Adaptive Frequency Hopping for 5G New Radio mMTC Security

Wai Ming Chan, Hyuck M. Kwon, Rémi A. Chou, David J. Love, Sonia Fahmy, Syed Rafiul Hussain, Sang Wu Kim, Chris Vander Valk, Christopher G. Brinton, Vuk Marojevic, Khanh D. Pham, and Taejoon Kim

***Abstract*—3GPP standards (e.g., LTE and 5G New Radio (NR)) have revolutionized commercial broadband access. Unfortunately, the openness of 3GPP specifications and high-level of adaptability make fifth-generation (5G) networks increasingly sensitive to unsophisticated attacks in the network. While 5G NR has introduced frequency hopping (FH) for massive machine-type communications (mMTC), there has not been a unified approach to designing the FH patterns in practical 5G systems. In this paper, we investigate the multi-user FH design problem at the physical resource grid of the 5G communication networks. We present various criteria for FH pattern design and propose two algorithms that are implementable with low complexity. The first scheme utilizes known interference patterns to design a set of user equipment (UE) FH patterns that are immune to interfering attacks. The second scheme leverages interference statistics and minimizes the expected number of hits by the interferer. Through numerical simulations and analytical modeling, we demonstrate the efficacy of the proposed schemes, which outperform the uniform FH pattern and achieve near-optimal performance.**

***Index Terms*—Frequency hopping, 5G New Radio (NR) communications, massive machine type communications (mMTC), physical layer security**

I. Introduction

The fifth-generation (5G) cellular networks have been introduced to facilitate the growing demand for high-speed and reliable wireless use cases including: (i) enhanced mobile broadband (eMBB); (ii) massive machine-type communications (mMTC); and (iii) ultra-reliable low-latency communications (URLLCs). In particular, the mMTC user equipments (UEs) are allowed to use frequency hopping (FH) patterns [1], [2]. FH allows mMTC UEs to be flexible in accessing 5G spectrum resources and even be resilient to active interferers. When there are malicious entities capable of generating partial band interference, FH enables legitimate UEs to dynamically change their frequencies, mitigating interfering attacks as well as preventing information leakage. Unlike other mitigation methods such as pilot contamination detection [3] and spoofing detection [4] that are primarily concerned with threat monitoring, FH provides protection regardless of the status of threats.

While the 3GPP specifications provide unified standardization across multiple mobile network operators, its openness to the public has been making the 5G cellular networks increasingly fragile. This is mainly because cellular networks have primarily been designed to achieve the fundamental limits of traditional wireless channel models without the purposeful introduction of Zero Trust. In the 5G New Radio (NR) specifications [2], [5], the base station (BS) coordinates the physical layer resource allocation with the user equipment (UE) through the control-resource set (CORESET) over the downlink control channel (PDCCH). The 3GPP specifications specify the locations of the CORESET. Any capable malicious entities can learn the CORESET by snooping the resource allocation information. On the other hand, the intra-slot FH option in the 5G physical uplink control channel (PUCCH) [2] allows the FH at each orthogonal frequency division multiplexing (OFMD) symbol within a slot time[1]. The effectiveness of the intra-slot FH in PUCCH is largely dependent on the hopping rate and hopping pattern. This hopping information is public and malicious entities can exploit it to generate interference; it was shown that harm can be done by using even unsophisticated software-defined radios (SDRs) [6], [7].

It is well known in the game theory literature [8] that both the optimum UE FH pattern against an interferer and the most harmful interfering FH pattern against a UE FH pattern should be uniformly random. This is true when both interferer and UE play a game in which an interferer aims to maximize the number of hits with the FH UE while the FH UE aims to minimize the hits by the interferer [8], [9]. This direction is aligned with the existing protected tactical waveform (PTW) for a current military satellite communication system, which assumes the interfering FH patterns are uniformly random over

This work was supported in part by National Science Foundation (NSF) under Grant 2226447.

W. M. Chan and T. Kim are with the Department of Electrical Engineering and Computer Science, The University of Kansas, Lawrence, KS 66045 USA (email: waiming.chan@ku.edu; taejoonkim@ku.edu).

