Received: 26 April 2023 | Revised: 6 June 2023 | Accepted: 6 June 2023

DOI: 10.1109/xxx.xx.xxxx

REGULAR PAPERS

Network-Based GNSS Jamming Prediction Enabling Wideband Interference Observation

Sandeep Jada | **Mark Psiaki** | **Mathieu Joerger***

[1]Kevin T. Crofton Department of Aerospace and Ocean Engineering, Virginia Tech, Virginia, USA

Correspondence

*Mathieu Joerger, This is sample corresponding address.
Email: joerger@vt.edu

Abstract

In this paper, we develop and evaluate autonomous, self-calibrating, receiver-independent C/N0-based jamming detection algorithms capable of processing data from large receiver networks. The algorithm uses optimal detectors that target a predefined false alert rate. Using this algorithm, we processed 8 months of data from hundreds of receivers and identified patterns in jamming detection consistent with intentional interference, providing an opportunity to validate the C/N0 detector. We design a portable experimental RF data collection setup and develop an optimal power-based jamming monitor to independently detect jamming. With this setup, we detected a genuine jamming event while driving on I-25 in Colorado, USA, and validated the C/N0-based detector through time-frequency analysis of wideband RF data from the event.

Keywords

GNSS jamming detection, Neyman-Pearson test, Time-frequency analysis, PNT situational awareness

1 | INTRODUCTION

In this paper, we develop a method to detect, predict, and observe recurring GNSS jamming events caused by motorists on daily or weekly schedules. We first design and implement an autonomous, self-calibrating algorithm to detect jamming using carrier-to-noise-density ratio (C/N0) data from networks of hundreds of heterogeneous receivers. The detector is evaluated with respect to both its high sensitivity to low-power jammers and its robustness to false alerts. The detector offers GNSS jamming prediction capability that is validated through time-frequency analysis of wideband radio frequency (RF) data collected during an interference event that we anticipated on a U.S. highway.

Over the past decade, radio frequency interference (RFI), such as GNSS jamming and spoofing, has been a growing threat to critical infrastructure that depends on positioning, navigation, and timing (PNT) (C4ADS, 2019; The White House, 2020, 2021). Wide-area jamming is observed in conflict areas (Wu, Dong L., 2024), and has occurred in the US causing major air traffic disruptions (Dacus et al., 2022; Joerger et al., 2023). A more widely spread source of localized GNSS jamming includes easily acquirable and low-cost personal privacy devices (PPDs) (Federal Bureau of Investigation, 2014; M. Brunker, 2016).

To mitigate RFI, the methods by Hegarty et al. (2019), Mitch (2014), Mosavi et al. (2017), and Wesson et al. (2017) use sophisticated and data-intensive signal processing techniques that require dedicated hardware, which would be too expensive for wide-scale deployment.

Jamming detection can also be implemented using off-the-shelf GNSS receiver outputs including C/N0 and automatic gain control (AGC) (Kim et al., 2020; Levigne, 2019; Miralles et al., 2018; Scott, 2011; Strizic et al., 2018; Weston et al., 2010). C/N0-based jamming detectors using fixed detection thresholds are derived by Borio and Gioia (2015) and Fors et al. (2021). However, these C/N0 methods are insufficient when using hundreds of receivers and antennas of different ages, brands, and models such as those of the National Geodetic Survey's (NGS) continuously operating reference stations (CORS) and of the International GNSS Service (IGS). Manually setting thresholds on C/N0 measurements with time-varying distributions is not a viable approach.

In response, in this paper, we develop a self-calibrating GPS L1 C/N0-based jamming monitor that is equipment agnostic. We implement this algorithm using months of data at 900 CORS and IGS receiver locations to identify daily-repeating jamming. We then deploy our own equipment with a power-based detector to capture wideband data during an example predicted RFI event, thereby validating the C/N0 monitor and the jamming prediction idea.

The C/N0 monitoring and validation algorithms are designed to minimize the risks of missed detection while limiting the risks of false alerts. First, we derive locally Neyman-Pearson optimal detection tests, which minimize the probability of missed detection of small jamming signal power density. We provide three detectors using C/N0 measurements, time-differenced C/N0, and uncalibrated RF front-end signal power measurements. Second, to limit the risk of false alerts, we develop an automated, high-fidelity nominal C/N0 modeling methodology. Overbounding theory is leveraged to robustly model C/N0 variations, including at small quantiles (Blanch et al., 2017; DeCleene, 2000; Rife et al., 2006). The parametric error models account for individual receiver and satellite equipment and locations.

We implemented the C/N0-based algorithms using data from 900 CORS receivers over eight months in 2022. We identified daily recurring patterns to predict jamming events at specific locations. To further analyze such events, we built a deployable wideband data collection device with a power monitor that triggers recording and storage. We leveraged this equipment to observe a predicted RFI "in the wild" on a highway in Colorado. The RF front-end signal's time-frequency spectrogram analyses show peak power density variations consistent with those of a chirp jammer (Diez et al., 2022; Kraus et al., 2011; Mitch et al., 2011), which validates the network-based C/N0 jamming prediction method.

This article is organized as follows. In Section 2, we derive optimal hypothesis tests for C/N0 and RF front-end power-based jamming detection. In Section 3, we develop the nominal C/N0 measurement modeling methods. In Section 4, we implement and evaluate the C/N0-based jamming monitor using months of data from large receiver networks. Section 5 describes the detector validation through wideband RF data analysis capturing the signal of a PPD jammer. Section 6 provides concluding remarks.

2 | DERIVATION OF C/N0-BASED AND POWER-BASED GNSS JAMMING DETECTORS

In this section, we derive three methods to detect the presence of jamming using C/N0, using time-differenced C/N0, and using RF front-end power measurements. We also determine the theoretical probability distributions of the three detection test statistics. These distributions will be validated and their parameters evaluated using data in Section 3.

2.1 | C/N0 Test for GNSS Jamming Detection

This section shows that the instantaneous, one-sided, Neyman-Pearson-optimal test that minimizes missed-detection of small increases in jamming power density is the sum over all satellites of the differences between measured and mean C/N0 weighted by the inverse of their C/N0 measurement variance. The offline, a priori, data-based evaluation of the mean and variance of C/N0 measurements is described in Section 3.

Let $C_{i,k}$ be the received signal power (in watts) from GNSS satellite i, at time-step k. Let N_0 be the noise power density in watts per hertz (W/Hz). Let $c_{i,k}$ be the receiver-provided carrier-to-noise-density ratio (C/N0) estimate in $dB-Hz$ for the i^{th} satellite at time-step k. Under jamming-free conditions (hypothesis H_0), we model $c_{i,k}$ using a Gaussian overbounding distribution with mean $\mu_{i,k}$ and variance $\sigma^2_{i,k}$. The modeling procedure in Section 3.1 describes the Gaussian overbounding process. Gaussian overbounding of C/N0 measurements is consistent with (and a possible refinement over) the Gaussian models used by Murrian et al. (2019) and Wesson et al. (2017). Under H_0, $c_{i,k}$ is expressed as:

$$c_{i,k} = \left(\frac{C_{i,k}}{N_0}\right)_{dB-Hz} \sim N(\mu_{i,k}, \sigma^2_{i,k}). \tag{1}$$

where, for a C/N0 X, we define $(X)_{dB-Hz} = 10log_{10}(X)$. In the presence of jamming (hypothesis H_1), the jamming power density J_k (in W/Hz) adds to N_0 on the denominator, thus degrading the C/N0 for all the satellites in view. J_k is the received jamming power at time step k divided by the bandwidth of the RF front-end. Under H_1, the C/N0 is written as:

$$c_{i,k} = \left(\frac{C_{i,k}}{N_0 + J_k}\right)_{dB-Hz} = \left(\frac{C_{i,k}}{N_0}\right)_{dB-Hz} - \gamma_k \tag{2}$$

where we used the notation: $\gamma_k \triangleq (1 + J_k/N_0)_{dB-Hz}$. Parameter γ_k varies with J_k; it is the ratio of the noise power densities with and without jamming $((N_0 + J_k)/N_0)$ in decibels. Under H_1, $c_{i,k}$ is distributed as follows:

$$c_{i,k} \sim N(\mu_{i,k} - \gamma_k, \sigma^2_{i,k}) \tag{3}$$

The parameter γ_k is the drop in mean C/N0 due to jamming. We want to derive a test to detect jamming using the estimated C/N0 for all satellites in view at time k. We first define an observation vector of receiver provided C/N0s at time step k:

$$\boldsymbol{c}_k = [c_{1,k}, \ldots, c_{r,k}]^T \tag{4}$$

where r is the number of satellites in view at time k. C/N0 measurements are assumed to be uncorrelated across satellites. We define two mutually exclusive and exhaustive hypotheses, H_0 and H_1, which impact Equation (2), as follows:

$$\begin{gathered} \text{Null hypothesis } H_0 : \gamma_k = 0 \text{ (no jamming)} \\ \text{Alternate hypothesis } H_1 : \gamma_k > 0 \text{ (jamming)} \end{gathered} \tag{5}$$

The probability density functions (PDF) of the C/N0 vector $\boldsymbol{c}_k$ under these two hypotheses can respectively be written as:

$$p\left(\boldsymbol{c}_k \middle| H_0\right) = \frac{1}{\sqrt{(2\pi)^r |\boldsymbol{S}_k|}} \, exp\left(-\frac{1}{2}(\boldsymbol{c}_k - \boldsymbol{\mu}_k)^T \boldsymbol{S}_k^{-1} (\boldsymbol{c}_k - \boldsymbol{\mu}_k)\right) \tag{6}$$

$$p\left(\boldsymbol{c}_k \middle| H_1\right) = \frac{1}{\sqrt{(2\pi)^r |\boldsymbol{S}_k|}} \, exp\left(-\frac{1}{2}(\boldsymbol{c}_k - \boldsymbol{\mu}_k + \mathbf{1}\gamma_k)^T \boldsymbol{S}_k^{-1} (\boldsymbol{c}_k - \boldsymbol{\mu}_k + \mathbf{1}\gamma_k)\right) \tag{7}$$

where $\boldsymbol{\mu}_k \triangleq [\mu_{1,k}, \ldots, \mu_{r,k}]^T \in \mathbb{R}^{r\times 1}$ and $\boldsymbol{S}_k \triangleq diag\left(\left[\sigma^2_{1,k}, \ldots, \sigma^2_{r,k}\right]\right) \in \mathbb{R}^{r\times r}$ are the jam-free mean and covariance of the observation vector, $\boldsymbol{c}_k$, and $\mathbf{1} = [1, \ldots, 1]^T$ is an $r \times 1$ vector of ones. We use the Neyman-Pearson lemma to write the following optimal test statistic, which minimizes the probability of missed detection (P_{MD}):

$$\Lambda_k(\boldsymbol{c}_k, \gamma_k) = ln\left(\frac{p\left(\boldsymbol{c}_k \middle| H_1\right)}{p\left(\boldsymbol{c}_k \middle| H_0\right)}\right) \tag{8}$$

where $ln()$ is the natural logarithm function. Substituting Equations (6) and (7) into Equation (8) and simplifying, we obtain the following equation for the test statistic:

$$\Lambda_k(\boldsymbol{c}_k, \gamma_k) = -(\boldsymbol{c}_k - \boldsymbol{\mu}_k)^T \boldsymbol{S}_k^{-1} \mathbf{1}\gamma_k - \frac{1}{2}\mathbf{1}^T \boldsymbol{S}_k^{-1} \mathbf{1}\gamma_k^2 \tag{9}$$

