ANALYSIS OF A COVERT COMMUNICATION METHOD UTILIZING NON-COHERENT DPSK MASKED BY PULSED RADAR INTERFERENCE

Thomas W. Tedesso

United States Naval Academy
Department of Electrical and
Computer Engineering
Annapolis, Maryland 21402

Ric Romero and Zachary Staples

Naval Postgraduate School
Department of Electrical and
Computer Engineering
Monterey, California 93943

ABSTRACT

In this paper, a covert communication method is proposed that embeds a digital communication signal onto the radar return of a pulse Doppler radar. The interfering radar signal at the receiver is estimated and coherently subtracted from combined signal prior to demodulation of the communications signal to baseband and symbol detection. The robustness of the communication method to various estimation errors is investigated for several phase shift keying digital communication modulations through Monte Carlo simulations. It is demonstrated that differential encoding systems with non-coherent detection perform best in the presence of frequency estimation errors. However, it was also demonstrated that the system is not very robust to phase estimation errors. The performance of non-coherent differential phase shift keying and differential quaternary phase shift keying are investigated to determine the impact of varying different parameters upon symbol error rate.

Index Terms— digital communications, signal estimation, covert communications, radar

1. INTRODUCTION

Many military or civilian law enforcement operations rely on the ability to covertly communicate between platforms to maintain operational security and the tactical element of surprise. Such operations may include intelligence collection and reconnaissance or targeting of adversary positions. Methods of covertly communicating have been explored throughout history. In many instances, encryption is used to prevent an adversary from deciphering the content of an intercepted signal. However, it is often desired to prevent adversaries from detecting communications signals between friendly units which could compromise their location or provide adversaries with other intelligence. If the transmitting platform is to remain covert, a low probability of intercept (LPI) method of communication is required. Various LPI modulation techniques have been presented in the literature including direct sequence spread spectrum (DSSS) and frequency hopping (FH) communications to combat narrow band interference [1–3].

Other means of covertly communicating include embedding a communication signal into a large signal that occurs in the environment. A clandestine underwater acoustic communication system is examined in [7] that embeds a DSSS communication signal onto a whale noise masking it from detection by adversaries. A virtual time reversal mirror focuses the energy of the communication signal while channel estimation is conducted utilizing matching pursuit. In [8–11], covertly embedding a communication signal in radar backscatter is investigated. An eigen value based approach to the communication signal design is analyzed in [8]. In [11], multi-path time reversal introduces spatio-temporal focusing of the communication signal at the desired receiver while distorting the signal at other locations increasing its covertness. Theoretical limits of low probability of detection (LPD) communication in a channel corrupted by additive white Gaussian noise (AWGN) was explored in [4–6]. In [4], fundamental bounds on LPD comunicaton over wireless channels subject to AWGN are developed and a square root limit on the amount of information transmitted reliably and with LPD over a AWGN channel is presented. The results in [4] are extended and generalized in [5] through development of a coding scheme based on the principle of channel resolvability. While in [6], a privacy rate is defined and analyzed over an AWGN channel as well as a Rayleigh single input - single output and multiple input - multiple output channel.

In this paper, a covert communication method initially explored in [12] that masks a digital communication signal in the return of a pulse Doppler radar signal is analyzed. At the receiver, an estimate of the radar signal is produced and coherently subtracted from the received signal prior to demodulation and detection of the communication signal. Several phase shift keying (PSK) modulations are analyzed through Monte Carlo simulations to determine their robustness to frequency, phase, and amplitude estimation errors. To simplify the analysis, perfect system synchronization between the transmitter and the receiver of the communications signal is assumed.

Monte Carlo simulation results are also presented that analyze the impact of the pulse width, the fast Fourier transform (FFT) size used, and the number of radar pulses in the estimation for differential phase shift keying (DPSK) and differential quaternary PSK (DQPSK) using non-coherent detection. In section 2, the problem description is provided and the proposed covert communication method is proposed. Simulation results are presented in section 3 to evaluate the performance of different PSK modulations. Conclusions and areas of future research are discussed in section 4.

