Blind Opportunistic Navigation: Cognitive Deciphering of Partially Known Signals of Opportunity

Mohammad Neinavaie, Joe Khalife, and Zaher M. Kassas
University of California, Irvine, USA

BIOGRAPHIES

Mohammad Neinavaie is a Ph.D. student at the University of California, Irvine and a member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in electrical engineering and an M.S. in digital communication systems from Shiraz University. His research interests include opportunistic navigation, cognitive radio, wireless communication systems, and software-defined radio.

Joe Khalife is a postdoctoral fellow at the University of California, Irvine and member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering, an M.S. in Computer Engineering from the Lebanese American University (LAU) and a Ph.D. in Electrical Engineering and Computer Science from the University of California, Irvine. From 2012 to 2015, he was a research assistant at LAU, and has been a member of the ASPIN Laboratory since 2015. He is a recipient of the 2016 IEEE/ION Position, Location, and Navigation Symposium (PLANS) Best Student Paper Award and the 2018 IEEE Walter Fried Award. His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio.

Zaher (Zak) M. Kassas is an associate professor at the University of California, Irvine and director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. In 2018, he received the National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) award, and in 2019, he received the Office of Naval Research (ONR) Young Investigator Program (YIP) award. He is a recipient of 2018 IEEE Walter Fried Award, 2018 Institute of Navigation (ION) Samuel Burka Award, and 2019 ION Col. Thomas Thurlow Award. He is an Associate Editor for the IEEE Transactions on Aerospace and Electronic Systems and the IEEE Transactions on Intelligent Transportation Systems. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.

ABSTRACT

A blind opportunistic navigation (BON) framework is proposed. This framework deciphers partially known signals of opportunity (SOPs) in a cognitive fashion. BON enables acquisition and tracking of terrestrial or space-based SOPs with minimal prior knowledge about their beacon signal. A computationally efficient algorithm is presented to blindly decode the beacon signals and estimate the Doppler frequency. The BON framework is applied to decipher the C/A pseudorandom noise (PRN) sequences from four GPS satellites. Experimental results are presented demonstrating a percentage of correctly decoded chips for these four PRN sequences ranging between 91% and 99%. These deciphered sequences are fed to a software-defined Rx (SDR) which produce a two-dimensional (2-D) position error of 54.5m for a stationary antenna.

I. INTRODUCTION

Signals of opportunity (SOPs), including AM/FM radio [1, 2], Wi-Fi [3, 4], cellular [5–9], etc., are proving to be a reliable and accurate alternative navigation source in global navigation satellite systems (GNSS)-challenged environments. Along with terrestrial SOPs, low Earth orbit (LEO) satellite signals are particularly attractive for navigation [10–15]. Private companies, such as OneWeb, SpaceX, Boeing, and others are planning to launch thousands of

broadband Internet satellites into LEO, which increases the availability of these signals. Adapting the broadband protocols to support navigation capabilities due to the simpler receiver architectures and navigation algorithms have been considered in some studies [11]. However, this adaptation comes at the cost of significant changes to existing infrastructures. Consequently, private companies may not be willing to pay for these extra costs, and if they do so, it is likely that they would charge for the extended positioning services they would offer. To circumvent this, one could exploit the signals of both existing and future broadband LEO satellites in an opportunistic fashion [13, 15–17].

One of the main challenges of opportunistic navigation via SOPs transmitted by private broadband systems, e.g., LEO broadband satellites, is that the signal specifications of these SOPs may not be available to the public. This limitation makes acquiring and tracking these satellite signals impossible. As such, designing receivers that can blindly acquire partially known signals is an emerging need for the future of opportunistic navigation. In this paper, a blind opportunistic navigation (BON) framework is introduced to tackle this problem. Assuming that the SOP follows a standard modulation, e.g. code-division multiple access (CDMA) or orthogonal frequency-division multiplexing (OFDM), a BON framework recovers the partially known signal's structure to provide a navigation solution in the absence of GNSS signals. Most communication systems employ a synchronization beacon for receiver timing and carrier recovery. For example, in cellular CDMA, pseudorandom noise (PRN) sequences are used on the forward-link pilot channel for synchronization proposes [18]. Other examples of such beacons are the primary synchronization signal (PSS) and secondary synchronization signal (SSS) in cellular long-term evolution (LTE) systems. Even though different broadband services may use known modulation schemes, their underlying configuration and parameters can be different. For instance, the Globastar satellite system supposedly uses similar protocol to the IS-95 cellular CDMA system but with different PRN sequences [18]. As such, a crucial stage in the architecture of a BON framework is to blindly detect the unknown PRN sequence of the SOP in an online fashion or in a pre-navigation training stage.

The problem of discovering the unknown signal characteristics has been considered in both communications and navigation literature, e.g., see [19–24]. The algorithms for blindly detecting PRN sequences proposed in the communications literature rely on coherently integrating samples of the transmitted signals [19–24]. However, such approaches do not account for the time-varying Doppler shifts and delays, which make it impossible to accumulate enough signal power to detect the PRN sequence. Alternative approaches make use of high-gain antennas to accumulate enough signal power for PRN sequence detection [21]. Some algorithms to decipher the signals from Galileo and Compass satellites are presented in [21], which gives an insight into overcoming the challenges in discovering the unknown signal characteristics of a transmitting source. In contrast with these approaches, the BON framework has the flexibility of *cognitively* detecting the unknown PRN sequence of any broadband signal transmitter which uses a particular communication standard, e.g. CDMA. Therefore, unlike [21], which concentrates on deciphering one particular system, the BON framework is able to cognitively decipher partially known SOPs via a detection algorithm with a reasonable computational complexity and an acceptable detection performance.

