Enhanced Implementations for Arbitrary-Phase Spread Spectrum Waveforms

Michael John Fletcher

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical Engineering

Alan J. Michaels, Chair
Richard M. Buehrer
Aloysius A. Beex

May 7, 2019
Blacksburg, Virginia

Keywords: Spread Spectrum, Arbitrary-Phase, Chaotic Communications, Implementation.

Enhanced Implementations for Arbitrary-Phase Spread Spectrum Waveforms

Michael John Fletcher

(ABSTRACT)

The use of practically non-repeating spreading codes to generate sequence-based spread spectrum waveforms is a strong method to improve transmission security, by limiting an observers opportunity to cross-correlate snapshots of the signal into a coherent gain. Such time-varying codes, particularly when used to define multi-bit resolution arbitrary-phase waveforms, also present significant challenges to the intended receiver, which must synchronize correlator processing to match the code every time it changes. High-order phase shift keying (PSK) spread modulations do, however, provide an overall whiter spectral response than legacy direct sequence spread spectrum (DSSS) signals. Further, the unique ability to color the output signal spectrum offers new advantages to optimize transmission in a non-white frequency channel and to mitigate observed interference. In high data rate applications, the opportunity to inject a time-aligned co-channel underlay-based watermark for authentication at the receiver is an effective method to enhance physical layer (PHY) security for virtually any primary network waveform. This thesis presents a series of options to enhance the implementation of arbitrary-phase chaotic sequence-based spread spectrum waveforms, including techniques to significantly reduce fallthrough correlator hardware resources in low-power sensing devices for only minor performance loss, capabilities for programming chosen frequency domain spectra into the resulting spread spectrum signal, and design considerations for underlay watermark-based PHY-layer firewalls. A number of hardware validated prototypes were built on an Intel Arria 10 SoC FPGA to provide measurable results, achieving substantial computational resource gains and implementation flexibility.

Enhanced Implementations for Arbitrary-Phase Spread Spectrum Waveforms

Michael John Fletcher

(GENERAL AUDIENCE ABSTRACT)

This thesis presents a series of options for enhancing the implementation of arbitrary-phase spread spectrum waveforms, a highly-secure class of wireless technologies, in order to reduce design complexity with minimal loss, provide methods for real-time performance adaptations, and extend the traditional application space for increased security of communications in other networks. A number of enhanced hardware prototypes were implemented to provide measurable results, achieving substantial computational resource gains and design flexibility. Given the computational resources and power constraints of devices in the Internet of Things (IoT), the signal detection loss of 2.10 dB for reducing the hardware logic utilization of the brute force fallthrough correlator by more than 76% (and eliminating the need to dedicate computationally-expensive embedded multipliers) is a very reasonable trade. While the waveform is fundamentally designed for increased security, adapting to widespread and/or commercial use may allow some sacrifice of the signal's ability to avoid interception/detection to improve performance in undesirable operating conditions. In a similar, yet reversed, case, injecting a watermarking signature at the physical layer (PHY) of less-secure wireless technologies for receiver-side authentication also proves to be beneficial.

Contents

List of Figures

List of Tables

List of Abbreviations

AJ Anti-Jam

ALM Adaptive Logic Module

ALUT Adaptive Lookup Table

BER Bit Error Rate

BPSK Binary Phase Shift Keying

CDMA Code Division Multiple Access

CPM Continuous Phase Modulation

CSD Canonic Signed Digit

CSK Carrier Shift Keying

CSSS Chaotic Sequence Spread Spectrum

CW Continuous Wave

DSP Digital Signal Processing

DSSS Direct Sequence Spread Spectrum

FIR Finite Impulse Response

FPGA Field Programmable Gate Array

FS-HOPS Frequency-Selective High-Order Phase Shift Keying

FSK Frequency Shift Keying

HDL Hardware Definition Language

HOPS High-Order Phase Shift Keying Signaling

IoT Internet of Things

IP Intellectual Property

IP Internet Protocol

LPD Low Probability of Detection

LPI Low-Probability of Interception

LUT Lookup Table

MAC Medium Access Control

MCS Modulation and Coding Scheme

MLSE Maximum Likelihood Estimation

NCO Numerically Controlled Oscillator

OFDM Orthogonal Frequency Division Multiplexing

P_d Probability of Detection

PHY Physical Layer

PN Pseudo-Noise

PRNG Pseudo-Random Number Generator

PSD Power Spectral Density

PSK Phase Shift Keying

QPSK Quadrature Phase Shift Keying

RA-CDMA Receiver-Assigned Code Division Multiple Access

RF Radio Frequency

RFI Radio Frequency Interference

RNS Residue Number System

ROC Receiver Operating Characteristic

SINR Signal-to-Interference-plus-Noise Ratio

SNR Signal-to-Noise Ratio

SoC System on a Chip

TRANSEC Transmission Security

Chapter 1

Introduction

Spread spectrum modulations have frequently achieved reliable wireless communications, even in the presence of co-channel interference, since the interfering signal power is often much lower relative to the wider frequency band [7]. Direct sequence spread spectrum (DSSS) is a common spreading technique that fundamentally attempts to reduce the signal's power spectral density (PSD) by distributing the instantaneous symbol energy over spreading codes operating at a higher rate. Traditional DSSS employs 2-ary or 4-ary spreading codes resembling pseudo-noise (PN) sequences, effectively forming wideband versions of standard binary PSK (BPSK) and quadrature PSK (QPSK) signals.

Chaotic sequence-based spread spectrum (CSSS) operates similarly to DSSS, yet employs arbitrary-phase spreading codes derived from multi-bit resolution chaotic sequences [8]. Without *a priori* knowledge of the sequence generation process, it is unlikely that the spread signal will be successfully demodulated for exploitation, and the added diversity benefit of practically non-repeating sequence-based spreading codes also leads to improved code division multiple access (CDMA) networking operations [12].

Increasing the order of PSK-based spread modulations improves the low-probability of signal interception/detection (LPI/D) [14] by forming a more noise-like PSD. The "arbitrary-phase" nature of 2^k-ary PSK-based spreading codes ($k \geq 8$), such as those used by the High-Order PSK Signaling (HOPS) spread spectrum waveform [9], offers useful properties for signal acquisition, with impulse-shaped autocorrelation functions and constant envelope signals

similar to those of constant amplitude zero autocorrelation-function (CAZAC) sequences [2].

1.1 Motivation

In summary, the work presented in this thesis seeks to enhance arbitrary-phase spread spectrum signal processing hardware implementations with respect to application hardware performance trades and/or use cases. Specifically, the reliable asynchronous reception, physical layer (PHY) security, and scalable receiver-assigned CDMA (RA-CDMA) networks [12] of the digital chaos-based arbitrary-phase formulations are accompanied by computationally-intense receiver processing. For resource-constrained wireless networks, such as that of low-power sensing devices in the Internet of Things (IoT), adapting the ideal performance for reduced power consumption and/or hardware resources may be optimal. Hybridized modulation techniques are also considered to improve signal resiliency or to further increase transmission security. Lastly, while spread spectrum data links typically feature low data rates, supporting PHY-secured high throughput wireless communications is a desirable goal.

1.2 Contributions

This thesis provides enhancements, implementation trades, and design considerations for chaotic sequence-based arbitrary-phase spread spectrum waveforms. Each chapter in the body of this thesis is supported by real-world measurements from hardware prototypes built on an Intel Arria 10 system on a chip (SoC) field programmable gate array (FPGA), using synthesizable Verilog hardware description language (HDL) source code modified for the relevant implementation(s).[1]

[1]Noting that all hardware prototypes implement the arbitrary-phase HOPS spread spectrum waveform.

The work presented in Chapter 2 directly addresses the computationally-intense receiver signal processing that arises from the long spread spectrum delay lines in the matched-filter correlator, expounded by the time-varying multi-bit resolution correlation taps derived from arbitrary-phase chaos-based spreading codes. For context, the 1400 complex-valued correlations of the brute-force structure comprise 81% of overall hardware resources, and the Arria 10 FPGA lacks sufficient embedded multipliers to compute 4200 multiplications in parallel. This manuscript is cited by [4] and referenced below.

- **M. J. Fletcher**, A. J. Michaels, and D. B. Ridge, "Fallthrough Correlation Techniques for Arbitrary-Phase Spread Spectrum Waveforms," *IEEE Access Journal*, 2019 [submitted].

Chapter 3 presents methods to hybridize the arbitrary-phase / HOPS system by introducing frequency spectrum shaping of the signal. The introduction of color maps for the sequence-based phase words followed by incremental rolling-over of accumulated sums can be used to adapt the output spectra to resemble selectively programmed waveforms, while allowing dynamic frequency bin customizations. Alternatively, marginally colored instantaneous frequencies give additional capability to adapt to the environment, without sacrificing the LPI/D characteristics. In the paper listed below and in [10], my contributions included composition of results, predictable color map design methods, and implementing the design for verification on the FPGA hardware prototype.

- A. J. Michaels and **M. J. Fletcher**, "Frequency-Selective High-Order PSK Signaling." *IEEE Military Communications Conference 2019 (MILCOM)*, [submitted].

The discussion is furthered in Chapter 4 by demonstrating a PHY-layer firewall design for IEEE 802.11g using co-channel underlay-based watermark authentication. Building on

the concepts presented in [11], the sequence-based watermark may be implemented for virtually any wideband data link waveform. This approach gives the wireless device access control functions resembling those of traditional Ethernet-based firewalls, built from the time-evolving chaotic sequences, without sacrificing the use of high-rate data link modes. The manuscript of Chapter 4 is cited by [3] and referenced below.

- **M. J. Fletcher**, J. D. Gaeddert, and A. J. Michaels, "Physical Layer Firewall Design using Co-Channel Underlay-Based Watermark Authentication," *IEEE Military Communications Conference 2019 (MILCOM)*, [submitted].

In each of the above manuscripts, the introductions and background sections supply reviews of literature and comparisons to existing art. Specific methods are described in detail in the body of the chapters followed by hardware validation results that may include the measured probability of detection (P_d), bit error rate (BER), and/or hardware resource utilization. Finally, conclusions are offered and summarized altogether in Chapter 5, along with descriptions of potential revisions and proposals for future work.

1.3 Attribution

The primary goal of the researcher is to contribute to the wealth of academic knowledge and, having submitted [4] to IEEE Access Journal and [3] to the IEEE Military Communications Conference, with intellectual property (IP) creation and strong potential for patents in [4] and [10], that product has/will be achieved. Of course, the effort is not solitary; Dr. Alan Michaels served as co-author of the manuscripts in this thesis, giving direction to literature reviews and method formulation. Devin Ridge resourcefully aided FPGA hardware prototype implementations, while Dr. Joseph Gaeddert helped to architect the watermark-based

authentication prototype of Chapter 4, having previously developed the liquid-dsp [5] and liquid-wlan [6] open-source software libraries.

A considerable amount of effort went into FPGA implementations of the prototypes, including HDL source code composition, hardware debugging, and performing a number of measurements for a variety of operating modes. The HOPS hardware system originated from a fixed-point Simulink model created by Dr. Michaels, thus requiring hardware integration hours to run on the Arria 10 SoC FPGA (equipped with the Analog Devices AD9361-based FMCOMMS3 mezzanine card). Further efforts sought to improve digital signal processing (DSP) on the FPGA, specifically to minimize fixed-point round-off and overflow errors [13].

Chapter 2

Fallthrough Correlation Techniques

Abstract

The use of practically non-repeating spreading codes to generate sequence-based spread spectrum waveforms is a strong method to improve transmission security, by limiting an observer's opportunity to cross-correlate snapshots of the signal into a coherent gain. Such time-varying codes, particularly when used to define multi-bit resolution arbitrary-phase waveforms, present significant challenges to the intended receiver, who must synchronize acquisition processing to match the time-varying code each time it changes. This paper presents a series of options for optimizing the traditional brute-force matched-filter preamble correlator for burst-mode arbitrary-phase spread spectrum signals, achieving significant computational gains and flexibility, backed by measurable results from hardware prototypes built on an Intel Arria 10 FPGA. The most promising of which requires no embedded multipliers and reduces the total hardware logic by more than 76%. Extensions of the core fallthrough correlator techniques are considered to support asynchronous reception, underlay-based PHY-layer firewall functions, and RA-CDMA protocols in low-power devices.

2.1 Introduction

The design of burst-mode communication systems presents additional challenges over that of a standard continuous data link, in particular due to the need to re-acquire the signal on a burst-by-burst basis. In low-power devices, such as those suitable for Internet of Things (IoT), burst-mode waveforms traditionally employ techniques to make the acquisition preamble as easy to receive as possible, typically by embedding pilot tones [1], repeated cyclic prefixes [2], cyclic autocorrelation functions [3], soft-handoff between spreading codes [4], Barker-sequence / short preamble repetition [5], maximal-likelihood estimation [6], and/or variations of matched-filter techniques [7], [8]. Virtually all of these approaches rely on an inherent cyclostationary signal feature of the preamble bursts, facilitating blind detection and/or exploitation by an unintended receiver.

All signals considered in this paper are chaotic sequence-based arbitrary-phase spread spectrum waveforms with optional chip amplitude shaping, most of which use practically non-repeating spreading codes designed to eliminate cyclostationary signal content. Reception of these signals is therefore more complicated, using methods that adapt some aspects of the matched-filter/coherent receiver processing architectures for specific waveforms and/or use cases [9]-[12]. Further, most of these techniques are computationally intensive, making them difficult to implement in a low-power device.

Starting with the traditional brute-force matched-filter correlator, this paper presents computational efficiency improvements for a generic coherent receiver architecture where the matched-filter coefficients change on a burst-to-burst basis, offering lower-power / computationally efficient methods that achieve the same purpose. Similar analyses have evaluated the reduced-computation processing of the semi-coherent chaotic carrier shift keying (CSK) waveforms [13]. There, however, the timing and phase are effectively coherent.

The core fallthrough correlator design model is provided in Section II. Enhancements for reduced-precision correlations, optimally pruned coefficients, and variable-length operations are all considered in Section III. Measurable results from hardware prototypes built on an Intel Arria 10 field-programmable gate array (FPGA) are presented in Section IV, offering simpler methods for asynchronous reception, underlay-based watermark validation [14], and receiver-assigned code-division multiple access (CDMA) operations [15] in IoT-caliber devices. Finally, conclusions can be found in Section V.

2.2 Computational Model

The time-based evolution of matched-filter coefficients eliminates many of the standard methods for collapsing the digital logic structure to take advantage of a priori known cyclostationary preamble signal features, while the multi-bit resolution spreading codes used to generate the arbitrary-phase spread spectrum waveforms, such as the chaotic sequence spread spectrum (CSSS) [9], [10] or high-order PSK signaling (HOPS) [16] waveforms, increase overall complexity of the complex-conjugate multiplications (correlations) in contrast to 2-ary or 4-ary chip phase direct sequence spread spectrum (DSSS) signals [17]. To support the discussion, consider the matched-filter correlator model shown in Fig. 2.1, where each x is a complex-valued received signal sample and each y is a matched-filter coefficient taken from the internally generated preamble signal replica.

