Identifying Car Key Fobs as a Cause of Interference at GNSS Frequencies

Sandeep Jada, John Bowman, Mark Psiaki, *Virginia Tech,*
Steven Langel*, *The MITRE Corporation,*
Mathieu Joerger, *Virginia Tech*

ABSTRACT

This paper describes our methodology to investigate an unknown type of interference at the GPS L1 frequency. This interference does not cause GPS receivers to lose lock on signals and does not cause significant variations in the carrier-to-noise ratio (C/N0). However, it causes frequent false alerts in GNSS interference monitors, including in our own power-based jamming monitors that we had deployed in Virginia, North Carolina, and Colorado. We obtained data from three other independent groups in the US and Europe experiencing similar unexplained interference showing characteristic on-off keying or binary frequency-shift keying (BFSK). This paper describes how we identified their source as spurious emissions from car key fobs. Other remote-control and wireless devices used in automotive applications generate similar interference despite their specified broadcast frequency being nowhere near L1.

I. INTRODUCTION

GPS L1, L5 and Galileo E1, E5a and E5b signals are broadcast in protected ultra-high frequency (UHF) bands dedicated to Aeronautical Radio Navigation Services (ARNS) for safety-critical applications. However, illegal broadcasts at the L1 frequency are frequent, including from personal privacy devices (PPD) [1]. Several research efforts have therefore been focused on monitoring the GNSS radio frequency (RF) spectrum [2, 3, 4, 5, 6, 7, 8]. In particular, GNSS signal power monitors effectively detect PPDs.

In [3], we designed and tested a power-based jamming detector to capture and characterize PPD jamming using time-frequency analysis. However, the collected data included frequent, short, intermittent bursts of RF power from unknown sources near the GPS L1 frequency. We used a GNSS software-defined receiver and a commercial off-the-shelf receiver to show that these short bursts did not prevent continuous tracking of GPS signals. Therefore, these bursts did not cause GPS jamming, but they triggered jamming false alerts. Spectrograms of receiver front-end wide-band data collected using universal software radio peripherals (USRPs) showed on-off keying and BFSK signals. We saw similar signals in almost all of our datasets, in multiple US states, at different times of day, all year. At times, the signal was simultaneously caught on multiple nearby USRPs; at other times, it was not. Similar signals were recently reported in [4]. Other European colleagues found them on commercial ships as they approached coastal and port areas [9, 10]. Another source of interference at GPS L1 is from garage door openers [11].

In response, in this paper, we describe the steps we followed to identify the source of the unknown signals interfering at the GPS L1 frequency and causing false-alerts in power-based jamming monitors.

In Section II of this paper, we present the additional tests performed to ensure that the interfering signals are not aliases of signals at other frequencies that the USRPs are inadvertently bringing into the observed GPS band. We collected hours of data in May and August 2022 on a parking lot in Blacksburg, VA (of course, not knowing at the time that the interference source could be a car key fob). We used two USRPs, first with different sampling frequencies and later with different center frequency settings. If the unknown signal were aliased in the GNSS band, then it should not have appeared at the same frequency on the power spectral density (PSD) curves for both USRPs. The interfering signal was observed at the same frequency in all USRPs in these experiments, which confirms that the signal did not get aliased into the GNSS band due to faulty USRP hardware or setup. The USRP equipment might still be at fault if it somehow leaked power and could not yet be eliminated as the source of the observed interference.

Thus, Section III aims at characterizing the interfering signal. When observed on a spectrogram, the first milliseconds of the signal's power burst shows something that appears to be a communication message preamble followed by something that seems

* The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

to be data bits. We can distinguish two types of encoded data transmissions: 1) amplitude shift keying (ASK), which encodes data bits using the amplitude of a carrier sine wave at a single frequency, and 2) frequency shift-keying (FSK), which encodes data bits by switching the sine wave frequency between two distinct frequencies. The most frequently observed FSK message consists of four distinct 9-millisecond-long power bursts separated by 120 milliseconds. Focusing on the spectrogram of a single burst shows 160 chips representing 80 bits using "Manchester" encoding. This 80-bit message structure matches that of key fobs.

In Section IV, we analyze different key fobs' spurious emissions at the GPS L1 frequency. Key fobs are designed to broadcast at the 315 MHz frequency. This is approximately a fifth of the GPS L1 frequency. We use a spectrum analyzer to show that some 315 MHz key fobs generate peaks in PSD curves at 315 MHz, and at integer multiples of 315 MHz, including at 1260 MHz and near L1 at 1575 MHz. Some key fobs do not filter out their signal's fourth and fifth harmonics. The signal power magnitude varies from one key fob to the next.

Finally, in Section V, we present our conclusions.

II. BACKGROUND: GNSS JAMMING DETECTOR DESIGN AND INITIAL INTERFERENCE OBSERVATIONS

The background of this research is the design of a GPS L1 jamming detection test and its implementation to find unknown interference. In [3], we derived a new power-based jamming detection test statistic: it is briefly described below because it will help characterize interfering signals throughout the paper.

1. Power-Based Jamming Detector Design

An RF receiver's front-end signal is a sequence of pairs of real (in-phase) and imaginary (quadrature) parts of complex-valued samples. At front-end sample time step 'n', we define the RF-front-end signal as:

$$y_n \triangleq y_{I,n} + iy_{Q,n} \in \mathbb{C} \tag{1}$$

where $y_{I,n}$ and $y_{Q,n}$ are the in-phase and quadrature components, respectively. We compute the RF-front-end signal power from non-overlapping windows of 'N' samples, $\{y_n, \ldots, y_{n+N-1}\}$. Power measurements, which are available for every 'N' front-end samples, for example at power-computation time step 'm', are then defined as:

$$S_m \triangleq \frac{1}{N} \sum_{k=0}^{N-1} |y_{mN+k}|^2 \in \mathbb{R} \tag{2}$$

and the power distribution model in the presence of interference at time 'm' is:

$$S_m \sim N\left(\mu_m + J_m, \sigma_m^2\right) \tag{3}$$

where μ_m and σ_m^2 are the mean and variance of the nominal (interference-free) power model, and J_m is the power introduced by the interference in the front-end's frequency band. In [3], we determine values for μ_m and σ_m^2 by overbounding the interference-free power data distribution. We define the following two mutually-exclusive, exhaustive hypotheses of no RF interference (RFI), H_0, and RFI occurrence, H_1:

$$\begin{aligned} \text{Null hypothesis } H_0 &: J_m = 0 \text{ (no RFI)} \\ \text{Alternate hypothesis } H_1 &: J_m > 0 \text{ (RFI)} \end{aligned} \tag{4}$$

