RADAR Spoofing

By Brendan Amorin, ECE '22

Introduction

RADAR has emerged as a tool applicable to a host of contexts, both civilian and military, including vehicle navigation, weather surveillance, and space observation. Pulse-Doppler RADAR provides its user with information about not only an object in the environment's distance away, but also its motion, specifically velocity.

RADAR spoofing is the practice of imposing false information on a victim RADAR. One example of spoofing involves multiple objects simultaneously, both moving and stationary, such that RADAR user perceives the objects at false distances and velocities. The following sections will discuss the basic principles of RADAR and how they can be manipulated to achieve the desired spoofing effect.

RADAR Basic Principles

RADAR entails transmitting a wave from a source antenna and receiving a portion of the reflected wave back into a destination antenna. Information about the object inciting the reflection can be extracted from this received wave.

Distance

The distance of an object from a source RADAR can simply be determined from the amount of time that elapsed before the transmitted wave was detected by the receive antenna. It is assumed that the wave travels at the speed of light, c. This speed multiplied by the time ellapsed during the wave's journey, t, results in the total distance the wave travelled. The distance to and from the object should be equal, so the distance, d, between the RADAR and object is equivalent to half of the total distance the wave travelled. The above explanation is summarised with the below equation.

$$d = \frac{ct}{2}$$

Equation 1: Distance between RADAR and target object

Velocity

Pulse-Doppler RADAR utilizes the Doppler effect to determine the difference in velocity between the source RADAR and an object in the environment. The Doppler effect is the phenomenon that is responsible for the effect of a car horn on a passing pedestrian. The horn will have a higher frequency and intensity as it approaches the pedestrian and a lower frequency and intensity as it moves away. The below image illustrates this effect.

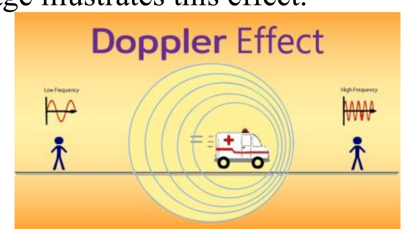

Figure 1: Doppler effect demonstrated (Davis, A. (2020) https://creativecommons.org/licenses/by-sa/4.0/deed.en)

The Doppler effect extends to Pulse-Doppler RADAR in that the frequency of the wave received at the destination antenna will be different than the frequency of the transmitted wave relative to the difference in velocity between the RADAR and the object. Additionally, the received wave will have a phase shift relative to the transmitted wave due to the Doppler effect. A phase shift simply implies that the wave is at a different moment of its cycle compared to the original wave. The below image illustrates this behavior. Note that the peak of the blue wave occurs later in time than the red wave.

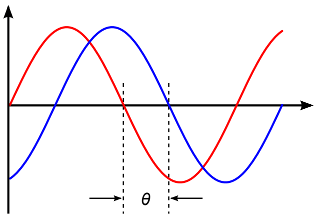

Figure 2: Phase-shifted waves (Peppergrower (2009) https://creativecommons.org/licenses/by-sa/3.0/deed.en)

Different RADAR make use of the frequency or phase to extrapolate velocity, but both characteristics of the wave can be used to achieve the desired result. The Pulse-Doppler RADAR designed by Team Mahogany utilizes phase-shift information, so the relationship between this quantity and velocity will be described here through the equation below.

$$v = \frac{\theta c}{4\pi f \Delta t}$$

Equation 2: Velocity of pulse related to its phase shift

Although the derivation of this expression is beyond the scope of this paper, its values can be explained. v represents velocity of the object, θ represents the phase shift of the wave, c again represents the velocity of light, f represents the frequency of the transmitted wave, and Δt represents the time duration between waves transmitted since Pulse-Doppler RADAR operates by emitting several waves separated by a fixed duration. In summary, Equation 2 states that if the received wave exhibits a phase shift, then it was reflected off a moving object. Furthermore, observing how the phase shift changes in between received waves would also describe how the velocity of the object changes.

RADAR Spoofing

RADAR spoofing can manipulate the above methods for extrapolating information about an object's distance and velocity by altering the results of Equations 1 and 2. Delaying the reflected wave returning to the receive antenna would suggest that an object is further away than it is and inciting an alternate phase shift in the reflected wave would suggest that the target has a different velocity. The below sections explore examples of these concepts being realized in different applications. Although the examples do not directly manipulate the equations discussed before, they demonstrate the potential for the manipulation of time delay and phase shift of a received signal to affect a system.

Manipulating Time Delay

Both [2] and [3] make use of FMCW (linear frequency modulated continuous wave) RADAR, which transmit waves that change speed as time progresses. For example, the below figure illustrates a wave that speeds up with time.

