國立臺灣大學電機資訊學院電信工程學研究所

碩士論文

Graduate Institute of Communication Engineering

College of Electrical Engineering and Computer Science

National Taiwan University

Master Thesis

基於多天線正交多頻分工及位元交錯調變碼系統之實體層安全機制整合設計

Integrated Physical Layer Security Design on MIMO-OFDM Systems and BICM-OFDM Systems

吳之堯

Chih-Yao Wu

指導教授：葉丙成 博士

Advisor: Ping- Cheng Yeh, Ph.D.

中華民國 100 年 7 月

July, 2011

誌謝

碩士班的兩年，咻的一聲一下子就過去了，在這其中有很多歡笑的時光，也有不少壓力很大的時刻，回首看看兩年前與現在的自己，當真感觸良多。在碩士班的最後能順利完成這篇論文，真的要感謝很多人的幫助。

首先感謝的，是我的指導教授葉丙成教授，兩年前也是被老師的風采所吸引而加入了博理 515 這間實驗室。這兩年來，在老師教導下，我學到如何成為一個做事專業的人，對於細節仔細而不馬虎，這樣的態度我相信是終生受用的。此外，老師對於我們的研究和生活都付出了相當多的心力關懷，相當謝謝老師。

再來感謝的，是我的父母親和我的姐姐，你們是我最重要也最親愛的家人。能順利的在台大完成我的學業，如果沒有你們我是不可能做到的。在我心情不好或沮喪時，你們永遠願意傾聽並給我鼓勵。從小到大都是如此，我常常很不懂事，但你們仍對我付出許多卻又不求回報，希望你們永遠身體健康，快快樂樂。

謝謝博理 515 的同學們，邦訔、省億、渝洋。這兩年一起相處的時光真的向你們學習到很多東西，你們每個人都有很多優點是我所沒有的，能跟你們當同學真是我的福氣。也很謝謝實驗室的學長們，彥寰、宗翰、煦杰、承佑，你們一直是我們所努力學習的對象，碩一的時候承蒙你們照顧了，謝謝你們。

另外謝謝台大電機 109 的帥哥們，你們實在太多人了我就不一一列名了我怕漏掉誰，你們豐富了我的大學生活，有你們真的棒透了。謝謝台大熱舞社 19 屆的好夥伴，儘管大家現在都有了不同的路也不再像以前一樣天天練舞，但當時一起努力的回憶我現在想起來還是覺得相當美好。謝謝圖資系一起辦宿營的好夥伴們，希望一直和你們會是很好的朋友。也謝謝十傑學生大會的朋友們，在大學生活的尾端能認識你們真好。

最後謝謝怡君，這兩年謝謝妳的照顧、陪伴和關心，妳永遠都是我最好的朋友。最後的最後，要謝謝我自己這兩年來的努力，不管未來的日子是如何，我都會勇敢面對，找到屬於自己的出路。

摘要

無線通訊網路在我們日常生活中日益普遍，但由於無線通訊的廣播性質，非法使用者相當容易便可接收相同訊號並進行竊聽。因此無線通訊網路的私密性和安全性是一個相當重要的課題。近年來如何在實體層上進行安全機制設計吸引了相當多的研究者，其中的一種方法是利用無線通道來汲取秘密資訊。基於無線通道的雙向對稱性，合法使用者可因此擁有相關的隨機參數。在本篇論文中，我們提出兩種不一樣的機制利用無線通道來汲取秘密資訊。第一種提出的機制為P-MOPI，它能在多天線正交多頻分工系統下產生秘密金鑰並且不會犧牲多天線系統的效能。我們利用預編碼矩陣的編號當作一個有效的金鑰產生方法，同時我們旋轉通道量測信號以避免竊聽者得到任何有用的金鑰資訊。P-MOPI 機制可以讓兩個通訊節點很輕易的產生大量相同的祕密位元作為金鑰使用，所以可以達成安全傳輸並同時擁有多天線系統的效能增益。本篇論文提出的第二個方法為 INTERSECT 機制。我們利用秘密的交織器在多天線位元交錯調變碼系統下達成安全通訊，而秘密交織器可由無線通道頻率響應的大小次序來產生。我們使用電腦模擬來檢驗我們提出機制的可行性，模擬的結果顯示我們提出的機制擁有優秀的安全性並相當適合用在現行的無線通訊系統上。

關鍵字 – 實體層安全機制、多天線正交多頻分工系統、位元交錯調變碼系統、秘密金鑰、密碼學、預編碼矩陣編號、秘密交織器、通道量測信號之旋轉。

Abstract

Wireless communication networks become increasingly pervasive in our daily life. But the broadcasting nature makes wireless communication networks vulnerable to eavesdropping. Any receivers receive the transmitted signals are able to analyze the signals. Thus, privacy and security take an important role in wireless communication networks. Recently, providing security on physical-layer draws lots of interests. Physical-layer security can be achieved by secrecy extraction from wireless channel. Based on channel reciprocity, the legitimate nodes share correlated randomness. In this thesis, we propose two different schemes that extract secrecy from wireless channel. The first one is called P-MOPI, proposed to generate secret keys without sacrifice of MIMO gain for MIMO-OFDM systems. The precoding matrix index (PMI) is utilized as an efficient key generation mechanism and the reference signals are rotated to prevent eavesdropper from learning any secret key information. The P-MOPI scheme easily allows two communicating parties to generate abundant identical secret bits. Both secure communication and the MIMO gain can be guaranteed by using the P-MOPI scheme. The second achievement is the INTERSECT scheme which uses the secret interleaver to ensure confidential transmission for BICM-OFDM system. The order of wireless channel is then utilized as a nature secret source for secret interleaver generation. Computer simulations are done to evaluate the feasibility of our proposed schemes. The results shows the proposed P-MOPI and INTERSECT scheme provides excellent security and are suitable for modern wireless communication systems.

Keywords — Physical-layer Security, MIMO-OFDM Systems, BICM Systems, Secret Key Generation, Cryptography, Precoding Matrix Index, Secret Interleaver, Rotated Reference Signals and etc.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Literature Review

Making confidential transmission in wireless environments is an important issue. Conventional cryptography techniques provides security on upper layers. Recently, building secure transmission scheme on physical-layer draws a lot of research interests. In Wyner's seminal work, he introduces the concept of wiretap channel [1]. Wyner's theoretical investigation has aroused many different proposals on achieving information-theoretic secrecy, such as [2–4]. It is noted that these schemes work without the help of traditional cryptography key. On the other hand, generating secret keys via correlated randomness provides another direction for physical-layer security. These schemes focused on information theoretic secret key distribution. The secure transmission is then achieved using the conventional secret key-based cryptography. The idea is proposed by Maurer [5], and Ahlswede and Csiszár [6]. For the time-division duplexing (TDD) systems, the wireless channel between two terminals is symmetric if channel reciprocity holds. It provides a suitable source for the secret key generation [7]. As a result, the research on physical-layer security can be classified into two categories: security scheme without secret key and the key-based scheme.

The work in [8] is one of the pioneer works that propose practical schemes for keyless PHY security without the knowledge of eavesdropper's information. In the work, a MIMO-OFDM PHY integrated (MOPI) scheme has been proposed to provide communication confidentiality without using any cryptographic ciphers. By the use of channel sounding, MOPI prevents an eavesdropper from learning the channel state information (CSI) of the channel between the eavesdropper and the transmitting node from the preambles or pilot tones. A bit-interleaved coded-modulation (BICM)-based physical layer network coding (PNC) scheme has been proposed such that an eavesdropper, due to lack of CSI, will suffer from very high bit error rate (BER) in decoding. The MOPI scheme has been shown to provide excellent security, forcing the eavesdropper to have large estimation error even if blind channel estimation is used. The computational complexity is also prohibitively expensive if the eavesdropper resorts to brute-force search to recover the CSI. Although the MOPI scheme is promising in providing PHY security, it also has limitations. Since the multiple antennas at the transmitter and the receiver are used for PNC and beamforming, it is impossible for this MOPI scheme to conduct spatial multiplexing nor use space-time codes. This limits the capability of the MIMO system and makes us seek further solution that achieves both MIMO gain and securiy.

As mentioned above, wireless transmission medium seems to be a promising choice as the randomness source for secrecy extraction. The rich scattering in wireless environments results in different multi-path fading at each mobile terminal. The random observations are shared among legitimate users and is inaccessible to the malicious user. Consider the situation where two nodes Alice and Bob want to seek secret key agreement. The observations among the legitimate pairs are denoted as $\mathbf{X^n}$ and $\mathbf{Y^n}$. The public error-free communication $\mathbf{\Phi}$ is allowed between legitimate terminals and is also revealed to malicious user. Alice generates her secret key $\mathbf{K_A}$ from $(\mathbf{X^n}, \mathbf{\Phi})$, and Bob computes his own secret key $\mathbf{K_B}$ from $(\mathbf{Y^n}, \mathbf{\Phi})$. In [9], The secret key rate $\mathbf{S}$ under this scenario is defined to be achievable if the following equations hold for every

$\varepsilon > 0$ and large $\mathbf{n}$,

$$\mathbf{Pr}\{\mathbf{K_A} \neq \mathbf{K_B}\} < \varepsilon \tag{1.1}$$

$$\frac{1}{\mathbf{n}}\mathbf{I}(\boldsymbol{\Phi}; \mathbf{K_A}, \mathbf{K_B}) < \varepsilon \tag{1.2}$$

$$\frac{1}{\mathbf{n}}H(\mathbf{K_A}) > \mathbf{S} - \varepsilon \tag{1.3}$$

$$\frac{1}{\mathbf{n}}\log|\mathcal{K}| < \frac{1}{\mathbf{n}}H(\mathbf{K_A}) + \varepsilon \tag{1.4}$$

here $\mathcal{K}$ denotes the alphabet of the secret key. Equation (1.1) ensures the reliability of secret key agreement; equation (1.2) implies the public discussion should communicates with no information about the generated secret key. The secrecy rate is measured by equation (1.3), and equation (1.4) limits the secret key to be uniformly distributed. In [5] and [6], the information-theoretic secret key capacity C_S which denotes the largest achievable secret key rate is given by

$$\mathbf{C_S} = \mathbf{I}(\mathbf{X}, \mathbf{Y}) \tag{1.5}$$

Equation (1.5) gives us the information-theoretic bound on the secrecy extraction from wireless channel. Nevertheless, how to design a practical key agreement scheme to achieve the secret key capacity remains an open problem. A lot of works has been proposed. In [10, 11], Maurer provided two fundamental steps to form a feasible key agreement protocol: information reconciliation and privacy amplification. Information reconciliation aims at generating two identical sequences based on the random observations among two legitimate users. The public discussion channel helps legal users to communicate with each other and get equal sequences. After the generation of identical sequences, information discussed using the public channel is revealed to the passive attacker and should be wiped out. In the step of privacy amplification, the secret key is extracted from the sequences generated in the information reconciliation phase using linear mapping or universal hash function [12]. The information leakage in the public discussion is eliminated [13].

For secrecy extraction from the channel state information, an intuitive way is to quantize the complex channel coefficient directly. The phase information [7, 14] and amplitude information [15,16] of the complex channel can be utilized to generate secret keys. Nevertheless, when considering practical situation with channel estimation error, the key agreement probability is rather low. To make direct channel quantization more robust, protocols utilizing the public discussion channel based on the principle of information reconciliation and privacy amplification are designed to improve the key agreement probability [17–19].

For the increased degree of freedom in the wideband channel and the MIMO channel, more secret bits are expected to be available with these channels. The problem of secret sharing and the information-theoretic bound in wideband systems have been discussed in [20, 21]. For MIMO channel, considering its channel correlation, direct channel quantization faces the problem of correlated generated secret keys not being uniformly distributed. The works in [22] and [23] attempt to decorrelate the correlated channel at the expense of extremely high feedback overhead for the decorrelation vector. Without the decorrelation vector, these schemes face the problem of the decreased security caused by the correlated channels. Besides the design of secrecy extraction protocol, experiments on secret key generation under different channel models and real wireless channels have been investigated in [24–27] to show the feasibility of physical layer secret key generation.

To provide information-theoretic security on secret key distribution, secrecy extraction from wireless channel seems to be a promising solution. Nevertheless, several recent publications address its vulnerabilities. In [28], a simple attack method is proposed to break the security of reciprocity-based key generation schemes. By estimating the pilot signals, eavesdropper is able to acquire channel information between itself and the legal parties. Based on the physical nature of the wireless channel, the eavesdropper has the opportunity to reconstruct the whole physical surroundings correctly. The eavesdropper is capable of simulating the channel information from the reconstructed wireless environments. On the other hand, there is another type of threat that comes from the nearby eavesdropper. It is generally assumed that the wireless channels are independent by the distance of about several wavelength. The work in [29] did some experiments to examine the channel correlation. Unexpectedly, the results shows that the assumptions may be questionable. The wireless channel are still highly correlated even the two nodes are separated by *one* meter. The experiments show that this might cause the aforementioned key generation method to be insecure when the eavesdropper is nearby.

As a result, several important issues for the reciprocity-based key generation schemes should be emphasized. The first one is the risk using the channel estimation schemes that use the reference signals. The second important issue is the nearby eavesdropper problem which is often omitted by most reciprocity-based schemes. The last issue is the correlated secret key bits. In this paper, a variant of the MOPI scheme—called P-MOPI –utilizing the precoding matrix index (PMI) and the rotated reference signals is proposed to make secrecy extraction from wireless channel with high feasibility and enhanced security. It is well known that the MIMO system performance can be enhanced by applying precoding at the transmitter [30], i.e., multiplying the signal vector by a matrix before transmission. With the optimal precoding at the transmitter, the MIMO channel can be transformed into several parallel subchannels, and the optimum channel capacity can be achieved. Due to the feedback overhead and the complexity issues, typically there is a universal codebook that consists of a finite number of precoding matrices. The precoding matrix indices is used as the secret key in P-MOPI. To prevent the aforementioned threats, we introduce the idea of rotating reference signals which is inspired by the original MOPI scheme. The secrecy information is hide in the rotation of reference signals. Our scheme of sending rotated reference signal does not introduce any overhead, yet the secret key information can still be obtained from the channel estimation procedure. It is noted that the attack method and the nearby eavesdropper problem are no longer annoying problems with our design. On the other hand, both key disagreement probability and communication overhead of public discussion are reduced. The problem of the secret key distribution not being uniform is also solved.

To rotate the reference signals, the signal is multiplied by a matrix before its transmission. Considering the transmission power constraint, only unitary matrices are used in precoding. Due to different channel realizations between the transmitter-legal receiver and the transmitter-eavesdropper pairs, the precoding matrix is only known between the transmitter and the legitimate receiver, so the precoding matrix indices can be used as keys. It is noted that the whole channel matrix contains higher entropy than its corresponding precoding matrix. In this paper, we also design the channel-based MOPI (C-MOPI) scheme to utilize the whole channel information. However, embedding secrecy in whole channel matrix makes the rotation on reference signals non-unitary and increases the channel estimation error. Thus it is only suitable for the situation with high signal to noise ratio (SNR). With our proposed efficient key generation schemes, the shared secret key can be used, e.g., as the seed to generate pseudo random bit sequences, and secured MIMO communications can then be achieved, by using a stream cipher or other cryptography techniques. Both security and MIMO gain are achieved with the proposed P-MOPI and C-MOPI scheme.

On the other hand, it is observed that traditional secrecy extraction from channel quantizes each channel independently. It is obvious some information about the relation between channel elements is thus lost. It is expected that more secrecy can be discovered in the relation between channel elements. The order of the channels can be regarded as another type of random source which cannot be detected by malicious user. The concept of random order is similar to an important element in the bit-interleaved coded modulation (BICM) system – the interleaver. From the communication point of view, interleaving is frequently used to arrange data in a non-contiguous way to improve transmission reliability. It inspires us to use the random order as a secret order to form a secret interleaver. Thus, we propose the interleaver-based secure transmission scheme (INTERSECT). During the channel estimation procedure, one can conceal the interleaving pattern by deliberately allocating the power of the vector of reference signals. legitimate receiver can easily extract the interleaving pattern to decode data, which is not possible for the eavesdroppers.

1.2 Organization

The rest of this thesis is organized as follows. In Chapter 2, relevant background information and system descriptions are introduced. The basic PMI-based MIMO OFDM PHY integrated secret key generation scheme (basic P-MOPI) is in Section Chapter 3. The enhanced PMI-based MIMO OFDM PHY integrated secret key generation scheme (enhanced P-MOPI) is detailed in Chapter 4. The channel-based MIMO OFDM PHY integrated secret key generation scheme (C-MOPI) scheme is shown in Chapter 5. The interleaver-based secure transmission scheme (INTERSECT) is described in Chapter 6. The performance of the proposed schemes is evaluated using computer simulation, with the results presented and discussed Chapter 7. Conclusions and future work are addressed in Chapter 8.