This paper considers the problem of cognitive deciphering of partially known SOPs via a joint detection and estimation of unknown characteristics of SOPs for navigation purposes. For the BON framework, the Doppler frequency, the modulation type, and the length and symbols of the beacon signal are not assumed to be known, but only the bandwidth of the SOP is known. The main contributions of the paper are as follows. The notion of BON to enable acquisition and tracking of partially known SOPs is introduced. Next, computationally efficient algorithms for *blind signal detection* and *blind Doppler estimation* are proposed. Finally, the proposed BON framework is applied to decipher the PRN sequences of GPS satellites. Experimental results are presented demonstrating a percentage of correctly decoded chips for these four PRN sequences ranging between 91% and 99%. These deciphered sequences are fed to a software-defined Rx (SDR), which produce a two-dimensional (2-D) position error of 54.5m for a stationary antenna.

The rest of the paper is organized as follows. Section II formulates the BON notion. Section III describes the architecture of the BON framework and presents the blind Doppler estimation and beacon signal detection algorithms. Section IV presents experimental results validating the proposed BON framework on real GPS signals. Finally, Section V gives concluding remarks.

II. PROBLEM FORMULATION AND SYSTEM MODELS

A. Problem Formulation

The main challenge a BON framework aims to address is the partially known nature of the SOPs it aims to cognitively decipher, acquire, and track. *Cognitive deciphering* in the BON framework refers to blind detection and tracking of the beacon signals, which in turn allows us to exploit the received signals for positioning and navigation purposes. Beacon signal detection requires estimating a number of unknown parameters from the observations, given partially known information about the SOP. For the BON framework, the Doppler frequency, the modulation type, and the length and symbols of the beacon signal are not necessarily known to the receiver. The receiver has knowledge of the bandwidth of the SOP only. Modulation classification and unknown signal length estimation are widely investigated in the literature, e.g., see [25]. In this paper, without loss of generality, the length of the beacon signal is assumed to be known (e.g., previously estimated using methods in [25]). Moreover, assuming the very likely scenario that the beacon signal symbols are drawn from an arbitrary M phase shift keying (MPSK) constellation, a heuristic method for estimating the order of the modulation type, i.e., M, is proposed.

It should be pointed out that, by definition, a beacon or pilot signal is a signal known by the receiver and is used for timing and carrier synchronization, e.g., the PRN sequence in 3G cdma2000 systems or the cyclic prefix (CP), SSS, or PSS in 4G LTE and 5G new radio (NR) systems. Correlation-based receivers are typically used to detect the presence of beacon or pilot signals and synchronize to them. Due to the properties of correlation-based receivers, the known beacon or pilot signals can still be detected reliably even at relatively low signal-to-noise ratios (SNRs). However, the beacon could be unknown and the signals' SNR could be too low for reliable blind detection. Consequently, coherent integration becomes crucial to increase the effective SNR of the received beacon signal. To be able to coherently integrate successive transmissions of the beacon signal, the Doppler frequency must be estimated. Even after increasing the effective SNR via coherent integration, a naive symbol-by-symbol detection approach of the beacon signal may fail. As such, a high-performance detection algorithm is needed to reliably estimate the beacon signal after coherent integration.

In summary, the three building blocks of a BON framework are: (i) blind Doppler estimation/tracking, (ii) coherent integration, and (iii) blind beacon detection/tracking. Once a blind estimate of the Doppler is produced, coherent integration is performed and the integrated signal is fed to an algorithm to estimate the symbols of the beacon sequence. The decoded beacon sequence is then used by an SOP navigation receiver, e.g., [26], [9], and [27], to acquire, track, and navigate with the received SOP.

B. Received Baseband Signal Model

Let $s(t)$ denote the beacon signal consisting of L consecutive symbols with symbol duration T_{symb}. Each symbol is drawn from an arbitrary MPSK constellation. The beacon signal is continuously transmitted at a period of $L \cdot T_{\text{symb}}$. After channel propagation and baseband sampling at an interval T_s, the received signal can be modeled as

$$y[n] = \sum_{i=-\infty}^{\infty} \alpha d_i \exp\left[j\left(2\pi \Delta f[n] n + \theta_0\right)\right] s[n - iL - n_d[n]] + w[n], \tag{1}$$

where $y[n]$ is the complex baseband sample at the nth time slot; $N = L\frac{T_{\text{symb}}}{T_s}$ is the length of the beacon in samples; $\Delta f[n] \triangleq f_D[n] T_s$ is the normalized Doppler frequency and f_D is the true Doppler frequency in Hz; θ_0 is the initial beat carrier phase; $w[n]$ models noise and interference; α is an unknown complex amplitude; d_i is a low rate data symbol drawn from the same constellation of the beacon signal, e.g., navigation bits in GPS signals; and n_d is the unknown delay of the received beacon signal which can be modeled as

$$n_d[n] = \left\lfloor \frac{t_d[n]}{T_s} \right\rceil, \qquad t_d[n] \triangleq t_{d_0} - \frac{\Delta f_D[n]}{f_c} n, \tag{2}$$

where t_{d_0} is the initial delay in seconds of the received beacon signal and f_c is the carrier frequency.

