# Implicit Channel Coordination to Tackle Starvation Attacks in 5G and Wi-Fi Coexistence Systems

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

***Abstract*—Due to the scarcity of spectrum bands, 5G and Wi-Fi systems are embracing coexistence in the unlicensed 5 and 6 GHz bands to support high data rate demands and growing number of users. To provide fair and effective coexistence in shared frequency bands, both technologies rely on carrier sensing. However, differences in sensing thresholds creates an unfair advantage for 5G nodes who access the shared wireless medium more aggressively and degrade the data rate and latency of Wi-Fi nodes. We show in this paper that an adversary who intends to deny service to Wi-Fi can stealthily exploit this unfairness to drastically reduce the spectrum occupancy and data rate of Wi-Fi nodes. We then propose a novel implicit channel coordination (ICC) approach to mitigate the attack and improve sharing fairness. In ICC, Wi-Fi nodes influence 5G gNB into choosing a precoding matrix that nearly nullifies downlink signals at Wi-Fi nodes. We demonstrate our starvation attack on a USRP testbed and further evaluate our proposed ICC approach using simulations. We show that ICC doubles the data rate of a Wi-Fi network subject to an active attack.**

***Index Terms*—Wi-Fi, NR-U, spectrum sharing security, channel coordination, beamforming**

## I. Introduction

Emerging applications of cellular and Wi-Fi networks with increasing number of users, high data rate demands, and/or ultra-reliable low latency communication requirements have pushed the spectrum policy makers, i.e., FCC, to open additional unlicensed bands in the 5 and 6 GHz for sharing, aiming to supply additional bandwidth to meet the rising demands [1], [2]. Subsequently, 3GPP Release 16 (finalized in 2020) introduced 5G New Radio Unlicensed (5G NR-U), allowing the use of the above bands, and IEEE introduced Wi-Fi 6E to operate on unlicensed 6 GHz band in April 2020. However, this has introduced new coexistence challenges. For example, in an indoor environment, it might be easy for NR-U downlink signals to interfere with Wi-Fi 6E ones over the same band unless a coexistence mechanism is enforced.

Over the past few years, different strategies have been explored in the literature for cellular and Wi-Fi coexistence over the same band [3], highlighting challenges such as data rate degradation due to differences in carrier sensing energy detection (ED) thresholds [4], [5]. 5G NR-U currently facilitates coexistence with heterogeneous technologies by leveraging Listen-Before-Talk (LBT) mechanism, where an NR-U device senses the medium before accessing it so as to avoid collisions and interference with other networks [6]. Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism is being used in Wi-Fi for decades for similar purposes. Both schemes use ED to determine the state of the medium– idle or busy, and perform exponential backoff in the latter case. However, the default ED threshold used in NR-U is higher than the one used in Wi-Fi [7]. As a result, in Wi-Fi/NR-U coexistence scenarios, NR-U nodes access the medium more aggressively, causing Wi-Fi nodes to enter backoff state more frequently and for longer periods of time, and subsequently, creating an unfair situation where the data rate of Wi-Fi nodes degrades and its delay increases more than those of NR-U [8].

This unfair coexistence can become even more challenging in the presence of malicious actors who want to take advantage of and potentially exacerbate the consequences of such a discrepancy in ED thresholds of 5G NR-U and Wi-Fi. In this paper, we demonstrate in a hardware testbed a smart attacker that emulates a 5G node at the physical layer, sniffs on surrounding 5G and Wi-Fi transmissions and intelligently transmits during gaps in legitimate NR-U transmissions to completely starve a Wi-Fi access point (AP). By tuning the transmission power of the attacker, it repeatedly forces the AP into backoff state while not affecting the neighboring 5G nodes. This way, an attacker can carry out a *resource starvation attack* on the AP. Such attacks can have an adverse effect on current and emerging applications of Wi-Fi, especially in dense deployments with high data rate demands.