Chapter 2

Backgrounds and System Descriptions

2.1 Background Knowledge

2.1.1 MIMO-systems with precoding

First let us review how the precoding matrix is used in the MIMO system. For the MIMO system, precoding is an operation which utilizes the best subchannel gains. After precoding, the optimal channel capacity can be achieved by appropriate transmission power along with the water-filling principle [30, 31]. For a MIMO channel $\mathbf{H}$, if we decompose $\mathbf{H}$ using the singular value decomposition (SVD) [32] and obtain $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\dagger}$. Love proved in his paper that the optimal precoding matrix is $\bar{\mathbf{V}}$ which consists of the first several columns of the right singular vectors $\mathbf{V}$ [33]. To obtain the optimal precoding matrix, channel state information is required by the transmitter. Nevertheless, in practical situations where feedback overhead is an important issue, full channel state information is usually not available at the transmitter side. As a result, codebook-based precoding [34] seems to a promising solution to strike a balance between feedback overhead, equalizer complexity and the system performance. A universal codebook that consists of a finite number of precoding matrices is shared among the communication terminals. The suboptimal precoding matrix is selected from the finite precoding matrices set. Each precoding matrix in the codebook has an index called PMI. For its simplicity, codebook-based precoding is widely adopted by the modern communication protocols (e.g., LTE, WiMAX) [35].

We briefly illustrate the steps to acquire PMI. There are two nodes involved in the communication and both nodes use MIMO-OFDM system. The transmitter first sends out a reference signal for the receiver to estimate the channel matrix $\mathbf{H}$ and decide the optimal precoding matrix. Note that the channel here stands for the channel on a subcarrier or on certain subcarriers of OFDM. A universal codebook $\mathcal{F}$ is used.

Consider the following MIMO channel capacity formula with precoding [36]

$$\mathcal{C}_{\mathbf{H},\mathbf{F}} = \log_2 \det \left[\mathbf{I}_n + \frac{E_s}{n_s \sigma^2} \mathbf{F}^\dagger \mathbf{H}^\dagger \mathbf{H} \mathbf{F} \right] \tag{2.1}$$

where $\mathbf{I}_n$ is the identity matrix with n denoting the minimum number of antennas at Alice and Bob, E_s is the total power of transmitted signal vector, n_s is the number of data stream, σ^2 is the noise variance, $\dagger$ means the Hermitian, $\mathbf{F}$ is the precoding matrix. As in [36], the receiver finds the precoding matrix and its corresponding PMI from the codebook that maximizes the channel capacity. Mathematically,

$$\hat{\mathbf{F}} = \underset{\mathbf{F} \in \mathcal{F}}{\operatorname{argmax}}\, \mathcal{C}_{\mathbf{H},\mathbf{F}} \tag{2.2}$$

where $\hat{\mathbf{F}}$ is the best precoding matrix from the codebook $\mathcal{F}$. We denote the PMI associated with $\hat{\mathbf{F}}$ by i_{Right} for the reason that optimal precoding matrix is come up with the right singular vectors.

2.1.2 Secret key capacity of the MIMO-OFDM channel

Another question needs to be investigated is how many secret bits can be extracted from the MIMO-OFDM channel. The secret key capacity for MIMO-OFDM channel can be easily derived under the assumption that both the channel and estimation error are joint complex gaussian distributed with zero mean. Considering the situation where Alice has M_A antennas and Bob has M_B antennas, and the OFDM system works with N subcarriers. We rearrange the total estimated channel elements at each terminal to a vector with length $M_A * M_B * N$ and denote it as $\mathbf{H}_A$ and $\mathbf{H}_B$. Alice estimates the channel as $\mathbf{H}_A = \mathbf{H} + \mathbf{Z}_A$ while Bob obtains $\mathbf{H}_B = \mathbf{H} + \mathbf{Z}_B$. Channel estimation error $\mathbf{Z}_A$ and $\mathbf{Z}_B$ are assumed zero mean with variance σ_A^2 and σ_B^2.

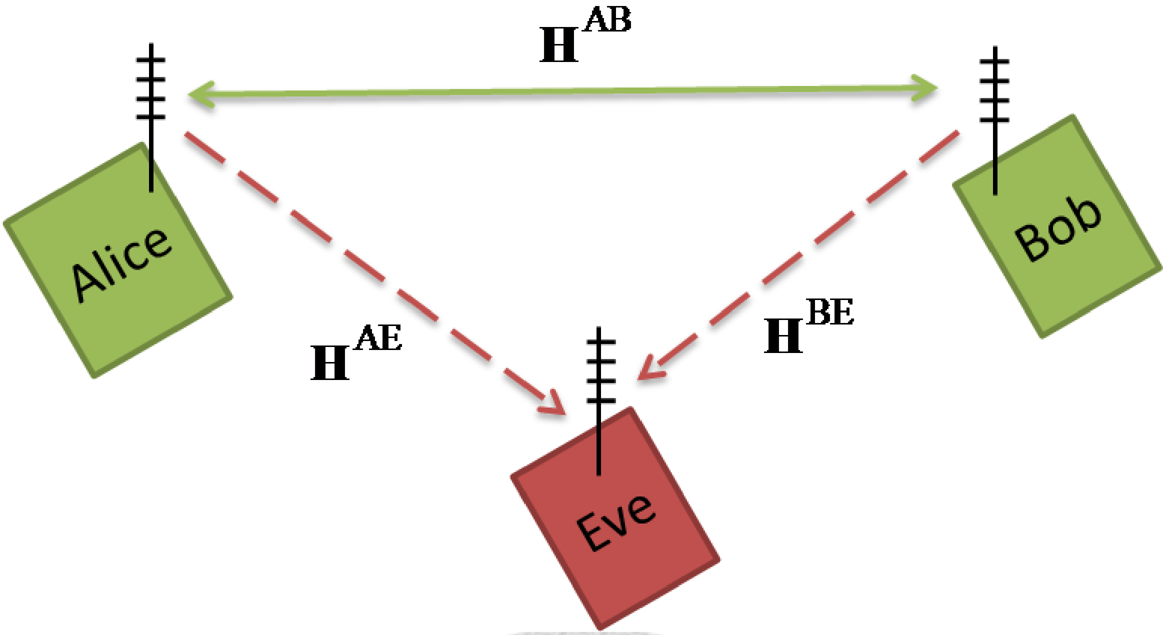


Figure 2.1: System Model

As mentioned above, the secret key capacity for MIMO-OFDM channel can be derived by

$$
\begin{aligned}
&\mathbf{I}(\mathbf{H}_A, \mathbf{H}_B)\\
=&\mathbf{h}(\mathbf{H}_A) + \mathbf{h}(\mathbf{H}_B) - \mathbf{h}(\mathbf{H}_A, \mathbf{H}_B)\\
=&\log_2\left[\frac{(\pi e)^{M_A*M_B*N}det(\mathbf{R}_{H_A}) * (\pi e)^{M_A*M_B*N}det(\mathbf{R}_{H_B})}{(\pi e)^{2*M_A*M_B*N}det(\mathbf{R}_{H_A,H_B})}\right]\\
=&\log_2\left[\frac{det(\mathbf{R}_H + \sigma_A^2\mathbf{I})det(\mathbf{R}_H + \sigma_B^2\mathbf{I})}{det\left(\begin{bmatrix}\mathbf{R}_H + \sigma_A^2\mathbf{I} & \mathbf{R}_H\\ \mathbf{R}_H & \mathbf{R}_H + \sigma_B^2\mathbf{I}\end{bmatrix}\right)}\right] \qquad (2.3)
\end{aligned}
$$

Where **h** denotes the differential entropy, *det* means the determinant.

2.2 System Setup

The system model, shown in Fig. 2.1, consists of three nodes, Alice, Bob, and Eve, and three wireless MIMO channels: $\mathbf{H}^{AB}$, $\mathbf{H}^{AE}$, and $\mathbf{H}^{BE}$. The source node, Alice, wants to transmit confidential messages to the destination node, Bob, through $\mathbf{H}^{AB}$.

Due to the broadcast nature of wireless channels, these messages will be overheard by the eavesdropper, Eve, through $\mathbf{H}^{AE}$. If Bob transmits some signals to Alice, those signals will also be overheard by Eve through $\mathbf{H}^{BE}$. The communications among each terminals are based on MIMO-OFDM structure. It is assumed that the system uses time-division duplexing (TDD) and channel reciprocity holds. The channel between Alice and Bob is therefore symmetric. It is noted that the MIMO channel reciprocity holds in the transpose form, i.e. , $\mathbf{H}^{AB} = (\mathbf{H}^{BA})^T$. The location of Eve is **not** restricted. Alice, Bob and Eve are assumed to equipped with $\mathbf{M}_A$, $\mathbf{M}_B$ and $\mathbf{M}_E$ multiple antennas.

The universal codebooks containing precoding matrices and corresponding PMI's are available to Alice, Bob, and Eve. Both Alice and Bob use the MIMO channel capacity function for PMI estimation and is known by Eve. The whole protocols used by Alice and Bob are known by Eve, too. Eve is assumed to be a passive attacker who will not jam the channel and falsify the public discussion between Alice and Bob. In this paper, for a matrix $\mathbf{A}$, $\mathbf{A}^\dagger$ denotes the hermitian of $\mathbf{A}$. $\mathbf{A}'$ denotes the conjugate of $\mathbf{A}$, and $\mathbf{A}^T$ denotes the transpose of $\mathbf{A}$.

Chapter 3

Basic P-MOPI Scheme

In this section, the basic P-MOPI scheme is proposed. Basic P-MOPI scheme simply describes that how to obtain secret keys from a MIMO-OFDM channel via PMI estimation. The signalling procedure of the basic P-MOPI scheme are depicted in Fig.3.1

3.1 Basic P-MOPI Scheme

In a typical MIMO system with codebook-based precoding, Alice acquires the PMI via the feedback from Bob. Eve can easily detect the PMI through eavesdropping. But what if the PMI is not fed back to Alice, and instead, Bob sends the same reference signal to Alice? Under the assumption of channel reciprocity ($\mathbf{H}^{AB} = (\mathbf{H}^{BA})^T$) , Alice is able to compute the PMI that is the same as Bob's. At Eve's side, without the feedback, she is unable to figure out the PMI if the channel $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$ is independent from $\mathbf{H}^{AB}$ (and $\mathbf{H}^{BA}$). Now the PMI, only shared between Alice and Bob, can be used as a secret key. We know that the estimated precoding matrix has the minimum *chordal distance* from the optimal precoding matrix. The optimal precoding matrix spans the same space as the space spanned by right singular vectors of the channel matrix. Therefore, the estimated precoding matrix can be regarded as a quantized version of space spanned by the right singular vectors. To extract more secrecy from the channel matrix, the transposed channel matrix is also used in P-MOPI for PMI estimation to utilize the left singular vectors. Twice secret keys can

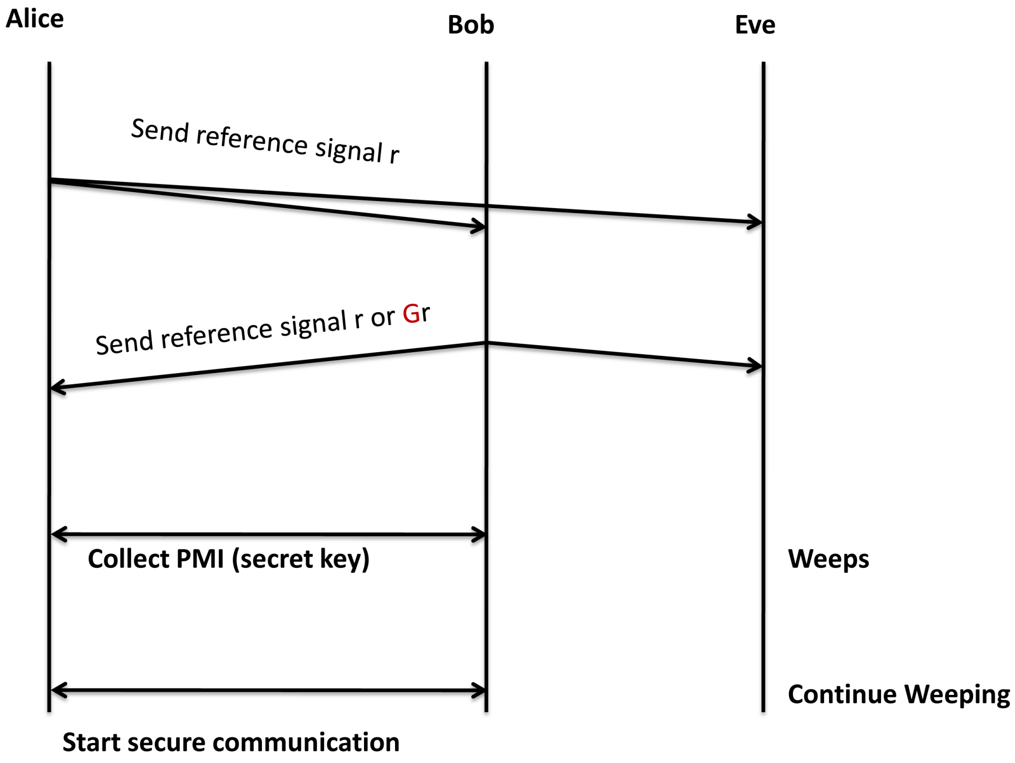


Figure 3.1: Signalling Procedure of Basic P-MOPI

be achieved with the utilization of original channel and the transposed channel.

It is noted that a well-designed codebook (e.g. DFT codebook [37]) can be easily extended to different size according to the requirement. This means that the codebook size in the P-MOPI can be adaptively adjusted with the instantaneous condition, thus providing excellent flexibilities. To fully utilize channel information on each subcarrier, the correlated estimated channel in the same subband are averaged. The channel averaging method is similar to [23]. While [23] aims at temporally and spatially correlated channel, P-MOPI utilizes this method on the correlated channels in frequency domain. If the channel estimation errors on each subcarrier are independent, the variance of the error can be reduced by the number of the correlated channels in one subband. The steps of the basic P-MOPI scheme are detailed as follows.

1. Alice transmits a reference signal $\mathbf{r} \in \mathbb{C}^{\mathbf{M}_A \times \mathbf{N}_r}$ to Bob to let Bob make channel estimation. $\mathbf{N}_r$ is the length of the reference signal.

2. Bob estimates the channel on a single subcarrier or a subband (which consists of several subcarriers depending on the channel coherence bandwidth or precoding granularity). Different channel realizations $\mathbf{H}_k^{AB} \in \mathbb{C}^{\mathbf{M}_B \times \mathbf{M}_A}$ is acquired for the k_{th} subcarrier at Bob's side.

3. Bob computes the averaged channel $\mathbf{H}^{AB} = \frac{1}{n}\sum_{k=1}^{n} \mathbf{H}_k^{AB}$ for the subband consists of n subcarriers.

4. Bob conducts the corresponding precoding matrix $\hat{\mathbf{F}}_{\text{Bob,Right}} = \underset{\mathbf{F}}{\operatorname{argmax}}\, \mathcal{C}_{\mathbf{H}^{AB},\mathbf{F}} (\in \mathbb{C}^{\mathbf{M}_A \times \mathbf{n}_s})$. $\mathbf{n}_s$ is normally the number of transmitted data stream which can be controlled by the nodes. He regards the PMI $i_{\text{Bob,Right}}$ of the precoding matrix $\hat{\mathbf{F}}_{\text{Bob,Right}}$ as a key and put it into his key set $\mathcal{K}_{\text{Bob}}$.

5. Bob does the same step above, but using $(\mathbf{H}^{AB})^T$ instead of $\mathbf{H}^{AB}$. He collects the PMI $i_{\text{Bob,Left}}$ by finding $\hat{\mathbf{F}}_{\text{Bob,Left}} = \underset{\mathbf{F}}{\operatorname{argmax}}\, \mathcal{C}_{(\mathbf{H}^{AB})^T,\mathbf{F}} (\in \mathbb{C}^{\mathbf{M}_B \times \mathbf{n}_s})$ and puts it into $\mathcal{K}_{\text{Bob}}$, too. Note here the used codebook might be changed according to the required rank.

6. During the next time slot, Bob sends a sounding reference signal to Alice. Alice acquires the corresponding precoding matrices $\hat{\mathbf{F}}_{\text{Alice,Right}}$ and $\hat{\mathbf{F}}_{\text{Alice,Left}}$ from $\mathbf{H}^{BA}$ and $(\mathbf{H}^{BA})^T$ for the subband. Alice then puts $i_{\text{Alice,Left}}$ and $i_{\text{Alice,Right}}$ into its key set $\mathcal{K}_{\text{Alice}}$.

