Design of an Automotive Radar Sensor Firmware Resilient to Cyberattacks

Onur Toker
Advanced Mobility Institute
Florida Polytechnic University
Lakeland, FL 33805
otoker@floridapoly.edu

Suleiman Alsweiss
Advanced Mobility Institute
Florida Polytechnic University
Lakeland, FL 33805
salsweiss@floridapoly.edu

Jorge Vargas
Advanced Mobility Institute
Florida Polytechnic University
Lakeland, FL 33805
jvargas@floridapoly.edu

Rahul Razdan
Advanced Mobility Institute
Florida Polytechnic University
Lakeland, FL 33805
rrazdan@floridapoly.edu

***Abstract*—In this paper, we introduce a novel automotive radar sensor design resilient to cyberattacks. The proposed design can be implemented at the firmware level of the system which provides faster detection of cyberattacks without adding hardware complexity or being computationally expensive. This approach can be combined with any predictive filtering based approach implemented at higher system layers to provide additional security. Frequency modulated continuous wave (FMCW) radar is chosen to demonstrate the efficiency of the design in preventing cyberattacks as will be demonstrated by simulation results.**

***Index Terms*—Automotive radar sensors, Cybersecurity, Physical Layer, Sensor Firmware.**

I. Introduction

Over the last decade, the automotive industry has evolved to include various levels of connectivity and autonomy in vehicles. This fundamental transformation is supported by multitude of advancements in electronic, communication, and remote sensing technologies, to increase efficiency and improve safety and reliability.

However, these advancements are usually accompanied by new challenges to both researchers and the industry. One challenge that has been front and center when talking about connected and autonomous vehicles (CAV) is cybersecurity [2]. It can come in the form of passive attacks attempting to listen to the information received by the sensor, or active attacks where unknown communication sources, in disguise, try to spoof the sensor [2].

In this paper, we will specifically address the issue of cyberattacks related to radar sensors utilized by CAVs for object detection and ranging. Of special interest to the automotive industry are the Frequency Modulated Continuous Wave (FMCW) radar systems. Although there exist several radar systems that can provide higher immunity to cyberattacks, the relatively simple RF front-end, and low cost of FMCW radar makes them ideal for the task at hand, and partially justifies the research direction adopted in this paper. Thus, the main question we are trying to answer here is how to improve the resiliency of FMCW radars to cyberattacks, and hence combine the best of two worlds, simplicity and resilience.

978-1-7281-6861-6/20/$31.00 ©2020 IEEE

Our approach to the solution is to study the cybersecurity problem close to the physical layer where all signals are analog, all measurements are noisy, and different energy levels of signals can provide different information. This is quite different compared to cyberattack detectors defined at higher levels of the AV system. There are numerous papers using model based prediction filters, including Kalman, and artificial intelligence (AI) based estimation techniques. A common idea in most of these papers is to "compare" the received sensor data and a prediction filter output. Depending on how the comparison is done, and prediction filter is constructed, different cyberattack detectors can be constructed. See [13] and the references therein for Kalman filtering centered techniques.

The techniques used in this paper are similar to the main ideas introduced in [3], [4]. In this paper, we will define a series of detectors, and a single threshold value, η, to detect cyberattacks. First, we will define the mathematical model (attack model), and then use simulations to demonstrate the effectiveness of the proposed method. In an ideal cyberattack detector, we would like to have both the probability of false alarm (P_F), and the probability of miss (P_M) equal to zero. Our design objective will be choosing the threshold value, η, according to the optimization problem,

$$\min_{\eta} \max\{P_F(\eta), P_M(\eta)\}.$$

By using simulation results, we will experimentally compute $P_F(\eta)$, and $P_M(\eta)$, for various cyberattack signal levels. It will be demonstrated that, for "weak" cyberattacks, $P_F(\eta)$, and $P_M(\eta)$, curves will have significant overlap. Here "weak" cyberattack means, the root means square (RMS) value of the cyberattack signal is small compared to the root mean square value of the noise. In other words, the signal level is interpreted as the RMS value, and being "weak" is interpreted as being small compared to the noise in the RMS sense. For stronger cyberattacks, we observe smaller overlap between $P_F(\eta)$, and $P_M(\eta)$, and finally after some point, we observe no overlap between $P_F(\eta)$, and $P_M(\eta)$. However, simulation based computation/estimation of very small probabilities, e.g. probabilities like 10^{-10}, is not a simple task. Not observing an overlap between $P_F(\eta)$, and $P_M(\eta)$ simply means the following: Despite the large number of simulated attacks, there

is a range of η values for which detectors neither triggered a false cyberattack alarm, nor missed an actual cyberattack. In summary, simulation results show that for $\eta = 1.5$, no false alarm is observed, and all cyberattacks which have attack signal level a couple of times (3-to-5 times) of the noise level (or larger) are always detected. Again, this does not mean $P_F = 0$, and $P_M = 0$, it only means we were unable to generate even a single false alarm or miss despite the large number of simulated cases. In summary, these results do demonstrate the effectiveness of the proposed methods.

