Combat Jamming: An Innovative Mini-Slot Frequency Hopping in B5G Networks

Walaa AlQwider, Minglong Zhang, Aly Sabri Abdalla and Vuk Marojevic
Department of Electrical and Computer Engineering, Mississippi State University, MS 39762, USA
Email: {wq27, mz354, asa298, vm602}@msstate.edu

***Abstract*—This paper explores an innovative approach to enhance the resilience and security of beyond 5G (B5G) networks through the implementation of cross-bandwidth part (C-BWP) frequency hopping at mini-slot granularity. Utilizing dynamic channel estimation, the proposed system assigns resource blocks (RBs) to user equipment (UEs) of varying priorities, mitigating the impact of jamming in hostile radio environments. We introduce strategic C-BWP frequency hopping for high-priority UEs, optimizing the use of unaffected RBs. This method is shown to effectively counter various types of jamming, ensuring robust and secure communication in both current and future cellular networks. Through rigorous simulation, we demonstrate that intra-slot frequency hopping offers superior resilience by adapting quickly to dynamic channel conditions, significantly enhancing the performance and security of the communications system.**

***Index Words*—B5G networks, frequency hopping, jamming avoidance, bandwidth part, resource allocation.**

I. Introduction

Communications and various industrial sectors heavily rely on wireless technologies. Wireless technology is pivotal in unlocking new applications and enhancing the efficiency and safety of transportation and mission-critical networking, among other services. Next-generation wireless networks, encompassing beyond 5G and 6G, must accommodate escalating connectivity demands. This necessitates additional spectrum and innovative approaches to efficiently manage and utilize existing spectrum resources [1], [2]. As the spectrum becomes increasingly valuable, developing strategies for spectrum access and management is essential to overcome the challenges of operating in congested and hostile radio environments [3]. These challenges include interference, security threats, and maintaining uninterrupted connectivity under adverse conditions. Addressing these issues requires innovative spectrum access and management strategies that dynamically adapt to changing radio conditions, optimize resource allocation, and implement measures to safeguard particularly mission-critical users [4].

Unintentional and intentional interference, commonly known as jamming, is becoming a significant threat to wireless networks due to the rising availability of custom radio frequency (RF) transmission hardware and software [5], [6]. Jamming attacks compromise the integrity of communications, disrupting connectivity and services. Consequently, the importance of strengthening defenses against jamming to maintain the resilience and security of beyond 5G (B5G) networks is increasingly apparent. Effective spectrum access and management strategies are vital in this context. The literature extensively investigates various anti-jamming strategies, including frequency hopping [7] and spread spectrum [8] technologies. Modern wireless networks, which utilize multi-carrier communications, particularly orthogonal frequency division multiple access (OFDMA), require the development of efficient anti-jamming techniques that retain the advantages of OFDMA while enhancing its robustness.

Frequency hopping (FH) enables user equipment (UEs) to circumvent potential interference, noise, and other channel impairments. It involves the dynamic and rapid alteration of the carrier frequency during communication. By constantly changing the frequency at which communication occurs, the technique introduces an element of unpredictability, making it challenging for adversaries to disrupt communications. Frequency hopping increases the robustness of spectrum access against both intentional and unintentional interference [9]. It can be leveraged to ensure communications resilient against evolving jamming attacks and hostile conditions [10].

The third Generation Partnership Project (3GPP) specifications for 5G New Radio (NR) define two distinct frequency hopping methods for the Physical Uplink Shared Channel (PUSCH): inter-slot and intra-slot frequency hopping [11], [12]. Inter-slot frequency hopping allows for the dynamic allocation of resources across different time slots within a radio frame, permitting frequency changes at the beginning of each slot. Conversely, intra-slot frequency hopping offers finer granularity by enabling frequency changes within each mini-slot. A mini-slot consists of up to 7 Orthogonal Frequency Division Multiplexing (OFDM) symbols, compared to a full slot, which includes 14 OFDM symbols.

Although many research have been conducted to enhance the resilience against intentional jamming in cellular networks by taking advantage of frequency hopping, few of them can effectively handle the jamming issue in 5G or B5G networks, especially accounting for the existing 5G standard. Paper [13] modeled the outage probability for millimeter wave uplink in 5G when FH is adopted to suppress the frequency-selective fading and co-channel interference. It does not consider the intentional jamming. The work [10] attempted to utilize FH to avoid the jamming, but the proposed scheme is not applicable to 5G numerology, in which the hopping should be based on resource blocks rather than subcarriers. A frequency hopping scheme has been proposed and its impact on the positioning capabilities of the narrowband Internet of things (NB-IoT) has been evaluated [14].

A game theoretic framework is provided while considering capturing the interactions between jammer and legitimate user employing proactive frequency hopping [15]. However, the framework is only useful in 802.11 network.