7. The step 3 to 6 is performed for all subbands among the OFDM system. Since the channel reciprocity holds, we have $\mathbf{H}^{BA} = (\mathbf{H}^{AB})^T$. $\hat{\mathbf{F}}_{\text{Bob,Right}}$ and $\hat{\mathbf{F}}_{\text{Alice,Left}}$ are the same, and so are $\hat{\mathbf{F}}_{\text{Bob,Left}}$ and $\hat{\mathbf{F}}_{\text{Alice,Right}}$. As a result, $\mathcal{K}_{\text{Bob}}$ and $\mathcal{K}_{\text{Alice}}$ are identical.

8. Alice and Bob may drop out-of-date keys to make sure $\mathcal{K}_{\text{Bob}} = \mathcal{K}_{\text{Alice}}$ at any time.

9. Alice uses a stream cipher to encrypt data X with the key set $\mathcal{K}_{\text{Alice}}$, along with the SHA-256 digest of X in *plaintext*. Afterwards, Alice transmits the encrypted data to Bob and Bob decrypts the data using its own key set $\mathcal{K}_{\text{Bob}}$. Bob calculates the SHA-256 digest of decrypted data, checks to see if it matches the received digest. A key agreement error is declared if there is a mismatch. During the transmission, MIMO precoding is applied in order to achieve better MIMO performance.

3.2 Security Discussion and the Risk Concern of Basic P-MOPI Scheme

The security of the reciprocity-based secret key generation schemes is established by the wireless environments. Secrecy extraction from PMI also falls into this category. The distance of the eavesdropper from the legitimate nodes decides the security level. Under general assumption, the distance of several wavelength provides nearly independent channel. For MIMO case, Eve experiences an even difficult situation. The antenna arrangement and the movement direction of Alice and Bob has dramatic impact on the MIMO channel between them.

Nevertheless, we observe some risks threaten the feasibility and security of basic P-MOPI scheme and other reciprocity-based key generation schemes. The first risk comes from the equation (1.4). If the MIMO channel has no correlation between each element, it can be expected that the quantized keys will be distributed uniformly. However, under real channel which exists the channel correlation. The estimated keys may concentrate on certain bits, which decreases the security. This is the common risk of the reciprocity-based security scheme. [22,23] tries to smooth the keys uniformly by using the decorrelation vector. Yet, It is shown that the key disagreement probability is very high due to the estimation error if Alice and Bob estimate the decorrelation vector independently. If the decorrelation vector is estimated by one node and transmitted to other nodes with no error, the extremely large communication overhead is needed.

The second risk comes from the annoying estimation error during channel estimation. In some situation, error is not a problem. But if the wireless channel, unfortunately, is located on the boundary of two different quantization regions. It is obvious Alice and Bob will easily estimate the biased keys and fail to achieve secret key agreement. It is noted that the steps of information reconciliation and privacy amplification, utilizing channel coding and universal hash function, can reduce the error rate of PMI estimation. The steps of information reconciliation and privacy amplification use error correction codes (e.g. LDPC codes [15] and coset assignment [21]) and universal hash function. For specific operation on information reconciliation and privacy amplification, one can refer to [18]. Additional public transmission is required and therefore increases the complexity and feedback overhead on both terminals.

The third risk is the physical nature of the wireless channel. If the eavesdropper obtains the complete knowledge of the full wireless environments, the wireless channel between two nodes can be fully recovered. This feature inspires [28] to propose an attack method. The attack method uses both the channels $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$ to reconstruct the reflectors surroundings by the geometric methods. The simulation results shows that under simple wireless environments, Eve has the possibility to recover similar channel of $\mathbf{H}^{AB}$. This risk reminds us to notice the usage of the normal pilot signals.

The last risk, the bottleneck of all key generation scheme using wireless channel, is the nearby malicious user. The security of basic P-MOPI and other PHY secret key generation scheme are all based on the spatial separation of legitimate nodes and eavesdropper. If the wireless channel experienced by Eve is similar to that estimated by Alice and Bob, the security will be easily broken. These risks prickle us to seek for further solution to reduce them.

Chapter 4

Enhanced P-MOPI Scheme

4.1 Idea Description

As mentioned above, there exist some risks which threaten the basic P-MOPI scheme. Therefore, we propose a revised version – Enhanced P-MOPI secret key generation scheme. The enhanced P-MOPI scheme is inspired by the idea of rotated reference signals in the former MOPI Scheme [8]. Recall in [8], the rotated reference signals is to create the artificial fast-varying channel. In this paper, this concept is utilized as an effective method to reduce the risks which harms the security and feasibility. With the proper design of rotation matrix, both Alice and Bob are able to control the PMI estimated by others. This provides several advantages for enhanced P-MOPI to overcome the risks in basic P-MOPI.

First, since the legitimate nodes have the ability to control the PMI (and the key), uniformly distributed secret keys are easily achieved by generating pseudo-random secret keys in advance. After that, Alice and Bob control the PMI to match the pseudo-random sequence. Therefore non-uniform secret keys are avoided. It is noted that with the unitary rotation, it is not possible to control the keys if we use direct channel quantization which quantizes the whole channel matrix. The unitary rotation only has impact on the singular vectors, so it changes the optimal precoding matrix alone. This is why PMI-based quantization is proposed for its harmony with the unitary-rotated reference signals.

Second, with the rotation matrix, the instantaneous channel experienced by the nodes can be transformed into an ”optimal” channel for the universal codebook . Alice and Bob control the optimal precoding matrix of the rotated channel to make it exactly a precoding matrix in the codebook. The rotated channel will have further distance from the decision boundary. The perturbation of estimation error can be minimized. Moreover, we can apply channel coding to the pseudo-random keys before we transmit the reference signal. The step of applying channel coding by the rotated reference signal has some advantages over the traditional steps of information reconciliation and privacy amplification. Since the usage of the channel coding is embedded in the procedure of channel estimation, additional public communication is no longer needed. This reduce the transmission overhead and the complexity of using universal hash function. It is noted that the transmission of reference signal is also another kind of public discussion. It is proven that public discussion is necessary in the secret key generation [38].

The attack method proposed in [28] is also prevented. The reference signals is multiplied by the rotation matrix. Thus the eavesdropper loses its ability to acquire both $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$ simultaneously. Instead, Eve received the rotated version. Without knowing these two channels correctly, Eve is unable to reconstruct the complete wireless physical surroundings. The attack method is no longer valid to break the security of P-MOPI scheme. The last risk avoided is the nearby malicious user problem. The rotation of the reference signal successfully retard the eavesdropper from acquiring complete secret key information. Because of the rotation, the eavesdropper is forced to lose track of half information of secret key. The detailed discussion will be addressed in the following description. The anxiety caused by the annoying risks in basic P-MOPI and other reciprocity-based schemes are all released by the rotated reference signal in enhanced P-MOPI. It is noticed that with the rotated reference signals, our design still guarantees the same MIMO precoding gain as before. Both security and MIMO gain are achieved with the proposed P-MOPI scheme.

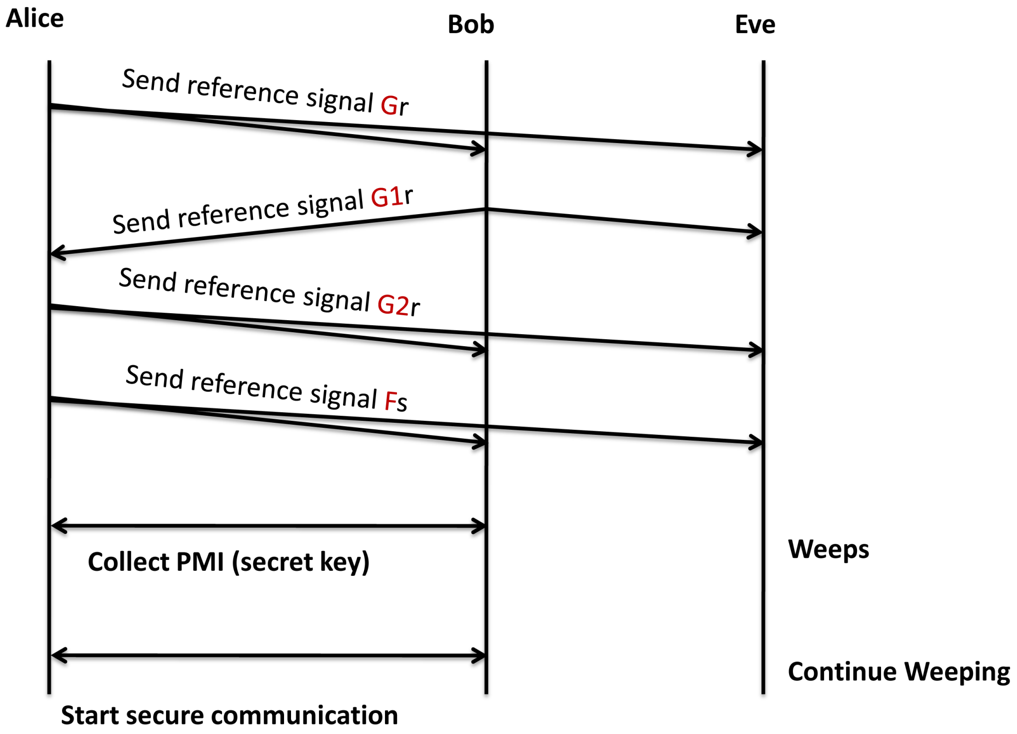


Figure 4.1: Signalling Procedure of Enhanced P-MOPI

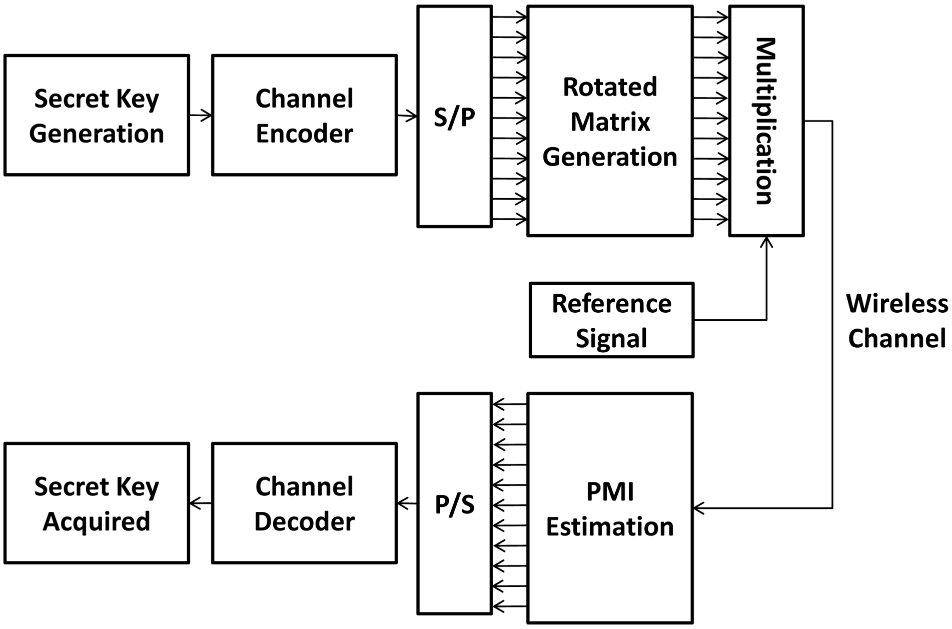


Figure 4.2: Block Diagram of Enhanced P-MOPI

4.2 Enhanced P-MOPI Scheme

The following descriptopn will show how enhanced P-MOPI works. The signalling procedure of enhanced P-MOPI is depicted in Fig. 4.1 while the block diagram of enhanced P-MOPI is shown in Fig. 4.2.

1. Alice transmits the reference signal $\mathbf{Gr}$ to Bob to let Bob make channel estimation. $\mathbf{G}$ is a random complex unitary matrix ($\in \mathbb{C}^{\mathbf{M}_A \times \mathbf{M}_A}$) and independent for each subband. Bob estimates the averaged channel $\mathbf{H}_i^{AB}\mathbf{G}_i$ for the subband i. After the estimation, Bob decomposes $\mathbf{H}_i^{AB}\mathbf{G}_i$ by SVD and obtains $\mathbf{H}_i^{AB}\mathbf{G}_i = \mathbf{U}_{B,i}\mathbf{\Sigma}_i(\mathbf{V}_{B,i}^{\dagger}\mathbf{G}_i)$, where $\mathbf{U}_{B,i} \in \mathbb{C}^{\mathbf{M}_B \times \mathbf{M}_B}$ and $\mathbf{V}_{B,i}^{\dagger} \in \mathbb{C}^{\mathbf{M}_A \times \mathbf{M}_A}$ are unitary matrices and $\Sigma_i \in \mathbb{C}^{\mathbf{M}_B \times \mathbf{M}_A}$ is a diagonal matrix.

2. According the required secret key length, Bob generates an n-bit random secret key sequence $\mathbf{S}_B$ and puts it into $\mathcal{K}_{\text{Bob}}$. Based on the instantaneous situation, Bob can optionally apply channel coding on $\mathbf{S}_B$ and gets coded key sequence $\mathbf{C}_B$.

3. If a p-bit codebook is used, Bob divides $\mathbf{C}_B$ into $\left\lceil \frac{n}{p} \right\rceil$ groups of p-bit sequences. Each p-bit sequence is then denoted by $\mathbf{C}_{B,i}$ separately.

4. For the subband i, Bob finds the corresponding precoding matrix $\mathbf{F_{B,i}}$ which has index equals to $\mathbf{C}_{B,i}$. It is noted that precoding matrix used here is usually *tall* matrix which is not full-rank. Bob appends some random orthogonal columns to the original precoding matrix and makes it a full-rank unitary matrix $\tilde{\mathbf{F}}_{B,i} \in \mathbb{C}^{\mathbf{M}_B \times \mathbf{M}_B}$.

5. Bob transmits the rotated reference signal $\mathbf{G}_{1,i}\mathbf{r}$ to Alice, where $\mathbf{G}_{1,i} = \mathbf{U}'_{B,i}\tilde{\mathbf{F}}^{\dagger}_{B,i}$. Alice estimates PMI for the rotated averaged channel $\mathbf{H}_i^{BA}\mathbf{G}_{1,i}$ for the subband i.

6. Step 2-6 is done repeatedly among all subbands. After collecting PMI for all subbands, Alice combines all PMI to form the secret key $\mathbf{S}_B$. If channel coding

is applied, Alice decodes the coded key sequence and gets the secret key.

7. Alice generates another secret key sequence $\mathbf{S}_A$ and optionally encodes it to $\mathbf{C}_A$. Separation is applied on $\mathbf{C}_A$ by Alice to make it into several p-bit sequences. The sequences are denoted by $\mathbf{C}_{A,i}$.

8. For each subband i, Alice first searches the precoding matrix $\mathbf{F_{A,i}}$ which related to $\mathbf{C}_{A,i}$ and refines it to full-rank unitary matrix $\tilde{\mathbf{F}}_{A,i} \in \mathbb{C}^{\mathbf{M}_A \times \mathbf{M}_A}$ with some random orthogonal columns.

9. Alice computes SVD on $\mathbf{H}_i^{BA}\mathbf{G}_{1,i} = (H_i^{AB})^T\mathbf{G}_{1,i}$ and obtains $(H_i^{AB})^T\mathbf{G}_{1,i} = \mathbf{V'}_{A,i}\mathbf{\Sigma}_i^T(\mathbf{U}_{A,i}^T\mathbf{G}_{1,i})$. Alice is able to acquire the singular vectors $\mathbf{V}_{A,i}$. Then Alice transmits the rotated reference signal $\mathbf{G}_{2,i}\mathbf{r}$ to Bob, where $\mathbf{G}_{2,i} = \mathbf{V}_{A,i}\tilde{\mathbf{F}}^\dagger_{A,i}$.

10. Bob makes PMI estimation on rotated channel $\mathbf{H}_i^{AB}\mathbf{G}_{2,i}$. Same steps is applied among all subbands to get the secret key $\mathbf{S_A}$.

11. To achieve MIMO capacity, Alice finds the optimal MIMO precoding matrix from the codebook by $\hat{\mathbf{F}} = \underset{\mathbf{F}}{\operatorname{argmax}}\, \mathcal{C}_{(\mathbf{H}^{AB})^T\mathbf{G}_1,\mathbf{F}}(\in \mathbb{C}^{\mathbf{M}_B \times \mathbf{n}_s})$. Alice generates an random unitary matrix $\mathbf{R} \in \mathbb{C}^{\mathbf{n}_s \times \mathbf{n_s}}$. She makes $\tilde{\mathbf{F}} = \hat{\mathbf{F}}\mathbf{R}$ and uses $\tilde{\mathbf{F}}$ as the MIMO precoding matrix.

12. Alice transmits another rotated reference signal $\tilde{\mathbf{F}}\mathbf{s}$ where $\mathbf{s} \in \mathbb{C}^{\mathbf{n}_s \times \mathbf{N}_s}$ has different length $\mathbf{N}_s$ compared to $\mathbf{r}$.

13. Bob estimates the precoded channel $\mathbf{H}^{AB}\tilde{\mathbf{F}}$. With the help of the estimation results, ZF or MMSE receiver can be utilized by Bob to receive the precoded data.

