Physical-layer Cyberattack Resilient OFDM Automotive Radars

Onur Toker*, and Ozgur Ozdemir†
* Dept. of ECE, Florida Polytechnic University, Lakeland FL, USA
† Dept. of ECE, North Carolina State University, Raleigh NC, USA
otoker@floridapoly.edu, oozdemi@ncsu.edu

2020 IEEE Vehicular Networking Conference (VNC) | 978-1-7281-9221-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/VNC51378.2020.9318366

***Abstract*—In this paper, we present a physical-layer cyberattack resilient OFDM radar design for automotive applications. A typical FMCW radar system sends multiple chirp signals in a coherent processing interval, whereas an OFDM radar sends multiple OFDM frames [1]. OFDM radar approach has a potential advantage for automotive applications, which is the use same RF hardware and bandwidth for both AV radar and V2V/V2X communication [2]. Cyberattack resilience of FMCW radars has been studied in [3], [4], [5], [6], in this paper we address the same problem for OFDM radars, propose a new radar algorithm called OFDM-i, and a cyberattack detector D_1. The proposed idea is based on selecting a fixed percentage of subcarriers as null, and changing these null bands randomly for each frame. To minimize the impact of this on range resolution, we also require no more than two neighboring null bands in each frame. We demonstrate the performance of OFDM-i both by using simulations, and then using real data obtained from a National Instruments 39 GHz mmwave system. We also provide an upper bound for the false cyberattack alarm rate, study the resilience of the proposed system using a combinatorial analysis, and then using simulated attacks. Finally, we summarize possible future research directions.**

I. Introduction

Automotive radars are gaining increasing importance for advanced driver assistance systems (ADAS) and autonomous vehicle (AV) applications [7]. Although frequency modulated continuous wave (FMCW) architecture is quite popular compared to other radar architectures, orthogonal frequency division multiplexing (OFDM) radars offer joint radar and communication capability [8], [9], [2]. OFDM radar algorithms and joint radar-communication methods have been studied by multiple different researchers, see [10], [11], [12], [1], and [13], [2], [14].

Physical-layer cyberattacks is an important problem for automotive radars [3], [4]. Cyberattack resilient FMCW designs has been studied [5], [6], and in this paper we extend these results for OFDM radars. The high level block diagram given in Fig. 1 summarizes the problem setup considered in this paper. We have an M dimensional complex (I/Q) vector which is converted to an N dimensional vector by inserting zeros at randomly selected positions. Although two neighboring zeros are allowed, three or more neighboring zeros are not allowed in the proposed algorithm to limit effects of interpolation on radar performance. After this point, we have the standard N subcarrier OFDM modulator on the transmit (TX) side, and demodulator on the receive (RX) side. The n and a before the OFDM demodulator represents the noise, and equivalent attack signal.

This work has been supported in part by NASA under the Federal Award ID number NNX17AJ94A, NSF grant 1919855, Advanced Mobility Institute grants GR-2000028, GR2000027, and the Florida Polytechnic University grant GR-1900022.

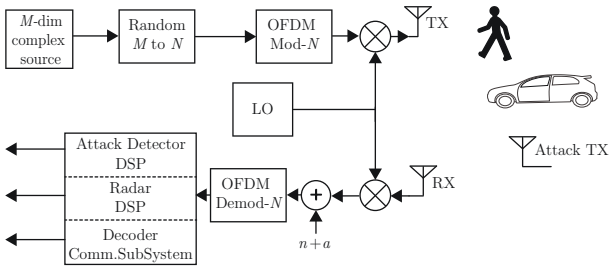

Fig. 1. System block diagram of the proposed attack resilient OFDM radar.

In this paper, we propose an Attack Detector DSP block, i.e. a detector D_1 and study its basic properties. We also propose a simple Radar DSP block based on the OFDM-i algorithm and analyze its performance using both simulations and experimental data. However, the communication subsystem and all associated problems including frame detection/synchronization, and communication protocols are not addressed.

This paper is organized as follows: In Section II we present mathematical preliminaries, and in Section III introduce the attack detector D_1, and summarize the proposed OFDM-i algorithm, the attack detector D_1. Simulation results are presented, in Section IV, real measurements are presented in Section V, and concluding remarks are made in Section VI.

