A PLATFORM FOR FALSE DATA INJECTION IN FREQUENCY MODULATED CONTINUOUS WAVE RADAR

by

Ruchir Chauhan

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Electrical Engineering

Approved:

Dr. Ryan Gerdes Major Professor	Dr. Reyhan Baktur Committee Member
Dr. Scott Budge Committee Member	Dr. Mark R. McLellan Vice President for Research and Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2014

Abstract

A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar

by

Ruchir Chauhan, Master of Science

Utah State University, 2014

Major Professor: Dr. Ryan Gerdes
Department: Electrical and Computer Engineering

Frequency-modulated continuous-wave (FMCW) radars are widely used in vehicle automation technologies such as adaptive cruise control (ACC) and collision avoidance systems (CAS), which are now gradually replacing cruise control systems, to give vehicles autonomous capabilities. But in designing these systems, little attention has been given to security, and these systems are prone to attacks similar to the ones common in warfare radars, such as jamming and injecting false distance/velocity information, and in light of the fact that these and similar mechanisms are soon going to be an integral part of automobiles, such attacks are capable of exploiting the vulnerabilities in the system and compromising the whole purpose of making these systems.

In this work one such vulnerability in FMCW radar was exploited to design an attack that was capable of decreasing the apparent distance, as measured by a radar system. A platform to carry out a false distance/velocity information attack against FMCW radar was conceptualized, built, and experimentally validated. With a main focus on decreasing the apparent range of an object of interest through the analog channel, a range-decreasing attack was verified for feasibility through simulation and by carrying out the attack against an FMCW radar modeled on automotive radars and built using software-defined radios. The software-defined radio system specifically used in this experimentation is the Universal

Software Radio Peripheral (USRP) by Ettus Research. Results indicate that it is possible to decrease apparent object range in general and by arbitrary amounts in particular, with very high probability of success.

(78 pages)

Public Abstract

A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar

by

Ruchir Chauhan, Master of Science

Utah State University, 2014

Major Professor: Dr. Ryan Gerdes
Department: Electrical and Computer Engineering

Radar is an acronym for RAdio Detection And Ranging. In general terms, it is a machine that uses radio waves for object-detection in its near periphery. It transmits radio waves in a known direction, which when intercepted by an obstruction/object are reflected by its surface and are received back at the radar system. The round trip delay time along with the known velocity of radio waves gives an accurate measurement of the distance of the object from the radar system. In a somewhat similar fashion, some radars are even capable of measuring the velocity of this object. Frequency-modulated continuous-wave (FMCW) radar is one such radar system, which is a subclass of continuous wave (CW) radars, where a continuous sinusoidal radio energy is transmitted, reflected, and received back at the radar system. These radar systems are widely used in vehicle automation technologies such as adaptive cruise control (ACC) and collision avoidance systems (CAS) to measure the distance from the nearest vehicles and maintain a safe following distance. But in designing these systems, little attention has been given to security, and these systems have vulnerabilities that are capable of compromising the whole purpose of making such systems.

In this work one such vulnerability in FMCW radar was exploited to design an attack that was capable of decreasing the apparent distance, as measured by a radar system. The attack was designed in such a way that there was no tampering with the radar system being attacked. Instead, false distance information was introduced in the return path of the transmitted radio wave by absorbing the original victim transmission and sending out a modified radio wave on the return path. It was shown that the distance could be decreased to alarming values, which at the level of the vehicle automation system results in decreasing the speed of the automobile when actually it should have increased.

To my loving family.

Acknowledgments

I graciously extend my gratitude towards my advisor, Dr. Ryan Gerdes, for giving me this opportunity to work with him, guiding me through all the turns where roads were hazy, for motivating and sharing his knowledge and enthusiasm for hardware security.

Besides my advisor, I would like to thank my other committee members, Dr. Reyhan Baktur and Dr. Scott Budge, for their insightful comments. I would also like to thank Heidi Harper for her help with setting up a part of the system for physical simulation.

Finally, I would like to thank my family; my parents for their unconditional support throughout my degree, through all ups and downs and for having faith in me; my little sister Vidhi, for her care and affection; and my fiance Prachi, for being my strength and inspiration and for her unconditional love.

Ruchir Chauhan

Contents

List of Tables

List of Figures

Acronyms

ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
CAS	Collision Avoidance System
CFAR	Constant False Alarm Rate
CW	Continuous Wave
ECM	Electronic Counter Measure
FDI	False Data Injection
FFT	Fast Fourier Transform
FMCW	Frequency Modulated Continuous Wave
FPGA	Field Programmable Gate Array
GPS	Global Positioning System
IR	Impulse Radio
MIMO	Multiple Input Multiple Output
OS-CFAR	Ordered Statistic Constant False Alarm Rate
RAM	Radar Absorbing Material
RADAR	RAdio Detection And Ranging
RCS	Radar Cross Section
RF	Radio Frequency
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
UHD	USRP Hardware Driver
USRP	Universal Software Radio Peripheral
VCO	Voltage Controlled Oscillator

Chapter 1

Introduction

1.1 Background

German physicist Heinrich Hertz, in 1886, established that radio waves could be reflected from solid objects, a concept that would later give birth to many applications of general and military use. One such invention, RAdio Detection And Ranging, popularly known as radar, independently developed in a veil of great secrecy before the Second World War [1] by researchers in France, Germany, Italy, Japan, the Netherlands, the Soviet Union, the UK, and the US, has come a long way since its inception, from being of exclusive war application to being at the core of vehicle automation systems.

Frequency-modulated continuous-wave (FMCW) radars are widely used in sensing applications to acquire the range and velocity of objects of interest [2]. By virtue of their cost, power characteristics, low measurement time, computational complexity [3], and high bandwidth [4], FMCW radars have proven especially popular in vehicle automation technologies, such as adaptive cruise control (ACC) and collision avoidance (CA) systems [5,6]. Available from all major automotive manufacturers, these technologies represent the first stage of vehicle automation by helping vehicles to automatically maintain a safe following distance in changing traffic flows (ACC) and brake when an obstruction is identified (CA) [7,8]. As has been stated, radar technology has come a long way. All along this journey, one feature of this invention remains consistent among all its applications, its ability to assist in defending against potential threats, be it from incoming missiles, fighter jets, or automobiles in the immediate periphery. Examined under this light, what could be worse than a defense mechanism against potential threats turned into a threat itself? In spite of their long use in both military and civilian applications, no work has come to light that examines the vulnerability of FMCW radars to analog false data injection (FDI) attacks aimed at altering the apparent distance/velocity of an object. A fair question would be: Why would an attacker want to mount such an attack and what could be some possible negative effects of this kind of attack?

The following two scenarios can be considered motivating enough to answer these questions.

- Collision avoidance system attack: Collision avoidance system (CAS), also termed precrash system or forward collision warning system, is an automobile safety system designed to mitigate the severity of a potential accident or, even better, proactively avoid one from occurring. Radar, laser, and cameras are the widely used sensors in this type of system, used to detect range or velocity or both of a vehicle in front. This system is so well integrated within the automobile that it is capable of detecting and providing warning signs to the driver when a crash is imminent, and in dire scenarios even take actions autonomously. An attack, such as the one examined in the present work, on the analog channel of a collision avoidance system's radar system can modify the victim's radar transmissions on their return path to make it appear as though they were reflected from an object much closer to the radar system than it actually is. This can make the car slam on the brakes abruptly and can even lead to an accident if the car is moving at a very high speed on a freeway, compromising the whole purpose of having this system in the first place.

- Jeopardizing a platoon of vehicles: Vehicle platooning is a highway automation system in which vehicles are grouped and follow a lead vehicle, drastically increasing the capacity of roads. It has its potential benefits such as greater fuel economy due to reduced air resistance, reduced congestion, and fewer traffic collisions [9, 10]. One way to control vehicles in a platoon is to equip the vehicles with range and velocity sensors like radar or laser sensor to measure the distance and velocity of the preceding vehicle [11]. Chang et al. [12] describes how in conjunction with range and velocity sensors, platooning on a highway is also supported by inter-vehicle communication architecture. Using this architecture the lead vehicle of a platoon can share its information, such as, time clock, vehicle speed, and acceleration with the following vehicle [12]. Since these systems use wireless channel for communication, they expose themselves to security threats [13] as discussed by Blum and Eskandarian [14]. They examine a concept of *intelligent collisions* that is a class of threats involving hackers attacking the wireless communication channel used in inter-vehicle communication architecture, with a goal to cause accidents. They examine in great detail how this channel sharing exposes the network to denial-of-service attacks and also to false-data injection attacks such as impersonation, fabrication, or modification of data. Blum and Eskandarian [14] also observe that the wireless channel of inter-vehicle communication architecture is vulnerable to false-data injection attacks due to the absence of any authentication mechanism for the origin of a signal. Similarly, if the attacker shows up anywhere in a platoon it can mount the present attack, making it appear to the following vehicle that the distance in between them is less than it actually is and given the small spacing between two vehicles of a platoon, accident is inevitable.

1.2 Related Work

An electronic counter measure (ECM) is an electronic device designed to deceive radar, sonar, and other detection systems. The creation of ECMs coincided with the inception and development of radar systems in the Second World War. The earliest forms of ECM included deception by producing swarms of pulses to make the radar believe it was receiving reflections off a large object or formation, deliberate jamming, and sowing a dense field of spurious reflectors [1]. Basic radar ECM techniques that are commonly deployed in the battlefield are as follows [15].

- Radar interference: These techniques involve jamming and deception. Jamming at any frequency is accomplished by transmitting at the same frequency but at levels much higher than that of legitimate transmissions. This results in blocking the legitimate transmissions and disrupting the communication channel. A more sophisticated attack is deception, wherein the jammer has the ability to mimic radar echo, which it then uses with a delay in order to create targets at false range.

- Target modification: The technique involves tricking a victim into believing wrong information about the size and shape of a target. This is accomplished by coating the target with radar-absorbing material (RAM) or by modifying its outer reflective surface. The purpose of using radar-absorbing material or outer surface modification is to decrease the radar cross-section (RCS) in certain frequencies. RCS is the effective area of an object visible to a radar.
- Modifying the electrical properties of air: Aircraft and targets spread thin pieces of aluminum or metallized glass fiber, commonly known as chaff, in the air, to deluge the radar with multiple false returns, suggesting the presence of multiple targets, thus cloaking the original target.

There has been a considerable history of spoofing radar reflections using digital radio frequency memory (DRFM) [16] and deceptive jamming techniques such as range gate pull off (RGPO) [17]. DRFM techniques involve capturing an incoming signal and retransmitting it after some modification at a later time to create false targets. A DRFM system on one hand creates a digital duplicate of the captured incoming RF signal that is coherent with the original source of that RF signal. This digital replica of the original analog signal can then be reconstructed and transmitted at a later time when required. RGPO, on the other hand, has as its major objective breaking the “lock-on” state that a radar system places in order to identify potential targets with precision. This technique is executed in a sequence of steps, initiating with low-power transmissions to jam the radar system. The power is gradually increased, which in turn makes the victim radar bring down its own gain levels, thus desensitizing itself to real received signals. Once this process is in place for a period of time, the attacker is said to have stolen the range gates and is now capable of fooling the victim radar into detecting false targets.

Yet another relevant domain of related works is attacks on distance-bounding protocols. Distance-bounding protocols are cryptographic protocols that provide a way for a verifier A to establish an upper bound on the spatial distance to a prover B. The upper bound calculations are made, based on the round-trip delay measured between sending out challenge bits for B and receiving back the corresponding response bits from B. It is a distance estimation technique and is vulnerable to internal and external attacks [18]. Clulow et al. [19] exposed the vulnerability in the proposed distance-bounding protocols of Hu et al. [20, 21], Sastry et al. [22], and Capkun and Hubaux [18, 23] by carrying out guessing attacks. Sastry et al. [22] designed a new protocol for location verification which they call echo protocol. In this protocol first the verifier A establishes if a prover is inside a circle centered at A. The verifier then sends a packet containing a nonce to the prover over a radio channel, upon which the prover echoes back the packet to the verifier but this time over ultrasound. The verifier already has an upper-bound distance, which then is compared to the round-trip time taken by the prover to respond to the packet. This is how the location of a prover is verified. Capkun and Hubaux [18, 23] proposed a technique they call "verifiable multilateration" to securely verify positions of mobile devices. They propose using three or four verifier reference points, instead of using just one, for a prover to prove its distance. These are single-exchange challenge-response protocols and Clulow et al. [19] proposed that they are prone to guessing attacks. The attacker can guess the last bit transmitted by the verifier and transmit a response, thus gaining on the round-trip time. It was found that the attacker can guess the correct bit 50% of the time. Clulow et al. [19] also introduced physical-layer attacks such as early-detect and late-commit attacks. Ranganathan et al. [24] demonstrated the feasibility of physical-layer attacks on chirp-based ranging systems. A chirp-based ranging system is the one in which the transmitted wave is a sinusoid whose frequency varies over time. The frequency variation depends on the chirp selected. The concept is discussed at length in chapter 2 alongside the discussion of FMCW radar, which is a chirp-based ranging system. They discuss two methods of early detection.

- Zero crossing detectors: They detect the transition of a signal waveform through zero level. In this method they observe the signal over a small period of time that is shorter than the chirp duration, and the number of zero crossings thus detected are then compared to template chirps to predict symbol value. They were able to early detect by observing at least 20% of the chirp duration.

- Early correlation using dispersive delay lines: Their results indicate that it is possible to predict early by correlating over only 5% of the chirp duration.

Their experimental results showed that an attacker can decrease the distance by more than 150 m for 1 µs chirps and approximately 600 m for 4 µs [24].

Nighswander et al. proposed a new hardware platform for global-positioning system (GPS) attacks and developed novel attacks against GPS systems [25]. They showed how GPS-dependent systems are more vulnerable than previously thought by expanding the attack surface to include the data and OS layer. For example, they verified two spoofed modes for position spoofing: first, for spoofing receivers going in a certain direction at a particular velocity and second, for receivers going in a circle.

Most closely related is the Cicada attack of Poturalski et al. [26], in which degradation and denial of service in impulse radio (IR) ranging in multipath environment are used to effect a distance spoofing attack. In this attack the attacker degrades the performance of receivers based on energy detection, resulting either in effective distance reduction or complete denial of service, by continuously transmitting a sequence of pulses in a multipath environment with power greater than that of the authentic transmitter. Consider two transceivers A and B. A transmits a sequence of pulses as preamble for B to estimate the time of arrival. Now if a third node M with malicious intentions transmits its own much stronger sequence of pulses constantly, it travels along with the original preamble in this multipath environment and based on strength, B will accept and lock on M's transmission, rejecting A's packet, resulting in denial of service. Similarly, even if the strength of M is less than A and in fact B does lock on A's preamble, there does exist a chance that the search algorithm will estimate a wrong distance in the signal of M if it arrives before the authentic transmission, thus degrading the service. Their experimental results demonstrate that attacks on all the receivers exhibit similar behavior, i.e. mean absolute error spanning from 24 to 56 ns (which translates to a ranging error of 7 to 17 m).

1.3 Proposed Attack

In the false data injection attack, as introduced by Liu et al. [27], sensor readings from smart power meters were changed through digital means, i.e. an offset was added to a previous measurement, though tampering with the actual measurement mechanism was not excluded. Tire pressure monitor systems have also been targeted in a similar fashion [28]. The analog channel (physical layer) has since been used to perpetrate FDI against microphones, implantable cardiac electronic devices [29] and anti-lock braking systems [30].

