Physical Layer Key Generation Using Virtual AoA and AoD of mmWave Massive MIMO Channel

Long Jiao, Jie Tang, Kai Zeng
Department of Electrical and Computer Engineering
George Mason University, Fairfax, VA, US 22030
Email:{ljiao, jtang20, kzeng2}@gmu.edu

Abstract—Shared secret key generation from wireless channel characteristics has attracted a lot of research attention in recent years due to its low computational overhead and potentials to achieve information-theoretic security. In this paper, for millimeter wave (mmWave) Massive MIMO channel, we propose to use new channel characteristics – virtual AoA (Angle of Arrival) and AoD (Angle of Departure), to generate a shared secret key between two devices. Other than reciprocity, AoA and AoD of the virtual channel present sparsity and their estimation is efficient and robust against noise. Through theoretical analysis and extensive simulations, we show that the proposed key generation using virtual AoA and AoD achieves much higher bit agreement ratio than existing mechanisms directly using channel state information. Our method can achieve above 99% bit agreement ratio even under very low SNR (e.g., -10dB), which is not achievable by the existing mechanisms. Besides, in our proposed mechanism, the bit agreement ratio becomes higher when number of antennas increases, along with higher key generation rates achieved per channel sounding.

I. INTRODUCTION

Physical layer key generation that exploits reciprocity and the randomness of wireless fading channels has attracted a lot of research attention in recent years [1]. Different from the traditional Diffie-Hellman (D-H) key exchange mechanism, generating a shared key using physical layer characteristics enjoys low computational overhead and has the potential to achieve information-theoretic security. That is, the secrecy of the generated key is not dependent on the hardness of a computational problem but relies on the physical laws of the wireless fading channels.

As one of the most advanced wireless communication technologies, millimeter wave (mmWave) Massive MIMO is considered as a key enabler for the upcoming 5G communication systems [2]. mmWave uses spectrum from 30 GHz to 300 GHz separating itself from the current WiFi and cellular systems operating at carrier frequency below 6 GHz. Owing to its high carrier frequency, mmWave communication can achieve very high bandwidth and data rates. In Massive MIMO system, the tiny wavelengths (5.35mm) allow for hundreds of antenna elements to be placed in an array on a relatively small physical platform [3].

Although many physical layer key generation mechanisms have been proposed for 3G/4G networks, no physical layer key generation concerning 5G techniques, such as mmWave Massive MIMO, have appeared. Different from the existing key generation mechanisms, physical layer key generation in mmWave Massive MIMO communication faces new challenges due to its unique channel characteristics and large number of antennas.

First, millimeter wave channel exhibits a limited scattering nature, thus cannot be treated as a Gaussian channel. Therefore, existing theoretical analysis on the key capacity based on Gaussian channel model assumption cannot be directly applied. Second, for Massive MIMO, as dimensions of the channel matrix grow large, the channel estimation becomes particularly challenging due to the need to estimate a large number of matrix entries [4]. Third, in previous work [5], a large portion of bits generated at two devices can be different in low SNR regimes, thus requires significant amount of overhead for reconciliation, which leads to low key generation efficiency.

In this paper, aiming at an efficient and secure physical layer key generation in mmWave Massive MIMO communication, we propose to use two new channel characteristics, virtual Angle of Arrival (AoA) and Angle of Departure (AoD), as random sources to generate a secret key. Using virtual AoAs and AoDs brings the following advantages. 1) They are easily estimated with low overhead using a virtual sparse channel estimation method. The estimation overhead is largely reduced compared to that of channel state information estimation. 2) Due to the discrete nature and high estimation accuracy of virtual AoAs and AoDs, the quantization can be eliminated in the key generation, which simplifies the process, reduces the number of discarded bits, and improves the key generation efficiency. 3) Virtual AoAs and AoDs estimation is robust against noise and present very high reciprocity even in low SNR regimes. This allows us to achieve a very high bit agreement ratio (e.g., above 99%) in low SNR (e.g., -10dB), which is usually unachievable by directly using estimated channel state information. High bit agreement ratio largely reduces the reconciliation overhead, which is important for the usability and efficiency of physical layer key generation. Moreover, in our schemes for Massive MIMO, when the number of antennas increases, the bit agreement ratio becomes...
higher, along with higher key generation rates.