The impact of an example power peak interference on the RF-front-end data collected at the data collection sites in Figure 2 is shown in Figure 1. We derived the following test statistic:

$$\alpha_m \triangleq \frac{S_m - \mu_m}{\sigma_m} \text{ such that } \alpha_m \sim N(0,1) \tag{5}$$

This detector is locally Neyman-Pearson optimal (about the nominal power value), i.e., it minimizes the probability of missed detection (PMD) for small positive deviations from the nominal power. The detection threshold T_m is set to meet a predefined requirement $P_{FA,REQ}$ on the probability of false alert (PFA). T_m is determined using the following equation:

$$P_{FA,REQ} = P(\alpha_m > T_m | H_0) \text{ i.e., } T_m = Q^{-1}(P_{FA,REQ}) \tag{6}$$

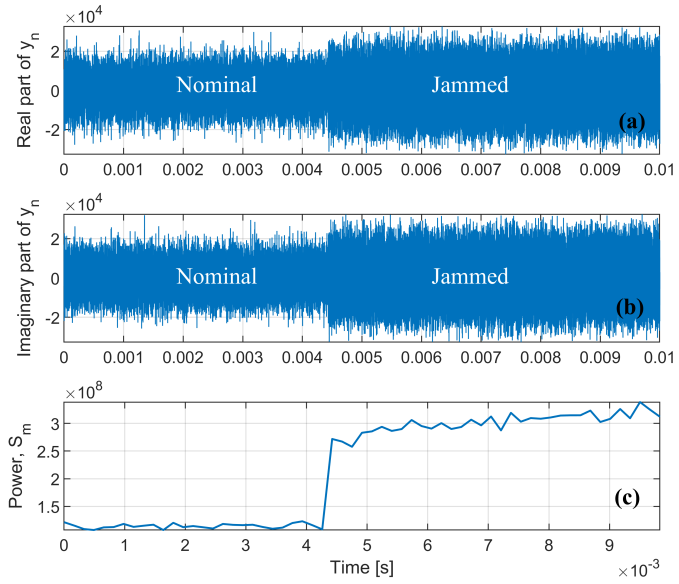

Figure 1: Impact of interference on data collected in Blacksburg, Virginia, in August 2022: (a) for the RF-front-end signal's real part, (b) for the imaginary part, and (c) for the power measurement.

where $Q^{-1}()$ is the inverse tail probability of the standard normal distribution. The remainder of the paper shows curves of α_m/T_m over time to identify jamming monitor detection occurrences.

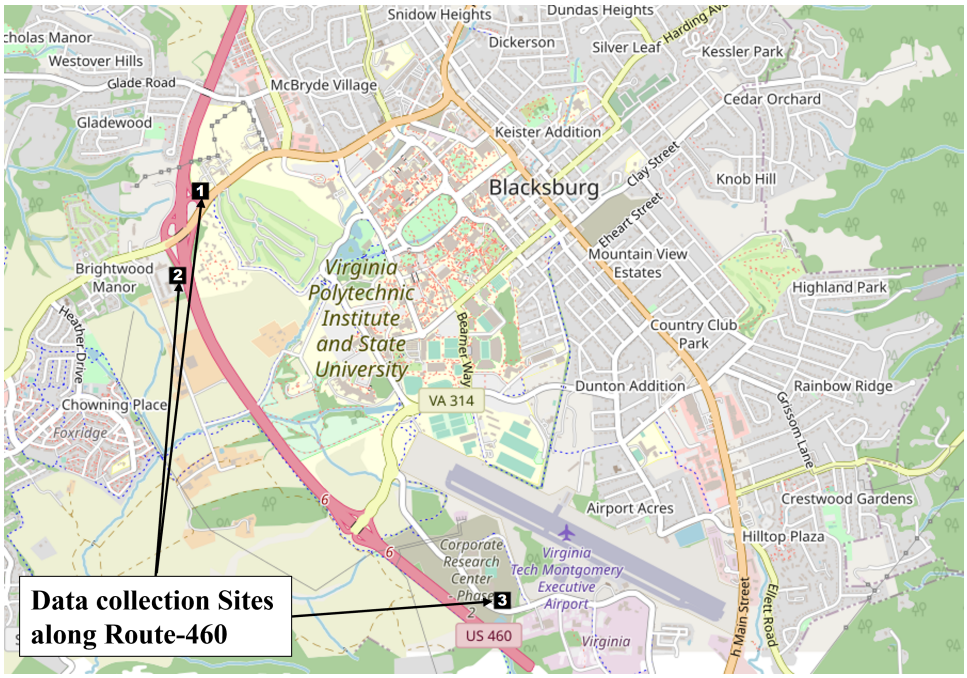

Figure 2: Map showing data collection sites near Blacksburg, VA.