Parameter γ_k is unknown because the received jamming power is unknown (it depends on the transmitted jamming power, antenna gain patterns, distance to the jamming source, propagation channel path loss, etc.). Still, we can express a locally optimal test statistic for small jamming power ($\gamma_k \to 0$) as:

$$\alpha_k \triangleq \left.\frac{\partial \Lambda_k(\boldsymbol{c}_k, \gamma_k)}{\partial \gamma_k}\right|_{\gamma_k = 0} = -(\boldsymbol{c}_k - \boldsymbol{\mu}_k)^T \boldsymbol{S}_k^{-1} \mathbf{1} \tag{10}$$

Under H_0, the test statistic α_k is distributed as follows:

$$\alpha_k \sim N\left(0, \sigma^2_{\alpha,k} \triangleq \mathbf{1}^T \boldsymbol{S}_k^{-1} \mathbf{1}\right) \tag{11}$$

Let T_k be the detection threshold for the test. Detection occurs if the following inequality is satisfied:

$$\alpha_k > T_k \tag{12}$$

We set T_k to meet a predefined requirement on the probability of false alert $P_{FA,REQ}$. T_k is computed using the following equation:

$$P_{FA,REQ} = P(\alpha_k > T_k | H_0), \quad \text{i.e.,} \quad T_k = Q(1 - P_{FA,REQ})\, \sigma_{\alpha,k} \tag{13}$$

where $Q(\,)$ is the quantile function, i.e., the inverse cumulative distribution function (CDF) of the standard normal distribution.

This test is optimal for detecting small, simultaneous drops in C/N0. We designed the test to be one-sided because we focus on degradation in C/N0 due to jamming. The test can easily be modified to be two-sided, e.g., to detect increased C/N0 due to spoofing, by applying an absolute value operator to α_k in Equations (12) and (13) and by dividing $P_{FA,REQ}$ by two (2) in Equation (13) to account for both tails of the jam-free distribution.

The method could also be extended to account for C/N0 drops on satellite subsets by considering additional hypotheses that do not fit under nominal conditions H_0 and jammed conditions H_1. As described by Jada et al. (2021), we carried out a side analysis showing that the test was robust to non-nominal C/N0 variations on satellite subsets caused by higher-than-usual ionospheric activity. Detailed treatment of C/N0 drops on satellite subsets is beyond the scope of this paper and will be addressed in future work.

The computation of the test statistic α_k and its threshold T_k requires a jamming-free model of the mean C/N0 vector, $\boldsymbol{\mu}_k$, and covariance matrix, $\boldsymbol{S}_k$. We develop an automated data-based approach for modeling the mean and variance of nominal C/N0 for any receiver and satellite in Section 3.

2.2 | Time-Differenced C/N0 Test for Jamming Detection

In contrast with the method described in Section 2.1, jamming detection using time-differenced C/N0 only requires a variance model because time-differencing C/N0 over short time intervals (e.g., over one second) eliminates the C/N0's slow varying mean value. The time-differenced test is useful when processing data for which the mean C/N0 model is yet to be identified.

A time-differenced C/N0 measurement, $\Delta c_{i,k}$, is defined as follows under jamming:

$$\Delta c_{i,k} \triangleq \left(\frac{C_{i,k}}{N_0 + J_k}\right)_{dB-Hz} - \left(\frac{C_{i,k-1}}{N_0 + J_{k-1}}\right)_{dB-Hz} \tag{14}$$

Substituting Equation (2) into (14) and rearranging gives the following expression:

$$\Delta c_{i,k} = \left(\frac{C_{i,k}}{N_0}\right)_{dB-Hz} - \left(\frac{C_{i,k-1}}{N_0}\right)_{dB-Hz} - \Delta\gamma_k \tag{15}$$

where $\Delta\gamma_k$ is defined as: $\Delta\gamma_k \triangleq (\gamma_k - \gamma_{k-1})$. $\Delta\gamma_k$ captures the impact of jamming power variations from time $k-1$ to k. The distribution of $\Delta c_{i,k}$ can be expressed as follows:

$$\Delta c_{i,k} \sim N(-\Delta\gamma_k, \sigma^2_{\Delta i,k}) \tag{16}$$

We model the overbounding Gaussian function's variance $\sigma^2_{\Delta i,k}$ based on data using the method described in Section 3 and the mean of $\Delta c_{i,k}$ is $-\Delta\gamma_k$ because $(\mu_{i,k} - \mu_{i,k-1} \approx 0)$. We want to derive a test to detect jamming signals from time-differenced C/N0s for all r satellites in view at time-step k. We define the observation vector as follows:

$$\boldsymbol{\Delta c}_k \triangleq \boldsymbol{c}_k - \boldsymbol{c}_{k-1} = [\Delta c_{1,k}, \ldots, \Delta c_{r,k}]^T \tag{17}$$

For any two satellites i and j, $\Delta c_{i,k}$ is assumed to be statistically uncorrelated from $\Delta c_{j,k}$. We define two mutually exclusive and exhaustive hypotheses, H_0 and H_1, which impact Equation (15), as follows:

$$\begin{aligned} &\text{Null hypothesis } H_0 : \Delta\gamma_k = 0 \text{ (no change in jamming power density)} \\ &\text{Alternate hypothesis } H_1 : \Delta\gamma_k > 0 \text{ (increase in jamming power density)} \end{aligned} \tag{18}$$

Following the same steps as in Section 2.1, we derive a locally optimal test statistic for $\Delta\gamma_k \to 0$, which is expressed as follows:

$$\beta_k \triangleq -\boldsymbol{\Delta c}_k^T \boldsymbol{S}_{\Delta k}^{-1} \mathbf{1} \tag{19}$$

Under H_0, the test statistic β_k is distributed as follows:

$$\beta_k \sim N\left(0, \sigma^2_{\beta,k} \triangleq \mathbf{1}^T \boldsymbol{S}_{\Delta k}^{-1} \mathbf{1}\right) \tag{20}$$

This test statistic is optimal for detecting small simultaneous drops in time-differenced C/N0 across satellites. The computation of β_k requires a model for the jam-free time-differenced C/N0 covariance matrix $\boldsymbol{S}_{\Delta k}$, which can be modeled a priori using C/N0 data as described in Section 3. The detection threshold for this test is the product of the quantile function evaluated at $(1 - P_{FA,REQ})$ times $\sigma_{\beta,k}$.

2.3 | RF-Front-End Signal Power Model

Increased temperature and sun exposure can cause the C/N0 to drop for all satellites as the noise density N_0 increases (Kriezis et al. (2024)). Nominal daily variations are captured by the model described in Section 3. Other sources of jamming-unrelated drops in nominal C/N0 at network receivers include ionospheric disturbances, multipath due to moving objects near the antenna, etc. Some reports by Fors et al. (2021) and Lewis (2023) even attribute C/N0 drops to snow accumulation and bird landings on antennas. Although such disturbances are rare and only impact a subset of satellite C/N0 measurements, they can be a source of false alerts. To confirm the presence of jamming, in Sections 4 and 5, we develop a method to identify and predict repeated jamming events, deploy our own equipment, and record RF front-end data when triggered by a power-based detector.

In this section, we design an RF front-end signal power monitor to detect jamming independently of the C/N0-based detectors. The digitized RF front-end signal is a stream of pairs of real (in-phase), $y_{I,n}$, and imaginary (quadrature), $y_{Q,n}$, parts of complex-numbered samples at each RF front-end time index 'n' defined as follows:

$$y_n \triangleq y_{I,n} + iy_{Q,n} \in \mathbb{C} \tag{21}$$

where i is the imaginary unit. Let m be a time index for power measurements. We compute the signal power for the m^{th} non-overlapping window of 'N' samples, $\{y_{mN}, \ldots, y_{mN+N-1}\}$, as follows:

$$s_m \triangleq \frac{1}{N}\sum_{l=0}^{N-1} |y_{mN+l}|^2 \in \mathbb{R} \tag{22}$$

For an RF-front-end sampling at 25 MHz, we can choose a window of $N = 4096$ to give about 6000 power measurements per second. Under jamming-free, nominal conditions, the power measurement can be overbounded by a Gaussian distribution, which is expressed as follows:

$$s_m \sim N\left(\mu_{s,m}, \sigma^2_{s,m}\right) \tag{23}$$

This assumption is justified using data in Section 3.4.

Under jamming, the RF front-end signal at the RF front-end time index n includes additional components defined as follows:

$$y_{n,jam} \triangleq (y_{I,n} + iy_{Q,n}) + (\psi_{I,n} + i\psi_{Q,n}) \tag{24}$$

where $\psi_{I,n}$ and $\psi_{Q,n}$ are the in-phase and quadrature components of the jamming signal. To express the signal power under jamming, we first expand the magnitude squares of $y_{n,jam}$ as follows:

$$|y_{n,jam}|^2 = \left(y^2_{I,n} + y^2_{Q,n}\right) + \left(\psi^2_{I,n} + \psi^2_{Q,n}\right) + 2y_{n,I}\psi_{n,I} + 2y_{n,Q}\psi_{n,Q} \tag{25}$$

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

$$E[y_{n,I}\psi_{n,I}] = 0 \quad \text{and} \quad E[y_{n,Q}\psi_{n,Q}] = 0 \tag{26}$$

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

$$\begin{aligned} s_m &= \frac{1}{N}\sum_{l=0}^{N-1} |y_{mN+l,jam}|^2 \\ &= \frac{1}{N}\sum_{l=0}^{N-1} |y_{mN+l}|^2 + \frac{1}{N}\sum_{l=0}^{N-1} \left(\psi^2_{I,mN+l} + \psi^2_{Q,mN+l}\right) \end{aligned} \tag{27}$$

The cross-product terms $y_{n,I}\psi_{n,I}$ and $y_{n,Q}\psi_{n,Q}$ are not included because they average out to zero over for sufficiently large N, under the assumption in Equation (26). We define the jamming power contribution term as follows:

$$\Gamma_m \triangleq \frac{1}{N}\sum_{l=0}^{N-1} \left(\psi^2_{I,mN+l} + \psi^2_{Q,mN+l}\right) \tag{28}$$

Under jamming, using Equations (23) and (28) , the RF front-end signal power distribution can be written as:

$$s_m \sim N\left(\mu_{s,m} + \Gamma_m, \sigma^2_{s,m}\right) \tag{29}$$

where $\mu_{s,m}$ and $\sigma^2_{s,m}$ are the jamming-free mean and variance defined in Equation (23). Jamming causes an offset Γ_m to the mean of s_m. Thus, we can define two mutually exclusive and exhaustive hypotheses as follows:

$$\begin{aligned} \text{Null hypothesis } H_0 &: \Gamma_m = 0 \text{ (no jamming)} \\ \text{Alternate hypothesis } H_1 &: \Gamma_m > 0 \text{ (jamming)} \end{aligned} \tag{30}$$

Using Equations (23) and (29) and following the process described in Section 2.1, we can derive a locally optimal hypothesis test for small jamming powers $(\Gamma_m \to 0)$, with a test statistic defined as:

$$\hat{\eta}_m \triangleq \frac{s_m - \mu_{s,m}}{\sigma^2_{s,m}} \tag{31}$$

Under H_0, this test statistic has the following distribution: $\hat{\eta}_m \sim N(0, 1/\sigma^2_{s,m})$. We define a normalized test statistic as follows:

$$\eta_m \triangleq \hat{\eta}_m \sigma_{s,m} = \frac{s_m - \mu_{s,m}}{\sigma_{s,m}} \quad \text{and} \quad \eta_m \sim N(0,1) \tag{32}$$

The computation of η_m requires a model of mean jamming-free power $\mu_{s,m}$, and a model of standard deviation $\sigma_{s,m}$. The method for modeling these quantities is described in Section 3.4. The detection threshold for the test is the quantile function evaluated at $(1 - P_{FA,REQ})$.