II. Mathematical Preliminaries

In this section, we will summarize our mathematical notation and review some preliminaries from [15] and [1]. The overall system from the TX to the RX is modelled a transfer function

$$H(s) = \sum_q a_q e^{-h_q s} L_q(s),$$

where each term in the summation represents a reflector in the environment with a_q's are complex scalars, and $L_q(s)$'s are band-pass centered around f_c. The RF subsystem, EM properties of the environment, and the antennas define the filters $L_q(s)$. In the following, the radar problem will be reduced to the estimation of the impulse response of the baseband transfer function $H_b(s)$, or its discretized version.

Consider the system defined in Fig. 2 with local oscillator (LO) frequency f_c, and complex baseband signals in the frequency range $[-B, B]$. For the radar component of the joint radar-communication problem, both RX and TX antennas will be on the same vehicle, received echos of the transmitted signals (OFDM symbols) will be used for radar, and local oscillator will be shared between RX and TX. For a complex baseband signal, $s_b(t)$,

978-1-7281-9221-5/20/$31.00 ©2020 IEEE

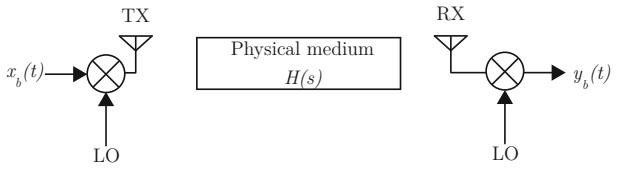

Fig. 2. The physical medium has transfer function $H(s)$, and the LO frequency is f_c.

band limited to $[-B, B]$ with $B < f_c$, the passband version, $s(t)$, will be $s(t) = \sqrt{2}\mathrm{Re}\left(s_b(t)e^{j2\pi f_c t}\right)$. Fourier transforms of continuous time signals are denoted in capital letters, and we have the following equations for the baseband and passband signals,

$$S_b(f) = \sqrt{2}S^+(f + f_c), \quad S(f) = \frac{S_b(f - f_c) + S_b^*(-f - f_c)}{\sqrt{2}},$$

where $S^+(f) = S(f)I_{\mathbb{R}^+}$, and $I_{\mathbb{R}^+}$ is the characteristic function of the set $\mathbb{R}^+$, see [15]. For the system shown in Fig. 2, with $x_b(t)$ as the input and $y_b(t)$ as the output, we have

$$Y(f) = H(f)X(f), \quad Y_b(f) = \frac{1}{\sqrt{2}}H_b(f)X_b(f).$$

For a given complex baseband signal, $s_b(t)$, we will also define a (complex) discrete time signal, $s_d[n] = s_b(nT)$, where T is the sampling period equal to $1/(2B)$.

If we assume that $L_q(s) = 1$, we will have

$$H_b(s) = \sum_q e^{-j2\pi f_c h_q}\sqrt{2}\ a_q\ e^{-h_q s}.$$

If the digital to analog converter subsystem of the transmitter is using the sinc interpolator, then for the input $x_d[n] = \delta[n]$, we will have $x_b(t) = \mathrm{sinc}(t/T)$, where $T = 1/(2B)$, and

$$y_b(t) = \sum_q e^{-j2\pi f_c h_q} a_q\ \mathrm{sinc}((t - h_q)/T).$$

If we simply look at the sampled version, $y_d[n] = y_b(nT)$, can we detect all reflectors, and estimate their radar cross section simply from this discrete-time impulse response? For $H(s) = e^{-h_q s}$, we expect $y_d[n] \approx \delta[n - n_o]$ where $n_o \approx h_q/T$ but depending on the exact value of the ratio, h_q/T, $y_d[n]$ may have a very small main lobe, and much smaller side lobes. Sampling $r_b(t) = y_b(t - T/2) + y_b(t + T/2)$ or sampling at a higher rate may be used to mitigate this problem.

A detailed discussion of performance metrics of OFDM radars, range/velocity resolution, and maximum unambiguous range/velocity is available in [1].