The proposed attack also leverages the analog channel through the crafting and transmission of false radar responses that are designed to appear as though they originate from a source much closer to the radar system than they actually are. The main focus is on distance-decreasing attacks, as apparent distances can be easily increased by delaying the return time of a radar system's signal, e.g., by replaying the signal at a later time. While FMCW radar systems have been deployed for ACC and CAS, their security has so far not been analyzed. The novelty of this work is in the fact that this attack is mounted on the analog channel of FMCW radar for decreasing the apparent distance of a target rather than attacking the distance-bounding protocols of a system. As velocity estimates in FMCW radar are based on the Doppler effect, it was felt that apparent velocity could be increased or decreased in much the same way (i.e. replaying a radar signal at a higher or lower frequency) and is thus not considered in this work.

Since there was no access to a commercial FMCW radar, one was constructed using software-defined radios and GNU Radio. Another justification for this choice is that documentation on commercial radars is scarce, and thus a great deal of reverse engineering would have been necessary to understand the internal workings of a commercial radar. Finally, because of their popularity in vehicle automation technologies, automotive FMCW radars have been investigated. Thus, this radar platform is modeled on proposed FMCW radar systems for automotive applications found in the literature [2–4, 31–33]. It is under investigation if there are techniques used by existing radar systems that could counter this attack. The focus of this work is to demonstrate the feasibility of such an attack.

Chapter 2

Vehicle Automation Systems and FMCW Radar

2.1 Introduction

Any vehicular system that involves the use of techniques such as artificial intelligence, adaptive learning, and mechatronics in order to simplify things and make driving hassle free for the operator can be termed a vehicle-automation system. Such systems have existed in the transportation industry for a long time now, the following being some famous examples.

- Vehicle-tracking system [34, 35]: These systems are capable of tracking a vehicle in real time, utilizing the capabilities of GPS or other positioning technologies. The two kinds of vehicle-tracking systems available on the market are active and passive tracking devices. Passive devices are those which regularly collect such data as position, velocity, and direction of heading and then are removed from the vehicle to connect and download this data to a server or any computer system for further analysis once the vehicle has reached a predetermined resting point. Active devices share all the same properties with passive devices except that they transmit data in real time to a server via established networks such as cellular or satellite.

- Rear-view alarm [36,37]: Also known as a parking sensor, it is used to detect obstacles behind the vehicle and is mostly used to assist a driver while parking. It alerts the driver when the vehicle is in dangerously close proximity to an obstacle, with the alert signal frequency depending on the distance from that object. This system uses ultrasonic proximity detectors to accomplish the task.

- Anti-lock braking system (ABS) [38, 39]: This system is a lifesaver on snow-covered roads, where it takes little time for a driver to lose control of the vehicle and start skidding. On slippery roads, the wheels lose traction and start skidding, a phenomenon commonly known as wheel lockup, at which point even trained drivers find it hard to regain control over the vehicle. The anti-lock braking system keeps the wheels from skidding while slowing down, which results in faster slowdown and better steering control over the vehicle. This system continually monitors velocity sensors and keeps track of rapid decelerations beyond a normal range, usually just before the wheel would go into a lock state. An ABS can autonomously take care of this rapid deceleration by controlling the pressure valves to the brakes of every single wheel. This keeps the wheels just short of slipping into lockup state and gives the driver full freedom to concentrate on steering, while the system takes care of pumping the brakes, which otherwise would again fall on the driver.

- Traction-control system [40, 41]: This system works in conjunction with ABS. A traction-control system monitors the wheels and detects if one or more wheels are spinning faster than the others. If such a scenario is encountered, it activates ABS to take control.

- Dynamic steering response [42]: This is a car safety mechanism which controls the steering response of a vehicle based on the vehicle's speed and road conditions. For example, on straight highways at high speeds, it gives directional stability to the steering, and on twisting roads at lower speeds, it increases the steering precision by decreasing steering response time.

The applicability of automation to vehicles has increased considerably in recent times, especially automation focused on either modifying preexisting car designs to incorporate certain semi-autonomous abilities or even introducing autonomous robotic cars. The most common automation systems in these two variants are the following.

- Adaptive cruise control (ACC): Cruise control is a system that controls the speed of an automobile. It takes control and maintains the same speed until brought back into manual mode. This can be a big relief on straight highways, where there is almost no traffic fluctuation for miles. But this system alone can be hazardous on busy thoroughfares like city roads, where it requires human sense and human response mechanisms to react to sudden changes in traffic. Adaptive cruise control is capable of adjusting the vehicle's speed in order to maintain a safe following distance.

- Autonomous driving: Autonomous robotic cars, also known as driverless or self-driving cars, are vehicles which do not require a driver; instead they are capable of navigating through traffic on roads and highways with absolutely no input from a driver. These cars use multiple sensor-based technologies like radar sensors and laser sensors to sense their environment and surrounding traffic conditions to make smart decisions while navigating.

- Collision avoidance system (CAS): Also known as collision mitigation, precrash, or forward collision warning systems, these work in conjunction with ACC to mitigate the severity of an impending accident or, better, prevent one from occurring. This system detects imminent threats from vehicles or other obstacles that are in alarmingly close proximity to the vehicle and forewarns the driver using auditory or visual cues, or both, in different phases. It is also capable of taking control of the vehicle in dire circumstances to avoid any crash if it appears to the system that driver is not taking necessary measures.

2.2 Radar Sensing and Its Working Principle

The three car-automation techniques mentioned involve safety control systems with frequency-modulated continuous-wave (FMCW) radar sensors [7, 8] in the car's front and sides, used to detect when the vehicles are uncomfortably close and in turn slow down the vehicle in order to avoid collision. FMCW radar systems by virtue of their advantages over pulsed radar, i.e. low measurement time, computational complexity [3], and higher bandwidth [4], as well as capability to measure target range and relative speed simultaneously [2], are now a common component in vehicle automation systems.

In an FMCW radar (Figure 2.1) the transmitting end of the system transmits a continuous frequency-modulated signal for target detection. A carrier wave at the transmitter

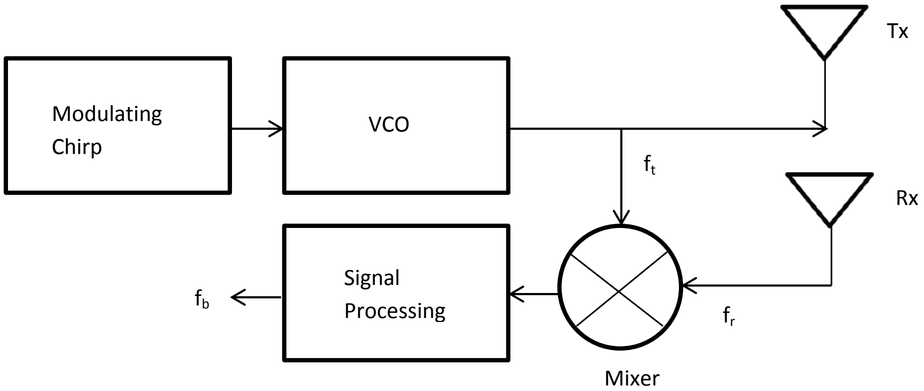


Fig. 2.1: Block diagram of an FMCW radar.

is linearly swept in frequency over time by a chirp signal, as shown by the spectrogram of Figure 2.2, which results in a frequency-modulated output signal that, when reflected from an object and received back at the receiver, is mixed with some part of the original transmitted signal. The received signal is time shifted, because of the distance R between transmitter and the object, by $t_d = 2R/c$, where c is the speed of light in the transmission medium. This time shift results in a frequency difference between the two signals when the transmitted and received signals are multiplied, known as the beat frequency, f_b. This beat frequency is in direct proportion to the range of the target and is defined as $f_b = f_t - f_r$, where f_t and f_r are the frequencies of transmitted and received signals, respectively, at the same time instance.

2.3 Modulating Waveforms

Continuing the discussion from the previous section, frequency modulation requires two major components: a carrier waveform and a modulating waveform. The modulating waveform is the low-frequency message signal that is to be transmitted over the channel, and the carrier waveform is the high-frequency sinusoidal waveform whose one or more properties (in this case frequency) are varied in accordance with the modulating waveform. As will be evident from the following discussion, the type of modulating waveform selected for a radar application depends on a few criteria. The two most commonly used modulating waveforms for FMCW radar are the following.

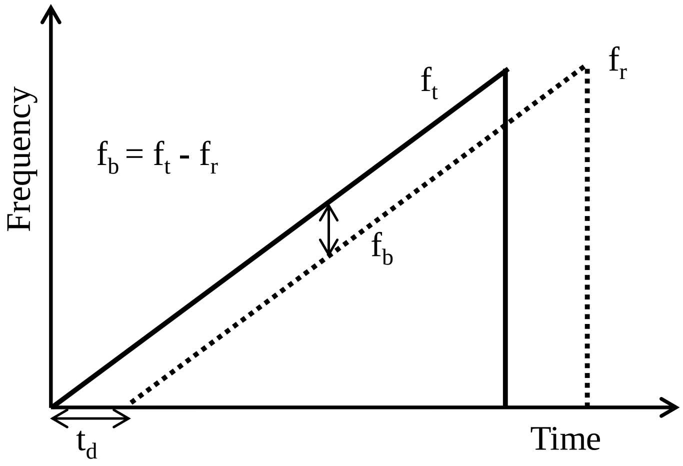


Fig. 2.2: A modulating chirp waveform for ranging purposes.

2.3.1 Sawtooth Waveform

As depicted in Figure 2.2, this is a sawtooth waveform. It frequency modulates a sinusoidal carrier as in Figure 2.3. In practice a train of such waveforms (Figure 2.4) is used to calculate the range of a target.

2.3.2 Triangular Waveform

Using the sawtooth waveform for frequency modulation gives a quite accurate range estimation for stationary targets but introduces an error for moving objects due to the range-doppler coupling effect [43]. That is, a Doppler shift introduced by a moving object changes the beat frequency, resulting in an erroneous estimate of both the range and velocity. One way to solve this issue is by estimating the error and then applying error compensation, but the best way to resolve this ambiguity is to use a different modulating waveform altogether. Because of its inherent ability to accurately estimate both the range and velocity of an object, automotive radars typically make use of a triangular waveform (Figure 2.5) [2,3,44–47]. Figure 2.6 represents what frequency modulation with a triangular function does to a sinusoidal carrier.

A triangular waveform, upon being reflected back from a moving target, undergoes two frequency shifts, one due to range and the other due to relative motion of target with respect to the radar unit. The two frequency shifts in the downconverted signal due to both

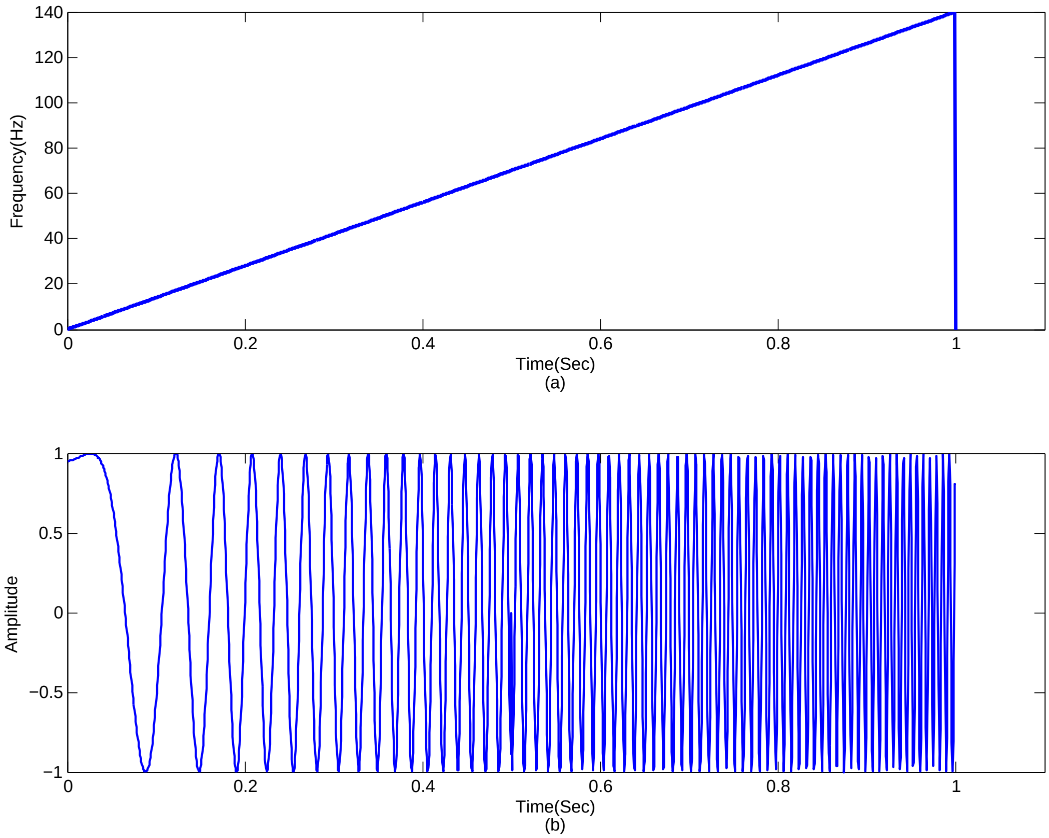


Fig. 2.3: Frequency modulation using sawtooth waveform: (a) Spectrogram of the sawtooth function, (b) Modulated signal in the time domain.

the target range R and velocity V are denoted as

$$\begin{aligned} f_\tau &= \left(\frac{2R\Delta f}{ct_m}\right), \\ f_D &= \left(\frac{-2V}{\lambda}\right), \end{aligned} \tag{2.1}$$

where Δf is the chirp signal bandwidth, c is the speed of light in the medium, t_m is the sweep time of a single modulating chirp, and λ is the wavelength of the carrier frequency. After being reflected from the target, the signal that is received back and mixed with the transmitted waveform gives not one but two beat frequencies which experimentally show peaks at low frequencies in the spectral analysis of mixed and downconverted baseband signal. Theoretically, the two beat frequencies can be calculated from the two previously

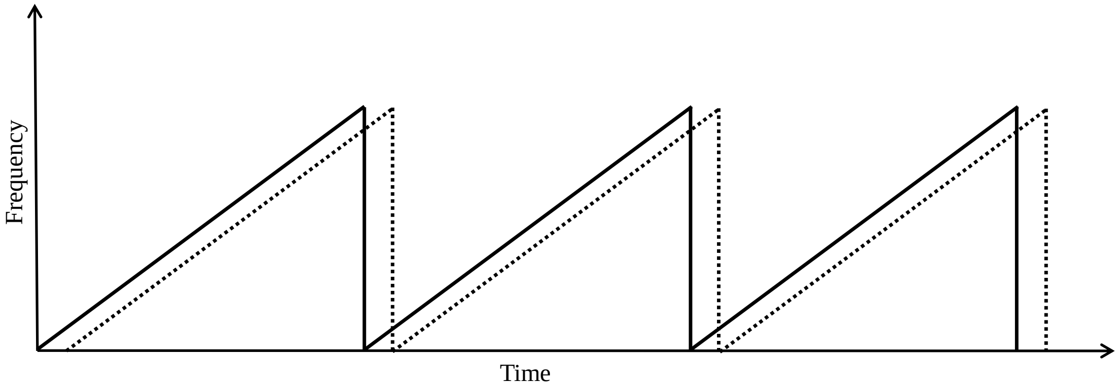


Fig. 2.4: Sequence of sawtooth waveforms.

