IMPROVING PHYSICAL LAYER GROUP KEY GENERATION EFFICIENCY IN 5G WIRELESS NETWORKS

by

Long Jiao

A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
In Partial fulfillment of
The Requirements for the Degree
of
Master of Science
Electrical Engineering

Committee:

_____ Dr. Kai Zeng, Thesis Director

_____ Dr. Brian L. Mark, Committee Member

_____ Dr. Parth Pathak, Committee Member

_____ Dr. Monson H. Hayes, Department Chair

Date: _____ Spring 2022
George Mason University
Fairfax, VA

Improving Physical Layer Group Key Generation Efficiency in 5G Wireless Networks

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science at George Mason University

By

Long Jiao
Bachelor of Science
Xidian University, 2016

Director: Dr. Kai Zeng, Professor
Department of Electrical and Computer Engineering

Spring 2022
George Mason University
Fairfax, VA

Dedication

I dedicate this thesis to my parents and my wife.

Acknowledgments

Many thanks to my adviser, Dr. Kai Zeng, for his invaluable and insightful instruction and continuous encouragement. I would like to sincerely thank Prof. Brain L. Mark and Prof. Parth Pathak for being my committee members and their encouraging words and thoughtful feedback. Thank you to my parents and wife, for your endless support and unconditional love.

Table of Contents

List of Tables

List of Figures

Abstract

IMPROVING PHYSICAL LAYER GROUP KEY GENERATION EFFICIENCY IN 5G WIRELESS NETWORKS

Long Jiao

George Mason University, 2022

Thesis Director: Dr. Kai Zeng

In this thesis, we investigate the scheme to improve the group secret key generation efficiency in 5G mmWave Massive MIMO networks by enhancing the efficiency of channel probing for group key generation. A new channel probing strategy for star-topology networks group key generation is proposed, which focuses on multiplexing of downlink probing signals to perform the downlink channel probing concurrently. The hybrid precoder has been considered in this scenario to mitigate the inter-group interference, which includes a analog precoder and baseband precoder. To further balance the group key rates, a genetic algorithm (GA) based power allocation algorithm is developed to allocate more power to the nodes with unfavorable channel conditions. What's more, we propose a scheme to estimate group key rates based on the maximum likelihood estimator (MLE) so that we can estimate the group key rates based on the probing samples. Various numerical results are provided including the group key rates and bits disagreement ratio (BDR). The numerical results show that the GA-based downlink channel probing scheme can increase the efficiency of channel probing and have higher group key rates compared with the existing channel probing schemes. When the SNR is 25dB, the key rates of GA-based power allocation scheme are 20% higher than the scheme with the conventional channel probing strategy.

Chapter 1: Introduction

1.1 Background and Motivation

Thanks to the emerging fifth generation (5G) technologies, such as millimeter wave (mmWave), massive MIMO and hybrid precoding, 5G wireless communication are supposed to be the key enabler to satisfy the increasing demand for data service like ultra-reliable communication, massive machine type communication and so on [1–3]. To ensure the secure and reliable communication service, the efficient and lightweight security mechanism is desired in the design of 5G networks. To this end, we focus on the security of 5G mmWave wireless networks and consider physical layer key generation in the aforementioned networks.

Different from the traditional Diffie-Hellman (D-H) key exchange mechanism, physical layer key generation mechanisms do not require expensive computation and have the potential to achieve information-theoretic security. For instance, instead of relying on D-H key exchange, physical layer key generation is based on the principle of channel reciprocity. That is, within the channel coherence time, two wireless devices, operating on the TDD-mode, can observe a similar small-scale wireless channel fading induced by the multipath effect, so that the identical secret bits can be extracted independently at the both side by the sampling the common radio channel between them. In this thesis, we focus on the physical layer group key generation, which is an extension of the concept of physical layer key generation. For instance, physical layer group key generation extends the pair-wise physcial layer key generation to a multiple-node scenario. Here multiple wireless nodes in a group aim to generate the common secret key shared among the group members, independently by observing the randomoness extracted from the wireless channels.

Although significant efforts and progress on physical layer group key generation have been made in recent years [4–9], there are many roadblocks need to be addressed. First,

the sequential channel probings conducted to obtian the channel measurements between any two nodes in the same group can cause huge overhead. For example, for multi-user mmWave wireless networks operating in the time division duplex (TDD) mode [2], the bi-directional channel probings are required, which are performed sequentially. As the increasing of the group size, the time spent on a single-round channel probing for all of group members can grow rapidly. At the same time, the number of channel measurements that can be observed in a given time period will be limited as well. In this manner, the scalarbility of physical layer group key generation can be limited by the large communication overhead.

To tackle the challenge mentioned above, techniques like multi-user multiplexing in 5G mmWave communication networks can be utilized to improve the efficiency of channel probings, especially for the networks with the star-topology. In this thesis, we propose an efficient channel probing scheme for star-topology wireless networks. Please note, the proposed scheme can be extended to the ring-topology and mesh networks with further efforts. To achieve the concurrent tranmission at the downlink stage to improve the channel probing efficiency, a baseband (BB) precoder is applied to combine with the analog precoder, which is a new concept named as the hybrid precoding [2]. In the downlink channel probing, the channel probing signals of several edge nodes (ENs) are multiplexed in a single slot for channel probing, which enables the central node (CN) to send downlink probing signals to ENs concurrently. For example, for M ENs, in TDD mode, the existing probing schemes need $2M$ channel probings while in our scheme, only $M + 1$ channel probings are required. Such a function is enabled by BB precoder within the hybrid precoder. By allowing to set a precoder at baseband, hybrid precoding provides the design of freedom to have each downlink effective channel approximately orthogonal to other downlink effective channels.

Secondly, to further improve the efficiency of downlink channel probing and increase the group key rate per channel probing, we model the power allocation for group key generation as a multi-objective optimization problem and propose a power allocation algorithm for downlink channel probing. At each algorithm run, GA applies the genetic operator to get the offspring population produced by the parent population. To avoid the algorithm wandering

in the infeasible searching region, non-dominant sorting genetic algorithm (NSGA II) [10] is incorporated in the power allocation scheme. The assignment of the transmission power on each downlink stream is determined by NSGA II, which can guide to a spread-out solution set for power allocation parameters and avoid the local optimality.

What's more, to quantify the performance of the group key rate for the proposed downlink channel probing scheme and the GA-based power allocation algorithm, the group key rate at each round is approximated/estimated via maximum likelihood estimator (MLE). For instance, at first, the group key rates are decoupled and represented as the combination of several joint entropy. In the second step, parameters defining the distribution of each joint entropy are estimated based on the MLE. Finally, with the estimated parameters, the group key rates are computed. The numerical results show that the group key rates after estimation and the rates based on theoretical derivations are in good agreement.

1.2 Contributions of Thesis

To sum up, regarding the challenges reside in existing group key generation schemes, the main contributions of this paper are summarized as below:

- We investigated the channel probing efficiency in the physical layer group key generation. Two different network topologies are discussed: star-topology and chain-topology.
- The downlink channel probing scheme for the star-topology networks, based on hybrid precoding, has been proposed and carefully investigated. Please note, due to the reason star-topology is the most common network topology, we focus on the star-toplogy in this work. In future work, the proposed scheme will be extended to ring-topology and mesh networks.
- To further improve the group key rates, a GA-based power allocation algorithm is developed to achieve the Pareto optimality, which can efficiently improve the performance.

- To have a better estimation on the key rate, a fast group key rate estimation method based on MLE is proposed and its performance is discussed later.

1.3 Notations and Abbreviations

In this paper, boldface lowercase letters represent vectors and matrices are represented by boldface uppercase letters. $(\cdot)^\star$ and $(\cdot)^H$ denote the conjugate and the conjugate transpose operations, respectively. $|\mathcal{A}|$ represents the size of a set $\mathcal{A}$. $||\mathbf{a}||^2$ stands for the squared 2-norm of vector $\mathbf{a}$. $\mathbf{max}(\cdot)$ denotes the element-wise maximization. $\mathcal{C}^{M\times N}$ represents the space of complex-valued matrices with the size $M \times N$. We use $\mathcal{R}\{\cdot\}$ to denote the real part of its argument.

1.4 Organization of Thesis

In Chapter 2, we introduce the specifications of our system, the basic concept of physical layer group key generation including its challenges and current network topologies. After this, the link initialization, uplink, and downlink channel probing are introduced later. In the following chapter 3, the existing group key generation schemes are introduced. In chapter 4, the proposed downlink channel probing scheme is introduced. Specifically, the multiplexing of downlink probing signals, enabled by hybrid precoding, is discussed in detail. Besides, the group key generation protocol utilized in this work is also introduced. In Section 5.1, we will give an tutorial on the genetic algorithm at first and then the GA-based power allocation algorithm for physical layer group key generation is presented. By the end of this chapter, some numerical results are shown, while the conclusions and future work are listed in Chapter 6.

Table 1.1: Summary of abbreviations

5G	the fifth generation
D-H	Diffie-Hellman
mmWave	millimeter wave
TDD	time division duplex mode
BB	baseband
CN	central node
EN	edge node
MLE	maximum likelihood estimator
GA	genetic algorithm
SNR	signal-to-noise ratio
MIMO	multiple-input multiple-output
MSE	mean-squared-error
CSI	channel state information
SCA	successive convex approximation
ADMM	alternating direction method of multipliers
BDR	bits disagreement ratio
RSS	received signal strength
NSGA	Non-dominant Sorting Genetic Algorithm
ULA	Uniform linear array
RF	radio-frequency
NOVA	Northern Virginia
CCI	Commonwealth Cyber Initiative

Chapter 2: Preliminaries

In this chapter, we will introduce some preliminaries on the system model and techniques adopted in this work including the physical layer group key generation and so on. The schemes for downlink and uplink channel probings are given in 2.3.

2.1 System Model

We assume all of the nodes operate in the TDD mode and at mmWave frequency band (28GHz). In the scope of this paper, there are M ($M \geq 3$) nodes, wishing to generate a common group secret key through wireless fading channels under a passive eavesdropper.

