Time-Frequency Analysis of GNSS Jamming Events Detected on U.S. Highways

Sandeep Jada, John Bowman, Mark Psiaki, Chenming Fan, Mathieu Joerger, *Virginia Tech*

Sandeep Jada obtained a masters degree (2011) in aerospace engineering from Indian Institute of Science, Bangalore, India. He worked for Airbus India (2011 to 2018). He is a doctoral candidate at Virginia Tech working with Dr Mathieu Joerger, with a focus on error time correlation modeling and GNSS interference detection.

John Bowman John Bowman is a Ph.D. student at Virginia Tech working with Dr. Mark Psiaki. His research interests include satellite orbit determination, GNSS interference detection and localization, and navigation using software-defined radio.

Mark Psiaki is Professor and Kevin T. Crofton Faculty Chair of Aerospace and Ocean Engineering at Virginia Tech. He is also Professor Emeritus of Mechanical and Aerospace Engineering at Cornell University. He holds a Ph.D. in Mechanical and Aerospace Engineering from Princeton University. He is a Fellow of both the ION and the AIAA. His research interests are in the areas of navigation, spacecraft attitude and orbit determination, remote sensing, and general methods for estimation, filtering, and detection.

Chenming Fan is a third year undergraduate student studying aerospace engineering and computer science at Virginia Tech. He is a committee chair at Student Engineers' Council, a student member of AIAA, and a student member of IEEE. His academic interests are in the fields of guidance, navigation, and control, machine learning, and computer vision.

Mathieu Joerger (M.S., INSA Strasbourg - Illinois Tech, 2002; Ph.D., Illinois Tech 2009) is assistant professor at Virginia Tech, senior editor of Navigation for IEEE TAES, member of EU/US Cooperation on Satellite Navigation, Working Group C - ARAIM.

ABSTRACT

In this paper, we implement jamming detectors designed for off-the-shelf GNSS receivers using publicly available data collected at more than 900 receiver locations during an eight-month-long period. We identify spatial and temporal patterns in the detected events to predict when and where jamming may occur. We find patterns that coincide with daily driver commutes and weekly delivery schedules along U.S. highways. We then validate this approach by developing a new Neyaman-Pearson locally-optimal signal power monitor using wideband radio-frequency (RF) data, and by deploying our own equipment at the locations and times of the predicted jamming. Two example wideband data sets are presented, which we collected in Colorado and Virginia. We analyze this data in the time-frequency domain and show interference in the GPS L1 band caused by recurring unidentified communication broadcasts and by personal privacy devices (PPDs).

I. INTRODUCTION

The threat to GNSS-based positioning, navigation, and timing (PNT) of radio frequency interference (RFI) including jamming and spoofing has been growing over the past decade [1]. Widespread sources of GNSS jamming on U.S. highways include personal privacy devices (PPDs) [2,3]. Jamming detection using off-the-shelf GPS receiver outputs such as carrier to noise ratio (C/N0) [4–9] and automatic gain control (AGC) [10] can be implemented using existing receiver networks. However, while these methods provide evidence of signal disturbances, they do not prove the presence of jamming signals. In contrast, radio frequency (RF) spectrum-based detectors in [11–13] can unambiguously identify jammers, but their deployment over a large network of ground stations may be cost-prohibitive. In [12,13], a C/N0 detector was validated using wideband RF data collected at Swedish Continuously Operating Reference Stations (CORS). The data showed peaks in power spectral density (PSD) that were tens of dB-Hz higher than the jam-free PSD in the GPS L1 band, which constitutes clear evidence of interference.

In this paper, we develop, test, and analyze a new RF front-end signal power-based jamming detector that minimizes the probability of missed detection while quantifiably limiting the risk of false alerts. We use this power-based detector to validate a C/N0-detector implemented using off-the-shelf receivers.

In the first part of this paper, we implement the receiver-independent, self-calibrating, C/N0-based jamming detection method in [4] to find spatial and temporal jamming patterns. Jamming patterns on U.S. highways are to be expected, for example, corresponding to a driver's daily commute or to weekly delivery schedules. Data from 900 CORS receivers is processed, which illustrates the monitor's automated capability to collect data, identify nominal C/N0 model parameters, and detect jamming while meeting a predefined false alert requirement. We then identify temporal patterns using time-domain and frequency-domain analyses of eight-month-long data sets collected at two specific sites: one from the International GNSS Service (IGS)

in Colorado Springs, Colorado, and the other from a CORS station near Charlotte, North Carolina.

Identifying jamming patterns provides the means to predict opportunities to observe outdoor jamming events using equipment that is more sophisticated than that available at receiver networks. Thus, in the second part of the paper, we design a portable hardware setup and a real-time signal-power monitor to collect memory-expensive wideband RF data. We deployed this equipment along route-460 near Blacksburg, VA, and near the IGS site in Colorado where we detected various types of GPS L1 interferences that are analyzed in this paper.

The organization of the paper is as follows. In Sec. II, we use a C/N0 monitor to detect jamming events over a network of 900 receivers in the Eastern United States, and we describe temporal jamming patterns identified at two specific locations. In Sec. III, we develop the wideband RF data collection hardware and software used to validate the C/N0 based jamming detector. In Sec. III, we analyze the detected the interference in the time-frequency domain. Finally, Sec. V we present our conclusions.

II. C/N0-BASED DETECTION FOR SPATIAL AND TEMPORAL JAMMING PATTERN IDENTIFICATION

1. C/N0-Based Jamming Detectors

In [4], we derive two different jamming monitors for detecting simultaneous drops in C/N0 across multiple satellites: (1) using C/N0 from all satellites in view, and (2) using time-differenced C/N0s from all satellites. Both monitors test statistics are derived as Neyman-Pearson optimal hypothesis tests. Their detection thresholds are set to meet a predefined probability of false alert. Thus, the two monitors require satellite-specific, receiver-location-specific, and elevation-dependent models of probability distributions for nominal C/N0 and time-differenced C/N0, respectively. Nominal model parameters are developed by applying overbounding theory in [14] to jam-free data. This process is automated because this method is intended for deployment over a network of receivers.

2. C/N0-based Jamming Detection at 906 CORS Network Receiver Locations

We use the jamming detection approach described in [4] to process data from CORS network receivers. In Fig. 1, we show a snapshot in time of the color-coded test statistic to detection threshold ratio at all 906 CORS sites that provide data at a 1 Hz update rate in the East of the United States. Excluded sites, e.g., in Michigan, appear with 'x'-markers. Detection, which is declared when the statistic-to-threshold ratio exceeds 1 (color-coded as orange to red), is highlighted with a black marker edge. Fig. 1 shows two such events, one in Eastern North Carolina on the left panel, the other in Texas near the Gulf of Mexico on the right panel.

The right-hand-side panel shows yellow-to-orange marker colors in North Carolina, which were caused by heightened ionospheric activity on August 4, 2021. Because the test statistic was designed to detect drops in C/N0 across *all* satellites, and because ionospheric events only impact a subset of satellite measurements at a time, no detection was declared at these North Carolina locations. This illustrates the jamming monitors' robustness to ionospheric events. Still, the events in Fig. 1 were detected based on drops in C/N0 measurements, which does not guarantee that they were caused by jamming. The remainder of the paper aims at consolidating the fact that the monitors actually detects jamming at CORS stations.