14. After the above steps, both Alice and Bob acquire $\mathbf{S_A}$ and $\mathbf{S_B}$. Secure transmission can be achieved similar to the basic P-MOPI. The MIMO capacity gain is also fully utilized by the communication parties.

In order to recover the secret key, Alice and Bob should make correct PMI estimation. Here we show how they can achieve the secret key agreement easily and efficiently. To recover secret key $\mathbf{S}_B$ generated by Bob. Alice estimates precoding matrix for the rotated channel $\mathbf{H}_i^{BA}\mathbf{G}_{1,i}$ by

$$\hat{\mathbf{F}} = \underset{\mathbf{F}\in\mathcal{F}}{\operatorname{argmax}}\, \mathcal{C}_{\mathbf{H}_i^{BA}\mathbf{G}_{1,i},\mathbf{F}} \tag{4.1}$$

Is is well-known that the optimal precoding matrix which achieves the maximum capacity is the right singular vectors of the estimated channel. After the singular value decomposition, the rotated channel $\mathbf{H}_i^{BA}\mathbf{G}_{1,i}$ can be decomposed by

$$\begin{aligned}\mathbf{H}_i^{BA}\mathbf{G}_{1,i} &= (\mathbf{H}_i^{AB})^T\mathbf{G}_{1,i}\\ &= (\mathbf{U}_{B,i}\mathbf{\Sigma}_i\mathbf{V}_{B,i}^{\dagger})^T\mathbf{U}'_{B,i}\tilde{\mathbf{F}}_{B,i}^{\dagger}\\ &= \mathbf{V}'_{B,i}\mathbf{\Sigma}_i^T\mathbf{U}_{B,i}^T\mathbf{U}'_{B,i}\tilde{\mathbf{F}}_{B,i}^{\dagger}\\ &= \mathbf{V}'_{B,i}\mathbf{\Sigma}_i^T\tilde{\mathbf{F}}_{B,i}^{\dagger} \end{aligned} \tag{4.2}$$

Therefore, the optimal precoding vectors are exactly $\mathbf{F_{B,i}}$. It is noted that the SVD decomposition is not unique so $\mathbf{U}_{B,i}$ is not unique. However, the different decompositions will span the same space. Therefore, the optimal precoding vectors still spans the same space as $\mathbf{F_{B,i}}$ does. And the corresponding PMIs are all equal to $\mathbf{S}_{B,i}$ or $\mathbf{C}_{B,i}$. With this optimality, robust noise resistance is expected. At Bob's side, Bob estimates PMI from the rotated channel $\mathbf{H}_i^{AB}\mathbf{G}_{2,i}$ to obtain $\mathbf{S}_A$ generated from Alice. The rotated channel can be decomposed by

$$\begin{aligned}\mathbf{H}_i^{AB}\mathbf{G}_{2,i} &= \mathbf{U}_{A,i}\mathbf{\Sigma}_i\mathbf{V}_{A,i}^{\dagger}\mathbf{V}_{A,i}\tilde{\mathbf{F}}_{A,i}^{\dagger}\\ &= \mathbf{U}_{A,i}\mathbf{\Sigma}_i\tilde{\mathbf{F}}_{A,i}^{\dagger} \end{aligned} \tag{4.3}$$

As a result, the optimal precoding matrix for $\mathbf{H}_i^{AB}\mathbf{G}_{2,i}$ is $\mathbf{F_{A,i}}$ or the unitary matrices span the same space. The corresponding PMI is $\mathbf{S}_{A,i}$. Alice and Bob are capable of acquiring the identical secret key.

In our design, we use $\tilde{\mathbf{F}}$ for MIMO precoding instead of the codebook's element $\hat{\mathbf{F}}$. However, the same MIMO capacity is achieved [36]. This design can prevent eavesdropper acquire the channel information $\mathbf{H}^{AE}$ and will be detailed later. Although the reference signals are always rotated, Bob is still able to receive the precoded data symbols. As in [39], both the ZF and the MMSE receiver can receive the precoded symbols correctly with the precoded channel information $\mathbf{H}^{AB}\tilde{\mathbf{F}}$. The detailed information about MIMO precoding system structure can be referenced in [30].

4.3 Security Discussion for Enhanced P-MOPI Scheme

Enhanced P-MOPI scheme seems to be a promising way to maintain confidential transmission in the wireless environments and solve many problems on PHY secrecy extration. However, the detailed inspection on the enhanced P-MOPI scheme is essential to assure its security. In this section, we will show how the normal eavesdropper and, especially, the nearby eavesdropper are retarded under enhanced P-MOPI scheme.

To obtain the complete secret key information, it seems that the information of $\mathbf{H}^{AB}$ is not enough. $\mathbf{H}^{BA}\mathbf{G}_1$ and $\mathbf{H}^{AB}\mathbf{G}_2$ are necessary for Eve to get $\mathbf{S}_A$ and $\mathbf{S}_B$. From Fig. 4.1, we can see that the total information obtained by Eve are $\mathbf{H}^{AE}\mathbf{G}$, $\mathbf{H}^{BE}\mathbf{G}_1$, $\mathbf{H}^{AE}\mathbf{G}_2$ and $\mathbf{H}^{AE}\tilde{\mathbf{F}}$. If Eve is far away from the legitimate nodes, $\mathbf{H}^{AE}\mathbf{G}_2$ and $\mathbf{H}^{BE}\mathbf{G}_1$ will be nearly independent of $\mathbf{H}^{BA}\mathbf{G}_1$ and $\mathbf{H}^{AB}\mathbf{G}_2$. Eve is unable to acquire any information about key. But how's the things going when Eve comes near Alice or Bob? It happens that $\mathbf{H}^{BE} \approx \mathbf{H}^{BA}$ when Eve is close to Alice. With receiving the rotated reference signal from Bob, she has $\mathbf{H}^{BE}\mathbf{G}_1 \approx \mathbf{H}^{BA}\mathbf{G}_1$. Therefore, Eve has the information of the secret key $\mathbf{S}_B$ by PMI estimation on $\mathbf{H}^{BA}\mathbf{G}_1$. She can also learn the information about right singular vectors $\mathbf{V}$ by applying SVD on $\mathbf{H}^{BA}\mathbf{G}_1$. It is obvious that Eve can obtain the secret key $\mathbf{S}_A$ if she has access to $\mathbf{G}_2$ for $\mathbf{G}_2 = \mathbf{V}\tilde{\mathbf{F}}_A^\dagger$. However, she only knows $\mathbf{H}^{AE}\mathbf{G}$, $\mathbf{H}^{AE}\mathbf{G}_2$ and $\mathbf{H}^{AE}\tilde{\mathbf{F}}$, and $\mathbf{H}^{AE}$ is not observable for her. Eve will found herself unconscious of $\mathbf{G}_2$. As a result, when Eve comes close to

Eve's Position	Acquired information
Arbitrarily	$\mathbf{H}^{AE}\mathbf{G}, \mathbf{H}^{BE}\mathbf{G}_1, \mathbf{H}^{AE}\mathbf{G}_2, \mathbf{H}^{AE}\tilde{\mathbf{F}}$
Near Alice	$\mathbf{H}^{AE}\mathbf{G}, \mathbf{H}^{BA}\mathbf{G}_1, \mathbf{H}^{AE}\mathbf{G}_2, \mathbf{H}^{AE}\tilde{\mathbf{F}}$
Near Bob	$\mathbf{H}^{AB}\mathbf{G}, \mathbf{H}^{BE}\mathbf{G}_1, \mathbf{H}^{AB}\mathbf{G}_2, \mathbf{H}^{AB}\tilde{\mathbf{F}}$

Table 4.1: Information Acquired by Eve under Enhanced P-MOPI

Alice, she can only acquire $\mathbf{S}_B$ but lose track of the information about $\mathbf{S}_A$.

On the other hand, we consider the situation where Eve stays near Bob. Eve finds the estimated channel $\mathbf{H}^{AE}\mathbf{G}$ and $\mathbf{H}^{AE}\mathbf{G}_2$ are similar to $\mathbf{H}^{AB}\mathbf{G}$ and $\mathbf{H}^{AB}\mathbf{G}_2$. The secret key information $\mathbf{S}_A$ is obtained from PMI estimation on $\mathbf{H}^{AB}\mathbf{G}_2$. The left singular vectors $\mathbf{U}$ is also obtainable from SVD. Nevertheless, Eve fails to decodes the secret key $\mathbf{S}_B$. The reason is that she only has the information $\mathbf{H}^{BE}\mathbf{G}_1$. Because $\mathbf{H}^{BE}$ is unknown for Eve, she is impotent to obtain $\mathbf{S}_B$ from $\mathbf{G}_1$. Table. 4.1 lists the information that Eve can access under different situation. To sum up, consider the situation where Eve wants to gain secret key information by following closely to Alice and Bob. With appropriate operation of enhanced P-MOPI, it is helpless for Eve to obtain the complete secret key information. It should be pointed out that Eve can still have about half of secret key information and the security level is therefore decreased by half. Yet, with the author's best knowledge, there's no previous work deal with the security problem aroused by the nearby malicious user. The proposed enhanced P-MOPI scheme is a pioneer work which successfully retards the threaten from the nearby eavesdropper. Another merit of enhanced P-MOPI is that both Alice and Bob don't need to know the existence and the distance of Eve. The secure transmission is achieved easily among legitimate nodes with just a little additional complexity.

Chapter 5

C-MOPI Scheme

5.1 Idea Description

In P-MOPI, we only use the space spanned by singular vectors as the medium to carry the secret key information. Inspired by the traditional reciprocity-based key generation scheme, it is worth investigating the efficiency of using the whole channel matrix to carry the secret key information. In this section, we propose the channel-based MOPI (C-MOPI) scheme to examine the feasibility of extract secrecy by direct channel quantization. Notice that in order to prevent eavesdropper from learning $\mathbf{H}^{AB}$ by both $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$, either one of the reference signal transmitted by Alice or Bob should be rotated. To hide the secret information in the rotated reference signal, the rotation matrix $\mathbf{G}$ is designed as $(\mathbf{H}^{AB})^{-1}\mathbf{K}$. $\mathbf{K}$ is the secret key matrix having the secret key information inside. The real part and imaginary part of each channel element of $\mathbf{K}$ have the format $\mathbf{F}^{-1}((\mathbf{S}+0.5)/\mathbf{N})$. $\mathbf{F}$ is the cumulative density function (CDF) of gaussian distribution. $\mathbf{S}$ denotes the decimal value of the secret bits and $\mathbf{N}$ is the quantized level for each part. At the receiving side, receiver simply quantizes the received channel elements as gaussian distribution and gets the secrecy bits. For detail information of secrecy extraction from gaussian source, one can reference [15].

Unlike P-MOPI, C-MOPI cannot rotate both reference signals or the MIMO precoding will not be valid. It is because the rotation in P-MOPI only rotates the space spanned by the one-side singular vectors. The space spanned by the other side singular vectors is not affected. Yet, the rotation in C-MOPI destroys the whole channel matrix and PMI estimation is no longer effective. The detailed steps of C-MOPI scheme is as follows and depicted in Fig.5.1.

1. Alice transmits the reference signal $\mathbf{r}$ to Bob to let Bob make channel estimation $\mathbf{H}^{AB}$.

2. Bob generates secret key sequence $\mathbf{S}_B$ and optionally encodes it to $\mathbf{C}_B$.

3. Bob generates the secrecy matrix $\mathbf{K}$ by hiding the secret key information into the real part and the imaginary part of the channel elements.

4. Bob transmits the rotated reference signal $\mathbf{G}_1\mathbf{r}$ to Alice, where $\mathbf{G}_1 = (\mathbf{H}^{BA})^{-1}\mathbf{K}$. Alice quantizes the channel elements and decodes it into $\mathbf{S}_B$.

5. Bob estimates the optimal precoding matrix and feedbacks the PMI to Alice.

6. After the coherence time, the above steps is repeated but the role of Alice and Bob is exchanged to prevent the nearby eavesdropper.

7. To make Bob receive precoded data symbols correctly, this time Alice transmits another rotated reference signal $\tilde{\mathbf{F}}\mathbf{s}$ like the steps in P-MOPI.

8. The secret key obtained in the two steps are mixed, e.g. linear mapping, and secure transmission is achieved.

To prevent the nearby eavesdropper, Alice and Bob do the steps twice with the role exchanged. For a malicious Eve eavesdropping for the confidential transmission, she will move closely to Alice for it is the only position capable of stealing the secret key information in the first step. Nevertheless, if she wants to acquire secret keys at the second step, Eve is forced to move very quickly to somewhere near Bob in the coherence time. The generated secret keys in these two steps should be mixed to force Eve face the dilemma of moving from Alice to Bob in a very short period.

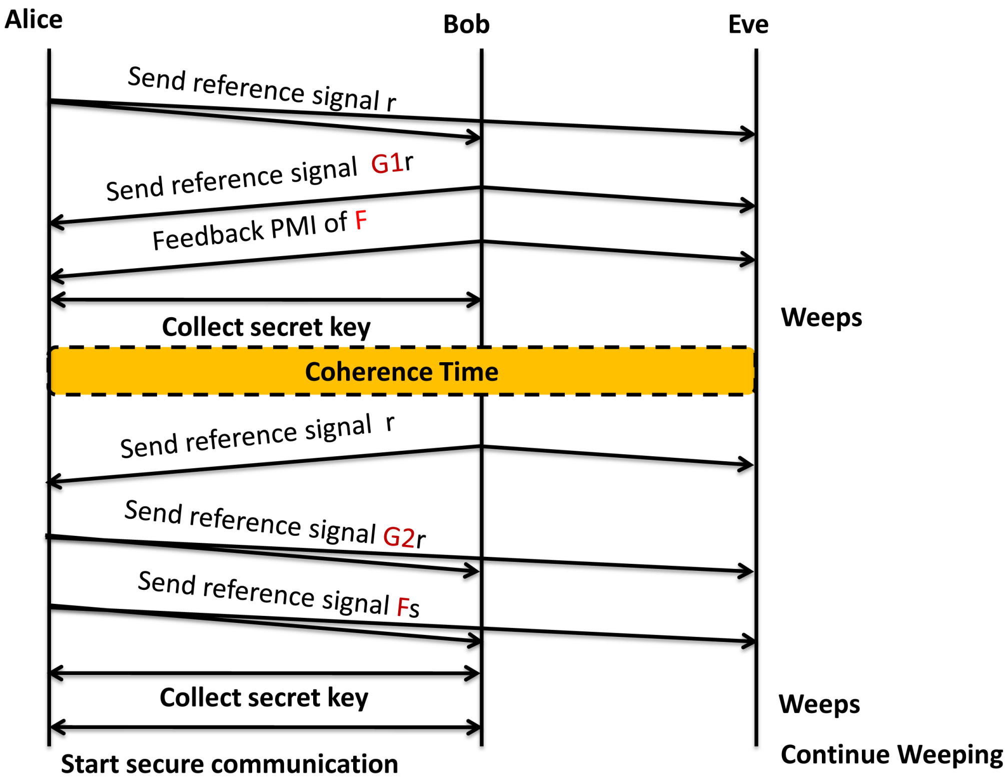


Figure 5.1: Signalling Procedure of Channel-based MOPI

5.2 Limitations on C-MOPI

Although C-MOPI has the chance to extract more secret keys, it has some limitations which restrict its performance. The limitations on C-MOPI consist of the following aspects. The steps in C-MOPI should be done at least twice, this means the users should wait at least the coherence time to make sure the secret key is secure after mixing. On the other hand, $(\mathbf{H}^{AB})^{-1}$ does not exist for non-square matrix. For the situation where Alice and Bob have different number of antennas, some channel elements will be dropped to form a square channel matrix and the secrecy rate is decreased. In addition to the above limitations, it is also noted that the rotation matrix $\mathbf{G}$ in C-MOPI is not unitary, the transmission power of the rotated reference signals is deviated. This adds not only the complexity on the power amplifier of antennas. When $\mathbf{H}^{AB}$ is correlated, $(\mathbf{H}^{BA})^{-1}$ has large power. Therefore, if we assume the channel Bob estimated is $\mathbf{H}^{AB} + \mathbf{Z}_B$, he makes $\mathbf{G} = (\mathbf{H}^{BA} + \mathbf{Z}_B^T)^{-1}\mathbf{K}$. After transmission of rotated reference signals, the channel Alice estimates is

$$\mathbf{H}^{BA}(\mathbf{H}^{BA} + \mathbf{Z}_B^T)^{-1}\mathbf{K} + \mathbf{Z}_A \tag{5.1}$$

$$=(\mathbf{I} - \mathbf{Z}_B^T(\mathbf{H}^{BA} + \mathbf{Z}_B^T)^{-1})\mathbf{K} + \mathbf{Z}_A \tag{5.2}$$

The estimation error $\mathbf{Z}_B$ may be amplified by the large power of the inverse channel. Compared to the P-MOPI scheme, the rotation matrix $\mathbf{G}$ is designed by Bob as $(\mathbf{U}' + \Delta\mathbf{U})\tilde{\mathbf{F}}$. $\Delta\mathbf{U}$ is the singular vector perturbation caused by the channel estimation error. After transmission, the channel estimated by Alice becomes

$$\mathbf{H}^{BA}(\mathbf{U}' + \Delta\mathbf{U})\tilde{\mathbf{F}}^{\dagger} + \mathbf{Z}_A \tag{5.3}$$

$$=\mathbf{V}'\mathbf{\Sigma}^T(\tilde{\mathbf{F}} + \mathbf{U}^T\Delta\mathbf{U}\tilde{\mathbf{F}}^{\dagger}) + \mathbf{Z}_A \tag{5.4}$$

We can see the perturbation power of singular vector is not amplified for $\mathbf{U}^T$ and $\tilde{\mathbf{F}}$ are unitary matrices. As a result, P-MOPI will outperforms C-MOPI when the channel estimation error is not small enough to be omitted. Due to these limitations, although C-MOPI has the chance to carry more secrecy, it is expected that C-MOPI only works well under high SNR scenario and thus has lower flexibility.