It is worth noting that the signal model in (1) is descriptive of the majority of BON scenarios. In some cases, (1) directly applies, i.e., the received signal consists purely of one signal of interest and observation noise. In other scenarios, such as CDMA-based communication systems, the presence of interference should also be taken into account. For example, there is a total of 128 logical channels multiplexed onto one cdma2000 forward-link channel: (i) one pilot channel, (ii) one sync channel, (iii) up to seven paging channels, and (iv) traffic on the remaining channels. Each of these logical channels is spread orthogonally by a 128-Walsh code, multiplexed with the rest of the channels, and the resulting signal is multiplied by a complex PRN sequence which consists of a pair of maximal-length sequences. The CDMA signal is then filtered to limit its bandwidth before transmission. In such a system, and CDMA systems in general, the signal on the pilot channel simplifies to the complex PRN sequence, which is the beacon of interest. Therefore, one can look at the CDMA signal as the sum of two terms: (i) the signal on the pilot channel, or the beacon signal, and (ii) the sum of the signals on the remaining channels. Due to the properties of Walsh codes and assuming the symbols on the sync, paging, and traffic channels are uncorrelated, one can model the sum of the signals on the remaining channels as noise. In fact, for a large number of logical channels such as in cdma2000, the *central limit theorem* practically applies and the resulting noise can be modeled as a zero-mean Gaussian random variable. Consequently, the CDMA signal can be modeled according to (1), where $s[n]$ is the beacon on the pilot channel, and $w[n]$ captures channel noise and interference from the rest of the logical channels.

III. THE BON FRAMEWORK

The core of the BON framework comprises: (i) detection of multiple SOPs, (ii) blind Doppler tracking, (iii) coherent accumulation, and (iv) beacon signal decoding (see Fig. 1).

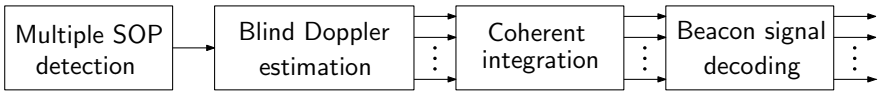

Fig. 1. BON framework.

This paper mainly focuses on the blind Doppler estimation and the beacon signal decoding steps. However, properly designed algorithms for signal activity detection of multiple SOPs in the bandwidth of interest and the coherent integration of the observations are essential steps to cognitively decipher the SOPs. It should be pointed out that signal activity detection of multiple SOPs may also include an additional modulation classification step to identify the modulation type of the beacon signals of the corresponding SOPs. Spectrum sensing techniques in cognitive radio systems, e.g, the energy detector [28], and blind modulation classification methods, e.g., [25] and the references therein, can be employed to detect the presence of SOPs and classify the modulation type of their beacon signal. In the BON framework developed in this paper, a heuristic algorithm for *joint signal activity detection and modulation classification* is presented. The algorithm performs a nonlinear operation to wipe-off the data symbols and turn the received signal into a pure tone. Then, the fast Fourier transform (FFT) of the resulting signal is taken to detect the tone and estimate its location in the frequency spectrum. For instance, for MPSK modulated data, raising the received signal to the power of M wipes off the data symbols. For an MPSK signal where M is unknown, the signal is raised to varying powers until a pure tone is observed in the FFT. The value of M for which the tone appears determines the order of the PSK modulation of the unknown signal. Next, the Doppler frequency of the resulting tone is tracked and the beacon symbols are subsequently decoded using the methods discussed in the following subsections. It is important to note that this operation can be performed simultaneously on multiple SOPs with different Doppler frequencies. In the sequel, M is assumed to be known via the aforementioned procedure.

A. Blind Doppler Estimation

A.1 Coherent Processing Interval for Doppler Estimation

As mentioned previously, blind Doppler estimation is one of the main challenges that has to be addressed in the BON framework. To this end, a blind Doppler estimation algorithm is discussed next. Define a coherent processing interval (CPI) of length I samples in which the Doppler frequency is assumed to be constant. Therefore, for a CPI index k, the Doppler within the kth CPI can be expressed as $f_D[n] = f_{D_k}$ for $kI \leq n \leq (k+1)I - 1$. The blind

Doppler estimator in the BON framework processes one CPI at a time to estimate the time history of the Doppler frequency. Define the vector of wiped-off observations in the kth CPI as

$$\bar{\boldsymbol{y}}_k^M \triangleq \left[(y[kI])^M, (y^M[kI+1])^M, \ldots, (y^M[(k+1)I-1])^M\right]^{\mathsf{T}}, \tag{3}$$

which can now be approximated by samples of a pure tone with normalized Doppler frequency $M\Delta f$. The Doppler tracking algorithm relies on estimating the frequency of this tone in each CPI, and is stated in Algorithm 1. Define the vector of estimated Doppler frequencies as

$$\hat{\boldsymbol{f}}_D^K \triangleq \left[\hat{f}_{D_0}, \hat{f}_{D_1}, \ldots, \hat{f}_{D_{K-1}}\right]^{\mathsf{T}}.$$

Algorithm 1 summarizes the steps to obtain $\hat{\boldsymbol{f}}_D^K$ from $\left\{\bar{\boldsymbol{y}}_k^M\right\}_{k=0}^{K-1}$.

Algorithm 1 Blind Doppler estimator

Input: $\left\{\bar{\boldsymbol{y}}_k^M\right\}_{k=0}^{K-1}$
Output: $\hat{\boldsymbol{f}}_D^K$
For $k \in \{0, \ldots, K-1\}$
- Find $\hat{b}_k = \arg\max\left\{\left|\mathrm{FFT}\left(\bar{\boldsymbol{y}}_k^M\right)\right|\right\}$.
- Calculate $\Delta\hat{f}_k = \begin{cases} \frac{\hat{b}_k}{M \cdot I} & \hat{b}_k \leq \frac{I}{2} \\ \frac{I-\hat{b}_k}{M \cdot I} & \hat{b}_k > \frac{I}{2} \end{cases}$
- Calculate $\hat{f}_{D_k} = \frac{\Delta\hat{f}_k}{T_s}$.