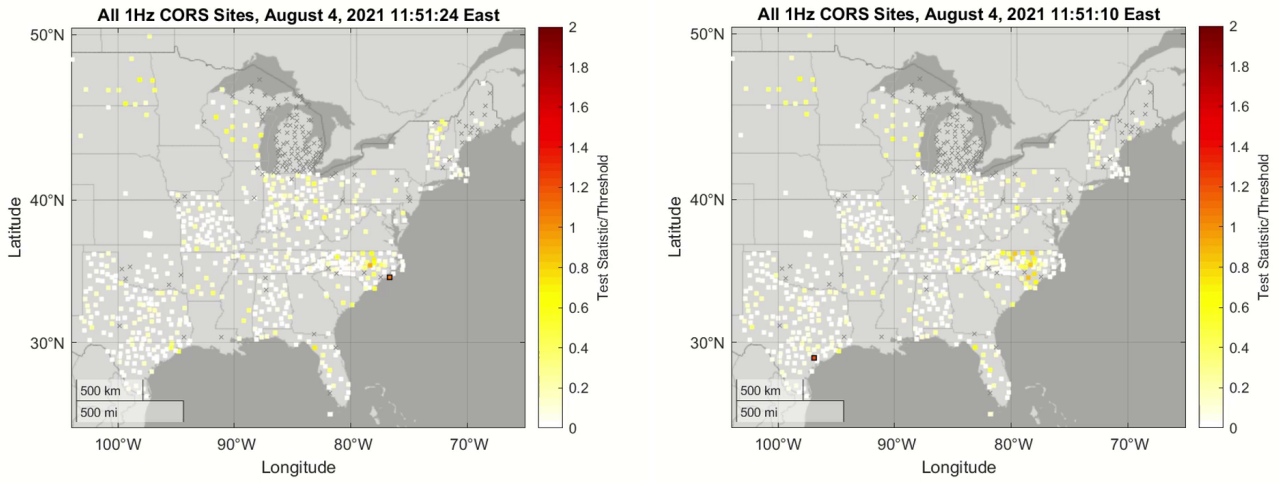

Figure 1: Jamming monitor results for 1 Hz CORS network.

3. Temporal Pattern Identification in Detected Jamming Events

Identifying detection patterns corresponding to driving schedules along highways would provide strong evidence of man-made interference, as opposed to other phenomena that can impact C/N0, such as ionospheric activity. Identifying such patterns may also provide opportunities to further validate C/N0-based detection through independent wideband RF data collection. We therefore analyzed eight months of data at a North Carolina (NC) location near Virginia Tech's Blacksburg campus. We selected the CORS site 'NC77' in Charlotte, NC. NC77 is ideal for future deployment of our own equipment because it is on an accessible drivers' rest area. NC77 is also likely to offer opportunities for vehicle-PPD jamming detection because it is located approximately 200 m away from interstates I-77 and I-485. Fig. 2 shows detected events at NC77 from January 2022 to August 2022. The left-hand-side plot shows the temporal distribution of events. The x-axis is the local time of day (ToD) and the y-axis is in increments of day-of-year (DoY) over eight months. Each circle-marker represents a jamming event. The marker size scales with the ratio of (C/N0-test-statistic over detection-threshold), which can be interpreted as capturing the intensity of the event. Makers are color-coded from blue to red to distinguish days of the week (DoW) for Monday to Sunday. The same color-code is used for the two histograms in the right-hand-side panels. These histograms show the numbers of event occurrences versus ToD (on top) and versus DoW (bottom). It is worth noticing that the top right-hand-side plot's y-axis is on a log scale: detected events predominantly occur during daytime, and more often on Tuesdays than on Sundays. We observe an order of magnitude difference in the number of daytime versus nighttime events. We also observe peak counts around local times 8:00 AM, 12:00 PM and 7:00 PM, which correspond to rush hours.

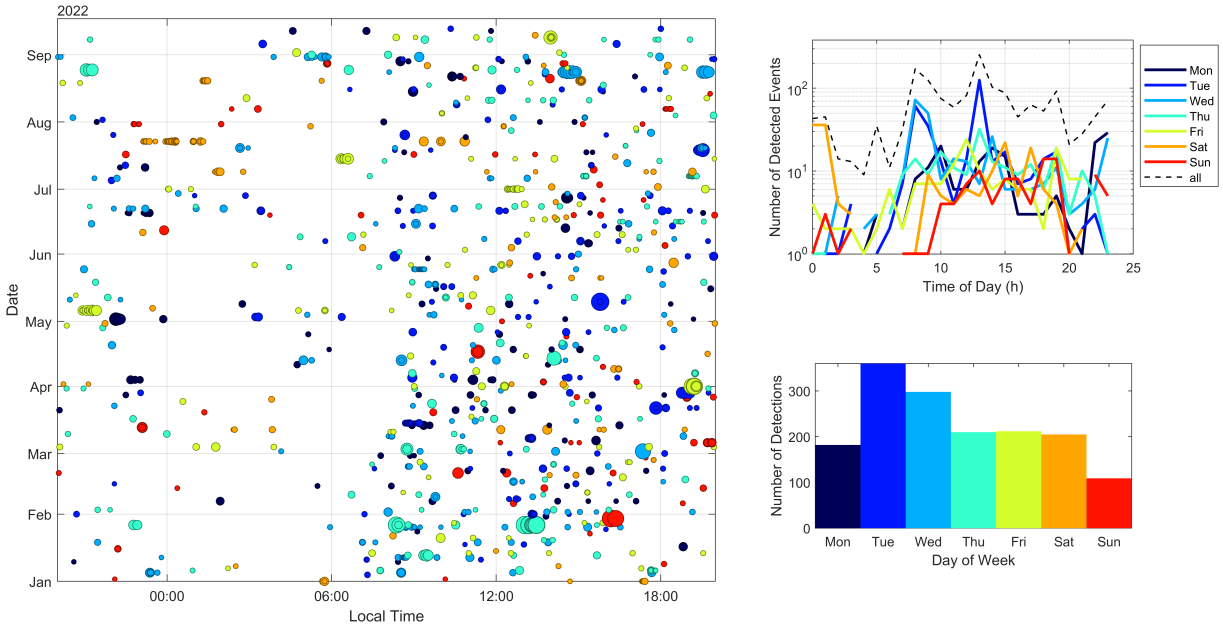

Figure 2: Jamming events at CORS site NC77 over the first eight months of 2022.

In addition, we perform a preliminary frequency-domain analysis to identify periodic patterns in the C/N0 test-statistic-over-threshold (TSOT) data. The TSOT power spectral density (PSD) should show peaks at the repeated-events frequencies. The left-hand-side plot in Fig. 3 shows the eight-month-long TSOT time-history. The right-hand-side plot is a PSD estimate. Three vertical lines are included to highlight frequencies corresponding to daily, weekly and fortnightly occurrences. The highest PSD values are found for daily occurrences, and PSD-increases are found over multiple-day periods. More data is needed to identify events at a lower repetition rate.

In addition to the U.S. CORS network, we processed data from the worldwide IGS network from January to August 2022. Fig. 4 shows the distribution of events detected at the IGS site AMC4 located in Colorado Springs, CO, USA. In this remote location, a clear pattern is visually discernible, with events regularly detected at 6:00 AM and 2:15 PM on weekdays, and relatively few detections on weekends. (IGS data was not available during the second half of February 2022.)

