2011

Addressing/Exploiting Transceiver Imperfections in Wireless Communication Systems

Lihao Wang
University of Massachusetts Amherst

ADDRESSING/EXPLOITING TRANSCEIVER IMPERFECTIONS IN WIRELESS COMMUNICATION SYSTEMS

A Thesis Presented

by

LIHAO WANG

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

September 2011

Electrical and Computer Engineering

ADDRESSING/EXPLOITING TRANSCEIVER IMPERFECTIONS IN WIRELESS COMMUNICATION SYSTEMS

A Thesis Presented

by

LIHAO WANG

Approved as to style and content by:

Dennis L. Geockel, Chair

Robert W. Jackson, Member

Patrick A. Kelly, Member

C. V. Hollot, Department Head
Electrical and Computer Engineering

To my family

ACKNOWLEDGMENTS

In the first place, I would like to thank Professor Dennis Goeckel to give me an opportunity to be part of his research group. Professor Goeckel makes a complete role model for advisor-advisee interactions. His advice and direction is invaluable and gratefully appreciated. Thank you also to Professor Jackson for providing me assistance and knowledge to model the envelope detector. I am also grateful to Professor Kelly for being such a great teacher on digital signal processing.

I would also like to thank the members of the Wireless Systems Lab who constantly help me and encourage me to move forward. Thanks to my family and friends for their encouraging support and motivation as well.

Finally, I would also like to convey thanks to Analog Devices and NSF for financial support.

ABSTRACT

ADDRESSING/EXPLOITING TRANSCEIVER IMPERFECTIONS IN WIRELESS COMMUNICATION SYSTEMS

SEPTEMBER 2011

LIHAO WANG

B.S., UNIVERSITY OF JINAN

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Dennis L. Geockel

This thesis consists of two research projects on wireless communication systems. In the first project, we propose a fast inphase and quadrature (I/Q) imbalance compensation technique for the analog quadrature modulators in direct conversion transmitters. The method needs no training sequence, no extra background data gathering process and no prior perfect knowledge of the envelope detector characteristics. In contrast to previous approaches, it uses points from both the linear and predictable nonlinear regions of the envelope detector to hasten convergence. We provide a least mean square (LMS) version and demonstrate that the quadrature modulator compensator converges.

In the second project, we propose a technique to deceive the automatic gain control (AGC) block in an eavesdropper's receiver to increase wireless physical layer data transmission secrecy. By sharing a key with the legitimate receiver and fluctuating

the transmitted signal power level in the transmitter side, a positive average secrecy capacity can be achieved even when an eavesdropper has the same or even better additive white gaussian noise (AWGN) channel condition. Then, the possible options that an eavesdropper may choose to fight against our technique are discussed and analyzed, and approaches to eliminate these options are proposed. We demonstrate that a positive average secrecy capacity can still be achieved when an eavesdropper uses these options.

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

1.1 Motivation

In a world of increasing mobility, the demand for wireless communication systems has led to a better understanding of fundamental issues in communication theory. However, most communication theory works with idealized transceiver assumptions neglecting imperfections and defects of practical transceiver designs. In reality, there exists challenges and opportunities in understanding wireless transceiver non-idealities.

For direct conversion transceivers, a prerequisite of digital predistortion of the power amplifier nonlinear transfer function is compensating inphase and quadrature (I/Q) imbalance in transmitters. In order to predistort the power amplifier within a reasonable number of iterations, the error figure (EF) should be mitigated below the level in (1.1) [1]:

$$EF = \frac{\varepsilon^2 + \varphi^2}{4} + \frac{c_1^2 + c_2^2}{P_q} < 10^{-4} \tag{1.1}$$

where ε, φ, c_1 and c_2 are the gain imbalance (ε), phase imbalance (φ) and dc-offsets (c_1, c_2), respectively, and P_q is the average power at the quadrature modulator (QM) output. In this thesis, such an I/Q imbalance compensation technique is designed and analyzed.

Another important issue considered in this thesis is whether we can utilize the defects of practical receivers to increase data transmission security. Most of the former information theoretical approaches based on idealized transceiver assumptions have few concerns about the defects of RF receiver front-ends. In this thesis, we analyze the

practical design of an eavesdropper's RF receiver front-end and propose a technique to deceive it.

Therefore, this thesis can be classified into two parts:

1. An inphase and quadrature(I/Q) imbalance compensation technique for the analog quadrature modulators in direct conversion transmitters.

2. A technique to deceive the automatic gain control(AGC) block in an eavesdropper's receiver to increase wireless physical layer data transmission secrecy.

1.1.1 Imperfections in Direct Conversion Transmitters

Direct conversion transmitters are attractive due to increased efficiency and hardware simplicity. However, their use is limited because of I/Q imbalance in analog quadrature modulators. Although I/Q imbalance compensation is a topic which often appears in the literature, most of these approaches concern compensation methods in the receiver, but compensation methods for the transmitter are a significant issue as well.

In the transmitter, to achieve linearization of the power amplifier, which is another important step to increase the performance of direct conversion transmitters, the I/Q imbalance should first be mitigated, because its presence makes perfect predistortion for linearizaton impossible. Therefore, in the first part of our thesis, we will address this issue and propose an I/Q imbalance compensation technique for the transmitter that converges more rapidly than previously proposed methods.

1.1.2 Physical Layer Security

Wireless communications, which are particularly susceptible to eavesdropping because of the broadcast nature of the transmission medium, continue to flourish worldwide. Therefore, the encryption for securing information in wireless systems has taken on an increasingly important role. In general, encryption is done above the physical layer with powerful cyphers using cryptographic protocols (e.g., RSA and AES). In

contrast, theoretical physical layer security contributions, which builds on Shannon's notion of perfect secrecy[19], significantly strengthen the security of digital communication systems. In spite of numerous theoretical contributions, the consideration of implementation aspects of a practical eavesdropper receiver, which may have some defects that could be utilized to decrease the signal-to-noise ratio (SNR) of its received signal, has not received much attention.

For a digital communication system, the analog-to-digital converter in the receiver has a fixed dynamic range. However, the received signal varies over a wider range. Therefore, an automatic gain control (AGC) circuit is necessary before the analog-to-digital converter (ADC) to keep the signal amplitude at a apriori fixed level. There exists several works [11][12][13][14] on designing a decibel-based linear AGC system with constant settling time which operates as a high pass filter. In the settling period of the AGC, the signal amplitude may be outside the apriori fixed level and cause clipping of the ADC, which introduces a large amount of quantization noise. Thus, our approach to artificially change the transmitted signal amplitude level may deceive the AGC-ADC cascade in the eavesdropper.

1.2 Contribution

The main contribution in the first part of the thesis is a faster I/Q imbalance compensation technique, which employs a more accurate parametrization that accounts for both the linear and square law regions of the envelope detector. The method needs no training sequence, no extra background data gathering process and no prior perfect knowledge of the envelope detector characteristics. Part two of the thesis contributes towards a thorough analysis of a typical eavesdropper's receiver RF front-end, especially the AGC system block. We propose a varied power amplification technique which could deceive the AGC-ADC cascade in the eavesdropper's receiver while maintaining the function of the legitimate receiver. It is shown that a

positive average secrecy capacity can be achieved even if the legitimate receiver Bob has no additive white gaussian noise (AWGN) channel signal-to-noise ratio (SNR) advantage. The technique successfully turns a short-term cryptographic advantage into everlasting security.

1.3 Organization

This thesis is organized broadly in two sections. Chapter 2 is the first section of the thesis and presents the I/Q imbalance compensation technique. In Chapter 2, the operating characteristic of the envelope detector is analyzed and an adaptation algorithm employing sample points falling into the envelope detector's linear and square law regions is proposed. Then, we prove that the proposed algorithm has a least mean square (LMS) implementation that drives the overall impairments in the quadrature modulator compensator (QMC) and quadrature modulator (QM) cascade to zero. Chapter 3 considers considering physical layer secrecy issues. The AGC block of the eavesdropper receiver is analyzed and a technique to deceive the AGC-ADC cascade of the eavesdropper receiver is proposed. Then, the possible options that Eve may use to fight against the proposed technique are discussed and eliminated. Chapter 4 summarizes our thesis work based on the results from Chapter 2 and 3.

CHAPTER 2

I/Q IMBALANCE COMPENSATION

2.1 Introduction

Analog quadrature modulators (QM) are commonly implemented in direct conversion transceiver designs due to their wider bandwidth and lower power consumption compared to all-DSP based approaches [2]. However, they have three principle impairments [3]: gain imbalance, phase imbalance and dc-offset, which can have a devastating effect on amplifier linearization circuits. There are several existing compensation techniques [2][3][4][5][6] that employ a digital signal processor (DSP) or analog circuit. Most of these approaches are adaptive to maintain acceptable performance quality, because these impairments are expected to change with temperature, channel frequency and device biasing [4]. In [7] and [8], a recursive least squares (RLS) method and an adaptive traditional least mean square (LMS) method have been proposed respectively, both of which can adapt from random transmitted data and need no prior knowledge of the envelope detector's characteristic. These approaches simplify algorithm development by only using sample points that fall into the envelope detector's linear region, and the remainder of the points are ignored.

2.2 System Model

The model of the amplifier linearization loop based on predistortion used in [7] is considered in this letter, as shown in Fig. 2.1. $v_d(t)$ is the baseband signal after predistortion and $v_q(t)$ is the complex bandpass signal. There are two feedback loops

in the system model: the first is for predistorter (PD) adaptation with a quadrature demodulator (QDM) and its compensator (QDMC); the other loop is for QM compensator (QMC) adaptation with an envelope detector. This chapter focuses on the latter one, which drives the complex bandpass signal $v_q(t)$ to an envelope detector. The output of the envelope detector $V_{eo}(t)$ is then directed to the adaptation algorithm for the QMC, which adjusts the parameters of the QMC using $V_{eo}(t)$ and $v_d(t)$.