In this study, we examine the effectiveness of PUSCH inter-slot and intra-slot FH in the presence of two typical jamming attacks: burst jamming and frequency-selective jamming. We introduce a cross bandwidth part (C-BWP) FH strategy, which is a measurement-driven method and considering diverse priorities among different UEs. Our study demonstrates that with the capability of fine frequency adjustments within a slot, intra-slot FH can rapidly adapt to dynamic channel conditions over shorter time intervals, thus improving the resilience and performance of the communications in 5G networks.

The rest of the paper is organized as follows: Section II dedicates to delineating 5G NR frame structure and outlines the resource allocation types for the PUSCH. Section III delves into a detailed description of C-BWP inter-slot and intra-slot frequency hopping. Numerical results and the corresponding analysis are presented in Section IV, before conclusions are drawn in Section V.

II. 5G NR Numerology and Resource Allocation

The introduction of 5G NR in 3GPP Release 15 from 3GPP featured a multi-numerology structure, characterized by the subcarrier spacing (SCS) and the transmission time interval (TTI) [16]. This innovation holds promise for addressing a diverse range of use cases, including enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (URLLC), and massive machine-type communications (mMTC) [17], as well as supporting diverse frequency bands. Geared towards providing per-user data rates exceeding 100 Mbps, eMBB enhanced legacy wireless broadband services and is in contrast to URLLC, which targets mission-critical applications of lower data rates (0.1–10 Mbps) but extremely stringent latency requirements on the order of 1 ms [18]. The variability in latency and data rate requirements between these services necessitates the adoption of different TTIs. Additionally, the concept of mini-slots further enhances the adaptability of 5G NR to diverse communication needs. Mini-slots represent smaller time intervals within a TTI and are particularly relevant for URLLC. By subdividing a TTI into multiple shorter slots, the system offers the flexibility to efficiently handle short, sporadic communication bursts. This granularity in time division allows for quicker response times and improved reliability in situations where latency is a critical factor.

A. 5G NR Frame and Carrier Structure

The duration of an NR time frame is 10 ms, which is consistent with the 4G long-term evolution (LTE) frame, and comprises 10 subframes of 1 ms each. Unlike LTE, where the subframe serves as the minimum TTI and consists of 14 OFDM symbols, NR introduces a novel approach where the OFDM symbol itself becomes the minimum time scheduling unit [19]. Commercial LTE solutions employ a single SCS of 15 kHz, whereas NR introduces a more flexible subframe structure with SCS options of 15, 30, 60, 120, and 240 kHz. The lower SCSs are used for frequency range (FR) 1, or roughly sub-7 GHz bands whereas the higher SCSs are reserved for FR2, or millimeter wave bands. Because of the fixed 1 ms subframe duration, which is independent of the SCS, the number of slots per subframe and the OFDM symbol duration vary based on the selected numerology. As the SCS doubles, the number of slots per subframe is also doubled, and the symbol duration is halved. The fixed number of OFDM symbols per slot remains at 14 for normal cyclic prefix (CP) and 12 for extended CP. Figure 1 illustrates the NR frame structure and its dependence on the chosen SCS.

As opposed to LTE, the 5G NR carrier supports wider bandwidths, extending up to 400 MHz. The fundamental frequency resource of NR is the resource element (RE), defined by a single subcarrier (SC) in the frequency domain and one OFDM symbol in the time domain [20]. It represents one modulation symbol in the OFDM resource grid. The smallest unit allocated to a user is the resource block (RB), consisting of 12 consecutive REs regardless of the selected SCS. RBs can be assigned to different users within the TTI and are dynamically reallocated across TTIs, with each RB exclusively allocated to a single user within a TTI. As the SCS increases, so does the bandwidth occupied by a single RB. Another important concept in frequency resources is the resource grid, characterized by OFDM symbols in the time domain and the full carrier bandwidth in the frequency domain. For each numerology and carrier, there exists a singular resource grid. The number of RBs in the resource grid is influenced by the numerology in use. A standalone NR carrier is constrained to 3300 active SCs, resulting in a maximum of 275 RBs per resource grid. Figure 1 visualizes the NR resources grid.

B. 5G NR BWP

5G NR subdivides the carrier bandwidth into distinct BWPs to enhance the flexibility of resource assignment and accommodate varying UE capabilities [21]. Each BWP is linked to a specific numerology and encompasses the SCS and CP configurations. Within the full carrier bandwidth, a BWP comprises a contiguous set of common resource blocks (CRBs). For each serving cell, a UE can be configured with up to four downlink BWPs and up to four uplink BWPs. However, the UE is only assumed to receive or transmit within the active downlink or uplink BWP, respectively, using the associated numerology. As outlined in the 3GPP specifications, a serving cell can have multiple configured BWPs, but only one downlink BWP and one uplink BWP are active at any given time. This dynamic activation enables efficient use of the available spectrum and adapts to the specific requirements of the communications scenario. The BWP concept allows for tailored configurations to accommodate different services or use cases, facilitating optimization of the radio resources.