This model is similar to a direct form finite impulse response (FIR) filter, where a fully pipelined set of outputs is derived from incoming samples as they progress through the delay line structure. With FIR filters, significant improvements may typically be made (a) due to symmetry of wisely chosen coefficients (pre-additions), (b) elimination of sufficiently small / zero coefficients (pruning), (c) canonic signed digit (CSD) mapping of static coefficients

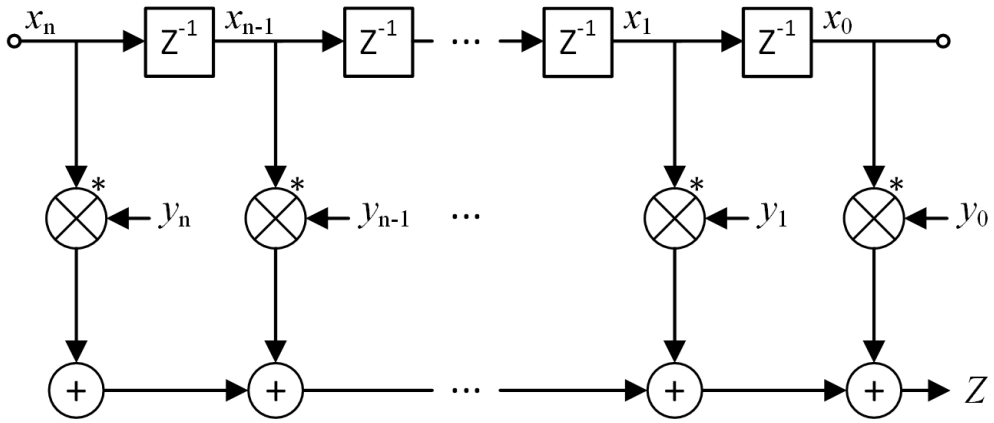


Figure 2.1: Fallthrough correlator in direct form FIR structure. The matched-filter coefficients $\{y_0, y_1, ..., y_n\}$ are registered for use each time epoch.

to shift-adds [18], (d) employing computationally efficient multi-rate processing structures [19], and (e) variable control of the coefficient word widths.

Within the correlation calculation, these traditional simplifications are limited: (a) the correlation of a preamble without any cyclostationary features can not have easily exploitable symmetries, (b) coefficients may be pruned, though the correlation taps generally contribute a similar amount of energy to the composite correlation value, (c) CSD mappings may also be applied, but must be dynamically addressable with variable barrel shifters, (d) the notionally fixed sample rate hinders any multi-rate signal processing benefit, (e) and the coefficient word width in hardware will need to support the largest width that the coefficient may ever be, burst-to-burst.

In addition to these distinctions from a standard FIR filter, the logic within the fallthrough correlator must support clocking in of new coefficients on a burst-by-burst basis, so that they are in place and ready for correlation processing when the next sample arrives. Under the assumption of normalized inputs, the correlator output response Z ideally triggers based on a defined correlation peak having magnitude equal to the average chip energy times the

length of the correlation. The coherent preamble signal is trivial to normalize, while the incoming received signal is variable and highly dependent on any system gains that may occur prior to the correlator. This is particularly important for spread spectrum systems, since the signal often operates at or below the ambient noise floor of the receiver and allows for power level estimates of the incoming signal and/or its multipath components based on the magnitude of the resulting correlation peak(s).

The next distinction is that of phase rotations, with particular focus on center frequency offsets. The static phase rotation may be detected from the phase offset of the correlation peak (referenced to the center of the correlation window) and subsequently corrected prior to despreading. Frequency offset, on the other hand, requires comparison of multiple sub-correlation values throughout the correlator structure, so that the phase rotations may be measured as a function of time and translated, via the known sample rate, to an instantaneous frequency offset that can be applied to the remainder of the pulse. If the frequency offset causes the correlation values to drift more than $\approx \pi/2$ radians over the duration of the preamble, then the integration process underlying the addition of the taps will begin to fail.

The final distinction of timing uncertainty due to phase noise or oscillator drift is also not supported by this FIR structure. Practical clocks (<100 ppm) will tend not to drift beyond that which is supported, and the detection of future preambles will have unique starting sample points, making only the short-term stability of individual bursts relevant.

2.3 Fallthrough Correlator Enhancements

The chief focus of this paper is on the computational efficiency improvements that may be made to the fallthrough correlator to achieve reasonably solid performance from a minimum amount of hardware. In particular, the allowable resource and performance trades from

the hardware baseline of a brute-force design that implements a complex multiplication $z = (y_I + jy_Q)(x_I - jx_Q)$ using the three real-multiplier reduction in (2.1) and (2.2), where $z_I + jz_Q$ is a partial sum.

$$z_I = (y_I x_I + y_Q x_Q) \tag{2.1}$$

$$z_Q = ((y_I + y_Q)(x_I - x_Q) - y_I x_I + y_Q x_Q) \tag{2.2}$$

To adapt this model to an IoT-relevant context, the following series of identified improvements may be incorporated.

2.3.1 Truncated Coefficients

The precision of the matched-filter coefficients may be reduced with acceptable detection loss, even for arbitrary-phase waveforms.[1] Such truncation must account for the full processing chain of the transmitted signal, including any interpolation, prior to transmission. Since each arbitrary-phase spreading chip is taken from an allowable set of discretized phase points on the unit circle [16], truncation in both the in-phase (I) component y_I and quadrature (Q) component y_Q will introduce amplitude and phase mismatch loss to the calculation. Using a bit precision ≥ 6 bits gives almost no performance loss, while truncation to 1-bit coefficients provides the largest computational gains, offering a hardware structure resembling the correlator of DSSS signals.

Choosing the 1-bit truncated coefficients, the correlation logic may be implemented as four negations of $\{x_I, x_Q\}$ based on sign$\{y_I, y_Q\}$ followed by two additions. However, any quantization effects of truncation should be considered prior to processing the correlation peak for received signal power estimations. For the hardware prototypes, the overall HOPS waveform

[1] The arbitrary-phase nature results from the use of 2^k, $k > 8$ allowable phase words.

is constant envelope (i.e., $x_I^2 + x_Q^2 = 1 \forall x$), and the output response can be scaled by the reciprocal of the expected coherent signal correlation $E\left[|x_I| + |x_Q|\right] = 2 \cdot E\left[|x_I|\right] = 4/\pi$ to correct for this distortion.

2.3.2 Dynamic Pruning

Upon definition of the matched-filter coefficients, if either component in I or Q does not contribute a meaningful amount of energy to the correlation, then the coefficient may be collapsed into a single real-valued or imaginary-valued correlation tap. For the spread spectrum waveforms with amplitude-varying chips, this pruning may be pursued consistent with the selective noise cancellation techniques described in [20], while for the constant envelope modulations, a parameter λ can be defined to represent the amplitudes of components to be discarded, as shown in Fig. 2.2.

In any scenarios where $\min\{|y_I|, |y_Q|\} < \lambda$, then $\max\{|y_I|, |y_Q|\} > \sqrt{1-\lambda^2}$, resulting in the detection performance loss shown as a function of λ in Fig. 2.3. The simulated loss of 0.87 dB at the median value $\lambda = \sqrt{2}/2$ allows a simplified pruning process equivalent to selecting the larger of $\{|y_I|, |y_Q|\}$ for correlations with the received signal. In other words, (2.1) is reduced to:[2]

$$z_I \approx \begin{cases} y_I x_I, & |y_I| \geq |y_Q| \\ y_Q x_Q, & |y_I| < |y_Q| \end{cases} \tag{2.3}$$

[2]By using only correlation taps that do not contain points at $|y_I| = |y_Q|$, which is easily achieved by rotating the entire set of allowed discretized points by the phase of one half LSB, a strict maximum may be achieved. In the case where the two values are equal (within the chosen comparator's precision), then the choice of which one to take forward is arbitrary.

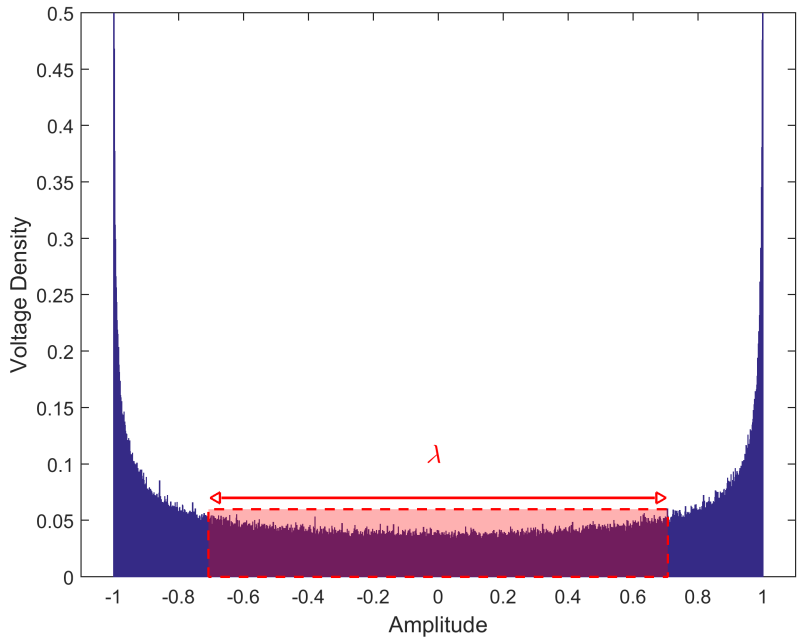


Figure 2.2: Conceptual depiction of correlation tap pruning; overlaid on voltage distribution of randomly selected points on the unit circle projected onto one axis.

and (2.2) is reduced to:

$$z_Q \approx \begin{cases} -y_I x_Q, & |y_I| \geq |y_Q| \\ y_Q x_I, & |y_I| < |y_Q| \end{cases} \tag{2.4}$$

With 1-bit truncated $\lambda = \sqrt{2}/2$ pruned coefficients, the correlation logic may be implemented as four negations of $\{x_I, x_Q\}$ based on sign$\{y_I, y_Q\}$ followed by max$\{|y_I|, |y_Q|\}$-induced selection of the complex-valued output. Despite the further hardware savings, pruning at the median value eliminates the amplitude mismatch by rotating the allowable taps onto the axes and reduces any phase mismatch to within $[-\pi/4, \pi/4]$, giving a degradation reduction of 3 dB over truncated coefficients without pruning. Using a smaller value for λ provides only marginal performance increases and requires dynamic placement of the adders - to allocate these adders on a burst-to-burst basis is likely to take more logic than simply provisioning

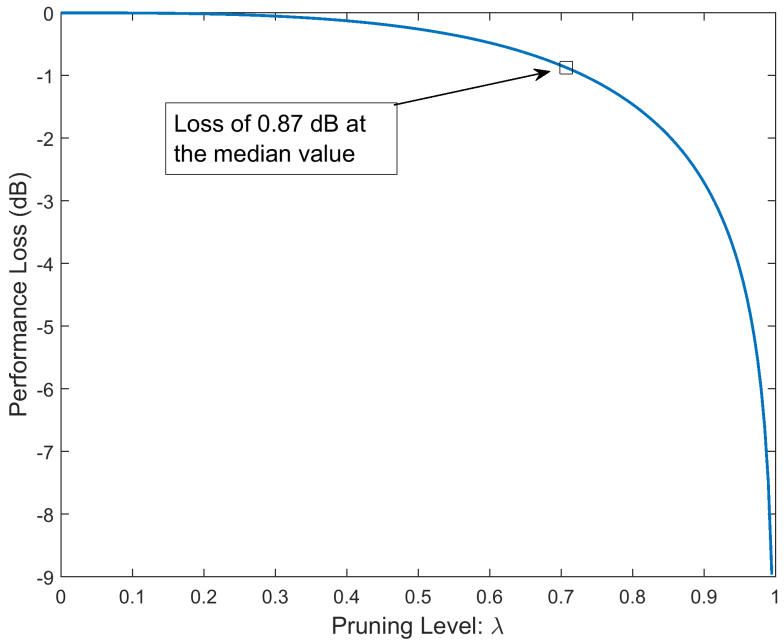


Figure 2.3: Simulated performance degradation based on choice of λ. The median value corresponds to a 0.87 dB loss (equivalently, $\lambda = \sqrt{2}/2$).

all taps with the same two adder structure.

2.3.3 Folded Correlation Taps

The sequence of matched-filter coefficients may be folded by consciously aliasing the correlation taps onto one another, achieving a significant reduction in the digital logic dedicated to the long delay lines of the received signal. While the increase in false positives would be unacceptable for lightly spread signals, the self-interference characteristics of deeply spread signals allow for minimal performance loss. However, shorter preambles do have more difficulty in estimating phase rotations / frequency offsets, placing a practical minimum bound on the order of 2 symbols.

Consider the 4× folded correlator shown in Fig. 2.4, trading some additional control logic for

an effectively reduced delay line length of one-fourth its original length. For the folded taps hardware prototype, the 1400 correlation taps are divided into four equal-length sets of 350 taps each. That is, $\{a_0, a_1, ..., a_{349}\} \equiv \{y_0, y_1, ..., y_{349}\}$, $\{b_0, b_1, ..., b_{349}\} \equiv \{y_{350}, y_{351}, ..., y_{699}\}$, and so on.

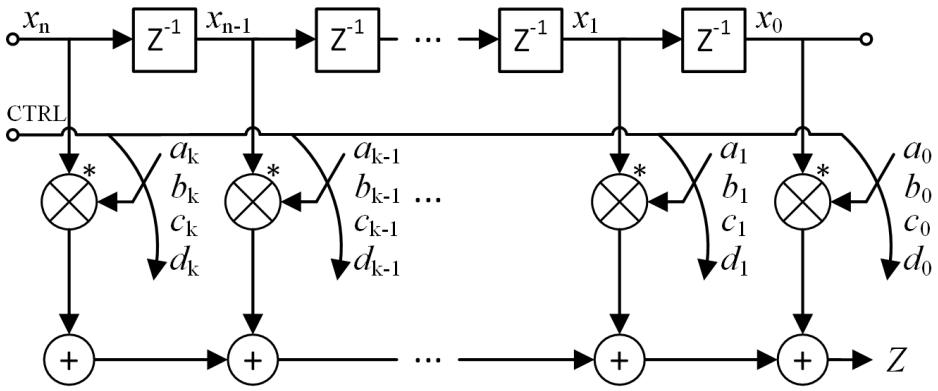


Figure 2.4: Fallthrough correlator with 4× folded correlation taps in direct form FIR structure. The control line selects one set of taps based on the pipelined detection state.

The control circuitry can be implemented in any number of ways. Within the context of this paper, the logic operates as follows. Each time a new incoming sample is clocked into the delay line, the control selects one of the four sub-preamble sequences to be used for correlations in that sample clock cycle. The selection is based on the pipeline decision state of previous sub-preamble detections, with reference to when the sample that just exited the delay line was the incoming sample. If a detection was triggered for the exiting sample, then the correlation taps progress to the next sequence (until another new sample is clocked in). Signal timing is acquired after four sub-preamble detections have triggered in succession.

