

Article

Iterative List Patterned Reed-Muller Projection Detection-Based Packetized Unsourced Massive Random Access

Wenjiao Xie ^{1,*} , Runhe Tian ²  and Huisheng Zhang ¹

¹ School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710129, China; zhanghuisheng@nwpu.edu.cn

² Department of Architecture and Built Environment, University of Nottingham, Nottingham NG7 2RD, UK; runhe.tian@nottingham.ac.uk

* Correspondence: jiao89825@mail.nwpu.edu.cn

Abstract: In this paper, we consider a slot-controlled coded compressed sensing protocol for unsourced massive random access (URA) that concatenates a shared patterned Reed–Muller (PRM) inner codebook to an outer error-correction code. Due to the limitations of the geometry-based decoding algorithm in single-sequence settings and due to the message interference that may result in decreased decoding performance under multi-sequence circumstances, a list PRM projection algorithm and an iterative list PRM projection algorithm are proposed to supplant the signal detector associated with the inner PRM sequences in this paper. In detail, we first propose an enhanced path-saving algorithm, called list PRM projection detection, for use in single-user scenarios that maintains multiple candidates during the first few layers so as to remedy the risk of spreading errors. On this basis, we further propose an iterative list PRM projection algorithm for use in multi-user scenarios. The vectors for PRM codes and channel coefficients are jointly detected in an iterative manner, which offers significant improvements regarding the convergence rate for signal recovery. Furthermore, the performances of the proposed algorithms are analyzed mathematically, and we verify that the theoretical simulations are consistent with the numerical simulations. Finally, we concatenate the inner PRM codes that employ iterative list detection in two practical error-correction outer codes. According to the simulation results, we conclude that the packetized URA with the proposed iterative list projection detection works better than benchmarks in terms of the number of active users it can support in each slot and the amount of energy needed per bit to meet an expected error probability.

Keywords: machine-to-machine communications; complex Reed-Muller codes; unsourced massive random access; error correction code



Citation: Xie, W.; Tian, R.; Zhang, H. Iterative List Patterned Reed-Muller Projection Detection-Based Packetized Unsourced Massive Random Access. *Sensors* **2023**, *23*, 6596. <https://doi.org/10.3390/s23146596>

Academic Editors: Khaled Rabie, Wali Ullah Khan and Belal Alsinglawi

Received: 12 June 2023
Revised: 19 July 2023
Accepted: 19 July 2023
Published: 21 July 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

One of the most prominent uses for 6G wireless networks remains massive machine-type communication's (mMTC+) continuous evolution [1]. Indeed, mMTC+ services feature the presence of a large number of machines that sporadically link to the system while carrying short data packets. Notably, they are battery-limited and are intended to achieve low transmission latency [2–4].

Grant-free transmission [5,6], in which packets are transmitted to the network without informing the base station in advance, is the approach that provides the most promise. “Sourced Random Access” [7] uses grant-free transmission and allocates distinct dictionaries to different users.

Given that there are so many users, employing various encoders would complicate reception since the decoder would first have to determine which encoders were being used. Therefore, using the same coding technique for all users is the most promising strategy. These systems are referred to as “Unsourced Random Access (URA)” [8]. In this way, the identification and decoding responsibilities are decoupled, and the URA receiver only needs to decode the messages without knowing who sent them. A comparison of

uncoordinated/unsourced grant-free schemes and coordinated/sourced grant-free (based on compressed sensing technique) schemes in terms of application scenarios, typical access performance, and their characteristics is shown in Table 1. All active users' per-user probability of error (PUPE) is used to examine the access and transmission performance of the entire system.

Table 1. Uncoordinated/unsourced grant-free vs. coordinated/sourced grant-free (based on compressed sensing technique).

Schemes	Application Scenarios	Typical Access Performance	Advantages and Disadvantages
Uncoordinated/unsourced grant-free [8]	Providing complete data transfer for active users in a large-scale random access environment	It is possible to achieve a BER of 0.05 using 30,000 channels, a 3 dB SNR, and 200 active users	Advantages: can support a large number of total users, does not need user identity recovery process, and is suitable for low latency transmission scenarios Disadvantages: no pilot sequence, hard to estimate the channel estimations, and high complexity of decoders
Coordinated/sourced grant-Free based on Compressed sensing technique [9–12]	Providing active user identity detection and channel estimation in a large-scale random access environment	Using a pilot sequence of length-800, an SNR of 3 dB, and a setup of 40,000 users, it is possible to achieve a BER of 0.0125	Advantage: can jointly recover users' ID and their channel estimations Disadvantages: the overhead of the pilot sequence is large, and the total number of supported users is constrained by the length of the pilot sequence

The fundamental limits of the Gaussian multiple-access channel are described in Reference [8], which formulates the URA problem from an information-theoretic perspective. Based on Reference [8], an asymptotic improvement is presented in Reference [13]. Both examine a scenario in which the receiver has a fixed count of active users. These findings are expanded in Reference [14] to a case in which the receiver's active user count is arbitrary and unknowable. For the Gaussian multiple-access channel, a range of low-complexity URA algorithms has been suggested. The main schemes are T -fold irregular repetition (which includes the T -fold irregular repetition slotted ALOHA protocol with collision detection [15,16]), the sparse interleave division multiple access (IDMA) scheme [17], random spreading and correlation-based energy detection [18,19], as well as the coded compressed sensing (CCS)-based URA scheme [20]. Coded compressed sensing is a divide-and-conquer strategy that concatenates the inner codes to outer A-channel codes, where a tree code is a specific instance of an outer A-channel code devised for this kind of application [21,22]. This makes it simple to accommodate novel channel models owing to the concatenated form's adaptability to URA. Several later investigations on URA employed an outer A-channel code [23–28]. In paper [29], the study scope of a tree code behaving as the outer A-channel code is extended through the integration of the approximate message passing (AMP) mechanism with sparse regression codes [20]. The coded compressed sensing approach is further enhanced in Reference [23] by enabling the inner AMP decoder and the outer tree decoder to communicate soft information through a common message-passing protocol. In order to simplify the high-dimensional sparse signals' joint detection pertaining to several bases, the research work in Reference [30] suggests a coded demixing method.

Compressed sensing has made extensive use of codebook construction techniques related to second-order Reed–Muller (RM) sequences [31]. RM sequences are excellent options for massive access scenarios during the continuous evolution of massive machine-

type communication owing to their high capacity and capability for low-complexity random access [32].

In Reference [33], non-orthogonal Reed–Muller sequences are used as user identifiers (IDs) for active user identification in the grant-based access mechanism in mMTC+, which has low access potency and high signaling expenses. In Reference [34], a strategy for massive random access is proposed that makes use of the nested characteristics of RM codes. Additionally, the coded compressed sensing scheme makes extensive use of inner codebook construction techniques related to second-order RM sequences [35,36], i.e., RM sequences are utilized as inner codes for the CCS protocol, and the outer tree codes are employed for coupling messages for slotted transmissions. In Reference [37], a shared patterned Reed–Muller (PRM) codebook that embeds zero patterns in the second-order RM codes according to a binary vector space partition principle is employed as the inner codebook for the coded compressed sensing protocol.

This paper is inspired by a slot-controlled CCS protocol that concatenates outer error-correction codes to a common PRM inner codebook [37]. In this scheme, a slot-pattern-control (SPC) criterion that corresponds one-to-one to an information segment to construct the slot occupation guideline for each active user. The users' messages are partitioned into several sub-blocks and add the same SPC segment in each block as a prefix to make up the input signal of the inner encoder. On this basis, each sequence is related to a single codeword from a proposed common codebook called patterned Reed–Muller codes. For recovering the PRM sequences received at the receiver, an algorithm exploiting the geometry of PRM sequences is proposed. Moreover, the outer tree code is replaced with an error-correcting code, and codewords with a distance at most t from the channel output are recovered by outer codes. In view of this scheme, it is anticipated that there is a potential rise in the efficiency of the PRM sequence-related geometry-based decoding algorithm for single-sequence scenarios due to the limited number of active users that can be served over a slot. In addition, message interference may also lead to a decreased decoding efficiency in multi-sequence scenarios. In view of these shortcomings, we replace the inner decoder related to PRM with a proposed list PRM projection algorithm to enhance the efficiency of the inner decoder for a single sequence. Additionally, we construct an iterative list PRM projection algorithm in order to decrease the multi-interference between sequences for the multi-sequence scenario. We then deduce the theoretically successful detection probabilities of the proposed algorithm and validate its correctness via numerical simulations. Subsequently, we demonstrate that the proposed schemes can accommodate more active users within each slot using numerical simulations. We finally assess the performance of the slot-controlled URA system with the proposed iterative list algorithm as the inner code detector. According to simulation results, we demonstrate that the schemes using the proposed detection can help improve the overall system's performance.

1.1. Contributions and Arrangement

Here is a summary the contributions of this article:

- A shared PRM codebook that embeds zero patterns in the second-order RM codes according to a binary vector space partition principle is employed as the inner codebook for the coded compressed sensing protocol. On this basis, we propose an enhanced algorithm called the "list PRM projection algorithm" that uses a list of candidates to hinder error spreading in each detection layer.
- As for the multi-sequence scenario, an iterative list PRM projection algorithm is proposed. More specifically, except for the user's information during the current loop, we consider all signals as interference. We remove the interference in priority and then employ the proposed list projection algorithm to recover the PRM sequence. The PRM estimations are then inserted into the channel estimator to enhance precision. After that, the modified channel estimations are utilized in the subsequent iteration to improve PRM detection further. As a result, the proposed iterative list PRM projection algorithm offers significant advantages regarding the convergence rate.

- The theoretical successful detection probabilities of the proposed list projection and the iterative list projection algorithms are analyzed mathematically, and the results demonstrate that: (i) The factors that affect the efficiency of the list PRM projection algorithm are shown in the simulation results, which validate that the recovery reliability of the first few layers is crucial to the whole performance; (ii) Simulation results further explore the effect of the relationship between rank Y and m for PRM sequence properties on the theoretical successful detection probability; (iii) We verified that the theoretical results are consistent with the simulation results.
- We substitute the inner decoder of the scheme [37] with the proposed iterative list PRM projection algorithm. Simulations of the quasi-static Rayleigh fading multiple-access channel (MAC) are performed numerically, and we conclude the observations as follows: (i) The proposed scheme is superior to the OMP-based inner codes detection, i.e., the chance of successful recovery is significantly improved since the PRM detector and channel estimator share information, and the negative impacts can be further reduced by eliminating those sequences that are incorrectly detected in each operation. (ii) By increasing the count of candidates in the first few layers, we can boost the original PRM projection algorithm's performance, which further confirms the above proof of the importance of ensuring the reliable recovery of the first few layers. (iii) The simulation results of the overall URA system confirm that the packetized URA with the proposed iterative list projection detection method works better than benchmarks in terms of the number of active users it can support in each slot and the amount of energy needed per bit to meet an expected error probability.

The rest of this paper is arranged as follows: In Section 2, we induce the system model and review the patterned Reed–Muller sequences as well as their projection algorithm. An enhanced list PRM projection algorithm and an iterative list PRM projection algorithm are proposed in Section 3. The theoretical probability of the algorithms proposed is derived in Section 4. The simulation results are presented in Section 5, and the paper is concluded in Section 6.

1.2. Conventions

It is stipulated that all vectors, whether complex or binary, will be column vectors. We employ \mathbb{F}_2^m to present the finite (binary) field in this paper. \mathbf{P}_m denotes the size of an $m \times m$ matrix.

\mathbf{P}^T stands for the transpose of matrix \mathbf{P} and \mathbf{P}^{-T} stands for the inverse transpose of matrix \mathbf{P} . The superscript H stands for the conjugate transpose of a matrix. Vectors $\mathbf{0}_N$ and $\mathbf{1}_N$ are all-zero and all-one vectors of size $N \times 1$, respectively. We use $\mathbf{A} = [a_i]_{i=1}^I$ to stand for a vector whose capacity is I , consisting of the components a_i ($i = 1, \dots, I$). The vectors $\mathbf{B}_1 \in \mathbb{C}^{T_1 \times 1}$ and $\mathbf{B}_2 \in \mathbb{C}^{T_2 \times 1}$ are added together to produce $\mathbf{B} = [\mathbf{B}_1; \mathbf{B}_2] \in \mathbb{C}^{(T_1+T_2) \times 1}$. $\mathcal{CN}(0, \mathbf{I}_N)$ stands for a complex standard normal random vector. The notation $x \sim \mathcal{N}(\mu, \sigma^2)$ indicates that x is a Gaussian random variable whose mean is μ and variance is σ^2 ; its probability density function (PDF) is written as $f_{\mathcal{N}}(x; \mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$, while $x \sim \mathcal{CN}(\mu, \sigma^2)$ denotes that the random variable x follows the circular symmetric complex Gaussian distribution with its PDF being $f_{\mathcal{CN}}(x; \mu, \sigma^2) = \frac{1}{\pi\sigma^2} \exp\left(-\frac{|x-\mu|^2}{\sigma^2}\right)$.

2. System Model

In this section, we first review the studies of the slot-controlled URA scheme in Reference [37] and then propose an enhanced slot-controlled URA scheme. In the scheme, each active user partitions the message into several sub-blocks and repeatedly adds a slot-pattern-controlled (SPC) sequence as a prefix to form an outer encoder input signal. Then, error correction encoding is employed to stitch the message through all sub-blocks. A geometry-based technique is employed to detect the sub-blocks transmitted by active users in all sub-slots, and an error correction algorithm stitches these sub-blocks in order to recover the original messages.

2.1. Encoding Process

The transmission strategy includes two encoders: an inner-code encoder and an error-correction code/outer-code encoder. The error-correction code encoder uses two practical outer A-channel codes, i.e., the t-tree code and the Reed—Solomon code with Guruswami—Sudan list decoding. The inner encoder maps each sub-block into a codeword in the common PRM codebook.

As for the transmitter of practical transmission, a B -bit message is carried by each active user as part of the set $\{W_1, W_2, \dots, W_{K_a}\}$ for accessing the system. We let $\mathcal{N} = 2^B$, and each message W_k ($1 \leq k \leq K_a$) is encoded into an H_N -length outer error-correction code, thus $W_k \in [\mathcal{N}]$, where $[\mathcal{N}] = \{1, \dots, \mathcal{N}\}$. The A-channel code used for the outer encoding is derived from paper [27]: the k th user's message $\mathbf{U}^{(k)}$ of length B is mapped to a J -ary Reed—Solomon code of length H_N , designated $[\mathcal{M}_{RS,h}^{(k)}]_{h=1}^{H_N} = (M_{RS,1}^{(k)}, M_{RS,2}^{(k)}, \dots, M_{RS,H_N}^{(k)}) \in [J]^{H_N}$, $0 \leq h \leq H_N$. We then repeatedly append the binary prefix sequence $\mathbf{X}_p^{(k)}$ to each J -ary bit $M_{RS,h}^{(k)}$ to create the G -ary sequence. Thus, the length of the binary sequence $\mathbf{X}_p^{(k)}$ is set to $\log_2(G/J)$ and we denote $x_p = \log_2(G/J)$. For further interpretation, a G -ary bit is divided into 2^{x_p} cosets, each containing 2^J components, and this process can be summarized as $\check{\mathbf{m}}_{PRM,h}^{(k)} = F([\mathbf{X}_p^{(k)}; M_{RS,h}^{(k)}])$, where $F(\cdot)$ is the bijective mapping: $F(\cdot) : [2^{x_p}] \times [J]$ and $\check{\mathbf{m}}_{PRM,h}^{(k)} \in G$. By repeating the above processes H_N times, an H_N -length sequence $[\check{\mathbf{m}}_{PRM,h}^{(k)}]_{h=1}^{H_N} = (\check{\mathbf{m}}_{PRM,1}^{(k)}, \check{\mathbf{m}}_{PRM,2}^{(k)}, \dots, \check{\mathbf{m}}_{PRM,H_N}^{(k)})$ is obtained, which serves as the input sequence for the inner encoder. We require one-to-one matching between $\check{\mathbf{m}}_{PRM}^{(k)}$ and codeword $\mathbf{C}_{PRM}^{(k)}$ from the common codebook (we omit the subscript m here for simplicity), and, herein, $\check{\mathbf{m}}_{PRM}^{(k)}$ is the input signal of the inner encoder while the output codeword is $\mathbf{C}_{PRM}^{(k)}$. Finally, the output of inner coding over H slots is recorded as $[\mathbf{C}_{PRM,h}^{(k)}]_{h=1}^{H_N} = (\mathbf{C}_{PRM,1}^{(k)}, \mathbf{C}_{PRM,2}^{(k)}, \dots, \mathbf{C}_{PRM,H_N}^{(k)})$. This process of the transmitter is depicted in Figure 1. In detail, a length- $N = 2^m$ sequence $\mathbf{C}_{PRM,h}^{(k)}$ represents an inner PRM code randomly picked from a shared codebook Γ that is sent by the k -th user within the n -th chunk, where $1 \leq n \leq H_N$. There is a one-to-one match between the sequence $\mathbf{C}_{PRM,h}^{(k)}$ and a partitioned message of length B/H_N . Next, using the slot-pattern-control rule, the H_N PRM sequences are arranged into N_T chunks, which leads to the system employing $T = N \cdot N_T$ channel uses to operate a slotted-controlled transmission.