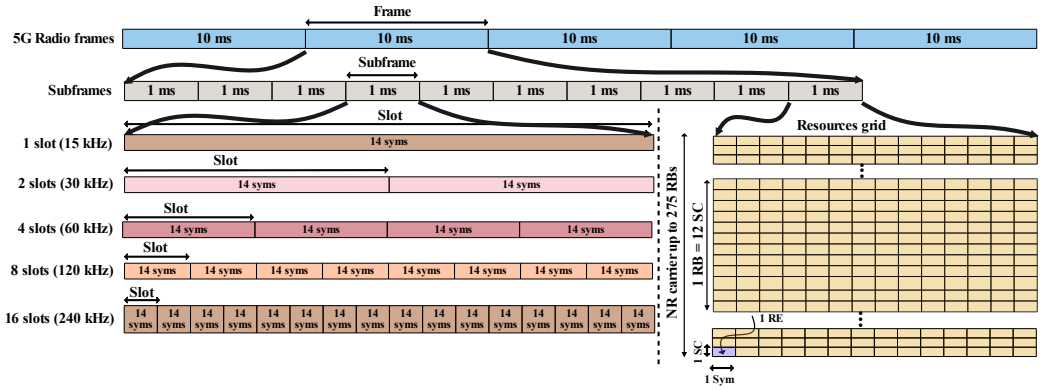


Fig. 1: Illustration of 5G NR frame and resources grid structure.

TABLE I: Size of RBG (P) in terms of RBs

BWP Size	Configuration 1	Configuration 2
1–36	2	4
37–72	4	8
73-144	8	16
145-275	16	16

C. Frequency Resources Allocation in 5G NR

The allocation of frequency resources, or RBs, to different users for uplink or downlink transmission is enabled by two frequency resource allocation schemes: Type 0 and Type 1, illustrated in Fig. 2 . Resource allocation Type 0 utilizes a bitmap, where the information indicates the resource block groups (RBGs) allocated to the user. The RBG is a set of consecutive RBs, with the number of RBs in the RBG determined by two parameters: a higher layer parameter $rbg\text{-}Size$ and the size of the BWP, as outlined in Table I. The number of RBGs N_{RBG} in a BWP of size N_{BWP}^{size} is calculated using [21]

$$N_{RBG} = \left\lceil \frac{N_{BWP}^{size} + mod(N_{BWP,i}^{start}, P)}{P} \right\rceil, \qquad (1)$$

where $N_{BWP,i}^{start}$ is the start RB of BWP_i, P is the RBG size from Table I, and the function $mod(\cdot)$ stands for modulus operation.

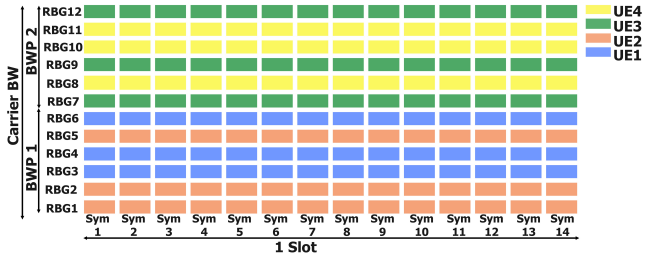
The sizes of the first and last RBGs differ from the others and are defined in [22]. The first RBG (RBG_0) is obtained as

$$RBG_0^{size} = P - mod(N_{BWP,i}^{size}, P). \qquad (2)$$

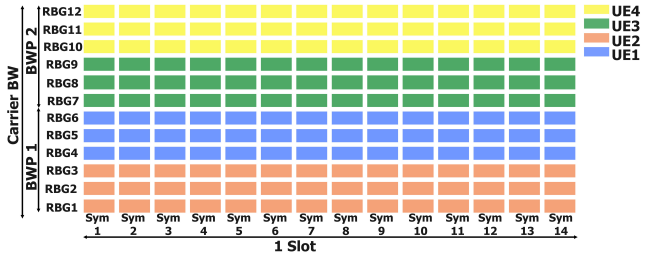
The size of the last RBG (RBG_{last}) is calculated using (3).

This RBG based allocation scheme provides flexibility, allowing resources to be distributed through the active BWP. However, this flexibility comes at the cost of an increased number of bits in the resource allocation field within the Downlink Control Information (DCI) [22].