If the cyberattack signal level is less than 3-to-5 times the noise level, then the probability of miss could be higher. However, these lower signal level (weaker) attacks will have only limited effect on the AV radar system, and can safely be ignored for most cases. An important conclusion from this simulation based analysis is the following: An AV radar system with lower noise level is more effective in detecting even weaker cyberattacks. Normally, even if there is no cyberattack possibility, a poorly designed higher noise level AV radars will have poor target detection, and range estimation performance, and hence should be avoided in AVs. On the other hand, given a low noise AV radar system, the proposed method will result an AV radar system with high cyberattack resilience and good detection/ranging performance.

The remainder of this paper is organized as follows: In Section 2, we review basic FMCW radar equations, and in Section 3, Texas Instruments' (TI) 77 GHz automotive radar system is introduced. In Section 4, core ideas of this paper are presented together with our mathematical model, and in Section 5, detector design and simulation results presented. Finally, in Section 6, we make some concluding remarks and summarize possible future research directions.

II. Review of FMCW radar equations

Compared to pulsed radars, FMCW radars can be built with simpler and lower cost components. In a FMCW radar system, there can be one or multiple transmit and receive antennas. This multi-input/multi-output (MIMO) architecture can be used for beam forming and direction finding. Regardless of the number of antennas, FMCW radar system has a voltage controlled oscillator (VCO) with output frequency depending on the input voltage. Normally this relationship is nonlinear, and multiple techniques exist to mitigate this problem. In the following simplified analysis, we will consider single transmit, single receive antenna architecture, and linear VCO model, and assume that one of the known non-linearity correction methods are already implemented, see [9]–[11] and references therein for details.

The transmitted signal $S_T(t)$ can be mathematically represented as:

$$S_T(t) = A(t)\cos\left(2\pi\int_0^t f_T(v_{in}(q))dq + \theta_t\right)$$

where θ_t is a constant representing the original phase of the transmitted signal, $A(t)$ is a low pass filtered signal representing the VCO output amplitude, f_T is the frequency of the transmitted signal that is a function of the VCO control input voltage v_{in}. As stated earlier, we assume that one of the known VCO non-linearity correction methods is already implemented, and $f_T(v_{in}) = f_0 + B(v_{in}/v_{max})$, where f_0 is the initial VCO frequency, v_{max} is the maximum control input voltage which corresponds to the maximum VCO frequency (f_{max}), and B is the VCO bandwidth ($f_{max} - f_0$). For an object at distance d from the radar, the signal round trip time will be $\tau = 2d/c$, and the received signal will be $S_R(t) = S_T(t-\tau)$, where c is the speed of light. After the echo signal is received by the radar antenna, and passed through the low noise amplifier (LNA), it is mixed (multiplied) by the transmit signal and the result is low pass filtered. The output of this low pass filter is called the beat signal, $S_b(t)$, and can be expressed as:

$$S_b(t) = A_b(t)\cos\left(2\pi f_T(v_{in}(t))\frac{2d(t)}{c} + \theta_b\right),$$

where θ_b is a constant, and $A_b(t)$ is the beat signal amplitude. If the VCO input is a positive saw-tooth like signal, $v_{in}(t) = (t/t_d)v_{max}$, $t \in [0, t_d]$, where t_d is the chirp duration, then the frequency of the beat signal will be

$$f_{b+} = \frac{2Bd}{t_d c} + \frac{2f_0 v_r}{c},$$

where d is the target distance, and v_r is the target velocity. If the VCO is driven by a triangular signal having both positive and negative sweeps, spectral analysis of the beat signal for positive and negative sweeps can be used to estimate the target distance and velocity. If multiple repeated chirps are generated, a 2D FFT based technique can be used to estimate both the target range and velocity. For sensors with multiple antennas, it is also possible to estimate the angular direction of the target. See [1] for a summary of more advanced data processing options.

In summary, FMCW radars estimate the target distance and velocity using spectral techniques. To improve the accuracy, multiple measurements and averaging techniques can be used as well.