3 | NOMINAL C/N0 & POWER MEASUREMENT MODELING FOR JAMMING DETECTION

In this section, we develop methods to determine models of the nominal mean and variance of C/N0, the variance of time-differenced C/N0, and the mean and variance of power measurements. These models are determined under H_0, i.e., using jamming-free C/N0 and power measurements. The modeling methods must be automated for implementation on a network of heterogeneous receivers.

3.1 | Elevation-Dependent C/N0 Mean and Overbounding Variance Model

Figure 1 shows one week of raw, unprocessed GPS L1 C/N0 data collected in May 2021 at the NGS CORS station located in Charlotte, North Carolina (CORS site index: NC77) (NGS, n.d.) for one satellite with pseudorandom code number: PRN8. Figure 1(c) is an azimuth-elevation sky-plot with color-coded C/N0 showing that the satellite trajectory observed at NC77 repeats itself. In Figure 1(b) the seven overlapping curves, color-coded to distinguish seven days, illustrate the fact that the mean and variance of the C/N0 values exhibit repeating patterns with a cycle period of one sidereal day (the x-axis is in sidereal time). 1(a) emphasizes the elevation dependence of the C/N0 measurements.

Figure 2(b) shows a sky-plot for all the satellites over 24 hours. The red-to-blue color-code represents C/N0 values ranging from 25-to-54 dB-Hz, highlighting again the strong dependence, for all PRNs, on elevation angle and, to a lesser extent, on individual satellites and their azimuth angles. This dependence is driven by the satellite transmission antenna gain pattern, the signal travel path through the atmosphere, the multipath environment, and the receiver antenna gain pattern (Fante et al. (2012) (Chapter 1), O'Brien et al. (2020)). In addition, Figure 2(a) suggests that, while C/N0 primarily depends on elevation angle, the range of C/N0 variations across satellites can exceed 15 dB-Hz at low elevation angles and 10 dB-Hz at high elevation. Designing a sensitive detector requires that we narrow down the range of nominal, predictable C/N0 variations.

Therefore, for each individual satellite 'i' at a time step 'k', we model the C/N0 mean as a function of elevation angle using the following quartic polynomial:

$$\mu_{i,k} = a_{0,i} + a_{1,i}\theta_{i,k} + a_{2,i}\theta^2_{i,k} + a_{3,i}\theta^3_{i,k} + a_{4,i}\theta^4_{i,k} \tag{33}$$

where $\theta_{i,k}$ is the elevation angle of satellite 'i' at time step 'k', and $[a_{0,i}\ a_{1,i}\ a_{2,i}\ a_{3,i}\ a_{4,i}]$ are the coefficients of the quartic polynomial determined by fitting jamming-free C/N0 data over a day as illustrated in 3(a).

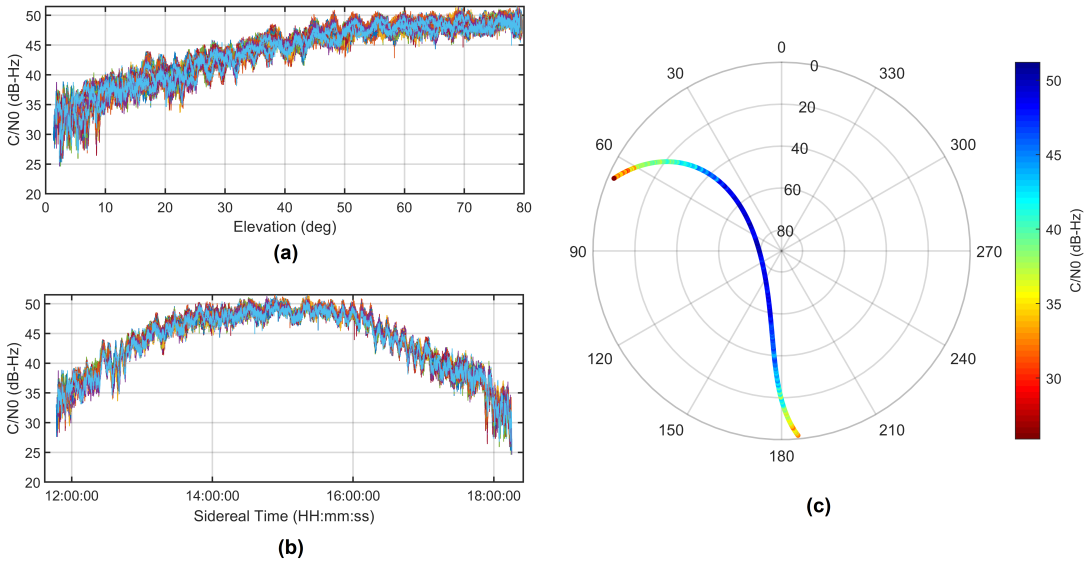

FIGURE 1 GPS L1 C/N0 for PRN8 at Charlotte, NC (CORS site index: NC77) during a week in May 2021, (a) as a function of elevation, and (b) as a function of sidereal time. The plots show 7 color-coded curves corresponding to 7 days. (c) Color-coded C/N0 on an azimuth-elevation sky-plot for PRN8 on May 1, 2021. A single day is shown because azimuth-elevation curves overlap over multiple days.

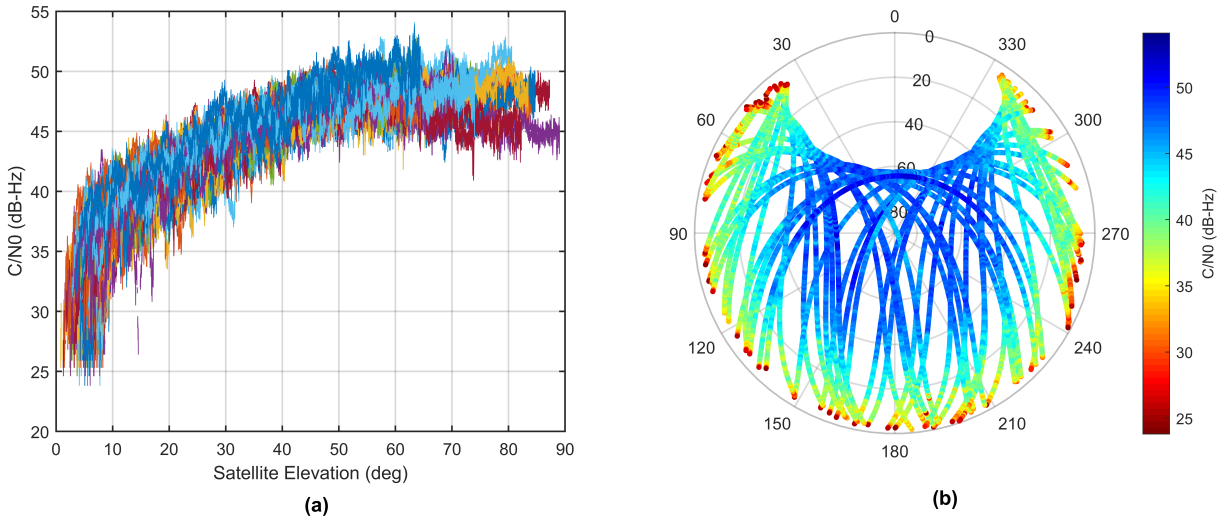

FIGURE 2 (a) GPS L1 C/N0 for all satellites (color-coded) at Charlotte, NC as a function of elevation, over 24 hours. (b) Color-coded GPS L1 C/N0 on an azimuth-elevation sky plot: elevation is a major cause for C/N0 variations, but C/N0 values also vary with satellite and azimuth angle.

Then, to model the variance, we subtract the mean C/N0 model from the sample data to compute the C/N0 residuals plotted in Figure 3(b). C/N0 residuals also show an elevation dependence. A 20-degree elevation mask is applied to avoid C/N0 variations largely affected by the multipath reflections from the environment surrounding the receiver antenna, where satellite azimuth angle dependence is significant. The 20-to-90-degree elevation range can be segmented into 2.5-degree bins to compute the sample standard deviation of the C/N0 residuals versus elevation angle for all satellites over a day. We then fit an elevation-dependent two-term exponential model to the sample standard deviations. The C/N0 standard deviation model at time step k for satellite i is expressed as follows:

