Experimentation with Prolate Spheroidal Wave Function Pulses for Physical-Layer Security

Tyan-Lin Wang and Ivan B. Djordjevic

Abstract—**Prolate spheroidal wave functions (PSWF) are a temporally orthogonal set of waveforms in which energy is concentrated in a finite time window and finite bandwidth. In wireless communications, where binary information is encoded onto a sequence of pulses, individual symbols can conceivably be represented by different orders of PSWF pulse shapes for transmission. Because these pulses have approximately constant bandwidth and pulsewidth across all orders, they are an interesting alternative to conventional modulation formats. Although they are certainly capable of improving spectral efficiency and data capacity, in this study we investigate their feasibility in achieving physical-layer security in wireless RF transmissions.**

Keywords— **Physical-layer security, pulse shape modulation, wireless communications.**

I. Introduction

One of the outstanding goals of physical-layer security is to develop an infrastructure in which data can be securely transmitted without requiring the management of a secret key. Indeed, the discrete memoryless wiretap channel model [1] aims to exploit the transmission and reception of a noisy and distorted signal emerging from the communications channel in order to achieve a certain amount of secrecy between the transmitter (Alice) and the receiver (Bob) in spite of wiretapping attacks by an eavesdropper (Eve). One possibility that may help to enable physical-layer security in wireless RF communications is to generate the pulses that correspond to a transmitted data sequence as prolate spheroidal wave functions (PSWF). These wave functions were extensively studied by Slepian in the late 1970s [2] and are oftentimes informally called Slepian functions. In the discrete-time representation, they are also referred to as discrete prolate spheroidal sequences (DPSS). From the perspective of a digital communications system, pulse shape modulation (or orthogonal pulse modulation) can in principle be implemented for increasing spectral efficiency and data capacity. Researchers in the early 2000s had already proposed using PSWF pulses for M-ary pulse shape modulation in ultra-wideband systems [3] and those from a decade later revisited the concept and proposed extending the waveform design to frequencies in the W-band [4]. Even within the past couple of years there was a study comparing the use of PSWF pulses to other orthogonal waveforms such as Hermite pulses [5] and a proposed transmitter and receiver system architecture for modified Hermite pulse shapes [6].

We note that all of these studies were simulation-based and believe that the lack of published experimental results involving PSWF pulses is perhaps due to the technical challenges in actually generating and receiving these pulses with adequate fidelity and the anticipated mediocre data rate performance that would result even if an experimental setup were established. That said, nowadays high-speed arbitrary waveform generators (AWG) with sampling rates of at least 10 GS/s and up to 120 GS/s are commercially available so it is possible to generate these waveforms with sufficient resolution that enables experimentation with PSWF pulses. In this paper we investigate utilizing these pulses for physical-layer security purposes.

The paper is organized as follows. In Section II we describe the concept behind applying PSWF pulses to physical-layer security. Section III provides details of the experimental setup. Finally, Section IV presents and discusses the results.

II. Applying PSWF pulses to physical-layer security

The most intriguing aspect of PSWF pulses is that their bandwidth and pulsewidth remain almost unchanged across all orders. In the context of communications, PSWF pulses comprise a set of doubly orthogonal bandlimited functions that have the greatest concentration of energy inside a single symbol interval. This orthogonality property is thought to provide an inherent degree of resiliency to intersymbol interference (ISI) even as timing jitter causes neighboring pulses to spread into adjacent time intervals. The discrete-time version of PSWF pulses, or DPSS, can be formulated as eigenvectors of either a Hermitian matrix or symmetric tridiagonal matrix parameterized by the number of time samples describing the pulse and its normalized bandwidth [7]. DPSS pulses can therefore be generated using numerical matrix techniques. Furthermore, the time-half bandwidth product is a constant which means designing a set of these pulse shapes usually incorporates a tradeoff between bandwidth and pulsewidth.