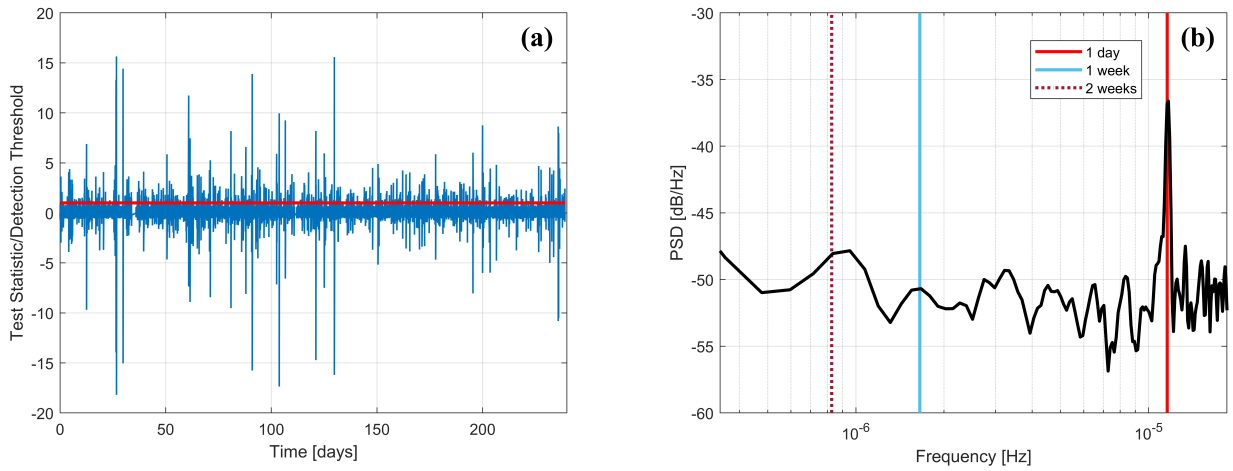

Figure 3: Spectral analysis of test statistic to detection threshold ratio. (a) Test statistic ratio over eight months, and (b) PSD of the test statistic ratio.

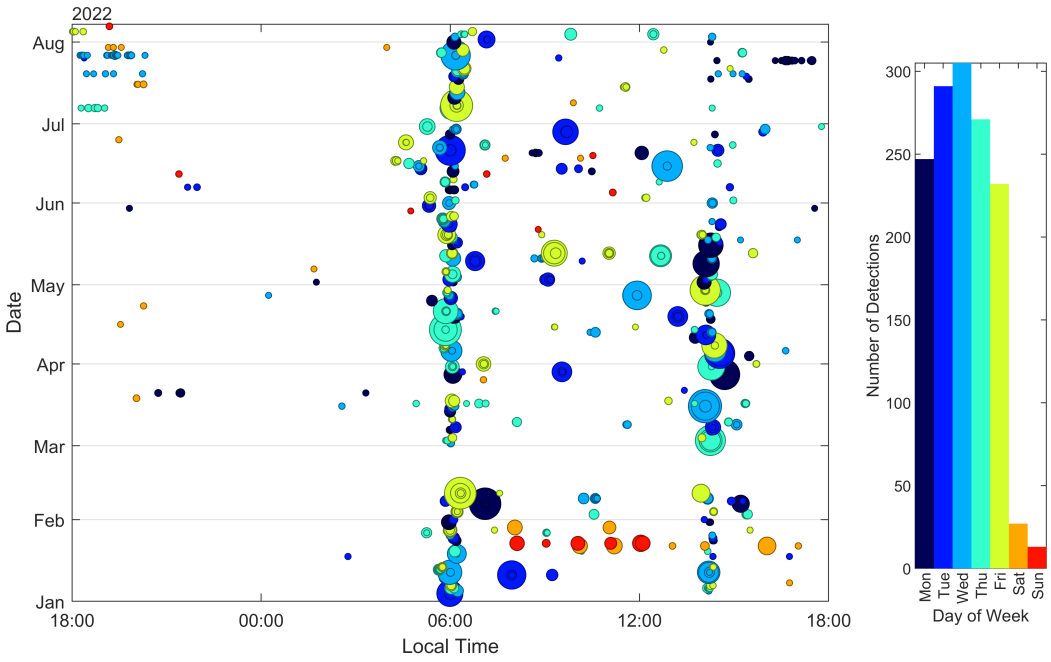

Figure 4: Jamming events at IGS site AMC4 during the first eight months of 2022.

III. DEVELOPMENT OF WIDEBAND RF DATA COLLECTION HARDWARE AND SIGNAL POWER DETECTOR

1. Hardware Description

To further confirm that C/N0 monitors at CORS and IGS receivers are detecting RF interference, and to demonstrate that we can predict repeatable jamming events, we develop an independent RF monitor. This monitor must be able to identify the type of interference being observed, which can be computation and memory expensive.

To enable deployment of a wideband RF data collection system, we selected the transportable and power-efficient hardware components listed in Fig. 5. The Ettus Universal Software Radio Peripheral (USRP) N200 with a DBSRX2 daughterboard can collect RF data is connected to an external Connor Winfield Ovenized Crystal Oscillator (OCXO) OH100. The OCXO is mounted on a circuit board, which sends a 10 MHz timing signal as a square wave with a +/-10 parts per billion frequency

stability, which is essential for GPS software receiver operations. The USRP is also connected to a Tallysman 33-8829NMAT GPS patch antenna. The USRP is controlled by an Intel Next Unit in Computing (NUC) 6 via a gigabit ethernet connection. The Intel NUC6 has 4 GB of RAM and a quad-core Intel Celeron processor running the Linux Mint 17 operating system.

In parallel, a u-blox GNSS receiver EVK-M8F serves as independent source of C/N0 and Automatic Gain Control (AGC) measurements. The u-blox receiver is controlled by the Intel NUC via a USB port. The Intel NUC is setup for remote access via a hotspot with a mobile broadband connection. Our setup is designed to run on 12 V DC power, thus allowing to directly power the entire setup using a car's DC power output. We wrote a Python software for data collection, RF-front-end power monitoring, and C/N0-based jamming monitoring.

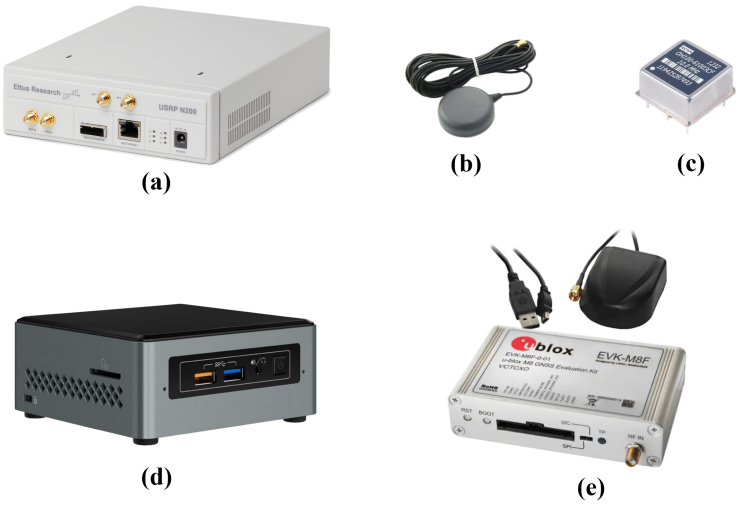

Figure 5: Equipment used for wideband RF data collection: (a) Ettus USRP N200 with DBSRX2 daughterboard, (b) Tallysman GPS Antenna 33-8829NMAT, (c) Connor Winfield ovenized crystal oscillator OCXO-OH100, (d) Intel NUC6, (e) u-blox GNSS receiver EVK-M8F.