2. Preliminary Detection of GNSS Interference

Figure 3 shows an example of a set of four short-duration power peaks that we detected in the data collected in December of 2023 along Route 460 near Blacksburg, VA, at the static receiver location at site 3 indicated Figure 2. We first observed this

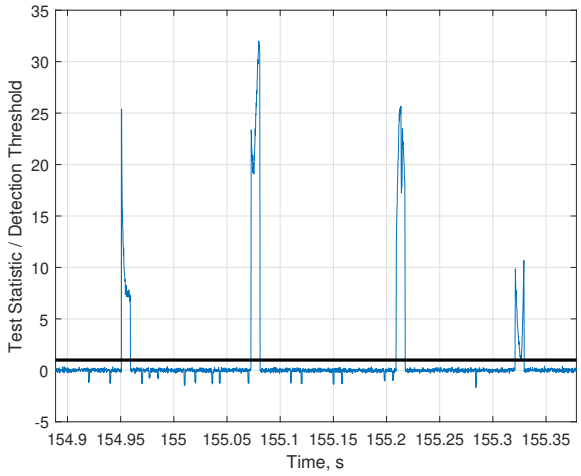

Figure 3: Plot showing power-peak events detected by the signal power monitor data collection site number 3 in Figure 2 on December 6, 2023.

signal in May of 2022. Since then, we have detected many such power peak sequences. They are present in all data sets, whether they were collected alongside highways in Virginia, North Carolina, or Colorado.

These peaks caused no apparent disruption of GPS receiver operations: during these events, all visible satellites were continuously tracked by our software-defined receiver and by another collocated commercial off-the-shelf receiver, which we use for redundancy, without significant C/N0-variations. The power peaks cause false alerts (FAs) in our jamming detectors. We could have easily dismissed them by setting a threshold on the duration of a power peak, but (1) we wanted to understand their origin, and (2) we had no rationale other than a few empirical observations to set this threshold. Understanding the source of these FAs and characterizing them will help design more robust power-based jamming monitors that can autonomously operate over months at a time.

In addition, we analyzed the frequency content of the RF-front-end signal during power peaks using spectrograms and PSDs. The first objective is to check that the signals causing the peaks are not aliases of other signals at frequencies outside the intended observation frequency band. Poorly designed RF data collection equipment can pick up powerful signals that are outside the intended band. To confirm that the signals causing FAs are not aliased into the band centered at L1, we recorded data using two separate nodes, each node consisting of a USRP and its data-collection computer. The two nodes recorded data *using two different center frequencies*. Figure 4 shows PSDs of an interfering signal simultaneously recorded at the two nodes. PSDs indicate that power density is concentrated at two distinct frequencies as if the signal was a two-tone sinusoid. The fact that the PSD peak pairs coincide across USRPs despite their different center-frequency settings proves that the interfering signal is not an alias of some out-of-band signal.

3. Frequent Short-Pulse GPS L1 Interference Consistently Observed at Multiple Locations

We carried out additional multi-USRP experiments using different sampling frequencies to further confirm that the two-tone signals could not be aliases of out-of-band signals. The characteristic four-pulse signal shown in Figure 3 in all of the multiple-hour-long datasets collected along highways in Virginia, North Carolina, and Colorado. We found reports of similar signal recordings by other groups [4, 9, 10]. These references show peaks in power density at a single frequency, suggesting a single tone or continuous wave interference.

We have since found other single, dual, and multi-tone signals. In all cases, we used multiple USRPs to check that the signals were not aliases of out-of-band signals. These signals would again be ineffective at jamming a GPS signal that spreads over a 5-to-25 MHz bandwidth, but these interfering signals cause false alerts for power monitors. To better understand, classify, and then identify these signals, we study their time-frequency characteristics.

III. TIME-FREQUENCY ANALYSIS OF MULTI-POWER-PEAK SIGNALS AT THE GNSS L1 FREQUENCY

To improve jamming detector design by reducing the FA risk, we analyze the frequently-occurring quadruple power peaks detected in Section II.

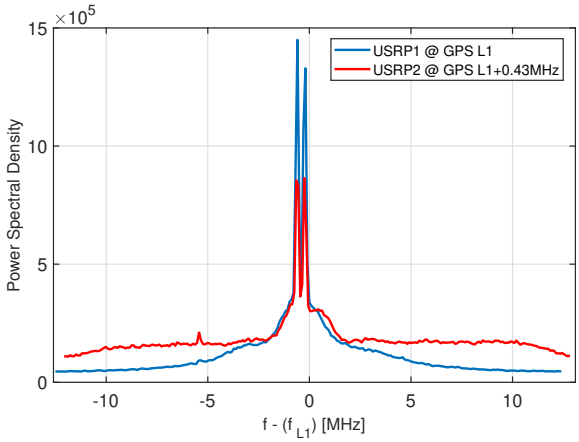

Figure 4: PSD RF-front-end signal from two USRPs collecting data at two different center frequencies during power peak events. f_{L1}=1575.42 MHz.

1. Spectrogram Analysis of Signals Causing Power-Peak Sequences

This section presents the interfering signals' spectrograms, i.e., three-dimensional plots of power density versus frequency over time. A spectrogram is obtained (1) by computing Fast Fourier Transforms (FFT) over ±2.5MHz about the baseband frequency for overlapping 256-RF-front-end-sample windows, and (2) by sliding the sample window over time, one sample at a time. Selecting a window size of 256 $\left(2^8\right)$ receiver-front-end samples was instrumental for message visualization in the following figures. In these figures, the spectrogram's y-axes are frequency offsets with respect to the L1 frequency converted to baseband; the x-axes represent the sliding window's time offset with respect to the start of the time interval of interest.

The interference near the L1 frequency we most often observe can be categorized into two main types.

1. A quadruple-power-pulse sequence is shown in Figure 5. Each signal power-pulse appears to encode data using binary frequency shift keying (BFSK). The example in Figure 5 was recorded in Blacksburg, VA, on December 6, 2023.
2. A six-pulse sequence observed in Denver, CO, is shown in Figure 6. In this case, data is encoded using amplitude shift keying (ASK) or on-off keying (OOK).

For the quadruple-pulse BFSK signals in Figure 5, each power-peak (or pulse) is 8.5-millisecond long, and pulses are separated by an interval of 110-140 ms. The signal's power can vary from one pulse to the next. The PSD for one of these pulses shows higher power content at two separate frequencies, similar to the PSD in Figure 4. The separation between the two frequencies is 350 kHz. The rate at which these quadruple-pulse messages are recorded is about two per hour when driving on highways such as I-25 in Colorado and I-77 in North Carolina and Virginia.