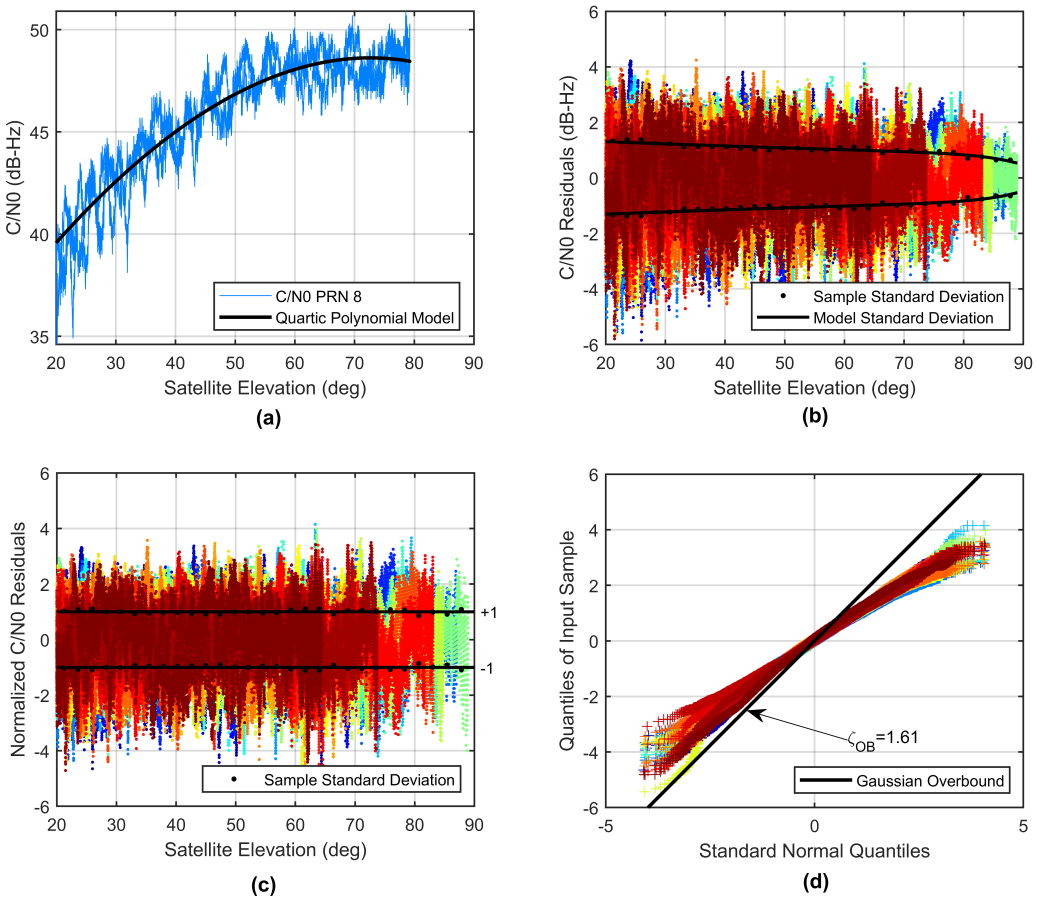

FIGURE 3 Overview of the elevation-dependent nominal C/N0 modeling method. (a) Mean C/N0 model for PRN 8. (b) Sample and modeled standard deviations of C/N0 residuals (samples-minus-mean) over 2.5-degree elevation bins for all satellite PRNs (color-coded). (c) Normalized C/N0 measurement residuals for all PRNs. (d) Gaussian overbounding of the sample distribution of normalized C/N0 residuals for all PRNs.

$$\hat{\sigma}_{i,k} = b_1 e^{-c_1 \theta_{i,k}} + b_2 e^{-c_2 \theta_{i,k}} \tag{34}$$

The coefficients b_1, b_2, c_1, and c_2 are the same for all satellites. Figure 3 (c) shows that C/N0 residuals normalized by their model standard deviation have zero mean and unit variance.

This elevation-dependent variance model accounts for 68% of the data, corresponding to samples within plus-or-minus one standard deviation (1-σ) of the mean of a normal distribution. However, the sample C/N0 measurement distribution has wide tails, which must be accounted for when seeking a risk of false alert $P_{FA,REQ}$ of about 10^{-6}. A false alert risk of 10^{-6} will be manually verifiable in Section 4, and will help ensure a much higher number of true versus false alerts.

The quantile-to-quantile (QQ) representation in Figure 3(d) helps visualize the distribution's tails. The distribution shows the CDF of normalized C/N0 residuals in Figure 3(c) (y-axis) versus the standard normal distribution (x-axis). The color-code distinguishes 32 GPS satellites. If the samples were following a standard normal distribution, their QQ plot would describe a straight line passing through the origin with a slope of one.

We can determine a single-CDF overbounding Gaussian model of the normalized random C/N0 residuals using methods by Blanch et al. (2017), DeCleene (2000), and Rife et al. (2006). It is obtained by multiplying the standard deviation $\hat{\sigma}_{i,k}$ by a factor ζ_{OB} determined such that the Gaussian overbound, represented by a black line in Figure 3(d), lower-bounds the left tail

of the sample CDF and upper-bounds its right tail. This model is conservative more than 68% of the time. The model may be of lower fidelity than more complex, higher-order, non-Gaussian distributions, but: first, it provides a means to determine an overbound on the detection test statistic distribution in Equation (10) (the overbound for α_k is derived as a linear combination of Gaussian overbounds); second, according to overbounding theory, it guarantees an upper bound on the risk of false alerts; third, the process can be automated, which is instrumental for systematic threshold setting at hundreds of receiver locations. Thus, the overbounding, elevation-dependent standard deviation is expressed as:

$$\sigma_{i,k} = \zeta_{OB}\ \hat{\sigma}_{i,k} \tag{35}$$

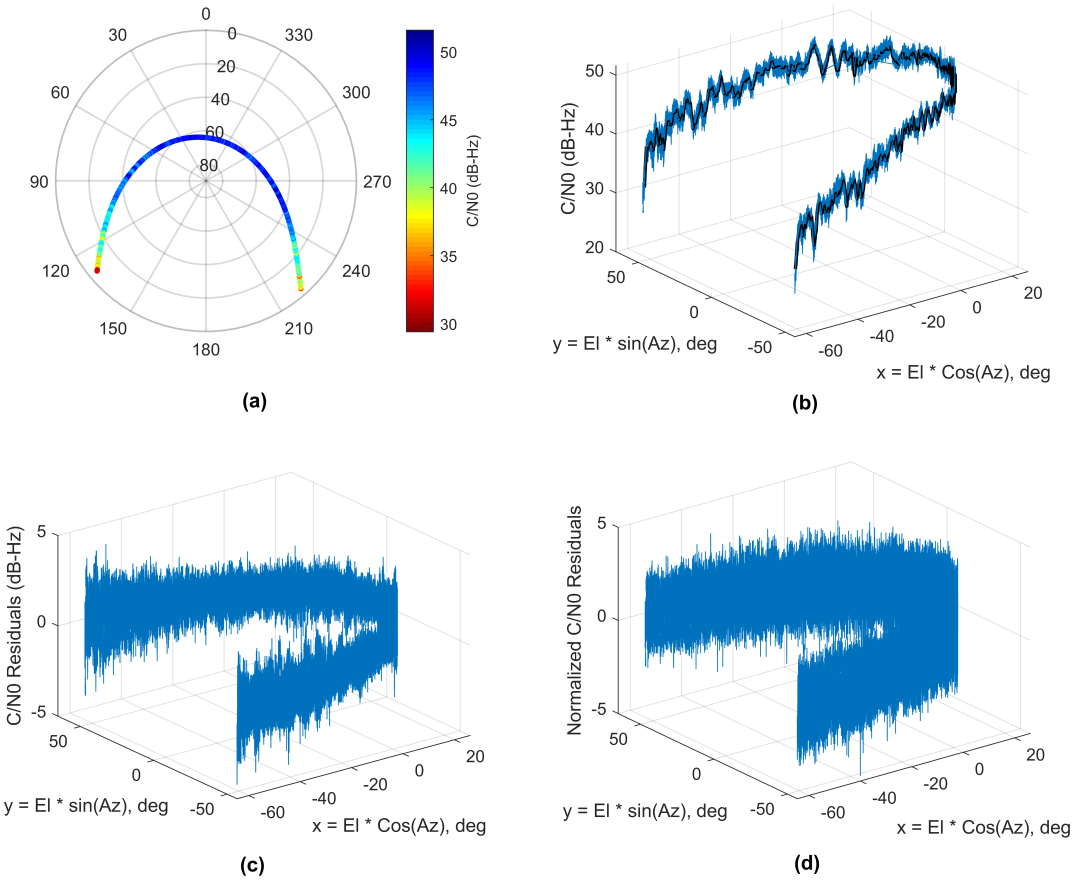

FIGURE 4 Overview of the azimuth-and-elevation-dependent C/N0 measurement modeling method. (a) Azimuth-elevation (Az-El) sky-plot for PRN2 at Charlotte, NC on May 1 to May 8, 2021. (b) C/N0 measurements over eight days (blue) and C/N0 mean model (black). (c) C/N0 measurement residuals: samples 'minus' mean model. (d) Normalized C/N0 residuals: C/N0 residuals divided by modeled standard deviation.

3.2 | Azimuth and Elevation-Dependent C/N0 Model

Equation (33) does not capture the short-time-scale C/N0 fluctuations seen in Figure 1(b), occurring over tens of seconds to tens of minutes, that repeat with sidereal time and arise from azimuth-dependent antenna gain and multipath effects. If we account for such mean variations using a higher-order model, then the C/N0 model variance can be tightened and the jamming detector sensitivity can be increased. For a given satellite (or PRN), we repeatedly observe that the C/N0 residual variations due

to changes in azimuth angle, elevation angle, temperature, and other sensitive parameters can be captured as variations over time. We observed that this model holds with high fidelity for multiple weeks (the model is refreshed monthly). This approach also captures the C/N0 variations due to the azimuth-and-elevation-dependent antenna gain pattern and multipath. We therefore derive a refined model that we refer to as the azimuth and elevation-dependent model for each individual satellite.

Figure 4(b) shows that the GPS L1 C/N0 measurement variations versus azimuth-elevation at the Charlotte, NC location are repeatable over eight days, from May 1 to May 8, 2021. We partitioned the data points for these eight jamming-free days into 2880 azimuth-elevation bins. In each bin, we computed the sample mean: the resulting model is represented as a solid black curve in Figure 4(b).

Figure 4(c) shows the residual C/N0 variations (sample 'minus' mean). Similar to the mean model, in each azimuth-elevation bin, we derive an azimuth-elevation-dependent variance model derived from the residual sample variance. Figure 4(d) shows the C/N0 residual normalized by the model standard deviation, which has a zero mean and a unit standard deviation. An inflation factor is applied using the same overbounding method as in Equation (35) to account for the wide tails of the C/N0 residual distribution.

As compared to the elevation-dependent model, each one of the 2880 variance parameters is computed using a lower number of data points. Thus, this higher-dimensional azimuth-and-elevation-dependent model more accurately captures the mean C/N0 variations, but the variance model is derived from a smaller number of data samples.

This shortcoming is mitigated by using more jamming-free data (e.g., eight days of data instead of one). To efficiently sort through C/N0 data and find jamming-free data, we use the following time-differenced C/N0-based detector, whose nominal model is simpler.

3.3 | Elevation-Dependent Time-Differenced C/N0 Measurement Variance Model

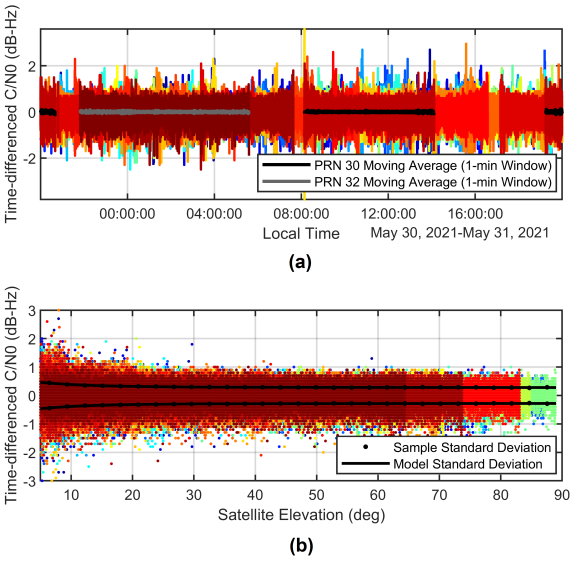

FIGURE 5 Time-differenced C/N0 data from all satellites (PRNs are color-coded) at CORS site NC77 on May 31, 2021, (a) as a function of time, and (b) as a function of elevation angle.