2. Preliminary Hardware Validation and Testing

To confirm proper functioning of the hardware components, we run a GPS software receiver that checks if GPS L1 signals can be acquired and tracked for positioning and velocity estimation, as illustrated in Fig. 6. We run the GPS software receiver with every wideband data set presented in this paper.

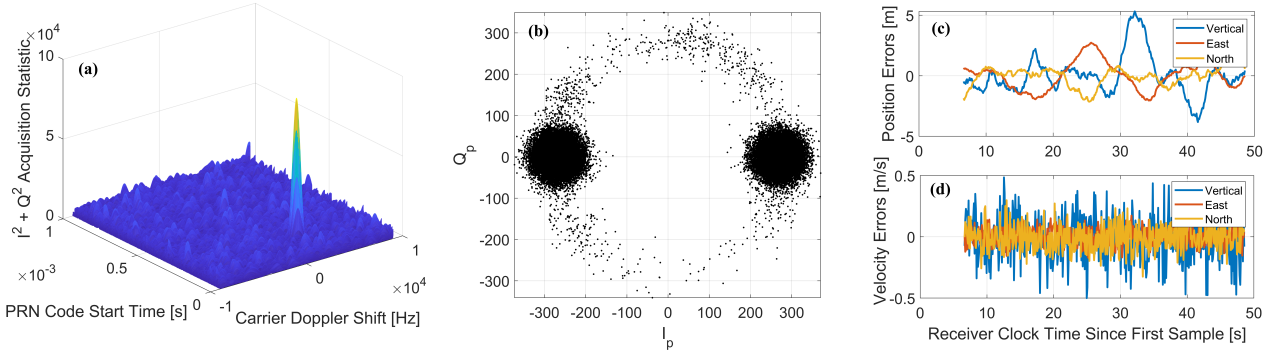

Figure 6: Plots showing GPS software receiver outputs checked when collecting wideband RF data: (a) acquisition, (b) phase-lock loop, (c) positioning error, and (d) velocity error over time.

3. RF-Front-End Signal Power Model

To detect the presence of jamming in wideband RF data, we monitor the RF-front-end signal power. The USRP RF-front-end signal is a stream of ordered pairs of real (in-phase) and imaginary (quadrature) parts of complex-numbered samples at each time step 'n'. We define the RF-front-end signal at time step 'n' as:

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

where $y_{I,n}$, $y_{Q,n}$ 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 every 'N' samples, are defined as:

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

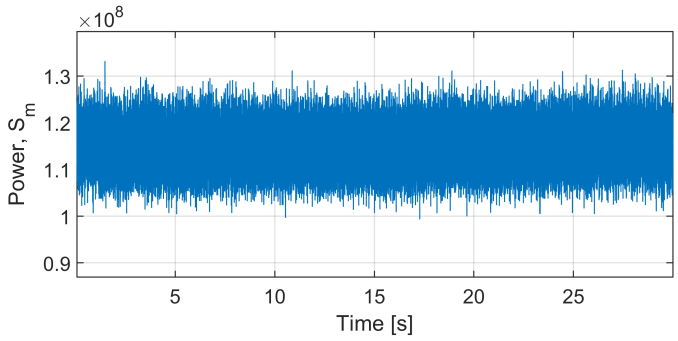

Figure 7: Time-history of RF-front-end signal power.

An example RF-front-end signal power curve over time is shown in Fig. 7. Figure 8 shows the distribution of power measurements under nominal, jam-free conditions on a quantile-to-quantile (Q-Q) plot. The curve shows power data quantiles on the y-axis versus quantiles of a standard normal distribution on the x-axis. If the samples (blue dots) were normally distributed, they would be aligned along a line of slope the sample standard deviation, and of y-intercept the sample mean. Power-samples are almost aligned, i.e., quasi-normally distributed. To robustly model the entire empirical distribution, including the tails, we use a Gaussian overbound (black line) [14] and identify the mean μ_m and variance σ_m^2 of the power measurement model. Thus, the jam-free nominal power is modeled as:

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

When jamming is present, additional signal components impact the RF-front-end signal, which can the be written as:

$$y_{n,jam} \triangleq (y_{I,n} + iy_{Q,n}) + (\psi_{I,n} + i\psi_{Q,n}). \tag{4}$$

where $\psi_{I,n}$ and $\psi_{Q,n}$ are in-phase and quadrature components of the jamming signal in the RF front-end's frequency band. The magnitude squares of $y_{n,jam}$ becomes:

$$|y_{n,jam}|^2 = \left(y_{I,n}^2 + y_{Q,n}^2\right) + \left(\psi_{I,n}^2 + \psi_{Q,n}^2\right) + 2y_{n,I}\psi_{n,I} + 2y_{n,Q}\psi_{n,Q} \tag{5}$$

Assuming that the nominal signal is independent of the jamming signal, we can write:

$$E[y_{n,I}\psi_{n,I}] = E[y_{n,Q}\psi_{n,Q}] = 0 \tag{6}$$

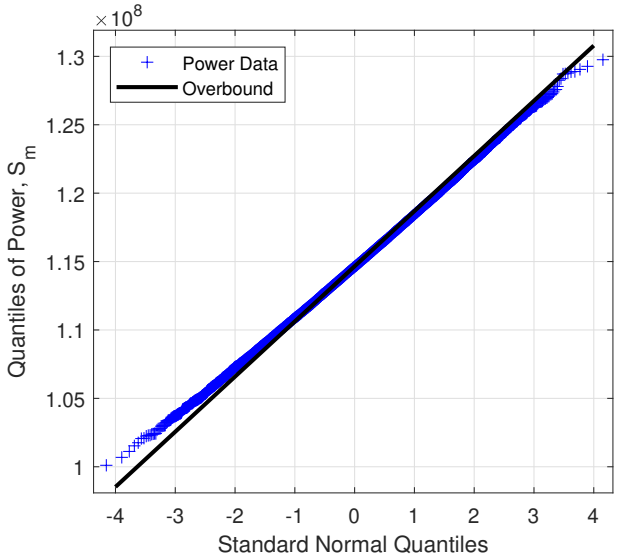

Figure 8: Q-Q plot showing a Gaussian overbound for the RF-front-end signal power.

Thus the RF-front-end signal power under jamming becomes:

$$\begin{aligned} S_m &= \frac{1}{N}\sum_{k=0}^{N-1} |y_{mN+k,jam}|^2 \\ &= \frac{1}{N}\sum_{k=0}^{N-1} \left(y_{I,mN+k}^2 + y_{Q,mN+k}^2\right) + \frac{1}{N}\sum_{k=0}^{N-1} \left(\psi_{I,mN+k}^2 + \psi_{Q,mN+k}^2\right) \\ &= \frac{1}{N}\sum_{k=0}^{N-1} |y_{mN+k}| + \frac{1}{N}\sum_{k=0}^{N-1} \left(\psi_{I,mN+k}^2 + \psi_{Q,mN+k}^2\right) \end{aligned} \tag{7}$$

where the cross-product terms $y_{n,I}\psi_{n,I}$ and $y_{n,Q}\psi_{n,Q}$ are not included because they average out over N samples when N is sufficiently large and under the assumption in Eq. 6. Thus, the jamming power introduced in band can be expressed as:

$$J_m \triangleq \frac{1}{N}\sum_{k=0}^{N-1} \left(\psi_{I,mN+k}^2 + \psi_{Q,mN+k}^2\right) \tag{8}$$

and the power distribution under jamming can be written as:

$$S_m \sim N\left(\mu_m + J_m, \sigma_m^2\right) \tag{9}$$

Fig. 9 shows example in-phase, quadrature, and power samples over time collected in Blacksburg, Virginia, during an interference at GPS L1. The amplitude of the real and imaginary components of the RF-front-end signal increase during the interference. The mean of the power profile shifts at the onset of the interference.

