increased nearly $3\times$. With just the attack active and ICC inactive, Wi-Fi spectrum usage reduces to nearly zero, indicating that the starvation attack is highly effective only in the absence of ICC. But when we also activate ICC, we see that Wi-Fi is now able to achieve more than 50% spectrum occupancy even in the presence of an active starvation attack. We also observe that, even though gNB transmission durations are usually longer than the AP, the concurrency of transmissions facilitated by ICC allows the AP to obtain the shared spectrum more frequently. This shows that our enhanced ICC technique improves access fairness, accounting for airtime differences, while being resilient against denial-of-service attacks such as our starvation attack on Wi-Fi.

In Fig. 11(a), we see the effect of our starvation attack on the AP by measuring its data rate. We run a speed-test application on the Wi-Fi client for a duration of 100 seconds. In this case, the attack was started at timestamp $t = 54\,\text{s}$, after which the data rate was completely reduced to zero. As a result, the Wi-Fi network is suffering from a complete denial of service. In Fig. 11(b), we plot the spectrum of the gNB downlink signal at the AP both when ICC is ON and OFF. It can be observed that ICC can nullify the gNB downlink signal to the point where it becomes indistinguishable from noise. This allows the AP to access the medium more freely as it is no longer being forced to repeatedly enter back-off state because of the aggressive channel access mechanism of gNB.

In Fig. 13, we measure the average data rate, with rate adaptation, of NR-U and Wi-Fi coexistence system over different SNR values while both NR-U and Wi-Fi devices may transmit at the same time and with our starvation attack active. Note that we manually increase the received SINR by decreasing the noise variance at the receivers. Consequently, the data rate of Wi-Fi devices increases with increasing modulation coding schemes (MCS), which in turn increases adaptively when received SINR increases. The data rate of 5G is related to the channel quality index (CQI) observed by the UE, which is also directly related to the received SINR. We measured the total data rate of AP and UE both when ICC is OFF and ON. We observe that Wi-Fi cannot transmit at all when ICC is OFF, so its data rate is zero across all levels of SNR. This is because we kept the starvation attack active during these experiments. At the same time, UE achieves $12 - 54\,\text{Mbps}$, which is also the total data rate of the system. Now when we activate ICC, the UE data rate remains the same for the same SNR, but Wi-Fi achieves $5 - 20\,\text{Mbps}$. Clearly, the total system data rate has almost doubled to $18 - 108\,\text{Mbps}$. This was the direct result of the enhancements we made to ICC (see Section IV-E and IV-F) which limit the negative effects on the data rate of UE. The fact that the total data rate of the system is higher when ICC is ON shows that ICC is achieving a net positive result. Also, Wi-Fi achieves a significantly higher data rate when ICC is active. The AP is now able to transmit more frequently and achieve its expected data rate while keeping the negative effect on the data rate of UE as low as possible and achieving an overall higher system data rate.

In Fig. 14, we compare the performance of ICC against the recent online backoff optimization scheme (OBO) proposed in [13], the only other work that attempts to achieve fair coexistence using an implicit technique. OBO determines the optimum backoff window size for Wi-Fi devices to increase their opportunities for transmitting over the channels shared with NR-U. It is observed that ICC allows Wi-Fi devices

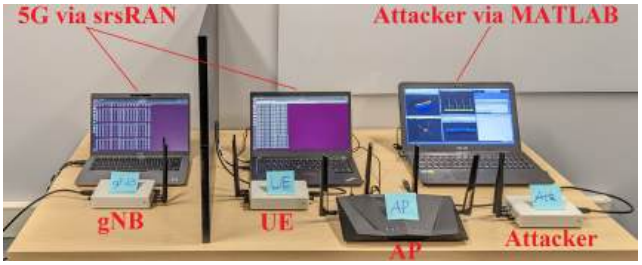


Fig. 12. Experimental setup of 5G and Wi-Fi Coexistence testbed.

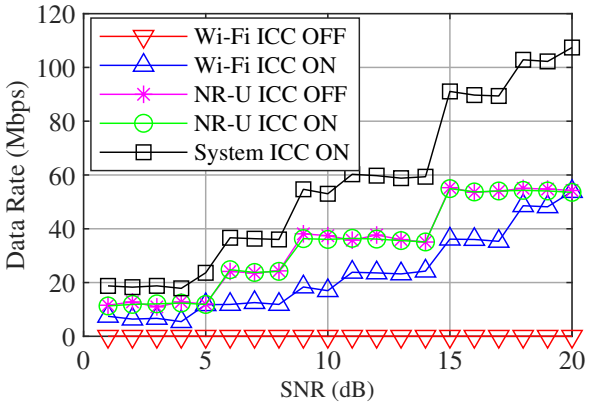


Fig. 13. Total data rate of the NR-U and Wi-Fi Coexistence System when ICC is ON and OFF, with Wi-Fi starvation attack active.

