This article presents a receiver that could exploit downlink orthogonal frequency-division multiplexing (OFDM)-based cellular signals to navigate opportunistically to meter-level accuracy in a real-world GPS-denied environment. The proposed receiver exploits signals from multiple logical antenna ports simultaneously, which dramatically improves the receiver’s sensitivity. The efficacy of the proposed receiver is demonstrated experimentally in an environment under intentional GPS jamming, in which the ground vehicle-mounted receiver navigated for 5 km in 180 s. The receiver was able to acquire and track signals from seven long-term evolution (LTE) eNodeBs, one of which was more than 25 km away, achieving a 2-D position root mean-squared error (RMSE) of 2.6 m.

I. INTRODUCTION

The past decades have witnessed extensive research to utilize cellular signals for navigation purposes. Among various cellular generations, 4G and 5G orthogonal frequency-division multiplexing (OFDM)-based systems have shown tremendous promise [1], [2]. Cellular navigation approaches can be categorized into: network-based and user-based. This article considers the latter approach, in which the user equipment (UE) exploits downlink signals, in an opportunistic fashion, from any cellular provider without being a subscriber in the network.

Previous studies have demonstrated meter-level and submeter-level positioning accuracy on the ground vehicles and unmanned aerial vehicles, respectively, with 4G and 5G signals [3], [4], [5], [6], [7], [8], [9], [10], in which synchronization reference signals (RSs) were exploited to extract navigation observables [11], [12]. A particularly desirable RS for navigation is the cell-specific RS (CRS), due to its high bandwidth. Due to OFDM’s spectral nature, the CRS is transmitted on distinct OFDM symbols and subcarriers,
also known as logical ports. In [13], a maximum likelihood-based method to estimate the first path was proposed, which utilized one antenna port. Positioning in multipath environments was studied in [14] and [15], both of which considered one antenna port. A recent study developed a tracking algorithm that adaptively mitigated multipath in long-term evolution (LTE) positioning receivers, while utilizing CRS from one antenna port [4]. The effect of antenna ports on time-of-arrival (TOA) estimation using CRS was investigated in [16]. The study showed that different channel responses were recorded for different antenna ports, which can diversify the incoming signals and improve positioning. The signal diversity provided via multiple antenna ports was exploited for cycle slip detection in the LTE carrier phase measurements in [3]. Exploiting two antenna ports was considered in [17], where signals from each port was treated as a separate measurements, while [18] tracked signals from each port independently. However, none of the aforementioned studies considered the simultaneous exploitation of all antenna ports as a single navigation source. In general, to extract navigation observables from OFDM signals, existing methods have approached the receiver design from a communication systems perspective [15].

This article exploits additional LTE available resources in generating the receiver’s locally generated code, which offers two advantages: 1) construct a pseudorandom noise (PRN)-like code that possesses a higher bandwidth; thus, improving the precision of TOA estimates; and 2) increase the power by exploiting more available resource elements. The acquisition of LTE signals can be modeled as a detection problem. Increasing the power results in an increase in the carrier-to-noise ratio (CNR), which in turn results in a better probability of detection. Moreover, in terms of estimation of the code and carrier phase, it is known that the phase estimation errors depend on the CNR and the correlation properties [19]. Exploiting the CRS corresponding to all the antenna ports results in less code and carrier phase error (better tracking performance), leading to more precise navigation observables.

This article presents a novel opportunistic OFDM-based navigation receiver design that exploits all available resources from various antenna ports simultaneously. Unlike previous generation receivers, the proposed receiver exploits the orthogonality property of OFDM signals without the need for reconstructing the received OFDM frame. The proposed approach significantly improves the receiver’s sensitivity, amplifying the received power by a factor up to 120 while also improving the carrier phase estimation accuracy. Experimental results in a real-world GPS-denied environment are presented to demonstrate the efficacy of the proposed receiver. A ground vehicle was driven at Edwards Air Force Base (AFB), California, USA, during NAVFEST: a live GPS jamming event with high-powered jammers transmitting a variety of waveforms at a jamming-to-signal ratio ($J/S$) exceeding 100 dB. A previous state-of-the-art LTE navigation receiver [20] was able to acquire and track only one LTE eNodeB as far as 5 km away, achieving a 2-D position root mean-squared error (RMSE) of 29.4 m over a trajectory of 5 km [21]. In contrast, the proposed receiver was able to acquire and track 7 LTE eNodeBs with favorable geometry, one of which was more than 25 km away, achieving a 2-D position RMSE of 2.6 m. To the authors’ knowledge, the proposed design represents the most sensitive OFDM receiver to date, achieving unprece-dented navigation accuracy in an exclusive GPS-denied environment.

