UPPSALA
UNIVERSITET

UPTEC F 23036
Examensarbete 30 hp
Juni 2023

Evaluation of FMCW Radar Jamming Sensitivity

Ludvig Snihs

Civilingenjörsprogrammet i teknisk fysik

UPPSALA
UNIVERSITET

Evaluation of FMCW Radar Jamming Sensitivity

Ludvig Snihs

Abstract

In this work, the interference sensitivity of an FMCW radar has been evaluated by studying the impact on a simulated detection chain. A commercially available FMCW radar was first characterized and its properties then laid the foundation for a simulation model implemented in Matlab. Different interference methods have been studied and a selection was made based on the results of previous research. One method aims to inject a sufficiently large amount of energy in the form of pulsed noise into the receiver. The second method aims to deceive the radar into seeing targets that do not actually exist by repeating the transmitted signal and thus giving the radar a false picture of its surroundings.

The results show that if it is possible to synchronize with the transmitted signal then repeater jamming can be effective in misleading the radar. In one scenario the false target even succeeded in hiding the real target by exploiting the Cell-Averaging CFAR detection algorithm. The results suggests that without some smart countermeasures the radar has no way of distinguishing a coherent repeater signal, but just how successful the repeater is in creating a deceptive environment is highly dependent on the detection algorithm used. Pulsed noise also managed to disrupt the radar and with a sufficiently high pulse repetition frequency the detector could not find any targets despite a simulated object in front of the radar. On the other hand, a rather significant effective radiated power level was required for the pulse train to achieve any meaningful effect on the radar, which may be due to an undersampled signal in the simulation. It is therefore difficult based on this work to draw any conclusions about how suitable pulsed noise is in a non-simulated interference context and what parameter values to use.

Teknisk-naturvetenskapliga fakulteten

Uppsala universitet, Utgivningsort Uppsala/Visby

Handledare: Patrik Lindström Ämnesgranskare: Mikael Sternad

Examinator: Tomas Nyberg

Sammanfattning

Frekvensmodulerad dopplerradar (Frequency-Modulated Continuous Wave radar, FMCW radar) är en vanligt förekommande millimetervåglängdsradar som med sin lätta vikt och låga energiförbrukning ser en ökad närvaro i sensorsammanhang. Genom att modulera frekvensen kan en utsänd signal på låg effekt pulskomprimeras vid mottagaren och på så vis åstadkomma en hög upplösning även i brusiga miljöer, samtidigt som andra system kan ha svårt att ens upptäcka radarns närvaro. Millimetervåglängdsradar får allt fler tillämpningsområden inom både det civila och militära, exempelvis inom utvecklingen av autonoma fordon. Eftersom radar kan verka under förhållanden där andra typer av sensorer är obrukbara så är det ur en säkerhetssynvinkel kritiskt att radarn fungerar vid till exempel kollisionsvarningar eller avståndshållning. Således är det utav intresse att studera och utvärdera hur känslig en generisk samt kommersiellt tillgänglig frekvensmodulerad dopplerradar är för avsiktlig störning och vilka etablerade störmetoder som är applicerbara.

I detta arbete har störkänsligheten hos en simulerad frekvensmodulerad dopplerradar utvärderats genom att studera påverkan på detektionskedjan. Detta gjordes genom att först karaktärisera en kommersiellt tillgänglig frekvensmodulerad dopplerradar och dess egenskaper lade sedan grunden till en simuleringsmodell implementerad i Matlab. Olika störmetoder har studerats och ett urval gjordes baserat på tidigare studiers resultat. Den ena metoden syftar till att injicera en tillräckligt stor mängd energi i form av pulsat brus i mottagaren så att detektion av objekt försvåras eller till och med omöjliggörs. Den andra metoden ämnar vilseleda radarn till att se mål som egentligen inte existerar genom upprepning av utsänd signal och på så vis ge radarn en missvisande bild av sin omgivning.

Resultatet visar att upprepningsstörning är effektivt i att vilseleda radarn ifall det är möjligt att synkronisera med den utsända signalen. Första scenariot placerade ett stationärt falskmål närmare radarn med en starkare signalstyrka än det riktiga ekot. Detta ledde till nästa scenario där ett falskmål placerades i närheten av objektet så att det riktiga målet lyckades döljas genom att utnyttja detektionsalgoritmen i Cell-Averaging CFAR. Resultatet tyder på att utan några smarta motåtgärder har radarn ingen möjlighet att skilja på en koherent upprepningssignal, men hur långt upprepningen kan nå i att skapa vilseledande miljöer är också starkt beroende på vilken detektionsalgoritm som används. Även pulsat brus lyckades störa radarn och med tillräckligt hög repetitionsfrekvens på pulserna kunde detektorn inte hitta några mål trots ett simulerat objekt framför radarn. Pulsstörningen visade också att bara en mindre mängd energi från störningarna följer med till hastighetsestimeringen, vilket antyder att radarn fortfarande skulle vara användbar för dopplermätningar fastän den aktivt blir utsatt för störning. Däremot krävdes något väl hög effekt för pulståget vilket kan bero på en undersamplad signal i simuleringen. Det är därför svårt att utifrån detta arbete dra någon slutsats om hur lämpligt pulsat brus är i ett riktigt störsammanhang och för vilka uteffekter.

Keywords: FMCW Radar, FMCW Jamming, Pulse Train, Spoofing Attack, Repeater, Automotive Radar, CFAR

Acknowledgements

I would like to express my gratitude to my advisor Patrik Lindström for his useful guidance provided throughout the thesis. The same goes with Sven Berglund and Francis Görmarker, since much of the work would not be possible without their support and aid with measurements. I would also like to thank my subject reviewer, Prof. Mikael Sternad at Uppsala University. Thanks should also go to Tomas Boman who constructed one of the Matlab scripts used in the directivity assessment.

Contents

Acronyms

ADC	Analog-to-Digital Converter.
AoA	Angle-of-Arrival.
BW	Bandwidth.
CUT	Cell Under Test.
DFT	Discrete Fourier Transform.
DRFM	Digital Radio Frequency Memory.
DSP	Digital Signal Processing.
ERP	Effective Radiated Power.
EW	Electronic Warfare.
FFT	Fast Fourier Transform.
FMCW	Frequency-Modulated Continuous Wave.
IF	Intermediate Frequency.
JSR	Jam-to-Signal Ratio.
LFM	Linear Frequency Modulation.
LPF	Low-Pass Filter.
LPI	Low-probability-of-intercept.
MIMO	Multiple-Input Multiple-Output.
PRF	Pulse Repetition Frequency.
RADAR	Radio Detection and Ranging.
RCS	Radar Cross-Section.
RF	Radio Frequency.
RX	Receiver Antenna.
SNR	Signal-to-Noise Ratio.
TX	Transmitter Antenna.

1 Introduction

1.1 Background

Robust sensors are a critical piece of the puzzle that must fit in order for fully autonomous vehicles to become a reality. The immense progress being made in the autonomous sector is fueling a development in which many sensors are becoming both cheaper and more readily available. Radar is a sensor which has many advantages over an image-based camera; a radar can see through fog, darkness, rain and smoke while being able to provide accurate distance and speed estimates. Radars have been used since the 1940s and the rapid technological development has allowed an entire radar system to fit in the palm of your hand. One type of radar that is becoming more commonly employed today is the Frequency-Modulated Continuous Wave radar. An FMCW radar may have several transmitter and receiver antennas operating simultaneously, allowing the system to measure angle of incidence as well as velocity, while the frequency modulation makes it possible to measure distance. The fact that the system works with low frequencies allows it to use cheap, stable electronic components making it a lucrative sensor in the context of autonomous vehicles. Moreover, since other sensors may become inoperable in certain conditions such as bad weather, the radar unit is a key safety component in e.g. self-driving cars. Thus, it is of interest to study and understand what types of intentional electronic attacks can significantly affect an FMCW radar which in turn paves the road for countermeasures to be developed.

There are a variety of ways to prevent a radar from working properly. One of these is interference, which means that the radar receives enough electromagnetic energy in its receiver antenna to hide real targets in noise when they would otherwise be visible to the system. There is both unintentional interference that can originate from nearby cell towers or other radars, but there is also intentional interference with the aim of hiding a target's exact position. Another angle of attack is deception, where an antagonist may actively transmit a signal that is supposed to mislead the radar in different ways. The deception can then cause e.g., an unmanned vehicle to draw incorrect conclusions which could be disastrous. In addition to autonomous vehicles, other platforms have use for FMCW radars, such as UAVs. Hence, there is an interest in being able to deny these platforms the use of the electromagnetic spectrum over unauthorized territory like airports.

1.2 Aim and Scope

This report aims to investigate which established jamming and deception methods could work to disrupt the functionality of an FMCW radar. This is initially done by studying previous literature and research carried out in this field. The literature study serves to aid in the selection of interference models and different scenarios that are to be applied on a principle model of a simulated FMCW radar in Matlab. Conclusions are then drawn about how applicable and to what extent the disturbances are in reality based on how the detection chain is affected.

1.3 Thesis Outline

This thesis begins by reviewing the basics of how FMCW radars works by presenting relevant mathematical equations and explaining how various parameters control specific characteristics of the system. A brief overview of detection algorithms and how CFAR works is also given. The theory part concludes by going through the very basics of electromagnetic jamming and deception, as well as mentioning a selection of previous research conducted in this area. Next, the characterization of a commercial off-the-shelf FMCW radar is presented as part of the method, which then lays the foundation for the Matlab model. Disturbance models are implemented in the simulation model and the results are evaluated by studying the different FFTs and range-Doppler maps to see how the performance of an FMCW radar is affected under certain conditions. The practicality of the results and its implications are then discussed to draw conclusion about their applicability in reality. Finally, suggestions are presented regarding future work on this topic.

2 Theory

2.1 Frequency-Modulated Continuous Wave Radar

Radar stands for Radio Detection and Ranging in which a transmitting antenna emits an electromagnetic signal and a receiving antenna listens for any echo, which may indicate a reflection and thus the presence of an object. There are two main families of radar, namely pulse and continuous wave radars. A frequency-modulated continuous wave radar is a variant of the latter type but with a frequency modulation, allowing it to determine range and velocity simultaneously. Additionally, multiple receiving antenna elements can be used to determine the angle of arrival with MIMO radars going even further by creating virtual antenna arrays to increase the performance of the system.

The FMCW radar can determine range and velocity by emitting a continuous transmission with a varying frequency. The frequency can both increase or decrease linearly, or use a custom frequency modulation. Usually the signal is modulated only for a short period of time whereupon it is reset back to the carrier frequency again. Each modulated transmission is commonly referred to as a *chirp* and lasts for a chirp period T_c. As will be shown, a single chirp is enough to determine distance but multiple consecutive chirps are required to assert the velocity of the target. Thus, multiple chirps span a time frame T_f. A common type of FMCW radar is Linear Frequency Modulated and typically has a carrier frequency f_c of around 24 GHz or 77 GHz. The transmitted LFM signal's frequency sweep covers a bandwidth BW and this span is key in shaping the properties of the radar. A typical LFM chirp sequence during a time frame is illustrated in Figure 1.

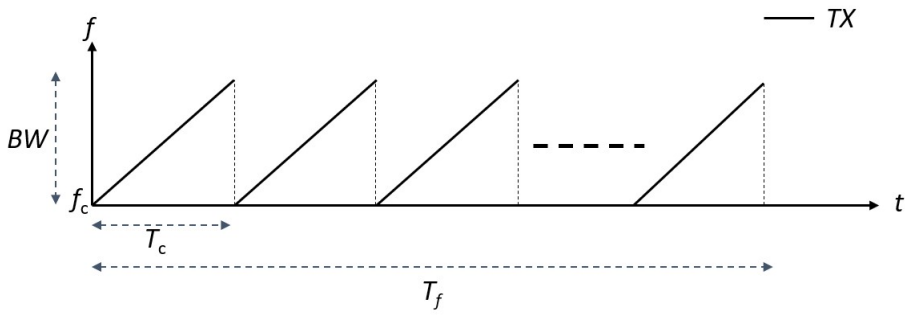


Figure 1: Shows a time-frequency representation of a LFM signal emitted by the transmitting antenna in an FMCW radar during a timeframe T_f.

The rate of the frequency modulation is the sweep rate S and is given by:

$$S = \frac{BW}{T_c} \tag{1}$$

The transmitted signal propagates until it diminishes due to signal losses or it reflects back off of something. The range of the transmitted signal can be described by the noise-including two-way radar range equation:

$$R = \sqrt[4]{\frac{P_t \cdot G^2 \cdot \lambda^2 \cdot \sigma \cdot T_f}{(4\pi)^3 \cdot SNR \cdot k \cdot T_e \cdot F \cdot L}} \tag{2}$$

where P_t is the peak transmitted power, G is the TX and RX antenna gain, λ is the carrier wavelength, σ is the radar cross section, T_f is the time frame, SNR is the signal-to-noise ratio, k is Boltzman's constant,

T_e is the effective noise temperature of the antenna, F is the noise figure, and L is the total losses due to attenuation [1]. One also sees that after some rearranging of equation 2 the received power at the RX antenna will be proportional to the inverse of the range to the power of four. If only the signal received at the RX antenna is of interest instead of the signal-to-noise ratio SNR, then the power received is obtained by [2]:

$$P_r = \frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 R^4} \tag{3}$$

As can be seen in equation 3 the power received at the RX antenna will also depend on the RCS of the target. The Radar Cross Section is a measure of how much of the transmitted wave can reflect of the target; a car with a lot of perpendicular and concave conductive surfaces will reflect more of the wave than of e.g., a small bird. The analogy of a an electromagnetic wave striking an object and reflecting like visible light off a mirror is only a simplification, since the metal surface will absorb the energy and begin the oscillate. The oscillations will then radiate the energy away, and directionality occurs because local oscillations generarate partial energies with a difference in phase, in turn causing destructive and constructive interference [3]. Thus, an object of a particular geometry can have a much larger RCS than its actual physical area. An example of such an object is the trihedral corner reflector. It is commonly used to calibrate or benchmark the performance of radar systems due to its high RCS in relation to its actual size and calculating the theoretical RCS is simple [4]. A trihedral corner reflector is shown in figure 2.

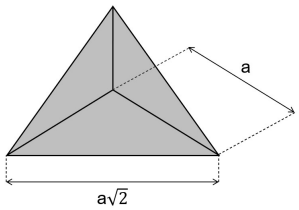


Figure 2: Shows a typical symmetric trihedral corner reflector with dimensions highlighted.

The RCS of an object is mainly dependent on aspect angle, size, shape and frequency. The effective area of the trihedral corner reflector seen from the perspective shown in figure 2 is:

$$A_{eff} = \frac{a^2}{\sqrt{3}} \tag{4}$$

The effective area can be seen as the projection of the shape onto a plane perpendicular to the incident waves. To obtain the RCS of the trihedral corner reflector from the perspective shown in figure 2 the effective area in equation 4 can be plugged into the equation governing RCS of a plane surface:

$$\sigma = \frac{4\pi A_{eff}^2}{\lambda^2} = \frac{4\pi a^4}{3\lambda^2} \tag{5}$$

In contrast, the one-way propagation wave received by the RX antenna does not depend on any reflective surface and only suffers free space losses which is proportional to the inverse of the range to the power of two. The one-way radar range equation is [5]:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2} \tag{6}$$

The transmission line loss and similar attenuation is combined with antenna gain in equation 6. The reflected attenuated signal will take a certain amount of time to traverse the distance between the target and back to the radar receiver, causing a time delay in the received chirp. Furthermore, if the target of interest has a relative velocity to the RX antenna then a phase shift due to the Doppler effect is added, further distinguishing the received signal from the one transmitted. A time-frequency representation of the process described is shown in figure 3.

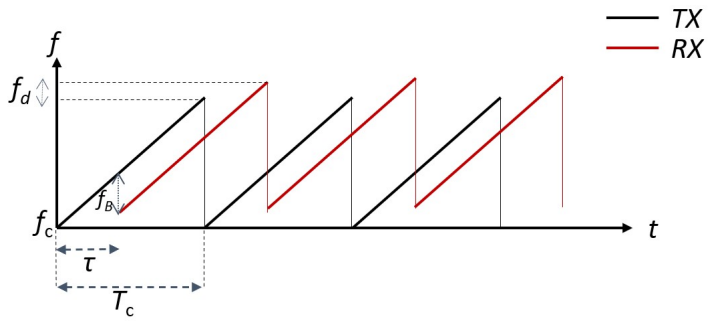


Figure 3: Shows the TX chirp signal in black and the RX signal in red. Note the time delay τ and subsequent frequency drag denoted f_B. The RX signal illustrated also experiences a Doppler shift, f_d.

The time delay τ stems from the time-of-flight of the propagating signal from the TX antenna to target and then back to the RX antenna. The delay is related to the target distance d as:

$$\tau = \frac{2d}{c} \tag{7}$$

where c is the speed of light. The delay gives rise to a difference in frequency between the two signals, which is directly correlated to the sweep rate S:

$$S_\tau = S \cdot \frac{2d}{c} \tag{8}$$

The received signal is mixed upon return with a copy of the transmitted signal, producing an intermediate frequency signal. The difference in frequency due to the delay τ causes a non-zero constant frequency tone of the IF signal, which corresponds to the beat frequency f_B [6]. Note that multiple objects at different distances from the transmitting radar will cause several returns and thereby multiple IF signals, as seen in figure 4.