4. Signal Power Monitor Derivation

In Sec. III.3, we derived models of nominal and jammed signal power. We use these models to monitor the RF-front-end signal power monitor, S_m, defined in the Eq. 2. We first define two mutually-exclusive, exhaustive hypotheses of no jamming, H_0, and jamming, H_1, as:

$$\begin{aligned} &\text{Null hypothesis } H_0 : J_m = 0 \text{ (no jamming)} \\ &\text{Alternate hypothesis } H_1 : J_m > 0 \text{ (jamming)} \end{aligned} \tag{10}$$

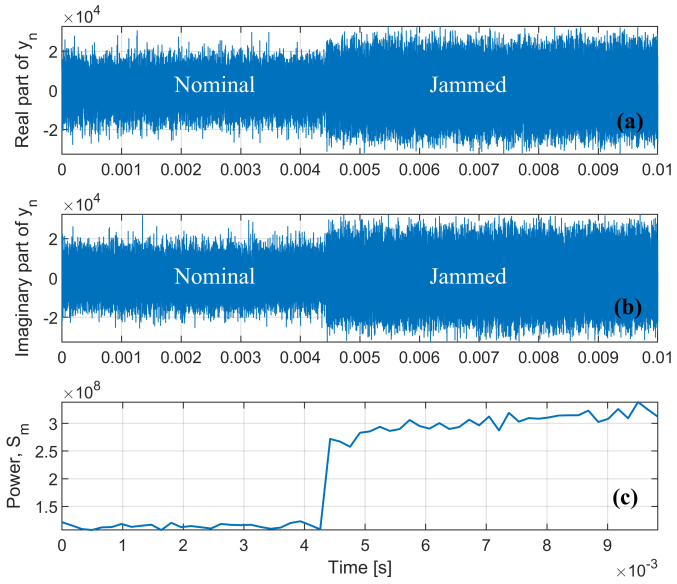

Figure 9: Impact of interference on data collected in Blacksburg, Virginia, in August 2022: (a) for the RF-front-end signal's real part, (b) for the imaginary part, and (c) for the power measurement.

The probability density functions (PDF) of signal power under the two hypotheses can be written as:

$$p\left(S_m|\,H_0\right) = \frac{1}{\sigma_m\sqrt{2\pi}}\; exp\left(-\frac{\left(S_m-\mu_m\right)^2}{2\sigma_m^2}\right)$$
$$p\left(S_m|\,H_1\right) = \frac{1}{\sigma_m\sqrt{2\pi}}\; exp\left(-\frac{\left(S_m-\mu_m-J_m\right)^2}{2\sigma_m^2}\right) \tag{11}$$

We use the Neyman-Pearson lemma to express the test statistic that minimizes the probability of missed detection (P_{MD}) as:

$$\Lambda_m(S_m, J_m) = ln\left(\frac{p\left(S_m|\,H_1\right)}{p\left(S_m|\,H_0\right)}\right) \tag{12}$$

where, $ln()$ is the natural logarithm function. Substituting Eq. 11 into Eq. 12, we can write Λ_m as:

$$\Lambda_m(S_m, J_m) = \frac{-J_m + 2J_m(S_m-\mu_m)}{2\sigma_m^2} \tag{13}$$

Since the jamming power and jammer locations are unknown, the parameter J_m is an unknown arbitrary constant. We can derive the locally most powerful test statistic for small jamming power ($J_m \to 0$) as:

$$\hat{\alpha}_m \triangleq \left.\frac{\partial\Lambda_m(S_m, J_m)}{\partial J_m}\right|_{J_m=0} = \frac{S_m-\mu_m}{\sigma_m^2} \tag{14}$$

Under H_0, the test statistic $\hat{\alpha}_m$ has the following distribution: $\hat{\alpha}_m \sim N(0, 1/\sigma_m^2)$. We define a normalized test statistic as:

$$\alpha_m \triangleq \hat{\alpha}_m\sigma_m = \frac{S_m-\mu_m}{\sigma_m} \;\text{ such that }\; \alpha_m \sim N(0,1) \tag{15}$$

The detection threshold T_m is set to meet a predefined requirement on the probability of false alert $P_{FA,REQ}$. T_m is determined

using the following equation:

$$P_{FA,REQ} = P(\alpha_m > T_m|H_0) \text{ i.e., } T_m = Q^{-1}(P_{FA,REQ}) \tag{16}$$

where $Q^{-1}()$ is the inverse tail probability of the standard normal distribution.

IV. TIME-FREQUENCY WIDEBAND DATA ANALYSIS DURING DETECTED INTERFERENCE AT GPS L1

In this section, we analyze the power-based detector derived in Sec. III.4 and further characterize jamming events using time-frequency representations.

1. Data Collection and Processing of Wideband RF Data at a Location in Southwestern Virginia

We first analyze data collected in the GPS L1 band at three locations along Route-460 in Blacksburg, Virginia. Route-460 is a major highway connecting Kentucky to Eastern Virginia. The locations of the three receivers are shown in Fig. 10. The data was collected in the GPS L1 band at a 6.25 MHz sampling rate. The wideband RF data was first processed using our GPS software receiver to confirm acquisition and tracking of GPS signals. In parallel, we used the signal monitor to find increases in signal power .

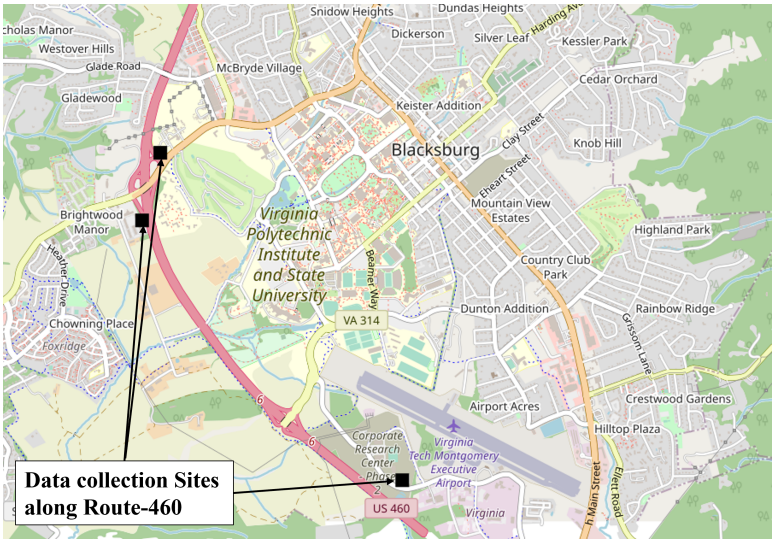

Figure 10: Map showing data collection sites near Blacksburg, VA.

Fig. 11 shows example power peaks found in the data. The plot represents the ratio of the power monitor's test statistic over its detection threshold. Detection is declared When this ratio exceeds 1.