We summarize our contributions below: 1) To the best of our knowledge, we are the first to propose the use of virtual AoAs and AoDs of mmWave Massive MIMO channel to generate a shared secret key between two devices. 2) We demonstrate that the estimation of sparse mmWave Massive MIMO virtual channel has low complexity. Due to the sparsity of mmWave channel, a limited number of virtual AoAs and AoDs can be fastly estimated at both sides with high accuracy even in low SNR regimes. 3) By analyzing the distributions of virtual AoAs and AoDs, we conduct theoretical analysis on the key capacity and secret bit rates for mmWave Massive MIMO channel. 4) With our proposed estimation algorithm, the estimated AoAs and AoDs are highly agreed at both sides even in low SNR regimes, thus the quantization process can be eliminated, which greatly reduces the reconciliation overhead.

II. RELATED WORK

In recent years, researchers have investigated a new key generation mechanism that exploits the reciprocity of the random wireless fading channel [1, 6–9]. This mechanism is generally called physical layer key generation, in which wireless devices measure highly correlated wireless channel characteristics (e.g., channel impulse responses or received signal strengths) and use them as shared random sources to generate a shared key.

According to the number of antennas in the transceivers, we can classify the physical layer key generation works into two categories: single antenna and MIMO based key generation. In single antenna cases, various channel characteristics have been proposed to generate the secret key, including received signal strength (RSS) [10], channel impulse response/channel state information [6], and phases [7]. In a recent work, researchers propose to use AoA as the common random source to generate the shared key [11], where the AoA is different from virtual AoAs and AoDs in our work. Furthermore, [11] only considered the single antenna scenario. There are hundreds of antennas in the mmWave Massive MIMO system. Besides, direct channel estimation can be challenging because of computation complexity and time consumption caused by the large dimension of Massive MIMO channel. Moreover, using AoA at both sides, it only fits for a line-of-sight propagation path between the two communication parties. Therefore, based on the reason listed on above, work [11] cannot be applied in mmWave Massive MIMO systems. In our work, we consider the non line-of-sight propagation condition and estimate virtual AoAs and AoDs, which can reflect the sparsity of mmWave channel.

In MIMO key generation cases, works in [12, 13] conducted an indoor MIMO measurement campaign in the 2.51 to 2.59 GHz band and studied the number of available key bits in both line-of-sight and non-line-of-sight environments. But the number of antennas considered is relatively small and the carrier frequency is not as high as millimeter wave. In [12], a theoretical upper bound for the maximum size of the generated secret key is derived based on the mutual information between the channel estimates at the two legitimate nodes. However, all the theoretical analysis are based on the Gaussian channel assumption which cannot be satisfied in mmWave channel because of the unique limited scattering nature of mmWave channel [14, 15].

Different from all the existing physical layer key generation works, we propose to use two new characteristics, AoAs and AoDs of virtual mmWave Massive MIMO channel, to generate the shared key between two devices. Owing to the sparsity of mmWave Massive MIMO channel, virtual AoAs and AoDs can be accurately estimated with relatively low overhead. They also present high reciprocity even in low SNR regimes, which is usually unachievable by using other channel characteristics. We will discuss this effect in section VI.

III. SYSTEM MODEL

In this section, we will discuss the virtual mmWave channel and its sparsity characteristics. The key generation model
A. mmWave Massive MIMO channel model and virtual channel representation

The mmWave Massive MIMO channel poses a sparse scatter characteristic. The scatters in mmWave Massive MIMO channel always exhibit limited number of multipaths [2] thus lead to a non-gaussian channel matrix. For a non-gaussian channel, existing theoretical analysis on the key capacity based on Gaussian channel model assumption [12, 13] cannot be directly applied. In our scheme, we consider the narrowband and block fading channel model in non-line-of-sight (NLOS) conditions, where channel is assumed to be independent between two blocks [2]. Our work can be extended to line-of-sight (LOS) conditions easily. The NLOS narrowband mmWave Massive MIMO channel model testified by mmWave measurements campaign can be presented below. The $N_r \times N_t$ column channel matrix $\mathbf{H}$ can be written as

$$ \mathbf{H} = \sqrt{\frac{N_r N_t}{\rho}} \sum_{l=1}^{L} \mathbf{a}_r(\phi_{r,l})^* \mathbf{a}_t(\phi_{t,l}) $$

(1)

where $\rho$ denotes the average path-loss, $L$ denotes the number of scatters, which can characterize the sparsity of channel, and $\alpha_l$ is the corresponding fading coefficients with zero mean complex Gaussian distribution. The variables $\phi_{r,l}, \phi_{t,l} \in (0, 2\pi]$ denote the physical AoD and AoA angles at the transmit and receive sides, respectively. The vector $\mathbf{a}_r(\phi_{r,l}) \in \mathbb{C}^{N_r \times 1}$ and $\mathbf{a}_t(\phi_{t,l}) \in \mathbb{C}^{N_t \times 1}$ are the antenna array response vectors at transmit and receive sides, where uniform linear arrays (ULA) are used [2].