End

B. Coherent Integration

In this subsection, it is assumed that $I = N$. The following results can be extended to $I > N$. Given an estimate of the Doppler frequency, an estimate of the change in the beacon signal delay $\hat{t}_{d_k}$ at the kth CPI can be formed according to

$$\hat{t}_{d_k} = \sum_{l=0}^{k-1} \frac{\hat{f}_{D_l}}{f_c} NT_s.$$

Subsequently, the Doppler frequency can be wiped-off from the original observation, resulting in

$$\hat{y}_k[m] \triangleq y[m+kI] \exp\left[-j\left(2\pi\Delta\hat{f}_k m + \hat{\theta}_k\right)\right] \otimes \delta[m+kI-\hat{n}_{d_k}], \qquad 0 \leq m \leq N-1, \tag{4}$$

where $\hat{n}_{d_k} = \left\lfloor \frac{\hat{t}_{d_k}}{T_s} \right\rceil$, $\hat{\theta}_k \triangleq 2\pi f_c \hat{t}_{d_k}$ is the estimated carrier phase, and $\otimes$ denotes the circular convolution. Subsequently, F frames of the resulting signal are accumulated according to

$$\tilde{y}[m] = \frac{1}{F}\left(\hat{y}_0[m] + \sum_{k=0}^{F-1} \hat{d}_k \hat{y}_k[m]\right) \approx \alpha' s[m-n_0] + w'[m], \tag{5}$$

where $n_0 \triangleq \lfloor \frac{t_{d_0}}{T_s} \rfloor$ is the initial beacon signal delay; w' models the resulting noise; α' is a constant complex amplitude capturing the channel effect, initial beat carrier phase, and the residual Doppler; and $\hat{d}_k = \Pi_{\kappa=0}^k \tilde{d}_r$ is the estimate of the low rate data, where

$$\tilde{d}_r = \mathrm{sgn}\left\{\mathrm{Re}\left\{\sum_{m=0}^{N-1} \hat{y}_r[m]\hat{y}_{r-1}[m]^*\right\}\right\}; \tag{6}$$

where $\mathrm{Re}\{\cdot\}$ denotes the real part. Note that the signal part of the right-hand side of (5) is a shifted version of the beacon signal with a complex scaling. Let the vector $\boldsymbol{z}$ of length L denote the resampled vector $\tilde{\boldsymbol{z}} \triangleq [\tilde{y}[0], \ldots \tilde{y}[N-1]]^T$ down to the symbol rate. The vector $\boldsymbol{z}$ is then fed to the beacon decoding algorithm to decipher the beacon signal.

C. Blind Beacon Decoding

After wiping-off the Doppler, performing coherent integration, and resampling, the symbols of the beacon signal are decoded. The decoding problem can be modeled as

$$\boldsymbol{z} = \bar{\alpha}\boldsymbol{s} + \bar{\boldsymbol{w}}, \tag{7}$$

where $\bar{\alpha}$ is the unknown complex amplitude and $\bar{\boldsymbol{w}}$ the resulting noise vector after resampling. Consider the set $\mathcal{L}$ consisting of all M^L combinations of L-dimensional vectors $\boldsymbol{q}$ whose elements are the integers between 0 to $M-1$. For MPSK signals, a beacon sequence is given by $\boldsymbol{s} = \exp\left(\frac{j2\pi}{M}\boldsymbol{q}\right)$, where $\boldsymbol{q} \in \mathcal{L}$. The maximum likelihood (ML) decoder of $\boldsymbol{q}$ is

$$\hat{\boldsymbol{q}} = \arg\max_{\boldsymbol{q}\in\mathcal{L}} \left| \boldsymbol{z}^H \exp\left(\frac{j2\pi}{M}\boldsymbol{q}\right)\right|, \tag{8}$$

where $(\cdot)^*$ and $(\cdot)^H$ are the complex conjugate and Hermitian operators, respectively.

A naïve solution to the optimization problem (8) consists of a brute-force search over all possible values of $\boldsymbol{q}$, which has exponential complexity. The order of the brute-force search is M^L. In an effort to solve (8) in less than quadratic complexity, the methods described in [29] and later again in [30] are used to decode the beacon signal. It can be shown that the complexity of the algorithms proposed in [29] and [30] are on the order $L\log_2 L$.

IV. EXPERIMENTAL RESULTS

In order to demonstrate the capability of the BON framework in cognitively deciphering a signal of interest, an experiment was conducted with real GPS signals. The GPS L1 C/A signals contain PRN codes at 1.023 Mega chips per second (Mcps), modulated by binary PSK (BPSK) ($M = 2$) navigation bits at 50 bits per second (bps). Multiple GPS satellites transmit simultaneously in the same channel using CDMA. In what follows, the experimental setup is first described. Next, GPS PRNs are decoded using the BON framework. The decoded PRNs are then used in an SDR to produce pseudorange measurements on GPS satellites and in turn solve for a stationary receiver's position.

A. Experimental Setup

The setup consists of a GPS antenna, which was mounted on the roof of the Winston Chung Hall at the University of California, Riverside, USA. The GPS signals were down-mixed and sampled via a National Instruments universal software radio peripheral (USRP), driven by a GPS-disciplined oscillator (GPSDO). The samples of the received signals were stored for off-line post-processing.