We further analyze the power peaks using time-frequency analysis to identify the source of interference. The time-frequency analysis aims at visualizing the time variations of a signal's PSD. A time-frequency plot, or spectrogram, is generated by computing the magnitude of the signal's Fast Fourier Transform (FFT) in a window, and then sliding that window to generate a 2-D plot with time on the x-axis, frequency on the y-axis, and color-coded PSD on the z-axis.

Fig. 12 is a spectrogram capturing the start of the first power peak in Fig. 11. The 50-μs pulses alternating between two frequencies (0.56 MHz and 0.22 MHz below GPS L1) are consistent with a Binary Frequency Shift Keying (BFSK) signal broadcast. The regular frequency shifts at the start of a power peak even seem to indicate a communication message preamble. To confirm that this signal actually exists at the GPS L1 frequency, we must verify that it is not an alias of an out-of-band signal.

2. Verifying that the PSD Pulses are not Aliases of Out-of-band Signals

In May 2022, to check that the signal in Fig. 12 is not an alias of an out-of-band signal, we collected data at a same location using two different Ettus N200 USRPs, two independent OCXOs, two different antennas, and two different sampling rates. We used the GPS software receiver to synchronize the two data sets by identifying the navigation message' sub-frame start times. This method of synchronization achieves sub-millisecond timing accuracy.

In Fig. 13, the synchronized power plots of the May 2022 data show peaks occurring at same time at both USRPs. In addition,

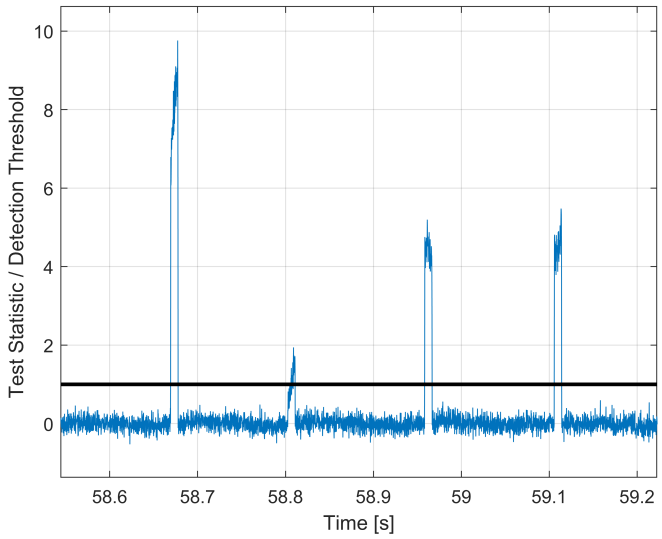

Figure 11: Power peak events detected by the signal power monitor at data collection sites.

the spectrograms in Fig. 14 correspond to the power peaks shown in Fig. 13. They show the same BFSK signal recorded at both USRPs. The PSD peaks occur at same frequencies as shown in Fig. 15. They also match the frequencies of PSD peaks in Fig. 12, which were recorded a few days earlier. If the signals were aliased in, the PSD peaks should appear at different frequencies. This BPSK signal actually is near GPS L1.

To further confirm this finding, we collected additional data at the same location in August 2022. We used the same equipment. To guarantee the signal was not aliased, the USRP settings were modified to a different center frequency: GPS L1 + 0.5 MHz, i.e., 1575.92 MHz. If the BFSK signal was aliased, the pulses would be shifted to another frequency. But Fig. 16 shows that the pulses occur at the same frequency as in the May 2022 data, thus definitely proving that the BFSK signal is not aliased in. In the process, we have also shown that the BPSK was recurring over several months. Figures 14 and 16 seem to support that the BPSK is a communication signal with a constant preamble of regular pulses followed by a data stream.

3. Analysis of PPD Jamming Observed on Interstate I-25 in Colorado

The pattern in Fig. 4 motivated us to collect wideband RF data on Colorado highways. Fig. 17 shows an example power peak and spectrogram for data collected on Interstate I-25 on the outskirts of Denver, Colorado, at location 39°30'54.9"N 104°52'06.3"W on September 21, 2022 at 8:03 AM local time. The spectrogram on the right-hand-side is generated using a 20-sample sliding hamming window. This data was collected at a 25 MHz sampling rate with a center frequency at GPS L1. The power increase lasted about 5 seconds, which is consistent with crossing path with a vehicle carrying a PPD. The time-frequency analysis of the signal during the power peak leaves little doubt as to the nature of the interference. Repeated sweeps of peak power density are typical of chirp jammers [11].