The rest of this article is organized as follows. Section II overviews the LTE OFDM frame structure and discusses the idea behind exploiting the transmitter’s multiple antenna ports. Section III presents the proposed time-domain-based receiver design. Section IV shows experimental results in a real-world GPS-jammed environment, demonstrating the superiority of the proposed receiver to previous receiver design. Finally, Section V concludes this article.

II. FRAME STRUCTURE: EXPLOITING MULTIPLE ANTENNA PORTS

The Third Generation Partnership Project (3GPP) standard defines what is known as an antenna port for 4G LTE cellular system. Antenna ports do not necessarily correspond to physical antennas, but rather, they are logical entities distinguished by their reference sequences [22]. A single logical antenna port can include multiple RSs that correspond to the same physical antenna. Correspondingly, a single antenna port can be spread across multiple transmit antennas. The formal definition of an antenna port is: “An antenna port is defined such that the channel over which an OFDM symbol on the antenna port is conveyed can be inferred from the channel over which another symbol on the same antenna port is conveyed [23].” There is one resource grid per antenna port, and the antenna ports used for transmission of a physical channel or signal depends on the number of antenna ports configured for the physical channel or signal.

This article proposes an opportunistic navigation approach; thus, it only considers the downlink signals, which use OFDM with cyclic prefix (CP) as its modulation. An LTE OFDM frame has a duration of 10 ms. The subcarrier spacing in LTE is fixed and defined as $\Delta f = 15$ kHz. In the time-domain, each subframe breaks down into multiple OFDM symbols. In the frequency-domain, a slot can be decomposed into multiple resource elements (REs). Thus, the subcarrier and symbol are the frequency and time indices of an RE, respectively. Further details about the LTE frame structure can be found in [20].

Fig. 1 shows CRS allocation within the LTE OFDM frame for all antenna ports. The number of subcarriers in an LTE frame $N$, and the number of used subcarriers $N_r$, are not unique and are assigned by the network provider. They can only take the values that are tabulated in Table I [23]. The subcarrier spacing is typically $\Delta f = 15$ kHz. Hence, the occupied bandwidth can be calculated using $W = N_r \Delta f$ (which, here, equals 20 MHz, after adding a 2 MHz guard band). The CRS spans the entire bandwidth of the 4G LTE system and is known to the UE. For CRS, the associated
antenna ports $p$ can be $p = 0$, or $p \in \{0, 1, 2, 3\}$. Although, by definition, different antennas do not have to correspond to different physical antennas for the various LTE RSs, the CRS is a special RS that has a one-to-one mapping between logical and physical antennas. For LTE, there are 504 possible eNodeB physical Cell IDs, leading to 504 possible URS sequences resulting from the possible CRS sequences. In the proposed receiver, different sectors of the same eNodeB, i.e., Cell IDs with different primary synchronization signal (PSS) but the same secondary synchronization signal (SSS) is combined to form the proposed URS. In other words, the three sectors of a particular eNodeB will have one unique URS, which is generated once as a local code in the receiver. As a result, the correlation of signals coming from different sectors of a particular eNodeB with its corresponding locally generated URS can be considered as the coherent summation of the correlation of signals coming from every sector of a particular eNodeB with the locally generated URS.