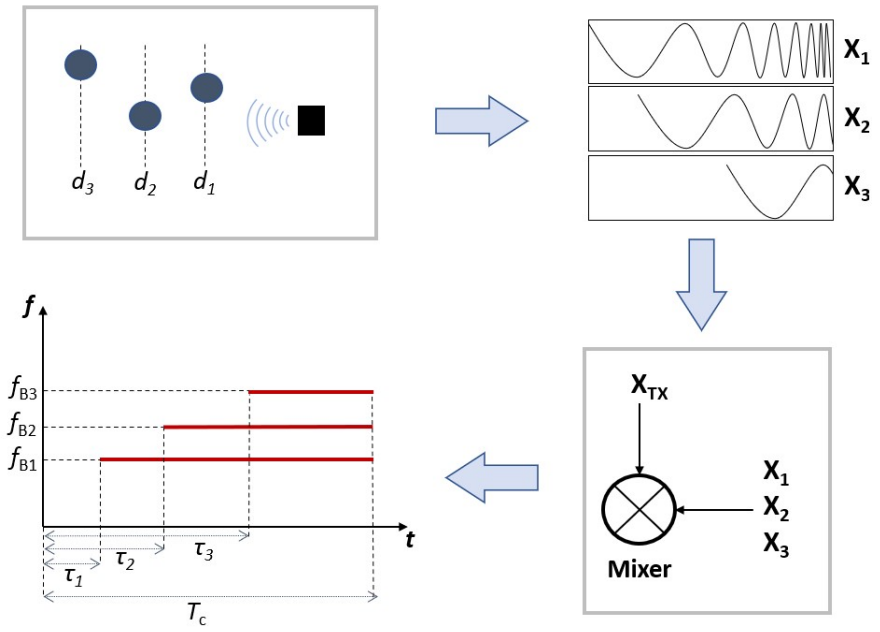


Figure 4: Shows the process of converting different radial distances to beat frequencies. Object 1, 2, and 3 will each reflect an echo and give rise to three signals being received at the RX antenna at different time stamps, as seen in the top-right box. The various delays gives rise to different signals X_{1-3} which in turn are run through a mixer outputting three baseband IF tones directly associated with each object's distance to the radar.

The constant IF signals gives rise to distinct peaks in the frequency spectrum, which allows the radar to determine the distance since different time delays will result in particular beat frequencies. Furthermore, by introducing multiple chirps in a time frame a phase shift between consecutive modulation periods will occur which allows the radar to determine velocity. Before arriving at the final equations transforming beat frequency and phase shift into range and velocity, a model describing the FMCW signal is needed. A thorough mathematical derivation of the transmitted and received signal model is done in [7] and the results are briefly presented here as well.

The instantaneous phase of the transmitted signal is modelled as:

$$\mu(t) = 2\pi \int_0^t f(t)\, dx + \mu_0 = 2\pi(f_c t + \frac{St^2}{2}) + \phi_0$$

where ϕ_0 is the initial phase and $f(t)$ is the frequency at time t, given by:

$$f(t) = f_c + S \cdot t \tag{9}$$

For the nth sweep we have $t = nT_c + t_s$ where $0 < t_s < T_c$. The transmitted signal $x_{tx}(t)$ can then be written as:

$$x_{tx}(t) = \mathrm{A}\cos\left(\mu(t)\right) = \mathrm{A}\cos\left(2\pi(f_c(nT_c + t_s) + \frac{St_s^2}{2}) + \phi_0\right) \tag{10}$$

Note that it does not matter whether the signal x_{tx} is modelled as sine or cosine since the initial phase ϕ_0 can accommodate for either case. If the target is located at a distance R from the radar and moving with relative radial velocity v, then the delay in equation 7 is:

$$\tau = \frac{2(R + vt)}{c} = \frac{2(R + v(nT_c + t_s)}{c} \tag{11}$$

The received signal x_{rx} reflecting off the target is modelled as:

$$x_{rx}(t) = \mathrm{B}\cos\left(\mu(t - \tau)\right) = \mathrm{B}\cos\left(2\pi(f_c(nT_c + t_s - \tau) + \frac{S(t_s - \tau)^2}{2}) + \phi_0\right) \tag{12}$$

where the amplitude B has changed in accordance to the radar range equation 2, suffering from attenuation and varying depending on the target's RCS. The received signal is then mixed with x_{tx} to produce the IF tone. Mixing two sinusoidal signals effectively multiplies them. For cosine multiplication we use the trigonometric formula:

$$\cos\left(\alpha\right)\cos\left(\beta\right) = \frac{\cos\left(\alpha + \beta\right) + \cos\left(\alpha - \beta\right)}{2} \tag{13}$$

Since the carrier frequency f_c usually is on the scale of GHz, a low-pass filter is used to remove the summing term after mixing, leaving only the subtractive term which has a frequency around baseband.

By only processing the the low-frequency term stemming from mixing the two signals together, FMCW radar does not need to use high-frequency components which are often expensive and sometimes even unstable. Thus, by performing the subsequent signal processing on a relatively low-frequency range the processing circuit realization is simplified [8]. The intermediate frequency is then the subtractive term given by:

$$x_{IF}(t) = \frac{AB}{2}\cos\left(2\pi(f_c(nT_c + t_s) + \frac{St_s^2}{2} - f_c(nT_c + t_s - \tau) - \frac{S(t_s - \tau)^2}{2})\right) \tag{14}$$

Equation 14 can be simplified into:

$$x_{IF}(t) = \frac{AB}{2}\cos\left(2\pi(f_c\tau + S\tau t_s - \frac{S\tau^2}{2})\right) \tag{15}$$

By replacing τ with equation 11 we obtain:

$$\begin{aligned} x_{IF}(n, t_s) = \frac{AB}{2}\cos\Bigg(2\pi\Bigg(&\left(\frac{2SR}{c} + \frac{2f_cv}{c} + \frac{2SvnT_c}{c} - \frac{4SRv}{c^2} - \frac{4SnT_cv^2}{c^2}\right)t_s \\ &+ \left(\frac{2f_cv}{c} - \frac{4SRv}{c^2}\right)nT_c \\ &+ \left(\frac{2f_cR}{c} + \frac{2Svt_s^2}{c} - \frac{2SR^2}{c^2} - \frac{2Sv^2n^2T_c^2}{c^2} - \frac{2Sv^2t_s^2}{c^2}\right)\Bigg)\Bigg) \end{aligned} \tag{16}$$

Studying equation 16 one can identify three parts. The first part corresponds to the beat frequency f_B and the second to the Doppler shift f_d. The third part can be omitted since the preceding terms provide all the information needed. In every denominator either c or c^2 appears, rendering several terms negligible. Equation 16 can then be approximated as:

$$x_{IF}(n, t_s) = \frac{AB}{2} \cos\left(2\pi\left(\frac{2SR}{c}t_s + \frac{2f_c v}{c}nT_c\right) + \frac{4\pi f_c R}{c}\right) \tag{17}$$

It is assumed that T_c is sufficiently small such that v and R does not change much in one frequency sweep. During a chirp period $n \cdot T_c$ will stay constant but t_s will increase, hence the frequency of the IF signal will only be dependent on the distance R to the target. By acquiring the frequency of the IF signal the range can be calculated since S is already known. The frequency is obtained by performing a Fast Fourier Transform on the sampled input. See appendix A for a brief recap on the definitions of DFT and FFT.

2.1.1 Range Estimation

By studying the IF signal which is obtained by mixing the RX echo with the TX reference one can obtain the range to target. As can be seen in equation 17 the beat frequency f_B is given by:

$$f_B = 2\frac{SR}{c} \tag{18}$$

and the range is therefore calculated as:

$$R = \frac{f_B c}{2S} \tag{19}$$

To obtain f_B the IF signal is sampled by an ADC and an FFT is performed on the dataset as illustrated in figure 5. This step is referred to as the *range-FFT*.

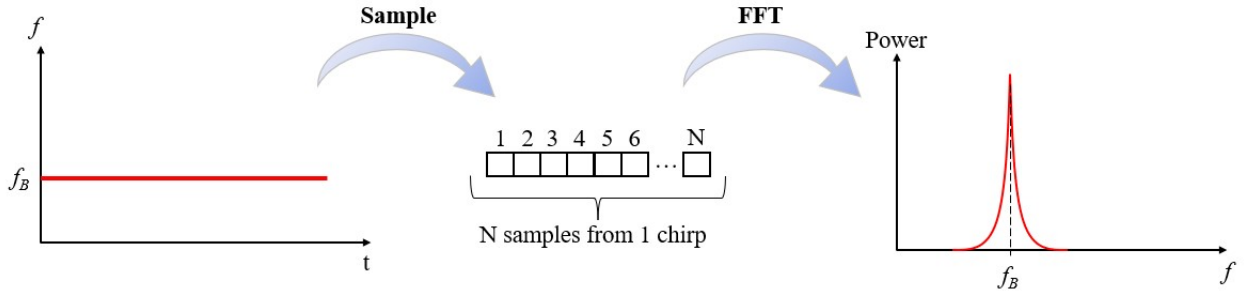


Figure 5: Shows the process of sampling the intermediate frequency signal from one modulation period or *chirp*, and then performing an FFT on the dataset to acquire the frequency which is often the most distinct peak in a power-frequency plot.

From the acquired beat frequency the range is calculated using equation 19. Note that sampling an analogue RX signal through an ADC will produce an I-component and a Q-component, representing the in-phase and quadrature component, respectively. The quadrature component is identical to the in-phase component but shifted by 90^o [1]. Usually both components are kept to be processed in the DSP, but for the sake of simplicity the result of the sampling will only be using one of the quadrature components from now on.

The FMCW radar is limited in its ability to accurately determine the range to the target by its range resolution. The radar places the target in a *range bin*, where each bin represents the smallest distinguishable distance. For example, if two targets are sufficiently close to each other then the radar will place them in the same range bin and if no other information is available then the two objects will show up as a single target. In general, if the radar listens for T seconds then it can differentiate frequency components which

are separated by more than $\frac{1}{T}$ Hz [6]. In other words, the longer the observation period, the better the resolution. If each observation window is a chirp period, then the range resolution is [7]:

$$\Delta f_B = \frac{2S\Delta R}{c} = \frac{2 \cdot \text{BW}\Delta R}{T_c c} \geq \frac{1}{T_c} \iff \Delta R = \frac{c}{2 \cdot \text{BW}} \tag{20}$$

By increasing the observation window the modulation time of the signal's frequency is also increased given that S is held constant, in turn increasing BW and improving resolution ΔR. The maximum distance measurable by the FMCW radar depends on the sampling frequency which is chosen so that ambiguity does not occur. The sampling frequency is usually selected to be double the expected bandwidth, which means that the maximum measurable beat frequency is half the sampling frequency.

$$d_{max} = \frac{f_{B,max} c}{2S} = \frac{f_s c}{4S} \tag{21}$$

The minimum distance is simply the first range bin, which is ΔR.

2.1.2 Velocity Estimation

A single chirp is sufficient to determine the range to a target, but a minimum of two chirps are required to resolve radial velocity. A slow-moving target may have a velocity of only a few meters per second and the subsequent chirps will not be able to pick up the narrow shifts in beat frequency, which poses a problem if velocity is to be determined. The solution lies in the phasor description of a chirp. The result from each *range-FFT* will produce peaks that may appear at the same frequency location, but varies in phase if the target is moving. In contrast to the beat frequency, the phase of the IF tone is very sensitive to small changes in distance [6]. According to equation 17, the phase of the IF signal does not shift during a single chirp since only t_s varies. Instead, the term associated with velocity depends on nT_c, also known as *slow-time* in radar terms. Given that the velocity is fixed, the *range-FFT* will produce a phase shift rate that is constant. This can be interpreted as if there are two frequencies present in equation 17, one linked to fast-time t_s and the other to slow-time nT_c. Similar to the *range-FFT*, the frequency arising from the phase shift between chirps can be found with yet another FFT. The concept is illustrated in figure 6. Consider the phasor defined as in equation 22:

$$Ae^{j\omega} = A(\sin\omega + j\cos\omega) \tag{22}$$

If a signal corresponding to a phasor rotating with ω rad/sample is discretized and sampled, the angular rotation can be found through an FFT [6].

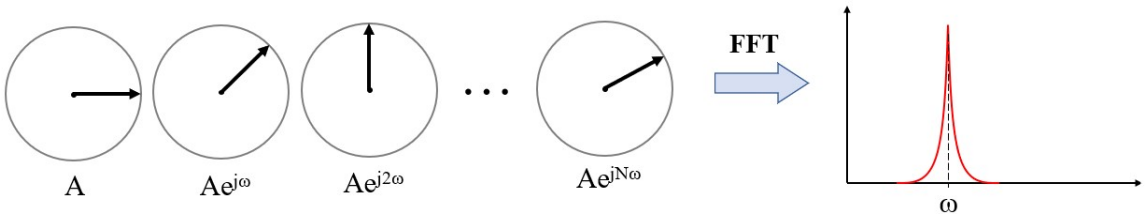


Figure 6: Shows a discretized signal's phasor representation rotating with ω rad/sample. After an FFT is applied on the samples the angular rotation rate can be found.

The process visualized in figure 6 is called the *Doppler-FFT*. The phase shift rate ω is converted to frequency by dividing it with $2\pi T_c$. This is the *Doppler frequency*, referring to the Doppler shift caused by an object in motion. The velocity is found by associating f_d with the second term in equation 17 which then yields:

$$f_d = 2\frac{f_c v}{c} \iff v = \frac{f_d c}{2f_c} \tag{23}$$

The maximum measurable velocity goes back to phasors and the ambiguity of angular rotation. For an object moving towards the radar the object's return echo will experience a positive Doppler shift and the phase rotates clockwise. The opposite is true when the object is moving away from the radar. For example, a signal sample corresponding to a phasor with a particular phase may have rotated to that position either moving clockwise or anti-clockwise as illustrated in figure 7.

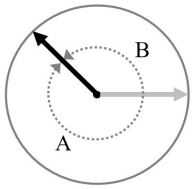


Figure 7: Shows the ambiguity of phasor rotation in a single sample. The phase of the phasor could have moved to the position shown moving either clockwise (A) or anti-clockwise (B) [6].

To avoid any ambiguity the phase of the signal is bounded. The measurement is unambigiuous only if $|\omega| < \pi$. This in turn imposes a boundary on the maximum measurable velocity [6]:

$$|\omega| = 2\pi T_c |f_d| = \frac{4\pi f_c T_c |v|}{c} < \pi \iff |v_{max}| = \frac{\lambda_c}{4T_c} \tag{24}$$

Similar to the range resolution criteria, if the FMCW radar collects N samples then it can differentiate phase components separated by more than $\frac{2\pi}{N}$ rad/sample. This determines the velocity resolution:

$$\Delta\omega = \frac{4\pi T_c \Delta v}{\lambda_c} > \frac{2\pi}{N} \iff \Delta v = \frac{\lambda_c}{2NT_c} \tag{25}$$

From equation 25 it is clear that the velocity resolution improves as the number of temporally equispaced chirps N increases. In practice, the FMCW radar transmits N chirps and mixes the return echoes down to baseband. It samples this IF signal $N \times M$ times, where N is the number of chirps and M is the number of samples per chirp. Consequently, a $N \times M$ data map is created where each row contains samples and a new row is added or replaced every time the radar receives a chirp. The *range-FFT* is performed row-wise on the data map to produce the beat frequency f_B which translates into range. The subsequent *Doppler-FFT* is performed on the chirps instead of on the samples which means that it must be done column-wise to produce the Doppler frequency f_d. However, it is often a simpler process to flip the 2D data map in the physical memory and perform another row-wise FFT. This is known as the *corner turn* in radar lingo, alluding to the process of going from row-wise to column-wise FFTs. When the two FFTs have been performed on the data a range-Doppler map has been created, where magnitude peaks imply the presence of a target with a certain distance and velocity. The process is illustrated in figure 8-10.

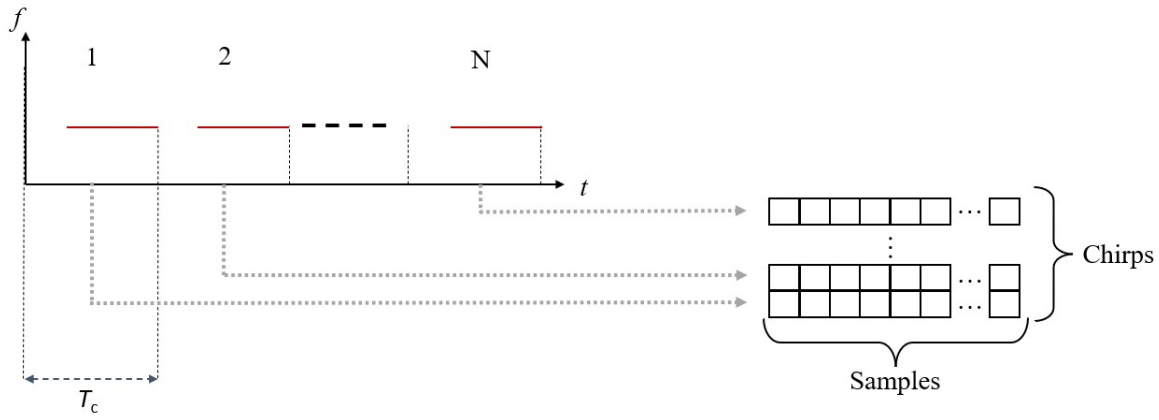


Figure 8: Shows the IF signal being sampled to produce a 2D data map. Each chirp is sampled and stored in a row of its own. Note that the IF signal experiences a delay τ before RX overlaps with TX and can produce a constant tone. See figure 3 for reference.

