Detecting RADAR Spoofing and Jamming

By Benjamin M. Pradko, ECE '22

Introduction

In recent years, RADAR technology has become more and more common, leading to both interactions between RADAR devices and all types of electronic warfare requiring increasingly robust systems to ensure functionality. RADARs are used heavily in military applications from fighter jets to naval vessels, which could be subject to intentional electronic warfare. On the civilian side, airport RADAR systems and even those in modern automobiles are exposed to other RADAR signals and such that result in a sort of unintentional electronic warfare, though there is the potential that someone wishes to have civilian systems fail. Thus, in all RADAR applications, the need to be able to combat electronic warfare, or similar phenomenon, is paramount to ensure that the system can accurately understand its environment. Failure in these systems could lead to dire consequences as systems such as brake assist and blind spot detection rely upon accurate RADAR data to either act autonomously or inform the operator.

Electronic warfare, as it pertains to RADAR systems, is broken down into two categories: jamming and spoofing. Jamming seeks to render the system inoperable by flooding the RADAR sensors with nonsense. Spoofing has a different goal, which is to deceive the RADAR by sending the RADAR data as if additional targets existed, in essence making the RADAR hallucinate. While jamming seems like a brute force technique and spoofing a more finesse technique, both are designed so that it is difficult to detect that the RADAR is under attack. It is important to note that jamming and spoofing can be difficult to detect even in civilian applications despite there being no attacker.

RADAR Jamming

Detection

Much like a bat uses sonar to detect its surroundings, a RADAR works instead by sending out radio pulses and catching the reflections as they bounce off objects. The RADAR is therefore always listening to capture all reflections as it pieces together a picture of the surroundings. RADAR jamming can then be performed by filling the air with garbage radio signals so that the RADAR cannot pick up its reflections. In the case of detecting RADAR jamming, techniques are used to find abrupt changes in the signal as markers of jamming with the intention being that further anti-jamming techniques can be implemented once detection has occurred. This is because an attacker will have to initiate jamming at some point, and it is the switch between no jamming and jamming that can be detected.

One such method is that of Approximate Entropy (ApEn), which is a method of quantifying the complexity of a signal. This technique was originally developed for medical purposes in the 1990s and has since been applied to several other fields due to its versatility in detecting signals with different attributes. There are RADAR systems that use signals with two unique attributes, which can be picked up by ApEn. The ApEn technique is a complex statistical calculation that looks at the most recent recording of the incoming signal and evaluates how likely a new pattern is to emerge from the signal. In an effort to more clearly determine transition points, the original ApEn method was modified to create the Moving Cut data ApEn (MC-ApEn). This method provides a sharp change in complexity when different types of jamming are introduced to the signal, in contrast to the gradual change seen in ApEn.

While things become complicated in extremely electromagnetically active environments, where random radio signals are emitted as a product of the environment, the MC-ApEn technique can be used on a set of sequential overlapping signal snippets with success. As you would likely expect, the introduction of jamming signals will drastically increase the complexity of the signal and as a result can be used as a reliable marker for determining whether the system is being targeted by any number of different jamming attacks. Based upon the principle that an attackers jamming will introduce some distinct change in the attributes of the incoming signal, other attributes such as signal power can be looked at as a marker for detection besides complexity.

Avoidance

Unfortunately, avoiding jamming is difficult to do as jamming is not targeted, but affects everything in the range of the jammer. As such, avoidance would typically require the destruction of the source of the jamming or simply leaving the area affected by the jamming device.

Spoofing

Detection

Unlike jamming, spoofing is something that can be encountered in more readily outside of military applications, though still with potentially fatal implications. As alluded to earlier, detecting spoofing leads to RADAR sensing on cars to detect distances between vehicles for safety features such as braking assist and other autonomous safety measures. This is an issue as most sensors do not account for possible security issues both intentional and not, which could include spoofing. An example scenario is two traveling cars where the lead car is spoofing its location to be further ahead than it really is. The gravity of this situation is obvious as the rear car is unable to detect that the lead car is at a dangerous distance, and so different techniques can be compared for efficiency of assessing the *threat level* of whether spoofing is occurring and then attempting to determine which of the incoming signals is the proper signal. One solution proposes spatio-temporal challenge-response (STCR) to both detect and mitigate spoofing attacks through a signal verification process. This technique revolves around using multiple beam-forming signals sent out in a random subset of predetermined directions allowing the system to identify with high accuracy the location of a potential attack as well detecting high noise reflections coming from unprobed angles. This is like using laser pointers to find a mirror in a room rather than using a light bulb, because the laser pointers are able to find where in the room the mirror is while the light bulb can only reveal that there is a mirror reflecting light somewhere in the room. This technique therefore allows for the ability to detect spoofing attacks and through this detection, the system can maintain accurate functionality despite being under attack. The robustness of this technique is such that, in practice, even when under attack, the system can return the location of the lead car with an error margin of almost zero meters. Detecting RADAR spoofing is difficult because you cannot trust any of the signals that come back and must check that they are legitimate. Consider the situation where you hear a voice but are not entirely sure where it is coming from until you are able to scan and see or otherwise confirm that someone’s mouth is moving or through positioning your head in different positions to try and track the voice.