2. PROBLEM STATEMENT

In this section, a covert communication method is proposed that embeds a digital communication signal into the radar return of a high power microwave pulse Doppler radar. In Fig. 1, two friendly ships desire to communicate covertly. Station 1 (STA1) transmits a pulsed radar in the presence of additive white Gaussian noise (AWGN) that is received at station 2 (STA2), $s_{2R}(t) = r_{2R}(t) + w(t)$, where $w(t)$ is AWGN and $r(t)$ is a pulsed radar signal with a carrier frequency, f_r, a pulse width, T_{PW}, and a pulse repetition frequency,

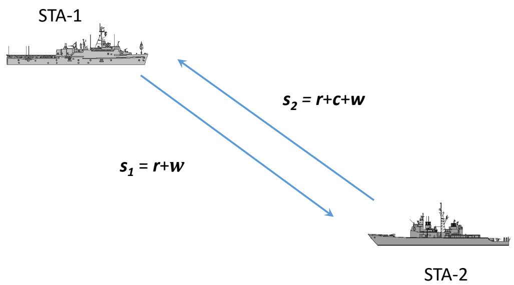

Fig. 1. Covert communications scenario. Station 2 embeds a digital communications signal onto the reflected radar return to mask the communication.

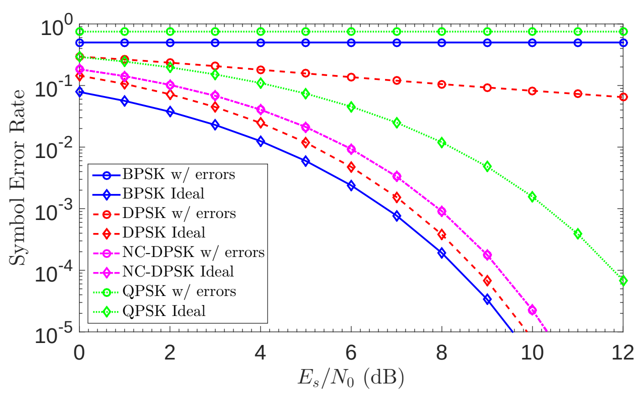

Fig. 2. Effects of a one percent frequency estimation error on symbol error rate. Ideal results are represented by $\diamond$ symbols and the results with errors are represented by $\circ$ symbols. BPSK results are represented with a solid line, DPSK a dashed line '$--$', NC-DPSK a '$-\cdot-$' line and QPSK with a '$\cdots$' line.

PRF. As is customary in signal processing analysis, we normalize the sampling time such that the signal received by STA2 is given by

$$\mathbf{s_{2R}} = \mathbf{r_{2R}} + \mathbf{w} \tag{1}$$

where $\mathbf{r_{2R}}$ is the radar signal received by STA2 and $\mathbf{w}$ is the AWGN.

At STA2, an estimate of the carrier frequency is made and a phase shift keyed digital communication signal, $c(t)$ with a carrier frequency, $\widehat{f_r}$, is transmitted to STA1 that is masked in the radar return signal and received by STA1. The signal received by STA1 is $s_{1R} = r_{1R}(t) + c(t) + w(t)$. After normalizing the frequency with respect to the sampling time, the received signal at STA1 is expressed in vector format as

$$\mathbf{s_{1R}} = \mathbf{r_{1R}} + \mathbf{c_{1R}} + \mathbf{w}. \tag{2}$$

At STA1, $\mathbf{s_{1R}}$ is received and an estimate of the radar signal is subtracted from $\mathbf{s_{1R}}$, prior to demodulation to baseband and symbol detection.

Two separate estimation problems exist. First, the radar signal parameters are estimated at STA2. The radar signal is

$$r[n] = A_r e^{j\theta_r} p[n] e^{j\omega_r n}, \tag{3}$$

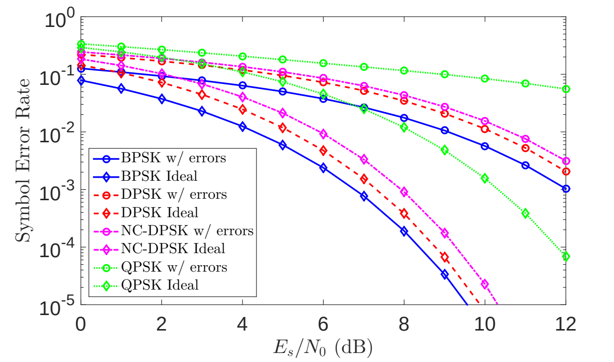

Fig. 3. Effects of phase estimation error of $\theta_{err} = \pi/64$ on symbol error rate. Ideal results are represented by $\diamond$ symbols and the results with errors are represented by $\circ$ symbols. BPSK results are represented with a solid line, DPSK a dashed line '$--$', NC-DPSK a '$-\cdot-$' line and QPSK with a '$\cdots$' line.