Chapter 6

Interleaver-based Secure Transmission (INTERSECT) Scheme

6.1 Overview

In this chapter, we propose the interleaver-based secure transmission scheme which tries to extract secrecy from the relation between channel elements. The order of channel response provides us a nature secret interleaver which can be used to achieve the confidential transmission. The common used interleaver, e.g. block interleaver, in the BICM system is replaced by this secret interleaver. The secret interleaver is introduced to provide security. The communication block diagram of the proposed INTERSECT scheme with BICM system is depicted in Fig.6.1. Our objective is to prevent Eve from obtaining the interleaving pattern to decode the data. It is also necessary to show that Eve is helpless to decrypts the secret messages without the secret interleaver.

In general, in order for Alice and Bob to estimate the channel state information (CSI), Alice transmits reference signals to Bob, and subsequently Bob transmits reference signals to Alice. After estimating the channel, Alice and Bob learn the CSI of $\mathbf{H}^{AB}$. In the meantime, Eve can obtain the CSI of $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$. After channel estimation, the order of the CSI vector can be used as the interleaving patterns. However, as there exists many threats harm the security of proposed P-MOPI and C-MOPI scheme, the INTERSECT scheme also faces several risks. First, we face the risk from

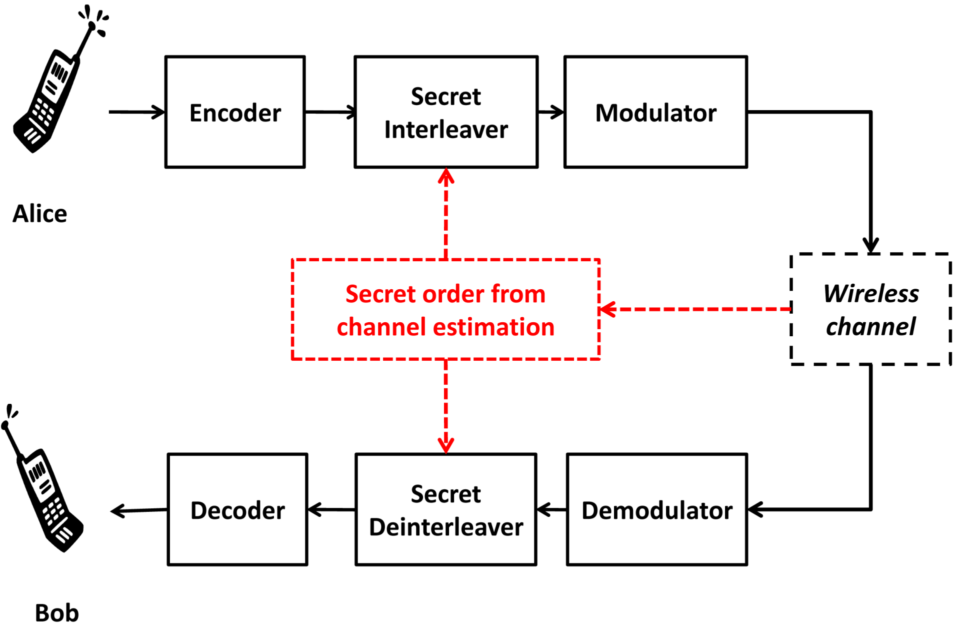


Figure 6.1: Communication Block Diagram of INTERSECT Scheme with BICM System

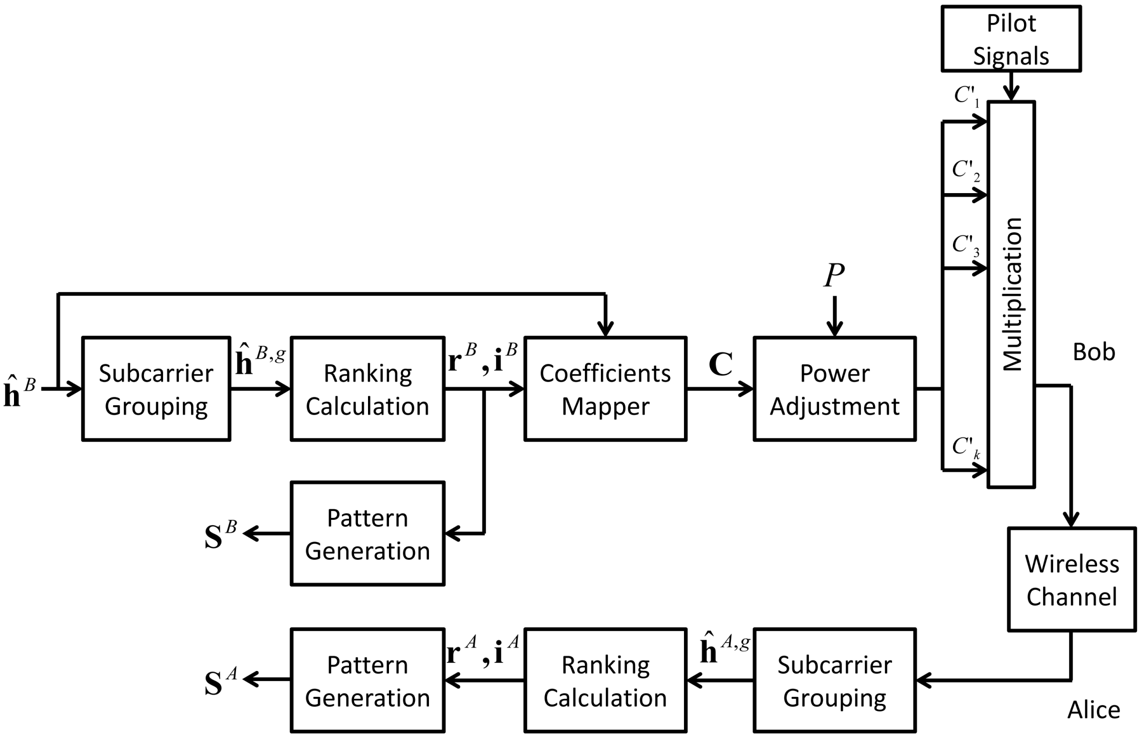


Figure 6.2: Block Diagram of INTERSECT Algorithm

channel correlation upon subcarriers in OFDM system. The neighboring subcarriers share high correlation thus the randomness of the order is decreased. Second, if there are two channel have similar channel response, misorder easily happens. In theory, channel measured by Alice and Bob is the same due to reciprocity. But for the practical application, estimated channel may be similar, but not the same due to noise and channel estimation error.

Similar to the previous proposed P-MOPI scheme and C-MOPI scheme, the reference signals transmitted by Bob is rotated to reduce these risks. First, Alice transmits reference signals to Bob. After estimating the CSI of $\mathbf{H}^{AB}$, Bob sorts the value of $\mathbf{H}^{AB}$, and modifies the value of the reference signals according to the INTERSECT algorithm. Again, Bob transmits the modified reference signals to Alice, and Alice sorts the received signals to obtain the interleaving patterns. Then, both Alice and Bob know the interleaving pattern, whereas the products of modified reference signals and $\mathbf{H}^{AE}$ which Eve receives are out of order. Moreover, to prevent misorder and reduce complexity, we separate subcarriers into several groups. If Bob decides to put thirty subcarriers into one group, he averages every thirty subcarriers firstly, and then sorts the average of all groups to obtain interleaving sequence. Thus, the estimation error ε is reduces to $\varepsilon/30$.

The method mentioned above generates one interleaving sequence at a time. The size of interleaving sequence is constrained by the number of subcarriers. To further improve the system performance, we apply the INTERSECT algorithm to the real part and imaginary part of channels respectively. Both Alice and Bob obtain two interleaving sequences from the order of the real and imaginary part. These two secret sequences can be utilized to form a secret interleaver with larger size. In our work, we also propose a simple method which utilizes the concept of traditional block interleaver to construct the secret interleaver by the two secret sequences.

6.2 Algorithms

The algorithm of INTERSECT scheme is shown in Fig.6.2, and detailed explanations are as follows.

6.2.1 Subcarrier Grouping

At the beginning, Bob selects a desired group size **g**, which is determined by a specific requirement. The average channel $\hat{\mathbf{h}}_g$ is calculated by grouping the estimated channel $\hat{\mathbf{h}}$.

$$\hat{\mathbf{h}}_g^i = \sum_{k=1}^{g} \frac{\mathbf{h}^{g(i-1)+k}}{g} \tag{6.1}$$

where $\mathbf{h}^i$ denotes the channel of ith subcarrier. There are total $\mathbf{m} = \left\lceil \frac{\mathbf{n}}{\mathbf{g}} \right\rceil$ groups and **n** denotes the number of subcarriers in the OFDM system.

6.2.2 Ranking Calculation

Secondly, Bob sorts the real part and the imaginary part of $\hat{\mathbf{h}}_g$ separately. **r** and **i** denotes the ranking of real and imaginary part in decreasing order, respectively. For example, $\mathbf{r}^i$ equals zero when $\hat{\mathbf{h}}_g^i$ is the largest one, and so forth. The range of **r** and **i** is from 0 to $m-1$. It is noted **r** and **i** are two secret sequences and can be used to from larger interleaver with size m^2.

6.2.3 Coefficients Mapper

It has been mentioned that groups with similar channel response easily leads to misorder. In order to enlarge the difference among channels estimated by Alice, Bob introduces a complex sequence **c** with length n. The reference signals are multiplied by this complex sequence to make the estimated channel rotated. **c** is generated with the form

$$\mathbf{c}_k = \frac{(\frac{-\mathbf{m}+\mathbf{1}}{2} + \mathbf{r}^{\lceil \frac{k}{g} \rceil}) + (\frac{-\mathbf{m}+\mathbf{1}}{2} + \mathbf{i}^{\lceil \frac{k}{g} \rceil})\mathbf{j}}{\hat{\mathbf{h}}_k} \tag{6.2}$$

The mean of **c** is made to zero.

6.2.4 Power Adjustment

In practice, power is one of strict criteria that should be considered carefully. In this thesis, we consider the situation that total power is constrained by $\mathbf{P}$. Bob makes a new sequence $\mathbf{c}'$ which is a modified version of $\mathbf{c}$ under the constrained power $\mathbf{P}$. $\mathbf{c}'$ is derived as

$$\begin{aligned} \mathbf{c}'_k &= \mathbf{c}_k \times \sqrt{\frac{P}{\sum_{k=1}^{n} |\mathbf{c}_k|^2}} && (6.3) \\ &= \mathbf{c}_k \times \sqrt{\frac{P}{\mathbf{E}}} && (6.4) \end{aligned}$$

$\mathbf{E}$ denotes $\sum_{k=1}^{n} |\mathbf{c}_k|^2$. Finally, Bob transmits the product of reference signals and the vector of coefficients $\mathbf{c}'$.

6.2.5 Pattern Generation

After channel estimation, both terminals use these two secret sequences $\mathbf{r}$ and $\mathbf{i}$ to generate a new secret order $\mathbf{S}$ for interleaving. In this section, we develop a simple method to generate a size $\mathbf{m}^2$ interleaver $\mathbf{S}$ utilizing the concept of traditional block interleaver. The detailed steps is as follows,

1. A $\mathbf{m} \times \mathbf{m}$ matrix $\mathbf{M}$ is generated with number 1 to $\mathbf{m}^2$ put into the matrix in order from the first row to the last row, i.e. $\mathbf{M}_{a,b} = m(a-1) + (b-1) + 1$.

2. Columns of $\mathbf{M}$ is exchanged by the secret order in the sequence $\mathbf{r}$, i.e. $\mathbf{M}_{a,\mathbf{r}^b+1} = \mathbf{M}_{a,b}$.

3. Rows of $\mathbf{M}$ is exchanged by the sequence $\mathbf{i}$, i.e. $\mathbf{M}_{\mathbf{i}^a+1,b} = \mathbf{M}'_{a,b}$.

4. After that, we read the secret order from the first column to the last column to form the secret interleaver $\mathbf{S}$, i.e. $\mathbf{S}_k = \mathbf{M}_{k \bmod m, \lfloor \frac{k}{m} \rfloor}$.

The concept of pattern generation is similar to traditional block interleaver. However, the exchange of columns and rows are defined by the two secret sequences instead of predefined. This $\mathbf{S}$ is then taken as the interleaving pattern in our scheme.

6.2.6 Receiver

After receiving the signals, Alice calculates the averaged channel using the same subcarrier grouping mentioned above. Deinterleaving patterns $\mathbf{S}'$ is retrieved by ranking and pattern generation as the previous steps. The secure transmission is then achieved with both terminals using the secret interleaver in the BICM system.

6.3 Channel Selection

It is noted that the instantaneous channel is not always suitable for the interleaving pattern generation. Under the situation where there is no channel estimation error, the modified channel estimated by Alice is

$$\mathbf{c}'_k\mathbf{h}_k = [(\frac{-\mathbf{m}+\mathbf{1}}{2} + \mathbf{r}^{\lceil \frac{k}{g} \rceil}) + \mathbf{j} * (\frac{-\mathbf{m}+\mathbf{1}}{2} + \mathbf{i}^{\lceil \frac{k}{g} \rceil})]\sqrt{\frac{\mathbf{P}}{\mathbf{E}}} \tag{6.5}$$

The difference on real part and imaginary part of groups is dominated by $\sqrt{\frac{\mathbf{P}}{\mathbf{E}}}$. It is appeared that channels with large $\mathbf{E}$ happens to be bad channels for it has lower difference and easily leads to misorder. As a result, bad channels should be rejected. In the INTERSECT scheme, we reject channel if channel satisfies the following relation

$$\mathbf{E} > \mu_{\mathbf{E}} + \beta\sigma_{\mathbf{E}} \tag{6.6}$$

Where $\mu_{\mathbf{E}}$ denotes the expectation of $\mathbf{E}$, $\sigma^2_{\mathbf{E}}$ denotes the variance of $\mathbf{E}$. $\mu_{\mathbf{E}}$ and $\sigma^2_{\mathbf{E}}$ can be adaptively updated from the instantaneous channel during the communication procedure using the following formula

$$\begin{cases} \hat{\mu_{\mathbf{E}}} &= (1-\alpha)\mu_{\mathbf{E}} + \alpha\mathbf{E} \\ \hat{\sigma^2_{\mathbf{E}}} &= (1-\alpha)\sigma^2_{\mathbf{E}} + \alpha(\mathbf{E}-\mu_{\mathbf{E}})^2 \end{cases} \tag{6.7}$$

With rejecting the bad channels, the probability of misorder is decreased. With lower β, we can have higher interleaving pattern agreement rate. Yet, rejecting channels continuously keeps the same interleaving pattern used. The security level may be decreased if we use the same interleaving pattern for a long time. Practically, a maximum number of rejecting times should be set. If the channel is rejected continuously and reached the maximum rejecting times, Alice and Bob still use the instantaneous channel to form the secret pattern. As a result, it is no longer better when we set lower β. Optimum β should be chosen according to the required security constraint.

Chapter 7

Performance Evaluation

While using the proposed P-MOPI schemes and C-MOPI scheme for secret key generation, the number of secret keys N generated in *one* OFDM symbol is computed using the following equation:

$$\mathbf{N}_{key} = \frac{\mathbf{B}}{\mathbf{n}}\mathbf{Nc}(1 - KER) \tag{7.1}$$

where **B** denotes the total bandwidth in the OFDM system. **n** denotes the size of a subband, i.e the number of subcarriers of a subband. Total bits generated for the whole channel matrix is **N**. KER is the key error probability. **c** is the code rate of channel coding (equals to 1 if there's no channel coding applied). The generated keys should also satisfy equation (1.4) which means it is uniformly distributed. The efficiency of P-MOPI and C-MOPI can be evaluated by the above equation. In this section, we use computer simulation to show the feasibility of the proposed P-MOPI schemes and C-MOPI scheme.