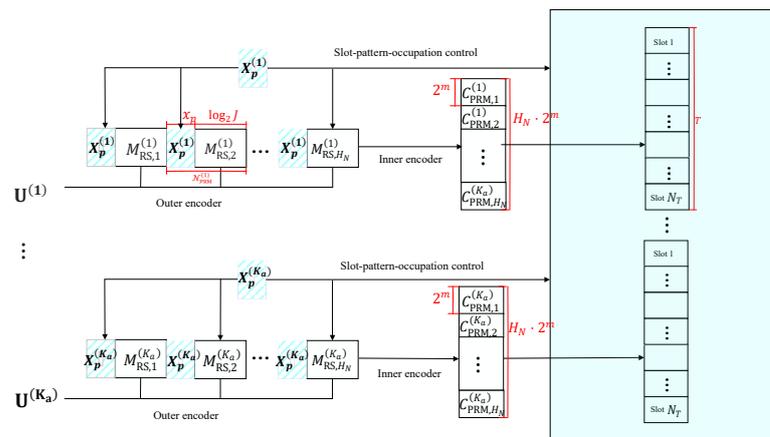


Figure 1. The procedures of the transmitter for the slot-control URA.

The inner codeword in the h -th slot $\mathbf{C}_{PRM,h}^{(k)}$ is derived as follows: a new version of the binary subspace chirp (BSSC) [38–40], which embeds zero patterns in the second-order RM codes according to the partition rule of the binary vector space, is proposed by reducing the subspace matrix \mathbf{H}_χ to \mathbf{I}_χ , where $\chi \subseteq [m]$ indicates all possible subsets of rank

$Y \in \{1, 2, \dots, m\}$ under full dimension m . The simplified sequence is denoted as patterned Reed–Muller (PRM) and can be written as follows

$$\mathbf{C}_{\text{PRM},h}^{(k)}(\mathbf{v}) = \begin{cases} \frac{1}{\sqrt{2^Y}} i^{2\mathbf{w}^T \mathbf{B}|_1^Y + \mathbf{w}^T \hat{\mathbf{P}} \mathbf{w}}, & \text{if } \mathbf{v} = \mathbf{I}_\chi \mathbf{w} + \tilde{\mathbf{I}}_\chi \mathbf{B}|_{Y+1}^m, \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

where $\mathbf{w} \in \mathbb{F}_2^Y$, symmetric matrix $\hat{\mathbf{P}}$ and vector \mathbf{B} are dominant parameters for $\text{RM}(Y, 2)$; additionally, sub-vector $\mathbf{B}|_{Y+1}^m$ identifies the sequence of the last $(m - Y)$ -bit segment of the m -length vector \mathbf{B} , and subspace \mathbf{I}_χ is a matrix of size $(m \times Y)$ with column vectors $\mathbf{e}_{\chi(1)}, \mathbf{e}_{\chi(2)}, \dots, \mathbf{e}_{\chi(Y)}$, where $\mathbf{e}_{\chi(r)}$ is the unit vector with non-zero at the r -th position, $1 \leq r \leq Y$. Similarly, matrix $\tilde{\mathbf{I}}_\chi$ follows the same rule.

2.2. Decoding Process

The signal received in the receiver for the n -th slot ($1 \leq n \leq N_T$) is expressed as

$$\mathbf{y}_n = \sum_{k=1}^{K_a} h_{k,n} \cdot \mathbf{x}_{k,n} + \mathbf{n}_n, \quad (2)$$

where $h_{k,n} \sim \mathcal{CN}(0, 1)$ represents a constant channel coefficient that is supposed to be stable for the duration of a user's transmission between the active user k and the access point (AP) in n -th chunk. While, $\mathbf{n}_n \sim \mathcal{CN}(0, \mathbf{I}_N)$ is the complex additive white Gaussian noise (AWGN). For the inner-code decoder: PRM codes have their geometry property: for any $\mathbf{z} \in \mathbb{F}_2^{m-Y}$, the PRM sequence satisfies

$$\mathbf{E} \left(\mathbf{I}_\chi \mathbf{e}_\tau, \tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_\tau \right) \cdot \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} = (-1)^{\mathbf{B}^T (\mathbf{e}_\tau; \mathbf{0}^{m-Y}) + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}} \cdot \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}, \quad (3)$$

where $\hat{\mathbf{P}}_\tau = \hat{\mathbf{P}} \mathbf{e}_\tau$. According to Equation (3), the PRM sequence obtains its specific projective property by letting $\mathbf{z} = \mathbf{0}^{m-Y}$:

$$\lambda_{\text{PRM}, \omega}^{(\tau)}(\mathbf{0}^{m-Y}) \cdot \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} = \begin{cases} \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} & \text{if } \omega = (-1)^{B_\tau}, \\ 0, & \text{if } \omega \neq (-1)^{B_\tau}, \end{cases} \quad (4)$$

where

$$\lambda_{\text{PRM}, \omega}^{(\tau)}(\mathbf{0}^{m-Y}) = \frac{\left[\mathbf{I}_N + \omega \cdot \mathbf{E} \left(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{I}_\chi \hat{\mathbf{P}}_\tau \right) \right]}{2} \quad (5)$$

is a projection operator for PRM sequences. We decode the inner code using the OMP and the projective-based algorithm. Owing to the slot-controlled URA, the inner-code sequence based on projective property and the channel estimations are recovered sequentially. For the outer-decoding process, the number of output codewords is equivalent to the count of decoding iterations K_0 . The outer Reed–Solomon decoding process is suggested. The efficiency of the method described above can be improved using a modified version based on list decoding, which will be described in the next part.

We assess performance from the perspective of messages and use the miss-detection rate (MDR) and the false-alarm rate (FAR) as the primary indicators, which are given as

$$P_e \triangleq \frac{1}{K_a} \sum_{k \in \mathcal{K}_a} \Pr[W_k \notin \hat{\mathcal{D}}(\mathcal{Y})] \quad (6)$$

and

$$P_f \triangleq \Pr[\hat{\mathcal{D}}(\mathcal{Y}) \setminus \{W_k | k \in \mathcal{K}_a\} \neq \emptyset], \quad (7)$$

respectively, where $\mathcal{K}_a = \{1, \dots, K_a\}$.

3. Iterative List PRM Projection Algorithm-Based Inner-Code Detector

Our proposed detection scheme for inner codes is described in this section. In addition to the modified list PRM projection detection adopted for a single sequence, we propose an iterative list PRM projection algorithm implemented at the AP for multiple sequences.

3.1. List PRM Projection Algorithm

The received signal is $\mathbf{y} = \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{n}$, and the enhanced algorithm based on the detection proposed in Reference [37] is executed for the single-user scenario. Specifically, in this single-user scenario, we propose a modified algorithm that utilizes a candidate-saving technique during each layer of detection to boost performance. Algorithm 1's particular processes are outlined in the following section.

Three elements $\{\mathbf{I}_\chi, \hat{\mathbf{P}}, \mathbf{B}\}$ of the PRM sequence need to be recovered, and the subspace matrix \mathbf{I}_χ should be retrieved first. Since the rank is unknown, we go over every conceivable rank in $1 \leq Y \leq m$ and set aside L potential subspace matrices for each one (in Lines 3 and 4) after we calculate $F_{\text{sum}}(\mathbf{f}_{\chi(Y)}) = \sum_{j=1}^{2^{(m-Y)}} \left| \mathbf{y}^H \mathbf{E}(\mathbf{0}, \mathbf{f}_{\chi(Y)}^{(j)}) \mathbf{y} \right|$ for every $\mathbf{f}_{\chi(Y)}^{(j)} \in \mathbb{F}_2^m$, employ the relation of $\left[\mathbf{f}_{\chi(Y)}^{(j)} \right]_{j=1}^{2^{(m-Y)}} = \text{span}(\tilde{\mathbf{I}}_{\chi(Y)})$ and seek the biggest $2^{(m-Y)}$ estimations of F_{sum} , the set $\left[\mathbf{f}_{\chi(Y)}^{(j)} \right]_{j=1}^{2^{(m-Y)}}$ and the subspace matrix $\tilde{\mathbf{I}}_{\chi(Y)}$ can be identified. We finally keep L candidates as $\mathcal{I}_{\chi(Y)} = \left\{ \left[\tilde{\mathbf{I}}_{\chi(Y)}^{(l)} \right]_{l=1}^L, Y \right\}$.

The recovery of remaining elements $\{\hat{\mathbf{P}}, \mathbf{B}\}$ depends on the subspaces in $\mathcal{I}_{\chi(Y)}$. In the following, we will decode the vector $\hat{\mathbf{P}}_l$ and bit \mathbf{B}_l in a layer-by-layer manner. Furthermore, we will keep H parent candidates for the next layer at the end of each iteration. We initialize the corresponding parameters in Line 6; we denote the list of updated symmetric matrix and vector (under $\tilde{\mathbf{I}}_{\chi(Y)}^{(l)}$) as \mathcal{H}_l during each layer, and update the list of search space as $\left[\mathcal{F}_{l,1}^{(h)} \right]_{h=1}^H$ using (6). During the iteration, as for each candidate derived from the previous layers, we obtain a list of H candidates for the current layer (in Lines 8–11); we first update the search space from the previous knowledge using (6) (in Lines 6 and 19). The detected layers notated as \mathcal{R} ($\mathcal{R} = 1, \dots, \tau - 1$) and utilize the recovered vector $\hat{\mathbf{P}}_{\tau,l}^{(h)}$ ($\hat{\mathbf{P}}_{\tau,l}^{(h)}$ is h -th candidates for τ -th column vector of $\hat{\mathbf{P}}$ under subspace $\mathbf{I}_{\chi(Y)}^{(l)}$) to fill out the symmetric matrix; thus, the matrix under the τ -th layer can be represented as $\hat{\mathbf{P}}_{\mathcal{R}}^{(h)}$. On this basis, the search space is limited to

$$\mathcal{F}_{l,\tau}^{(h)} = \left\{ \mathbf{f} \in \mathbb{F}_2^m \mid \mathbf{f}_i = \hat{\mathbf{P}}_{\mathcal{R}}^{(h)}(i, \tau) \text{ for all } i \in \mathcal{R} \right\}, \quad (8)$$

where the value of $\hat{\mathbf{P}}_{\mathcal{R}}^{(h)}(i, \tau)$ refers to the i -th row and τ -th column of matrix $\hat{\mathbf{P}}_{\mathcal{R}}^{(h)}$. Next, we derive H paths for each candidates of previous decoding (in Lines 9 and 10).

For all vectors $\mathbf{f} \in \mathcal{F}_{l,\tau}^{(h)}$, we compute $F_{\text{sum}}(\mathbf{f}) = \sum_{j=1}^{2^{(m-Y)}} \left| \mathbf{y}^H \mathbf{E}(\mathbf{I}_{\chi(Y)}^{(l)} \cdot \mathbf{e}_\tau, \mathbf{f}) \mathbf{y} \right|$ to search H largest F_{sum} , the corresponding H sets of $[\mathbf{f}_j]_{j=1}^{2^{(m-Y)}}$ are derived. Based on $[\mathbf{f}_j]_{j=1}^{2^{(m-Y)}} = \text{span}(\tilde{\mathbf{I}}_{\chi(Y)}^{(l)} + \mathbf{I}_{\chi(Y)}^{(l)} \hat{\mathbf{P}}_{\tau,l} \mathbf{e}_\tau)$, vector $\mathbf{P}_{\tau,l}^{(h)}$ can be obtained. Once 2^H iterations are complete, we finally get the $\left[\hat{\mathbf{P}}_{\tau,l}^{(h)} \right]_{h=1}^H$ within 2^H possibilities.

Algorithm 1: List PRM projection algorithm

input : $\mathbf{y} = \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{n}$ received at the AP.

output : PRM sequence $\hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}$ and its related elements $\{\mathbf{I}_\chi, \hat{\mathbf{P}}, \mathbf{B}\}$.

- 1 **for** $Y \leftarrow 1$ **to** m **do**
- 2 Initialize the L candidates of subspace matrices and their dimensions, we denote them as $\mathcal{I}_{\chi(Y)} = \left\{ \left[\mathbf{0}_{\chi(Y)}^{(i)} \right]_{l=1}^L, Y \right\}$;
- 3 Investigate $\binom{m}{Y}$ possibilities of set $\chi(Y)$. As for each $\chi(Y)$, it controls the subspace matrix $\tilde{\mathbf{I}}_{\chi(Y)}$, and the related $(m - Y)$ -dimensional subspaces are calculated via $\left[\mathbf{f}_{\chi(Y)}^{(j)} \right]_{j=1}^{2^{(m-Y)}} = \text{span}(\tilde{\mathbf{I}}_{\chi(Y)})$;
- 4 Update the L candidates with the maximum F_{sum} (within $\binom{m}{Y}$ possibilities) by substituting $\left[\mathbf{f}_{\chi(Y)}^{(j)} \right]_{j=1}^{2^{(m-Y)}}$ in $F_{\text{sum}}(\mathbf{f}_{\chi(Y)}) = \sum_{j=1}^{2^{(m-Y)}} \left| \mathbf{y}^H \mathbf{E}(\mathbf{0}, \mathbf{f}_{\chi(Y)}^{(j)}) \mathbf{y} \right|$, we denoted them as $\mathcal{I}_{\chi(Y)} = \left\{ \left[\tilde{\mathbf{I}}_{\chi(Y)}^{(l)} \right]_{l=1}^L, Y \right\}$;
- 5 **for** $\left\{ \tilde{\mathbf{I}}_{\chi(Y)}^{(l)}, Y \right\} \in \mathcal{I}_{\chi(Y)}$ **do**
- 6 Initialize the $\left[\hat{\mathbf{P}}_{1,l}^{(h)} \right]_{h=1}^H = [\mathbf{0}_{N \times 1}]^H$, $\mathcal{R} = \{1\}$, Update the List $\mathcal{H}_l = \left\{ \left[\hat{\mathbf{P}}_{\mathcal{R}}^{(h)} \right]_{h=1}^H, \left[\mathbf{B}_{1,l}^{(h)} \right]_{h=1}^H \right\} = \left\{ [\mathbf{0}_{N \times N}]^H, [0]^H \right\}$, compute $\left[\mathcal{F}_{l,1}^{(h)} \right]_{h=1}^H$ using (6);
- 7 **for** $\tau = 1, \dots, Y$ **do**
- 8 **for** $h = 1, \dots, H$ **do**
- 9 Compute $F_{\text{sum}}(\mathbf{f}) = \sum_{j=1}^{2^{(m-Y)}} \left| \mathbf{y}^{(h)H} \mathbf{E}(\mathbf{I}_{\chi(Y)}^{(l)} \cdot \mathbf{e}_\tau, \mathbf{f}) \mathbf{y}^{(h)} \right|$ for all possible $\mathbf{f} \in \mathcal{F}_{l,\tau}^{(h)}$ and save H sets of $\left[\mathbf{f}_j \right]_{j=1}^{2^{(m-Y)}}$ with largest value;
- 10 According to $\left[\mathbf{f}_j \right]_{j=1}^{2^{(m-Y)}} = \text{span}(\tilde{\mathbf{I}}_{\chi(Y)}^{(l)}) + \mathbf{I}_{\chi(Y)}^{(l)} \hat{\mathbf{P}}_{\tau,l} \mathbf{e}_\tau$ and the current $\tilde{\mathbf{I}}_{\chi(Y)}^{(l)}$, the H vectors of $\left[\mathbf{P}_\tau^{(h)} \right]_{h=1}^H$ is saved;
- 11 **end**
- 12 Sort all $\left[\mathbf{P}_\tau^{(h)} \right]_{h=1}^H$, keep the H largest vectors as $\left[\hat{\mathbf{P}}_{\tau,l}^{(h)} \right]_{h=1}^H$;
- 13 **for** $h = 1, \dots, H$ **do**
- 14 We set $\mathbf{z}^{(m-Y)} = \mathbf{0}^{m-Y}$, and calculate $F_\tau^{(h)}(\mathbf{f}) = \mathbf{y}^{(h)H} \mathbf{E}(\mathbf{I}_{\chi(Y)}^{(l)} \cdot \mathbf{e}_\tau, \mathbf{I}_{\chi(Y)}^{(l)} \hat{\mathbf{P}}_{\tau,l} \mathbf{e}_\tau) \mathbf{y}^{(h)}$, we then obtain $\omega = \text{sign}(F_\tau^{(h)}(\mathbf{f}))$;
- 15 Compute sign-bit vector $B_{\tau,l}^{(h)}$ according to (7);
- 16 The projection operator is $\lambda_{PRM,\omega}^{(\tau)}(\mathbf{0}^{m-Y}) = (\mathbf{I}_N + \omega \cdot \mathbf{E}(\mathbf{I}_{\chi(Y)}^{(l)} \mathbf{e}_\tau, \mathbf{f})) / 2$, then we have $\mathbf{y}_{\tau+1}^{(h)} = \lambda_{PRM,\omega}^{(\tau)}(\mathbf{0}^{m-Y}) \cdot \mathbf{y}^{(h)}$;
- 17 Let $\mathbf{y}^{(h)} = \mathbf{y}_{\tau+1}^{(h)}$;
- 18 **end**
- 19 Update $\left[\hat{\mathbf{P}}_{\tau,l}^{(h)} \right]_{h=1}^H, \mathbf{y}^{(h)}$ and List \mathcal{H}_l , compute $\mathcal{F}_{l,\tau+1}^{(h)}$ using (6);
- 20 **end**
- 21 Save all candidates as \mathcal{H}_l ;
- 22 **end**
- 23 Save L candidates $\mathcal{H}_1, \dots, \mathcal{H}_L$;
- 24 **end**
- 25 Denote the closest codeword to \mathbf{y} as $\hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}$;