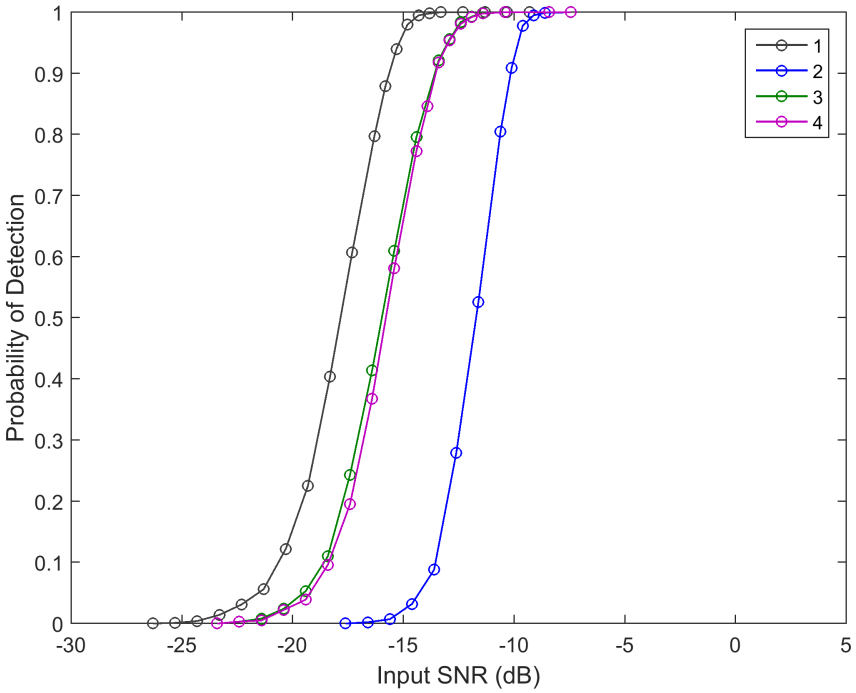


Figure 2.5: Comparative preamble detection performance for each of the fallthrough correlator design variants.

2.4 Hardware Prototype Validation

A selection of hardware prototypes was built on an Intel Arria 10 SoC FPGA for reception of the arbitrary-phase HOPS spread spectrum waveform [16], including: (1) a brute-force[3] matched-filter model, (2) a 1-bit truncated coefficients model, (3) a truncated coefficients model with $\lambda = \sqrt{2}/2$ pruning, and (4) a truncated pruned coefficients model with $4\times$ folded correlation taps. Of primary interest is the hardware reduction achieved by the computational enhancements, the comparative utilization numbers are provided in Table 2.1 as extracted from the Quartus fitter reports, focusing on the relevant use of adaptive logic modules (ALMs), combinational adaptive look-up tables (ALUTs), dedicated registers, and

[3]The hardware prototype HOPS system employs an 8 symbol preamble and 175 chip spread ratio. Since the Arria 10 FPGA is limited to 3374 multipliers, the $3 \cdot 8 \cdot 175 = 4200$ multiply operations required by the brute-force design are clocked at a higher rate to fit on the device.

DSP blocks.

Table 2.1: FPGA Hardware Resource Utilization.

Model	ALMs	ALUTs	Registers	DSP Blocks
1	79000	144690	180035	4200[1]
2	72801	145281	117985	0
3	62151	106257	112321	0
4	18698	27280	32301	0

[1] Increased from an initial 1400 DSP blocks operating at more than 3× real-time clock speed.

The most significant reduction is the elimination of hardware multipliers, a major advantage of truncation to 1-bit coefficients. An application-specific design could likely benefit more from the adder-less $\lambda = \sqrt{2}/2$ pruned correlations, since it is not limited by the static embedded structure of an FPGA, although the 17% ALM reduction from (2) to (3) is notable. Model (4) provides the most dramatic hardware reduction, where the 70% ALM reduction from (3) to (4) is on par with a correlator of 1/4th size.

Also of interest is the measured preamble detection performance for the hardware prototypes. All of the non-correlator modules were synthesized using the same Verilog hardware description language (HDL) source, including the actual phase / frequency offset estimator circuits. The thresholding scheme does behave slightly differently between variants - to ensure accurate results, the trigger level was set by empirically searching for the threshold that gives the best performance without returning false detections.

The measured probability of detection (P_D) is shown with respect to signal-to-noise ratio (SNR) in Fig. 2.5 with the degradation at $P_D = 0.9$ highlighted in Fig. 2.6 and Fig. 2.7. As expected, the computationally reduced models do yield reduced performance, yet in a very controlled manner. Given the transformation of complex multipliers to sign-selected adder trees, the loss of 5.49 dB for (2) is tolerable. Model (3) reduces the degradation by 3.43 dB, demonstrating the inherent noise cancellation properties of the amplitude-selective

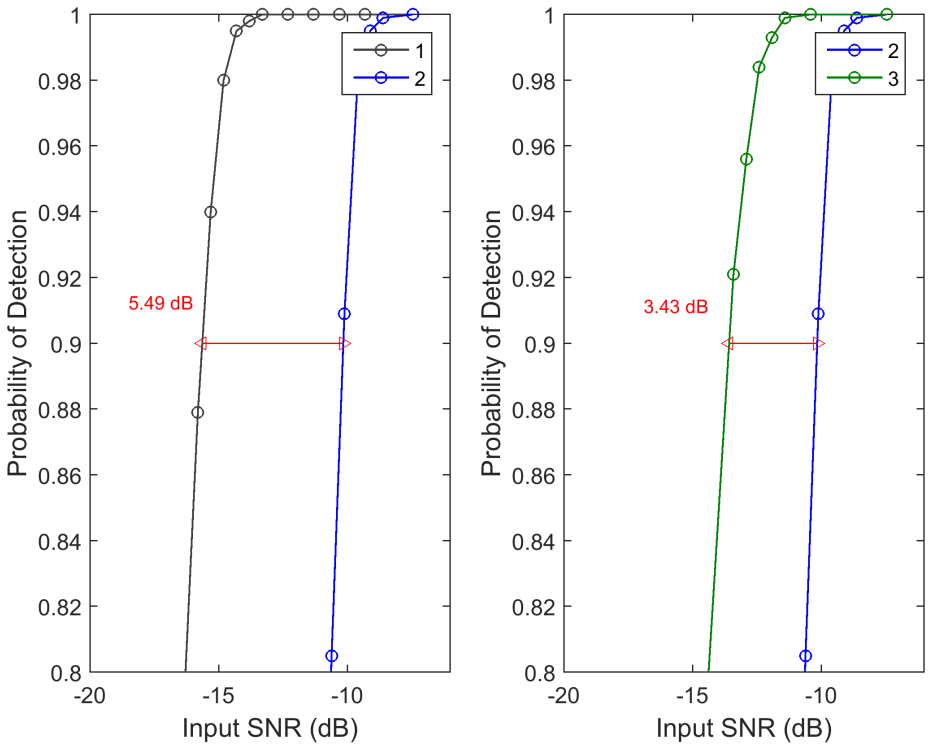


Figure 2.6: Measured implementation loss due to truncation to 1-bit coefficients and $\lambda = \sqrt{2}/2$ pruning degradation reduction.

collapse of truncated coefficients. The 2.10 dB performance loss of (4) is the most promising, offering performance almost identical to (3), while providing an overall 76% ALM reduction, requiring 82% fewer dedicated registers, and using no DSP blocks.

2.5 Conclusion

This paper proposed a variety of candidate improvements to the brute-force fallthrough correlator structure, allowing significant computational efficiency improvements and hardware utilization reductions with minimal degradation to preamble detection performance. The truncation of multi-bit precision matched-filter coefficients to 1 bit offers a consolidation

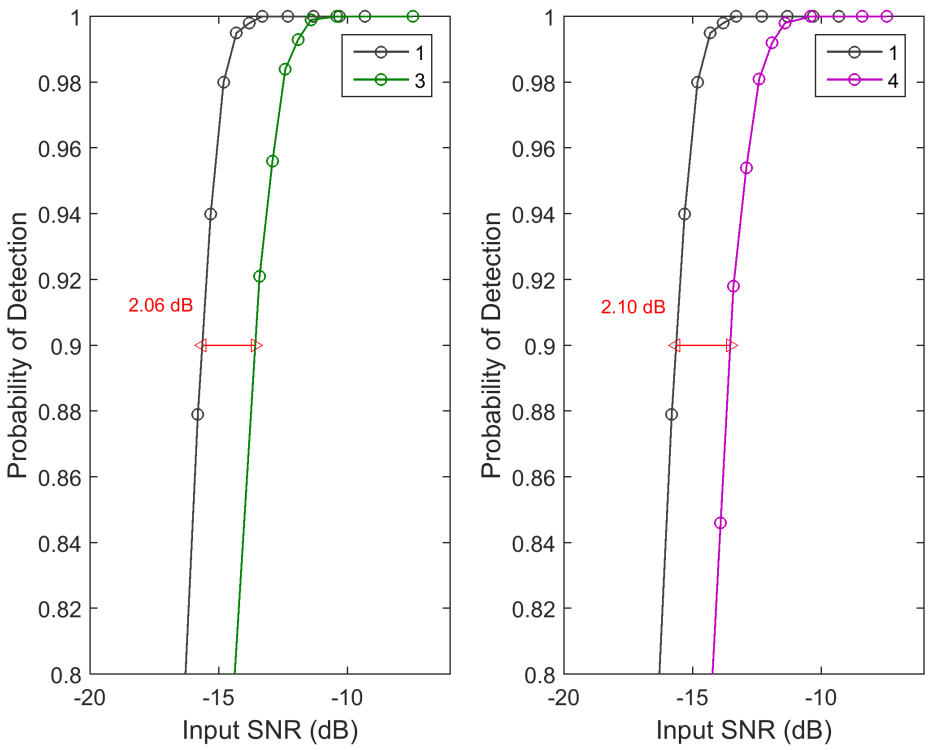


Figure 2.7: Measured implementation loss of the unfolded and folded correlation tap structure with $\lambda = \sqrt{2}/2$ pruned 1-bit truncated coefficients.

of FPGA resources from the brute-force 4200 embedded multipliers and 79000 ALMs to no multipliers and 72801 ALMs. The amplitude-selective collapse of complex-valued coefficients into a single real or imaginary correlation tap further reduces the hardware logic for an overall detection loss of 2.06 dB. Achieving the most substantial hardware reductions is the 4× folded structure with pipelined detection decisions, using no multipliers and 76% fewer ALMs overall, for the trade of only a 2.10 dB performance loss. Moreover, this approach is completely extensible to the Gaussian-shaped digital chaotic spread spectrum signals.

The processing of outputs from computationally reduced correlators needs to consider the expected correlation peak loss in received signal strength estimations, while phase / frequency offset estimations will also be less accurate. By performing an on-time accumulation

of the detected preamble signal, any performance loss can be mitigated at the cost of a single shared full-precision multiply-accumulate circuit and some added processing latency. The correlation of shorter preambles will increase estimation error, as necessary for the folded correlation tap structure and largest hardware logic reduction shown in this paper. In that case, storing sub-correlation peak outputs in appropriately sized reference registers is a potential solution, and the optimal sizing of these registers based on the allowable probability of false accept per stage is considered for future work.

References

[1] Jing Lei and Tung-Sang Ng, Pilot-tone-based maximum likelihood estimator for carrier frequency offset in OFDM systems, Communications, 2003. ICC '03. IEEE International Conference on, 2003, pp. 2046-2050 vol.3.

[2] D. Yan and P. Ho, Code acquisition in a CDMA system based on Barker sequence and differential detection, in IEEE PIMRC'95, Toronto, ON, Canada, 1995, pp. 233–236.

[3] C. Du, H. Zeng, W. Lou and Y. T. Hou, On cyclostationary analysis of WiFi signals for direction estimation, 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 3557-3561.

[4] G. E. Corazza and A. Vanelli-Coralli, Burst vs. continuous pilot acquisition in wideband CDMA cellular mobile systems, WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No.99TH8466), New Orleans, LA, 1999, pp. 1080-1084 vol.3.

[5] S. J. Lee and J. Ahn, Acquisition performance improvement by Barker sequence repetition in a preamble for DS-CDMA systems with symbol-length spreading codes, in IEEE Transactions on Vehicular Technology, vol. 52, no. 1, pp. 127-131, Jan 2003.

[6] W. S. Yuan and C. N. Georghiades, Rapid carrier acquisition from baud-rate samples, in IEEE Transactions on Communications, vol. 47, no. 4, pp. 631-641, Apr 1999.

[7] J. Lindenlaub and K. Chen, Performance of Matched Filter Receivers in Non-Gaussian Noise Environments, in IEEE Transactions on Communication Technology, vol. 13, no. 4, pp. 545-547, December 1965.

[8] M. K. Sust and A. Goiser, A combinatorial model for the analysis of digital matched filter receivers for direct sequence signals, Global Telecommunications Conference and Exhibition 'Communications Technology for the 1990s and Beyond' (GLOBECOM), 1989. IEEE, Dallas, TX, 1989, pp. 1634-1640 vol.3.

[9] G. Heidari-Bateni and C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, in IEEE Transactions on Communications, vol. 42, no. 234, pp. 1524-1527, Feb/Mar/Apr 1994.

[10] A. J. Michaels and D. B. Chester, Efficient and flexible chaotic communication waveform family, 2010 - MILCOM 2010 Military Communications Conference, San Jose, CA, 2010, pp. 1250-1255.

[11] A. Martin, Y. Hasan and R. M. Buehrer, Physical layer security of hybrid spread spectrum systems, 2013 IEEE Radio and Wireless Symposium, Austin, TX, 2013, pp. 370-372.

[12] A. J. Michaels and D. B. Chester, Adaptive correlation techniques for spread spectrum communication systems, MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, 2016, pp. 678-681.

[13] A. A. Zaher, An improved chaotic shift keying technique, 2012 5th International Symposium on Communications, Control and Signal Processing, Rome, 2012, pp. 1-4.

[14] R. Chakravarthy, Kaiyu Huang, Lin Zhang and Z. Wu, Primary User authentication of cognitive radio network using underlay waveform, 2017 Cognitive Communications for Aerospace Applications Workshop (CCAA), Cleveland, OH, 2017, pp. 1-5.

[15] E. Petrosky and A. Michaels, Network scalability comparison of IEEE 802.15.4 and Receiver-Assigned CDMA, in IEEE Internet of Things Journal, 2019, pp 1–1. ISSN 2327-4662.

[16] A. J. Michaels, High-Order PSK Signaling (HOPS) Techniques for Low-Power Spread Spectrum Communications, 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Chania, Greece, 2018, pp. 01-07.

[17] M. B. Pursley, T. C. Royster and M. Y. Tan, High-rate direct-sequence spread spectrum, IEEE Military Communications Conference, 2003. MILCOM 2003., 2003, pp. 1101-1106 Vol.2.