III. Review of the 77GHz TI automotive radar

In this section, we review some of the basic configuration parameters of the TI AWR1642 automotive radar (See Fig. 1). AWR1642 is basically an FMCW radar operating at 77GHz with a maximum bandwidth of 4GHz. When used with the DCA1000 FPGA board, a single chirp will have $t_d = 160$ μs duration, which is repeated $N_r = 128$ times over a $T_m = 40$ ms time frame. During a single chirp, data is acquired only for 25.6 μs at a rate of 10 MHz.

Although the target distance can be estimated using only a single chirp, we process all of the N_r chirps together, and define T_m as the measurement duration. After N_r chirps of duration t_d, there will be a blank period (guard band) of a duration equals to $T_m - N_r t_d$ where no chirp signal is generated and no data is acquired. If there is no cyberattack, all of this data can be used for distance estimation.

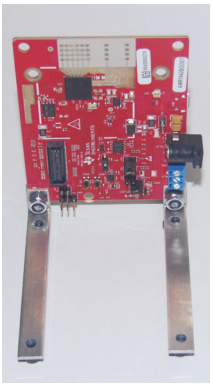

Figure 1. 77GHz Texas Instruments AWR1642 automotive radar.

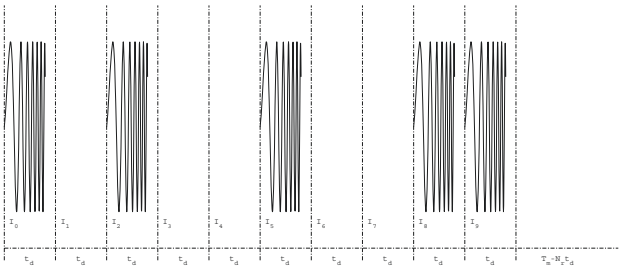

Figure 2. Measurement cycle of an AV radar for $N_r = 10$.

IV. Mathematical Model

In this section, we review our mathematical model. We have an AV radar with N_{TX} transmit antennas, and N_{RX} receive antennas. Multiple transmit antennas can be useful for beamforming, but for mathematical modelling purposes, they can be viewed as a single physical or virtual antenna with a specific radiation pattern.

The AV radar outputs a new measurement result in every T_m seconds, which is also called as the measurement cycle. Within a single measurement cycle, we have N_r nonoverlapping chirp windows $I_0, \cdots, I_{N_r-1}$, each of which having length t_d seconds. In each measurement cycle, we randomly select half of these intervals I_k, $k = 0, \cdots, N_r - 1$, and the transmitters are active only during these selected intervals (See Fig. 2). But, the data acqusition is done during every chirp interval I_k, and a total N_s samples are acquired from each receiver during a single I_k.

We define $\mathbb{Z}_{N_r}$ as the set $\{0, \cdots, N_r - 1\}$. The set of all such functions, $\rho : \mathbb{Z}_{N_r} \to \{0, 1\}$, will be denoted by $\{0, 1\}^{\mathbb{Z}_{N_r}}$. We call such functions (or binary sequences) as radar activation functions (or sequences). In our proposed design, the AV radar is operated according to the following procedure:

1. In every measurement cycle, a radar activation sequence $\rho \in \{0, 1\}^{\mathbb{Z}_{N_r}}$ is generated randomly.
2. The generated radar activation sequence, ρ, must have equal number of 0's and 1's.
3. Throughout the measurment cycle, the transmitter(s) will be active only during intervals I_k's with $\rho(k) = 1$.
4. Throughout the measurment cycle, data acqusition will be done during all I_k intervals.

In Fig. 2, a sample AV radar firing sequence is shown. There are $N_r = 10$ chirp windows, and half of them, I_0, I_2, I_5, I_8, I_9, are randomly selected for transmitter activation. A new random selection is made for each measurement cycle. Data acquisition is done during all of the chirp windows, $I_0, \cdots, I_9$, regardless of whether the transmitter is active or not.

We define "received data" as what is observed at the output of ADC's immediately after the low pass filters, i.e. after the received waveform goes through all of the RF and analog blocks. To illustrate the proposed approach in a simpler notation, we assume that only the in-phase components are digitized, and quadrature components do not exist. Furthermore, we also assume that there is only a single receive antenna. Extensions for in-phase + quadrature component based systems with multiple transmitter/receiver antennas is similar, and will be discussed later.