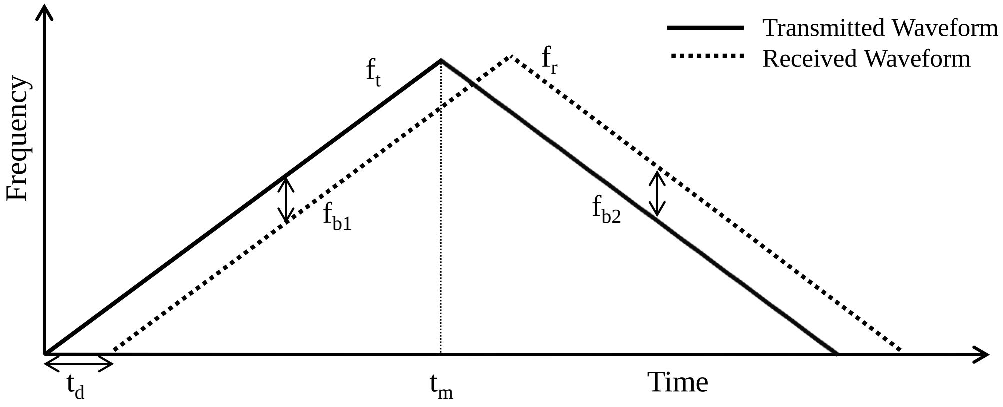


Fig. 2.5: A modulating chirp waveform (triangular) for ranging and velocity detection purposes.

described frequency shifts [44] as

$$\begin{aligned} f_{b1} &= f_D - f_\tau, \\ f_{b2} &= f_D + f_\tau, \end{aligned} \tag{2.2}$$

where f_{b1} is the beat frequency for the up chirp and f_{b2} is the frequency for the down chirp. As is discussed in later sections, the two beat frequencies can either be same or different based on the velocity and direction of motion of the target relative to the radar unit. The two beat frequencies obtained in theory or by experimentation can then be employed to estimate the object range R, which can then be calculated as

$$R = \left(\frac{f_{b2} + f_{b1}}{2}\right) \times \left(\frac{ct_m}{2\Delta f}\right). \tag{2.3}$$

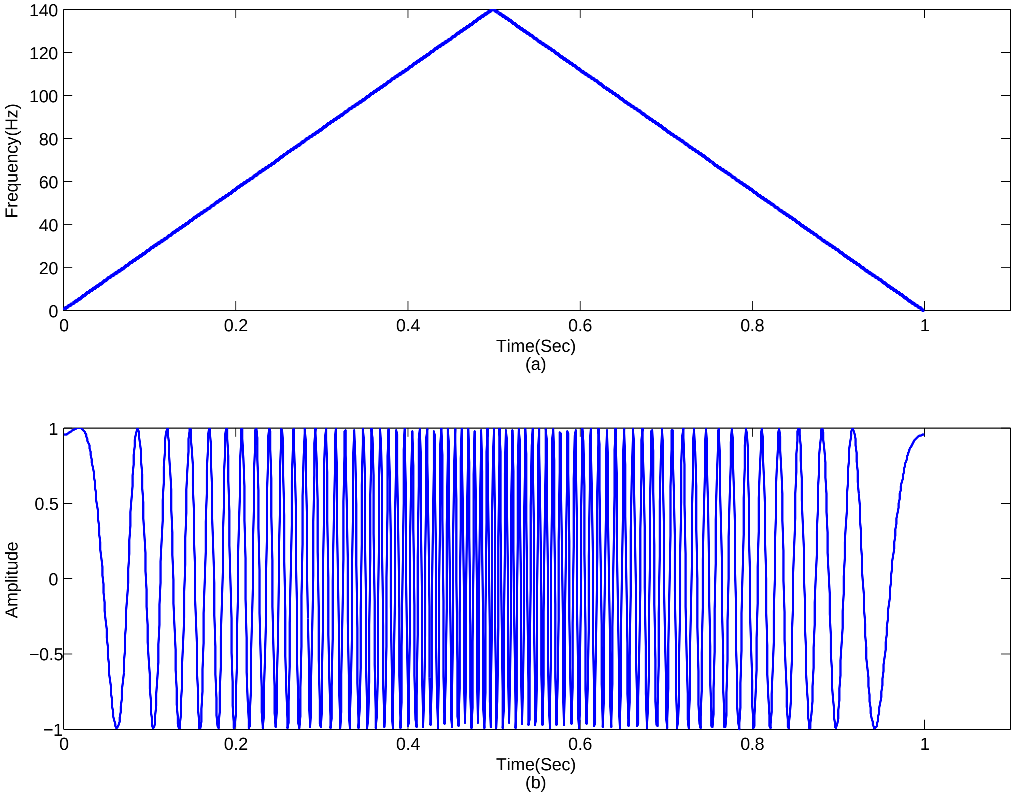


Fig. 2.6: Frequency modulation using a triangular waveform: (a) Spectrogram of the triangular function, (b) Modulated signal in the time domain.

Along similar lines, radial velocity V is calculated as

$$V = \left(\frac{f_{b2} - f_{b1}}{2}\right) \times \left(\frac{c}{2f_c}\right), \tag{2.4}$$

where f_c is the carrier frequency of the transmitter.

The range resolution ΔR and velocity resolution ΔV of a triangular-chirp radar (i.e. the minimum resolvable differences in range and velocity) [43] are given by

$$\begin{aligned} \Delta R &= \left(\frac{c}{2\Delta f}\right), \\ \Delta V &= \left(\frac{\lambda}{2t_m}\right). \end{aligned} \tag{2.5}$$

A modified range resolution equation is discussed by Jankiraman [48], the derivation of which is outside of the scope of this work. The equation is

$$\Delta R = max \left\{ \frac{R}{f_b} \sqrt{\Delta f_{tar}^2 + \Delta f_{rec}^2}, \frac{c}{2\Delta f (1 - \frac{t_d}{t_m})} \right\}, \tag{2.6}$$

where $\Delta f_{tar} = \frac{NL}{100} \times \Delta f$ is the target beat frequency spectral width, and Δf_{rec} is the receiver frequency resolution. To improve ΔR, this equation allows three possibilities: (1) increase t_m; (2) increase sampling frequency f_s; (3) decrease nonlinearities (NL). t_m cannot be changed because as already discussed in the introduction, the parameters are taken from the literature. There is a physical limitation on f_s that USRP can support. Algorithms have already been designed to reduce nonlinearities [49], but that is not the focus of this work as the experimental results in Section 4.2 suggest good enough range resolution for demonstrating the feasibility of this attack.

Mixing the received signal from the object with the instantaneous carrier frequency produced a baseband signal, which was then analyzed to extract object range and radial velocity. This process was carried out in the signal processing block of Figure 2.1. The input this block received from the mixer was sampled and converted to the frequency domain using fast Fourier transform (FFT). The beat frequencies, from which the range and velocity were calculated, appear as peaks in the frequency domain.

In the design of this radar receiver, all phases after the mixing phase were carried out using software for the purpose of this research. A dedicated program was made in MATLAB in order to carry out signal processing on the received signal after mixing with some part of the transmitted waveform. The MATLAB code in Appendix B.1 performed all the necessary post-processing on the received and downconverted baseband signal. It is a well commented code, divided into modules and sub-modules for ease in troubleshooting. The whole MATLAB code follows a process flow which is as follows.

- Code accepts the input from mixer stage.

- The mixed signal is then divided and reshaped such that upsweep and downsweep across the signal length are separated into two mixer outputs which are stored in mxu and mxd variables, respectively.

- The two stored and reshaped signals are then forwarded to be Fourier transformed for spectral analysis.
- Once the two are converted to frequency domain, they are ready for the next stage of range validation through constant false alarm rate (CFAR) analysis, which is dealt with in detail in a later section in this chapter.
- Beat frequencies corresponding to upsweep and downsweep can now be extracted from the CFAR output.
- Once the beat frequencies are extracted, they can be employed to calculate range from the Equation (2.3).

The above steps provide a concise overview of the whole process flow of the MATLAB code, which is implemented by the MATLAB code, that can then be understood in greater detail by a code walkthrough. So the main code, "Signal Processing at the Victim's End," starts with declaring variables and constants that are going to be used throughout the program. This code also calls two custom-built functions which are discussed later in this section. The first module, "Chirps transmitted by the victim," takes the input from the actual transmitted waveform as a reference for future calculations as described below. "Mixer output" takes the input (mxr_out) from a file, exported to the MATLAB environment from the receiver. The direct output of the mixing stage is fed into the code. In the next module, "Separate FFTs of upsweep and downsweep after mixer," mixer data for up chirp and down chirp within mxr_out are separated based on the reference input, reshaped, and stored in mxu and mxd respectively and are ready for the next step of spectrum analysis. A fast-Fourier transform (FFT) of the input signal converts the time domain signal into frequency domain making it available for spectral analysis. Successively, this frequency domain signal becomes the input for the next stage of constant false alarm rate (CFAR) analysis "CFAR and extraction of beat frequencies," which helps in target validation. The topic of CFAR and its theoretical background are treated in detail in the following sections of this chapter. A custom function *"MyCFAR"* is built using the CFARDetector function implemented in the phased array toolbox of MATLAB. This returns the result in terms of probability of detecting the target in every frequency bin corresponding to a range. Frequency bins are even intervals by which frequency lines are spaced in a frequency domain signal. Since the analysis is not real time, CFAR takes the input corresponding to all the received chirps.

Every triangular wave comprises of a single pair of up and down chirps that represent one scan of the radar. Many such pairs represent as many scans. Each scan when undergoes the same signal processing and frequency domain conversion gives the spectrum for all the scans and each scan has data corresponding to all the possible ranges that can be resolved by the radar receiver in the form of energy at the corresponding beat frequencies. These are known as frequency or range bins. CFAR validated the object for every single scan and returns the result in form of probability of detection of a target in every range bin for every scan. Followed by CFAR is the module that calculates range from the returned data set from CFAR detection. It takes this data and averages out the values for every range bin separately across all the subsequent scans and calculates the range corresponding to the highest energy levels in range bins.

Stationary Target Detection with Triangular Waveform FMCW

Since there is no motion in the target, the two generated beat frequencies are the same (Figure 2.7), and the range can even be directly extracted from this single frequency.

Moving (Approaching) Target Detection with Triangular Waveform FMCW

As already mentioned, a moving target introduces a Doppler frequency shift in the beat frequency, which results in one portion of the beat frequency being increased and the other decreased. The received signal frequency is increased for a target approaching the radar, which shifts up the whole received signal spectrogram, resulting in decreasing the upsweep beat frequency and increasing the downsweep beat frequency as shown in Figure 2.8.

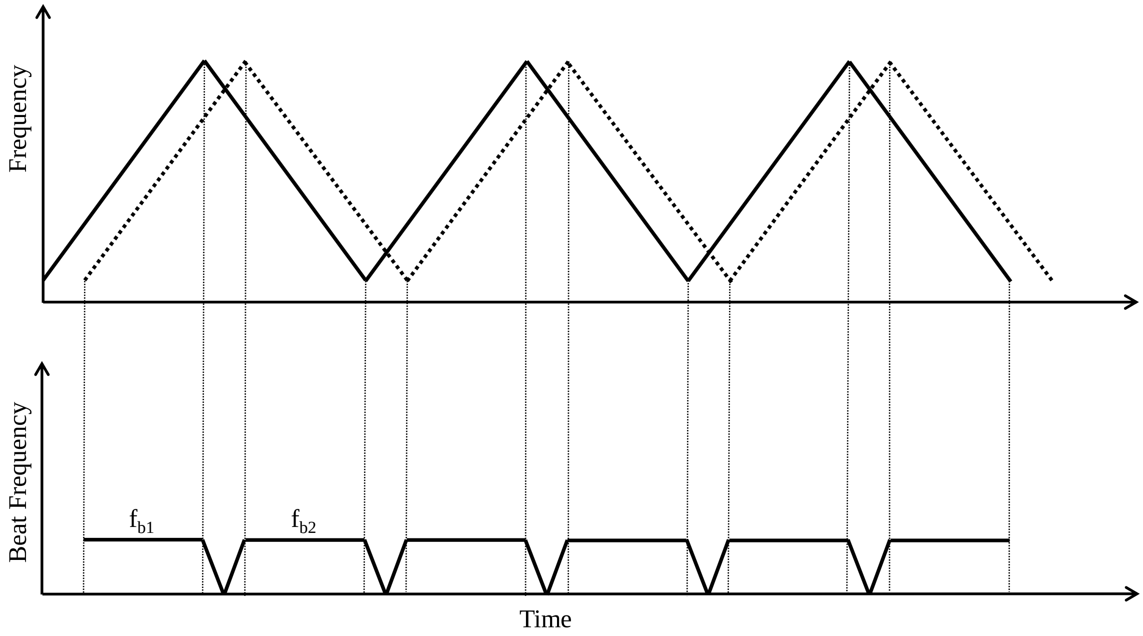


Fig. 2.7: Stationary target: Top plot is the spectrogram of transmitted (solid line) and corresponding received (dotted line) waveform. Bottom figure is the difference of these two waveforms, that is also termed as beat frequency.

Moving (Receding) Target Detection with Triangular Waveform FMCW

For a target receding from the radar, the received signal frequency is decreased, which shifts down the whole received signal spectrogram, resulting in increasing the upsweep beat frequency and decreasing the downsweep beat frequency as shown in Figure 2.9.

2.4 CFAR

2.4.1 General Concept

The returning echoes are received by antenna at the radar receiver end, amplified, and downconverted to baseband and then analyzed for range and velocity information extraction. In this process, noise is added to the received signal at different stages, including the unwanted power from the internal circuit and from the external environment. In practical scenarios, external noise interference levels are variable and cause significant deviations from radar's ideal performance. For this reason a mechanism, with roots in stochastic theory, was formulated to detect the presence of beat signals. Constant false alarm rate (CFAR) detection, also referred to as "adaptive threshold detection," is a set of stochastic techniques formulated to help a radar system make decisions about whether received signals indicate the presence of objects by setting adequate threshold values [4]. The CFAR detector is fed with the mixer output after it has been Fourier transformed into the frequency domain, so the separate FFTs of up chirp and down chirp are fed into the CFAR detector in order to help make decisions and check the validity of a potential target.

2.4.2 Threshold and Probability of False Alarm

An important statistical measure on which CFAR bases its detection decision is probability of false alarm. For the simplest case of a single data sample (N=1) and analysis done in terms of normalized linear detector output, the probability of false alarm is given by

$$P_{FA} = e^{-T}, \tag{2.7}$$

where T is the detector threshold. One more way of looking at the equation, which gives the threshold value required to achieve a certain value of probability of false alarm, is

$$T = -ln(P_{FA}). \tag{2.8}$$

In terms of an unnormalized data sample and a square law detector, the probability of false alarm is given by

$$P_{FA} = e^{-T/\beta^2}, \tag{2.9}$$

where β^2 is the total noise power (I and Q channels) of the interference and threshold T is given by

$$T = -\beta^2 ln(P_{FA}). \tag{2.10}$$

Threshold T is of the form $T = \alpha\beta^2$, where multiplier α is a function of the desired false alarm probability. In order to tune a CFAR detector for a particular radar application, a P_{FA} value is selected, out of which threshold value is computed by Equation (2.10). The probability of detection is then determined by the target *signal-to-noise ratio (SNR)* [4].