H. M. Kwon is with the Department of Electrical and Computer Engineering and R. A. Chou is with the School of Computing, Wichita State University, Wichita, KS 67260 USA (e-mail: hyuck.kwon@wichita.edu; remi.chou@wichita.edu).

D. J. Love and C. G. Brinton are with the Elmore Family School of Electrical and Computer Engineering and S. Fahmy is with the Department of Computer Science, Purdue University, West Lafayette, IN 47907 USA (e-mail: djlove@purdue.edu; cgb@purdue.edu; fahmy@purdue.edu).

S. R. Hussain is with the Department of Computer Science and Engineering, The Pennsylvania State University, State College, PA 16802 USA (e-mail: hussain1@psu.edu).

S. W. Kim is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: swkim@iastate.edu).

C. Vander Valk is with Raytheon BBN, Cambridge, MA 02138 USA (email: christopher.vandervalk@raytheon.com).

V. Marojevic is with the Department of ECE, Mississippi State University, Starkville, MS 39762, USA (e-mail: vuk.marojevic@ece.msstate.edu).

K. Pham with Air Force Research Laboratory, Albuquerque, NM 87123 USA (email: khanh.pham.1@spaceforce.mil).

[1]One 5G NR slot time consists of 14 OFDM symbols with the symbol time less than 70 μs.

the entire frequency band [10]. Then, the optimum signal FH pattern against this uniform FH interference is also uniform logically. In addition, to maximize the spectrum utilization, an FH UE uses the entire band uniformly also. Therefore, the existing PTW adopted uniform FH patterns for all UEs. However, in practice, an intelligent interferer can jam only the targeted UE signals rather than the entire band to save its power and maximize its interference efficacy. This is the motivation for the proposed investigation.

In this paper, we investigate the problem of FH pattern design for 5G NR mMTC UEs presented at the physical resource grid in 5G terrestrial communication networks. The problem is challenging due to the substantial computational overhead associated with the FH patterns for numerous mMTC UEs with short hopping intervals. We address this challenge by formulating the FH pattern design problem at the 5G PUCCH that prevents both attackers and friendly UE collisions. We present two FH schemes: one that utilizes known interference patterns, and another that utilizes only the interference statistics. Simulation results illustrate improved protection performance against interference for our proposed schemes compared to the traditional uniform FH scheme [10].

The proposed adaptive FH scheme can be implemented without modifying 5G standards because the uplink and downlink frequency ranges and time slots can be scheduled by a BS or requested by UEs. Once the frequency range and time slots are assigned, multiple UEs' symbols can be permuted at a gateway on the UE side, which is equivalent to a subcarrier permutation within an OFDM symbol interval. Subcarrier permutations can be scheduled by a BS or a gateway at the UE side to achieve the desired FH patterns. A cooperative BS can distribute the FH pattern key to each UE via downlink control information (DCI). In the case of a non-cooperative and zero-trusted BS, a UE can request a schedule using uplink control information (UCI).

II. System Model and Design Criteria

Consider a BS serving N_u mMTC UEs in the 5G NR resource block and OFDM modulation with N_s available subcarriers. Each UE could access at least one subcarrier in one OFDM symbol duration if $N_u \leq N_s$; otherwise, time-division multiple access (TDMA) is adopted. Intra-slot FH is allowed for UE subcarrier allocation where one slot time consists of N_h FH intervals and the duration of each FH interval is T_h. For the intra-slot frequency hopping in PUCCH, a FH pattern represents the sequence of subcarrier location carrying the demodulation reference signals (DM-RS) of each mMTC UE. The FH pattern of UE i is denoted by a sequence $X_i = (X_i[1], \ldots, X_i[N_h]) \in \mathcal{F}^{N_h}$ where $\mathcal{F} = \{f_1, \ldots, f_{N_s}, f_{\text{null}}\}$ is the subcarrier alphabet set and f_{null} is the null subcarrier used for an OFF state in an intermittent FH. The intermittent FH is not considered.

Suppose the physical channels suffer from multi-tone interference with the ability to obstruct $N_{\text{Inf}} \geq 1$ subcarriers. Denote the interference FH pattern in one time slot as the sequences $X_{\text{Inf},l} \in \mathcal{F}^{N_h}$, for $l = 1, \ldots, N_{\text{Inf}}$. We assume that the FH pattern of a multi-tone interferer is measurable at the end of each time slot. This assumption is practical because the FH patterns of friendly UEs are known by the BS, and the signal-to-noise ratio (SNR) can be measured at each FH interval. If the SNR is smaller than a normal operational SNR, then the corresponding subcarrier is likely to be interfered.