[18] R. M. Hewlitt and E. S. Swartzlantler, Canonical signed digit representation for FIR digital filters, 2000 IEEE Workshop on signal processing systems. SiPS 2000. Design and Implementation (Cat. No.00TH8528), Lafayette, LA, 2000, pp. 416-426.

[19] F. Harris, C. Dick, and M. Rice, Digital receivers and transmitters using polyphase filter banks for wireless communications, IEEE Trans. on Microwave Theory and Techn., vol. 51, pp. 1395–1412, April 2003.

[20] A. Michaels, Digital chaotic communications, PhD dissertation, Georgia Institute of Technology, 2009.

Chapter 3

Frequency-Selective High-Order Phase Shift Keying

Abstract

This paper presents a candidate arbitrary-phase spread spectrum modulation technique that offers similar performance to spread continuous phase modulation (CPM) waveforms, yet supports additional capabilities for programming a chosen frequency domain spectra into the resulting spread spectrum signal. The proposed frequency-selective high-order phase shift keying (PSK) signaling (FS-HOPS) waveform is derived from arbitrary-phase sequence-based spread spectrum signals, with multi-bit resolution chaos-based sequences defining incremental phase words, enabling real-time efficient generation of practically non-repeating waveforms. The result of the FS-HOPS formulation is a parameterized hybrid modulation capable of selectively mitigating narrowband interference. Adaptation in this modulation may be easily implemented as a time-varying evolution, increasing the security of the waveform against tone jammers, while retaining many efficiently implementable receiver design characteristics of standard PSK modulations.

3.1 Introduction

Nearly all sequence-based spread spectrum systems are based on the interpretation of a stream of independent and identically distributed (iid) random variables translated to discrete phase words. These phase words are subsequently combined as a time series into a bandlimited spread spectrum signal, traditionally combined with phase-shift keying (PSK)-based data words. In direct sequence spread spectrum (DSSS) modulations, the discrete phase words are typically selected as 2-ary [1] or 4-ary [2]-[3] PSK-based spread modulations, effectively representing a higher rate version of a standard BPSK or QPSK modulation. In chaotic sequence spread spectrum (CSSS) modulations [4]-[6], the discrete phase words may be represented as arbitrary-phase modulations [7]-[8] that are drawn as nearly random points on the unit circle, representable by 2^8-ary up to 2^{16}-ary PSK modulations. The increased order of the representative PSK modulation produces a whiter overall spectral response.[1] Ignoring windowing effects, the spectral content can be approximated as consisting of concentrations of energy represented by the phase difference between each successive iid phase word (instantaneous frequency being approximated as the rate of change of phase within the chosen chip period), which if drawn from a uniform distribution, will also be uniform.

This paper proposes a candidate reinterpretation of the 2^k-ary PRNG output as an iid phase word to instead be an accumulated phase increment whose sum rolls over uniformly on each new PRNG value. By so doing, easy additions may be incorporated to programmably define a spread spectrum output signal that contains tailored/colored frequency responses, which cannot be achieved when phase words are taken as iid entities. In some ways, this aggregation of phase between spreading chips looks like a continuous phase modulation (CPM) structure [9]-[10], and shares both the spectral efficiency and continuous envelope nature of those

[1] In Gaussian-shaped CSSS, additional pseudorandom number generator (PRNG) words may be applied through the Box Muller transformation to create chip-by-chip amplitude variations as well.

signals, yet the number of phase states is taken sufficiently large (2^8-ary up to 2^{16}-ary) that traditional maximum likelihood sequence estimation (MLSE) techniques [11] would quickly become too cumbersome to employ for spread spectrum correlations. The ability to uniquely color the spectrum of the output signal however offers new advantages for optimizing transmission in a non-white or frequency dispersive channel as well as mitigating interference observed in the channel. Further, the ability to parameterize and adapt the selective coloring of the modulated CSSS signals offers a real-time interference suppression technique that improves communication performance while retaining most of the CSSS security advantages.

A foundational framework for the frequency-selective high-order phase shift keying (FS-HOPS) modulation concept is introduced in Section II, including a discussion of methods to increase the adaptability in the PSK-based spreading process. This is followed by an analysis of the FS-HOPS techniques, including extensibility to optimized implementation on different types of hardware platforms in Section III; a proof-of-concept implementation of the FS-HOPS modulator was constructed in Verilog for verification on an Intel Arria 10 SoC FPGA. Future work and conclusions are provided in Section IV.

3.2 Frequency-Selective HOPS Methods

Consider the comparative hardware models shown in Fig. 3.1, representing a traditional sequence-based spread spectrum generation process (DSSS top, CSSS middle) and the modified FS-HOPS model (bottom). In the comparative FS-HOPS path, the multi-bit resolution binary PRNG words first encounter a deterministic, yet programmable, "color" mapping whereby the assumed uniformly distributed PRNG words (values on GF(2^k)) may be surjectively mapped onto any chosen subset of GF(2^k). The simplest such case(s) are (1) that of a bypass/no-operation where the k-bit input/output words of the color mapping are iden-

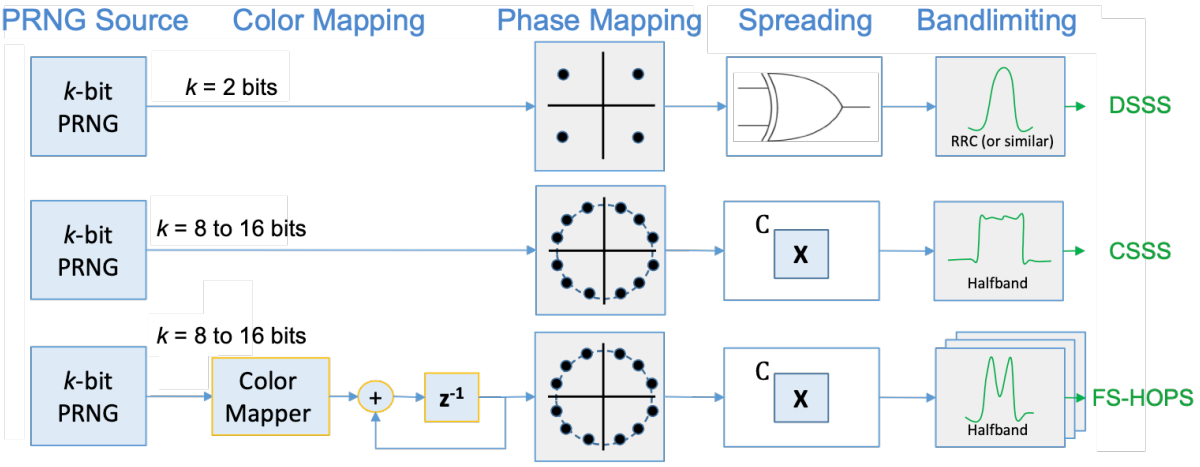


Figure 3.1: Comparative sequence-based spreading mechanisms for DSSS, CSSS, and FS-HOPS modulations.

tical and (2) that of an arbitrary permutation (any bijective mapping) of PRNG values. Both cases maintain the identical statistical distribution as the input, so no change to the power spectral density (PSD) is induced. The accumulator structure following the color mapper does represent an interpretation of the resulting PRNG output as an additive phase increment / instantaneous frequency word, acting much like a variable-input numerically controlled oscillator (NCO). In these scenarios, the bulk signal properties are identical to the multi-bit resolution style CSSS signals.

More interesting scenarios occur when the color mapping is taken as an adaptable array of values representative of a surjective mapping from the input GF(2^k) domain onto a chosen subset of values. A few scenarios for this mapping include (a) uniform definition of the color mapping table to be a single phase value, producing a continuous wave (CW) signal, (b) subdivision of the 2^k memory entries into a discrete number of M allowable phases, establishing a discrete number of phase steps (instantaneous frequency content) that are reflective of a randomized traditional M-ary frequency shift keying (FSK) modulation, (c) non-uniform definition of the color mapping table to uniquely allocate frequency content

into specific bins, (d) a time-varying programmable set of phase values that achieve any of the previously described modes or newly developed ones, (e) an externally or internally driven swap between parallel instantiated phase word tables, and/or (f) a spread bandwidth expansion/contraction selection. For each of these scenarios:

3.2.1 CW Signals

The color mapping function may be configured to act as a straightforward continuous input (at any chosen center frequency) to the accumulator structure, truly acting as a NCO. This function may be used as a pilot tone, a time-adapted CW pulse (an FSK modulation with variability in symbol durations), and/or as a test tone signal for obtaining detailed characterization of the RF output chain.

3.2.2 Blended FSK

By sub-dividing the 2^k allowable phase outputs into a discrete set, an M-ary FSK signaling set may be assumed, where each FSK pulse occurs over a single or defined number of chip durations. As such, an FS-HOPS modulator may be configured for traditional FSK signals, yet still be synchronized to the underlying spreading sequence generator.

3.2.3 Dynamic PSD

Under the assumption of a uniformly distributed input, dividing the 2^k allowable phase outputs over a much larger discrete set in a non-uniform manner, allows discrete control of the (unfiltered) power spectral density of the resulting spectrum. Filtering of these interleaved FSK "chips" will distort the spectrum in a manner that limits the nulls in unselected bins,

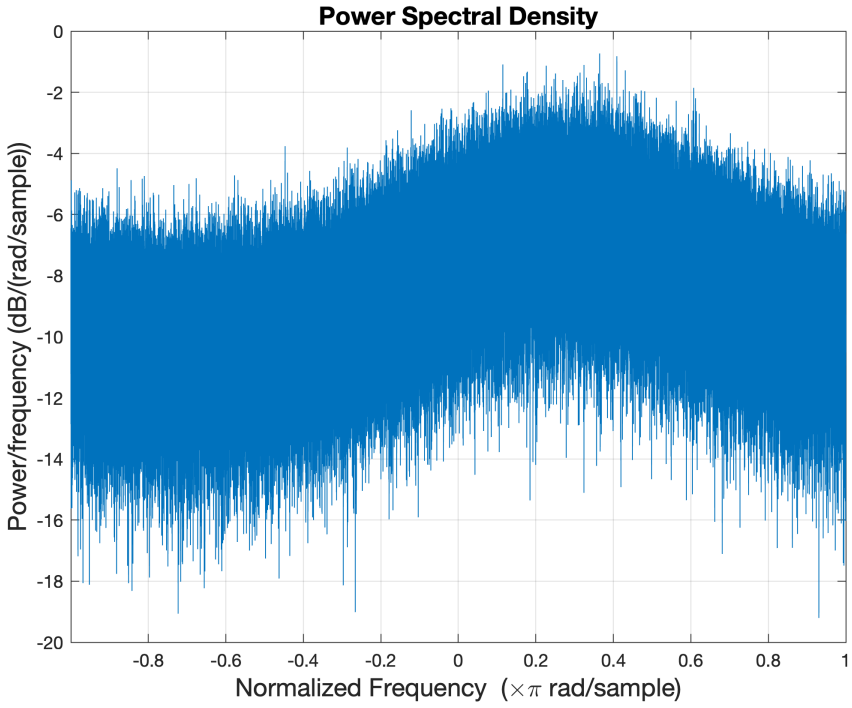


Figure 3.2: Example of dynamic PSD spreading mode.

but does enable coarse shaping of the signal spectrum in a way to avoid interferers and/or equalize the spread signal in a frequency dispersive propagation environment.

An example of this dynamic PSD mode was constructed in Matlab (Fig. 3.2) to emulate the spectral effects of accentuating one side of a baseband signal's instantaneous bandwidth. More extreme shaping may also be performed, although the core assumption of "shaping" is that the total power is conserved, so accentuating half a band by 3 dB represents a null in the other half of the band. The traditional correlation process of despreading remains identical, leading to no additional losses. Note that the signal spectrum estimate shown in Fig. 3.2 represents the spectrum of a maximal entropy (one complex sample per chip) signal, so no band limiting/interpolation filter has been applied except the inherent windowing of the periodogram.

3.2.4 Programmable Color Maps

By enabling the color mapping to be a time-varying vector of phase words, (a) a CW signal may be converted to a short duration arbitrary phase chirp signal, (b) the static FSK symbol set of center frequencies may be re-defined, and/or (c) the chosen frequency spectra of a dynamic PSD model may be changed to meet observed changes in propagation or interferers.[2] This programmable characteristic may be updated periodically, based on an external pseudorandom process, and/or on a burst-by-burst basis, offering additional waveform dynamics. The most common anticipated use for the adaptation is coupling with an RF interference (RFI) measurement/scanning receiver that permits re-shaping of the signal in addition to changing channels as part of a dynamic spectrum access algorithm.

3.2.5 Selectable Color Maps

The final suggested bandwidth preserving mechanism is to actually employ multiple color mapping tables and to then select between them based on some portion of the k-bit PRNG output, an externally provided control signal (periodic or non-periodic), or an externally provided PRNG source. Selection between these color mapping tables may also be data dependent, allowing integration of FS-HOPS spreading mechanisms with carrier shift keying (CSK) modulations [12], yet appropriate synchronization schemes must be integrated.

In all cases so far, the waveforms retain the constant envelope characteristic, making them power efficient from a transmission perspective, and the arbitrary phase behavior that lends security from an unintended recipient (on par with the quality of the k-bit PRNG). Correlation processing using a coherent replica of the signal inside the receiver remains a robust

[2] If desired, the color mapping table may actually be swapped to occur after the accumulator structure, enabling better timing / code synchronization between two end points, since the intervals over which the phase words accumulate must be perfectly aligned at the transmitter and receiver.

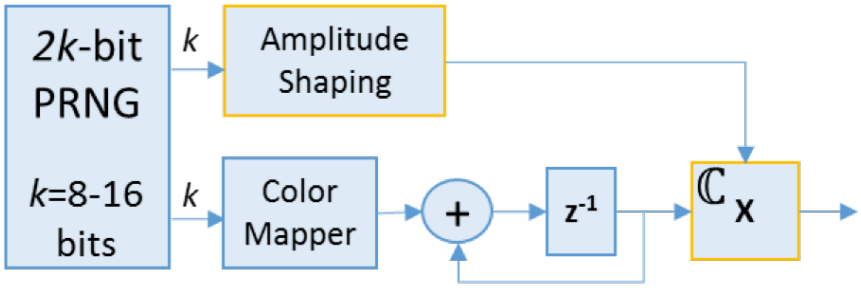


Figure 3.3: Modified FS-HOPS model with amplitude shaping.

option on par with traditional correlation techniques applied to sequence-based spread spectrum. Further, chip energy amplitude shaping, such as used with Gaussian-shaped digital CSSS signals [13] may also be optionally applied in order to increase the security of the signal, while retaining a chosen colored spectrum. A modified view incorporating this amplitude mapping is shown in Fig. 3.3.

