Channel Fading in Mobile Broadband Systems: Challenges and Opportunities

by

Dan Shan

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Information Systems Engineering)
in the University of Michigan-Dearborn
2014

Doctoral Committee:

Professor Paul Richardson, Chair
Associate Professor Jinhua Guo
Assistant Professor Hafiz Malik
Associate Professor Weidong Xiang

ACKNOWLEDGEMENTS

First of all, I would like to show my greatest appreciation to my co-advisors, Prof. Paul Richardson and Prof. Weidong Xiang. I would like to thank both of you for your guidance on research, publications and the dissertation. My research experiences gained from your projects equip me for life.

I would like to extend my gratitude to Prof. Kai Zeng for your guidance on my publications. Your research ideas and professional knowledge helped me to publish several top-level papers during my PhD study.

My sincere thanks also go to the other two committee members, Prof. Hafiz Malik and Prof. Jinhua Guo. Your insightful comments, discussions and suggestions enhance the quality of this dissertation significantly.

I would like to offer my special thanks to Prof. Pankaj Mallick and Prof. William Grosky who hold regular meetings for PhD students to exchange research ideas and experiences.

Special thanks also to my supervisor at General Motors, Dr. Fan Bai, who offers me flexible time for the meetings and discussions with my advisors and committee members during the writing of this dissertation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

3GPP	3rd Generation Partnership Project
ASIC	application specific integrated circuit
AWGN	additive white Gaussian noise
BEM	basis expansion model
BER	bit error rate
BPSK	binary phase-shift keying
CE-BEM	complex-exponential BEM
CIR	channel impulse response
CP	cyclic prefix
CSI	channel state information
DFT	discrete Fourier transformation
DSF	double-selective fading
DSRC	dedicated short-range communications
DKL-BEM	discrete Karhunen-Loeve BEM
DLP-BEM	discrete Legendre polynomial BEM
DPS-BEM	discrete-prolate spheroidal BEM
FFT	fast Fourier transform
FPGA	field-programmable gate array
FSF	frequency-selective fading
GCE-BEM	generalized complex-exponential BEM

HST	high-speed trains
ICI	inter-carrier interference
IDFT	inverse discrete Fourier transformation
LMMSE	linear minimum mean square error
INSR	interference plus noise to signal ratio
LOS	line-of-sight
LS	lease squares
LTE	Long Term Evolution (the 4G mobile communication technology)
MAC	media access control
ML	maximum likelihood
MITM	man-in-the-middle
MMSE	minimum mean square error
NMSE	normalized mean squared error
OFDM	orthogonal frequency-division multiplexing
P-BEM	polynomial BEM
PDSCH	physical downlink shared channel
PHY-CRAM	physical-layer challenge-response authentication mechanism
PITIA	piece-wise time-invariant approximation
PWLA	piece-wise linear approximation
QPSK	quadrature phase-shift keying
RF	radio frequency
RSS	received signal strength
Rx	receiver
SER	symbol error rate

SIC	successive interference cancellation
SINR	signal to interference plus noise ratio
SNR	signal-to-noise ratio
SVD	singular value decomposition
TVCE	time-varying channel estimation
Tx	transmitter
VANET	vehicular and ad hoc network
WLAN	wireless local area network

ABSTRACT

High-speed data signals transmitted over mobile broadband channels are seriously distorted by both time-varying effect and frequency-selective fading (FSF). These distortions introduce challenges since channel variances in both time-domain and frequency-domain form a two-dimensional channel matrix which is hard to estimate, but meanwhile provide opportunities for information security since all signals are directly encrypted by the channels which are adequately random over time, frequency and space. These challenges and opportunities are studied in this thesis as two parts. In the first part, we propose a novel time-varying channel estimation (TVCE) algorithm named piece-wise time-invariant approximation (PITIA) to estimate a typical type of mobile broadband channels - the high-speed train (HST) channels. PITIA customizes general time-varying channel models according to HST channels' specific features, and outperforms conventional TVCE algorithms by 5-8 dB in terms of estimation error in typical HST channels. In the second part, we propose the first physical-layer challenge-response authentication mechanism (PHY-CRAM) which uses the mobile broadband channels to prevent eavesdropping during authentication. Since pilots and reference signals are eliminated, eavesdroppers cannot demodulate credential information, while legitimate receivers use the channels' reciprocal property to cancel FSF. PITIA is evaluated by computer based simulations, and the effectiveness of PHY-CRAM is validated by prototyping and real-world experiments. Both pieces of works are built upon a unified system model and orthogonal frequency-division multiplexing (OFDM) modulation.

Keywords - Wireless communications, OFDM, PITIA, PHY-CRAM, Channel estimation, Authentication

CHAPTER 1

Introduction

1.1 Background

Wireless radio frequency (RF) communications provide voice and data services for highly mobile users. As the infrastructure continues to mature, users are offered the promise of ubiquitous voice and internet connectivity. However, wireless communications face severe challenges as the number of users, coverage area and data rates grow, because a signal traversing the wireless medium not only loses energy density at a quadratic rate, but is also disturbed by ground clutter and interferences. Moreover, relative frequency shifts (e.g. Doppler spread) become more serious when users move at higher speeds. These challenges must be addressed to provide reliable services to users at any time and from anywhere.

Over the years, tremendous efforts have been expended in the areas of channel measurements, channel modelling, and channel estimation to meet the expanding demands of wireless users. These focuses are motivated by the need to transmit data over dynamic, time varying, frequency dependent, and location dependent wireless channels, which convolve the data signals and must be compensated at receivers. Among all wireless channels, the ones experienced by high-speed communication systems in mobile environments are most interested in this thesis and called mobile broadband channels.

Estimating mobile broadband channels is very challenging, because they have large delay spread and Doppler spread, and vary drastically in both time-domain and frequency-domain. To capture channel variances in both domains simultaneously, channel estimators have to adopt two-dimensional channel models which contain too many parameters and cannot be estimated directly. Although various methods are proposed to simplify two-dimensional channel models, they consider general applications and suffer from large modelling error. In this thesis, we propose a novel channel estimation algorithm with the name piece-wise time-invariant approximation (PITIA) [1], which is dedicated for specific mobile broadband channels - the high-speed train (HST) channels, and uses the unique features of HST channels to enhance performance.

On the flip side, mobile broadband channels can also be harnessed by communication systems. The main motivation for overcoming the challenges of RF signal propagation characteristics described above is that mobile users can exchange data over very large coverage areas. This same property also introduces privacy and security concerns, because the transmitted signal is directly available to all receivers including legitimate users and eavesdroppers, and the capability for high speed data transaction over a large coverage area exacerbates these concerns. As eavesdroppers face the same obstacle of channel estimation as legitimate users do, the characteristics of mobile broadband channels complicate eavesdropping and may enhance information security.

Mobile broadband channels are able to secure confidential information much better than other channels do, since the former ones vary much faster over time, frequency and space, and contain significantly larger amount of randomness which is crucial for information security. Moreover, such randomness exists in nature, while that in conventional security systems is generated artificially and need to be secured cryptographically. The ever-increasing computation power and enhanced mathematical theories may break conventional security systems, but cannot guess the randomness in mobile broadband channels. These unique features provide great opportunities for security systems. While most related works focus on key generation through wireless channels, this thesis studies non-cryptographic challenge-response authentication which has not been touched in academy before, and devises a novel system named PHY-CRAM [2]. In this system, shared keys exchanged by legitimate users during authentication are secured directly by the channel, and the feasibility of this mechanism is validated by prototyping and extensive real-world experiments.

In short, this thesis discusses both challenges and opportunities of mobile broadband channels. The challenges are addressed by PITIA which estimates HST channels with improved accuracy compared with conventional methods, while the opportunities are leveraged by PHY-CRAM which is the first non-cryptographic challenge-response authentication mechanism.

1.2 Contributions, Novelties and Significances

1.2.1 Addressing the challenges

In high-mobility environments such as HST environments, Doppler effect becomes a dominant challenge for mobile broadband systems, and the reasons are given below. Conventional single-carrier modulation schemes in wireless/mobile environments can only offer a few Mbps bandwidth which is insufficient for broadband applications, and must be replaced by orthogonal frequency-division multiplexing (OFDM) [3]. However, OFDM is designed for quasi-static environments where wireless channels are time-invariant, while mobile broadband systems experience serious Doppler effect and time-varying effect especially when users travel very fast. Consequently, conventional OFDM systems suffer from very high noise-floor in mobile broadband channels, and the symbol error rates (SER's) at OFDM receivers approach a constant high value no matter how high signal-to-noise ratio (SNR) is. Specifically, when normalized Doppler spread equals to 0.064, the best SER achieved by a conventional OFDM receiver is only 0.08 [4], which is unacceptable for most applications even with channel coding.

The prevailing technique to estimate time-varying channels is called basis expansion model

(BEM), which approximates the channels by a series of basis functions and reconstructs them by BEM coefficients. This way, estimating a time-varying channel is equivalent to estimating BEM coefficients. Being different from BEM, PITIA approximates the time-varying channel by a series of time-invariant channels, and is more suitable for HST channels which usually have large Doppler spread, small delay spread and high SNR.

PITIA outperforms BEM by 5-8 dB with respect to estimation error in HST channels, and has low computational complexity. The main reason for this improvement is that, PITIA considers the unique features of HST channels and reduces the number of parameters to model them, while less parameters lead to less estimation error according to estimation theories [5]. To achieve satisfactory modelling error, a L-tap HST channel is modelled by only $2L$ parameters in PITIA, i.e., L complex gains (linear parameters) and L Doppler shifts (non-linear parameters), compared with at least $3L$ parameters in BEM. Some existing channel estimation algorithms [6] [7] also adopt the same non-linear channel model as the one used by PITIA, but since estimating non-linear parameters (Doppler shifts) is very hard, their computational efforts are prohibitively large. PITIA models HST channels with the least channel parameters, decouples the FSF and time-varying effect in HST channels for the first time, and is the simplest one among all algorithms that estimate Doppler shifts directly.

1.2.2 Leveraging the opportunities

Two features of mobile broadband channels are favoured by information security: (1) channel responses at different times, locations and frequencies are random and uncorrelated; (2) channel responses are reciprocal (or symmetrical) in both directions, i.e., channel responses from A to B and from B to A at the same time are exactly the same. The randomness and reciprocal property have potential to achieve a high level of privacy, since such randomness exists in nature and can be perceived only by legitimate users, while attackers reside at different locations and perceive different channel responses. The amount of randomness, quantified by entropy, is proportional to multipath delay spread σ_τ, channel bandwidth B, relative velocity v between legitimate users, and time span. For example, if $\sigma_\tau = 0.2\mu s$, $B = 10MHz$, $v = 110km/h$ and central frequency equals to 5.9 GHz, the overall entropy during one second is about 66,000 bits, which is huge compared with the lengths of secret keys in most cryptographic security protocols.

Researchers have used the randomness and reciprocal property of mobile broadband channels to enhance or replace cryptographic protocols, such as message authentication [8, 9] and key exchange protocols [10–13]. Being different from them, we propose a novel authentication mechanism named PHY-CRAM, where legitimate users do not transmit any pilots or reference signals for channel estimation, but cancel the effect of channels by an reciprocal operation. In this way, legitimate receivers can decode the secret information while eavesdroppers get nothing.

Contributions of PHY-CRAM are two-fold: (1) it is the first non-cryptographic challenge-response user authentication mechanism in the literature; (2) it is the first OFDM system that uses reciprocal operation to eliminate channel estimation. Due to the first contribution, PHY-CRAM does not need to increase its key length in order to maintain the same security strength if the attacker's computational power is increased, while conventional authentication schemes (such as CRAM-MD5 [14] and CHAP [15]) must increase key lengths in this case. Longer keys usually imply more computation overhead, energy consumption and storage overhead, which are not desirable in resource constrained networks, such as wireless sensor networks. Moreover, the reciprocal operation in the second contribution eliminates channel estimation, prevents attackers from probing the channel, and increases security strength.

The significance of PHY-CRAM is further enhanced by field-programmable gate array (FPGA) based prototyping and real-world experiments. FPGA provides us with two benefits: (1) it reduces processing delay and maintains the channel's reciprocal property; (2) it is very close to an ASIC (application specific integrated circuit) in a commercial device, and makes the experimental results more convening. The one-way processing delay in our prototype is only $40\mu s$ during which the reciprocal property of mobile broadband channels is well maintained, and PHY-CRAM maintains a high level of confidentiality during authentication according to the real-world experiments.

1.2.3 Publications related to this thesis

PITIA is presented in part in [16], and its journal version is in the final revision stage [17]. PHY-CRAM is published in [2], and is enhanced in [18] to cover multi-hop networks. Moreover, the hardware/software platform which prototypes PHY-CRAM is based on the work presented in [19], and is also used by our research works on cognitive radios [20, 21].

1.3 Related works

1.3.1 Basic channel estimation algorithms for OFDM

Basic channel estimation algorithms for OFDM assume that the channel response is constant over the entire OFDM block (also called OFDM symbol). Such channel has the name time-invariant channel (with the implication that there exists frequency-selective fading), and is synonymous with frequency-selective fading (FSF) channel throughout this thesis. Although these algorithms cannot be used to estimate HST channels, they are the foundation of advanced channel estimation algorithms including PITIA.

Existing algorithms for FSF channel estimation can be grouped into two types: blind (or semi-blind) estimation algorithms [22–26] and pilot-aided ones [27–37]. Some blind estimation algorithms [22, 23] first calculate the covariance matrix of the received signal for each OFDM block, and then derive the channel impulse response (CIR) through singular value decomposition (SVD) of this covariance matrix. Another set of (semi-)blind estimation methods conduct channel estimation and data symbol detection iteratively or jointly [24] [25], and are called EM-type estimator. Some EM-type estimators are semi-blind because they need knowledges about the channel responses in initial stages, which can be derived from the pilots only at the beginnings of all frames. Afterwards, EM-type estimator is merged into Turbo decoder for Turbo-coded OFDM systems to further enhance the bit error rate (BER) performance [26].

Since most blind estimators suffer from high complexity, practical OFDM systems rely on pilots (also called reference signals) for channel estimation. Among these pilots-aided channel estimation algorithms, minimum mean square error (MMSE) [27,28,30], maximum likelihood (ML) [29] and lease squares (LS) [30] estimators are the most famous ones, and they are all derived from statistical signal processing theories [5]. MMSE estimator has the best performance with the highest complexity among all algorithms, since it utilizes both SNR and a priori information about the correlation of channel responses on adjacent subcarriers. Derivation of channel correlation is not as simple as SNR, and is discussed in [32, 33]. Although MMSE estimator reaches a certain degree of optimality, it considers all subcarriers as a whole and requires either matrix inverse operation or pre-known pilots at all subcarriers, both of which may not be realistic in practical OFDM systems. A simplified version of MMSE estimator named LMMSE (linear MMSE) estimator is proposed in [28], which derives rough channel estimates with LS estimator first and then corrects them. LMMSE replaces matrix inverse with matrix multiplication, which is simpler but still too computationally demanding for embedded devices. To further reduce complexity, the channel response on each pilot subcarrier can be estimated one by one [34]. This method utilizes neither SNR nor frequency-domain correlation of the channel, and is classified as LS or zero-forcing (ZF) estimator. The channel responses on data subcarriers can be derived from various interpolators, like the linear interpolator [35], polynomial interpolator [28], MMSE interpolator [34] or some other ones [36, 37]. Furthermore, recovered data symbols can also be used for channel estimation for the next OFDM block or iteratively for current OFDM block, generating the decision-directed estimators [25, 38].

Channel parameters in PITIA are estimated by LS estimator which can effectively resist noise with low computational complexity. Although LS estimator is designed for linear systems, PITIA uses it to estimate non-linear parameters - Doppler shifts, and such usage is rarely found in the literature. PHY-CRAM does not use any estimator since channel estimation is eliminated.

1.3.2 Time-varying channel estimation

The wireless channel whose response varies during each OFDM block is called time-varying channel (with the implication that there exists frequency-selective fading), and is synonymous with double-selective fading (DSF) channel throughout the thesis. Existing time-varying channel estimators are built upon general time-varying channel models, while PITIA is built upon a specific model for HST channels.

OFDM systems exposed to time-varying channels suffer from inter-carrier interferences (ICI's), which is the cause of noise floor and calls for advanced remedies [39, 40]. In early works, ICI's are cancelled by diversity over subcarriers [41–43] and estimated by grouped pilots on continuous subcarriers [44], both with very low spectrum efficiency. Since ICI's come from the sidelobes of adjacent subcarriers, a Hanning windowing (instead of a rectangular window) used by the pulse shaping filter reduces ICIs significantly [45], but also increases the complexity greatly, since the fast Fourier transform (FFT) operation can no longer be used to simplify OFDM modulation. The windowing and diversity methods are combined and generalized in [46], with the same issue of low spectrum efficiency.

Most ICI cancellation/mitigation methods adopt multi-tap frequency-domain equalizers instead of the one-tap equalizers for time-invariant channels. Estimating the weights of all taps on all subcarriers is challenging, since these weights form a two-dimensional matrix with too many parameters to estimate [47]. In other words, a non-diagonal channel matrix can fully describe the time-varying channel [48], and if this channel matrix can be estimated, the unknown data at the transmitter can be derived from matrix inverse operation. This idea is realized in [49], where a time-domain reference signal is transmitted periodically to facilitate channel matrix estimation; however, very few OFDM systems have this kind of reference signal.

Another famous ICI cancellation method is called minimum-mean-squared error with successive interference cancellation (SIC) scheme (MMSE-SIC), which makes decision on the value of the strongest symbol in current loop and nulls its waveform based on the decision iteratively [50, 51]. However, this method suffers from the error propagation issue that, a wrong decision in one symbol affects the decisions of many other symbols. In order to solve this problem, [52] adds a Turbo decoder in the receiver with a penalty of much higher complexity. A similar work is found in [52], where the EM-type channel estimation algorithm is combined with MMSE-SIC.

Recent works in time-varying channel estimation (TVCE) model the time-varying channel as $h(t,\tau)$ where t and τ denote time and channel dispersion, respectively. Some algorithms focus on the estimation of $h(t,\tau)$ [53–67], while others are devoted to designing low-complexity channel equalizers when $h(t,\tau)$ has been estimated [68, 69]. In this thesis, we focus on the first problem - estimation of $h(t,\tau)$.

The two-dimensional channel model $h(t,\tau)$ contains too many parameters and must be simplified to facilitate TVCE. For examples, $h(t,\tau)$ is approximated by linear functions in [70] and by polynomials in in [65]. The first model has smaller number of channel parameters and better ability to resist noises, but suffers from larger modelling error, while the latter one shows opposite properties. PITIA achieves a better balance between modelling error and the ability to resist noise, compared to these two techniques.

BEM is widely adopted to simplify time-varying channels, and TVCE downgrades to the estimation of BEM coefficients. In [58], LS and LMMSE estimators are used to estimate BEM coefficients through a group of clustered pilots. For OFDM systems without pilots, blind estimation methods are proposed in [66] with very high computational complexity. Moreover, BEM coefficients can also be estimated through superimposed training [67].

Proper design on basis functions is crucial for BEM based TVCE algorithms (named BEM methods hereafter), since these basis functions must model the variance of time-varying channels precisely, so that the modelling error could be reduced. Various types of basis functions are proposed, including complex-exponential BEM (CE-BEM) [71], generalized complex-exponential BEM (GCE-BEM) [53], polynomial BEM (P-BEM) [54], discrete-prolate spheroidal BEM (DPS-BEM) [55], discrete Legendre polynomial BEM (DLP-BEM) [61, 64] and discrete Karhunen-Loeve BEM (DKL-BEM) [56] etc. Actually the polynomial channel model in [65] is a special P-BEM. These models require either a large number of basis functions or preknown channel statistics to keep modelling error small, and require more basis functions when Doppler spread grows. According to our study, BEM methods require at least $3L$ channel parameters to model a HST channel with L resolvable multipath, while PITIA requires only $2L$ ones with similar modelling error. Fewer number of parameters to be estimated result in smaller estimation error according to estimation theories [5].

The proposed algorithm falls into the category of pilot-assisted TVCE algorithms, in which pilots suffer from interference generated by data symbols. This problem can be mitigated by joint channel estimation, equalization and data detection algorithms [64, 72]. However, computation complexity of these algorithms is at least $O(N^2L)$ for N subcarriers, which is too high for LTE and

WiMax systems where $N > 1000$.

The channel model proposed in this work is similar to the ones adopted in [6] and [7], where the $2L$ channel parameters are derived from multidimentional minimization algorithms whose computational complexities are extremely high. Other methods to solve multidimentional minimization problems also suffer from high complexity, for examples, ML [5], MUSIC [73] and ESPRIT [74]. Compared to these works, PITIA has much lower computation complexity with closed-form expressions for all estimates.

PITIA is fundamentally different from piece-wise linear approximation (PWLA) [70] although they have similar names. PITIA assumes that the phase of a channel response at each channel tap changes linearly over time, while PWLA assumes that the real and imaginary parts of a channel response are linear. As a result, the channel model in PITIA is non-linear while that in PWLA is linear. Due to this difference, PITIA shows very small modelling error in the channels with small delay spread and large Doppler spread, for example, the HST channels, while PWLA is only applicable in low-mobility environments.

Finally, [75] proposes a TVCE algorithm for HST channels which adopts P-BEM and relies on block-type pilots embedded in LTE uplink channel, while PITIA favours both block-type pilots and comb-type pilots. Again, PITIA has fewer number of channel parameters than [75] has.

1.3.3 Physical-layer security

Existing works on physical-layer security can generally be categorized into four types: (1) the ones based on transceiver hardware differences, i.e., RF fingerprinting [76–78], (2) the ones based on wireless channels [8, 9, 79–81], (3) physical layer signal watermarking [82, 83] and (4) key generation from wireless channels [10–13]. None of them study challenge-response user authentication while PHY-CRAM does.

(1) RF fingerprinting exploits the transceivers' hardware impairments to identify different wireless devices. Two main approaches for RF fingerprinting are introduced in the literature: transient-based method [76] and modulation-based method [77]. The former one identifies devices according to the transient behaviours of the devices' amplifiers during the switch from idle state to transmission state, while the latter one applies the imperfection of modulated signals. It was recently found that RF fingerprinting is vulnerable to impersonation attack [78], while PHY-CRAM is immune to such attack. To attack the existing RF fingerprinting schemes, an attacker does not necessarily reproduce a legitimate radio, but only needs to reproduce/replay the signal used for RF fingerprint verification. Furthermore, measurements on RF fingerprinting are expensive, since they need high-end signal analysers to extract subtle differences in the signals. Lastly, RF fingerprinting usually requires a relatively stationary channel condition to accurately extract fingerprints.

(2) Wireless channel based authentication mechanism is based on the fact that the channel state information (CSI) is location-specific due to path loss and channel fading [8, 9]. In a relative stable environment, an attacker, whose location is different from the legitimate user's location, will present different CSI profile or link signature from the legitimate one. This type of authentication requires a legitimate user to be authenticated at a specific location, and might not work well in highly dynamic environments where channel states change drastically over time due to fading or mobility. The authentication algorithm may need a large number of samples to ensure a desirable performance, and is also subject to mimicry attacks [84] where an attacker can gain the legitimate channel information when it is close to the legitimate devices. A recent remedy is proposed to prevent mimicry attacks, but it requires time synchronization among legitimate parties [81].

Time correlation property of the wireless channels is also exploited to support message authentication in time-varying channels [79, 80]. For example, [75] proposes a physical-layer authentication algorithm that utilizes channel probing and hypothesis testing to determine whether current and prior communication attempts are made by the same transmit terminal. If the time interval between two frames coming from the same transmitter is smaller than channel coherence time, CSI [79] or received signal strength (RSS) [80] of these two frames should be highly correlated. A similar approach based on RSS is proposed in [80]. These authentication mechanisms check the message authenticity during communication sessions, while they assume that the very first message (frame) is already authenticated.

PHY-CRAM does not require the legitimate user be at a specific location, and eliminates channel profile training/probing. Moreover, PHY-CRAM utilizes the randomness in the channels to hide the shared secret used for authentication, while channel based authentication decides if the frames are sent from the same channel or not.

(3) Physical layer signal watermarking or fingerprinting is a mechanism to convey a cryptographically secured authentication code/tag along with the primary transmission or message [82, 83]. General signal watermarking through low-power perturbations of the signal constellation is proposed in [82], with the basic idea that a low-power signal for message authentication is superimposed on the waveforms carrying data information.