III. Proposed Method and Mathematical Analysis

In this section, we define the proposed OFDM-i algorithm for a single coherent processing interval (CPI). Here N represents the total number of available subcarriers, M is the number of complex I/Q data available for each symbol, and pN is the number of intentionally unused subcarriers. In a single CPI, we have N_r symbols, CFR stands for channel frequency response, and CIR is the channel impulse response.

Algorithm 1: OFDM-i Radar Algorithm

Input: $0 < p \ll 1$, and $M \times N$ complex I/Q data
Result: Range-velocity heatmap for a CPI

Set $X = [\ ]$;
for ($i = 0;\ i < N_r;\ i = i + 1$) {
  Among the available subcarriers, select randomly pN of them as extra null carriers, subject to no more than two neighboring unused subcarriers;
  Generate the OFDM symbol and transmit;
  Use the received OFDM symbol for channel estimation, and interpolate at null carriers;
  Estimate complex baseband CIR from baseband CFR;
  Write the estimated complex baseband CIR as the last row of X; }
Compute 1D-FFT of columns of X;
Optional thresholding, background subtraction. Display the absolute value in a colormap.

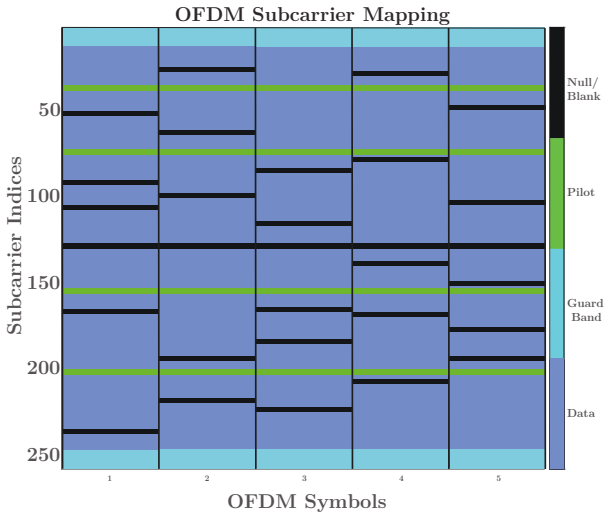

Fig. 3. For each OFDM symbol, randomly selected fixed number of subcarriers are not used, and no more than two neighboring unused subcarriers are allowed.

A. Combinatorial Bounds

In this subsection, we derive a lower bound for the number of possible combinatorial cases with each OFDM symbol having pN unused subcarriers with no more than two neigboring unused carriers. The lower bound is proved to be a large value, which implies that for an adversarial agent it is very difficult to generate a nonzero signal which will avoid the same ununsed subcarriers.

Consider N subcarriers, and divide them into pN groups of size $1/p$. Here we implicitly assume that $1/p \in \mathbb{Z}$, and $pN \in \mathbb{Z}$,. If these conditions are not satisfied, then the analysis presented here will still give some idea but the results will be approximate. For each group of size $1/p$, if the group does not have the DC subcarrier we can select a single unused subcarrier in $1/p$ ways. Therefore, total number of configurations with pN unused subcarrier with maximum two neigboring unused subcarriers will be at least

$$N_C \geq \left(\frac{1}{p}\right)^{pN-1}.$$

For $p = 0.1$, and $N = 256$, we have $N_C \geq 10^{0.1N-1} \geq 10^{24}$, and for $p = 0.05$, and $N = 256$, we have $N_C \geq 20^{0.05N_o-1} \geq$

10^{15}. Therefore N_C is a large number, and hence suggests strong cyberattack resilience of the OFDM-i algorithm.