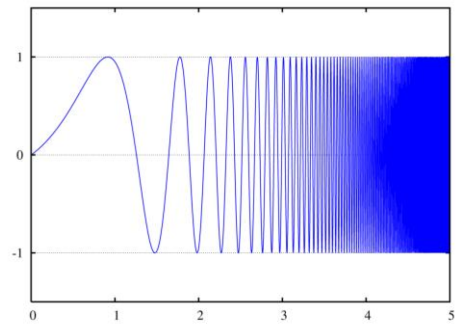

Figure 3: Linear frequency modulated continuous wave (Omegatron (2005) https://creativecommons.org/licenses/by-sa/2.0/deed.en)

FMCW RADAR determines target distance based on the frequency of the resulting signal when the transmitted and received waves are mixed, although the derivation of this expression and the mixing process are beyond the scope of this discussion. However, both [2] and [3] utilize an artificial time delay to manipulate the distance measurement of a target, since the delay will affect the result of the mixing process between the received and transmitted waves. Additionally, both attempt to achieve this goal utilizing an additional RADAR that mirrors the original one. The mirrored RADAR synchronizes with the victim RADAR such that it is aware of the true time distance between them. This synchronization is important because it enables the mirrored RADAR to know when waves from the victim RADAR will arrive. [2] and [3] have slightly different approaches to achieving this synchronization. For example, [3] computes the difference in time of arrival between intermediate received waves from the victim RADAR to approximate the time distance between the two RADAR. With this synchronization acquired, both [2] and [3] transmit a signal with artificial delay that is more powerful than that of a reflected wave, since it would lose energy as it propagates through air. This results in any reflected wave becoming dominated by the wave with artificial delay. After applying the appropriate time delay, researchers in both papers experimentally demonstrated that errors in detected distance by the victim RADAR can be achieved for a range of distances.

Manipulating Phase Shift

[1] alludes to the use of RADAR to detect different features in the cardio-respiratory cycle. Additionally, it mentions RADAR indicating the presence of humans and the possession of a concealed weapon. All this information evidently can be extracted from the Doppler effect on the transmitted wave from the RADAR and corresponding phase shift of the received wave, although this analysis is beyond the scope of this discussion. Thus, [1] proposes a method for disrupting this detection. It introduces a system into the environment that receives the transmitted signal from the RADAR and sends it into a phase shifter, which is driven by a signal generator. The resulting phase shift is applied to the wave before it is transmitted from the system back to the awaiting RADAR. The system is further illustrated with the figure below.

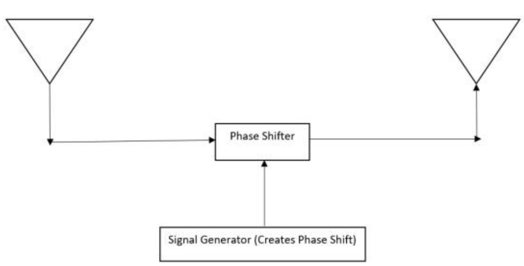

Figure 4: Phase-shift system (Amorin, B. (2022))

After applying the appropriate phase shift to account for the respiratory and cardiac movements of a person, the researchers in [1] experimentally recovered a typical signal indicative of a human presence, suggesting that this technique could be used for different spoofing applications. Operating the signal generator at the frequencies corresponding to those of the respiratory and cardiac movements also resulted in these respective components of the human signal operating at the correct frequencies.

[3] also discusses the ability of a mirrored RADAR to manipulate the velocity measurement of a victim RADAR by manipulating phase shift, while [2] alludes to a similar method without thorough analysis. FMCW RADAR can be used to measure the velocity of an object using Equation 2. However, the equation now utilizes the difference in phase between two consecutive pulses, resulting in the updated equation below, where $\Delta\varphi_{i+1,i}$ corresponds to the difference in phase between two consecutive received waves.

$$v = \frac{c\Delta\varphi_{i+1,i}}{4\pi f \Delta t}$$

Equation 3: Velocity from FMCW RADAR

To achieve velocity manipulation with respect to Equation 3, [3] assigns a modified phase shift that includes the phase shift from the true difference in velocity between the mirrored RADAR and victim RADAR. Since the measurement of distance and velocity are independent of each other, a new phase shift is assigned to each transmitted pulse from the mirrored RADAR such that the victim RADAR is processing incorrect distance and velocity information. The results of [3] did not only display effective distance manipulation, but also velocity manipulation.

Conclusion

RADAR can be used to determine both the distance and velocity of objects in the environment. However, RADAR is also vulnerable to spoofing devices, which can result in incorrect data that could be costly depending on the situation. This paper discusses the basics of how RADAR achieve distance and velocity measurements and provides examples of spoofing devices developed to successfully sabotage the measurements of RADAR. While these spoofing methods provide potential defense advantages, they also leave systems critically dependent on RADAR at risk. Understanding these methods is an important part of recognizing methods for defending against spoofing as well.

References

1. D. Rodriguez, J. Wang and C. Li, "Spoofing Attacks to Radar Motion Sensors with Portable RF Devices," 2021 IEEE Radio and Wireless Symposium (RWS), 2021, pp. 73-75, doi: 10.1109/RWS50353.2021.9360393.

2. Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, Makoto Nagata, Shoei Nashimoto, and Daisuke Suzuki. 2019. A Low-Cost Replica-Based Distance-Spoofing Attack on mmWave FMCW Radar. In <i>Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop</i> (<i>ASHES'19</i>). Association for Computing Machinery, New York, NY, USA, 95–100. DOI:https://doi.org/10.1145/3338508.3359567

3. Rony Komissarov and Avishai Wool. 2021. Spoofing Attacks Against Vehicular FMCW Radar. In <i>Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security</i> (<i>ASHES '21</i>). Association for Computing Machinery, New York, NY, USA, 91–97. DOI:https://doi.org/10.1145/3474376.3487283