The six-pulse ASK/OOK signals are comprised of 29-ms-long pulses separated by 140-to-180-ms-long intervals (e.g., see Figure 6). Signal power may vary for each pulse. Their PSD shows a single peak of power density near the GPS L1 frequency, with small variations in frequency offsets with respect to L1 at 1575.42 MHz, typically 0.5-1.0 MHz lower than GPS L1. The rate of occurrence of this message type is approximately one per hour.

2. Analyzing the BFSK and ASK/OOK Messages

BFSK spectrograms show peaks of power density switching between two frequencies with transitions occurring at multiples of 50 μs. There are 160 such intervals or *chips*. The same 160 chips are repeated in each one of the four 8.5-ms-long power-pulses.

ASK spectrogram chips are encoded by switching between two amplitude levels at a single frequency. The recorded ASK signals include 240 chips lasting 120 μs. The same 240 chips are repeated in each one of the six 29-ms-long pulses.

Within a power-pulse, each chip sequence, or message, starts with a preamble, i.e., a fixed number of regular zero-to-one chip-pair transitions: 30 transitions for BFSK and 80 transitions for ASK. The rest of the chip sequence is the message's data.

3. Identifying Automotive Key Fobs as Potential Interference Sources

Spectrograms revealed data message structures that carry strong similarities with signals used in automotive remote control and wireless communication systems. (We found this through a web search for signals with the above characteristics.)

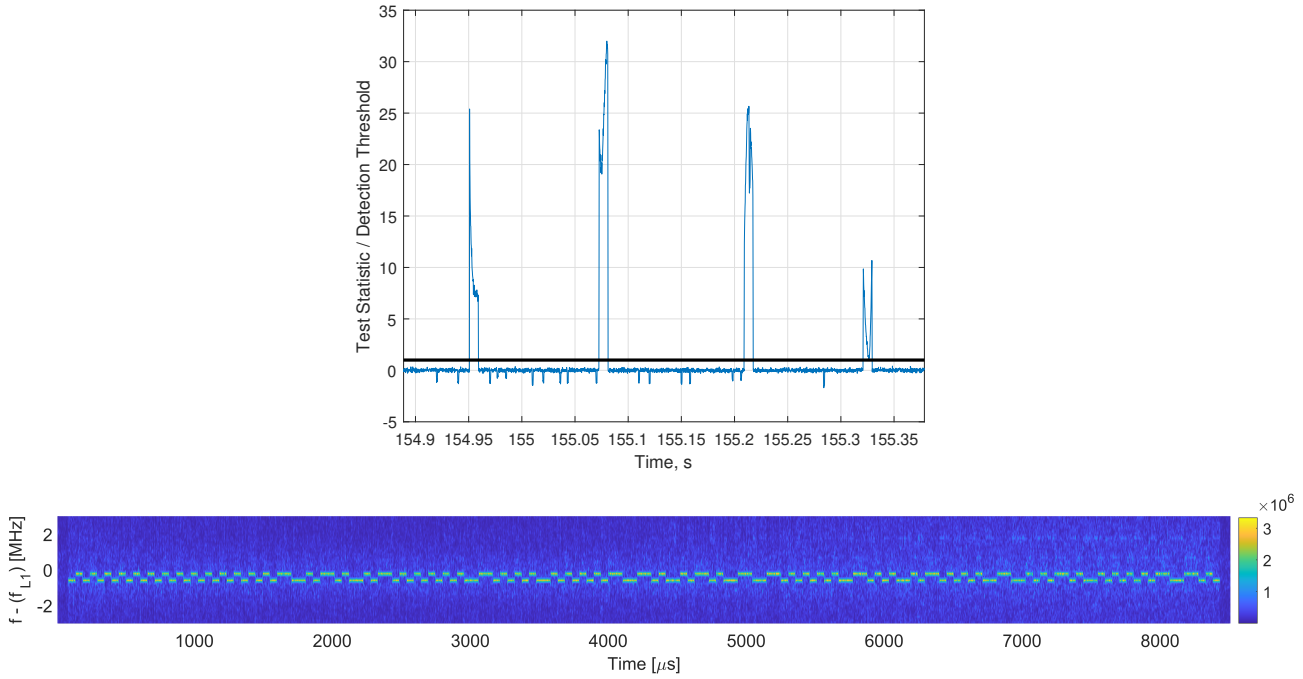

Figure 5: Test statistic to detection threshold ratio and spectrogram of 4-pulse power peak received in Blacksburg along route-460 (site 3 in Figure 2) on December 6, 2023. The message (bottom) repeats four times.