Note that, the "received data", i.e. the signal observed at the input of ADC's, is denoted by $R_k[m]$, where $k = 0, \cdots, N_r - 1$ is the index of the interval I_k, and $m = 0, \cdots, N_s - 1$ is the sample index. Therefore, our mathematical model is

$$R_k[m] = n_k[m] + \rho(k)x_k[m] + a_k[m],$$

where n_k is the noise term, x_k is the term representing reflections from objects, and a_k representing the attack signal. We assume that $n_k[m]$'s are all i.i.d. $N(0, \sigma_n)$. The term x_k is either independent of k, or has weak dependence on k, simply because t_d is too short for noticeable changes in the environment. Basically, the AV radar system knows ρ, but does not know $a_k[m]$'s. We assume that the attacking agent has full information about all of the details of the AV radar algorithm, except for the randomly generated radar activation sequence. Because of the rapid switching pattern of the AV radar, we assume that the attacking agent cannot determine the value of $\rho(k)$ while we are in the interval I_k.

For any signal, $s[m]$, defined for $m = 0, \cdots, N_s - 1$, we define the root mean square (RMS) value as

$$\|s\|_r := \sqrt{\frac{1}{N_s}\sum_{m=0}^{N_s-1} s^2[m]} = \frac{\|s\|_2}{\sqrt{N_s}},$$

where, $\|\cdot\|_2$, is the Euclidean norm, also known as the 2-norm.

V. Design of Detectors and Threshold Selection

In this section, we first define detectors, and then present simulation results. The motivation for our the detector design is easy to explain:

If there is no cyberattack, all received signals during which the transmitter is not active, is expected to have small RMS power. And all signals received when the transmitter is active, is expected to have similar RMS power. Any observation which is not consistent with these requirements is classified as a cyberattack.

However, a careful analysis of all details is necessary to demonstrate the effectiveness of the proposed method.

A. Detector Design

Consider a radar activation sequence $\rho \in \mathbb{Z}^{N_r}$. All of the detectors defined in this subsection depend on this activation sequence, ρ, however to simplify the notation this dependence is not shown explicitly. Ideally, an extra argument, or subscript can be added to indicate this dependence on ρ.

We define the detector D_0 as

$$D_0(k) = \frac{\|R_k\|_r}{\sigma_n}, \quad k = 0, \cdots, N_r - 1,$$

which measures the RMS value of the received signal during the chirp k relative to noise RMS level. We also define the detector D_1 as

$$D_1(k) = \frac{\mid \|R_k\|_r - \overline{R}_\rho \mid}{(\overline{R}_\rho + \sigma_n)}, \quad k = 0, \cdots, N_r - 1,$$

where $\overline{R}_\rho$ is the average of RMS level of all R_k's when the transmitter is active, i.e.

$$\overline{R}_\rho = \frac{1}{N_r/2} \sum_{\rho(k)=1} \|R_k\|_r.$$

We define the combo detector $D(k)$ as

$$D(k) = \begin{cases} D_0(k) & \text{if } \rho(k) = 0 \\ D_1(k) & \text{if } \rho(k) = 1 \end{cases},$$

for $k = 0, \cdots, N_r - 1$. Namely, we choose the detector D_0 when the transmitter is not active, and the detector D_1 when the transmitter is active. We also define

$$Q = \max_{k=0,\cdots,N_r-1} D(k),$$

and finally, the cyberattack detector $C(\eta)$, as

$$C(\eta) = \frac{1}{\eta} \max_{k=0,\cdots,N_r-1} D(k),$$

where η is a threshold, which will be later selected as $\eta \approx 1.5$ to minimize $\max\{P_F(\eta), P_M(\eta)\}$, i.e. maximum of false alarm and miss rates. However, different design objectives can be used as well. One very popular design objective is constant false alarm rate (CFAR) design, where η is chosen to set the false alarm rate to a fixed low value. Another very popular design is to choose η to minimize the sum $P_F(\eta) + P_M(\eta)$. As long as the design objective is decided, and we are able to generate $P_F(\eta), P_M(\eta)$ curves, optimal threshold can be selected, and false alarm and miss rates can be estimated.

In summary, our proposed cyberattack detection algorithm is simply

If $C(\eta) \geq 1$ then generate cyberattack alarm

where the recommended value for the threshold is $\eta \approx 1.5$. Justification for this selection will be explained after the simulation results.

The following is the algorithmic description of the proposed cyberattack resilient AV radar algorithm.