As for the detection of $\mathbf{B}_l^{(h)}$ (in Lines 14–17), we make $\mathbf{z}^{(m-Y)} = \mathbf{0}^{m-Y}$ and compute $F_\tau(\mathbf{f}) = \mathbf{y}^H \mathbf{E} \left(\mathbf{I}_{\chi^{(Y)}}^{(l)} \cdot \mathbf{e}_\tau, \mathbf{I}_{\chi^{(Y)}}^{(l)} \hat{\mathbf{P}}_{\tau,l} \mathbf{e}_\tau \right) \mathbf{y}$, then we obtain $\text{sign}(F_\tau(\mathbf{f})) = (-1)^{B_{\tau,l}}$. In light of this, B_τ can be obtained as follows

$$B_{\tau,l} = \begin{cases} 1, & \text{if } \text{sign}(F_\tau(\mathbf{f})) = -1, \\ 0, & \text{if } \text{sign}(F_\tau(\mathbf{f})) = 1. \end{cases} \tag{9}$$

Line 19 updates all parameters for the next layer detection. In Line 23, after conducting all iterations, we evaluate each rank's ($L \times H$) results and retain the optimal results. The final results are selected at the end of the procedure for all ranks (in Line 25).

3.2. Iterative List PRM Projection Algorithm

We consider a scenario where the simultaneous presence of multiple active users in a system. As described below, we will detect multiple PRM sequences iteratively. We begin by introducing some notations in this section: it is possible to detect a maximum of K_0 users. We denote the notation $\hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(s,k)}$ as the detected PRM sequence, and $\hat{h}_k^{(s)}$ represents the channel estimation. Both notations indicate the case under the k -th user and during the s -th iteration ($1 \leq s \leq S_{max}$). The particular processes of Algorithm 2 are outlined in the following section.

Algorithm 2: Iterative List PRM projection Algorithm

input : the sequence \mathbf{y} received at receiver, the maximum count of iterations S_{max} , and the maximum detected users count K_0 .

output : the sequences send by active users $\left\{ \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(1)}, \dots, \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(K_0)} \right\}$, and the channel coefficient $\hat{\mathbf{h}}$.

1 Initialize $\hat{\mathbf{C}}^{(0)} = \left\{ \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(1)}, \dots, \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(K_0)} \right\} = \{ \mathbf{0}^N, \dots, \mathbf{0}^N \}$, and $\hat{\mathbf{h}}^{(0)} = \mathbf{0}^{K_0}$;

2 **for** $i \leftarrow 1$ **to** S_{max} **do**

3 **for** $k \leftarrow 1$ **to** K_0 **do**

4 Calculate the $\Lambda_k^{(s)}$ using (9);

5 Input the result of $(\mathbf{y} - \Lambda_k^{(s)})$ to Algorithm 1 and denoted the detected sequence as $\hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(s,k)}$;

6 Identify the current $\hat{\mathbf{h}} = (\hat{h}_1, \dots, \hat{h}_{K_0})$ that minimize

$$\mathbf{h}^{(s)} = [h_1^{(s)}, \dots, h_{K_0}^{(s)}]^T = \arg \min_{[h_1, \dots, h_{K_0}]^T \in \mathbb{C}^{K_0}} \left\| \mathbf{y} - \sum_{k=1}^{K_0} \hat{h}_k \cdot \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(s,k)} \right\|^2. \tag{10}$$

 Reduce \mathbf{y} to $\mathbf{y} = \mathbf{y} - \sum_{k=1}^{K_0} \hat{h}_k \cdot \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(s,k)}$;

7 **end**

8 **end**

First, the PRM sequence and the channel coefficient are initialized as $\hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(0,k)} = \mathbf{0}^N$ and $\hat{h}_k^{(0)} = 0$ for $s = 0$, respectively, (in Line 1). We then denote an interference for the user k during the s -th iteration as

$$\Lambda_k^{(s)} = \sum_{k'=1 \text{ and } k' \neq k}^{K_0} \hat{h}_{k'}^{(s')} \cdot \hat{\mathbf{C}}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_X}^{(s',k')} \tag{11}$$

where

$$\begin{cases} s' = s, & \text{if } 1 \leq k' \leq k - 1, \\ s' = s - 1, & \text{if } k + 1 \leq k' \leq K_0. \end{cases} \tag{12}$$

Then, in order to retrieve a PRM sequence $\widehat{\mathbf{C}}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^{(s,k)}$, we feed the signal $(\mathbf{y} - \Lambda_k^{(s)})$ into Algorithm 1.

Next, when detecting each user’s PRM sequence, the detected sequences are inserted into the linear least square channel estimator in order to improve their accuracy further, specified as (8) in Algorithm 2. Due to the exchange of information between the sequence detector and the channel estimator, the effectiveness gradually improves, and it terminates once the results have converged or the maximum number of iterations has been reached.

4. Performance Analysis

4.1. Successful Recovery Probability of the List PRM Projection Algorithm

For detecting a single PRM sequence, Algorithm 1 recovers the column vectors of the matrix $\widehat{\mathbf{P}}$ layer by layer. In this section, we will derive the probability of successful recovery of each layer element $\widehat{\mathbf{P}}_\tau$ for $1 \leq \tau \leq m$. The corresponding conclusions are summarized in Lemma 1 as well as Theorem 1.

Lemma 1. Suppose that Algorithm 1’s input signal is $\mathbf{y} = h\mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{n}$, where $h \sim \mathcal{CN}(0, 1)$ is the channel coefficient, and $\mathbf{n} \sim \mathcal{CN}(0, \mathbf{I}_N)$ denotes the complex additive white Gaussian noise (AWGN). The notation $\mathcal{P}^{(\tau)} (1 \leq \tau \leq m)$ represents the event “the vector $\widehat{\mathbf{P}}_\tau$ is recovered successful” and the notation $\mathcal{P}^{(1, \dots, \tau-1)}$ denotes the event “the vectors $\widehat{\mathbf{P}}_1, \dots, \widehat{\mathbf{P}}_{\tau-1}$ are correctly recovered”. On this basis, if h and $\mathcal{P}^{(1, \dots, \tau-1)}$ is given, then for any $\mathbf{z} \in \mathbb{F}_2^{m-Y}$, $\Pr(\mathcal{P}^{(\tau)} | \mathcal{P}^{(1, \dots, \tau-1)}, h)$ can be expressed as

$$\Pr(\mathcal{P}^{(\tau)} | \mathcal{P}^{(1, \dots, \tau-1)}, h) \geq \left[Q\left(-\frac{2^Y |h|^2 \cdot (-1)^{B_\tau + (\mathbf{B}|_{Y+1})^T \mathbf{z}}}{\sqrt{2}\sigma_{F, \tau}}\right) \cdot Q\left(-\frac{2^Y |h|^2 \cdot (-1)^{B_\tau + (\mathbf{B}|_{Y+1})^T \mathbf{z}}}{2\sigma_{F, \tau}}\right) \right]^{2^{(Y-\tau+1)}-1} \quad (13)$$

In (13), function $Q(\cdot)$ is $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) dt$, and the variance $\sigma_{F, \tau}^2$ is defined as

$$\sigma_{F, \tau}^2 = 2^{m-1} \left[2|h|^2 \frac{N_0}{2^{\tau-1}} + \left(\frac{N_0}{2^{\tau-1}}\right)^2 \right]. \quad (14)$$

Theorem 1. Taking into account the channel coefficients h and the results of (13), the average probability of successful detection for Algorithm 1 can be calculated as

$$P_{succ} = \int_h f_{\mathcal{CN}}(h; 0, 1) \cdot \check{P}(Y, N_0 | h) dh, \quad (15)$$

where $\check{P}(Y, N_0 | h) = \prod_{\tau=1}^Y \Pr(\mathcal{P}^{(\tau)} | \mathcal{P}^{(1, \dots, \tau-1)}, h)$ and $f_{\mathcal{CN}}(h; 0, 1) = \frac{1}{\pi} \exp(-|h|^2)$.

Proof. We assume that the subspace matrix \mathbf{I}_χ is decoded correctly and $H = 1$. Define a concept $F_S(\mathbf{f}_\tau)$ related to $\mathbf{f}_\tau \in \mathbb{F}_2^m$ as

$$F_S(\mathbf{f}_\tau) = (h\mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{n})^H \cdot \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{f}_\tau) \cdot (h\mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{n}) \\ = \underbrace{|h|^2 \mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{f}_\tau) \mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}}_{F_A(\mathbf{f}_\tau)} + \underbrace{\mathbf{n}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{f}_\tau) \mathbf{n}}_{Z_1(\mathbf{f}_\tau)} + \underbrace{h \left[\mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{f}_\tau) \mathbf{n} + \mathbf{n}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_\tau, \mathbf{f}_\tau) \mathbf{C}_{\widehat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} \right]}_{Z_2(\mathbf{f}_\tau)}. \quad (16)$$

According to (16), $Z_1(\mathbf{f}_\tau)$ and $Z_2(\mathbf{f}_\tau)$ are the sources of interference, and we use $\mathbf{Z}(\mathbf{f}_\tau) = Z_1(\mathbf{f}_\tau) + Z_2(\mathbf{f}_\tau)$ to conclude all interferences. The following discussion will demonstrate Lemma 1 through mathematical induction.

(1) When $\tau = 1$: according to Algorithm 1, the event $\mathcal{P}^{(1)}$ occurring is described as $\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} |F(\widehat{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1})| > \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} |F(\widehat{\mathbf{I}}_\chi \mathbf{z} + \bar{\mathbf{p}}_{\chi, 1})|$ (we omit the subscript S and record it

as $F(\cdot)$ in this section), where $\tilde{\mathbf{p}}_{\chi,1} = \mathbf{I}_{\chi}\hat{\mathbf{P}}\mathbf{e}_1$, and symbol $\bar{\mathbf{p}}_{\chi,1}$ denotes any possible vector that is different from $\tilde{\mathbf{p}}_{\chi,1}$. It is known that the vector $\bar{\mathbf{p}}_{\chi,1}$ has a total of $(2^Y - 1)$ possibilities, then we denote the probability of the event $\mathcal{P}^{(1)}$ as follows:

$$\begin{aligned} \Pr(\mathcal{P}^{(1)}|h) &= \Pr\left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \tilde{\mathbf{p}}_{\chi,1})\right| > \max_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \bar{\mathbf{p}}_{\chi,1})\right|\right) \\ &= \prod_{[\bar{\mathbf{p}}_{\chi,1}^{(j)}]_{j=1}^{2^{Y-1}}} \Pr\left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \tilde{\mathbf{p}}_{\chi,1})\right| > \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y}} \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \bar{\mathbf{p}}_{\chi,1}^{(j)})\right|\right). \end{aligned} \quad (17)$$

In (17), $[\bar{\mathbf{p}}_{\chi,1}^{(j)}]_{j=1}^{2^{Y-1}}$ is the set of all possible vectors except $\tilde{\mathbf{p}}_{\chi,1}$. Since each term within the summation function obeys the same distribution, calculating (17) is equivalent to computing its approximate probability as

$$\prod_{[\bar{\mathbf{p}}_{\chi,1}^{(j)}]_{j=1}^{2^{Y-1}}} \Pr\left(\left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \tilde{\mathbf{p}}_{\chi,1})\right| > \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \bar{\mathbf{p}}_{\chi,1}^{(j)})\right|\right). \quad (18)$$

For convenience, we let the notation $\tilde{\mathbf{e}}_{\chi,z}^{(1)} = \tilde{\mathbf{I}}_{\chi}\mathbf{z} + \tilde{\mathbf{p}}_{\chi,1}$ and $\bar{\mathbf{e}}_{\chi,z}^{(1)} = \tilde{\mathbf{I}}_{\chi}\mathbf{z} + \bar{\mathbf{p}}_{\chi,1}$. Since the $(2^Y - 1)$ events in (18) are independent of one another, we calculate the probability of one event first:

$$\begin{aligned} &\Pr\left(\left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \tilde{\mathbf{p}}_{\chi,1})\right| > \left|F(\tilde{\mathbf{I}}_{\chi}\mathbf{z} + \bar{\mathbf{p}}_{\chi,1})\right|\right) \\ &\stackrel{(a)}{=} \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > \left|\mathbf{Z}(\bar{\mathbf{e}}_{\chi,z}^{(1)})\right|\right) \\ &\stackrel{(b)}{=} \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > \left|\mathbf{Z}(\bar{\mathbf{e}}_{\chi,z}^{(1)})\right|\right) \\ &\quad \cdot \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > 0\right) \\ &\quad + \Pr\left(-\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} - \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > \left|\mathbf{Z}(\bar{\mathbf{e}}_{\chi,z}^{(1)})\right|\right) \\ &\quad \cdot \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) < 0\right) \\ &\stackrel{(c)}{\geq} \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > \left|\mathbf{Z}(\bar{\mathbf{e}}_{\chi,z}^{(1)})\right|\right) \\ &\quad \cdot \Pr\left(\left|h\right|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} + \mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)}) > 0\right), \end{aligned} \quad (19)$$

where the equal sign (a) is based on $\mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \bar{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}} = 0$, (b) and (c) are obtained according to the following equations:

$$\begin{aligned} \Pr(|A| \geq |B|) &= \Pr(A > |B|)\Pr(A > 0) + \Pr(-A > |B|)\Pr(A < 0) \\ &\geq \Pr(A > |B|)\Pr(A > 0), \end{aligned} \quad (20)$$

and $||A| - |B|| \leq |A \pm B| \leq |A| + |B|$.