to achieve an almost 5 times higher data rate compared to OBO. This is because ICC facilitates concurrent gNB and AP transmissions. At the same time, the data rate achieved by UEs in the NR-U networks remains close to the same, as seen in Fig. 14a. Also, in Fig. 14b, we observe that the channel capacity achievable by Wi-Fi is almost $1.7\times$ higher when using ICC compared to OBO because Wi-Fi devices receive signals at a higher SINR when using ICC thanks to gNB interference nullification.

As shown in Fig. 15, we conducted experiments in a more complex indoor environment where our gNB is situated in the lobby outside our RF-shielded lab, while our UE and AP are located inside the lab. Since we are using USRP B210 which has a low transmit power of only 10 dBm at 5.935 GHz [30], our experiments are limited in the maximum distance between the nodes. Hence, we chose to use a complex indoor setup where we experiment in relatively low SNR settings to show the practicality of our ICC scheme, while also ensuring that our testbed remains within operational range. Additionally, since we are limited to using 2×1 MISO on the B210s acting as the gNB and UE, we are able to test with only a 2-antenna gNB. We use this new setup to experimentally verify the theoretical analysis of our enhanced ICC design presented in Section V. In Fig. 16a, we can see the channel estimation MSE at the AP when it is estimating the $\mathbf{h}_{gW}$ and h_{WU} channels. Overall, the channel estimation error is less than 0.5, which aligns with our theoretical analysis. In Fig. 16b, we vary the SNR at the AP and plot the magnitude of residual gNB signal power at the AP after it has been nullified thanks to our enhanced ICC scheme. We can see that the signal power of the gNB is less than -10 dB at the AP for SNR 15 dB, meaning that ICC is achieving its intended goal.

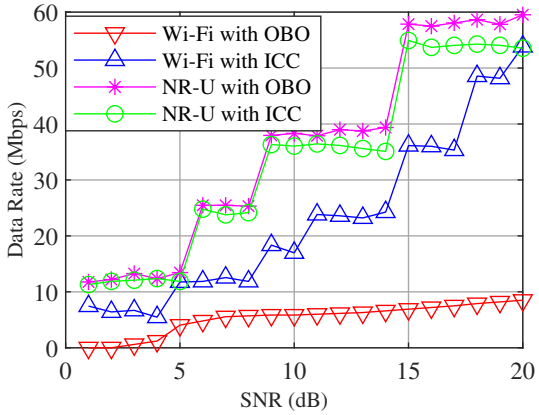
VII. Related Work

Unlicensed Technologies of 4G: LTE Licensed Assisted Access (LAA) [31] and MulteFire [32] first introduced coordination frameworks for unlicensed spectrum sharing beyond legacy Wi-Fi systems. Specifically, LAA utilizes licensed anchors on cellular channels to assist unlicensed LTE operations through techniques like Listen Before Talk to improve coexistence fairness. Building on top of LAA protocols, MulteFire takes unlicensed LTE deployment further by enabling standalone, anchor-less small cell networks to operate solely in unlicensed bands without any licensed spectrum.

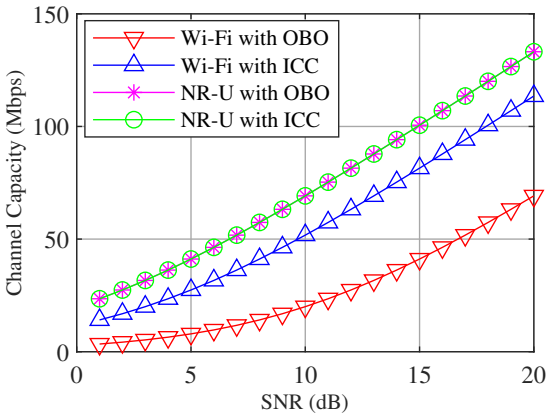
Implicit and Explicit Channel Coordination: Prior works in implicit coordination that operate mainly on the PHY layer are inadequate in improving sharing fairness. Adjusting ED thresholds is proposed in [21] deviating from typical power levels in respective systems and increasing carrier sensing inaccuracies. Optimally tuning backoff windows of NR-U and Wi-Fi is proposed in [13] but it only improves spectrum occupancy of Wi-Fi by 10%. Evading LTE interference on Wi-Fi using LTE features, like Almost Blank Subframes (ABS) is proposed in [12], but ABS is no longer used in NR-U making it impractical. Explicit coordination techniques that operate across layers (PHY, MAC, and above) are better at improving fairness but suffer from penalties due to latency. Unidirectional [8] and bidirectional [9] cross-technology communication is likely vulnerable to message spoofing attacks and, further, if these approaches are extended to NR-U, they can incur 1–2 ms delay due to the addition of coordination messages. Likewise, cooperative beamforming techniques either apply interference nulling under a line-of-sight (LOS) assumption that is not always available, especially in indoor settings [10], or use dedicated devices to facilitate coordination with added latency [11].