where, A_r is the magnitude of $r[n]$, θ_r is its phase angle, and ω_r is the digital frequency of the radar signal. A rectangular periodic pulse train is represented by $p[n]$ which has a pulse width of N_p samples and a pulse repetition frequency, $PRF = 1/N_T$,

$$p[n] = \begin{cases} 1, & n = [0, 1, \ldots, N_p - 1] \\ 0, & n = [N_p, N_p + 1, \ldots N_T - 1] \end{cases} \tag{4}$$

where $p[n + kN_T] = p[n]$ and $k \in \{0, 1, 2, \ldots\}$. At STA2, an estimate of radar signal's digital frequency, $\widehat{\omega_r}$, is obtained from the power spectral density (PSD) of $\mathbf{s_{2R}}$ using the Welch method [13] and a weighted average of the frequency components composing the main lobe of the PSD of $\mathbf{s_{2R}}$. The baseband communication signal is modulated with complex exponential signal with a digital frequency equal to $\widehat{\omega_r}$. The communication signal is modeled in the simulations as

$$c[n] = d[n] p[n] e^{j\widehat{\omega_r} n} \tag{5}$$

where $d[n]$ is an M-array PSK signal. The communication signal would undergo digital to analog conversion and further upconversion to the estimated radar carrier frequency $\widehat{f_r}$ prior to transmission. In the simulations, the radar signal power to communications signal power ratio is $20dB$.

The second estimation problem occurs upon receipt of the signal, $\mathbf{s_{1R}}$, at STA1. The radar signal must be estimated and coherently subtracted from the received signal to remove the interference and allow detection of the digital communication signal. The amplitude of the received signal can be estimated through determination of the PSD as previously discussed or by determining the standard deviation of the signal,

$$\widehat{A}_r = \sqrt{\frac{1}{LN_p} \sum_{l=0}^{L-1} \left[\sum_{n=lN_p}^{N_P(l+1)-1} s_{1R}[n] s_{1R}^*[n] \right]}, \tag{6}$$

where L is the number of radar pulses used to make the estimate.

The radar signal's phase is estimated by demodulating the $\mathbf{s_{1R}}$ to baseband and determining the average values of the real and imaginary (I & Q) components of the signal in the radar pulse. The phase

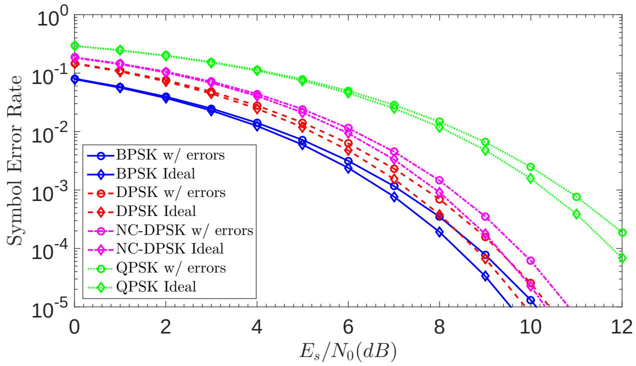

Fig. 4. Effect of a one percent radar signal amplitude estimation error on SER. Ideal results are represented by $\diamond$ symbols and the results with errors are represented by $\circ$ symbols. BPSK results are represented with a solid line, DPSK a dashed line '$--$', NC-DPSK a '$- \cdot -$' line and QPSK with a '$\cdots$' line.

estimate is then determined by taking the inverse tangent as given by

$$\widehat{\theta}_r = \arctan\left(\frac{\sum_{l=0}^{L-1}\sum_{n=lN_p}^{(l+1)N_P-1}\Im(\widetilde{s_{1R}}[n])}{\sum_{l=0}^{L-1}\sum_{n=lN_p}^{(l+1)N_P-1}\Re(\widetilde{s_{1R}}[n])}\right), \qquad (7)$$

where $\widetilde{s_{1R}}[n]$ is the baseband signal. The estimated radar signal received at STA1 is

$$\widehat{r_{1R}}[n] = \widehat{A}_r e^{j(\omega_r[n]+\widehat{\theta}_r)}. \qquad (8)$$

Following estimation of the radar signal it is subtracted from $\mathbf{s_{1R}}$, leaving the communication signal with AWGN,

$$\mathbf{y} = \mathbf{c} + \mathbf{w} + \mathbf{e}, \qquad (9)$$

provided $\mathbf{e} = \widehat{\mathbf{r_{1R}}} - \mathbf{r_{1R}}$ is small.