In order to calculate the two probabilities of the result of (19), it is necessary to study the distribution of the variables $|h|^2 \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}^H \mathbf{E}\left(\mathbf{I}_{\chi}\mathbf{e}_1, \tilde{\mathbf{e}}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}},\mathbf{B},\mathbf{I}_{\chi}}$, $\mathbf{Z}(\tilde{\mathbf{e}}_{\chi,z}^{(1)})$ and $\mathbf{Z}(\bar{\mathbf{e}}_{\chi,z}^{(1)})$,

respectively. We prioritize the study of $|h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi, z}^{(1)}) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}$: we omit the factor $1/2^r$ for the representation of $\mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}$ and denote $F_A(\tilde{\Xi}_{\chi, z}^{(1)})$ as follows

$$\begin{aligned} F_A(\tilde{\Xi}_{\chi, z}^{(1)}) &= |h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi, z}^{(1)}) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} \\ &= |h|^2 \cdot i^{(\mathbf{I}_\chi \mathbf{e}_1)^T \cdot \tilde{\Xi}_{\chi, z}^{(1)}} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}(\mathbf{w} + \mathbf{I}_\chi \mathbf{e}_1)} \cdot (-1)^{\mathbf{w}^T \cdot \tilde{\Xi}_{\chi, z}^{(1)}} \cdot \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}(\mathbf{w}) \\ &= |h|^2 \cdot \sum_{\mathbf{w} \in \mathbb{F}_2^m} i^{2(\hat{\mathbf{P}}_1; \mathbf{0})^T \cdot \mathbf{Q}^{-1} \mathbf{w} + P_{1,1} + 2\mathbf{B}^T(\mathbf{e}_1; \mathbf{0})} \cdot i^{(\mathbf{I}_\chi \mathbf{e}_1)^T \cdot \tilde{\Xi}_{\chi, z}^{(1)}} \cdot (-1)^{\mathbf{w}^T \cdot \tilde{\Xi}_{\chi, z}^{(1)}} \\ &\quad \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w} + (\mathbf{e}_1; \mathbf{0}), \mathbf{Y}] \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w}, \mathbf{Y}] \\ &= |h|^2 \cdot i^{2\mathbf{B}^T(\mathbf{e}_1; \mathbf{0}) + P_{1,1}} \sum_{\mathbf{w} \in \mathbb{F}_2^m} i^{2(\hat{\mathbf{P}}_1; \mathbf{0})^T \cdot \mathbf{Q}^{-1} \mathbf{w} + 2\mathbf{w}^T \cdot \tilde{\Xi}_{\chi, z}^{(1)} + (\mathbf{I}_\chi \mathbf{e}_1)^T \cdot \tilde{\Xi}_{\chi, z}^{(1)}} \\ &\quad \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w} + (\mathbf{e}_1; \mathbf{0}), \mathbf{Y}] \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w}, \mathbf{Y}], \end{aligned} \quad (21)$$

where $P_{1,1} = \mathbf{e}_1^T \mathbf{P} \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{P}_1$ and $\phi(\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w}, \mathbf{Y}) = 1$ in the case of $\mathbf{B}|_{\mathbf{Y}+1}^m = (\mathbf{Q}^{-1} \mathbf{w})|_{\mathbf{Y}+1}^m$. We then substitute $\tilde{\Xi}_{\chi, z}^{(1)} = \tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}$ in (21), and the equation expression becomes:

$$\begin{aligned} F_A(\tilde{\Xi}_{\chi, z}^{(1)}) &= F_A(\tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}) \\ &= |h|^2 \cdot i^{2\mathbf{B}^T(\mathbf{e}_1; \mathbf{0}) + 2P_{1,1}} \cdot \sum_{\mathbf{w} \in \mathbb{F}_2^m} i^{2(\tilde{\mathbf{I}}_\chi \mathbf{z})^T \mathbf{w}} \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w} + (\mathbf{e}_1; \mathbf{0}), \mathbf{Y}] \cdot \phi[\mathbf{B}, \mathbf{Q}^{-1} \mathbf{w}, \mathbf{Y}] \\ &= |h|^2 \cdot i^{2\mathbf{B}^T(\mathbf{e}_1; \mathbf{0}) + 2P_{1,1}} \cdot \sum_{\mathbf{w} \in \mathbb{F}_2^m} i^{2(\mathbf{B}|_{\mathbf{Y}+1}^m)^T \mathbf{z}} \\ &= 2^Y \cdot |h|^2 (-1)^{B_1 + (\mathbf{B}|_{\mathbf{Y}+1}^m)^T \mathbf{z}}, \end{aligned} \quad (22)$$

where $B_1 = \mathbf{e}_1^T \mathbf{B}$ and $\mathbf{z} \in \mathbb{F}_2^{m-Y}$. To sum up, $F_A(\tilde{\Xi}_{\chi, z}^{(1)})$ takes the value of $2^Y \cdot |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{\mathbf{Y}+1}^m)^T \mathbf{z}}$ if and only if $\tilde{\Xi}_{\chi, z}^{(1)} = \tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}$.

Next, we calculate the distribution of $\mathbf{Z}(\tilde{\Xi}_{\chi, z}^{(1)})$: we expand $\mathbf{Z}(\tilde{\Xi}_{\chi, z}^{(1)})$ into two parts:

$$\begin{aligned} \mathbf{Z}_1(\tilde{\Xi}_{\chi, z}^{(1)}) &= \mathbf{n}_1^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}) \mathbf{n}_1 \\ &= i^{(\mathbf{I}_\chi \mathbf{e}_1)^T \cdot \sum_{\mathbf{z} \in \mathbb{F}_2^{m-r}} (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{n}_1(\mathbf{w} + \mathbf{I}_\chi \mathbf{e}_1)} \cdot (-1)^{\mathbf{w}^T \cdot \sum_{\mathbf{z} \in \mathbb{F}_2^{m-r}} (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \cdot \mathbf{n}(\mathbf{w}). \end{aligned} \quad (23)$$

Therefore, the variance of $\mathbf{Z}_1(\tilde{\Xi}_{\chi, z}^{(1)})$ is $2^m \cdot N_0^2$. Following the same rule, \mathbf{Z}_2 turns into

$$\begin{aligned} \mathbf{Z}_2(\tilde{\Xi}_{\chi, z}^{(1)}) &= h \cdot \left[\mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}) \mathbf{n} + \mathbf{n}^H \mathbf{E}(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi, 1}) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} \right] \\ &= h \cdot i^{(\mathbf{I}_\chi \mathbf{e}_1)^T \cdot (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}(\mathbf{w} + \mathbf{I}_\chi \mathbf{e}_1)} \cdot (-1)^{\mathbf{w}^T \cdot (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \cdot \mathbf{n}(\mathbf{w}) \\ &\quad + h \cdot i^{(\mathbf{I}_\chi \mathbf{e}_1)^T \cdot (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{n}(\mathbf{w} + \mathbf{I}_\chi \mathbf{e}_1)} \cdot (-1)^{\mathbf{w}^T \cdot (\tilde{\mathbf{I}}_\chi \mathbf{z} + \mathbf{I}_\chi \hat{\mathbf{P}}_1)} \cdot \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}(\mathbf{w}). \end{aligned} \quad (24)$$

According to (24), the mean of variable $\mathbf{Z}_2(\tilde{\Xi}_{\chi, z}^{(1)})$ is 0 and the variance is $2 \cdot 2^m |h|^2 N_0$. We denote the notation $\sigma_{F,1}^2 = 2^{m-1} (2|h|^2 N_0 + N_0^2)$. Since the distribution of $\mathbf{Z}(\tilde{\Xi}_{\chi, z}^{(1)})$ is

the same with $\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)})$, we have $\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \sim \mathcal{CN}(0, 2\sigma_{F,1}^2)$, $\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \sim \mathcal{CN}(0, 2\sigma_{F,1}^2)$ and $F_A(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \sim \mathcal{CN}(2^Y \cdot |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}, 2\sigma_{F,1}^2)$.

Based on above distribution, the first term of the last equation in (19) can be approximated as:

$$\begin{aligned} & \Pr\left(|h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) > \left|\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)})\right|\right) \\ &= 1 - \Pr\left(\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) - \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \geq |h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}\right) \cdot \Pr\left(\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) > 0\right) \\ &\quad - \Pr\left(-\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) - \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) - \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \geq |h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}\right) \cdot \Pr\left(\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) < 0\right) \quad (25) \\ &= 1 - 2\Pr\left(\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) - \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \geq |h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}\right) \cdot \Pr\left(\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) > 0\right) \\ &\stackrel{(d)}{\geq} 1 - Q\left(\frac{2^Y |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}}{2\sigma_{F,1}}\right), \end{aligned}$$

where (d) depends on $\mathbf{Z}_1(\tilde{\Xi}_{\chi,z}^{(1)}) + \mathbf{Z}_2(\tilde{\Xi}_{\chi,z}^{(1)}) - \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) \sim \mathcal{N}(0, 4\sigma_{F,1}^2)$. We then compute the latter term of (19) as

$$\begin{aligned} & \Pr\left(|h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) > 0\right) \\ &= \Pr\left(\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) > -|h|^2 \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}^H \mathbf{E}\left(\mathbf{I}_\chi \mathbf{e}_1, \tilde{\Xi}_{\chi,z}^{(1)}\right) \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi}\right) \\ &= \Pr\left(\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(1)}) > -2^Y |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}\right) \quad (26) \\ &= Q\left(-\frac{2^Y |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}}{\sqrt{2}\sigma_{F,1}}\right). \end{aligned}$$

By substituting (25) and (26) into (18), we finally get

$$\begin{aligned} & \prod_{[\tilde{\mathbf{p}}_{\chi,1}^{(j)}]_{j=1}^{2^Y-1}} \Pr\left(\left|F(\tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi,1})\right| > \left|F(\tilde{\mathbf{I}}_\chi \mathbf{z} + \tilde{\mathbf{p}}_{\chi,1}^{(j)})\right|\right) \\ & \geq \left[Q\left(-\frac{2^Y |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}}{\sqrt{2}\sigma_{F,1}}\right) \cdot Q\left(-\frac{2^Y |h|^2 \cdot (-1)^{B_1 + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}}{2\sigma_{F,1}}\right)\right]^{2^Y-1}. \quad (27) \end{aligned}$$

Equation (27) is consistent with (13) in Lemma 1, so Lemma 1 holds for $\tau = 1$.

(2) When $2 \leq \tau \leq Y$: Algorithm 1's input signal becomes

$$\begin{aligned} \mathbf{y}_\tau &= \lambda_{PRM,\omega}^{(\tau)} \cdot \mathbf{y}_{\tau-1} \\ &= \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \prod_{i=1}^{\tau-1} \lambda_{PRM,\omega}^{(i)} \cdot \mathbf{n} \quad (28) \\ &= \mathbf{C}_{\hat{\mathbf{P}}, \mathbf{B}, \mathbf{I}_\chi} + \frac{1}{2^{i-1}} \prod_{i=1}^{\tau-1} \left(\mathbf{I}_N + \omega_i \cdot \mathbf{E}\left[\mathbf{I}_\chi \mathbf{e}_i, \mathbf{I}_\chi \hat{\mathbf{P}}_i\right]\right) \cdot \mathbf{n}. \end{aligned}$$

By substituting (28) into (16), we have $\sigma_{F,\tau}^2 = 2^{m-1} \left[2|h|^2 \frac{N_0}{2^{\tau-1}} + \left(\frac{N_0}{2^{\tau-1}}\right)^2\right]$. Thus, $\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(\tau)}) \sim \mathcal{CN}(0, 2\sigma_{F,\tau}^2)$, and $\mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(\tau)}) \sim \mathcal{CN}(0, 2\sigma_{F,\tau}^2)$. Furthermore, we get $F_A(\tilde{\Xi}_{\chi,z}^{(\tau)}) + \mathbf{Z}(\tilde{\Xi}_{\chi,z}^{(\tau)}) \sim \mathcal{CN}(2^Y \cdot |h|^2 (-1)^{B_\tau + (\mathbf{B}|_{Y+1}^m)^T \mathbf{z}}, 2\sigma_{F,\tau}^2)$. The derivation process is similar to $\tau = 1$, and we omit it here. The result is consistent with (13) and (14) in Lemma 1.

The PRM sequence is reconstructed successfully if the estimations for all layers are correct. Therefore, Algorithm 1 has a successful detection probability as follows:

$$\check{P}(Y, N_0|h) = \prod_{\tau=1}^Y \Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h). \quad (29)$$

Taking the channel coefficient h into account, we get the following equation

$$P_{succ} = \int_h f_{\mathcal{CN}}(h; 0, 1) \cdot \check{P}(Y, N_0|h) dh, \quad (30)$$

Thus, the proof of Theorem 1 is complete. \square

The factors that affect the efficiency of the layer-by-layer PRM projection algorithm are discussed below. According to Lemma 1, the conditional probability $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ of the vector $\hat{\mathbf{P}}_{\tau}$ is related to three factors, namely Y , τ , m and N_0 . Since it is challenging to mathematically express the relationship between them, we fix two elements and track the changes in the conditional probability as a result of changing the third factor. In accordance with Figures 2–5, the following results are obtained:

- Assume that the PRM code is of full rank with $Y = m$, when m and N_0 are given, as τ increases from 1 to m , the value of $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ increases (Figure 2). The results illustrate the properties of the projection algorithm: if the first few layers are error-free, then the remaining layers are highly likely to be recovered correctly. Additionally, a further conclusion can be drawn by observing the above proof that $\mathbf{n}_{\tau} \sim \mathcal{CN}(0, \frac{N_0}{2^{\tau-1}})$ indicates that the noise power in each layer decreases exponentially as τ increases, leading to the successful recovery probability of the vector increasing layer by layer. Overall, the recovery reliability of the first few layers of the layer-by-layer PRM projection algorithm is crucial to its performance. This motivates us to increase the number of candidate paths in the first few layers to obtain better detection.
- As shown in Figure 3, when τ , Y and N_0 are given, $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ increases as m increases, which shows that we can improve the performance of the PRM sequence detection algorithm by increasing the length of the PRM sequence.
- Figure 4 details the variation of $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ with N_0 for fixed τ , m and Y . It is clear that as N_0 increases, the signal-to-noise ratio (SNR) decreases, resulting in $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ decreasing consequently.
- Figure 5 gives the variation of $\Pr(\mathcal{P}^{(\tau)}|\mathcal{P}^{(1,\dots,\tau-1)}, h)$ with τ for fixed N_0 , m and Y : the larger Y indicates the better performance under the same m , and this result is consistent with the fact that a greater signal power will result in a greater signal-to-noise ratio. Furthermore, the larger the m , the worse the performance under the same layer τ , indicating that the closer Y to m , the better the performance will be.

4.2. Successful Recovery Probability of the Iterative List PRM Projection Algorithm

In this section, Lemma 2 and Theorem 2 analyze the performance of the iterative list PRM projection algorithm in a multi-user scenario.

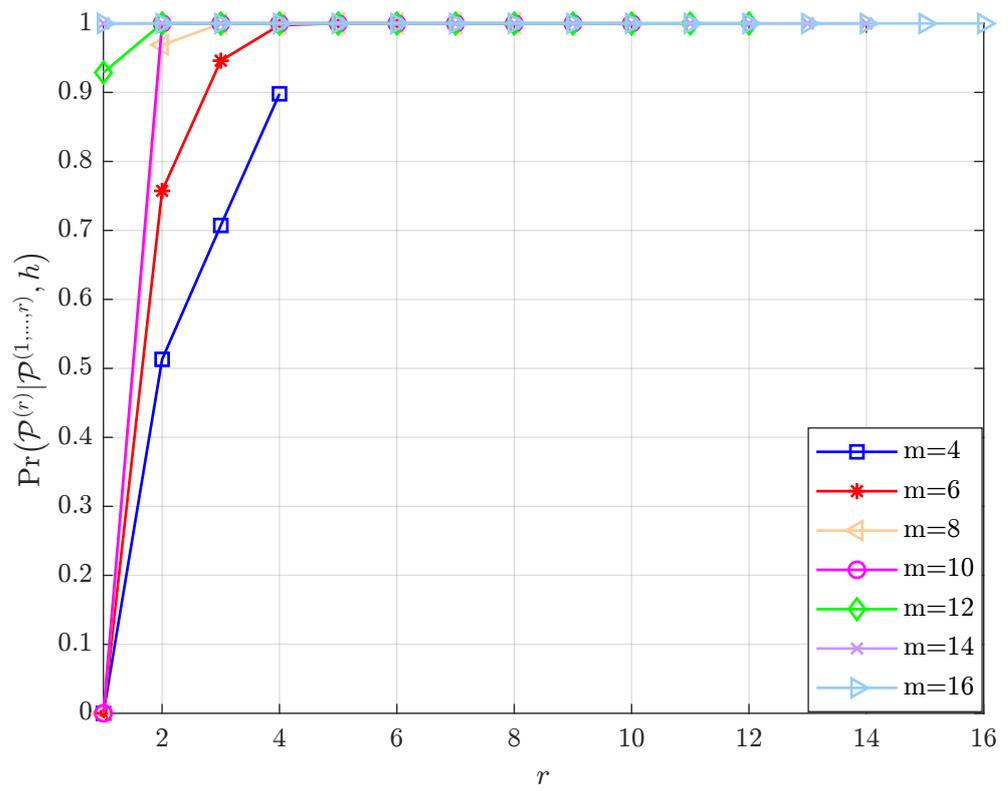


Figure 2. Given m , $N_0 = 10$ and Y , the variation of $\Pr(\mathcal{P}^{(r)} | \mathcal{P}^{(1, \dots, r-1)}, h)$ with r .

