Radio Hackers: Jamming & Spoofing Fundamentals

Investigator515

.

Follow

Published in

Radio Hackers

7 min read

.

Jul 9, 2024

Listen

Share

More

Understanding Spoofing and Jamming is an essential part of your offensive toolkit.

If you aren't a medium member, you can read with no paywall via **substack**

We strive to provide informative articles, however, it is important for users to ensure their research is both ethical and responsible. Additionally, it is your responsibility to ensure you're compliant with all applicable laws and regulations for your region. The information provided in this article is intended for educational purposes only.

During our Radio Hackers journey, we've started to lay down

fundamental techniques to assist in developing a framework that will help leverage some of your new skills and information. We've looked at the importance of antennas as well as exploring some of the different types of signals that you might see while experimenting with the radio spectrum. However, in Signals Intelligence, we're going to find ourselves dealing with large amounts of data, and in the world of intelligence, we don't automatically trust everything we discover without attempting to validate it first.
So, during the process of conducting Signals Intelligence (SIGINT), this means that determining the authenticity of a signal is an important part of the assessment process. Today, we'll be exploring some of the fundamentals behind signal spoofing and jamming and looking at why we need to know how to identify malicious signals. There's also a real-life example of a spoofed signal at work.

What Is Spoofing And Jamming?

Despite both being forms of electronic attack there's a distinct difference in the way we observe them in the wild. But, like many other radio hacking scenarios, we can often see links to traditional cyber attacks when we start examining them a little more closely. Spoofing, for instance, could be considered to be similar to an evil twin attack, where a rouge signal is impersonating a legitimate one for malicious purposes. Whereas a jamming attack is similar to a Denial of Service as the jammer's signal will deny usage of parts of the radio spectrum to anyone who is in range indiscriminately. While electronic warfare (EW) has been prevalent for military purposes since the days of World War

two, the prevalence of Wi-Fi, the Internet and consumer devices means that the overlap between EW and the civilian world now is much more noticeable than it once was.
It's also worth mentioning that these attacks can often be personalized or discriminate, where they are targeting a specific person or device of interest. We'll mostly see that at a nation-state level. Or, they could be indiscriminate, affecting everyone within the transmitting jammers range. The AN/ALQ-99 jamming pod on an electronic warfare aircraft is a good example of something that can work indiscriminately, providing general area effects.

How Does It Work

Typically, a jamming attack is applied over a large chunk of the radio spectrum at high power, providing the indiscriminate area-based effects we discussed earlier. However, these attacks can also be targeted at specific frequencies. This allows the jamming transmitter to focus its power on a particular part of the spectrum leading to a much stronger jamming effect due to higher output power from the jammer targeting that wavelength.
At its most basic level though, a jamming attack is effectively

using one transmitter to overpower the other, while a spoofing attack relies on the transmission of malicious signals to achieve its end goal. And while we have used military examples to assist in explaining how things might work, it’s important to realise that we can also see similar attacks in the real world.
It’s pretty unlikely you’ll have to deal with the consequences of an EA-18 Growler overhead anytime soon but it’s entirely plausible that you’ll see civilian examples of SIGINT and EW, particularly if you're working in sensitive or government-focused installations.

> The AN/ALQ-99 is capable of jamming frequencies from 64 MHz to 20 GHz. Jamming frequency ranges are set forth in 10 bands:
>
> - **Band 1:** 64 - 150 MHz
> - **Band 2**: 150 - 270 MHz
> - **Band 3:** 270 - 500 MHz
> - **Band 4:** 0.5 - 1 GHz
> - **Band 5/6:** 1 - 1.25 GHz
> - **Band 7:** 2.5 - 4 GHz
> - **Band 8:** 4 - 7.8 GHz
> - **Band 9:** 7.8 - 11 GHz
> - **Band 10:** 11 - 20 GHz [6]

Military Spec jammers are wide-band with high output power. In the civilian world, jammers are often single-use and lower-powered. Source: Wikipedia.