In the next section, Monte Carlo simulation results are presented to analyze the impact of various estimation inaccuracies on the performance of the communication method. The robustness of BPSK, DPSK, and QPSK are analyzed for errors in estimation of the radar signal's frequency, phase, and amplitude. For DPSK, both coherent and non-coherent detection are explored.

3. SIMULATION RESULTS AND ANALYSIS

In the following analysis, it is assumed that the communication signal and the radar signal are perfectly synchronized (i.e. the communication signal is transmitted to coincide with the radar return). First, the effects of frequency, phase, and amplitude estimation errors are examined to determine which digital modulation scheme is most robust. Following that analysis, the system performance is analyzed using non-coherent (NC) detection of DPSK and differential QPSK (DQPSK) to determine the effects on the symbol error rate (SER) of changing the number of samples per pulse or pulse width, the FFT size, and the number of radar pulses used in the estimation of the radar parameters.

For the Monte Carlo simulations, 1×10^8 trials were conducted. The robustness of the various phase modulation techniques were examined for errors in the frequency, phase, and amplitude estimation of the radar signal.

First, the impact of errors in estimating the radar signal's frequency at STA2 was examined when using different PSK modulations. For the Monte Carlo simulations, $\widehat{\omega}_r = \omega_r + \omega_{err}$, where $\omega_{err} = 2\pi f_{err}/f_s$ is equal to a percentage of the ω_r. To demodulate the communication signal to baseband the signal $y[n]$ is multiplied by $e^{-j\omega_r n}$, resulting in a baseband signal

$$y_{bb}[n] = c[n]e^{j\omega_{err} n} + w[n]. \qquad (10)$$

Due to the frequency estimation error, the signal space rotates at a digital frequency of ω_{err} resulting in poor performance for all of the coherent detection methods analyzed. However, for NC-DPSK, system performance mirrored that of the theoretical curve when there was a 1% frequency error as shown in Fig. 2. The immunity of non-coherent detection to frequency estimation errors was the major factor for choosing NC-DPSK and DQPSK for further analysis.

Next, phase estimation error was examined assuming perfect estimation of the other parameters. Several values of phase estimation were examined. The results shown in Fig. 3, demonstrate that the SER for all modulation types examined degraded significantly when the phase estimation error was greater than $\pi/64 \approx 3\,\text{deg}$. This result is due to incomplete interference cancellation as

$$\mathbf{r} - \widehat{\mathbf{r}} = A_r e^{j(\omega_r n+\theta_r)}(1 - e^{j\theta_{err}}), \qquad (11)$$

where θ_{err} is the phase estimation error. Therefore, the covert communications scheme being examined is highly dependent upon accurate phase estimation to coherently subtract the interfering radar signal prior to demodulation and symbol detection.

The effect of amplitude estimation error, A_{err}, was evaluated to determine the SER with the other estimated parameters, phase and frequency, assumed to be perfectly estimated. The amplitude error was provided as a percentage of the A_r, $\widehat{A}_r = A_r + A_{err}$. An amplitude estimation error of 1% was determined to be acceptable based upon the results shown in Fig. 4. All of the modulations examined performed well under these conditions.

Based upon the results obtained above, DPSK and DQPSK modulations using non-coherent detection were chosen for analysis of the overall system performance due to the robustness of the non-coherent detection methods to frequency offset between the radar signal and the communications signal. The proposed communication method's performance is further analyzed below, where the effects of varying the pulse width (or number of samples per pulse), the FFT size, and the number of radar pulses used in parameter estimation are evaluated.

The effects of the radar signal pulse width (T_{PW}) and subsequently the number of samples per radar pulse were evaluated for DPSK and DQPSK using non-coherent detection. To evaluate the impact of the T_{PW} on system performance, the following parameters were used, $K = 256$, $L = 4$, $PRF = 10$kHz, and $f_s = 64\,$MHz for the Monte Carlo simulations. The intermediate radar frequency was chosen as a random value, where $f_r \in \{9000, 9010, 9020, \ldots, 11000\}$ kHz. The value of θ_r was a random number uniformly distributed between $[-\pi, \pi]$ radians. The pulse widths examined were $T_{PW} = [8, 4, 2, 1]\,\mu s$. In Fig. 5, the results are displayed along with the theoretical or ideal SER curves for DPSK and DQPSK. The results in Fig. 5 demonstrate that satisfactory performance can be obtained with a pulse width of $1\mu s$, (total of 256 samples), although performance is slightly degraded.