The virtual channel representation [16] characterizing the mmWave Massive MIMO channel can be written as

$$ \tilde{\mathbf{H}} = \mathbf{U}_r \mathbf{H} \mathbf{U}_t^H $$

(2)

where $\mathbf{U}_r \in \mathbb{C}^{N_r \times N_r}$ and $\mathbf{U}_t \in \mathbb{C}^{N_t \times N_t}$ are unitary discrete Fourier transform (DFT) matrices. The matrix $\tilde{\mathbf{H}} \in \mathbb{C}^{N_r \times N_t}$ is the virtual channel matrix [16]. The channel matrix $\mathbf{H}$ and $\tilde{\mathbf{H}}$ are unitarily equivalent because $\mathbf{H}$ is characterized by its virtual representation $\tilde{\mathbf{H}}$. Due to the limited scattering property of mmWave channel, each pair of physical AoA and AoD in physical channel $\mathbf{H}$ is projected to a pair of angles (virtual AoAs and AoDs) in the unitary discrete DFT matrices $\mathbf{U}_r$ and $\mathbf{U}_t$. Each pair of virtual AoA and AoD is assigned a large complex value in the virtual representation $\tilde{\mathbf{H}}$. The complex values of other virtual AoAs and AoDs that are not associated with the $L$ physical AoAs and AoDs have very small complex values and can be seen as noise.

As the antenna size increases, the $\tilde{\mathbf{H}}$ becomes more and more sparse and on grid [17]. We plot the magnitude of $\tilde{\mathbf{H}}$ to demonstrate it. In Fig. 1 (a), when $L = 5$ and $N_r = N_t = 16$, here are multiple “hills” spread all over the coordinates, which indicate that the sparsity is not very significant. In Fig. 1 (b), as the number of antennas increases to 128, virtual AoAs and AoDs on virtual channel can be denoted by $L$ distinct pulses in $\tilde{\mathbf{H}}$, which shows notable sparsity. By estimating the coordinates of such peaks, we can get $L$ pairs of virtual AoAs and AoDs corresponding to the $L$ pairs of physical AoAs and AoDs. In the following parts of the article, we use the term "peaks" to denote the pulses representing the magnitude values of virtual AoAs and AoDs. The advantages brought by using virtual AoAs and AoDs are discussed in section IV. We will also present our channel estimation algorithm for key generation in that section.

B. Key generation model

Fig. 2 illustrates the key generation model for mmWave Massive MIMO system, where Alice and Bob are legitimate users that intend to generate the secret key, while Eve is a potential eavesdropper. Assume Alice and Bob are equipped with $N_a, N_b$ antennas, respectively. The overall key generation model consists of several steps. In the beginning, Alice and Bob send sounding signals to each other within the channel coherence time. After receiving sounding signals, Alice and Bob use an algorithm (that will be proposed in section IV) to extract the virtual AoAs and AoDs, which are the coordinates of peaks in virtual channel $\tilde{\mathbf{H}}$. Note that, because the coordinates representing virtual AoAs and AoDs are pre-quantized, the quantization process is not required in our work. In the end, Alice and Bob conduct information reconciliation and privacy amplification to generate the secure bits.

Other than channel sounding for random source extraction, a typical key generation process also includes quantization, information reconciliation, and privacy amplification. By exploiting virtual AoAs and AoDs as common source, we will enjoy the following benefits.

At first, in our work, estimated coordinates of virtual AoAs and AoDs are pre-quantized and thus quantization is not required. Secondly, our key generation scheme can achieve a low bit disagreement ratio at Alice and Bob sides, which is desirable to achieve a high key generation rate and efficiency.
Such effect can bring a lot of benefits. A low bit disagreement ratio after channel sounding can greatly reduce the reconciliation overhead, which can be significant if the bit disagreement ratio is high before the reconciliation. Besides, during the reconciliation, parity bit information may be exchanged to correct errors. A low bit disagreement ratio reduces the amount of bit information revealed to Eve during the reconciliation. For example, if existing reconciliation Cascade algorithm is used to reconcile two bit strings having a 10% bit mismatch, the number of exposed bits can be around 60% [18].