B. Deciphering GPS PRNs with the BON Framework

B.1 Multiple Signal Detection

A heuristic method to detect and localize multiple SOPs in the frequency-domain was proposed in Section III. In order to detect and classify multiple SOPs, the observations are raised to the power of M to wipe off the PRNs and the low rate data symbols and detect the resulting pure tone. Since GPS satellites transmit BPSK signals, when the received signal is raised to the power $M = 2$, the data is wiped off and results in complex exponentials with twice the Doppler frequencies. This allows the BON framework to detect several satellites that transmit in the same channel, and multiple peaks will be seen in the Fourier transform of the dataless signal, as shown in Fig. 2.

B.2 Blind Doppler Estimation

Next, the peaks shown in Fig. 2 are tracked over time by performing Algorithm 1 on sequential CPIs of the stored samples, producing Doppler frequency estimates to each satellite, as shown in Fig. 3(b). The CPI is considered to be

$I = 120N$. The estimated Doppler was compared with the Doppler calculated from the known receiver position and the satellite positions obtained from the two-line element (TLE) files and orbit determination software (e.g., SGP4 [31]). TLE files contain the Keplerian elements parameterizing the orbits of LEO satellites and are made publicly available and updated daily by the North American Aerospace Defense Command (NORAD) [32]. As it can be seen in Fig. 3(b) and 3(c), the blind chirp parameter estimator successfully tracks the Doppler frequency of multiple SOPs producing negligible residuals when subtracted from the Doppler frequencies obtained from TLE and SGP4.

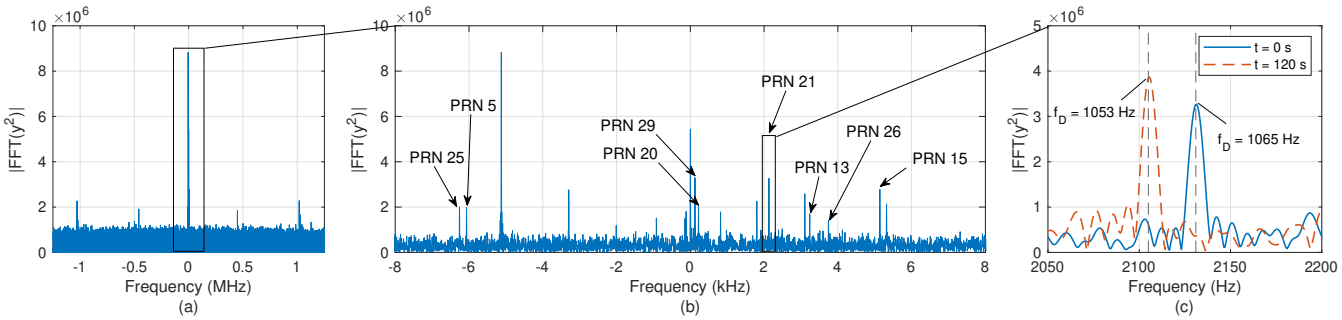

Fig. 2. (a) Joint signal activity detection and modulation classification of the beacon signals: Recall that the frequency component of power of two will be double that of the original signal. (b) Multiple satellite detection: FFT peaks corresponding to different GPS satellites. (c) FFT peaks of PRN 21 at $t = 0$ s and $t = 120$ s.

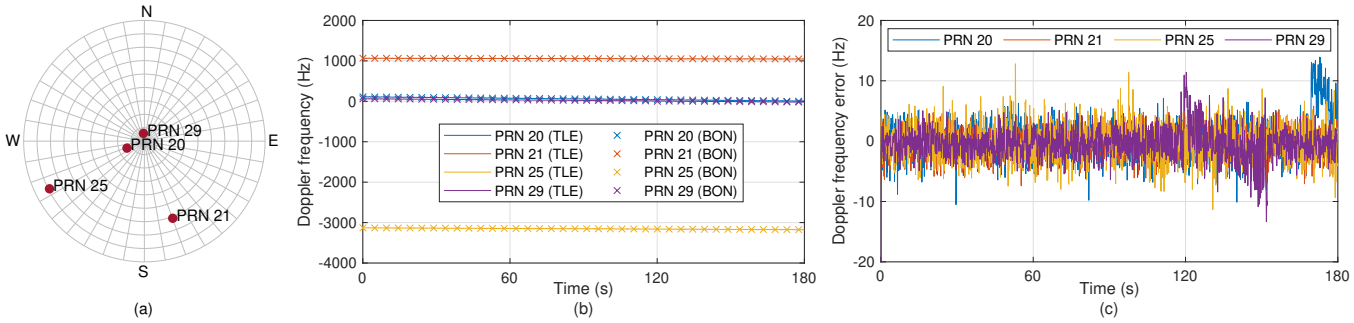

Fig. 3. (a) Skyplot of 4 of the visible GPS satellites. (b) Time history of (i) the Doppler frequency of 4 of the GPS satellites obtained from the TLE and SGP4 orbit determination software and (ii) the estimated Doppler frequencies of the corresponding satellites using the BON framework. (c) Errors between the Doppler frequencies obtained from the TLE and the ones obtained using the BON framework.