From a methodological point of view, PHY-CRAM is different from signal watermarking since it does not add any authentication code or tag into the signal. Moreover, PHY-CRAM initializes a secure communication, while signal watermarking applies to message authentication during the communication session.

(4) PHY-CRAM is different from physical layer key generation algorithms [10–13] although they are based on common physical layer foundations (i.e., channel reciprocity, randomness, and location decorrelation). First, they serve for different purposes, since the former is for authentication and the latter is for shared key generation. Second, PHY-CRAM exploits the reciprocity to “decrypt” the shared secret used for authentication, while wireless channel key generation relies on

the reciprocity to ensure that channel states observed by the two key generation parties are highly similar. Furthermore, PHY-CRAM does not need to sound the channel explicitly or to reconcile the key disagreement, and none of the participants knows CSI after authentication. Elimination of (explicit) channel sounding operation not only simplifies the mechanism, but also increases the security strength. For example, the “Man-In-The-Middle” (MITM) attack introduced in [85] is not applicable to PHY-CRAM.

CHAPTER 2

System Model

In this chapter, we first introduce OFDM which is adopted as the modulation scheme for most mobile broadband systems. Then channel models and problem definitions are introduced in section 2.2 and section 2.3, respectively. Finally, the experimental set up and design tools are introduced in section 2.4.

2.1 Basics of OFDM

An OFDM system divides a frequency-selective fading channel into N narrow-band channels (subcarriers) and transmits data symbols over them, so that all data symbols experience flat fading channels which can be easily estimated and compensated.

The block diagram of OFDM system is shown in figure 2.1. At the transmitter, binary data to be transmitted are first mapped to symbols according to a certain constellation, for examples, binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK). Then pilots and nulls are mixed with data symbols for channel estimation and spectrum control, respectively. Next, inverse discrete Fourier transformation (IDFT) is conducted over all symbols, and a cyclic prefix (CP) is inserted at the beginning of the output signal $\mathbf{x}$ to overcome multipath. When the length of CP is larger than the maximum delay spread of multipath, adjacent OFDM symbols (IDFT blocks) are separated by CP and immune from inter-symbol-interference (ISI). The final baseband signal samples are denoted as $\tilde{\mathbf{x}}$, which are sent to digital-to-analogue converter (DAC) and RF front-end for transmission. At the receiver side, timing and frequency synchronization are first achieved

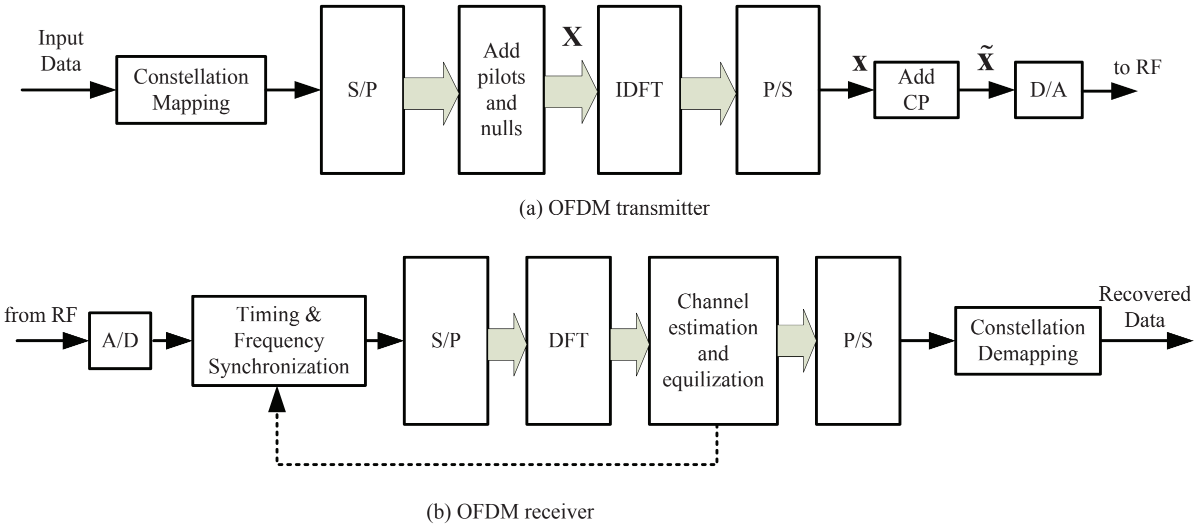

Figure 2.1: The block diagram of an OFDM system

through CP and synchronization header. Then discrete Fourier transformation (DFT) is conducted over received signal samples within appropriate time window, which is also called observation window and should just cover a single OFDM block. Finally, channel estimation and equalization are conducted after DFT, and binary data are recovered.

According to the analysis above, $\mathbf{x} = \mathbf{F}^{-1}\mathbf{X}$ where $\mathbf{F}$ denotes the $N \times N$ Vandermonde matrix in which the j^{th} element at the i^{th} line equals to ω^{ij} with $\omega := exp(-2\pi i/N)$.

2.2 Channel Models for Mobile Broadband Systems

The wireless channels in mobile broadband systems have two major characteristics: frequency-selective fading (FSF) and time-varying effect.

FSF arises when the root mean squared (RMS) delay spread of multipath, denoted as σ_τ, is much larger than the duration of a data symbol. This situation usually happens when the data rate is very high (so that symbol duration is short), as the case in broadband systems. Frequency-domain analysis is widely used in broadband systems, and we consider a channel as FSF when channel bandwidth B is larger than coherence bandwidth B_C, which is approximated by $1/(5\sigma_\tau)$ [86]. For example, when Long Term Evolution (LTE) operates in open area, $\sigma_\tau \approx 0.5\mu s$, $B_C \approx 400$ kHz while $B = 20$ MHz; therefore, the LTE system experiences serious FSF. OFDM introduced in the previous section is the best technique to overcome FSF so far, and is adopted by almost all broadband systems including LTE.

The time-varying effect of a wireless channel is caused by Doppler effect which happens in high-mobility environments. Doppler effect both shifts a signal's spectrum in frequency-domain and rotates a signal's phase in time domain, and cannot be compensated easily in multipath environments since Doppler shifts on different multipath components may be different. Time-varying effect is usually studied in time-domain, and we consider a channel as time-varying when the observation window (DFT window for OFDM) for channel estimation is comparable to channel coherence time T_C, which can be approximated by $0.423/f_d$ where f_d denotes the maximum Doppler shift. For example, when LTE operates on a high-speed train, f_d may be as big as 1 kHz, $T_C \approx 423\mu s$, and the observation window equals to the duration of one OFDM symbol which is 70 μs. Therefore, this HST channel is considered as time-varying when LTE is adopted. On the flip side, when a Dedicated Short-Range Communications (DSRC) [87] system operates in urban area, T_C is at the level of mini-second [88], while observation window (or duration of one OFDM symbol) is only 8 μs. As a result, DSRC channel is considered as time-invariant by channel estimators. Note that time-invariant channels in mobile environments also vary over time.

A wireless channel exhibiting both FSF and time-varying effect has the name double-selective fading (DSF) channel which is very hard to estimate, and the HST channel falls into this category according to the analysis above. On the flip side, a DSRC channel exhibits only FSF and we call it FSF channel, which can be easily estimated [89].

2.2.1 The DSF channel

The DSF channel is modelled by $h(t,\tau)$ where t and τ denote time and channel dispersion, respectively. It has a digitized version $g_{n,m}$, where n and m denote time index and channel tap index respectively, with $0 \leq n \leq N-1$ and $0 \leq m \leq L-1$. Here N represents the number of samples in observation window, and L denotes the number of multipath components. Define $\mathbf{x}(k) := [x_0(k),...,x_{N-1}(k)]^T$ as the time-domain samples within the k^{th} OFDM block at the transmitter, and $\tilde{\mathbf{x}}(k) := [x_{N-L}(k),...,x_{N-1}(k),\mathbf{x}(k)^T]^T$ as the transmitter's final output with CP. We will drop index (k) when necessary. By assuming that the receiver is synchronized to the first path of signal x_0 and CP is disregarded, the received signal $\mathbf{y} := [y_0,...,y_{N-1}]^T$ is given by

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{n} \tag{2.1}$$

where $\mathbf{G}$ is a $N \times N$ matrix defined as

$$\mathbf{G} := \begin{bmatrix} g_{0,0} & 0 & \cdots & 0 & g_{0,L-1} & \cdots & g_{0,1} \\ & & & \cdots & & & \\ g_{L-2,L-2} & \cdots & g_{L-2,0} & 0 & \cdots & 0 & g_{L-2,L-1} \\ g_{L-1,L-1} & \cdots & & g_{L-1,0} & 0 & \cdots & 0 \\ 0 & & \cdots & \cdots & & & \cdots \\ 0 & & \cdots & 0 & g_{N-1,L-1} & \cdots & g_{N-1,0} \end{bmatrix} \tag{2.2}$$

Here, 2.2 is the time-varying channel model which is well-accepted by the literature.

2.2.2 The FSF channel

In a FSF channel, an OFDM system can be considered as the superposition of N independent narrow band subsystems that experience flat-fading channels, and each subsystem is modelled simply by

$$Y_n = H_n X_n + W_n, n = 0, ..., N-1 \tag{2.3}$$

where Y_n and X_n denote the frequency-domain symbols at the receiver and the transmitter, respectively, W_n the additive white Gaussian noise (AWGN), and H_n the frequency-domain channel response, all at subcarrier n. Here X_n is also the n^{th} element in $\mathbf{X}$.

2.2.3 Discussions

While the models for a DSF channel and a FSF channel appear quite different, they share a fundamental theoretical connection. To show this, we concatenate Y_n, X_n and W_n for $n = 0, ..., N-1$ into vectors $\mathbf{Y}$, $\mathbf{X}$ and $\mathbf{W}$, and rewrite 2.3 in a matrix format:

$$\mathbf{Y} = \mathbf{HX} + \mathbf{W} \tag{2.4}$$

where $\mathbf{H}$ is a diagonal matrix with H_n as its n^{th} element on the main diagonal.

Meanwhile, 2.1 can be formatted as

$$\mathbf{Fy} = \mathbf{Y} = \mathbf{FGF^{-1}X} + \mathbf{Fn} \tag{2.5}$$

and obviously $\mathbf{Fn} = \mathbf{W}$. As a result, both channels may use the same channel $\mathbf{Y} = \mathbf{HX} + \mathbf{W}$, where $\mathbf{H}$ is a diagonal matrix for FSF channel, and $\mathbf{H} = \mathbf{FGF^{-1}}$ for DSF channel. One may verify that, if the channel is time-varying, i.e., $g_{m,k} \neq g_{n,k}$ when $m \neq k$, $\mathbf{FGF^{-1}}$ is a non-diagonal matrix whose non-zero elements surround the main diagonal. On the flip side, when the channel is time-invariant, $g_{m,k} = g_{n,k}$ for any $0 \leq m < N$ and $0 \leq k < L$, and interestingly, $\mathbf{FGF^{-1}}$ becomes a diagonal matrix, and 2.4 is equivalent to 2.5.

2.3 Problem Definition

We first focus on the DSF channel modelled in 2.1. In each OFDM symbol, the channel matrix $\mathbf{G}$ has NL non-zero elements, while there are only N observations since the received signal $\mathbf{y}$ is with length N. Unfortunately, conventional estimators like LS and LMMSE require that the observations are more than the parameters to be estimated [5], which is not the case at here. Moreover, $\mathbf{x} = \mathbf{F^{-1}X}$ may not be fully known by the receiver, since $\mathbf{X}$ may contains both data and pilots. Last but not the least, mobile broadband applications run on embedded devices and cannot afford computationally demanding channel estimation algorithms.

Problem 1: Given the model in 2.1 with $\mathbf{x} = \mathbf{F^{-1}X}$ where $\mathbf{X}$ is partially or fully known by the receiver, find out an estimate to $\mathbf{G}$, denoted as $\hat{\mathbf{G}}$, which is accurate enough to recover all the data with affordable computation complexity for embedded devices.

Next, we notice that the FSF channel model 2.3 is very simple and can be easily estimated. However, the frequency-domain channel response H_n is random and only perceivable by the receiver. This fact can be leveraged to enhance information security.

Problem 2: Given the model in 2.3, design a mechanism to enhance information security utilizing the random value H_n.

Problem 1 falls into the research area of TVCE, while *Problem* 2 belongs to physical-layer security. These two problems represent the negative side and positive side of the same physical phenomenon - the mobile broadband channel. In *Problem* 1 we mainly focus on the application of a LTE system running on a HST. *Problem* 2 finds its applications in general mobile and wireless systems, and is extremely interested in vehicular and ad hoc network (VANET) like DSRC, where channel responses change drastically over time and frequency, but the channel response during one OFDM symbol is constant [90].

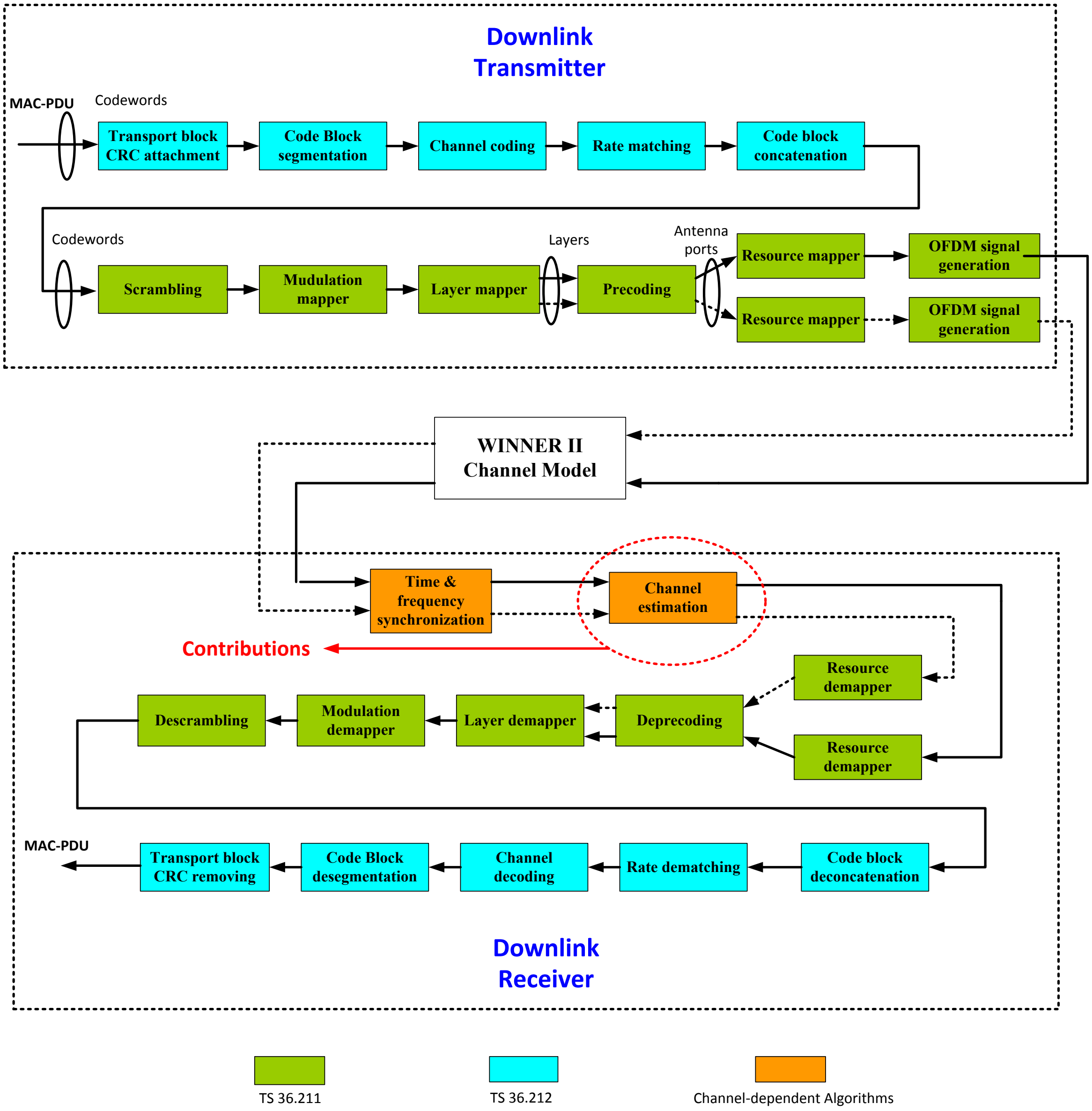

Figure 2.2: The block diagram of a LTE simulator developed to evaluate the performance of PITIA

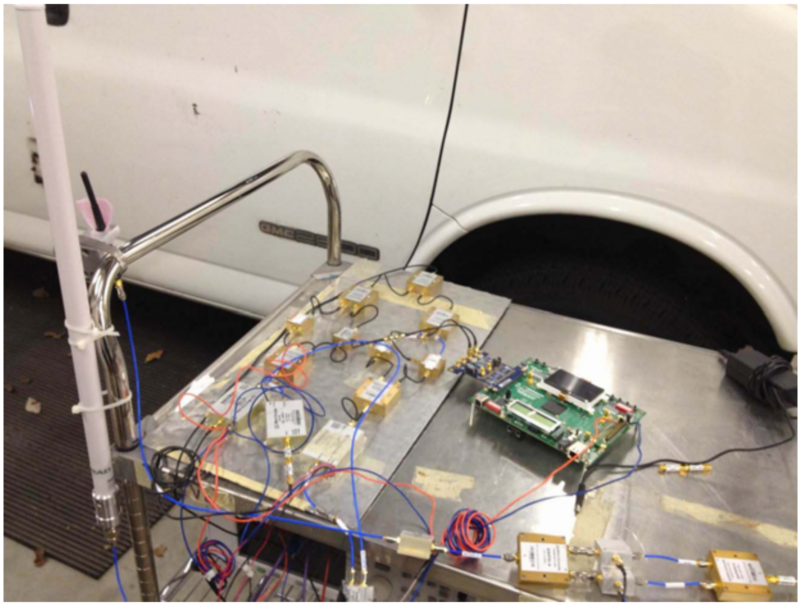

Figure 2.3: The photo of the FPGA-based prototype for PHY-CRAM

2.4 Research Methods

2.4.1 The research method for *Problem* 1

Problem 1 looks like a pure mathematical problem, but it's closely related to the physical properties of mobile broadband channels, because current statistical signal processing theories cannot directly solve equation 2.1 where unknown parameters are more than observations. Instead, researchers first examine the stochastic properties of channel model **G** through extensive channel measurement campaigns, then try to approximate **G** by simpler models where the number of unknown parameters is much less than N and estimate **G**. This is the prevailing research method for TVCE, and has four major steps: (1) channel measurements; (2) channel modelling; (3) parameter estimation; and (4) performance evaluation.

Step (1) is time consuming and expensive. Fortunately, there are already lots of such works, and their outcomes are collected by an empirical channel model named WINNER II [91], which is adopted by 3rd Generation Partnership Project (3GPP) as a standard evaluation tool for LTE channels. WINNER II provides a set of Matlab programs that generate time-domain channel responses (the matrix $\mathbf{G}$) with given conditions, for examples, speed of mobile terminal, channel type (urban, rural or hilly), frequency band, bandwidth, and antenna gains. It covers the HST scenario which is the focus of this thesis.

With the channel responses generated by WINNER II, we study the specific characteristics of HST channels, find out a mathematical model that describes $\mathbf{G}$ with fewer parameters than those in conventional models, and propose a novel algorithm PITIA to estimate these parameters.

Similar to most research works on channel estimation, the performances of PITIA are evaluated by computer based simulations. To this end, we design a set of Matlab programs (a LTE simulator) to study LTE's physical-layer according to 3GPP specification [92], as shown in figure 2.2. The wireless channel is simulated by WINNER II as described above, and channel estimation is conducted by both BEM methods and PITIA for performance comparison. We focus on the physical downlink shared channel (PDSCH) which is the major data pipe for broadband access, and only consider the single-antenna case.

2.4.2 The research method for *Problem* 2

To address *Problem* 2, we propose a novel challenge-response user authentication mechanism named PHY-CRAM, which is built upon OFDM and adopts the FSF channel model 2.3. We both develop a Matlab simulation program and design a hardware prototype to evaluate PHY-CRAM's performance, which is characterized by successful authentication rate β (the rate that a legitimate user passes authentication) and false acceptance rate α (the rate that an attacker passes authentication).

In simulations, we follow DSRC's physical-layer specification [87], and adopt a FSF channel model [93] with rural and urban scenarios. Two legitimate users are assumed to share a set of secret keys, while two attackers who do not have these keys pretend to be one of them and conduct authentication with the counterpart. Under this scenario, we derive α and β under different SNR and channel conditions.

Performance of PHY-CRAM is determined by not only the coherence time and coherence bandwidth of mobile broad channels, but also the processing delay, since PHY-CRAM utilizes the channel's reciprocity which is valid only in a very short period. Therefore, we develop a FPGA-based prototype for PHY-CRAM to ensure low processing delay, and conduct extensive real-world experiments. The RF front end is designed by discrete RF components, and the whole prototype is put on a cart to support mobility, as shown in figure 2.3. The FPGA together with RF front end serve as a software-defined radio (SDR) that is also used for many other research works . Two sets of the prototype perform as legitimate users, while another two sets perform as a naive attacker and a smart attacker, respectively. Data frames for authentication are generated by FPGA at transmitters, while the baseband I/Q signals at receivers are captured by an oscilloscope. These I/Q signal samples are then copied to a computer which runs a Matlab program to get α and β. The Matlab simulation program, which is a float-point program by default, is converted to a fixed-point one and serves as the golden reference for FPGA design.

CHAPTER 3

Channel Estimation in HST Environments

3.1 Overview

With the rapid deployment of HST's around the world and development of intelligent transportation systems, providing broadband wireless communications between a HST and infrastructure is becoming indispensable to support various attractive services, such as Internet access, on-board data services, and multimedia advertisements, etc [94, 95]. The most prospective solutions for the broadband communication are Long Term Evolution (LTE) [92] and Worldwide Interoperability for Microwave Access (WiMax) [96], which adopt OFDM due to its immunity to multipath, especially when the communication range is long. However, the high-mobility feature of HST's introduces DSF channel which is very hard to estimate.

Since FSF is inevitable in broadband OFDM systems, a HST channel is considered as a DSF channel when Doppler spread is comparable to subcarrier spacing. As an example, in a LTE system which will be equipped on HST's in many countries [97, 98], subcarrier spacing is 15 kHz while Doppler spread is 0.84 kHz when the travelling speed of the HST is 350 km/h; therefore, the HST channel is considered as time-varying by this LTE system. It is well-known that, time-varying channels cause ICI's in OFDM systems and increase the noise floor if a traditional single-tap channel equalizer is adopted [99].

Time-varying channels contain much more parameters than those of time-invariant channel. When an OFDM system with N subcarriers runs in a time-varying channel with L taps (L resolvable multipath components), the general time-varying channel matrix $\mathbf{G}$ contains NL unknown parameters, which is much more than the observations at the receiver (at most $N+L$ observations for each OFDM symbol). This challenge is formulated as $Problem$ 1 in chapter 2. Reducing the number of channel parameters is essential for TVCE, but is also risky since fewer parameters often lead to larger modelling error. To address this issue, we use the specific features of HST channels to reduce the number of channel parameters, which are then estimated by a novel algorithm named PITIA.

The most important feature of HST channels is that, there exists only one Doppler shift on each resolvable multipath component in most cases, and this fact is validated by WINNER II channel model. Motivated by this finding and the necessity to reduce the number of channel parameters, we propose a novel TVCE algorithm for HST channels based on this simplified channel model. The major challenge introduced by this channel model is to estimate non-linear parameters - Doppler shifts. To this end, we approximate the channel by a bunch of time-invariant channels whose CIR's can be estimated through pilots, and name this technique as PIece-wise Time-Invariant Approximation (PITIA). Then the variations of these CIR's derive both Doppler shifts and complex channel gains for all channel taps, from which $h(t,\tau)$ is reconstructed. In other words, PITIA decouples FSF and time-varying effect in HST channels and estimates them in two separate steps, each with very simple operations. The computational complexity of PITIA is $O(NL)$ which is affordable for most OFDM receivers.