Due to the limitation of pages, we will start with a star network, which is most commonly seen in practice, such as WLAN and cellular networks. In the network, we have M nodes $\mathcal{M} = \{1, 2, ..., M\}$, where $\mathcal{M}$ consists of a CN $c \in \mathcal{M}$, e.g., base station (BS) or access point (AP), and $M-1$ ENs. Each node $m \in \mathcal{M} \setminus c$. Each EN and CN are equipped with N_{EN} and N_{CN} antennas. What's more, the number of RF chains at every central node is N_{RF}, which affects the maximum number of users that can be simultaneously served by the central node [2]. Moreover, we assume that the reciprocity of mmWave channels between two nodes holds for the downlink and uplink. We adopt the narrow band block fading channel models, as specified in [1, 2, 11], which are constant over multiple channel slots, and change randomly at the beginning of the next block.

Before bi-directional channel estimations, none of the nodes have the prior channel state information (CSI). However, the distributions of CSI are available at each node. For simplicity, the distribution coefficients of channel gains defined in [1, 2, 11] are applied in this work and the developed scheme can be easily extended to other coefficients. Please note that the above assumptions have been widely used in existing works.

2.2 Physical Layer Group Key Generation

2.2.1 Concept and challenges

Physical layer group key generation aims to generate the shared secret at each node in the network based on the random channel measurements. The group size or the node numbers in the network can be varied but most of time the group size must be greater than three.

This problem can be a challenging because of the following factors:

1. The reciprocity of wireless channels which are contaminated by the noise at the channel estimation stage, can be weakened or even doesn't hold well due to the accumulated noise as the group size increasing. The appropriate group key generation protocols is highly desired to prevent the noise accumulation in the channel measurements.

2. Most importantly, physical layer key generation must rely on the reciprocial wireless channels to establish the shared secret key and nodes in the group have to operate on the same frequency in a TDD mode. To collect the channel measurement samples from all of nodes, channel probing is usually conducted in a sequential manner. As the network size expanding, the channel probing overhead will increase as well. The large channel probing overhead limits the number of channel measurements observed in a give time period, which thus limits the group key generation rate. Therefore, how to decrease the channel probing overhead in group key generation is an interesting topic.

2.2.2 Network Topologies for Group Key Generation

Star topology

The first one is when all wireless devices inside the group under consideration are within each other's communication range, which means any two devices are directly connected. For example, a group of nodes are randomly scattered in a region but locates within the communication range of each other and they would like to establish the shared secret key among them. In this scenario, we can randomly choose one device as the virtual central

node (CN) and the rest of the devices as the edge node (EN). All of CN and ENs in the group form a network with the star topology. As mentioned above, this type of topology is common in the practice for instance the cellular communication and the wifi communication systems. The function of the virtual CN is to facilitate the group key extraction by passing the broadcasted information of key generation to other nodes so that the key generation can be performed in a collaborative way.

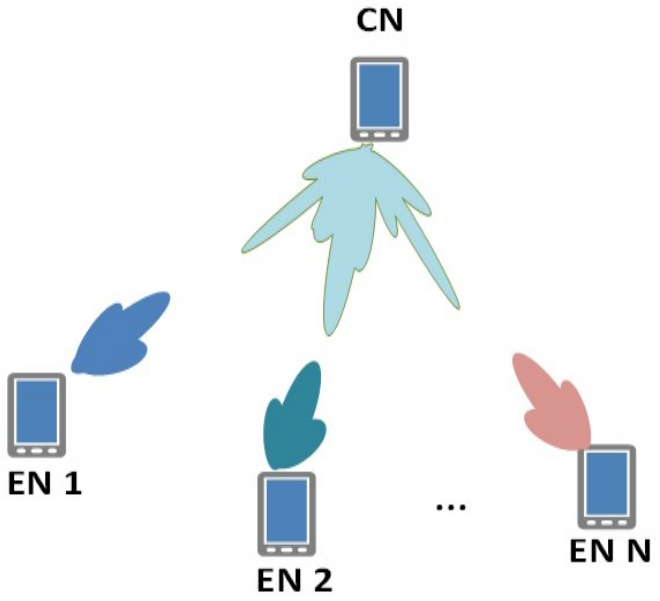


Figure 2.1: Star Topology

In Fig. 2.1, one node, denoted by, is randomly selected as the CN and the rest of nodes scatter around the CN. To generate the shared secret key, the common secret is required here to facilitate the key generation. For instance, all of nodes have to perform the key generation over the common randomness. However, the problem is that the channel measurements in

the star topology are the pairwise channels between the CN and any EN. This means each pairwire channel measurement are unique and couldn't serve as the common randomness in this group.

Chain Topology

In a network with the chain topology, nodes locates far off. In this case, not all the wireless devices in the group are within the communication range of each other. We can image the nodes to form a chain with nodes connected end to end.

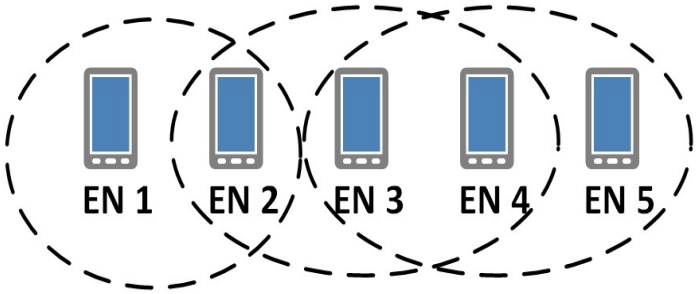


Figure 2.2: Chain Topology

In Fig.2.2, a node chain with 5 nodes are illustrated. In this topology, the head node and tail node can be labeled with different collor. This type of networks is common to see in the satellite ground station networks. Due to the fact the nodes locates far off geographically, it is challenging to extract the shared common randomness in this case. For instance, the channel observations extracted from the network with a chain topology are the end to end channels connecting two nodes. Apparently, such channels are not identical and thus cannot serve as the common randomness for the physical layer key generation directly.

2.3 Channel Probing

Link Establishment

According to our design, there is a fast link establishment process between CN and EN for the purpose of angle of arrival (AoA) and angle of departure (AoD) estimation. Here, we only consider the None-line-of-sight (NLOS) paths.

Due to the power constraint at EN, according to [2], we consider the analog precoding scheme which could provide the sufficient antenna gain. Analog combiners utilize the phase shifter at ENs for the purpose of beamforming and has a predefined codebook $\mathcal{W}$. Supposing that EN u equips with the codebook $\mathcal{W}^{EN}$ and tries to establish a link with CN c. EN u and CN c need to search over the codebook $\mathcal{W}$ and find the combining vectors $\mathbf{w}_u \in \mathcal{W}^{EN}$ and $\mathbf{w}_c \in \mathcal{W}^{CN}$ [1, 2, 11]. The entries in $\mathcal{W}^{EN}$ and W^{CN} are normalized to satisfy $|\mathbf{W}_{i,j}^{EN}|^2 = N_{EN}^{-1}$ and $|\mathbf{W}_{i,j}^{CN}|^2 = N_{CN}^{-1}$ with a finite set of possible values, i.e., $\mathbf{W}_{i,j}^{CN} = \frac{1}{\sqrt{N_{CN}}} e^{j\psi_{i,j}}$.

Similar to [2,12], we assume the number of ENs meets the condition that $1 \leq N_r \leq N_{RF}$. For every EN associated with CN c, the CN c serves every EN using a single RF chain. In Fig. 2.3, the beam sweeping has been illustrated. In this process, the beamformers $\mathbf{w}_u$ and $\mathbf{w}_c$ try to maximize the received signal by solving the following problem:

$$\begin{aligned} \max_{\mathbf{w}_u, \mathbf{w}_c} \quad & |\mathbf{w}_u^H \mathbf{H}_{uc} \mathbf{w}_c|^2, \\ \text{subject to} \quad & \mathbf{w}_u \in \mathcal{W}^{EN}, \\ & \mathbf{w}_c \in \mathcal{W}^{CN}, \end{aligned} \tag{2.1}$$

Here combining vectors $\mathbf{w}_u$ and $\mathbf{w}_c$ provide the high antenna gain, which involves the antenna patterns at EN u and CN c. For mathematical tractability and similar to [13], the

antenna pattern is approximated as a sectored antenna model:

$$G_b(\theta) = \begin{cases} M_s & \text{if } |\theta| \leq \theta_b \\ m_s & \text{otherwise,} \end{cases} \tag{2.2}$$

where θ_b is the beam width of the main lobe, M_s and m_s are array gains of the main lobe and side lobe, respectively.

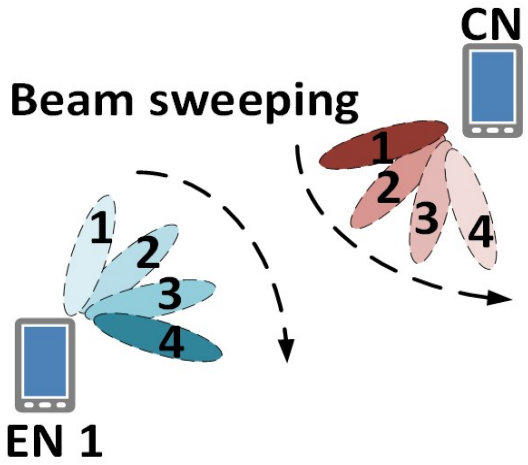


Figure 2.3: Beam sweeping in the Link Initialization

Uplink Channel Estimation

After the link initialization stage, the appropriate beamformers have been selected. In the next stage, the uplink channel probing from every EN u to CN c is conducted. Every EN

$u \in \mathcal{M} \setminus c$ sends channel probing signals sequentially to CN, which can be expressed as:

$$y_{cu}^{1} = \mathbf{w}_c^H \mathbf{H}_{cu} \mathbf{w}_u s_u + \mathbf{w}_c^H \mathbf{n}_{cu}, \tag{2.3}$$

where $\mathbf{n}_{cu} \in \mathcal{C}^{N_c \times 1}$ is the noise, which satisfies the circular-symmetry complex Gaussian distribution. $\mathbf{H}_{cu}$ is the narrow-band mmWave channel matrix. The definition of beamformers $\mathbf{w}_c$ and $\mathbf{w}_u$ will be given later.

After obtaining the uplink channel probing y_{cu}^{1}, CN c would like to estimate the effective channel $\mathbf{w}_c^H \mathbf{H}_{cu} \mathbf{w}_u$, which can be performed by the estimators like least squares (LS) or MLE.