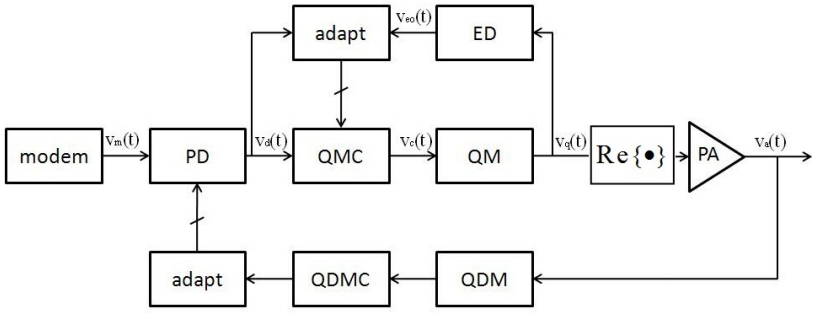

Figure 2.1. An amplifier linearization loop based on predistortion

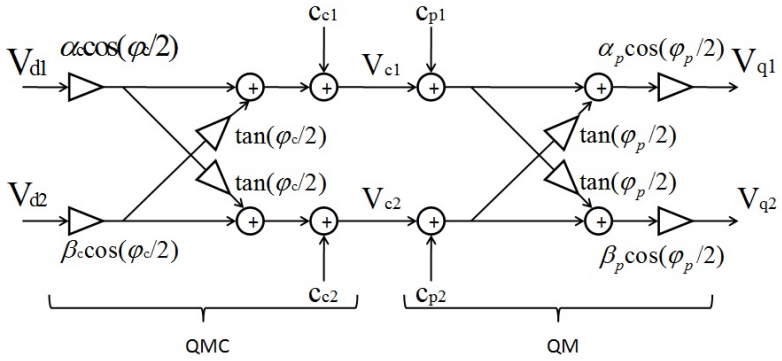

Figure 2.2. Internal structure of the QMC and QM cascade

2.2.1 The QM and Compensator

The quadrature modulator is the interface between the baseband digital signals and the RF transmission bandpass signals. For the analysis, a symmetric model for the internal QM and QMC is illustrated in Fig. 2.2. Following [7] closely, we use the matrix representations to demonstrate the characteristics of the QM and QMC. We represent the QM and QMC internal parameters by the subscript p and c respectively, and denote the overall QM-the cascade of QMC and QM, by no subscript. Then, the primary impairments of the QM can be summarized in the error vector $q = [\varepsilon_p \ \phi_p \ c_{p1} \ c_{p2}]^T$, where ε_p is the gain imbalance, ϕ_p is the phase imbalance and c_{p1} and c_{p2} are the real and imaginary dc offsets, and

$$\varepsilon_p = \gamma_p - 1 \text{ and } \gamma_p = \alpha_p/\beta_p \tag{2.1}$$

In (2.1), γ_p is the gain ratio and α_p and β_p are the gains in the real and imaginary branches. We can calculate the two gains α_p and β_p when knowing the gain imbalance ε_p[2] by

$$\begin{aligned} \alpha_p &= (1+\varepsilon_p)\sqrt{\frac{2}{2+2\varepsilon_p+\varepsilon_p^2}} \\ \beta_p &= \sqrt{\frac{2}{2+2\varepsilon_p+\varepsilon_p^2}} \end{aligned} \tag{2.2}$$

The QMC transfer characteristic is then

$$\vec{v_c} = M_c\vec{v_d} + \vec{c_c} \tag{2.3}$$

where $\vec{v_d}$ and $\vec{v_c}$ are length-2 vectors denoting the real and imaginary components of the corresponding complex signals, c_c is the vector of real and imaginary dc offsets, and

$$M_c = \begin{bmatrix} \alpha_c\cos(\frac{\phi_c}{2}) & \beta_c\sin(\frac{\phi_c}{2}) \\ \alpha_c\sin(\frac{\phi_c}{2}) & \beta_c\cos(\frac{\phi_c}{2}) \end{bmatrix} \tag{2.4}$$

The QM transfer characteristic is then

$$\vec{v_q} = M_p(\vec{v_c} + \vec{c_p}) \tag{2.5}$$

where

$$M_p = \begin{bmatrix} \alpha_p \cos(\frac{\phi_p}{2}) & \alpha_p \sin(\frac{\phi_p}{2}) \\ \beta_p \sin(\frac{\phi_p}{2}) & \beta_p \cos(\frac{\phi_p}{2}) \end{bmatrix} \tag{2.6}$$

The overall QM (cascade of QMC and QM) transfer characteristic is then

$$\vec{v_q} = M_p M_c \vec{v_d} + M_p(\vec{c_c} + \vec{c_p}) \tag{2.7}$$

Since ε_p and ϕ_p are normally very small, typically $\phi_p = 0.05$ radians (3°) and $\varepsilon_p = 0.03$, we can use the first-order series approximations $\alpha_p \approx 1 + \frac{\varepsilon_p}{2}$, $\beta_p \approx 1 - \frac{\varepsilon_p}{2}$. In this case, the overall QM error vector equals the sum of the QMC and QM error vectors, that is $\vec{q} \approx \vec{q_c} + \vec{q_p}$. For small quantities ε, ϕ, c_1, and c_2, the complex bandpass signal applied to the PA are denoted by a length-2 vector

$$\vec{v_q} \approx \begin{bmatrix} (1 + \frac{\varepsilon}{2})v_{d1} + \frac{\phi}{2}v_{d2} + c_1 & \frac{\phi}{2}v_{d1} + (1 - \frac{\varepsilon}{2})v_{d2} + c_2 \end{bmatrix}^T \tag{2.8}$$

where v_{d1}, v_{d2} are the real and imaginary components of the predistorted input signal $v_d(t)$. From (2.8), $\vec{v_q} \neq \vec{v_d}$ because of QM impairments. Thus, the adaptation algorithm is critical to estimate and adjust the impairments of the overall QM by adapting the DSP-based QMC parameters.

2.2.2 The Envelope Detector

Generally, an envelope detector operation characteristic can be divided into three working regions: square law, transition and linear. For small signals (below some

voltage level depending on the parameters of the specific envelope detector), the envelope detector works in the square law region, which can be represented as

$$V_{eo} = g_{sl} V_{ei}^2 + d_{sl} \tag{2.9}$$

where g_{sl} and d_{sl} are the differential gain and bias of the square law region respectively, and $V_{ei} = \|\vec{v}_q\|$ is the ideal magnitude of the complex bandpass signal $v_q(t)$. Expanding (2.8) and (2.9), and keeping only first order terms yields

$$V_{eo} \approx \vec{U}_{sl}^T \vec{X}_{sl} \tag{2.10}$$

where

$$\vec{U}_{sl} = \begin{bmatrix} g_{sl} \\ g_{sl}\varepsilon \\ g_{sl}\phi \\ g_{sl}c_1 \\ g_{sl}c_2 \\ d_{sl} \end{bmatrix}, \vec{X}_{sl} = \begin{bmatrix} v_{d1}^2 + v_{d2}^2 \\ v_{d1}^2 - v_{d2}^2 \\ 2v_{d1}v_{d2} \\ 2v_{d1} \\ 2v_{d2} \\ 1 \end{bmatrix}$$

For slightly larger signals, the envelope detector works in the transition region, whose characteristic is non-linear and unpredictable. However, for high voltage signals (above some voltage level), the characteristic turns linear, which can be represented as

$$V_{eo} = g_{ln} V_{ei} + d_{ln} \tag{2.11}$$

where g_{ln} is the differential gain of the envelope detector's linear region and d_{ln} is its bias. Similarly, expanding (2.8) and (2.11), the first-order approximation is

$$V_{eo} \approx \vec{U}_{ln}^T \vec{X}_{ln} \tag{2.12}$$

where

$$\vec{U}_{ln} = \begin{bmatrix} g_{ln} \\ g_{ln}\varepsilon \\ g_{ln}\phi \\ g_{ln}c_1 \\ g_{ln}c_2 \\ d_{ln} \end{bmatrix}, \vec{X}_{ln} = \begin{bmatrix} \sqrt{v_{d1}^2 + v_{d2}^2} \\ (v_{d1}^2 - v_{d2}^2)/2\sqrt{v_{d1}^2 + v_{d2}^2} \\ v_{d1}v_{d2}/\sqrt{v_{d1}^2 + v_{d2}^2} \\ v_{d1}/\sqrt{v_{d1}^2 + v_{d2}^2} \\ v_{d2}/\sqrt{v_{d1}^2 + v_{d2}^2} \\ 1 \end{bmatrix}$$

In order to use more signal points to increase the actual convergence speed, the algorithm proposed works with both the square law and linear regions of the envelope detector.

2.2.3 Proposed Adaptation Algorithm

The adaptive algorithm runs in a series of iterations. In each iteration, the algorithm first obtains the estimate of the error vector $\hat{\vec{q}}$ using input $\vec{v}_d$ and corresponding envelope sample V_{eo}. Assume the current input complex envelope is $\vec{v}_{d,k}$, where k is the iteration number. If its corresponding digitalized envelope sample falls in the square law region, (2.10) is applied; if it falls in the linear region, (2.12) is applied; if it falls in the transition region, the algorithm does not update for this input and corresponding output value. These steps are readily implemented in the DSP. We use $\vec{X}_k$ to represent either $\vec{X}_{sl,k}$ or $\vec{X}_{ln,k}$ and the same rule applies to $\vec{U}_k$, g and d, where the context will make clear the designation. Since this algorithm expands the working region, it can use more input points than [7] and [8] to hasten convergence.

The operation of the adaptation algorithm at iteration k is given next. From (2.10) or (2.12), calculate the corresponding vector $\vec{X}_k$ from the input $\vec{v}_{d,k} = [v_{d1,k}, v_{d2,k}]^T$. Then the gradient estimate is

$$\hat{\vec{\nabla}}_k = -2e_k\vec{X}_k \tag{2.13}$$

and the error is

$$e_k = V_{eo,k} - \hat{\vec{U}}_k^T \vec{X}_k \tag{2.14}$$

In (2.14), $\hat{\vec{U}}_k$ is the estimate of vector $\vec{U}$, either $\hat{\vec{U}}_{sl,k}$ or $\hat{\vec{U}}_{ln,k}$, with initial value $[1\ 0\ 0\ 0\ 0\ 0]^T$. With the gradient estimate (2.13),

$$\hat{\vec{U}}_{k+1} = \hat{\vec{U}}_k - \mu \hat{\vec{\nabla}}_k \tag{2.15}$$

where μ is the step size parameter that determines the tradeoff between the speed and the stability of convergence. From (2.10) or (2.12)

$$\begin{aligned} \hat{\varepsilon}_k &= \hat{U}_{k+1}[2]/\hat{U}_{k+1}[1] \quad & \hat{\phi}_k &= \hat{U}_{k+1}[3]/\hat{U}_{k+1}[1] \\ \hat{c}_{1,k} &= \hat{U}_{k+1}[4]/\hat{U}_{k+1}[1] \quad & \hat{c}_{2,k} &= \hat{U}_{k+1}[5]/\hat{U}_{k+1}[1] \end{aligned} \tag{2.16}$$

where $\hat{U}_k[i]$ is the ith element of the vector $\hat{\vec{U}}_k$. Then the estimate error vector is $\hat{\vec{q}}_k = [\hat{\varepsilon}_k\ \hat{\phi}_k\ \hat{c}_{1,k}\ \hat{c}_{2,k}]^T$, and $\hat{\vec{U}}_{k+1}$ is set to $[\hat{U}_{k+1}[1]\ 0\ 0\ 0\ 0\ \hat{U}_{k+1}[6]]^T$, where $\hat{U}_{k+1}[1] = \hat{g}_k$ and $\hat{U}_{k+1}[6] = \hat{d}_k$, the estimate of envelope detector's gain and bias, respectively. With $\hat{\vec{q}}_k$, the algorithm updates the QMC immediately by subtracting this estimate from the current value in the QMC. In other words, the operation at step k is

$$\vec{q}_{c,k+1} = \vec{q}_{c,k} - \hat{\vec{q}}_k \tag{2.17}$$

where $\vec{q}_{c,k+1}$ is the updated error vector of the QMC.