Since PITIA reduces the number of channel parameters without increasing modelling error, the proposed algorithm is expected to get better performance, and this expectation is validated by our LTE simulator. Specifically, PITIA's performance is better than and comparable to the performances of typical BEM methods [58] in high SNR regime and low SNR regime, respectively, while LTE channels have clear line-of-sight (LOS) and enjoy high SNR most of time. Although the proposed algorithm is designed for HST channels, it is also suitable for other applications with the following three channel characteristics: short delay spread, large Doppler spread, and only one Doppler shift on each resolvable multipath component.

3.2 The HST Channel Model

The wireless channel between the infrastructure and a HST is a typical time-varying channel given in (2.1) with specific characteristics. Based on the field testing and channel models found in the literature, we customize the general time-varying channel model for HST channels, and set up the foundation for PITIA.

The measurement campaigns reported in [97] show that, HST channels at 2.1 GHz frequency band have very small root-mean-squared (RMS) delay spread, typically smaller than half microsecond. Consequently, $L = 16$ is large enough in the model given in section 2, when baseband sampling rate is 30.72 MHz according to LTE specifications. This is due to the fact that, most HST systems operate in rural or open areas. When a HST reaches a city with an urban channel, it slows down and becomes a normal-speed train; as a result, the “time-varying channel" degrades to a time-invariant channel. The hilly channel is an exceptional case, where the train travels along a big mountain, travelling velocity is very high and delay spread is large. We focus on the HST channels in open and rural areas where L is small, while considering the hilly channel as future works.

We further evaluate the features of HST channels through WINNER II channel model. This channel model not only validates the fact of small delay spread, but also reveals a very important characteristic that, there exists only one Doppler shift on most channel taps. To show this feature, we generate $g_{n,m}$ for $n = 0, ..., 2047$ and $m = 0, ..., 14$ using the simulation code provided by WINNER II channel model with HST scenario, and examine the phase changes on each channel tap (indexed by m).

Figure 3.1 shows a snapshot of $g_{n,m}$'s phases, which change linearly over m. Since the slope of phase changes denotes Doppler shift, a constant slope means that there is only one Doppler shift. This characteristic can be explained by two reasons. Firstly, the wireless channels in open and rural areas contain limited number of multipath components, and there is very little chance that multiple multipath components fall into the same channel tap. Secondly, in case that some multipath components collide with each other, they likely come from the reflectors located close to each other and suffer from similar Doppler shifts. When several multipath components have equal time delay and similar Doppler shifts, they can be considered as a single but stronger multipath component.

With this feature, there is no need to identify the wireless channel's Doppler spectrum, for example, the bell-shaped Doppler spectrum predicted by Jakes model [100]; instead, the time-varying channel can be represented by the following simple model

$$g_{n,m} = g_m e^{j2\pi\delta_m n/N} \tag{3.1}$$

where $g_m := g_{0,m}$ denotes the complex channel gain at time index 0, and δ_m denotes the normalized Doppler shift with respect to B_S, i.e., $\Delta f_m / B_S$ where Δf_m denotes the Doppler shift in hertz, all for channel tap m. This channel model shares the same form as the ones adopted in [6, 7], where the time-varying channel is solely determined by g_m and δ_m for $m = 0, ..., L-1$; however, these algorithms suffer from high complexity due to the nonlinearity of this model. PITIA introduces a much simpler algorithm to estimate these $2L$ channel parameters in the next section.

Note that in the channel model (3.1), the delay of each multipath component is represented by index m implicitly. When channel tap m_1 contains a multipath component, g_{m_1} is a non-zero value; on the contrary, when channel tap m_2 contains no multipath, g_{m_2} equals to 0, and the phase of g_{n,m_2}

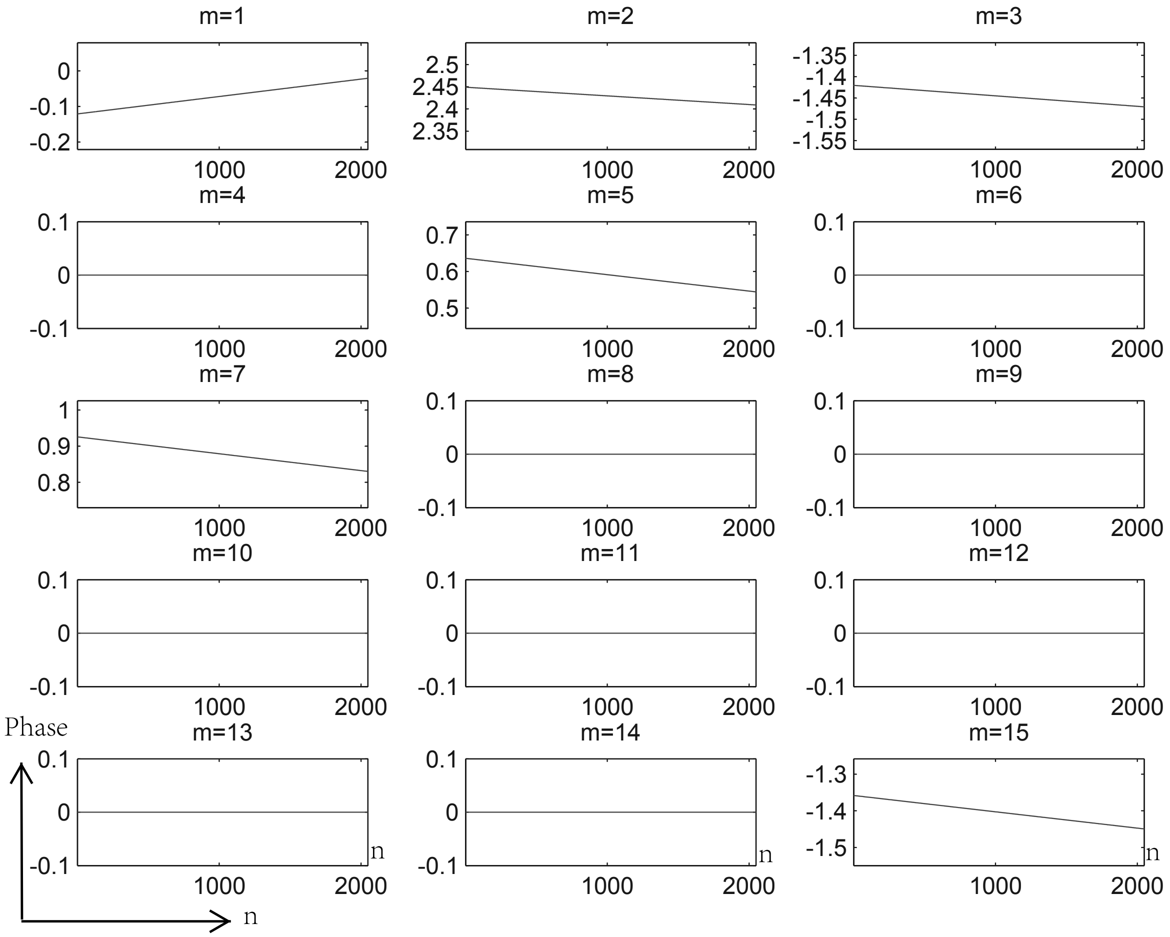

Figure 3.1: Phases of the time-varying channel response on channel taps 1 to 8 derived from WINNER II channel model; x-coordinate denotes n while y-coordinate denotes the phase of $g(n,m)$ for a given number of m

.

is defined as 0 too, as shown in figure 3.1.

Given the channel model in (3.1), estimating a time-varying channel is equivalent to estimating $2L$ parameters g_m and δ_m for $m = 0, ..., L-1$. As a comparison, BEM methods model the channel by $L(Q+1)$ parameters where $(Q+1)$ denotes the number of basis functions. Note that Q is mainly determined by f_M, instead of the number of distinguished Doppler shifts in each multipath component. In HST channels where f_M is high, Q is usually larger than 1. As a result, the number of channel parameters in BEM methods is larger than $2L$. Moreover, for a linear system with fixed number of observations, fewer parameters lead to better NMSE performance [5]. Therefore, the proposed channel estimation algorithm based on a simplified channel model customized for HST channels is expected to outperform BEM methods.

3.3 The Proposed Algorithm

3.3.1 Piece-wise time-invariant approximation

PITIA is inspired by the specific features of HST channels. Consider the channel model (3.1) where Doppler shifts δ_m for all m dominate the time-varying characteristic of the wireless channel. Note that $\delta_m \leq f_M$ and in most practical OFDM systems the normalized Doppler shift with respect to subcarrier spacing $f_M < 0.1$. As an example, f_M equals to 0.064 in a LTE system operating at 2.6 GHz (which is the highest frequency band allocated for LTE in Europe and Asia) on a HST with travelling speed 400 km/h. Moreover, the maximum delay spread L is in the order of $0.1N$ for most practical systems, and is in the order of $0.01N$ in HST channel according to the analysis in subsection 3.2 (considering that $N = 2048$ according to LTE specification, and $L = 16$). Therefore, phase changes caused by Doppler shifts during time span L, which is $2\pi\delta_m L/N$, is in the order of 1E-3 and can be neglected. This property serves as the foundation of PITIA.

In order to utilize this property, $\mathbf{G}$ is partitioned into N/LK_1 matrixes from top to bottom, each of which has the size $LK_1 \times N$ where $K_1 = 2^{K_0}$ where K_0 is a positive integer. From (2.1) we have

$$\mathbf{y}^{(u)}{=}\mathbf{G}^{(u)}\mathbf{a}{+}\mathbf{n}^{(u)} \tag{3.2}$$

where $\mathbf{y}^{(u)} := [y_{uLK_1},...,y_{(u+1)LK_1-1}]^T$, $\mathbf{n}^{(u)} := [n_{uLK_1},...,n_{(u+1)LK_1-1}]^T$ and $\mathbf{G}^{(u)} := [\mathbf{G}^T_{uLK_1},...,\mathbf{G}^T_{(u+1)LK_1-1}]^T$ where $\mathbf{G}_n$ denotes the n^{th} row of $\mathbf{G}$, for $u = 0,...,N/LK_1 - 1$. Given any u with $0 < u < N/LK_1 - 1$, let's rewrite (3.2) in the following form

$$\begin{bmatrix} y_{uLK_1} \\ \cdots \\ y_{(u+1)LK_1-1} \end{bmatrix}$$
$$= \begin{bmatrix} \cdots & 0 & g_{uLK_1,L-1} & & \cdots & & g_{uLK_1,0} & 0 & \cdots & \\ & & & & \cdots & & & & & \\ & \cdots & & 0 & g_{(u+1)LK_1,L-1} & \cdots & & g_{(u+1)LK_1,0} & 0 & \cdots \end{bmatrix} * \begin{bmatrix} a_0 \\ \cdots \\ a_{N-1} \end{bmatrix} + \mathbf{n}^{(u)} \tag{3.3}$$

and make an approximation that $g_{n,m} = g_{(u+1/2)LK_1,l}$ for $n = uLK_1,...,(u+1)LK_1 - 1$ and $m = 0,...,L-1$, as stated in the beginning of this section. Then (6) becomes

$$\begin{bmatrix} y_{uLK_1} \\ \cdots \\ y_{(u+1)LK_1-1} \end{bmatrix} = \begin{bmatrix} a_{uLK_1} & \cdots & a_{uLK_1-L+1} \\ & \cdots & \\ a_{(u+1)LK_1} & \cdots & a_{(u+1)LK_1-L+1} \end{bmatrix} \begin{bmatrix} g_{(u+\frac{1}{2})LK_1,0} \\ \cdots \\ g_{(u+\frac{1}{2})LK_1,L-1} \end{bmatrix} + \mathbf{n}^{(u)} \tag{3.4}$$
$$\overset{def}{=} \mathbf{A}^{(u)}\mathbf{g}^{(u)} + \mathbf{n}^{(u)}.$$

Note that (3.4) only holds for $u = 1,...,N/LK_1 - 1$; when $u = 0$, all the negative indices on a should be added by N. The physical meaning of (3.4) is that, a time-varying channel over time period N is approximated by N/LK_1 time-invariant channels with CIRs $\mathbf{g}^{(u)}$ for $u = 0,...,N/LK_1 - 1$, as shown in figure 3.2. The channel response within time index 0 to $LK_1 - 1$ is considered to be constant and approximated by CIR $\mathbf{g}^{(0)}$, while channel response within time index LK_1 to $2LK_1 - 1$

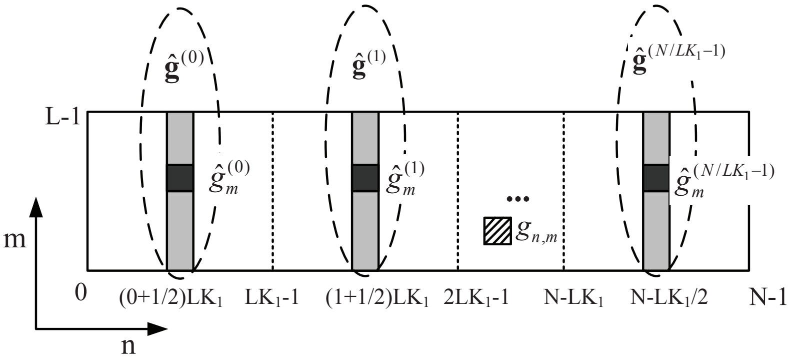

Figure 3.2: The basic principle of PITIA: the time varying channel $g_{n,m}$ is approximated by a series of $\hat{\mathbf{g}}^{(u)}$

.

is again considered to be constant (but may be different from the previous one) and approximated by CIR $\mathbf{g}^{(1)}$, and so on. This technique is called PITIA.

In this technique, LK_1 determines the duration of time-invariant channels used to approximate the time-varying channel. We consider K_1 as an important design parameter, since it determines both modelling error and anti-noise ability. Larger K_1 results in larger modelling error and better anti-noise ability and vice versus. When $K_1 = N/L$, PITIA approximates the time-varying channel by a single time-invariant channel, and (3.4) downgrades to the conventional channel estimation algorithms in time-invariant channels. Moreover, K_1 must be larger than or equal to 1, so that $\mathbf{g}^{(u)}$ can be estimated by the method below.

If $\mathbf{a}$ is known by the receiver, $\mathbf{A}^{(u)}$ is also known, and $\mathbf{g}^{(u)}$ can be derived from the LS estimator [5]:

$$\hat{\mathbf{g}}^{(u)} = ((\mathbf{A}^{(u)})^H \mathbf{A}^{(u)})^{-1} (\mathbf{A}^{(u)})^H \mathbf{y}^{(u)} \tag{3.5}$$

where $((\mathbf{A}^{(u)})^H \mathbf{A}^{(u)})^{-1} (\mathbf{A}^{(u)})^H$ can be derived offline, and the estimator enjoys low complexity. The MMSE estimator [5] and LMMSE estimator [28] are not considered to ensure low computation complexity.

All the channel parameters g_m and δ_m for $m = 0, ..., L-1$ can be derived from $\hat{\mathbf{g}}^{(u)}$, and the whole time-varying channel $\mathbf{G}$ can be reconstructed.

Note that the receiver may not fully know $\mathbf{a}$ since it may contain both pilots and data symbols. To address this issue, we discuss the pilot allocation scheme in the next section, which is followed by the method to estimate $\hat{\mathbf{g}}^{(u)}$ through pilots.

3.3.2 Pilot allocation schemes

Two different pilot allocation schemes are widely used in pilot assisted OFDM systems: comb-type and block-type, as shown in Fig. 1 (a) and (b) respectively, where solid ellipses and rotundities denote pilot subcarriers, while circles denote null subcarriers. All blank areas are occupied by data symbols.

When block-type pilots exist, $\mathbf{A}^{(u)}$ is known by the receiver, $\hat{\mathbf{g}}^{(u)}$ in pilot blocks can be derived from (3.5) directly, and $\hat{\mathbf{g}}^{(u)}$ in data blocks can be derived from interpolation. However, when comb-type pilots are adopted, $\mathbf{A}^{(u)}$ cannot be derived directly, and this situation is further discussed below.

We denote the distance between two adjacent combs, the width of each pilot cluster, and the width of each null subcarrier group as N_b, N_p and N_f, respectively, as shown in figure 3. Moreover, the number of null subcarriers used for channel estimation at the receiver is denoted as $N_f^{(R)}$, and usually $0 \leq N_f^{(R)} \leq N_f$. When $N_p = 1$, the corresponding pilot pattern is referred to as frequency-domain Kronecker delta (FDKD) [63], as shown in figure 3(c). It is very important to adapt these three parameters to channel characteristics. In channels with large delay spread and dense multipath, N_b must be small, while channels with large Doppler spread favour large N_f. Moreover, pilots and null subcarriers should not occupy all subcarriers, i.e., $N_p + 2N_f < N_b$. As a result, N_b, N_p and N_f may vary significantly for OFDM systems working in different channel environments.

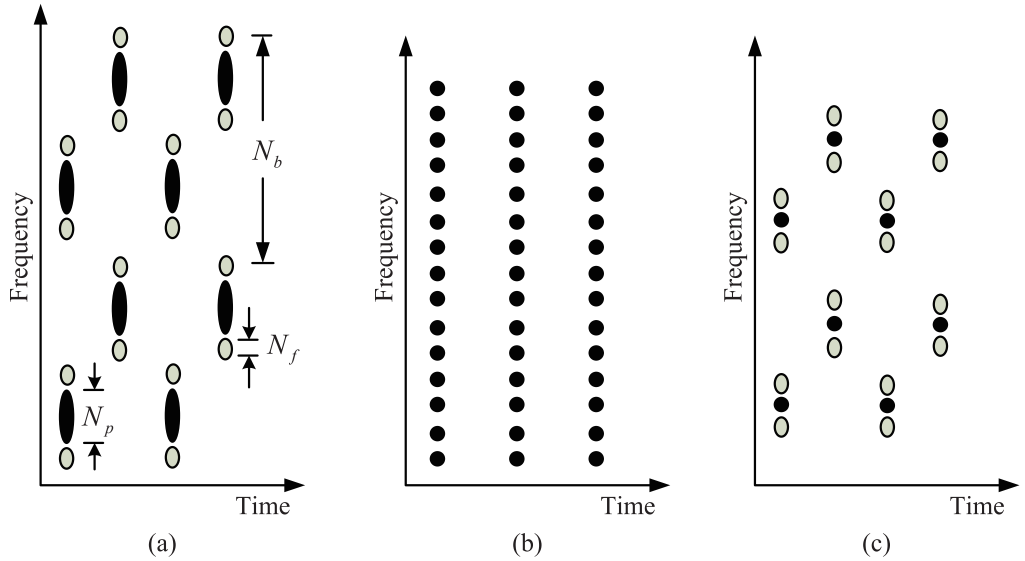

Figure 3.3: Comb-type (a), block type (b) and FDKD (c) pilot allocation schemes

HST channels with small delay spread and large Doppler spread favour large N_b and large N_f.

3.3.3 Channel estimation through pilots

Although **a** is partially known by the receiver, $\hat{\mathbf{g}}^{(u)}$ can still be estimated by the method introduced in this section, which has been published in [16] in part.

Define Ξ_V as the set of indices of the subcarriers used for channel estimation. Then the time-domain pilot signal $\mathbf{a_p} := [b_0, ..., b_{N-1}]^T$ is derived from $b_n = \sum_{k \in \Xi_V} X_k e^{j2\pi nk/N}$ where $X_k = \sum_{n=0}^{N-1} a_n e^{-j2\pi nk/N}$, or equivalently

$$\mathbf{a_p} = \mathbf{F^{-1} Q_V F a} \tag{3.6}$$

where **F** denotes the $N \times N$ Vandermonde matrix whose j^{th} element at the i^{th} line equals to ω^{ij}

with $\omega := exp(-2\pi i/N)$. Moreover, $\mathbf{Q_V} := diag(e_0, ..., e_{N-1})$ where

$$e_i = \begin{cases} 0, \ if \ i \notin \Xi_V \\ 1, \ if \ i \in \Xi_V \end{cases}, for \ i = 0, ..., N-1.$$

The matrix $\mathbf{F^{-1}Q_VF}$ serves as a comb-type filter that rejects data symbols and accepts pilots. Similarly, the time-domain data signal is obtained by

$$\mathbf{a_d} = \mathbf{F^{-1}}(\mathbf{I}_N - \mathbf{Q_V})\mathbf{Fa} \tag{3.7}$$

Obviously $\mathbf{a} = \mathbf{a_d} + \mathbf{a_p}$, and from (2.1) we get

$$\mathbf{y} = \mathbf{G}(\mathbf{a_d} + \mathbf{a_p}) + \mathbf{n}. \tag{3.8}$$

Applying the same filter $\mathbf{F}^{-1}\mathbf{Q_VF}$ on $\mathbf{y}$ we get

$$\begin{aligned} \mathbf{y_p} &:= \mathbf{F}^{-1}\mathbf{Q_VFy} \\ &= \mathbf{F^{-1}Q_VFGa_p} + \mathbf{F^{-1}Q_VFGa_d} + \mathbf{F^{-1}Q_VFn}. \end{aligned} \tag{3.9}$$

Define $\mathbf{M} := \mathbf{F}^{-1}\mathbf{Q_VFGa_d}$ which is the second term in (3.9) and represents the interference of data over pilots. From (3.7) we have $\mathbf{M} = \mathbf{F^{-1}Q_V}(\mathbf{FGF}^{-1})(\mathbf{I}_N - \mathbf{Q_V})\mathbf{Fa}$ where $\mathbf{FGF}^{-1}$ denotes the frequency-domain channel matrix. When Doppler spread equals to 0, $\mathbf{FGF}^{-1}$ is a diagonal matrix, and $\mathbf{M} = \mathbf{0}$ accordingly. When Doppler spread is non-zero, $\mathbf{FGF}^{-1}$ is close to a diagonal matrix, the values of whose items diminish rapidly around the main diagonal. Here we consider $\mathbf{M}$

as extra noise for simplicity. Then (3.9) becomes

$$\begin{aligned}\mathbf{y_p} =& \mathbf{F^{-1}Q_VFGa_p}+\mathbf{n_p}\\ =& \mathbf{F^{-1}Q_V(FGF^{-1})Q_VFa}+\mathbf{n_p}\\ \approx& \mathbf{F^{-1}(FGF^{-1})Q_VQ_VFa}+\mathbf{n_p}\\ =& \mathbf{GF^{-1}Q_VFa}+\mathbf{n_p}\\ =& \mathbf{Ga_p}+\mathbf{n_p}\end{aligned} \tag{3.10}$$

where

$$\begin{aligned}\mathbf{n_p} :=& \mathbf{F}^{-1}\mathbf{Q_VFGa_d}+\mathbf{F}^{-1}\mathbf{Q_VFn}\\ :=& \mathbf{e_p}+\mathbf{w_p}\end{aligned} \tag{3.11}$$

denotes the sum of noise $\mathbf{w_p}$ at pilot subcarriers and interference $\mathbf{e_p}$ coming from data symbols. The reason for the approximation in (3.10) is that, $\mathbf{FGF}^{-1}$ is close to a diagonal matrix, and for two diagonal matrices $\mathbf{Q}_A$ and $\mathbf{Q}_B$, $\mathbf{Q}_A\mathbf{Q}_B = \mathbf{Q}_B\mathbf{Q}_A$. Adopting the same operations as shown in section III.A, we have

$$\mathbf{y_p}^{(u)}=\mathbf{G}^{(u)}\mathbf{a_p}+\mathbf{n_p}^{(u)} = \mathbf{P}^{(u)}\mathbf{g}^{(u)}+\mathbf{n_p}^{(u)} \tag{3.12}$$

where $\mathbf{y_p}^{(u)} := [y_{\mathbf{p},uLK_1},\ldots,y_{\mathbf{p},(u+1)LK_1-1}]^T$, $\mathbf{n_p}^{(u)} := [n_{\mathbf{p},uLK_1},\ldots,n_{\mathbf{p},(u+1)LK_1-1}]^T$ and

$$\mathbf{P}^{(u)} := \begin{bmatrix} b_{uLK_1} & \cdots & b_{uLK_1-L+1}\\ & \cdots & \\ b_{(u+1)LK_1} & \cdots & b_{(u+1)LK_1-L+1}\end{bmatrix} \tag{3.13}$$

where $y_{\mathbf{p},m}$ and $n_{\mathbf{p},m}$ denote the m^{th} element in $\mathbf{y_p}$ and $\mathbf{n_p}$, respectively, and $\mathbf{P^{(u)}}$ is determined solely by pilots. Then $\mathbf{g}^{(u)}$ can be estimated by

$$\hat{\mathbf{g}}^{(u)} = ((\mathbf{P}^{(u)})^H \mathbf{P}^{(u)})^{-1} (\mathbf{P}^{(u)})^H \mathbf{y}_{\mathbf{p}}^{(u)}. \tag{3.14}$$

3.3.4 Channel reconstruction

Let $\hat{g}_m^{(u)}$ denote the m^{th} element in $\hat{\mathbf{g}}^{(u)}$. For a given u, $\hat{\mathbf{g}}^{(u)}$ denotes the L-tap CIR at time index $(u+1/2)LK_1$, or in other words, the L non-zero elements at the $(u+1/2)LK_1$'th row of matrix $\mathbf{G}$ defined in (2.2). For a given m on the other hand, the function $\hat{g}_m^{(u)}$ over u reveals the variation of channel tap m over time. These relationships are shown in figure 2.

