Report In Request For FCC Experimental License For Operating In GPS L1 Frequency Band

Enhanced coverage, navigation accuracy and low equipment cost have resulted in the global positioning systems (GPS) to be used widely in everyday life. However, GPS is vulnerable to radio-frequency (RF) interference – both, intentional and unintentional. While increasing signal strength, and/or improving antennas may improve the signal strength, it will not eliminate potential outages due to RF interference. The vulnerability of GPS systems to RF interference was clear from the incident in 2009 when positioning receivers for a new navigation system at Newark airport suffered from daily outages. The investigation of the problem by the FCC revealed that, which essentially took about two months to track down, a truck passing by the New-Jersey turnpike had an active GPS jammer emitting jamming signals. Such jamming devices are illegal to posses, distribute and sell in the US (as directed by FCC), yet it is not difficult to buy a low-cost jamming device from the plethora of online portals available today (which is still illegal).

The Newark airport turnpike truck incident opens up an important question as to if these devices are used in some trucks - typically drivers would use them to mask employee tracking such as in trucks, rental cars or even stolen vehicles. GPS jammers are designed to overwhelm GPS receivers by broadcasting a high-power wideband (about 10-20MHz) noise signal centered on GPS L1 frequency (1.57542 GHz). At these power levels these jammers could potentially jam GPS receivers even at a radius of 10s of meters. This would lead to significant problems, especially on major highways, thus need to be pro-actively detected and appropriate actions need to be taken.

Our goal is to design a system that can automatically localize the GPS jammer and identify the car that carries it. Such an ability is essential to penalize the illegal GPS jammer usage, which eventually will hinter the illegal usage and protect civilian GPS receivers from destructive denial-of-service (DoS) attacks. However, it is impossible to design a candidate methodology without understanding and studying the available GPS jammers in the market.

We want to understand the signal characteristics of commercial jammers to be able to identify them in road-side measurements. To understand the characteristics of the jammer(s), we will need to run calibration experiments using the jamming device itself, and in typical use-case scenarios; such as near the highways or near local roads. We understand that the possession of such a jamming device and its usage is not permitted by FCC, but without which we would not be able to potentially detect an active commercial jammer. Hence, we request the FCC to grant us permission, first, to acquire such a device for experimentation purposes only, and secondly, allot the appropriate experimentation license.

Proposed Experimentation Methodology: Given a jamming device and the license to operate the same, we plan to perform active jammer characterization and calibration tests using a jammer fitted to the car cigarette lighter and observe the received signal power spectrum. We propose to detect the presence of a GPS jammer using the measured GPS signal strength on our custom receiver. For this purpose, we will use a Universal Software Radio Peripheral (USRP) N210 [1] as a receiver and a GPS Multiband Antenna [2] at 1575 MHz for GPS reception. Over a period of a few weeks we expect a few tests with a handful of jammer activations each. A jammer activation is typically shorter than a minute. We plan to conduct the calibration experiments in the parking lot of Winlab at the address of 671 Route 1 South, North Brunswick, NJ (coordinates: 40.468233,-74.445119). After having the calibration results, we plan to conduct another experiment in the Rutgers Botanic Garden at the address 112 Ryders Ln, New Brunswick, NJ(coordinates: 40.474032,-74.422541). This time, we will observe the effects of the jammer inside the car when the car is moving with different speeds where the jammer activation is shorter than a minute. With this experiment, we can test our calibration results and actually see whether we can identify the jammers in road-sides.

As the next step towards detecting active jammers on highways, we will **passively** monitor a wideband of frequencies centered on the GPS L1 frequency using the USRP receiver and antenna fitted in a car. We will log the received signal

strength with the time-stamp and the frequency of the signal when it exceed a pre-set threshold. We deem it as a suspicious activity when the received signal power over the entire wideband of reception exceeds the pre-set threshold. Even such a simple thresholding based mechanism would require us to know the fundamental characteristics of the jammer (what band is it operating in, what is its power level in that band, what is the spectrum shape, etc.) which cannot be obtained without real-world calibration experiments with the jammer. This remains as the prime motivation for us to acquire and experiment with a jamming device, for which we request the FCC to grant the appropriate permissions based on the project details explained in this report.

References

[1] "Usrp un210-kit," https://www.ettus.com/product/details/UN210-KIT. [Online]. Available: https://www.ettus.com/product/details/UN210-KIT

[2] "Gps multiband antenna at 1575mhz," http://bit.ly/XJTrRR. [Online]. Available: http://bit.ly/XJTrRR