2.3 Performance Analysis

2.3.1 Traditional LMS Counterpart

The proposed LMS technique updates the QMC and reset vector $\hat{\vec{U}}_k$ in each iteration. Although the proposed technique is easy to implement, it is necessary to find

its traditional LMS counterpart which is possible for analytical analysis. At iteration k, substituting (2.10) or (2.12) in (2.14), expanding and recombining yields

$$e_k = \left(\begin{bmatrix} g \\ g\varepsilon_p \\ g\phi_p \\ gc_{p1} \\ gc_{p2} \\ d \end{bmatrix}^T - \begin{bmatrix} \hat{g}_k \\ -g\varepsilon_{c,k} \\ -g\phi_{c,k} \\ -gc_{c1,k} \\ -gc_{c2,k} \\ \hat{d}_k \end{bmatrix}^T \right) \vec{X}_k \tag{2.18}$$

Define

$$d_k = \begin{bmatrix} g \\ g\varepsilon_p \\ g\phi_p \\ gc_{p1} \\ gc_{p2} \\ d \end{bmatrix}^T \vec{X}_k,\ \vec{W}_k = \begin{bmatrix} \hat{g}_k \\ -g\varepsilon_{c,k} \\ -g\phi_{c,k} \\ -gc_{c1,k} \\ -gc_{c2,k} \\ \hat{d}_k \end{bmatrix} \tag{2.19}$$

where d_k is the output of the QM and envelope detector cascade without compensation and $\vec{w}_k$ is the weight vector that need to be adjusted. Then (2.18) is equivalent to

$$e_k = d_k - \vec{W}_k^T \vec{X}_k \tag{2.20}$$

In each iteration, the proposed technique updates the QMC with (2.16) and (2.17), then

$$\vec{W}_{k+1} = \begin{bmatrix} \hat{g}_{k+1} \\ -g\varepsilon_{c,k+1} \\ -g\phi_{c,k+1} \\ -gc_{c1,k+1} \\ -gc_{c2,k+1} \\ \hat{d}_{k+1} \end{bmatrix} = \begin{bmatrix} \hat{g}_k \\ -g\varepsilon_{c,k} \\ -g\phi_{c,k} \\ -gc_{c1,k} \\ -gc_{c2,k} \\ \hat{d}_k \end{bmatrix} + \begin{bmatrix} \tilde{g}_k \\ g\hat{\varepsilon}_k \\ g\hat{\phi}_k \\ g\hat{c}_{1,k} \\ g\hat{c}_{2,k} \\ \tilde{d}_k \end{bmatrix} \tag{2.21}$$

where $\tilde{g}_k$ and $\tilde{d}_k$ are the increment of the estimated envelope detector's gain and bias respectively in iteration k. From (2.15) and (2.16)

$$-\mu\hat{\vec{\nabla}}_k = \begin{bmatrix} \tilde{g}_k \\ \hat{g}_{k+1}\hat{\varepsilon}_k \\ \hat{g}_{k+1}\hat{\phi}_k \\ \hat{g}_{k+1}\hat{c}_{1,k} \\ \hat{g}_{k+1}\hat{c}_{2,k} \\ \tilde{d}_k \end{bmatrix} \tag{2.22}$$

With (2.22), (2.21) can be represented as

$$\vec{W}_{k+1} \approx \vec{W}_k - \mu'\hat{\vec{\nabla}}_k \tag{2.23}$$

where $\mu' = \frac{\hat{g}_{k+1}}{g}\mu$. For small quantities $\tilde{g}_k$ and $\tilde{d}_k$, $\tilde{g}_k \approx \frac{\hat{g}_{k+1}}{g}\tilde{g}_k$ and $\tilde{d}_k \approx \frac{\hat{g}_{k+1}}{g}\tilde{d}_k$. For k large enough, $\hat{g}_{k+1} \to g$, then $\mu' \to \mu$. With (2.20) and (2.23), theoretically, the proposed technique has a traditional LMS algorithm counterpart for each iteration with μ'.

2.3.2 Proof of Convergence

The goal of the proposed technique is to adjust $q_k = q_{c,k} + q_p \to 0$. To prove the convergence of the QMC in expectation, which is $\|E[q_{c,k}] - (-q_p)\| \to 0$, we need to prove $\|E[\vec{W}_k] - \vec{W}_{opt}\| \to 0$, where $\vec{W}_{opt} = [g\ g\varepsilon_p\ g\phi_p\ gc_{p1}\ gc_{p2}\ d]^T$. Because

$$\|E[\vec{W}_k] - \vec{W}_{opt}\| = \left\| \begin{array}{c} E[\hat{g}_k] - g \\ -g(E[\varepsilon_{c,k}] + \varepsilon_p) \\ -g(E[\phi_{c,k}] + \phi_p) \\ -g(E[c_{c1,k}] + c_{p1}) \\ -g(E[c_{c2,k}] + c_{p2}) \\ E[\hat{d}_k] - d \end{array} \right\| \tag{2.24}$$

If $\|E[\vec{W}_k] - \vec{W}_{opt}\| \to 0$, then $(E[\varepsilon_{c,k}] + \varepsilon_p)^2 + (E[\phi_{c,k}] + \phi_p)^2 + (E[c_{c1,k}] + c_{p1})^2 + (E[c_{c2,k}] + c_{p2})^2 \to 0$, which is $\|E[q_{c,k}] - (-q_p)\| \to 0$, and $(E[\hat{g}_k] - g) \to 0$, $(E[\hat{d}_k] - d) \to 0$. Therefore, we will prove $\|E[\vec{W}_k] - \vec{W}_{opt}\| \to 0$ next.

Define $\tilde{\vec{W}}_k$ as the weight error at iteration k, then

$$\tilde{\vec{W}}_k = \vec{W}_k - \vec{W}_{opt} \tag{2.25}$$

From (2.18), $e_k = (\vec{W}_{opt}^T - \vec{W}_k^T)\vec{X}_k = \vec{X}_k^T(\vec{W}_{opt} - \vec{W}_k)$. Taking the expected value of both sides of (2.23) and substituting (2.13) yields the difference equation

$$\begin{aligned} E[\vec{W}_{k+1}] &= E[\vec{W}_k] + 2\mu' E[e_k \vec{X}_k] \\ &= E[\vec{W}_k] + 2\mu' E[\vec{X}_k \vec{X}_k^T (\vec{W}_{opt} - \vec{W}_k)] \\ &= E[\vec{W}_k] - 2\mu' \mathbf{R} E[\tilde{\vec{W}}_k] \end{aligned} \tag{2.26}$$

where $\mathbf{R} = E[\vec{X}_k \vec{X}_k^T]$ is the input correlation matrix. Then, the expected value of weight error at iteration $k+1$ is

$$\begin{aligned} E[\tilde{\vec{W}}_{k+1}] &= E[\vec{W}_{k+1}] - \vec{W}_{opt} \\ &= E[\vec{W}_k] - 2\mu' \mathbf{R} E[\tilde{\vec{W}}_k] - \vec{W}_{opt} \\ &= (\mathbf{I} - 2\mu' \mathbf{R}) E[\tilde{\vec{W}}_k] \end{aligned} \tag{2.27}$$

After rotating the recursion (2.27), we get

$$E[\tilde{v}_{k+1,r}] = (1 - 2\mu'\lambda_r)E[\tilde{v}_{k,r}] \tag{2.28}$$

where $E[\tilde{v}_{k,r}]$ is the r^{th} element of expected rotated weight errors and λ_r is the r^{th} eigenvalue of $\mathbf{R}$. As long as $\mu' < \frac{2}{\lambda_{max}}$, as k increases without bound, $E[\tilde{v}_{k,r}] \to 0$, which means $\|E[\tilde{\vec{W}}_{k+1}]\| \to 0$. With (2.25), we proved $\|E[\vec{W}_k] - \vec{W}_{opt}\| \to 0$ and $\|E[q_{c,k}] - (-q_p)\| \to 0$. Therefore, the expected value of the QMC elements converge to the negative value of corresponding QM impairments. With (2.18), one can easily prove that the mean square error (MSE) converges to zero[10].

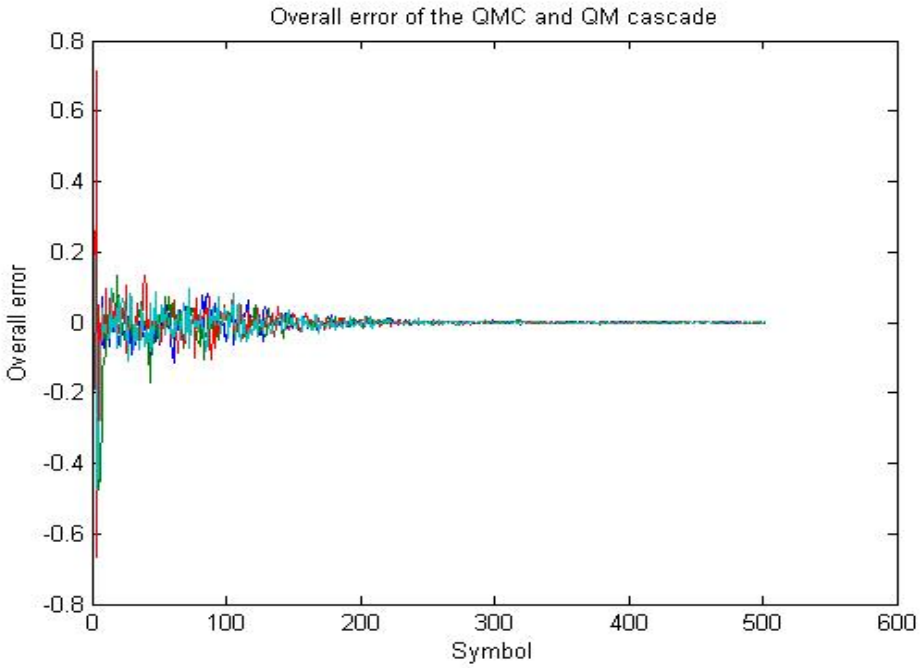

Figure 2.3. Overall error in QMC and QM cascade after QMC compensation

Fig. 2.3 and Fig. 2.4 are generated with orthogonal frequency division multiplexing (OFDM) input signals. The OFDM signals have the following characteristic: 64 subcarriers, quadrature phase shift keying (QPSK) modulation scheme, 8 guard interval samples. Thus, each OFDM symbol modulates 128 bits and consists of 72