Illustrative Example: Fig. 1 shows an example of FH patterns of a set of UEs and an interferer, where each UE only occupies a single subcarrier at one FH interval of T_h. In the example, $N_u = 4, N_s = 12, N_h = 3$, and $N_{\text{Inf}} = 1$ are assumed. In the first time slot (i.e., first three FH intervals), the FH patterns of UEs and interferer can be represented as $X_1 = (f_1, f_4, f_7)$, $X_2 = (f_2, f_5, f_8)$, $X_3 = (f_3, f_6, f_9)$, and $X_{\text{Inf}} = (f_1, f_4, f_7) = X_1$, respectively. All three UEs adopted linear FH patterns, and the interferer targets the UE 1. The whole UE 1's FH pattern is interfered because the adversary can easily acquire the FH knowledge if it is linear. In the second time slot, the UE 1 changes its linear pattern dynamically to $X_1 = (f_5, f_1, f_{10})$, and the FH patterns for other UEs remain the same. The interferer's attack on UE 1 is unsuccessful in the second time slot.

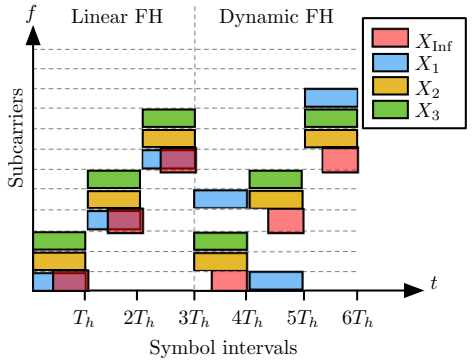


Figure 1: Example of FH patterns $X_1, X_2, X_3, X_{\text{Inf}}$ of three UEs and one interferer with $N_s = 12, N_h = 3, N_{\text{Inf}} = 1$.

A. Frequency Hopping Pattern Design Criteria

The most common approach used to measure the distance between two (binary) sequences employs Hamming distance. We propose two Hamming distance-related metrics, the number of successes and the number of hits. We also employ traditional multiple-access communication performance such as minimum signal-to-interference-plus-noise ratio (SINR).

1) Number of successes: We count the number of successful transmissions for all UEs in the one-time slot by using given FH patterns $X_1, \ldots, X_{N_u}$. Let $j^\star_{i,n} = X_i[n]$ denote the subcarrier index assigned to UE i at the n-th FH interval conditioned on $X_i[n] \neq f_{\text{null}}$. The number of successes at the n-th FH interval can be written as

$$N_{\text{success},n} = \sum_{i=1}^{N_u} \left(\prod_{\substack{i'=1 \\ i' \neq i}}^{N_u} \mathbb{1}_{\{X_{i'}[n] \neq f_{j^\star_{i,n}}\}} \right) \left(\prod_{l=1}^{N_{\text{Inf}}} \mathbb{1}_{\{X_{\text{Inf},l}[n] \neq f_{j^\star_{i,n}}\}} \right).$$

where $\mathbb{1}_{\{\cdot\}}$ denotes the indicator function. The total number of successes for the whole time slot can then be computed by

$$N_{\text{success}} = \sum_{n=1}^{N_h} N_{\text{success},n}. \quad (1)$$

The computation of (1) has the complexity $\mathcal{O}(N_h N_u^2 N_{\text{Inf}})$ which grows quadratically with N_u.

2) Number of hits: Similar to the number of successes, one can also compute the number of hits of UE i as $N_{\text{hit},i,n} = |\mathcal{I}_{i,n}| + |\mathcal{L}_{i,n}|$, where $\mathcal{I}_{i,n} = \{i' : X_{i'}[n] = X_i[n] \neq f_{\text{null}}, 1 \leq i' \leq N_u\}$ and $\mathcal{L}_{i,n} = \{l : X_{\text{Inf},l}[n] = X_i[n], 1 \leq l \leq N_{\text{Inf}}\}$, respectively, are the set of UE indices and the set of interferer indices causing interference to UE i at the n-th interval. The total number of hits during the entire time slots is given by

$$N_{\text{hit}} = \sum_{n=1}^{N_h} \sum_{i=1}^{N_u} N_{\text{hit},i,n}. \quad (2)$$

The computation of (2) has the complexity $\mathcal{O}(N_h(N_u^2 + N_{\text{Inf}}))$ which is within the same order as (1).