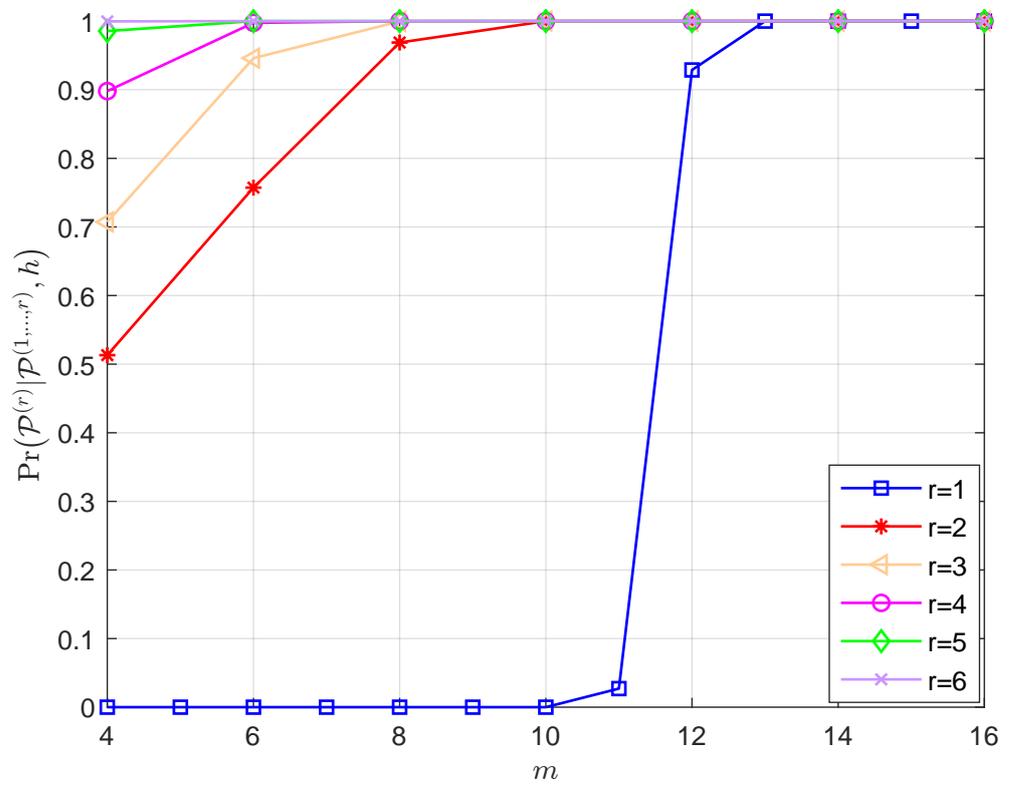


Figure 3. Given r , $N_0 = 10$ and Y , the variation of $\Pr(\mathcal{P}^{(r)} | \mathcal{P}^{(1, \dots, r-1)}, h)$ with m .

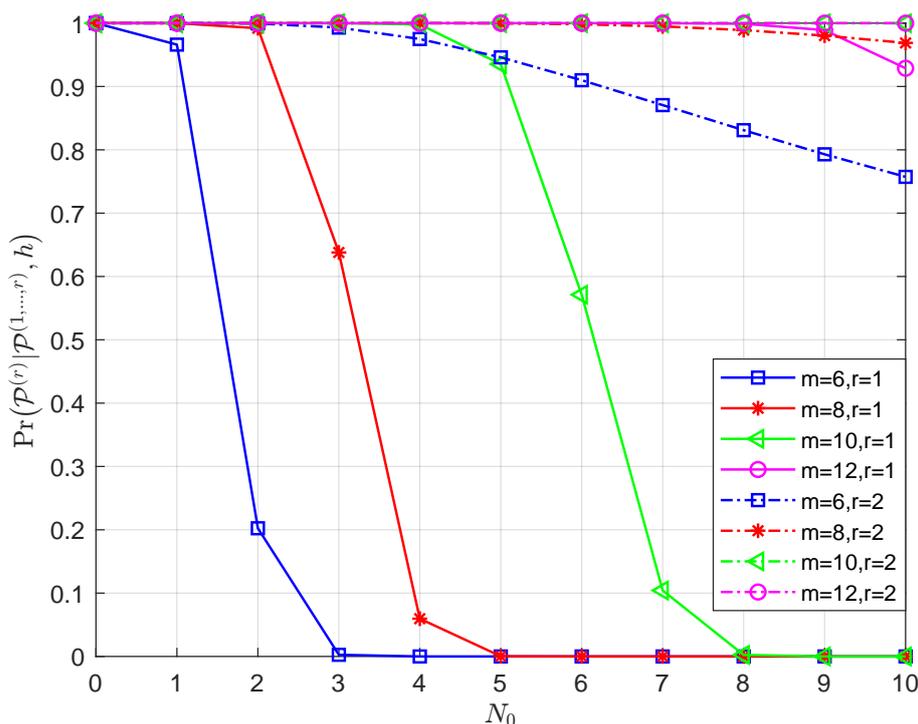


Figure 4. Given τ , m and Y , the variation of $\Pr(\mathcal{P}^{(\tau)} | \mathcal{P}^{(1, \dots, \tau-1)}, h)$ with N_0 .

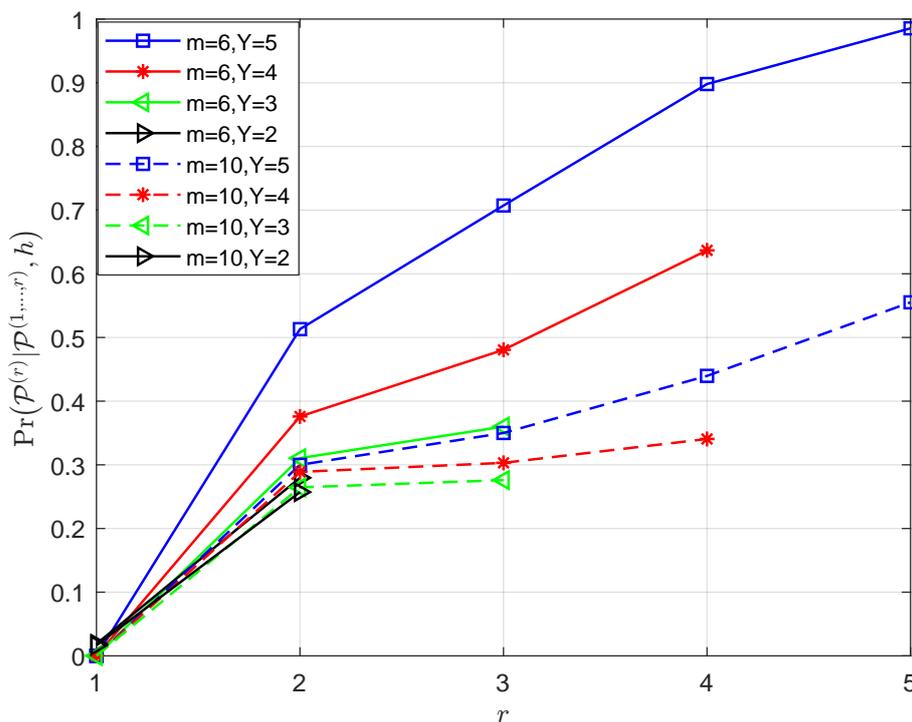


Figure 5. Given N_0 , m and Y , the variation of $\Pr(\mathcal{P}^{(\tau)} | \mathcal{P}^{(1, \dots, \tau-1)}, h)$ with τ .

Lemma 2. Suppose that the input signal of Algorithm 2 contains a linear combination of all K_a active users' sequences. We let these sequences be detected in the order of $(\rho_1, \rho_2, \dots, \rho_{K_a})$. We denote the event "the ρ_k -th recovered sequence has been successfully detected" as \mathcal{B}_{ρ_k} and the event "the sequences with order $(\rho_1, \dots, \rho_{k-1})$ have been successfully detected and have been subtracted from the received signal" as $\mathcal{B}_{\rho_1, \dots, \rho_{k-1}}$. Thus, given the channel parameters $\mathbf{h} = [h_1, \dots, h_{K_a}]$ and the event $\mathcal{B}_{\rho_1, \dots, \rho_{k-1}}$, the chance of the event $\mathcal{B}_{\rho_1, \dots, \rho_{k-1}}$ occurs in the first iteration of Algorithm 2 can be approximated as

$$\Pr(\mathcal{B}_{\rho_k} | \mathcal{B}_{\rho_1, \dots, \rho_{k-1}}, \mathbf{h}) = \Pr(\mathcal{P}_{\rho_k}^{(1)} | \mathbf{h}) \cdot \check{P}\left(Y_{\rho_k} - 1, N_0^{(Y_{\rho_k} - 1)} | \mathbf{h}\right). \quad (31)$$

In (31), $\Pr(\mathcal{P}_{\rho_k}^{(1)} | \mathbf{h})$ refers to the probability of $\hat{\mathbf{P}}_{\rho_k} \mathbf{e}_1$ being successfully recovered under the condition \mathbf{h} , which is expressed as

$$\begin{aligned} & \Pr(\mathcal{P}_{\rho_k}^{(1)} | \mathbf{h}) \\ &= \prod_{j=1}^{2^{Y_{\rho_k} - 1}} Q\left(-\frac{2^{Y_{\rho_k}} |h_{\rho_k}|^2 + \sum_{\rho_{k+1} \leq i \leq \rho_{K_a}} (n_{\rho_k, i} \cdot 2^{Y_{\rho_i}} |h_i|^2 - n_{i, j} \cdot 2^{Y_{\rho_i}} |h_i|^2)}{\sqrt{2}\sigma_{\Lambda, 1}}\right) \\ & \cdot Q\left(-\frac{2^{Y_{\rho_k}} |h_{\rho_k}|^2}{\sigma_{\Lambda, 1}}\right)^{2^{Y_{\rho_k} - 1}}, \end{aligned} \quad (32)$$

where the notation $n_{\rho_k, i}$ indicates the number of intersections of positions corresponding to non-zero $F(\cdot)$ for the i -th detected sequence and ρ_k -th detected sequence. The notation $n_{i, j}$ represents the number of intersections of positions corresponding to non-zero $F(\cdot)$ for the i -th detected sequence and the j -th coset of the set related to non-zero $F(\cdot)$ for the first layer recovery of the ρ_k -th detected sequence. Additionally, the variance in (32) is

$$\sigma_{\Lambda, 1}^2 = \sum_{\rho=\rho_k}^{\rho_{K_a}} \left[\sum_{\rho'=\rho_k \text{ and } \rho' \neq \rho}^{\rho_{K_a}} |h_{\rho}^H \cdot h_{\rho'}|^2 \cdot \sigma_{\mu, 1}^2 + 2^{m-1} \cdot \left(\sum_{\rho=\rho_k}^{\rho_{K_a}} 2|h_{\rho}|^2 N_0 + N_0^2 \right) \right], \quad (33)$$

in which μ is the inner product created by two PRM sequences of length- 2^m , and $\sigma_{\mu, 1}^2$ denotes the variance of the inner product. The second component $\check{P}\left(Y_{\rho_1} - 1, N_0^{(Y_{\rho_1} - 1)} | \mathbf{h}\right)$ in Equation (31) represents the matrix $\hat{\mathbf{P}}^{Y_{\rho_k} - 1}$'s likelihood of a successful recovery given \mathbf{h} , where $\hat{\mathbf{P}}^{Y_{\rho_k} - 1}$ denotes the submatrix of the symmetric matrix $\hat{\mathbf{P}}_{\rho_k}$ with rank $(Y_{\rho_k} - 1)$ for order ρ_k . Additionally, the notation $N_0^{(Y_{\rho_k} - 1)} = \frac{1}{2}(\sum_{\rho=\rho_{k+1}}^{\rho_{K_a}} |h_{\rho}|^2 + N_0)$.

Theorem 2. Suppose that the input signal of Algorithm 2 contains a linear combination of all K_a active users' sequences. We denote each sequence by the specific notation k ($1 \leq k \leq K_a$) and let these sequences be detected in the order of $(\rho_1, \rho_2, \dots, \rho_{K_a})$. Then, given the channel parameter \mathbf{h} , the probability that Algorithm 2 can successfully detect the sequence ρ ($1 \leq \rho \leq K_a$) in the first iteration is

$$\begin{aligned} & \check{P}_{\rho}(\mathcal{K}_a, m, N_0 | \mathbf{h}) \\ &= \Pr(\mathcal{B}_{\rho} | \mathbf{h}) + \sum_{k=2}^{K_a} \left\{ \sum_{(\rho_1, \dots, \rho_{k-1}) \in \mathcal{N}_k} \left[\left(\prod_{k'=1}^{k-1} \Pr(\mathcal{B}_{\rho_{k'}} | \mathcal{B}_{\rho_1, \dots, \rho_{k'-1}}, \mathbf{h}) \right) \cdot \Pr(\mathcal{B}_{\rho} | \mathcal{B}_{\rho_1, \dots, \rho_{k-1}}, \mathbf{h}) \right] \right\}, \end{aligned} \quad (34)$$

where the set \mathcal{N}_k contains all permutations of $(k - 1)$ indexes of order from the set $\mathcal{K}_a \setminus \rho$. Furthermore, by taking the channel parameters into consideration, the average probability of successful detection for the first iteration of the iterative PRM sequence can be approximated as

$$\check{P}_{ave}(\mathcal{K}_a, m, N_0 | \mathbf{h}) = \frac{1}{K_a} \int_{\mathbf{h}} \left\{ \prod_{\rho=1}^{K_a} f_{\mathcal{CN}}(h_{\rho}; 0, 1) \cdot \sum_{\rho=1}^{K_a} \check{P}_{\rho}(\mathcal{K}_a, m, N_0 | \mathbf{h}) \right\}. \quad (35)$$

Proof. For convenience, two users are assumed to be active in the system. Since users are not provided with IDs in the URA scenario, we can deduce the theoretical results of successful detection probabilities with the help of the detection order between sequences;

we denote two sequences as a and b , respectively, and the detection order between them is represented by ρ_a and ρ_b . At this point, the input signal of the algorithm is rewritten as a linear superposition of the two users of the form: $\mathbf{y} = h_a \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}} + h_b \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}} + \mathbf{n}$. The rank of PRM codes $\mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}$ and $\mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}$ are noted as Y_a and Y_b , respectively. According to the expansion of (16), the $F_{\mathcal{M}}$ can be expanded regarding the τ -layer as

$$\begin{aligned}
 F_{\mathcal{M}}(\mathbf{f}_{\tau}) &= (h_a \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}} + h_b \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}} + \mathbf{n})^H \cdot \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \cdot (h_a \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}} + h_b \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}} + \mathbf{n}) \\
 &= \underbrace{|h_a|^2 \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}}_{F_a(\mathbf{f}_{\tau})} + \underbrace{|h_b|^2 \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}}_{F_b(\mathbf{f}_{\tau})} \\
 &\quad + \underbrace{h_a^H \cdot h_b \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}}_{\mathbf{Z}_{ab,1}(\mathbf{f}_{\tau})} + \underbrace{h_a \cdot h_b^H \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}}_{\mathbf{Z}_{ab,2}(\mathbf{f}_{\tau})} \\
 &\quad + \underbrace{h_a \left[\mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{n} + \mathbf{n}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi,a}} \right]}_{\mathbf{X}_{a,1}(\mathbf{f}_{\tau})} \\
 &\quad + \underbrace{h_b \left[\mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{n} + \mathbf{n}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi,b}} \right]}_{\mathbf{X}_{a,2}(\mathbf{f}_{\tau})} + \underbrace{\mathbf{n}^H \mathbf{E}(\mathbf{I}_{\chi} \mathbf{e}_{\tau}, \mathbf{f}_{\tau}) \mathbf{n}}_{\mathbf{N}(\mathbf{f}_{\tau})}.
 \end{aligned} \tag{36}$$

For ease of use, we make $(\mathbf{Z}_{ab,1} + \mathbf{Z}_{ab,2} + \mathbf{X}_{a,1} + \mathbf{X}_{a,2} + \mathbf{N})(\mathbf{f}_{\tau}) = \Lambda(\mathbf{f}_{\tau})$.