There are various ways to derive all the channel parameters g_m and δ_m from $\hat{\mathbf{g}}_m^{(u)}$, and the whole channel matrix $\mathbf{G}$ can be reconstructed. Since the main purpose of this work is to introduce piecewise time-invariant approximation, we only demonstrate a simple and effective method here. Performance improvement may be achieved if more advanced approaches are adopted in future works.

We denote the phase of $\hat{g}_m^{(u)}$ as $\angle\hat{g}_m^{(u)}$ for $u = 0, 1, ..., N/LK_1 - 1$, and plot a snapshot of these values derived in a very noisy channel in figure 4. Since these phase shifts are caused by a single Doppler shift, they can be regressed by a straight line whose slope V_m determines the Doppler shift δ_m, and whose start point Q_m determines the phase of g_m at $n = 0$. Such linear regression can be conducted for each $m = 0, 1, ..., L-1$, while g_m and δ_m are hereby estimated by

$$\hat{\delta}_m = \frac{1}{LK_1} \frac{V_m}{2\pi} \tag{3.15}$$

and

$$\hat{g}_m = \frac{LK_1}{N} e^{jQ_m} \sum_{u=0}^{N/LK_1-1} |\hat{g}_m^{(u)}| \tag{3.16}$$

In (3.15), there is a coefficient $1/LK_1$ because u at x-coordinate in figure 4 grows LK_1 times

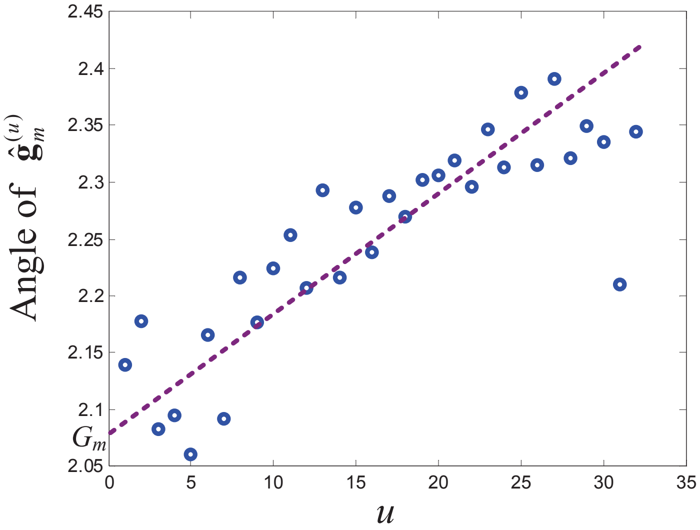

Figure 3.4: Phases of $\hat{\mathbf{g}}_m^{(u)}$ for $u = 0, 1, ..., N/LK_1 - 1$; the phase of g_m and the Doppler shift δ_m are derived from the start point G_m and the slope of the dashed straight line that fits all the data points with least squares approach, respectively.

faster than n in the channel model (3.1). The amplitude of g_m is estimated by averaging the amplitudes of $\hat{g}_m^{(u)}$ over u in (3.16), while the phase of g_m is estimated by Q_m directly. At here, two parameters $\hat{\delta}_m$ and $\hat{g}_m$ are derived from $N/(LK_1)$ values, i.e., $\hat{g}_m^{(u)}$ $u = 0, 1, ..., N/LK_1 - 1$, and there exists much redundancy since both L and K_1 are much smaller than N. As a result, the noise is reduced significantly in this estimation process.

Finally, the time-varying channel response $g_{n,m}$ is estimated by

$$\hat{g}_{n,m} = \hat{g}_m e^{j2\pi\hat{\delta}_m n} \tag{3.17}$$

and the channel matrix $\mathbf{G}$ can be reconstructed according to (2.2).

Note that the operator $\angle$ makes the proposed TVCE algorithm non-linear. We will evaluate the performance of this non-linear operation in section 3.4.

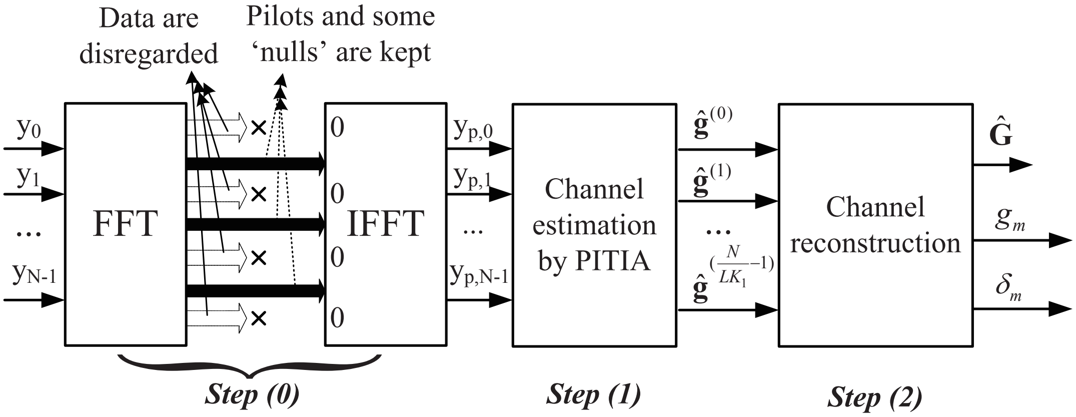

Figure 3.5: The workflow of PITIA

3.3.5 The overall workflow

The overall workflow of the proposed algorithm is shown in figure 5. Firstly, observations $\mathbf{y}$ are sent to a FFT processor, and symbols on subcarriers allocated for pilots and (part of) nulls are sent to an IFFT processor, with zeros inserted on data subcarriers. These operations, called step (0), serve as a comb-type filter that extracts the pilots for channel estimation. The outputs of step (0) are denoted as $\mathbf{y_p}$ which derive $\hat{\mathbf{g}}^{(u)}$ as CIR samples of the time-varying channel according to the estimator (3.14) in step (1). Finally, in step (2), all $\hat{\mathbf{g}}^{(u)}$ for $u = 0, 1, ..., N/LK_1 - 1$ derive the $2L$ channel parameters g_m and δ_m by (3.15) and (3.16), respectively, and the estimated channel matrix $\hat{\mathbf{G}}$ can be constructed according to (3.17). We refer to this step as "channel reconstruction".

We use the term PITIA to represent only step (1) while introducing the proposed algorithm, and use it to represent the whole algorithm during performance comparison with conventional methods.

3.4 Performance Analysis

The performance of PITIA is determined by various factors which are discussed in this section.

First of all, the comb-type filter in PITIA cannot completely isolate pilots and data symbols, and pilots used for channel estimation are interfered by data symbols. This is because the power of each subcarrier is dispersed over a large frequency band in high-mobility environments. We model these interference as extra AWGN noise $\mathbf{e_p}$ in (3.11). This is not an inherent problem of PITIA, since BEM methods also suffer from the same issue. These interferences may be resisted by advanced signal processing techniques [58, 64, 72] regardless of the channel estimation algorithms (either PITIA or BEM) used. To conduct fair comparison, we assume that BEM methods also treat these interferences as extra AWGN noise, so that both types of methods have similar computation complexity.

Secondly, PITIA has an modelling error introduced by the operation to approximate the time-varying channel during LK_1 samples by a time-invariant channel. As shown in the next subsection, this error is determined by $f_M LK_1$. This property is different from that of BEM, whose modelling error is determined only by f_M if basis functions are given. As a result, PITIA is able to reduce modelling error in channels with small delay spread, and fits HST channels well. We will give the upper bound of the modelling error in PITIA, and compare it with the PWLA approach [70] and BEM methods with LS estimator [58].

Finally, the modelling error in step (2) arises when multiple multipath components with distinguished Doppler shifts fall into a single channel tap. We ignore this situation in theoretical studies, but evaluate its effect using WINNER II channel model through simulations. The overall performance of PITIA in noisy HST channels is evaluated by the LTE simulator introduced in section 2.4.1, where the ground truth of channel responses are derived from either the channel model from (3.1) or WINNER II channel model.

3.4.1 The modelling error of PITIA and BEM

Modelling error refers to the error introduced during channel approximation, and is determined solely by the method to simplify a time-varying channel rather than SNR. The normalized modelling errors σ_M^2 of both PITIA and BEM with respect to the energy of $|g_{n,m}|$ are evaluated by theoretical studies and/or simulations in this subsection.

As shown in figure 2, the HST channel $g_{n,m}$ modelled by (3.1) during the time span from uLK_1 to $(u+1)LK_1 - 1$ is approximated by $g_{(u+1/2)LK_1,m}$, for $u = 0,...,N/LK_1 - 1$ and $m = 0,...,L-1$. Therefore, the normalized modelling error of PITIA is given by

$$\begin{aligned}
&\sigma^2_{M,PITIA} \\
&:= \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} |g_{uLK_1+k,m} - g_{(u+\frac{1}{2})LK_1,m}|^2 \\
&= \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} |g_m e^{jp_{m,k,u}} - g_m e^{jq_{m,k,u}}|^2 \\
&= \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} |g_m||e^{jp_{m,k,u}} - e^{jq_{m,k,u}}|^2
\end{aligned} \tag{3.18}$$

where $p_{m,k,u} := 2\pi\delta_m(uLK_1+k)/N$, $q_{m,k,u} := 2\pi\delta_m(u+1/2)LK_1)/N$ and $P_H := \sum_{n=0}^{N-1}\sum_{m=0}^{L-1} |g_{n,m}|^2$.

Lemma 1: When $\pi/2 > |c_4 - c_3| \geq |c_2 - c_1|$, $|e^{jc_4} - e^{jc_3}|^2 \geq |e^{jc_2} - e^{jc_1}|^2$.

This lemma is simple and we omit the proof for it.

Proposition 1 : The upper bound of $\sigma^2_{M,PITIA}$ defined in (3.18) is well approximated by $(\pi f_M LK_1/N)^2$.

Proof. For $k = 0,...,LK_1 - 1$, $|p_{m,k,u} - q_{m,k,u}| \leq \pi\delta_m LK_1/N \leq \pi f_M LK_1/N$. According to the channel model given in section 2, $\pi f_M LK_1/N$ is in the order of 1E-3 and much smaller than $\pi/2$.

According to *Lemma* 1 we have

$$
\begin{aligned}
&\sigma^2_{M,PITIA} = \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} g_m |e^{jp_{m,k,u}} - e^{jq_{m,k,u}}|^2 \\
&\leq \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} g_m |e^{j\pi f_M LK_1/N} - e^{j0}|^2 \\
&\approx \frac{1}{P_H} \sum_{u=0}^{\frac{N}{LK_1}-1} \sum_{k=0}^{LK_1-1} \sum_{m=0}^{L-1} g_m (\pi f_M LK_1/N)^2 \\
&= (\pi f_M LK_1/N)^2
\end{aligned}
\tag{3.19}
$$

□

It is shown in *Proposition* 1 that, the modelling error of PITIA is quadratically proportional to Doppler shift f_M, the maximum delay spread L in number of samples, and the design parameter K_1. Therefore, PITIA favours the channels with small L, like HST channels.

The upper bound in *Proposition* 1 as a function of f_M is plotted in figure 6, together with the modelling errors of PITIA, PWLA, GCE-BEM [53] and DLP-BEM [61] derived by simulations. For GCE-BEM, Q must be odd and no smaller than 2, while for DLP-BEM proposed in [61], $Q = 2$ is large enough for most practical OFDM systems. The simulations use the channel model in (3.1) as ground truth with $N = 2048$ and $L = 16$. It is shown that the modelling error of BEM with a large Q enjoys small modelling error, for example, DLP-BEM with $Q = 2$ and GCE-BEM with $Q = 4$. However, since the number of BEM coefficients equals to $L(Q+1)$, larger Q leads to more channel parameters, and the estimation performance in noisy environments would be degraded.

PWLA and DLP-BEM with $Q = 1$ approximate the channel by $2L$ parameters like PITIA does. Compared to these two methods, PITIA shows smaller modelling error when $K_1 = 1$. When $K_1 = 2$ and $K_1 = 4$, PITIA outperforms them when $f_M > 0.02$ and $f_M > 0.04$, respectively, as shown in figure 6. Therefore, K_1 controls the balance between the modelling error and the error caused by noises and interferences. Smaller K_1 leads to smaller modelling error and vice versus, while its optimal value is evaluated in sections 3.4.3 and 3.4.4. When $Q = 1$, DLP-BEM is equivalent to PWLA which suffers from large modelling error in HST channels with large Doppler shifts. As a result, DLP-BEM should set $Q \geq 2$ in order to estimate HST channels, and the number of BEM coefficients is equal to or larger than $3L$.

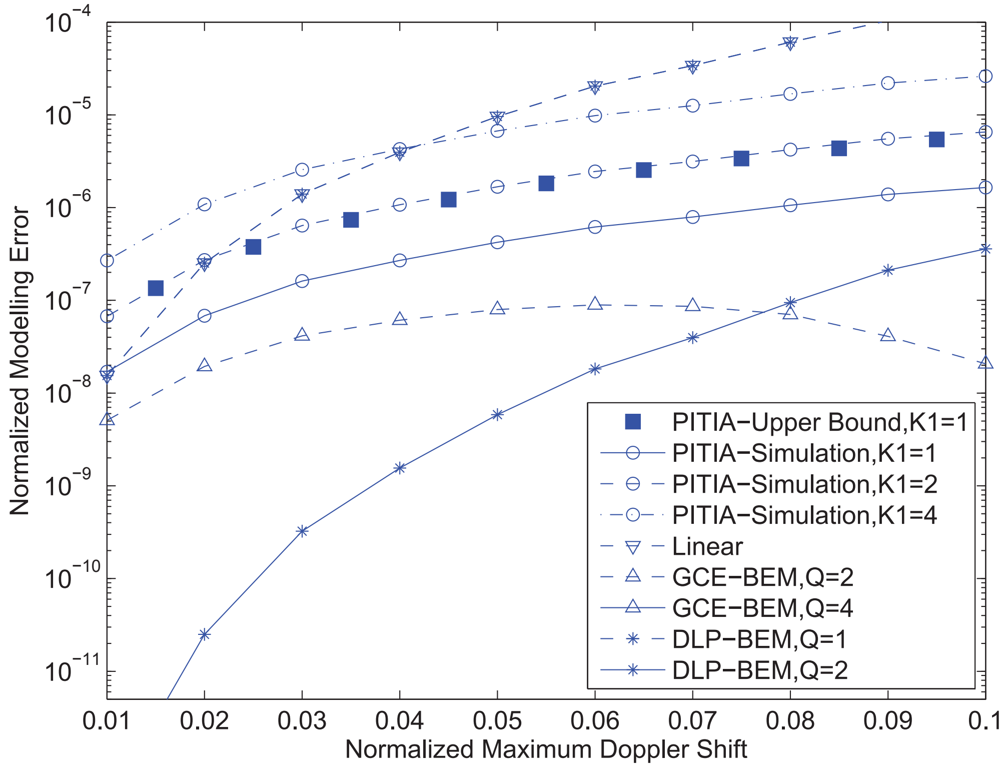

Figure 3.6: Modelling errors of PITIA, piece-wise linear approximation, GCE-BEM and DLP-BEM, with $N = 2048$ and $L = 16$; the curve labelled with “linear" denotes “piese-wise linear approximation".

3.4.2 Complexity analysis

As shown in figure 5, PITIA contains three functional blocks: FFT, CIR estimation, and channel reconstruction through linear regression. The complexity of FFT operation is in the order of $O(Nlog(N))$. CIR estimates are derived from (3.5) with complexity $O(NL)$, which is slightly larger than $O(Nlog(N))$. The complexity of linear regression is around $O(N/K_1)$ and is negligible. Therefore, the overall complexity of PITIA is at the level of $O(NL)$ which is similar to that of BEM methods.

3.4.3 The overall performance

The overall performances of PITIA and BEM methods are characterized by normalized mean squared error (NMSE) σ^2_{All}, which is defined as

$$\sigma^2_{All} := \frac{1}{P_H} \sum_{n=0}^{N-1} \sum_{m=0}^{L-1} |g_{n,m} - \hat{g}_{n,m}|^2 \tag{3.20}$$

where $\hat{g}_{n,m}$ denotes the channel estimates. This expression contains channel modelling error σ^2_M, the estimation error σ^2_{NI} caused by noise and interference, and extra errors σ^2_{Extra} introduced by error propagation along multiple estimation steps and the non-linear operation to get $\angle \hat{g}^{(u)}_m$. In other words, σ^2_{All} is approximated by

$$\sigma^2_{All} = \sigma^2_M + \sigma^2_{NI} + \sigma^2_{Extra}. \tag{3.21}$$

The definition in (3.20) is equivalent to the definition of interference plus noise to signal ratio (INSR), or the reciprocal of signal to interference plus noise ratio (SINR), if we consider channel estimates as “signals”. According to [5], for a linear system with N_o independent observations and

p variables, the LS estimator enhances the SINR of these p variables by N_o/p times, or in other words, reduces the INSR by N_o/p times, given that the interferences follow Gaussian distribution. For BEM methods, N_o equals to the number of subcarriers used for channel estimation, which equals to the size of Ξ_V denoted as N_V, while p equals to $L(Q+1)$. As a result, σ^2_{NI} of BEM methods is estimated by

$$\sigma^2_{NI,BEM} = \frac{1}{\Upsilon_{in}} \frac{L(Q+1)}{N_V} \tag{3.22}$$

where Υ_{in} denotes the SINR at the input the receiver. According to its definition, Υ_{in} is obtained by

$$\Upsilon_{in} = \frac{P_S}{P_N + P_I} \tag{3.23}$$

where $P_N := E\{\mathbf{w}_\mathbf{p}^H \mathbf{w}_\mathbf{p}\}$ denotes the energy of noise, $P_I := E\{\mathbf{e}_\mathbf{p}^H \mathbf{e}_\mathbf{p}\}$ the energy of interference and $P_S := E\{(\mathbf{G}\mathbf{a}_\mathbf{p})^H \mathbf{G}\mathbf{a}_\mathbf{p}\}$ the energy of pilot signals.

Combining (3.21) and (3.22), σ^2_{All} of BEM methods is estimated by

$$\sigma^2_{All,BEM} = \frac{1}{\Upsilon_{in}} \frac{L(Q+1)}{N_V} + \sigma^2_{M,BEM} + \sigma^2_{Extra,BEM} \tag{3.24}$$

where $\sigma^2_{M,BEM}$ and $\sigma^2_{Extra,BEM}$ denote the modelling error and extra noises in BEM methods, respectively.

Similarly, NMSE of PITIA which is denoted as $\sigma^2_{All,PITIA}$ can also be derived. For example, the original INSR at the input, which equals to $1/\Upsilon_{in}$, is reduced by K_1 times in step (1) and by $N_V/(2LK_1)$ times in step (2), and changes to $1/(K_1\Upsilon_{in})$ and $2L/(\Upsilon_{in}N_V)$, respectively. Moreover, we consider that the operator $\angle$ introduces extra noises whose power is proportional to the power of noise and interference in $\hat{g}_m^{(u)}$. According to these analysis, $\sigma^2_{All,PITIA}$ is approximated by

$$\sigma^2_{All,PITIA} = \frac{1}{\Upsilon_{in}} \frac{2L}{N_V} + (\pi f_M L K_1/N)^2 + \frac{C_1}{K_1 \Upsilon_{in}} \tag{3.25}$$

where C_1 is a constant.

3.4.4 Parameter optimization

It is shown in (3.25) that, NMSE of the proposed algorithm contains three items: 1) the estimation error caused by noises and interferences, 2) the modelling error σ^2_M and 3) extra errors caused by error propagation and non-linear operations. Moreover, we consider that SINR Υ_{in}, channel length L, the number of subcarriers N and the number of pilots N_V are determined by the application or the wireless channel, while K_1 is the only design parameter in PITIA.

Obviously, (3.25) as a function of K_1 is convex, and there exists a certain value of K_1 that minimizes (3.25), or in other words, maximizes the NMSE performance of PITIA. By setting the first derivative of (3.25) to 0, this optimal value is obtained by

$$K_1^* = \arg\min_{K_1} \sigma^2_{All,PITIA} = (C_1/2\Upsilon_{in})^{1/3} (N/(\pi f_M L))^{2/3} \tag{3.26}$$

which shows that larger C_1 and smaller maximum Doppler shift f_M lead to larger K_1^*. However, K_1^* is insensitive to these factors due to the exponential operations $(\cdot)^{1/3}$ and $(\cdot)^{2/3}$.

3.4.5 Numerical results

We further evaluate K_1^* and NMSE with the simulation tool developed in section 2.4.1, with $N = 2048$ and $B_S = 15kHz$ as specified in LTE, and $L = 16$ as analysed in section 3.2. The corresponding sampling rate over baseband signal is $30.72MHz$. QPSK modulation is adopted for both data and pilots with equal transmission powers. The comb-type pilot pattern as shown in figure 3(a) is adopted, with $N_b = 16$, $N_f = 2$ and $N_p = 3$.

The NMSE values as a function of K_1 under different SNR and Doppler shift conditions are plotted in figure 7, where $K_1 = 2$ shows best performance in most cases, while $K_1 = 4$ is slightly better than $K_1 = 2$ when SNR is low. This result is consistent with (3.26) where smaller SINR results in larger value of K_1^*. These curves also validate the fact that the optimal design parameter K_1^* is not sensitive to channel conditions, and PITIA is able to reach optimality with $K_1 = 2$ in most conditions. As a result, we set $K_1 = 2$ and proceed with two scenarios.

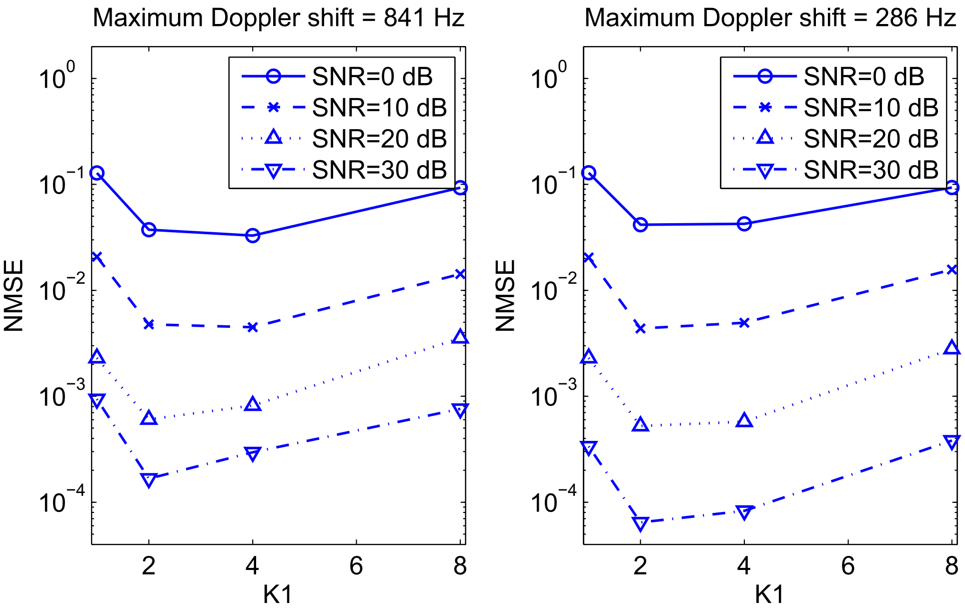

Figure 3.7: NMSE changes over K_1 under different SNR and Doppler shift conditions

In scenario 1, the ground truth of the time-varying channel $g_{n,m}$ is generated by (3.1) which has a single Doppler shift and a random initial phase evenly distributed over $[0, 2\pi]$ on each multipath component. Powers of multipath components decay exponentially over channel dispersion with a 1-dB random shadowing factor. Maximum Doppler shift is set to $f_{max} = 841$ Hz and $f_{max} = 361$

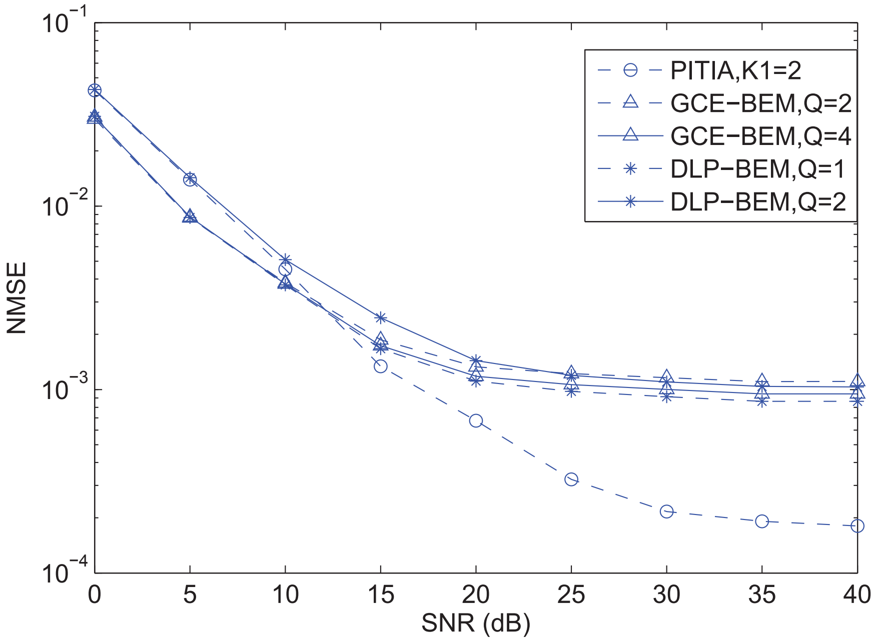

Figure 3.8: NMSE of the proposed algorithm, piece-wise linear approximation, GCE-BEM and DLP-BEM, with $N = 2048$, $L = 16$ and $f_{max} = 841$ Hz; “ground truth" of the wireless channel is simulated by (3.1).