The mean of time-differenced C/N0 is zero when the time interval between C/N0 measurements is one second or lower. Figure 5(a) and (b) show time-differenced C/N0 for all 32 GPS satellites over a day versus time and versus satellite elevation, respectively. In Figure 5(a), the moving averages of two example PRNs (PRNs 30 and 32), computed over a 1-minute window, are shown to support the zero-mean assumption. We use a two-term exponential time-differenced C/N0 nominal model for the variance, identified using the approach described in Section 3.1.

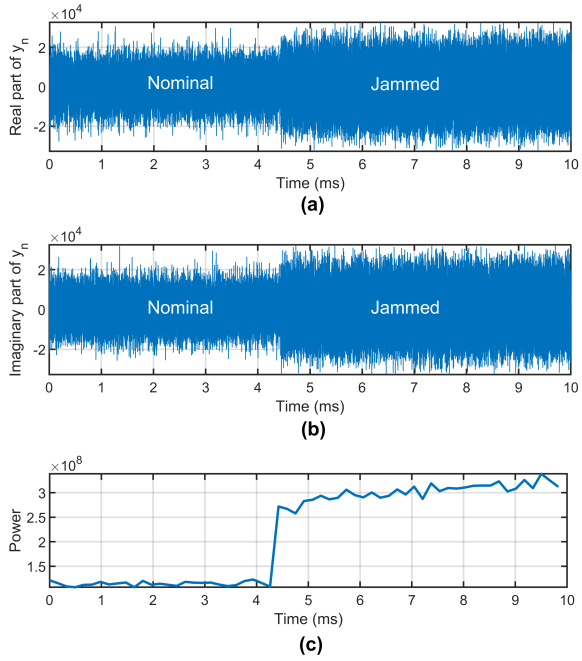

FIGURE 6 Impact of interference on RF front-end data collected in Blacksburg, Virginia, in August 2022: (a) for the RF-front-end signal's real part, (b) for the imaginary part, and (c) for the power measurement.

3.4 | RF-Front-End Nominal Power model

The power-based jamming detector in Equation (32) requires an RF front-end nominal, jamming-free power model. This detector is implemented on equipment that we deploy and is 'manually' calibrated assuming that jamming-free data is identified at start-up time. The mean power, $\mu_{s,m}$, is computed by averaging the power samples from jamming-free time periods, and the standard deviation, $\sigma_{s,m}$, is computed by overbounding the power residuals (samples-minus-mean).

Figure 6 shows an example of in-phase, quadrature, and signal power samples, with and without interference. This data was collected during a GPS interference observed in Blacksburg, Virginia, and described by Jada et al. (2023). The amplitude of the real and imaginary components of the RF front-end signal increases as compared to the nominal amplitude during the interference; consequently, the mean of the signal power increases. (This increase is captured by the term Γ_m in Equation (29).)

4 | JAMMING EVENTS DETECTED USING C/N0 DATA FROM CORS AND IGS NETWORKS

In this section, we apply the C/N0-based jamming detection methods to GPS L1 C/N0 data from receiver networks and present an overview of the detected interference leading to interference pattern identification and prediction.

4.1 | Automated Jamming Monitor

We developed an automated jamming detection process described by the block diagram in Figure 7. First, a web scraping program retrieves the C/N0 data from CORS or IGS databases and downloads GPS almanacs from the United States Coast Guard's Navigation Center database accessible at US Coast Guard (n.d.). We use the GPS satellite almanacs' Keplerian elements to compute satellite azimuth and elevation corresponding to each GPS L1 C/N0 entry at all receiver locations in the network. The algorithm first uses the time-differenced C/N0 detector to identify event-free data because it is effective even with a coarse variance model and a constant zero-mean C/N0 model. Once event-free data is identified, receiver- and satellite-specific nominal models are identified from one or more days of data, and the models are stored for future use. The algorithm incorporates this model to run the C/N0-based detectors and record events. All the steps in this process are designed to be executed autonomously. We

deployed this method on the following website: Nayak et al. (2025): this interference monitor is refreshed approximately monthly and uses 1-Hz-update-rate data from approximately 900 U.S. CORS sites to generate the interference maps and day-of-year versus time-of-day plots presented in this section.

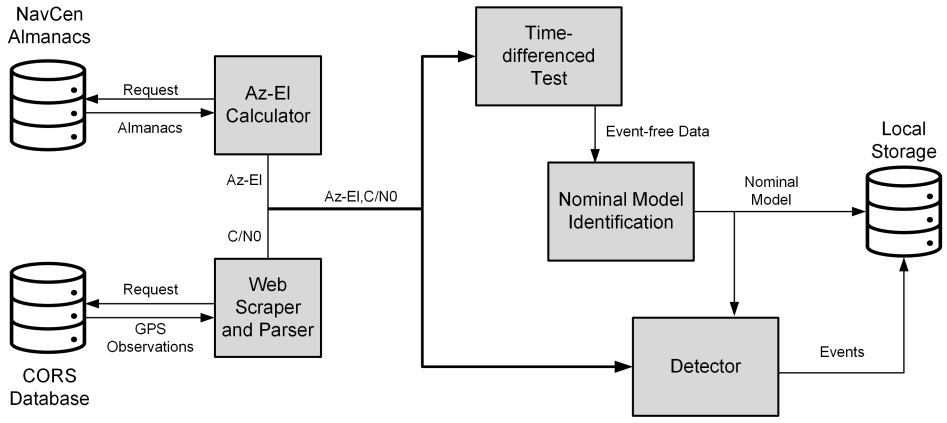

FIGURE 7 Block diagram illustrating the nominal C/N0 measurement modeling process and the jamming detector using CORS data.

4.2 | Comparison Between the Three C/N0-Based Detectors for an Example Dataset

In this section, we evaluate the following three C/N0-based detector implementations: first, the detector derived in Section 2.1 using Section 3.1 's elevation-dependent model; second, the same detector but using the high-order, azimuth-elevation-dependent model in Section 3.2 ; third, the time-differenced C/N0-based detector derived in Section 2.2 using Section 3.3 's elevation-dependent variance model. We use C/N0 measurements from an example CORS site, indexed as NC77, in Charlotte, NC (latitude: 35° 7' 21" N, longitude: 80° 54' 58" W) to characterize the performance of the three detector implementations. NC77 is located within 200 meters from the intersection of Interstates I-77 and I-485 and next to a truck stop, as shown in Figure 8 (a). NC77 provides data at a 1 Hz sampling rate. It is a suitable location for observing jamming caused by illegal Personal Privacy Devices (PPDs). PPDs are used by commercial vehicle drivers to avoid being tracked by their employers or by criminals to elude authorities (Coffed et al., 2015; Space-Based PNT National Advisory Board, 2018).

We first evaluate the C/N0-based jamming detector in Section 2.1 with an elevation-dependent nominal model described in Section 3.1. Figure 8(b) shows the ratios of the test statistic to the detection threshold at one-second intervals on May 19, 2021. Jamming is detected when the ratio exceeds one. The detection threshold is computed for a false alert risk requirement $P_{FA,REQ}$ of 10^{-6}. Figure 8(c) shows the C/N0 for all satellites (color-coded) during one of the six detected events on May 19. This simultaneous decrease in C/N0 over all satellites is typical of a jamming event.

Figure 8(d) shows the same sequence of test statistic to threshold ratio as in Figure 8(b), but for the entire month of May 2021. In this monthly plot, the marker sizes are proportional to the ratio; weekends and weekdays are color-coded; red marker edges indicate ratios exceeding one.

To verify that the actual false alert rate met the required $P_{FA,REQ}$, we individually checked each of the three dozen detected events: we counted cases where C/N0 was simultaneously dropping across three or more satellites. This verification is further described in our conference paper by Jada et al. (2021). Out of 2.6×10^6 test samples during this month, we found no false alerts.

The monthly plots can reveal patterns in the detected events (red markers), for example, caused by PPDs in vehicles following a weekly schedule. One such weekly pattern seems to occur on Wednesdays at midnight, on May 05, 12, and 19, but not on May 26.

Figure 8(d) also shows repeating, watermark-looking variations in marker sizes of the test-statistic-to-threshold ratio. These variations correspond to the sidereal-time-dependent changes in C/N0 caused by multipath. These repeated fluctuations can be seen over seven days for PRN8 in Figure 1(b). Their repeatability is represented in Figure 4(b) for PRN2 over eight days versus azimuth and elevation (for a receiver at a fixed location, GPS satellites appear at the same azimuth and elevation angles every