Algorithm 1 CARAV_RADAR(η, N_r, N_s)

1: Generate a random sequence of length N_r consisting of equal number of 0's and 1's. This sequence will be the radar activation sequence, ρ, and will be randomly generated for each measurement cycle.
2: For the current measurement cycle, operate the transmitter based on this randomly selected activation sequence ρ. Namely, for the chirp interval I_k, the transmitter will be active iff $\rho(k) = 1$. However, we collect N_s samples during each chirp interval I_k, regardless of transmitter activation status, and this will be our received signal, R_k.
3: Compute $\overline{R}_\rho$, i.e. the average of all received signals when the transmitter is active.
4: Compute $D_0(k), D_1(k)$'s for $k = 0, \cdots, N_r - 1$, then the combo detector D, and the cyberattack detector $C(\eta)$.
5: If $C(\eta) \geq 1$, then generate cyberattack alarm, and go to Step 1 to start the next measurement cycle.
6: Otherwise, process the received data for target detection and range estimation. For example, one may use popular spectral analysis algorithms (FFT peak location, MUSIC, etc) to process the received data.
7: Go to Step 1 to start the next measurement cycle.

B. Phased array toolbox of MATLAB

To simulate an AV radar system together with the proposed cyberattack detection algorithm, we used the phased array toolbox of MATLAB. The authors do not claim that this is the most accurate AV radar simulation platform, but it is one of the well-known options. Our focus will be on cyberattack detection, but not on how post processing is done.

We will first study the cyberattack detection using a particular propagation model, radiation pattern, vehicle radar cross section, target distance/velocity, etc. We call all of these parameters as physical parameters, i.e. everything except the threshold η, will be considered as physical parameters. We will first simulate the AV radar system with these typical physical parameters, generate curves for $P_F(\eta), P_M(\eta)$ for different cyberattack signal levels, and discuss "optimal" threshold selection for cyberattack resilience. Later, we will present additional simulation results when these physical parameters are modified. For all of the simulated cases, the threshold value of $\eta = 1.5$ results very good cyberattack resilience.

C. Typical physical parameters

Our first set of simulations are based on MATLAB's phase array toolbox example `phased/FMCWExample` (See Table I).

Table I
PHYSICAL PARAMETERS (MATLAB'S PHASE ARRAY TOOLBOX).

Parameter	Value
Sweeps/Cycle, N_r	64
Operating frequency	77 GHz
Sweep time	7.33 μs
Sweep bandwidth	150 MHz
Sample rate	150 MHz
Target distance	43 m
Target speed	96 km/h
Target radar cross section	100 m^2
Radar speed	100 km/h
Antenna, propogation and other RF parameters	See the `phased/FMCWExample` example of MATLAB

In our simulations, we selected the noise level, σ_n, for signal to noise ratio (SNR) to be equal to 0 dB. However, what effects the simulation results and false alarm/miss probabilities is the ratio of attack signal RMS, σ_a, to the noise RMS, σ_n. This ratio, σ_a/σ_n, is called the relative attack RMS (RARMS), and all results are reported using this ratio.

D. Analysis of random attacks

In this subsection, we simulate cyberattacks by using presudo-random number generators. In the next subsection, we will simulate "smarter" attacks to fool the detectors.

Basically, in this section $a_k[m]$'s are simulated as i.i.d. $N(0, \sigma_a)$. Simulation results are shown in Fig. 3. We see that, for RARMS $\geq$ 3, there is no detected overlap between P_F and P_M curves, and $\eta = 1.5$ separates these two with a "good" margin. Again, we cannot claim that our simulation results based on 1000 random cases estimate these probabilities with 100% accuracy. However, no matter how many times we tried to do the same simulation experiment, we have observed the same clear separation around the $\eta = 1.5$ line.

The proposed method works quite well for RARMS $\geq$ 3 (See Fig. 3). However for RARMS $<$ 3, the probability of miss can be quite high for the $C(2)$ detector. The proposed method ignores such less harmful attacks, because their negative effects will be comparable to the effects of noise. Basically, we can conclude that, all harmful attacks are detected by the $C(2)$ detector.

E. Analysis of "smart" attacks

In this subsection, we simulate another attack method. A smarter attack strategy to fool all of these detectors could be repeating the same attack sequence over all chirps. This may at least fool all $D_1(k)$ detectors. However, simulation results presented in Fig. 4 show that, for RARMS $\geq$ 3, $P_F(\eta)$ and $P_M(\eta)$ curves are still separated by the $\eta = 1.5$ line. In other words, all harmful attacks are still detected by the $C(1.5)$ detector. This type of attacks are smarter because miss rates are higher compared to previous case.