For resource allocation type 1, the UE is assigned contiguous RBs for downlink/uplink data transmission. The network encodes the starting RB (RB_{start}) and the length of the contiguously allocated RBs (L_{RBs}) using the resource indication value (RIV) of the resource allocation field within the DCI. The UE decodes the RIV value to determine where to receive/send data. The RIV is calculated using N_{BWP}^{size}, L_{RBs}, and (RB_{start}) as given in (4). This formula ensures that the RIV is appropriately calculated based on the BWP size, the length of the allocated RBs, and the starting RB. It provides a mechanism for determining the specific frequency resources allocated to the UE within the active BWP for efficient data transmission.



(a)



(b)

Fig. 2: Illustration of types for resources allocation: (a) Type 0; (b) Type 1.

III. Inter-Slot and Intra-Slot Cross-BWP Frequency Hopping

In this section, we outline our detailed design for inter-slot and intra-slot C-BWP FH for the uplink. The downlink C-BWP FH can be equivalently designed. This design takes

$$RBG_{last}^{size} = \begin{cases} mod\left((N_{BWP,i}^{start} + N_{BWP}^{size}), P\right) & \text{if } mod\left((N_{BWP,i}^{start} + N_{BWP}^{size}), P\right) \geq 0, \\ P & \text{otherwise.} \end{cases} \tag{3}$$

$$RIV = \begin{cases} N_{BWP}^{size} \times (L_{RBs} - 1) + RB_{start} & \text{if } (L_{RBs} - 1) \geq \left\lfloor \frac{N_{BWP}^{size}}{2} \right\rfloor, \\ N_{BWP}^{size} \times (N_{BWP}^{size} - L_{RBs} + 1) + (N_{BWP}^{size} - 1 - RB_{start}) & \text{otherwise.} \end{cases} \tag{4}$$

into account the available channel quality and user priority information.

A. Channel Estimation

The Sounding Reference Signal (SRS) serves as a reference signal for uplink channel sounding. It plays an important role in the network's capability to assess channel conditions and adapt its configuration accordingly. The SRS is generated by the UE, and the UE periodically transmits it to the gNodeB. The transmission adheres to the configured SRS parameters including periodicity, frequency and time positions, and the configuration of SRS resources. The periodic SRS transmission ensures that the gNodeB obtains timely and updated information about the uplink channel. More precisely, through the analysis of the received SRS, the gNodeB obtains valuable channel characteristics, encompassing channel gain, delay spread, and Doppler shift for each UE in each RBG within the available bandwidth. Leveraging this information, the gNodeB can optimize the resource allocation, dynamically adjusting resource assignments to UEs based on their individual channel conditions.

Consider a scenario where a gNodeB serves N UEs with diverse priorities in the uplink within a limited frequency-selective bandwidth, denoted as BW. The gNodeB is responsible for allocating frequency resources to the various UEs for their data transmission. Adhering to the 5G NR specifications outlined in the previous section, this BW is divided into M RBs, each with a size of 12 SCs. Additionally, the BW is segmented into B equal-sized BWPs. In this analysis, we adopt Resource Allocation Type 0. Without loss of generality, each UE is allocated an equal number of RBGs for uplink transmission within a given time slot and BWP. Leveraging the uplink channel quality information (CQI) obtained through SRS and the priority information for each UE, the gNodeB efficiently allocates resources and designs the C-BWP FH pattern. It is assumed that the SRS has a periodicity of one frame, aiming to minimize the control signal transmission between the gNodeB and the UEs. The gNodeB acquires the channel quality of each RBG for every UE from the SRS signal and utilizes this information for the entire frame duration. The number of slots per frame is determined by the adopted numerology.

B. The Proposed C-BWP Frequency Hopping Strategy

The C-BWP hopping strategy entails the gNodeB receiving the CQI of each RBG for each UE before allocating resources in the upcoming frame. Suppose there are $\mathcal{B}$ BWPs within the whole channel bandwidth, and $\mathcal{K}$ UEs to transmit data. Throughout a frame $\mathcal{F}$, UEs can only occupy the RBGs winthin the same BWP during each transmission but can hop to another BWP for next transmission. We define that each transmission is either a slot $\mathcal{S}$ or a mini-slot τ. The gNodeB manages the allocation of RBGs for all UEs and acquires the channel measurement CQI of those RBGs. It then orders all the RBGs from high CQI value to low CQI value. The UEs are also sorted according to their priority from high to low. After the process, without loss of generality, $\mathcal{M}$ (where $\mathcal{M} = \mathcal{B}N_{RBG}$) RBGs are ordered as RBG_1, RBG_2, ... , $RBG_{\mathcal{M}}$, and $\mathcal{K}$ UEs are ordered as $\mathcal{U}_1$,$\mathcal{U}_2$, ... , $\mathcal{U}_{\mathcal{K}}$. We further define a $\mathcal{K} \times \mathcal{M}$ matrix $\mathcal{A}$ to denote the allocation and the hopping pattern:

$$\mathcal{A}_{i,j} = \begin{cases} 1, \text{ if } RBG_j \text{ is allocated to UE } \mathcal{U}_i \\ 0, \text{ otherwise} \end{cases}, \tag{5}$$

under the following conditions:

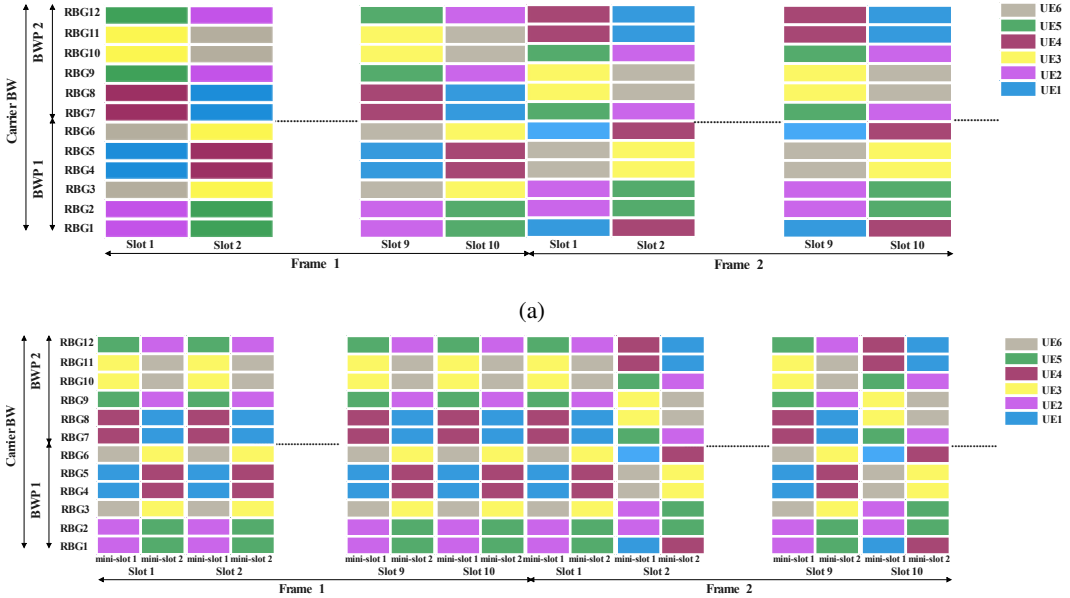
$$\mathcal{A}_i \ \overline{XOR} \ \mathcal{A}_k = \{0, 0, .., 0\}, (i \neq k) \text{ and} \tag{6}$$

$$Q_{RBG}^{(i,\Delta)} < Q_{RBG}^{(i+1,1)}, \tag{7}$$

where $\overline{XOR}$ is the reverse exclusive OR operation, $\mathcal{A}_i$ is the set of RBGs assigned to UE i, and $Q_{RBG}^{(i,\Delta)}$ (or $Q_{RBG}^{(i,1)}$) denote

Algorithm 1: Resource Allocation Procedure for C-BWP Frequency Hopping

```
Initialize CQI values for all RBG;
Initialize RBG allocation by a default order;
for each transmission do
    Obtain CQIs for all M RBGs via measurement;
    Order the RBGs from high CQI to low CQI;
    Order K UEs from high priority to low priority;
    for U_i do
        if BP_i + 1 < B then
            BP_i ← BP_i + 1;
        else
            BP_i = 0;
        end
        while Q_RBG^(i,1) ≥ Q_RBG^(i−1,Δ) (i ≥ 1) do
            i ← i + 1;
        end
        U_i ← RBG_i;
    end
end
```



(a)

(b)

Fig. 3: Illustration of cross-BWP frequency hopping (a) inter-slot and (b) intra-slot.

the sequence number of the last RBG in set $\mathcal{A}_i$ (or the first RBG in set $\mathcal{A}_i$). The first constraint (6) makes sure that any two UEs do not have duplicate allocation, while the second constraint (7) means high-priority UE will be assigned RBGs with higher CQI.

Based upon the above discussion, the procedure of resource allocation for C-BWP FH is described in Algorithm 1.

C. Inter-slot and intra-slot Frequency Hopping

The inter-slot C-BWP hopping strategy entails the gNodeB receiving the CQI of each RBG for each UE before the frame starts. With B BWPs, UEs are authorized to transmit data within a singular BWP during each time slot throughout the frame. The gNodeB manages the allocation of RBGs to diverse UEs and starts the process with the highest-priority UE. It acquires the CQI for RBGs associated with the UE, arranges them based on CQI, and assigns R RBGs with the highest channel quality within one BWP. This sequence repeats for the other active UEs in order of decreasing priority. Finally, the gNodeB delivers this RBG allocation information to UEs through the DCI within the Physical Downlink Control Channel (PDCCH) before the transmission frame starts. UEs utilize their designated RBGs sequentially across BWPs, transitioning between BWPs within from time slot to time slit, subsequently repeating until the gNodeB provides a new allocation at the beginning of the next frame.