Downlink Channel Probing

In the downlink channel probing, for every EN u, beamformer $\mathbf{w}_u$ developed in the link establishment stage is applied to receive the signal. Due to the large path loss and high directionality of mmWave signal, it is possible to increase the probing efficiency by sending the downlink channel probing signals concurrently. That is, for every single round of channel probings, CN only needs to perform the channel probing once. For instance, for the CN c, the downlink probing signals are concurrently sent using a beamformer $\mathbf{f}_{cu}$ to $M-1$ ENs, which means the downlink channel probing is performed in a multiplexing manner. Here, $\mathbf{f}_{cu}$ is the hybrid beamformer and it incorporates the analog beamformer and a baseband precoder. The design of the hybrid precoder will be given in section 4.1.

For every EN u, if the interference from other ENs is denoted as $\mathcal{I}_1$, the corrupted downlink channel probing signals, received at EN u, can be represented as:

$$y_{cu}^{2} = \mathbf{w}_u^H \mathbf{H}_{cu} \mathbf{f}_{cu} s_u + \underbrace{\sum_{j \in \mathcal{M} \setminus \{u,c\}} \mathbf{w}_u^H \mathbf{H}_{cu} \mathbf{f}_{cj} s_j}_{\mathcal{I}_1} + \mathbf{w}_u^H \mathbf{n}_{cu}, \tag{2.4}$$

In the next section, we will give more details about the design of multiplexing beamformer, which can mitigate the interference $\mathcal{I}_1$. The design of every beamformer $\mathbf{f}_{cu}$ will be given in the next section.

Chapter 3: Existing Schemes for Physical Group Key Generation

Existing group key generation methods can be broadly classified into two mechanisms. In the first mechanism, every node tries to generate pairwise keys among users using physical layer key generation first, and then generate a group key based on the pairwise keys (e.g., broadcast one of the keys (shortest one) xor'ed with the key associated with each user). In this way, each user can reconstruct the shortest key) [5–7]. In the second mechanism, every node tries to conduct channel probing for each pair of users first. In the next step, a user's reference channel information is selected and shared with other users by sending the channel state difference to other users or broadcast linear combinations of the collected channel information at each node. Finally, every node generates a group key based on a reference channel or all the channel information [14, 15].

For the first category, a classical strategy for group key generation using the pairwise keys is to utilize tree-based algorithms related to graphs [6, 7]. The basic idea is to treat the group key generation model as a multigraph, in which each pairwise key rate can be viewed as the weight of the edge associated with the corresponding two nodes. Then, a spanning tree can be found in this multigraph, and the group key information can be propagated over this spanning tree by dividing each pairwise key into multiple one-bit segments and transmitting one-time pads of these segments. Simple multi-segment algorithms are further developed to achieve or approach the group key rate upper bound in [5]. The time allocation problem in the channel estimation steps to maximize the group key rates is proposed.

For the second category, in [4], a secret group key generation scheme was proposed for star topology using the received signal strength (RSS). Specifically, the channel between an edge node (EN) and a central node (CN) is selected as the reference channel and estimated

first. Then, for each other EN, the CN forwards the difference of two RSSs of the reference channel and the channel linked to that EN. As that EN has the estimation of channel linked to the CN, it can also estimate the reference channel using the received RSS difference. Finally, all nodes can have the reference channel information, and use it to generate the group key.

Chapter 4: Efficient Group Key Generation for the Star Networks

In this chapter, we discuss the design of spatial-multiplexing beamformer at first, where the hybrid precoding is adopted. Based on the developed multiplexing beamformer, the group key generation protocols are proposed in section 4.2. In section 4.2.1, we will give the analytical expression for the group key rates. To further improve the group key rates at the downlink channel probing stage, the power allocation is reformulated into a multi-objective optimization problem in Eq. 4.20. Finally, in section 4.2.2, we propose an MLE-based group key rates estimator, which can efficiently estimate the group key rates based on the probing samples.

4.1 Probing Efficiency Improvement with Hybrid Precoding

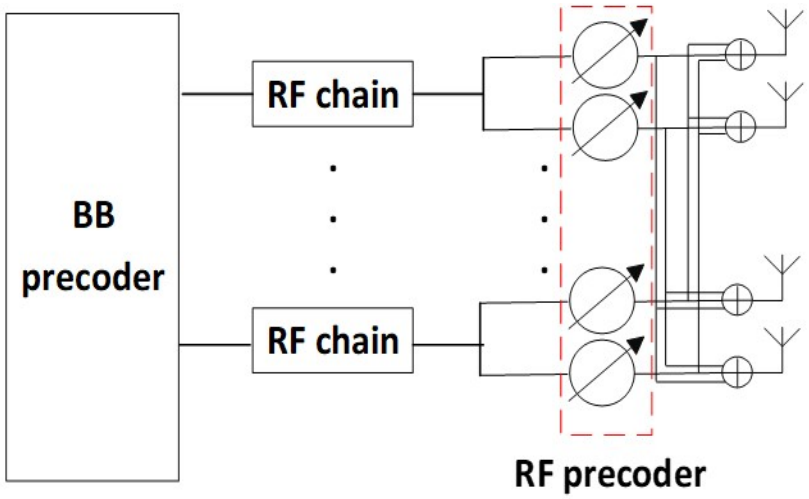


Figure 4.1: Hybrid Precoder

As specified in the previous section, CN c has N_{RF} RF chains. Due to the hardware limitations of Massive MIMO, the analog beamformer combined with the baseband beamformer is usually adopted at mmWave band, which is illustrated in Fig. 4.1. The analog beamformer can be regrouped into a single RF precoder $\mathbf{F}_{RF} = [\mathbf{f}_{c1}, ..., \mathbf{f}_{cM}]$. If we add an extra baseband precoder $\mathbf{F}_{BB}$ at the front end of CN c [1, 2], the combined beamformer and training sequences can be expressed as:

$$\mathbf{x} = \mathbf{F}_{RF}\mathbf{F}_{BB}\mathbf{s} \tag{4.1}$$

where vector $\mathbf{s} = [s_1, s_2, ..., s_M]^T$ is the training sequence for channel probing and needs to meet $\mathbf{E}[\mathbf{s}^H\mathbf{s}] \leq P$. In this way, the received signal at each EN u can be expressed as:

$$y_{cu}^2 = \sum_u \mathbf{w}_u^H \mathbf{H}_{bu}\mathbf{x} + \mathbf{w}_u^H \mathbf{n}_{cu}, \tag{4.2}$$

Due to the sparsity of channel $\mathbf{H}$, the solution in Eq. 2.1 can be satisfied with the matched beamformer [2]. Consequently, the EN u sets $w_u = \mathbf{a}_{EN}(\theta_u)$ and CN c takes $\mathbf{v}_{cu} = \mathbf{a}_{CN}(\phi_{cu})$. Here (θ_u) and (ϕ_c) are quantized in the angular space and meet the specifications of the analog beamformers. After gathering the beamforming vectors for the $M-1$ ENs, the RF beamformer of CN c can be represented as $\mathbf{F}_{RF} = [\mathbf{v}_{c1}, ..., \mathbf{v}_{cM}]$.

Due to the design freedom provided by baseband precoder $\mathbf{f}_{BB}$ and high directionality of mmWave communication, the effective channel of any EN $u \in \mathcal{M} \setminus \{c\}$ can be viewed as the combination of antenna gains. Based on the uplink channel estimation, the effective antenna gain vector can accordingly be collected and expressed as $\hat{\mathbf{H}}_a = [\hat{\mathbf{h}}_1/g_{c,1}; ...; \hat{\mathbf{h}}_M/g_{c,M}]^T$, where $\hat{\mathbf{h}}_M \in \mathcal{C}^{1\times M}$ can be expressed as $\hat{\mathbf{h}}_u = \mathbf{w}_u^H \mathbf{H}_{cu}\mathbf{F}_{RF}$. Derived from the zero-forcing techniques, the baseband precoder can be adopted here to achieve downlink channel probings concurrently instead of sequentially. We give the definition of the baseband precoder as below:

$$\mathbf{F}_{BB} = \hat{\mathbf{H}}_a^H(\hat{\mathbf{H}}_a\hat{\mathbf{H}}_a^H)^{-1}, \tag{4.3}$$

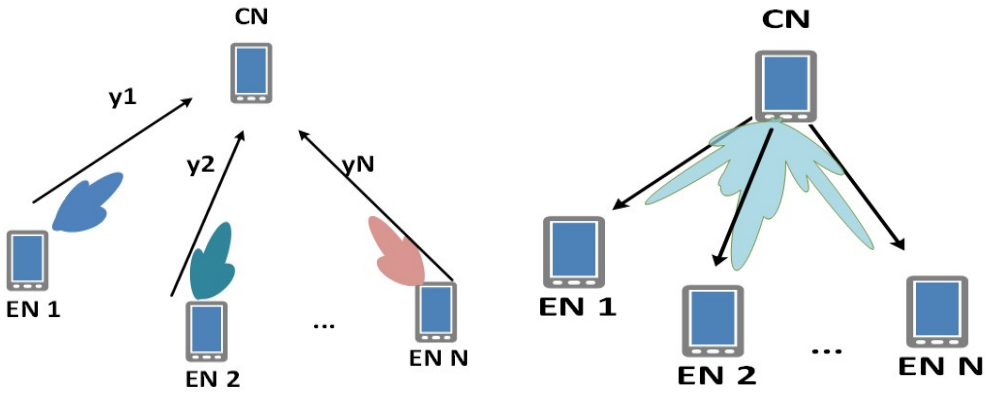
We defined the downlink probing symbols as $\mathbf{s} = [\sqrt{\rho}_1, ..., \sqrt{\rho}_M]$, where $\sqrt{\rho}_u$ is the power loaded on the baseband beamformer of EN u. If the effect of the channel estimation is considered, the designed baseband precoder $\mathbf{f}_{BB}^j$ of EN j is orthogonal to the other effective channels $\overline{\mathbf{h}}_u,\ u \neq j$ and such an effect can be represented as:

$$\mathbf{w}_u^H \mathbf{H}_{cu}\mathbf{F}_{RF}\mathbf{f}_{BB}^j \approx 0,\ j \neq u,\quad j, u \in \mathcal{M} \setminus \{c\} \tag{4.4}$$

If we adopt the sparse multi-path mmWave channel model [1, 2, 11], for EN u, the uplink and downlink signal can be further simplified into:

$$y_{cu}^1 \approx \sqrt{\rho_{uc}} g_{cu} + \mathbf{f}_{cu}^H \mathbf{n}_{cu}, \tag{4.5}$$

$$y_{cu}^2 \approx \sqrt{\rho_{cu}} g_{cu} + \mathbf{w}_{cu}^H \mathbf{n}_{cu}, \tag{4.6}$$



(a) (b)

Figure 4.2: Improving Channel Probing Efficiency

ρ_{cu} is the allocated power at the RF chain and ρ_{uc} is the power for uplink probing signals. g_{cu} is the equivalent channel gain. Eq. 4.6 indicates that the strongest multipath has been selected in the link initialization stage and the effect of other multipath is filtered by the beamformer. The total power constraint is $\sum_{u=1}^{M} \rho_{cu} \leqslant P$ and P is the total power budget. g_{cu} is the fading coefficient. If the MLE is applied at both sides, accordingly, the measured channel gain of uplink and downlink can be represented as h_{cu}^1 and h_{cu}^2, respectively, as

below:

$$\begin{aligned}
\overline{h}_{c,u} &= \frac{1}{\sqrt{\rho_{uc}}} y_{cu}^{1}, \\
&= g_{cu} + G_{uc}\mathbf{f}_{cu}^{H}\mathbf{n}_{cu}, \qquad (4.7) \\
\overline{h}_{u,c} &= \frac{1}{\sqrt{\rho_{cu}}} y_{cu}^{2}, \\
&= g_{cu} + G_{cu}\mathbf{w}_{u}^{H}\mathbf{n}_{cu}, \qquad (4.8)
\end{aligned}$$

Based on Eq. 4.8, the equivalent channel gain g_{cu} can be estimated.