Hz ($f_M = 0.056$ and $f_M = 0.024$), respectively, which correspond to a travelling speed of 350 km/h and 150 km/h if carrier frequency equals to 2.6 GHz. It is shown in figures 8 and 9 that, the proposed algorithm with $K_1 = 2$ outperforms all BEM methods when SNR is higher than 13 dB and 25 dB when $f_{max} = 841$ Hz and $f_{max} = 361$ Hz, respectively. In low-SNR regimes, both types of algorithms have similar performances.

In scenario 2, $g_{n,m}$ is generated by a more realistic channel model - WINNER II channel model with HST scenario, while other conditions are the same as those in scenario 1. This scenario differ from the previous one in that, the order of the channel responses in simulations may exceed 16 occasionally, and there may be more than one Doppler shifts on a few multipath components. Simulations results are plotted in figures 10 and 11, which are similar as those in scenario 1. It

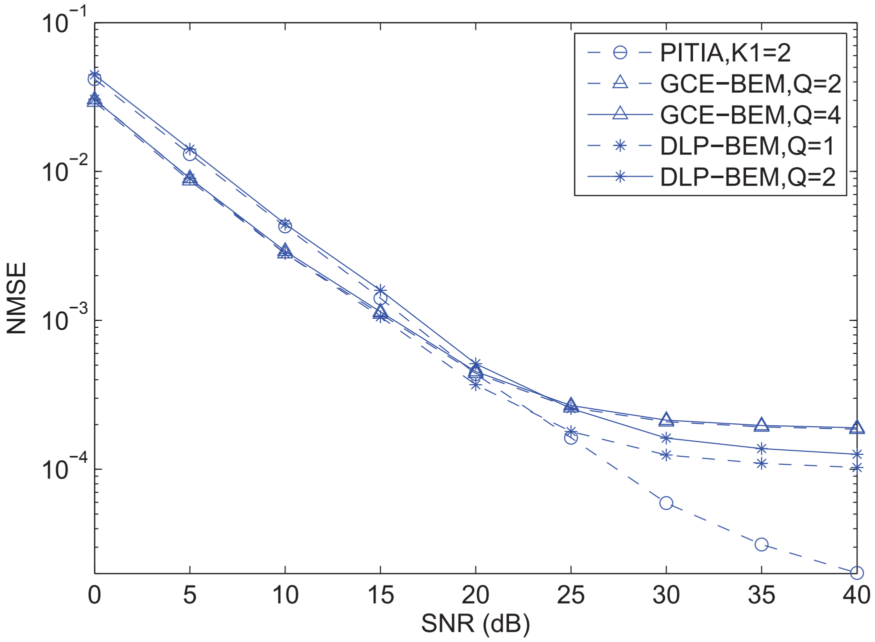

Figure 3.9: NMSE of the proposed algorithm, piece-wise linear approximation, GCE-BEM and DLP-BEM, with $N = 2048$, $L = 16$ and and $f_{max} = 361$ Hz; “ground truth" of the wireless channel is simulated by (3.1).

is also shown that, the degree of performance enhancement does not vary significantly with the change of f_{max}, because f_{max} in WINNER II channel model is stochastic and we can only define its mean value. We claim that HST channels are modelled by (3.1) properly, and PITIA works well when there is occasional mismatch between the assumed channel model (3.1) and the ground truth.

Moreover, these simulation results show consistence with (3.24) and (3.25). First of all, σ^2_{All} is mainly determined by the number of channel parameters and the corresponding channel modelling error. When $Q = 1$, modelling errors (i.e., the first term) in (3.24) and (3.25) equal each other, but $\sigma^2_{M,BEM} > \sigma^2_{M,PITIA}$ (with $K_1 = 2$ and $f_M = 0.056/0.024$), as shown in subsection 3.4.1. When $Q > 1$, $\sigma^2_{M,BEM} < \sigma^2_{M,PITIA}$, but the modelling error in (3.24) is larger than that in (3.25). In short, PITIA achieves a better balance between the number of channel parameters and the modelling

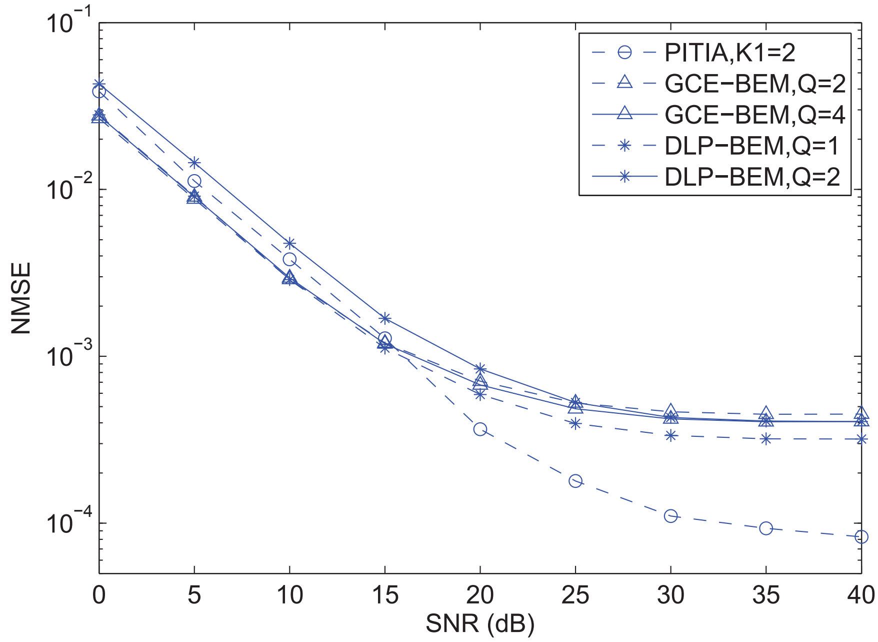

Figure 3.10: NMSE of the proposed algorithm, piece-wise linear approximation, GCE-BEM and DLP-BEM, with $N = 2048$ and $L = 16$; “ground truth" of the wireless channel is simulated by WINNER II, and f_{max} is around 841 Hz.

error, compared with BEM methods. Moreover, the power of extra noises in (3.25) is small when SNR is high, and performance enhancement is thereby achieved in high SNR regime.

We conclude that PITIA outperforms BEM methods in high-mobility and high-SNR environments.

3.4.6 Discussions

Simulation results show that, NMSE of PITIA is 1-2 dB lower in low SNR regime, but 5-8 dB higher in high SNR regime, compared to that of BEM methods. If we model the SNR at receiver as a random variable distributed evenly over 0 to 40 dB, the proposed algorithm is able to reduce the mean value of NMSE significantly. Moreover, as HST's often operate in rural and open

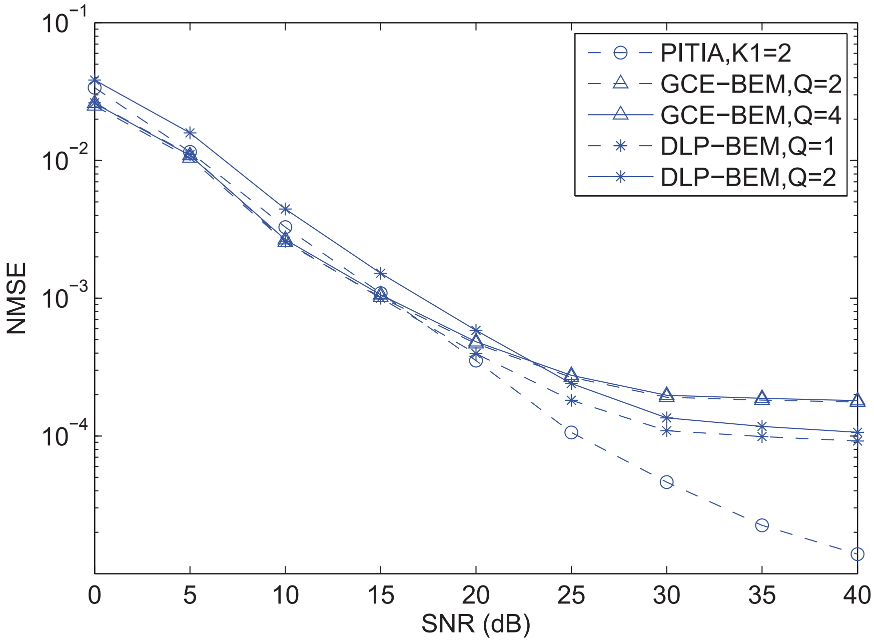

Figure 3.11: NMSE of the proposed algorithm, piece-wise linear approximation, GCE-BEM and DLP-BEM, with $N = 2048$ and $L = 16$; “ground truth" of the wireless channel is simulated by WINNER II, and f_{max} is around 361 Hz.

environments, they enjoy high SNR most of the time.

PITIA requires that clustered pilots are embedded at the transmitter. This requirement is popular in existing TVCE algorithms, but is not fulfilled by current LTE systems. We argue that LTE systems should be enhanced to facilitate TVCE in HST and other high-mobility environments.

3.5 Summary

We propose a simple and effective TVCE algorithm named PITIA to address the challenges introduced by mobile broadband channels. It is based on the finding that there exists only one Doppler shift on each resolvable multipath component. It reduces the number of channel parameters to be estimated while keeping modelling error low, and thereby reduces estimation error. We derive PITIA's optimal design parameter K_1 whose value is stable under various channel conditions. Moreover, the computation complexity of PITIA is comparable with that of a FFT operation. As a result, PITIA is suitable for practical OFDM systems on HST's.

CHAPTER 4

PHY-CRAM: Harnessing Mobile Broadband Channels

4.1 Overview

With the rapid advancement of wireless communication technology and ever-increasing mobile applications, securing wireless communication becomes more and more important and challenging. Compared to a wired network, ensuring security in a wireless/mobile network faces greater challenges mainly due to its "open air" nature since an attacker can easily eavesdrop or intercept the wireless communication channel. On the flip side, the inherent and unique properties of mobile broadband channels can be exploited to enhance the wireless network security. There has been an increasing interest in complementing or enhancing authentication in wireless networks by exploiting physical layer characteristics [8,9,76–83,101–103]. Physical layer authentication/identification benefits a number of wireless applications such as forensics [104], identity-based attack detection [105], access control [106, 107], malfunctioning detection [108], and tracking [109, 110] etc.

In this chapter, we propose the first physical layer challenge-response authentication mechanism (PHY-CRAM) to leverage the opportunities provided by mobile broadband channels and to address *Problem* 2. Being different from encryption based challenge-response authentication techniques, PHY-CRAM exchanges unencrypted shared secrets among participants. These shared secrets are masked by a random number and the channel fading, while the verifier is able to verify the secrets without knowing the channel state information (CSI) owing to a reverse operation in the response signal and channel reciprocity. An attacker, on the other hand, cannot experience exactly the same channel fading as any legitimate user experiences due to location distinction, and can hardly learn the shared secrets from the signals transmitted from legitimate users.

The security strength of PHY-CRAM depends on the randomness of the fading channel and the relative geographic location between the attacker and legitimate users, but not depends on the computation complexity. That is, even when the attacker's computational power is increased, PHY-CRAM does not need to increase its key length in order to maintain the same security strength, as long as the channel randomness is remained. This property is not owned by conventional authentication schemes (such as CRAM-MD5 [14] and CHAP [15]).

PHY-CRAM features another unique characteristic that, it eliminates channel coding, channel estimation and frequency offset compensation for most messages during the challenge-response authentication. This feature does not only simplifies the baseband design, but also prevents the attackers from probing the channel and provides better security strength.

PHY-CRAM is also unique compared to other existing physical layer authentication mechanisms. Being different from the existing RF fingerprinting schemes [76–78,102,103], PHY-CRAM is immune to impersonation attacks, it does not require a high end signal analyzer, and it favors dynamic environments. Compared to wireless channel based authentication [8, 9, 79–81, 101], it does not require the legitimate user to be at a specific location and does not need channel estimation or training. PHY-CRAM is also different from signal watermarking [82, 83], which conveys a cryptographically secure digital signature along with the primary transmission by superposition or superimposing. In short, PHY-CRAM is simple, secure, robust, and flexible, and can be applied in any wireless networks for authenticating nodes that share a secret without the requirements of any auxiliary instruments, channel estimation or being at a specific location.

4.2 System Setup

4.2.1 Application model

We consider a wireless network with I legitimate users B_i, $i = 0, ..., I-1$. Node pairs that need to authenticate each other share a set of secrets. For example, in a wireless local area network (WLAN), the access point shares different secret keys with each client. Specifically, the shared keys (bit strings) between B_j and B_k are denoted as $\{\mathbf{X}_j^{(j,k)}, \mathbf{X}_k^{(j,k)}\}$, where $\mathbf{X}_j^{(j,k)} := [X_{0,j}^{(j,k)}, ..., X_{M-1,j}^{(j,k)}]^T$, $X_{m,j}^{(j,k)} \in \{0,1\}$ $(m = 0, ..., M-1)$ is the $(m+1)^{th}$ bit, and M is the key length. $\mathbf{X}_k^{(j,k)}$ follows the same definition. For one-way authentication, only one key is necessary, while for mutual authentication two keys are used in PHY-CRAM. For simplicity, we drop the index $^{(j,k)}$ whenever there is no misunderstanding.

Each legitimate user B_j has a Media Access Control (MAC) address, which is equipped in most MAC protocols. Security of the system relies on the secrecy of $\{\mathbf{X}_j, \mathbf{X}_k\}$. If an attacker knowns $\{\mathbf{X}_j, \mathbf{X}_k\}$, it has the ability to impersonate either B_j or B_k.

4.2.2 Communication model

A frequency band with bandwidth W is occupied by the wireless network, where the users who want to authenticate each other are within their communication ranges. We consider a three-layer communication model: (1) the physical-layer modulation scheme, (2) the MAC protocol, and (3) the authentication scheme running as an application. PHY-CRAM contributes in (1) and (3), while adopts conventional MAC protocols, for examples, carrier sense multiple access (CSMA) for ad hoc networks or time division multiple access (TDMA) for centralized networks.

Orthogonal frequency-division multiplexing (OFDM) is adopted as the physical layer technique, since it enjoys high spectrum efficiency and good immunity to multipath, and can utilize the reciprocal feature of wireless channels easily. Many modern wireless network standards adopt OFDM technology, such as 802.11 (WiFi), 802.16 (WiMax), LTE, etc. Users in the network may be indoor, outdoor, static or mobile, resulting in different channel types. Each channel associates with a channel coherence time T_C, below which the channel is considered as temporally correlated. Define N and L as the number of subcarriers and length of cyclic prefix (CP) in OFDM modulation, respectively. Then the subcarrier spacing equals to W/N. A proper design on the system guarantees that N and L are large enough to overcome frequency-selective fading, while N is also small enough to overcome the Doppler shifts in mobile environments [111].

4.2.3 Attacker model

We assume a very powerful attacker E, who knows all the communication protocols and authentication schemes adopted in the network. Besides, E is able to monitor and replay any messages and signals sent in the network. E may be very close to a legitimate user, say just one or few wavelengths away from legitimate users. The radio on E is assumed to be perfect, with no LO drift or modulation error. However, E does not know $\{\mathbf{X}_j, \mathbf{X}_k\}$. E's goal is to pass the authentication with legitimate user(s).

4.3 The Physical Layer Mutual Authentication Mechanism: PHY-CRAM

4.3.1 The basics

PHY-CRAM is realized by transmission and reception of a bunch of wireless frames between two participants. All these frames have $(K_1 + K_2)$ OFDM symbols. The first K_1 symbol is modulated with differential phase shift keying (DPSK) scheme, and contains binary data regarding the traffic information and user information, like frame type, MAC address, and time stamp etc (referred to

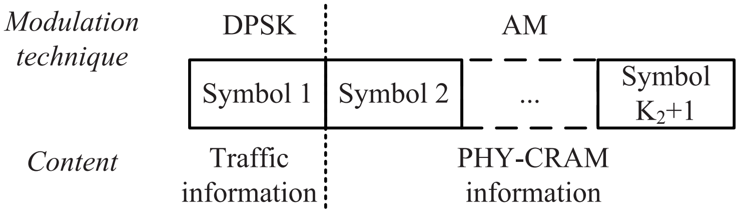

Figure 4.1: Frame structure of PHY-CRAM messages

as traffic information). Due to the importance of traffic information, data interleaving, convolutional encoding and cyclic redundancy check (CRC) are adopted. We randomize the amplitude of each subcarrier since equal power level reveals CSI to the attacker, while CSI is not required to demodulate DPSK signal.

The last K_2 symbols in each frame carry PHY-CRAM information, which contains the shared keys $\mathbf{X}_j$ and $\mathbf{X}_k$, as well as a set of random values D_n. PHY-CRAM information may be repeated for several times to resist noise. For simplicity, we assume that both traffic information and PHY-CRAM information can be accommodated in a single OFDM symbol (however, PHY-CRAM is not confined to this condition). As a result, $K_1 = 1$ and K_2 equals to the number of repetitions for PHY-CRAM information, and the corresponding frame structure is shown in figure 4.1.

Note that the DPSK modulation for traffic information does not require at least two OFDM symbols or an "initial" OFDM symbol with pre-known phase information, since the differential encoding can be conducted subcarrier-by-subcarrier [112]. Taking DQPSK as an example, the phase difference between subcarrier 10 and subcarrier 11 carries two bits, while the phase difference between subcarrier 12 and subcarrier 13 carries another two bits (all these subcarriers are within one OFDM symbol). Since the subcarrier spacing is designed to be much smaller than the coherence bandwidth, the channel responses on two adjacent subcarriers are highly correlated. The phases at subcarriers 10 and 12 may be randomized to further increase the security strength.

The term "frame" may be misunderstood such that it only defines the data at MAC layer, which is further encapsulated at physical layer. Actually, all "frames" defined here refer to the final signal "in the air". More importantly, these frames do not contain any pre-known synchronization header, pilots or reference signals. Timing and frequency synchronization to these frames at the receiver are realized simply through autocorrelation on CP [113]. Throughout the procedure of PHY-CRAM, channel estimation is never needed.

Based on the communication model given in subsection 4.2.2, Doppler spread caused by relative speed between two participants are neglected, and there is no inter-carrier interference (ICI) in the system. As a result, the OFDM system can be considered as the superposition of N independent narrow band subsystems that experience flat-fading channels, and each subsystem is modelled simply by 2.1. Due to its simplicity, frequency-domain representation is used throughout this chapter.

Without loss of generality, we map the M-length shared key $\mathbf{X}_j$ or $\mathbf{X}_k$ onto the subset of subcarriers with M smallest indices; for example, $X_{0,j}$ is mapped onto subcarrier 0, and $X_{M-1,j}$ onto subcarrier $M-1$ etc. Then the index n in $X_{n,j}$ or $X_{n,k}$ denotes both the subcarrier index and bit location.

4.3.2 The authentication procedure

We use subcarrier n to show the basic principle of PHY-CRAM, with two participants B_j and B_k. Without loss of generality, assume that B_k wants to start a conversation with B_j. The mutual authentication between them contains three stages as shown in figure 4.2.

In stage 0, B_k sends an "authentication request" frame to B_j. The frame contains only traffic information, so only symbol 1 is used. All the information in this frame is not encrypted. This frame does not reveal CSI information to the attackers, since there is no pilot or synchronization header and the amplitudes of all subcarriers are randomized.

After receiving the authentication request, B_j authenticates B_k in stage 1. If B_k passes the authentication, B_j will also be authenticated by B_k (actually B_k does not need to know the result in stage 1, but can always send challenge to start the authentication; however, B_j responds to this challenge only if B_k passes the authentication in stage 1). The mutual authentication succeeds if and only if both stage 1 and stage 2 show positive results. One-way authentication can be realized by only applying stage 0 and stage 1.

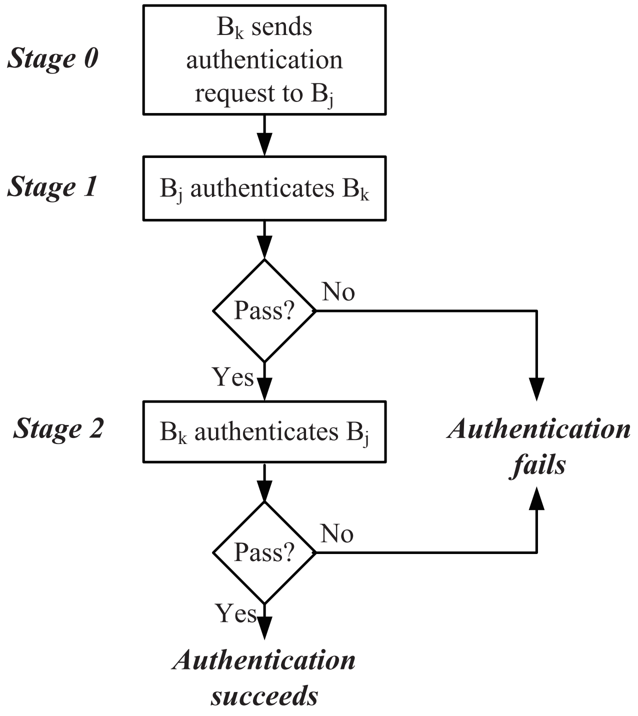

Figure 4.2: The basic procedure of PHY-CRAM

During stages 1 and 2, a typical challenge-response procedure is defined. Detailed steps of stage 1 are shown in figure 4.3, while those of stage 2 can be derived by switching two participants. These steps include:

Step (1) At time t_1, B_j uses a random number D_n within the range $[K_3, K_4]$ to modulate amplitudes of subcarriers in the last K_2 OFDM symbols, where $0 < K_3 < 1 < K_4$, and transmits the resulting frame to B_k. Here D_n is a random number with the purpose to prevent the attacker from probing the channel. This frame is actually a challenge for authentication.

Step (2) B_k receives $D_n H_{jk,n} + W_n^{(1)}$, where $H_{jk,n}$ denotes the wireless channel between B_j and B_k at the n^{th} subcarrier, and $W_n^{(1)}$ the AWGN. As a response to the challenge, $\mathcal{M}(X_{n,k})/(D_n H_{jk,n} + W_n^{(1)})$ is transmitted by B_k at time t_2, where $X_{n,k}$ is the n^{th} element in $\mathbf{X}_k$ and $\mathcal{M}(\cdot)$ denotes a constellation mapping scheme. The shared key $\mathbf{X}_k$ is masked by the wireless channel $H_{jk,n}$. At time t_3, this frame arrives at B_j , who authenticates B_k according to its received signal. Both B_j and B_k should do these processing fast enough to ensure that $t_3 - t_1 \ll T_C$.