For the mini-slot (or intra-slot) C-BWP hopping strategy, a single slot is partitioned into H mini-slots during which FH happens. The RBG allocation strategy mirrors that of the inter-slot approach, where the gNodeB leverages the CQI and user priority to allocate RBGs within each BWP for each UE.By contrast, the UEs switch the BWP at each mini-slot rather than each slot. In the initial mini-slot, UEs utilize RBGs allocated in the first BWP according to the gNodeB's specified order. Subsequently, in each successive mini-slot, UEs transition to RBGs within the next BWP in the specified order and continue this sequence until the final mini-slot of a slot. This process repeats until the next frame, in which the gNodeB allocate RBGs according to the updated channel quality measurements. The number of mini-slots within a slot aligns with the total number of BWPs.

D. Illustration by Examples

We provide an example to illustrate the process. Assuming an available uplink bandwidth with a size of 288 subcarriers, using a 15 kHz SCS, we can calculate the number of available RBs in this bandwidth as $\frac{288}{12} = 24$ RBs. The bandwidth is segmented into 2 BWPs, namely BWP1 and BWP2, each with a size of $N_{BWP}^{size} = 12$ RBs. Following Configuration 1 from Table I and equations (1), (2), and (3), the number of RBGs in each BWP is 6, with each RBG consisting of 2 RBs. Given 6 UEs with different priorities, where UE1 has the highest priority and UE6 has the lowest, the gNodeB allocates the same number of RBGs to each UE, resulting 2 RBGs per UE.

The gNodeB receives the SRS from each UE to determine the RBG allocation and the C-BWP hopping pattern. The gNodeB then orders the RBGs for each UE based on their channel quality.The RBG ordering may result in {RBG5, RBG4, RBG7, RBG8, RBG1, RBG12, RBG9, RBG10, RBG2, RBG6, RBG3, RBG11}. In this configuration, BWP1 spans RBG1 to RBG6 and BWP2 spans RBG7 to RBG12. Given the presence of only two BWPs, there is one hop, meaning the UEs alternate between BWP1 and BWP2 from

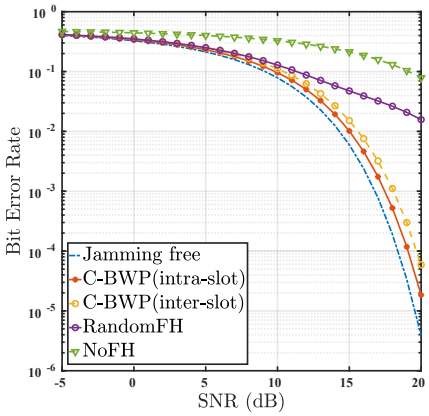


Fig. 4: BER over SNR for intra-slot and inter-slot C-BWP FH under burst jamming.

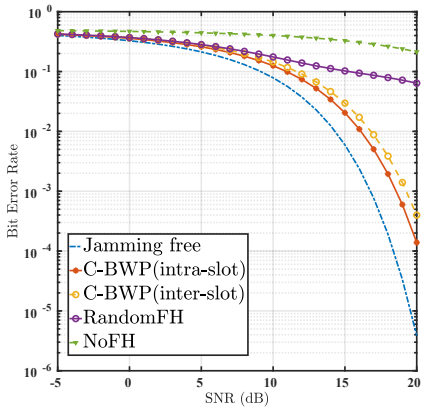


Fig. 5: BER over SNR for intra-slot and inter-slot C-BWP FH under follower frequency selective jamming.

one slot to the next or from one mini-slot to the next. Since there are 2 BWPs, each containing 6 RBGs and 6 UEs, and each UE gets 2 RBG within the same BWP, three UEs will start transmission in BWP1, and three in BWP2. This results in two hopping patterns: BWP1 then BWP2 or BWP2 then BWP1. An additional bit is added to the bitmap allocation to define the hopping pattern. As there are 12 RBGs, the total number of bits within the DCI is increased to 12 + 1 = 13 bits.

The gNodeB proceeds with defining the bitmaps and configuring the frequency hopping pattern. RBG5 and RBG4 in BWP1 and RBG7 and RBG8 in BWP2 are allocated to UE1 with hopping pattern 1. The bitmap is (0,0,0,1,1,0,1,1,0,0,0,0,0). RBG1 and RBG2 in BWP1 and RBG12 and RBG9 in BWP2 are allocated to UE2 with hopping pattern 1, resulting in bitmap (1,1,0,0,0,0,0,0,1,0,0,1,0). UE3 gets RBG3 and RBG6 in BWP1 and RBG10 and RBG11 in BWP2, starting transmission in BWP1 and then hopping to BWP2. The corresponding bitmap is (0,0,1,0,0,1,0,0,0,1,1,0,0). UE4 initiates transmission with BWP2 and then switches to BWP1, allocating RBG5 and RBG4 in BWP1 and RBG7 and RBG8 in BWP2. The bitmap is (0,0,0,1,1,0,1,1,0,0,0,0,1). UE5 follows the same allocation as UE2 but with hopping pattern 2, resulting in bitmap (1,1,0,0,0,0,0,0,1,0,0,1,1). Finally, UE6 replicates the allocation of UE3 but with hopping pattern 2, yielding bitmap (0,0,1,0,0,1,0,0,0,1,1,0,1). This allocation strategy ensures that no more than one UE is allocated the same RBG at the same time, and the UEs hop based on channel quality.