B.3 Beacon Signal Decoding

Once the Doppler frequencies are estimated, the residual carrier is wiped off from the received signal, compensated for delays due to Doppler, and coherently accumulated. The navigation bits are wiped off by two successive frames to determine whether a transition occurred or not. The resulting accumulations are decimated to the chipping rate of GPS PRNs and processed by the beacon decoding algorithm of the BON framework. A scatter plot of the accumulated signal before beacon signal decoding is shown in Fig. 4(a) for the 4 satellites. While the scatter plots of PRNs 20, 21, and 25 look significantly noisy, their effective SNR is high enough for the blind beacon decoding algorithm to decode the PRNs with less than 10% chip error, as shown in Table I. The correlation function between the decoded and true PRNs of the 4 GPS satellites are shown in Fig. 4(b). In addition to Table I, the correlation plots in Fig. 4(b) also demonstrate that the PRN of each of the 4 satellites was adequately decoded.

TABLE I

THE PERCENTAGE OF CORRECTLY DECODED GPS PRN CHIPS USING THE BON FRAMEWORK

PRN number	PRN 20	PRN 21	PRN 25	PRN 29
Percentage of correctly decoded Chips	96%	94%	91%	99.9%

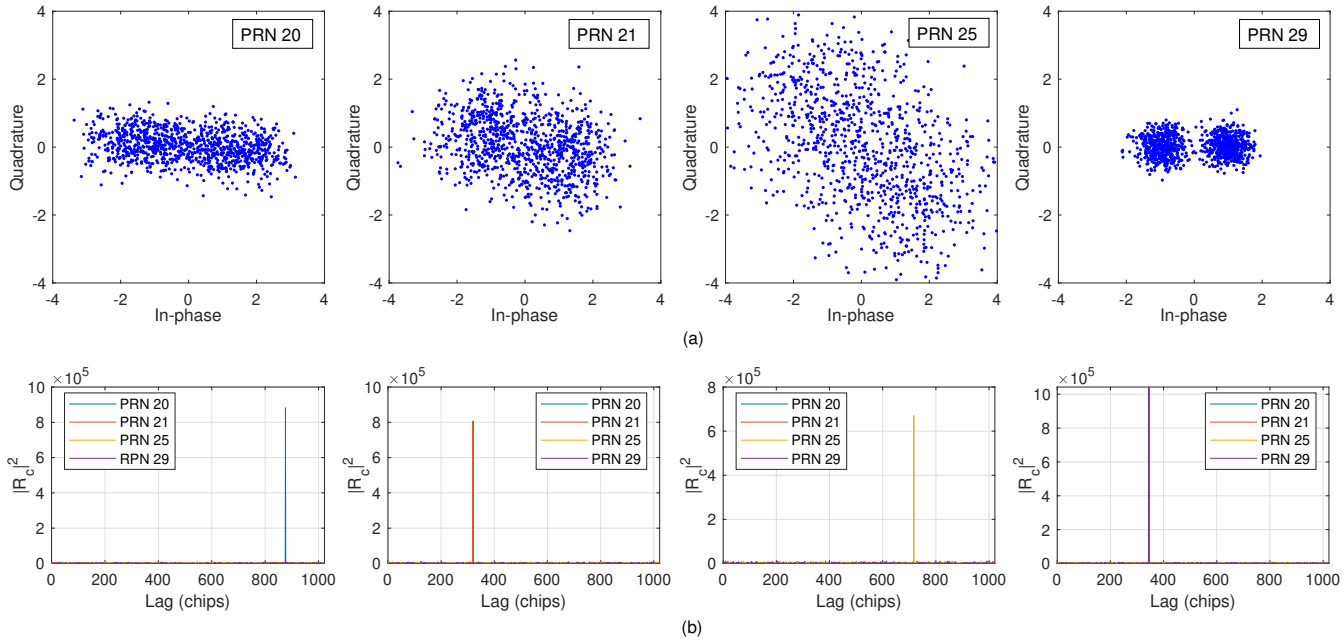

Fig. 4. (a) Scatter plots of the coherent accumulation for the 4 satellites before beacon detection. (b) Correlations between the decoded PRN of each satellite and the true PRNs.

B.4 Producing Navigation Observables from Decoded PRNs

The decoded beacons are then used to produce pseudorange observables from the received GPS signals. The initial Doppler is known from the previous steps. The code phases are also known to be zero, since the decoded beacon has the phase of the PRN at the time of initial reception. Therefore, signal acquisition is already performed; however, it is shown in Fig. 5(a) for illustration purposes. The initial Doppler and code phase estimates are used to initialize an SDR's tracking loops: a third-order phase-locked loop (PLL) with a carrier-aided delay-locked loop (DLL) with the dot product discriminator. The in-phase and quadrature components of the tracked prompt correlation for PRN 21 are shown in Fig. 5(b) for a period of 5 seconds. Since GPS signals are exploited opportunistically in this paper, it is not assumed that the receiver can decode the navigation message. As a result, the code phase estimate expressed in meters will be considered as the pseudorange estimate. The delta range of PRN 21 measured using the BON framework is shown in Fig. 5(c) along with the delta range estimated via TLE and SGP4 software. The delta range is a pseudorange from which the initial value is subtracted.