Channel coordination among coexisting 5G and Wi-Fi networks (a proactive approach) can help increase spectral awareness, subsequently mitigating unfair conditions and preventing starvation attacks. One may consider utilizing existing techniques, such as cross-technology communication (CTC), to facilitate explicit channel coordination among coexisting systems. For example, in LTE and Wi-Fi over unlicensed bands, unidirectional [9] and bidirectional [10] CTC approaches aim at establishing a direct control channel between the LTE and Wi-Fi nodes. However, even if these approaches can be extended to NR-U, they are likely vulnerable to spoofing attacks and further can incur a delay of $1-2$ ms, which is significant for delay-sensitive 5G NR-U applications where messages need to be sent within $0.5$ ms [7]. Alternatively, cross-technology interference nulling (CTIN) has been proposed in [11] which applies beamforming using a uniform linear array of antennas to nullify downlink signals from eNodeBs at the Wi-Fi nodes. However, it requires line of sight (LOS) between the eNodeB and Wi-Fi nodes, which is not always

978-1-6654-3540-6/22 © 2022 IEEE

feasible in an indoor setting. Another beamforming-based approach has been proposed in [12] that leverages coordinated multi-point (CoMP) technology to perform joint beamforming to limit interference from gNodeBs (gNB) in an NR-U system. However, it requires explicit channel coordination via a CoMP server, which, again, increases latency.

Instead of an explicit coordination scheme, we propose an *implicit* channel coordination (ICC) approach for more reliable and fair 5G NR-U and Wi-Fi coexistence that also mitigates the starvation attack we disclose in this paper. To the best of our knowledge, we are the first to address the benign and adversarial interference issues of 5G NR-U and Wi-Fi coexistence using a completely implicit technique that does not incur additional delays since it does not require explicit communication between 5G and Wi-Fi nodes. We considered simpler ways to solve the starvation problem by increasing the ED threshold of Wi-Fi, but that can lead to large number of packet collisions [13]. In ICC, the AP first overhears reference signals transmitted by 5G NR-U nodes (gNB and UE) to estimate the channel between the gNB, UE, and the AP. Next, the AP influences the channel estimation process by carefully interfering/jamming these reference signals. This results in the gNB (with multiple antennas) choosing a precoding matrix that optimizes SINR at the UE while almost nullifying the downlink signals at the AP. We show that ICC almost doubles the average throughput of the AP without affecting the latency at gNB or UE while mitigating an active starvation attack.

The rest of the paper is organized as follows. In Section II, we describe our system and channel models, 5G channel estimation techniques, and a brief overview of 5G and Wi-Fi channel access mechanisms showing how they can lead to unfair coexistence. We then experimentally demonstrate the Wi-Fi starvation attack in Section III. In Section IV, we propose our ICC-based mitigation technique to solve the unfairness problem directly. Finally, we present the experimental and simulation results for our attack and mitigation techniques respectively in Section V before concluding in Section VI.

## II. Background and System Model

In this section, we provide an overview of the 5G NR-U and Wi-Fi coexistence system and their channel models, and how 5G estimates the channels. We also briefly take a look at the channel access mechanisms of LBT and CSMA/CA and describe how their differences can lead to unfair situations.

*System Model*–We assume dense urban environments, such as office spaces in metropolitan regions, where gNBs can create interference of up to $-45$ dBm on APs due to being within $50$ m of one another [14]. Consider the simplified coexistence system illustrated in Fig. 1. It consists of a 5G NR-U network with one gNB and one user equipment (UE). The gNB has $M$ antennas while the UE has only one, creating a multiple-input-single-output (MISO) system. Multiple antennas allow the gNB to maximize its SINR at the UE. We have a Wi-Fi AP with one antenna that is present in close proximity to the UE (within a few meters). We also consider a nearby attacker

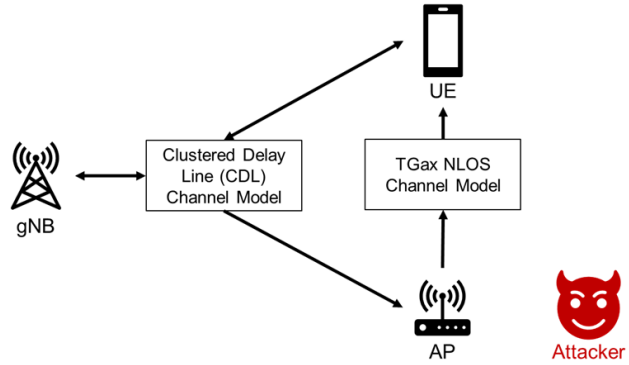


Fig. 1: Simplified 5G NR-U and Wi-Fi coexistence model with one each of gNB, UE, Wi-Fi AP, and attacker.

who performs the Wi-Fi Starvation Attack against the AP. A more detailed threat model will be discussed in Section III.

