RADAR Spoofing

John Davis, Brendan Amorin, Benjamin Pradko
Sam Cohen, Youssef Soliman

Tufts University
Lincoln Laboratory, Massachusetts Institute of Technology

Background Information

RADAR works by bouncing radio waves off objects. By analyzing the reflected signal, the object's position, size, and velocity can be obtained.

An object's position is determined by finding the amount of time it takes a light pulse to reflect and come back. This round trip time can be easily converted to distance since the speed of light is a known constant.

An object's size will determine how much signal gets reflected back. The amplitude of the received signal can be used as a rough gauge of a target's physical size.

An object's velocity is determined by comparing the reflected signal's frequencies to the original signal. Objects moving towards the radar reflect back a higher frequency, while objects moving away reflect a lower frequency. This is manifested as a phase shift observed on a pulse-by-pulse basis.

RADAR signals can be spoofed by creating fake reflections. Using the properties above, fake objects can be created with arbitrary position, speed, and size to confuse RADAR systems.

Motivation & Scope

To better understand the basic principles of RADAR and RADAR spoofing, our team has partnered with MIT Lincoln Laboratory to create a simple RADAR spoofing system called a DRFM. Our contact at the Lab, Dan Rabinkin, has provided us with the necessary hardware and resources about electronic warfare to pursue our desired goal.

Project Goals

- Develop simulations for both RADAR and DRFM in MATLAB to verify algorithms and methods in a simulated environment.
- Design a RADAR system that can detect multiple stationary and moving objects at different ranges.
- Design a DRFM system that can spoof the RADAR by manipulating received RADAR pulses to suggest false object range and velocity.
- Implement both systems in hardware for field testing and verification.

System Design

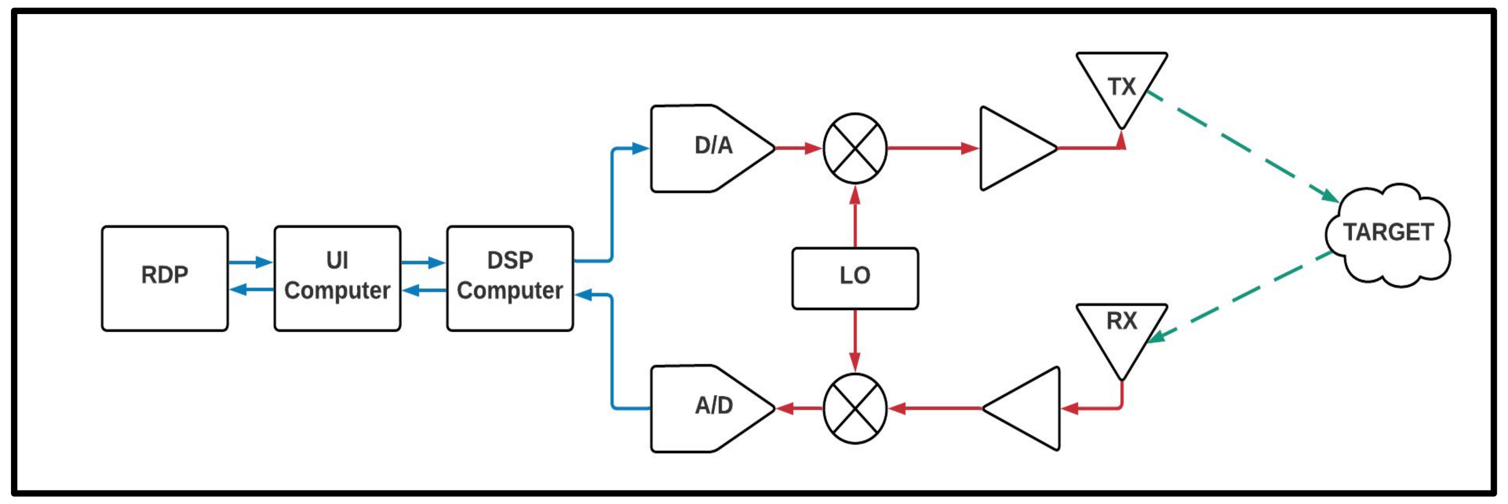
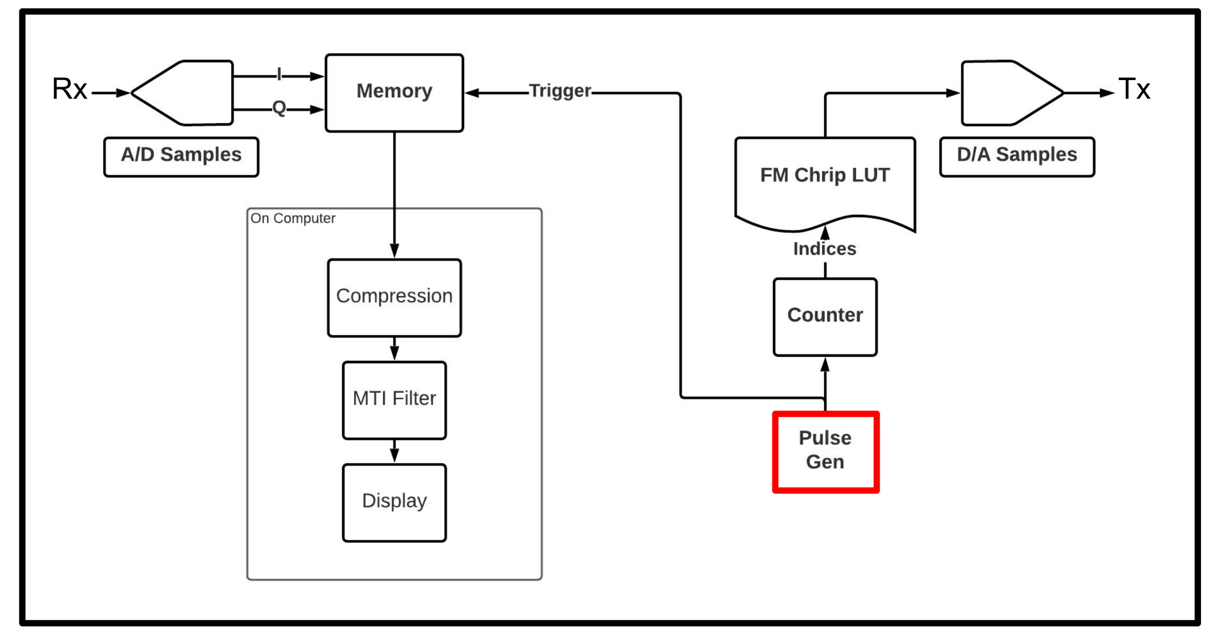