In previous work, estimated physical channel $\hat{H}_A$ and $\hat{H}_B$ are chosen as the random common source. The maximum number of generated bits that Alice and Bob can extract can be denoted as $I_k = I(\hat{H}_A; \hat{H}_B)$ [12], where $I(\cdot)$ denotes the mutual information operator. For virtual channel matrix key generation, the maximum number of generated bits of legitimate devices can be written as $I_k = I(\hat{H}_A; \hat{H}_B)$.

C. Eavesdropping model under mmWave channel

The number of secure bits is the conditional mutual information between Alice and Bob’s measurements given the leaked information to Eve. In this work, it can be written as $I_{sk} = I(\hat{H}_A; \hat{H}_B|\hat{H}_C, \hat{H}_D)$. In the mmWave system, two channels become independent if they are separated by several wavelengths [19]. As is known, the millimeter wavelength is on the scale of millimeter and the distance between two antenna elements in the Massive MIMO transceiver can be very small (0.5 wavelength or 5.35mm) [3]. Thus we can pack Alice and Bob’s antennas in a protected zone with a certain radius (e.g., half a meter) box or container [20]. The protected zone can prevent an eavesdropper from being close to Alice or Bob within a certain range. It is not difficult to realize this protected zone in the real world. According to the millimeter wave channel coherence property [19], the $\hat{H}_C$ and $\hat{H}_D$ can be considered independent with $\hat{H}_A$ and $\hat{H}_B$. Thus we assume $I_{sk} \approx I_k$. We will derive $I_k$ in Section V.

IV. mmWave Virtual Channel Estimation for Secret Key Generation

In this section, we present the channel estimation algorithm in our work. Our algorithm ensures that as the antenna numbers $N_A, N_B$ become larger, the virtual AoAs and AoDs can be estimated more accurately.

There are some existing works for virtual channel estimation [17, 21, 22]. According to [17], mmWave Massive MIMO systems with $N_A$ and $N_B$ antennas are utilized at Alice and Bob sides, respectively. At Alice side, the received signal $Y_A \in \mathbb{C}^{N_A \times T_a}$ can be written as

$$Y_A = H_A X_A + W_A$$ (3)

The signal can be observed in a window size of $T_a$ for Alice. $H_A \in \mathbb{C}^{N_A \times N_B}$ represents mmWave MIMO channel from Bob to Alice, with antenna size $N_A, N_B$ at Alice and Bob sides, respectively. $X_A \in \mathbb{C}^{N_B \times T_a}$ is the transmitted pilot signal. The signal received at Bob can be represented similarly by changing the subscript in Eq. 3 to B. We assume channel calibration techniques are used here and the channel reciprocity holds. In this case, we treat two channels as the transpose of each other so that $H_B = H_A^T$. $X_A \in \mathbb{C}^{N_a \times T_a}$ and $X_B \in \mathbb{C}^{N_a \times T_B}$ are the transmitted pilot signals with length $T_a$ and $T_B$, respectively. Taking the virtual channel representation in (2), we can rewrite (3) using sparse entries in virtual channel $\hat{H}_A$ and $\hat{H}_B$ as follows [17].

$$\hat{Y}_A = U_A^H Y_A = \hat{H}_A U_B^H X_A + U_B^H W_A = \hat{H}_A \hat{X}_A + \hat{W}_A$$

$$\hat{Y}_B = U_B^H Y_B = \hat{H}_B U_A^H X_B + U_B^H W_B = \hat{H}_B \hat{X}_B + \hat{W}_B$$ (4)

where $U_A \in \mathbb{C}^{N_a \times N_a}$ and $U_B \in \mathbb{C}^{N_B \times N_a}$ are the unitary discrete Fourier transform (DFT) matrices. $\hat{X}_A = U_B^H X_A$ and $\hat{X}_B = U_A^H X_B$. Because of the reciprocity of channel, Alice and Bob can estimate the virtual AoAs and AoDs of peaks in matrix (2) and obtain a set of quantized virtual AoAs and AoDs corresponding to the peaks.

A. Virtual AoAs and AoDs estimation algorithm

In the following part, we briefly explain our algorithm to estimate virtual AoAs and AoDs of peaks. Because Alice and Bob have the same estimation procedure at each side, we use $\hat{Y}$ to represent $\hat{Y}_A$ and $\hat{Y}_B$, $\hat{X}$ to represent $\hat{X}_A$ and $\hat{X}_B$, and $\hat{W}$ to represent $\hat{W}_A$ and $\hat{W}_B$. The estimation algorithm is described below.