We first assess the performance of the first-layer ($\tau = 1$) detection for the ρ_a -th sequence: suppose in the first iteration of Algorithm 2, active users are detected successively according to the order (ρ_a, ρ_b) . In the following, we write the probability of the event $\mathcal{P}_{\rho_a}^{(1)}$ as form

$$\begin{aligned}
 \Pr(\mathcal{P}_{\rho_a}^{(1)} | \mathbf{h}) &= \Pr \left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F(\tilde{\mathbf{I}}_{\chi,a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi,a,1})| > \max_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F(\tilde{\mathbf{I}}_{\chi,a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi,a,1})| \right) \\
 &= \prod_{[\tilde{\mathbf{p}}_{\chi,a,1}^{(j)}]_j^{2^{Y_a-1}}} \Pr \left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F(\tilde{\mathbf{I}}_{\chi,a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi,a,1})| > \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F(\tilde{\mathbf{I}}_{\chi,a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi,a,1}^{(j)})| \right).
 \end{aligned} \tag{37}$$

We omit the subscript \mathcal{M} and record it as $F(\cdot)$ in this section. As seen in (37), the present situation is more complicated than the single-user scenario. One of the problems is that the 2^{m-Y_a} jointly summed events are no longer independent and no longer obey the same distribution. In addition, for the property of the PRM sequence, the vector $(\tilde{\mathbf{I}}_{\chi,a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi,a,1})$ in (37) is specific to the ρ_a -th detected sequences, and the ρ_b -th sequence utilizes a PRM whose rank Y_b is not necessarily equivalent to Y_a ; therefore, the analysis requires a detailed consideration of the interference of the other user. For simplicity, we first approximate a single term in (37) as follows:

$$\begin{aligned}
 &\Pr \left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} \left(|(F_a + \Lambda)(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)})| + |F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)})| \right) \geq \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} \left(|F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| + |\Lambda(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| \right) \right) \\
 &\stackrel{(e)}{=} \Pr \left(|(F_a + \Lambda)(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)})| + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)})| \geq |\Lambda(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| \right) \\
 &\stackrel{(f)}{\geq} \Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)}) + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)})| \geq |\Lambda(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(j,1)})| \right) \cdot \Pr((F_a + \Lambda)(\tilde{\Xi}_{\chi,a,\mathbf{z}}^{(1)}) > 0),
 \end{aligned} \tag{38}$$

where $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)} = \tilde{\mathbf{I}}_{\chi_a, a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi_a, 1}$, $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)} = \tilde{\mathbf{I}}_{\chi_a, a} \mathbf{z} + \tilde{\mathbf{p}}_{\chi_a, 1}^{(j)}$ (different from (19), the superscript “j” can not be removed from $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}$ since the events in joint multiply from (37) are not independent anymore) and $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}$ is the j -th coset of the set $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}$ ($1 \leq j \leq 2^{Y_a} - 1$). It is known that $F_a(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ take non-zero values for the set $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}$. Additionally, the equal sign (e) in (36) retains one of the terms on both sides owing to the same distribution. The inequality sign (f) follows the formula (18). In the following, we will calculate each of the two probabilities of the result of (38).

We first solve the probability of the latter term. Since we know that $F_a(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ takes a fixed value, it is sufficient to obtain the distribution of $\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$. Thus, the distribution of $\mathbf{Z}_{ab,1}(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ and $\mathbf{Z}_{ab,2}(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ in $\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ can be extended as

$$\begin{aligned} \mathbf{Z}_{ab,1}(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) &= h_a^H \cdot h_b \cdot \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi_a}}^H \mathbf{E} \left(\mathbf{I}_{\chi_a} \mathbf{e}_\tau, \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)} \right) \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi_b}} \\ &= h_a^H \cdot h_b \cdot i^{(\mathbf{I}_{\chi_a} \mathbf{e}_\tau)^T \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi_a}}(\mathbf{w} + \mathbf{I}_{\chi_a} \mathbf{e}_\tau)} \cdot (-1)^{\mathbf{w}^T \cdot \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \cdot \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi_b}}(\mathbf{w}) \\ &= h_a^H \cdot h_b \cdot i^{(\mathbf{I}_{\chi_a} \mathbf{e}_\tau + 2\mathbf{w})^T \cdot \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \cdot \mu_{\rho_a, \rho_b}^{(1)} \end{aligned} \quad (39)$$

and

$$\begin{aligned} \mathbf{Z}_{ab,2}(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) &= h_a \cdot h_b^H \cdot \mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi_b}}^H \mathbf{E} \left(\mathbf{I}_{\chi_a} \mathbf{e}_\tau, \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)} \right) \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi_a}} \\ &= h_a \cdot h_b^H \cdot i^{(\mathbf{I}_{\chi_a} \mathbf{e}_\tau)^T \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \sum_{\mathbf{w} \in \mathbb{F}_2^m} \overline{\mathbf{C}_{\hat{\mathbf{P}}_b, \mathbf{B}_b, \mathbf{I}_{\chi_b}}(\mathbf{w} + \mathbf{I}_{\chi_a} \mathbf{e}_\tau)} \cdot (-1)^{\mathbf{w}^T \cdot \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \cdot \mathbf{C}_{\hat{\mathbf{P}}_a, \mathbf{B}_a, \mathbf{I}_{\chi_a}}(\mathbf{w}) \\ &= h_a \cdot h_b^H \cdot i^{(\mathbf{I}_{\chi_a} \mathbf{e}_\tau + 2\mathbf{w})^T \cdot \tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}} \cdot \mu_{\rho_a, \rho_b'}^{(1)} \end{aligned} \quad (40)$$

respectively, where $\mu_{\rho_a, \rho_b}^{(1)}$ and $\mu_{\rho_a, \rho_b'}^{(1)}$ are the inner product of two sequences. The inner product is related to the pattern form of the PRM. Since the distribution of the occupancy pattern has equal probability, the mean of the inner product is 0, and we denote its variance as $\sigma_{\mu,1}^2$. Thus, we can obtain that $\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})$ obeys the distribution $\mathcal{N}(0, \sigma_{\Lambda,1}^2)$, where the variance is

$$\sigma_{\Lambda,1}^2 = (|h_a^H \cdot h_b|^2 + |h_a \cdot h_b^H|^2) \cdot \sigma_{\mu,1}^2 + 2^{m-1} \left[2(|h_a|^2 + |h_b|^2) N_0 + N_0^2 \right].$$

In light of this, the latter term of (38) can be computed as

$$\begin{aligned} &\Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > 0 \right) \\ &= \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > -F_a(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) \right) \\ &= \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > -2^{Y_a} |h_a|^2 \cdot (-1)^{B_{a,1} + (\mathbf{B}_a |_{Y_1}^m)^T \mathbf{z}} \right) \\ &\stackrel{(g)}{=} Q \left(-\frac{2^{Y_a} |h_a|^2}{\sigma_{\Lambda,1}} \right). \end{aligned} \quad (41)$$

In equal sign (g), we set $\mathbf{z} = \mathbf{0}^{m-Y}$; this setting is also extended in the following formulas.

We next solve the probability of the first term in (38), we suppose that the set corresponding to one-zero $F_b(\cdot)$ is noted as $\tilde{\Xi}_{\chi_b, \mathbf{z}}^{(1)}$, and we make $|\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)} \cap \tilde{\Xi}_{\chi_b, \mathbf{z}}^{(1)}| = n_{ab}$, obviously, $|\tilde{\Xi}_{\chi_b, \mathbf{z}}^{(1)}| = 2^{m-Y_b}$. We further denote $|\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)} \cap \tilde{\Xi}_{\chi_b, \mathbf{z}}^{(1)}| = n_{b,j}$ and $n_{ab} + \sum_{j=1}^{2^{Y_a}-1} n_{b,j} = 2^{m-Y_b}$. On this basis, the first term of the results of (38) yields the following equation:

$$\begin{aligned}
& \Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})| \geq |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right) \\
&= \Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) + n_{ab} \cdot 2^{Y_b} |h_b|^2 \geq |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| + n_{b,j} \cdot 2^{Y_b} |h_b|^2 2^{Y_b} \right) \\
&= 1 - \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) - \Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) \geq 2^{Y_a} |h_a|^2 + n_{ab} \cdot 2^{Y_b} |h_b|^2 - n_{b,j} \cdot 2^{Y_b} |h_b|^2 \right) \cdot \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) > 0 \right) \\
&\quad - \Pr \left(-\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) - \Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) \geq 2^{Y_a} |h_a|^2 + n_{ab} \cdot 2^{Y_b} |h_b|^2 - n_{b,j} \cdot 2^{Y_b} |h_b|^2 \right) \cdot \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) < 0 \right) \\
&\geq 1 - \Pr \left(\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) - \Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) \geq 2^{Y_a} |h_a|^2 + n_{ab} \cdot 2^{Y_b} |h_b|^2 - n_{b,j} \cdot 2^{Y_b} |h_b|^2 \right) \\
&\stackrel{(h)}{=} 1 - Q \left(\frac{2^{Y_a} |h_a|^2 + n_{ab} \cdot 2^{Y_b} |h_b|^2 - n_{b,j} \cdot 2^{Y_b} |h_b|^2}{\sqrt{2}\sigma_{\Lambda,1}} \right),
\end{aligned} \tag{42}$$

the equal sign (h) is based on $\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) - \Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) \sim \mathcal{N}(0, 2\sigma_{\Lambda,1}^2)$. On this basis, we return to (38) and get the final result

$$\begin{aligned}
& \prod_{j=1}^{2^{Y_a}-1} \Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})| \geq |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| + \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right) \\
&= \prod_{j=1}^{2^{Y_a}-1} \left(Q \left(-\frac{2^{Y_a} |h_a|^2 + n_{ab} \cdot 2^{Y_b} |h_b|^2 - n_{b,j} \cdot 2^{Y_b} |h_b|^2}{\sqrt{2}\sigma_{\Lambda,1}} \right) \cdot Q \left(-\frac{2^{Y_a} |h_a|^2}{\sigma_{\Lambda,1}} \right) \right).
\end{aligned} \tag{43}$$

This equation is consistent with (32) in Lemma 2.

Now we present a special example to provide a further explanation for the result of (43): We suppose that two users have the same submatrix \mathbf{I}_χ and different vectors $\hat{\mathbf{P}}_1$; thus, (37) directly becomes

$$\begin{aligned}
& \prod_{j=1}^{2^{Y_a}-1} \Pr \left(\sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |(F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)})| > \sum_{\mathbf{z} \in \mathbb{F}_2^{m-Y_a}} |(F_b + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right) \\
&\geq \prod_{j=1}^{2^{Y_a}-1} \left(\Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| + |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right) \cdot \Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > 0 \right) \right) \\
&= \left(Q \left(-\frac{2^{Y_a} |h_a|^2}{\sigma_{\Lambda,1}} \right) \right)^{2^{Y_a}-1} \cdot \left(\prod_{j=1}^{2^{Y_a}-2} \underbrace{\Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right)}_I \right) \\
&\quad \cdot \underbrace{\Pr \left((F_a + \Lambda)(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}) > |F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| + |\Lambda(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)})| \right)}_{II} \\
&= \left(Q \left(-\frac{2^{Y_a} |h_a|^2}{\sigma_{\Lambda,1}} \right) \right)^{2^{Y_a}-1} \cdot \left(Q \left(-\frac{2^{Y_a} |h_a|^2}{\sqrt{2}\sigma_{\Lambda,1}} \right) \right)^{2^{Y_a}-2} \cdot Q \left(-\frac{2^{Y_a} |h_a|^2 - 2^{Y_b} |h_b|^2}{\sqrt{2}\sigma_{\Lambda,1}} \right).
\end{aligned} \tag{44}$$

In this case, term *I* refers to interference imposed by the cosets other than set $\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(1)}$ on the ρ_a -th detected sequence. Since $|\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)} \cap \tilde{\Xi}_{\chi_b, \mathbf{z}}^{(1)}| = 2^{Y_b}$ for one particular j , we conclude that there is only one case in term *II*. Additionally, owing to $F_b(\tilde{\Xi}_{\chi_a, \mathbf{z}}^{(j,1)}) = 0$ for the remaining $(2^{Y_a} - 2)$ possible j , it allows $(2^{Y_a} - 2)$ possibilities for the term *I*. The results of (44) satisfy (43) provided that $n_{ab} = 0$ and $n_{b,j} = 1$ for one j , $1 \leq j \leq 2^{Y_a} - 1$. This equation is also consistent with (32) in Lemma 2.

Based on the above results, after recovering vector $\widehat{\mathbf{P}}_{\rho_a} \mathbf{e}_1$, the \mathbf{y}_2 becomes

$$\begin{aligned} \mathbf{y}_2 &= \boldsymbol{\lambda}_{PRM, \rho_a}^{(1)} \cdot \mathbf{y}_1 \\ &= h_{\rho_a} \mathbf{C}_{\widehat{\mathbf{P}}_{\rho_a}, \mathbf{B}_{\rho_a}, \mathbf{I}_{\chi, \rho_a}} + \boldsymbol{\lambda}_{PRM, \rho_a}^{(1)} \cdot \left(h_{\rho_b} \mathbf{C}_{\widehat{\mathbf{P}}_{\rho_b}, \mathbf{B}_{\rho_b}, \mathbf{I}_{\chi, \rho_b}} + \mathbf{n} \right) \\ &= h_{\rho_a} \mathbf{C}_{\widehat{\mathbf{P}}_{\rho_a}, \mathbf{B}_{\rho_a}, \mathbf{I}_{\chi, \rho_a}} + \boldsymbol{\lambda}_{PRM, \rho_a}^{(1)} \cdot h_{\rho_b} \mathbf{C}_{\widehat{\mathbf{P}}_{\rho_b}, \mathbf{B}_{\rho_b}, \mathbf{I}_{\chi, \rho_b}} + \boldsymbol{\lambda}_{PRM, \rho_a}^{(1)} \cdot \mathbf{n}, \end{aligned} \quad (45)$$

where $\boldsymbol{\lambda}_{PRM, \rho_a}^{(1)}$ is the first layer projection operator for the user whose detection order is ρ_a . We can approximate the noise as a Gaussian random variable whose mean is 0 and whose variance is set to be $N_0^{(Y_a-1)} = \frac{|h_{\rho_b}|^2 + N_0}{2}$. In light of this, the following detection procedure in layer $2 \leq \tau \leq Y_a$ is equivalent to the recovery of the symmetric matrix $\widehat{\mathbf{P}}_{\rho_a}^{Y_{\rho_a}-1}$ in a single sequence scenario under the condition that the noise variance is $N_0^{(Y_a-1)}$. Since the ρ_a -th detected sequence can be successfully recovered if and only if both $\widehat{\mathbf{P}}_{\rho_a} \mathbf{e}_1$ and $\widehat{\mathbf{P}}_{\rho_a}^{Y_{\rho_a}-1}$ are correct, the successful detection probability of event “the ρ_k -th recovered sequence has been successfully detected” is

$$\Pr(\mathcal{B}_{\rho_a} | \mathbf{h}) = \Pr(\mathcal{P}_{\rho_a}^{(1)} | \mathbf{h}) \cdot \check{P}(Y_{\rho_a} - 1, N_0^{(Y_a-1)} | \mathbf{h}). \quad (46)$$

This result is consistent with (31) in Lemma 2.