4.2 Group Key Generation Protocols for Star-topolog Networks

In section 4.1, the multiplexing of downlink probing signals has been given. The group key generation protocol for mmWave star networks, which consists of 5 steps, will be specified in Fig. 4.3.

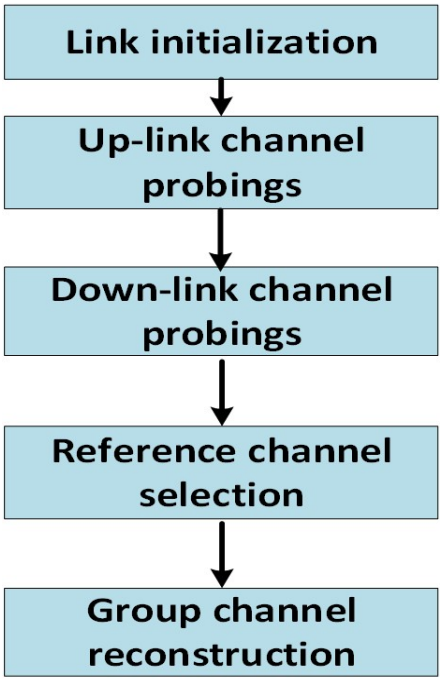


Figure 4.3: The mmWave Group Key Generation Protocol

Step 1. RF Precoder Design Right before the uplink channel probing, CN and every EN need to find the RF precoder that can provide the largest effective gain according to [2]. This problem can be viewed in Eq. 2.1. This procedure is usually named as beam sweepings.

Step 2. Uplink Channel Probing and Effective Channel Estimation Based on the designed RF beamformer $\mathbf{F}_{RF}$, every EN u sends channel probings sequentially. In the uplink, CN c estimates the effective channels of every ENs in set $\mathcal{M}/\{c\}$. The collection of effective antenna gain at CN c can be represented as $\hat{\mathbf{H}}_a$. Based on the effective antenna gain matrix $\hat{\mathbf{H}}_a$, the baseband precoder $\mathbf{F}_{BB}$ is specified.

Step 3. Downlink Channel Probing and Basedband Precoder Design After the precoder design in the last step, at the CN c, analog precoder $\mathbf{F}_{RF} = [\mathbf{v}_1, ..., \mathbf{v}_M]$ and baseband precoder $\mathbf{F}_{BB}$ have been constructed. In this step, CN c needs to perform the downlink channel probing, which results in the received signal at every EN u as Eq. 4.6.

Step 4. Reference Channel Selection and Broadcasting In this step, CN c randomly picks up EN j from $\mathcal{M} \setminus \{c\}$ and the effective channel $\overline{\mathbf{h}}_j$ is selected as the reference channel. CN c gets the difference between the reference channel $\overline{\mathbf{h}}_j$ and effective channel matrix as $\mathbf{\Delta} = \{\overline{h}_{c,j} - \overline{h}_{c,1}, ..., \overline{h}_{c,j} - \overline{h}_{c,N_r}\}$.

Step 5. Group Channel Reconstruction As claimed in [**?**], in the process of group key generation, current works usually assume there is a noiseless public channel with infinite capacity to exchange messages among group members. Apparently, such a public channel can be completely accessed by the eavesdropper. Based on the channel difference $\mathbf{\Delta}$ broadcasted to every EN u over the public channel, each EN u can retrieve the reference channel $\overline{h}_{c,j}$ based on the estimation of downlink effective channel $\overline{h}_{u,c}$ by solving $\overline{h}_{c,u} - \overline{h}_{c,j}$, where we assume the reciprocity holds and $\overline{h}_{c,u} \approx \overline{h}_{u,c}$.

4.2.1 Group Key Rates and Power Allocation

The efficiency of group key generation can be further improved by appropriate power allocation on the baseband beamformer. That is, we are trying to tune the power of baseband beamformer at CN to increase the group key rates.

Utilizing the slepian-wolf coding as specified in [4], let R^u_{sec} represent the secure key rates at the EN u. It can be represented as:

$$R_{star} \triangleq \min_{i \in \mathcal{A} \setminus j} \lim_{T \to \infty} I([\overline{\mathbf{h}}_{c,1}, ..., \overline{\mathbf{h}}_{c,M}]; [\mathbf{\Delta}, \overline{\mathbf{h}}_{c,j}]) \tag{4.9}$$

$$R_e \triangleq \lim_{T \to \infty} I([\overline{\mathbf{h}}_{c,1}, ..., \overline{\mathbf{h}}_{c,M}]; [\mathbf{\Delta}, \mathcal{Y}^e]) \tag{4.10}$$

$$R^u_{sec} = R_{star} - R_e \tag{4.11}$$

where $\overline{\mathbf{h}}_{c,j}$ is the uplink reference channel between the CN c and the EN j. Considering the channel difference $\mathbf{\Delta}$, the secure key rates R^u_{sec} can be expressed as:

$$\begin{aligned}
R^u_{sec} &= R_{star} - R_e \\
&= I(\overline{h}_{c,j}; \overline{h}_{u,c} | \mathbf{\Delta}) \\
&= H(\overline{h}_{c,j} | \mathbf{\Delta}) - H(\overline{h}_{c,j} | \overline{h}_{u,c}, \mathbf{\Delta}) \\
&= H(\mathbf{\Delta} | \overline{h}_{c,j}) + H(\overline{h}_{c,j}) - H(\mathbf{\Delta}) - \big(H(\overline{h}_{u,c}, \mathbf{\Delta} | \overline{h}_{c,j}) + H(\overline{h}_{c,j}) - H(\overline{h}_{u,c}, \mathbf{\Delta})\big) \\
&= H(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{-\overline{h}_{c,j}\}) - H(-\overline{h}_{c,u}, \overline{h}_{u,c}) \\
&\quad -H(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{\overline{h}_{c,u}, \overline{h}_{c,j}\}) - H(\mathbf{\Delta}) \\
&\quad +H(\mathbf{\Delta}, \overline{h}_{u,c})
\end{aligned} \tag{4.12}$$

which is the modified group key rates based on [14]. From Eq. 4.12, we can observe that secure group key rates R^u_{sec} for EN u can be decoupled into the combination of joint entropy $H(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{-\overline{h}_{c,j}\})$, $H(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{\overline{h}_{c,u}, \overline{h}_{c,j}\})$, $H(-\overline{h}_{c,u}, \overline{h}_{u,c})$ and $H(\mathbf{\Delta}, \overline{h}_{u,c})$. If we take a term $H(-\overline{h}_{c,u}, \overline{h}_{u,c})$, the joint entropy is defined by the joint distribution of the vector $\{-\overline{h}_{c,u}, \overline{h}_{u,c}\}$. Such a vector is the linear combination of estimated effective channel gains and its distribution needs to be derived. The joint distribution of terms in Eq. 4.12 will be given as follows.

At first, according to [1], we assume the fading coefficient $g_{cu} \in \mathcal{C}$ follows a circular-symmetric complex gaussian $g_{cu} \sim \mathcal{CN}(0, \sigma^2_{gu})$. Noise $\mathbf{n} \in \mathcal{C}^{N_{EN} \times 1}$ for every EN has a circular-symmetric complex gaussian distribution $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_n \mathbf{I_N})$. We list the distribution

of terms in Eq. 4.12 in the next few paragraphs. The derivation in detail is omitted due to the page limit.

For every single downlink effective channel gain $\overline{h}_{c,u}$ and uplink effective channel gain $\overline{h}_{u,c}$, based on the distribution of g_{cu} and $\mathbf{n}$, we can easily find the derived distributions as:

$$\begin{aligned} \overline{h}_{c,u} &\sim \mathcal{CN}(0, (\sigma_{g,u}^2 + |G_{u,c}|^2 ||\mathbf{f}_{cu}||^2 \sigma_n^2)) \\ \overline{h}_{u,c} &\sim \mathcal{CN}(0, (\sigma_{g,u}^2 + |G_{c,u}|^2 ||\mathbf{w}_u||^2 \sigma_n^2)) \end{aligned} \tag{4.13}$$

The vector $\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{-\overline{h}_{c,j}\}$ contains the negative of uplink channel gains, except for the reference channel gain. The corresponding distribution can be expressed as:

$$\begin{aligned} &\{-h_{c,1}, ..., -h_{c,M}\} \setminus \{-\overline{h}_{c,j}\} \\ &\sim \mathcal{CN}(\mathbf{0}, \text{diag}(\sigma_{g,1}^2 + |G_{1,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2, \sigma_{g,2}^2 \\ &+ |G_{2,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2, ..., \sigma_{g,M}^2 + |G_{M,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2)) \end{aligned} \tag{4.14}$$

Vector $\mathbf{\Delta} = \{..., \overline{h}_{c,i} - \overline{h}_{c,j}, ...\},\ u \neq j$ has the effective channel difference between the effective channel gain of any EN u and the reference effective channel gain $\overline{h}_{c,j}$. The distribution of vector $\mathbf{\Delta}$ can be represented as:

$$\begin{aligned} \mathbf{\Delta} &\sim \mathcal{CN}(\mathbf{0}, \text{diag}(..., \sigma_{g,u}^2 + |G_{u,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2, ...) \\ &+ (\mathbf{1}_{(M-1)\times(M-1)})(\sigma_{g,i}^2 + |G_{i,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2)), u \neq j \end{aligned} \tag{4.15}$$

The distribution of $\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{-\overline{h}_{c,u}, -\overline{h}_{c,j}\}$ can be derived as:

$$\begin{aligned} \{-h_{c,1}, ..., -h_{c,M}\} \setminus \{-\overline{h}_{c,u}, -\overline{h}_{c,j}\} &\sim \mathcal{CN}(\mathbf{0}, \\ &\text{diag}(\sigma_{g,1}^2 + |G_{1,c}|^2 ||\mathbf{f}_{(\cdot)}||^2 \sigma_n^2, ...)) \end{aligned} \tag{4.16}$$

Finally, the distribution of $\{-\overline{h}_{c,u}, \overline{h}_{u,c}\}$ and $\{\mathbf{\Delta}, \overline{h}_{u,c}\}$ can be expressed in Eq. A.1 and Eq. A.2, in which $\mathbf{c} \in \mathcal{C}^{M-1\times 1}$, whose elements are zeros except for the u_{th} element.