2.4.3 OS-CFAR

To cope with dense traffic situations while simultaneously keeping track of fixed objects like trees and road signs in ever-changing weather conditions (broadly construed as background noise), automotive radars make use of a variant of CFAR known as ordered statistic CFAR (OS-CFAR) [32]. The decision threshold calculation in OS-CFAR is carried out in the frequency domain thus: OS-CFAR rank orders reference window data $\{x_1, x_2, ..., x_n\}$, which represent the frequency bins in the power spectrum of the mixed signal, in an ascending numerical sequence. The interference level is then selected by the k^{th} element of this new ordered list and is called the k^{th} order statistic. A threshold is then set as a multiple of this value $T = \alpha_{os}x_k$, where α_{os} is the multiplying factor for the threshold for probability of false alarm (i.e. detecting an object as present when it is not). The false alarm probability is given by

$$P_{FA} = \frac{N!(\alpha_{os} + N - k)}{(N-k)!(\alpha_{os} + N)!}, \tag{2.11}$$

where N is total number of elements in the window and k is so chosen to satisfy $N/2 < k < N$ [50]. The main advantage of OS-CFAR is that masking via nearby objects is eliminated so long as the number of cells contaminated by interfering targets does not exceed $N - k$ [4]. It is noted that this property of OS-CFAR is a potential impediment to the attack, as explained in Chapter 3.

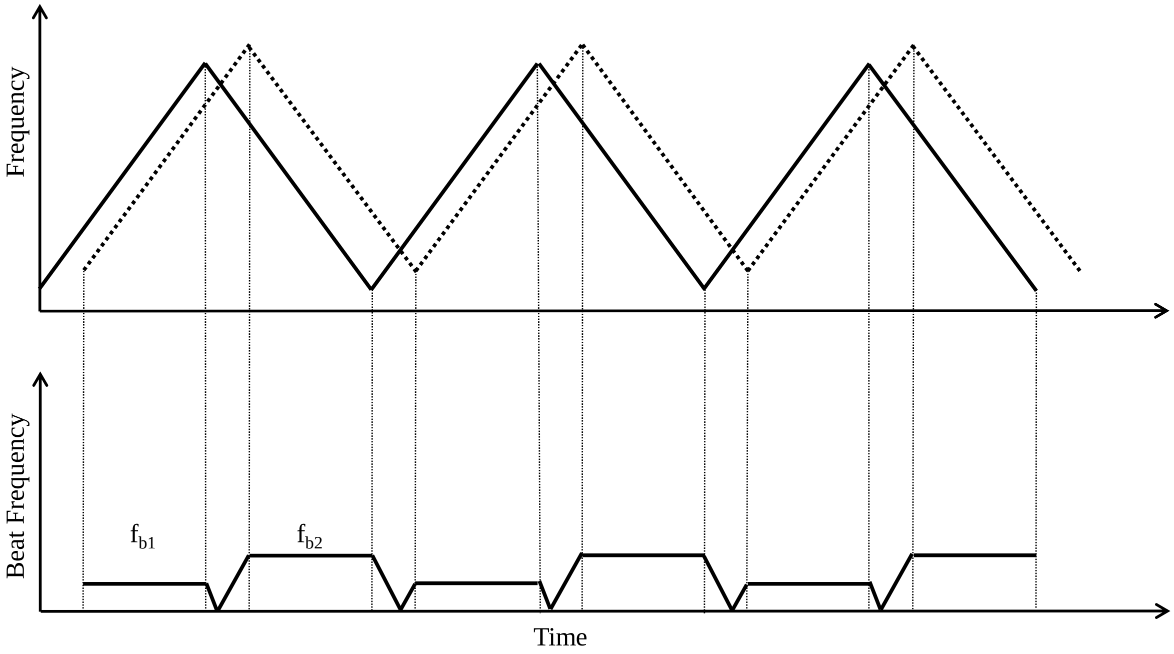


Fig. 2.8: Moving (approaching) target: Top plot is the spectrogram of transmitted (solid line) and corresponding received (dotted line) waveform. Bottom figure is the difference of these two waveforms, which is also termed a beat frequency.

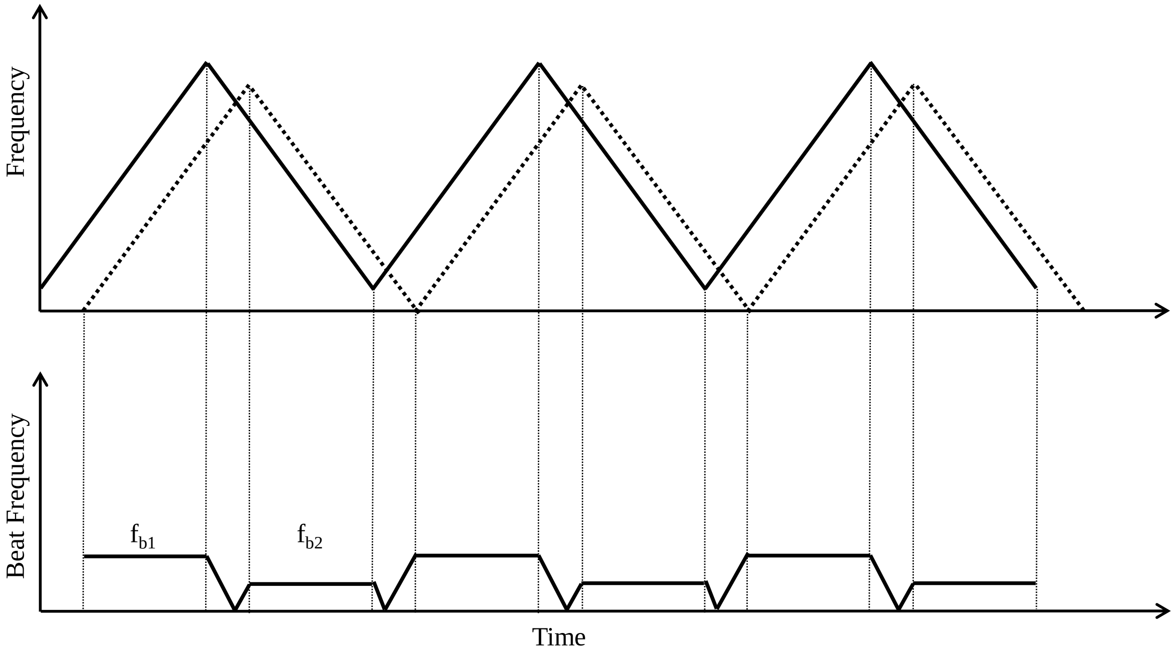


Fig. 2.9: Moving (receding) target: Top plot is the spectrogram of transmitted (solid line) and corresponding received (dotted line) waveform. Bottom figure is the difference of these two waveforms, which is also termed a beat frequency.

Chapter 3

A Distance-Decreasing Attack on FMCW Radar

In this section the theoretical chance of success of an attack in which an active, malicious object could appear closer to a radar system than it actually is has been evaluated.

3.1 Threat Model

It is the goal of the attacker to decrease their apparent distance to an FMCW radar system. The attack has been built on the premise that the actual distance between the victim radar unit and an object (vehicle) controlled by the attacker is known to the attacker but not to the victim. This premise is fulfilled by giving attackers additional radar capabilities to measure distance to victim. Furthermore, it has been assumed that the technical standards of the victim radar system (modulation technique, type of chirp signals, carrier frequency, and bandwidth) are known to the attacker; i.e. the attacker knows what the radar signal will look like and at which frequency it will be transmitted but not when it will be transmitted. Given that there are only a handful of automotive radar manufacturers, this ought to be feasible for an attacker with sufficient resources or a desire to target only certain vehicles (because of certification issues, it is assumed that a given model vehicle would use the same radar for the entire production run of the vehicle).

Finally, it has also been assumed that attackers have the ability to deflect and/or absorb authentic radar signals from the victim system and transmit their own, spurious, signals to the victim. The latter feat is accomplished by equipping the attacker with a highly configurable radar system of their own, while the former is conceivable if the attacker's vehicle is coated with a radio-frequency absorbing material (e.g. ferrite tile, broadband foam, or hybrid absorber [51–53]) and/or has installed paneling to reduce its radar cross-section [54]. Materials are available commercially specifically for absorbing automotive radar signals at 24 GHz and 77 GHz that can attenuate the incident signal by 110.6 dB/cm at 24 GHz and up to 136.7 dB/cm at 77 GHz [55]. Dong et al. prepared some absorbers that can absorb up to 99.3% of incident electromagnetic energy at 24 GHz [56]. Also, the false return signal is more powerful than the remaining reflected signal. A realistic scenario could be the problem of multipath interference, but because of the absorbing materials discussed and the fact that OS-CFAR validates only those hits as targets which are consistent in successive scans as discussed in Section 2, this problem settles on a lower ground of concern.

3.2 Attack Model

The attack is based on the victim's receiving a spurious radar signal from the attacker that makes the attacker appear closer than it actually is. For the attacker to decrease its apparent distance requires that its own spurious signal reach the victim in less than the round-trip time an actual signal would take given the attacker's distance. As c limits the speed at which signals can propagate, this is only possible if the attacker can anticipate when the victim will transmit, and at a time shortly before this transmit their own signal. Since it cannot be assumed that an attacker can know the instant at which the victim will transmit, the attacker continuously transmits an ensemble of chirps that are time shifted in such a way as to correspond to all, or nearly all, of the resolvable distances of the victim radar (Figure 3.1). Figure 3.1 and Figure 3.3 do not represent the complete ensemble signal but rather are just example representations of the ensemble concept with fewer time shifts. The two figures were obtained from simulation of the attack model in a pure MATLAB environment. The ensemble signal can be achieved using a single transmitter, as will be discussed in Chapter 4. When the attacker senses a transmission from the victim radar, it immediately stops transmitting the ensemble of signals and selects that signal which corresponds to its desired distance.

For clarity, the attack has been divided into the following stages.

1. The attacker begins transmitting the spurious ensemble signal (Figure 3.2(a)) and waits for the victim to start transmitting (Figure 3.2(b)).

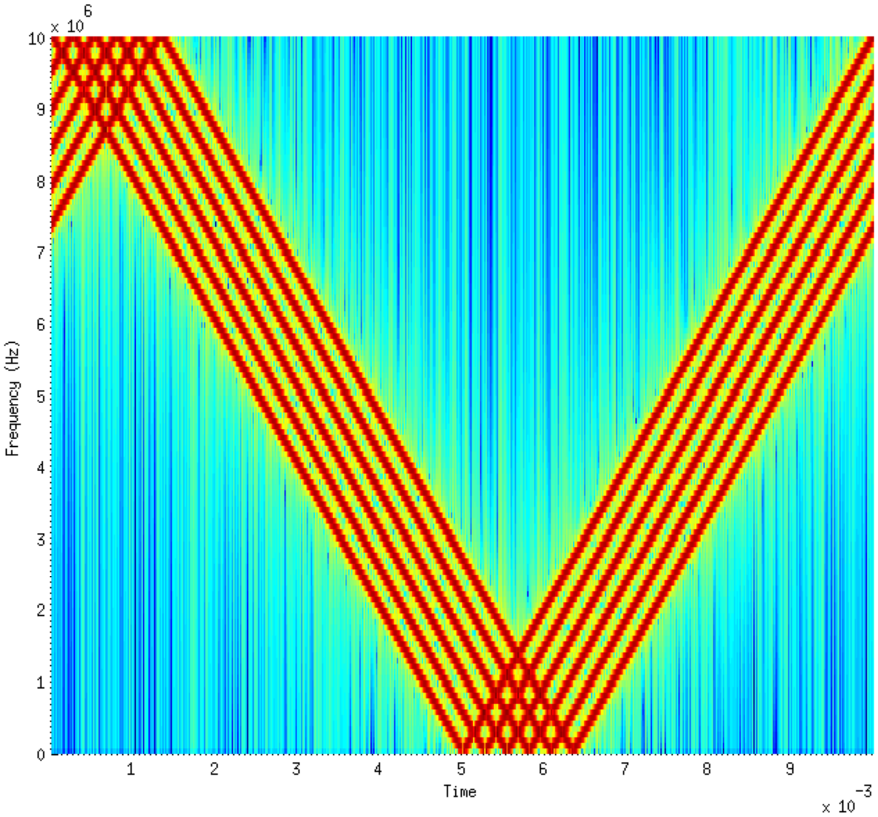


Fig. 3.1: Ensemble of time-shifted triangular chirp signals (spectrogram). The separation between signals corresponds to the minimal resolvable range of the radar. Note: Illustrative only; not all time shifts shown.

2. The victim's transmitted signal V_t is received at the attacker end and absorbed. Based on the transmission received from the victim, the attacker modifies their own transmission to include only the desired distance (Figure 3.2(c)).

3. Instead of a signal corresponding to the attacker's true position V_r, the victim receives A_t, which contains only the beat frequencies corresponding to the attacker's desired distance (Figure 3.2(d)).

Below are detailed the calculations and procedures needed for each stage of the attack.

Stage 1: A timer was triggered when the ensemble transmission started. This timer provided a reference time for all further calculations. Since there was no way of knowing prior to the transmission when the victim would start transmitting, the ensemble needed to have a chirp signal (delayed signal) corresponding to every possible transmission from the

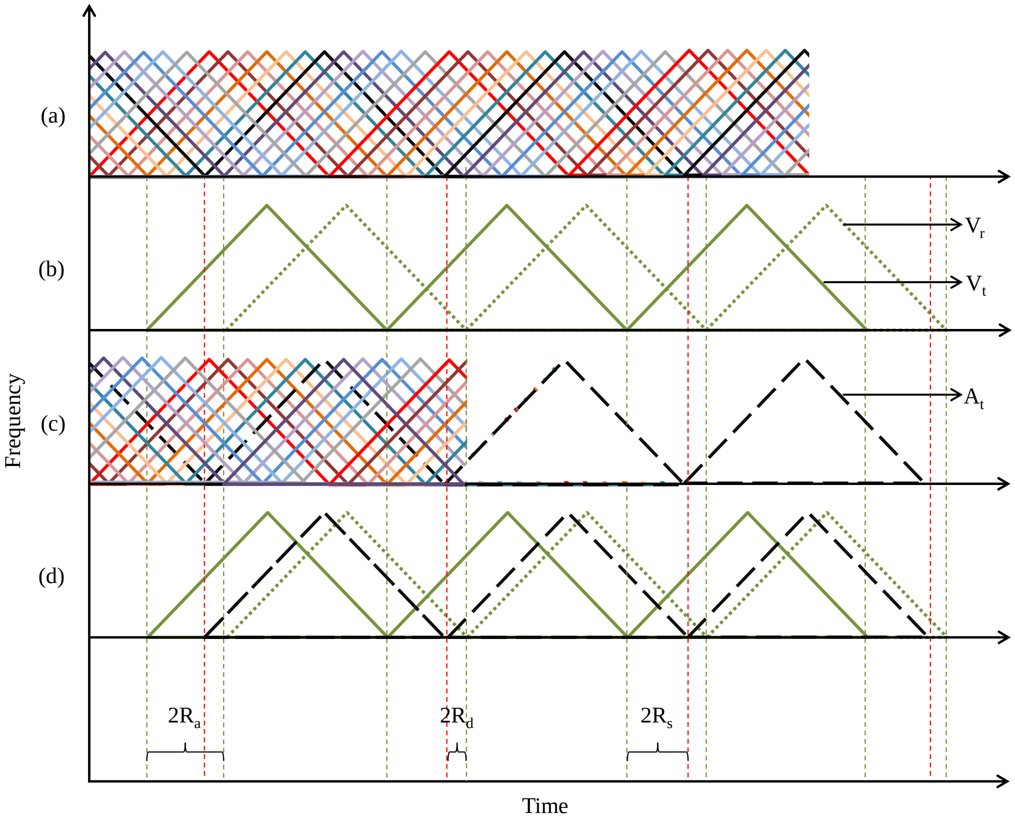


Fig. 3.2: A graphical representation of the attack: (a) the attacker transmits an ensemble of signals; (b) the victim radar's transmitted signal V_t and the authentic received signal V_r that corresponds to the attacker's true distance; (c) the attacker receives V_t and selects the signal A_t that results in their desired distance; and (d) the actual distance of the attacker R_a, the distance R_d that the attacker decreases their distance by, and the attacker's apparent (spoofed) distance R_s.

victim. The total number of these delays was $D_t = 2t_m/t_s$, where $2t_m$ was the chirp period (up chirp + down chirp) and $t_s = 1/(\text{sampling frequency}) = f_s$.