IV. Numerical Analysis and Discussion

In this section, we analyze the BER results of inter-slot and intra-slot C-BWP hopping for various signal-to-noise ratio (SNR) levels in the presence of two typical jamming attacks: burst jamming, and follower frequency selective jamming. The results are obtained through simulations using the MATLAB 5G Toolbox. Each simulation lasts 5000 frames, maintaining a consistent modulation scheme of 16QAM for all cases. The system bandwidth is 50 MHz with 15 kHz SCS, accommodating 10 UEs. The available bandwidth is divided into 4 BWPs. The number of mini-slots equals 4 for the intra-slot FH case. The characteristics of the jamming techniques used in our simulation are detailed as follows: burst jamming intermittently activates and silent, producing distinct bursts of interference. Specifically, the burst jammer targets two out of the four available BWPs, remaining active for 0.5 ms and then silent for 0.5 ms, and cycles through the targeted BWPs every 20 ms. On the other hand, follower frequency-selective jamming targets multiple frequencies across a specified bandwidth. In our simulation, this technique is capable of jamming half of the bandwidth and actively follows the high-priority UEs, selecting frequencies that these UEs are using for jamming purposes. The jammer changes the selected frequencies every 1 ms to maintain effective disruption.

Fig. 4 displays the average BER across SNR for the top 50% of high-priority UEs subjected to burst jamming with a 10 dB Jamming-to-Noise Ratio (JNR), comparing the proposed intra-slot and inter-slot C-BWP methods against the theoretical BER performance for 16QAM modulation without jamming ('No Jammer'). It also includes comparisons with inter-slot random hopping without considering the CQI ('RandomFH') and scenarios without any frequency hopping ('NOFH'). The results show that frequency hopping methods outperform non-hopping scenarios. Both intra-slot and inter-slot C-BWP hopping perform well, achieving BER results close to the jamming-free case. Notably, intra-slot C-BWP hopping demonstrates superior performance, closely approaching the theoretical results without jamming. This advantage is attributed to the higher frequency of hops, which provides UEs with more opportunities to evade jammed BWPs. The intra-slot scheme is especially effective in avoiding sustained bursts of jamming; even if a hop coincides with a burst, subsequent hops are likely to occur during the jammer's off-cycle, thus minimizing the overall BER. Conversely, with inter-slot hopping, if a hop aligns with a

jammer's active phase, the impact is more sustained, resulting in a higher BER for that slot.

Fig. 5 illustrates the effect of the follower frequency selective jamming on the proposed methods with 10 dB JNR. The results confirm the superiority of intra-slot over inter-slot FH compare to the NoFH and RandomFH cases. Same as in the previous figure, the intra-slot outperforms the inter-slot case. Intra-slot C-BWP provides resilience by not allowing the jammer to effectively lock onto a single frequency for long. This continuous movement across the spectrum complicates the jammer's task, especially if the jamming strategy requires adjustment based on observed traffic, while inter-slot C-BWP is more susceptible to being tracked and jammed, as each frequency is used longer, giving follower jammers more time to react and optimize their jamming strategy against the observed pattern.

Intra-slot hopping generally provides better protection against the described jamming techniques due to its agility and the reduced time window during which any given frequency is exposed to jamming. This frequent hopping helps in minimizing the impact of both continuous and intermittent jamming, making it harder for jammers to effectively target and disrupt communications. This approach is particularly advantageous in highly contested environments where jammers are active and adaptive. However, the choice between intra-slot and inter-slot hopping can also depend on other factors such as system complexity, power consumption, hardware capabilities, and specific operational requirements. If stability and lower complexity are more critical, or if the jamming environment is less intense, inter-slot hopping might be sufficient and more practical.

V. Conclusions

This paper introduces C-BWP inter-slot and intra-slot FH for the PUSCH in 5G NR. We formulate the necessary protocol extension for proper transmission and reception leveraging the existing 5G control fields and signals. We numerically analyze the efficacy of these techniques against jamming with known CSI and diverse UE priorities wit the presensce of two types of jamming : burst and follower frequency selective jamming. The results highlight the enhancement in resilience against jamming using both C-BWP FH methods, emphasizing the importance of the channel estimation. The superiority of intra-slot hopping over inter-slot hopping is demonstrated, particularly for follower jamming, and is attributed to the finer granularity of FH and the higher hopping rates.