### A. Channel Models

In this system, we are mainly considering two types of channel models. For all transmissions involving the gNB, we consider the Clustered Delay Line (CDL) channel model defined in 3GPP specifications [15]. 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. Given the environment of our system, we assume the CDL-C delay profile that can represent non-LOS (NLOS) scenarios. Although the AP does not communicate with the UE, it will inevitably create interference on the UE (as described in Section IV). Hence, we model the channel for these interference signals based on the TGax indoor NLOS channel model [16].

### B. 5G Channel Estimation Procedure

Understanding the channel estimation procedure of gNB and UE is necessary to build our implicit channel coordination technique. The goal of the gNB is to maximize the SINR of its downlink signals at the UE while ensuring optimum recovery of the uplink signals sent by the UE. To achieve this goal, the gNB requires estimating the Channel State Information (CSI) between gNB and UE to determine the optimum precoding matrix that will maximize the downlink and uplink SINRs. Note that in 5G, downlink and uplink signals are sent in alternate time slots scheduled by the gNB [7].

The CSI reporting procedure is illustrated in Fig. 2. The gNB's CSI Reference Signal (CSI-RS) contains pilot symbols located in predetermined locations as specified in [7], which are used by the UE to estimate CSI parameters. These parameters include Channel Quality Index (CQI), precoding matrix indicator (PMI) and rank indicator (RI). PMI contains indices corresponding to a MIMO precoding matrix while RI indicates the number of possible transmission layers for downlink transmission. After selecting PMI and RI, the SINR is determined and mapped to a CQI value ranging from $0$ to

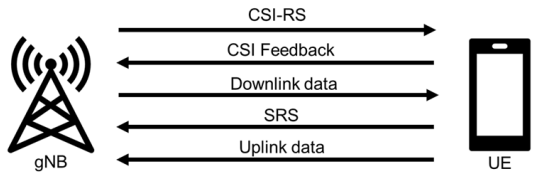


Fig. 2: 5G CSI Reporting Procedure used by gNB and UE to estimate uplink and downlink channels.

15 that indicates channel quality. After estimating these parameters, UE sends the RI, PMI and CQI values back to gNB in CSI Feedback. Accordingly, gNB calculates an optimum precoding matrix for its $M$ antennas and then transmits the downlink data to the UE. Before uplink transmission, the UE sends a Sounding Reference Signal (SRS) containing known pilot symbols similar to CSI-RS. The gNB estimates similar CSI parameters for the uplink channel based on the received SRS and then applies a precoding matrix on the received uplink data. In Section IV, we will show how this channel estimation process can be influenced by an AP to create a more fair scenario for themselves.

### C. Channel Access Mechanisms

To prevent unintended interference, both gNB and AP use channel access mechanisms LBT and CSMA/CA, respectively, to detect whether the shared medium is busy or idle based on ED threshold values. However, the UE does not use LBT as it is scheduled by the gNB to transmit during the uplink time slots only. If the medium is sensed as busy, the gNB or AP will enter a backoff state. The key difference between LBT and CSMA/CA is their ED threshold values. Wi-Fi devices tend to select the *lower* ED value of $-79\,\text{dBm}$ since most Wi-Fi devices are intended for indoor applications operate at a lower transmit power [16]. The gNB, on the other hand, operates at high transmit power to support longer transmission ranges, subsequently choosing higher ED values of $-69$ or $-59\,\text{dBm}$ [6]. In our system model, gNB sets the ED threshold to $-59\,\text{dBm}$.

### D. Unfairness Problem

Given the proximity of gNB and AP, Wi-Fi/NR-U coexistence scenarios are prone to unfairness problems [8]. Due to having a lower ED threshold, Wi-Fi devices are more sensitive to surrounding heterogeneous signals and so better at detecting NR-U signals even if their received power is less than $-59\,\text{dBm}$. In contrast, gNB sometimes incorrectly detects the medium as idle even if a Wi-Fi signal is present as long as the received signal strength is less than $-59\,\text{dBm}$ at the gNB. As a result, gNB may schedule downlink transmissions that interferes with Wi-Fi ones. Due to lack of multiple antennas for interference cancellation, the AP is likely unable to recover the Wi-Fi signals it receives in the presence of gNB interference. Therefore, the AP identifies the medium as busy and enter CSMA/CA backoff state. The gNB, however, keeps transmitting since the UE often successfully recovers the signal due to the MISO nature of the transmission from gNB. This causes the AP to enter backoff state more frequently, degrading its data rate and increasing its latency. Moreover, it hampers the APs capability to serve its Wi-Fi clients. Since Wi-Fi devices transmit at a lower power, raising their ED threshold would make it more likely not to detect Wi-Fi transmissions; leading to unintended collisions between Wi-Fi transmissions.