3.2.6 Spreading Bandwidth Expansion and Contraction

The final FS-HOPS method focuses on variable-bandwidth controls applied to the overall spreading sequence. By incorporating a gain term ($\delta \leq 1$) after the color mapper (or equivalently within the color mapping values), the instantaneous bandwidth of the signal may be constrained to $\delta\%$ of the overall bandwidth; i.e. each successive incremental phase word will use a non-complete portion of the overall available spectrum when viewed at the chip rate. By making this δ term an externally controlled parameter as shown in Fig. 3.4, the bandwidth may be varied on a symbol-by-symbol basis (total energy per symbol is conserved), enabling yet another free parameter for encoding data into the spread signal. A second use of the gain word is to periodically slew the bandwidth of a spread spectrum communications signal, reducing its signature under rate line detection techniques. Choosing a value of $\delta > 1$ results in potential aliasing of the phase increments (rollover within the

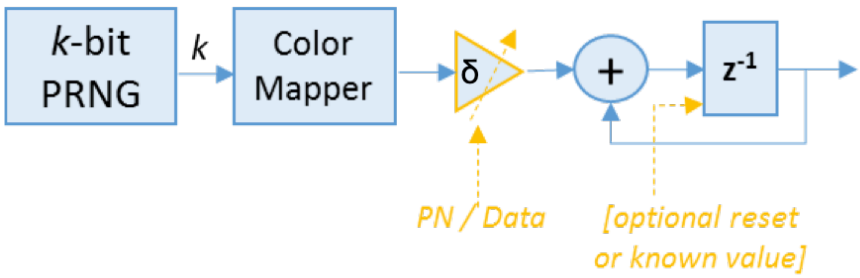
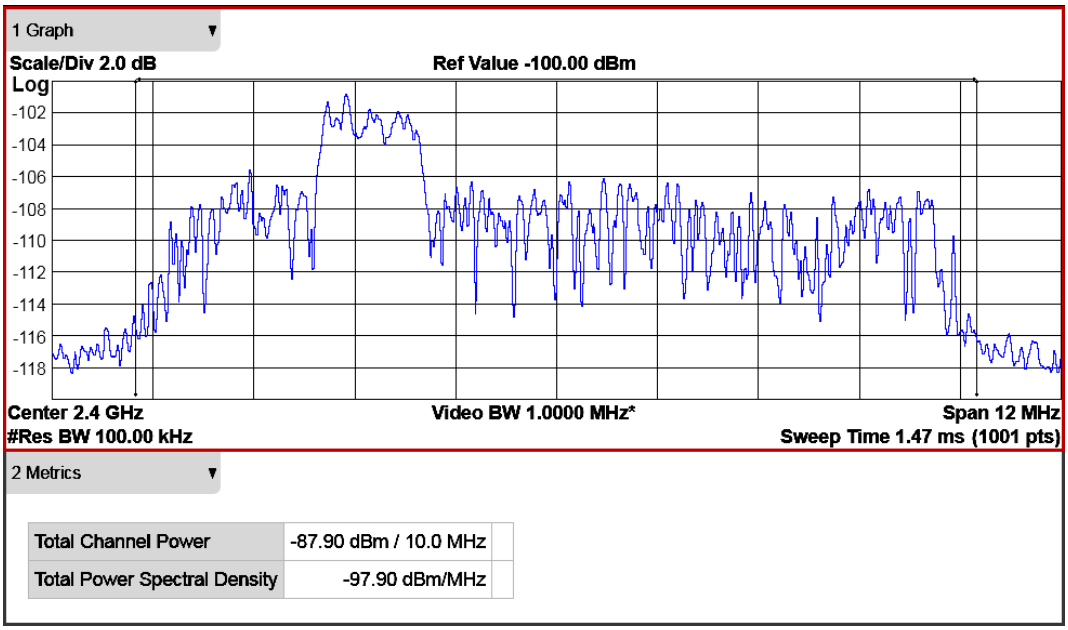


Figure 3.4: Time-varying signal bandwidth expansion and contraction in spread spectrum systems.

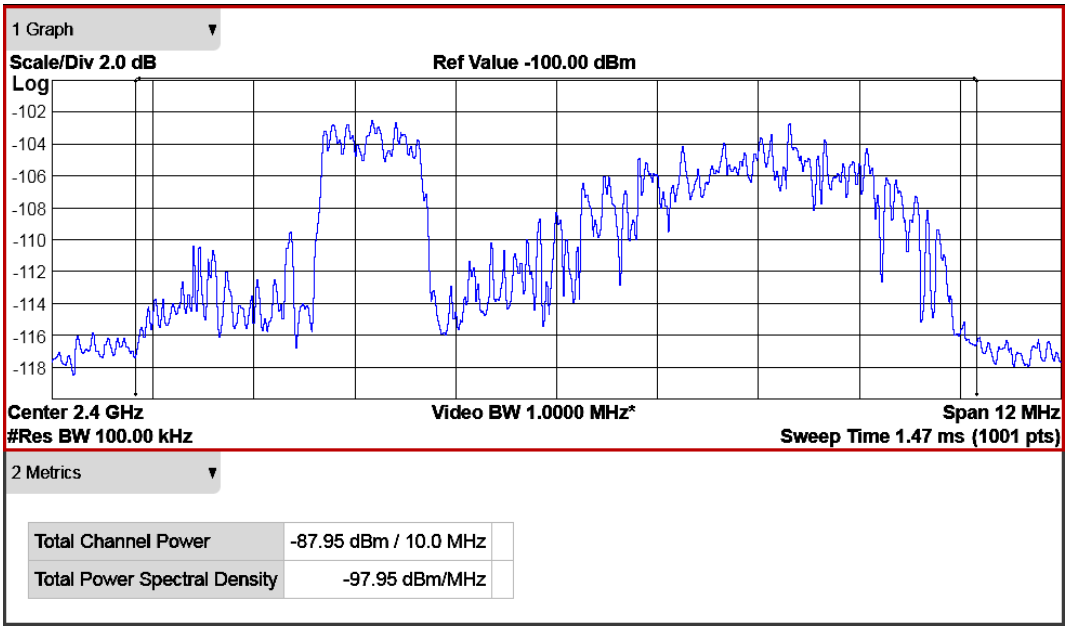
accumulator), and equivalently an aliasing of the spectrum, yet may also be used.

The resulting waveform will remain constant envelope and present similar computational challenges for reception as a CPM signal. Most notably, the phase of the resulting signal accumulates through the duration of a symbol, allowing the option for an accumulator reset (to a known, optionally PN-driven, phase value) between symbols to eliminate most of the CPM-required MLSE processing [14]. With the arbitrary phase nature of the resulting signals, time-domain cross-correlations between signals of different scaled bandwidths will quickly devolve into phase incoherent entities (amplitude scaling will remain coherent if employed) giving solid orthogonality, even though they can start on symbol boundaries at similar values.

One final note on the use of these FS-HOPS variants is that the chosen instantaneous frequency components will naturally blur when passed through an interpolation and/or band limiting filter. As such, the programmability of the frequency spectra observed at a symbol level, or any other long-term observation, will be inherently limited in its variation. Additional work to make these transitions tighter would likely require different types of band limiting filters.



(a) Standard frequency spectrum.



(b) Colored frequency spectrum.

Figure 3.5: Comparitive frequency spectrum for dynamic PSD mode FS-HOPS and the standard spread spectrum modulation.

3.3 Hardware Implementation Trades

The primary deviation from a traditional sequence-based spread spectrum communication system in the FS-HOPS modulation is the color mapping circuit and phase word integrator highlighted in yellow in Fig. 3.1. For relatively small values of k, implementing the color mapping in a simple lookup table (LUT) offers negligible increases in computational resources for most modern devices ($k < 12$). For larger values of k, a structure of smaller LUTs conditioned upon MSBs of the input phase is likely the better approach; given the inherent smoothing effect of the subsequent channel filter and the RF output chain, granular frequency controls are less impactful. Stated differently, the practical value of exceeding $k = 12$ bits for phase word precision is offset by the band limiting effects that will occur during the transmission of the signal, and the extra precision in phase words provides negligible benefits in deterring observation.

The precision of the color mapper output is a flexible parameter, preferably chosen with a dynamic range that exceeds resolution provided by k. In modes (a)-(e) of section II, the resolution of the phase word value, and the resulting size of the accumulator, may be comparable without any loss of performance. The final case (f) of an optional gain term requires consideration of the level of precision desired in the PN / Data driven scaling. Provided the transmitter and receiver use the identical bit width, the signals will remain coherent, making the extra precision have a minimal impact. Further, choosing a higher output phase word precision has practically no impact on overall system resources.

To validate the FS-HOPS modulation model, the dynamic PSD mode (c) was implemented in Verilog (parallel to the standard burst-mode HOPS [7] spread spectrum modulator) for deployment on an Intel Arria 10 SoC FPGA. Using $k = 8$, the color mapping LUT was configured identically as in the Matlab simulation of Fig. 3.2, by uniformly mapping the set

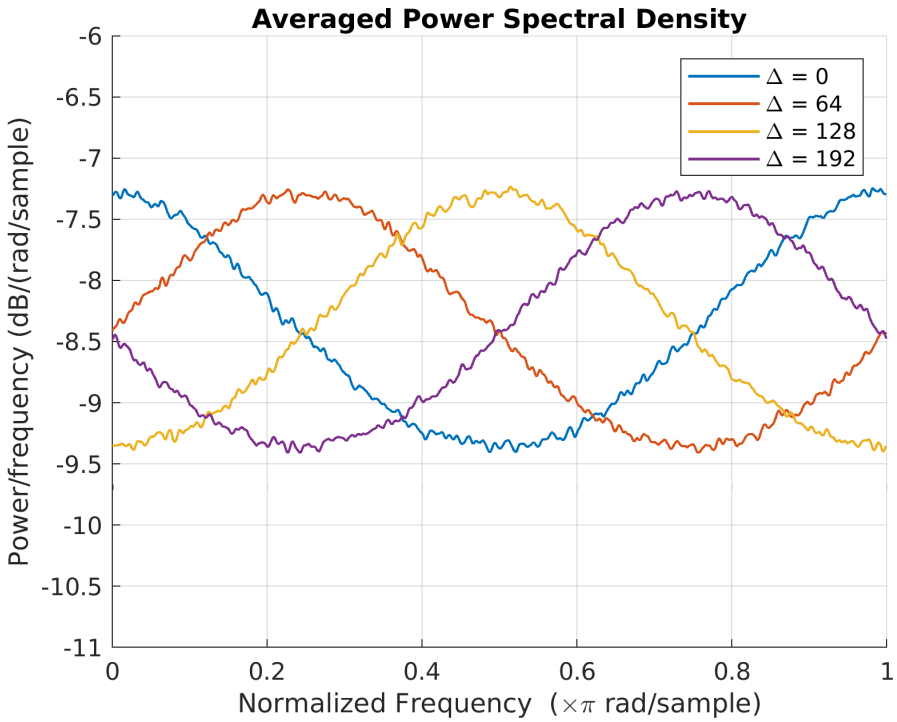


Figure 3.6: Frequency domain rotation of the resulting PSD by color mapping entry additions on GF(2^8).

of inputs $[193, 256]$ to equally spaced output values ≤ 192, followed by a left circular shift of the memory by 32 words.[3] Note that additions to the memory entries on GF(2^k) serves to rotate the output frequency spectra, as shown in Fig. 3.6. Relative to the resources available in the FPGA, the added logic is negligible (one 256-entry LUT and an 8-bit sum).

A real-time spectrum analyzer observation is shown in Fig. 3.5 at high signal-to-noise ratio (SNR) for comparison of the colored frequency response to that of the standard sequence-based spread spectrum modulation, pictured with a narrowband interfering signal in the lower sideband. As expected, subsequent transmitter processing of the spread signal negates some of the spectral coloring, although an approximated upper sideband power level increase of 3 dB is on par with the prediction in Fig.3.2. In further verification tests, the interference

[3]Circular shifts of the LUT words also shifts the output frequency spectra. This very simplistic permutation of the color maps rapid frequency selection of any envelope "shape."

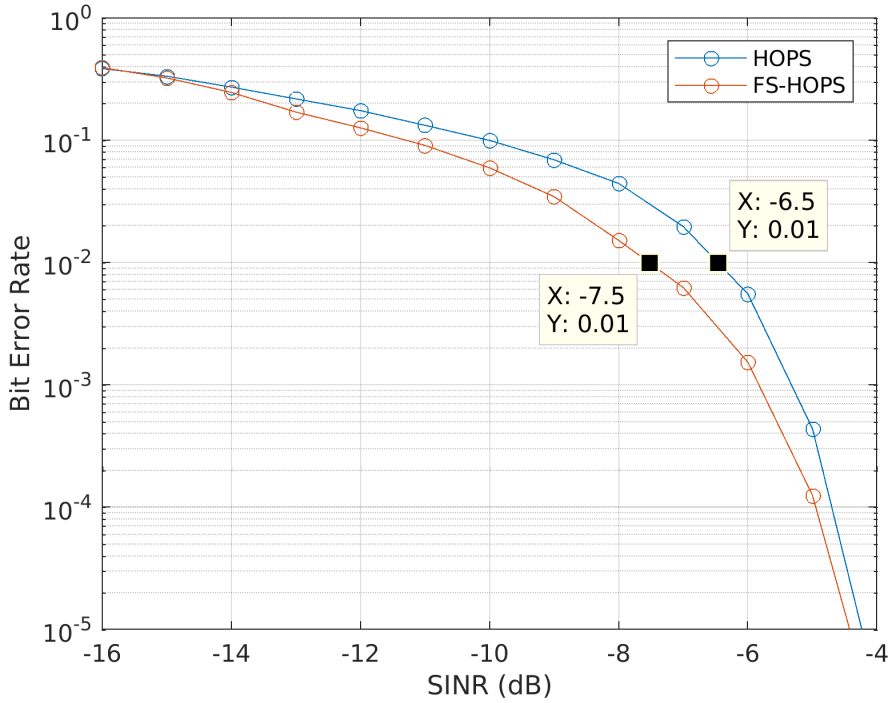


Figure 3.7: BER performance measurements as a function of SINR for HOPS and FS-HOPS.

avoidance use case is emulated by generating the interfering signal as shown in Fig. 3.5 for bit error rate (BER) performance measurements. These results are provided in Fig. 3.7 in terms of the signal-to-interference-plus-noise ratio (SINR), showing measured BER performance improvement of around 1 dB.

3.4 Conclusion

This paper presented a novel adaptation of an arbitrary-phase spread spectrum waveform that is configured to support a variety of frequency-selective spread modulations, incorporate optional amplitude shaping, and optionally enable spreading bandwidth expansion and contraction. Each of these methods is exceedingly hardware efficient, making them practical additions to virtually any sequence-based spread spectrum communication system. More-

over, the proposed modulation retains the constant envelope behavior of CPM signals, yet the approach is computationally efficient for receiver processing, resembling much more the standard despreader correlation processing of a carrier shift keyed or traditional sequence-based spread spectrum signal. Hardware prototyping results show improved performance of spectrum shaping modes than the standard modulation, assuming sensed narrowband interference in the channel.

References

[1] Global Positioning Systems (GPS) Directorate, Interface Specification IS-GPS-200, Rev. H, 24 Sep 2013.