B. False Cyberattack Alarm Rate

In this subsection, we define an attack detector and derive an upper bound for its false cyberattack alarm rate. Consider a random variable $Y = \sum_{m=0}^{q-1} y_m^2$ with y_m's i.i.d. $N(0,1)$ random variables. The Chernoff bound [16] implies that

$$Pr(Y \geq a) \leq e^{-sa} M_Y(s), \quad \text{for} \quad s \in (0, 1/2)$$

where $M_Y(s) = (1-2s)^{-q/2}$ is the moment generating function of Y. For a given $s \in (0,1/2)$, let $z = 1/(1-2s)$ and $a = zq$. The Chernoff bound implies

$$Pr\left(\sum_{m=0}^{q-1} y_m^2 \geq zq\right) \leq z^{q/2} e^{(1-z)q/2},$$

and for $z = 1.5$,

$$Pr\left(\frac{1}{q}\sum_{m=0}^{q-1} y_m^2 \geq 1.5\right) \leq 10^{-q/21.16}.$$

Let y_m's be the real and imaginary parts of the OFDM demodulator at unused subcarriers. We assume that they are i.i.d. $N(0,\sigma^2)$ when there is no cyberattack. We now define the cyberattack detector

$$D_1 = \frac{1}{\sigma^2}\frac{1}{N_r}\sum_{\ell=0}^{N_r-1}\sum_{k \text{ ununsed}} pP_{k,\ell},$$

where $P_{k,l}$ is the measured power of the k^{th} subcarrier for the ℓ^{th} OFDM symbol. Note that, this detector is defined for a single CPI and is equal to the average power for the pN_rN ununsed subcarriers for N_r OFDM symbols, normalized to σ^2. Using the Chernoff bound analysis given in the previous paragraph, the probability that this detector exceeds 1.5 when there is no cyberattack is really small;

$$P_F = Pr(D_1 \geq 1.5 \mid \text{no cyberattack}) \leq 10^{-2pN_rN_O/21.16}.$$

As a numerical example, consider $N_r = 128$, $N = 256$, and $p = 0.05$. We have 256 subcarriers, only 5% of the randomly selected subcarriers are intentionally unused for each OFDM symbol, there are 128 OFDM symbols in a CPI, and

$$P_F \leq 10^{-100},$$

which is an extremely small probability. This suggests that even a smaller threshold can be used as a cyberattack detector. Selection of different thresholds and simulation/experiment based tests are considered as future research.

IV. Simulation Results

In this section, we present simulation results for a 39 GHz radar system with $B = 600$ MHz bandwidth. The simulated environment has a single object (reflector) at location 35 m with velocity 1 m/s, all with respect to the x-axis.

The following two different radar systems are simulated and their outputs are compared:

- FMCW radar with chirp bandwidth equal to B,
- OFDM transmitter/receiver using bandwidth B with 5% of the subcarriers randomly selected and intentionally not used.

There are total 400 subcarriers, $N_r = 64$ chirps or OFDM symbols are simulated in a single coherent processing interval, and coherent processing duration is selected as $T_c = 1/25$ s. The baseband channel is modeled as a continuous time system with transfer function

$$H(s) = \frac{2}{(as)^2 + 1.5(as) + 1}\sum_q e^{-h_q s}$$

where $a = 8 \times 10^{-9}$, h_q is the round trip delay for the q^{th} object. During the simulation, the baseband equivalent $H_b(s)$ is recomputed before each chirp or OFDM symbol is applied to the channel. The second order low-pass filter is added to capture the effects of reflection from large surfaces and the spread in round trip delays.

In Fig. 4, we present comparison of range profiles computed using FMCW and OFDM-i when there is no cyberattack. As it is

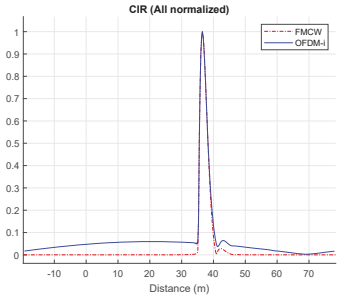

Fig. 4. (Simulation) Comparison of FMCW and OFDM-i radar methods when there is no cyberattack.

clear from this figure, both range profiles obtained using FMCW and OFDM-i are quite similar.

For the rest of the simulations, we set SNR = 15 dB, and use the received signal for an object at 15 m with velocity -1 m/s as the cyberattack signal. This signal is scaled by `asf` (attack scaling factor), and added to the mixer output on the receiver side to simulate cyberattacks, see Fig. 1. In Fig. 5, the range-velocity heatmap for a simulated cyberattack is shown. As it is clear from this figure, the cyberattack signal results an increased background noise, and this effect is more noticeable for larger `asf` values.