Avoidance

Avoiding spoofing can also be done in other creative ways. While the previously discussed system sends out beams in random directions to detect spoofing and mitigate its affects, another group took a frequency hopping technique used in Bluetooth and applied it to RADAR systems. Essentially, RADAR signals are sent at a certain frequency just you're your WiFi operates at a range of frequencies centered at 2.4GHz or 5GHz. Similar to how you can have multiple WiFi networks at the same frequency this system is considering the situation of multiple RADARs interfering with each other, as a result of sharing frequencies, as well as spoofing. This technique, BlueFMCW (Frequency Modulated Continuous-Wave) takes the hopping technique from Bluetooth, which constantly hops between 79 different frequencies at a rate of 1600 hops per second and applies it to a RADAR system. Random hopping patterns then allow for multiple RADARs to share the same frequency ranges without collision, this works to prevent spoofing and other interference which would arise from multiple RADARs in the same general area. This method is also combined with a very specific signal, that maximizes the effectiveness of frequency hopping. Frequency hopping causes a blurriness or imprecision in the RADAR that this specific type of signal mitigates. As discussed, this system addresses spoofing concerns by spreading out the signals across multiple frequencies, while the hopping will hopefully confuse an attacker's spoofing devices.

Conclusion

Spoofing and jamming are both incredibly complex techniques and countering them requires equally complex systems to identify and mitigate them. While RADAR systems can provide invaluable data that can be used in all sorts of machines from planes and automobiles to watercraft to either inform operators or control autonomous functions, their vulnerabilities to jamming and spoofing can render them useless or destructive before someone can understand what is going on and correct. As a result, techniques and the investment in additional sensors and computing power necessary to safeguard both civilian and military RADARs against jamming and spoofing attacks is crucial for the continued development of RADARs as reliance on them becomes commonplace.

As it pertains to this project, applying counter measures to our RADAR system is beyond the scope of the project as we built a RADAR so that we could test our spoofing device. If we were able to apply counter measures to our RADAR it would push us to create a more robust spoofing device than our setup could handle. As it is, our group has encountered difficulties having our current system execute our simple RADAR system. To enhance our RADAR we would need to significantly improve our physical hardware and increase our computing power, and the implications would likely be similar for the spoofing device. An exploration of implementing RADAR countermeasures and upgrading the spoofing device to still compromise the RADAR would in essence be a project on its own, exploring which algorithms can bypass certain countermeasures.

This research revealed some different spoofing and jamming techniques, but it also affirmed that countering these attacks is difficult and likely would require much better hardware and a more complete system then our group could implement on our system due to the algorithms and the occasional need for multiple sensors and precise beam forming.

References

1. Kapoor, Vora, A., & Kang, K. (2018). Detecting and Mitigating Spoofing Attack Against an Automotive Radar. *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 1-6*. doi:10.1109/VTCFall.2018.8690734

2. Markin. (2009). Jamming detection in providing for radar jamming immunity. *IEEE EUROCON 2009*, 1565–1567. https://doi.org/10.1109/EURCON.2009.5167849

3. Moon, Park, J., & Kim, S. (2022). BlueFMCW: random frequency hopping radar for mitigation of interference and spoofing. *EURASIP Journal on Advances in Signal Processing*, *2022*(1), 1–17. https://doi.org/10.1186/s13634-022-00838-7

4. Yan Xingwei, Lu Dawei, Zhang Jun, & Wan Jianwei. (2012). Radar jamming detection based on approximate entropy and moving-cut approximate entropy. *IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012),* 2.46–. https://doi.org/10.1049/cp.2012.2359