While the presence of all D_t delays ensures 100% probability of success, and hence represents the best case scenario, it will increase channel noise and thus, possibly, degrade object recognition success when CFAR is employed. For the purpose of experimentation, the MATLAB implementation of OS-CFAR from the phased array toolbox of MATLAB was used. A limited number of delays (D_a) can be used instead, although with decreased probability of success. Table 3.1 summarizes the success rate and minimum spoofable range versus the number of delays used by the attacker when $D_a < D_t$. In Sections 3.2.1 and 3.2.2

the effect of number of delays on the attack is discussed. For now, let us assume that some number of delays $D_a \leq D_t$ have been selected by the attacker and that the resulting ensemble is being transmitted.

Stage 2: As soon as the victim's transmission V_t was received at the attacker's end, the arrival time T_r was logged in the form of time elapsed since the timer was started (seconds). T_r was then used with an equation (discussed below) to select the chirp signal corresponding to the appropriate delay for the attacker's desired distance. At this point the attacker ceased transmission of the ensemble and only transmitted the selected delay signal (Figure 3.3).

Stage 3: Now there was no ensemble of signals in the attacker's transmission, but only the time shifted signal A_t. When this spurious signal was processed by the victim, beat frequencies corresponding to the attacker's falsified position would be detected, thus injecting false information about the apparent range between the two.

Now is the time to examine the effects of the number of delays the attacker uses to build the ensemble signal and how the attacker selects which delay in the ensemble to continue transmitting.

3.2.1 $D_a = D_t$ (Best Case)

When all D_t delays were present in the ensemble of signals, the attacker had the ability to decrease their apparent distance arbitrarily. The delay that corresponded to a decrease of R_d meters is given by

$$D_{spoof} = \left\{ T_r - 2t_m \times floor\left(\frac{T_r}{2t_m}\right) + \frac{(R_a - 2R_d)}{C} \right\} \times f_s, \tag{3.1}$$

Table 3.1: Theoretical success rates for $D_a < D_t$.

	Best Case	Worst Case
Success Rate %	100	$\frac{D_a}{D_t} \times 100$
Minimum range served for 100% success rate	$\left(\frac{D_t}{D_a} + 2\right) \times \left(\frac{\Delta R}{2}\right)$	$1.5 \times \Delta R$

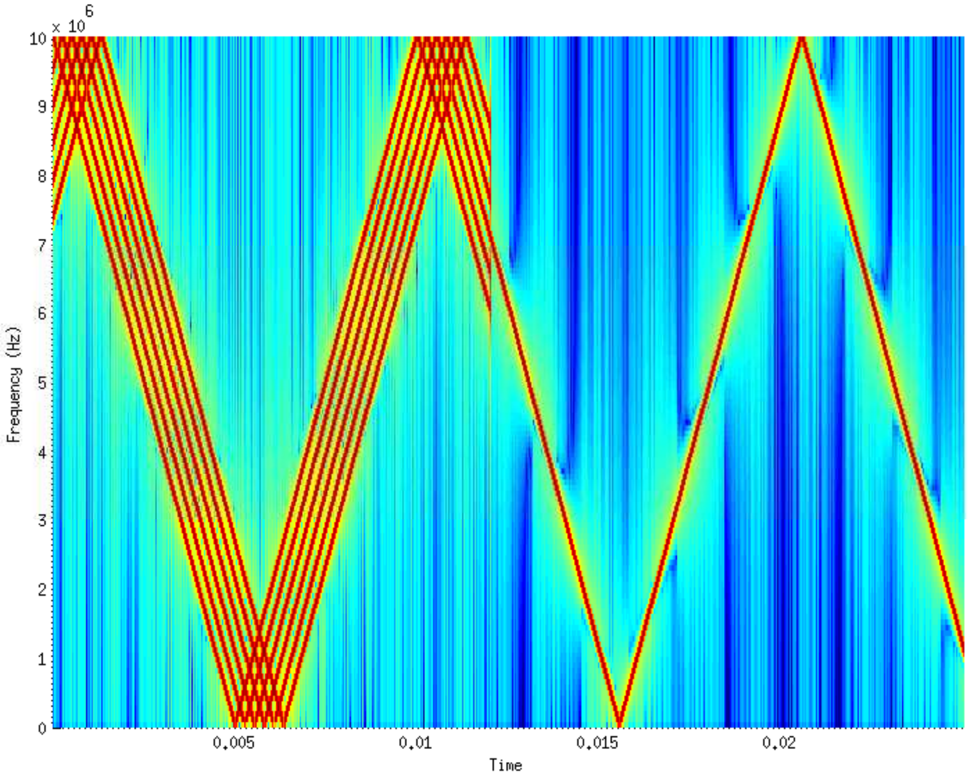


Fig. 3.3: A single time-delayed waveform selected from the ensemble of signals (spectrogram). Note: Illustrative only; not all time shifts shown.

where T_r is the time (seconds) logged by the timer on first reception of V_t and R_a is the actual range of the attacker. (See Appendix A.1 for the derivation.)

3.2.2 $D_a < D_t$ (Limited Case)

When not all D_t delays were present in the ensemble, the attacker no longer had the ability to select an arbitrary distance to decrease their apparent distance by and must instead choose a delay that provides the greatest decrease in distance

$$D_{spoof} = round\left(\frac{K}{S_d} - 0.5\right) \times S_d, \tag{3.2}$$

where $K = \left\{T_r - 2t_m \times floor\left(\frac{T_r}{2t_m}\right) + \frac{R_a}{C}\right\} \times f_s$ and $S_d = \frac{D_t}{D_a} = \frac{2t_m \times f_s}{D_a}$. (See Appendix A.2 for the derivation.)

Given T_r this equation will calculate the first possible spoofing delay, i.e. the closest delay that is less than the actual one.

3.2.3 MATLAB Simulation of the Theoretical Concept

The whole attack scenario was simulated in MATLAB to test its theoretical feasibility before being mounted on a radar system. The MATLAB code in Appendix B.2 simulates an FMCW radar with a triangular waveform as the modulating signal. The code starts with the first module, "Transmitted signal generation," where variables and constants to be used throughout the simulation are declared and initialized. A triangular waveform is created using the built-in function of MATLAB "sawtooth," which takes the frequency of the signal (Fm) and its required duty cycle (0.5) as input parameters. This triangular wave is then used to drive a voltage controlled oscillator (VCO), which again is simulated by a built-in function, "vco." "Creating delayed signals for ensemble" produces the output ensemble signal consisting of time-shifted waveforms, which is transmitted and received back by the receiver, shown as the next module in this code. But before that, in order to simulate the attack, the ensemble signal is so modified that only for a certain initial time period is the complete ensemble transmitted and for the rest just one time-delayed signal is kept on and the rest are switched off. This one specific delay (Figure 3.3) is selected in the module "Selecting delay using the two equations." The two equations, Equation (3.1) and Equation (3.2), were selected to obtain D_spoof, based on the number of delays used, as is described in theory in the previous section. If all possible delays are used in the ensemble signal then Equation (3.1) is used for calculating the delay and if fewer delays are present in ensemble then Equation (3.2) is used. This theoretically simulates the conditions created at the victim's end when under attack. The time-shifted signal that is selected to be kept on injects false data into the victim receiver about the distance. In the next module, "Received signal simulation," white Gaussian noise is added to the signal generated in the transmitter module, in order to simulate a real channel environment, which consists of wideband noise coming from various sources which are random processes by nature and cannot be predicted, such as black body radiation and internal thermal noise of the electronic components and conductors. As already discussed, the next few steps include converting the received time shifted signal to baseband by mixing it with some part of the transmitted waveform, so mxr_out is the output of this mixing stage, which is then ready for post processing. The next module, "Separate FFTs of up-sweep and down-sweep after mixer," reshapes the mixer output and separates it to extract both up-sweep and down-sweep data and store them separately in mxu and mxr respectively. Spectrum analysis of this time domain signal is what follows next, which is carried out using a custom-built FFT function ($MyFFT$), which returns two separate FFTs of mxu and mxr. Successively, this becomes the input for the next stage of constant false alarm rate (CFAR) analysis "CFAR and extraction of beat frequencies," which helps in target validation. The two beat frequencies If_up and If_down, as described in the previous chapter, are extracted after this stage and used to calculate range and velocity. The last module plots the experimental data for visual analysis.

This theoretical MATLAB simulation work successfully demonstrates that the two equations work exactly the way they are supposed to and select a delay depending on the time the victim's transmission T_r is received, to which the victim's receiver of the victim reacts in such a way as to detect the attacker's range as corresponding to the delay falsely injected by the attacker. As already discussed, Figure 3.3 demonstrates the selection of this one delay out of the ensemble that results in false range estimation.

Chapter 4

Experimental Setup

4.1 Background

Experimental setup consisted of two independently controlled Ettus Research USRP N210; one for the attacker and the other for the victim radar system (Figure 4.1). USRP was chosen among other options for simulating radar systems as this was what was available at the time of experimentation; the work will eventually be extended to include countermeasures for these attacks. To spare the expense and complexity of building a wireless RF front end (antenna, amplifier, etc.) for both the attacker and victim, and also lacking RF absorbing material or deflecting structures, a set distance was simulated between the two using a UV-resistant polyethylene-jacketed high-performance flexible low-loss coaxial cable "L-com CA-400 coax" [57] (this also allowed us to conduct the experiments indoors). Cables of the same length were used to connect the victim TX port to the attacker RX port and the attacker TX port to the victim RX port (Figure 4.2), which mimics the attacker's ability to absorb or deflect the victim's signal assumed in the threat model. Cable of 304 m was purchased and divided in four parts consisting of two 121 m cables and two 31 m cables. These two lengths were chosen to simulate two different ranges of 121 m and 31 m, which are quite widely apart from each other and provide an efficient way of utilizing the whole cable length without wasting a single inch.

The experimental setup also used an external coupler/mixer to mix the victim's transmitted and received signals (Figure 4.1). While GNU Radio can be made to perform this function, the timing delays inherent in sending and receiving samples from a USRP produce a shift in the beat frequencies; the necessary compensation process is nontrivial [58], but since the distance was simulated by physical coaxial connection and not by wireless, the unknown delay needed to be compensated for, thus justifying the use of an external mixer/coupler. Since the delay between host computer and USRP is inherently unpredictable, there was no way in which this delay could be removed. The safest resort was to introduce in the reference signal the same unknown delay with which the reflected signal was multiplied, thus compensating in real time. Finally, instead of using the RX port on the victim USRP for receiving the attacker signal, a Tektronix DPO7254C oscilloscope was used, configured to sample the mixed signal at 20MS/s (the same as the victim USRP), and MATLAB was used for range calculations. It is noted that both of these functions could be performed in GNU Radio but that the victim USRP lacked a daughterboard with sufficient frequency range to sample the beat frequencies, which are on the order of a few kHz at the ranges tested.

4.2 Victim Configuration

The victim radar system was designed to imitate an actual automotive FMCW radar system (parameters given in Table 4.1), as per the literature [2–4, 31–33]. Due to lack of a 77/24 GHz signal generator, tests were mounted on a 500 MHz carrier. Because of the limited sampling rates of the USRPs, the only achievable range resolution was 15 meters. The radar system (Figure 4.3) consists of a transmitter section developed in part using USRP N210 and the GNU Radio Companion.

It had a triangular wave generator that frequency modulated a carrier using a VCO, which was outputted on the USRP RF Port-T_1 to a forward direction coaxial cable through an external coupler. A MATLAB implementation of OS-CFAR included with the phased array toolbox, designed around Equation (2.11), was used. In the module "UHD:USRP source/sink," UHD is an acronym for USRP Hardware Driver. It is a driver developed by Ettus research and is compatible with all USRP devices and allows development on multiple operating systems including Windows, Linux, and Mac OS. The Hilbert Transform block converted float type data to complex data, as the UHD:USRP sink block expected only I/Q data. The coupler took a small part of the transmitted signal out via the CPL Port to serve as the local oscillator at the mixer for the down conversion of the received signal on the return path coaxial cable (Figure 4.4). This mixing process gave the required beat signal,

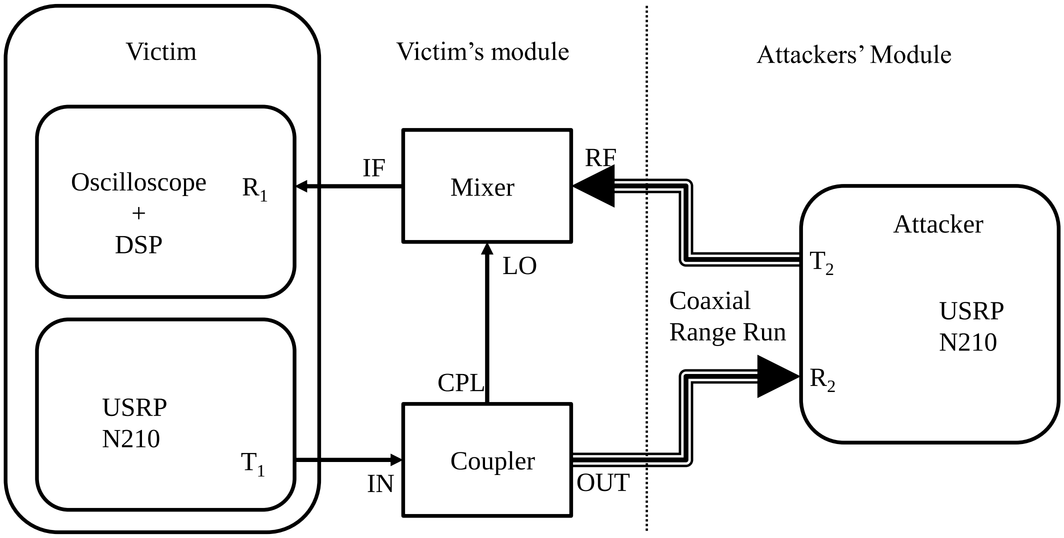


Fig. 4.1: Block representation of the experimental setup.

Table 4.1: FMCW parameters of the USRP radar.

Parameter	Value
Chirp Type	Triangular
Carrier Frequency	500 MHz
Sampling Frequency	20 MHz
Bandwidth	10 MHz
Chirp Period	5 ms
Range Resolution	15 m

which was captured using an oscilloscope on Port-R_1. The oscilloscope was controlled via MATLAB, where the rest of the signal processing, including filtering, frequency domain conversion, beat frequency extraction, and corresponding range estimation, was done (see Appendix B.1).