7.1 Simulation Scenario

To provide convincing simulation results, the realistic simulation setup is considered. We reference the simulation setup generally used in the Long Term Evolution (LTE) [40, 41] to evaluate the performance of P-MOPI schemes and C-MOPI. The detailed simulation parameters are provided in the following tables. The total number of subcarriers used in the simulation is derived by total bandwidth divided by the subcarrier bandwidth, equaling to $\frac{20M}{15k} \approx 1333$. Considering that lower rank precoding

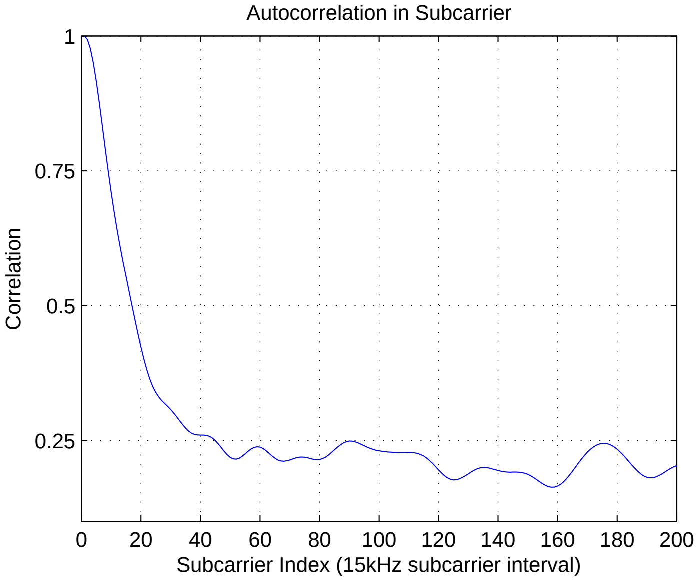


Figure 7.1: Channel correlation among the subcarriers under noiseless Spatial Channel Modeling Extended (SCME) urban-macro channel model.

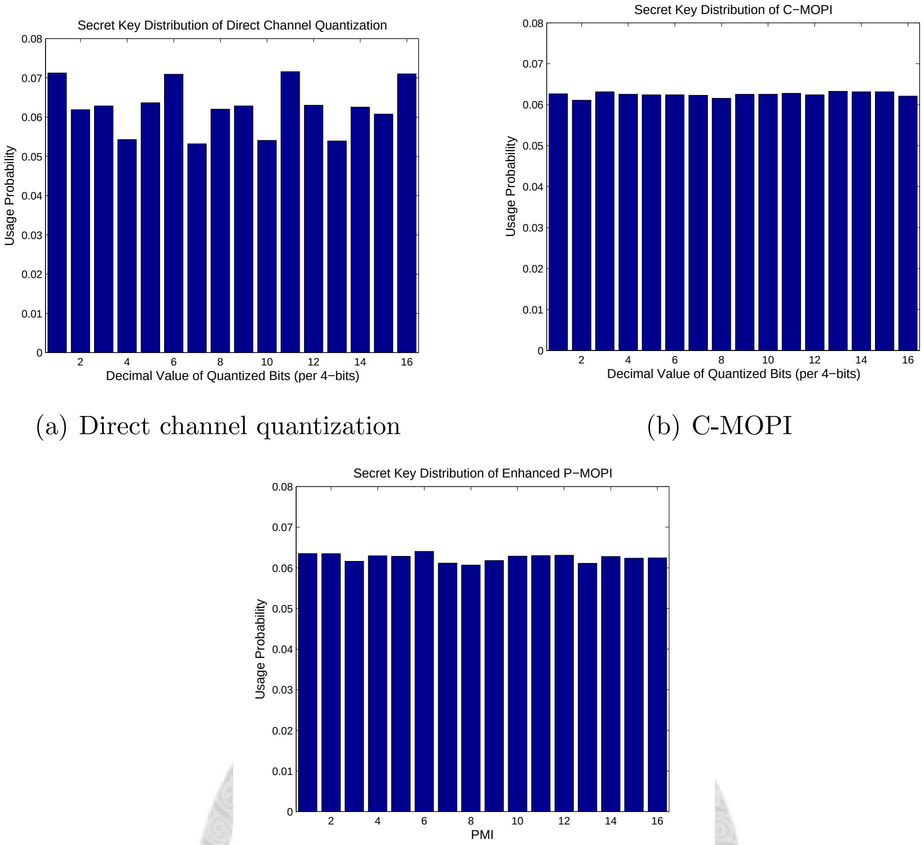
provides more capacity gain compared to higher rank precoding [42], it is expected that using lower rank codebook will has better PMI estimation error resistance. Therefore, rank 1 codebook is used in our simulation to evaluate the performance.

7.2 Performance Evaluation on P-MOPI and C-MOPI Schemes

7.2.1 Subband Size

From equation (7.1), it is clear that subband size dominates the number of generated secret keys. The subband size has its impact in two ways. First, the larger the subband size, the fewer resources we can used in a OFDM symbol for the total system bandwidth is fixed. Yet, it should be noticed that if the subband contains more subcarriers, the estimation error is reduced more for the averaged effective channel. Therefore, smaller subband size is preferred but the larger subband size is not totally a waste.

From the security point of view, the subband size should be at least equal to the channel coherent bandwidth, or Eve can easily break the system from the highly correlated channel. Fig. 7.1 shows the simulation result of the channel correlation among the subcarriers in the SCME urban-macro channel model. In general, a correlation



(a) Direct channel quantization

(b) C-MOPI

(c) Enhanced P-MOPI

Figure 7.2: Secret key distribution of direct channel quantization, enhanced P-MOPI and C-MOPI

below 0.5 can be regarded as nearly uncorrelated. We can see that the correlation decreases to 0.5 at about a 20-subcarrier separation, which shows that the coherence bandwidth of the channel is about $20 \times 15\text{k} = 300$ kHz. With total system bandwidth 20 MHz and subband size 300 kHz, the number of independent PMI's can be acquired is $20\text{M}/300\text{k} \cong 66$ in one time slot. If we use a 2-bit codebook, $2 \times 2 \times 66 = 264$ bits are generated as the cryptography key which easily outperforms the required security level of conventional cipher. As a result, subband size is chosen as 20 subcarriers in our simulation.

7.2.2 Secret Key Distribution

From equation (1.4), a well-defined secret key should be uniformly distributed. For the tradition secrecy extraction from wireless channel, the correlated channel leads to the correlated secret keys and the security level is decreased. The decorrelation methods of using decorrelation vector costs tremendous feedback overhead. This problem is solved by proposed P-MOPI and C-MOPI schemes and is examined in the simulation. Fig. 7.2 depicts the secret key distribution of direct channel quantization (traditional solution), C-MOPI and enhanced P-MOPI. A 4-bit codebook and 2-bit quantization on one channel element are used in the simulation. We separate the secret keys into groups with 4-bit long (equal to PMI in P-MOPI), and observe its decimal value distribution. The secret key distribution is focused on certain value in direct channel quantization due to the correlation in MIMO channel. The delay spread is also constrained in the used SCME channel model and the degree of freedom is limited. Therefore, biased secret key distribution is appeared and the security level is decreased. On the other hand, we can see that the secret key distribution becomes uniform in the C-MOPI and enhanced P-MOPI scheme. The reason is that the secret keys are generated randomly at the terminals and not affected by the instantaneous channel. It means $\mathbf{H}^{AB}$ and secret keys $\mathbf{S}$ are independent. As a result, the uniform secret key distribution is guaranteed in enhanced P-MOPI and C-MOPI scheme.

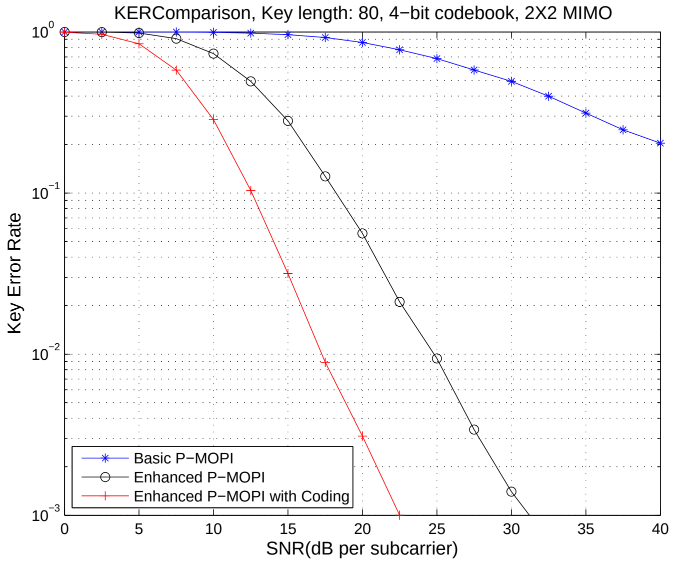


Figure 7.3: Key Error Rate (KER) comparison for the P-MOPI schemes

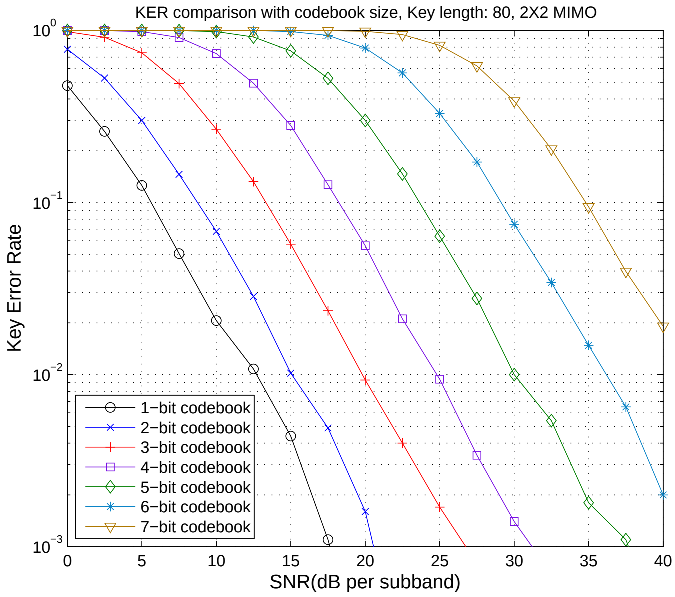
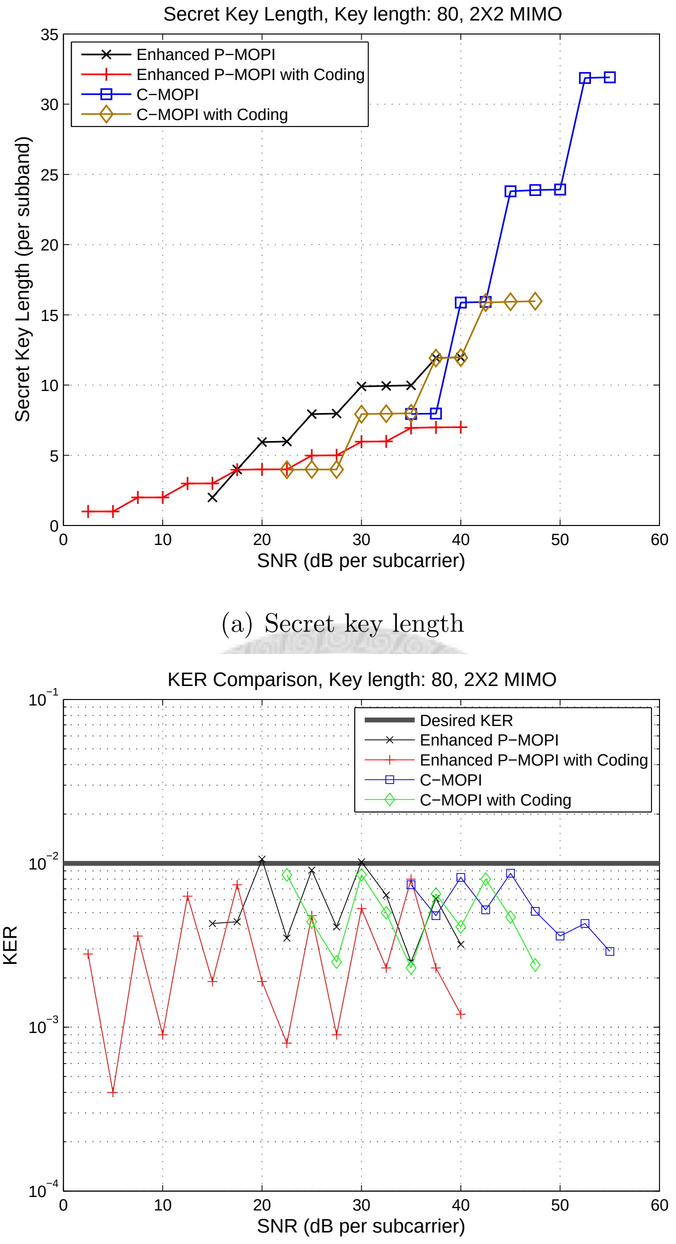


Figure 7.4: Key Error Rate (KER) for enhanced P-MOPI with different size of DFT codebooks

7.2.3 Secret Key Error Rate and Secret Key Length

Secret key agreement probability is the most important target of the secret key generaiotn scheme. In the ideal situation where there is no annoying channel estimation error and Alice and Bob estimate the channel simultaneously, the secret key error rate (KER) should be zero. However, in practical scenario, we should take these annoyances into account. In the simulation, we still assume the legitimate nodes estimates the identical channel, but estimation error happens independently on each node and modeled as gaussian distribution. The subband size is chosen as 20 subcarriers. Fig.7.3 presents the KER of different P-MOPI schemes under 2×2 MIMO environment with 4-bit DFT codebook. The 80-bits secret key is used. It is found the KER of basic P-MOPI scheme is about 0.5 at SNR 30, which seems not very robust. Yet, with the introduce of rotation matrix in enhanced P-MOPI, the KER is decreased sharply to nearly 10^{-3} at the same SNR. If the channel coding is applied, nearly 10dB SNR gain at KER 10^{-3} can be obtained. The proposed enhanced P-MOPI scheme shows its tremendous ability on error reduction.

Fig.7.4 shows the relation between the size of universal codebook and KER. As



(a) Secret key length

(b) Corresponding KER

Figure 7.5: Secret key length comparison for enhanced P-MOPI and C-MOPI for a tagret KER 10^{-2}

expected, the smaller codebook has lower KER compared to the larger one which segments the space into more regions. The influence of channel estimation error becomes dramatic with the growth of codebook size. Yet, for the larger codebook provides more secret bits, the adaptive codebook seems to be necessary to strike a balance between key agreement probability and the secret key length. Therefore, a efficient codebook whose size can be adaptively adjusted is needed. The DFT codebook proposed in [37] can be extend to the desired size easily, and is a suitable choice for the proposed P-MOPI scheme.

Determination on the threshold for changing codebook size arouse another question. [22] suggests us two different goals – **Maximize secret key length** and **Minimize key error rate**. Considering checking the correctness of secret key needs additional public discussion, the loss of system throughput will be huge if the secret key agreement fails often. For that reason, in the simulation we change the codebook size based on a target KER 10^{-2}. If the larger codebook still maintains the desired KER, the codebook size is extended. For the C-MOPI scheme, the number of quantization region can be adaptively adjusted similarly. Based on this criterion, the performance of using adaptive codebook and quantization level is simulated and depicted in Fig.7.5. In Fig.7.5(a), secret key length of enhanced P-MOPI and C-MOPI is found. At the large SNR, C-MOPI provides longer secret key length. But due to the error enhancement introduced by the non-unitary rotation on reference signals. C-MOPI fails to maintain the desired error rate 10^{-2} for lower SNR. On the other hand, enhanced P-MOPI operates well at the appropriate SNR from 15 to 40. With the addition of channel coding, the secret key length is sacrificed for better key agreement probability. C-MOPI with coding can work well at lower SNR compared to C-MOPI, but the performance is worse than P-MOPI scheme with no coding. P-MOPI with coding can extend the operation region of P-MOPI to nearly SNR 0. As a result, coding is not a good choice for C-MOPI who only works under higher SNR scenario. When both channel estimates channel imperfectly, P-MOPI becomes a better choice for its reliability and flexibility on secrecy extraction. Fig.7.5(b) shows the KER of adaptive enhanced P-MOPI and C-MOPI. The target KER 10^{-2} is satisfied during the operation.

The effect on number of MIMO antennas is also simulated. Fig.7.6 shows the performance comparison of P-MOPI under 2×2 MIMO and 4×4 MIMO scenario. As expected, the increasing MIMO antennas leads to better performance. However, for

C-MOPI whose rotation matrix enhances the channel estimation error, Fig.7.7 shows that C-MOPI fails to achieve the desired KER with 4×4 MIMO with SNR lower than 55. It is because larger MIMO matrix may lead to larger power enhancement. With total 32 bits generated in one channel matrix, the performance in 2 is even better than 4×4 MIMO. This result shows the inflexibility on the operation of C-MOPI .