[2] D. N. Knisely, S. Kumar, S. Laha and S. Nanda, Evolution of wireless data services: IS-95 to cdma2000, in IEEE Communications Magazine, vol. 36, no. 10, pp. 140-149, Oct 1998.

[3] M. B. Pursley, T. C. Royster and M. Y. Tan, High-rate direct-sequence spread spectrum, IEEE Military Communications Conference, 2003. MILCOM 2003, pp. 1101-1106 Vol.2.

[4] G. Heidari-Bateni and C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, in IEEE Transactions on Communications, vol. 42, no. 234, pp. 1524-1527, Feb/Mar/Apr 1994.

[5] A. J. Michaels and D. B. Chester, Efficient and flexible chaotic communication waveform family, MILCOM 2010, San Jose, CA, 2010, pp. 1250-1255.

[6] J. Yu, H. Li, Y. D. Yao and N. J. Vallestero, LPI and BER Performance of a Chaotic CDMA System, IEEE Vehicular Technology Conference, Montreal, Que., 2006, pp. 1-5.

[7] A. J. Michaels, High-Order PSK Signaling (HOPS) Techniques for Low-Power Spread Spectrum Communications, 2018 IEEE 19th International Symposium on A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Chania, 2018, pp. 01-07.

[8] G. Kaddoum and F. Gagnon, Design of a High-Data-Rate Differential Chaos-Shift Keying System, in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 59, no. 7, pp. 448-452, July 2012.

[9] T. Aulin and C. Sundberg, Continuous Phase Modulation - Part I: Full Response Signaling, in IEEE Transactions on Communications, vol. 29, no. 3, pp. 196-209, March 1981.

[10] B. E. Rimoldi, A decomposition approach to CPM, in IEEE Transactions on Information Theory, vol. 34, no. 2, pp. 260-270, Mar 1988.

[11] W. Zhai, Z. Li, J. Si and J. Bai, Performance analysis of a joint estimator for timing, frequency, and phase with continuous-phase modulation, in IET Communications, vol. 10, no. 3, pp. 263-271, 2 11 2016.

[12] A. J. Michaels and C. Lau, Generalized Multi-carrier Chaotic Shift Keying, 2014 IEEE Military Communications Conference, Baltimore, MD, 2014, pp. 657-662.

[13] G. Box and M. Muller, A note on the generation of random normal deviates, Princeton University, pp. 610–611, Jan 1958.

[14] L. Yiin and G. L. Stuber, MLSE and soft-output equalization for trellis-coded continuous phase modulation, Proceedings of ICC/SUPERCOMM '96 - International Conference on Communications, Dallas, TX, 1996, pp. 1005-1009 vol.2.

Chapter 4

Co-Channel Underlay-Based Watermark Authentication

Abstract

The time-aligned injection of a co-channel underlay-based watermark for authentication at the receiver is an effective method to enhance physical layer security. While firewalls have traditionally been used to manage authorized traffic in wired networks, this paper provides the design and implementation of similar functions for wireless networks. The physical layer firewall only allows receiver access in cases where the valid watermark is detected concurrent to the incoming primary signal, and may be used with virtually any network waveform. Moreover, the use of non-repeating arbitrary-phase spread spectrum signals eliminates many common replay attacks. A hardware prototype is built to receive IEEE 802.11g primary signals with arbitrary-phase spread spectrum underlays, showing reliable authentication performance with only minor bit error rate degradation up to Modulation and Coding Scheme (MCS) 5. Future prototypes are suggested to further optimize performance, for use with other data waveforms, and to demonstrate higher layer protocols.

4.1 Introduction

A multi-layered security approach is a valid method to improve a system's resilience to outside threats and maintain data integrity. In communication systems with data links that traverse public/unsecured networks, such as those based on the Internet Protocol (IP) suite, security mechanisms tend to be present at each layer in the model [1], with methods for data encryption, authentication codes, anti-replay counters, encapsulation, and access control [2]-[3]. Radio frequency (RF) communications however are more easily intercepted and/or exploited, leading to threats of rogue base stations [4], cloned mobile personal devices [5], and medium access control (MAC) address spoofing [6] in wireless networks.

Nearly all of the widely-adopted wireless technologies, including ZigBee [7], IEEE 802.11 [8], and 4G LTE [9], focus on MAC layer security features using similar methods to those in wired networks. The threats noted above can be mitigated by increasing the physical layer (PHY) security of the receiver, implementing any technique that helps authenticate the origin of incoming signals. Waveforms designed for greater transmission security (TRANSEC) are fundamentally more PHY layer secure, usually requiring *a priori* knowledge of some pseudo-noise (PN) code generation process, as is the case with the spread spectrum waveforms derived from non-repeating digital chaotic sequences [11]-[12]. Yet, receiver processing of those signals is typically too computationally intense for low-power devices in the Internet of Things (IoT), while allowable data rates are generally too low for high-throughput applications.

This paper provides a hardware proof-of-concept implementation of a PHY layer firewall using the co-channel underlay-based approach proposed in [13]. Traditionally, firewalls have been used at the network layer for access control/user authorization in wired networks [3], and the opportunity to inject a co-channel RF underlay-based watermarking signal (water-

mark) is a strong method to enhance authentication in virtually any wireless network. Other techniques have been proposed to provide similar functionality, including methods for coherently distorted signals [4] and methods to extract unique PHY characteristics [10]. These approaches do work well for specific use cases, however, networks containing mobile users and/or a large number of edge nodes may choose to implement the information additive methods in [13].

While the concept of underlay signals has been presented before [14], the co-channel signal framework of this paper is less obvious to the unintended receiver, prioritizing a low probability of interference/detection (LPI/LPD) signal. Further, while the conjoined signal is fully compatible with legacy networks that do not perform watermark validation on the received signal, the PHY layer firewall is an added defense to the existing MAC layer (and higher layer) security mechanisms of a system. The IEEE 802.11g [8] design example in this paper is built by extending the primary signal PHY for use with a time-evolving watermark, without modification.

The remaining sections are organized as follows. The co-channel underlay framework is presented in Section II, deriving specific timing, power, and bandwidth constraints from the primary signal specification, the core processing architecture, and potential firewall configurations. Section III provides the functional description of a PHY layer firewall with further higher layer design considerations. For hardware performance results, Section IV presents the measured probability of authentication (P_A) and bit error rate (BER) degradation for the hardware prototype that employs co-channel 802.11g primary signals. Conclusions are provided in Section V.

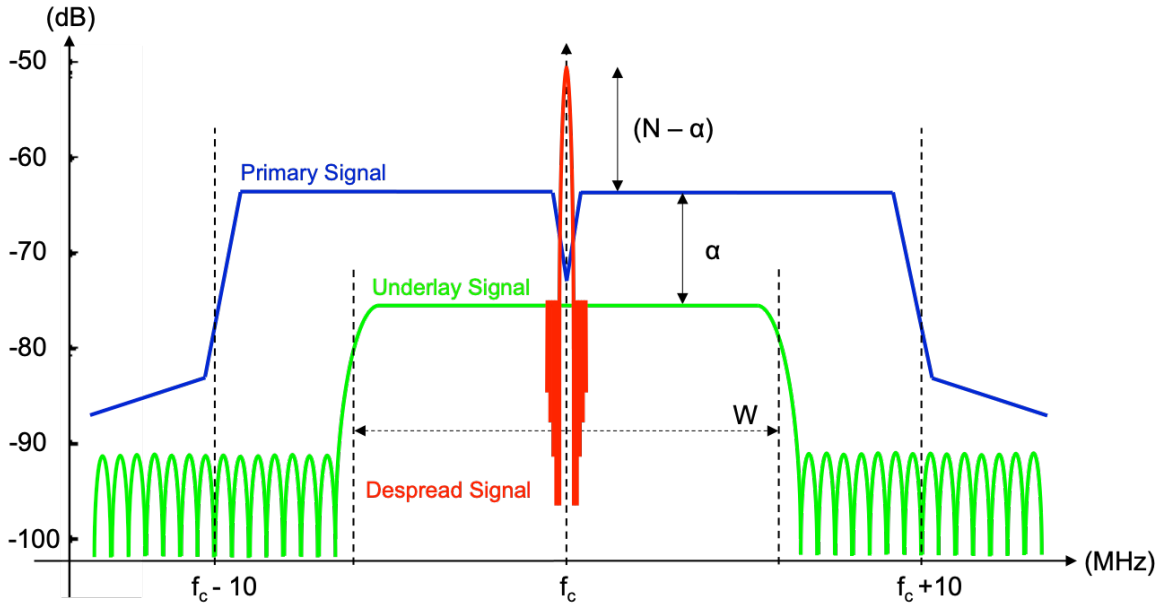


Figure 4.1: Co-channel frequency-domain depiction of 802.11g/HOPS, overlaid with the despread watermark, and centered at f_c.

4.2 Implementation

The best choice of underlay signal is any noise-like or arbitrary-phase spread spectrum modulation, regardless of network waveform used in the primary data link, since the relatively low required signal-to-noise ratio (SNR) operating points of those signals minimize co-channel interference. For example, the hardware prototype employs 802.11g primary signals with high-order phase shift keying (PSK) signaling (HOPS) waveform underlays [11]. Given an underlay signal that only needs to provide its presence at the receiver, the watermark itself may consist entirely of preamble chips, and detection is sufficient to provide authentication.

Consider the frequency-domain depiction of co-channel 802.11g/HOPS in Fig. 4.1, where the underlay has bandwidth W, spreading gain N, and signal power spectral density (PSD) backoff α. Increasing W and N will trade improved authentication performance for primary signal degradation, while lowering these values reduces any BER degradation for degraded

authentication. The backoff α may be adjusted dynamically based on the desired signal-to-interference plus noise ratio (SINR) operating point. Since the 802.11g occupied bandwidth is 16.6 MHz, although the channel bandwidth is 20 MHz, the LPI/LPD watermark is constrained to $W \leq 16.6$ MHz. Co-channel interference of the primary signal makes it more difficult for an eavesdropper to (at least partially) reconstruct the watermark without first knowing the transmitted data.

Each HOPS underlay spreading chip $x = (a + jb)$ of the hardware prototype is taken from arbitrary points on the unit circle, so N is also the length of the watermarking sequence $\{x_n\}$. This watermark is time-aligned to the primary signal samples prior to transmission, as shown in Fig. 4.2. It is clear to see why $t_1 > t_0$ must be held for x_0, however the 802.11g data payload sample length may vary from burst to burst. Note that the primary signal sample length is known by the transmitting PHY, and the potentially higher rate modulated data payload is less-resilient to co-channel interference than the binary PSK (BPSK) modulated preamble/header, so longer watermarks may not be preferable at the receiver.

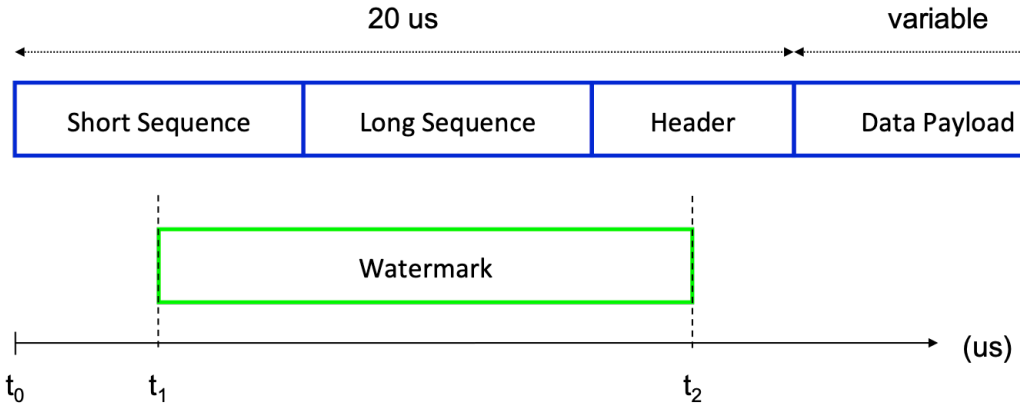


Figure 4.2: Co-channel time-domain depiction of 802.11g/HOPS.

To construct time-evolving or receiver-assigned watermarks, the transmitter must synchronize its pseudorandom number generator (PRNG) used to produce sequence-based spread spectrum underlays to the spreading code of the receiver. This is relatively straightforward

with PRNG methods based on residue number system (RNS) arithmetic [18], and involves selecting the appropriate residue value inputs (keys). As shown in the block diagrams of Fig. 4.3 and Fig. 4.5, the selected keys correspond to a residue vector that is input to the PRNG, giving an N-length sequence of chip phases $\{\theta_n\}$ uniformly taken from an arbitrary distribution of allowable phase words. Each of $\theta_i \in \{\theta_n\}$ is mapped[1] to the relevant spreading chip $x_i \in \{x_n\}$ of the watermark.

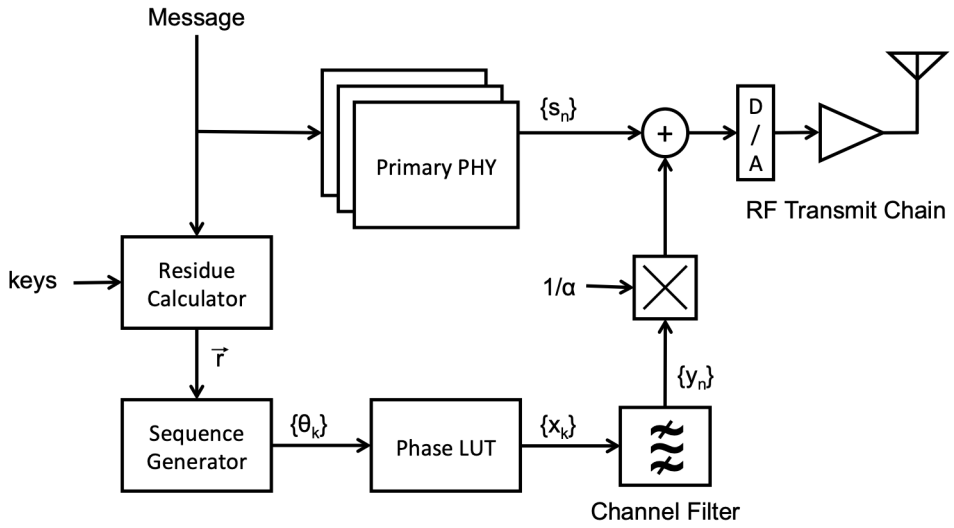
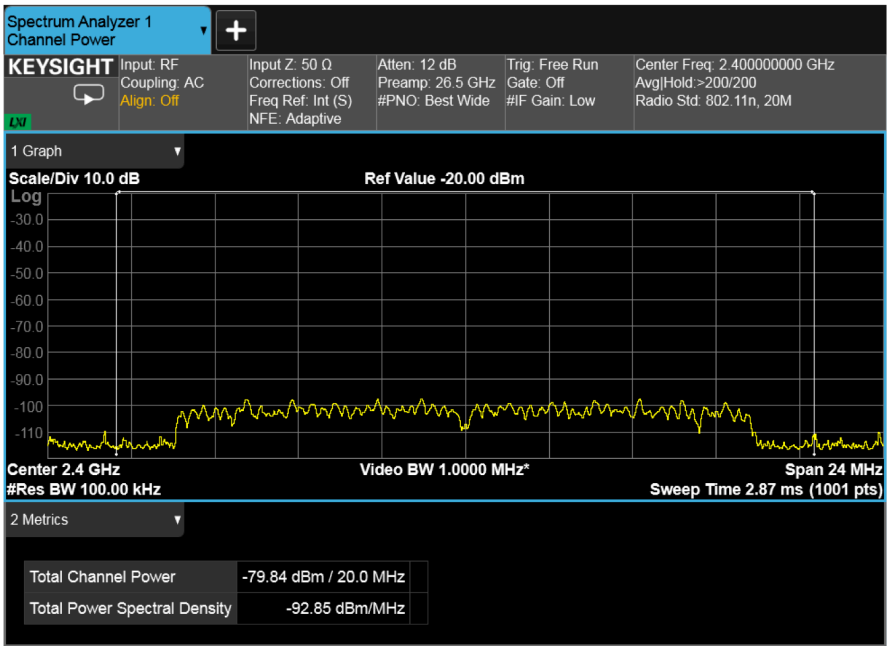


Figure 4.3: Block diagram for the transmitter PHY.