Figure 1 (Left): Here we have a visualization of our entire system. The blue lines represent connections in the computer while the red connections are within our software defined radios (SDR).

Figure 2 (Right): This is a flow chart of our RADAR software. Our data runs through two paths, the first begins with pulse generation (in red), and is manipulated via frequency modulation up to a 5.8GHz chirp, which is converted to an analog signal for transmission. The next data path begins at the Rx side, where our reflections are captured and written to memory on the SDR before they are transmitted back to the computer for processing and generation of our range-doppler plot for presentation of the user.



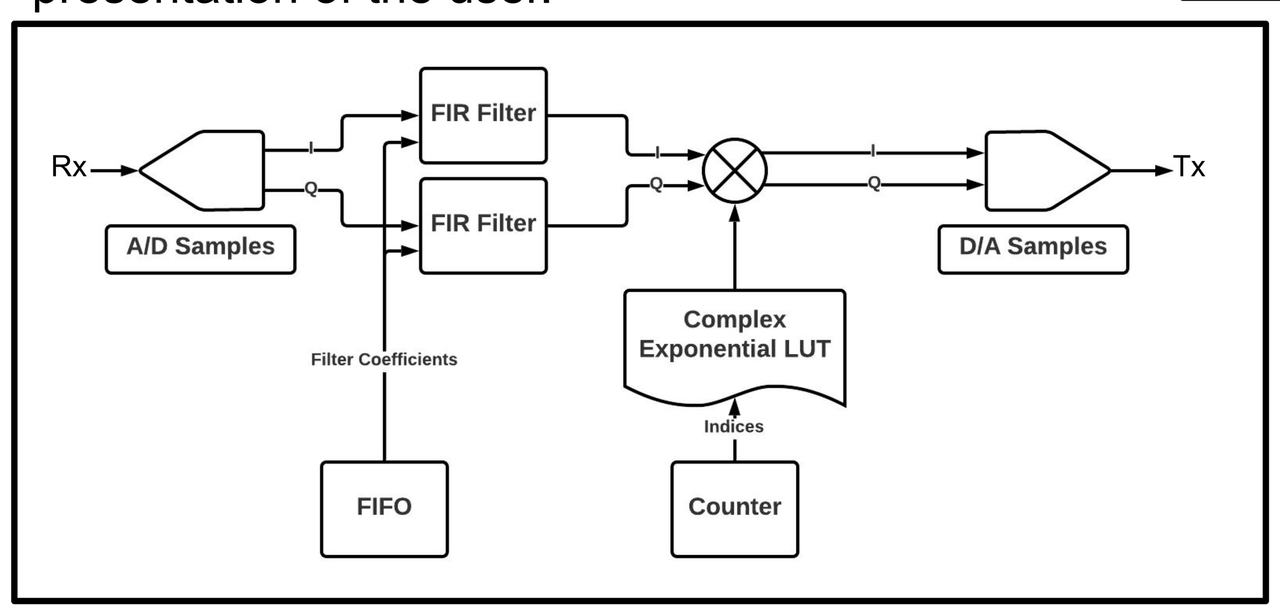


Figure 3 (Left): This is a flow chart of our spoofing hardware. The incoming RADAR pulses are delayed and replicated by being passed through an FIR filter. These filters model the spoofed environment. The pulses are then multiplied by a complex exponential term, which introduces a desired phase shift. Then, the signal is transmitted back to the target RADAR.