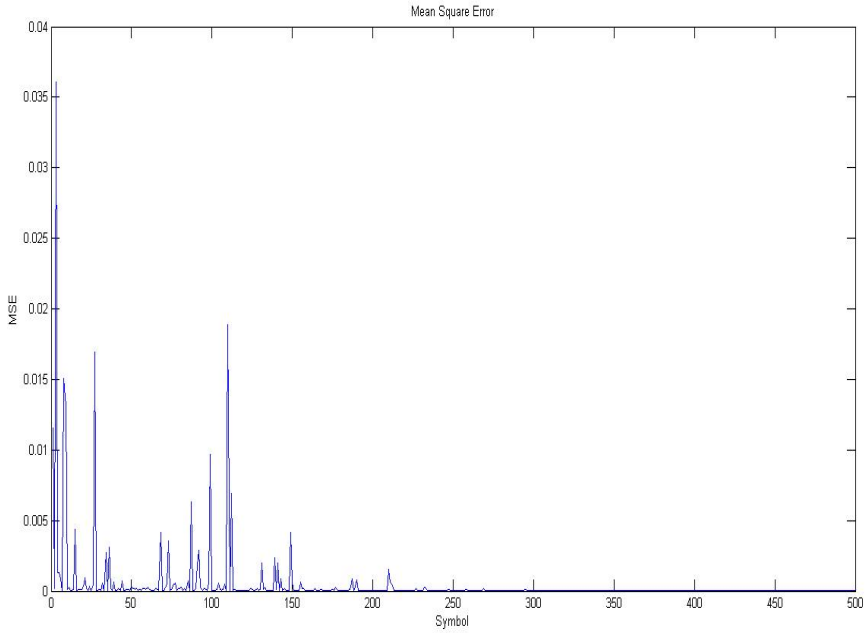

Figure 2.4. The means square error of the proposed algorithm

sample points. For the OFDM symbols generated, roughly 15% and 5% of total sample points fall into the simulated diode detector's square law region and linear region, respectively. It's shown that the mean square error converges to approximately zero and the overall errors in QMC and QM cascade, which are elements in $q_{c,k} + q_p$, decrease substantially to an extremely small value around zero.

2.3.3 Performance of The Proposed Technique

The goal of our proposed compensation technique is to mitigate the I/Q imbalance to satisfy (1.1). In addition, since the proposed technique has the ability to use points falling into the envelope detectors's both linear and square law regions, it should be faster than using only linear regions.

To compare the convergence rate, we should compare the rate under the same steady-state misadjustment, because there is a trade-off between the misadjustment

and the rate of convergence. The misadjustment in the adaptive process is defined as [10]

$$M \approx \mu \cdot tr[\mathbf{R}] \tag{2.29}$$

where $tr[\mathbf{R}]$ is the trace of $\mathbf{R}$, which is also the total power of the inputs to the weights. For linear and square law regions, the expression of $\vec{X}_{ln,k}$ and $\vec{X}_{sl,k}$ are different as in (2.12) and (2.10). Therefore, to achieve the same level of misajustment, the step sizes for linear and square law should satisfy (2.30)

$$\frac{\mu_{sl}}{\mu_{ln}} \approx \frac{tr[\mathbf{R}_{ln}]}{tr[\mathbf{R}_{sl}]} \tag{2.30}$$

To test the performance of our proposed technique with a practical envelope detector, a simple diode peak-detector, which consists of only one diode, one resistor and one capacitor, has been simulated with Pspice. We extracted the input/output voltage characteristic relationship and imported it to Matlab. The simulated envelope detector has the three working regions: square law, transition and linear, as illustrated in Section 2.2.2. However, in the square law and linear regions, the input/output relationship is not perfectly square law and linear, which affects the performance of our proposed technique. Therefore, besides simulating the proposed technique with a real envelope detector, we should also simulate with a semi-ideal envelope detector, which is defined as having the same working region range as the real envelope detector but with an ideal input/output relationship for each region.

In simulations, OFDM signals have been used as the input baseband signal $\vec{v}_d(t)$ in order to verify the behavior of the proposed algorithm. The OFDM signals have the same characteristic as in Section 2.3.2. For such an input signal, (2.30) yields $\frac{\mu_{sl}}{\mu_{ln}} \approx 1$.

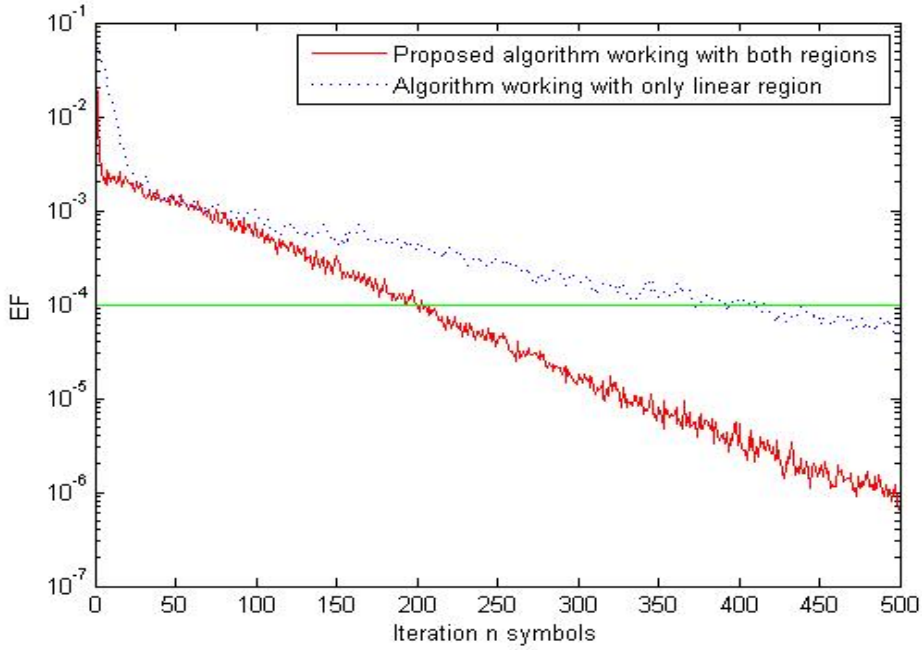

Figure 2.5. Convergence performance with a semi-ideal envelope detector. $\mu_{ln} = \mu_{sl} = 0.2$.

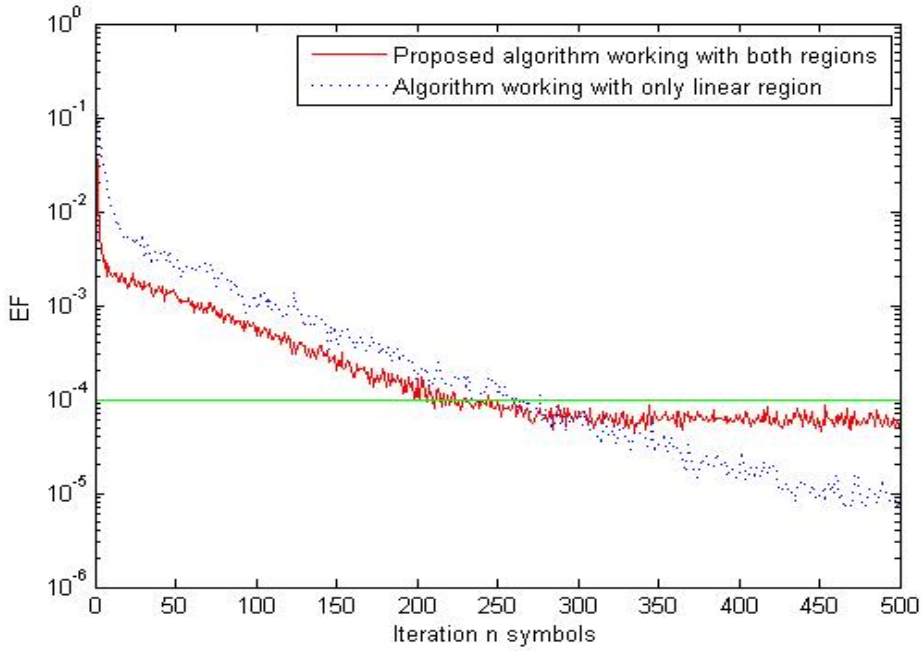

Figure 2.6. Convergence performance with a practical envelope detector. $\mu_{ln} = \mu_{sl} = 0.2$.

Fig. 2.5 is generated with a simulated semi-ideal envelope detector. It shows that the proposed algorithm working with both square law and linear regions decreases the EF in (1.1) to the 10^{-4} level in 200 symbols comparing to the 380 symbols required for the algorithm working with only linear region.

Fig. 2.6 is generated with a simulated practical envelope detector. Although the proposed algorithm working with both square law and linear regions decreases the EF to the 10^{-4} level faster than algorithm working with only linear region, it is not so fast as in Fig. 2.5. The reason is that the non-ideal input/output relationship introduce noises into d_k in (2.19), which affects the performance of the technique. Therefore, if one can generate a practical envelope detector with almost ideal input/output relationship and use it for our proposed technique, the performance will more closely match that of Fig. 2.5.

2.4 Conclusion

In this chapter, a fast I/Q imbalance compensation technique for analog quadrature modulators in the direct conversion transmitters has been proposed. We proved that the proposed technique has a least mean square (LMS) implementation that converges and compared its convergence speed with algorithm only working with envelope detector's linear region. The increased parametrization of the envelope detector leads to more unknowns to be estimated in our I/Q imbalance compensation technique, but the number of points available for adaptation is also increased in compensation. The simulation results demonstrate that our proposed technique satisfies (1.1) and converges slightly faster.

CHAPTER 3

PHYSICAL LAYER SECURITY

3.1 Introduction

One of the critical concerns in wireless communication is security of data transmission. Traditionally, security has been the domain of cryptographers, who encrypt information so that it is easy to decode for a receiver with the appropriate key, but presents a "hard" problem to the eavesdropper, who is assumed to not be able to solve "hard problems"[15]. However, there are numerous historical examples of schemes being broken that were supposedly secure, often when the signal was recorded for later processing and eventually broken[16], which, combined with recent advances in computation[17][18], yields clear motivation to consider forms of security that are provably everlasting.

Hence, there has been a significant revival of interest in information-theoretic techniques which presume no limitation on the eavesdropper's computational capability. The theoretical basis for this information-theoretic approach builds on Shannon's notion of perfect secrecy[19] which stated that to transmit b bits of information securely required a key of length b, and that key must be kept secret indefinitely. The next major advance was made by Wyner[20], who studied the so-called "wiretap channel" shown in Fig. 3.1. He showed that if the receiver has a better channel than the eavesdropper, there are schemes that can transmit information at a positive rate such that the eavesdropper gets almost no information about the transmitted bits - regardless of the current or future computation capabilities of that eavesdropper. After Wyner's work, the problem laid roughly dormant for almost three decades be-

fore becoming a topic of extreme interest in recent times for guaranteeing secrecy in wireless communication systems.