In our experiment, we focus solely on the different orders of PSWF pulse shapes and their temporal orthogonality. Our experimental design also leverages the cross-correlation properties of these orthogonal pulses which theoretically allow multiple pulses to be transmitted together with minimal interference between them. The conceptual implementation of such a system is as follows. Firstly, we emphasize that the PSWF pulses are envelope functions which shape and modulate an underlying sinusoidal carrier frequency. Secondly, we allocate a bank of *N* pulse shape orders (creating a set of cardinality *N*) and designate on-off-keying (OOK)

Tyan-Lin Wang and Ivan B. Djordjevic are with the Electrical and Computer Engineering Department, University of Arizona, 1230 E. Speedway Blvd., Tucson, AZ, USA (e-mails: tyanlinw@email.arizona.edu, ivan@email.arizona.edu).

978-1-7281-0878-0/19/$31.00 ©2019 IEEE

modulation such that every "1" bit is represented by the transmission of a randomly selected PSWF order while every "0" bit is represented by no transmission at all. Thirdly, as a proof-of-concept, we establish a secure transmitter paradigm in which lower order pulse shapes (e.g. orders 1 to 4) are used as data symbols (bits) and higher order shapes (e.g. orders 5 to 7) multiplied by an additive white Gaussian noise (AWGN) waveform are used as artificial masking pulses. The combiner superimposes each masking pulse on the data pulse before transmitting the result.

Another aspect which is expected to further enhance the security of the transmission is for Alice and Bob to share a pre-determined seed for a random number generator that dictates the choice of the PSWF order used for each signal pulse transmission. The encoding procedure is such that the "1" bits are represented by a random choice of orders from 1 to 4. Therefore, Bob's knowledge of the seed allows him to always test for the correct PSWF pulse order in search of each "1" bit at the receiver. On the other hand, Eve must always test for each PSWF pulse shape. This not only increases the latency by occupying more hardware processing resources but also increases the likelihood that the final decoded message contains more errors. Thus, the emphasis in this experiment is placed on measuring Bob's bit-error rate (BER) performance in physical-layer security scenario. In practical applications, a much larger cardinality DPSS set is needed.

III. Experimental Setup

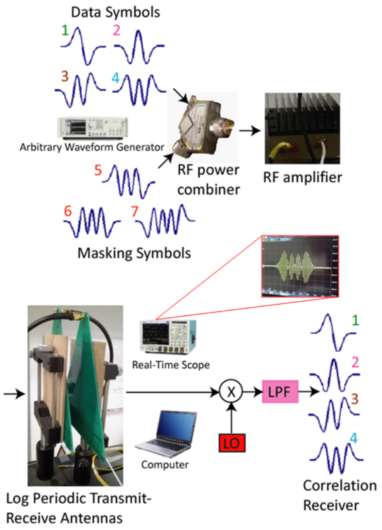

Fig. 1. Hardware layout of the PSWF experiment. The inset shows an ideal order 3 pulse captured by the real-time oscilloscope in the laboratory.

The carrier frequency used to perform this experiment was deliberately chosen to be 4 GHz, primarily taking into account the electromagnetic compatibility issues with the other electronic equipment and to avoid interference from both the 2.4 GHz and 5 GHz WiFi signals. Needless to say, the carrier frequency can certainly be moved to frequencies in other parts of the electromagnetic spectrum such as the U-NII (around 5 GHz), the microwave (1 to 30 GHz), and the millimeter wave (30 to 300 GHz) bands, albeit with different front-end hardware involved. Of course, the details of the sampling period, the choice of intermediate frequency, and the up-conversion process should be properly addressed [4]. A similar argument can be made in regard to the amount of radiated power, which for this experiment was intentionally made low for safety and interference concerns. But this experiment can certainly be replicated with operating powers on the order of 100 mW, which is typical for standard WiFi access points.

An individual pulse shape modulated carrier waveform is directly digitally synthesized by programming a Tektronix AWG70002A arbitrary waveform generator. The Tektronix AWG has an analog bandwidth of 13.5 GHz and a sampling rate of 25 GS/s in its digital-to-analog converter (DAC). Here we specified 1024 samples per symbol in order to smoothly resolve the 4 GHz carrier oscillations underneath the shape of each PSWF pulse envelope. Since the AWG sampling interval is 40 ps a single pulse occupies a symbol interval of 40.96 ns, which corresponds to a data rate of 24.4 Mbps. Although this is a mediocre data rate it was necessary to be conservative in prescribing a large number of samples per symbol because sufficient resolution of the pulse shape is very important for this type of experiment. This is the same reasoning for creating only the first seven PSWF orders in the AWG and choosing orders 5 to 7 as masking pulses. In general, using higher orders will be better for masking purposes but those envelopes have more oscillations and there needs to be a sufficient number of carrier cycles underneath those oscillations as well. Alternatively, an RF modulator and up-converter can be used if increasing the data rate is desired.