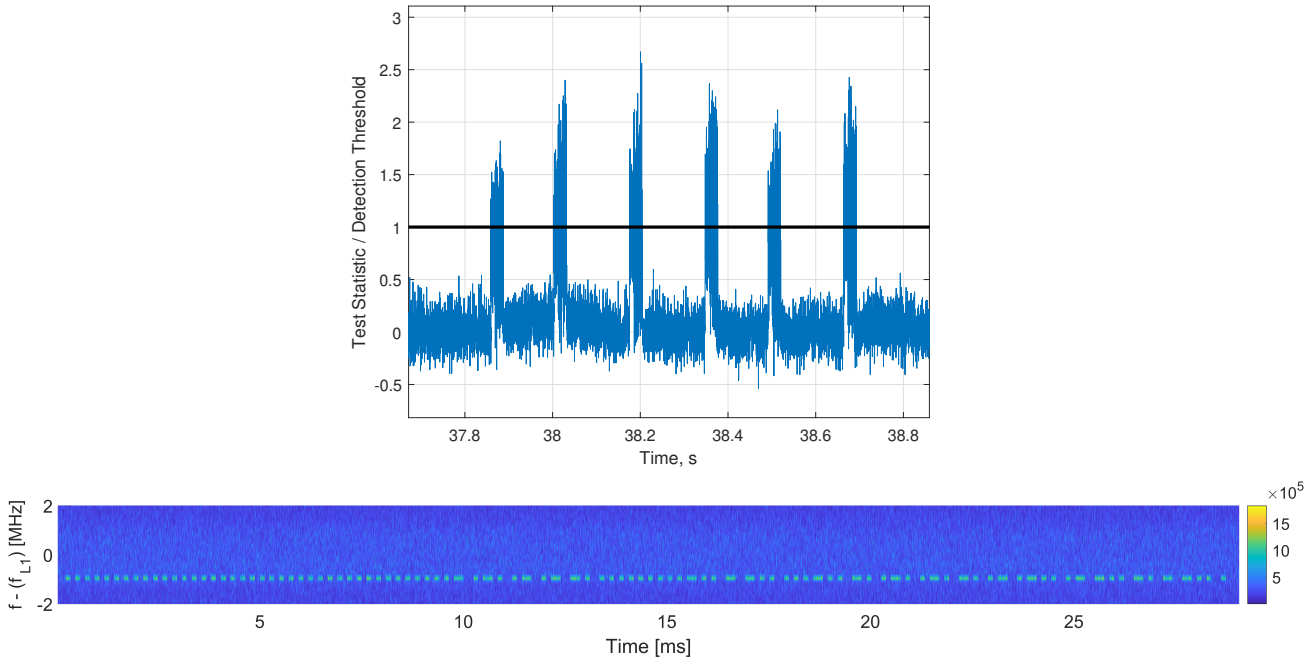

Figure 6: Test statistic to detection threshold ratio and spectrogram of an example six-power-pulse sequence recorded along I-25 in Denver, CO. The pulsed message shown at the bottom is repeated six times (once per power peak).

In particular, automotive key fobs are RF devices used to unlock cars. They typically transmit ASK/OOK messages at the 315-MHz frequency [12]. Their message structure bears a striking resemblance with the 4-pulse and 6-pulse signals that we

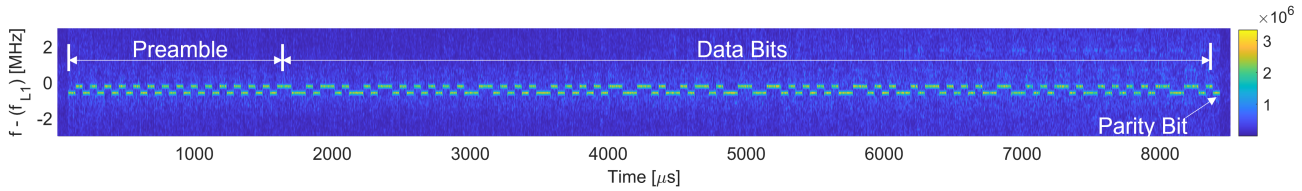

Figure 7: Structure of the BFSK Message.

recorded. Messages from key fobs are modulated using the Manchester encoding. Bits are encoded using level transitions: 1-to-0 transitions represent bit 0, and 0-to-1 transitions represent bit 1. In addition, the number of pulse repetitions, the preamble bit-length, and the data-bit-length for key fob messages match that of the signals we recorded. However, at this point, it was unclear why signals emitted at 315MHz were observed near the GPS L1 frequency.

IV. SPECTRUM ANALYSIS OF KEY FOBS

In this section, we analyze spectrograms at the L1 frequency in the presence of automotive key fob emissions.

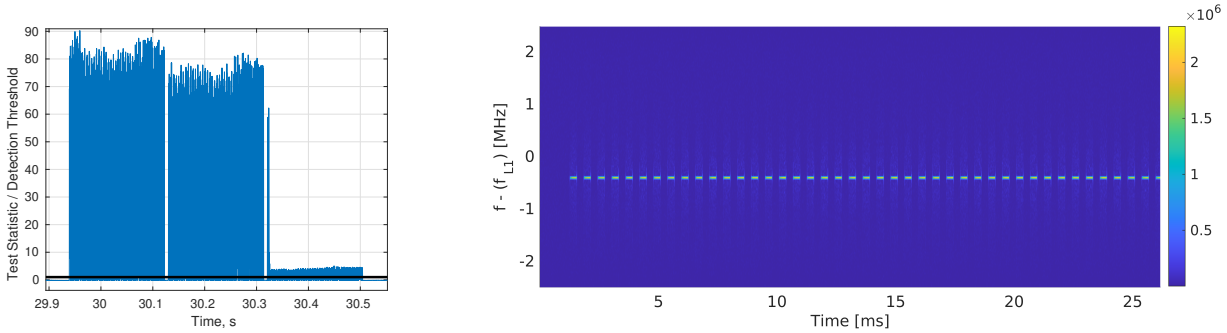

Figure 8: Power time-history (LEFT) and spectrogram (RIGHT) of Volkswagen key fob emissions near the GPS L1 frequency.

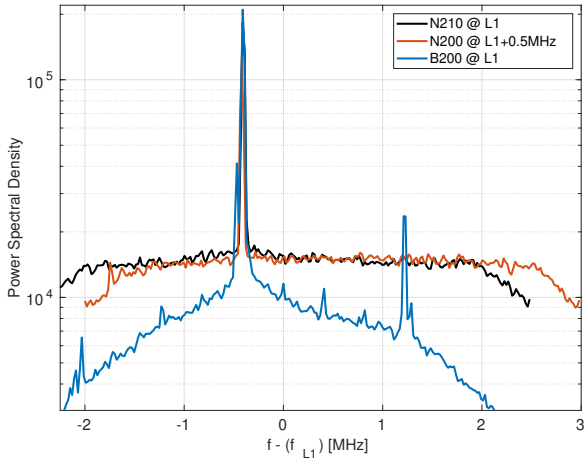

Figure 9: PSD of a Volkswagen key fob signal recorded using three different USRPs around the L1 frequency

Figure 8 shows a power peak sequence and a spectrogram (only showing the ASK message preamble) of a USRP data recording while activating a Volkswagen key fob with FCC Part number NBG010180T. The test and figure are experimental proof that key fobs cause non-jamming interference near the L1 frequency.

We also tested key fobs for a Toyota car and a Ford truck. Nothing was observed for the Toyota. For the Ford truck, the PSD and spectrogram are shown in Figure 10. This shows that the interference characteristics vary significantly between key fobs.