Deep Learning and Game Theory: Several works have used game theory and deep learning methods at the PHY layer to model and optimize coexistence problems between cellular and Wi-Fi networks in both licensed and unlicensed bands. For example, the work in [14] formulates the coexistence issue as an optimization problem to maximize total network throughput under fairness constraints to derive optimal initial backoff window sizes. Meanwhile, [15] leverages deep reinforcement learning and federated learning frameworks based on partially observable Markov decision processes to learn optimal channel access policies. The competitive interactions between networks are also modeled as non-cooperative games in [16], [17] which are used to improve fairness and overall data rates of cellular and Wi-Fi coexistence systems.

Optimization of Spectrum Resource Blocks: Some PHY layer techniques optimize spectrum resource blocks, *i.e.*, time slots or frequency bands, for cellular and Wi-Fi users to improve data rate and fairness. The work in [18] uses spatial-stream multiplexing and derives a stream selection and user replacement strategy to determine optimal spectrum allocation



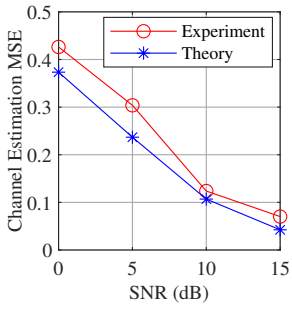
(a) Data rate.



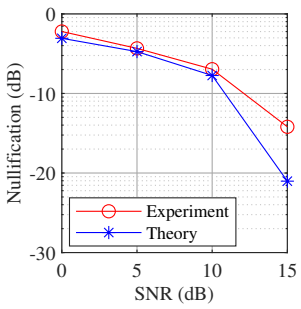
(b) Channel capacity.

Fig. 14. Performance comparison of ICC with OBO on NR-U and Wi-Fi.

Fig. 15. Complex indoor experimental setup with the AP, UE, and Attacker inside a room and the gNB outside in a hallway.



(a) Channel estimation error.



(b) Residual gNB signal power at the AP after nullification by ICC.

Fig. 16. Experimental verification of the theoretical analysis of ICC in a complex indoor environment with a 2-antenna gNB.

fractions for LAA and Wi-Fi given their traffic loads. On the other hand, [19] assigns frequency and spatial resources across licensed and unlicensed bands by maximizing cellular capacity or quality of experience under coexistence constraints and deriving an iterative channel allocation and hybrid beamforming algorithm. Finally, the work in [20] puts forth a signaling mechanism based on a clear-to-reserve message that reduces collisions and wastage of channel resources, improving throughput for both LTE and Wi-Fi in shared bands.

Other techniques have also been proposed. The work in [33] proposes a scheme to detect misbehavior in the coexistence between LTE and Wi-Fi systems using implicit sensing techniques that can accurately estimate the operational parameters of LTE transmissions and detect whether they deviate from expected values. In [34], an extensive measurement study has been conducted with commodity LTE and Wi-Fi devices to identify key coexistence challenges, one of which confirms that LTE interference causes Wi-Fi performance to degrade, harming 802.11ac high-throughput features and propose DeMiLTE to react to LTE interference which is shown to improve the throughput of Wi-Fi by 110 %. A "trap theory" to analyze temporal throughput fluctuations is proposed in [35] where analytical tools have been developed for computing the "degrees of starvation" for CSMA networks, showing that the existing remedies designed to solve equilibrium starvation may not work well as far as temporal starvation is considered.

VIII. Conclusion

In this paper, we have proposed a novel and critical technique to optimize how we influence the 5G channel estimation procedure to facilitate concurrent gNB and AP transmissions. We theoretically analyzed the robustness of our enhanced ICC design, under varying noise levels and number of gNB antennas, and proved that ICC is robust under practical considerations where the gNB has up to 10 antennas. We have developed two novel attacks that attempt to circumvent ICC and we have shown how, by design, our enhanced ICC scheme is resilient against both attacks. We have experimentally evaluated our enhanced ICC design on a 5G NR-U and Wi-Fi coexistence testbed using software-defined radios and shown that the total data rate of the coexistence system increases by 30% when ICC is enabled, even under a Wi-Fi starvation attack. For future work, we intend to further improve ICC's robustness under highly dynamic channels in mobile environments.