3) SINR: For any given FH patterns, we can compute the SINR of the UE i at the n-th FH interval as

$$\gamma_{i,n} = \frac{P_{S,i,n}}{\sigma_N^2 + \sum\limits_{i' \in \mathcal{I}_{i,n}} P_{S,i',n} + \sum\limits_{l \in \mathcal{L}_{i,n}} P_{J,l,n}} \quad (3)$$

where $P_{S,i,n}$, $P_{J,l,n}$, and σ_N^2, respectively, are the received UE i signal power at the n-th FH interval, the received interference power of interferer's l-th tone at the n-th FH interval, and the received noise power. To measure the quality of service (QoS) in terms of the fairness, we employ the minimum SINR in a whole time slot as

$$\min_{1 \leq i \leq N_u} \left\{ \sum_{n=1}^{N_h} \gamma_{i,n} \right\}. \quad (4)$$

The computation complexity of the minimum SINR in (4) is the same as that of the total number of hits in (2).

B. SINR Bound and Its Surrogate

When the received power values of a UE and interferer to occupy one subcarrier are equal, i.e., $P_{S,i,n} = P_{J,l,n} = P_S$, $\forall i, l$, which is the case when the BS employs uplink power control to mitigate the near-far effects, the maximization of minimum SINR can be linked to the minimum number of hits as follows. From (3), the SINR of UE i for the whole time slot can be bounded as

$$\begin{aligned}\gamma_i &= \sum_{n=1}^{N_h} \left(\frac{\sigma_N^2}{P_S} + \sum_{i' \in \mathcal{I}_{i,n}} 1 + \sum_{l \in \mathcal{L}_{i,n}} 1 \right)^{-1} \\ &= \sum_{n=1}^{N_h} \left(\frac{\sigma_N^2}{P_S} + N_{\text{hit},i,n} \right)^{-1} \overset{(a)}{\geq} N_h^2 \left(N_h \frac{\sigma_N^2}{P_S} + N_{\text{hit},i} \right)^{-1},\end{aligned}$$

where (a) is due to Jensen's inequality applied to a convex function $f(x) = x^{-1}$ for $x > 0$ and $N_{\text{hit},i} = \sum_{n=1}^{N_h} N_{\text{hit},i,n}$ denotes the number of hits of UE i in one slot. Thus, we have $\min_i \gamma_i \geq N_h^2 \min_i \left(N_h \frac{\sigma_N^2}{P_S} + N_{\text{hit},i} \right)^{-1}$ and

$$\max_{\{X_1,\ldots,X_{N_u}\}} \min_i \gamma_i \geq N_h^2 \max_{\{X_1,\ldots,X_{N_u}\}} \min_i \left(N_h \frac{\sigma_N^2}{P_S} + N_{\text{hit},i} \right)^{-1}. \quad (5)$$

The solution on the right-hand-side (RHS) is equivalent to

$$\operatorname*{argmax}_{\{X_1,\ldots,X_{N_u}\}} \min_i \left(N_h \frac{\sigma_N^2}{P_S} + N_{\text{hit},i} \right)^{-1} = \operatorname*{argmin}_{\{X_1,\ldots,X_{N_u}\}} \max_i N_{\text{hit},i}. \quad (6)$$

It is shown that the max-min SINR optimization is often complicated due to its combinatorial nature [11]. Instead, we leverage its lower bound in (5), which is equivalent to minimizing the maximum number of hits on the RHS of (6). Exploiting the tractability offered by (6) provides insights into the optimal FH pattern design with low-complexity algorithms.

III. Frequency Hopping Pattern Designs

We gave FH pattern-solving criteria earlier. In this section, we present two greedy schemes for solving (6).