4.3 Attacker Configuration

The attacker setup resembled a regular radar system with only a few modifications (Figure 4.5). The first modification enabled us to transmit all the time-shifted signals using just one USRP transmitter. To accomplish this, a file was written using the MATLAB program "Ensemble Generation" (Appendix B.3) taking the sum of all the time-shifted signals to make the ensemble signal. The main code "Ensemble Generation" started with

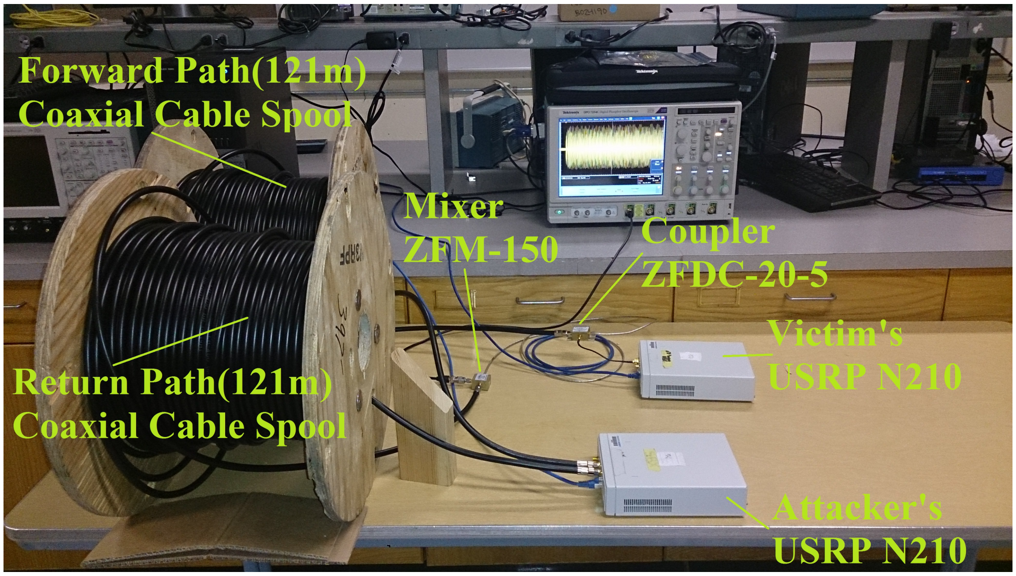


Fig. 4.2: Test bench setup for the attack.

declaring variables and constants that were going to be used throughout the program. The next module, “Creating delayed signal,” created a triangular waveform using a MATLAB function called “sawtooth,” which then was written into binary file “data_file.bin” in the last module. This file was then used as a file source in GNU Radio and added to the output of the VCO. One of the time-shifted signals, removed intentionally from the ensemble, instead was added to the ensemble through VCO. This eliminated the use of one multiply constant block at the output of VCO, thus saving the attack routine some time in switching that block on/off. A multiply block allowed us to turn the ensemble signal on (default state, value set to 1) or off (value set to 0).

Second, there was a variable delay block (default vaule of 0) set, using the delay calculated by Equation (3.1) or Equation (3.2), when the victim signal T_v is detected. The first two modifications worked in tandem to carry out the attack: when the victim's signal was detected the multiply block was set to zero and the variable delay block was set according to Equation (3.1) or Equation (3.2), which resulted in only the correct chirp signal being transmitted to the victim.

Third, a custom attack block was written in Python that included a threshold detector responsible for triggering the main attack routine as soon as it detected a signal above a

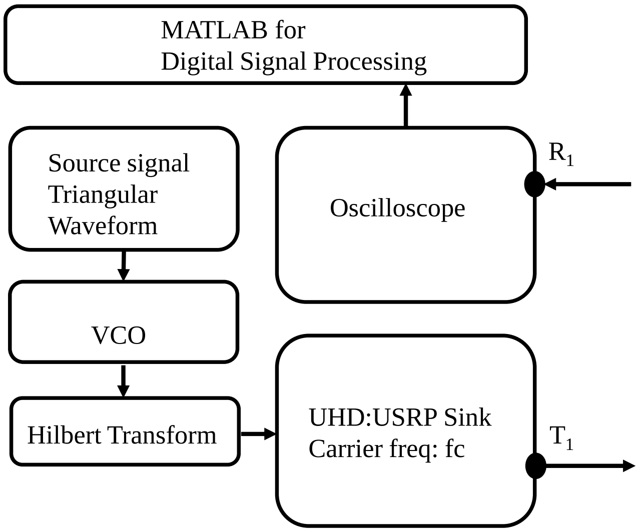


Fig. 4.3: Block diagram for the victim radar system.

set threshold on the forward line on Port-R_2 (the attacker's RX port). The attack routine was responsible for disabling the ensemble signal by setting the multiply block and then calculating the correct delay and setting the variable delay block.

In summary, GNU Radio code started the ensemble transmission and waited until a threshold was crossed on Port-R_2. As soon as it was crossed, a function was called that: 1) logged the receive time T_r with respect to a timer; 2) used T_r with Equation (3.1) or Equation (3.2) to calculate the delay; 3) set the variable delay block to the correct delay; and 4) stopped the transmission from the ensemble file source by setting the constant in multiplication block to 0. In this way it became possible to falsely inject A_t, which traveled through Port-T_2 to the RF-Port of the victim, via the return path, and resulted in a false range calculation at the victim's end.

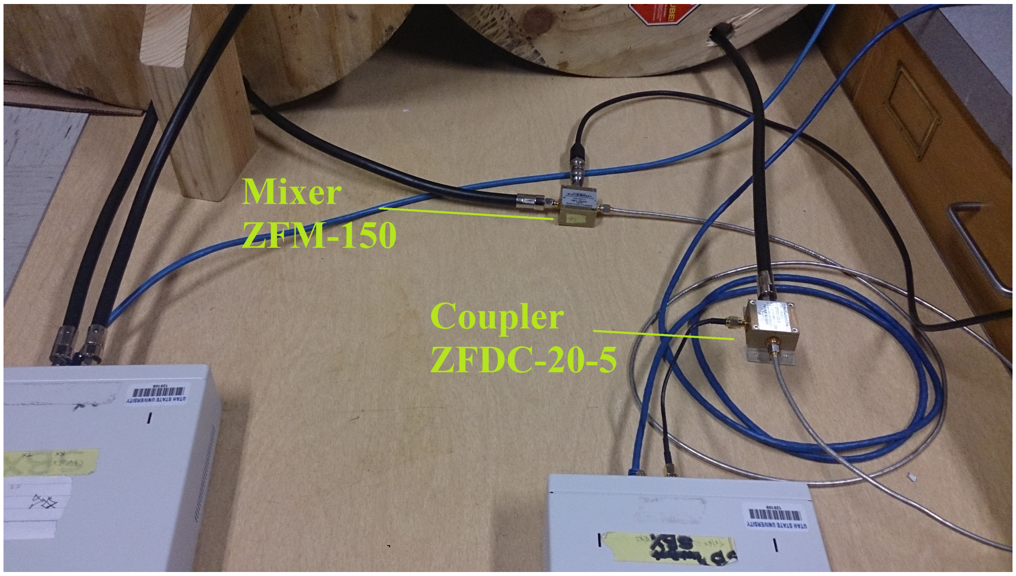


Fig. 4.4: Detail of test bench setup: mixing stage.

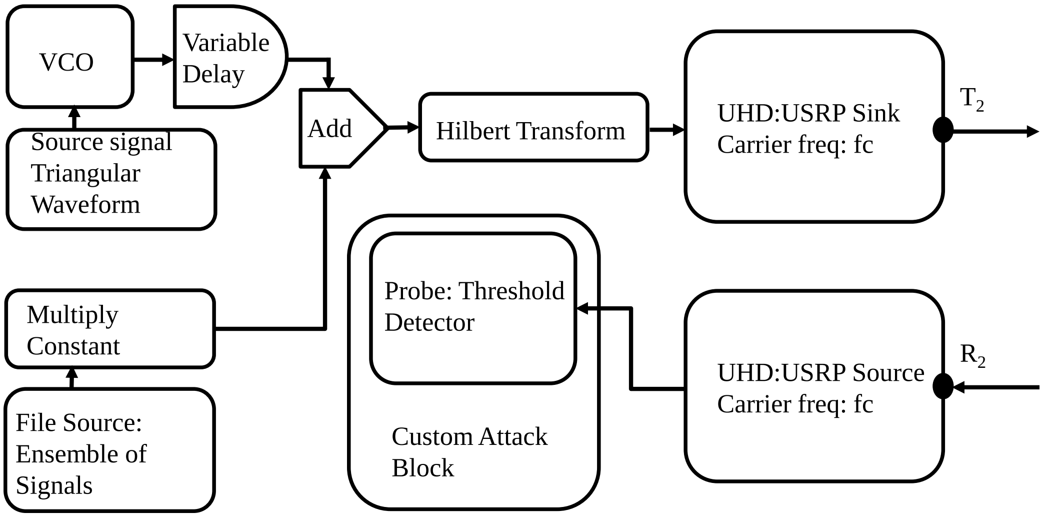

VCO
Variable Delay
Source signal Triangular Waveform
Add
Hilbert Transform
UHD:USRP Sink Carrier freq: fc
T_2
Multiply Constant
File Source: Ensemble of Signals
Probe: Threshold Detector
Custom Attack Block
UHD:USRP Source Carrier freq: fc
R_2

Fig. 4.5: Block diagram for the attacker's radar system.

Chapter 5

Results

Initial tests were run without the attacker module in order to ensure that the system was able to calculate the correct range. Two different ranges were simulated for the purpose of the experimental analysis of this attack.

- 121 m: Two 121 m (one-way) coaxial cables were connected in series to make a round-trip distance of 242 m, which corresponds to an object at a range of 121 m. A total of 50 measurements were taken and averaged to find a mean distance of 128 m, which given a 15 m resolution (from Equation (2.6)) is indistinguishable from 121 m.

- 31 m: Two 31 m (one-way) coaxial cables were connected in series to make a round-trip distance of 62 m, which corresponds to an object at a range of 31 m. Fifty measurements were taken and averaged to find a mean distance of 34 m, which given a 15 m resolution is indistinguishable from 31 m.

Having verified the operation of the system, the attacker module was deployed in the middle of the 242 m and 62 m paths respectively, to examine the effect of a false data injection attack at two different ranges, 121 m and 31 m.

For the attack scenarios it was assumed that the attacker knew the actual distance between the victim's radar and their own. In the first scenario the attacker created an ensemble signal with bins that corresponded to objects at distances smaller than the actual distance R_a, and in the second the ensemble contained all the range bins for an object at the resolution of the radar. That is, in the first scenario an attacker was only seeking to decrease the apparent range, while in the second the attacker attempted to appear at a specific distance from the victim.

For the first scenario with an actual distance of 121 m, the setup was able to falsify range data every single time the experiment was run (50 runs total). It was possible to decrease the apparent distance to as low as the resolution of the system, in many cases.

Efforts to decrease the apparent range by a predefined amount, scenario two, resulted in 90% success for $R_s = 15\,\mathrm{m}$ and 80% success for $R_s = 30\,\mathrm{m}$, where R_s represents the apparent distance of the attacker; i.e. the attacker could be made to appear to be located 15 m and 30 m from the victim in 90% and 80% of the runs (ten for each case), respectively. While attempts to make the attacker appear at greater distances were more variable, the attack nonetheless produced a decrease in distance in every case. Figure 5.1 shows the outcome of OS-CFAR (i.e. probability of detection) for several attacks at the distance of 121 m. Figure 5.1(a) provides the baseline response of the system in the absence of an attacker (the correct range of 121 m is detected). In Figures 5.1(b)–(d) the attacker attempts to spoof a specific range (15 m, 30 m, and 45 m, respectively). It can clearly be seen that the apparent range as detected by the victim has been considerably decreased from the original 121 m. Also visible are harmonics in different range bins, which have been masked. This coupled with the latency issues in the system result in always decreasing the distance in the range of 5 m–20 m, which can be approximated to 15 m; 25 m–35 m, which can be approximated to 30 m; and 40 m–50 m, which can be approximated to 45 m.

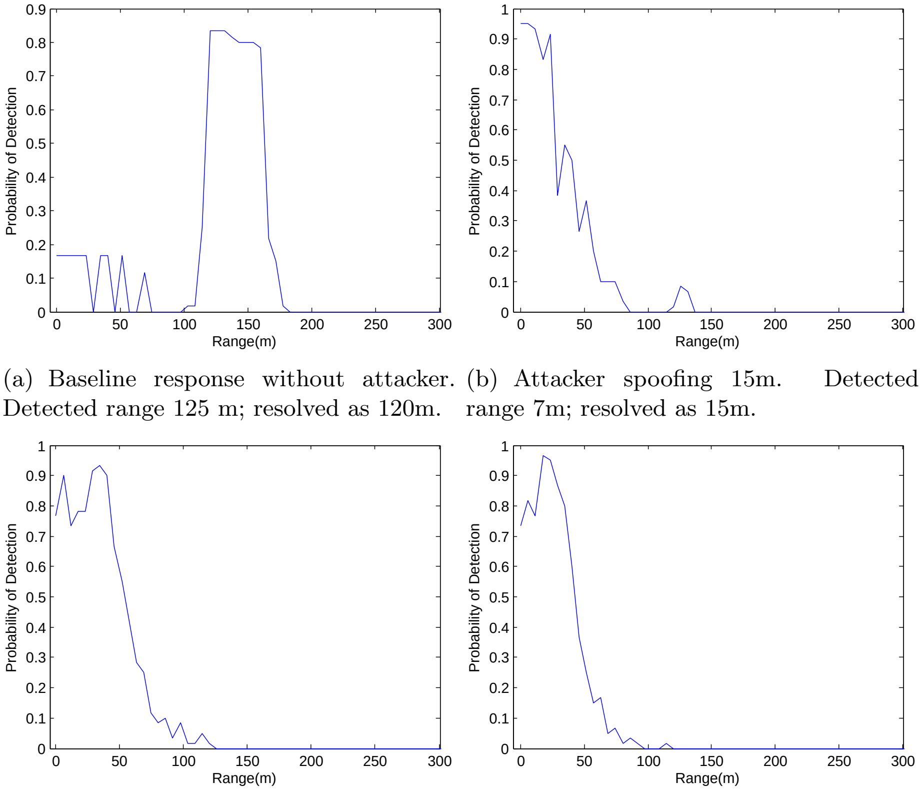
For the 31 m cable (actual distance 31 m), in scenario two, a range resolution of 15 m implies that it is only possible for an attacker to decrease their apparent range to 15 m. However, testing showed the practical application to deviate by 4 m from the theoretical ideal: in 50 runs, the average was found to be 19 m. The minimum value in these 50 runs was 6 m and the maximum was 30 m.

Over 100 samples were used to demonstrate that indeed the distance was decreased every single time, but the amount of the decrease did not match the range resolution specified.

The most significant result of the experiments was determining the number of non-ensemble chirps that an attacker needs to successfully decrease their apparent distance.

In both scenarios, it takes just one complete and clean set of up and down chirps for the attacker to fool the victim into calculating the wrong distance. That is, given a radar system that transmits n chirps (up+down) to estimate range, for the attack to be viable the attacker only needs to be able to calculate the spoofing delay and transmit the single delay signal within $n-1$ set of chirps. This result corroborates the theoretical results that arise due to object estimation and qualification by the OS-CFAR detector.

OS-CFAR qualifies an object in a noise clutter by estimating the probability of false alarm for every range bin under test. The one with the least probability of false alarm is then qualified as a potential object; i.e. OS-CFAR can clearly identify the spoofed range in the single delay signal and when it looks to past chirps it also sees the spoofed range (because of the ranges present in the ensemble signal), which results in a high probability of the spoofed range being identified as a legitimate object. By reducing latency in the setup (turning off interrupt coalescing for the Ethernet card and using small frame sizes for the attacker), it was observed that the attacker was able to respond within 2.5–5 chirps for all cases. This number could be further reduced by moving the attack module to the USRP itself.



(a) Baseline response without attacker. Detected range 125 m; resolved as 120m.

(b) Attacker spoofing 15m. Detected range 7m; resolved as 15m.

(c) Attacker spoofing 30m. Detected range 40m; resolved as 45m.