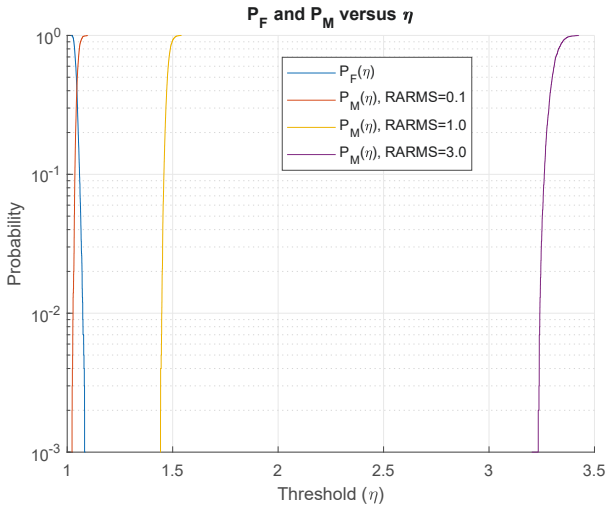

Figure 3. $P_F(\eta)$ and $P_M(\eta)$ curves for various RARMS values. For each curve, 1000 cases are simulated. For RARMS $\geq$ 3, we see no overlap between P_F and P_M curves.

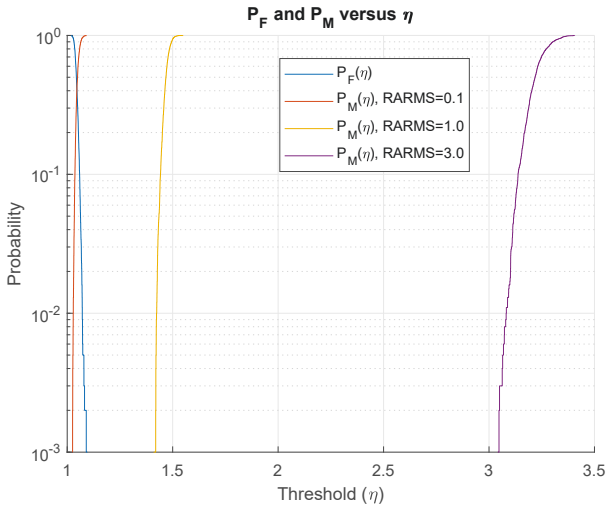

Figure 4. $P_F(\eta)$ and $P_M(\eta)$ curves for "smart" attacks.

Normally, we cannot claim that our simulation results based on 1000 random cases estimate probabilities with 100% accuracy. However, no matter how many times we tried to do the same simulation experiment, we have observed the same clear separation around the $\eta = 1.5$ line. Basically, we can conclude that, all harmful attacks are detected by the $C(1.5)$ detector.

F. Simulations with the Texas Instruments AWR1642 Radar

In this subsection, we present simulation results based on a different set of physical parameters given in Table II. There are two main differences: (1) We use Texas Instruments AWR1642 radar parameters, and (2) We have very high relative velocity. The probability curves given in Fig 5 show that, for RARMS $\geq$ 3, the $\eta = 1.5$ line separates $P_F(\eta)$ and $P_M(\eta)$ curves with a good margin. Basically, we again conclude that, all harmful attacks are detected by the $C(1.5)$ detector.

Table II
PHYSICAL PARAMETERS (TEXAS INSTRUMENTS AWR1642 RADAR).

Parameter	Value
Sweeps/Cycle, N_r	128
Operating frequency	77 GHz
Sweep time	25.6 μs
Sweep bandwidth	2000 MHz
Sample rate	10 MHz
Target distance	20 m
Target speed	-120 km/h
Target radar cross section	100 m^2
Radar speed	180 km/h
Antenna, propogation and other RF parameters	See the `phased/FMCWExample` example of MATLAB

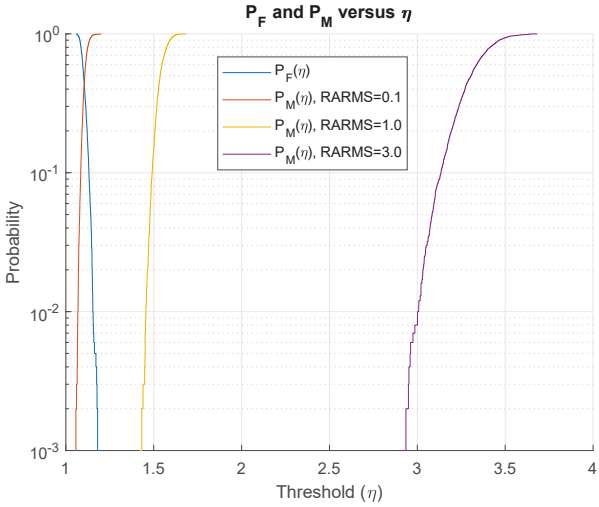

Figure 5. $P_F(\eta)$ and $P_M(\eta)$ curves for "smart" attacks. Alternative physical parameters given in Table II are used for simulations.