While previous work in the literature only exploited the CRS from one antenna port ($p = 0$), this article exploits the CRS from all antenna ports $p \in \{0, 1, 2, 3\}$ simultaneously. This is achieved by adopting a novel representation of an OFDM frame to obtain navigation observables. Detecting active CRS subcarriers is a challenging problem that requires reconstructing the OFDM frame, while tracking the signal for each received frame. In conventional receivers, the timing sequences (PSS and SSS) are used to detect the OFDM frame start time. Then, the CRSs corresponding to one antenna port are detected in the frame and exploited for navigation. In general, conventional OFDM-based receivers in communication and navigation systems use the following steps for timing and synchronization: 1) estimation of the frame start time for each individual OFDM frame; 2) reconstruction of the OFDM frame; 3) detection of the CRS subcarriers; and 4) exploiting the CRS to estimate the channel impulse response (for communication purposes) and provide the navigation observable, e.g., TOA (for navigation purposes). This article proposes an unorthodox method to exploit the CRSs of different antenna ports for navigation purposes, which allows the receiver to track the code and carrier phase in a way that is similar to a GPS receiver. Recall that the GPS receiver regenerates a replica of the satellites’ PRN code. Generating a PRN-like code in OFDM-based systems is more challenging: other CRSs corresponding to different antenna ports are spread among different subcarriers. The idea presented in this article is to use the time series representation of an OFDM frame as a code (similar to GPS PRN). The time series representation of the OFDM frame should contain all the available resources (including the PSS, SSS, and CRSs corresponding to all antenna ports), and is referred to as the ultimate reference signal (URS). In this article, in order to generate the URS, the subcarriers corresponding to all antenna ports are used. After reconstruction of the OFDM frame (which is performed only once at the receiver) and considering all the available resource elements, including the CRSs corresponding to all antenna ports, the time representation of the frame (i.e., the URS) is used as a PRN-like code in the GPS-like tracking loops. The phase-locked-loop (PLL) and the delay-locked loop (DLL) track the carrier and code phases of the URS, respectively, eliminating the need to reconstruct the frame and detect the CRS at every time epoch corresponding to the frame start time.

In state-of-the-art opportunistic LTE receiver in [20], only one OFDM symbol of the CRS resources corresponding to $p = 0$ was exploited, as shown in blue in Fig. 1. Two metrics are defined to compare state-of-the-art receiver with the proposed receiver.

1) $r_{B,RS}$: bandwidth ratio of the RS versus the entire downlink bandwidth of the LTE signal. Higher $r_{B,RS}$ means narrower autocorrelation function (ACF), which results in more precise TOA estimation.

2) $r_{T,RS}$: duty factor, i.e., the percentage of time in which the RS is active. Higher $r_{T,RS}$ results in a more accurate carrier phase and Doppler estimation.

The state-of-the-art receiver has $r_{T,RS} = \frac{1}{140} = 0.71\%$ (only one OFDM symbol is active), where 140 is the total number of OFDM symbols in an OFDM frame. In the proposed approach, the various available ports are utilized.

![Figure 1](CRS allocation within the LTE OFDM frame for all antenna ports. The vertical axes show the subcarrier index of each resource element, while the horizontal axes show the symbol index. In the lower figure, one subframe that consists of 14 symbols is zoomed upon to better illustrate the spread of CRS across subcarriers and symbols.)
III. PROPOSED TIME-DOMAIN RECEIVER

This section presents a time-domain-based receiver that operates on the proposed URS to exploit time orthogonality and extract navigation observables from the received LTE signals. State-of-the-art LTE navigation receivers only consider the orthogonality of the synchronization and channel estimation RSs in the frequency-domain, i.e., the transmitted OFDM frame is always reconstructed from the received time-domain serial data. Then, the navigation observables are estimated by utilizing the RS with the highest bandwidth. This approach was adopted from a communication perspective, in which it is necessary to reconstruct the OFDM frame to extract various system information, which allows two-way communication between the UE and the eNodeB. However, for opportunistic UE-based navigation, the ultimate goal is to obtain navigation observables by utilizing the most available frequency (bandwidth) and time (duty factor) resources in the received signal. The proposed receiver exploits all available REs, which are combined and used simultaneously in a time-domain-based URS denoted by $URS_i$, where $i$ is the eNodeB physical Cell ID. The rest of the section presents: 1) URS generation; and 2) receiver stages: acquisition and tracking.