(d) Attacker spoofing 45m. Detected range 18m; resolved as 15m.

Fig. 5.1: OS-CFAR output demonstrating outcome of the attack at 121m. Range with highest probability taken to be actual range.

Chapter 6

Conclusions and Future Work

In this work a distance-decreasing attack on FMCW-based ranging systems using analog false data injection has been proposed. Theoretical and experimental analysis demonstrates the feasibility of such an attack on an actual system modeled on automotive radars.

While it turns out that it was not possible to decrease the range at predefined amounts for every spoofable range, attacks were always successful in decreasing the apparent distance to the object. This inaccuracy can be attributed to two causes: multi-target clutter and delay in the attacker's system. As Cheng et al. [59] describe, in an N-target environment, the reflected signals from different targets blend with one another at the receiver, resulting in masking (harmonics of targets increasing the amplitudes of other bins), and thus the system ends up detecting a random target. The ensemble signal used in the attack module simulates such a multi-target environment; by reducing the granularity of the spoofed position it might be possible to reduce this effect. Additionally, since both the victim and attacker modules were designed using USRPs, inherent delays in host-to-radio communication prevented 100% success rates in spoofing arbitrary distances; however, by migrating the attack code to field programmable gate arrays (FPGA) of the USRPs, delays should be minimized and a correspondingly higher attack success rate achieved.

While it has been shown that distance-decreasing attacks are feasible against FMCW radar, future work will focus on extending the attack model to allow the attacker to falsify their apparent velocity and mounting attacks against commercial automotive radars, or even, in the short term, higher-performing analogues of such systems. USRPs with higher sampling rates of up to 120 MHz could be used to decrease the range resolution, for example. Mounting the attack against commercial automotive radar, which operate at 24/77 GHz, presents several challenges—such as the difficulty of tracking the victim's carrier and minimizing self-interference due to coupling and reflections of the attack platform—that suggest that scaling the attack to commercial radars will be nontrivial.

These challenges are also suggestive of possible countermeasures to a distance-decreasing attack: randomizing the chirp pattern (Figure 6.1), the bandwidth of the chirp, the duration of the chirp, and the initial frequency of the chirp. It is not clear at present whether commercial radars use a preset carrier frequency randomly selected at manufacture time to avoid interference, or one that varies. Even should commercial radars vary their carrier, a resourceful attacker could employ USRPs in a MIMO configuration to cover a large bandwidth and create ensembles that vary in their starting and ending frequencies or utilize an array of external VCOs to apply the ensemble signal to a subset of carriers. Random chirp patterns present a stronger defense, as they would require an attacker to guess the pattern ahead of time, leading to a probabilistic chance of success that would be dependent on the particular false alarm detection technique used. Future work will evaluate the efficacy of these approaches to adapted forms of this attack.

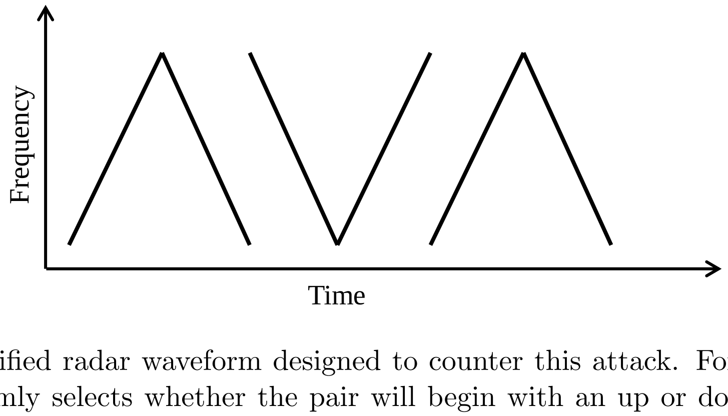


Fig. 6.1: A modified radar waveform designed to counter this attack. For each chirp pair the radar randomly selects whether the pair will begin with an up or down chirp. Other possible countermeasures include changing the duration of the chirp and its bandwidth or starting frequency.

References

[1] R. Jones, *Most Secret War.* Wordsworth Editions Limited, 1998.

[2] H. Rohling and E. Lissel, "77 ghz radar sensor for car application." in *Record of the IEEE 1995 International Radar Conference. IEEE*, pp. 373-379, 1995.

[3] H. Rohling and M. Meinecke., "Waveform design principles for automotive radar systems." in *Proceedings, CIE International Conference on Radar. IEEE*, 2001.

[4] M. A. Richards, *Fundamentals of Radar Signal Processing*, S. S. Chapman, Ed. McGraw-Hill, 2005.

[5] F. Semiconductor, "Automotive radar millimeter-wave technology," http://www.freescale.com/webapp/sps/site/overview.jsp?code=AUTRMWT, [Online; accessed 27-May-2014].

[6] C. AG, "Ars 300 long range radar sensor 77 ghz," http://www.conti-online.com/www/industrial_sensors_de_en/themes/ars_300_en.html, [Online; accessed 27-May-2014].

[7] T. Beez., W. (DE), K. Lehre, and M. (DE), "Radar sensor for motor vehicles," U.S. Patent US 7,151,479 B2, 2006.

[8] A. Wise, M. Dean, H. Dong, and W. D. Oberpriller, "Configurable radar sensor," U.S. Patent US 7,612,707 B2, 2009.

[9] K. S. Chang, J. Karl Hedrick, W.-B. Zhang, P. Varaiya, M. Tomizuka, and S. E. Shladover, "Automated highway system experiments in the path program," *Journal of Intelligent Transportation Systems*, vol. 1, no. 1, pp. 63–87, 1993.

[10] S. Tsugawa, S. Kato, K. Tokuda, T. Matsui, and H. Fujii, "A cooperative driving system with automated vehicles and inter-vehicle communications in demo 2000," in *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE.* IEEE, pp. 918–923, 2001.

[11] L. Li and F.-Y. Wang, *Advanced motion control and sensing for intelligent vehicles.* Springer, 2007.

[12] K.-S. Chang, W. Li, P. Devlin, A. Shaikhbahai, P. Varaiya, J. Hedrick, D. McMahon, V. Narendran, D. Swaroop, and J. Olds, "Experimentation with a vehicle platoon control system," in *Vehicle Navigation and Information Systems Conference, 1991*, vol. 2. IEEE, pp. 1117–1124, 1991.

[13] P. Kavathekar and Y. Chen, "Vehicle platooning: A brief survey and categorization," in *ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference.* American Society of Mechanical Engineers, pp. 829–845, 2011.

[14] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Professional*, vol. 6, no. 1, pp. 24–29, 2004.

[15] N. Polmar, "The U. S. navy electronic warfare (part 2)," in *United States Naval Institute Proceedings*, pp. 121–122, Nov.1979.

[16] S. Roome, "Digital radio frequency memory," *Electronics & Communication Engineering Journal*, vol. 2, no. 4, pp. 147–153, 1990.

[17] D. L. Adamy, *Introduction to Electronic Warfare Modeling.* Norwood: Artech House, 2006.

[18] S. Capkun and Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks*, vol. 2, no. 24, pp. 221–232, 2006.

[19] J. Clulow, G. Hancke, M. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," in *3rd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks, Lecture Notes in Computer Science*, pp. 83,97, Chicago: Springer, 2006.

[20] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks." in *INFOCOM 2003, Twenty-Second Annual Joint Conference of IEEE Computer and Communications. IEEE Societies*, vol. 3, 2003.

[21] Y. Hu, A. Perrig, and Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," no. 22, pp. 30–40.

[22] Sastry, Naveen, U. Shankar, and D. Wagner., "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on wireless security. ACM*, 2003.

[23] S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE.*, vol. 3, 2005.

[24] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical layer attacks on chirp-based ranging systems," in *WISEC '12 Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pp. 15-26, 2012.

[25] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "Gps software attacks," in *Proceedings of the 2012 ACM Conference on Computer and communications security.* ACM, pp. 450–461, 2012.

[26] M. Poturalski, M. Flury, P. Papadimitratos, J. Hubaux, and J. Le Boudec, "The cicada attack: Degradation and denial of service in ir ranging," in *Ultra-Wideband (ICUWB), IEEE International Conference*, pp. 1-4, 2010.

[27] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York: ACM, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[28] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proceedings of the 19th USENIX Conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929848

[29] D. Kune, J. Backes, S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy (SP)*, pp. 145–159, May 2013.

[30] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems - CHES 2013*, ser. Lecture Notes in Computer Science, G. Bertoni and J.-S. Coron, Eds. Springer Berlin Heidelberg, 2013, vol. 8086, pp. 55–72. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40349-1_4

[31] M. Schneider, "Automotive radar: status and trends," in *German Microwave Conference*, 2005.

[32] H. Rohling and R. Mende, "Os cfar performance in a 77 ghz radar sensor for car application," in *Proceedings, CIE International Conference of Radar*, pp. 109-114. IEEE, 1996.

[33] M. Ghada, "Radio wave propagation characteristics in fmcw radar." *Dynamic Dipole-Dipole Magnetic Interaction and Damped Nonlinear Oscillations*, p. 275, 2009.

[34] E. A. Sheffer and M. J. Thompson, "Vehicle tracking system," U.S. Patent US 5,218,367, 1993.

[35] X. Li, X. Yao, Y. L. Murphey, R. Karlsen, and G. Gerhart, "A real-time vehicle detection and tracking system in outdoor traffic scenes," in *Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004*, vol. 2. IEEE, pp. 761–764, 2004.

[36] C.-H. Hsu, "Electronic parking sensor apparatus," U.S. Patent US 4,855,736, 1989.

[37] A. Takahashi, Y. Ninomiya, M. Ohta, M. Nishida, and M. Takayama, "Rear view lane detection by wide angle camera," in *Intelligent Vehicle Symposium, 2002. IEEE*, vol. 1. IEEE, pp. 148–153, 2002.

[38] F. Brugger, M. Burckhardt, and A. Faulhaber, "Anti-lock brake system," U.S. Patent US 4,861,118, 1989.

[39] O. Tur, O. Ustun, and R. N. Tuncay, "An introduction to regenerative braking of electric vehicles as anti-lock braking system," in *Intelligent Vehicles Symposium, 2007 IEEE*. IEEE, 2007, pp. 944–948.

[40] T. Abe, M. Hara, S. Kamio, K. Sakita, and M. Takao, "Traction control system," U.S. Patent US 5,018,595, 1991.

[41] T. Tanaka and K. ISODA, "Traction control system," *JSME International Journal. Ser. 3, Vibration, Control Engineering, Engineering for Industry*, vol. 35, no. 1, pp. 116–120, 1992.

[42] "A car that raises the tempo," 2014.

[43] A. Jalil, H. Yousaf, F. Fahim, and Z. Rasool, "Fmcw radar signal processing scheme," in *Proceedings of International Bhurban Conference on Applied Science and Technology*, 2011.

[44] H. Rohling and C. Moller., "Radar waveform for automotive radar systems and applications." in *Radar Conference, RADAR'08. IEEE*, 2008.

[45] D. F. Pierrottet, F. Amzajerdian, L. Petway, B. Barnes, G. Lockard, and M. Rubio., "Linear fmcw laser radar for precision range and vector velocity measurements," in *Materials Research Society Proceedings, vol. 1076*, pp. 1076-K04, 2008.

[46] H. Griffiths, "New ideas in fm radar," *Electronics & Communication Engineering Journal*, vol. 2, no. 5, pp. 185 – 194, Oct. 1990.

[47] S.-H. Jeong, H.-Y. Yu, J.-E. Lee, J.-N. Oh, and K.-H. Lee., "A multi-beam and multi-range radar with fmcw and digital beam forming for automotive applications." *Progress in Electromagnetics Research*, vol. 124, pp. 285–299, 2012.

[48] M. Jankiraman, *Design of Multi-Frequency CW Radars.* SciTech Publishing, 2007.

[49] G. M. Brooker, "Understanding millimetre wave fmcw radars," in *1st International Conference on Sensing Technology*, pp. 152–157, 2005.

[50] F. Nathanson, J. Reilly, and M. Cohen, *Radar Design Principles*, 2nd ed. McGraw-Hill, 1991.

[51] Vinoy, K. Joseph, and R. M. Jha, *Radar Absorbing Materials: From Theory to Design and Characterization.* Boston: Kluwer, 1996.

[52] K. Gaylor, "Radar absorbing materials-mechanisms and materials," Materials Research Labs Ascot Vale (Australia), Tech. Rep. MRL-TR-89-1, 1989.

[53] P. Saville, "Review of radar absorbing materials," Defence Research and Development Atlantic Dartmouth (Canada), Tech. Rep. DRDC-TM-2005-003, 2005.

[54] E. F. Knott, J. Shaeffer, and M. Tuley, *Radar Cross Section.* SciTech Publishing, 2004.

[55] A. Technologies, "Absorber for automotive radar sensors," 2014.

[56] D. W. Hahn and K. S. Lee, "Microwave absorber for 24ghz short range automotive radar system," in *Vehicle Power and Propulsion Conference (VPPC), 2012 IEEE*, pp. 1023–1026, Oct. 2012.

[57] February 2014. [Online]. Available: http://www.l-com.com/coaxial-l-com-ca-400-coax-cable-bulk-reel-1000-feet

[58] A. B. Suksmono, “A simple solution to the uncertain delay problem in usrp based sdr-radar systems,” *arXiv preprint arXiv:1309.4843*, 2013.

[59] K.-W. Cheng and H.-J. Su, “Multi-target signal processing in fmcw radar system with antenna array,” in *Radar Conference, 2008. RADAR’08*, pp. 1–5, IEEE, 2008.