G. Cyberattack from a moving secondary antenna

In this subsection, instead of simulating $a_k[m]$'s as pseudo-random numbers, we consider a secondary antenna acting as an adversarial agent. Physical paramaters will be as in Table I, target distance will be 43 m, but we will add a secondary antenna moving at 50 km/h. Then, we will simulate three different cases, where the antenna transmit power is low, medium, and high. More precisely, simulate three cases where $P_F(\eta)$ and $P_M(\eta)$ curves overlap, very close but separate, and completely disjoint. For each case, we will plot range estimation error and Q values. Range estimation is done by using the MUSIC algorithm as in the MATLAB phased array toolbox example. In figures 6-8, on the left we have $P_F(\eta)$ and $P_M(\eta)$ curves, and on the right we have various simulated attacks with their Q and range estimation errors. All points below the $Q = 1.5$ line correspond to missed cyberattacks, and all points above this line correspond to detected cyberattacks.

- In Fig. 6, we have low transmit power cyberattacks. $P_F(\eta)$ and $P_M(\eta)$ curves overlap, and $C(1.5)$ detector will have very high miss rate. But all missed attacks are "harmless", i.e. result in small estimation error.

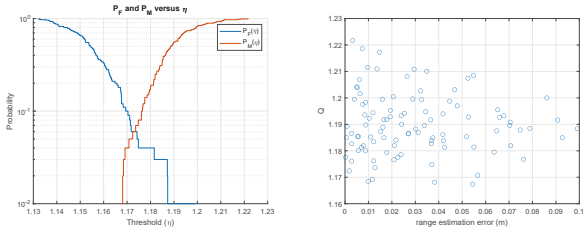

Figure 6. Low transmit power cyberattacks.

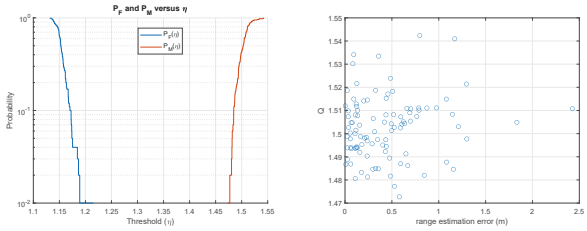

Figure 7. Medium transmit power cyberattacks.

- In Fig. 7, we have medium transmit power cyberattacks. $P_F(\eta)$ and $P_M(\eta)$ curves are separate but close. The $C(1.5)$ detector miss rate is around 40%. On the right, all points below the $Q = 1.5$ line correspond to missed cyberattacks, and all points above this line correspond to detected cyberattacks. We again see that all missed attacks are "harmless", i.e. result in small estimation error.
- In Fig. 8, we have high transmit power cyberattacks. $P_F(\eta)$ and $P_M(\eta)$ curves are completely disjoint. Most attacks are "harmful", i.e. result in large estimation error. But all cyberattacks are detected by the $C(1.5)$ detector.

H. Summary

These results show that, cyberattacks with relatively low signal strength will be difficult to detect, as they will look similar to measurement noise. However, harmful effects of such smaller cyberattacks will be comparable to the effects of noise itself. The authors have simulated various cases, and observed that

All harmful cyberattacks are detected by $C(1.5)$

In the cybersecurity literature, it is known that gradually increasing attacks are difficult to detect because they fool the

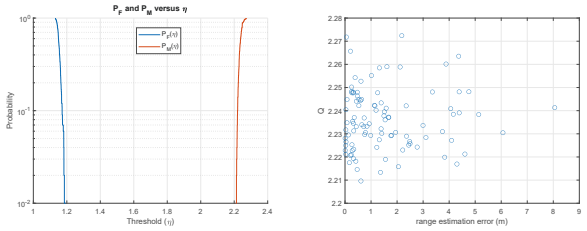

Figure 8. High transmit power cyberattacks.

detectors by keeping their rate of change small, indeed small enough so that none of the detectors trigger an alarm [12]. However, such systems are inherently unstable and accumulation of small errors cause gradual but sustained divergence to a dangerous portion of the state space. For AV radar systems, each measurement cycle is independently processed, and at the sensor level measurement errors do not accumulate.