For the Volkswagen key fob signal, Figure 9 shows PSDs obtained using simultaneous recordings by three Ettus USRP models: N200, N210, and B200. The N200 center frequency setting was offset from L1 by +0.5 MHz. All three PSDs exhibit a power density peak at the exact same frequency: the key fob signal is not the alias of an out-of-band signal.

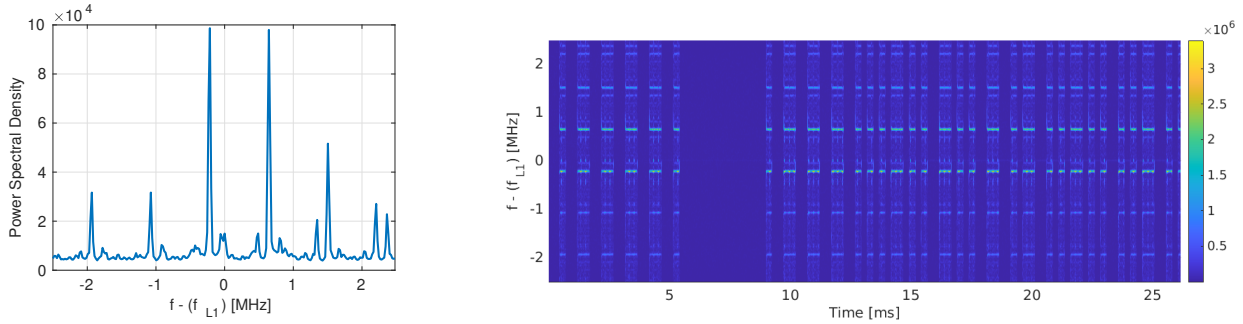

Figure 10: PSD (LEFT) and spectrogram (RIGHT) for Ford Truck key fob emissions near the L1 frequency.

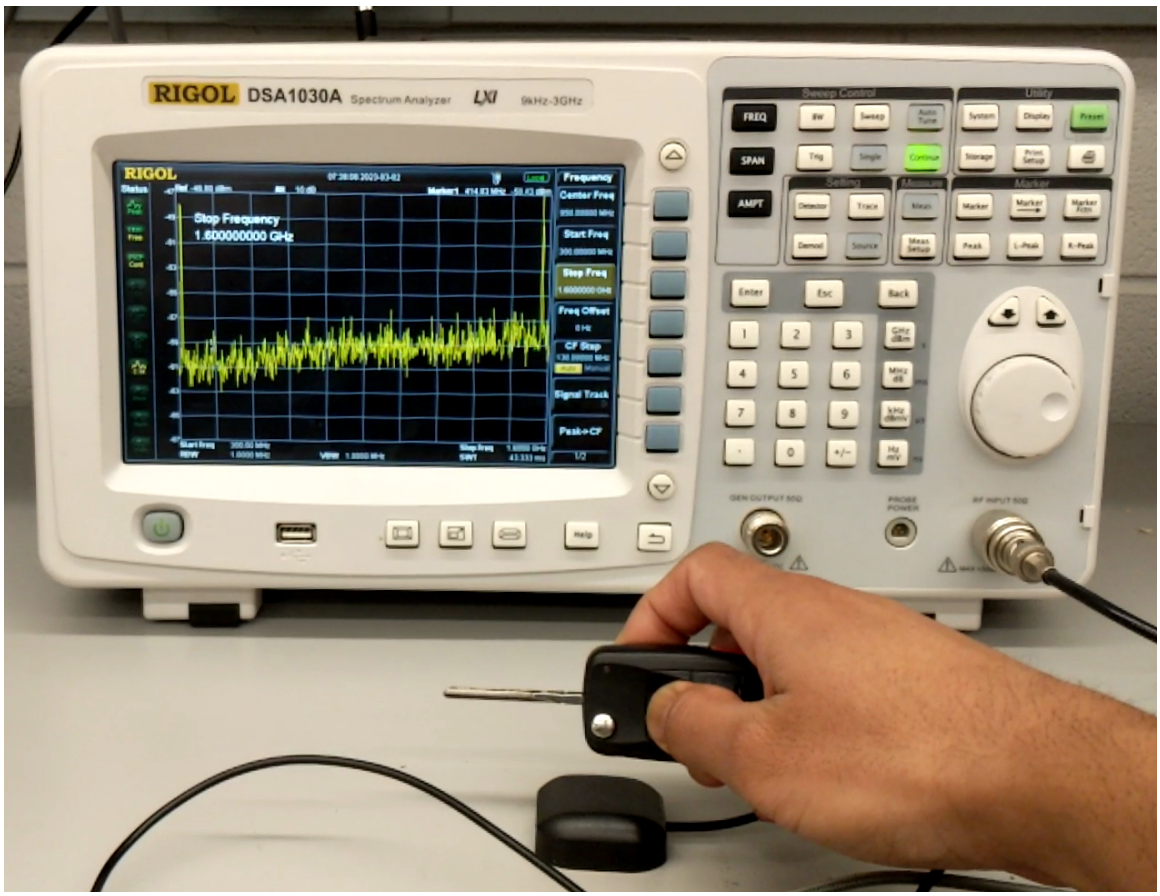

Figure 11: Spectrum analyzer showing the PSD from 300-1600 MHz. When we press the key fob near the antenna, there are two peaks, at 315 and 1575 MHz

The main transmitting frequency of the key fob is 315 MHz. The fifth harmonic of the 315 MHz is 1575 MHz, very close to the GPS 1575.42 MHz L1 frequency. The higher harmonics are termed *spurious emissions*. To confirm that the observed power density peaks correspond to the fifth harmonic of the 315 MHz key fob signal, we used a spectrum analyzer: we recorded key fob emissions over a wide frequency band. In Figure 11, the spectrum analyzer's screen x-axis spans the entire lower half of the UHF band from 300 MHz to 1600 MHz. Each x-axis tick is 130-MHz-wide. The pictured PSD shows two simultaneous peaks at 315 MHz and 1575 MHz. The power density at 315 MHz and 1575 MHz is clearly visible more than other harmonics because

of the different gains and band-pass filters at the key fob emitting and GPS receiving antennas. Visibility was maintained at key fob-to-GPS antenna distances exceeding 5 meters. The spectrum analyzer test reinforces the fact that a key fob operating at 315 MHz can interfere with GPS at the L1 frequency. It is a fact even though this specific key fob model has a Federal Communications Commission (FCC) testing report that shows compliance with the Code of Federal Regulations (CFR) Title 47 §15.209 [13, 14].