**Algorithm 1** Virtual AoAs and AoDs Peaks Estimation

**Input:** $\hat{Y}$, $\hat{X}$, $L$, $N_r$, $N_I$

**Output:** $i_{AoA}$, $\hat{j}_{AoD}$

$$\mathbf{J} = \mathbf{0}, \mathbf{V} = \mathbf{0}$$

$$i_{AoA} = \mathbf{0}, \hat{j}_{AoD} = \mathbf{0}$$

for $i = 1 : N_r$ do

$$j_{max} = \text{argmax}_{j=1, \ldots, N_I} | < Y_{i,:}, X_j > |$$

$$\text{value} = | < Y_{(i,:), X_{(j_{max},:})} > |$$

$$\mathcal{J} \leftarrow j_{max}, \mathbf{V} \leftarrow \text{value}$$

delete $Y_{i,:}$ from $\hat{Y}$

end for

for $j = 1 : L$ do

$$i_{max} = \text{argmax}_{i=1, \ldots, N_I} | < Y_{,:}, X_i > |$$

$$\text{value} = | < Y_{(:,j), X_{(i_{max},:})} > |$$

$$i_{AoA} \leftarrow i_{max}, \hat{j}_{AoD} \leftarrow j_{max}$$

delete $\mathbf{V}(i_{max})$ from $\mathbf{V}$, delete $\mathcal{J}(i_{max})$ from $\mathcal{J}$

end for

In Algorithm 1, $\mathbf{0}$ denotes the null set. Inputs $\hat{Y}$, $\hat{X}$, $L$, $N_r$, and $N_I$ are the received signal, transmitting sequences, number of paths, number of receiving antennas and number of transmitting antennas, respectively. The output $i_{AoA}$, $\hat{j}_{AoD}$ are the sets containing estimated virtual AoAs and AoDs of peaks, respectively. In our algorithm, each row of received signal $\hat{Y}$
is processed separately to find the maximum magnitude value on each row. The $i^{th}$ row of $\hat{Y}$ is

$$\hat{Y}_{i,:} = \hat{H}_{i,:}X + \hat{W}_{i,:};$$  \hfill (5)

where only the $i$-th row of $\hat{H}$, $\hat{X}$ and $\hat{W}$ are involved. The virtual AoD with maximum magnitude in this row is calculated as follows. The product of all transmitted training sequences $\mathbf{X}_{j,:}$ ($j = 1, ..., N_t$) with the selected row $\hat{Y}_{i,:}$ are calculated, which have forms

$$\hat{j}_i = \arg\max_{j=1, ..., N_t} | <\mathbf{X}_{j,:}, \hat{Y}_{i,:}> |$$ \hfill (6)

B. Estimation algorithm is robust against noise

Since only the peaks are needed in this work, our algorithm finds the possible virtual AoDs with the biggest magnitude in each row at the beginning. The reason we take this measure to estimate possible virtual AoDs of peaks is introduced below. For the term $| <\mathbf{X}_{j,:}, \hat{Y}_{i,:}> |$, we can write it as

$$| <\mathbf{X}_{j,:}, \hat{Y}_{i,:}> | = \sqrt{\sigma^2 H_{i,j}^2 + \sigma^2 W_{i,j}^2}$$ \hfill (7)

where $\mathbf{u}_r = [\mathbf{u}_{r1}, \mathbf{u}_{r2}, ..., \mathbf{u}_{rN_r}]$ and $\mathbf{u}_j \in \mathbf{U}_r$. We can choose orthogonal training sequences $\mathbf{X}$ so that it meets the requirement that $\mathbf{X}_A \mathbf{X}_A^H = \sigma^2_n I_{N_a}$ and $\mathbf{X}_B \mathbf{X}_B^H = \sigma^2_n I_{N_b}$, where $\sigma^2_n$ is the power of training sequences.

As the increase of SNR, the magnitude of noise term $\mathbf{X}_{(j,:)}^H \hat{W}_{(i,:)}$ will become negligible compared with the magnitude of term $\sigma^2 H_{(i,j)}^2$. According to (7), for $i^{th}$ row of virtual channel $\hat{H}$, the peaks show up at the column with the largest value of magnitude. In Algorithm 1, at first, the indices and values of possible peak locations on each row will be identified in the first loop by finding the largest magnitude. This process ensures all the column indices of possible peaks are identified. After that, the rows of peaks are needed to find out. In Algorithm 1, the number of rows with the largest $L$ magnitude values are identified in the second loop. The outputs of Algorithm 1 are the indices of rows and columns which represent virtual AoAs and AoDs of peaks.