The signals defined in these two steps as shown in figure 4.3 are classified as PHY-CRAM information, and are modulated on the last K_2 OFDM symbols. Similar to the "authentication request" frame, traffic information in stage 1 and stage 2 is carried in the first OFDM symbol.

The constellation mapping scheme $\mathcal{M}(\cdot)$ is defined as

$$\mathcal{M}(x) = \begin{cases} K_3, x = 0 \\ K_4, x = 1 \end{cases} \tag{4.1}$$

which maps the binary values to positive real values K_3 or K_4. In other words, we adopt amplitude modulation (AM) for PHY-CRAM information, while K_3 and K_4 determine both the randomness of D_n and the euclidean distance of the constellation. The ratio K_4/K_3 should be large enough to hide the CSI, while too large value of K_4/K_3 leads to high transmission power at some subcarriers. In practice, $[K_3, K_4]$ should have the similar range as the channel fading (the normalized value of $H_{jk,n}$) has. For example, if the largest channel gain is 10 dB larger than the smallest channel gain in all subcarriers, it is appropriate to set $K_3 = 0.5$ and $K_4 = 1.5$.

The key feature of this authentication mechanism is that, the shared key $X_{n,k}$ is secured by the wireless channel which is cancelled out at the verifier, and only the verifier can derive $X_{n,k}$ in

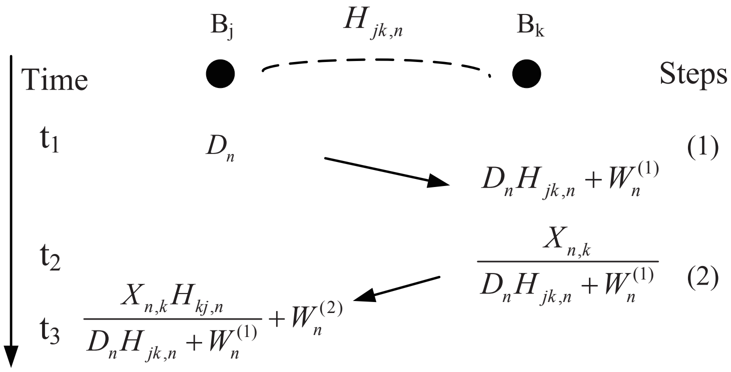
B_j
$H_{jk,n}$
B_k
Time
Steps
t_1
D_n
(1)
$D_n H_{jk,n} + W_n^{(1)}$
t_2
$\frac{X_{n,k}}{D_n H_{jk,n} + W_n^{(1)}}$
(2)
t_3
$\frac{X_{n,k} H_{kj,n}}{D_n H_{jk,n} + W_n^{(1)}} + W_n^{(2)}$

Figure 4.3: Detailed steps in stage 1 of PHY-CRAM

multipath environments.

We denote the symbols at subcarrier n in step u before and after transmission as $T_n^{(u)}$ and $R_n^{(u)}$, respectively; for example,

$$R_n^{(2)} = \frac{X_{n,k} H_{kj,n}}{D_n H_{jk,n} + W_n^{(1)}} + W_n^{(2)}. \tag{4.2}$$

In real systems, all the signals modulated on subcarriers are complex values, with real and imaginary parts represented by I-branch and Q-branch respectively. However, phases of all signals defined in steps (1) and (2) are useless, since they adopt AM modulation. Therefore, all the notations defined in this section represent their absolute values.

Timing must be met during the procedure, otherwise the wireless channel is no longer reciprocal. In static channels with pedestrians walking around at a speed of 1 m/s, T_C is around 20 ms, while in high mobility environments with moving speed 30 m/s, T_C is around 0.7 ms, when carrier frequency equals to 2.4 GHz. On the other hand, off-the-shelf wireless devices can maintain the round-trip delay well below 0.7 ms (not including the processing delay at application layer), while our prototype achieves a round-trip delay of only 36 μs.

4.3.3 The verification scheme

In step (2) of stage 1, B_j needs to verify that whether the counterpart is legal or not through the response received, while B_k meets exactly the same problem in stage 2. So we only take B_j as an example.

To enhance the signal quality, B_j combines the received signals on all subcarriers, and get

$$\mathbf{R}^{(2)} := [R_0^{(2)}, ..., R_{M-1}^{(2)}]^T. \tag{4.3}$$

Moreover, B_j knowns $\mathbf{X}_k$ since it is the shared key. Then B_j wants to verity the identity of B_k through comparison between $\mathbf{R}^{(2)}$ and $\mathbf{X}_k$. To be precise, we define this problem as follows:

Problem 1 : Given $\mathbf{R}^{(2)}$ and $\mathbf{X}_k$, make a decision on whether frame (2) is sent from B_k or not.

To solve this problem, we first ignore the noise, and make an approximation that $H_{kj,n} = H_{jk,n}$. Then (4.2) becomes

$$R_n^{(2)} = \frac{X_{n,k}}{D_n} \tag{4.4}$$

where $n \leq M-1$, and (2.2) becomes

$$\mathbf{R}^{(2)} = \left[\frac{X_{0,k}}{D_0}, ..., \frac{X_{M-1,k}}{D_{M-1}}\right]^T. \tag{4.5}$$

Then we get the following relationship

$$\mathbf{R}^{(2)} \odot \mathbf{D} = [X_{0,k}, ..., X_{M-1,k}]^T = \mathbf{X}_k \tag{4.6}$$

where $\mathbf{D} := [D_0, ..., D_{M-1}]^T$ is known by B_j (since $\mathbf{D}$ is generated by B_j), while the unknown channel responses $H_{kj,n}$ and $H_{jk,n}$ cancel each other.

With existence of low noises and slight difference between $H_{kj,n}$ and $H_{jk,n}$, $\mathbf{R}^{(2)} \odot \mathbf{D}$ and $\mathbf{X}_k$ are not exactly the same, but should be similar. Therefore, a straightforward solution to *Problem* 1 is to check the Euclidean distance between $\mathbf{X}_k$ and $\mathbf{R}^{(2)} \odot \mathbf{D}$:

Solution 1: Frame (2) is sent from B_k if and only if $||\mathbf{R}^{(2)} \odot \mathbf{D} - \mathbf{X}_k|| < C_0$, where C_0 is a constant real number.

□

However, it is hard to determine C_0, since bounding Euclidean distance is hard. On the other hand, the value of cross-correlation is tightly bounded between [0,1]. Then we define $\bar{\mathbf{R}}_{\mathbf{D}}$ and $\bar{\mathbf{X}}_k$ as mean values of $\mathbf{R}^{(2)} \odot \mathbf{D}$ and $\mathbf{X}_k$ respectively, and give another solution:

Solution 2: Frame (2) is sent from B_k if and only if

$$\frac{(\mathbf{R}^{(2)} \odot \mathbf{D} - \bar{\mathbf{R}}_{\mathbf{D}})^H \cdot (\mathbf{X}_k - \bar{\mathbf{X}}_k)}{||\mathbf{R}^{(2)} \odot \mathbf{D} - \bar{\mathbf{R}}_{\mathbf{D}}|| \cdot ||\mathbf{X}_k - \bar{\mathbf{X}}_k||} < C_1. \tag{4.7}$$

□

The value of parameter C_1 in *Solution* 2 must be selected properly in order to get a balance between the successful authentication rate β (the rate that a legitimate user passes the authentication) and false acceptance rate α (the rate that an attacker passes the authentication). We will use receiver operating characteristic (ROC) to evaluate PHY-CRAM's performance.

4.3.4 Peak reduction

Let's focus on the response $T_n^{(2)} := \mathcal{M}(X_{n,k})/(D_n H_{jk,n} + W_n^{(1)})$ sent by B_k in step (2) of stage 1. The absolute value of $T_n^{(2)}$ may be extremely large if (1) $\mathcal{M}(X_{n,k}) = K_4$, (2) $D_n = K_3$ and (3) $H_{jk,n}$ experiences deep fading ($|H_{jk,n}| \ll 1$). The probability that these three conditions occur simultaneously is low; as a result, the number of high peaks is small compared to the number of subcarrier N. However, a few high peaks at frequency-domain may cause multiple issues for wireless communication systems. For examples, the transmission powers at some subcarriers may exceed the limitation defined by the regulator, and the peak-to-average power ratio (PAPR) may be deteriorated. Note that, we always normalize the baseband signal so that the average power over all subcarriers is constant, in order to fit the dynamic range of downstream components at the transmitter (like digital-to-analogue converter and amplifier). As a result, the high peaks at some subcarriers does not increase the the total transmission power, but actually decrease the transmission power at other subcarriers, and may reduce the spectrum efficiency.

We solve the high-peak issue by adding a peak reduction operation defined as follows:

$$\widetilde{T}_n^{(2)} = \begin{cases} T_n^{(2)}, & if\ |T_n^{(2)}| \leq A_{\max} \\ A_{\max} T_n^{(2)} / |T_n^{(2)}|, & otherwise \end{cases} \tag{4.8}$$

where $\widetilde{T}_n^{(2)}$ denotes the signal after peak reduction, and $A_{\max}$ denotes the maximum allowable amplitude of the signal at any subcarrier.

In (4.8), all the high peaks are cut off, and the channel effect cannot be cancelled out. However, since all subcarriers are independent, the peak reduction operation does not affect the subcarriers without high peaks (named good subcarriers). Since good subcarriers dominate the system, the peak reduction operation does not affect the value of C_1 too much, and, as a result, have limited effect on the verification scheme (either $Solution$ 1 or $Solution$ 2).

4.3.5 Effect of timing offset

When CP is used for timing synchronization, timing offset is more serious, since the peak of CP-correlator is smooth. Performance of traditional OFDM systems is not affected as long as the timing offset plus channel delay spread (in number of samples) does not exceeds L (we call this kind of timing offset as “tolerated timing offset"), since the effect of timing offset is absorbed by channel estimation [114]. Now we analyse the effect of tolerated timing offset to PHY-CRAM where channel estimation is absent.

Assume that the timing offset at B_k in step (1) and at B_j in step (2) are δ_k and δ_j respectively. Then according to [115], the equivalent channel response from B_j to B_k, and from B_k to B_j, are $H'_{jk,n} = H_{jk,n}e^{j2\pi\delta_k/N}$ and $H'_{kj,n} = H_{kj,n}e^{j2\pi\delta_j/N}$ respectively. Then in the ideal case of static channel with no noise, (4.5) changes to

$$\begin{aligned}\mathbf{R}^{(2)'} = [&\tfrac{X_{0,k}}{D_0}e^{j2\pi(\delta_j-\delta_k)0/N},\ldots,\\ &\tfrac{X_{M-1,k}}{D_{M-1}}e^{j2\pi(\delta_j-\delta_k)(N-1)/N}]^T\end{aligned} \tag{4.9}$$

which has the same amplitude but different phase compared with (4.5). As only the amplitude is used for further processing, the performance of PHY-CRAM with existence of tolerated timing offsets at either B_j or B_k is not affected. Once δ_k or δ_j exceed L, SNR is reduced dramatically, and CRC in symbol 1 may be wrong; we classify this situation as frame drop/error, rather than timing offset. Any frame drop/error causes time-out and triggers retransmission of the same frame.

4.3.6 Effect of frequency offset

Frequency offset comes from two sources: LO drift between Tx and Rx, and Doppler effect. It imposes two impairments to OFDM systems: ICI and phase shifts [116]. Most short range OFDM systems have large subcarrier spacing, which is much bigger than frequency offset caused by LO drift and Doppler shift. For example, the WiFi system features subcarrier spacing of 312.5 KHz, while the frequency offset mentioned above is at the level of 3 KHz. As a result, ICI can been ignored in such system. Due to the same reason analysed in subsection 4.3.5, phase shifts caused by either timing offset or frequency offset do not affect PHY-CRAM. Therefore, frequency offset estimation and compensation are unnecessary in PHY-CRAM. The real-world testing we conduct show good results without frequency offset compensation.

4.4 Analyses on the attacks

To evaluate the security strength of PHY-CRAM, we analyse various types of attackers in this section. Without loss of generality, we only take subcarrier n for example.

4.4.1 Passive attackers

A passive attacker E_P only monitors all frames inside the network during authentication, and tries to learn $\{\mathbf{X}_j, \mathbf{X}_k\}$ from whatever it gets. If E_P learns something in $\{\mathbf{X}_j, \mathbf{X}_k\}$, it may initiate an authentication procedure with some users; however, as long as E_P is silent during legitimate users' authentication procedure, it is still considered as passive.

Stage 0 does not need to be secured, since it does not reveal the shared key or CSI.

As shown in figure 4.3, stages 1 and 2 are symmetrical with each other and undergo the same passive attacks. Therefore, we only analyse stage 1.

We first assume that E_P is not too close to B_j and B_k, so that h_{jk}, h_{jE} and h_{kE} are all uncorrelated (case 1). The noises at E_P's receiver are ignored. Then all the frames received by E_P, except "link set up request" which contain no information about the shared keys, are

$$R_{E,n}^{(1)} = D_n H_{jE,n} \tag{4.10}$$

and

$$R_{E,n}^{(2)} = \frac{X_{n,k} H_{kE,n}}{D_n H_{jk,n} + W_n^{(1)}} \tag{4.11}$$

where $H_{jE,n}$ and $H_{kE,n}$ denotes the wireless channels between B_j and E_P, and between B_k and E_P, respectively. In (4.10) and (4.11), five unknown factors exist in two equations, despite of the noise. Therefore, there is no way for E_P to derive $\mathbf{X}_k$.

Note that if D_n is not random but a value known by everyone, E_P is able to estimate $H_{jE,n}$ in stage 1 and $H_{kE,n}$ in stage 2, according to (4.10). Then E_P can estimate $X_{n,k}/H_{jk,n}$ in stage 1 and $X_{n,j}/H_{jk,n}$ in stage 2 according to (4.11). As a result, $X_{n,k}/X_{n,j}$ is known by E_P, and the shared keys between B_j and B_k are compromised to some degree.

Then we consider two more aggressive cases that, E_P is very close to B_j (case 2) and B_k (case 3) respectively. Then besides (4.10) and (4.11), E_P gets more information. For case 2, it gets

$$H_{jE,n} \approx 1 \tag{4.12}$$

because the direct path between E_P and B_j is much stronger than any multipath if they are very close to each other, and

$$H_{jk,n} \approx H_{kE,n} \tag{4.13}$$

which is obvious.

Combing 4.10 to 4.13 and ignoring the noise, we have

$$X_{n,k} \approx R_{E,n}^{(1)} R_{E,n}^{(2)} \tag{4.14}$$

and interestingly, for case 3, we get the same result as in (4.14).

As a result, E_P is able to get a rough estimate on $\mathbf{X}_k$ through what it hears for both case 2 and case 3. It seems dangerous to PHY-CRAM. However, E_P cannot be too close to B_j or B_k, since each radio occupies a certain area of space, and it is impossible in most cases for E_P to go inside of another radio. Furthermore, due to the approximation in (4.12) and (4.13), $\mathbf{X}_k$ estimated by E_P is very noisy (due to the channel variations over space), while B_k has perfect information about $\mathbf{X}_k$. Therefore, the attacker E_P is still identifiable.

A passive attacker is able to derive part of the information in $\mathbf{X}_k$ from channel correlation among adjacent subcarriers. We consider this as a truncation to the shared key. Actually if we modulate shared keys on a selected set of subcarriers with a spacing bigger than the coherence bandwidth, a passive attacker will learn nothing about $\mathbf{X}_k$ through channel correlation. The maximum number of shared keys in this ideal case determines the security strength of PHY-CRAM, which is analysed in section 4.5.4.

4.4.2 Active attackers

A passive attacker E_A may transmit messages to facilitate his attacks.

If an attacker initiates stage 0 (sends authentication request to B_j), it will be authenticated by B_j in stage 1, and it can hardly succeed since it does not have the shared key. On the other hand, stage 1 is more vulnerable than the other two stages, since during stage 0 B_k does not know the legality of its counterpart. After procedure 1 is finished successfully, B_j will know that whether B_k is legal or not, and any further response to B_k is safe. Therefore, a threat to PHY-CRAM comes from step (2) in procedure 1, since B_k needs to identify whether the challenge is sent from B_j or not.

We first assume that all users are active and will respond to all requests timely. Therefore, in step (1) B_j will definitely sends a challenge. Moreover, since the channel is symmetrical in two directions, B_j is able to adjust its transmission power properly to guarantee a nearly constant SNR at B_k, with the help from its received signal's SNR at stage 0. The underlying assumption here is that, in stage 0 the transmission power of B_k must be constant (transmission power on each subcarrier is random, but the overall transmission power is constant). In this way, any active attacks during step (1) or (2) can be easily detected. For example, if E_A tries to overcast B_j's signal by using high transmission power, B_k detects the attack directly; on the other hand, if E_A maintains the signal at the same power level, it cannot effectively modify the challenge information as it wants. Note that due to the absence of any pre-known signal contained in all OFDM symbols, there is no way for E_A to estimate the channel between itself and B_k in order to modify the challenge signal precisely; the only way E_A can modify the challenge is to overcast it by high transmission power. As a result, PHY-CRAM is still safe facing active attackers.

In case that B_j does not send respond to B_k timely, E_A may take the role of B_j successfully, and steal $\mathbf{X}_k$ from the response of B_k. We solve this problem by sharing two distinguished keys, $\mathbf{X}_j$ and $\mathbf{X}_k$, between B_j and B_j. After B_k has been authenticated by B_j, B_k also authenticates B_j; if B_j cannot provide a valid response, B_k would consider that its shared key has been compromised and revoke it. Moreover, E_A cannot actively steal the shared key since it impersonates B_j; it can only wait for other users to initiate the conversation, as shown in figure 4.2.

The active attack introduced in [85] requires that both participants in the authentication procedure send pre-known sounding signals. However, in PHY-CRAM, the sounding signals D_n are random signals, so neither two participants nor attackers can derive CSI.

4.4.3 Impersonation attacks

Although impersonation attacks [78] belong to active attacks, it is emphasized here due to its significant threat to other physical-layer security schemes [76, 77, 102, 103, 106, 117]. Two kinds of impersonation attacks, signal replay attack, and feature replay attack, are analysed here.

In a signal replay attack, the attacker E stores the waveforms shown in (4.10) and (4.11), and use 4.11 to impersonate B_k. However, E cannot succeed for two reasons. Firstly, the challenge sent from B_j contains a random number D_n, and an old version of (4.11) cannot be used in future authentication procedures. Secondly, even if D_n is unchanged, $H_{kE,n}$ also randomizes (4.11) and makes this waveforms useless.

Feature replay attack is also similar to "mimicry attack" as introduced in [81]. Conventional physical-layer security schemes rely on training sequence and synchronization sequences for channel estimation and timing/frequency synchronization at the counterpart. As a result, CSIs become no longer random to the attacker, while the attacker is able to forge frames that show legal shared key at B_j.

However, in PHY-CRAM no training or synchronization sequences exist, and the challenge signal is randomized by D_n. Timing and frequency synchronization are realized by CP, while channel estimation is not necessary. Therefore, the attacker cannot derive CSI, and cannot control the signal arrives at legitimate users. As a result, feature replay becomes impossible, only except that the attacker is very close to one of the participants.

We notice that, the information contained in OFDM symbol 1 are related with the identity of Tx and Rx, as well as the logic of PHY-CRAM protocol. If an attacker knows that B_j is authenticating B_k, it knows the content of source/destination MAC address and frame type directly. As a result, by using the known information in symbol 1 as a "training signal", the attacker would be able to estimate the channel. However, what the attacker gets here is just phase information (because symbol 1 is DPSK modulated with randomized amplitude on each subcarrier), while the shared keys are represented by amplitudes, which show little correlation to the phase. Therefore, by using different modulation schemes, PHY-CRAM is able to keep the useful CSI (the amplitudes of subcarriers) secret to the attacker.

4.5 Performance Evaluation

Performance of PHY-CRAM is determined by many factors, including signal quality, randomness of the channel over space, processing delay, key length M, and distance between legitimate user and attacker etc.

Signal quality affects PHY-CRAM's performance dramatically. When signal quality is good, the cross-correlation in (4.7) generates a high value, the threshold C_1 can be high, and the false alarm rate is low accordingly, and vice versus. As introduced in section 4.3, frequency offset and tolerated timing offset does not affect PHY-CRAM, and channel estimation is unnecessary. Therefore, signal quality in PHY-CRAM is mainly determined by noises and deep fading. We will evaluate how these two factors affect PHY-CRAM's performance by computer based simulations.

Randomness of the channel over space determines the ability of PHY-CRAM to resist passive attackers and feature replay attackers that are very close to one of the legitimate users, as discussed in subsection 4.4. Processing delay determines how small $t_3 - t_1$ could be, and how well the reciprocal property of the wireless channel is maintained. These factors are closely related with channel's spatial and temporal correlation characteristics, as well as implementation issues. As a result, we design a prototype for PHY-CRAM and conduct extensive real-world testing in various channel environments to evaluate these factors. The prototype contains MAC, baseband and radio frequency (RF) designs, among those the baseband signal processing algorithms and MAC protocol are realized on a field-programmable gate array (FPGA) platform to ensure low latency.

4.5.1 Simulation results

We conduct Monte Carlo simulation to get an initial estimate on the performance of PHY-CRAM with respect to noises, multipaths, the number of repetitions K_2, and key length M, while W, N and L are fixed at 10 MHz, 64 and 16, respectively. There are 100 pairs of legitimate users. The rural/urban channels defined in [93] are selected as channel models, with 10/20 multipaths, fixed amplitudes and random phase shifts. Maximum delay spread of two channels equal to 0.528 μs and 2.14 μs, respectively, the latter of which exceeds the length of CP adopted in the simulation. In other words, we select a very bad urban channel in order to evaluate the effect of deep fading to PHY-CRAM's performance. We adopt DQPSK modulation for symbol 1 due to its good balance between spectrum efficiency and BER performance, and conduct peak reduction for the rest symbols.

Figure 4.4 plots a snapshot of the frequency-domain channel response's amplitudes ($|H_{jk,n}|$) in urban channel, where most amplitudes fall in the range of $[0.5, 2.5]$. The fading condition in rural channel is much better. As a result, we set $K_3 = 0.5$, $K_4 = 2.5$ and $A_{max} = 5$ in the simulations.

Performance of PHY-CRAM is represented by ROC, which reflects successful authentication rate (the rate that two legitimate users pass the authentication, denoted as β) versus false acceptance rate (the rate that an attacker passes the authentication conducted by a legitimate user, denoted as α). Moreover, the performance of both one-way authentication (stages 0 and 1) and mutual authentication (stages 0, 1 and 2) are evaluated. For both cases, legitimate users use shared keys for authentication, while a naive attacker generates length-M random vectors for authentication.

The performance of PHY-CRAM with respect to K_2 is shown in figure 4.5, where all ROC curves are derived in the rural channel with SNR=10 dB. It is shown that, the performance enhancement is not obvious when $K_2 > 3$. Since larger K_2 leads to larger energy consumption, we set $K_2 = 3$ in the following simulations.