Based on the derivations above, the secure key rates can be expressed as:

$$\begin{aligned}
&R^u_{sec} = R_{star} - R_e \\
&= \log((\pi e)^{M-1}\big|Cov(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{-\overline{h}_{c,j}\})\big|) \\
&- \log((\pi e)^{M-2}\big|Cov(\{-\overline{h}_{c,1}, ..., -\overline{h}_{c,M}\} \setminus \{\overline{h}_{c,u}, \overline{h}_{c,j}\})\big|) \\
&- \log((\pi e)^{M-1}\big|Cov(\mathbf{\Delta})\big|) + \log((\pi e)^{M}\big|Cov(\{\mathbf{\Delta}, \overline{h}_{u,c}\})\big|) \\
&- \log((\pi e)^{2}\big|Cov(\{-\overline{h}_{c,u}, \overline{h}_{u,c}\})\big|)
\end{aligned} \tag{4.17}$$

In order to compute $\big|Cov(\{\mathbf{\Delta}, \overline{\mathbf{h}}_{u,c}\})\big|$, the Sylvester's determinant theorem is adopted, which represents the determinant of covariance matrix in a block-wise form as specified below in Eq. 4.18. When D is invertible, let $B = \mathbf{c}$, $C = \mathbf{c}^T$, and $D = \sigma^2_{g,u} + |G_{c,u}|^2||\mathbf{w}(\cdot)||^2\sigma^2_n$.

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} \;=\; \det(\mathbf{A})\det\left(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}\right) \tag{4.18}$$

To further simplify and get the analytical expression of Eq. 4.18, the matrix can be reformulated as:

$$\begin{aligned}
&\det\left(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}\right) \\
&= \log(\sigma^2_{g,u} + |G_{c,u}|^2||\mathbf{w}_{(\cdot)}||^2\sigma^2_n \\
&- \frac{1}{\sigma^2_{g,u} + \sigma^2_{g,j} + 2|G_{u,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma^2_n})
\end{aligned}$$

Finally, gathering all of derived expressions above, the simplified secure group key rates

can be expressed as:

$$R^u_{sec} = \log(\sigma^2_{g,u} + |G_{u,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma^2_n) - x_u - \log(|G_{u,c}|^2\sigma^2_n) + \log(\sigma^2_{g,u} + |G_{c,u}|^2||\mathbf{w}_{(\cdot)}||^2\sigma^2_n$$
$$- \frac{1}{\sigma^2_{g,u} + \sigma^2_{g,j} + 2|G_{u,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma^2_n}) \tag{4.19}$$

where $x_u = \log(|G_{u,c}|^2||\mathbf{f}_{(\cdot)}||^2||\mathbf{w}||^2\sigma^2_n)$. The assignment of transmission power $\rho = \{\rho_{c,1}, ..., \rho_{c,M}\}$, for the downlink channel probing, can be performed by adjusting the power on M RF chains under the total power budget constraint at CN c, where vector ρ needs to meet the constraint $\sum_{u=1}^{M} \rho_{cu} \leqslant P$. Due to the fact that, for every EN u, the distribution of each equivalent channel gain g_{cu} is affected by the antenna pattern and the number of multipath, the coefficients of group key rates R^u_{sec} are not the same between different nodes. According to the definition in Eq. 4.11, the objective function of group key rates can be reformulated into a multi-objective function with the constraints on the power allocation, whose maximum can be obtained by properly tuning the ρ. The objective function is represented as: $\min\{\max[R^1_{sec}(\rho), ..., R^M_{sec}((\rho))]\}$. While maximizing the group key rates, the CN c can solve the following problem:

$$\begin{aligned} &\max_{\rho} && [R^1_{sec}(\rho), R^2_{sec}(\rho), ..., R^M_{sec}(\rho)] \\ &\text{subject to} && \sum_{u=1}^{M} \rho_{cu} \leqslant P \end{aligned} \tag{4.20}$$

We can observe that the objective function in Eq. 4.20 is a multi-objective function, which usually has a set of solutions and we need to achieve a tradeoff among objectives and constraints. In section 5.1, a GA-based algorithm will be developed for problem 4.20.

4.2.2 MLE-based Entropy Estimation

In this section, we propose a lightweight entropy estimation scheme based on Maximum Likelihood Estimation (MLE), in which the joint entropy in Eq. 4.19 is derived based on the parameter of joint gaussian distribution, estimated from MLE.

From the distribution derived in Eq. 4.8, we can observe that if we collect the measurements of effective channels for the EN u in a single vector $\overline{\mathbf{h}}_{c,u}$, the real/image part for $\overline{\mathbf{h}}_{c,u}$ which has a circular-symmetric gaussian distribution, is a normal distribution $\mathcal{N}(\mathrm{Re}(\overline{\mathbf{h}}_{c,u}), \mathrm{Re}(\mu), \mathrm{Re}(\mathbf{\Sigma}))$ or $\mathcal{N}(\mathrm{Im}(\overline{\mathbf{h}}_{c,u}), \mathrm{Im}(\mu), \mathrm{Im}(\mathbf{\Sigma}))$. For instance, for the ease of presentation, we omitted the constant terms in the likelihood $\log\mathcal{N}(\mathrm{Re}(\overline{\mathbf{h}}_{c,u}), \mathrm{Re}(\mu), \mathrm{Re}(\mathbf{\Sigma}))$ and terms involving unknowns can be represented as:

$$\log(\cdot) \triangleq \frac{-1}{2}\log|\mathbf{\Sigma}| + \frac{-1}{2}(\overline{\mathbf{h}}_{c,u} - \mathrm{Re}(\mu))^T \mathbf{\Sigma}(\overline{\mathbf{h}}_{c,u} - \mathrm{Re}(\mu)), \tag{4.21}$$

Here we take the MLE for real part as an example. By setting derivative w.r.t. $\mathrm{Re}(\mu)$ to zero, we can derive the estimated real part of mean μ as:

$$\mathrm{Re}(\hat{\mu})_{ML} = \frac{1}{|\overline{\mathbf{h}}_{c,u}|}\sum \mathrm{Re}(\overline{\mathbf{h}}_{c,u})^i \tag{4.22}$$

$$\mathrm{Re}(\hat{\mathbf{\Sigma}})_{ML} = \frac{1}{|\overline{\mathbf{h}}_{c,u}|}\sum (\overline{\mathbf{h}}_{c,u} - \mathrm{Re}(\hat{\mu})_{ML})^i \tag{4.23}$$

where $|\overline{\mathbf{h}}_{c,u}|$ indicates the number of elements in vector $\overline{\mathbf{h}}_{c,u}$. Based on the two estimators above, the joint gaussain distribution of the joint entropy terms listed in Eq. 4.19 can be estimated accordingly. The numerical results in section **??** show that the theoretical group key rates are closely in agreement with the estimation of group key rates.

Chapter 5: Power Allocation in the Group Key Generation

5.1 Group Key Rates Optimization Using Genetic Algorithm

A genetic algorithm is a search heuristic that is inspired by Charles Darwin's theory of natural evolution. This algorithm reflects the process of natural selection where the fittest individuals are selected for reproduction in order to produce offspring of the next generation.

A typical genetic algorithm requires: (a) a genetic representation of the solution domain; (b) a fitness function to evaluate the solution domain. That means to apply the GA we have to define the genetic representation and the fitness function, respectively.

Here genetic representation is required to represent the solutions/individuals of the GA. For instance, various attributes can be collected to represent the individuals uniquely. A fitness function is the objective function which is used to quantify the evolutionary directions. It can be viewd as as a single figure of merit and it represents how close a given design solution is to achieve the target.

A GA proceeds to initialize a population of solutions and then to improve it through repetitive application of the mutation, crossover, inversion and selection operators. The detailed explanation for these process can be found below.

Initialization

Population Initialization is the first step in the Genetic Algorithm Process, where population is a subset of solutions in the current generation. Population P can also be defined as a set of chromosomes. The initial population $P(0)$, which is the first generation is usually created randomly. In an iterative process, populations $P(t)$ at generation $t,\ t = 1, 2, \ldots$ are constituted. Initialization is critical in the GA because it determines the diversity of

the population at the beginning stage of GA. Starting from a population with low diversity might lead to a condition known as premature convergence.

5.1.1 Selection

During each successive generation, a portion of the existing population is selected to breed a new generation. Selection usually includes: (a) selection from the current generation to take part in reproducing(Parent Selection); (b) selection from parents + offspring to go into the next generation (Survivor Selection). For parent slection, an individual is to be chosen as a parent for the next generation of the population, based on its fitness. The Survivor Selection determines which individuals are to be kicked out and which are to be kept in the next generation, which is also known as replacement.