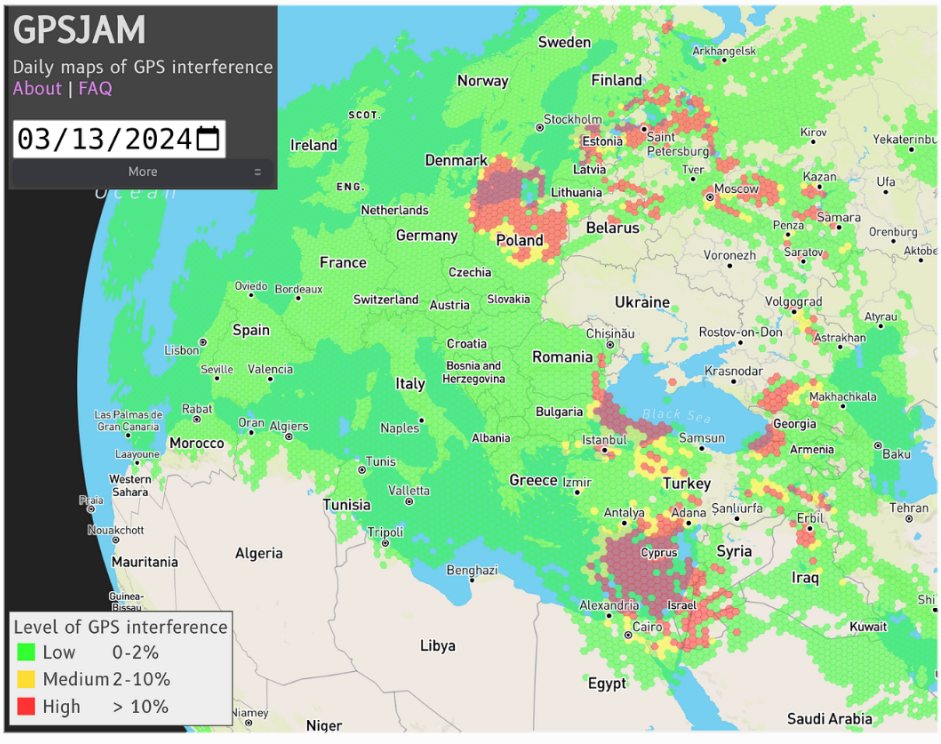
Does This Even Happen?

If you aren’t studying cyber or infosec you might be reading this and thinking it’s not relevant to the civilian world and there's no way things like this can happen in our modern world. And while that might be true if you’re living in the

southern hemisphere, the northern hemisphere people are regularly exposed to this type of thing and the reality is that often, it barely even makes a headline. So, to take a look at some real-world examples of this occurring we're going to look at some infrastructure that's regularly used by many people the world over. The GPS Satellite constellation on 1575.42 and 1227.60mhz.
If you're not great with converting frequency to wavelengths, this is a weak signal right in the middle of the 1ghz band.

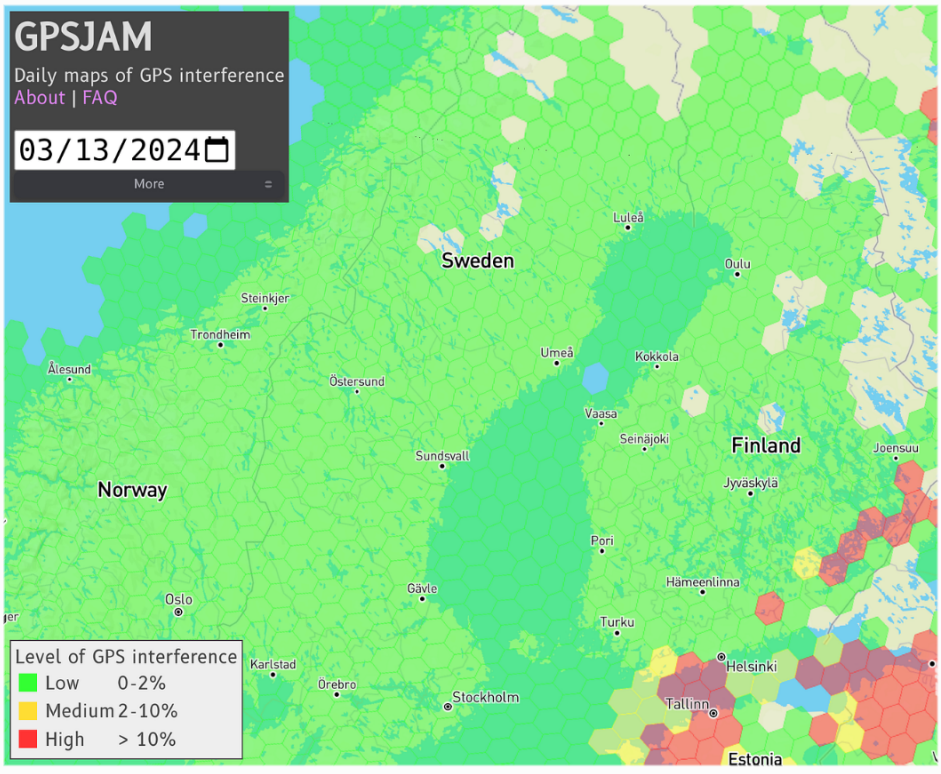
GPS Signals are regularly jammed and spoofed in certain parts of the world. Source: Wikipedia.
It's fair to say that most people understand that there is an active war in Europe that's been going on for many years. And while the frontlines may be a long way away for some readers, the reality is that Electronic Warfare strategies know no borders and some of this active EW has spilled out to

cover parts of Europe outside of the conflict zone.
More importantly, we've seen both types of attacks while this has been occurring as both Spoofing and Jamming attacks have been reported on multiple occasions since the conflict escalated. To explore this in a bit more detail, we're going to use a simple but extremely useful website that attempts to track ongoing and active attacks on civilian GPS.