Data

Figure 4 (Left): Ben and Brendan running in opposite directions

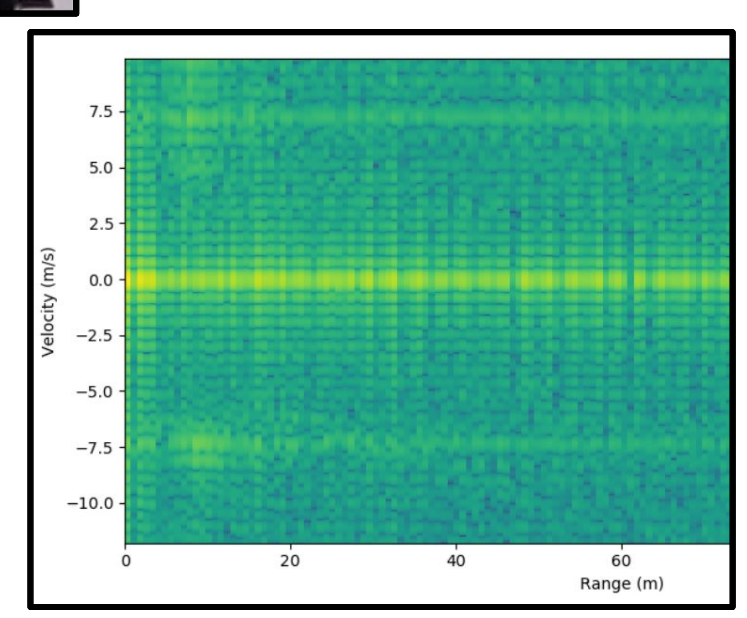


Figure 5 (Right): Corresponding RADAR signature of Ben and Brendan running in opposite directions

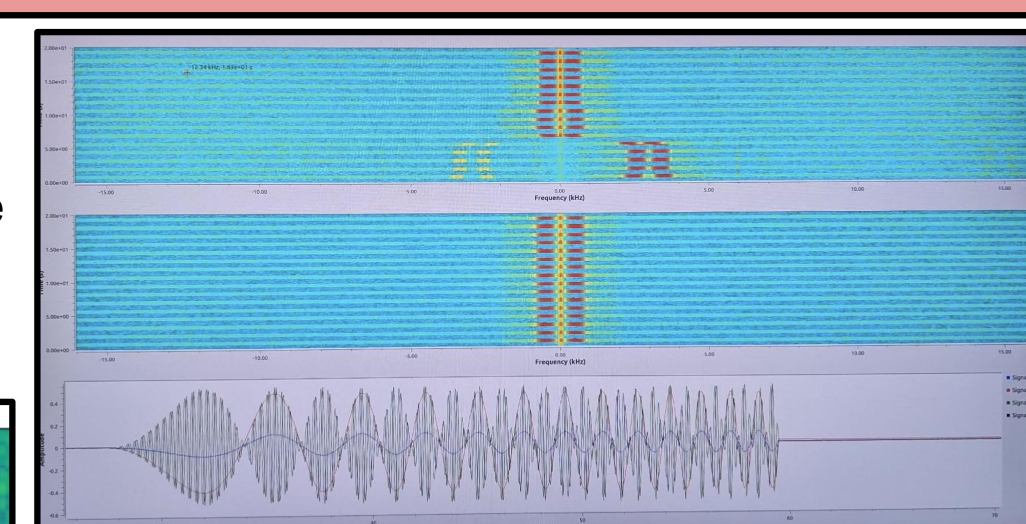


Figure 6 (Above): Frequency and phase shift imposed on signal by the DRFM running on an SDR

Project Challenges

- Detecting reflections on the order of meters requires high sampling rates and data throughput which were beyond the limits of our system.
- Supply chain issues impacting prices and shipping times for components.
- Being able to unit test our hardware and system setup due to 5.8GHz frequency.
- Proper version control and software compatibility.
- Computer hardware and ethernet throughput.
- Navigating conflicts with other commitments and this course's assignments.

Conclusion

RADAR principles were verified in both in simulation and physical implementation. This is demonstrated by the successful detection of moving objects by the designed system. Spoofing techniques were explored by generating arbitrary delays and frequency/phase shifts in arbitrary input signal, which was immediately received by a SDR. While these delays and shifts were not observed in the field due to system limitations, we believe that with more advanced hardware, the desired behavior could be observed.

Thus, although we did not successfully integrate all of the components of the desired system together, the system constructed and the algorithms utilized are a sufficient basis for future work to complete the project fully and to a higher standard.

Future Directions

- Implement DRFM GUI so an unskilled operator could use the functionality.
- Increase the output power of the device to be able to operate at longer ranges.
- Make the device portable so it could be used on a land vehicle/drone.

Acknowledgements

Dan Rabinkin, Ron Lasser, Emily Carlson, Dante DeMeo, Zach Kranefeld, Ian Fletcher, Celia Lewis, Josh Pfosi, Zachary Mcgowan