In effect, 5G devices occupying the shared medium more frequently, compared to Wi-Fi, leads to an unfair situation biased towards gNB and UE. Note that uplink transmissions from UE have much lower power, since most UEs are battery powered, and do not cause significant interference on the AP. Hence, we consider downlink transmissions to be the dominant cause of unfairness. In the following, we will demonstrate how this unfairness can be exploited to almost completely deny service to the APs.

## III. Wi-Fi Starvation Attack

We now describe our threat model including, the attacker's motives and assumptions. We will then describe the Wi-Fi Starvation Attack and highlight its impact on nearby APs.

### A. Threat Model

We assume the attacker emulates a gNB, without joining the NR-U network, using low-cost Software Defined Radios (SDRs) such as USRP B210 (see Section V). The attacker is located within 5-10 m of the victim AP, which is plausible in a public indoor environment, e.g., in a coffee shop. The attacker's goal is to deny the AP access to the shared medium and degrade the AP's data rate by repeatedly forcing the AP into backoff state. The attacker remains stealthy by smartly limiting the duration of its signals.

### B. Attack Procedure

Our stealthy attack is performed by only transmitting when the gNB is idle. The attacker first synchronizes with incoming NR-U transmissions using gNB's plaintext Primary and Secondary Synchronization Signals (PSS/SSS) sent in downlink slots. By performing PSS/SSS correlation, the attacker identifies the incoming signal as a 5G (NR-U) transmission and synchronizes with the gNB, so as to accurately detect the time offsets of the downlink slots in the frame. From the time slots of successive downlink transmissions, the attacker determines the transmission schedule of gNB. If no PSS/SSS signal is detected, it senses the medium by comparing the received signal strength against the $-59\,\text{dBm}$ threshold. If the signal strength is lower, then a gap in NR-U transmissions is detected and the attacker starts transmitting bogus signals immediately. To the victim AP, it appears as if the NR-U transmissions never stopped, and hence it remains in its backoff state after performing CSMA/CA. This reduces the data rate of the AP to nearly zero (see Section V).

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

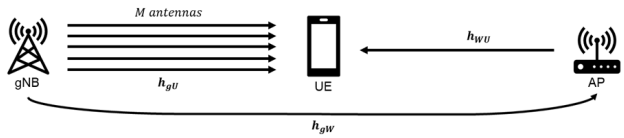


Fig. 3: Simplified channel model of a 5G NR-U and Wi-Fi Coexistence system with one gNB, UE and Wi-Fi AP.

## IV. Implicit Channel Coordination

To understand how an AP can influence gNB into choosing a desirable precoding matrix, we must first describe how gNB calculates an optimum precoding matrix to maximize the downlink and uplink SINR at the UE and gNB, respectively. We will then describe the procedure of our ICC approach.

### A. Calculating the optimum precoding matrix

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

$$\mathsf{r}(\mathsf{t}) = m(t)\mathsf{w}^{\mathsf{H}}\mathsf{h} + \mathsf{n}(\mathsf{t}) \tag{1}$$

where $m(t)$ is the downlink signal, $\mathsf{h} \in \mathbb{C}^{M\times K}$ is the channel matrix containing complex coefficients[1] that gNB has estimated via the CSI reporting procedure described in Section II-B, $\mathsf{w} \in \mathbb{C}^{M\times 1}$ is the precoding matrix chosen by gNB to maximize the downlink SINR at UE, the superscript $(.)^{\mathsf{H}}$ denotes the matrix Hermitian operation, and $\mathsf{n} \in \mathbb{C}^{1\times K}$ is the noise vector.

Typically, gNB tries to maximize SINR at UEs while constrained on meeting a Quality-of-Service (QoS) criteria (e.g., data rate). We model this criteria as $\mathsf{w}^{\mathsf{H}}\mathsf{h} = \mathsf{e}$ where $\mathsf{e} \in \mathbb{C}^{1\times K}, 0 < |e_i| < 1, i = 1, \ldots, K$ is the matrix containing values associated with QoS of each of the UEs. Without loss of generality, we assume $\mathsf{e} = \mathsf{1}_{K\times 1}$, i.e., the QoS is same for all UEs.