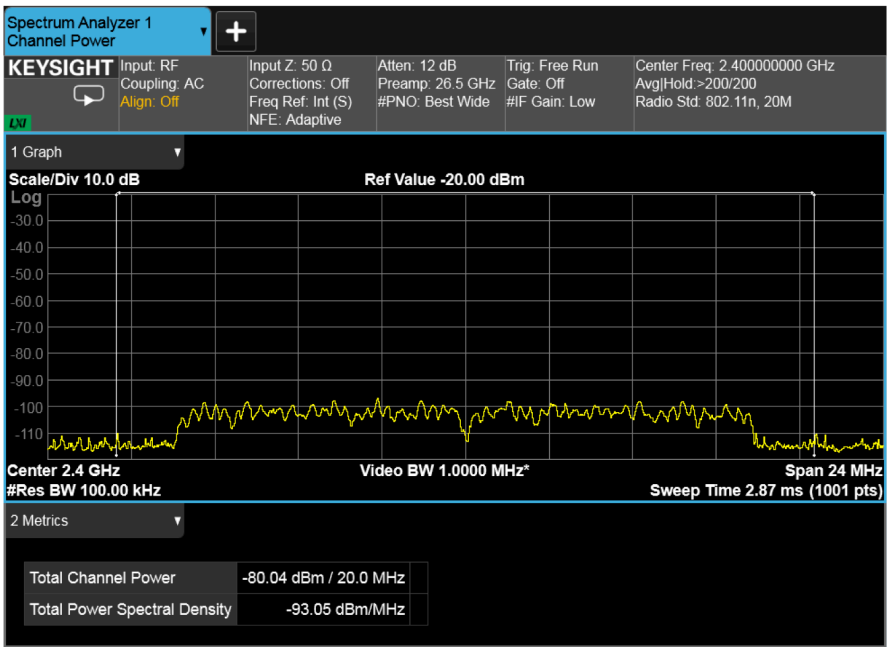
The transmitter block diagram in Fig. 4.3 follows the core technique described in [13], requiring no modifications to the primary signal PHY. However, since the watermark is internally generated at the chipping rate (R), if R is less than the baseband sampling rate (f_s), then an interpolating channel filter is inserted prior to the time-aligned addition with the primary signal. Choosing to attenuate the watermark by α prior to interpolation is also acceptable. The transmit spectrum for bursts with/without the underlay is shown in Fig. 4.4 with $\alpha = 12$ dB, resulting in a slight channel power increase.

At the receiver, if the incoming signal samples form a data frame, authentication is successful

[1]Efficiently implemented as a look-up table that computes $x = e^{j\theta}$ for all 2^8 possible values of θ.



(a) With underlay.



(b) Without underlay.

Figure 4.4: Burst transmission spectrum comparison with α12 dB.

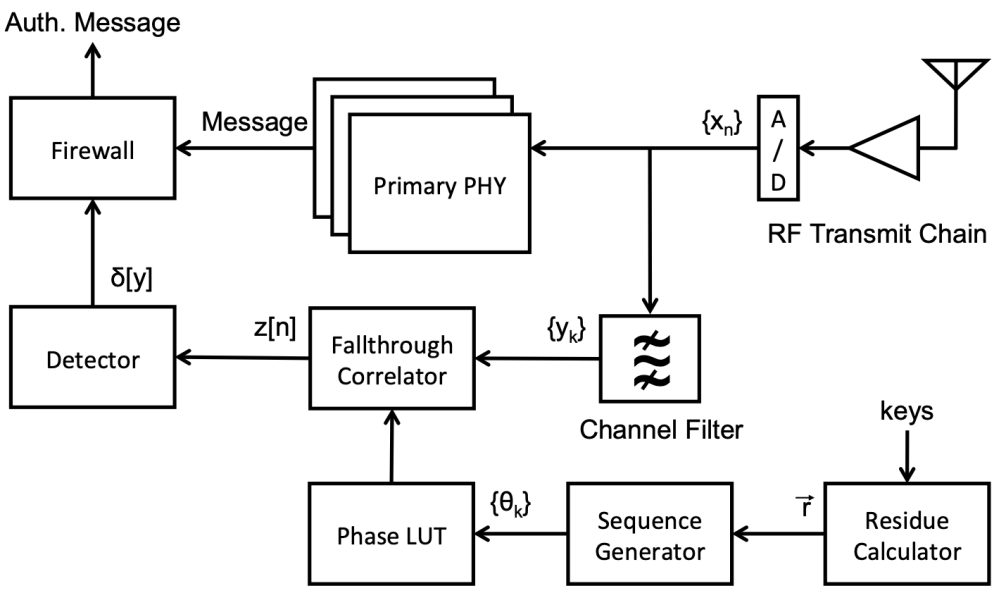


Figure 4.5: Block diagram for the receiver PHY.

if watermark detection occurs concurrent to the received frame (see Fig. 4.2). Therefore, as shown in Fig. 4.5, extending the traditional PHY with underlay signal detection logic sufficiently implements the watermark validation functions. Designs with $R < f_s$ should bandpass filter the received signal to lessen out-of-band noise/co-channel interference, and optionally decimate the incoming samples for reduced receiver complexity.

4.3 Firewall Configurations

Assuming $\{y_n\}$ is a valid received watermark for the internally generated watermark $\{x_n\}$, the ideal correlator output signal $z[n]$ will have magnitude N for the arbitrary-phase HOPS waveform. Decisions to authenticate the incoming signal use the sufficient statistic $Z = |z[n]|$ and a detection threshold τ set relative to the expected primary signal plus noise power. The computation in (1) is performed each time a received chip is clocked into the delay line, requiring a fully pipeline accumulation of partial sum terms.

$$Z = \left| \sum_{i=0}^{n} x_i y_i^* \right| \tag{4.1}$$

The known latency of (4.1) gives a timestamp relative to the received signal delay line for each authentication decision δ. That is, if $\delta[y] = 1$, then $\{y_n\}$ is decidedly valid, and the incoming primary signal is authentic in origin, where

$$\delta[y] = \begin{cases} 1 & \text{if } Z \geq \tau \\ 0 & \text{if } Z < \tau \end{cases} \tag{4.2}$$

Ignoring the potential for false positives, detection of the watermark can be used to optimize τ for future authentication decisions in (4.2). The correlation length N is used to divide Z to provide the underlay signal power estimate, while values of $|z(n)|$ at instances before/after detection (plus 10-20 received chips to account for filtering) can be used to estimate co-channel interference plus noise power.

The hardware prototype PHY layer firewall performs hard authentication decisions of the incoming signal: if the watermark is detected reasonably relative to 802.11g frame processing, the message is accepted; otherwise, the message is rejected. This is an effective means for wireless access control, even in the presence of MAC address spoofing [6], since it is difficult for an adversary to forge the valid time-varying watermark. While it may be possible to perform successive interference cancellation and recover some/all of the transmitted watermark, choosing to evolve the spreading codes at a sufficient time interval (i.e., once per second or millisecond) means that the adversary will need to successfully recover the valid watermark each time it changes and rapidly exploit that data.

In a practical system, it may be beneficial to flag any unauthenticated messages as not

trusted, and allow them further processing. These situations lead to the realization of higher level protocols for flagged messages, including to (a) request the message be resent for authentication, (b) process as normal if the message is not requesting unauthorized privileges, (c) obtain trust/integrity through other means, such as digital signatures or authentication codes, or (d) only require periodic watermarks, as part of challenge-request, or for certain message sequence numbers. In all provided cases, messages can simply be appended an authentication flag prior to being passed up to the MAC layer. With (a), the MAC layer may attempt re-delivery 2-3 times before ending that data link to a given node, or choose to accept the message, but specifically challenge the node as in (d). If certain links or information is privileged, (b) can effectively allow authorized users that access, while continuing all other network operations. The layering of multiple varied security features comes into play with (c), and is a viable option for watermark usage to supplement existing security.

4.4 Hardware Prototype Validation

The hardware prototype was built on an Altera Arria 10 SoC FPGA for reception of co-channel 802.11g/HOPS, with an 802.11g PHY implemented in software using liquid-wlan [19] and supplied by a circular buffer of received signal samples (I and Q) from the FPGA. Each authentication pulse from the underlay signal correlator prompts the buffer to be read by software into local memory for demodulation and subsequent decoding. The HOPS underlay consists of 1400 preamble spreading chips that are 2× upsampled and bandpass interpolated, occupying 10 MHz of the 20 MHz shared channel.

Since the underlay spreading gain is more than 31 dB and considering the SNR operating region(s) of 802.11g, selecting $\alpha = \{12, 15, 18\}$ dB for the hardware performance measurements in this section is a reasonable choice. To ensure accuracy in results, the detection

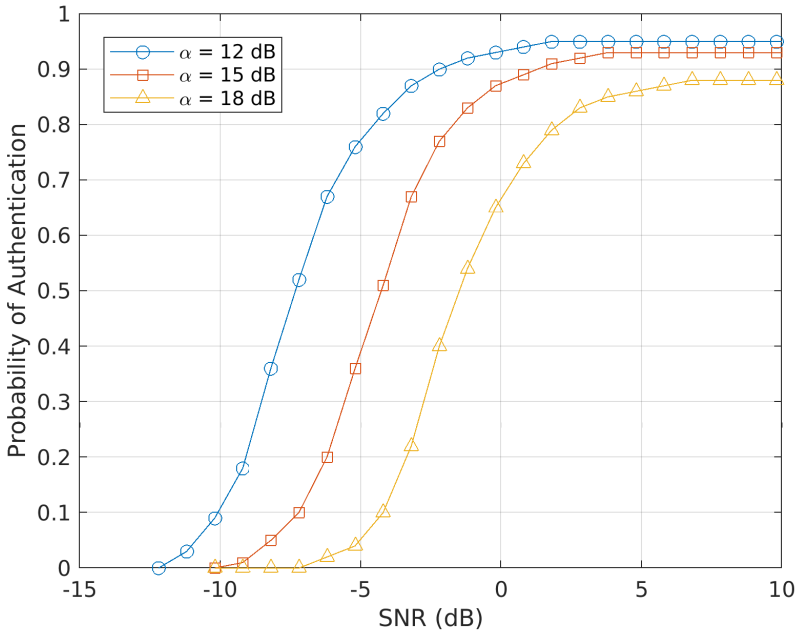


Figure 4.6: Measured authentication performance results in terms of primary signal SNR for co-channel 802.11g/HOPS, using $\alpha = \{12, 15, 18\}$ dB and $P_{\text{FA}} \leq 1\%$.

threshold was set prior for each test run such that the probability of false accept (P_{FA}) was less than 1%. The measured P_{A} is shown in terms of primary signal SNR in Fig. 4.6. As expected, $\alpha = 12$ dB offers greater authentication performance than the other α in Fig. 4.6; however, all of the test cases demonstrate effective performance for an 802.11g SNR greater than 0 dB. For $\alpha = 18$ dB, the measured results converge to $P_{\text{A}} = 0.88$ and, allowing the constraint on P_{FA} to increase to 5-10%, is suitable for most applications.

It is equally important to measure possible degradations to the primary signal. Given the

Table 4.1: Overview of MCS modes under test.

MCS	Data Rate	Sync/Header Mod.	Payload Mod.	Code Rate
3	18 Mbps	BPSK	QPSK	3/4
4	24 Mbps	BPSK	16-QAM	1/2
5	36 Mbps	BPSK	16-QAM	3/4

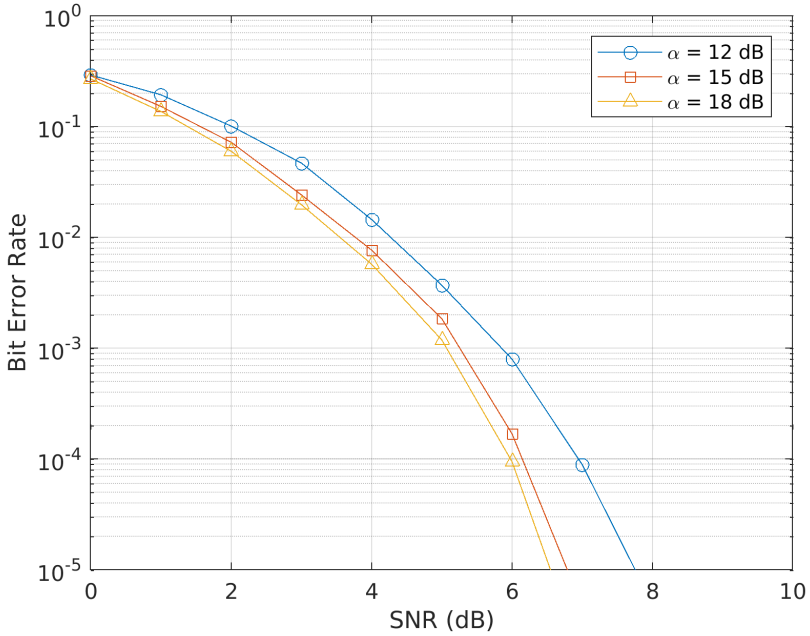


Figure 4.7: Measured BER for co-channel 802.11g/HOPS $\alpha = \{12, 15, 18\}$ dB and MCS 3.