The random sequence used in the proposed algorithm should be "truly" random. One may consider a linear feedback shift register (LFSR) based pseudo random binary sequences (PRBS) for simplicity, however there are reported techniques for predicting LFSR generated sequences [5]. Authors suggest a PUF based "true" random number generator as described in [6], [7].

VI. Conclusion

In this paper we presented a new firmware design for automotive radar systems that can increase resiliency against cyberattacks. The fact that this algorithm is mostly implemented near the physical layer provides agility and robustness which makes it suitable for the problem at hand. In addition, the main aspect of the proposed algorithm is that it makes use of the cyberattack signal RMS value as one of the parameters to be considered in the detection process. Depending on the operating frequency, bandwidth, chirp duration, ADC sampling frequency, and the inherent measurement noise of the RF subsystem, several of parameters have critical importance for the overall system performance. The authors used a simulation based analysis for estimation of false cyberattack alarm, and missed cyberattack probabilities. Using these simulation results an optimal threshold is selected. Basically, attack signals with weaker RMS values are harder to detect, but they also have smaller impact for post processing, target detection and estimation. As the cyberattack signal RMS value is increased, errors will get larger, but attack detection will also improve. After a certain level, simulations results show all attacks being detected. Basically, our design goal is to limit worst case effects of missed cyberattacks. A future version of this paper will have more in depth performance analysis of the algorithm including different cyberattack models, and characterization of sensor measurements errors during missed cyberattacks.

Acknowledgment

This work is supported Florida Polytechnic University, Advanced Mobility Institute (AMI), and National Science Foundation under Grant No. CNS-1919855. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Texas Instruments Training: Introduction to mmWave Sensing https://training.ti.com/intro-mmwave-sensing-fmcw-radars-module-1-range-estimation

[2] Chandra Bhat, "Cybersecurity Challenges and Pathways in the Context of Connected Vehicle Systems," Technical Report 134, Center for Transportation Research, February 2018.

[3] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Attack Resilience and Recovery using Physical Challenge Response Authentication for Active Sensors Under Integrity Attacks," arXiv:1605.02062v2 [cs.CR], 12 May 2016.

[4] P. Kapoor, A. Vora, K. D. Kang, "Detecting and Mitigating Spoofing Attack against an Automotive Radar," IEEE Vehicular Technology Conference, August 27 - 30, 2018, Chicago, USA.

[5] A. Peinado, and A. Ortiz, "Prediction of Sequences Generated by LFSR Using Back Propagation MLP," In: de la Puerta J. et al. (eds) International Joint Conference SOCO'14-CISIS'14-ICEUTE'14. Advances in Intelligent Systems and Computing, vol 299. Springer.

[6] C. W. O'Donnell, G. E. Suh, and S. Devadas, "PUF-Based Random Number Generation," MIT CSAIL CSG Technical Memo 481, Computer Science and Artificial Intelligence Laboratory (CSAIL), MIT.

[7] S. Buchovecka, R. Lorencz, F. Kodytek, and J. Bucek, "True random number generator based on ring oscillator PUF circuit," Microprocessors and Microsystems, Volume 53, August 2017, pp. 33-44.

[8] R. G. Dutta, X. Guo, T. Zhang, K. Kwiat, C. Kamhoua, L. Njilla, Y. Jin, "Estimation of safe sensor measurements of autonomous system under attack," 54th ACM/EDAC/IEEE Design Automation Conference (DAC), June 2017.

[9] M. Brinkmann, O. Toker, and S. Alsweiss, "Design of an FPGA/SoC Hardware Accelerator for MIT Coffee Can Radar Systems," IEEE SouthEastCon 2019, Huntsville, AL, April 2019.

[10] M. Brinkmann, "Design and Implementation of Improved Nonlinearity Correction Algorithms for FMCW Radar Sensors," M.S. Thesis, Florida Polytechnic University, Lakeland, FL 33805, August 2019.

[11] O. Toker, and M. Brinkmann, "A Novel Nonlinearity Correction Algorithm for FMCW Radar Systems for Optimal Range Accuracy and Improved Multitarget Detection Capability," MDPI Electronics, **2019**, 8(11):1290.

[12] Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Control Systems," First Workshop on Secure Control Systems, CPS Week, Stockholm, Sweden, Apr 13-14, 2010.

[13] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems," IEEE Transactions on Signal and Information Processing over Networks, **2018**, 4(1):125–136.