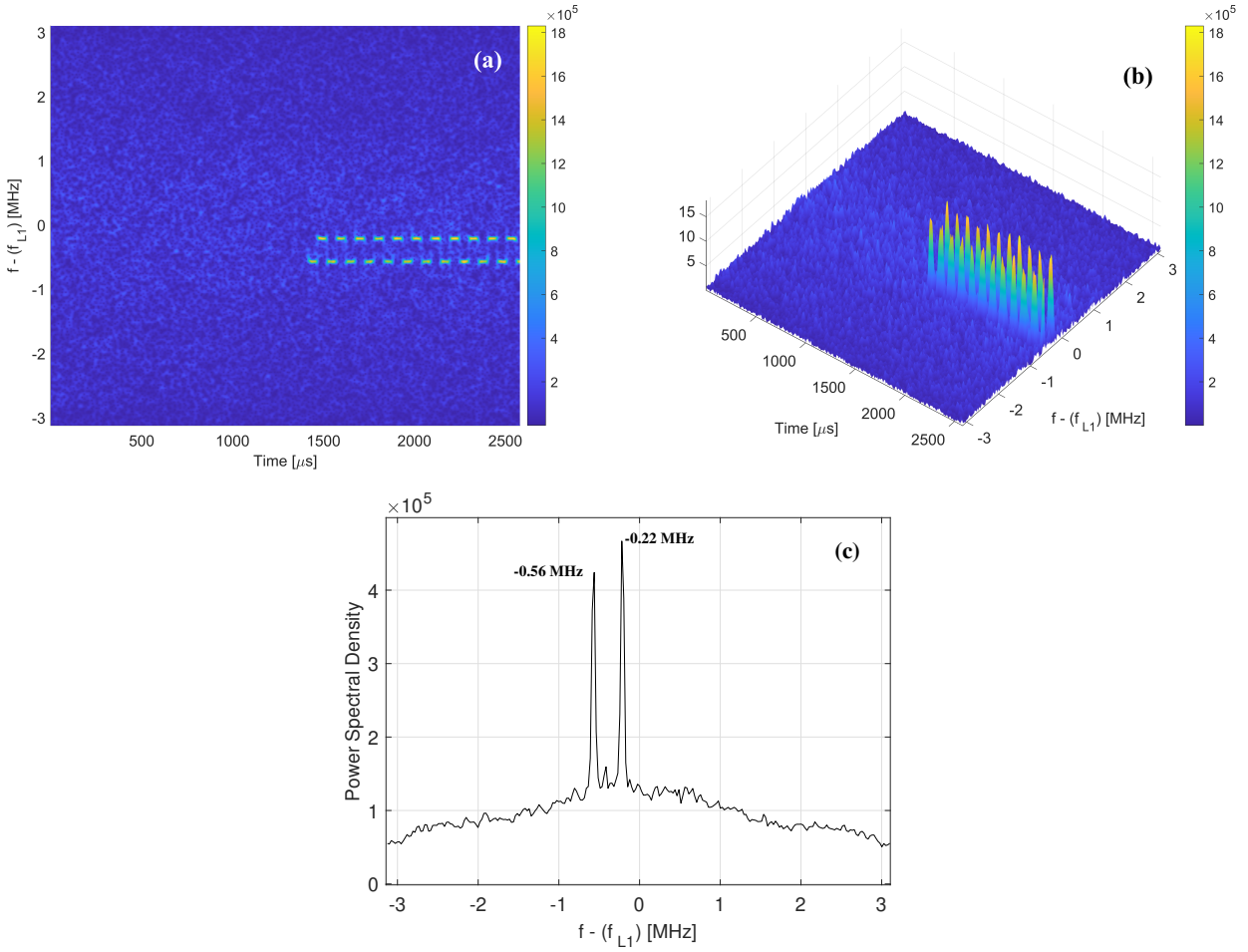

Figure 12: Time-frequency analysis of the power peaks in Fig. 11: (a) spectrogram of RF-front-end signal during power peak, (b) isometric view of the spectrogram showing 50 μs pulses, and (c) PSD estimate computed by averaging the spectrogram's PSD values over time.

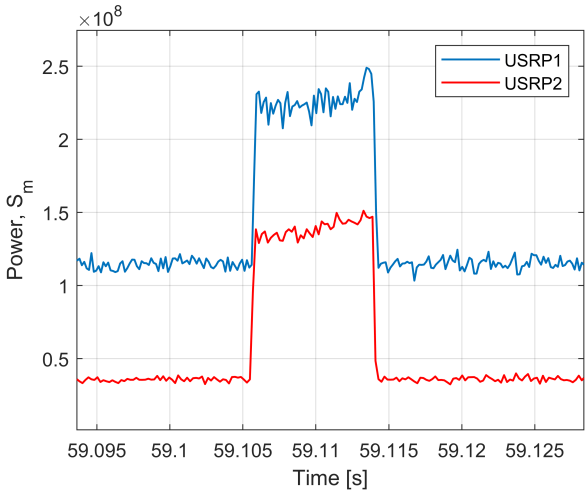

Figure 13: Time-sequences of synchronized RF-front-end signal power showing peaks at two different collocated USRPs in May 2022.

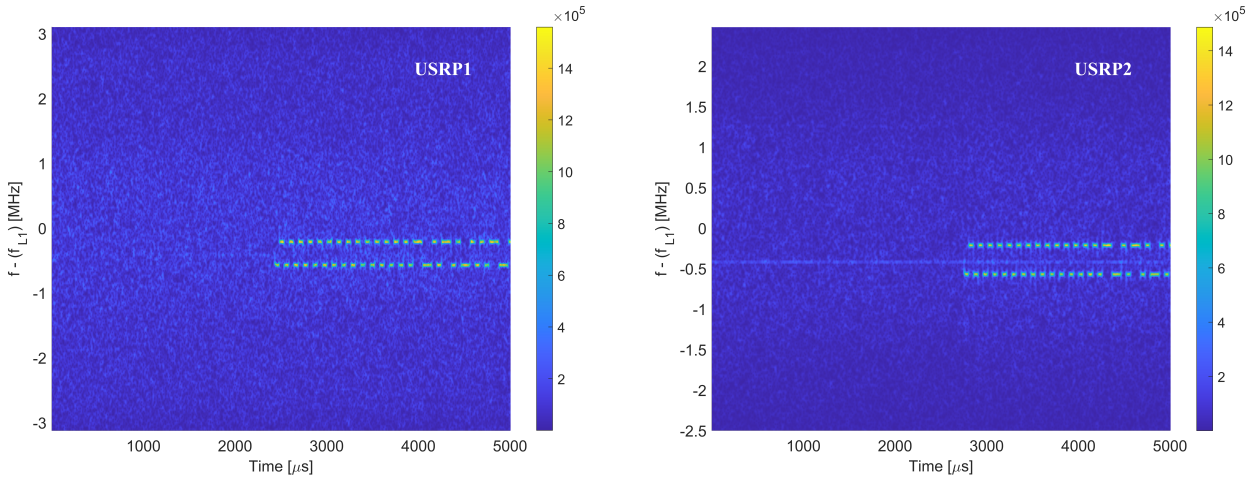

Figure 14: Spectrograms of the May 2022 power peaks showing the same BFSK signals in both USRPs. USRP1 was sampling at 6.25 MHz and USRP2 was sampling at 5 MHz.

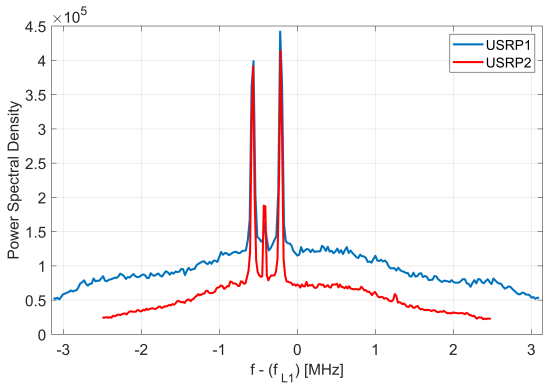

Figure 15: Average PSDs from spectrograms in Fig. 14 showing peak power concentrations at the same frequencies, also matching those observed a few days earlier in Fig. 12.

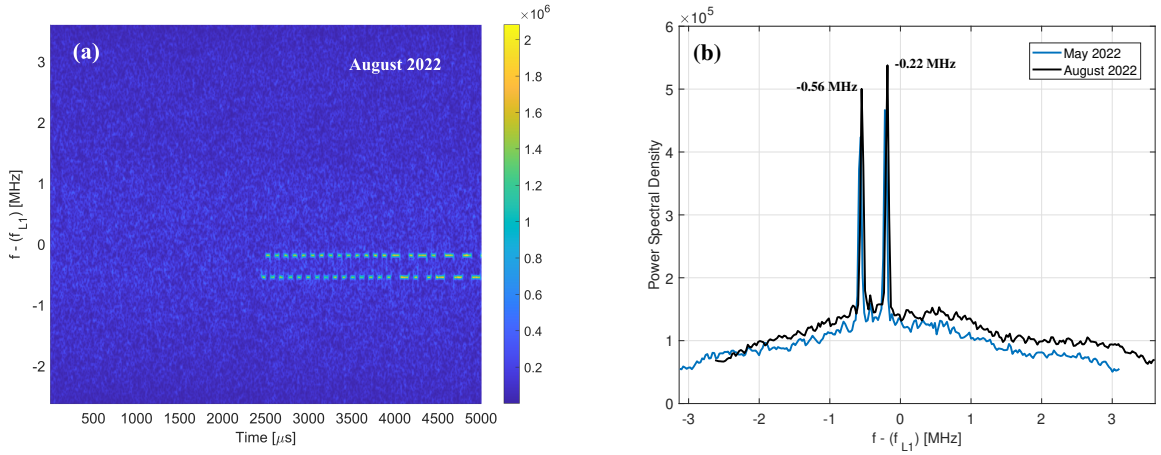

Figure 16: BFSK signal observed in August 2022. (a) Spectrogram of RF-front-end data with BPSK pulses similar to those observed in May 2022 in Fig. 14). (b) PSD comparison for data collected in May 2022 and in August 2022.