References

[1] E. Bastug, M. Bennis, M. Medard, and M. Debbah, "Toward interconnected virtual reality: Opportunities, challenges, and enablers," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 110–117, Jun. 2017.

[2] G. Naik and J. Park, "Coexistence of Wi-Fi 6E and 5G NR-U: Can we do better in the 6 GHz bands?" in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Vancouver, BC, Canada, May 2021, pp. 1–10.

[3] *Release 16 Description; Summary of Rel-16 Work Items*, 3GPP Technical Report 21.916, Jun. 2021.

[4] *Release 17 Description; Summary of Rel-17 Work Items*, 3GPP Technical Report 21.917, Sep. 2022.

[5] *Physical layer procedures for data*, 3GPP Technical Specification 38.214, Jul. 2020.

[6] N. Patriciello, S. Lagén, B. Bojović, and L. Giupponi, "NR-U and IEEE 802.11 technologies coexistence in unlicensed mmWave spectrum: Models and evaluation," *IEEE Access*, vol. 8, no. 1, pp. 71 254–71 271, Apr. 2020.

[7] S. Dongre and H. Rahbari, "Implicit channel coordination to tackle starvation attacks in 5G and Wi-Fi coexistence systems," in *Proc. IEEE Global Comm. Conf. (GLOBECOM)*, Rio de Janeiro, Brazil, Dec. 2022, pp. 4136–4141.

[8] P. Gawlowicz, A. Zubow, and A. Wolisz, "Enabling cross-technology communication between LTE unlicensed and WiFi," in *Proc. IEEE Int. Conf. on Comput. Commun. (INFOCOM)*, Honolulu, HI, USA, Apr. 2018, pp. 144–152.

[9] P. Gawłowicz, A. Zubow, and S. Bayhan, "Demo abstract: Cross-technology communication between LTE-U/LAA and Wi-Fi," in *Proc. IEEE Int. Conf. on Comput. Commun. Workshop (INFOCOM WKSHPS)*, Toronto, ON, Canada, Jul. 2020, pp. 1272–1273.

[10] A. Zubow, P. Gawlowicz, and S. Bayhan, "On practical coexistence gaps in space for LTE-U/Wi-Fi coexistence," in *European Wireless Conf.*, Catania, Italy, May 2018, pp. 1–8.

[11] Q. Chen, K. Yang, H. Jiang, and M. Qiu, "Joint beamforming coordination and user selection for CoMP enabled NR-U networks," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 530–14 541, Aug. 2022.

[12] C. Bocanegra, T. E. Kennouche, Z. Li, L. Favalli, M. D. Felice, and K. Chowdhury, "E-Fi: Evasive Wi-Fi measures for surviving LTE within 5GHz unlicensed band," *IEEE Trans. Mobile Comput.*, vol. 18, no. 4, pp. 830–844, Apr. 2019.

[13] F. Luo, X. Sun, Y. Gao, W. Zhan, P. Liu, and Z. Guo, "Optimal coexistence of NR-U with Wi-Fi under 3GPP fairness constraint," in *IEEE Int. Conf. Commun. (ICC)*, May 2022, pp. 4890–4895.

[14] X. Sun and L. Dai, "Towards Fair and Efficient Spectrum Sharing Between LTE and WiFi in Unlicensed Bands: Fairness-Constrained Throughput Maximization," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2713–2727, Apr. 2020.

[15] Y. Liu, H. Zhou, Y. Deng, and A. Nallanathan, "Channel Access Optimization in Unlicensed Spectrum for Downlink URLLC: Centralized and Federated DRL Approaches," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 7, pp. 2208–2222, Jul. 2023.

[16] A. K. Bairagi, S. F. Abedin, N. H. Tran, D. Niyato, and C. S. Hong, "QoE-Enabled Unlicensed Spectrum Sharing in 5G: A Game-Theoretic Approach," *IEEE Access*, vol. 6, pp. 50 538–50 554, Sep. 2018.

[17] A. K. Bairagi, N. H. Tran, W. Saad, Z. Han, and C. S. Hong, "A Game-Theoretic Approach for Fair Coexistence Between LTE-U and Wi-Fi Systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 442–455, Jan. 2019.

[18] Q. Chen and Z. Ding, "Accommodating LAA Within IEEE 802.11ax WiFi Networks for Enhanced Coexistence," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7621–7636, Nov. 2020.