Next, the effect of the FFT size, K, utilized in the estimation was examined. Since the PSD was only used to find $\widehat{f}_r$, which DPSK was shown to be robust to frequency estimation errors in Fig. 2, it is expected that the value of K could be chosen to be relatively low. For

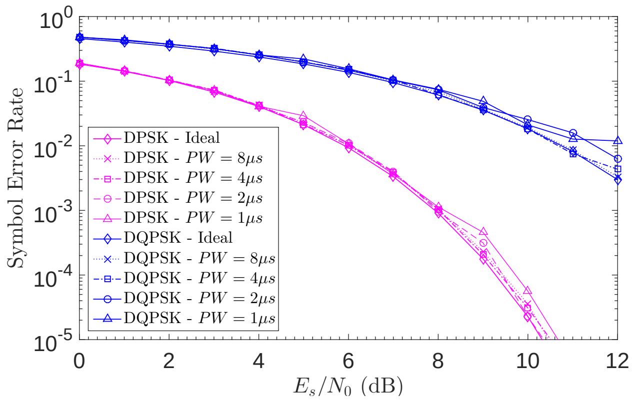

Fig. 5. Effect on pulse width on SER. Blue colored curves are DQPSK, magenta colored curves are DPSK. Markers correspond to ideal (◇), $T_{PW} = 8\mu s$ (×), $T_{PW} = 4\mu s$ (□), $T_{PW} = 2\mu s$ (○), and $T_{PW} = 1\mu s$ (△)

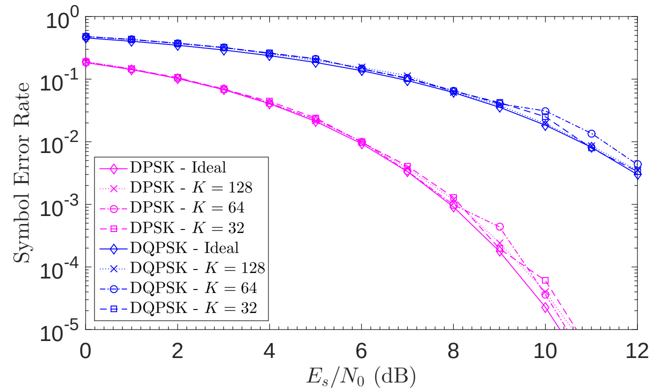

Fig. 6. Effect of FFT size, K, on symbol error rate. Blue colored curves are DQPSK, magenta colored curves are DPSK. Markers correspond to ideal (◇), $K = 128$ (×), $K = 64$ (○), and $K = 32$ (□).

this set of simulations, the system parameters used in the estimation were four radar pulses with a pulse width of $2\mu s$. The other radar parameters used in the simulation were the same as used previously. The performance of the proposed communication method was examined using $K \in \{128, 64, 32\}$. The results are displayed in Fig. 6. Satisfactory performance was observed for the DPSK modulation for $K \geq 32$ and DQPSK for $K \geq 64$. Based upon these results, relatively small FFT sizes may be used, lowering computation costs.

The minimum number of pulses used in the radar signal estimation was also examined. For the Monte Carlo simulation, the following parameters were used: the FFT size, $K = 256$, the pulse width, and $T_{PW} = 2\mu s$. The SER was determined when using $L \in \{1, 2, \ldots 6\}$. In Fig. 7, the results for $L = \{1, 2, 3\}$ are displayed along with the theoretical SER curves for DPSK and DQPSK modulations using non-coherent detection. From the results in Fig. 7, the system performance approaches the theoretical SER curves as the number of pulses used to make the estimate rises. Satisfactory performance was achieved in all cases examined. These results are consistent with those obtained where the pulse width was varied.