Information-theoretic approaches often have difficulty with a near eavesdropper whose channel is better than the receiver's channel. Early results showed that the fading could be exploited, either when the eavesdropper's channel is known, or when only statistical information is available on the eavesdropper channel[21]. When the eavesdropper channel is statistically very good, it can be difficult to maintain a reasonable secrecy rate, so people have considered various cooperative jamming approaches. However, such approaches are not robust to the channel model that may be encountered by the system.

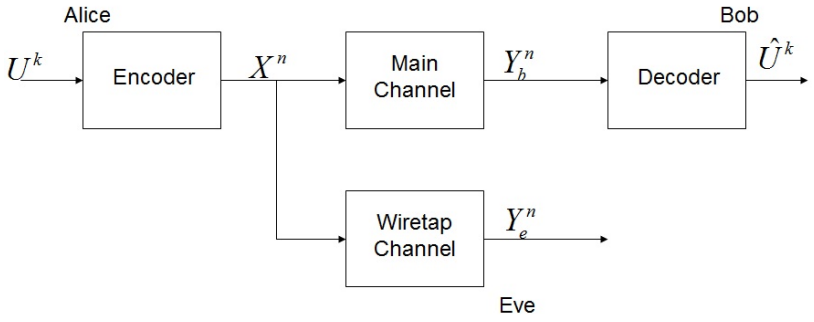

Figure 3.1. Gaussian wiretap channel. Alice encodes a message block, represented by the random variable U^k, into a codeword, represented by the random variable X^n, for transmission over the channel. Bob observes the output of the main channel Y_b^n and Eve observes the output of the wiretap channel Y_e^n.

Hence, we are more interested in a second set of techniques, which can operate when Bob's channel is worse than Eve's. An early version of this was the work of Maurer[22], where public discussion using common randomness provided by a third party is effective. More recently, authors have exploited two-way schemes; in essence, Bob generates an (information) secret key that is used to communicate information over a public channel[24][25]. All of these schemes still need to choose a secrecy rate

that is a function of the channel parameters, which in turn are a function of the channel geometry, and thus it is still difficult to guarantee the desired security for a positive secrecy rate.

Talking a different approach, Cachin and Maurer[23] exploited the realizability of hardware to consider the case of everlasting security, as is our interest. In particular, they introduced the "bounded memory model" - signal in such a way that the receiver cannot store the information it would need to eventually crack the code. This approach suffers from two detriments:

1. By Moore's Law(see NAND scaling plot at [26]), the density of memories increases as at an exponential rate with time.

2. Memories can be stacked arbitrarily subject only to (large) space limitations.

Hence, although the bounded memory model is a viable approach to everlasting security, it is difficult to pick a memory size beyond which it will be effective, making its employment for secret wireless communication extremely difficult. Our contention is that [23] attacked the wrong part of the receiver - the back-end rather than the front-end. In this thesis, we demonstrate a technique to attack the eavesdropper receiver's radio-frequency(RF) front-end such that a short-term cryptographic advantage can be turned into everlasting security. In short, the trick is to establish an ephemeral cryptographic key between Alice and Bob (such as employing a Diffie-Helman protocol) that is used for warping the signal at the transmitter and receiver. Since Eve does not obtain the key until later, her ADC and unwarping operations are in a different order than Bob's, and, because nonlinear and time-varing systems are not commutative, this can be used to obtain a positive secrecy rate.

3.2 System Model

The enhanced version of the wiretap channel including hardware components in Fig. 3.2 is considered in this thesis. A legitimate user (Alice) sends signal samples

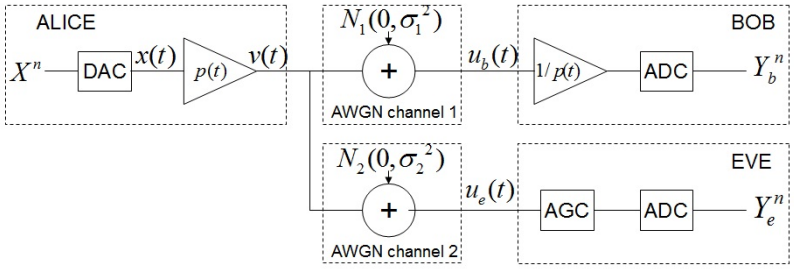

Figure 3.2. Enhanced version of the wiretap channel to include hardware components. In particular, Alice's transmitter has a digital-to-analog converter (DAC) and a power amplifier, whereas Bob and Eve have a low noise amplifier followed by an analog-to-digital converter (ADC) and automatic gain control (AGC) followed by an ADC, respectively.

after modulation represented by the random variable sequence X^n to another user (Bob). The actual signal sent by Alice is the power amplified signal $v(t)$ with power constraint $E\{|v(t)|^2\} \leq P$ and

$$v(t) = x(t) \cdot p(t) \tag{3.1}$$

where $p(t)$ is the gain of the power amplifier and $E\{p^2(t)\} \leq \frac{P}{E\{|x(t)|^2\}}$. Bob receives the output of an additive white gaussian noise(AWGN) channel given by

$$u_b(t) = v(t) + n(t) \tag{3.2}$$

where $n(t) \sim N_1(0, \sigma^2)$. Since Bob knows $p(t)$, he can implement an analog-to-digital converter(ADC) for $x(t)$ and a low noise amplifier (LNA) with gain $1/p(t)$ to adjust the dynamic range of the received signal to be compatible with the ADC.

A third party(Eve) is also capable of eavesdropping on Alice's transmissions. Eve observes the output of the AWGN channel $u_e(t)$. Although Eve does not know $p(t)$ directly, she could implement an automatic gain control(AGC) loop to adjust the dynamic range of the received signal to be compatible with her ADC.

3.3 Automatic Gain Control

In Eve's receiver, the level of the incoming signal varies over a wide dynamic range and Eve does not know $p(t)$. Therefore, the AGC loop is critical to make sure the signal is not out of the ADC's dynamic range. For analysis, assume Eve is using the same ADC as Bob, and the AGC loop is then employed to attempt to copy the same function as the low noise amplifier with gain $1/p(t)$.

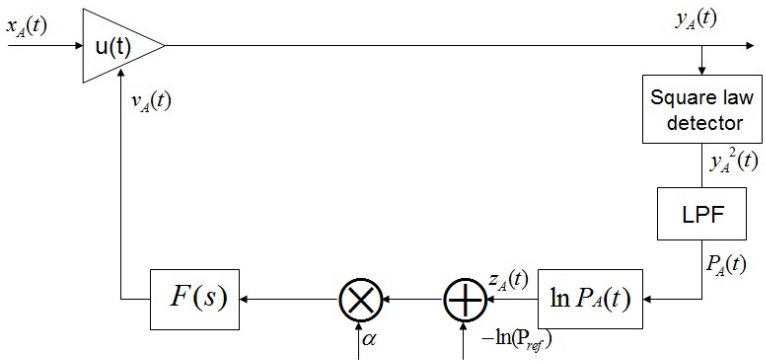

Figure 3.3. Decibel based linear AGC block diagram

A typical decibel based linear AGC model which is widely used is shown in Fig. 3.3. The input signal $x_A(t)$ is amplified by an exponential variable gain amplifier (EVGA), whose gain $u(t)$ is controlled by the signal $v_A(t)$ such that $u(t) = e^{-v_A(t)}$. All modern AGCs tend to approximate the exponential gain characteristic because it gives the desired dynamic range with a moderate range of the gain control voltage. Then, the amplitude of $y_A(t)$ is

$$y_A(t) = e^{-v_A(t)} x_A(t) \tag{3.3}$$

Following the signal path, the output of the logarithmic amplifier is

$$z_A(t) = \ln P_A(t) \tag{3.4}$$

where $P_A(t)$ is the low frequency component of $y_A^2(t)$. With the logarithmic amplifier, the AGC system operates as decibel based linear, which means that if the amplitude of the input and output signals of the AGC are expressed in decibels (dB), then the system response is linear with respect to these values.

The transfer function of the simplest low pass filter that can be used in the system is $F(s) = \frac{1}{s}$, which is an ideal integrator in the time domain. Combining (3.3) and (3.4), the expression for the AGC model in the time domain is

$$y_A(t) = exp\{-\alpha \int_0^t [\ln P_A(\tau) - \ln (P_{ref})] d\tau\} x_A(t) \tag{3.5}$$

The performance of the designed AGC to a independent and identically distributed Gaussian input signal sequence is shown in Fig. 3.4. The input signal sequence $x_A[n] \sim N(0, 9)$; thus, the average power of the input signal is approximately 9. In the steady state, the average power of the output signal is approximately 1 and $u[n] \approx 0.33$. Although the AGC system successfully adjusted the average power of the signal, there exists an obvious tracking period. Comparing Fig. 3.4 and Fig. 3.5, we find that the loop gain α determines the tradeoff between settling time and steady state error. In a practical AGC system, α is set such that a fast settling time can be achieved while maintaining a relatively small steady state error.