V. MITIGATING JAMMING MONITORS FALSE ALERTS CAUSED BY COMPLIANT RADIATORS

This section describes an approach to mitigate false alerts in power-based jamming monitors that are caused by spurious emissions of compliant intentional radiators. This approach is based on regulations to avoid having to characterize spurious emissions from individual commercially-available RF communication devices.

1. Regulations on Spurious Emissions

The International Telecommunications Union (ITU) recommends worldwide radio frequency spectrum allocations [15]. ITU-participating countries require compliance of RF-transmitting equipment manufacturers to specific standards. In the US, radio energy transmission at the L1 frequency is regulated by the FCC. The US CFR Title 47 §15.205 mandates that all manufacturers test for RF emissions in restricted bands. They must demonstrate that at these frequencies, the transmitted energy is below a required level. Spurious emissions are allowed, including in the band allocated for aeronautical radionavigation service (ARNS) that contains GPS L1, but with limitations that are detailed below. Thus, devices operating at 315 MHz, such as, for example, key fobs, garage door openers, automotive wireless devices, etc. can have spurious emissions at GPS L1 band .

Higher harmonics of an intended emission are called spurious emissions. The emission limits are specified in terms of electric field intensity. According to §15.231, the electric field strength of spurious emissions should be 20 dB below that of the original frequency. For spurious emissions at restricted frequencies, additional limits are specified in §15.209. The left panel in Figure 12 shows electric field strength (EFS) intensity limits of spurious emissions for 315 MHz transmissions. The limit for spurious emissions near GPS L1 is highlighted in red

For pulsed emitters such as key fobs, the EFS intensity limits apply to the average EFS intensity, which is computed by multiplying the peak intensity by a duty cycle correction factor following §15.35. The duty cycle correction factor is the fraction of the time the emitter is on over a 100-millisecond time window. This regulation allows the peak intensity to exceed the limits specified in §15.231 and §15.209. In addition, paragraph §15.35 limits the peak intensity to no more than ten times the average value. The right panel in Figure 12 shows representations of two rectangular pulses with compliant average EFS intensity but different peak intensities. The yellow pulse reaches ten times the intensity limit but only transmits for 10 ms, which matches the average intensity of the green pulse.

For power-based jamming monitor design, one might dismiss the detection of power peaks lasting less than 10 milliseconds in any 100-millisecond period.

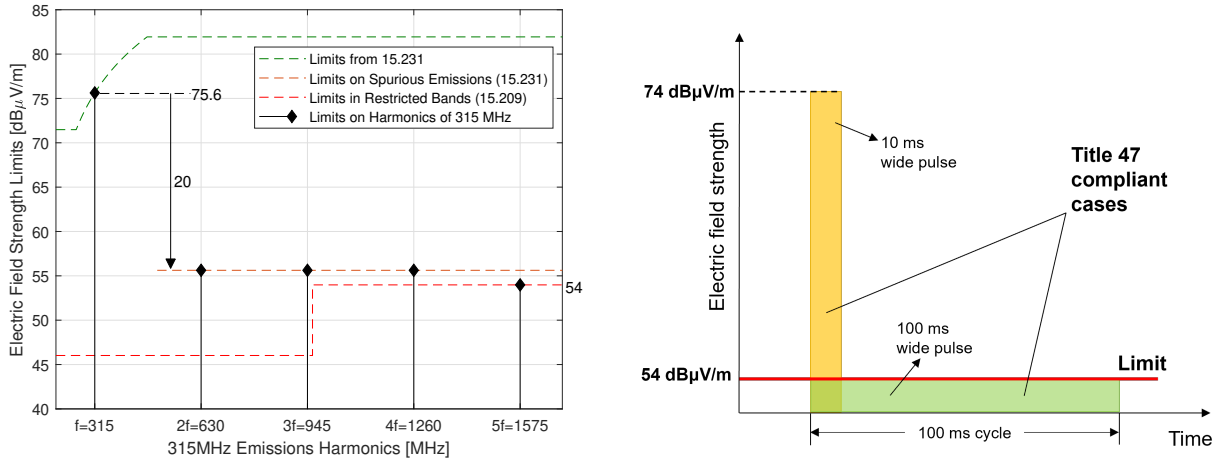

Figure 12: Interpretation of CFR Title 47 Chapter 15 Regulations. LEFT: limits on spurious emissions according to §15.209 and §15.231; RIGHT: duty cycle correction factor according to §15.35

2. Maximum Allowable Peak Power at GPS L1

We begin with the equation of irradiance as follows: We use the Friis transmission equation to write the received peak power versus distance as:

$$P_{R,peak}(R) \leq 0.3\,(10E_{lim})^2\,G_T G_R \left(\frac{\lambda}{4\pi R}\right)^2 \tag{7}$$

where a bound on the allowable peak transmission $0.3\,(10E_{lim})^2$ was computed for a target EFS intensity at 3 m at GPS L1 assuming vacuum impedance, no near-field effects (CFR Title 47 §15.209), and a factor 10 to account for the maximum allowable peak (§15.35). G_T and G_R are the transmitting and receiving anatenna gains, respectively ($G_T = G_R = 1$ for isotropic antennas), λ is the frequency of the spurious emission (at GPS L1, λ = 1575.42 MHz) and R is the emitter to receiver distance. According to Title 47 §15.209, the maximum allowable field intensity for any RF device with residual power in UHF above 960 MHz is E_{lim} =500 μV/m (54 dBμV/m).