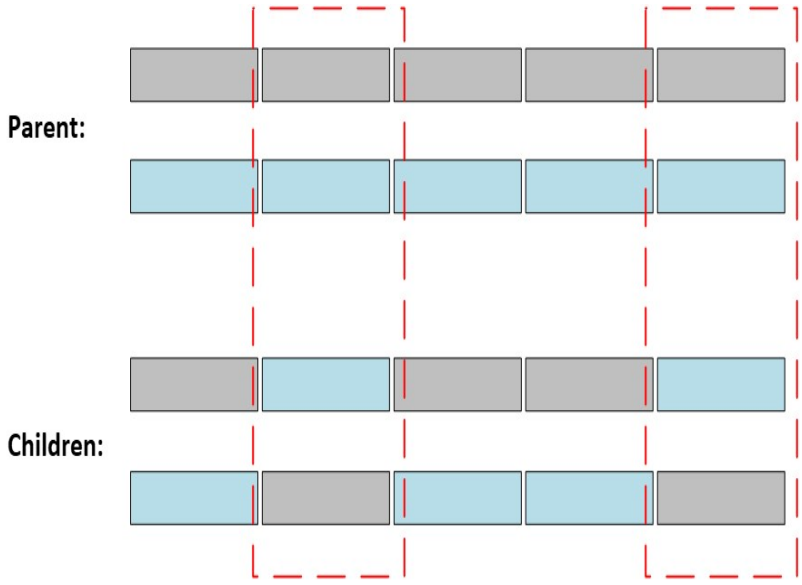


Figure 5.1: Crossover

5.1.2 Genetic operator

The next step is to generate a second generation population of solutions from those selected, through a combination of genetic operators: crossover, and mutation.

Crossover is the process of taking more than one parent solutions to produce a child solution from them. For instance, recombining portions of good solutions is usually considered in the genetic algorithm and this operation is named as crossover. It is more likely to create a better solution. The mutation operator encourages genetic diversity amongst solutions in order to prevent the genetic algorithm converging to a local minimum by having the solutions becoming too close to one another. For instance, mutating the current pool of solutions reproduces a given solution, which may change entirely from the previous solution. A genetic algorithm can reach an improved solution solely through the mutation operator.

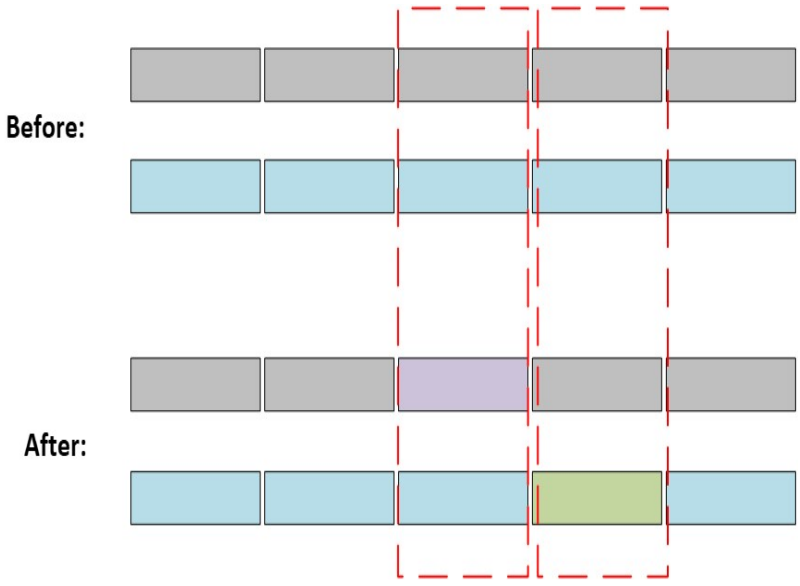


Figure 5.2: Mutation

5.1.3 Termination

The aforementioned generational process is repeated until a termination condition has been reached. Therefore, termination is the sign of the algorithm converges. Common terminating conditions that are considered in the existing works are: (a) a solution is found that satisfies minimum criteria; (b) the fixed number of generations is reached; (c) allocated budget (computation time/money) for the evolutionary computation is reached and so on.

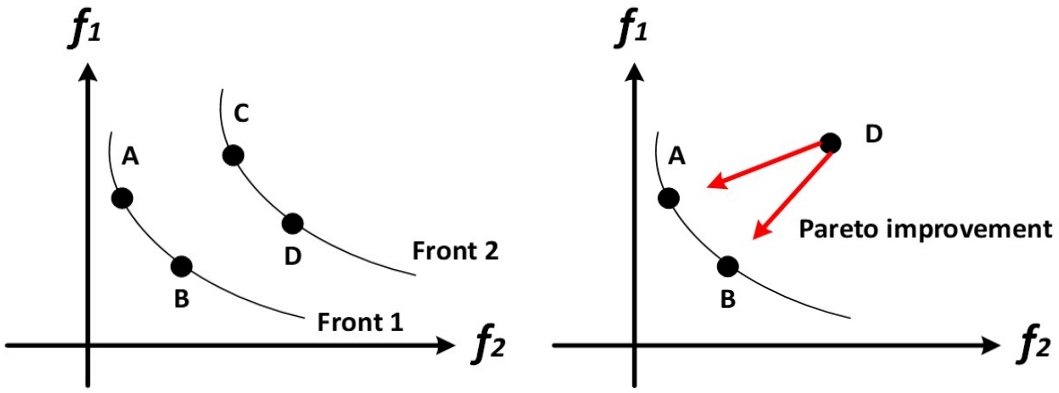
5.1.4 Multi-objective Optimization

In Eq. 4.20, the power allocation problem for downlink probing is a multi-objective optimization problem, which involves more than one objective function to be optimized. As we all know, the answer for such a problem is a set of solutions, where the goodness of a solution for the multi-objective problem is determined by the *dominance*. Let's define the notion of *dominance* as below: For two feasible solutions $\mathbf{x}_1$ and $\mathbf{x}_2$, $\mathbf{x}_1$ dominates $\mathbf{x}_2$ iff, solution $\mathbf{x}_1$ is no worse than $\mathbf{x}_2$ in all objectives, and solution $\mathbf{x}_1$ is strictly better than $\mathbf{x}_2$ in at least one objective.

One way to find good solutions to multi-objective problems is according to *Pareto optimality*, named after economist Vilfredo Pareto.

Pareto Front

For the multi-objective problem, maxmizing or minimizing a single objective function may be harmful to other objective functions. We are interested in finding solutions that upgrade some objective functions without downgrading anyone else. The movement (upgrading) from the previous solutions to a set of better solutions is called "Pareto improvements". If the current solutions are restricted to a solution set and cannot make Pareto improvements in the next solution updates, the *Pareto optimality* is achieved. Many existing multi-objective optimization algorithms involve the concept of *Pareto optimality* [10]. Any point belonging to this set is said to be on a front called *Pareto front*, which can be illustrated in Fig. 5.3(a).



(a) (b)

Figure 5.3: Pareto Front and Pareto Improvement

Existing algorithms

For multi-objective optimization, classical optimization methods tend to convert the multi-objective optimization problem to a single-objective optimization problem, i.e., averaged weighting, which can only emphasize one particular Pareto-optimal solution at a time. In this case, the genetic algorithm is very popular in solving the multi-objective optimization which aims to achieve the pareto optimality.

5.2 Non-dominant Sorting Genetic Algorithm for Constrained Optimization

In this paper, to solve the multi-objective defined in Eq. 4.20, we customize a Genetic Algorithm called Non-dominant Sorting Genetic Algorithm (NSGA II) and modify constraints handling process for NSGA II. In the next few paragraphs, we will give more details about the group key generation scheme based on NSGA II. Right before giving the scheme and the NSGA II in detail, we list several common notions in GA, non-dominant set sorting,

crowding distance assignment and reproduction.

Non-dominant Set Sorting

NSGA II is based on an operation by sorting the population into several *Non-dominated solution sets*. According to [10], the *Non-dominated solution set* can be defined as:

Given a set of solutions, the non-dominated solution set is a set of all the solutions that are not dominated by any member of the solution set.

The non-dominated set of the entire feasible decision space is called the Pareto-optimal set. The boundary defined by the set of all points mapped from the Pareto optimal set is called the Pareto optimal front. In order to approach to Pareto optimality front, the overall population, in each round of algorithm, is divided into several fronts $\mathcal{F} = \cup \mathcal{F}_i$.

To sort the non-dominated set, for every solution p in the population, two quantities are specified: 1) domination count n_p and 2) $\mathbf{S}_p$, a set containing the solutions dominated by p. In Fig. 5.4, non-dominated sorting can be viewed.

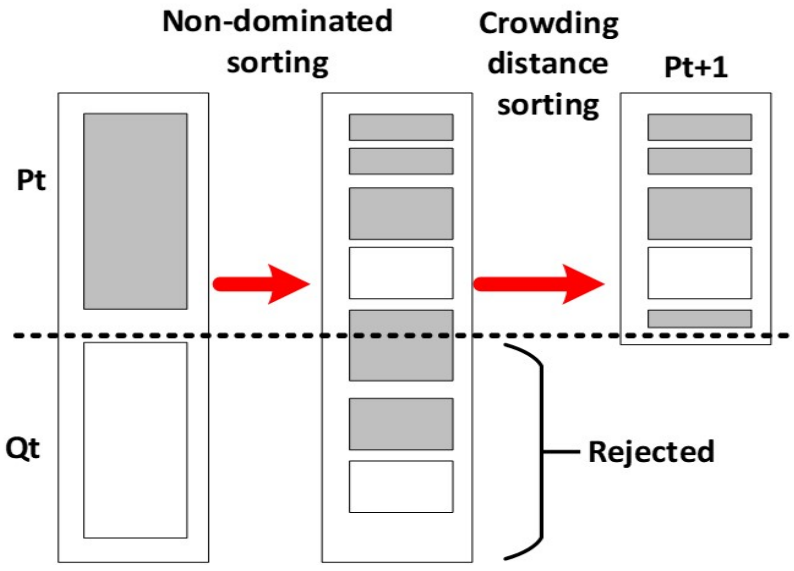


Figure 5.4: Non Dominated Sorting

Crowding Distance Assignment

As mentioned earlier, it is desired that the obtained solution sets spread widely in the feasible region, along with convergence to the Pareto-optimal set. In NSGA II, crowding distance for every element in the front indicates its distance to near neighbors and guides the selection process toward the uniformly sampled Pareto-optimal front.

- Density Estimation: To get an estimate of the density of solutions surrounding a particular solution in the population, crowding distance serves as an estimate of the perimeter of the cuboid formed by using the nearest neighbors as the vertices. To compute the crowding-distance, the population, at first, needs to be sorted in ascending order of magnitude according to the value of each objective function. Secondly, the boundary solutions for each objective function are assigned an infinite distance value. The rest intermediate solutions are assigned a distance value equal to the absolute normalized difference in the function values of two adjacent solutions.