A. Known Interference Scenario

Assuming the interference FH patterns $X_{\text{Inf},l}$ for $l = 1, \ldots, N_{\text{Inf}}$ are given, BS designs the FH patterns at each FH interval independently according to the criterion in (6), which is described in Algorithm 1. At each FH interval, we initialize the collision set $\mathcal{I}$ as an empty set and compute the interference set $\mathcal{J}$ to contain all interfered subcarriers from $X_{\text{Inf},l}[n], \forall l$. It is straightforward to conclude that the known-interference-pattern case assumed in this subsection can always ensure zero number of hits. In Algorithm 1, the FH patterns are assigned to each UE in sequential order. The UE i FH location $X_i[n]$ is picked uniformly from the collision-free set $\mathcal{F} \backslash (\mathcal{J} \cup \mathcal{I})$, where $\backslash$ denotes set substraction. Then the collision set $\mathcal{I}$ is updated to include the UE i's pattern $X_i[n]$. The UE assignment is repeated until all UEs are assigned or the collision-free set $\mathcal{F} \setminus (\mathcal{J} \cup \mathcal{I})$ becomes empty. In the 5G NR setting, a large amount of mMTC UEs are supported, i.e., $N_u > N_s = |\mathcal{F}|$. Thus, TDMA to divide multiple user access is considered, i.e., $X_i(n) = f_{\text{null}}$ for $i \geq |\mathcal{F} \setminus \mathcal{J}|$. Algorithm 1 outlines the above-mentioned FH pattern design procedure.

Algorithm 1 Procedures of FH pattern design under known interference FH pattern

Input
  $\{X_{\text{Inf},l} : l = 1, \ldots, N_{\text{Inf}}\}$ Interferer's pattern
Output
  $\{X_i \in \mathcal{F}^{N_h} : i = 1 \ldots, N_u\}$ UEs' FH patterns
for $n = 1, \ldots, N_h$ **do**
  Initial condition: $\mathcal{I} = \emptyset$
  Initial condition: $\mathcal{J} = \{X_{\text{Inf},l}[n] : 1 \leq l \leq N_{\text{Inf}}\}$
  for $i = 1, \ldots, N_u$ **do**
    if $i \geq |\mathcal{F} \setminus \mathcal{J}|$ **then**
      $X_i[n] \leftarrow f_{\text{null}}$
    else
      $X_i[n] \leftarrow \text{uniform}(\mathcal{F} \setminus (\mathcal{J} \cup \mathcal{I}))$
      $\mathcal{I} \leftarrow \{\mathcal{I}, X_i[n]\}$
    end if
  end for
end for

The assumption of known interference pattern is not practical and, in our paper, the former scenario is only considered as a baseline for the evaluation (see Section IV). Therefore, we next consider the FH pattern design based on interference statistics as we assume the interference pattern is randomized under some *unknown* distributions.

B. Statistical interference Scenario

Same as Algorithm 1, the statistical FH pattern design is done sequentially. The design is based on the conditional probability of interference statistics. Since we assign the UE pattern sequentially, the interference at the UE i consider the UE $[1,\ldots,i-1]$'s patterns as interference.

Suppose we are given a interference probability vector $\mathbf{p}^I \in \mathcal{P}^{N_s}$ which is stationary over the time slot, and $\mathcal{P}^{N_s}$ denotes the unit (probability) simplex such that $\sum_{i=1}^{N_s} \mathbf{p}_i^I = 1$, $\mathbf{p}_i^I$ denotes the i-th entry of $\mathbf{p}^I$, and the probability of the index of each interference subcarrier is independent and identically distributed (i.i.d.). Unlike the known interference pattern case in Algorithm 1, the FH design criterion in (6) is now changed to minimizing the maximum expected number of hits with interference-plus-collision probability $\mathbf{p}^{I+C}$:

$$\underset{\{X_1,\ldots,X_{N_u}\}}{\operatorname{argmin}} \max_i E[N_{\text{hit},i}] = \underset{\{X_1,\ldots,X_{N_u}\}}{\operatorname{argmin}} \max_i \langle \mathbf{e}_i, \mathbf{p}^{I+C} \rangle, \quad (7)$$

where $\langle \cdot,\cdot \rangle$ denotes the vector inner product, $\mathbf{e}_i \in \{0,1\}^{N_s}$ denotes a one-hot vector with 1 at the i-th entry, and the interference-plus-collision probability $\mathbf{p}^{I+C}$ which will be discussed in below.