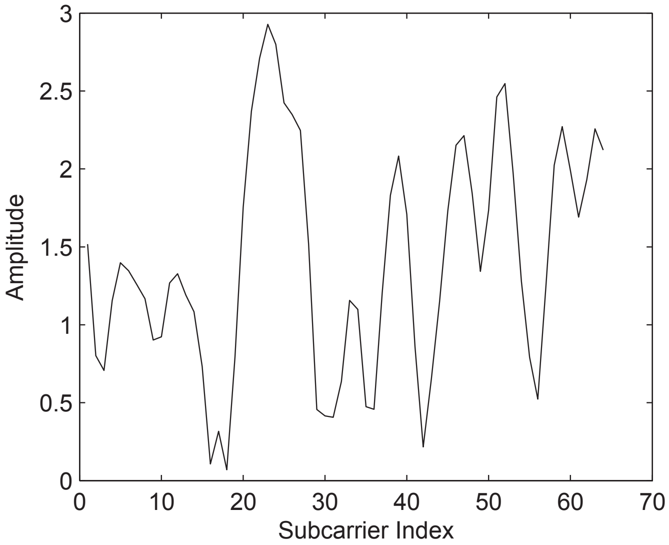

Figure 4.4: Amplitude of the frequency-domain channel response $|H_{jk,n}|$ in urban channel over subcarrier index

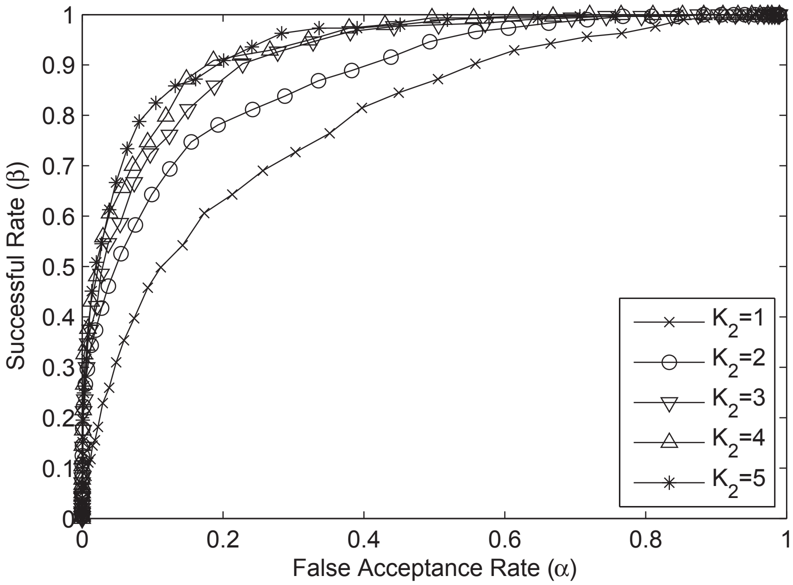

Figure 4.5: ROC curves of PHY-CRAM for one-way authentication under rural channel derived by simulation, with various settings for K_2

Figures 4.6 and 4.7 plot the ROC curves for one-way and mutual authentication under rural and urban channels with key length M = 40 and 60, respectively. As expected, larger M and higher SNR lead to better results. In both channels, the performance is very good when $M = 60$ and SNR ≥ 15 dB.

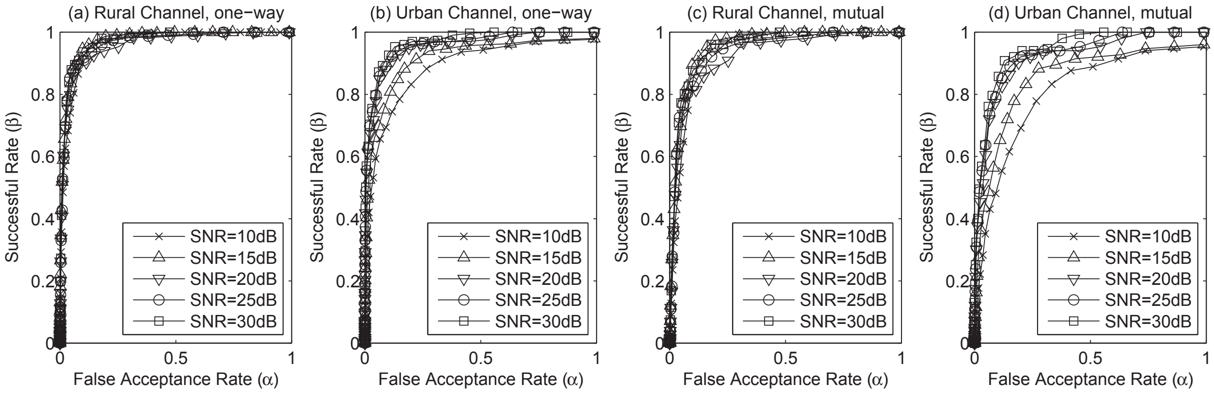

Figure 4.6: ROC curves of PHY-CRAM for one-way (a)(b) and mutual (c)(d) authentication under rural channel (a)(c) and urban channel (b)(d) derived by simulation, with key length M = 40

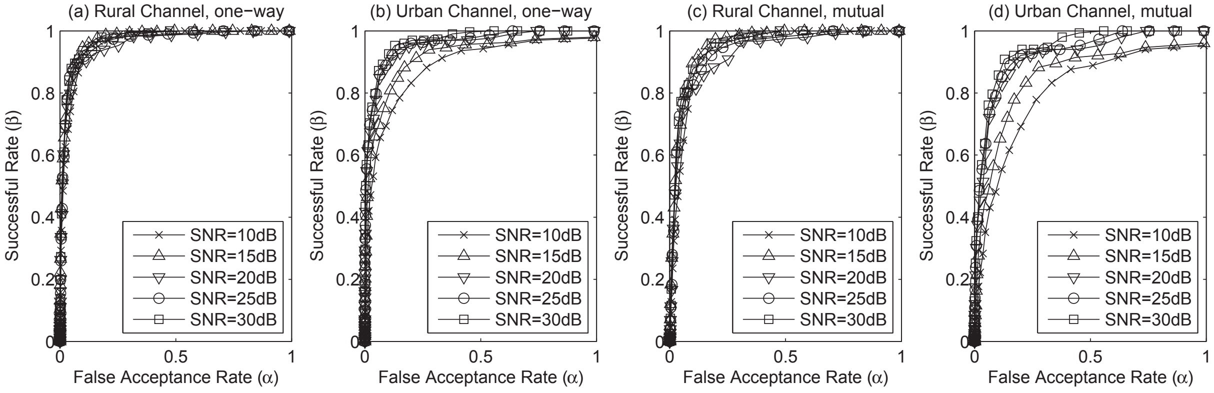

Figure 4.7: ROC curves of PHY-CRAM for one-way (a)(b) and mutual (c)(d) authentication under rural channel (a)(c) and urban channel (b)(d) derived by simulation, with key length M = 60

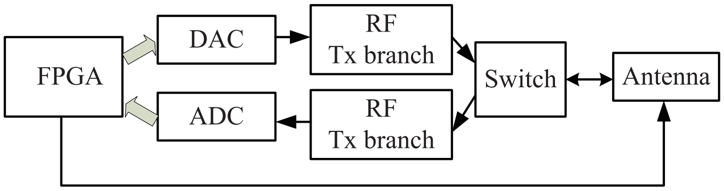

Figure 4.8: Block diagram of the prototype

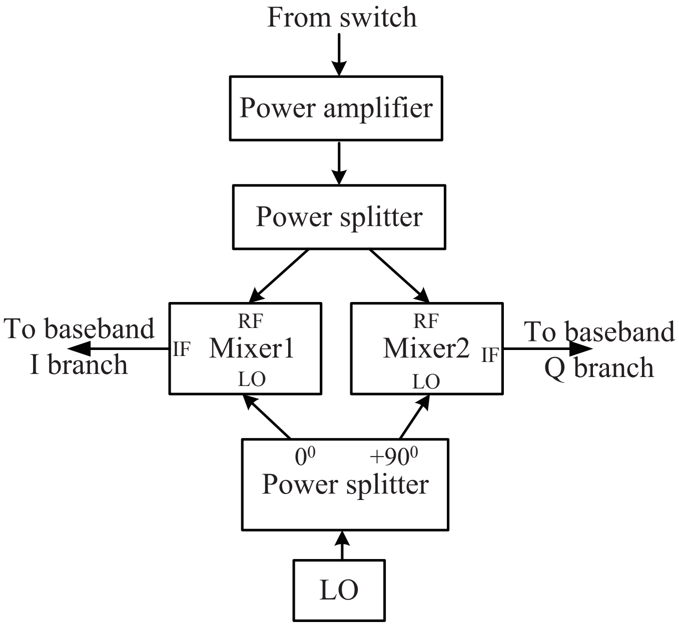

Figure 4.9: Receiver branch of RF circuits designed by discrete RF components

4.5.2 Design of the prototype

Block diagram of the prototype is given in figure 4.8, which is composed of Altera Cyclone III FPGA, analogue-to-digital converter (ADC) and digital-to-analogue converter (DAC) fabricated by ADI, RF circuits, a switch and an antenna. The FPGA features 120K logic elements, 4M memory, 288 multipliers and 531 I/O pins, and is mounted on a Terasic Cyclone III development board, while ADC and DAC on a daughter board are manufactured by the same company. These two boards connect each other through the High Speed Mezzanine Card (HSMC) interface defined by Altera. Analogue inputs/outputs of the daughter board are connected to Rx/Tx branch of RF circuits, which are designed using discrete RF components. These two branches are connected to a switch to realize a half duplex transceiver. On/off state of the switch is controlled by FPGA through I/O pins. Figure 4.8 shows the picture of the whole prototype.

Moreover, principle of Rx branch in the RF circuits is shown in figure 4.9. The RF signal from switch is amplified by one or two low-noise amplifiers (LNAs), split into two identical streams, and sent to the 'RF' ports of two mixers, respectively. Meanwhile, the carrier signal from signal generator (the LO) is sent to another power splitter with 90° phase shift between two outputs, in order to get in-phase and quadrature carriers. Then these two carriers are sent to the 'LO' ports, and the baseband signal with real part (I-branch) and imaginary part (Q-branch) can be derived from the 'IF' ports, of two mixers respectively. The Tx branch has the same structure as that of the Rx branch with different signal directions. The system operates on 2412 MHz which falls into the industrial, scientific and medical (ISM) band. Transmission power for all frames is between -5 dBm to 5 dBm according to the distance between Tx and Rx.

The whole PHY-CRAM mechanism is implemented on FPGA to ensure low processing delay.

4.5.3 The real-world testing

We conduct extensive real-world testing using the prototype to further evaluate PHY-CRAM's performance. Four channel types are considered: line-of-sight (LOS) with 3-meter distance between Tx and Rx (LOS-3m), LOS-6m, non-line-of-sight (NLOS) with 6-meter distance (NLOS-6m), and LOS-28m. The first three channels are inside of a garage with a truck and metal roof, while the last one locates at a courtyard with concrete ground and surrounded by walls. Radios of legitimate users use CP for timing synchronization, while do not conduct frequency offset estimation or compensation. Two sets of prototype acts as B_j and B_k respectively, while other two sets of prototype act as two attackers, who mounts their antennae 10 m and 0.1 m away from B_j respectively. B_k starts the conversation and is identified by B_j, as introduced in subsection 4.3.2. During the authentication procedure, attackers record all the frames and try to figure out $\mathbf{X}_k$. The nearby attacker estimates $\mathbf{X}_k$ according to (4.14) (we call it smart attacker), while the far away attacker generates values for $\mathbf{X}_k$ randomly (we call it naive attacker). The naive attacker defined here helps us to evaluate the upper-bound of PHY-CRAM's performance, as well as to detect any hardware imperfection. Finally, two attackers start their conversations with B_j and uses their estimates on $\mathbf{X}_k$ as the response to B_j's challenge.

Although in real situation B_k only has one set of $\mathbf{X}_k$, 99 different values of $\mathbf{X}_k$ are tested in different runs in order to cover a more general case. In other words, we test 99 different legitimate users with one pair of radios by changing the software, while each user's authentication procedure is repeated for 5 times. The successful authentication rates for all users in all runs in a certain channel are averaged, while results belonging to different channels are separated. SNRs at Rx for all frames are maintained at 15 dB to 20 dB, by adjusting the transmission power and the gain of Rx's LNA. We set $K_1 = 0.5$ and $K_2 = 1.5$ since the frequency-domain channel response on all subcarriers fall in the range of $[0.5, 1.5]$ in most cases in all channel conditions, and $K_2 = 3$. A_{max} is set to 8 due to hardware limitations (mainly due to the maximum range of integers that can be presented by FPGA in our design). All other design parameters adopt the same values as used in the simulations.

We first measure $t_3 - t_1$ (the round-trip latency of one-way authentication defined in figure 4.3) by examining the signal received by passive attackers (the attacker might never expect that it facilitates system testing). It is found that $t_3 - t_1$ is as low as 36 μs, and is pretty stable. This is the benefit we get from FPGA design, with the price of much longer development time compared with that of the digital signal processor (DSP) based solution.

The ROC curves with existence of the naive attacker under four channel types are plotted in figure 4.10, which shows very good performance under all channel types. Successful authentication rate and false acceptance rate follow the same definitions as those in subsection 4.5.1. Performance of PHY-CRAM in short-distance channels is even better than those obtained by simulation, because the delay spreads in these channels are much lower than those assumed in the simulations, and the low-SNR case (SNR=10 dB) is avoided. Figure 4.10 also validates the reciprocal property of the wireless channel, and shows the near-perfect upper-bound of PHY-CRAM's performance in good channel conditions.

The ROC curves with existence of a smart attacker under four channel types are plotted in figure 4.11. Performance differs dramatically in different channels. Short-distance LOS channels show the best performance, followed by short-distance NLOS case. Long distance LOS channel is the worst case, since 0.1 m is too short compared with 28 m, and the approximation in (4.13) becomes more precise. However, the attacker does not always have chance to stay so close to the legitimate user.

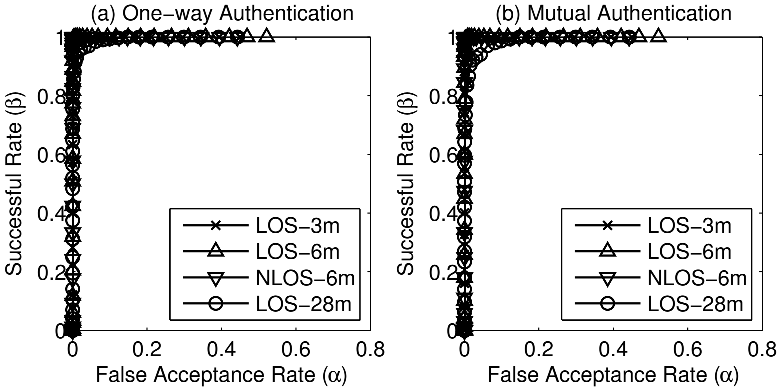

Figure 4.10: ROC curves of PHY-CRAM for one-way (a) and mutual (b) authentication derived from real-world testing under four channels, with existence of a naive attacker

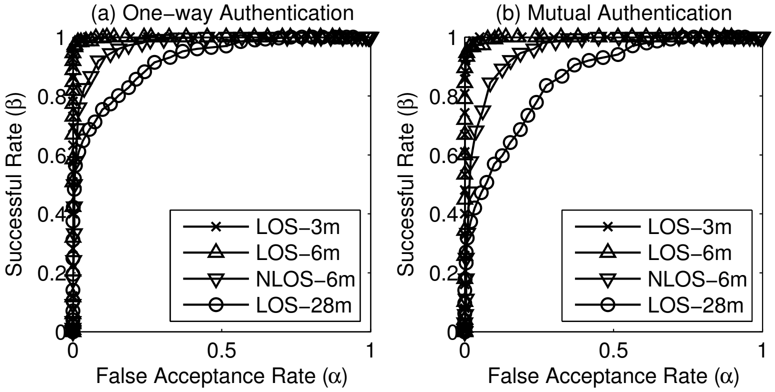

Figure 4.11: ROC curves of PHY-CRAM for one-way (a) and mutual (b) authentication derived from real-world testing under four channels, with existence of a smart attacker

4.5.4 Security analysis

Shared keys are encrypted by the wireless channel in PHY-CRAM, so the security strength of PHY-CRAM is determined by the entropy of wireless channel. The real-world experiments in [118] reveals that, each independent channel provides 4.38 bits of entropy with 0.5 dB quantization accuracy, and 3.5 bits of entropy with 1 dB quantization accuracy, while the quantization accuracy is mainly determined by SNR. In PHY-CRAM, there is no quantization step. However, higher SNR leads to a larger value of C_1 in (4.7), and as a result, more efforts for attackers to forge a shared key that satisfies (4.7); this is equivalent to a larger entropy on the encryption key that secures the shared keys.

Given the works in [118], we make a moderate assumption that each independent channel provides 4 bits of entropy. Then the overall entropy of the wireless channel is determined by the number of independent channels over the frequency band occupied by the wireless network, which equals to W/B_C, where B_C denotes the coherence bandwidth. According to [86], $B_C = 1/(5\sigma_\tau)$, where σ_τ denotes the root mean square (RMS) delay of the wireless channel. For a WiFi system running at 20 MHz bandwidth with $\sigma_\tau = 0.2\ \mu$s, the overall entropy is 80 bits.

Note that the system provided in this chapter is only a baseline of PHY-CRAM. Additional entropy can be obtained by utilizing the time-varying characteristic of the wireless channel, i.e., to partition the shared keys into multiple pieces and conduct authentication for all of them in multiple runs of the baseline PHY-CRAM procedure. The time interval between two runs should be larger than the channel coherence time T_C. In this case, β of each run will be enhanced; this can be easily achieved by increasing SNR or enlarging K_2. Doing this kind of repetition does not leak more information to attackers, but takes more time and consumes more energy.

4.5.5 Comparison with conventional authentication algorithms

Compared with conventional challenge-response authentication schemes, PHY-CRAM consumes less power at transceivers' baseband, due to the missing of channel estimation and frequency offset estimation for all OFDM symbols, and the missing of channel coding and decoding for PHY-CRAM information.

On the flip side, PHY-CRAM requires higher transmission power compared with conventional schemes. For performance comparison, we assume that the length of (encrypted) shared key is 60 bits, $K_2 = 2$, while conventional schemes adopt rate 1/2 convolutional encoder, Viterbi decoder and LMMSE estimator [119]. Conventional schemes need to maintain a BER of 8E-4 to keep β in one-way authentication above 95%, and the corresponding SNR under the rural channels simulated in subsection (4.5.1) is about 10 dB, while PHY-CRAM requires 13-15 dB SNR under the same conditions.

Figure 4.12 gives rough estimation on the dynamic power consumptions of both transceivers with respect to the distance between Tx and Rx, if the baseband of transceiver is designed by FPGA, DSP and application-specific integrated circuit (ASIC), respectively. We consider that dynamic power consumption equals P^{BS} (dynamic power consumed at baseband) plus P^{RF} (dynamic power consumed at RF). In our FPGA design, $P^{BS} \approx 100$ mW, which is about 15 mW less than the power consumption of conventional baseband; this is mainly due to the elimination of Viterbi decoder IP core, which consumes 12 mW dynamic power [120]. DSP design and ASIC design for the same function are believed to consume about 10 times [121] and 10% [122] of the power consumed by FPGA, respectively. We ignore the power consumed at the Rx's RF circuitry and assume that $P^{RF} = \eta P_T$, where η and P_T denote the power efficiency and power level of the RF amplifier at Tx. Moreover, the signal power at Rx with distance d is modelled by $P_T/(L_0 d^{\gamma})$, which must satisfy the SNR requirements (15 dB for PHY-CRAM and 10 dB for conventional system), with L_0 and γ denoting pathloss at $d = 1$m and pathloss exponent, respectively. We assume that $W = 10$ MHz, noise floor equals to -114 dBm/MHz, $\eta = 0.25$, $L_0 = 10^4$, and $\gamma = 3.3$ [123]. Based on these conditions, PHY-CRAM consumes less power than the cryptographic system when communication range is shorter than 20 m, 40 m and 10 m, if FPGA, DSP and ASIC are adopted, respectively.

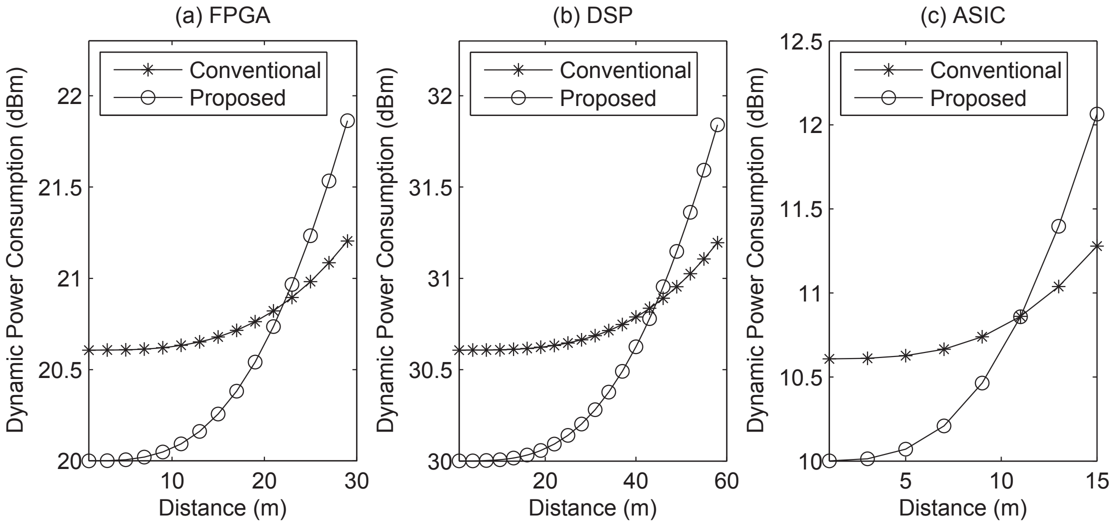

Figure 4.12: Rough estimation on the power consumptions of conventional wireless transceiver during authentication and the transceiver of PHY-CRAM

4.6 Summary

We proposed a novel mutual challenge-response authentication mechanism named PHY-CRAM, which is simple, low-complexity, robust, and flexible. By eliminating any training and synchronization sequences, the CSI is kept secret to attackers, while the transmission of shared keys are secured by CSI. We analyzed the security strength of PHY-CRAM under various attacks. With the existence of a naive feature replay attacker, PHY-CRAM achieves almost perfect performance in dense multipath environments. When there exists a smart attacker, PHY-CRAM still works well under various channel conditions.

Moreover, PHY-CRAM is prototyped by FPGA and discrete RF components. Based on this prototype, we conducted real-world tests to validate PHY-CRAM's performance, and eliminated channel modelling error. These testing results show that the reciprocal property of wireless channel is well maintained when processing delays of the challenge-response signals are less than 40 μs, and that PHY-CRAM is robust under various channel environments.

Security strength of PHY-CRAM increases proportionally to RMS delay and bandwidth of the wireless channel. Energy consumption of PHY-CRAM can be comparable to or even lower than that of cryptographic authentication schemes in short range applications. As a result, PHY-CRAM can be a good alternative to traditional authentication schemes.

CHAPTER 5

Conclusions

Mobile broadband channels, which suffer from time-varying effect and FSF, are experienced by 4G communication systems in mobile environments. We argue that these channels not only increase the complexity of these 4G systems, but also provide new opportunities for information security. The main body of this thesis can be divided into two parts, which discuss challenges and opportunities respectively.

In the first part, a channel estimation algorithm named piece-wise time-invariant approximation (PITIA) is proposed to effectively estimate HST channels which are typical mobile broadband channels. PITIA first identifies a specific feature of HST channels which is not discussed in conventional TVCE algorithm, and adopts a non-linear channel model which has the smallest number of parameters among all channel models. Then this non-linear and time-varying channel model is approximated by a series of linear and time-invariant channels, through which the time-varying effect and FSF are decoupled and estimated separately. This novel design both reduces estimation error and maintains low computation complexity. According to extensive simulation results derived from a self-developed LTE simulator, PITIA outperforms conventional BEM methods in typical HST environments by 5-8 dB in high-SNR regime.

PITIA not only serves as a novel TVCE algorithm, but also showcases a general idea to solve complex problems: dividing the whole task into multiple simpler ones and solving them individually. The same idea may apply to other fields of studies, for example, non-linear system analysis where the non-linear system may be approximated by a series of linear systems and analysed one by one. Performances of PITIA can be further enhanced by several ways: (1) more advanced non-linear signal processing techniques may be adopted to reduce the extra noise generated during channel reconstruction; (2) interference coming from data symbols may also be reduced by joint channel estimation and data detection algorithms. Moreover, PITIA is not fully compatible with LTE specification, since PITIA requires that pilots are surrounded by nulls while LTE is not designed like this. Compatibility with commercial OFDM systems is still a challenge for most TVCE algorithms.

In the second part, we devise the first non-cryptographic challenge-response authentication mechanism (PHY-CRAM) to leverage new opportunities. During authentication, no pilot is transmitted, and the shared keys between both participants are randomized by mobile broadband channels. The FSF's perceived by both participants at the same time are identical and cancelled by an division operation, while an eavesdropper, locating at a different place for sure and perceiving different FSF, can neither estimate channel nor decode shared keys. Performance of PHY-CRAM is evaluated by a FPGA-based hardware platform and real-world experiments, which validate that PHY-CRAM achieves very high successful authentication rate when false acceptance rate is very low, even if there is an eavesdropper nearby. Moreover, PHY-CRAM achieves higher energy efficiency in small-scale networks compared with cryptographic authentication protocols, and finds applications in WLAN and DSRC.