Next, we assume that the sequence $\mathbf{C}_{\widehat{\mathbf{P}}_{\rho_a}, \mathbf{B}_{\rho_a}, \mathbf{I}_{\chi, \rho_a}}$ is ideally eliminated from the signal \mathbf{y} , the receiver proceeds to recover $\mathbf{C}_{\widehat{\mathbf{P}}_{\rho_b}, \mathbf{B}_{\rho_b}, \mathbf{I}_{\chi, \rho_b}}$, and we denote its probability of successful detection as $\Pr(\mathcal{B}_{\rho_b} | \mathcal{B}_{\rho_a}, \mathbf{h}) = \check{P}(Y_{\rho_b}, N_0 | h_{\rho_b})$.

As a next step, we will calculate the average probability of two sequences a and b being detected successfully. In the following two scenarios, the sequences a can be recovered:

- In the first instance, sequence a is detected successfully first, which has a chance of $\Pr(\mathcal{B}_a | \mathbf{h})$.
- In the second instance, sequence b is detected in priority with the probability of $\Pr(\mathcal{B}_b | \mathbf{h})$, followed by sequence a being detected from the subtracted signal with the probability $\Pr(\mathcal{B}_a | \mathcal{B}_b, \mathbf{h})$.

As a result, the probability that sequence a will be successfully detected equals

$$\check{P}(\mathcal{K}_a, m, N_0 | \mathbf{h}) = \Pr(\mathcal{B}_1 | \mathbf{h}) + \Pr(\mathcal{B}_2 | \mathbf{h}) \cdot \Pr(\mathcal{B}_1 | \mathcal{B}_2, \mathbf{h}). \quad (47)$$

The equation is consistent with (34) in Theorem 2. Finally, the average probability of successful detection equals

$$\check{P}_{\text{ave}}(\mathcal{K}_a, m, N_0 | \mathbf{h}) = \frac{1}{2} \int_{\mathbf{h}} \left\{ \prod_{\rho=1}^2 f_{\mathcal{CN}}(h_{\rho}; 0.1) \cdot \left(\check{P}_1(\mathcal{K}_a, m, N_0 | \mathbf{h}) + \check{P}_2(\mathcal{K}_a, m, N_0 | \mathbf{h}) \right) \right\}. \quad (48)$$

The equation is consistent with (35) in Theorem 2. \square

5. Simulation Results

In this section, we first examine the effectiveness of the proposed algorithms by evaluating the numerical simulation of the successful detection probability in Section 5.1. Additionally, in Section 5.2, a slot-controlled CCS scheme with the proposed iterative list projection algorithm in place of the origin inner decoder has been measured against several benchmarks.

5.1. Performances of the Algorithms 1 and 2

In this section, we will examine the detection capability of Algorithms 1 and 2, and our proposed scheme's performance is determined by computing the successful access probability. In the sequel, the received signal-to-noise ratio (SNR) at the AP is given by

$$\text{SNR}(\text{dB}) = \mathbb{E} \left[10 \lg \frac{\|\mathbf{y}^{(t)} - \mathbf{e}^{(t)}\|^2}{\|\mathbf{e}^{(t)}\|^2} \right]. \quad (49)$$

The successful detection probability is the mean proportion of determined active users to the system's overall number of active users.

As for the performance of Algorithm 1: Figure 6 compares the numerical simulation results of the list PRM projection algorithm (Algorithm 1) with the theoretical analysis results based on (13) for different settings of m . We fix $Y = m$, $H = 1$, and the transmit power of an active user is normalized to one. This figure illustrates that, although we employed Gaussian approximation during the theoretical analysis process, the numerical simulation results and the theoretical analysis are closely matched, and definitely, the difference between the two simulations is the result of the Gaussian approximations. Thus, this result confirms the correctness of the theoretical analysis in Lemma 1. In addition, comparing the successful detection probability for different m , we find that the performance of the list PRM projection algorithm improves as the sequence length increases, further validating the conclusion in Section 4.1.

Next, we will compare the performance of the list PRM projection algorithm (Algorithm 1) with the existing decoding compressed sensing algorithm for RM sequences as the common codebook for all active users in a random access system. The numerical simulation results are shown in Figure 7, where "Origin PRM" and "List PRM" represent the origin projection detection algorithm in [37] and its list version (Algorithm 1), respectively. "RM LLD" represents the RM sequence detection algorithm proposed in Reference [33], which is based on the shift-and-multiply operation on the received signal, and "List RM LLD" represents its list version detection. For all algorithms, we set the sequence length to $N = 2^8$ and the list size to $H = 8$. As can be seen from Figure 7, the successful detection probabilities of all algorithms are close to one when the signal-to-noise ratio (SNR) is larger than -2 dB. However, the "RM LLD" algorithm suffers from severe performance degradation under low SNR conditions compared to the "Origin PRM", which shows strong robustness. In addition, due to the enhanced list detection, the "List RM LLD" and the "List PRM" provide a more outstanding performance gain under lower SNR when compared with no candidate-saving algorithms.

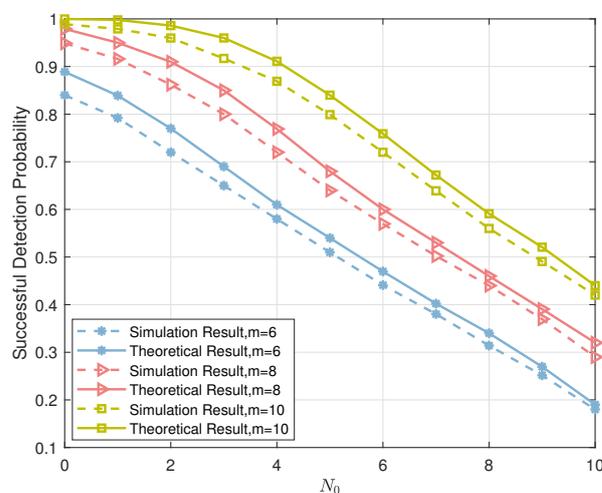


Figure 6. The comparison of numerical simulation results and theoretical analysis results of list PRM projection algorithm.

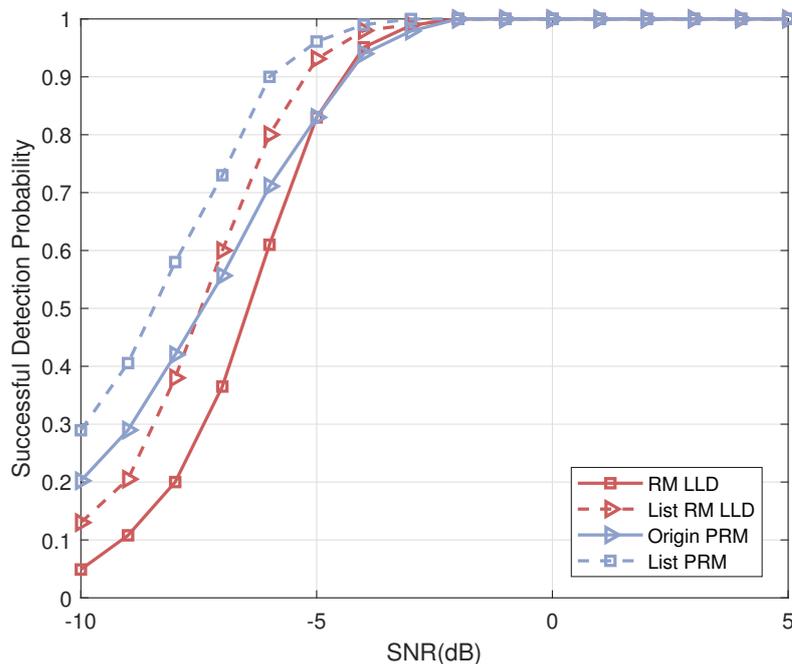


Figure 7. The successful detection probability versus SNR for different schemes, $m = 8$.

As for the performance of Algorithm 2: in Figure 8, we compare the numerical simulation results of the iterative list PRM projection detection (Algorithm 2) with the theoretical analysis results derived from Lemma 2. We set the number of iterations in the numerical simulation 1. From Figure 8, the theoretical analysis results fit the numerical simulation results well, especially under high SNR conditions, thus verifying the correctness of Theorem 2.

In addition, both simulation and theoretical results show that the detection capability of the algorithm decreases as the number of active users in the system increases.

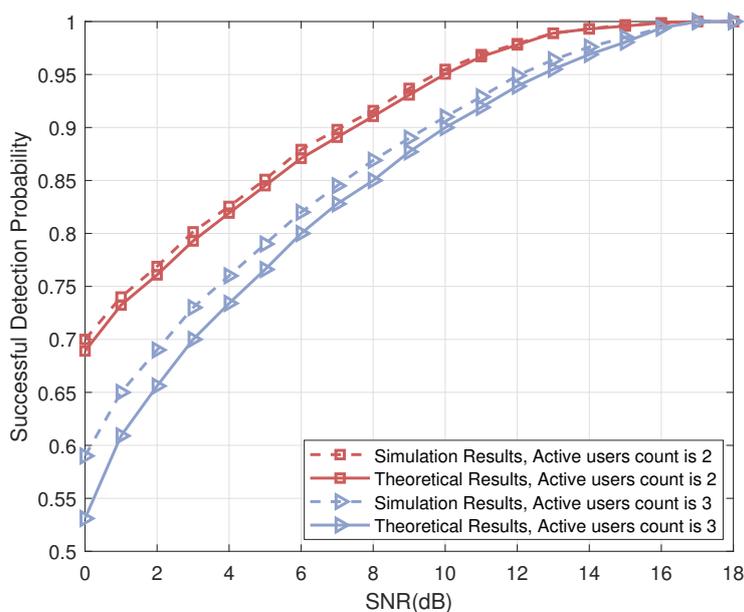


Figure 8. The successful detection probability of Algorithm 1 versus SNR.

5.2. Iterative List PRM Projection Algorithm-Based Slot-Controlled URA

In this section, we combine an inner code employing an iterative list PRM projection detector as the decoder with two types of practicable outer codes (t -tree and Reed–Solomon

codes) to form a slot-pattern control-based CCS system (as illustrated in Section 2). We demonstrate the positive effects of the proposed algorithms on the overall system via simulation results. We consider a communication system in which each user transmits $B = 100$ bits by employing a H_N length G -ary outer-code using $T = 2^{15}$ channel uses. The H_N positions are carefully selected within N_T chunks. There are G codewords in the inner codebook, each of which has a length of $N = T/N_T$. We employ the PRM sequence under one rank Y rather than all ranks in this section, and Algorithm 2 is used to decode the inner codes for multi-sequence scenarios. The energy efficiency of different schemes is plotted as follows: energy efficiency is the minimum E_b/N_0 over the possible scheme-specific parameters in the URA scheme, $P_e < 0.1$ is the probability of error constraint for each user, and $P_f < 0.001$ is the FAR (false-alarm rate) constraint. Numerical results are presented in Figure 9.

This section first compares the numerical simulations of the enhanced slot-controlled URA system where the outer-code is a t -tree code with some benchmarks. We cite benchmarks as follows: We denote a “list PRM-tree” scheme that concatenates the inner-code with an OMP decoder to an outer decoder that can correct up to t errors for various setups, i.e., the benchmarks called “ $t = 3$, list PRM-tree, $H = 1$ ”, “ $t = 2$, list PRM-tree, $H = 1$ ” and “ $t = 1$, list PRM-tree, $H = 1$ ” are plotted in light blue in Figure 9. These benchmarks are drawn from Reference [27] and named “PRM-RS” in Reference [27]. We employ blue lines to illustrate the simulations for the proposed “ $t = 3$, iterative list PRM-tree, $H = 8$ ”, “ $t = 2$, iterative list, $H = 8$ ” and “ $t = 1$, iterative list PRM-tree, $H = 8$ ” schemes. Specifically, for these proposed “iterative list PRM-tree, $H = 8$ ” schemes, the PRM sequences are employed as the inner codewords, in which the former x_p -bit message is filled with the selected SPC, and the remaining J -bit is used to transport the user’s messages. The enhanced Iterative list PRM projection algorithm is adopted in order to jointly recover the list of messages and the channel estimations of all sequences within one slot. Moreover, the decoder capable of correcting t errors continues to make up the outer code. A greedy information bit allocation method is applied to all list PRM-tree schemes, where each subsequent slot is assigned the maximum amount of information bits while maintaining the $\mathbb{E}[|V_i|] \leq 2^{25}$ constraint and finding the minimum E_b/N_0 . The energy efficiency is the minimum power needed to serve K_a users with the per-user probability of error less than 0.1, we depict the curves in the blue line in Figure 9 under the optimal setups. The optimal setups of H_N , N , N_T , G , J and x_p are shown in Table 2. From Table 2, we find that the outer-code length $H_N = 32$ is used for $t = 1$ and $H_N = 64$ for $t = 2, 3$, which is due to the fact that the latter case performs relatively poorly since it has a greater number of simultaneous appearances, which leads to inner-code failure at $K_a = 185$ for $t = 1$, $K_a = 110$ and $K_a = 130$ for $t = 2$ and $t = 3$, respectively, under “list PRM-tree, $H = 1$ ” schemes; $K_a = 220$ for $t = 1$, $K_a = 125$ and $K_a = 150$ for $t = 2$ and $t = 3$, respectively, when conducting “iterative list PRM-tree, $H = 8$ ” schemes.

Next, we will compare the numerical simulations of the enhanced slot-controlled URA system where the outer-code is a Reed–Solomon code with some benchmarks. We cite benchmarks as follows: We denote the CCS scheme that concatenates the inner codes whose distribution is i.i.d. uniform on the power shell to an outer Reed–Solomon code as the “RS scheme” (it is named “Reed–Solomon scheme” in Reference [27]), and we use it as the first benchmark. Furthermore, the scheme called “list PRM-RS, $H = 1$ ” is directly drawn from Reference [37] as the second benchmark (it is named “PRM-RS” in Reference [37]), and this slot-controlled URA scheme “list PRM-RS, $H = 1$ ” that is described in the system model (Section 2) does not employ the enhanced detection algorithms. Additionally, the “iterative list PRM-RS, $H = 1$ ” scheme is the proposed scheme whose multi-user inner-code detector is substituted by Algorithm 2 without saving candidates while calling Algorithm 1 (since $H = 1$), whereas the proposed “iterative list PRM-RS, $H = 8$ ” scheme keeps $H = 8$ candidates during each layer while conducting Algorithm 1. The optimal setups of “list PRM-RS, $H = 1$ ”, “iterative list PRM-RS, $H = 1$ ” and “iterative list PRM-RS, $H = 8$ ” are shown in Table 3, and the energy efficiency outcomes are illustrated in Figure 9.

Table 2. URA system parameters for “PRM-tree” scheme.

Parameter Description	Specific Value
PRM sequence length, $N = 2^m$	2^7
The length of RS codes, H_N	$2^5(t = 1)/2^6(t = 2, 3)$
The number of slots, N_T	2^8
The number of complex channel uses, T	2^{15}
The length of slot-occupation control, x_p	$9(t = 1)/7(t = 2, 3)$
G -ary	$19(t = 1)/15(t = 2, 3)$
J -ary	$10(t = 1)/8(t = 2, 3)$
The capacity of PRM codebook, $ \Gamma_Y $	$286720(t = 1)/21504(t = 2, 3)$
The code rate	$0.3125(t = 1)/0.1953(t = 2, 3)$

Table 3. URA system parameters for “RS” scheme.