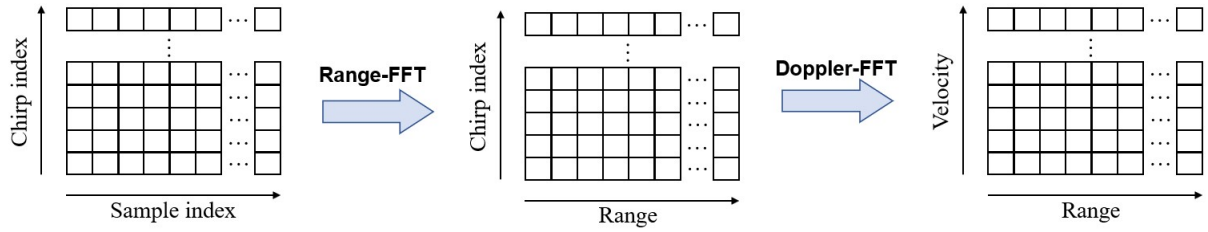


Figure 9: Shows the sequence of FFTs being applied to the 2D data map to produce range and velocity. The *range-FFT* converts the sample index into range bins and the subsequent *Doppler-FFT* converts the chirp index into velocity bins.

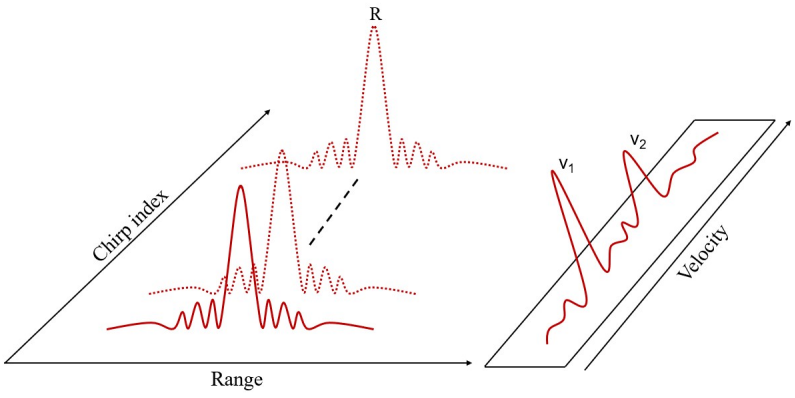


Figure 10: Shows the result after *range-FFT* and *Doppler-FFT* have been applied on the 2D data map. The range dimension has peak at frequency f_B which corresponds to range R. Additionally, the doppler dimension will have a peak at frequency f_d which corresponds to velocity v. In the figure above, there are two targets at the same distance but with two different radial velocities v_1 and v_2.

Note that according to figure 8, the delay τ arising from the time-of-flight to target and back will cause the IF signal to appear for varying lengths of time. If a target is further away, then the IF signal will only appear for a brief moment as the first RX chirp arrives just before the TX chirp period is over. Therefore, the peak magnitude of the FFT result will be lower in comparison to a target close to the radar. Any external signal or random noise occuring will thus become more apparent.

2.1.3 Angle-of-Arrival Estimation

The angle-of-arrival is crucial for separating objects with identical radial distances and velocities. A minimum of two RX antennas are required to determine the AoA, but additional antennas can be used to avoid ambiguity arising from targets with identical properties mirrored along the radar's boresight. The downside of adding more RX antennas is that every element requires its own signal processing chain including mixer, LPF, and ADC, which increases the cost and the complexity of the system. When a target is detected by the radar, it can often be regarded as being in the radar's far-field which means that the incident waves are approximated as being parallel [9]. The approximation is illustrated in figure 11. Moreover, if the target is offset by an angle θ in relation to the radar's boresight the incident waves will reach every RX antenna at a different time stamp. This in turn causes a measurable phase shift ϕ when comparing antenna inputs to each other. The phase shift is dependent on θ and the inter-elemental spacing d between RX antennas [6]. Keep in mind that every RX antenna with its signal processing chain is capable of producing a range-Doppler map, so by studying the phase of each target's range-Doppler peak it is possible to determine the angle of arrival. In practice, it is convenient to stack every DSP chain's 2D data map on top of each other so that each layer contains information from only a single RX antenna. This is called the *radar data cube* and allows for the final FFT to produce the phase difference ψ, commonly referred to as the *angle-FFT*.

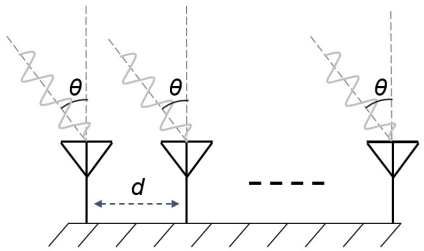


Figure 11: Shows how the incident waves can be approximated as parallel since the target is usually in the radar's far-field view. Every RX antenna separated by the inter-elemental spacing d in the array will receive a wave that is offset by θ from boresight.

From figure 11 it is clear that the wave reaching the first antenna will have travelled a shorter distance than the wave arriving at the second antenna and so on. The extra distance Δd_k travelled by the wave reaching the kth antenna in relation to the first antenna can be expressed as:

$$\Delta d_k = kd \cdot \sin(\theta) \tag{26}$$

The difference in distance travelled can be converted to a phase shift by viewing Δd as a fraction of the wavelength λ and multiplying it by 2π. This results in the following equation:

$$\psi_k = \frac{2\pi kd \sin(\theta)}{\lambda} \tag{27}$$

Applying equation 27 on equation 17 yields [7]:

$$x_{IF}(n, t_s, k) = \frac{AB}{2} \cos\left(2\pi\left(\frac{2SR}{c}t_s + \frac{2f_c v}{c}nT_c + \frac{d\sin(\theta)}{\lambda_c}k\right) + \frac{4\pi f_c R}{c}\right) \tag{28}$$

where $0 < k < K$ is the number of RX antennas. It is then clear that the angular phase can be extracted by taking the FFT with respect to k. Once the phase shift ψ is found the offset θ is calculated as:

$$\psi = \frac{2\pi d\sin(\theta)}{\lambda_c} \iff \theta = \sin^{-1}\left(\frac{\lambda\psi}{2\pi d}\right) \tag{29}$$

From equation 29 it is concluded that the phase shift ψ stemming from the angle of arrival is not linearly dependent on θ, but has a non-linear sinusoidal relationship. The phase shift will therefore be more sensitive when θ is around 0^o than when it is closer to $\pm 90^o$ [6]. In addition to reducing ambiguity, an increase of the number of RX antennas also improves the angular resolution. The question of how many RX antennas to have in an application therefore boils down to a trade-off between cost and complexity against performance.

2.1.4 FMCW Radar Parameters and Performance

When designing an FMCW radar there may be certain requirements that has to be fulfilled, for example velocity resolution must meet a specification or the maximum intermediate frequency cannot exceed a certain value. The performance of the radar can satisfy the requirements governing the performance by means of varying different design parameters. In figure 12 a block diagram illustrating the main segments of an FMCW radar is shown.

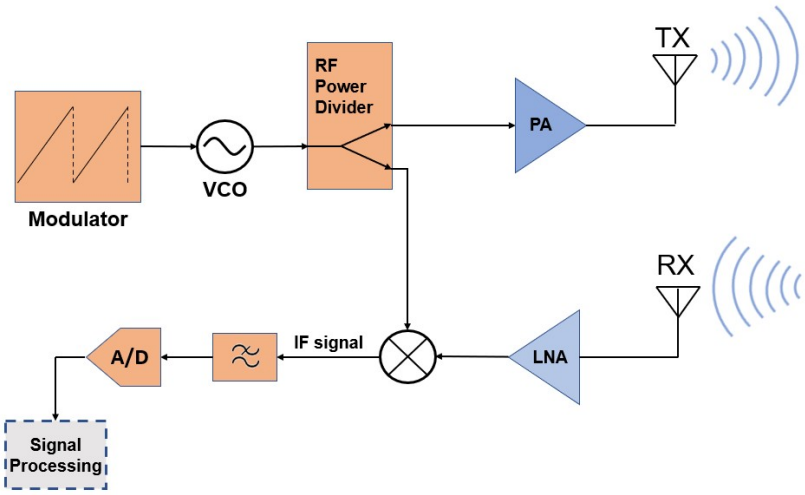


Figure 12: Shows a block diagram of a generic FMCW radar. After [10].

The choice of modulation is usually between a triangular and sawtooth shape sweep. A linear single slope sawtooth is the most commonly used modulation [10]. However, for fast moving targets some level of ambiguity is introduced and triangular modulation may be better suited depending on the application [11]. Furthermore, the sweep rate S during a modulation period T_c will not only put an upper limit on the measurable distance d_{max} but also affect the resolution as seen in equation 20. A short-range radar such as one used in automobiles will in general have a higher sweep rate S than a long-range search radar. The modulation period also determines the peak measurable radial velocity according to equation 25. The length of the modulation period is critical in moving target acquisition since it is desired to maintain the target

in the same range bin for every complete sweep [8]. Moreover, the modulator then controls the input to the voltage controlled oscillator that produces the signal that the TX antenna emits. Both the TX and RX antenna are usually constructed as patch antennas consisting of multiple elements. The arrangement of the antenna elements not only determines characteristics such as lobe pattern and antenna gain, but the dimensions of each element can assist in reducing the influence of side lobes.

The LPF removes any signal noise having frequency components exceeding the maximum intermediate signal frequency - therefore, the filter cutoff frequency is set at the beat frequency corresponding to the maximum measurable distance:

$$f_{IF,max} = S\frac{d_{max}}{c} \tag{30}$$

The hardware might not be able to support intermediate frequencies beyond a certain point and a compromise in equation 30 between sweep-rate and maximum distance is required.

2.2 Target Detection and CFAR

Given that a target is present in the radar's field of view and sufficient signal energy is retrieved in the RX antenna, a peak will appear at one or multiple frequencies after the FFT operations have been performed. This has been illustrated in figure 5 and figure 6. A radar must be able to differentiate targets from background noise and clutter, or at least have some way of automating the detection part in the processing chain. Due to the nature of noise in changing environments, an adaptive algorithm is advantageous since it can increase the detection threshold to an appropriate level when the noise floor increases, and vice versa. However, if the threshold level is set low then apart from real echos some clutter and interference will also get registered in the detection part of the radar module which creates false targets. On the other hand, a threshold level set too high will lessen the probability of picking up any unwanted clutter but will also hinder the radar's ability to discover a real target. Hence, the setting of the threshold level is a delicate balance between high sensitivity entailing higher probability of false alarms, and a low sensitivity with the risk of not detecting weak target reflections. Consequently, to be able to detect a weak target reflection some false alarms are unavoidable. One method of setting the threshold level is by allowing for a fixed probability of false alarm and continuously adjusting the threshold to keep the rate of false positives constant. This is known as Constant False Alarm Rate or CFAR, and there are numerous methods for how CFAR evaluates the data but the principle is the same. A common algorithm is Cell-Averaging CFAR, or CA-CFAR for short. Similar to other CFAR methods, CA-CFAR is a sweeping window type of detector which examines each cell in a given data set and compares it to some reference cells. The CFAR algorithm is applicable to both the one-dimensional range and Doppler data individually or on the 2D range-Doppler map. The concept is illustrated in figure 13.

The CA-CFAR method works by examining each cell one-by-one in a dataset and compares the cell under test (CUT) to some reference cells. Each cell corresponds to a range or velocity bin and has an intensity magnitude after the FFT operation has been performed. By letting a sliding window comprised of a CUT and reference cells navigate through the data any anomalous peaks will be registered and allow for target detection. Oftentimes the cells adjacent to the CUT are weighted so that their magnitude is negligible; the purpose of having deemphasized *guard cells* is to avoid including target energy which can leak over to neighbouring cells [12]. The two endpoints of the IF signal will introduce some level of discontinuity since the number of sinusoidal periods in the acquisition of the RX signal will rarely be an integer, in turn resulting in a smeared frequency spectrum commonly referred to as spectral leakage. To limit the effects of this phenomenon a windowing function is applied on the time-domain data before the first FFT, like a Hann or Hamming window [13]. In addition, the number of reference and guard cells can be varied to better accommodate for the specific dataset, typical target signature or noise environment. When the noise or clutter changes the threshold level will be modified accordingly since the magnitude average of the reference

cells surrounding the CUT will change. CA-CFAR can be performed on both 1D or 2D datasets as seen in figure 13.

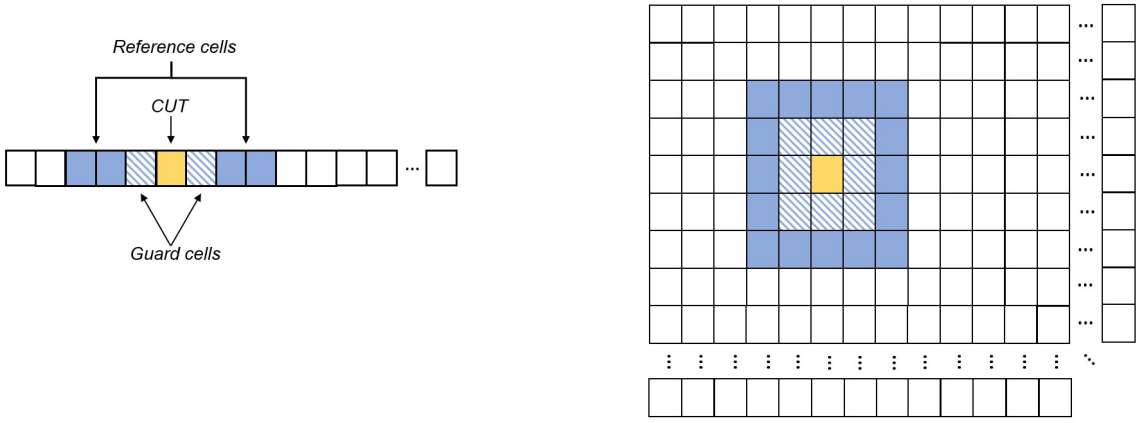


Figure 13: Shows a sweeping CFAR window applied on both one set of data cells and on a 2D data map. The CUT is enclosed by guard cells which effectively deemphasizes the magnitude in those particular locations. Further out is the reference cells which in CA-CFAR generates an average value that is used to calculate a threshold level. The CUT is classed as a detection if it surpasses the threshold level. Note that the number of reference and guard cells can vary.

There are multiple established CFAR algorithms, e.g. ordered statistics (OS-CFAR), smallest of (SO-CFAR) and greatest of (GO-CFAR). There is not a one-size-fits-all algorithm that is suitable for or used in all circumstances as each CFAR method fit some scenarios better or worse than others. The CA-CFAR algorithm will perform adequately in a homogeneous environment with a single target or multiple targets spread far apart. The advantage of CA-CFAR is that it is less resource intensive than its counterparts and it is easily implemented [14]. However, if a clutter edge appears at a certain distance or velocity then the performance of CA-CFAR will deteriorate when the CUT reaches the point of high noise. This is because the reference cells will contain cells from both a high and a low noise source which in turn creates a flawed threshold. GO-CFAR would outperform CA-CFAR in this case as it would only account for the high noise surroundings and would therefore create a more suitable threshold as the CUT moves into the clutter. On the other hand, both GO-CFAR and CA-CFAR will have a poor probability of detecting two closely spaced targets, which is where SO-CFAR would be more appropriate to use [14]. In short, the choice of detection algorithm will depend on what kind of environment the radar is expected to operate in and the required performance may be impaired whenever the operating conditions changes. With many radars, the information is expected in real-time and thus the processing interval is limited. Any CFAR algorithm used in small-sized radar modules with limited resources capacity must be efficient and its data processing sufficiently quick, which in turn excludes some of the algorithms available.

2.3 FMCW Radar Susceptibility to Jamming

The objective of intentional jamming is to prevent a radar from extracting any useful information by denying it use of the electromagnetic spectrum. Similarly, spoofing signals deceive the radar operator or control unit to base decision-making on misleading or false information. A representative example of spoofing is the injection of false targets into the radar's digital detecting, i.e. making targets appear that do not exist. Unintentional jamming and spoofing can occur in environments where there is a substantial amount of electromagnetic interference, such as among other electronic sensors or in the vicinity to transmitting masts. Jamming commonly introduces signals with different characteristics that raise the noise floor of the radar receiver, which hinders weak echo signals from being detected among the artificial clutter. Depending on

the type of radar, some methods of interference will be more effective than others.

Frequency-modulated continuous wave radar belong in the category of low-probability-of-intercept, or LPI radars, because of its low power, wide bandwidth and a time-varying frequency. The purpose of an LPI radar is to remain undetected by external receivers, which may otherwise relay the information gathered from the emitted signal. There is a large number of measures that can be employed to create a radar which has a low probability of intercept in certain situations; keep in mind that the properties of the intercepting receiver will also determine if the transmitting module is an LPI radar.

The FMCW radar transmits a continuous wave with a varying frequency, which in contrast to a pulsed radar has a 100% duty cycle and no energy peaks. Furthermore, an intercepting radar might have a larger bandwidth than the transmitting FMCW radar since the span of the frequency sweep may not be known to the counterpart, in turn increasing the SNR required for a detection since more noise is included in the intercepting antenna [15]. Moreover, because the received waveform is mixed with the transmitted signal, illustrated in figure 12, a significant correlation gain will be added to any coherent signal. The FMCW radar is a homodyne system meaning that it expects the receiver signal to have specific properties and coherency allows for the signal energy to be accumulated in the same filter of the spectrum, whereas the energy of an incoherent signal will be spread out in multiple filters [8]. The coherency gain is key in allowing the homodyne system to operate at low power since noise and waveforms from other sources are attenuated while the transmitted reflection is amplified. The input SNR at the FMCW receiver is improved by integrating the signal over time as any zero mean random noise will cancel itself out whilst the reflected signal energy accumulates during the integration period [15]. By integrating the signal over time at the receiving end it is possible to capture additional energy leading to more distinct peaks in the frequency spectrum. However, echoes stemming from objects far away from the radar will not overlap with the TX reference signal until after some delay τ, as can be seen in figure 8. Therefore, the further an object is from the radar the smaller the energy content both due to spreading losses but also due to the integrative element.