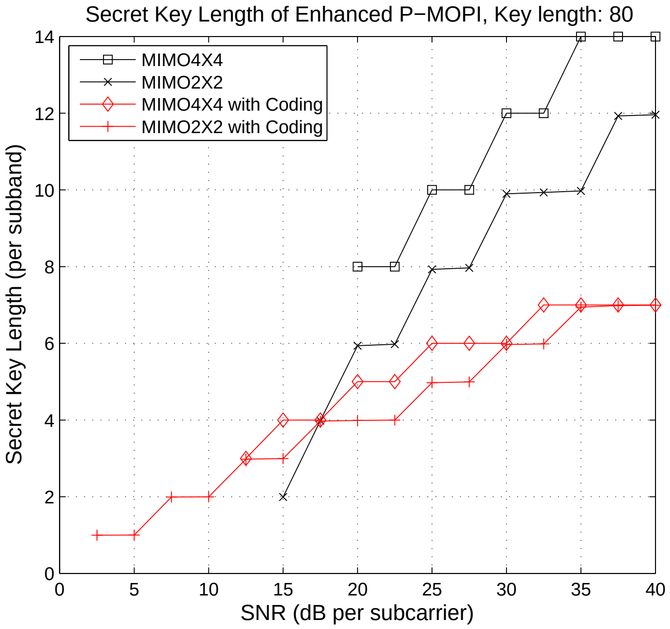


Figure 7.6: Secret key length of enhanced P-MOPI under 2×2 and 4×4 MIMO scenario

7.2.4 Nearby Eavesdropper's Performance

The major security concern for the traditional reciprocity-based secret key generation schemes is the existence of nearby malicious user. When Eve estimates a highly correlated channel similar to $\mathbf{H}^{AB}$, the secret keys may be decrypted in the situation. With the proposed P-MOPI and C-MOPI scheme rotating the reference signals, Eve is unable to decrypt secret keys even she is very close to the legal users. The rotated reference signals prevent Eve from learning both $\mathbf{H}^{AE}$ and $\mathbf{H}^{BE}$. It not only makes Eve cannot obtain the secret keys but also breaks the attack method proposed in [28]. Fig.7.8 shows the power delay profile of the original channel $\mathbf{H}^{BE}$ and the rotated one. It appears that two far different channels are estimated and Eve cannot reconstruct

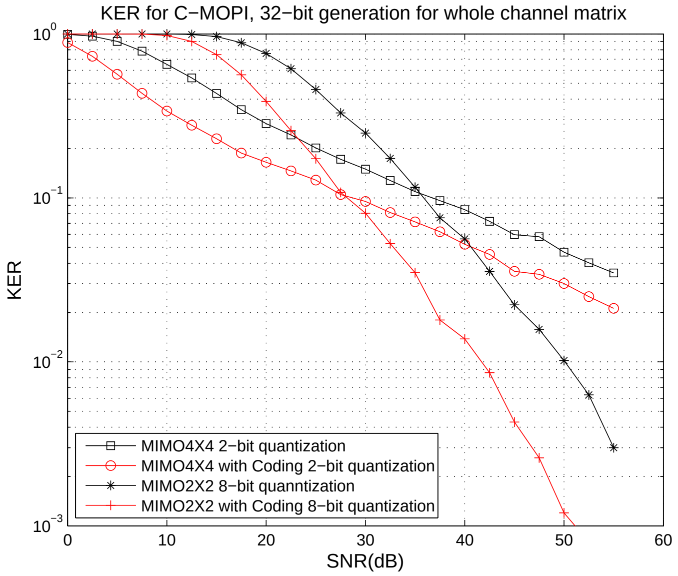


Figure 7.7: KER of C-MOPI under 2 × 2 and 4 × 4 MIMO scenario

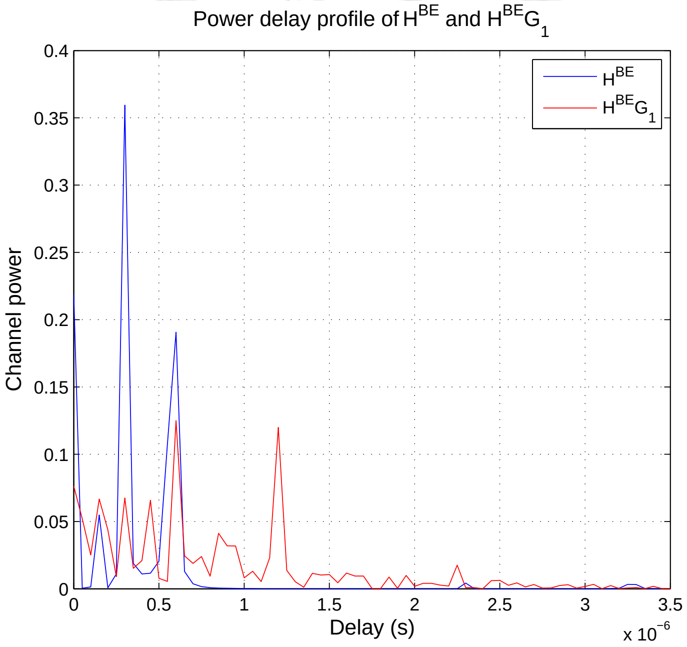
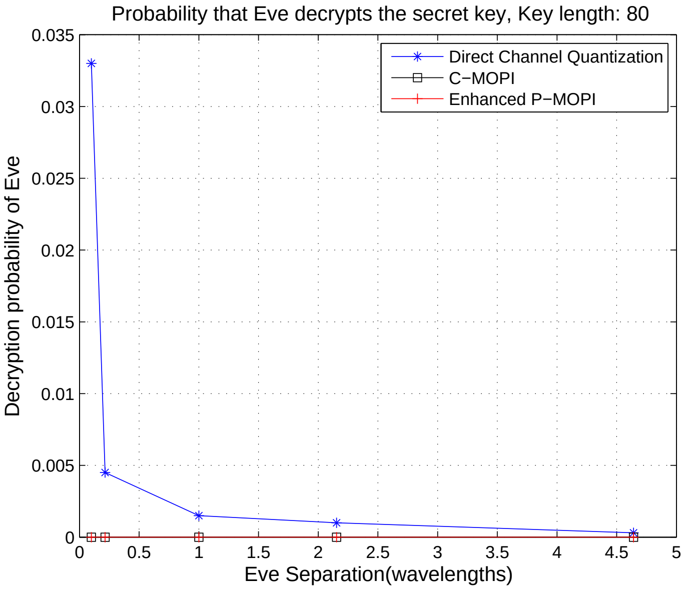


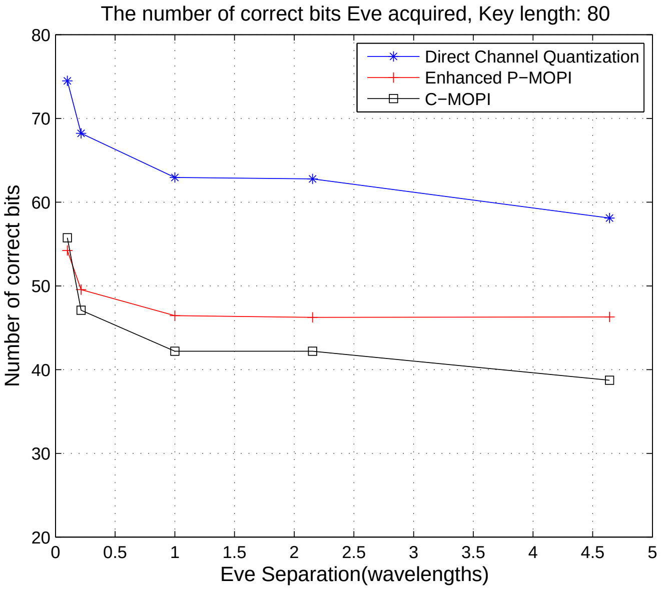
Figure 7.8: Power delay profile for $\mathbf{H}^{BE}$ and its rotation

$\mathbf{H}^{BE}$ without knowing the rotation matrix.

On the other hand, we investigate the probability that nearby eavesdropper acquires the information about the secret key. Two metrics are defined to evaluate Eve's performance. The first one is the probability that Eve successfully decrypts the complete secret key information. The security is broken under this situation. The



(a) Probability that Eve decrypts a 80-bit key



(b) Averaged identical bits Eve decrypts in a 80-bit key

Figure 7.9: Eve's Performance with Different Schemes

second one is the identical bits in a key Eve acquired compared to Bob's key bits. The decreased quantity of the security level is observed. In the simulation, we use a 80-bit secret key which is widely used in the traditional block cipher. 4-bit codebook and 2-bit quantization level is used in the simulation for totally 8-bits generated for whole channel matrix. Fig.7.9 shows the simulation results with 2 × 2 MIMO. If Eve's antenna is close to Alice's or Bob's within one wavelength, according to the near field EM theory [43,44], there will be significant coupling effect between the antennas. Therefore, we only need to consider the situation that Eve is located from Alice and Bob far than one wavelength. It is observed although the decryption probability is low for direct channel quantization scheme, the nearby eavesdropper still has chance to decrypts secret key. But with the proposed enhanced P-MOPI scheme and C-MOPI scheme, the eavesdropper is forced to lose half of the key information. The simulation results show that the probability Eve decrypts the secret key is approximately zero. It can be concluded that it is nearly impossible that Eve decrypts the secret key for the proposed enhanced P-MOPI and C-MOPI schemes.

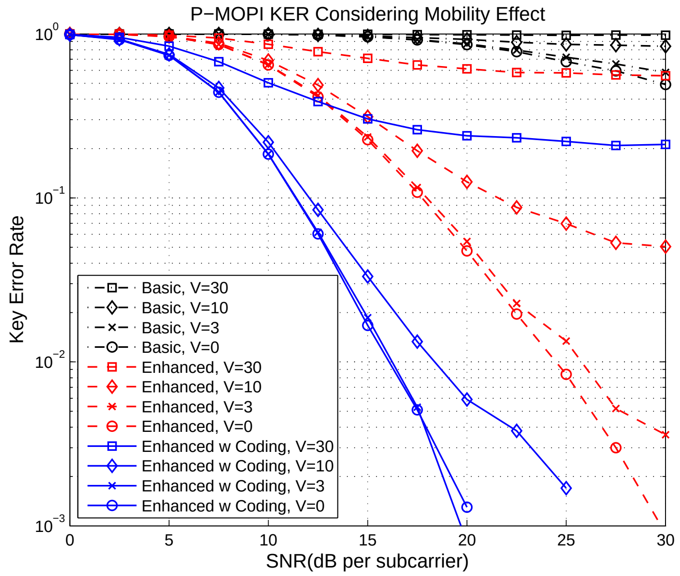
Another result is observed in Fig.7.9(b). If Eve gets no information about the secret key, the identical bits of her key should be 40. But with separation one wavelength, direct channel quantization still gives Eve average 63 identical key bits and the security is far decreased. Nevertheless, The proposed enhanced P-MOPI and C-MOPI scheme are able to decrease the identical bits obtained by Eve. As a result, we can see the nearby eavesdropper is not a problem for the proposed enhanced P-MOPI and C-MOPI scheme while direct channel quantization has difficulty with the situation.

7.2.5 Mobility Effect

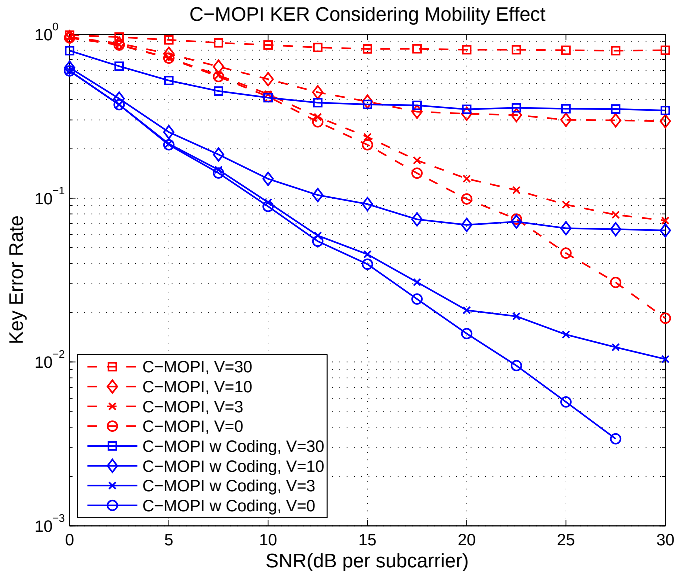
In our previous simulation, we assume both Alice and Bob estimates for the identical channel. Nevertheless, in reality they cannot estimate the channel simultaneously. The channel coherence time will affect the estimation error dramatically. In general, the coherence time is given as

$$\mathbf{T}_c = \sqrt{\frac{9}{16\pi \cdot \mathbf{f}_m^2}} \cong \frac{0.423}{\mathbf{f}_m} \tag{7.2}$$

Where $\mathbf{f}_m$ is the maximum doppler shift defined by $\mathbf{v}/\lambda$, $\mathbf{v}$ denotes the mobility of user and λ is the wavelength. It is noted that channel coherence time only shows how long the channels are "nearly" identical. In secret key agrrement, the minor difference on channel still influence KER a lot. Therefore, the mobility of user will dominate the performance of the proposed P-MOPI and C-MOPI scheme and worth investigating.



(a) P-MOPI with 4-bit codebook



(b) C-MOPI with 2-bit quantization level

Figure 7.10: KER considering mobility effect

Fig.7.10 shows the simulation results of P-MOPI and C-MOPI under different mobility. The channel estimation time difference for Alice and Bob is chosen as 1ms, which is the minimum period LTE supports in the TDD system. The codebook in P-MOPI is 4-bit and the quantization level in C-MOPI is 2. It makes both schemes output the same length of secret key. We can see that when the user moves at speed 10km/hr, with channel coding P-MOPI is still able to maintain the desired KER while C-MOPI fails to achieve it. However, it is shown that both P-MOPI and C-MOPI scheme fails to achieve target KER with user moves faster than 30km/hr. It suggests us that future works should take user's mobility into account when we decide the threshold to change the codebook size or quantization level. It also addresses the necessity of channel coding for its reduction on KER, stronger coding may be helpful to make robust secrecy extraction under fast mobility.

7.3 Performance Evaluation on INTERSECT Scheme

The security of INTERSECT scheme is provided by the two secret sequences which can be utilized to form a secret interleaver. The error rates of these two sequences dominate the performance of the proposed INTERSECT scheme. Intuitively, with larger group size, it is easier to provide nearly identical sequences but the security level is decreased for lower number of groups. With total 1333 subcarriers and group size 88, there are $1333/88 \cong 15$ groups. The randomness of these two secret order is $15! \times 15! \cong 2^{80}$. It provides security level at approximate 2^{80}. Fig.7.11 shows the simulation result with different group size and its corresponding security level with $\beta = 0.3$. With higher security level, higher sequence error rate appears in the simulation.

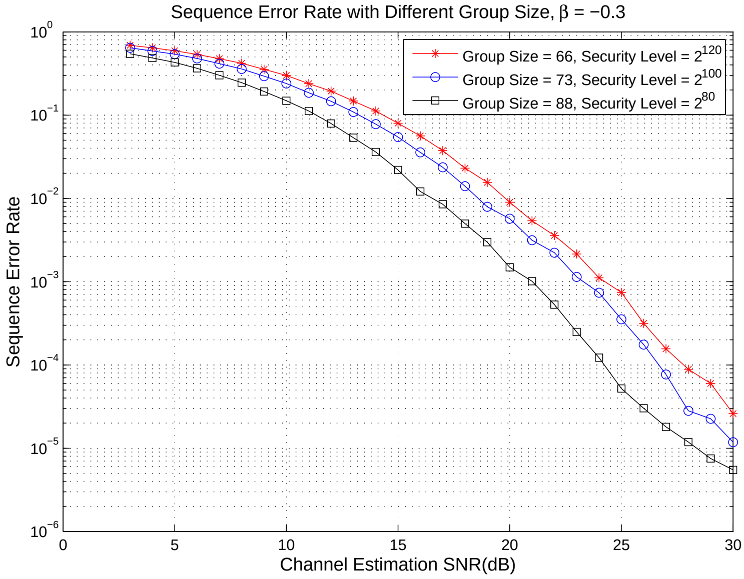


Figure 7.11: Sequence Error Rate with Different Group Size, $\beta = -0.3$

Considering the proposed channel selection algorithm, bad channels are rejected and better sequence error rate is expected. A simulation is done without constraint on maximum rejecting times and the result is depicted in Fig.7.12. It shows that better sequence error rate is achieved with lower β. However, higher rejecting rate is also happened.