Appendices

Appendix A

Derivation for Range Spoofing Equations

A.1 Derivation for Equation (3.1) ($D_a = D_t$)

The signal transmitted by victim is received by the attackers after T_r seconds have elapsed since the timer was started at the attacker's end. Divide T_r by $2t_m$ (t_m is the duration of one up/down chirp) to get an estimated number of waveforms. The whole number in this result represents n complete triangular waveforms while decimal value represents some portion of the $n + 1^{th}$ waveform. The decimal part needs to be extracted, as it will give the exact time at which the victim started transmitted and in turn the expected delayed reception on the return path. So, the division is

$$= \frac{T_r}{2t_m}.$$

Removing the decimal value by subtracting the whole number; $floor\left(\frac{T_r}{2t_m}\right)$,

$$= \frac{T_r}{2t_m} - floor\left(\frac{T_r}{2t_m}\right).$$

Multiplying this result with a single waveform time ($2t_m$) would scale down this decimal value to a location within a single triangle (up chirp+down chirp),

$$= 2t_m\left[\frac{T_r}{2t_m} - floor\left(\frac{T_r}{2t_m}\right)\right].$$

Divide this by time corresponding to delay of one sample, $T_{1d} = 1/f_s$, where f_s is the sampling frequency

$$= 2t_m f_s \left[\frac{T_r}{2t_m} - floor\left(\frac{T_r}{2t_m}\right)\right].$$

To this add time delay corresponding to actual range $\left(\frac{R_a f_s}{c}\right)$ and subtract time delay $\left(\frac{2R_d f_s}{c}\right)$ corresponding to $2R_d$

$$= 2t_m f_s \left[\frac{T_r}{2t_m} - floor\left(\frac{T_r}{2t_m}\right)\right] + \left(\frac{R_a f_s}{c}\right) - \left(\frac{2R_d f_s}{c}\right),$$

simplifying

$$= 2t_m f_s \left[\frac{T_r}{2t_m} - floor\left(\frac{T_r}{2t_m}\right)\right] + \left[\frac{(R_a - 2R_d) \times f_s}{C}\right].$$

By further simplification, the resultant equation is

$$D_{spoof} = \left\{T_r - 2t_m \times floor\left(\frac{T_r}{2t_m}\right) + \frac{(R_a - 2R_d)}{C}\right\} \times f_s. \tag{3.1}$$

A.2 Derivation for Equation (3.2) ($D_a < D_t$)

If not all D_t but only D_a delays are used, the number of delay bins that have to be skipped is given by $S_d = \frac{D_t}{D_a}$. Now using Equation (3.1),

$$K = \left\{T_r - 2t_m \times floor\left(\frac{T_r}{2t_m}\right) + \frac{R_a}{C}\right\} \times f_s.$$

Figure A.1 depicts the intent of Equation (3.2): that it is to select the $V_{R'}$ that occurs at a location just before the actual return delay in the ensemble of spoofing signal. V_R, $V_{R'}$, V_T and A_R denote the authentic received victim signal, attacker-induced victim received signal, victim transmitted signal, and the attacker received signal, respectively. The delay corresponding to $V_{R'}$ is a multiple of S_d, so $V_{R'} = m \times S_d$. Now in order to enforce the closest delay just before V_R condition

$$\begin{aligned} K - m \times S_d &< S_d, \\ &\rightarrow S_d(1+m) > K, \\ &\rightarrow 1 + m > \frac{K}{S_d}, \\ &\rightarrow \left(\frac{K}{S_d} - 1\right) < m, \end{aligned}$$

taking

$$\left(\frac{K}{S_d} - 1\right) < m,$$

taking an average and rounding off the result of

$$\left(\frac{K}{S_d}\right) + m,$$

gives

$$round\left(\frac{K}{S_d} - \frac{1}{2}\right) = m,$$

results in

$$D_{spoof} = m \times S_d,$$

which by expansion yields

$$D_{spoof} = round\left(\frac{K}{S_d} - 0.5\right) \times S_d. \tag{3.2}$$

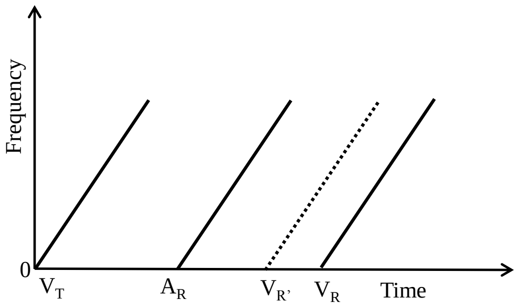


Fig. A.1: Depiction of the intent of Equation (3.2).

Appendix B

Source Code

B.1 Signal Processing at the Victim's End

Main MATLAB code:

```
clearvars -except final_ch; clc;
format longG;
tic;
%variables
C=3e8;              % velocity of light in free space
Fm=100;             % frequency of triangular wave
Tm=1/(2*Fm);        % sweep period (up sweep+down sweep)
fs=20e6;            % sampling frequency
B=fs/2;             % Bandwidth (amplitude) of triangular wave
M=5;                % number of triangular waveforms (up+down chirps)
% chirps transmitted by victim
seglen=300000;
fid1=fopen('data_fmcw_v4_Txd.dat','rt');
A = fread(fid1,seglen,'float');
A=A';
Txd=A;
fclose(fid1);

%% mixer output
mxr_out = final_ch(2,:);
```

```
%% Separate ffts of upsweep and downsweep after mixer
% extract up and down chirps from the mixed signal
nchrp=find(Txd==min(Txd),1)-find(Txd==10,1);
mxrs = mxr_out(1:end-(length(mxr_out)-nchrp*2*M));
mxrs = reshape(mxrs,nchrp,2*M);
mxu=mxrs(:,1:2:2*M);     %up chirps
mxd=mxrs(:,2:2:2*M);     %down chirps

% fft of upsweep
[fft_upsweep,f_upsweep,nfft_upsweep,nfft]=MyFFT(mxu,fs);
% fft of downsweep
[fft_downsweep,f_downsweep,nfft_downsweep,~]=MyFFT(mxd,fs);

% CFAR and extraction of beat frequencies
lim=300;
[detect_upbeat,th_upbeat,pd_upbeat]...
                                =MyCFAR(fft_upsweep(1:lim,:));
[detect_downbeat,th_downbeat,pd_downbeat]...
                                =MyCFAR(fft_downsweep(1:lim,:));
[pd_upbeat_maxvalue,pd_upbeat_maxloc]=max(pd_upbeat);
[pd_downbeat_maxvalue,pd_downbeat_maxloc]=max(pd_downbeat);
If_up=f_upsweep(pd_upbeat_maxloc);
If_down=f_downsweep(pd_downbeat_maxloc);

% Range calculation in practical scenario
f_range=abs(If_up+If_down)/2;
Range_measured=f_range*Tm*(C)/(2*B);
```

```
% disp(['Actual Range: ' num2str(R) 'm']);
disp(['Calculated␣Range:␣' num2str(Range_measured) 'm']);
toc


%range for all the frequencies (for plot)
range_measured = abs(f_upsweep)*Tm*(C)/(2*B);
%plots
figure;
plot(range_measured(1:length(detect_upbeat)),pd_upbeat);
lim1=90
figure;
subplot(4,1,1);
plot(abs(fft_upsweep(1:lim1,:)),'LineWidth',2);
hold on;
plot(th_upbeat(1:lim1),'color','red');
subplot(4,1,2);
plot(range_measured(1:lim1),...
    abs(fft_downsweep(1:lim1,:)),'LineWidth',2);
hold on;
plot(th_downbeat(1:lim1),'color','red');
subplot(4,1,3);
plot(range_measured(1:lim1),detect_upbeat(1:lim1,:));
subplot(4,1,4);
plot(range_measured(1:lim1),detect_downbeat(1:lim1,:));
```

FFT function:

```
%% This function converts time domain signal to
% frequency domain for spectral analysis
% It uses fft function of signal processing toolbox.
```

```
function [signal_fft ,f ,nfft_range ,nfft] = MyFFT(signal ,fs)
l_signal=size(signal ,1);
nfft=2^18;
fft_out = fft(signal ,nfft)/l_signal;
f = fs/2*linspace(0,1,nfft/2);
signal_fft=fft_out;
nfft_range=1:nfft/2;
end
```

OSCFAR detection using phased array toolbox in MATLAB:

```
%% This function uses CFARDetector implemented
% by phased array toolbox of MATLAB to calculate
% probability of detection
function [Z_detect ,Th,Pd] = MyCFAR(mx_signal)
[N,Ntrials] = size(mx_signal);
Ntraining = 70;
Nguard = 0;
Pfa_goal = 0.0001;
rank=round(0.75*Ntraining);
hdet = phased.CFARDetector('Method','OS',...
      'NumTrainingCells',Ntraining,'NumGuardCells',Nguard,...
      'ProbabilityFalseAlarm',Pfa_goal,'Rank',rank);

hdet.ThresholdOutputPort=true;
[Z_detect ,Th] = step(hdet ,abs(mx_signal).^2,1:N);
for i=1:N
     Pd(i,1) =sum(Z_detect(i,:))/Ntrials;  %Probability of detection
end
```

B.2 MATLAB Simulation of FMCW Radar

```
clear all; clc;


%% Transmitted Signal generation
%---------------------------------------------------------------
%---------------------------------------------------------------
% Triangle wave generation using Sawtooth function
%---------------------------------------------------------------
format longG


tic;
fc=5e6;             % carrier frequency
delfc=5e6;          % maximum frequency deviation
fmin=fc-delfc;      % minimum frequency
fmax=fc+delfc;      % maximum frequency
Tm = 10e-3;         % sweep period (up sweep+down sweep)
Fm = 1/Tm;          % frequency of triangular wave
B =2*delfc;         % Bandwidth (amplitude) of triangular wave
fs=2*(fmax);        % sampling frequency
ts=1/fs;            % time of 1 delayed sample or
                    % rate of change of transmit frequency
M = 3;              % How many periods are shown
R =121;             % range of the object
V =0;               % Velocity of the target in mtr/sec
C = 3e8;            % velocity of light in free space
del=(2*R)/C;        % extra time after Ts (due to R)
fd=(2*V*fc)/C;      % Doppler shift
totnum_dly=Tm/ts;% total number of delays
```

```
                        % for 100% attack at all the ranges
%Ndact = 6;
skip_pts=round(totnum_dly/num_dly);
dR = C/(2*B);     % range resolution
skip_pts=round(R/dR);

t = 0:ts:M*Tm;
l_total=length(t);
F=sawtooth(2*pi*Fm*t,0.5);

%Transmitted Signal
Txd0=-1+zeros(1,l_total);
Txd0=F;

% Modulation (using vco to generate
% sinusoid at frequency varying with sawtooth)
final_Txd0 = vco(Txd0,[fmin fmax],fs);
minus1to0_0 = find(Txd0==0);
final_Txd0(minus1to0_0)=0;

%% Creating delayed signals for ensemble
Txd=-1+zeros(1,l_total);
Txd(1,:)= F(1:l_total);
Txd2=vco(Txd(1,:),[fmin fmax],fs);
inter_Txd=zeros(Ndact,length(Txd2));
inter_Txd(1,:)=Txd2;
j=1;
for i=2:Ndact
```

```
    j=j+skip_pts;
    inter_Txd(i,:)=Txd2([end-j+1:end 1:end-j]);
end

%% Selecting delay using the two equations
flag=1; %all delays used: flag=1 otherwise flag=0
Tr= 12.02345;    % time victim's transmission received
Rd= 60;          % to be decreased by this range
if flag==1       % Eq-A
     D_spoof = (Tr-Tm*floor(Tr/(Tm))+((R-2*Rd)/c))* fs;
else             % Eq-B
    K = (Tr-Tm*floor(Tr/(Tm))+(R/c))* fs;
     D_spoof = round((K/skip_pts)-0.5)*skip_pts;
end

inter_Txd1=inter_Txd;

%zeroing out some chirps for some delays (t=y/fs)
inter_Txd1([1:D_spoof-1,D_spoof+1:end],0.017*fs+1:end)=0;
final_Txd=sum(inter_Txd1,1);

%%
%plot triangle wave
figure1 = figure(1);
plot(t,Txd0,'LineWidth',1,'color','b')
title('Modulating␣Triangle␣Function');
ylabel('Amplitude');
```

```
%% Received signal Simulation
%--------------------------------------------------------------
%--------------------------------------------------------------
%triangle wave definition (using sawtooth function)
%--------------------------------------------------------------
%adding white gaussian noise to the return signal
%to simulate real channel environment
final_Rxd_noise=awgn(final_Txd,34,'measured');
spectrogram(final_Txd(0.005*fs:0.015*fs),...
    kaiser(256,5),[],[],fs,'yaxis');

%mixing stage
mxr_out=final_Txd0.*final_Rxd_noise;

%% Separate ffts of upsweep and downsweep after mixer
% extract up and down chirps from the mixed signal
nchrp=find(Txd==min(Txd),1)-find(Txd==10,1);
mxrs = mxr_out(1:end-1);
mxrs = reshape(mxrs,nchrp,2*M);
mxu=mxrs(:,1:2:2*M);    %up chirps
mxd=mxrs(:,2:2:2*M);    %down chirps

% fft of upsweep
[fft_upsweep,f_upsweep,nfft_upsweep,nfft]=MyFFT(mxu,fs);
% fft of downsweep
[fft_downsweep,f_downsweep,nfft_downsweep,~]=MyFFT(mxd,fs);

% CFAR and extraction of beat frequencies
```

```
lim=300;
[detect_upbeat,th_upbeat,pd_upbeat]...
    =MyCFAR(fft_upsweep(1:lim,:));
[detect_downbeat,th_downbeat,pd_downbeat]...
    =MyCFAR(fft_downsweep(1:lim,:));
[pd_upbeat_maxvalue,pd_upbeat_maxloc]=max(pd_upbeat);
[pd_downbeat_maxvalue,pd_downbeat_maxloc]=max(pd_downbeat);
If_up=f_upsweep(pd_upbeat_maxloc);
If_down=f_downsweep(pd_downbeat_maxloc);

% Range calculation in practical scenario
f_range=abs(If_up+If_down)/2;
Range_measured=f_range*Tm*(C)/(2*B);
disp(['Actual␣Range:␣' num2str(R) 'm']);
disp(['Calculated␣Range:␣' num2str(Range_measured) 'm']);

% Velocity calculation in practical scenario
f_velocity=(If_down-If_up)/2; %this is also the fd
Velocity_measured=(C*abs(f_velocity))/(2*fc);
disp(['Actual␣Velocity:␣' num2str(V) 'm/s']);
disp(['Calculated␣Velocity:␣' num2str(Velocity_measured) 'm/s']);
% Decision of direction of motion with respect to the radar
if f_velocity<0
    disp(['Direction=␣Receding␣Target']);
elseif f_velocity>0
    disp(['Direction=␣Approaching␣Target']);
else
    disp(['Direction=␣Stationary␣Target']);
```

```
end

toc

%range for all the frequencies (for plot)
range_measured = abs(f_upsweep)*Tm*(C)/(2*B);
%plots
figure;
plot(range_measured(1:length(detect_upbeat)),pd_upbeat);
lim1=90
figure;
subplot(4,1,1);
plot(abs(fft_upsweep(1:lim1,:)),'LineWidth',2);
hold on;
plot(th_upbeat(1:lim1),'color','red');
subplot(4,1,2);
plot(range_measured(1:lim1),...
    abs(fft_downsweep(1:lim1,:)),'LineWidth',2);
hold on;
plot(th_downbeat(1:lim1),'color','red');
subplot(4,1,3);
plot(range_measured(1:lim1),detect_upbeat(1:lim1,:));
subplot(4,1,4);
plot(range_measured(1:lim1),detect_downbeat(1:lim1,:));
```

B.3 Ensemble Generation

```
clc; close all; clear all
format longG
```

```
tic;
fc=5e6;              % carrier frequency
fs=20e6;             % sampling frequency
B =fs/2;             % Bandwidth (amplitude) of triangular wave
delfc=B/2;           % maximum frequency deviation
fmin=fc-delfc;       % minimum frequency
fmax=fc+delfc;       % maximum frequency
Tm = 10e-3;          % sweep period (up sweep+down sweep)
Fm = 1/Tm;           % frequency of triangular wave
M = 1;               % How many periods are shown
R =70000;            % range of the object
V =0;                % Velocity of the target in mtr/sec
C = 3e8;             % velocity of light in free space
del=(2*R)/C;         % extra time after Ts (due to R)
fd=(2*V*fc)/C;       % Doppler shift
ts=1/fs;             % rate of change of transmit frequency
Ndtot=Tm/ts;         % total number of delays for 100% attack
Sd=10;
Ndact=round(Ndtot/Sd);

%% Creating delayed signal
t = 0:ts:M*Tm;
l_total=length(t);
F=sawtooth(2*pi*Fm*(t+0.5*Tm),0.5);
Txd=-1+zeros(1,l_total);
Txd(1,:)= F(1:l_total);
Txd2=vco(Txd(1,:),[fmin fmax],fs);
final_Txd(1,:)=Txd2;
```

```
j=1;
for i=2:Ndact
    j=j+Sd;
    inter_Txd(i,:)=Txd2([end-j+1:end 1:end-j]);
    final_Txd = final_Txd+inter_Txd;
end

%%
inter_Txd(1,:)=0;
final_Txd=2*final_Txd;
%spectrogram
figure; spectrogram(final_Txd,kaiser(256,5),[],[],fs,'yaxis');

%% File Creatiom
fid = fopen('data_file.bin', 'W');
fwrite(fid, final_Txd, 'float');
fclose(fid);
toc;
```