The LPI aspects of the FMCW radar renders it difficult for a passive receiver to distinguish the emitted waveform from background noise. However, once obtained the intercept module could store the signal in a DRFM and retransmit a waveform with delay and phase properties that resembles an echo at a certain velocity and range. This concept is illustrated in figure 14. The spoofing signal would appear no different than a true reflection off a target and would therefore receive the coherent gain when mixed with the reference signal. Furthermore, the retransmitted spoof signal would only be attenuated by one-way atmospheric losses proportional to equation 6 in contrast to the true echo suffering from two-way losses. Hence, a spoof signal would have a much higher energy content at the FMCW radar's receiver than the real reflection. On the other hand, excessive input power to the RX antenna carries the risk of damaging the circuitry, which in a way spoils any deceptive intentions. In short, the initial difficulty lies in detecting the emitted waveform in order to store it, then one must synchronize and retransmit a deceiving signal in a sufficiently short time span so that the waveform is still relevant to the FMCW's processing unit.

(a) Normal operating procedure.

(b) The victim radar is subject to a spoofing attack by an adversarial system.

Figure 14: Shows the working principle behind a spoofing attack on a radar. In subfigure 14b an adversarial system transmits a signal which is coherent to the victim radar. The adversary adds a delay and phase compensation to create a false target at a certain range and velocity to mislead the victim radar system. In addition, the adversarial signal only suffers from one-way losses, which in turn creates a stronger signal than the reflected echo.

When considering jamming using non-coherent waves there are additional attenuating steps affecting the injected signal. A common practice is to place a low-pass filter after the mixer with a cut-off frequency at the maximum intermediate frequency supported by the system. The cutoff frequency f_{-3dB} is normally only a fraction of the operating frequency of the TX and RX signals, which in turn results in a LPF that filters out any remnants of noise around the carrier frequency that could accompany a down-mixed IF signal. In addition to removing noise, the LPF would also remove a spoofing signal with a delay that results in a beat frequency exceeding the maximum intermediate frequency [8]. After the LPF the signal would get sampled and put through an FFT. As can be seen in appendix A, a sample $x[n]$ is correlated with a sine wave, which implies that the output $X[k]$ is larger in magnitude whenever the samples are coherent with the sinusoidal signal of a certain frequency. Discrete Fourier transform can therefore be seen as having an inherent processing gain and due to the spreading nature of the random noise power distribution, an FFT of a non-coherent waveform would result in it being scattered across the spectrum whereas a signal with a constant tone f_B would not only be accumulated in a single filter but also receive the DFT gain [8]. In other words, for a non-coherent jamming signal to be effective it must have sufficient power to pass through the mixing coherency attenuation and the lack of DFT gain while still being strong enough to raise the noise floor significantly. It may be necessary for a jamming device to inject noise spanning several hundred kilohertz for an FMCW radar, and even then the victim radar could increase transmit power to counter the jamming device. In short, for interfering signals in the context of FMCW jamming, *power* is the term to keep in mind. But similar to spoofing waveforms, a jammer would also only experience one-way attenuation which necessitates the need of a term describing the jamming intensity in comparison to the true reflection with respect to distance. This is known at the jamming-to-signal ratio or JSR, and the JSR increases the further away the reflective target is situated from the RX antenna of the FMCW radar because of two-way losses.

2.4 Previous Research

The introduction of false information received by a commercially available FMCW radar was achieved in [10] using a proof-of-concept device. The apparatus uses off-the-self components and 3D-printed directive lens antennas to achieve a low-cost semi-passive device capable of misleading and confusing a radar. Experimental validation verified the potential such a system could have on a commercial radar with false targets visible in the range-Doppler map. However, due to the modulation of the backscatter tag not being single sideband, the false targets appears in pairs which could give a sophisticated radar systems hints about a spoofing attempt.

Further research is suggested and countermeasures are proposed. In [16] another proof-of-concept spoofing system is built using Software Defined Radio which introduces delay and phase compensations to fool the victim radar's range and velocity measurements. Instead of emitting RF waves traversing through free-space, the proof-of-concept setup uses RF cables calibrated to simulate larger distances. The adversarial system focuses on more common sawtooth frequency modulation techniques and employs a spoofing signal resulting in false vehicle motion that still abide by the laws of physics, thus creating a more legitimate false target which could otherwise be ignored by a refined radar system. Jamming of FMCW radars was investigated in [8] using a collection of jamming waveforms in a computer simulation and on a Lab Volt Radar Training System. The effectiveness of the jamming waveforms was determined by observing how much the beat frequency changed when subject to external interference, indicating range manipulation. The hardware tests were inconclusive due to constraints of the radar system. The computer simulations indicated that spoofing could be effective in penetrating the radar's digital signal processing and injecting misleading detection results if enough is known about the victim system to synchronize to it. Moreover, tone jamming was found to completely overwhelm the victim system and thus appears very effective. However, it was found that the effectiveness was only due to alias shifting in the simulated quadrature mixing and therefore not suitable for real EW scenarios. Random noise jamming was observed to have the most impact on the beat frequency at some ranges in the hardware tests but the results were too inconsistent and negligible to draw any conclusion as to which jamming waveform is the most effective. Pulse jamming using a Gaussian modulation was suggested and found to lower the SNR in the simulations if the RF pulse can cover the passband of the FMCW radar. In [9] mitigation methods using convolution neural networks against unintentional jamming were studied. The CNNs developed performed differently depending on what kind of interference was present. When the simulated radar was being jammed non-coherently and real object reflections were below the noise floor the CNNs struggled to mitigate the noise - this was also the case for classical signal processing algorithms. In coherent jamming situations, such as spoofing, the mitigation techniques were able to distinguish ghost objects if frequency drift occured due to e.g., clock drift. However, when little to no smearing affected the ghost objects the CNNs could not distinguish it from a real target. Hence, a difficulty with spoofing has been proposed as two radar systems with seemingly identical properties cannot physically have the exact same internal clock which can result in discrepancies between the time keeping.

3 Methods

The following sections will present the steps taken in order to evaluate the sensitivity of an FMCW radar to a selection of jamming approaches. Section 3.1 describes how properties and parameters of a commercially available FMCW radar is obtained and verified with measurements. Section 3.2 presents the simulation model implemented in Matlab based on theory and using the parameters obtained in the preceding section 3.1, and also what assumptions were made.

3.1 Characterizing an FMCW Radar

The FMCW radar system available is a commercial automotive evaluation kit operating at 24 GHz. An associated software with a GUI and TCP/UDP protocol is also readily accessible. To control the radar and obtain raw data the data protocol TCP is used via PuTTY and the data is sent over Ethernet UDP. The data is in hexadecimal with the first two bytes acting as an identifier for e.g., range data, Doppler data, raw ADC values and so on. As this is a commercial product intended to be used to evaluate the feasibility in automotive scenarios, the user is not given all of the parameters governing the performance of the system. In order to establish a more extensive description of the radar several parameters need to be determined. The following parameters are given:

- $f_c = 24$ GHz
- $BW = 250$ MHz
- $d_{res} = 0.6$m
- $d_{max} = 76.4$m
- $f_s = 366.3$ kHz
- 128 samples per chirp
- $v_{max} = \pm\ 31.5$ km/h
- $\theta_{max} = \pm\ 32^o$
- 128 chirps per frame
- $P_t = 11$ dBm

To determine the chirp period T_c equation 24 is used:

$$T_c = \frac{\lambda_c}{4 \cdot |v_{max}|} = \frac{0.0125 \text{ m}}{4 \cdot 8.75 \text{ m/s}} = 357.1 \ \mu\text{s} \tag{31}$$

The sweep rate is found by using equation 1:

$$S = \frac{BW}{T_c} = \frac{250 \text{ MHz}}{351.1 \ \mu\text{s}} = 700.1 \text{ kHz}/\mu\text{s} \tag{32}$$

Since $T_c = 357.1\ \mu$s and repeats 128 times during one time frame, then T_f is obtained by:

$$T_f = N \cdot T_c = 128 \cdot 357.1 \ \mu\text{s} = 45.7 \text{ ms} \tag{33}$$

The velocity resolution is then obtained by equation 25:

$$\Delta v = \frac{\lambda_c}{2NT_c} = \frac{\lambda_c}{2T_f} = \frac{0.0125 \text{ m}}{2 \cdot (45.7 \cdot 10^{-3} \text{ s})} = 0.14 \text{ m/s} = 0.5 \text{ km/h} \tag{34}$$

Each range and velocity bin in the FMCW radar DSP will be have a size equal to $d_{res} = 0.6$ m and $\Delta v = 0.14$ m/s, respectively. The maximum intermediate frequency, which is used as the cutoff frequency by the LPF, is found using equation 30:

$$f_{IF,max} = S\frac{d_{max}}{c} = (700.1 \cdot 10^9 \text{ Hz/s})\frac{76.4 \text{ m}}{3 \cdot 10^8 \text{ m/s}} = 178.3 \text{ kHz} \approx f_s/2 \tag{35}$$

Furthermore, the range resolution which is specified by the manufacturer is also given by equation 20:

$$\Delta R = \frac{c}{2BW} = \frac{3 \cdot 10^8 \text{ m/s}}{2 \cdot (250 \cdot 10^6 \text{ Hz})} = 0.6 \text{ m} \tag{36}$$

The range resolution is also the smallest measurable distance by the radar unit, since the target would be placed in the first range bin governed by the range resolution. In other words, $d_{min} = 0.6$ m. Similarly, the smallest measurable velocity is the first Doppler bin which is the same size as the velocity resolution, resulting in $v_{min} = 0.14$ m/s.

The calculated characteristics of the FMCW radar system are verified through a series of measurements. The FMCW radar is allowed to continuously operate at a distance of 5 meters from a receiving antenna configured for 24 GHz. The collected signal is then down-mixed with a 18.5 GHz wave from a signal generator, which produces a 5.5 GHz signal. A local oscillator at a frequency of 5.1 GHz further down-mixes the signal to 400 MHz in order for the ADC to be able to capture the whole sweep with a sufficiently low sampling frequency. A bandpass filters out any noise below 200 MHz and above 800 MHz to accentuate the sweeps on the digital display. The measurement setup is illustrated in figure 15.

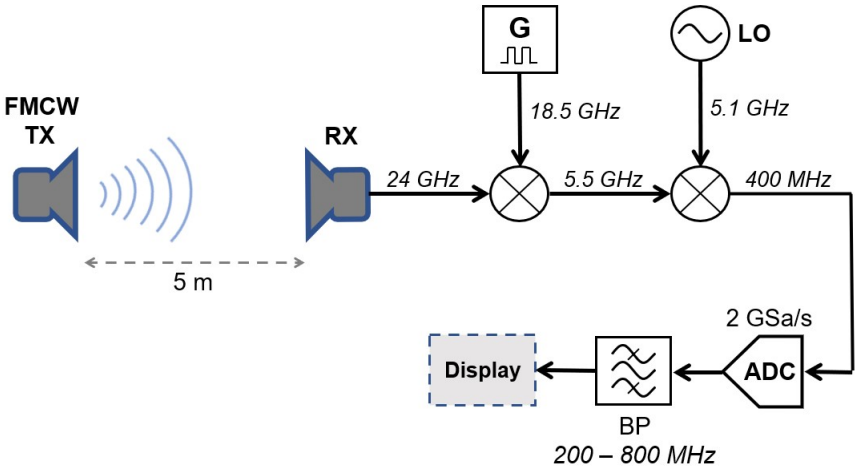


Figure 15: Shows the block diagram of the measurement setup used to obtain the emitted signal from the FMCW radar module. A passive RX antenna configured for 24 GHz is used to acquire the emitted FMCW signal. Multiple external signals are then used with the received one to acquire a lower frequency suitable for the ADC.

The ADC samples for 100 milliseconds which can encapsulate two whole sweeps since $T_f = 45.7$ ms. The results are post-processed in Matlab to produce the spectrograms in figure 16 to figure 18.

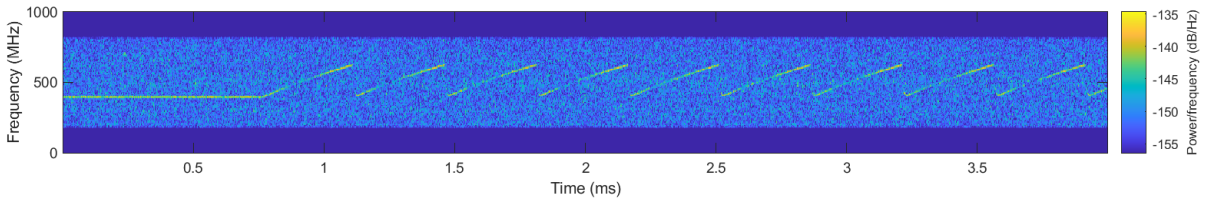


Figure 16: Shows the first emitted linear FMCW sweeps in the beginning of a time frame.

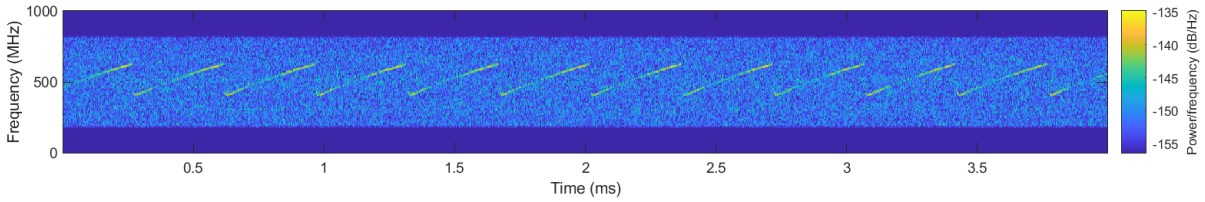


Figure 17: Shows a series of linear FMCW sweeps in the middle of a time frame.

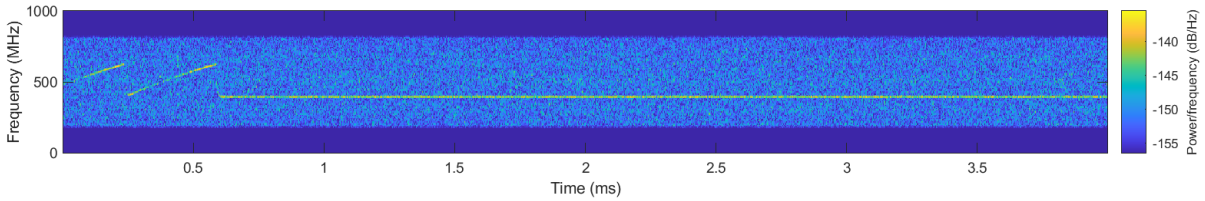


Figure 18: Shows the last emitted linear FMCW sweeps in the end of a time frame.

The spectrograms in figure 16 to 18 represent a snapshot of the data collected in the measurements. The characteristics previously stated are verified by observing the modulation period, bandwidth, number of chirps and the total time elapsed for one time frame. The proposed properties matched the measured ones. The gain of the patch array antenna also has to be roughly estimated in order to have something to work with ahead. This is done through Matlab by simulating 2x10 patch arrays of specific dimensions so that each individual patch element resonates at 24 GHz with a finite ground plane behind the array. This is only an idealisation since the real antenna consitutes of multiple connected patches which narrows the further away from the center they are to reduce the effects of sidelobes. However, the simulation can provide a rough estimate of the gain in a similar antenna which is sufficient. The toolbox *Phased Antennas* was used to generate gain patterns of the patch array. The gain in both the azimuth and elevation plane are shown in figure 19 and 20, respectively. The 2x10 patch array antenna is positioned so that is has 10 columns of patch elements in the azimuth plane and 2 rows in the elevation plane.

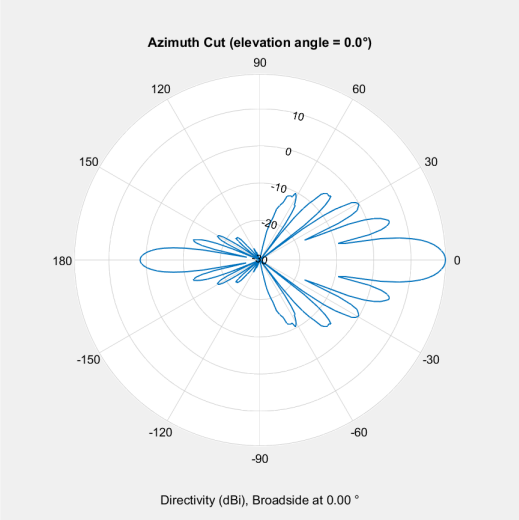


Figure 19: Shows the simulated azimuth gain of a 2x10 patch array antenna with each element resonating at 24 GHz.

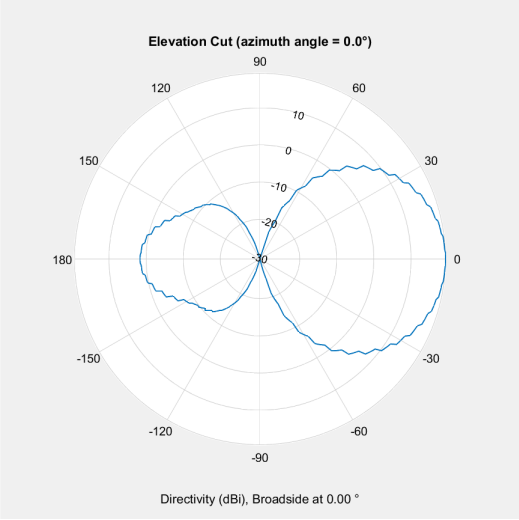


Figure 20: Shows the simulated elevation gain of a 2x10 patch array antenna with each element resonating at 24 GHz.