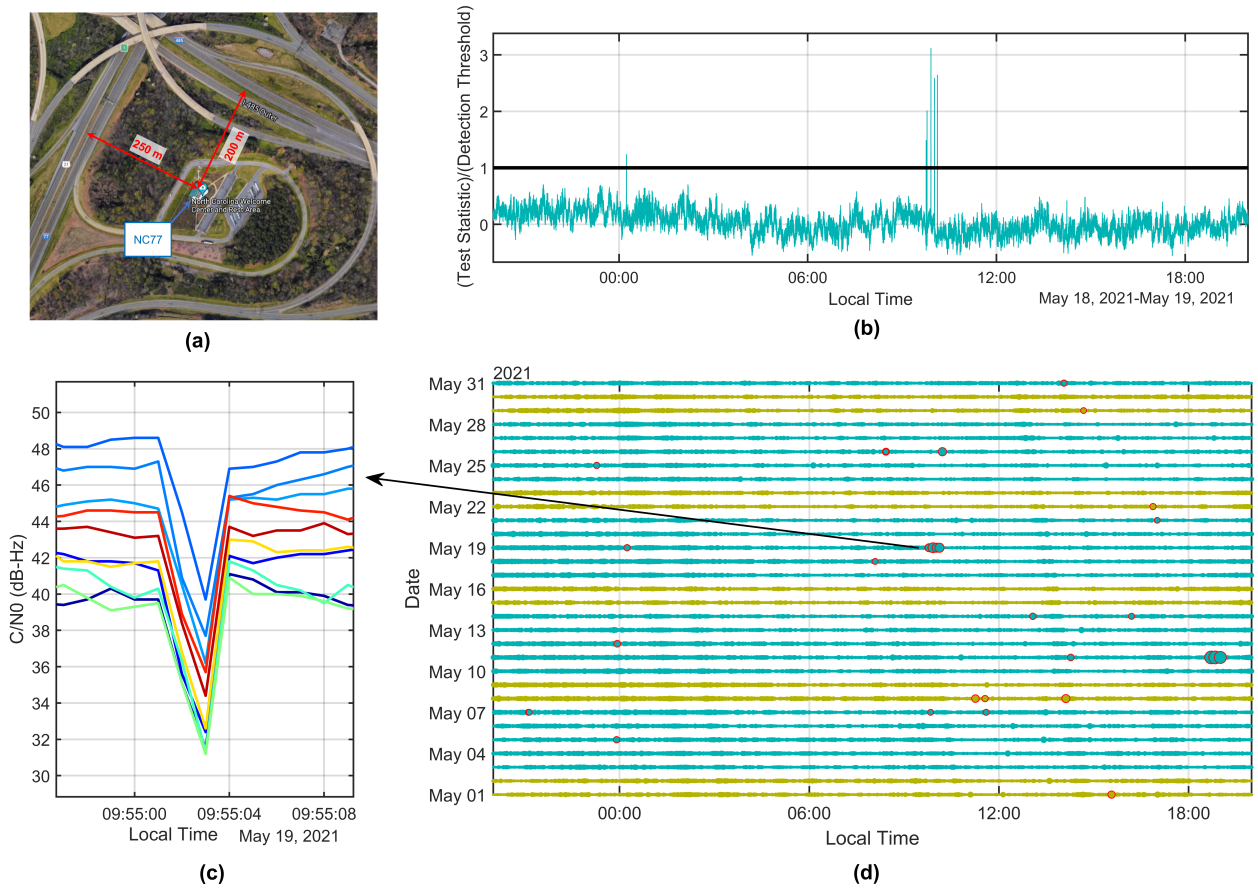

FIGURE 8 Testing using the first detector (time-undifferenced C/N0) with the low-order, elevation-dependent nominal model (Sections 2.1 and 3.1). (a) Map showing the geometry of Interstates around the CORS site NC77. (b) Time sequence of test statistic to threshold ratios on May 19, 2021. (c) C/N0 from all satellites (color-coded) in view during jamming. (d) One month of C/N0-based jamming monitoring using the elevation-dependent model at NC77 during May 2021.

sidereal day). In Figure 8(d), the repeating variations shift from one solar day to the next because a sidereal day is about four minutes shorter than a solar day.

In the elevation-dependent model, these variations are accounted for using a loosened overbound on the C/N0 residual distribution, which increases the probability of missed detection and decreases detection sensitivity. In contrast, the azimuth-and-elevation-dependent nominal C/N0 modeling in Section 3.2 captures these high-frequency variations, which are most likely due to multipath, in the C/N0 mean model. Figure 9(a) shows the resulting test-statistic-to-threshold ratios in May 2021. The repeating sidereal day variations disappear, and additional events are detected.

The time-differenced C/N0 test can also increase the detector's sensitivity, i.e., reduce its probability of missed detection, because it is unaffected by sidereal-time-dependent variations. The ratio of the time-differenced C/N0 test statistic in Equation (19) over its threshold in Equation (20) is used to generate the monthly detection plot in Figure 9(b) at NC77 over May 2021. The time-differenced C/N0 detector's sensitivity matches that of the C/N0 detector in Figure 9(a).

This dataset counts 2.6×10^6 samples. The actual false alert probabilities, as determined through visual inspection of raw (unprocessed) C/N_0 measurements during each individual detected event inspection of the detected events in Figures 9(a) and 9(b) respectively are 2×10^{-6} and 1.7×10^{-6} (Jada et al., 2021). (If C/N_0 measurements for all satellites do not simultaneously drop, then the detection is classified as a false alert)

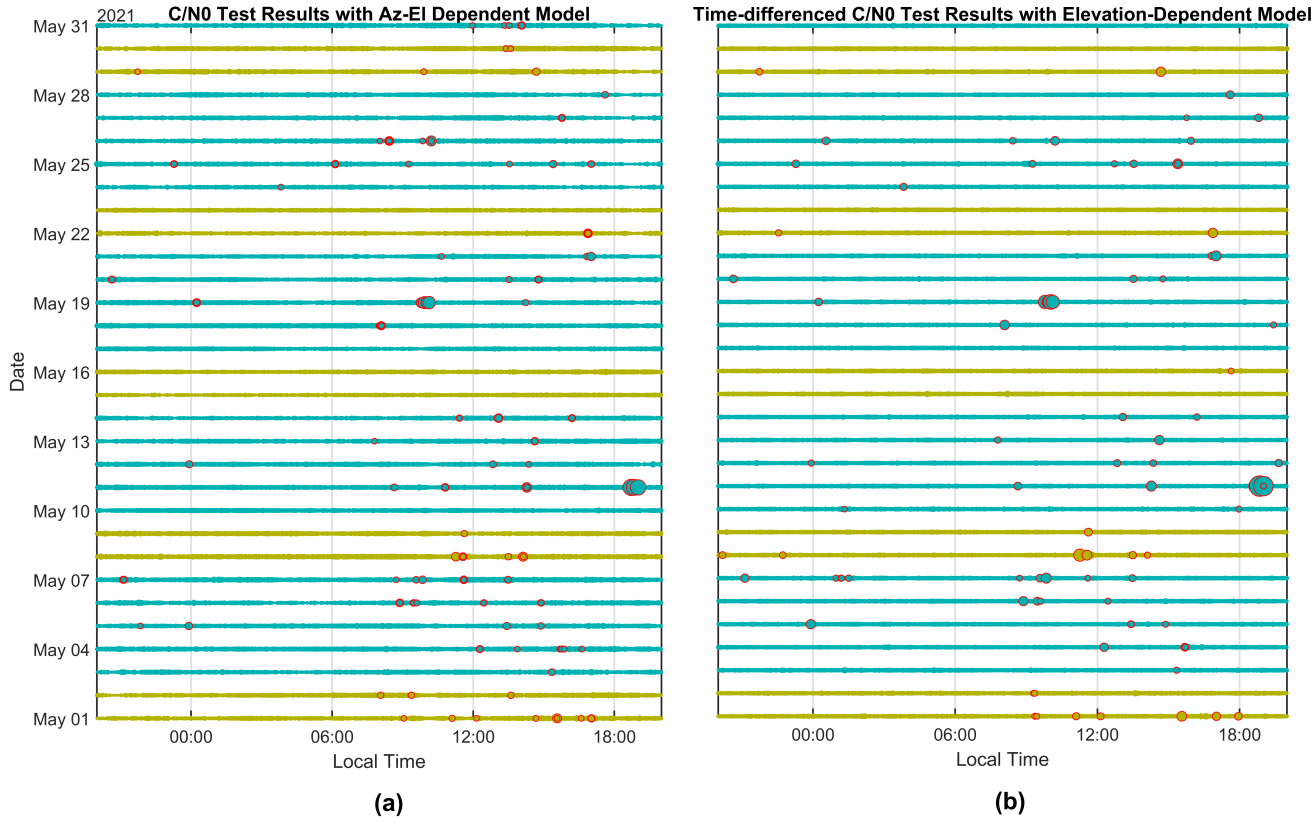

FIGURE 9 Testing using (a) the first, time-undifferenced detector with the azimuth-and-elevation-dependent nominal model (Sections 2.1 and 3.2; (b) the time-differenced detector (Sections 2.2 and 3.3).

This improved detection performance shown in Figure 9 as compared to Figure 8(d) is achieved at a cost; (i) more data, seven days instead of one, is needed for the azimuth-and-elevation-dependent modeling process; (ii) the time-differenced C/N0 test is only sensitive to rates of changes in C/N0.

4.3 | Temporal Pattern Identification in Detected Jamming Events

Identifying regularly repeating detection patterns can provide evidence of road user jamming as opposed to other natural disturbances that impact C/N0, such as ionospheric activity. Repeating jamming events detected using our C/N0 monitor can be predicted and then validated through independent wideband RF data analysis. We processed eight months of data from CORS site NC77 and from other sites, including from the International GNSS Service (IGS) network, to find repeated detection patterns.

While the CORS network is predominantly a US-based network, the IGS network is a global network of receivers, and the IGS database provides receiver outputs at 1-Hz update rate over the past two decades, as described in IGS (n.d.) and Johnston et al. (2017). In the US, the IGS network is sparser than the CORS network with about 50 IGS sites vs. 910 CORS sites with a 1-Hz sampling rate. We applied the method in Figure 7 to the IGS network of worldwide receivers and found clear patterns of interference from a site indexed AMC4 in Colorado Springs, CO, USA (latitude: 38° 48’ 10.8” N, longitude: 104° 31’ 30” W). This demonstrates that the algorithm can detect events from any receiver network’s C/N0 database with a customized web scraper and a parser, and the rest of the method is unchanged.

The plots in Figure 10 show the temporal distribution of jamming events at NC77 in (a) and AMC4 in (b) from January 2022 through August 2022. The x-axis is the local time of the day, and the y-axis is the day of the year. The marker sizes capture the event’s intensity, which scales with increases of test-statistic over detection threshold ratio exceeding one (for clarity, we only

display detection and do not show cases where the ratio is lower than one). Makers are color-coded from blue to red to identify days of the week from Monday to Sunday, respectively. This color code is shown in the histograms in the bottom panels with the number of events as a function of the day of the week.

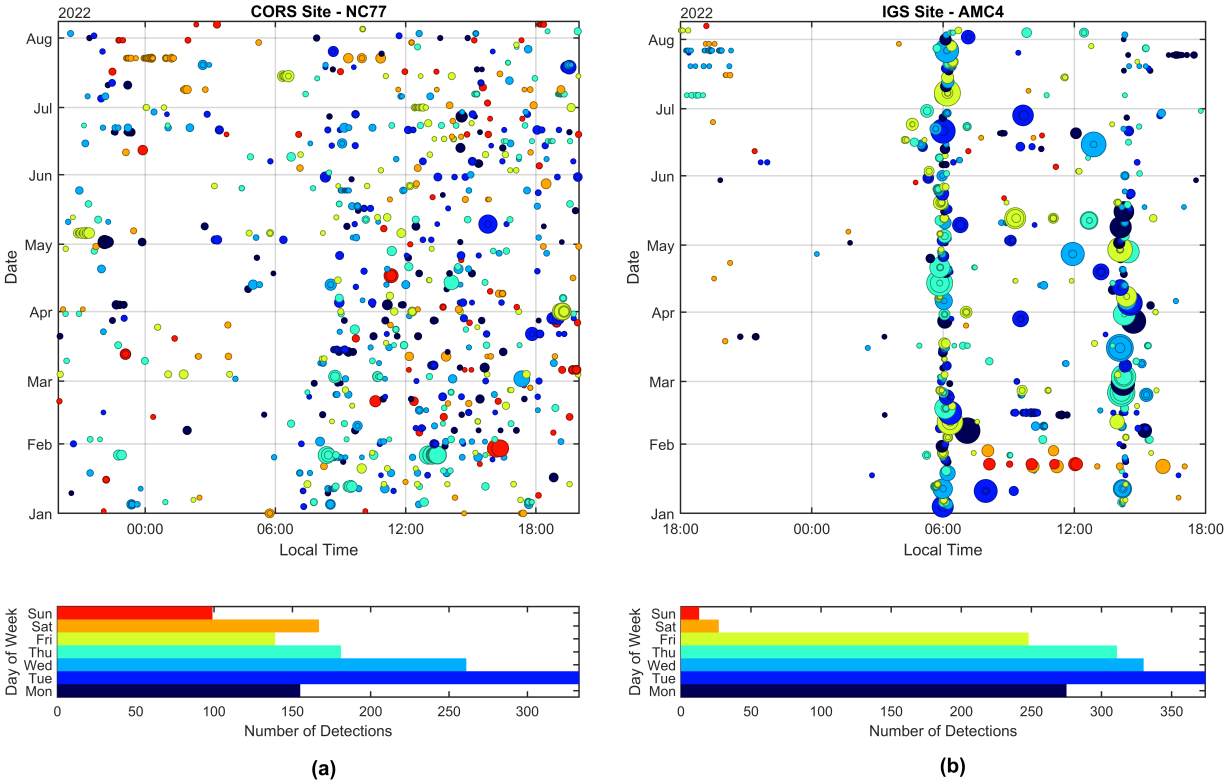

FIGURE 10 Jamming events over the first eight months of 2022, (a) CORS site NC77, and (b) IGS site AMC4. The bottom panels show the distribution of the events in the top panels versus the days of the week.