At the n-th FH interval, we initialize the empirical probability of interference-plus-collision as $\mathbf{p}_{j,i,n}^{I+C} = \mathbf{p}^I$. Unlike the sequential UE assignment in Step 8 of Algorithm 1, if the UE assignment is conducted sequentially based on the criterion in (7), the same FH pattern will be repeatedly assigned at every hop interval. To ensure the randomness of FH patterns, the UE assignment order requires permutation for every FH interval. Algorithm 2 depicts the proposed sequential procedure based on the interference statistics. At every time interval, we re-generate a permutation set $\mathcal{M}$ and assign the pattern sequentially according to the permutation set $\mathcal{M}$. At the UE i's FH pattern allocation, the empirical probability of interference-plus-collision for subcarrier f_j is computed by counting the number of occupancies of the subcarrier f_j as

$$\begin{aligned}
\mathbf{p}_{j,i,n}^{I+C} &= \frac{\sum_{l=1}^{N_{\text{Inf}}} \Pr\left(X_{\text{Inf},l}[n] = f_j\right) + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_{i'}[n]=f_j\}}}{N_{\text{Inf}} + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_{i'}[n]\neq f_{\text{null}}\}}} \\
&\overset{(a)}{=} \frac{N_{\text{Inf}}\mathbf{p}_j^I + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_i[n]=f_j\}}}{N_{\text{Inf}} + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_{i'}[n]\neq f_{\text{null}}\}}} \\
&= \left(\frac{N_{\text{Inf}} + \sum_{i'=1}^{i-2} \mathbb{1}_{\{X_{i'}[n]\neq f_{\text{null}}\}}}{N_{\text{Inf}} + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_{i'}[n]\neq f_{\text{null}}\}}}\right) \mathbf{p}_{j,i-1,n}^{I+C} \\
&\quad + \underbrace{\left(\frac{\mathbb{1}_{\{X_{i-1}[n]\neq f_{\text{null}}\}}}{N_{\text{Inf}} + \sum_{i'=1}^{i-1} \mathbb{1}_{\{X_{i'}[n]\neq f_{\text{null}}\}}}\right)}_{\triangleq \Phi_{i,n}} \mathbb{1}_{\{X_{i-1}[n]=f_j\}} \\
&= (1-\Phi_{i,n})\, \mathbf{p}_{j,i-1,n}^{I+C} + \Phi_{i,n} \mathbb{1}_{\{X_{i-1}[n]=f_j\}} \quad (8)
\end{aligned}$$

where (a) is due to the i.i.d. interference assumption. At each UE i's pattern assignment, we first compute the probability in (8) via Steps 11-13 of Algorithm 2. To satisfy the criterion in (7) sequentially, the UE i's FH pattern is computed by finding the index of the minimum entry in the probability of interference-plus-collision vector $\mathbf{p}_{j,i,n}^{I+C}$, i.e., $X_i[n] = \operatorname{argmin}_j \langle \mathbf{e}_j, \mathbf{p}_{:,i,n}^{I+C} \rangle$ in Step 15 of Algorithm 2. After UE i's FH pattern $X_i[n]$ is found, we update the $\mathbf{p}_{j,i,n}^{I+C}$ in Steps 11-13 and solve the UE $(i+1)$'s FH pattern in Step 15. The greedy approach applied in Algorithm 2 reduces the total computation complexity to $\mathcal{O}(N_h N_u N_s)$.

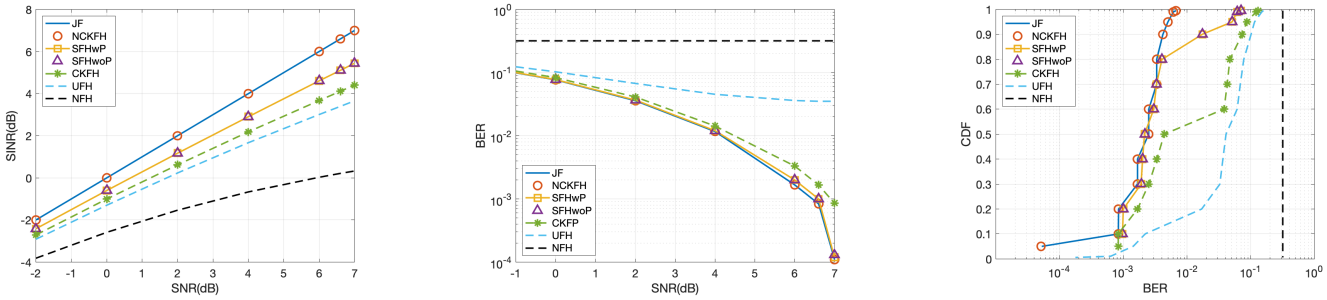
Algorithm 2 Procedures of FH pattern assignment under interference statistical