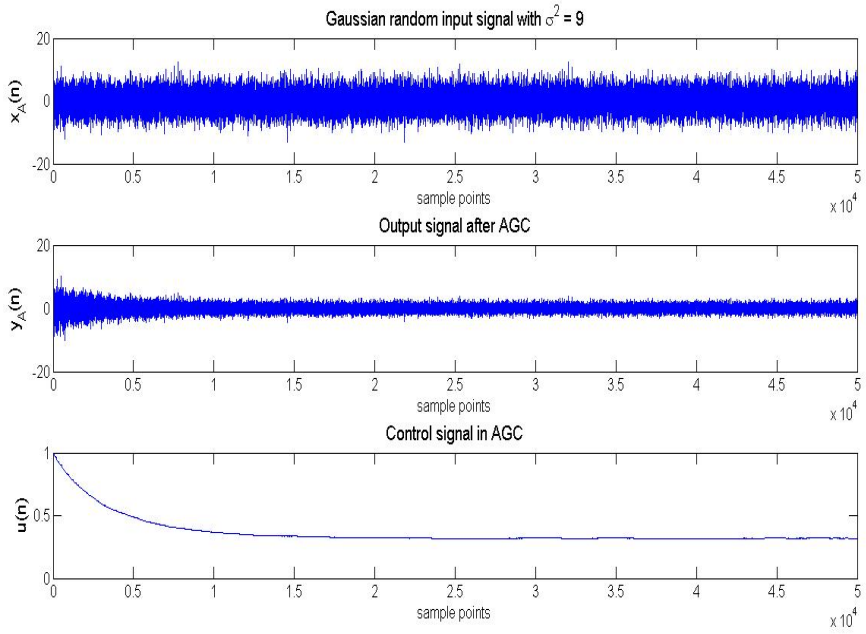

Figure 3.4. AGC input, output and control signals with $\alpha = 0.0001$

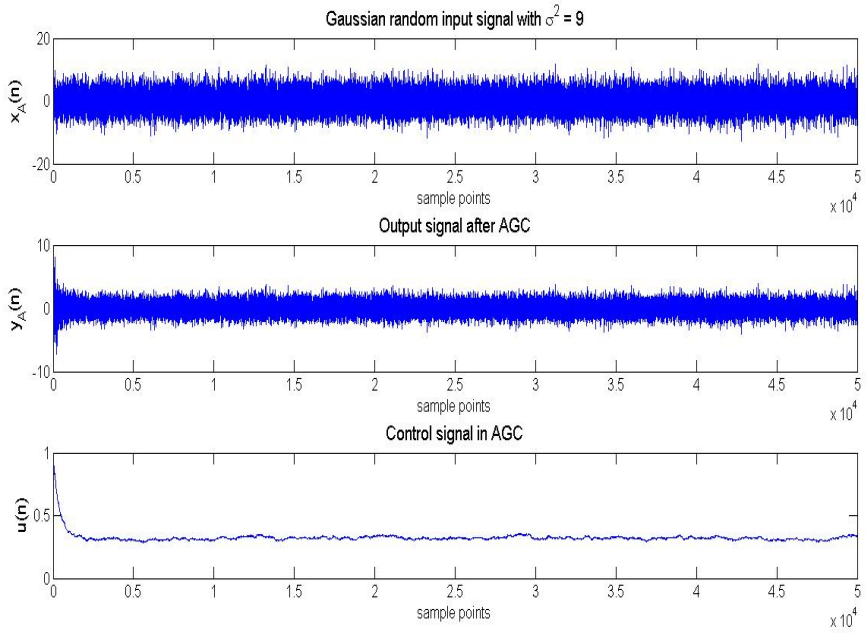

Figure 3.5. AGC input, output and control signals with $\alpha = 0.001$

3.4 Proposed technique

Consider the enhanced version of the wiretap channel shown in Fig. 3.2. The secrecy capacity is given by [27]

$$C_s = \max\{0, \frac{1}{2}\log(1 + \frac{E_s}{N_b}) - \frac{1}{2}\log(1 + \frac{E_s}{N_e})\} \tag{3.6}$$

where $E_s = \frac{1}{n}\sum_{i=1}^{n} E\{|X(i)|^2\}$ denotes the average power of the input signal and N_b and N_e denote the average noise powers for Bob and Eve, respectively. In order to achieve a positive secrecy capacity, the system should achieve $N_b < N_e$. For the enhanced system model considering the RF front-end system, N_b and N_e consists of two parts: channel noise and RF front-end noise. For a near eavesdropper, Eve has the same or even a better channel condition than Bob. Therefore, to achieve $N_b < N_e$, our proposed technique should increase the RF front-end noise of Eve's receiver.

This thesis proposes such a technique to deceive the AGC-ADC cascade in Eve's receiver RF front-end system while maintaining the proper operation of Bob's AGC-ADC combination. At Alice's side, instead of using a constant $p(t)$ to amplify $x(t)$, we set $p(t)$ to be a random variable determined by a randomly generated secret key, which is shared by Alice and Bob. Thus, Bob knows $p(t)$ and amplifies the received signal with $1/p(t)$. Therefore, the input signal of its ADC is under a constant signal power level and cannot be outside of the ADC's dynamic range.

However, since Eve does not know the key at this time, the most commonly used option is to implement an AGC loop to adjust the dynamic range of its received signal. From the last section, it has been shown that the AGC loop needs a settling time. If $p(t)$ changes the amplification gain level fast enough, the AGC loop will never reach its steady state. Then the AGC-ADC cascade of Eve's receiver is deceived, causing the noise power in Eve's received signal to be large. Assume Eve gets the key immediately after the signal passes the ADC, the noise power in her received

signal can not be decreased, because the signal is distorted by the failed AGC and the quantization noise of the ADC is too large.

3.5 Performance Analysis

Fig. 3.6 shows the block diagram to generate the power amplifier gain level $p(t)$.

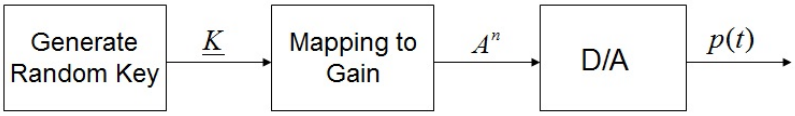

Figure 3.6. Generate the power amplifier gain $p(t)$

In this section, we will consider the simplest scenario that the varied power amplifier gain samples A^n are a sequence of discrete random variables with two possible outcomes A_{max} and A_{min}. Thus, it needs one bit of the key to represent each sample. The random variable is

$$A(k) = \begin{cases} A_{max}, & \text{if } k = 1 \\ A_{min}, & \text{if } k = 0 \end{cases} \tag{3.7}$$

The probability mass function is given by

$$p_A(a) = \begin{cases} p, & \text{if } A = A_{max} \\ 1 - p, & \text{if } A = A_{min} \end{cases} \tag{3.8}$$

For analysis, we assume that the signal samples X^n come from a Gaussian random distribution $X \sim (0, \sigma_x^2)$. Note that A should meet the power constraint $E[A^2] \leq \frac{P}{\sigma_x^2}$. Assume Bob and Eve have the same AWGN channel $N \sim (0, \sigma_n^2)$, then the average secrecy capacity is

Table 3.1. Average numbers of clippings in ADC

Channel	0dB	10dB	20dB	30dB	40dB	50dB
Bob	42	46	47	52	53	54
Eve	455	400	667	752	718	702

$$E_p[C_s] = C_{max}p + C_{min}(1-p) \tag{3.9}$$

where

$$C_{max} = \max\{0, \frac{1}{2}\log(1+\frac{\sigma_x^2}{\frac{\sigma_n^2}{A_{max}^2}}) - \frac{1}{2}\log(1+\frac{\sigma_x^2}{\frac{\sigma_n^2}{A_{max}^2}+N_{RF}})\} \tag{3.10}$$

$$C_{min} = \max\{0, \frac{1}{2}\log(1+\frac{\sigma_x^2}{\frac{\sigma_n^2}{A_{min}^2}}) - \frac{1}{2}\log(1+\frac{\sigma_x^2}{\frac{\sigma_n^2}{A_{min}^2}+N_{RF}})\} \tag{3.11}$$

In (3.10) and (3.11), N_{RF} is defined as the power of the RF front-end noise introduced to Eve when the channel input power is σ_x^2. We assume that N_{RF} is Gaussian and the ratio of the channel input power to the RF front-end noise power is $\frac{\sigma_x^2}{N_{RF}}$. In Bob's receiver, the ADC's upper and lower extreme voltages can be set as 3σ and -3σ respectively due to the 3-sigma rule – 99.7% of values drawn from a normal distribution are within three standard deviations, where $\sigma^2 = \sigma_x^2 + \sigma_n^2/A_{min}^2$. Although such an ADC may clip for a few samples due to the other 0.3% of values, its effect can be neglected. In Eve's receiver, Eve implements the same ADC with Bob. In addition, Eve implements an AGC with a small loop gain to achieve constant steady state control signal, and this control signal is employed as $1/p(t)$.

Fig. 3.7 and Table. 3.1 are generated via simulation under the assumption that Bob and Eve have the same channel condition. The only difference between Bob and Eve is the implementation of their RF front-end system due to whether they know the key or not. Fig. 3.7 and Table 3.1 shows that a positive secrecy capacity can be achieved even when Eve has the same channel condition with Bob. It is obvious to see that the proposed technique deceives the Eve's AGC block successfully; thus,

its feedback control signal fails to implement $1/p(t)$, causing more clippings for Eve's ADC.

One can also observe from Fig. 3.7 that the average secrecy capacity increases as the channel SNR increases. This is because Bob's received signals are distorted only by channel noises while Eve's received signals are distorted by both channel noise and RF-front end noise caused by gain fluctuations. When the channel SNR is low, the received signals for both Bob and Eve are severely distorted by channel noise; thus, the introduced RF-front end noises effect to Eve are not obvious. However, when the channel SNR is high, Bob's received signals are almost clear while Eve's received signals are mainly distorted by RF-front end noise. Then the advantage of Bob to Eve becomes obvious and a larger average secrecy capacity is achieved.

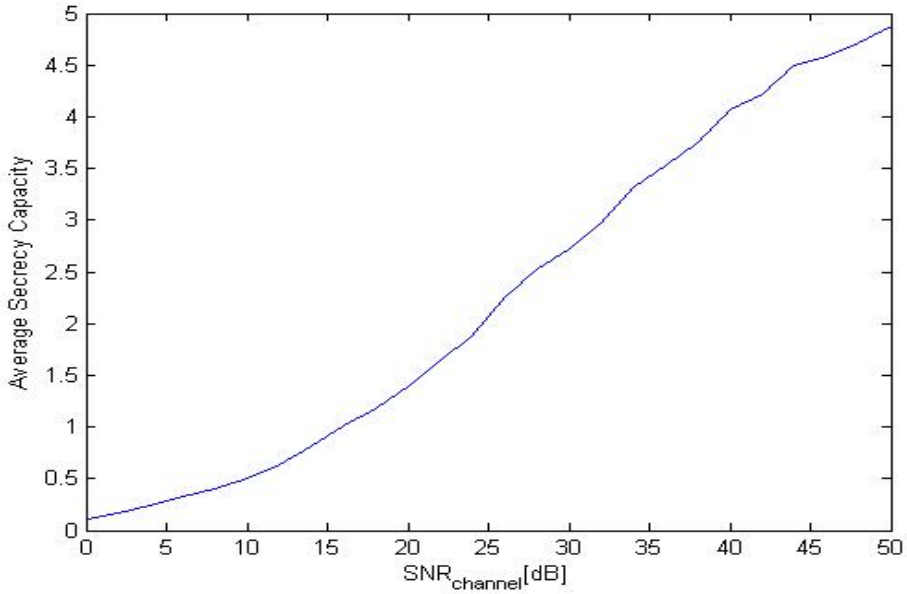

Figure 3.7. Average secrecy capacity versus channel SNR. Bob and Eve have the same AWGN channel condition.

From Fig. 3.8, one can observe that even if Eve has a better channel condition than Bob, a positive secrecy capacity can still be achieved with our propose technique.