The algorithm designed for the mmWave Massive MIMO key generation system brings several advantages. It reduces the channel estimation overhead since there are only a limited number of coordinates of virtual AoAs and AoDs to be estimated. Meanwhile, by using our algorithm, Alice and Bob can estimate the coordinates of virtual AoAs and AoDs with a higher agreement ratio especially when the number of antennas increases. Although only extracting the randomness from the location of peaks may lose some entropy, we will show that the entropy can always be increased with the number of antennas, and a higher key rate can be satisfied with large enough antenna numbers.

V. Secrecy Key Rate Analysis

In this section, we will analyze the secrecy key rate between Alice and Bob per channel sounding at first. Then we will analyze Eve's attack complexity.

A. Secrecy key rate under mmWave channel

As discussed in Section III, the mutual information of virtual channel matrix can be written as

$$I_k = I(\mathbf{H}_A; \mathbf{H}_B).$$ \hfill (8)

Alice and Bob need the coordinates of virtual AoAs and AoDs. We represent one peak coordinate as $(\hat{A}_i, \hat{D}_i)$, $i = 1, 2, ..., L$. We can write the matrix containing virtual AoAs and AoDs as $\mathbf{H}_A^v$:

$$\mathbf{H}_A^v = \begin{bmatrix}
AOA_{A1} & AOD_{A1} \\
AOA_{A2} & AOD_{A2} \\
... & ...
\end{bmatrix}$$ \hfill (9)

$\mathbf{H}_B^v$ has a similar form. The estimated coordinates at Alice and Bob can be written as:

$$\mathbf{H}_A^v = \mathbf{H}_A^v + [\mathbf{n}_A^H, \mathbf{n}_B^H]$$ \hfill (10)

where $\mathbf{n}_A^H$ and $\mathbf{n}_B^H$ are the estimate error vectors of virtual AoAs and AoDs at Bob and Alice, respectively.

In the high SNR scenario, when $N_t, N_r \to \infty$, the noise impact on peaks tends to be zero, thus it can approximate as $\mathbf{n}_A^H, \mathbf{n}_B^H \to 0$, which means Alice and Bob can obtain accurate virtual AoAs and AoDs coodinates. Thus the matrix can be written without noise terms as:

$$\mathbf{H}_A^v = \begin{bmatrix}
AOA_{A1} & AOD_{A1} \\
AOA_{A2} & AOD_{A2} \\
... & ...
\end{bmatrix} = \begin{bmatrix}
\beta_1 \\
\beta_2 \\
... \\
\beta_L
\end{bmatrix}$$ \hfill (11)

where vector $\beta_i$ includes $(AOA_i, AOD_i), i = 1, ..., L$.

**Property 1:** When scatter numbers $L$ is much less than $N_r, N_t$, the mutual information $I_k^v$ based on peak paths location can be written as:

$$I_k^v = I(\mathbf{H}_A^v; \mathbf{H}_B^v) \approx \sum_{i=1}^{L} I(\beta_{A_i}; \beta_{B_i})$$ \hfill (12)

**Proof.** As analyzed above, the mutual information $I_k^v$ can be written as:

$$I_k^v = I(\mathbf{H}_A^v; \mathbf{H}_B^v) = I(\beta_{A1}; \beta_{A2}; \beta_{AL}; \beta_{B1}; \beta_{B2}; ..., \beta_{BL})$$ \hfill (13)

when scatter numbers $L$ are much less than $N_r, N_t$, the impact of the $L$ scatters on each virtual AoA and AoD coordinates tend to be independent [17]. Thus based on the mutual information chain rules, $I_k^v$ can be approximately presented in
Eq.(14) and (15). Because of the independence of each scatters impact on virtual AoA and AoD coordinates, we can get

$$I(\beta_{A1};\beta_{B1}, \beta_{B2}, ..., \beta_{BL}) = I(\beta_{A1};\beta_{B1})$$

(16)

Then we can get property 1.