Now we add one AP to the system and create an adjusted channel matrix $\mathsf{h} \in \mathbb{C}^{M\times(K+1)}$ such that $\mathsf{h} = [\mathsf{h}\ \mathsf{h}_{gW}]$ by appending the column vector $\mathsf{h}_{gW} \in \mathbb{C}^{M\times 1}$ containing the coefficients of the channel between gNB and AP. For our implicit channel coordination scheme to work, the downlink signal needs to be nullified at the AP. Hence, we want to achieve $\mathsf{w}^{\mathsf{H}}\mathsf{h} = \mathsf{e}$, where $\mathsf{e} = [\mathsf{e}\ 0]$ is the adjusted QoS criterion vector. Given the null space $null(\mathsf{h}_{gW})$ of the channel between gNB and AP, then $\forall \mathsf{w} \in null(\mathsf{h}_{gW}), \mathsf{w}^{\mathsf{H}}\mathsf{h}_{gW} = 0$. This means, the precoding matrix $\mathsf{w}$ is able to nullify the downlink signal at the AP. The challenge is to find a way to influence gNB into choosing a precoding matrix $\mathsf{w}$ that belongs to the null space of $\mathsf{h}_{gW}$.

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

Without loss of generality, we simplify this NR-U system and assume $k = 1$, as shown in Fig. 3. Let the received signal at the UE be defined as

$$r(t) = m(t)\mathsf{w}^{\mathsf{H}}\mathsf{h}_{gU} + i(t)\mathsf{h}_{WU} + n(t) \tag{2}$$

where $\mathsf{h}_{gU} \in \mathbb{C}^{M\times 1}$ contains the coefficients of the channel between UE and gNB, $\mathsf{h}_{WU}$ contains channel coefficients between UE and AP, while $i(t)$ is the interference from AP. The SINR as a function of $\mathsf{w}$ is defined as,

$$SINR(\mathsf{w}) = \frac{\mathbb{E}\{|m(t)\mathsf{w}^{\mathsf{H}}\mathsf{h}_{gU}|^2\}}{\mathbb{E}\{|i(t)\mathsf{h}_{WU} + n(t)|^2\}} \tag{3}$$

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

where $\rho_S$ and $\rho_{RI}$ denote the variance of the downlink signal, and interference plus noise, respectively. The equality in equation (4) is satisfied if and only if $\mathsf{w} = c.\mathsf{h}_{gU}$, where $c$ is any scalar. Thus, the optimum precoding matrix $\mathsf{w}_{opt}$ is calculated as

$$\mathsf{w}_{opt} = \underset{\mathsf{w}\in\mathbb{C}^M}{\arg\max}\, SINR(\mathsf{w}) = c.\mathsf{h}_{gU} \tag{5}$$

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

$$\mathsf{w}_{opt} = \underset{\mathsf{w}=\mathsf{Q}\mathsf{y}}{\arg\max}\, |\mathsf{w}^{\mathsf{H}}\mathsf{h}_{gU}|^2 \tag{6}$$

We now rewrite this optimization problem in terms of $\mathsf{y}$ to find $\mathsf{y}_{opt}$ which we use to get the constrained and optimized precoding matrix $\mathsf{w}_{opt}$, as shown below.

$$\mathsf{y}_{opt} = \underset{y\in\mathbb{C}^M}{\arg\max}\, |\mathsf{y}^{\mathsf{H}}\mathsf{Q}^{\mathsf{H}}\mathsf{h}_{gU}|^2 = c.\mathsf{Q}^{\mathsf{H}}\mathsf{h}_{gU} \tag{7}$$

$$\Rightarrow \mathsf{w}_{opt} = c.\mathsf{Q}\mathsf{Q}^{\mathsf{H}}\mathsf{h}_{gU} \tag{8}$$

This $\mathsf{w}_{opt}$ precoding matrix is able to maximize downlink SINR at the UE, while minimizing interference at the AP. But gNB will not choose $\mathsf{w}_{opt}$ on its own since it is not concerned with the performance of the AP. Hence, the AP will need to influence gNB into choosing $\mathsf{w}_{opt}$.

### B. Influencing the CSI Reporting Procedure

The process of influencing the CSI reporting procedure has been illustrated in Fig. 4. In a nutshell, the AP carefully interferes with CSI-RS signals to influence gNB into choosing a desirable precoding matrix that nullifies the NR-U downlink signal at the AP. First, the AP needs to determine the optimum interference signal that can nullify the gNB downlink signal at the AP as much as possible. Let us again consider the simplified channel model illustrated in Fig. 3. The AP will need to estimate the channels $\mathsf{h}_{gU}, \mathsf{h}_{gW}$ and $\mathsf{h}_{WU}$ between the three devices.