Referring to Figure 1, the goal of the experiment is to demonstrate transmission and reception of a data sequence manifested as a train of PSWF pulses which are masked by superimposed noise pulses. A standard pseudo-random binary sequence (PRBS9) pattern commonly found in pulse pattern generators produces a sequence of 512 bits which translates to 512 bits x 1024 samples per bit = 524288 samples representing the entire train of PSWF pulses in the message. These values are then loaded onto the memory unit of one channel on the Tektronix AWG, converted to an analog voltage waveform by the DAC, and replayed continuously at the output. Similarly, the values for the masking noise pulses are loaded onto the other channel of the Tektronix AWG and the values from both channels are later superimposed by the RF combiner. Although in the signal channel each frame contains 512 total bits, the first 32 bits are actually replaced by a known preamble bit sequence. This leaves the remaining 480 bits to comprise the actual message. The purpose of this is to enable frame synchronization at the receiver. Note the preamble consists of regular OOK pulses (also having 1024 samples per bit) while the message still continues to be represented by PSWF pulses. Performing a cross-correlation operation with the known preamble at the receiver allows identification of the start of the frame and recovery of the symbol timing for subsequent BER analysis. In the noise channel the voltage values at the positions corresponding to the first 32 bits are simply set to zero since the preamble is already appended at the front of the signal channel.

The other hardware components involved in this setup (and their operating frequency range) are the HP 11667A RF power combiner (DC to 18 GHz), Mini-Circuits ZHL-4240W coaxial RF amplifier (up to 4.2 GHz), and Ettus LP0965 log periodic printed circuit board antennas (850 MHz to 6.5 GHz). Not explicitly shown in Figure 1 are pairs of RF Coax Inc. K086MMHFJ cables (DC to 40 GHz), with 2.92 mm male connectors on both ends that connect the various components. The receive antenna's output cable connects directly into a single channel on a Tektronix DSA73304D real-time oscilloscope having 33 GHz analog bandwidth and a maximum analog-to-digital converter (ADC) sampling rate of 100 GS/s. In order to match the sampling rate of the AWG on the transmit side, the sampling rate of the ADC in the real-time scope is also adjusted to be 25 GS/s. One million samples are captured in each real-time scope acquisition, and with the horizontal time base set at 40 ps per point, the whole record time is 40 µs. The remaining steps involve digital signal processing performed in MATLAB, where the received waveform is mixed with a 4 GHz pure sinusoidal local oscillator (LO) and passed through a finite impulse response equiripple low pass filter (LPF) having cutoff frequency slightly below 4 GHz and 60 dB stop band attenuation. This post-processing extracts the PSWF pulse envelopes and the results are shown by the orange curves in Figure 2.

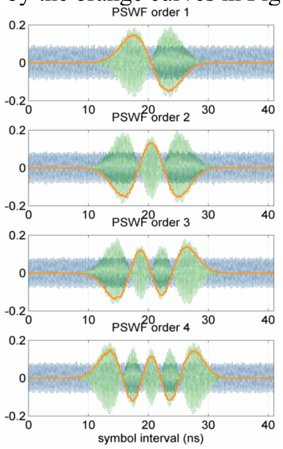

Fig. 2. Experimental data showing order 1 to 4 pulses modulating a 4 GHz carrier. The LO waveforms (blue) are used to demodulate the signal in post-processing and envelope pulse shapes (orange) are recovered after the LPF.