A. URS Generation

In the frequency-domain, the CRS sequences corresponding to different antenna ports and subframes are generated and mapped to the OFDM frame according to [24, Sec. 6.10.1]. After allocating all CRS REs in the OFDM frame and assigning zero to the rest of the REs. The resulting frame represents the frequency-domain URS denoted as $URS_i^f$. The $URS_i^f$ is converted into a serial time-domain-based sequence $URS_i$, by zero-padding $\frac{1}{2}N_{RB}^{max,DL} - N_{RB}$ REs on both sides of the signals in the frequency-domain. Then, the IFFT is taken, and the CP elements are added, which are nothing but an identical copy of the portion of the OFDM symbol appended before the OFDM symbol to prevent intersymbol interference (ISI). This procedure is the exact procedure occurring at the eNodeB, except for having zeros instead of having data in the data allocated REs, which is a necessary condition to prevent interference and guarantee orthogonality of the $URS_i^f$.
Fig. 4. Environment layout and J/S heatmap. The ground vehicle vehicle’s trajectory is within the dashed white rectangle.

B. Acquisition and Tracking

After generating the URS, acquisition is performed to determine eNodeBs in the UE’s proximity and find their corresponding coarse estimates of code phase and Doppler shift. Next, GPS-like receiver tracking loops (as in [25]) can be employed to refine these estimates and produce navigation observables. This can be done by essentially replacing the GPS code generator by the URS generator.

IV. EXPERIMENTAL RESULTS

This section presents an experimental demonstration of the proposed receiver mounted on a ground vehicle navigating in a real-world GPS-denied environment. A mapping campaign was conducted before the experiment to locate LTE eNodeBs in the environment. The vehicle was driven in the Mojave Desert at Edwards AFB, California, USA, during the intentional GPS jamming exercises, known as NAVFEST. The vehicle’s trajectory was composed of three segments: 1) GPS signals were available (0–40 s; 1.1 km); 2) GPS signals were intermittent (40–50 s; 0.4 km); and 3) GPS signals were not available (50–180 s; 3.5 km).

A. Hardware Setup

Six high-power jammers and one portable box jammer were spread over an area of approximately 50 miles north of Edwards AFB. Fig. 4 shows the J/S heatmap; which actually extends outside the depicted rectangle; however, this was the only data provided by Edwards AFB.

The ground vehicle, shown in Fig. 4, was equipped with a National Instrument (NI) universal software radio peripheral (USRP), two consumer-grade Laird cellular antennas, PCIe cable, laptop, and a Septentrio GNSS-inertial measurement unit (IMU) system, comprising a multifrequency GNSS AsteRx-i V receiver, an industrial-grade Vectornav VN-100 micro-electromechanical system (MEMS) IMU, and a dual-GNSS antenna system. The vehicle-mounted GNSS-IMU was used to obtain the vehicle’s ground truth trajectory, utilizing signals from nonjammed GNSS constellations (Galileo and GLONASS). The USRP utilized a GNSS-disciplined oscillator (GNSSDO) and was tuned to listen to two carrier frequencies corresponding to the TABLE II

eNodeBs’ Characteristics

<table>
<thead>
<tr>
<th>eNodeB</th>
<th>Carrier frequency</th>
<th>Cell ID</th>
<th>Cellular provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>751 MHz</td>
<td>417</td>
<td>Verizon</td>
</tr>
<tr>
<td>2</td>
<td>751 MHz</td>
<td>399</td>
<td>Verizon</td>
</tr>
<tr>
<td>3</td>
<td>751 MHz</td>
<td>393</td>
<td>Verizon</td>
</tr>
<tr>
<td>4</td>
<td>751 MHz</td>
<td>402</td>
<td>Verizon</td>
</tr>
<tr>
<td>5</td>
<td>2145 MHz</td>
<td>186</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>6</td>
<td>2145 MHz</td>
<td>195</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>7</td>
<td>2145 MHz</td>
<td>489</td>
<td>T-Mobile</td>
</tr>
</tbody>
</table>

U.S. cellular providers: Verizon Wireless and T-Mobile, as tabulated in Table II.

B. Tracking Results

The receiver discussed in Section III was used to acquire and track signals from 7 LTE eNodeBs (see Fig. 4). A second-order PLL with a bandwidth of 6 Hz was employed to track the carrier phase, and a carrier-aided DLL whose loop filter is a simple gain $K = 0.2$ was used to track the code phase.