1: **Input**
2: $\quad \mathbf{p}^I \in \mathcal{P}^{N_s+1}$ interference pmf vector
3: **Output**
4: $\quad \{X_i \in \mathcal{F}^{N_h} | i = 1,\ldots,N_u\}$ UEs' FH pattern
5: **for** $n = 1,\ldots,N_h$ **do**
6: $\quad \Phi_{1,n} \leftarrow N_{\text{Inf}}^{-1}$
7: $\quad \mathbf{p}_{:,1,n}^{I+C} \leftarrow \mathbf{p}^I$
8: $\quad \mathcal{M} \leftarrow \text{perm}\left(\{1,\ldots,N_u\}\right)$
9: $\quad$ **for** $i \in \mathcal{M}$ **do**
10: $\quad\quad$ **if** $i \geq 2$ **then**
11: $\quad\quad\quad \Phi_{i,n} \leftarrow \left(\Phi_{i-1,n}^{-1} + \mathbb{1}_{\{X_{i-1}[n]\neq f_{\text{null}}\}}\right)^{-1}$
12: $\quad\quad\quad \mathbf{p}_{:,i,n}^{I+C} \leftarrow \mathbf{p}_{:,i-1,n}^{I+C}$
13: $\quad\quad\quad \mathbf{p}_{:,i,n}^{I+C} \leftarrow (1-\Phi_{i,n})\, \mathbf{p}_{:,i,n}^{I+C} + \Phi_{i,n} \mathbb{1}_{\{X_{i-1}[n]=f_j\}}$
14: $\quad\quad$ **end if**
15: $\quad\quad X_i[n] \leftarrow \underset{1\leq j\leq N_s}{\operatorname{argmin}} \mathbf{p}_{j,i,n}^{I+C}$
16: $\quad$ **end for**
17: **end for**

IV. Simulation Studies

In this section, Simulations evaluate Algorithms 1 and 2, comparing their performance with a uniform FH scheme used in existing PTW systems [10]. Each curve is based on 10,000 Monte Carlo iterations. We chose the 5G NR resource block numerology $\mu = 1$ corresponding to the subcarrier spacing $\Delta f = 30$ kHz, and set the bandwidth $B = 50$ MHz with the number of usable subcarriers $N_s = 1620$. The slot time is set to 0.5 ms and each slot time contains $N_h = 14$ OFDM symbols. The number of UEs is set to $N_u = 3032$ and the number of interference subcarriers is set to $N_{\text{Inf}} = 512$. The indices of interference subcarriers follow i.i.d. truncated-Gaussian distribution with a mean of 810 (i.e., the center subcarrier) and a standard deviation of 128.

We compare our proposed statistical FH pattern design (Algorithm 2) with the following benchmarking schemes: (i) **Interference Free (IF)** refers to zero interference case which reveals the best performance; (ii) **Non-causally-known FH (NCKFH)** pattern represents the scenario in Algorithm 1 where the interference pattern is known in the current time slot; (iii) **Causally-known FH (CKFH)** pattern represents the scenario in Algorithm 1 where the interference pattern of the



(a) SINR of the best 95% UEs (b) BER of the best 40% UEs (c) CDF of BER at SNR 6 dB

Figure 2: Comparisons of different FH schemes.

previous time slot is only known; (iv) **Uniform FH (UFH)** pattern indicates the uniform FH [10]; and (v) **No FH (NFH)** stands for the case without FH.