The last part of Figure 1 shows a discrete-time correlation receiver. In this step a matched filtering operation is performed where the extracted pulse shape is convolved with a time-reversed replica of the original pulse shape of orders 1 to 4 (that are stored in the receiver ahead of time). This is done for every symbol interval and correlation peaks occur when there is a match. A final threshold comparison completes the decoding of the message. Since this setup involves a combination of hardware transmission and reception followed by post-processing on a computer, it is not considered as a purely real-time experiment. Nevertheless, it serves to demonstrate the implementation of the concept. Data collection was done with an electrical back-to-back (B2B) configuration (where a RF cable was used as the transmission conduit) and a free-space transmission configuration where the transmit and receive antennas are spaced 1 inch apart and the pulse train is radiated from one to the other. To further assist the execution of this experiment we synchronized an identical Tektronix AWG70002A AWG to the original AWG that generates the PSWF signal and masking pulses. When properly synchronized, both AWGs produce waveforms that are aligned to within 10 picoseconds of timing skew which is almost negligible compared to the time scales in this experiment. The output the second AWG is directly connected to the real-time scope via RF cables and serves two purposes: 1) to transmit a pristine reference copy of the PSWF signal pulse train with leading preamble and 2) to transmit a pure 4 GHz sine wave to serve as the LO waveform for post-processing. Doing this effectively emulates a coherent homodyne detection system without any frequency offset or significant phase offset.

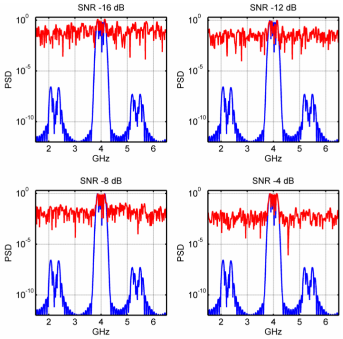

Fig. 3. Computed PSDs for an order 4 pulse without masking noise (blue) and with superimposed order 7 modulated masking noise (red).

Because the purpose of injecting artificial noise is to mask any apparent signal structure in both time and frequency, this implementation practically amounts to operating a communications system aided by a friendly jammer which provides a unique masking signature. Figure 3 shows the computed power spectral density (PSD) results for a PSWF order 4 pulse without masking noise and with superimposed order 7 modulated masking noise for several different signal to noise ratios (SNR). In the case of -16 dB SNR, the signal spectrum is fully embedded inside the artificial noise level but further increasing the SNR results in the eventual emergence of its spectral signature.

IV. Results and Discussion

Figure 4 shows examples of a PSWF order 3 pulse shape after transmission through the medium, comparing the case of pristine reference (without masking noise), electrical B2B (with superimposed masking noise), and transmit/receive antennas (with superimposed masking noise and amplified by the RF amplifier). Showing the case of a high SNR pulse allows us to observe the amount of distortion caused by the response function of the transmit and receive antennas. Even though there is only a small distance between the antennas, the bottom row of Figure 4 clearly shows the degradation to the PSWF envelope, which could be due to both phase distortion imparted by the RF amplifier and polarization mismatch of the antennas. Any distortion to the waveform will impact the demodulation and accuracy of the correlation receiver so pre-compensation methods and perhaps spectral filtering and pulse shape regeneration will need to be explored in order to make the transmission more robust.

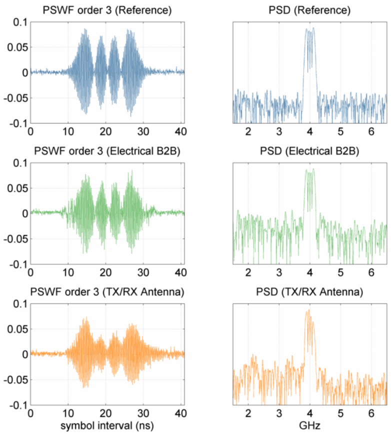

Fig. 4. Order 3 pulse shapes measured by the real-time oscilloscope after transmission for the case of pristine reference (top), electrical B2B (middle), and transmit/receive antennas (bottom) in a high SNR scenario.

Bob's correlation receiver uses pre-determined knowledge of the seed, which allows efficient testing against the correct PSWF pulse order. But Eve needs to test against all the orders, which is very inefficient and error-prone. The decoding is done by setting a hard decision threshold to determine if the bit is a "1" or a "0". Ideally this process takes advantage of the inherent orthogonality between the signal PSWF pulse orders (1 to 4) and the masking pulse orders (5 to 7) so that correlation maxima occur when there is a match and correlation minima occur when there is no match. In practice the distinction is less obvious especially in low SNR scenarios. Better algorithms may improve the decoding performance at the cost of further complexity. These include using dynamic thresholding based on machine learning or implementing an optimum receiver decision rule based on log-likelihood ratios.