Acknowledgment

This work is supported by NSF and Office of the Under Secretary of Defense (OUSD) – Research and Engineering, under Grant ITE2326898, as part of the NSF Convergence Accelerator Track G: Securely Operating Through 5G Infrastructure Program and by the Office of Naval Research under Award No. N00014-23-1-2808.

References

[1] L. Zhang, M. Xiao, G. Wu, M. Alam, Y.-C. Liang, and S. Li, "A survey of advanced techniques for spectrum sharing in 5G networks," *IEEE Wireless Communications*, vol. 24, no. 5, pp. 44–51, 2017.

[2] G. Gür, "Expansive networks: Exploiting spectrum sharing for capacity boost and 6G vision," *Journal of Communications and Networks*, vol. 22, no. 6, pp. 444–454, 2020.

[3] K. Ibrahim and S. B. Sadkhan, "Radio access network techniques beyond 5G network: A brief overview," in *2021 International Conference on Advanced Computer Applications (ACA)*, 2021, pp. 96–100.

[4] W. K. Alsaedi, H. Ahmadi, Z. Khan, and D. Grace, "Spectrum options and allocations for 6G: A regulatory and standardization review," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1787–1812, 2023.

[5] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 1010–1015.

[6] M. E. Flores, D. D. Poisson, C. J. Stevens, A. V. Nieves, and A. M. Wyglinski, "Implementation and evaluation of a smart uplink jamming attack in a public 5G network," *IEEE Access*, vol. 11, pp. 75 993–76 007, 2023.

[7] L. Liang, W. Cheng, W. Zhang, and H. Zhang, "Mode hopping for anti-jamming in radio vortex wireless communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7018–7032, 2018.

[8] B. Gopalakrishnan and M. A. Bhagyaveni, "Random codekey selection using codebook without pre-shared keys for anti-jamming in WBAN," *Computers & Electrical Engineering*, vol. 51, pp. 89–103, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790616300556

[9] H. Sharma, N. Kumar, and R. Tekchandani, "Mitigating jamming attack in 5G heterogeneous networks: A federated deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2439–2452, 2023.

[10] W. M. Chan, H. M. Kwon, R. A. Chou, D. J. Love, S. Fahmy, S. R. Hussain, S. W. Kim, C. V. Valk, C. G. Brinton, V. Marojevic, K. D. Pham, and T. Kim, "Adaptive frequency hopping for 5G new radio mMTC security," in *2023 IEEE International Conference on Industrial Technology (ICIT)*, 2023, pp. 1–5.

[11] The 3rd Generation Partnership Project (3GPP) "5G; NR; Physical layer procedures for control (3GPP TS 38.213 version 17.4.0 Release 17)," Technical specification (TS) 38.213, 2023, Version 17.4.0.

[12] The 3rd Generation Partnership Project (3GPP), "5G; NR; Physical channels and modulation (3GPP TS 38.211 version 17.4.0 Release 17)," Technical specification (TS) 38.211, 2023, Version 17.4.0.

[13] S. Talarico and M. C. Valenti, "Frequency hopping on a 5g millimeter-wave uplink," in *2015 49th Asilomar Conference on Signals, Systems and Computers*, 2015, pp. 333–337.

[14] J. A. del Peral-Rosado, J. A. López-Salcedo, and G. Seco-Granados, "Impact of frequency-hopping nb-iot positioning in 4G and future 5G networks," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 815–820.

[15] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "Gaming the jammer: Is frequency hopping effective?" in *2009 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, 2009, pp. 1–10.

[16] E. Dahlman and S. Parkvall, "NR – the new 5G radio-access technology," in *IEEE VTC Spring*, 2018, pp. 1–5.

[17] A. Yazar, B. Peköz, and H. Arslan, "Fundamentals of Multi-Numerology 5G New Radio." 2019.

[18] The 3rd Generation Partnership Project (3GPP), "Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC)," Technical Report (TR) 38.824, 2019, Version 16.0.0.

[19] The 3rd Generation Partnership Project (3GPP) "NR; Physical channels and modulation," Technical specification (TS) 38.211, 2022, Version 17.1.0.

[20] The 3rd Generation Partnership Project (3GPP), "Multiplexing and channel coding," Technical specification (TS) 38.212, 2022, Version 17.2.0.

[21] The 3rd Generation Partnership Project (3GPP) "Physical layer procedures for data," Technical specification (TS) 38.214, 2022, Version 17.1.0.

[22] The 3rd Generation Partnership Project (3GPP), "Physical layer procedures for control," Technical specification (TS) 38.213, 2020, Version 16.2.0.