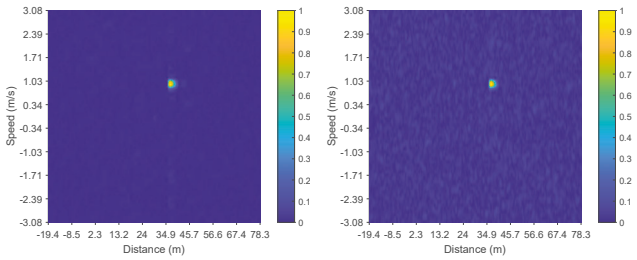

Fig. 5. (Simulation) OFDM-i radar range-velocity heatmap for a simulated cyberattack. On the left, `asf=0.1` (weaker cyberattack), and on the right `asf=1.0` (stronger cyberattack).

We now consider the cyberattack detection performance. For each OFDM symbol, the receiver computes the power of the received signal at ununsed subcarriers. In Fig. 6, these are given in (unnormalized form) for each symbol sent during a coherent

processing interval. It is clear from these figures that, when there is no cyberattack, i.e. `asf=0.0`, the detector values are around 0.3. On the other hand, when there is a simulated weak cyberattack with `asf=0.1`, then the detector values fluctuate around 1. Note that, for `asf=0.1`, the effect of the cyberattack signal results almost no noticeable effect on the range-velocity heatmap, see Fig. 5. Therefore, computing the average power

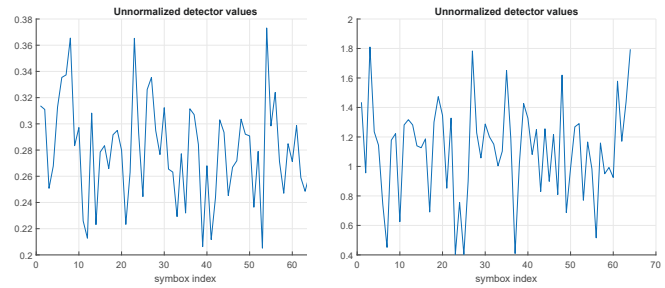

Fig. 6. Simulation) Unnormalized detector values vs symbol index. On the left, `asf=0.0` (no cyberattack), and on the right `asf=0.1` (weak cyberattack).

of ununsed subcarriers for a single coherent processing interval, and comparing this average with a threshold, can be used as a cyberattack detector. This threshold can be determined experimentally, and for this simulated experiment, a threshold value of 1 seems like a reasoanable choice. Lower thresholds will result more false cyberattack alarms, and higher ones will result less sensitive cyberattack detectors. The overall design objective is to select a threshold which will result a low P_F but will detect cyberttacks before they start to result a noticeable effect on the range-velocity heatmap. This threshold of 1 is about three times higher than the detector output when there is no cyberattack, hence P_F is expected to be low (Further simulations are required to estimate P_F). Yet, it will be a highly effective cyberattack detector because it will detect cases similar to the ones shown on the left hand-side of Fig. 5.

V. Experimental Results

In this section, we present experimental results obtained using a 39 GHz National Instruments mmwave system. For this experiment, we have used 256 OFDM subcarriers with a total of 600 MHz bandwidth. For the sake of simplicity, and since our focus is on radar, we used no guardbands, and no pilot frequencies. For the OFDM radar the DC subcarrier is not used, and for the OFDM-i radar DC subcarrier plus 10% of the 256 available subcarriers are not used. All unused subcarriers are selected randomly for each OFDM symbol, and the baseband channel frequency response at unused subcarriers are interpolated using available data. Authors used MATLAB's `interp1` method to (1) interpolate complex baseband CFR values directly, and then (2) to interpolate real magnitude and unwrapped phase values, and observed little difference in between. Higher order interpolation methods are not tested. As it is clear from Fig. 7, range profiles obtained using OFDM and OFDM-i seem to be almost the same.