From figure 19 and figure 20 the maximum gain achieved in the main lobe is around 20 dBi. It is also clear that multiple sidelobes appear off the mainlobe with the first sidelobe having a -13 dBi difference in the azimuth plane. Another Matlab simulation of the antenna gain is performed which calculates the source current given a prescribed current profile and in which medium the antenna is located in. Again a 2x10 patch array antenna is simulated but this time with an aperture in an isolator with a flat current profile at 24.125 GHz (middle of frequency sweep). The directivity and gain is shown in figure 21.

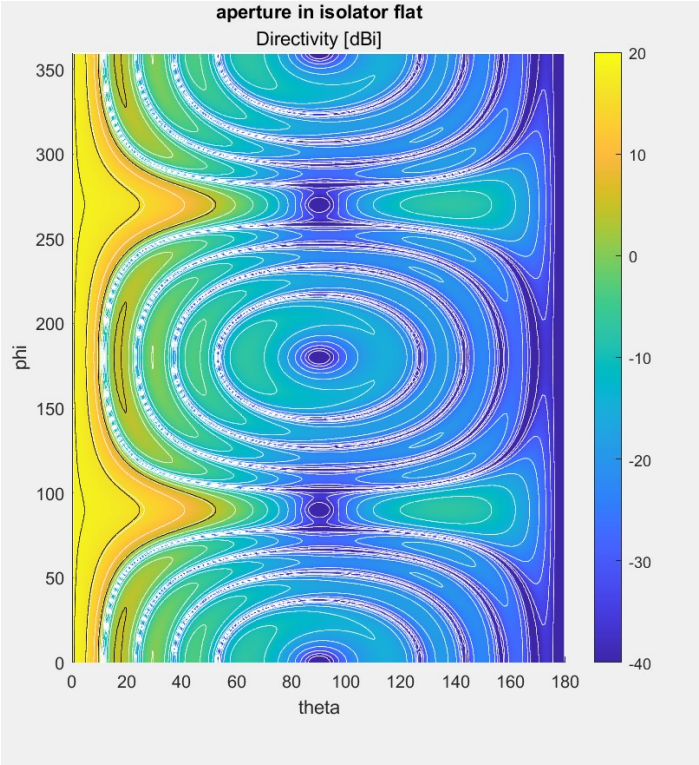


Figure 21: Shows the directivity of a 2x10 patch array antenna consisting of individual patch elements subject to an RF signal of 24.125 GHz. The aperture is located in an isolator and each element has a flat current profile.

From figure 21 one finds the mainlobe at $\theta = 0^o$ and $\phi \in$ [0,360], which indicates a gain of around 20 dBi according to the colormap. At $\phi = 90^o$ and $\phi = 270$ with $\theta \in$ [0,45] the elevation lobes also seen in figure 20 can be observed. Side lobes can also be seen. The two simulations agree with each other that the gain in the mainlobe is around 20 dBi of this idealized patch array antenna model.

3.2 Matlab Model

The model is based upon the block diagram in figure 12 and implements the main elements of the digital signal processing which are key in FMCW radars. It assumes a free space in which objects appear, i.e. no ground or clutter like trees or walls. Angular position of the object is not measurable since the model only implements 1 RX antenna. Parameters governing the performance of the FMCW radar are chosen so they match the ones found in section 3.1. The simulation creates a TX signal using equation 10 with an amplitude A which is given by:

$$A = \sqrt{P_t \cdot G_t} \tag{37}$$

where P_t is the power emitted by the TX antenna and G_t is the TX gain. By manually setting the distance R and velocity v of the object a reflective echo can be acquired by implementing equation 12. It is assumed that the object has an RCS of $\sigma = 10$ dBsm, which is not unusual for e.g., a car at 24 GHz [10]. The amplitude B of the RX signal is:

$$B = \sqrt{P_r \cdot G_r} = \sqrt{\frac{P_t G_t G_r \sigma \lambda^2}{(4\pi)^3 R^4}} \tag{38}$$

It is assumed that $G_r = G_t \approx 20$ dBi as per section 3.1. An LPF with cutoff frequency $f_{-3dB} = f_{IF,max}$ is implemented using Matlab's *lowpass()* function. The down-mixed and sampled signal is then resized to a 2D data map as shown in figure 9. Next, a Hann windowing function is applied on the data; the specifics of the return signal such as shape were not known at this point and a versatile window such as Hann is appropriate. The range-FFT is performed using the sampling frequency f_s to obtain the beat frequency f_B, and the range is then found using equation 19. The velocity is found by performing the Doppler-FFT and obtaining the Doppler frequency f_d, which allows the velocity to be calculated via equation 23. Note that when performing the Doppler-FFT the sampling frequency f_s is not used, since every sample stems from a unique sweep. The slow-time sampling frequency $f_{s,Doppler} = 1/T_c$ is used instead. The range and velocity magnitudes are then normalized and used to create a range-Doppler map. Thereafter the data is put through a CFAR algorithm to determine which FFT peaks are valid targets. This model uses CA-CFAR since no clutter edges will appear and the background noise is set to be zero-mean white noise. The CFAR algorithm is only implemented as a visualization tool to illustrate the working principle and how jamming waveforms interact with threshold levels; thus, there will not be any focus on the specific number of training cells, PFA or guard cells for each scenario as this was arbitrarily chosen to provide satisfactory results when no jamming is applied.

An example is given below simulating a target with $\sigma = 10$ dBsm having a closing radial velocity of 4 m/s at a range of 17 m.

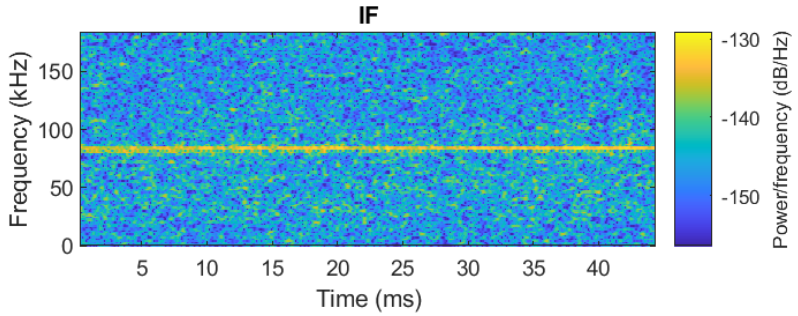


Figure 22: Shows the down-mixed intermediate frequency signal during a whole timeframe for a simulated object having a range of 17 m and a radial velocity of 4 m/s. White noise is added to each sample of the RX signal before mixing to get closer to a realistic scenario.

The signal illustrated in figure 22 is re-shaped to a 128x128 data map so that every column contains samples from a unique sweep. The range-FFT is performed on this data set to obtain the range, illustrated in figure 23.

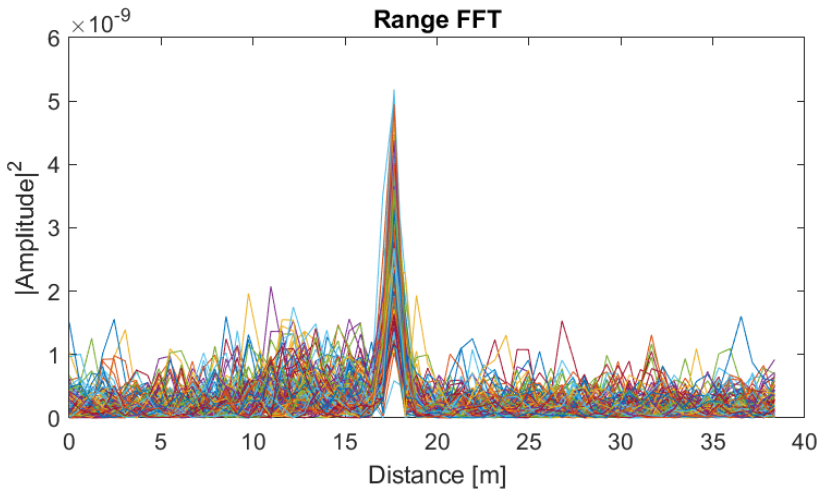


Figure 23: Shows the range-FFT of a simulated object at a range of 17m with a velocity of 4 m/s.

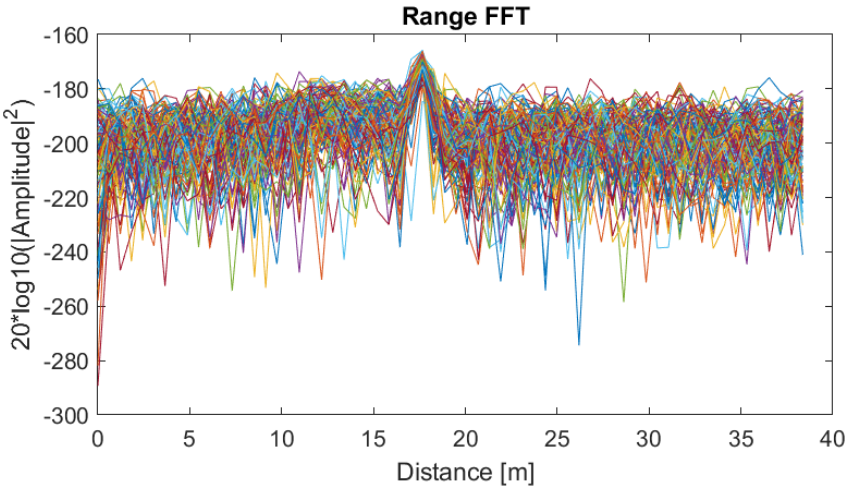


Figure 24: Shows the same range-FFT as in figure 23 but with the magnitude in decibels.

The *radar corner turn* is executed by transposing the 128x128 data map and then performing the Doppler-FFT to obtain the radial velocity, as seen in figure 25.

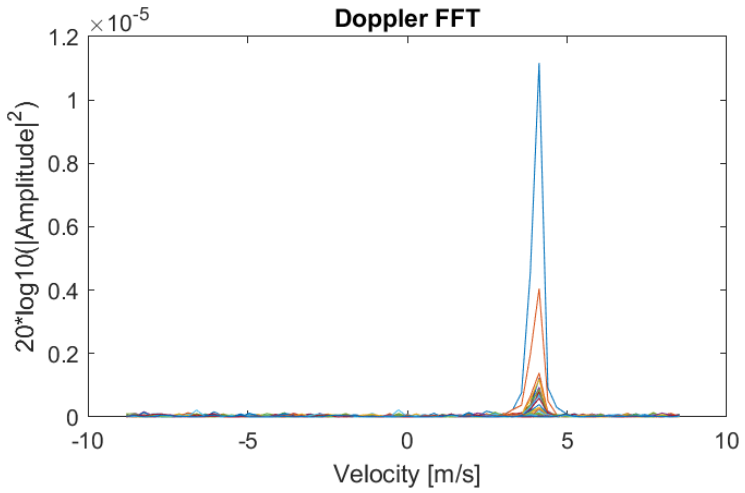


Figure 25: Shows the Doppler-FFT of a simulated object at a range of 17m with a velocity of 4 m/s.

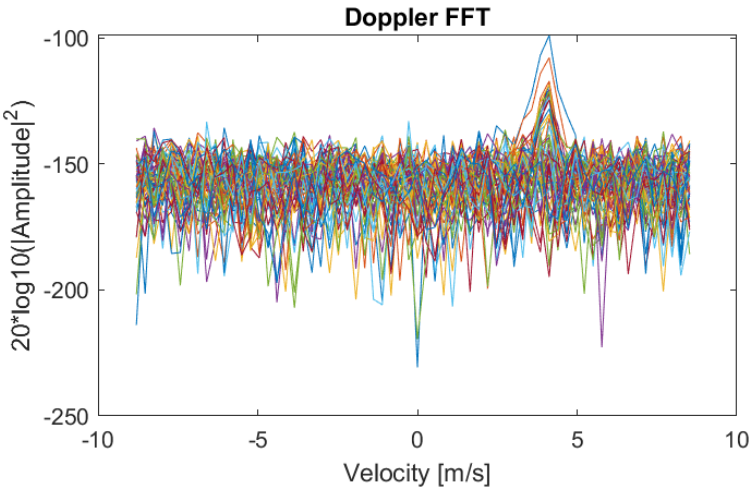


Figure 26: Shows the same Doppler-FFT as in figure 25 but with the magnitude in decibels.

The range and velocity of the object is better visualized in a range-Doppler map as shown in figure 27.

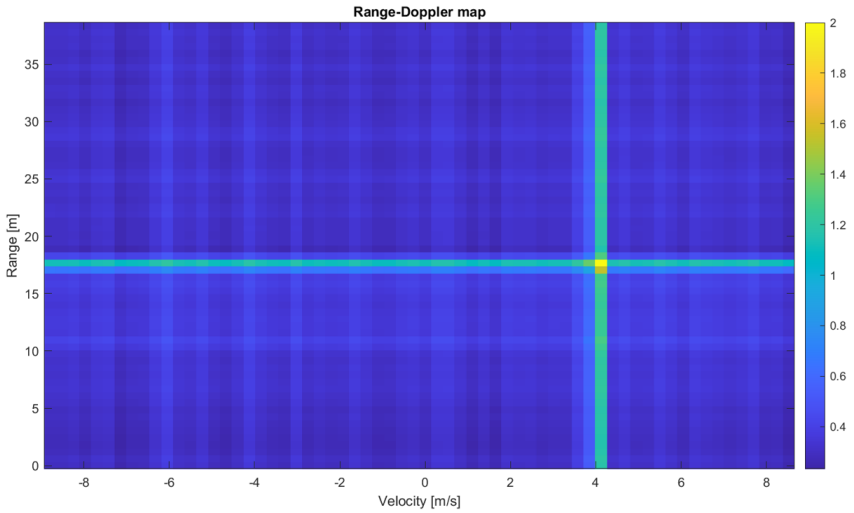


Figure 27: Shows a 2D visualization using the data from figure 23 in combination with figure 25 after having been normalized.

To automate detection the CA-CFAR algorithm sets a threshold level based on neighbouring cells and filters out any data below, effectively creating a map of 1s and 0s, as shown in figure 28.

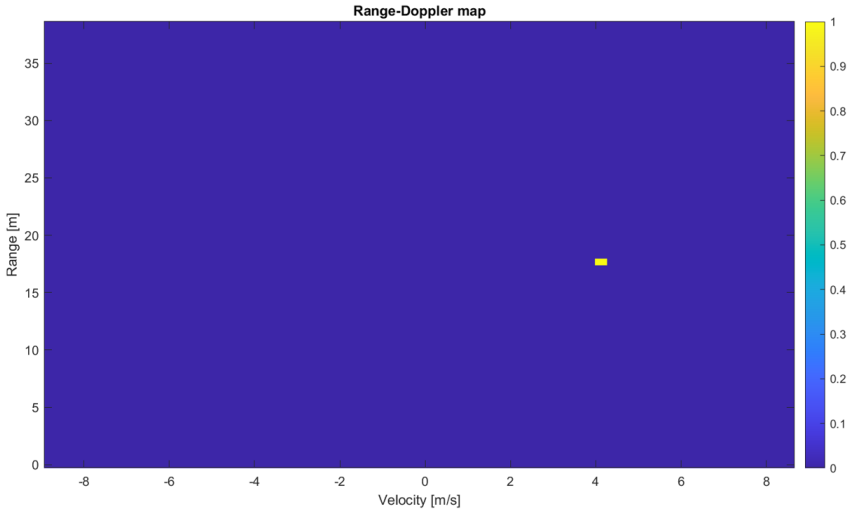


Figure 28: Shows the same data represented in figure 27 but having gone through the CA-CFAR algorithm to provide detection results.

The Matlab model is able to find the object at the correct distance and radial velocity by using the same fundamental digital signal processing which is key in FMCW DSP.

3.3 Jamming Models

Based on the literature study conducted and previous research done in the field two jamming approaches are selected to be evaluated. Deception using spoof signals has proven to be effective when sufficient information about the victim radar system is available. Studies on jamming an FMCW radar suggested that if the

passband is adequately small such that the bandwidth of the jamming signal can cover it, then Gaussian pulse jamming can cause significant noise in the detection chain. The following two sections describe the implementation of the selected jamming techniques in the Matlab model.

3.3.1 Repeater Jamming

The repeater jammer is modelled as an identical signal as the RX based on equation 12, but it has a slight difference in frequency and phase corresponding to an adversary postponing the transmit signal and adding a phase compensation. Furthermore, the amplitude of the signal does not need to reflect off a target like the original FMCW wave, so it only suffers from one-way spreading losses. Therefore, the amplitude D of the received signal at the victim RX antenna is obtained from equation 6. The effective radiated power of the adversary repeater is set to -8 dBm which is smaller than the output of the FMCW radar, since the repeater may not have access to the same power as an automotive radar if handheld or carried on a small mobile platform such as a drone. Similar to a real object, the placement of the false target is arbitrary and the independently received signals are added together after down-mixing. Due to hardware and memory constraints, the signals are pre-sampled to f_s before mixing instead of decimating after the LPF. The main steps describing the inclusion of a jamming or spoof signal into the Matlab model is illustrated in figure 29.