PHY-CRAM validates the previously mentioned concept that mobile broadband channels benefit information security, and we believe that these channels may also benefit other fields of studies, for examples, information forensics and localization. PHY-CRAM adopts the FSF channel model which does not fully utilize the randomness of mobile broadband channels, while the DSF channel model is a better but more challenging choice. Furthermore, the phases in channel responses are abandoned in PHY-CRAM, since they are sensitive to timing synchronization error and hardware imperfection, and may not be perfectly cancelled. The performance of PHY-CRAM may be enhanced by further addressing these issues.

Finally, the thesis is concluded by a philosophy that, challenges and opportunities are two sides of a coin, and researchers should never be frustrated by the sophistication of the nature.

Bibliography

[1] D. Shan, P. Richardson, W. Xiang, and K. Zeng, "Time-varying channel estimation through optimal piece-wise time-invariant approximation for high-speed train wireless communications," *Under review by Vehicular Communications, Elsevier*.

[2] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "Phy-cram: Physical layer challenge-response authentication mechanism for wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1817–1827, Sep 2013.

[3] H. Rohling, T. May, K. Bruninghaus, and R. Grunheid, "Broad-band ofdm radio transmission for multimedia applications," *Proceedings of the IEEE*, vol. 87, no. 10, pp. 1778–1789, 1999.

[4] W.-S. Hou and B.-S. Chen, "Ici cancellation for ofdm communication systems in time-varying multipath fading channels," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 5, pp. 2100– 2110, Sep 2005.

[5] L. Scharf, *Statistical Signal Processing - Detection, Estimation, and Time Series Analysis*. New York: Addison-Weslay, 1991.

[6] W. Hong, "A frequency offset estimation architecture of ofdm system in multipath doppler spread channel," in *Signals, Systems, and Computers, 1999. Conference Record of the Thirty-Third Asilomar Conference on*, Oct 1999.

[7] N. Zheng Du; Xuegui Song; Cheng, J.; Beaulieu, "Maximum likelihood based channel estimation for macrocellular ofdm uplinks in dispersive time-varying channels," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 1, pp. 176–187, Jan 2011.

[8] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 111–122. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287867

[9] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 26–37. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409949

[10] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 401–410.

[11] Suhas Mathur and Wade Trappe and Narayan Mandayam and Chunxuan Ye and Alex Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom 2008*, 2008, pp. 128–139.

[12] 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 *Proceedings of the 15th annual international conference on Mobile computing and networking MobiCom '09*, 2009, pp. 321–332.

[13] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *IEEE Infocom 2010*, March 2010.

[14] J. C. Klensin, R. Catoe, and P. Krumviede, "Imap/pop authorize extension for simple challenge/response," *RFC 2195*, September 1997.

[15] K. Fox and W. A. Simpson, "Ppp challenge handshake authentication protocol (chap)," *RFC 1994*, August 1996.

[16] D. Shan, P. Richardson, W. Xiang, and A. V. Vasilakos, "Time-varying channel estimation for ofdm with extended observation window," in *VANET '12 Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, June 2012.

[17] W. X. Dan Shan, Paul Richardson and K. Zeng, "Time-varying channel estimation through optimal piece-wise time-invariant approximation for high-speed train wireless communications," *submitted to Vehicular Communications, Elsevier*, 2014.

[18] K. Z. Xianru Du, Dan Shan and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *to appear in IEEE Infocom*, 2014.

[19] W. X. D. S. J. Yuan and S. Addepalli, "A full functional wireless access for vehicular environments (wave) prototype upon the ieee 802.11p standard for vehicular communications and networks," in *Consumer Communications and Networking Conference (CCNC)*, 2012.

[20] P. R. Dan Shan, Kai Zeng and W. Xiang, "Detecting multi-channel wireless microphone user emulation attacks in white space with noise," in *9th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM)*, 2013.

[21] ——, “isens: Detecting hidden busy channels in wm systems with interactive sensing for crn,” in *IEEE Globecom*, 2013.

[22] X. G. Doukopoulos, Moustakides, and G. V. ;, “Blind adaptive channel estimation in ofdm systems,” *Wireless Communications, IEEE Transactions on*, vol. 5, no. 7, pp. 1716–1725, Jul. 2006.

[23] F. Gao, Y. Zeng, N. A., and T.-S. Ng;, “Robust subspace blind channel estimation for cyclic prefixed MIMO ODFM systems: algorithm, identifiability and performance analysis,” *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 2, pp. 378–388, Feb. 2008.

[24] Y. Xie and C. N. . Georghiades, “Two EM-type channel estimation algorithms for OFDM with transmitter diversity,” *Communications, IEEE Transactions on*, vol. 51, no. 1, pp. 106–115, Jan. 2003.

[25] J. Akhtman and L. Hanzo, “Decision directed channel estimation aided OFDM employing sample-spaced and fractionally-spaced CIR estimators,” *Wireless Communications, IEEE Transactions on*, vol. 6, no. 4, pp. 1171–1175, Apr. 2007.

[26] J. Ylioinas and M. Juntti, “Iterative joint detection, decoding, and channel estimation in turbo-coded MIMO-ofdm,” *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 4, pp. 1784–1796, May 2009.

[27] Y. Li, J. Cimini, L.J., and N. Sollenberger, “Robust channel estimation for ofdm systems with rapid dispersive fading channels,” *Communications, IEEE Transactions on*, vol. 46, no. 7, pp. 902–915, 1998.

[28] M.-H. Hsieh and C.-H. Wei;, “Channel estimation for OFDM systems based on comb-type pilot arrangement in frequency selective fading channels,” *Consumer Electronics, IEEE Transactions on*, vol. 44, no. 1, pp. 217–225, Feb. 1998.

[29] M. Morelli, Mengali, and U. ;, “A comparison of pilot-aided channel estimation methods for OFDM systems,” *Signal Processing, IEEE Transactions on*, vol. 49, no. 12, pp. 3065–3073, Dec. 2001.

[30] J. J. van de Beek, O. Edfors, M. Sandell, S. Wilson, and P. Borjesson, “On channel estimation in ofdm systems,” in *Vehicular Technology Conference, 1995 IEEE*, no. 2, 1995, pp. 815–819.

[31] J. K. Moon and S. I. Choi, “Performance of channel estimation methods for OFDM systems in a multipath fading channels,” *Consumer Electronics, IEEE Transactions on*, vol. 46, no. 1, pp. 161–170, Feb. 2000.

[32] Z. Yuanjin, “A novel channel estimation and tracking method for wireless OFDM systems based on pilots and Kalman filtering,” in *Circuits and Systems*, vol. 2, 2003.

[33] Y. Li, “Pilot-symbol-aided channel estimation for OFDM in wireless systems,” *Vehicular Technology, IEEE Transactions on*, vol. 49, no. 4, pp. 1207–1215, 2000.

[34] S. Coleri, Ergen, M., Puri, A., Bahai, and A. ;, “Channel estimation techniques based on pilot arrangement in OFDM systems,” *Broadcasting, IEEE Transactions on*, vol. 48, no. 3, pp. 223–229, Sep. 2002.

[35] F. Shu, J. Lee, L.-N. Wu, and G.-L. Zhao, “Time-frequency channel estimation for digital amplitude modulation broadcasting systems based on ofdm,” *Communications, IEE Proceedings*, vol. 150, no. 4, pp. 259–264, Aug. 2003.

[36] S. G. K. Y. M. H. E. K. Joo;, “A comparative investigation on channel estimation algorithms for OFDM in mobile communications,” *Broadcasting, IEEE Transactions on*, vol. 49, no. 2, pp. 142–149, Jun. 2003.

[37] M.-X. Chang and Y. Su, “Model-based channel estimation for ofdm signals in rayleigh fading,” *Communications, IEEE Transactions on*, vol. 50, no. 4, pp. 540–544, Apr. 2002.

[38] Z. Wang, Y. Xin, Mathew, G., and X. Wang, “A low-complexity and efficient channel estimator for multiband OFDM-uwb systems,” *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 3, pp. 1355–1366, Mar. 2010.

[39] Y. Li and J. Cimini L. J., “;,.”

[40] ——, “Impact of carrier frequency offset, doppler spread and time synchronisation errors in ofdm based single frequency networks,” in *GLOBECOM ’00*, vol. 1, 1996, pp. 18–22.

[41] S. Tang, Gong, K., Song, J., Pan, C., Yang, and Z., “Intercarrier interference cancellation with frequency diversity for OFDM systems,” *Broadcasting, IEEE Transactions on*, vol. 53, no. 1, pp. 132–137, Mar. 2007.

[42] Y. Zhao, Haggman, and S. G., “Intercarrier interference self-cancellation scheme for OFDM mobile communication systems,” *Communications, IEEE Transactions on*, vol. 49, no. 7, pp. 1185–1191, 2001.

[43] H.-G. Ryu, Y. Li, and J.-S. Park, “An improved ici reduction method in ofdm communication system,” *Broadcasting, IEEE Transactions on*, vol. 51, no. 3, pp. 395–400, 2005.

[44] W.-G. Song and J.-T. Lim;, “Channel estimation and signal detection for MIMO-OFDM with time varying channels,” *Communications Letters, IEEE*, vol. 10, no. 7, pp. 540–542, Jul. 2006.

[45] M. Gudmundson and P. O. Anderson, “Adjacent channel interference in an OFDM system,” in *IEEE 46th Vehicular Technology Conf.*, Apr. 1996, pp. 918–922.

[46] A. Seyedi and S. G. J. ;, “General ICI self-cancellation scheme for OFDM systems,” *Vehicular Technology, IEEE Transactions on*, vol. 54, no. 1, pp. 198–210, Jan. 2005.

[47] W.-S. Hou and B.-S. Chen;, “Ici cancellation for OFDM communication systems in time-varying multipath fading channels,” *Wireless Communications, IEEE Transactions on*, vol. 4, no. 5, pp. 2100–2110, 2005.

[48] H.-C. Wu, X. Huang, and D. Xu;, “Novel semi-blind ICI equalization algorithm for wireless OFDM systems,” *Broadcasting, IEEE Transactions on*, vol. 52, no. 2, pp. 211–218, Jun. 2006.

[49] W. G. Jeon, K. H. Chang, and Y. S. Cho;, “An equalization technique for orthogonal frequency-division multiplexing systems in time-variant multipath channels,” *Communications, IEEE Transactions on*, vol. 47, no. 1, pp. 27–32, Jan. 1999.

[50] Y. S. Choi, P. J. Voltz, and F. A. Cassara, “On channel estimation and detection for multicarrier signals in fast and selective rayleigh fading channels,” *IEEE Trans. Commun.*, vol. 49, no. 8, pp. 1375–1387, Aug. 2001.

[51] Y. K. K. Park, J.-H.; Whang, “Low complexity mmse-sic equalizer employing time-domain recursion for ofdm systems,” *Signal Processing Letters, IEEE*, vol. 15, pp. 633–636, 2008.

[52] S. U. Hwang, J. H. Lee, and J. Seo;, “Low complexity iterative ICI cancellation and equalization for OFDM systems over doubly selective channels,” *Broadcasting, IEEE Transactions on*, vol. 55, no. 1, pp. 132–139, Mar. 2009.

[53] G. Leus, “On the estimation of rapidly time-varying channels,” in *Euro. Signal Process. Conf. (EUSIPCO)*. EURASIP, September 2004.

[54] D. K. Borah and B. D. Hart, “Frequency-selective fading channel estimation with a polynomial time-varying channel model,” *IEEE Trans. Commun.*, vol. 47, no. 6, pp. 862–873, June 1999.

[55] T. Zemen and C. Mecklenbrauker, “Time-variant channel estimation using discrete prolate spheroidal sequences,” *Signal Processing, IEEE Transactions on*, vol. 53, no. 9, pp. 3597–3607, Sept 2005.

[56] M. Visintin, “Karhunen-loeve expansion of a fast rayleigh fading process,” *IEEE Electron. Lett.*, vol. 32, no. 8, pp. 1712–1713, Aug 1996.

[57] J. K. Tugnait and W. Luo, "Linear prediction error method for blind identification of periodically time-varying channel," *IEEE Trans. Signal Process.*, vol. 50, no. 12, pp. 3070–3082, December 2002.

[58] Z. Tang, R. Cannizzaro, G. Leus, and P. Banelli, "Pilot-assisted time-varying channel estimation for ofdm systems," *IEEE Trans. Signal Process.*, vol. 55, no. 5, pp. 2226–2238, May 2007.

[59] X. Ma, G. Giannakis, and S. Ohno, "Optimal training for block transmissions over doubly selective wireless fading channels," *IEEE Trans. Signal Process.*, vol. 51, no. 5, pp. 1351–1366, May 2003.

[60] M. Rabbi, S.-W. Hou, and C. Ko, "High mobility orthogonal frequency division multiple access channel estimation using basis expansion model," *Communications, IET*, vol. 4, no. 3, pp. 353–367, February 2010.

[61] T. Hrycak, S. Das, G. Matz, and H. Feichtinger, "Practical estimation of rapidly varying channels for ofdm systems," *Communications, IEEE Transactions on*, vol. 59, no. 11, pp. 3040–3048, November 2011.

[62] P. Wan, M. McGuire, and X. Dong, "Near-optimal channel estimation for ofdm in fast-fading channels," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 8, pp. 3780–3791, Oct. 2011.

[63] A. Kannu and P. Schniter, "Design and analysis of mmse pilot-aided cyclic-prefixed block transmissions for doubly selective channelss," *Signal Processing, IEEE Transactions on*, vol. 56, no. 3, pp. 1148–1160, March 2008.

[64] H. Senol, E. Panayirci, and H. Poor, "Nondata-aided joint channel estimation and equalization for ofdm systems in very rapidly varying mobile channels," *Signal Processing, IEEE Transactions on*, vol. 60, no. 8, pp. 4236–4253, Aug 2012.

[65] H. C. Lee, C.-W. Chen, and S.-W. Wei, "Channel estimation for ofdm system with two training symbols aided and polynomial fitting," *Communications, IEEE Transactions on*, vol. 58, no. 3, pp. 733–736, March 2010.

[66] J. Tugnait and W. Luo, "Linear prediction error method for blind identification of periodically time-varying channels," *Signal Processing, IEEE Transactions on*, vol. 50, no. 12, pp. 3070– 3082, Dec 2002.

[67] R. Carrasco-Alvarez, R. Parra-Michel, A. Orozco-Lugo, and J. Tugnait, "Time-varying channel estimation using two-dimensional channel orthogonalization and superimposed training," *Signal Processing, IEEE Transactions on*, vol. 60, no. 8, pp. 4439–4443, Aug 2012.

[68] P. Schniter, "Low-complexity equalization of ofdm in doubly selective channels," *Signal Processing, IEEE Transactions on*, vol. 52, no. 4, pp. 1002– 1011, April 2004.

[69] T. Hrycak, S. Das, G. Matz, and H. Feichtinger, "Low complexity equalization for doubly selective channels modeled by a basis expansion," *Signal Processing, IEEE Transactions on*, vol. 58, no. 11, pp. 5706–5719, Nov 2010.

[70] Y. Mostofi and D. Cox, "Ici mitigation for pilot-aided ofdm mobile systems," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 2, pp. 765–774, March 2005.

[71] M. K. Tsatsanis and G. B. Giannakis, "Modeling and equalization of rapidly fading channels," *Int. J. Adapt. Control Signal Process.*, vol. 10, pp. 159–176, March 1996.

[72] E. Panayirci, H. Senol, and H. V. Poor, "Joint channel estimation, equalization and data detection for ofdm systems in the presence of very high mobility," *IEEE Trans. Signal Process.*, vol. 58, no. 8, pp. 4225–4238, Aug 2010.

[73] R. Schmidt, "Multiple emitter location and signal parameter estimation," *Antennas and Propagation, IEEE Transactions on*, Mar 1986.

[74] A. Paulraj, R. Roy, and T. Kailath, "Estimation of signal parameters via rotational invariance techniques- esprit," *Circuits, Systems and Computers, 1985. Nineteeth Asilomar Conference on*, Nov 1985.

[75] L. Yang, G. Ren, and Z. Yang, B.; Qiu, "Fast time-varying channel estimation technique for lte uplink in hst environment," *Vehicular Technology, IEEE Transactions on*, Aug 2012.

[76] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.

[77] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *In Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2008.

[78] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy, "Attacks on physical-layer identification," in *WiSec '10: Proceedings of the 3th ACM Conference on Wireless Network Security*. ACM, 2010, pp. 89–98.

[79] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," vol. 7, no. 7, pp. 2571–2579, July 2008.

[80] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1921927.1921939

[81] Y. Liu and P. Ning, "Enhanced wireless channel authentication using time-synched link signature," in *IEEE International Conference on Computer Communications (INFOCOM'12), Mini-Conference,*, 2012.

[82] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 1, pp. 38 –51, march 2008.

[83] N. Goergen, W. Lin, K. Liu, and T. Clancy, "Extrinsic channel-like fingerprint embedding for authenticating mimo systems," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 12, pp. 4270 –4281, december 2011.

[84] Y. Liu and P. Ning, "Poster: Mimicry attacks against wireless link signature," in *16th ACM Conference on Computer and Communications Security (CCS'11)*, 2011.

[85] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *The 17th European Symposium on Research in Computer Security (ESORICS)*, sep 2012.

[86] *Mobile Cellular Telecommunications Systems*. Mcgraw Hill, 1989.

[87] "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements; part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications; amendment 6: Wireless access in vehicular environments," in *IEEE Std. 802.11p*, July 2010.

[88] R. Sevlian, C. Chun, I. Tan, A. Bahai, and K. Laberteaux, "Channel characterization for 700 mhz dsrc vehicular communication," *Journal of Electrical and Computer Engineering*, 2010.

[89] Y.-S. Choi, P. Voltz, and F. Cassara, "On channel estimation and detection for multicarrier signals in fast and selective rayleigh fading channels," *Communications, IEEE Transactions on*, vol. 49, no. 8, pp. 1375–1387, Aug 2001.

[90] F. Bai, D. D. Stancil, and H. Krishnan, "Toward understanding characteristics of dedicated short range communications (dsrc) from a perspective of vehicular network engineers," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, 2010, pp. 329–340.

[91] P. K. et al., "Winner ii channel models," 2007.

[92] "Lte - evolved universal terrestrial radio access (e-utra) - physical channels and modulation," in *3GPP TS 36.211*, 2011.

[93] 3GPP, "Tr 25.943: Technical specification group radio access networks - deployment aspects," 3GPP, Tech. Rep., 2009.

[94] V. Riihimaki, T. Vaaramaki, J. Vartiainen, and T. Korhonen, "Techno-economical inspection of high-speed internet connection for trains," *Intelligent Transport Systems, IET*, vol. 2, no. 1, pp. 27–37, March 2008.

[95] O. J. L. C. W. Karimi, "Seamless wireless connectivity for multimedia services in high speed trains," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 4, pp. 729–739, may 2012.

[96] "Ieee802.16-2004, ieee standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems," July 2004.

[97] J. Qiu, C. Tao, L. Liu, and Z. Tan, "Broadband channel measurement for the high-speed railway based on wcdma," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*. IEEE, May 2012.

[98] H. Wei, Z. Zhong, K. Guan, and B. Ai, "Path loss models in viaduct and plain scenarios of the high-speed railway," in *CHINACOM*. IEEE, Aug 2010.

[99] Y. Li and J. Cimini, L.J., "Interchannel interference of ofdm in mobile radio channels," in *Global Telecommunications Conference, 2000. GLOBECOM '00*. IEEE, December 2000, pp. 706–710.

[100] W. C. Jakes, *Microwave Mobile Channels*. New York: Wiley, 1974.

[101] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," in *IEEE International Conference on Communications, ICC*, May 2008, pp. 1520–1524.

[102] R. Hippenstiel and Y. Payal, "Wavelet based transmitter identification," in *Signal Processing and Its Applications, 1996. ISSPA 96., Fourth International Symposium on*, vol. 2, aug. 1996, pp. 740 –742.

[103] B. Danev and S. Čapkun, "Transient-based identification of wireless sensor nodes," in *IPSN '09: Proceedings of the 8th IEEE/ACM Information Processing in Sensor Networks*. IEEE/ACM, 2009, pp. 25–36.

[104] A. Mikkilineni, "Forensic characterization of rf devices," in *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on*, Dec 2009, pp. 26–30.

[105] K. Zeng, K. Govindan, D. Wu, and P. Mohapatra, "Identity-based attack detection in mobile wireless networks," in *INFOCOM, 2011 Proceedings IEEE*, april 2011, pp. 1880 –1888.

[106] J. Hall, “Enhancing intrusion detection in wireless networks using radio frequency fingerprinting,” in *In Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT*. Kranakis, 2004, pp. 201–206.

[107] P. Harmer, M. Williams, and M. Temple, “Using de-optimized lfs processing to enhance 4g communication security,” in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, 2011, pp. 1–8.

[108] D. R. Reising, M. A. Temple, and M. J. Mendenhall, “Improving intra-cellular security using air monitoring with rf fingerprints,” in *Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–6.

[109] Z. Li, W. Trappe, Y. Zhang, and B. Nath;, “Robust statistical methods for securing wireless localization in sensor networks,” in *Information Processing in Sensor Networks, 2005. IPSN 2005*, 2005, pp. 91–98.

[110] S.-P. Kuo and Y.-C. Tseng, “Discriminant minimization search for large-scale rf-based localization systems,” *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 291–304, Feb 2011.

[111] T. Wang, J. Proakis, E. Masry, and J. Zeidler, “Performance degradation of ofdm systems due to doppler spreading,” *Wireless Communications, IEEE Transactions on*, vol. 5, no. 6, pp. 1422–1432, June 2006.

[112] P. Tan and N. C. Beaulieu, “Precise ber analysis of 4-dqpsk ofdm with carrier frequency offset over frequency selective fast fading channels,” *Wireless Communications, IEEE Transactions on*, Oct 2007.

[113] D. Lee and K. Cheun, “A new symbol timing recovery algorithm for ofdm systems,” *Consumer Electronics, IEEE Transactions on*, vol. 43, no. 3, pp. 767–775, Aug 1997.

[114] M. Morelli and U. Mengali, “A comparison of pilot-aided channel estimation methods for ofdm systems,” *Signal Processing, IEEE Transactions on*, vol. 49, no. 12, pp. 3065–3073, Dec 2001.

[115] B. Yang, K. Letaief, R. Cheng, and Z. Cao, “Timing recovery for ofdm transmission,” *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 11, pp. 2278–2291, Nov 2000.

[116] Y. Mostofi and D. C. Cox, “A robust timing synchronization design in ofdm systems part i: Low-mobility cases,” *Wireless Communications, IEEE Transaction on*, Dec 2007.

[117] J. Hall, M. Barbeau, and E. Kranakis, "Detecting rogue devices in bluetooth networks using radio frequency fingerprinting," in *In IASTED International Conference on Communications and Computer Networks*, 2006.

[118] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret keys from entangled sensor motes: Implementation and analysis," in *Proceedings of the Third ACM Conference on Wireless Network Security (WiSec '10).* ACM, mar 2010, pp. 139–144.

[119] M.-H. Hsieh and C.-H. Wei, "Channel estimation for ofdm systems based on comb-type pilot arrangement in frequency selective fading channels," in *Consumer Electronics, IEEE Transactions on*, vol. 44, Feb. 1998, pp. 217–225.

[120] S. Shaker, S. Elramly, and K. Sheriata, "Fpga implementation of a reconfigurable viterbi decoder for wimax receiver," in *Microelectronics (ICM), 2009 International Conference on*, 2009, pp. 264–267.

[121] H. K. Boyapati and R. V. R. Kumar, "A comparison of dsp, asic, and risc dsp based implementations of multiple access in lte," in *Communications, Control and Signal Processing (ISCCSP), 2010 4th International Symposium on*, 2010, pp. 1–5.

[122] I. Kuon, I. Kuon, and J. Rose, "Measuring the gap between fpgas and asics," in *FPGA '06 Proceedings of the 2006 ACM/SIGDA 14th international symposium on Field programmable gate arrays*, 2006, pp. 21–30.

[123] H. Hashemi, "The indoor radio propagation channel," *Proceedings of the IEEE*, vol. 81, no. 7, pp. 943–968, July 1993.