- Crowded-Comparison Operation: With the crowding distance defined above, a spread-out solution set is selected at various stages of the algorithm by using the crowded-comparison operator ($\prec$), with which we hope the solution set can approach to a uniformly spread-out Pareto optimal front. After two steps above (non-dominated sorting and crowding-distance assignment), every entry in the population is assigned two attributes: nondomination rank (i_{rank}) and crowding distance ($i_{distance}$). The crowded-Comparison Operator is defined as:

$$\begin{aligned} i \prec_n j \quad \text{if} \quad & \big(i_{rank} < j_{rank} \\ & \text{or } (i_{rank} = j_{rank} \text{ and } i_{distance} > j_{distance})\big) \end{aligned} \tag{5.1}$$

  By observing operator in Eq. 5.1, we notice that between two solutions with differing nondomination ranks, the lower (better) rank solution is preferred. Otherwise, if two solutions locate on the same front, then we prefer the solution that is located in a less

crowded region.

Algorithm 1 GA-based Group key generation for multi-users mmWave Massive MIMO systems

Initialization: Establish links between the CN and EN. The distribution of CSI. Power budget P. SNR for each round. Max generation size N_G
Output: Power allocation result ρ

For $t \leq N_G$
  $\mathbf{R}_t = \mathbf{P}_t \cup \mathbf{Q}_t$
  $\mathcal{F} =$ non-dominated sorting$(\mathbf{R}_t)$
  $\mathbf{P}_{t+1} = \emptyset,$ and $i = 1$
  until$|\mathbf{P}_{t+1}| + |\mathcal{F}_i| \leq N$
    crowding-distance assignment$(\mathcal{F}_i)$
    $\mathbf{P}_{t+1} = \mathbf{P}_{t+1} \cup \mathcal{F}_i$
    $i = i + 1$
  Sort$(\mathcal{F}_i, \prec_n)$
  $\mathbf{P}_{t+1} = \mathbf{P}_{t+1} \cup \mathcal{F}_i[1 : (N - |\mathbf{P}_{t+1}|)]$
  $\mathbf{Q}_{t+1} =$ Reproduction$(\mathbf{P}_{t+1})$
  $t = t + 1$

Reproduction

The non-dominated sorting above divided the solutions into several fronts. The entries within the same front can utilize genetic operators like crossover, mutation and selection to produce a new generation (children).

Here we give a brief introduction for them, which have various roles as the genetic operators.

- Crossover: For every single solution p, after the non-dominated sorting, several pieces of solution p are exchanged with other solutions at the same solution representations. This means the crossover works in a well-searched subspace, and the converged states will remain.

- Mutation: The operation of Mutation usually changes parts of one solution randomly, which increases the diversity of the population and provides a mechanism for escaping

from a local optimum. That is, mutation usually leads to a solution outside the current solution subspace.

Constraints Handling

If the infeasible solutions violating constraints marginally are placed in the same nondominated level with another solution violating constraints to a large extent, this may cause an algorithm to wander in the infeasible search region for more generations before reaching the feasible region through constraint boundaries. In NSGA II, the feasible solutions with large crowding distance are preferred and the infeasible solutions violating constraints will be discarded.

5.2.1 GA-based Group Key Generation

We have introduced the key concepts of NSGA II above and gathered all the pieces. In this section, we give the GA-based Group Key Generation algorithm in Algorithm 1.

In the Algorithm 1, a single algorithm run is listed. $\mathbf{R}_t$ contains the parent population $\mathbf{P}_t$ and offspring population $\mathbf{Q}_t$. The elements in $\mathbf{R}_t$ are classified into several non-dominant set front after the non-dominant sorting. In order to reach a uniformly spreading solution set, crowding distance for each element is computed and serves as the input of crowded comparison. After the crowded comparison sorting, the non-dominant set or the parent set produces the next generation (offspring). Current research has shown that NSGA II has a good performance on non-convex problems and can achieve the approximately uniformly spreading solution set.

5.2.2 Simulation Results

We use numerical results to illustrate the performance of the proposed schemes. We consider the mmWave Massive MIMO system adopting analog phase-shifter with multiple radio-frequency (RF) chains, which operates at 28Ghz. Uniform linear array (ULA) is adopted at CN and EN side with the dimension, 16×16. For the NSGA II algorithm, we set the

population size as 400 and the generation size as 600. The mutation probability is set to $1/M$. The initial population is randomly generated within the range $(0, P)$.

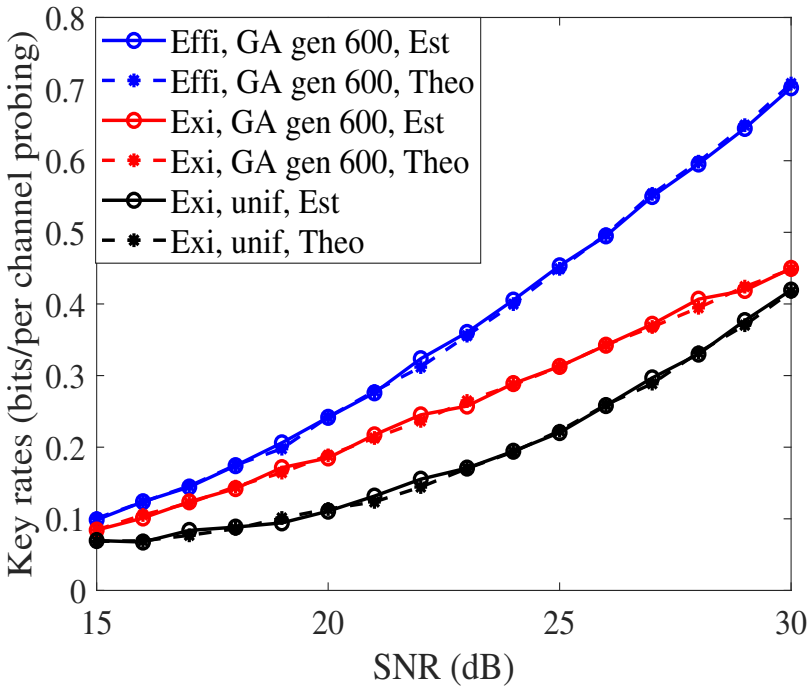


Figure 5.5: GKRs of proposed GA-based group key generation, $M = 6$

In Fig. 5.5, we start by evaluating the group key rate for the proposed channel probing scheme and the following schemes: 1) the scheme with the existing channel probing strategy and the uniform power allocation strategy, which is denoted by the black lines; 2) the scheme with the existing channel probing strategy and the optimized power allocation, which requires $M - 1$ ENs to have $M - 1$ rounds of bi-directional channel probings. It is denoted by the red lines. For all of cases, the solid line represents the theoretical GKRs and the dotted lines denotes the estimated GKRs using the proposed estimator in (4.23). It can be

observed that the curves representing the theoretical GKRs, overlaps with the dotted curves denoting the estimated GKRs nicely. Given SNR 9dB, the mean of MI difference is 0.0125 bits. Comparing with the GKRs at SNR=15dB, which is 0.1 bits/per channel probing, the mean of MI difference is invisible in this case. Besides, the proposed channel probing strategy could outperforms the existing probing strategies. For instance, the scheme with the GA-based power allocation has the higher GKRs compared with the existing channel probing strategy. In addition, it can be further observed that the performance gap between the proposed channel probing scheme and the existing scheme becomes wider as the SNR increases, which is due to the fact that less channel noise can be observed at the analogy beamformer side in the high SNR regimes and the good orthogonality among downlink channels thus can be maintained in the digital precoding domain. At the same time, after increasing the SNRs, the consistency among the channel measurements at two sides could be improved.

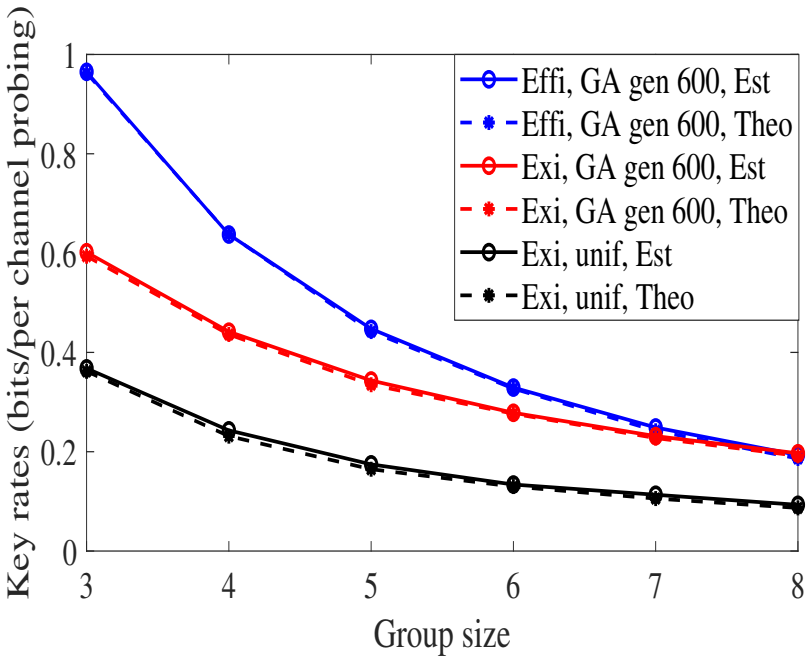


Figure 5.6: GKRs of the proposed scheme under various group size, $SNR = 25$dB

Besides the SNRs, the performance of GKR is determined by the group size as well, which is comprehensible. For instance, while observing the group key generation protocol, an enlarged group size can directly lead to a longer channel difference vector $\mathbf{\Delta} = \{\overline{h}_{c,j} - \overline{h}_{c,1}, ..., \overline{h}_{c,j} - \overline{h}_{c,M}\}$, which has to be broadcasted over the public channel. A longer channel difference, however, can give the eavesdroppers more hints on the reference channel and thus results in the information leakage of the group channels. A finding in the analytical group key rate also support this observation. For a large group size M, the term $\tilde{\sigma}_{i,g}^4 a_i^{-1}$ in the logarithm of the GKR has to be fully extracted, which greatly limits the increasing of the GKR. To give a better illustration of this phenomenon, we list the GKRs under various group sizes In Fig. 5.6, where two channel probing strategies are compared. It is observed that the GKR decreases while expanding the group size by incorporating more

group members. This observation coincides with the aforementioned analysis. Especially, we also find that the GKRs of the proposed channel probing scheme will quickly drop to the same level as the existing channel probing with the optimized power allocation. Such effect is due to the noise induced by the imperfect channel orthogonality realized in the digital precoding domain. For instance, imperfect channel orthogonality will introduce noise at the downlink channel estimation stage. The noise is then accumulated and broadcasted in the group channels, which will further impair the performance of GKRs.