[19] P. Wang, B. Di, and L. Song, "Cellular Communications Over Unlicensed mmWave Bands With Hybrid Beamforming," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 6064–6078, Aug. 2022.

[20] V. Loginov, E. Khorov, A. Lyakhov, and I. F. Akyildiz, "CR-LBT: Listen-Before-Talk With Collision Resolution for 5G NR-U Networks," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3138–3149, Sep. 2022.

[21] M. Mehrnoush, V. Sathya, S. Roy, and M. Ghosh, "Analytical modeling of Wi-Fi and LTE-LAA coexistence: Throughput and impact of energy detection threshold," *IEEE/ACM Trans. Netw.*, vol. 26, no. 4, pp. 1990–2003, Aug. 2018.

[22] V. Sathya, M. I. Rochman, and M. Ghosh, "Measurement-based coexistence studies of LAA & Wi-Fi deployments in Chicago," *IEEE Wireless Commun.*, vol. 28, no. 1, pp. 136–143, Feb. 2021.

[23] *Study on channel model for frequencies from 0.5 to 100 GHz*, 3GPP Technical Report 38.901, Nov. 2020.

[24] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)*, IEEE Standard 802.11ax, Jun. 2021.

[25] *Physical layer procedures for shared spectrum channel access*, 3GPP Technical Specification 37.213, Jun. 2020.

[26] A. C. Inc. (2019) RT-AX88U tech specs. Accessed: May 12, 2023. [Online]. Available: https://tinyurl.com/mpaf2kxf

[27] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: An open-source platform for LTE evolution and experimentation," in *Proc. ACM Int. Workshop Wireless Netw. Testbeds, Experimental Eval., and Characterization (WINTECH)*, New York City, New York, Oct. 2016, pp. 25—32.

[28] *Study on NR-based access to unlicensed spectrum*, 3GPP Technical Report 38.889, Dec. 2018.

[29] R. K. Jain, D.-M. W. Chiu, and W. R. Hawe, "A quantitative measure of fairness and discrimination," *Eastern Res. Lab., Digit. Equip. Corp*, vol. 21, pp. 1–38, Sep. 1984.

[30] M. W. O'Brien, J. S. Harris, O. Popescu, and D. C. Popescu, "An experimental study of the transmit power for a USRP software-defined radio," in *Proc. Int. Conf. Commun. (COMM)*, Jun. 2018, pp. 377–380.

[31] *Feasibility Study on Licensed-Assisted Access to Unlicensed Spectrum*, 3GPP Technical Report 36.889, Jan. 2015.

[32] MFA. (2023) Alliance for Private Networks. Accessed: Nov. 20, 2023. [Online]. Available: https://www.mfa-tech.org/

[33] I. Samy, X. Han, L. Lazos, M. Li, Y. Xiao, and M. Krunz, "Misbehavior detection in Wi-Fi/LTE coexistence over unlicensed bands," *IEEE Trans. Mobile Comput.*, vol. 22, no. 8, pp. 4773–4791, Aug. 2023.

[34] S. K. Saha, C. Vlachou, D. Koutsonikolas, and K.-H. Kim, "DeMiLTE: Detecting and mitigating LTE interference for enterprise Wi-Fi in 5GHz," in *Proc. Twentieth ACM Int. Symp. on Mobile Ad Hoc Netw. and Comput.*, Catania, Italy, 2019, pp. 31—40.

[35] C. Kai and S. C. Liew, "Temporal starvation in CSMA wireless networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1515–1529, 2015.

Siddharth Dongre (Graduate Student Member, IEEE) completed the M.S. degree in Computing Security from Rochester Institute of Technology (RIT) in 2020. He received the Bachelor of Engineering degree in Computer Engineering from Pune University, India in 2017. He is currently pursuing a Ph.D. degree in Electrical and Computer Engineering at RIT. His research interests include secure spectrum sharing in 5G, Wi-Fi, and radio astronomy services; beamforming in MIMO systems; and vehicle-to-vehicle (V2V) communications security.

Hanif Rahbari (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Arizona in 2016. He is currently an Assistant Professor with the Golisano College of Computing and Information Sciences and is affiliated with the ESL Global Cybersecurity Institute and Kate Gleason College of Engineering, Rochester Institute of Technology (RIT). In Spring 2018, he joined RIT after a brief experience as a post-doctoral associate with Virginia Tech. He is also a co-inventor on three U.S. patents. His broad research interests include wireless ecosystem security and wireless communications, with an emphasis on jamming and privacy (transmission attributes obfuscation) at the physical layer, connected vehicles security, applied cryptography in wireless systems, and spectrum sharing security. He received the NSF CAREER Award in 2023.