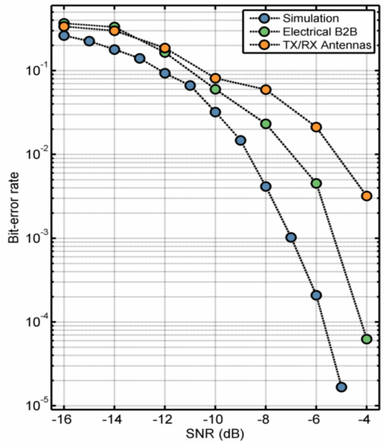

Fig. 5. Comparison of BER curve performance after hard decision decoding of the correlation receiver output.

The comparison of BER curves for a simulated transmission, the electrical B2B transmission, and the antenna transmission is shown in Figure 5. As expected the BER performance degrades going from the simulation to the antenna experiment. The target is to obtain a raw BER value below 10^{-3} in the experiment because forward error correction can then be used to reduce the errors by several more orders of magnitude. However the simultaneous requirement of having adequate signal masking makes this difficult since an SNR of at least -8 dB is needed to reach below a BER of 10^{-3}, but the spectral signature begins to appear under these conditions as shown in Figure 3. On the other hand, we'd expect better masking if a higher cardinality set of pulses could be created. The use of higher order PSWF modulated noise is desirable since they have more resemblance to actual noise waveforms. Doubling the symbol rate of the masking symbols (i.e. using two consecutive masking pulses to mask one signal pulse interval) will also achieve the same goal [8].

The technical challenges and performance limitations encountered in this experiment highlight the contrast that exists between the concept and the practical hardware implementation. With top-of-the-line AWGs now providing sampling rates exceeding 100 GS/s, higher data rates can be directly obtained without sacrificing signal fidelity and the carrier frequency can be increased while still satisfying the Nyquist criterion. It is also paramount to engineer antenna designs or radiating elements that better preserve the pulse shapes so that the correlation receiver performance is closer to the optimal. Ultimately the results of this experiment are underwhelming in terms of data rate, transmitted distance, and the tradeoff between obtaining low BER and having effective signal masking. However there are avenues for further research, especially with the choice of the carrier frequency and the engineering of antenna response functions since the degree of signal pulse shape preservation and the balance between the power in the signal and masking pulses will dictate the feasibility of a secure data transmission system.

Acknowledgment

ONR MURI (grant N00014-13-1-0627) and NSF (grants 1907918 and 1828132).

References

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] D. Slepian, "Prolate Spheroidal Wave Functions, Fourier Analysis, and Uncertainty-V: The Discrete Case," *Bell Syst. Tech. J.*, vol. 57, no. 5, pp. 1371–1430, May 1978.

[3] K. Usuda, H. Zhang, and M. Nakagawa, "M-ary Pulse Shape Modulation for PSWF-Based UWB Systems in Multipath Fading Environment," in *Proc. IEEE Global Telecommunications Conference, GLOBECOM 2004*, Dallas, TX, 2004, pp. 3498–3504.

[4] C. Sacchi, T. Rossi, M. Ruggieri and F. Granelli, "Efficient Waveform Design for High-Bit-Rate W-band Satellite Transmissions," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 2, pp. 974–995, Apr. 2011.

[5] P. Jadhav and J. Gomes, "Comparing PSWF, Hermite Pulses For High Speed Communication Using N-PSM," *Int. J. Comput. Netw. Commun. Sec.*, vol. 5, no. 5, pp. 90–95, May 2017.

[6] K. P. Pradhan, Y.-G. Li, A. K. M. Arifuzzman, and M. R. Haider, "Modified Hermite Pulse-Based Wideband Communication for High-Speed Data Transfer in Wireless Sensor Applications," *J. Low Power Electron. Appl.*, vol. 7, no. 30, pp. 1–16, Dec. 2017.

[7] D. M. Gruenbacher and D. R. Hummels, "A Simple Algorithm for Generating Discrete Prolate Spheroidal Sequences," *IEEE Trans. Signal Process.*, vol. 42, no. 11, pp. 3276–3278, Nov. 1994.

[8] I. B. Djordjevic, A. H. Saleh, F. Küppers, "Design of DPSS based fiber Bragg gratings and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing," *Opt. Express*, vol. 22, no. 9, pp. 10882–10897, May 2014.