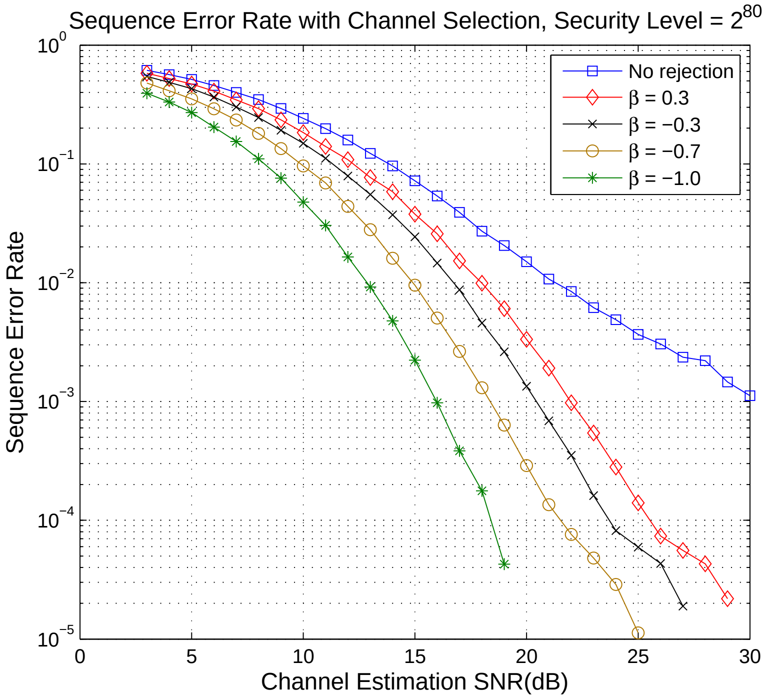


Figure 7.12: Sequence Error Rate with Channel Selection, Security Level: 2^{80}

For the security concern, the secret interleaver should be changed often. Fig.7.13 shows the simulation result with 5 as the maximum rejecting times . It is noted that if β is set too low, the system performance may be even worse. It is because in this situation we seldom accept channel, and the maximum rejecting time is easily achieved. As a result, we are forced to use the instantaneous channel if maximum rejecting time is reached. Therefore, the performance is similar to the case with no rejection if β is set too low.

It is noted that the BICM systems may have some tolerance on the error of interleaver. In Fig.7.14, the transmission bit error rate (BER) is examined with different sequence error rates. It is shown that with sequence error rate lower than 10^{-5}, the

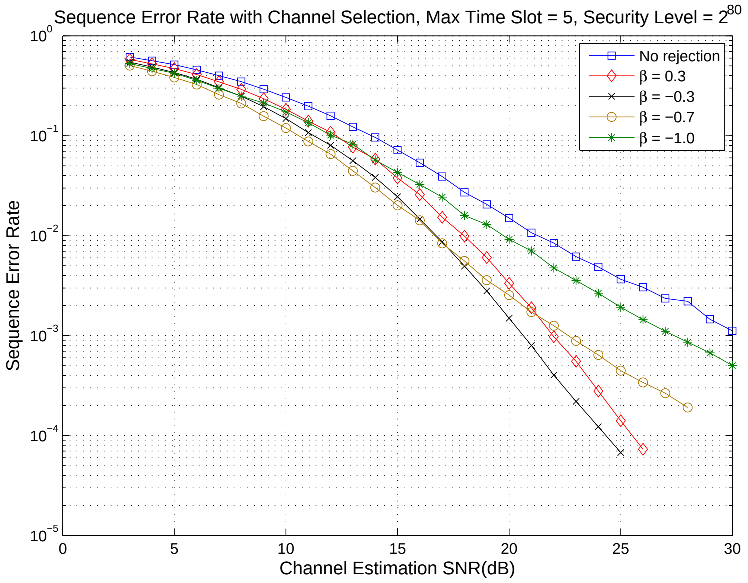


Figure 7.13: Sequence Error Rate with Channel Selection, Max Time Slot: 5, Security Level: 2^{80}

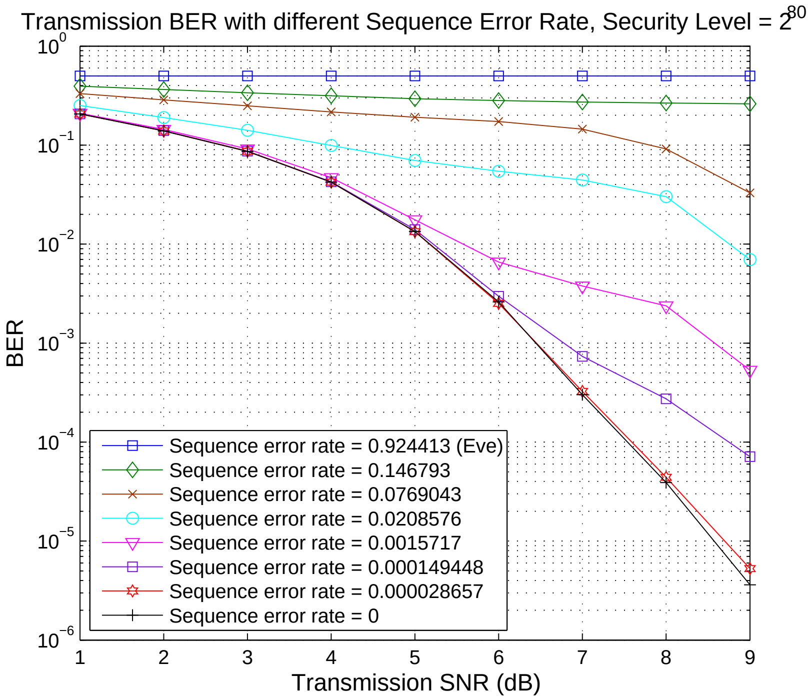


Figure 7.14: Transmission BER with different Sequence Error Rate, Security Level: 2^{80}

BER is very similar to the perfect BER with no sequence error. The 10^{-5} sequence error rate can be achieved with channel estimation SNR at approximately 30 and is not a difficult requirement. It can bee seen that with higher error rate, the transmis-

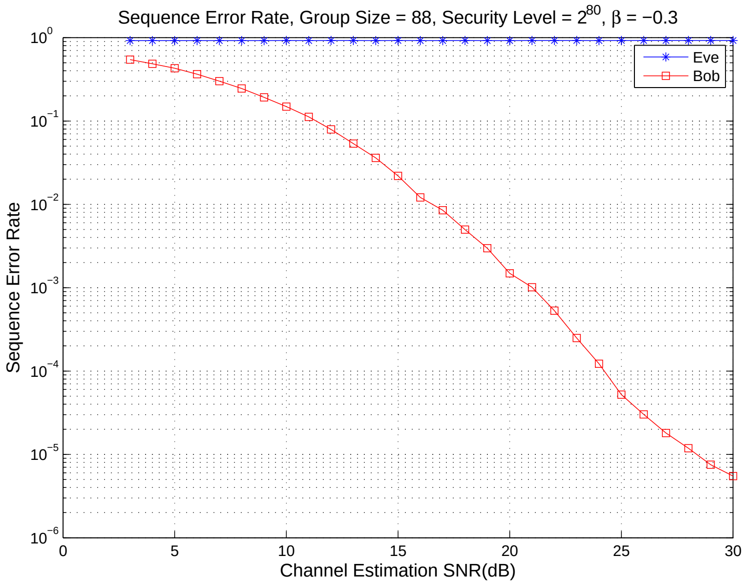


Figure 7.15: Sequence Error Rate, Group Size = 88, Security Level: 2^{80}, $\beta = -0.3$

sion BER is also higher. When sequence error rate achieve 0.1, the BER is nearly 0.5 and the receiver fails to decodes any information. It is the difference between INTERSECT scheme and traditional cryptography. INTERSECT scheme does not need totally correct pattern to decode the secret information. If a little error happens in the interleaving pattern, INTERSECT scheme still has the ability to obtain the secret message but at the expense of worse performance. However, the security level may decrease with the proposed INTERSECT scheme. This shows that there exists the tradeoff between reliability and security. It is noted that Eve is forced to have BER at 0.5 which means that she gets no information about the secret message. It can be seen in Fig.7.15 that the secret sequence error rate for Eve is nearly 1, i.e. she is failed to decode anything. These simulation results show secure transmission is easily achieved with our proposed INTERSECT scheme.

Simulation Setup	
Channel model	SCME channel model
MIMO system	2×2, 4×4 single user MIMO
Subcarrier bandwidth	15 kHz
Total bandwidth	20 MHz
Center frequency	2 GHz
SCME scenario	Urban macro
Codebook	DFT codebook
Channel coding in P-MOPI and C-MOPI	[5 7] convolutional code
Channel coding in Intersect Scheme	[133 171] convolutional code
Frame length	10000
user's velocity	0, 3, 10, 30 m/s

Table 7.1: Simulation Setup

Chapter 8

Conclusions and Future Work

8.1 Conclusions

In this thesis, we have proposed P-MOPI as an efficient secret key generation scheme for MIMO-OFDM systems. We also propose C-MOPI scheme as its extension. The vulnerabilities of traditional reciprocity-based key generation scheme, e.g. nearby eavesdropper, channel simulation attacking and correlated keys, are prevented in P-MOPI and C-MOPI. Inspired by the former MOPI scheme, the reference signals for channel estimation are rotated to achieve secrecy extraction. The public communication overhead and the secret key error rate are also reduced significantly with the well designed rotation matrix.

The proposed P-MOPI scheme utilizes the precoding matrix indices as secret keys while the proposed C-MOPI scheme quantizes the channel coefficients directly. The computer simulations show that C-MOPI results in more secret keys but only works well under high SNR scenario. The channel estimation error is increased by the non-unitary rotation on reference signals. On the other hand, P-MOPI shows its feasibility to provide robust secrecy extraction under low SNR scenario. With both schemes, secret key generation is valid without restriction on SNR. Although the reference signals is rotated, the MIMO precoding is still available in C-MOPI and P-MOPI to enhance the MIMO system throughput. Both MIMO gain and secure transmission are achieved by the proposed P-MOPI and C-MOPI schemes.

Another achievement of this thesis is the INTERSECT scheme. The proposed

INTERSECT scheme shows its feasibility to provides security for a BICM-OFDM system. It can extract a secret interleaver from the observed wireless channel. The reference signals is also modified to ensure the correct order of the secret interleaver. To further enhance the system performance, we propose a channel selection algorithm to reject unsuitable wireless channels. Far different from the concept of security from traditional cryptography, the proposed INTERSECT system have some tolerance for little error on channel estimation. It provides higher interleaver agreement probability with a little security loss. This shows that there exists the tradeoff between reliability and security.

8.2 Future Work

The feasibility of our work is evaluated using the computer simulation. The results show our work is capable of achieving physical layer security. However, the most important factor in our schemes, the wireless channel, is also simulated by computer with the common used channel model. To show the feasibility of our scheme, further implementation on the software defined radio (SDR) is needed. On the other hand, our scheme focus on only one pair of transmitter and receiver. With more transmitter and receiver together, it may have chance to provide more robust security. It is also noted that we assume the single eavesdropper in our scheme. Another possibility for extending our work is to maintain security under the situation where there are more than one eavesdropper.

Bibliography

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[3] M. Kobayashi and M. Debbah, "On the secrecy capacity of frequency-selective fading channels : A practical Vandermonde precoding," in *IEEE 19th Int. Symp. Personal, Indoor and Mobile Radio Communications*, 2008.

[4] S. Lakshmanan, C.-L. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *28th Int. Conf. Distributed Computing Systems*, 2008, pp. 19–27.

[5] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[6] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[7] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52–55, Feb. 2000.

[8] J.-P. Cheng, Y.-H. Li, P.-C. Yeh, and C.-M. Cheng, "MIMO-OFDM PHY Integrated (MOPI) scheme for confidential wireless transmission," in *2010 IEEE Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–6.

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Information theoretic security,” *Found. Trends Commun. Inf. Theory*, vol. 5, pp. 355–580, Apr. 2009.

[10] U. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Advances in Cryptology - EUROCRYPT 2000*, 2000, vol. 1807, pp. 351–368.

[11] C. Cachin and U. Maurer, “Linking information reconciliation and privacy amplification,” *J. of Cryptology*, vol. 10, pp. 97–110, 1997.

[12] J. L. Carter and M. N. Wegman, “Universal classes of hash functions,” *J. of Computer and System Sciences*, vol. 18, no. 2, pp. 143 – 154, 1979.

[13] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915 –1923, Nov. 1995.

[14] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” *Digital Signal Processing*, vol. 6, pp. 207–212, 1996.

[15] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly gaussian random variables,” in *Proc. IEEE Int. Symp. Information Theory*, July 2006, pp. 2593 –2597.

[16] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[17] C. Chen and M. Jensen, “Secrecy extraction from increased randomness in a time-variant mimo channel,” in *IEEE GLOBECOM*, Dec. 2009, pp. 1 –6.

[18] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 240 –254, June 2010.

[19] C. Chen and M. Jensen, "Improved channel quantization for secret key establishment in wireless systems," in *IEEE International Conference on Wireless Information Technology and Systems*, Sep. 2010, pp. 1 –4.

[20] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE ICASSP*, Apr. 2008, pp. 3013 –3016.

[21] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 3, pp. 364 –375, Sep. 2007.

[22] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, pp. 17–30, 2010.

[23] C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205 –215, Feb. 2011.

[24] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of itu channels," in *IEEE Vehicular Tech. Conf.*, Oct. 2007, pp. 2030–2034.

[25] J. Wallace and R. Sharma, "Experimental investigation of mimo reciprocal channel key generation," in *IEEE ICC*, May. 2010, pp. 1–5.

[26] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. ACM MobiCom*. ACM, 2009, pp. 321–332.

[27] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 3, pp. 381 –392, Sep. 2010.

[28] N. Dottling, D. Lazich, J. Muller-Quade, and A. de Almeida, “Vulnerabilities of wireless key exchange based on channel reciprocity,” in *Information Security Applications*, ser. Lecture Notes in Computer Science, 2011, vol. 6513, pp. 206–220.

[29] M. Edman, A. Kiayias, and B. Yener, “On passive inference attacks against physical-layer key extraction?” in *Proc. ACM European Workshop on System Security*, ser. EUROSEC ’11. New York, NY, USA: ACM, 2011, pp. 8:1–8:6.

[30] D. Tse and P. Viswanath, *Fundamentals of wireless communication.* Cambridge University Press, 2005.

[31] D. Love, J. Heath, R.W., and T. Strohmer, “Grassmannian beamforming for multiple-input multiple-output wireless systems,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735 – 2747, Oct. 2003.

[32] V. Klema and A. Laub, “The singular value decomposition: Its computation and some applications,” *IEEE Trans. Autom. Control*, vol. 25, no. 2, pp. 164 – 176, Apr. 1980.

[33] D. Love and R. Heath, “Limited feedback unitary precoding for spatial multiplexing systems,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2967 –2976, Aug. 2005.

[34] D. Love and J. Heath, R.W., “Limited feedback precoding for spatial multiplexing systems,” in *IEEE GLOBECOM*, vol. 4, Dec. 2003, pp. 1857 – 1861.

[35] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall, “LTE: the evolution of mobile broadband,” *IEEE Commun. Mag.*, vol. 47, no. 4, pp. 44 –51, Apr. 2009.

[36] J. Choi, B. Mondal, and R. Heath, “Interpolation based unitary precoding for spatial multiplexing MIMO-OFDM with limited feedback,” *IEEE Trans. Signal Process.*, vol. 54, no. 12, pp. 4730 –4740, Dec. 2006.

[37] Samsung, "MIMO for Long Term Evolution," in *R1-050889, 3GPPTSG RANWG1 ♯ 42,London,UK*, Aug.-Sep. 2005.

[38] P. G'acs and J. Korner, "Common information is far less than mutual information," *Probl. Inform. Control*, vol. 2, no. 2, pp. 149–162, 1973.

[39] D. Love and J. Heath, R.W., "Multimode precoding for mimo wireless systems," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3674–3687, Oct. 2005.

[40] *3GPP TR 25.996 V9.0.0*, 3GPP RAN1 SP-46, 3rd Generation Partnership Project Std., 2009.

[41] *3GPP TR 36.814 V9.0.0*, 3GPP RAN1 RP-47, 3rd Generation Partnership Project Std., 2010.

[42] B. Clerckx, Y. Zhou, and S. Kim, "Practical codebook design for limited feedback spatial multiplexing," in *IEEE ICC*, May. 2008, pp. 3982 –3987.

[43] A. Derneryd and G. Kristensson, "Signal correlation including antenna coupling," *Electronics Letters*, vol. 40, no. 3, pp. 157 – 159, Feb. 2004.

[44] S. Krusevac, P. Rapajic, R. Kennedy, and P. Sadeghi, "Mutual coupling effect on thermal noise in multi-antenna wireless communication systems," in *Proc. Communications Theory Workshop*, Feb. 2005, pp. 209 –214.