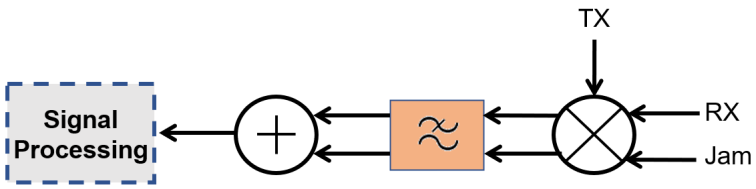


Figure 29: Shows a block diagram describing how a spoofing or jam signal is introduced into the Matlab model.

Two scenarios will be simulated. In the first one there is a stationary target at 26m that emits a repeater signal which injects a non-moving false target at closer to the radar at 12m to show how the difference in energy intensity when one signal only suffers one-way spreading losses. The second scenario simulates a false target being injected close to the real object but with a different velocity.

3.3.2 Pulse Jamming

The pulse jamming signal model is based on a Gaussian pulse. A Gaussian RF pulse not only has a temporal shape of a Gaussian function but the frequency spectrum of the pulse is one of similar characteristics, meaning that such a pulse allows for a span of frequencies to be incorporated into a single transmission. The Matlab model creates a Gaussian pulse using *gauspuls()* having a center-frequency at $f_c + \frac{BW}{2}$ and bandwidth BW, resulting in a pulse covering the frequencies included in the FMCW sweep of the victim radar system.

The generated pulse is repeated to create a pulse train using Matlab's *pulstran()* having a sampling frequency of 205 MHz to generate a signal of length T_f. The TX and RX signals of the victim radar are interpolated to the pulse train's sampling frequency, mixed separately and then decimated down to f_s following a summation of the signals. Four pulse repetitions frequencies are tested:

- PRF = 5 635 Hz $\rightarrow$ 2 pulses per chirp
- PRF = 11 270 Hz $\rightarrow$ 4 pulses per chirp
- PRF = 22 540 Hz $\rightarrow$ 8 pulses per chirp
- PRF = 45 080 Hz $\rightarrow$ 16 pulses per chirp

The range-Doppler map and individual FFTs are then inspected to observe any impact on the radar's detection performance when a simulated object of 10 dBsm is present at a range of 30m and velocity of 7 m/s. The location and velocity of the target is arbitrary, but when placed further away the JSR should increase and the results should appear more clearly. The pulse jammer is at the same distance as the object. The peak pulse power is increased until sufficient impact can be observed in the detection chain for any PRF.

4 Results

4.1 Matlab Model

4.1.1 Repeater Jamming

The first simulation is a scenario where a 10 dBsm object is at a range of 26m with a radial velocity of 0 m/s, i.e. same relative velocity as the FMCW radar system. The target emits a spoofing signal imitating a target with the same radial velocity but at a distance of only 12m. The results are shown in figure 30 to 32.

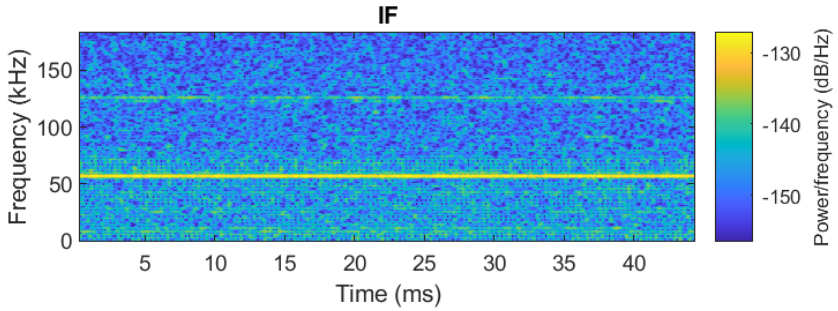
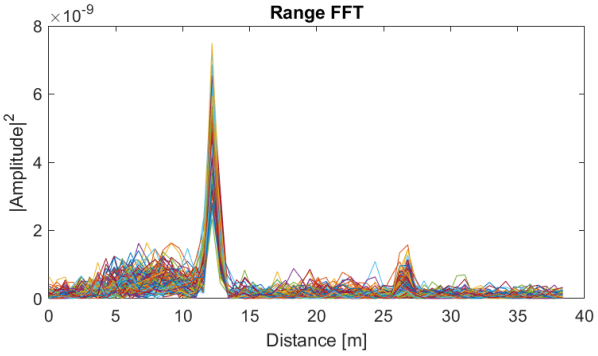
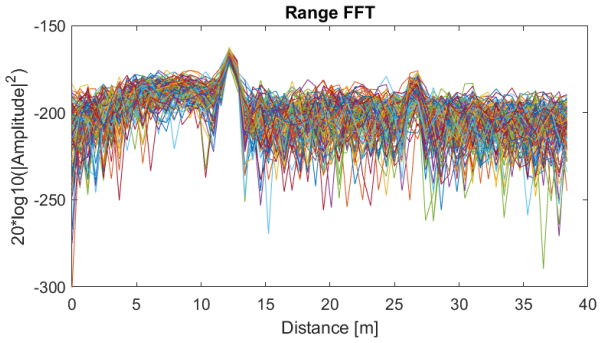


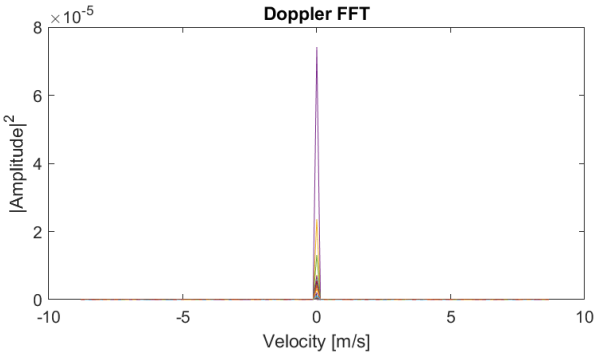
Figure 30: Shows the intermediate frequency signal when a simulated target is present at 26m and a false target at 12m.



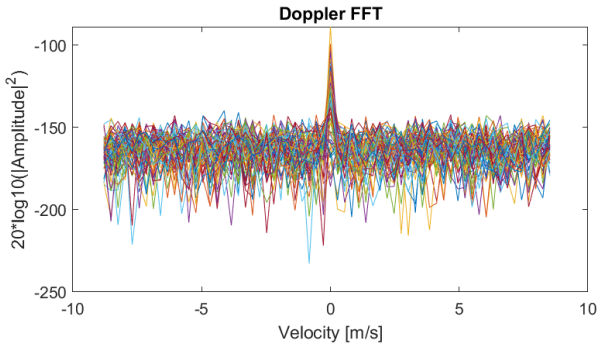
(a) The range-FFT of the data from the IF signal.



(b) The same data as in figure 31a but in decibels.



(c) The Doppler-FFT of the data from the IF signal.



(d) The same data as in figure 31c but in decibels.

Figure 31: The data from figure 30 having gone through range and Doppler-FFT.

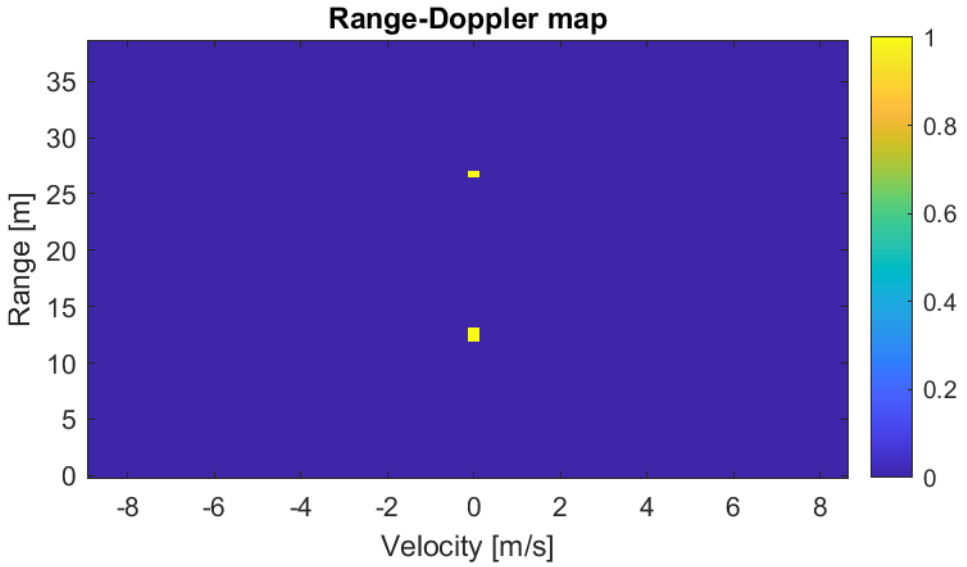


Figure 32: Shows the range-Doppler map after the data from figure 31 has gone through the CA-CFAR detector.

The second scenario is one where the real object emits a spoofing signal emulating a false target which is relatively close to the real target's location. A target at 20m moving with a closing velocity of 4 m/s is transmitting a spoof signal imitating an echo from a target at 25m moving away from the radar with 2 m/s. The results are shown in figure 33 to figure 35.

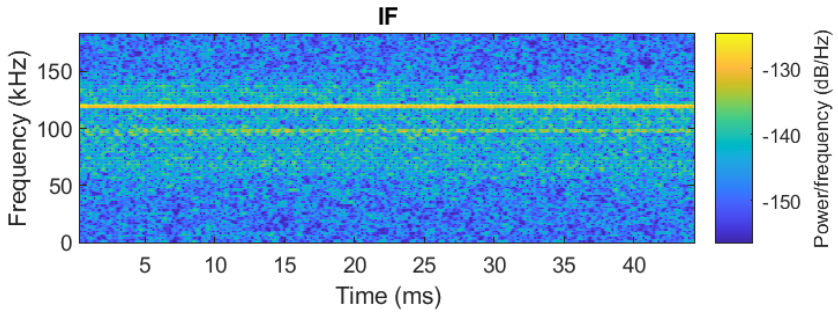
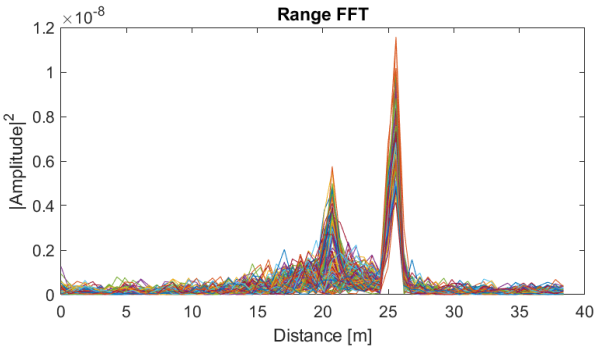
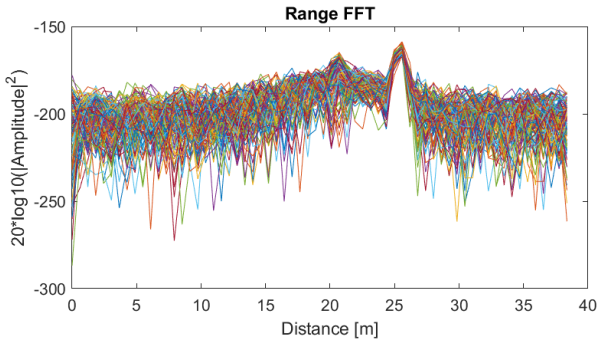


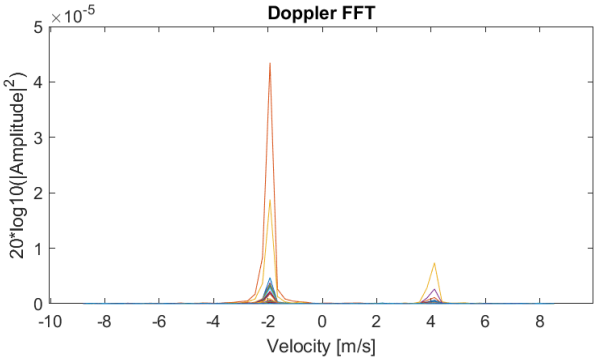
Figure 33: Shows the intermediate frequency signal when a simulated target is present at 20m and a false target at 25m.



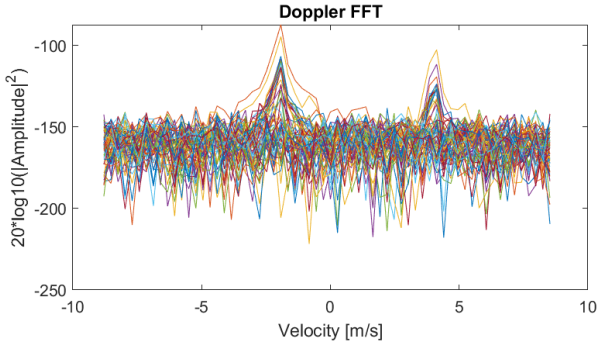
(a) The range-FFT of the data from the IF signal.



(b) The same data as in figure 34a but in decibels.



(c) The Doppler-FFT of the data from the IF signal.



(d) The same data as in figure 34c but in decibels.

Figure 34: The data from figure 33 having gone through range and Doppler-FFT.

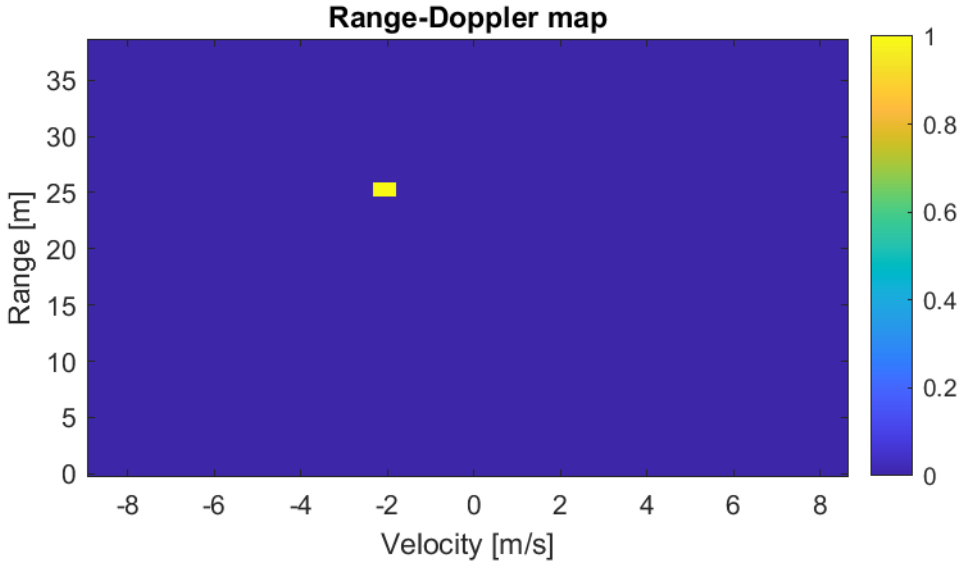


Figure 35: Shows the range-Doppler map after the data from figure 34 has gone through the CA-CFAR detector.

4.1.2 Pulse Jamming

The following sections presents the results from the simulations of an object at a distance of 30m traveling at 7 m/s while the radar is simultaneously being jammed by a pulsed Gaussian RF train of varying PRFs with a peak power set to $P_{peak} = 24$ dBW.

4.1.2.1 Intermediate Frequency Signals

This section presents the intermediate frequency spectrograms when the radar is subject to different jamming PRFs.

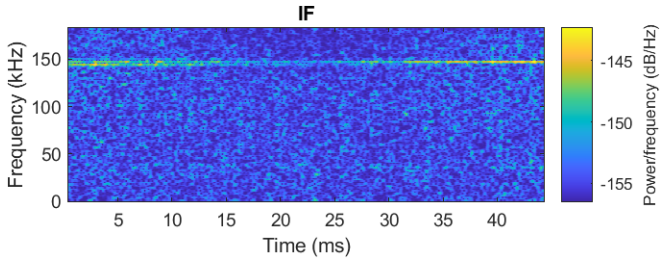
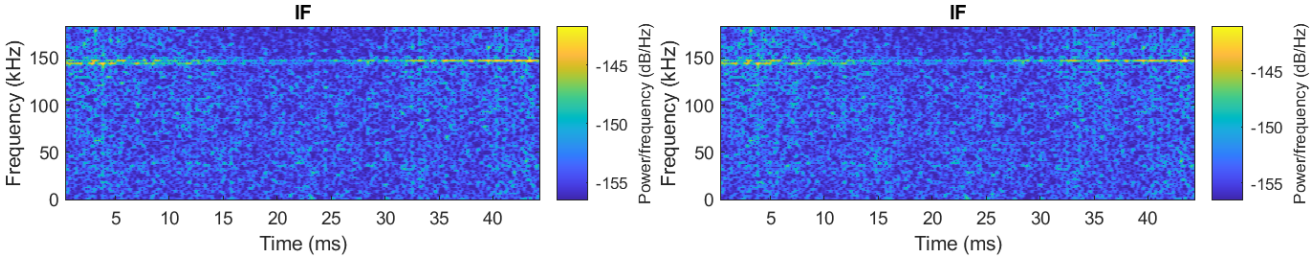
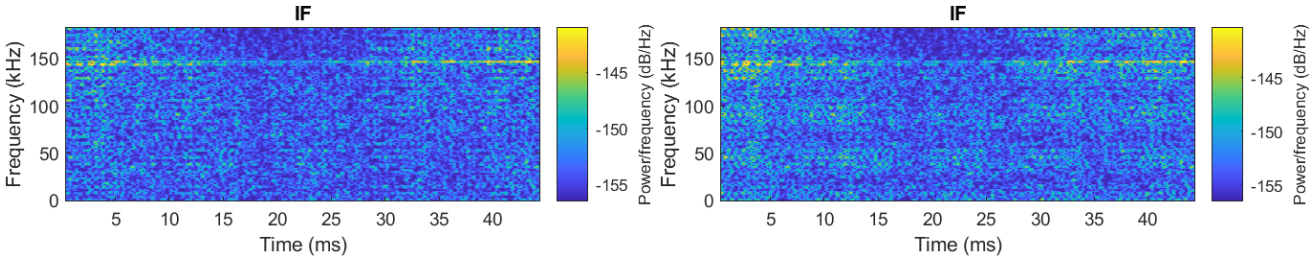


Figure 36: No jamming.