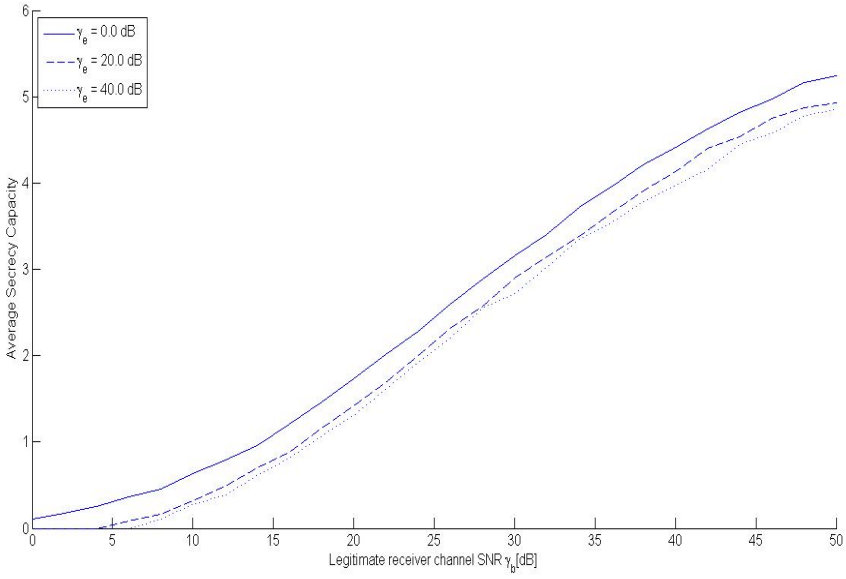

Figure 3.8. Average secrecy capacity versus γ_b, for selected values of γ_e.

As long as Bob has a high SNR, the average secrecy capacity is positive regardless of Eve's SNR.

3.6 Games with Eve

Besides implementing a "standard" AGC loop, Eve may have other possible options to fight against our proposed technique. In this section, we will discuss about these possible options and the approaches to eliminate these options.

3.6.1 Optimizing loop filter

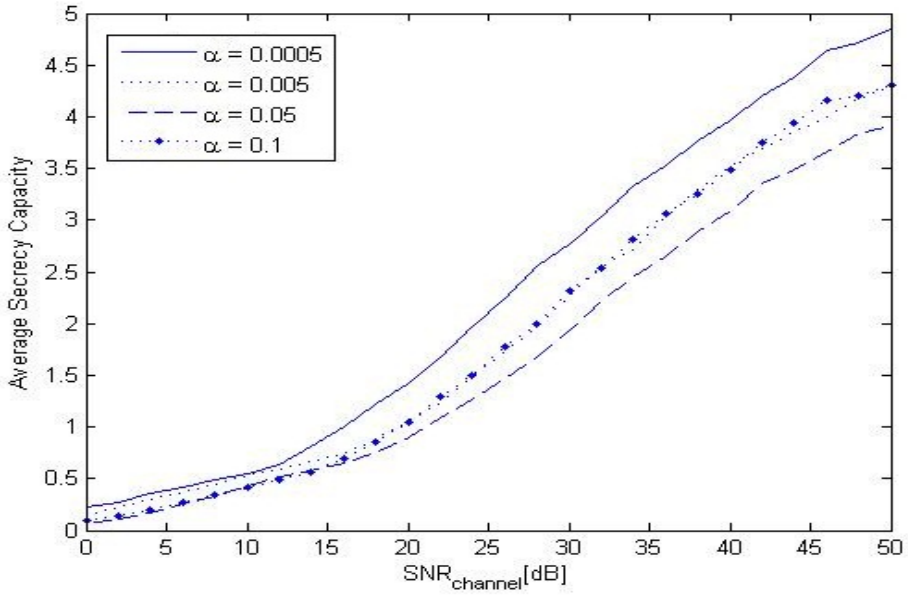

Figure 3.9. Secrecy capacity versus channel SNR, for selected values of loop gain α. Bob and Eve have the same AWGN channel condition.

Eve can optimize her AGC by optimizing the loop filter cutoff frequency. In other words, Eve can optimize her loop gain α. Fig. 3.9 shows that as the loop gain α increases, which means that Eve uses a loop filter with higher cutoff frequency, the average secrecy capacity is decreasing. However, there is a limit for the increasing of α. If α is too high such as $\alpha = 0.1$, the average secrecy capacity is smaller than that with $\alpha = 0.05$. The reason is that although the AGC's settling period errors are decreased with a high loop gain, the steady state errors of the feed back control signal are increased, which causes the feedback control signal to fluctuate around $1/p(t)$. Optimizing the loop filter cutoff frequency is equivalent to find the α such that the overall errors in the settling time period and in the steady state period are minimum. However, the dilemma is that decreasing one increases the other. Therefore, a positive average secrecy capacity is still achievable as long as the amplifier gain level changes fast enough when Eve optimizes her loop gain.

3.6.2 Recording the signal and breaking the key

Eve has the option to first record the signal and do unwrapping operation later with the broken key. To record the signal without the distortion of a failed AGC, Eve should stop using an AGC and place her ADC's full scale voltage range to cover the highest voltage that she receives. However, this approach decreases the ADC's resolution for signals amplified with a smaller gain.

Define the gain variation ratio in dB as $\lambda = 20 \log \frac{A_{max}}{A_{min}}$. Fig. 3.10 and Fig. 3.11 shows that an obvious positive average secrecy capacity is achieved even if Bob and Eve have the same channel SNR when the SNR is large enough. In the large channel SNR range (such as more than $38dB$ in Fig. 3.10 and more than $46dB$ in Fig. 3.11), a larger λ leads to a larger average secrecy capacity. Because when signals are mainly distorted by RF-front end noise caused by gain fluctuations, increasing λ will cause lower resolution for Eve's ADC for signals amplified with smaller gain while maintaining the performance of Bob's ADC.

However, in the low channel SNR range, enlarging λ cannot obviously increase the average secrecy capacity. When signals are severely distorted by channel noise, increasing RF-front end noise does not have much of an impacts. Therefore, in Fig. 3.10 and Fig. 3.11, the average secrecy capacities are approximately the same for $\lambda = 20dB$ and $\lambda = 30dB$ in the channel SNR range $0 - 38dB$ and $0 - 46dB$, respectively.

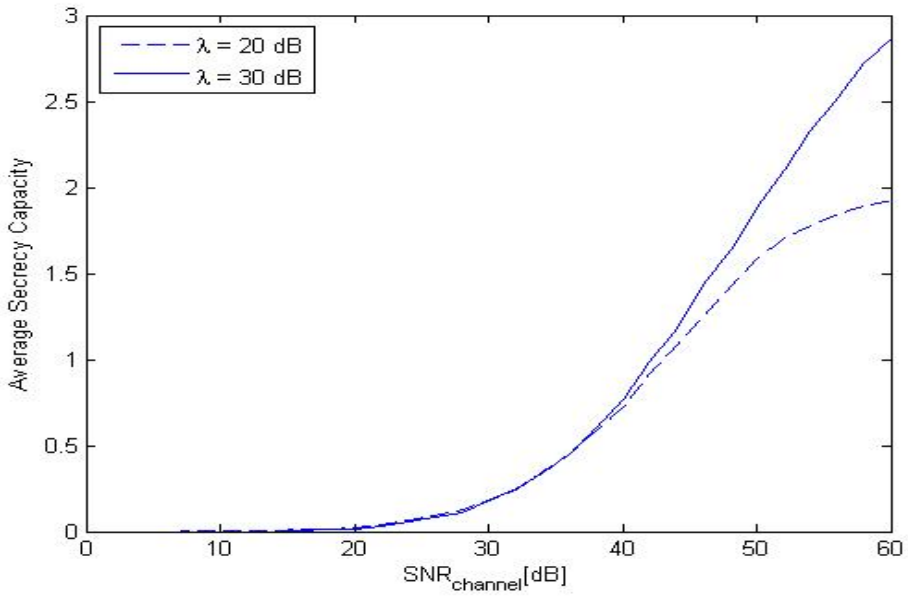

Figure 3.10. Average secrecy capacity versus channel SNR, for selected values of gain variation ratio $\lambda = 20\log\frac{A_{max}}{A_{min}}$, when an 8-bit ADC is implemented. Bob and Eve have the same AWGN channel condition.

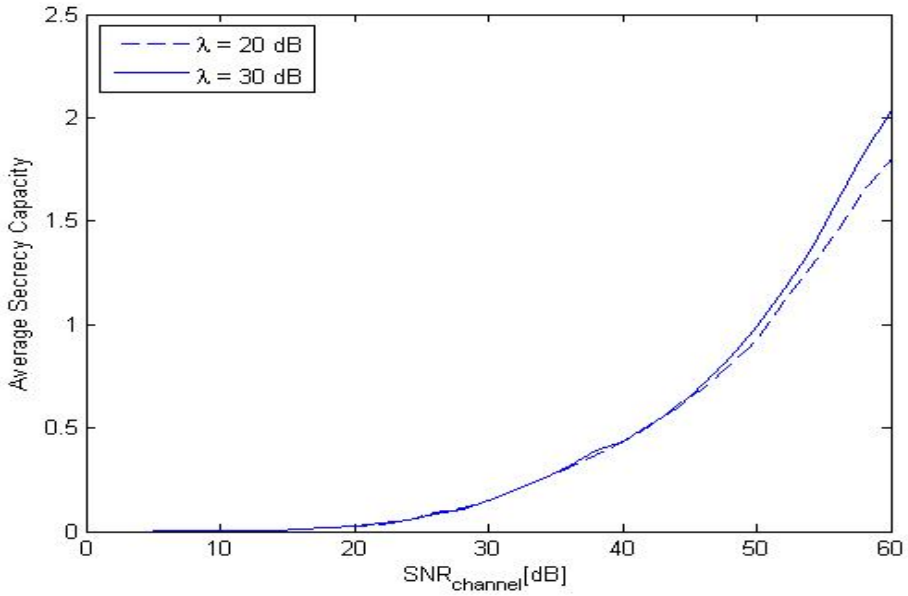

Figure 3.11. Average secrecy capacity versus channel SNR, for selected values of gain variation ratio $\lambda = 20\log\frac{A_{max}}{A_{min}}$, when a 10-bit ADC is implemented. Bob and Eve have the same AWGN channel condition.

3.6.3 Implementing multiple ADC branches

In the above sections, we showed that with two possible power amplifier gain levels A_{max} and A_{min}, it is enough to achieve positive average secrecy capacity if Eve implements one ADC branch. However, if Eve implements multiple ADC branches, the proposed technique with only two possible power amplifier gain levels can be defeated.