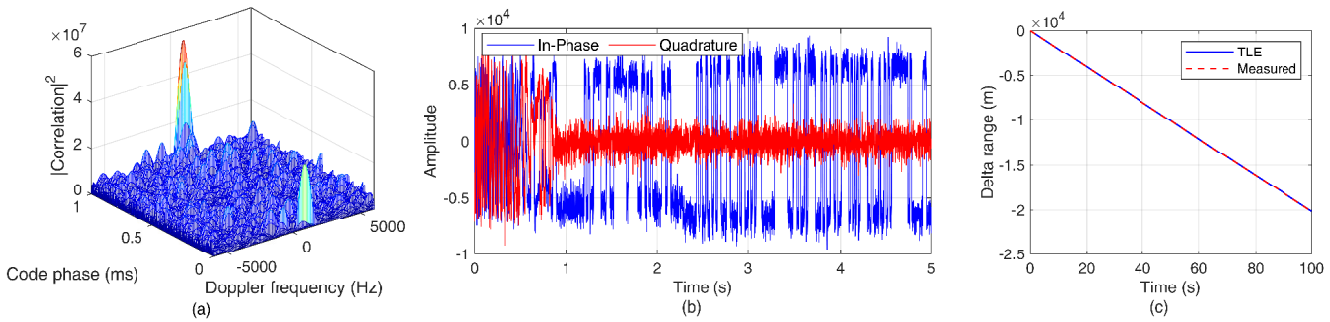

Fig. 5. (a) Signal acquisition for PRN 21 using the decoded beacon. (b) Signal tracking of PRN 21 over a period of 5 seconds. (c) Delta range computed from the TLE and the code phase measured by the BON receiver expressed in meters.

C. Navigation Solution

This section presents the navigation solution from the BON framework. The altitude $r_{r,z}$ of the stationary antenna which collected the GPS signals is assumed to be known; hence, only the two-dimensional (2-D) states $r_{r,x}$ and $r_{r,y}$ are estimated. The pseudorange from the ith satellite at time-step k can be modeled as

$$\rho_i(k) = \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}(k)\|_2 + b_i + \epsilon_i(k), \qquad k = 1, 2, \ldots, \tag{9}$$

where $\boldsymbol{r}_r \triangleq [r_{r,x}, r_{r,y}, r_{r,z}]^{\mathsf{T}}$ is the three-dimensional (3-D) position of the receiver, $\boldsymbol{r}_{s_i}$ is the 3-D position vector of the ith satellite obtained from the TLEs, b_i is a bias term that captures the unknown bias between the receiver's and ith satellite's clocks, and ϵ_i is the measurement error capturing ionospheric and tropospheric delays and measurement noise. The pseudorange measurements for all satellites at all time-steps are stacked in one measurement vector $\boldsymbol{\rho}$ and a batch nonlinear least-squares (NLS) estimator is implemented to solve for $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, b_1, \ldots, b_S\right]^{\mathsf{T}}$, where S is the total number of visible satellites. The receiver's position in the NLS was initialized around 150 km from the true receiver's position, and all the biases $\{b_i\}_{i=1}^{S}$ were initialized with zeros. The resulting position error with 4 satellites over a 110-second period was found to 54.4 meters. The experimental setup and results are shown in Fig. 6.

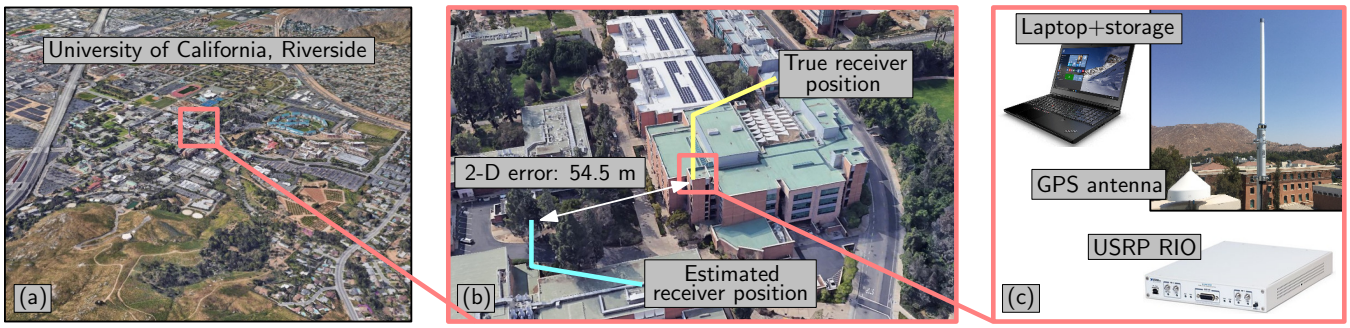

Fig. 6. (a) Experimental environment. (b) True and estimated receiver positions. (c) Experimental hardware setup.

V. CONCLUSION

This paper proposed a BON framework to exploit SOPs with partially known signal specifications. Two main challenges of BON were addressed. First, a blind Doppler tracking algorithm was proposed to estimate the Doppler frequencies of detected SOPs. Second, a blind decoding algorithm was proposed to decode the unknown beacon signals transmitted by SOP emitters. The BON framework was applied to decipher the GPS satellites' PRN codes from L1 C/A signals. The experimental results show that the BON framework is capable of cognitively decoding the PRNs of GPS satellites with a percentage of correctly decoded chips ranging between 91% and 99%. The PRNs decoded by the BON framework were used to produce a navigation solution, which was only 54.5 m away from the true position.

ACKNOWLEDGMENTS

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-19-1-2511 and in part by the National Science Foundation (NSF) under Grant 1929965.

References

[1] J. McEllroy, "Navigation using signals of opportunity in the AM transmission band," Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, 2006.

[2] S. Fang, J. Chen, H. Huang, and T. Lin, "Is FM a RF-based positioning solution in a metropolitan-scale environment? A probabilistic approach with radio measurements analysis," *IEEE Transactions on Broadcasting*, vol. 55, no. 3, pp. 577–588, September 2009.

[3] R. Faragher and R. Harle, "Towards an efficient, intelligent, opportunistic smartphone indoor positioning system," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 55–72, 2015.