The histograms for NC77 in Figure 10(a) show jamming events predominantly occurring on weekdays with a maximum number of occurrences on Tuesdays and a minimum on Sundays. Figure 10(b) shows the distribution of detections at the IGS site AMC4 located in Colorado Springs, CO, USA. In this remote location, a clear pattern is discernible, with events regularly detected at 6:00 AM and 2:15 PM on weekdays and relatively few detections on weekends. (Data was unavailable for this IGS site during the second half of February 2022.) This pattern indicates actual jamming. It is so predictable that we may be able to observe it using wideband RF data, which would validate the C/N0-based detector.

5 | POWER-BASED OBSERVATION OF A PREDICTED PPD JAMMING EVENT

To validate the C/N0-based detectors, we collected wideband RF front-end data during a jamming event for time-frequency analysis. In this section, we perform a time-frequency analysis of a PPD jamming event in Colorado Springs, Colorado.

5.1 | Hardware Description

The wideband RF data collection system consists of transportable and power-efficient hardware components listed in Figure 11. We use an Ettus Universal Software Radio Peripheral (USRP) N200 with a DBSRX2 daughterboard to collect RF data. The

USRP is connected to an external Connor Winfield Ovenized Crystal Oscillator (OCXO) OH100. The OCXO, mounted on a circuit board, sends a 10 MHz timing signal as a square wave with +/-10 parts per billion frequency stability. This stability is needed to compute the GPS PNT solution from wideband RF data. We use a Tallysman 33-8829NMAT GPS patch antenna for the USRP. 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 a Linux Mint 17 operating system.

In parallel, we use a u-blox GNSS receiver EVK-M8F as an independent source of C/N0 and Automatic Gain Control (AGC) measurements. The Intel NUC also collects data from the u-blox receiver via a USB port. Our setup is designed to run on 12 V DC power, which allows us to power the entire setup directly using a car's DC power output. We developed Python software for wideband RF data collection, power monitoring, and C/N0-based jamming monitoring.

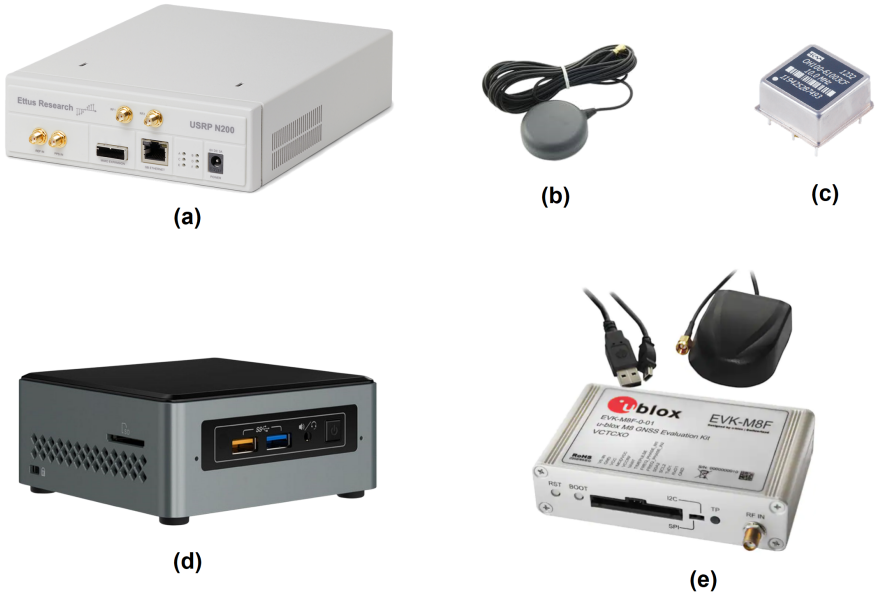

FIGURE 11 Equipment used for wideband RF data collection: (a) Ettus USRP N200 with DBSRX2 daughterboard, (b) Tallysman GPS Antenna 33-8829NMAT, (c) Connor Winfield ovenized crystal oscillator OCXO-OH100, (d) Intel NUC6, (e) u-blox GNSS receiver EVK-M8F.

5.2 | Analysis of PPD Jamming Observed on Interstate I-25 in Colorado

In order to analyze the pattern in Figure 10, we drove to the location AMC4 of the repeating interference and collected wideband RF data. Figure 12(a) shows the power-based jamming detector output and spectrogram of the signal from the event. This data was collected at a 25 MHz sampling rate with a center frequency at GPS L1. The power increase lasted about five seconds, consistent with crossing paths with a vehicle using a PPD. At the time of this data collection, we were not trying to identify a specific vehicle carrying the jammer. We were processing and visualizing the data with a five minute delay.

The spectrogram in Figure 12(b) is generated from the 50 μs segment of the signal with the highest power during the collection period. We use a 20-sample sliding Hamming window. The spectrogram at the power peak leaves little doubt about the nature of the interference. Repeated sweeps of peak power density are typical of chirp-type PPDs (Kraus et al., 2011; Mitch, 2014).

In parallel, we evaluated the impact of this PPD on a commercial u-blox receiver. The jamming event was detected by feeding the u-blox C/N0 measurements into our jamming detector. Figure 13(a) shows the u-blox receiver C/N0 dropping during the PPD jamming event. We also analyzed the PPD's impact on Automatic Gain Control (AGC), which can be used as a jamming indicator (Kim et al., 2020; Levigne, 2019; Miralles et al., 2018; Scott, 2011; Strizic et al., 2018). The AGC gain is a factor applied to a GNSS receiver RF-front-end signal before digitizing to prevent signal saturation in an environment with higher-than-usual in-band power (Bastide et al., 2003). Figure 13(b) shows the u-blox AGC suddenly dropping in reaction to the extra in-band power introduced by the jammer with a 1-second delay relative to the C/N0 drop.

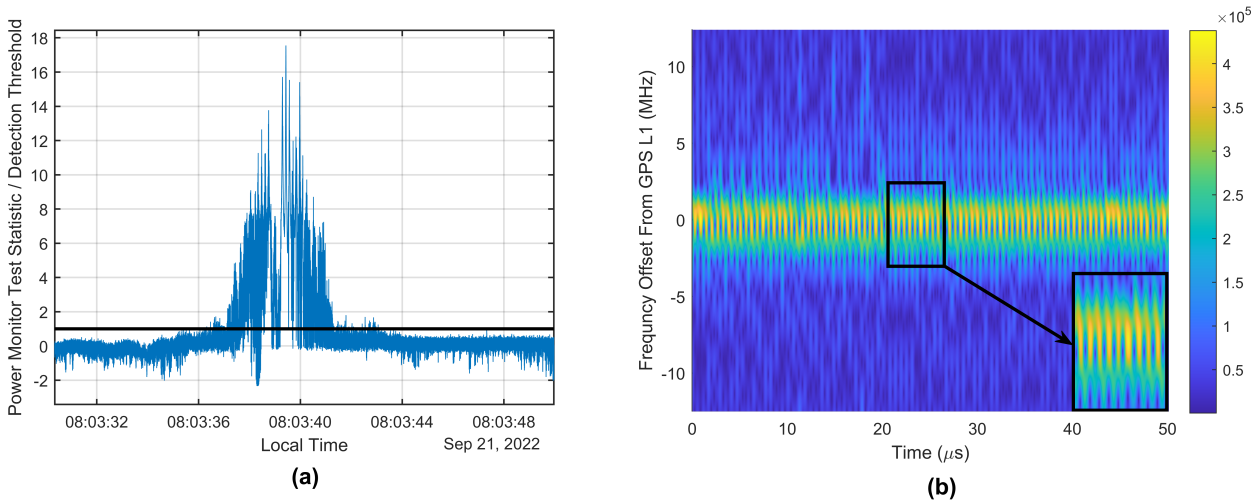

FIGURE 12 Time-frequency analysis of PPD jamming signal: (a) Signal power monitor output, and (b) Spectrogram showing sweeps in peak PSD.

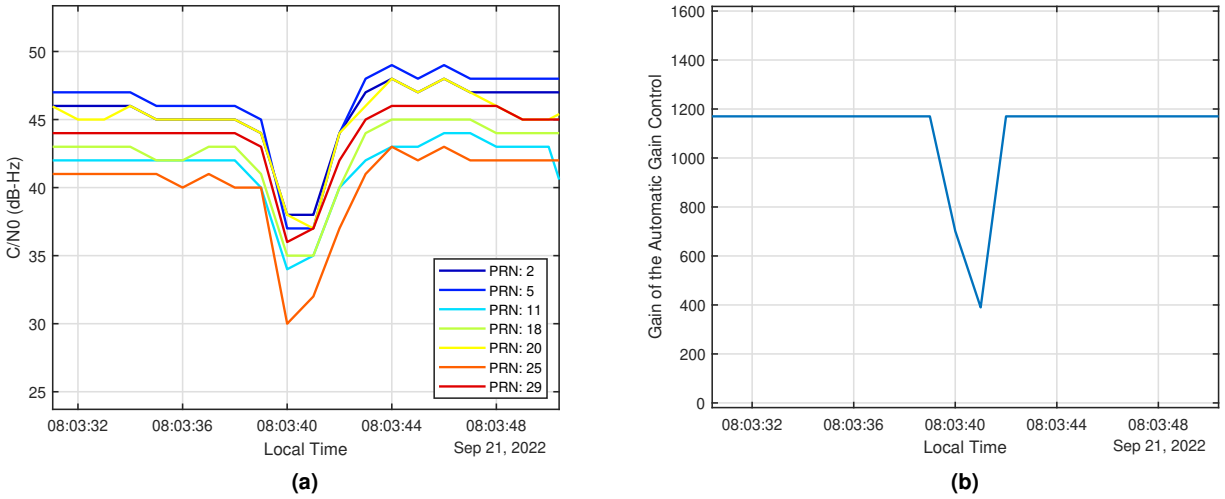

FIGURE 13 u-blox EVK-M8F receiver signal quality indicators collected during the PPD jamming event observed in Colorado: (a) C/N0, and (b) AGC.