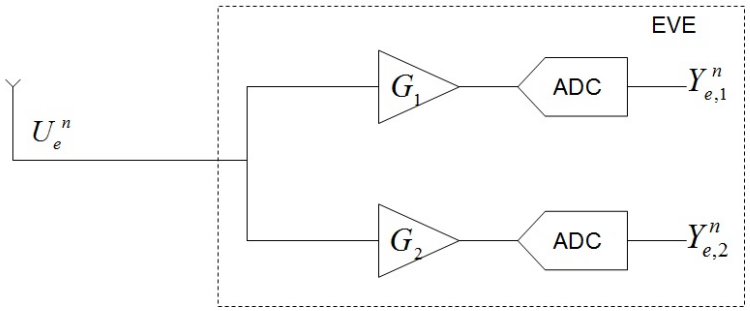

Figure 3.12. Eve implements two branches. One consists a variable gain amplifier with gain $G_1 = \frac{1}{A_{max}}$ and the other with gain $G_2 = \frac{1}{A_{min}}$.

For a powerful Eve, she might notice our trick and figure out A_{max} and A_{min}. Then, Eve can implement two branches: one has a low noise amplifier with gain $G_1 = \frac{1}{A_{max}}$ and an ADC, the other consists of a low noise amplifier with gain $G_2 = \frac{1}{A_{min}}$ and an ADC, as shown in Fig. 3.12. Eve may record the outputs of the two branches and later break the key. Then, the recorded outputs of the upper branch and lower branch are the same as what Bob received for the signals amplified with A_{max} and A_{min} respectively. With the key, Eve can choose the corresponding sections from the two recorded signals and form her received signal. Then, Eve successfully defeats our proposed technique and the average secrecy capacity is zero if there is no channel advantage for Bob.

However, if we use N levels rather than two, Eve should implement N branches to achieve zero secrecy capacity, which is hard to realize in reality. In addition, if an

infinite number of gain levels is used by setting A^n as a sequence of continuous random variables, it is impossible for Eve to implement infinitely numbers of branches. Then, a positive average secrecy capacity is achievable even if Bob does not have a channel advantage.

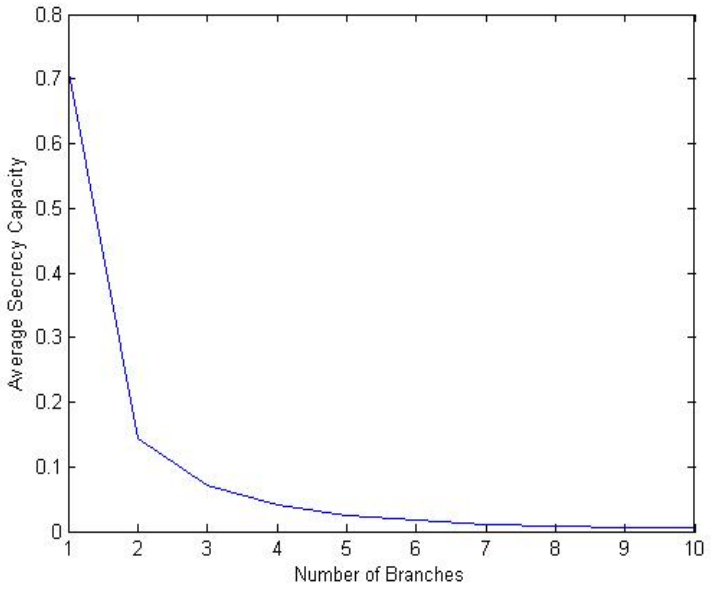

Figure 3.13. Average secrecy capacity versus number of branches implemented by Eve. Bob and Eve have the same AWGN channel condition with SNR = $40dB$.

In simulation, A^n are set as a sequence of continues random variables uniformly distributed between A_{min} and A_{max}. Eve implements N branches, each with a low noise amplifier and ADC. The gain of the amplifier of the k_{th} branch is set as $\frac{1}{G_k}$, where G_k is set as $A_{min} + (k - \frac{1}{2})\frac{A_{max} - A_{min}}{N}$. This means that Eve divides the region between A_{min} and A_{max} into N equal sections and use the middle point of each section as G_k. Fig. 3.13 shows that the average secrecy capacity is decreasing with an increasing number of branches implemented. However, even ten branches are implemented, a positive average secrecy capacity is still achieved.

3.7 Conclusion

In this chapter, we proposed a technique to deceive the AGC-ADC block in an eavesdropper's receiver to increase physical layer data transmission secrecy. By sharing a key with the legitimate receiver and fluctuating the transmitted signal power level in the transmitter side, a positive average secrecy capacity can be achieved even when Eve has the same or even better AWGN channel condition. We also examined the possible options that Eve may choose to fight against the proposed technique and demonstrated that a positive secrecy capacity can still be achieved when Eve uses these options.

CHAPTER 4

CONCLUSION

In this thesis, two imperfections of practical wireless transceiver designs, which are I/Q imbalance in transmitters and AGC-ADC cascade defects in receivers, have been addressed and exploited, respectively. The first imperfection challenges us to find a compensation technique to mitigate the QM impairments faster. The second imperfection gives us an opportunity to improve physical layer security.

In the first part, we propose a compensation technique which uses signal samples falling into the envelope detector's linear and square law regions. With the ability to use more transmitted signal samples for adaptation, the QM impairments can be compensated faster. To evaluate the performance of the proposed technique, we derive its traditional LMS implementation and prove that the overall impairments in the QMC and QM cascade converge to zero. Simulation results with a semi-ideal envelope detector reveal that the proposed technique mitigates the I/Q imbalance to the acceptable level much faster than an algorithm only working with envelope detector's linear region. However, if the envelope detector's input/output relationship is not ideal square law or linear, the convergence rate will be affected.

In the second part of the thesis, we propose a technique to attack the eavesdropper's AGC-ADC cascade by sharing an ephemeral secret key between Alice and Bob and using it for warping the signal at the transmitter and receiver. By fluctuating the power amplifier gain between two levels, a positive average secrecy capacity can be achieved even when Bob has no channel advantage. Furthermore, we consider three

options that a powerful Eve may choose to fight against the proposed technique when she notices our trick.

- The first is to optimize the loop gain in its AGC.
- The second is to record the received signal first with losing resolution of the ADC and use the later broken key to unwrap the recorded signal.
- The third is to implement multiple branches consisting an amplifier and an ADC each, then record the output of each branch and use the later broken key to unwrap each recorded signal and form the final correct signal.

The first two options have been shown to be unable to defeat the proposed technique with two gain levels. However, the third option is able to defeat an approach with two gain levels by implementing two branches under the assumptions that Eve can figure out the two gain levels. After noticing this, we propose to use infinitely many gain levels to warp the signal and demonstrate that a positive average secrecy capacity is achievable even if Eve implements numerous branches in her receiver.

BIBLIOGRAPHY

[1] J. K. Cavers, "The effect of quadrature modulator and demodulator errors on adaptive digital predistorters for amplifier linearization," *IEEE Transactions on Vehicular Technology*, Vol. 46, no. 2, pp. 456-466, 1997.

[2] J. K. Cavers and M. Liao, "Adaptive compensation for imbalance and offset losses in direct conversion transceivers," *IEEE Transactions on Vehicular Technology*, Vol. 42, no. 4, pp. 581-588, Nov 1993.

[3] M. Faulkner, T. Mattson, and W. Yates, "Automatic adjustment of quadrature modulators," *Electron Letters*, Vol. 27, no. 3, pp. 214-216, Jan 1991.

[4] D. Hilborn, S. Stapleton, and J. K. Cavers, "An adaptive direct conversion transmitter," *IEEE Transactions on Vehicular Technology*, Vol. 43, no. 2, pp. 223-233, May 1994.

[5] M. Windisch and G.Fettweis, "Blind I/Q imbalance parameter estimation and compensation in low-IF receivers," in *Proc. 1st ISCCSP*, Hammamet, Tunisia, pp. 75-78, Mar 2004.

[6] JJ. de Witt and GJ. van Rooyen, "A Blind I/Q Imbalance Compensation Techique for Direct-Conversion Digital Radio Transceivers," *IEEE Transactions on Vehicular Technology*, Vol. 58, no. 4, pp. 2077-2082, May 2009.

[7] J. K. Cavers, "New methods for adaptation of quadrature modulators and demodulators in amplifier linearization circuits," *IEEE Transactions on Vehicular Technology*, Vol. 46, no. 3, pp. 707-716, Aug 1997.

[8] Rossano Marchesani, "Digital Precompensation of Impefections in Quadrature Modulators," *IEEE Transactions on Communictions*, Vol. 48, no. 4, pp. 552-556, Apr 2000.

[9] Behzad Razavi, "Design Considerations for Direct-Conversion Receivers," *IEEE Transactions on Circuits and Systems-II Analog and Digital Signal Processing*, Vol. 44, no. 6, pp. 428-435, Jun 1997.

[10] B. Widrow, S. D. Stearns, *Adaptive Signal Processing*, Prentice-Hall, 1985

[11] W. K. Victor, M. H. Brockman, "The Application of Linear Servo Theory to the Design of AGC Loops," *Proceedings of the IRE*, Vol. 48, pp. 234-238, Feb 1959.

[12] J. M. Khoury, "On the Design of Constant Setting Time AGC Circuits," *IEEE Transactions on Circuits and Systems-II Analog and Digital Signal Processing*, Vol. 45, no. 3, pp. 283-294, Mar 1998.

[13] L. Liang, J. Shi, L. Chen and S. Xu, "Implementation of Automatic Gain Control in OFDM Digital Receiver on FPGA," *2010 International Conference On Computer Design and Applications (ICCDA 2010)*, 2010.

[14] A. Liu, J. An and A. Wang, "Design of a Digital Automatic Gain Control with Backward Difference Transformation," *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, Sep 2010.

[15] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*, Cambridge, 2006

[16] R. Benson, "The verona story," National Security Agency Central Security Service, Historical Publications (available via WWW).

[17] J. Eisert and M. Wolf, "Quantum computing," in *Handbook of Nature-Inspired and Innovative Computing*, Spring 2006

[18] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, Vol. 26, pp. 1484-1509, October 1997.

[19] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, Vol. 28, pp. 656-715, 1949.

[20] A. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, Vol. 54, pp. 1355-1387, October 1975.

[21] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information*, Seattle, WA, July 2006, pp. 356-360.

[22] U. Maurer, "Secret key agreement by public discussion from common information." *IEEE Transactions on Information Theory*, May 1993.

[23] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," *Lecture Notes in Computer Science*, Vol. 1294, pp. 292-306, 1997.

[24] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. H. Kin, "Wiretap channel with secure rate limited feedback," *IEEE Transactions on Information Theory*, Vol. 55, pp. 5353-5361, Dec 2009.

[25] G. Amariucai and S. Wei, "Feedback-based collaborative secrecy encoding over binary symmetric channels," axXiv:0909.5120v1.

[26] R. Kuchibhatia, "IMFT 25-nm MLC NAND: technology scaling barriers broken," *EE Times*, March 2010.

[27] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, Vol. 24, pp. 451-456, July 1978.