[4] J. Khalife, Z. Kassas, and S. Saab, "Indoor localization based on floor plans and power maps: Non-line of sight to virtual line of sight," in *Proceedings of ION GNSS Conference*, September 2015, pp. 2291–2300.

[5] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2016.

[6] A. Tahat, G. Kaddoum, S. Yousefi, S. Valaee, and F. Gagnon, "A look at the recent wireless positioning techniques with a focus on algorithms for moving receivers," *IEEE Access*, vol. 4, pp. 6652–6680, 2016.

[7] Z. Kassas, J. Khalife, K. Shamaei, and J. Morales, "I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals," *IEEE Signal Processing Magazine*, pp. 111–124, September 2017.

[8] J. Khalife and Z. Kassas, "Navigation with cellular CDMA signals – part II: Performance analysis and experimental results," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2204–2218, April 2018.

[9] K. Shamaei, J. Khalife, and Z. Kassas, "Exploiting LTE signals for navigation: Theory to implementation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173–2189, April 2018.

[10] D. Lawrence, H. Cobb, G. Gutt, M. OConnor, T. Reid, T. Walter, and D. Whelan, "Navigation from LEO: Current capability and future promise," *GPS World Magazine*, vol. 28, no. 7, pp. 42–48, July 2017.

[11] T. Reid, A. Neish, T. Walter, and P. Enge, "Broadband LEO constellations for navigation," *NAVIGATION, Journal of the Institute of Navigation*, vol. 65, no. 2, pp. 205–220, 2018.

[12] R. Landry, A. Nguyen, H. Rasaee, A. Amrhar, X. Fang, and H. Benzerrouk, "Iridium Next LEO satellites as an alternative PNT in GNSS denied environments–part 1," *Inside GNSS Magazine*, pp. 56–64., May 2019.

[13] Z. Kassas, J. Morales, and J. Khalife, "New-age satellite-based navigation – STAN: simultaneous tracking and navigation with LEO satellite signals," *Inside GNSS Magazine*, vol. 14, no. 4, pp. 56–65, 2019.

[14] J. Khalife, M. Neinavaie, and Z. Kassas, "Navigation with differential carrier phase measurements from megaconstellation LEO satellites," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2020, pp. 1393–1404.

[15] Z. Kassas, J. Khalife, M. Neinavaie, and T. Mortlock, "Opportunity comes knocking: overcoming GPS vulnerabilities with other satellites' signals," *Inside Unmanned Systems Magazine*, pp. 30–35, June/July 2020.

[16] J. Khalife and Z. Kassas, "Receiver design for Doppler positioning with LEO satellites," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2019, pp. 5506–5510.

[17] J. Khalife and Z. Kassas, "Assessment of differential carrier phase measurements from orbcomm LEO satellite signals for opportunistic navigation," in *Proceedings of ION GNSS Conference*, September 2019, pp. 4053–4063.

[18] L. Schiff and A. Chockalingam, "Signal design and system operation of Globalstar TM versus IS-95 CDMA – Similarities and differences, year = 2000, volume = 6, number = 1, pages = 47–57, month = February,," *Wireless Networks*.

[19] M. Tsatsanis and G. Giannakis, "Blind estimation of direct sequence spread spectrum signals in multipath," *IEEE Transactions on Signal Processing*, vol. 45, no. 5, pp. 1241–1252, May 1997.

[20] M. Tanda, "Blind symbol-timing and frequency-offset estimation in OFDM systems with real data symbols," *IEEE Transactions on Communications*, vol. 52, no. 10, pp. 1609–1612, October 2004.

[21] G. Gao, "Towards navigation based on 120 satellites: Analyzing the new signals," Ph.D. dissertation, Stanford University, 2008.

[22] W. Liu, J. Wang, and S. Li, "Blind detection and estimation of OFDM signals in cognitive radio contexts," in *International Conference on Signal Processing Systems*, vol. 2, July 2010, pp. 347–351.

[23] T. Zhang, S. Dai, W. Zhang, G. Ma, and X. Gao, "Blind estimation of the PN sequence in lower SNR DS-SS signals with residual carrier," *Digital Signal Processing*, vol. 22, no. 1, pp. 106–113, 2012.

[24] Y. Wei, L. Liu, and J. Zhang, "Blind estimation of PN sequence of DS-CDMA signal in multipath," in *Proceedings of International Conference on Consumer Electronics, Communications and Networks*, 2012, pp. 1695–1699.

[25] O. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: Classical approaches and new trends," *IET communications*, vol. 1, no. 2, pp. 137–156, 2007.

[26] J. Khalife, K. Shamaei, and Z. Kassas, "Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2191–2203, April 2018.

[27] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *NAVIGATION, Journal of the Institute of Navigation*, vol. 65, no. 4, pp. 655–675, December 2018.

[28] W. Lee and I. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless communications*, vol. 7, no. 10, pp. 3845–3857, 2008.

[29] K. M. Mackenthun, "A fast algorithm for multiple-symbol differential detection of mpsk," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1471–1474, February 1994.

[30] W. Sweldens, "Fast block noncoherent decoding," *IEEE Communications Letters*, vol. 5, no. 4, pp. 132–134, April 2001.

[31] J. Vetter, "Fifty years of orbit determination: Development of modern astrodynamics methods," *Johns Hopkins APL Technical Digest*, vol. 27, no. 3, pp. 239–252, November 2007.

[32] North American Aerospace Defense Command (NORAD), "Two-line element sets," http://celestrak.com/NORAD/elements/.