VI. Conclusion

In this paper, we have proposed a cyberattack resilient modified OFDM radar algorithm, and studied its detection performance and cyberattack resilience. Both simulations and experimental data suggest that the proposed algorithm performs as good as

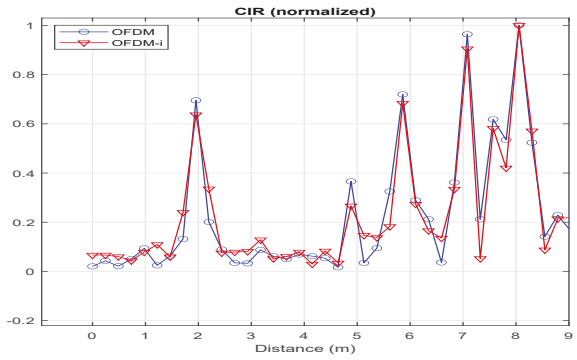

Fig. 7. (Real data) Comparison of OFDM and OFDM-i radars algorithms. Test equipment is 39 GHz National Instruments mmwave system.

standard FMCW and OFDM algorithms. Cyberattack resilience is studied first from a mathematical perspective, and an upper bound is derived for the false cyberattack alarm rate, and a lower bound is derived for the number possible combinatorial cases. Simulated attacks are also used to demonstrate the effectiveness of the proposed cyberattack detector. It has been observed that even "low" power cyberattacks will be detected well before a noticeable degradation in the range-velocity heatmap.

References

[1] M. Braun, "Ofdm radar algorithms in mobile communication networks," Ph.D. dissertation, Karlsruher Instituts für Technologie, 2014.
[2] C. D. Ozkaptan, E. Ekici, and O. Altintas, "Demo: A software-defined ofdm radar for joint automotive radar and communication systems," in *2019 IEEE Vehicular Networking Conference (VNC)*, 2019, pp. 1–2.
[3] C. Bhat, "Cybersecurity challenges and pathways in the context of connected vehicle systems," Data-Supported Transportation Operations & Planning Center (D-STOP), Austin, TX, Tech. Rep. 134, Feb. 2018.
[4] S. Alland, W. Stark, M. Ali, and M. Hegde, "Interference in Automotive Radar Systems: Characteristics, Mitigation Techniques, and Current and Future Research," *IEEE Signal Proc. Mag.*, vol. 36, pp. 45–59, Sep. 2019.
[5] O. Toker, S. Alsweiss, J. Vargas, and R. Razdan, "Design of an Automotive Radar Sensor Firmware Resilient to Cyberattacks," in *Proceedings of the 2020 IEEE SoutheastCon*, Raleigh, NC, 2020.
[6] O. Toker and S. Alsweiss, "Design of a Cyberattack Resilient 77 GHz Automotive Radar Sensor," *MDPI, Electronics*, 2020.
[7] S. M. Patole, M. Torlak, D. Wang, and M. Ali, "Automotive radars: A review of signal processing techniques," *IEEE Signal Proc. Mag.*, vol. 34, pp. 22–35, Mar. 2017.
[8] D. Garmatyuk and K. Kauffman, "Radar and data communication fusion with uwb-ofdm software-defined system," in *2009 IEEE International Conference on Ultra-Wideband*, 2009, pp. 454–458.
[9] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1236–1259, 2011.
[10] N. Levanon, "Multifrequency radar signals," in *The Record of the IEEE 2000 International Radar Conference*, 2000, pp. 683–688.
[11] G. E. A. Franken, H. Nikookar, and P. van Genderen, "Doppler tolerance of ofdm coded radar signals," in *Proc. 3rd European Radar Conference*, 2006.
[12] B. Donnet and I. Longstaff, "Combining mimo radar with ofdm communications," in *3rd European Radar Conference (EuRAD 2006)*, 2006.
[13] C. D. Ozkaptan, E. Ekici, O. Altintas, and C. Wang, "Ofdm pilot-based radar for joint vehicular communication and radar systems," in *2018 IEEE Vehicular Networking Conference (VNC)*, 2018, pp. 1–8.
[14] C. D. Ozkaptan, E. Ekici, and O. Altintas, "Enabling communication via automotive radars: An adaptive joint waveform design approach," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. IEEE Press, 2020, p. 1409–1418.
[15] U. Madhow, *Fundamentals of Digital Communication*. Cambridge University Press, 2008.
[16] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*. Dover Publications, 1965.