(a) Two pulses per FM period (5.635 kHz).

(b) Four pulses per FM period (11.270 kHz).



(c) Eight pulses per FM period (22.540 kHz).

(d) Sixteen pulses per FM period (45.080 kHz).

Figure 37: Shows the simulated intermediate frequency signals when the radar has a target in front of it while simultaneously being jammed with different PRFs.

4.1.2.2 Range-FFT

This section presents the Range-FFT data when the radar is subject to a Gaussian RF pulse train jamming signal with different PRFs.

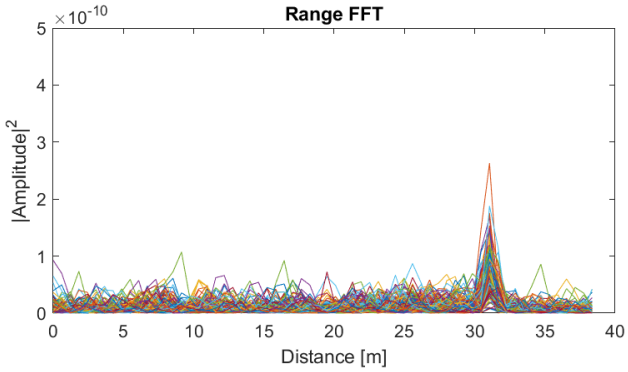
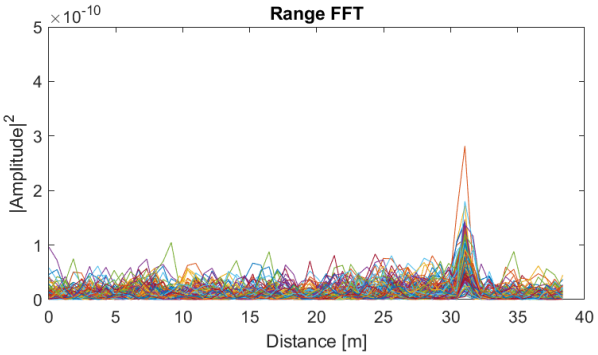
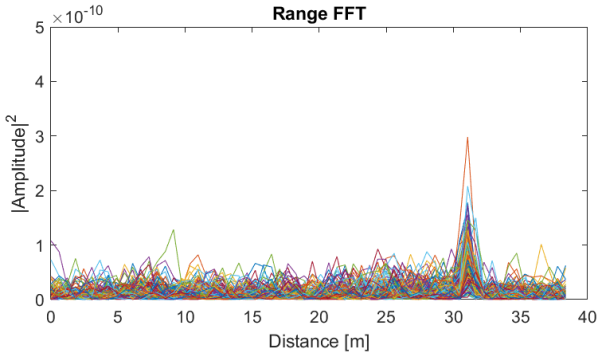


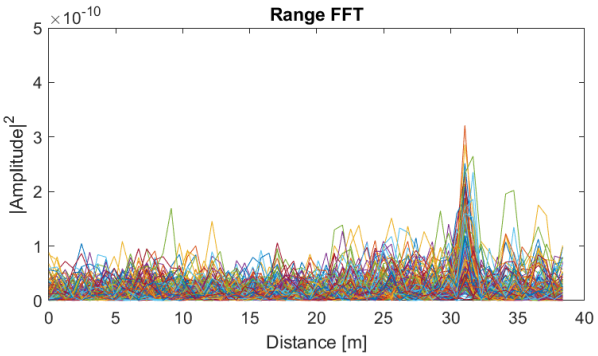
Figure 38: No jamming.



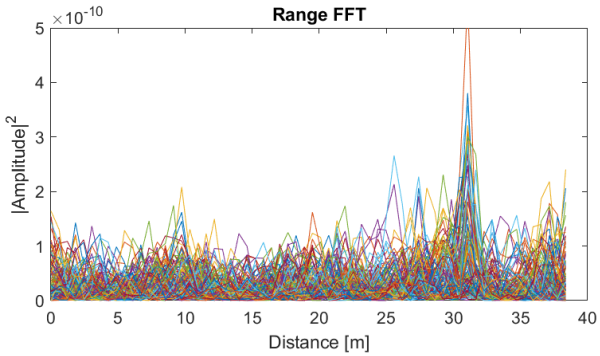
(a) Two pulses per FM period (5.635 kHz).



(b) Four pulses per FM period (11.270 kHz).



(c) Eight pulses per FM period (22.540 kHz).



(d) Sixteen pulses per FM period (45.080 kHz).

Figure 39: Shows the simulated Range-FFTs when the radar has a target in front of it while simultaneously being jammed with different PRFs.

4.1.2.3 Range-FFT (in dB)

This section presents the same data as in the preceding section but with the magnitude in decibels.

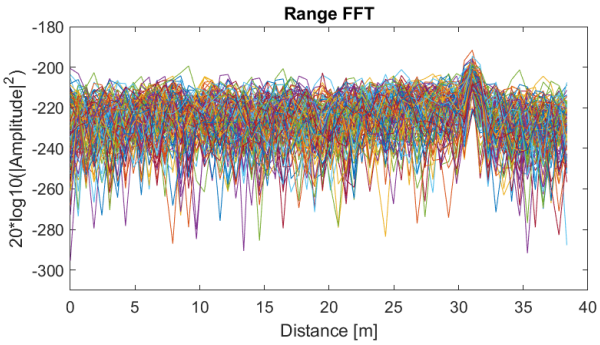
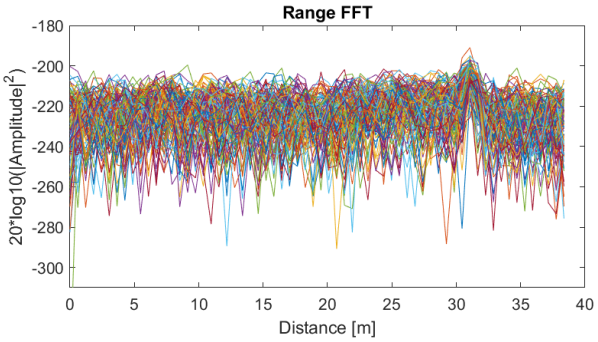
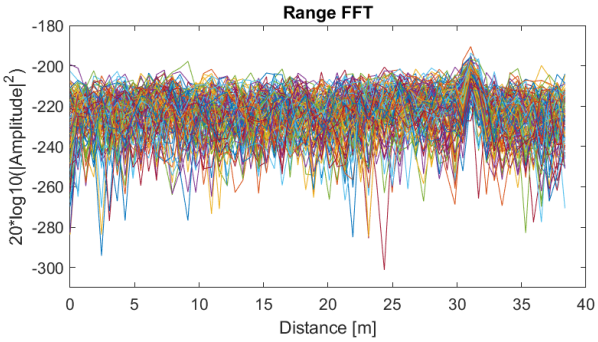


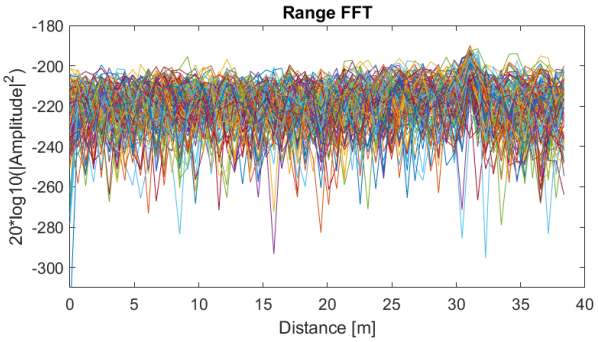
Figure 40: No jamming.



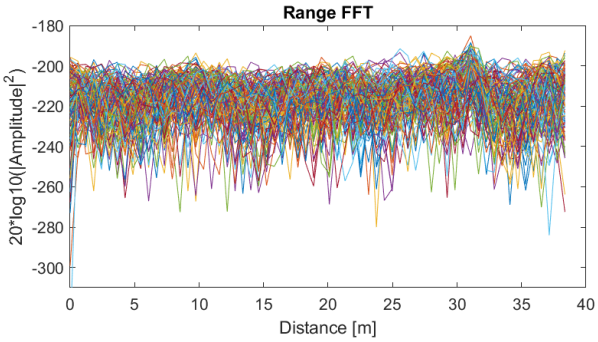
(a) Two pulses per FM period (5.635 kHz).



(b) Four pulses per FM period (11.270 kHz).



(c) Eight pulses per FM period (22.540 kHz).



(d) Sixteen pulses per FM period (45.080 kHz).

Figure 41: Shows the same range-FFTs as in figure 39 but in decibels.

4.1.2.4 Doppler-FFT

This section presents the Doppler-FFT data when the radar is subject to a Gaussian RF pulse train jamming signal with different PRFs.

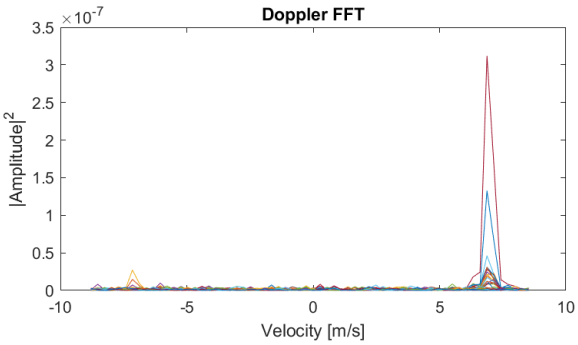
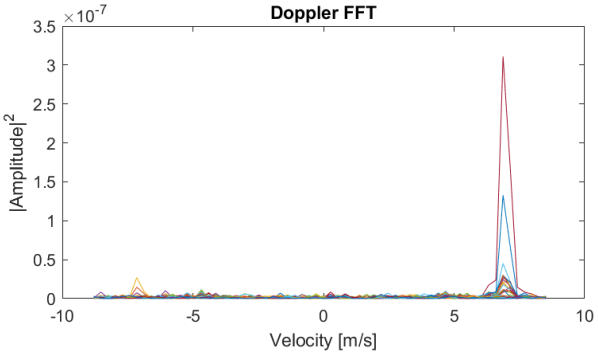
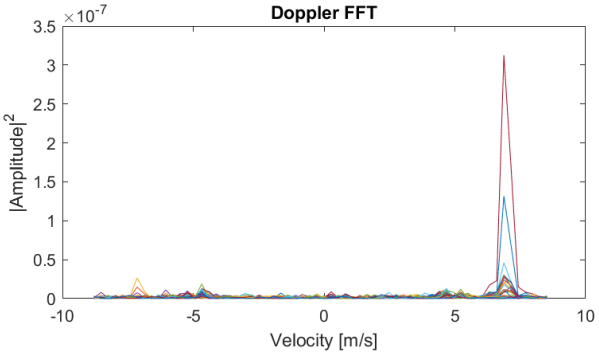


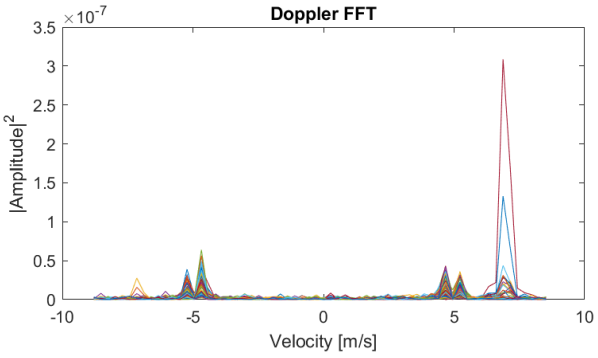
Figure 42: No jamming.



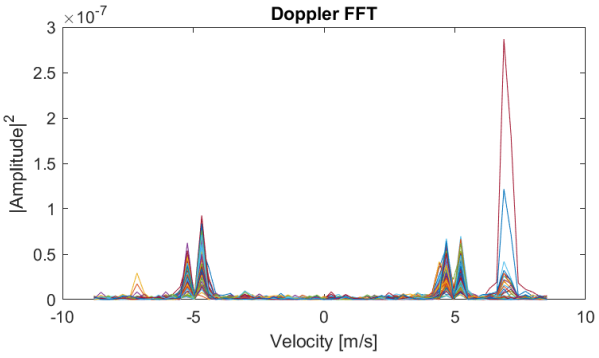
(a) Two pulses per FM period (5.635 kHz).



(b) Four pulses per FM period (11.270 kHz).



(c) Eight pulses per FM period (22.540 kHz).



(d) Sixteen pulses per FM period (45.080 kHz).

Figure 43: Shows the simulated Doppler-FFTs when the radar has a target in front of it while simultaneously being jammed with different PRFs.

4.1.2.5 Doppler-FFT (in dB)

This section presents the same data as in the preceding section but with the magnitude in decibels.

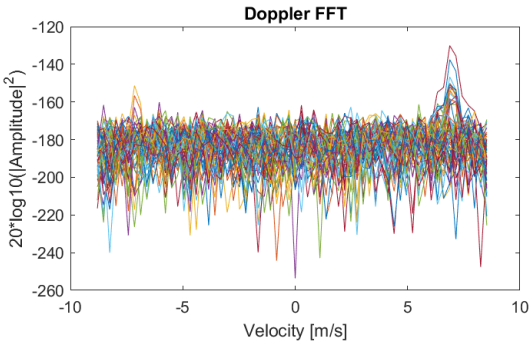
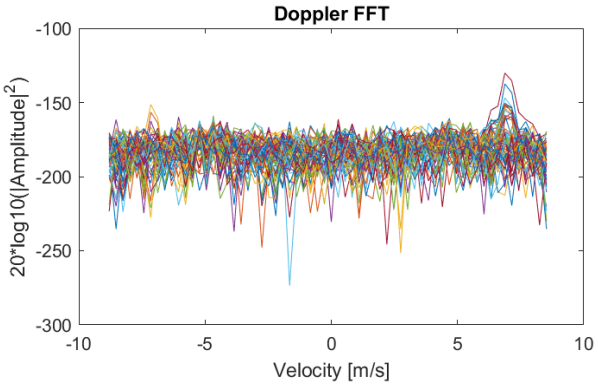
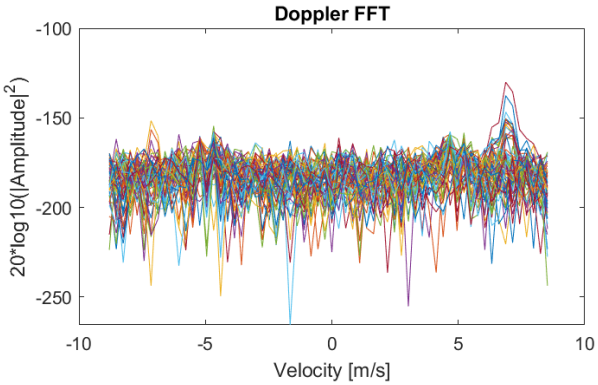


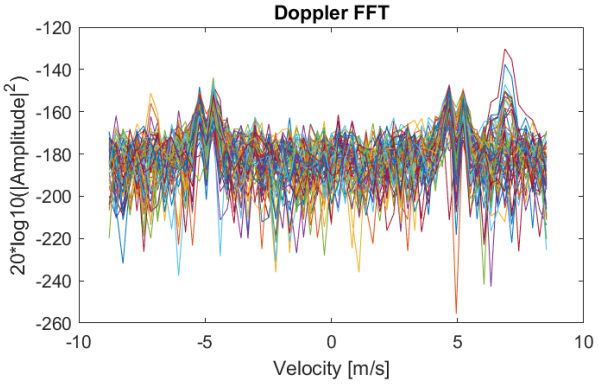
Figure 44: No jamming.



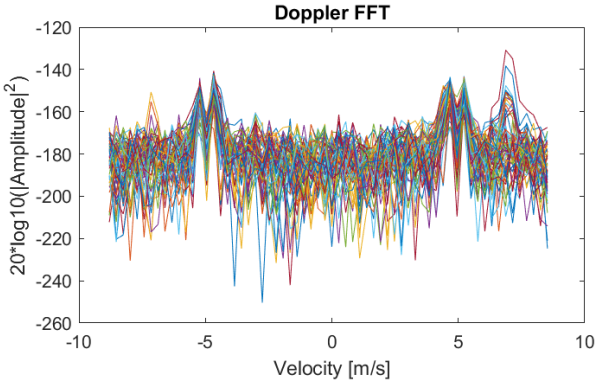
(a) Two pulses per FM period (5.635 kHz).



(b) Four pulses per FM period (11.270 kHz).



(c) Eight pulses per FM period (22.540 kHz).

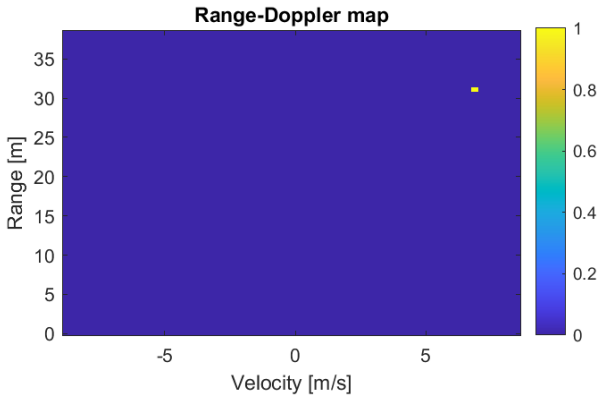


(d) Sixteen pulses per FM period (45.080 kHz).