Figure 13 shows how the maximum allowable peak power decays as a function of distance. Curves are shown for two receiver gains G_R, for $G_T = 1$. For power-based jamming monitors using larger than 100 ms windows for power estimation, a duty cycle correction factor of 1/100 on $P_{R,peak}(R)$ may be implemented following §15.209. The resulting power limit may be exploited in static monitors, for example, near parking lots where one might expect spurious emissions within a known distance. Window size for jamming monitor power averaging may also be adjusted to account for these regulations.

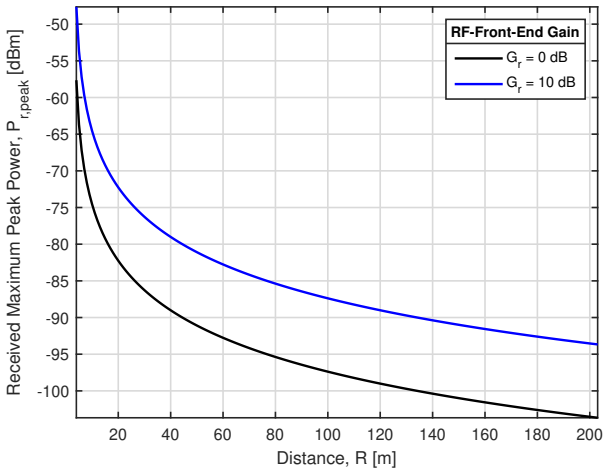

Figure 13: Maximum peak power

VI. CONCLUSION

This paper describes the methodology we developed and implemented to analyze repeatedly-observed interference at the L1 frequency. These interfering signals did not jam GPS but caused false alerts in our and other power-based GNSS jamming detectors. The methodology first establishes that the observations were not aliases of out-of-band signals. A time-frequency spectrogram analysis then reveals that data messages are modulated on these interfering single-tone and multi-tone signals. The signal structures match that of automotive key fobs. A spectrum analyzer was used to confirm that spurious key fob emissions were observable near the L1 frequency at distances as large as 5-to-8 meters. In order to mitigate jamming monitors' false alerts caused by these interferences, we analyzed the regulations governing spurious emissions: duty-cycle requirements can help set minimum-duration detection thresholds on suspected jamming events.

ACKNOWLEDGEMENTS

This paper is based upon research partly sponsored by the Center for Autonomous Air Mobility & Sensing (CAAMS) supported by the National Science Foundation (NSF)'s Industry-University Cooperative Research Centers (IUCRC). Any opinions, findings, or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the sponsors.

REFERENCES

[1] National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, "National PNT advisory board comments on jamming the global positioning system - a national security threat: Recent events and potential cures," Technical Report, November 2010, https://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf, Accessed on: June 30, 2023.

[2] A. Morrison, N. Sokolova, N. Gerrard, A. Rødningsby, C. Rost, and L. Ruotsalainen, "Radio-frequency interference considerations for utility of the Galileo E6 signal based on long-term monitoring by ARFIDAAS," *NAVIGATION: Journal of the Institute of Navigation*, vol. 70, no. 1, 2023.

[3] S. Jada, J. Bowman, M. Psiaki, C. Fan, and M. Joerger, "Time-frequency analysis of GNSS jamming events detected on US highways," in *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, 2022, pp. 933–946.

[4] N. Sokolova, A. Morrison, and A. Diez, "Characterization of the GNSS RFI threat to DFMC GBAS signal bands," *Sensors*, vol. 22, no. 22, p. 8587, 2022.

[5] K. Fors, N. Stenberg, and T. Nilsson, "Using the Swedish CORS network SWEPOS for GNSS interference detection," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 2021, pp. 4323–4333.

[6] S. Bergström, K. Fors, and S. Linder, "Long-term evaluation of noise and interference statistics in GPS L1-band," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 2021, pp. 4316–4322.

[7] S. Thombre, M. Z. H. Bhuiyan, P. Eliardsson, B. Gabrielsson, M. Pattinson, M. Dumville, D. Fryganiotis, S. Hill, V. Manikundalam, M. Pölöskey *et al.*, "GNSS threat monitoring and reporting: Past, present, and a proposed future," *The Journal of Navigation*, vol. 71, no. 3, pp. 513–529, 2018.

[8] J. Bennington and R. Zimmermann, "New GNSS multi-frequency interference detection and analysis solution for positioning, navigation and timing applications," Press Release by Spirent, September 2016, https://www.spirent.com/newsroom/press-releases/09-13-16_gss200d-gnss-multi-frequency-interference-detection-analysis-solution, Accessed on: June 30, 2023.

[9] E. Pérez-Marcos, A. Konovaltsev, S. Caizzone, M. Cuntz, K. Yinusa, W. Elmarissi, and M. Meurer, "Interference and spoofing detection for GNSS maritime applications using direction of arrival and conformal antenna array," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 2907–2922.

[10] Konovaltsev, A., "Unknown intermittent continuouse wave interference at GPS L1," Personal Communication, 2023.

[11] Aviles, J., "Garage door opener causing interference at GPS L1," Personal Communication, 2023.

[12] Keysight Technologies, "Decoding automotive key fob communication based on Manchester-encoded ASK modulation," Web Reference, December 2017, https://www.keysight.com/us/en/assets/7018-05710/application-notes/5992-2260.pdf, Accessed on: June 01, 2023.

[13] Trepper, R.,, "Test report acc. to the relevant standard 47 CFR part 15c - intentional radiators," Hella KGaA Hueck & Co., Tech. Rep., 2009, https://fcc.report/FCC-ID/NBG010180T/1159165, Accessed on: March 12, 2023.

[14] Federal Communications Commission, "Title 47 CFR 15 subpart C - intentional radiators," October 1989, https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15/subpart-C/section-15.209, Accessed on: June 30, 2023.

[15] ITU, "International Telecommunication Union," 2023, https://www.itu.int/en/about/Pages/default.aspx, Accessed on: June 30, 2023.