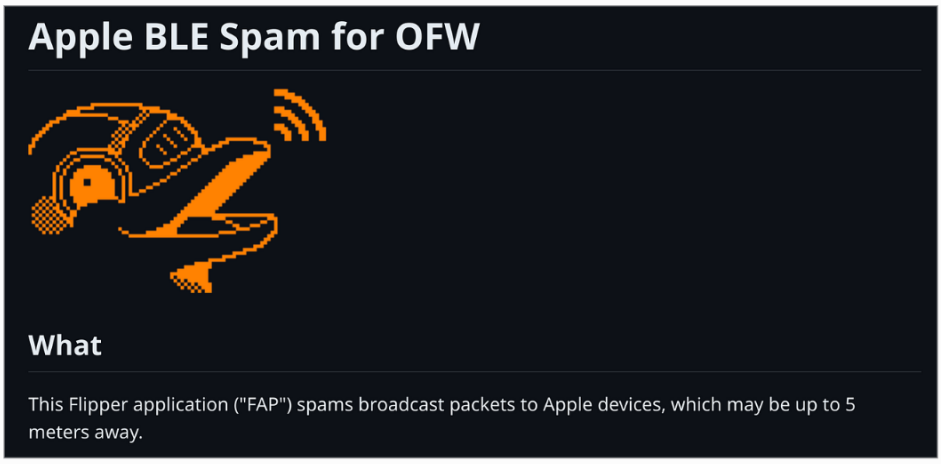
GPSJam lets us see jamming attacks in real time. Source: gpsjam.org
GPSJam logs interference to the GPS system in a hot spot fashion, using colour variations to determine the active level of interference. Looking at the attached image we can see that nearly every spot that has an active conflict shows some form of interference with GPS. We can also see that there are high levels of interference around certain parts of the Russian Federation, namely Moscow, or more specifically the Kremlin.
We should also note that many countries that are reporting interference are not active participants in said conflict

however the consequences of jamming the satellites still have an effect regardless of this.



Finland has suffered the effects of EW attacks on GPS pretty consistently of late. Source: GPSjam.org

And while you might not ever hold a pilot's license or use the GPS constellation for much more than personal navigation, it’s still plausible to see some other small-scale attacks in the real world regardless. The flipper zero made headlines recently for its ability to repeatedly spam BTLE signals (spoofing), while a simple de-auth packet transmitted repeatedly over Wi-Fi could interfere with legitimate devices on a network (jamming).



The Flipper Zero gained notoriety for its ability to transmit BTLE spam. Source: Github.com

In Closing.

If you'd like some more resources on the topic of spoofing and jamming attacks in the real world to help increase your knowledge level, and background then here are a few links to get you started.

Read about GPS and Civilian Aviation
Read about the Royal Navy & Spoofing GPS
Read more about EW in the Ukraine Conflict
Explore the Radio Spectrum in Europe via WebSDR

While this is the first piece we've written that covers spoofing and jamming theory, we'll be exploring this a lot more in future Radio Hackers articles. We'll also be reviewing more simulated data in a controlled, lab environment using low-powered software-defined radio systems, to help further your understanding of how to detect and defend against these types of attacks.

If you haven't got a transmit-capable SDR to go with your Radio Hackers tutorials, then now might just be the time to splash out and buy one.

Medium has recently made some algorithm changes to improve the discoverability of articles like this one. These changes are designed to ensure that high-quality content reaches a wider audience, and your engagement plays a crucial role in making that happen.

If you found this article insightful, informative, or entertaining, we kindly encourage you to show your support. Clapping for this article not only lets the author know that

their work is appreciated but also helps boost its visibility to others who might benefit from it.

🌟 Enjoyed this article? Join the community! 🌟

📢 Join our OSINT **Telegram** channel for exclusive updates or

🐦 Follow us on **Twitter**

🔗 Articles we think you'll like:

- Software Defined Radio & **Radio Hacking Pt 1**
- OSINT Investigators Guide to **Self Care & Resilience**

✉️ Want more content like this? **Sign up for email updates**

Hacking

Radio

Software Defined Radio

Learning