For our proposed FH pattern design scheme, we consider two scenarios: (i) **Statistical FH with prior (SFHwP)** refers to the statistical FH pattern designed with the true interference probability $\mathbf{p}^I$ in Algorithm 2 and (ii) **Statistical FH without prior (SFHwoP)** refers to the statistical FH pattern designed without true Interference probability and the $\mathbf{p}^I$ is replaced by an empirical interference probability $\hat{\mathbf{p}}^I$ in Algorithm 2. In case (ii), Algorithm 2 needs an extra step to update the empirical interference probability vector $\hat{\mathbf{p}}^I$ at every time slot which is low complexity.

Fig. 2 evaluates the performance of the proposed SFHwP and SFHwoP that are compared with the benchmarking schemes. Fig. 2a shows that the proposed SFHwP and SFHwoP converge to each other, which happens because the empirical interference probability of SFHwoP readily converges to the true probability with the number of iterations. The benchmarking scheme NCKFH in Algorithm 1 has zero interference and thus, overlaps with JF. The CKFH (Algorithm 1) suffers higher interference than SFHwoP (Algorithm 2) as using interference probability is more effective than just using the interference pattern from the previous time slot. Both Algorithms 1 and 2 have better interference mitigation capabilities than UFH because UFH does not exploit any interference information.

Fig. 2b shows the BER performance across different SNR values. All FH schemes show similar BER performance except for the UFH scheme for the best 40% of UEs. This again confirms that the interference information helps to improve the FH performance. Fig. 2c demonstrates the CDF of the BER performance. It is observed that our proposed SFHwP and SFHwoP perform closely to the JF curve for above 80% of UEs. The NFH curve indicates the lower bound performance at which the BER approaches the hit probability (0.3) as the SNR increases. The results demonstrate the efficacy of our FH pattern design using interference statistics (Algorithm 2).

V. Conclusion

We investigated the FH pattern design problem that can be used for 5G NR UEs in the presence of malicious interferers. Firstly, we demonstrated that minimizing the number of hits is a tractable criterion that allows low complexity algorithms. We analytically showed that it is on par with the max-min-SINR criterion. Then, we proposed two FH schemes leveraging the knowledge of interference. The first scheme utilizes known interference patterns to design a set of FH patterns that are immune to interference. The second scheme leverages interference statistics and minimizes the expected number of hits by interferers. Simulation results demonstrated the efficacy of the proposed schemes, which outperform the uniform FH scheme and achieve near-optimal performance.

References

[1] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[2] 3GPP, "5G; NR; Physical layer procedures for control (3GPP TS 38.213 version 17.4.0 Release 17)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.213, 01 2023, version 17.4.0.

[3] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmWave grant-free IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 658–670, 2020.

[4] S.-D. Wang, H.-M. Wang, C. Feng, and V. C. Leung, "Sequential anomaly detection against demodulation reference signal spoofing in 5G NR," *IEEE Transactions on Vehicular Technology*, 2022.

[5] 3GPP, "5G; NR; Physical channels and modulation (3GPP TS 38.211 version 17.4.0 Release 17) ," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211, 01 2023, version 17.4.0.

[6] F. Girke, F. Kurtz, N. Dorsch, and C. Wietfeld, "Towards resilient 5G: Lessons learned from experimental evaluations of lte uplink jamming," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019, pp. 1–6.

[7] R. M. Rao, S. Ha, V. Marojevic, and J. H. Reed, "LTE PHY layer vulnerability analysis and testing using open-source SDR tools," in *IEEE Military Communications Conference (MILCOM)*, 2017, pp. 744–749.

[8] Q. Wang, T. Nguyen, K. Pham, and H. Kwon, "Mitigating jamming attack: A game-theoretic perspective," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6063–6074, 2018.

[9] M. Hannon, S. Feng, H. Kwon, and K. Pham, "Jamming statistics-dependent frequency hopping," in *IEEE Military Communications Conference (MILCOM)*, 2016, pp. 138–143.

[10] T. C. Royster and J. Streitman, "Performance considerations for protected wideband satcom," in *MILCOM 2015-2015 IEEE Military Communications Conference*. IEEE, 2015, pp. 175–180.

[11] G. Xiong, T. Kim, D. J. Love, and E. Perrins, "Optimality conditions of performance-guaranteed power minimization in mimo networks: A distributed algorithm and its feasibility," *IEEE Transactions on Signal Processing*, vol. 69, pp. 119–135, 2021.