**Property 2:** When $L$ is much less than $N_s, N_t$, in the high SNR scenario, for $N_s, N_t$ become very large, the key rate of sparse virtual channel can be approximated as :

$$I(\mathbf{h}_A^v; \mathbf{h}_B^v) \approx L \log_2 N_s N_t$$

(17)

**Proof:** As analyzed above, each virtual angle $\text{AOA}_i, i = 1, 2, ..., L$ and $\text{AOD}_i, i = 1, 2, ..., L$ are independent of each other. Thus

$$I(\beta_{A1};\beta_{B1}) = I(\text{AOA}_{A1}, \text{AOA}_{A2}, \text{AOA}_{A3}, \text{AOA}_{A4}, \text{AOA}_{A5}, \text{AOA}_{A6})$$

$$\approx H(\text{AOA}_{A1}, \text{AOA}_{A2})$$

(18)

For each pair of virtual AoA and AoD is generated from one independent scatter, the distribution of it is close to a uniform distribution in $N_s$ and $N_t$. Then based on property 1, we can get the approximation of mutual information rate as:

$$I_k^v \approx L \log_2 N_s N_t$$

If $N_s = N_t = N = 2^\pi$, we can have

$$I_k^v \approx 2L \pi$$

(19)

(20)

The result of property 2 is very useful to estimate the essential time to generate a required key bits. For example, if the system needs a key length of 128 bits, under $N_s = N_t = 128$ with sparse path number $L = 5$, it needs at least 2 channel coherent time to generate a 128-bit secret key.

**B. The eavesdroppers under millimeter wave channel**

The only useful information Eve may obtain is the number of paths $L_E$ estimated from the eavesdropping channel. If $L_E \neq L$, Eve will not even know how many bits are generated between Alice and Bob per channel sounding. When $L_E = L$, Eve will obtain the same number of subpaths as Alice and Bob, but she needs to guess the virtual AoAs and AoDs of peaks of Alice and Bob. Eve has to guess $L$ locations in the $N_s \cdot N_t$ dimension components due to the uniform distribution of virtual AoAs and AoDs which is verified by the simulation in Section VI-A. Even Eve has 1 bit disagreed with the key generated between Alice and Bob, she will not be able to decrypt the encrypted communication between Alice and Bob. Since Eve’s eavesdropping channel is independent of Alice and Bob channel, Eve has to conduct a brute-force attack on the key. Based on description above, we can have the property 3 below to measure Eve’s attack complexity.

**Property 3:** When Eve gets the path number $L_E = L$, the probability that Eve can acquire the entire secrecy key will not be higher than:

$$\beta = \frac{1}{\left(\frac{N_s}{L}\right)^L} = \frac{1 \cdot 2 \cdot L}{(N_s - L + 1)(N_s - L + 2)...(N_s - N_t)}$$

(21)

**VI. SIMULATION AND NUMERICAL RESULTS**

In this section, we will evaluate the performance of our key generation mechanism by simulations. We will also compare the performance of our key generation with the existing ones directly using channel state information (For instance, the physical $\mathbf{H}$).

In our work, mmWave MIMO system operates at 28GHz and the statistical mmWave channel model is established according to NYU mmWave channel measurement campaigns [3, 19], according to which the parameters in model, like physical AoD/AoA denoted as $\phi_l, l$, are randomly generated as uniform distribution in $(0, 2\pi)$ [23]. The number of scatters is set as $L$ and each scatter is assumed to contribute to a single propagation path [2]. We set $N_s = N_t$. The length of the training sequence $\mathbf{X}$ is equal to the number of receiving
Figure 3: The virtual AoAs and AoDs of Alice and Bob when $N_r = N_t = 128, L = 3, 5$ at $SNR = 0dB$

Figure 4: The virtual AoAs and AoDs of Alice and Bob when $N_r = N_t = 128, L = 5$ at $SNR = 0dB, 5dB$

Figure 5: The estimated virtual AoAs and AoDs distribution when $N_r = N_t = 32, L = 2$ at $SNR=10dB$

Bob sides and their distribution. We first evaluate the AoAs and AoDs consistency and their distributions under different SNRs from figure 3 to 4. In figure 3 and 4, we plot 200 times of virtual $\hat{\mathbf{H}}^T$ estimated at Alice and Bob sides.

Figure 3 shows the virtual AoAs of Alice and AoDs of Bob under $N_r = N_t = 128, L = 3, 5$ under SNR=0db, respectively. The points on the $45^o$ straight line in the figure represent a pair of consistently estimated virtual AoAs at Alice side and AoDs at Bob side. From figure 3 (a), when $L = 3$ and $N_r = N_t = 128$ at SNR=0dB, we can find that the virtual AoAs and AoDs are on the $45^o$ straight line which indicate high consistency (>99%) at low SNR (even under SNR=0dB). Figure. 3 (b) shows that when there are more scatters existed in the mmWave channel (i.e, $L = 5$), the estimation accuracy is decreased slightly but remains high. The reason is, as the number of scatters increases, the magnitudes of scatters on virtual channel matrix are more possible to be more similar. The coordinates of peaks with similar value of magnitudes are more likely to be affected by noise and thus be wrongly estimated under low SNRs.