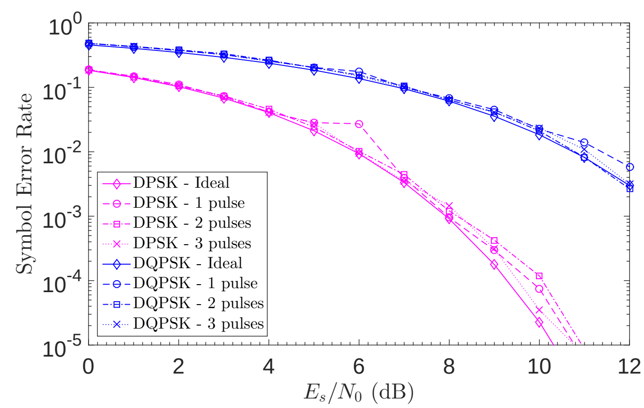

Fig. 7. Effect of the number of pulses used to make estimates on the SER. Blue colored curves are DQPSK, magenta colored curves are DPSK. Markers correspond to ideal (◇), $L = 1$ (○), $L = 2$ (□), and $L = 3$ (×).

4. CONCLUSION

In this work, an initial feasibility study of covert communications system which embedded a digital communication signal onto a coherent radar return pulse was examined. In this study, the radar interference was estimated and coherently subtracted from the received signal prior to demodulation and symbol detection. First, it was demonstrated that of the potential PSK modulation schemes that non-coherent DPSK was relatively immune to frequency estimation errors. It was also demonstrated that the proposed communication method is highly dependent upon accurate phase estimation. Then, DPSK and DQPSK were examined to determine the effect of the pulse width of the radar signal, the FFT size used, and the number of radar pulses used in the estimation. It was demonstrated through Monte Carlo simulations that both modulation methods performed well for pulse widths as small as $1\mu s$ and with an FFT size, $K \geq 64$. It was also demonstrated that as few as one to two radar pulses were sufficient to achieve satisfactory performance.

This work reports the findings of an initial feasibility study and does not include assessment of channel characteristics such as fading, system synchronization errors, or radar system characteristics such as pulse shaping, PRF jitter, and pulse compression. Future work will analyze the proposed covert communication method when taking these factors into account.

5. REFERENCES

[1] P. G. Flikkema, "Spread-spectrum techniques for wireless communication," *IEEE Signal Process. Mag.*, vol. 14, no. 3, pp. 26–36, May 1997.

[2] R. Iltis and L. Milstein, "Performance analysis of narrow-band interference rejection techniques in DS spread-spectrum systems," *IEEE Trans. Commun.*, vol. 32, no. 11, pp. 1169–1177, Nov. 1984.

[3] R. C. Robertson and J. F. Sheltry, "Multiple tone interference of frequency-hopped noncoherent MFSK signals transmitted over Ricean fading channels," *IEEE Trans. Commun.*, vol. 44, no. 7, pp. 867–875, Jul 1996.

[4] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable

communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[5] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[6] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[7] S. Liu, G. Qiao, A. Ismail, B. Liu, and L. Zhang, "Covert underwater acoustic communication using whale noise masking on DSSS signal," in *OCEANS - Bergen, 2013 MTS/IEEE*, Jun. 2013, pp. 1–6.

[8] S. D. Blunt and P. Yantham, "Waveform design for radar-embedded communications," in *2007 Int. Waveform Diversity and Design Conf.*, Jun. 2007, pp. 214–218.

[9] S. D. Blunt, J. Stiles, C. Allen, D. Deavours, and E. Perrins, "Diversity aspects of radar-embedded communications," in *Int. Conf. Electromagnetics in Advanced Applicat., 2007. ICEAA 2007.*, Sep. 2007, pp. 439–442.

[10] S. D. Blunt and C. R. Biggs, "Practical considerations for intra-pulse radar-embedded communications," in *2009 Int. Waveform Diversity and Design Conf.*, Feb. 2009, pp. 244–248.

[11] S. D. Blunt and J. G. Metcalf, "Using time reversal of multipath for intra-pulse radar-embedded communications," in *2010 Int. Waveform Diversity and Design Conf.*, Aug. 2010, pp. 000 155–000 158.

[12] G. Meager, R. A. Romero, and Z. Staples, "Estimation and cancellation of high powered radar interference for communication signal collection," in *2016 IEEE Radar Conference (RadarConf)*, May 2016, pp. 1–4.

[13] P. Welch, "The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms," *IEEE Trans. Audio Electroacoust.*, vol. 15, no. 2, pp. 70–73, Jun. 1967.