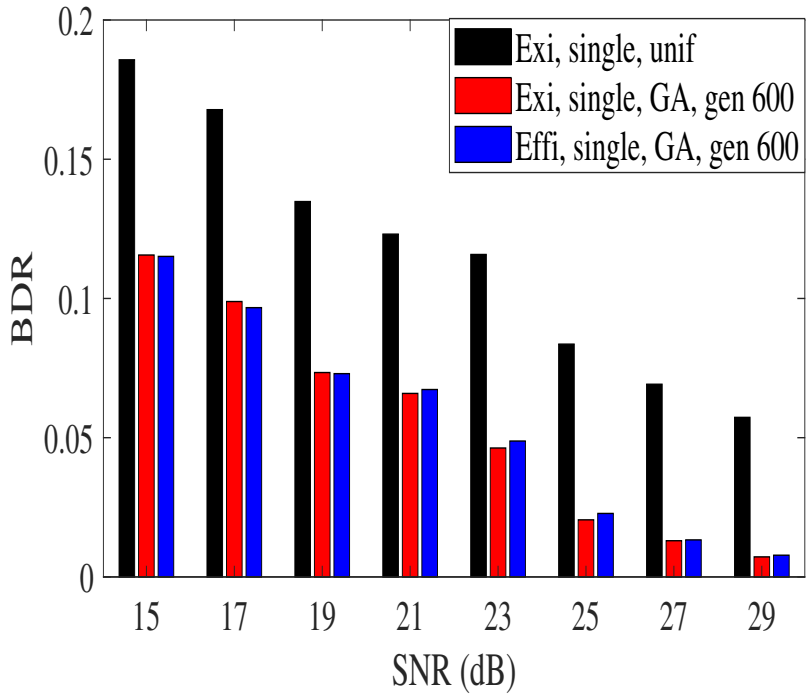


Figure 5.7: BDR under various SNRs, $M = 6$

Fig. 5.7 depicts the numerical results of bits disagreement ratio (BDR) under various SNRs. The quantization level is set to be 4. From this figure, in the high SNR regime, it can

be observed that the GA-based power allocation downlink probing outperforms the scheme that utilizes the uniform power allocation. However, BDR of GA-based power allocation and the existing probing scheme tend to have the same values in the high SNR regime. Based on Fig. 5.5 and Fig. 5.7, we can observe that channel probings with the higher energy can reduce the BDR efficiently. However, in a group, the actual group key rates are influenced by the power allocation strategy.

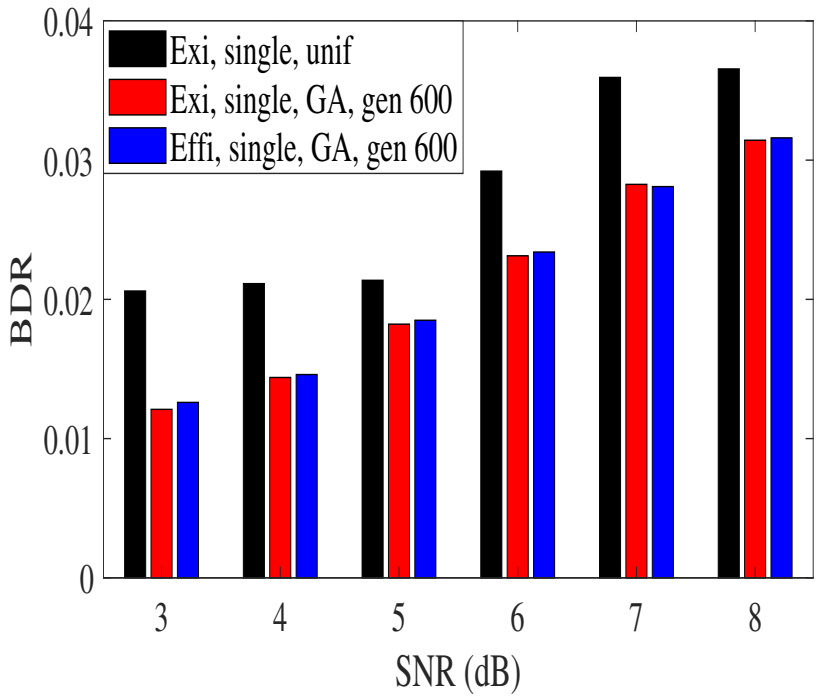


Figure 5.8: BDR under various group size, $SNR = 25dB$

In Fig. 5.8, if we set the $SNR = 25$dB, the BDR versus different group size from 3 to 8 are provided. We can observe that the BDR of GA-based algorithm and existing channel probing scheme, represented by the bars in blue and red, have lower value compared with the

BDR of uniform power allocation scheme. Besides, for the GA-based algorithm and current channel probing scheme, the BDR will grow as the increasing of group size. However, for the uniform power allocation, within a range of the group size between 3 to 5, the BDR is insensitive to the changing of group size. For the group size larger than 5, the BDR of the uniform power allcation schemem will increase accordingly.

Chapter 6: Conclusion and Future Works

6.1 Conclusion

An efficient channel probing strategy for group key generation in mmWave Massive MIMO networks has been proposed, which is based on the hybrid precoding and the NSGA II algorithm. Besides, a scheme for the group key rates estimation has been developed based on MLE. In the proposed group key generation scheme, a baseband precoder has been applied in the downlink probing, which enables the CN to send downlink channel probing signals to several ENs concurrently. Besides, to further improve the group key rates, the NSGA II is modified to optimize the power allocation for the downlink probings, which can reach a spread-out solution region and achieve the Pareto optimality. The estimated group key rates match the theoretical key rates.

6.2 Future Works

There are several possible directions for future research:

1. In chapter 3, we only consider the hybrid precoding based group key generation, where only the ULA antenna array is considered. In the future work, we can extend our design to the UPA-antennas case where the planar antenna array can be applied at the both side. For instance, UPA antennas can be applied for the 3-D beamforming, which can handle angles from the azimuth and elevation perspective. Higher design degree of freedom can be achieved.

2. In this work, we only consider the design for the networks with the star-topology, which is the most common network topology. In some scenarios, we have to consider

the networks with a chain topology, for instance regarding the satellite ground stations or other networks with nodes locating far off. In this case, the scheme developed for the star-topology cannot be applied directly in the chain-topology networks. For instance, each node EN_i in this network only connects to its former and latter points and other nodes are not visible. In this case, the efficient group key protocols have to be developed to share the common randomness. At the same, the channel probing efficiency has to be improved as well.

3. In this work, we focus on the channel probing efficiency improvement. In fact, group key generation rate is also affected by the factors like the quantization level specification, randomness extraction, whose effect are not discussed in this thesis. In the future work, we will develop advanced frameworks after considering these effect.

Appendix A:

$$\{-\overline{h}_{c,u}, \overline{h}_{u,c}\} \sim \mathcal{CN}(\mathbf{0}, \begin{bmatrix} \sigma_{g,u}^2 + |G_{u,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma_n^2 & -\sigma_{g,u}^2 \\ -\sigma_{g,u}^2 & \sigma_{g,u}^2 + |G_{c,u}|^2||\mathbf{w}_{bu}||^2\sigma_n^2 \end{bmatrix}) \tag{A.1}$$

$$\begin{aligned} \mathbf{A} &= \begin{bmatrix} \sigma_{g,1}^2 + |G_{1,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma_n^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_{g,M-1}^2 + |G_{M-1,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma_n^2 \end{bmatrix} \\ &+(\sigma_{g,j}^2 + |G_{j,c}|^2||\mathbf{f}_{(\cdot)}||^2\sigma_n^2) \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} \\ &= \mathbf{A}_1 + \mathbf{A}_2, \end{aligned} \tag{A.2}$$

$$\{\mathbf{\Delta}, \overline{h}_{u,c}\} \sim \mathcal{CN}(\mathbf{0}, \begin{bmatrix} \mathbf{A} & \mathbf{c} \\ \mathbf{c}^T & \sigma_{g,u}^2 + |G_{c,u}|^2||\mathbf{w}_{(\cdot)}||^2\sigma_n^2 \end{bmatrix}) \tag{A.3}$$

$$\mathbf{c}^T = \Big[0, ..., (-\sigma_{g,u}^2), ...0\Big] \tag{A.4}$$

Bibliography

Bibliography

[1] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 831–846, 2014.

[2] A. Alkhateeb, G. Leus, and R. W. Heath, "Limited feedback hybrid precoding for multi-user millimeter wave systems," *IEEE trans. on wireless commun.*, vol. 14, pp. 6481–6494, 2015.

[3] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, 2019.

[4] H. Liu, J. Yang, Y. Wang, Y. J. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, 2014.

[5] P. Xu, K. Cumanan, Z. Ding, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Trans. Info. Forensics Security*, vol. 11, no. 8, pp. 1831–1846, Aug 2016.

[6] C. Ye and A. Reznik, "Group secret key generation algorithms," in *IEEE ISIT*, June 2007, pp. 2596–2600.

[7] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Info. Theo.*, vol. 56, no. 12, Dec 2010.

[8] C. D. T. Thai, J. Lee, and T. Q. Quek, "Secret group key generation in physical layer for mesh topology," in *IEEE GLOBECOM*. IEEE, 2015, pp. 1–6.

[9] J. Tang, H. Wen, H.-h. Song, L. Jiao, and K. Zeng, "Sharing secrets via wireless broadcasting: A new efficient physical layer group secret key generation for multiple iot devices," *IEEE Int Things J.*, 2022.

[10] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: Nsga-ii," *IEEE trans. evol. comput.*, vol. 6, no. 2, pp. 182–197, 2002.

[11] O. El Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, "Spatially sparse precoding in millimeter wave mimo systems," *IEEE trans. on wireless commun.*, vol. 13, no. 3, 2014.

[12] J. Palacios, D. De Donno, and J. Widmer, "Tracking mm-wave channel dynamics: Fast beam training strategies under mobility," in *IEEE INFOCOM*. IEEE, 2017, pp. 1–9.

[13] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, 2016.

[14] H. Liu, J. Yang, Y. Wang, Y. J. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec 2014.

[15] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 18–33, Jan 2019.

Curriculum Vitae

Long Jiao received his B.S. from Xidian University, China, in 2016. He is currently working towards the Ph.D. degree at George Mason University under the supervision of Dr. Kai Zeng.