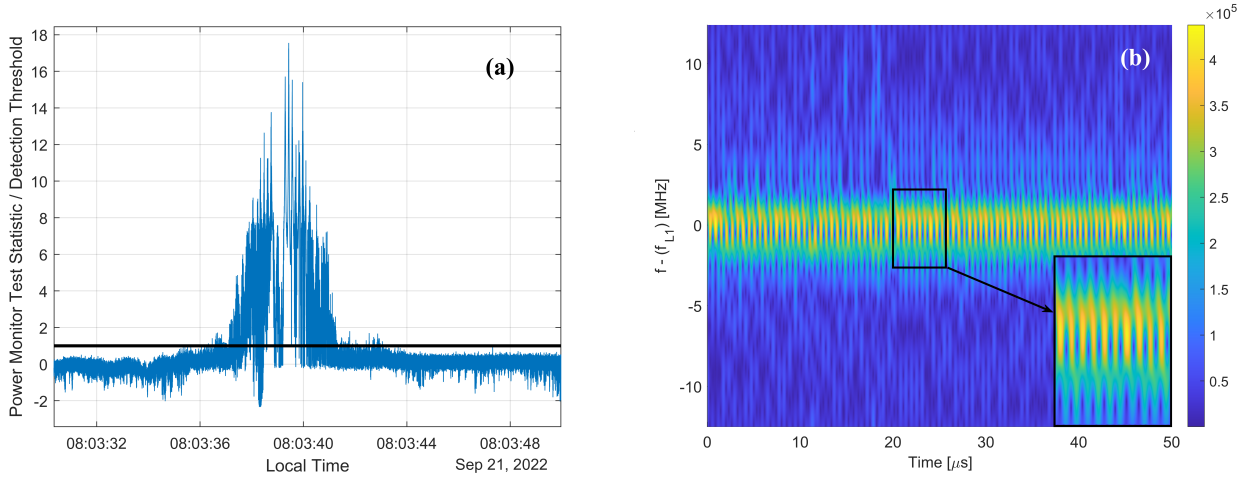

Figure 17: Time-frequency analysis of PPD jamming signal: (a) Signal power monitor output, and (b) Spectrogram showing sweeps in peak PSD.

We also analyzed the PPD's impact on C/N0 and Automatic Gain Control (AGC), which are often used as jamming indicators [10]. The left-hand-side plot in Fig. 18 shows the u-blox receiver C/N0 dropping during the PPD jamming event. The right-hand-side plot shows the u-blox AGC, which suddenly drops. The AGC gain is a factor applied to the RF-front-end samples to prevent saturation of the signal when the receiver operates in an environment with higher-than-usual in-band power. In Fig. 18 the drop in AGC is the receiver's reaction to the extra in-band power introduced by the jammer.

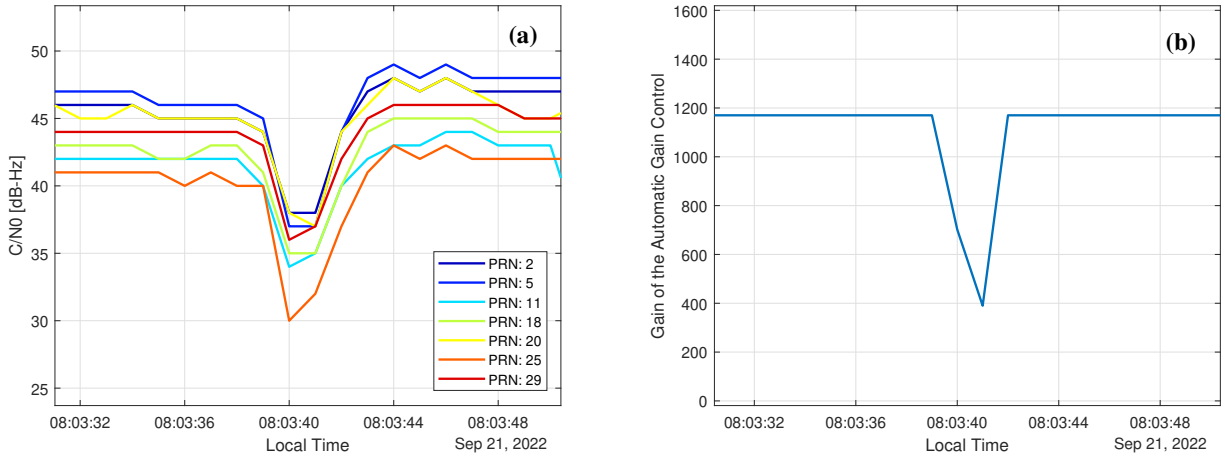

Figure 18: Off-the-shelf receiver signal quality indicators collected during the PPD jamming event observed in Colorado: (a) C/N0, and (b) AGC.

V. CONCLUSIONS

In this paper, we implemented C/N0-based jamming detectors over a network of 900 receivers, and over an eight-month-long time-period at two specific locations. We found patterns of events that are consistent with the daily commute of a driver carrying a personal privacy device (PPD). To further validate these findings, we designed a wideband RF data collection setup, and a sensitive signal power monitor. We collected both RF data and off-the-shelf GNSS receiver C/N0 data along U.S. highways in Virginia and Colorado. The time-frequency analysis of this data showed that the observed GPS L1 interference came from PPDs and from other recurring, unidentified communication signal broadcasts.

REFERENCES

[1] "Above us only stars," C4ADS (non-profit organization), Tech. Rep., 2019, Accessed on: December 13, 2020. [Online]. Available: https://www.c4reports.org/aboveusonlystars

[2] M. Brunker, "GPS under attack as crooks, rogue workers wage electronic war," News Brief at NBC, August 2016, Accessed on: January 10, 2022. [Online]. Available: https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761

[3] Federal Bureau of Investigation, "Cargo thieves use GPS jammers to mask GPS trackers," FBI Cyber Division Bulletin, December 2014, Accessed on: January 10, 2022. [Online]. Available: https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/

[4] S. Jada, M. Psiaki, S. Landerkin, S. Langel, A. Scholz, and M. Joerger, "Evaluation of PNT situational awareness algorithms and methods," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 2021, pp. 816–833.

[5] L. Scott, "J911: The case for fast jammer detection and location using crowdsourcing approaches," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2011, pp. 1931–1940.

[6] H.-P. Kim, G.-G. Jin, and J.-H. Won, "GNSS cloud-data processing technique for jamming detection, identification, and localisation," *IET Radar, Sonar & Navigation*, vol. 14, no. 8, pp. 1143–1149, 2020.

[7] D. Miralles, N. Levigne, D. M. Akos, J. Blanch, and S. Lo, "Android raw GNSS measurements as the new anti-spoofing and anti-jamming solution," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 334–344.

[8] L. Strizic, D. M. Akos, and S. Lo, "Crowdsourcing GNSS jammer detection and localization," in *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, 2018, pp. 626–641.

[9] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *2015 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2015, pp. 1–6.

[10] N. S. Levigne, "Automatic gain control measurements as a GPS L1 interference detection metric," Master's thesis, University of Colorado at Boulder, 2019.

[11] R. H. Mitch, "Model-based estimation techniques applied to Global Navigation Satellite System jammers," Ph.D. dissertation, Cornell University, 2014.

[12] 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.

[13] 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.

[14] B. DeCleene, "Defining pseudorange integrity-overbounding," in *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, 2000, pp. 1916–1924.