Finally, in Figure 12(a), the test statistic to threshold ratio increases by an order of magnitude over its nominal value. The spectrogram in Figure 12(b) shows that the PPS jamming power is concentrated within +/-3 MHz, i.e., targeting the RF front-end bandwidth of typical GNSS receivers. Assuming all the jamming power is within the u-blox receiver's RF front-end bandwidth, the jammer impact parameter γ_k defined in Equation 2 is on the order of 10 dB. We observe this 10 dB drop in C/N0 in Figure 13(a) for all satellites.

6 | CONCLUSION

In this paper, we developed, implemented, and evaluated an autonomous GNSS jamming detection algorithm using C/N0 measurements from large receiver networks. The detectors are self-calibrating, achieve a predefined false alert probability, and are locally Neyman-Pearson optimal in the sense that they minimize the risk of missed detection of small jamming power density. We processed data from networks of hundreds of receivers over several months and found jamming patterns suggesting Personal

Privacy Device (PPD) interference by road users on daily or weekly schedules. Regularly occurring interference is predictable. Thus, to validate the C/N0-based jamming detector, we designed a portable wideband RF data collection hardware setup and developed a power-based jamming monitor. We analyzed wideband data during a jamming event on a US highway in Colorado and confirmed that the GPS L1 interference that we predicted using a receiver network actually originated from a PPD. Wide-scale receiver-network-based interference monitoring and prediction opens the door for future local wideband data-based observations of illegal jamming.

ACKNOWLEDGMENTS

The authors would like to thank the MITRE Corporation and the U.S. Department of Transportation (DOT)'s University Transportation Center (UTC) program under CARNATIONS (the Center for Assured and Resilient Navigation for Advanced Transportation Systems) for their support of this research. However, the opinions expressed in this paper are our own and do not necessarily represent those of any other person or organization.

REFERENCES

Bastide, F., Akos, D., Macabiau, C., & Roturier, B. (2003). Automatic gain control (AGC) as an interference assessment tool. *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, 2042–2053. https://www.ion.org/publications/abstract.cfm?articleID=5389

Blanch, J., Walter, T., & Enge, P. (2017). A MATLAB toolset to determine strict Gaussian bounding distributions of a sample distribution. *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, 4236–4247. https://doi.org/10.33012/2017.15392

Borio, D., & Gioia, C. (2015). Real-time jamming detection using the sum-of-squares paradigm. *2015 International Conference on Localization and GNSS (ICL-GNSS)*, 1–6. https://doi.org/10.1109/ICL-GNSS.2015.7217161

C4ADS. (2019). *Above us only stars: Exposing GPS spoofing in Russia and Syria* (tech. rep.) [Accessed on: December 13, 2020]. C4ADS (non-profit organization). https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf

Coffed, J., Rolli, J., & Slutsky, C. (2015). Detecting and locating GPS jamming. *Proceedings of the ION 2015 Pacific PNT Meeting*, 484–492. https://www.ion.org/publications/abstract.cfm?articleID=12734

Dacus, M., Liu, Z., Lo, S., & Walter, T. (2022). Improved RFI localization through aircraft position estimation during losses in ADS-B reception. *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, 947–957. https://doi.org/10.33012/2022.18529

DeCleene, B. (2000). Defining pseudorange integrity-overbounding. *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, 1916–1924. https://www.ion.org/publications/abstract.cfm?articleID=1603

Diez, A., Morrison, A., & Sokolova, N. (2022). Automatic classification of RFI events from a multi-band multi-site GNSS monitoring network. *Proceedings of the 35th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2022)*, 3907–3914. https://doi.org/10.33012/2022.18572

Fante, R., Kunysz, W., McDonald, K., & Rao, B. (2012). GPS/GNSS antennas. Artech House. https://us.artechhouse.com/GPSGNSS-Antennas-P1538.aspx

Federal Bureau of Investigation. (2014). Cargo thieves use GPS jammers to mask GPS trackers [Accessed on: January 10, 2022]. https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/

Fors, K., Stenberg, N., & Nilsson, T. (2021). Using the Swedish CORS network SWEPOS for GNSS interference detection. *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 4323–4333. https://doi.org/10.33012/2021.18113

Hegarty, C., O'Hanlon, B., Odeh, A., Shallberg, K., & Flake, J. (2019). Spoofing detection in GNSS receivers through cross-ambiguity function monitoring. *Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019)*, 920–942. https://doi.org/10.33012/2019.16986

IGS. (n.d.). The international GNSS service. https://igs.org/data-products-overview/

Jada, S., Bowman, J., Psiaki, M., Langel, S., & Joerger, M. (2023). Identifying car key fobs as a cause of interference at GNSS frequencies. *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, 4110–4120. https://doi.org/10.33012/2023.19376

Jada, S., Psiaki, M., Landerkin, S., Langel, S., Scholz, A., & Joerger, M. (2021). Evaluation of PNT situational awareness algorithms and methods. *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, 816–833. https://doi.org/10.33012/2021.17935

Joerger, M., Fan, C., & Jada, S. (2023). The unsolved mystery of the 2022 Texas interference [Accessed on: Aug 10, 2024]. https://insidegnss.com/the-unsolved-mystery-of-the-2022-texas-interference/

Johnston, G., Riddell, A., & Hausler, G. (2017). The international GNSS service. In P. J. Teunissen & O. Montenbruck (Eds.), *Springer Handbook of Global Navigation Satellite Systems* (pp. 967–982). Springer International Publishing. https://doi.org/10.1007/978-3-319-42928-1_33

Kim, H.-P., Jin, G.-G., & Won, J.-H. (2020). GNSS cloud-data processing technique for jamming detection, identification, and localisation. *IET Radar, Sonar & Navigation*, *14*(8), 1143–1149. https://doi.org/10.1049/iet-rsn.2019.0518

Kraus, T., Bauernfeind, R., & Eissfeller, B. (2011). Survey of in-car jammers-analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation). *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 430–435. https://www.ion.org/publications/abstract.cfm?articleID=9605

Kriezis, A., Chen, Y.-H., Akos, D., Lo, S., & Walter, T. (2024). GNSS RFI detection and impact characterization in various interference environments using low-cost receivers. *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024)*, 3348–3360. https://doi.org/10.33012/2024.19713

Levigne, N. S. (2019). *Automatic gain control measurements as a GPS L1 interference detection metric* (Master's thesis). University of Colorado at Boulder. https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/qr46r104k

Lewis, S. (2023). Bird landings causing C/N0 disturbances.

M. Brunker. (2016). GPS under attack as crooks, rogue workers wage electronic war [Accessed on: January 10, 2022]. https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761

Miralles, D., Levigne, N., Akos, D. M., Blanch, J., & Lo, S. (2018). Android raw GNSS measurements as the new anti-spoofing and anti-jamming solution. *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 334–344. https://doi.org/10.33012/2018.15883

Mitch, R. H., Dougherty, R. C., Psiaki, M. L., Powell, S. P., O'Hanlon, B. W., Bhatti, J. A., & Humphreys, T. E. (2011). Signal characteristics of civil GPS jammers. *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, 1907–1919. https://www.ion.org/publications/abstract.cfm?articleID=9740

Mitch, R. H. (2014). *Model-based estimation techniques applied to Global Navigation Satellite System jammers* (Doctoral dissertation). Cornell University. https://hdl.handle.net/1813/37118

Mosavi, M. R., Rezaei, M. J., Pashaian, M., & Moghaddasi, M. S. (2017). A fast and accurate anti-jamming system based on wavelet packet transform for GPS receivers. *GPS solutions*, *21*(2), 415–426. https://doi.org/10.1007/s10291-016-0535-z

Murrian, M. J., Narula, L., & Humphreys, T. E. (2019). Characterizing terrestrial GNSS interference from low earth orbit. *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, 3239–3253. https://doi.org/10.33012/2019.17065

Nayak, A., Malani, S., Jada, S., & Joerger, M. (2025). Global Navigation Satellite System (GNSS) interference detection using C/N0 data from public databases. https://rfi.aoe.vt.edu/

NGS. (n.d.). The National Geodetic Survey (NGS)'s CORS network. https://geodesy.noaa.gov/CORS/

O'Brien, A., Chen, C.-C., & Gupta, I. J. (2020). GNSS receiver antennas and antenna array signal processing. In *Position, navigation, and timing technologies in the 21st century* (pp. 681–715). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119458449.ch26

Rife, J., Pullen, S., Enge, P., & Pervan, B. (2006). Paired overbounding for nonideal LAAS and WAAS error distributions. *IEEE Transactions on Aerospace and Electronic Systems*, *42*(4), 1386–1395. https://doi.org/10.1109/taes.2006.314579

Scott, L. (2011). J911: The case for fast jammer detection and location using crowdsourcing approaches. *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 1931–1940. https://www.ion.org/publications/abstract.cfm?articleID=9742

Space-Based PNT National Advisory Board. (2018). Protect, toughen, and augment Global Positioning System for users. www.gps.gov/governance/advisory/recommendations/2018-09-topic-papers.pdf

Strizic, L., Akos, D. M., & Lo, S. (2018). Crowdsourcing GNSS jammer detection and localization. *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, 626–641. https://doi.org/10.33012/2018.15546

The White House. (2020). Executive order on strengthening national resilience through responsible use of positioning, navigation, and timing services. https://www.transportation.gov/sites/dot.gov/files/2020-02/Executive%20Order%20on%20Strengthening%20National%20Resilience%20through%20Responsible%20Use%20of%20Positioning.pdf

The White House. (2021). Space policy directive 7, the United States space-based positioning, navigation, and timing policy. https://www.transportation.gov/sites/dot.gov/files/2023-11/Memorandum%20on%20Space%20Policy%20Directive%207.pdf

US Coast Guard. (n.d.). Navigation Center GPS almanacs. https://www.navcen.uscg.gov/gps-nanus-almanacs-opsadvisories-sof

Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2017). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(2), 739–754. https://doi.org/10.1109/TAES.2017.2765258

Weston, N. D., Mader, G. L., Marion, F., Schwarz, C., Snay, R., & Stone, W. (2010). A near real-time GPS interference detection system in the United States using the national CORS network. *Proceedings of FIG Congress 2010*. https://www.fig.net/resources/proceedings/fig_proceedings/fig2010/papers/ts03c/ts03c_weston_snay_et_al_4085.pdf

Wu, Dong L. (2024). Innovation: Recent GPS jamming in regions of geopolitical conflict [Accessed on: Aug 10, 2024]. https://www.gpsworld.com/innovation-recent-gps-jamming-in-regions-of-geopolitical-conflict/