Parameter Description	Specific Value
PRM sequence length, $N = 2^m$	2^7
The length of RS codes, H_N	2^5
The number of slots, N_T	2^8
The number of complex channel uses, T	2^{15}
The length of slot-occupation control, x_p	9
G -ary	15
J -ary	6
The capacity of PRM codebook, $ \Gamma_Y $	21504
The code rate of RS	0.5208

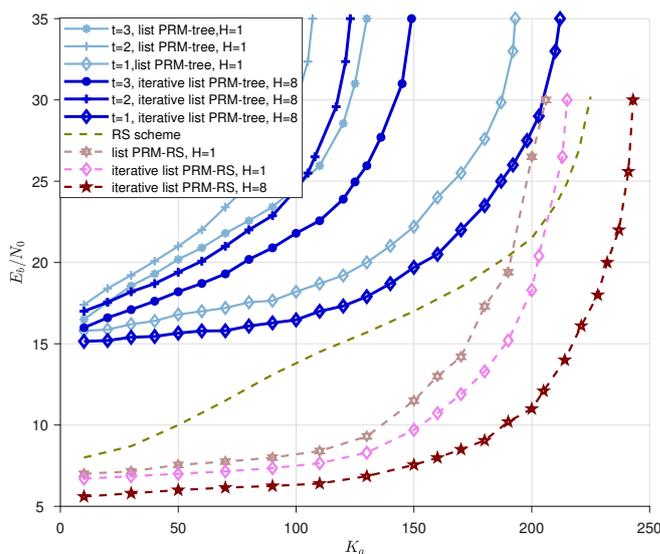


Figure 9. The simulations of energy efficiency are depicted. The simulations are listed as follows: list PRM-tree scheme for $t = 1, \dots, 3$ from [37], iterative list PRM-tree scheme for $t = 1, \dots, 3$, Reed-Solomon scheme from [27], list PRM-RS scheme without iteration form [37], and iterative list PRM-RS schemes for $H = 1$ and $H = 8$, respectively.

From the simulations depicted in Figure 9, the following observations can be drawn:

1. As for all “List PRM-tree” schemes, since the outer-code length $H_N = 32$ is suitable for scheme $t = 1$ and $H_N = 64$ for $t = 2, 3$ cases, the former case ($t = 1$ case) can accommodate more active users than $t = 2, 3$ owing to a smaller number of simultaneous appearances in each slot (the outer code length affects the probability of appearance over slots. See more setup details in Table 2). Additionally, a higher t for the outer code increases performance when the inner code has the same length. Therefore, $t = 3$ is superior to $t = 2$. Furthermore, when comparing the curves of “list PRM-tree” and “iterative list PRM-tree”, we conclude that the enhanced inner code with the proposed iterative list projection algorithm can help the entire system lower the energy-per-bit requirement to meet a target error probability as well as boost the ability to accommodate more users’ transmission.
2. Figure 9 illustrates how the “iterative list PRM-RS, $H = 1$ ” curve outperforms the “list PRM-RS, $H = 1$ ” curve regarding energy consumption when the number of active users is fixed. This observation is an unambiguous demonstration of the benefit of Algorithm 2, which carries out iterative detection.
3. When compared with different schemes of “iterative list PRM-RS, $H = 1$ ” and “iterative list PRM-RS, $H = 8$ ”, we demonstrate that the performance of the detection can be refined by raising the count of candidates in the first few layers, thereby confirming the significance of Algorithm 1, which guarantees the first few layers’ reliable recoveries.

The per-user error probability P_e as a function of E_b/N_0 for $K_a = 130, 180$ and 200 for the “list PRM-RS, $H = 1$ ”, “iterative list PRM-RS, $H = 1$ ” and “iterative list PRM-RS, $H = 8$ ” schemes are obtained (in Figure 10). The optimal system parameters are depicted in Table 3. It can be seen from Figure 10 that:

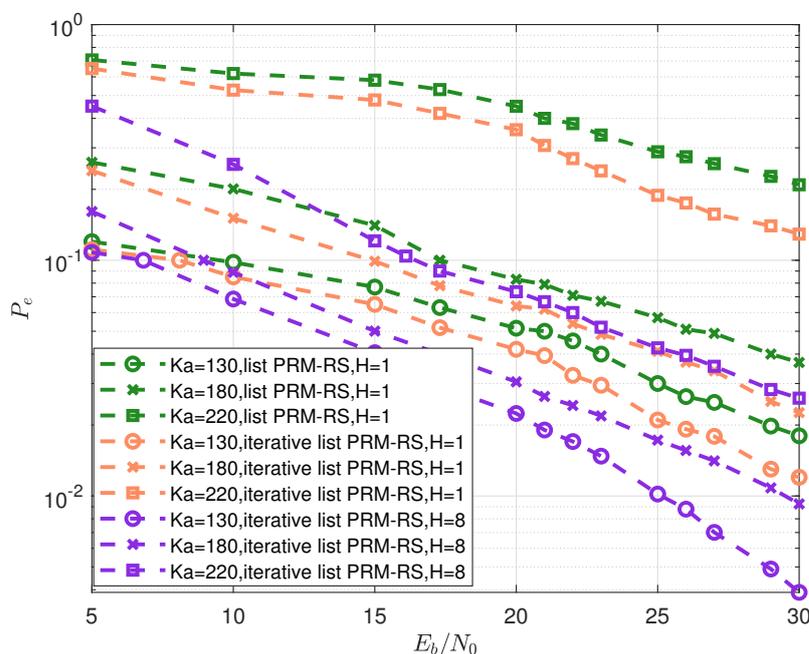


Figure 10. Probability of error P_e vs. E_b/N_0 for $K_a = 130, 180$ and 220 under three schemes, i.e., “list PRM-RS, $H = 1$ ”, “iterative list PRM-RS, $H = 1$ ” and “iterative list PRM-RS, $H = 8$ ”.

1. For “list PRM-RS, $H = 1$ ” and “iterative list PRM-RS, $H = 1$ ” schemes, the minimum P_e exceeds 0.1 when the user count reaches 220. Besides, the minimum P_e for “iterative list PRM-RS, $H = 8$ ” schemes below 0.1 when E_b/N_0 is beyond 16dB.
2. The simulation curves in Figure 10 are consistent with the performances in Figure 9, i.e., for “list PRM-RS, $H = 1$ ” and “iterative list PRM-RS $H = 1$ ” schemes, when

the number of users exceeds 205 and 213, respectively, the number of simultaneous transmissions exceeds the identifiable maximum.

For “iterative list PRM-RS, $H = 8$ ” schemes, when the number of users exceeds 243, the number of simultaneous transmissions exceeds the identifiable maximum.

6. Conclusions

In this paper, we address a packetized and slotted transmission CCS framework which concatenates an inner PRM code to an outer error correction code. First, we improve the decoder of the inner-code: we propose an enhanced algorithm that makes use of multiple candidates so as to remedy the venture of spreading errors. On this basis, an iterative list PRM projection algorithm is proposed for the multi-sequence scenario. We then deduce the theoretical probabilities of the list projection and iterative list projection detection methods. Via numerical simulations, we indicate the theoretical and the simulation results agreed. Finally, we implement the iterative list PRM projection algorithm in two practical error-correction codes. From the simulation results, we conclude that the packetized URA with the proposed iterative list projection detection works better than benchmarks in terms of the number of active users it can support in each slot and the amount of energy needed per bit to meet an expected error probability.

Additional interesting research avenues include: (i) the PRM-based system can be expanded to support multiple antennas; (ii) the decomposition of the Clifford matrix \mathbf{G}_F associated with the patterned RM code can be considered as a transmitter’s information reconstruction, and the iterative approach is generalized at the receiver.

Author Contributions: Methodology, W.X. and H.Z.; software, W.X. and R.T.; validation, W.X.; formal analysis, W.X. and R.T.; investigation, W.X. and R.T.; resources, W.X.; data curation, W.X.; writing—original draft preparation, W.X.; writing—review and editing, W.X. and R.T.; visualization, W.X. and R.T.; supervision, H.Z.; project administration, H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Saad, W.; Bennis, M.; Chen, M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Netw.* **2019**, *34*, 134–142. [[CrossRef](#)]
2. Guo, F.; Yu, F.R.; Zhang, H.; Li, X.; Ji, H.; Leung, V.C. Enabling massive IoT toward 6G: A comprehensive survey. *IEEE Internet Things J.* **2021**, *8*, 11891–11915. [[CrossRef](#)]
3. Pan, C.; Mehrpouyan, H.; Liu, Y.; Elkashlan, M.; Arumugam, N. Joint pilot allocation and robust transmission design for ultra-dense user-centric TDD C-RAN with imperfect CSI. *IEEE Wirel. Commun.* **2018**, *17*, 2038–2053. [[CrossRef](#)]
4. Chettri, L.; Bera, R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. *IEEE Internet Things J.* **2020**, *7*, 16–32. [[CrossRef](#)]
5. Masoudi, M.; Azari, A.; Yavuz, E.A.; Cavdar, C. Grant-free radio access IoT networks: Scalability analysis in coexistence scenarios. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
6. Shahab, M.B.; Abbas, R.; Shirvanimoghaddam, M.; Johnson, S.J. Grant-free non-orthogonal multiple access for IoT: A survey. *IEEE Commun. Surv. Tut.* **2020**, *22*, 1805–1838. [[CrossRef](#)]
7. Chen, X.; Chen, T.Y.; Guo, D. Capacity of Gaussian many-access channels. *IEEE Trans. Inf. Theory* **2017**, *63*, 3516–3539. [[CrossRef](#)]
8. Polyanskiy, Y. A perspective on massive random-access. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 2523–2527.
9. Chen, Z.; Sohrabi, F.; Yu, W. Sparse activity detection for massive connectivity. *IEEE Trans. Signal Process.* **2018**, *66*, 1890–1904. [[CrossRef](#)]
10. Liu, L.; Yu, W. Massive connectivity with massive MIMO—Part I: Device activity detection and channel estimation. *IEEE Trans. Signal Process.* **2018**, *66*, 2933–2946. [[CrossRef](#)]

11. Senel, K.; Larsson, E.G. Grant-free massive MTC-enabled massive MIMO: A compressive sensing approach. *IEEE Trans. Commun.* **2018**, *66*, 6164–6175. [[CrossRef](#)]
12. Yang, L.; Fan, P.; Li, L.; Ding, Z.; Hao, L. Cross validation aided approximated message passing algorithm for user identification in mMTC. *IEEE Commun. Lett.* **2021**, *25*, 2077–2081. [[CrossRef](#)]
13. Zadik, I.; Polyanskiy, Y.; Thrampoulidis, C. Improved bounds on Gaussian MAC and sparse regression via Gaussian inequalities. In Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 430–434.
14. Ngo, K.H.; Lancho, A.; Durisi, G. Unsourced multiple access with random user activity. *IEEE Trans. Inf. Theory* **2023**, *69*, 4537–4558. [[CrossRef](#)]
15. Ordentlich, O.; Polyanskiy, Y. Low complexity schemes for the random access Gaussian channel. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 2528–2532.
16. Marshakov, E.; Balitskiy, G.; Andreev, K.; Frolov, A. A polar code based unsourced random access for the Gaussian MAC. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
17. Pradhan, A.K.; Amalladinne, V.K.; Vem, A.; Narayanan, K.R.; Chamberland, J.F. Sparse IDMA: A Joint Graph-Based Coding Scheme for Unsourced Random Access. *IEEE Trans. Commun.* **2022**, *70*, 7124–7133. [[CrossRef](#)]
18. Ahmadi, M.J.; Duman, T.M. Random spreading for unsourced MAC with power diversity. *IEEE Commun. Lett.* **2021**, *25*, 3995–3999. [[CrossRef](#)]
19. Pradhan, A.K.; Amalladinne, V.K.; Narayanan, K.R.; Chamberland, J.F. LDPC Codes with Soft Interference Cancellation for Uncoordinated Unsourced Multiple Access. In Proceedings of the IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
20. Amalladinne, V.K.; Chamberland, J.F.; Narayanan, K.R. A Coded Compressed Sensing Scheme for Unsourced Multiple Access. *IEEE Trans. Inf. Theory* **2020**, *66*, 6509–6533. [[CrossRef](#)]
21. Amalladinne, V.K.; Vem, A.; Soma, D.K.; Narayanan, K.R.; Chamberland, J.F. A coupled compressive sensing scheme for unsourced multiple access. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; pp. 6628–6632.
22. Lancho, A.; Fengler, A.; Polyanskiy, Y. Finite-blocklength results for the A-channel: Applications to unsourced random access and group testing. In Proceedings of the 2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 28–30 September 2022; pp. 1–8.
23. Amalladinne, V.K.; Pradhan, A.K.; Rush, C.; Chamberland, J.F.; Narayanan, K.R. Unsourced random access with coded compressed sensing: Integrating AMP and belief propagation. *IEEE Trans. Inf. Theory* **2022**, *68*, 2384–2409. [[CrossRef](#)]
24. Andreev, K.; Rybin, P.; Frolov, A. Reed-Solomon coded compressed sensing for the unsourced random access. In Proceedings of the 2021 17th International Symposium on Wireless Communication Systems (ISWCS), Berlin, Germany, 6–9 September 2021; pp. 1–5.
25. Che, J.; Zhang, Z.; Yang, Z.; Chen, X.; Zhong, C.; Ng, D.W.K. Unsourced random massive access with beam-space tree decoding. *IEEE J. Sel. Areas Commun.* **2021**, *40*, 1146–1161. [[CrossRef](#)]
26. Fengler, A.; Haghghatshoar, S.; Jung, P.; Caire, G. Non-Bayesian Activity Detection, Large-Scale Fading Coefficient Estimation, and Unsourced Random Access With a Massive MIMO Receiver. *IEEE Trans. Inf. Theory* **2021**, *67*, 2925–2951. [[CrossRef](#)]
27. Andreev, K.; Rybin, P.; Frolov, A. Coded Compressed Sensing with List Recoverable Codes for the Unsourced Random Access. *IEEE Trans. Commun.* **2022**, *70*, 7886–7898. [[CrossRef](#)]
28. Liang, Z.; Zheng, J.; Ni, J. Index modulation-aided mixed massive random access. *Front. Commun. Networks* **2021**, *2*, 694557. [[CrossRef](#)]
29. Fengler, A.; Jung, P.; Caire, G. SPARCs for unsourced random access. *IEEE Trans. Inf. Theory* **2021**, *67*, 6894–6915. [[CrossRef](#)]
30. Ebert, J.R.; Amalladinne, V.K.; Rini, S.; Chamberland, J.F.; Narayanan, K.R. Coded demixing for unsourced random access. *IEEE Trans. Signal Process.* **2022**, *70*, 2972–2984. [[CrossRef](#)]
31. Zhang, L.; Luo, J.; Guo, D. Neighbor discovery for wireless networks via compressed sensing. *Perform. Eval.* **2013**, *70*, 457–471. [[CrossRef](#)]
32. Zhang, H.; Li, R.; Wang, J.; Chen, Y.; Zhang, Z. Reed-Muller sequences for 5G grant-free massive access. In Proceedings of the GLOBECOM 2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7.
33. Wang, J.; Zhang, Z.; Hanzo, L. Joint active user detection and channel estimation in massive access systems exploiting Reed-Muller sequences. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 739–752. [[CrossRef](#)]
34. Wang, J.; Zhang, Z.; Hanzo, L. Incremental massive random access exploiting the nested Reed-Muller sequences. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 2917–2932. [[CrossRef](#)]
35. Calderbank, R.; Thompson, A. CHIRRRUP: A practical algorithm for unsourced multiple access. *Inform. Inference J. IMA* **2020**, *9*, 875–897. [[CrossRef](#)]
36. Wang, J.; Zhang, Z.; Chen, X.; Zhong, C.; Hanzo, L. Unsourced massive random access scheme exploiting reed-muller sequences. *IEEE Trans. Commun.* **2020**, *70*, 1290–1303. [[CrossRef](#)]
37. Xie, W.; Zhang, H. Patterned Reed-Muller Sequences with Outer A-Channel Codes and Projective Decoding for Slot-Controlled Unsourced Random Access. *Sensors* **2023**, *23*, 5239. [[CrossRef](#)] [[PubMed](#)]
38. Pllaha, T.; Tirkkonen, O.; Calderbank, R. Binary subspace chirps. *IEEE Trans. Inf. Theory* **2022**, *68*, 7735–7752. [[CrossRef](#)]

39. Pllaha, T.; Tirkkonen, O.; Calderbank, R. Reconstruction of multi-user binary subspace chirps. In Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 21–26 June 2020; pp. 531–536.
40. Tirkkonen, O.; Calderbank, R. Codebooks of complex lines based on binary subspace chirps. In Proceedings of the 2019 IEEE Information Theory Workshop (ITW), Visby, Sweden, 25–28 August 2019; pp. 1–5.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.