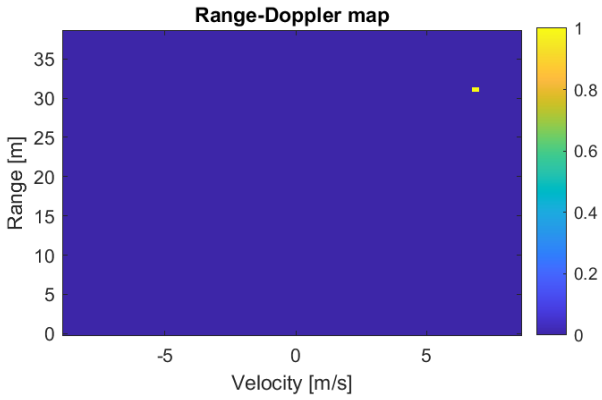
Figure 45: Shows the same Doppler-FFTs as in figure 43 but in decibels.

4.1.2.6 Range-Doppler Maps and Detections

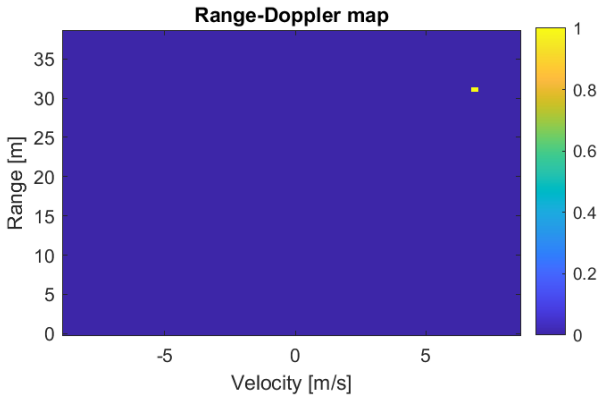
This sections presents the range-Doppler maps indicating positions, velocity and presence of the target while simultaneously being jammed with a Gaussian RF pulse train signal with different PRFs.



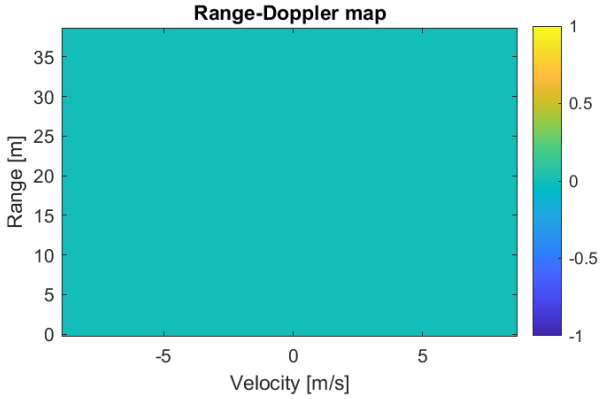
(a) Two pulses per FM period (5.635 kHz). Correct detection is made.



(b) Four pulses per FM period (11.270 kHz). Correct detection is made.



(c) Eight pulses per FM period (22.540 kHz). Correct detection is made.



(d) Sixteen pulses per FM period (45.080 kHz). No detection can be made.

Figure 46: Shows the simulated range-Doppler maps when the radar has a moving target in front of it while simultaneously being jammed with different PRFs.

5 Discussion

The results from the spoofing scenarios, i.e. using a repeater to mislead a simulated radar, showed promising results. The first spoof scenario simulated a stationary target at a smaller distance than the real object. As can be seen in figure 32 the repeater successfully injected a fake target into the system leading to a detection at a closer range, which could force e.g., a car with a distance-keeping FMCW radar to emergency brake or increase the distance to the real car at 26m. The successful injection of the false target agrees with the theory; the repeater waveform is coherent with the FMCW radar's transmitting signal and therefore receives no of the attenuation a random signal would experience. Furthermore, the repeater signal was quite a bit more intense than the energy reflected from the real echo due to only suffering one-way spreading losses. This is seen in figure 30 and figure 31a where the spoofing signal appears much stronger than the echo at 26m even though the repeater transmits at around 1% of P_t. It can therefore be deduced that the jamming-to-signal ratio, or JSR, is larger the further away the real target is and the spoofing can thus be more effective. The repeater could lower its transmit power to imitate a target of similar RCS, further indicating that such an adversarial system can be light and mobile. However, for the spoofing to be successful the repeater jammer needs to be tuned to the victim FMCW radar's bandwidth, sweep rate, modulation period and so on. In other words, spoofing requires considerable knowledge about the victim radar which might not always be readily available on the fly. On the other hand, with sufficient knowledge about the victim radar system a repeater jammer can be very efficient; a crude system would have no way of distinguishing a real target from a fake one. A more competent system could disregard fake targets with a non-zero radial velocity if e.g., the range does not change during some time interval, but perhaps a more efficient anti-spoofing solution would be to vary the sweep-rate and modulation period every now and then while compensating with bandwidth or carrier frequency to keep the design parameters the same. Such an approach would negate a spoofing attempt since the jamming waveform becomes non-coherent and would get attenuated. A parameter-varying FMCW system would make repeater jamming much more strenuous and forces continuous synchronizing of the adversarial system, adding system complexity and power consumption to any hostile EW system.

Perhaps often negligible in the context of long-range radar spoofing is the internal delay of the signal traveling through the repeater unit. The max range of an FMCW radar used in vehicles or motion detectors can be a few tens of meters which can pose a challenge in a spoofing attempts since a delay of e.g., 150 ns equals an extra distance of 45m added when the repeater finally starts retransmitting. Of course, one may then simply add a static delay to the transmission so that it matches with the subsequent chirp and then start to generate false targets. On the other hand, there is nothing stopping the victim radar from initializing each chirp with a random phase which in this case would result in the retransmitted spoofing chirp appearing incoherent to the subsequent chirp in turn leading to severe attenuation. Therefore, when using a repeater one must also take into consideration the internal signal delay and if it is significant then some measures must be taken in order to counteract the fact that the chirp is no longer coherent.

The second spoofing scenario emits a coherent signal back to the RX antenna which imitates the return of a target which is relatively close to the real object. This approach requires matching or surpassing the real echo's energy so that the threshold is increased. It is found that by emitting a spoofing signal which injects a false target that is spatially close to the real object the threshold could quench the weaker FFT peak, as seen in figure 35. The spoofing signal created a fake target at a different range with a velocity even differing in sign while simultaneously drowning out the real echo. An adversarial repeater could confuse a victim FMCW automotive radar and lead it to believe that the car in front of it is emergency braking while the real target remains hidden. A plethora of other similar possibilities not discussed in this paper is also applicable. Nonetheless, the results from the simulation is based off a singular antenna which results in the radar system not being able to determine the angle of arrival; two or more RX antennas would be able to differentiate two targets having separate AoAs. In addition, the scenario discussed is also highly dependent on the type of CFAR algorithm applied to the FFT data. For example, SO-CFAR would use the leftmost data in figure 34a to calculate the threshold level instead of also incorporating the large FFT peak to the right like CA-CFAR does, which would defeat the spoofing attempt shown. In other scenarios more sophisticated CFAR algorithms like OSGO-CFAR or CMLD-CFAR may need to be used due to several

closely spaced false targets appearing simultaneously. Yet, the results indicate that a repeater can mislead and confuse an FMCW radar which utilizes simpler detection algorithms by placing targets close to each other in either distance or radial velocity. Angular measurements and more complex CFAR algorithms may be able to circumvent such spoofing attempts.

The pulse jamming utilizing a Gaussian RF pulse train showed varied results. Four pulse trains with different PRFs with identical ERP were injected into the FMCW RX signal to observe any increase of noise even at relatively low repetition frequencies. The peak power was raised until any effects started to appear, which occured roughly around $P_{peak} = 24$ dBW. From figure 37 it is evident that the noise in the spectrogram is the highest when $f_{PRF} = 45.080$ kHz, but some noise is observed at $f_{PRF} = 11.270$ kHz and $f_{PRF} = 22.540$ kHz. The presence of noise being successfully added is more noticeable in figure 39 and figure 41. Barely any difference between the absence of pulse noise and $f_{PRF} = 5.635$ kHz can be seen. Yet, the results indicate that the pulse jamming becomes more efficient the higher the PRF is, which is especially obvious from figure 43 and figure 46d, where the pulse train with $f_{PRF} = 45.080$ kHz managed to raise the threshold level sufficiently high that the real target could not be differentiated from background noise. This is expected, since the amount of energy in the pulse train increases with a higher PRF. On the other hand, at a certain point it becomes meaningless to increase the PRF since the whole point of using pulses instead of continuous jamming is that pulse jammers can often achieve a higher P_{peak} compared to its continuous counterpart when concentrating the energy packets in short bursts. Another interesting observation is that the noise carried over into the Doppler-FFT is significantly lower than in the range-FFT as seen in figure 43. Even at $f_{PRF} = 45.080$ kHz it is obvious that some target has a radial velocity of 7 m/s. Perhaps this is due to adding another layer of DFT attenuation on top of the already weakened noise. This may indicate a strength of FMCW radars and the DSP behind them - the embedded Doppler-FFT can be difficult to affect with non-coherent or even semi-coherent noise, so a system being jammed with sufficient power to render the distance measuring useless can still determine velocities of targets. A more sophisticated platform would then be able to use a secondary system like pulsed radar or LiDAR to gauge the distance while still relying on the FMCW Doppler measurements. In addition to that finding, some conspicuous peaks apart from the target's velocity show up in the Doppler-FFT, which is clearly visible in figure 45c and figure 45d. It is most likely that the peaks are simply an aliasing remnant of the pulse train. This would make sense since the magnitudes of the peaks increase whenever the PRF grows, indicating that more energy is injected into the FMCW radar. Moreover, with sufficient repetition frequency these peaks could successfully increase the threshold level to the point where it is no longer possible to determine velocity with CA-CFAR.

At any rate, the pulse train was severely undersampled which was due to memory shortage on the computer used. Each pulse had a center frequency of 24.125 GHz and a bandwidth of 250 MHz, and to accurately recreate it a sample frequency of about 48 GHz would need to be used according to the Nyquist-Shannon theorem. Sampling at that frequency for a whole time frame T_f (45.7 ms) resulted in the simulation running out of memory. A trade-off had to be done, and at a pulse train sampling frequency of 205 MHz the characteristics of the pulse train was visible while the simulation did not run into any memory issues. Moreover, the ERP of the jamming signal is unreasonably high since 24 dBW is not practical for a mobile and light device. However, it is around that wattage that the jamming starts to provide noticeable effects on the output of the simulated FMCW radar. On the other hand, the high ERP may be an effect of the undersampled pulse train since it is impossible to include every pulse at a fraction of the Nyquist frequency. In other words, the pulse train has a lower effective PRF than what it should have. Thus, it may be possible that by increasing the ERP the lack of a complete pulse train can be compensated for. In other words, a pulse jammer used in a real-life situation might not need nearly the same wattage to achieve a similar effect as shown in the results above since it will not run into any problems caused by an undersampled signal. Nonetheless, the results indicate a more effective jamming with higher PRFs which at some point may raise the noise floor to an extent that target detection is no longer possible. The exact power and PRF required to accomplish that is not possible to extract from this simulation and is dependent on e.g., JSR and the type of detection algorithms used by the radar.

6 Conclusion

Two different jamming approaches and their effects on an FMCW radar were studied in a simulated environment. An FMCW radar with its key digital signal processing concepts was built in Matlab along with visualization tools to help observe the effects on range and Doppler measurements. The radar design parameters are based on an off-the-shelf product used in the context of advanced driver-assistance systems and the first half of the thesis was spent determining these parameters through calculations and simulations. The latter half was spent on simulating a repeater injecting false targets in the DSP chain and a pulse jammer injecting noise in order to raise the threshold level responsible for determining the presence of targets.

The repeater simulations showed that such spoofing attempts can be very effective in creating false targets since a repeater is emitting coherent waveforms no different than a reflected echo. Thus, a false target could appear just as real as a physical object in front of the radar. Another scenario also showed that depending on the detection algorithm used by the radar, the adversarial repeater is able to cause real targets to seemingly disappear by placing the false target adjacent to the actual object. Hence, the simulations also emphasizes a shortcoming of the CA-CFAR algorithm used in conjunction with several closely spaced targets. On the other hand, repeater jamming requires a lot of knowledge about the victim radar which might not be readily available, highlighting a potential flaw of this approach since synchronizing to a low-probability-of-intercept radar like FMCW is not the easiest of tasks.

Simulations of Gaussian RF pulse injections into the FMCW radar DSP chain had varied results. It showed that it did have a noticeable effect on the radar's ability to detect targets, even going as far as to entirely negating the detection of an object when the pulse repetition frequency was sufficiently high. Furthermore, the simulations showed that Doppler measurements were less affected by injected noise than the range gauging, which could make an FMCW radar still be reliable in determining velocity while range acquisition is rendered useless. However, the effective radiated power used in the simulation is unreasonably high in comparison to the output power of the victim radar, which may be due to poor sampling of the pulse train. Thus, the simulations cannot be used to draw any conclusions about the exact ERP and PRF to use in a similar real-life scenario.

Further research on this topic could include testing the jamming approaches on the actual hardware to see how the adversarial systems would perform in a non-ideal environment where there is clutter, thermal noise and a plethora of other factors that could interfere with the efficiency of a jamming attempt. It would also be interesting to investigate other jamming techniques such as random noise jamming of different noise colors or unintentional interference stemming from the use of other radars in the same ISM band.

References

[1] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*. Chapman and Hall/CRC, 2013.

[2] R. G. Wiley, *Electronic Intelligence: The Analysis of Radar Signals*. Artech House Inc., 1993.

[3] C. Wolff, "Corner reflectors." Available: https://www.radartutorial.eu/17.bauteile/bt47.en.html, radartutorial.eu.

[4] "Trihedral Corner Reflector." Available: https://www.miwv.com/wp-content/uploads/2020/06/Trihedral-Reflectors-for-Radar-Applications.pdf, Millimeter Wave Products Inc.

[5] "One-way radar equation / RF propagation." Available: https://www.phys.hawaii.edu/~anita/new/papers/militaryHandbook/one-way.PDF, UHM Physics and Astronomy.

[6] S. Rao, "Introduction to mmwave Sensing: FMCW Radars." Texas Instruments, unpublished.

[7] S. Suleymanov, "Design and Implementation of an FMCW Radar Signal Processing Module for Automotive Applications," Master's thesis, University of Twente, 2016.

[8] H.-R. Chen, "FMCW radar jamming techniques and analysis," Master's thesis, Naval Postgraduate School, 2013.

[9] L. Hassbring and J. Nilsson, "Machine Learning for FMCW Radar Interference Mitigation," Master's thesis, Lund University, 2020.

[10] A. Lazaro, A. Porcel, M. Lazaro, R. Villarino, and D. Girbau, "Spoofing Attacks on FMCW Radars with Low-Cost Backscatter Tags," *Sensors (Basel)*, 2022.

[11] D. Vivet, P. Checchin, and R. Chapuis, "Localization and Mapping Using Only a Rotating FMCW Radar Sensor," *Sensors (Basel)*, vol. 13, no. 4, pp. 4527–4552, 2013.

[12] M. Parker, *Digital Signal Processing 101*. Newnes, 2017.

[13] N. Instruments, "Understanding FFTs and Windowing." https://download.ni.com/evaluation/pxi/Understanding%20FFTs%20and%20Windowing.pdf, 2021 [obtained 2023-03-30].

[14] G. M. Hatem, J. W. A. Sadah, and T. R. Saeed, "Comparative study of various cfar algorithms for non-homogenous environments," *IOP Conference Series: Materials Science and Engineering*, vol. 433, p. 012080, November 2018.

[15] A. Sjöberg, "LPI waveforms for AESA radar," Master's thesis, Uppsala University, 2020.

[16] R. Komissarov and A. Wool, "Spoofing attacks against vehicular FMCW radar," *CoRR*, vol. abs/2104.13318, 2021.

[17] R. M. Gray and J. W. Goodman, *Fourier Transforms: An Introduction for Engineers*. Kluwer Academic Publishers Group, 1995.

A Discrete Fourier transform and FFT

If a signal is sampled in time then the discrete time Fourier transform is:

$$X(e^{j\omega}) = \sum_{n=0}^{N-1} x[n]e^{-j\omega n} \tag{39}$$

where ω is continuous. Since $e^{-j\omega n}$ can be expressed in sine and cosine through Euler's formula, the LHS of the equation above can be thought of as the correlation between x[n] and a unit signal with angular frequency ω.

Another case is when the frequency is discretized such that ω is:

$$\omega_k = \frac{2\pi}{N}k \tag{40}$$

where k = 0, 1,..., N-1. Equation 39 then becomes [17]:

$$X[k] = \sum_{n=0}^{N-1} x[n]e^{-j\frac{2\pi}{N}kn} \tag{41}$$

Equation 41 is the discrete Fourier transform. Similar to the previous analogy, $X[k]$ can now be thought of as the correlation between $x[n]$ and a unit signal with frequency k. Thus, when DFT is performed on a sampled signal the magnitude of $X[k]$ will be large whenever $x[n]$ matches with the frequency k. This can be seen as peaks in a frequency plot.

When DFT is implemented digitally it is usually done so through an algorithm called fast Fourier transform, more commonly referred to as FFT. The FFT algorithm is able to perform DFT on a dataset on length N in $Nlog(N)$ adds/multiplications instead of the N^2 adds/multiplications needed to acquire the DFT by brute force [17]. The algorithm is optimized when the length of the dataset is a power of 2, so the dataset is padded with zeros whenever necessary.