Moreover, the consistency is also affected by SNR. Figure 4 shows the virtual AoAs of Alice and AoDs of Bob when $N_r = N_t = 128$ and $SNR = 0, 5dB$. From Figure 4, we can see that the higher the SNR is, the more accurate the virtual angle estimation is, which leads to higher consistency.

Figure 5 illustrates the distribution of estimated virtual AoAs and AoDs at Bob side. As mentioned in Section V, theoretical upper bound for the secret key rate analysis is based on the distribution of estimated virtual AoAs and AoDs.

B. Key generation performance

From figure 6 to 9, we simulated $10^5$ bits to get the statistic performance of mutual information per bit, secret bits per channel sounding. We then compared the bit disagreement ratio of our schemes with traditional schemes based on channel state information.

Figure 6 illustrates the average mutual information per bit of Alice and Bob using our proposed scheme under different number of antennas and scatters. We can see that our scheme can achieve about 0.94 mutual information per bit when
Figure 6: Average mutual information per bit at Alice and Bob sides

Figure 7: Secret bits per channel sounding at different SNRs and antenna number

\[ N_r = N_t = 256 \text{ even the SNR is below 10dB. When antenna numbers decrease to } N_r = N_t = 128, \text{ the mutual information per bit at lower SNR tends to be relatively decreasing with higher scatter numbers. For example, for } N_r = N_t = 128 \text{ under } L = 7, \text{ the mutual information is about } 0.89 \text{ at SNR=10dB and increase to } 0.92 \text{ at SNR=0dB. However, for } N_r = N_t = 128 \text{ under } L = 3, \text{ the mutual information is about } 0.93 \text{ at SNR=-10dB. Figure 6 demonstrates that our scheme can achieve good performance even at low SNR.}

Figure 7 illustrates the average key rate per channel sounding under different SNRs. The transmit and receive antenna numbers are \( N_r = N_t = 128, 256 \) with scatter numbers set as \( L = 3, 5, 7 \), respectively. From figure 7, we can find that the increase of SNR does not have a significant impact on the key generation rate.

In Figure 8, the blue curve marked with \( \tilde{H} \) are the bit disagreement ratio based on our key generation scheme. The red curve marked with \( \tilde{H} \) represents existed works which quantize the amplitude of channel estimate \( H \). Using the quantization method in work [13], our method achieves a very low bit disagreement ratio even at low SNR, i.e. when \( N_r = N_t = 128 \) and \( L = 3 \) at SNR=-10dB, it shows that our scheme achieves much higher bit disagreement ratio than the existing scheme. The bit disagreement ratio is close to \( 10^{-2} \).

Figure 9 illustrates the bit disagreement ratio under different antenna numbers and SNRs. It is clearly seen from the figure that, as the increase of antenna number, bit disagreement ratio decreases.

VII. CONCLUSION AND FUTURE WORK

In this paper, we proposed to use virtual AoA (Angle of Arrival) and AoD (Angle of Departure) characteristics of the millimeter wave (mmWave) Massive MIMO channel to generate a shared secret key between two wireless devices. We have proposed a channel estimation method to estimate the values of AoAs and AoDs of peaks in the virtual channel matrix. Exploiting the sparsity of the mmWave Massive MIMO
channel, our method can achieve very high estimation accuracy with low computation overhead and the estimated AoAs and AoDs are highly agreed at both communication parties. Through theoretical analysis and extensive simulations, we showed that the proposed key generation mechanism using virtual AoAs and AoDs achieves much higher bit agreement ratio than existing mechanisms using channel state information. Our method can achieve above 99% bit agreement ratio even under very low SNR (e.g., -10dB), which is not achievable by the existing mechanisms. High bit agreement ratio implies low reconciliation overhead, which is highly desirable for physical layer key generation. Moreover, when the number of antennas increases, our mechanism achieves higher bit agreement ratio, along with higher key generation rate per channel sounding.

In this work, we assume Alice and Bob are equipped with the full-digital antennas. In the future work, we will extend our key generation scheme, exploiting virtual AoAs and AoDs, to mmWave Massive MIMO systems with hybrid analog/digital precoding structure [2, 23]. Theoretical analysis in our work can be adopted in this case. Besides, we only consider the NLOS propagation condition. It will be interesting to study mmWave Massive MIMO key generation under LOS conditions.

REFERENCES