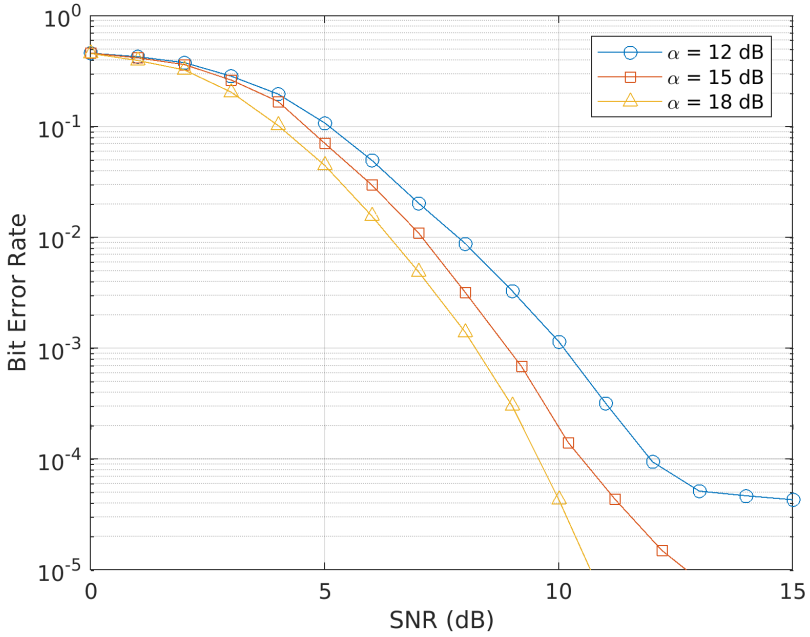


Figure 4.8: Measured BER for co-channel 802.11g/HOPS $\alpha = \{12, 15, 18\}$ dB and MCS 4.

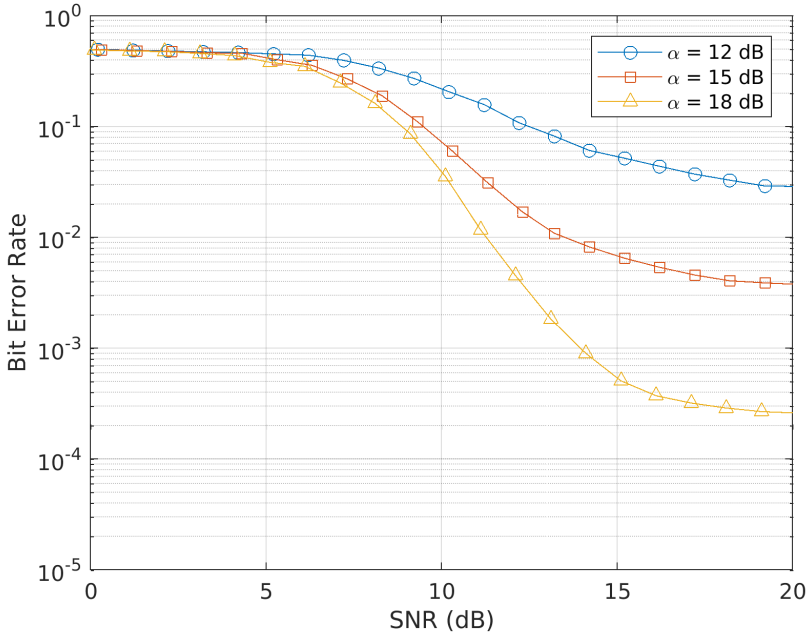


Figure 4.9: Measured BER for co-channel 802.11g/HOPS $\alpha = \{12, 15, 18\}$ dB and MCS 5.

various modulation and coding schemes (MCS) of 802.11g, measured results for a selection of MCS indexes were prepared using $\alpha = \{12, 15, 18\}$ dB, including MCS 3, MCS 4, and MCS 5 (18, 24, and 36 Mbps, respectively). The measured BER curves with MCS 3 are shown in Fig. 4.7 as a function of primary signal SNR. Performance in this case is almost ideal, especially using $\alpha = \{15, 18\}$ dB, and using $\alpha = 12$ dB still allows for minimal error rates with only very slight degradation at all SNR. The BER measurements with MCS 4 in Fig. 4.8 show that $\alpha = 18$ dB gives almost the ideal performance. As α increases, the BER curve noticeably begins to flare out (see $\alpha = 15$ dB), and using $\alpha = 12$ dB at SNR > 12 dB the BER only marginally improves beyond 10^{-4}. Finally, each curve for α is shown to flare with MCS 5 in Fig. 4.9. This mode exceeds the achievable primary signal data rate of co-channel 802.11g/HOPS for the transmitted watermark that consists of 1400 transmitted chips constrained to $P_{\text{FA}} \leq 1\%$. A relaxed constraint would allow for shorter length watermarks or reductions to the underlay PSD, and therefore improved BER

performance.

4.5 Conclusion

This paper demonstrates the PHY-layer injection of co-channel underlay-based watermarks [13] to be a reliable method of authenticating transmissions in a wireless network. The technique allows for PHY-layer firewall functions resembling access control/packet filtering in traditional Ethernet-based firewalls. Implemented for co-channel reception of 802.11g data signals and the arbitrary-phase HOPS spread spectrum underlay, the hardware prototype was evaluated for authentication performance and primary signal degradation using backoffs α of 12, 15, and 18 dB. As constructed, the watermark is sufficiently detectable for α over the SNR operating region of 802.11g, even for $P_{\text{FA}} \leq 1\%$. Using MCS 5 (36 Mbps) and above, the achievable BER curves degrade such that lower data rate modes may be preferred. Further statistical processing to determine the receiver operating characteristic (ROC) curves validated by hardware prototypes in future demonstrations. Other waveforms may also be employed as the primary data link, such as those used by mobile cellular devices, used by devices in the IoT, and/or to show a receiver-assigned code division multiple access (RA-CDMA) use case. Establishing protocols for MAC-layer processing of unauthenticated received messages is also considered.

References

[1] Y. M. Erten, and E. Tomur, A layered security architecture for corporate 802.11 wireless networks, 2004 Symposium on Wireless Telecommunications, Pomona, CA, USA, 2004, pp. 123-128.

[2] T. Kiravuo, M. Sarela, and J. Manner, A Survey of Ethernet LAN Security, in IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1477-1491, Third Quarter 2013.

[3] U. Murthy, O. Bukhres, W. Winn, and E. Vanderdez, Firewalls for security in wireless networks, Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Kohala Coast, HI, USA, 1998, pp. 672-680 vol.7.

[4] A. Chouchane, S. Rekhis, and N. Boudriga, Defending against rogue base station attacks using wavelet based fingerprinting, 2009 IEEE/ACS International Conference on Computer Systems and Applications, Rabat, 2009, pp. 523-530.

[5] M. S. M. Annoni Notare, F. A. da Silva Cruz, B. Goncalves Riso, and C. B. Westphall, Wireless communications: security management against cloned cellular phones, WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No.99TH8466), New Orleans, LA, USA, 1999, pp. 1412-1416 vol.3.

[6] Z. Akram, M. A. Saeed, and M. Daud, Real time exploitation of security mechanisms of residential WLAN access points, 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, 2018, pp. 1-5.

[7] V. Deep and T. Elarabi, Efficient IEEE 802.15.4 ZigBee standard hardware design for IoT applications, 2017 International Conference on Signals and Systems (ICSigSys), Sanur, 2017, pp. 261-265.

[8] IEEE Standard for Part 11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Mar. 2012.

[9] 36.101 - Evolved Universal Terrestrial Radio Access (E-UTRA), User Equipment (UE) radio transmission and reception, 2019.

[10] C. Zhao, M. Huang, and L. Huang, A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks, Computer Networks, Volume 128, 2017, Pages 164-171.

[11] A. J. Michaels, High-Order PSK Signaling (HOPS) Techniques for Low-Power Spread Spectrum Communications, 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Chania, Greece, 2018, pp. 01-07.

[12] G. Heidari-Bateni and C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, in IEEE Transactions on Communications, vol. 42, no. 234, pp. 1524-1527, Feb/Mar/Apr 1994.

[13] A. J. Michaels, W. C. Headley, J. M. Ernst, and S. D. Hitefield, Enhanced PHY-layer security via co-channel underlays, 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, 2016, pp. 1-6.

[14] R. Chakravarthy, Kaiyu Huang, Lin Zhang, and Z. Wu, Primary User authentication of cognitive radio network using underlay waveform, 2017 Cognitive Communications for Aerospace Applications Workshop (CCAA), Cleveland, OH, 2017, pp. 1-5.

[15] Z. Bakhshi, A. Balador, and J. Mustafa, Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models, 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, 2018, pp. 173-178.

[16] S. Singh and N. Singh, Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce, 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1577-1581.

[17] Mohammad Mehedi Hassan, Kai Lin, Xuejun Yue, and Jiafu Wan, A multimedia healthcare data sharing approach through cloud-based body area network, Future Generation Computer Systems, Volume 66, 2017, Pages 48-58.

[18] Y. Kong and M. S. Hossain, FPGA Implementation of Modular Multiplier in Residue Number System, 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS), Bali, 2018, pp. 137-140.

[19] Joseph Gaeddert. liquid-wlan. https://github.com/jgaeddert/liquid-wlan, 2019.

Chapter 5

Conclusions

Arbitrary-phase spread spectrum waveforms allow for reliable low rate data transmission, denser scalable networks that employ RA-CDMA protocols, LPI/D secure communications, and operational mode flexibilities. However, the time-varying spreading code sequences and high-order PSK constellations largely responsible for these capabilities present significant hardware implementation challenges.

This thesis first presented an optional series of modifications to the brute-force matched-filter correlator to enable computationally-reduced resource receiver signal processing for low-power devices similar to those in the IoT. The largest such reduction is attributed to truncation of multi-bit correlation taps to sign bits, eliminating the need for resource-intensive multiplications. For an implemented detection performance loss of 2.10 dB relative to the brute-force fallthrough correlator prototype, the 4-times folded preamble structure with $\lambda = \sqrt{2}/2$ pruned sign-bit coefficients permitted further ALM reductions of 76% and logic register reductions of 82%. Additionally, the 81% utilization of entire design resources was reduced to the more acceptable 57%.

Given that real-world environments are usually less ideal than in the laboratory, Chapter 3 proposed the sequence-based uniformly-distributed chip phase words be color mapped to an aliased 2^8-ary PSK-based constellation and defined incrementally. For dynamic output spectra modes, this thesis detailed methods to design color maps that accentuate the signal at more optimal frequencies with band selection by circular shifts of the LUT registers.

Hardware prototyping results showed that 3 dB shaping improved the measured BER performance at by around 0.5 dB compared to uniform PSD operations in the presence of a narrowband interferer.

Finally, Chapter 4 demonstrated the use of co-channel underlay-based watermarks to authenticate transmissions in IEEE 802.11g networks, while the core techniques and PHY-layer security improvement may be translated for use in nearly all wireless networks. Although, the maximum benefit is most likely gained in high data rate applications that employ commercial wireless technology standards, since those specifications tend to implement medium access control layer (MAC) security features. The open source availability of liquid-dsp [5] and liquid-wlan [6], however, made IEEE 802.11g an ideal primary data signal candidate for the hardware prototype. As constructed, primary signal authentication was capably achieved even for watermarks operating at the power level backoff $\alpha = 18$ dB signal to interference plus noise ratio (SINR), showing minimal link degradation up to 802.11g modulation and coding scheme (MCS) mode 4 (that is, 24 Mbps). In summary, the results prove the viability of PHY-layer firewalls built to perform authentication of time-evolving watermarks.

5.1 Future Work

Communications systems that employ similar chaotic sequence-based waveforms have traditionally been deployed to military wireless networks, specifically due to the inherent anti-jam (AJ) and LPI/D characteristics inherent to these spread spectrum signals [1]. In modern and future communication systems of wireless industrial, enterprise, and mobile networks, the dramatically increasing node densities lead to a desire for real-world MAC-layer layer demonstrations [12]. On a similar note, MAC-layer processing of unauthenticated PHY-layer firewall messages may be constructed from the statistical results obtained in this work,

and/or the detection statistic measurements be expanded to produce receiver operating characteristic (ROC) curves. To further adapt these highly secure waveforms for extra-military use in today's contested radio frequency bands, the integration of channel estimation and interference sensing with the customizable frequency spectra of Chapter 3 is also considered for future work.

Bibliography

[1] J. M. Alan and B. C. David. Efficient and flexible chaotic communication waveform family. In *2010 - MILCOM 2010 Military Communications Conference*, pages 1250–1255, Oct 2010. doi: 10.1109/MILCOM.2010.5680118.

[2] M. Colombo, C. De Marziani, Á. Hernández, J. Ureña, and M. Mayosky. Low-complexity timing synchronization for ofdm based on cazac and golay sequences. In *2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB)*, pages 1–5, Sep. 2017. doi: 10.1109/ICUWB.2017.8250961.

[3] M. J. Fletcher, J. D. Gaeddert, and A. J. Michaels. Physical layer firewall design using co-channel underlay-based watermark authentication. Submitted to *2019 Military Communications Conference*, 2019.

[4] M. J. Fletcher, A. J. Michaels, and D. B. Ridge. Fallthrough correlation techniques for arbitrary-phase spread spectrum waveforms. Submitted to *IEEE Access Journal*, 2019.

[5] J. D. Gaeddert. liquid-dsp. https://github.com/jgaeddert/liquid-dsp, 2019.

[6] J. D. Gaeddert. liquid-wlan. https://github.com/jgaeddert/liquid-wlan, 2019.

[7] R. Gupta and S. Anuradha. A direct sequence spread spectrum transceiver with enhanced security using chaotic and gold sequence. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–6, July 2018. doi: 10.1109/ICCCNT.2018.8494061.

[8] G. Heidari-Bateni and C. D. McGillem. A chaotic direct-sequence spread-spectrum

communication system. *IEEE Transactions on Communications*, 42(234):1524–1527, FEBRUARY 1994. ISSN 0090-6778. doi: 10.1109/TCOMM.1994.582834.

[9] A. J. Michaels. High-Order PSK Signaling (HOPS) techniques for low-power spread spectrum communications. In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pages 01–07, June 2018. doi: 10.1109/WoWMoM.2018.8449732.

[10] A. J. Michaels and M. J. Fletcher. Frequency-Selective High-Order PSK Signaling. Submitted to *2019 Military Communications Conference*, 2019.

[11] A. J. Michaels, W. C. Headley, J. M. Ernst, and S. D. Hitefield. Enhanced phy-layer security via co-channel underlays. In *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pages 1–6, Dec 2016. doi: 10.1109/PCCC.2016.7820662.

[12] E. E. Petrosky, A. J. Michaels, and D. B. Ridge. Network scalability comparison of IEEE 802.15.4 and Receiver-Assigned CDMA. *IEEE Internet of Things Journal*, pages 1–1, 2019. ISSN 2327-4662. doi: 10.1109/JIOT.2018.2884455.

[13] John G. Proakis and Dimitris G. Manolakis. *Digital signal processing - principles, algorithms and applications (2. ed.)*. Macmillan, 1992. ISBN 978-0-02-396815-0.

[14] J. Yu and Y. Yao. Detection performance of chaotic spreading LPI waveforms. *IEEE Transactions on Wireless Communications*, 4(2):390–396, March 2005. ISSN 1536-1276. doi: 10.1109/TWC.2004.842948.