Fig. 5 shows the code phase tracking error. From Table II and Fig. 5, it can be inferred that the receiver was able to track LTE signals at 751 and 2145 MHz, with the tracking loops failing to track as the receiver drove further away from the eNodeBs. It is worth noting that not all seven eNodeBs
were continuously tracked along the entire trajectory. In particular, while eNodeB 1, 2, and 7 were continuously tracked along the receiver’s trajectory, eNodeBs 5 and 6 were tracked during the earlier part of the trajectory, while eNodeBs 3 and 4 were tracked during the latter part of the trajectory.

Fig. 6 shows the tracking results: 1) CNR; 2) pseudorange estimates versus expected ranges (the latter calculated from the receiver’s ground truth trajectory and eNodeBs’ positions); and 3) range error (i.e., difference between pseudorange and range). The CNR is calculated from $\text{CNR} = \frac{P - N_0}{N_0T}$, where $P$, $N_0$, and $T$ denote the received signal power, noise power, and subaccumulation time interval, which is set to the LTE frame duration.

From Fig. 6(a), it can be seen that the CNR for tracked eNodeBs is about 50 dB-Hz, with some of the closer eNodeBs having a CNR exceeding 75 dB-Hz. The intermittency in tracking is due to the receiver tracking loops failing to acquire/track all eNodeBs along the entire trajectory. From Fig. 6(b), it can be seen that eNodeBs 3 and 6 were tracked, while being 25.5 and 23.6 km, respectively, away from the vehicle. The drift in the range error in Fig. 6(c) is due to the combined receiver–eNodeB’s clock error, which is dominated by the eNodeB’s clock error, since the receiver possessed a GNSSDO. These drifts are indicative of the eNodeBs being equipped with high-quality oven-controlled crystal oscillators (OCXOs). The correlatedness observed among some of the eNodeBs could be due to the “loose” network synchronization: eNodeBs need to be synchronized, as per the 3GPP standards, with certain eNodeBs tend to exhibit tighter synchronization, forming so-called “clusters” [6]. It is worth noting in Fig. 6(c) starting segment (C), which is when GPS signals become completely unavailable, there seems to be an “inflection” point impacting the range error. It is speculated that this is due to the jamming impact on eNodeBs’ clocks; however, it is difficult to assert such a statement.

C. Navigation Solution

The navigation filter fused code phase measurements from all eNodeBs via an extended Kalman filter (EKF) to estimate the vehicle-mounted receiver’s 3-D position $r$, and velocity $\dot{r}$, and relative clock bias and drift between the receiver’s and eNodeBs’ clocks $\{\delta t_r, \delta t_s\}_{u=1}^7$ and $\{\delta t_s, \delta t_w\}_{u=1}^7$, respectively. As observed in [21], and due to the high vertical dilution of precision when using terrestrial eNodeBs alone, the vertical estimation error was much higher than the horizontal error. As such, 2-D navigation errors are reported and compared with those achieved in [21]. The EKF dynamics and measurement models are described in [21]. Using expressions relating CNR to measurement noise variances [20], the variances were found to vary between 0.2 and 22 m$^2$.

After traversing a trajectory of 5 km in 180 s, a 2-D position RMSE of 2.6 m and a 2-D maximum error of 4.5 m were achieved using only LTE signals, without using other sensors (see Fig. 7). This unprecedented accuracy is an order of magnitude lower than previously published results in the same environment and same collected raw LTE in-phase and quadrature samples, in which a 2-D position RMSE of 29.4 m was achieved [21]. While the state-of-the-art receiver in [21] was only able to acquire and track the 5 km-away eNodeB 1, the proposed receiver acquired and tracked weaker signals from eNodeBs 2–6. The GPS-IMU navigation solution exhibited a position RMSE of 237.9 m.

V. CONCLUSION

A high-sensitivity receiver was presented that could exploit downlink OFDM-based cellular signals from multiple logical antenna ports simultaneously. The efficacy of the receiver was demonstrated in a real-world GPS-denied environment, in which the receiver produced pseudorange estimates to 7 LTE eNodeBs. The pseudoranges were fused via an EKF to navigate a ground vehicle for 5 km in 180 s, achieving a 2-D position RMSE of 2.6 m. One of the eNodeBs was more than 25 km away. It is worth highlighting that while cellular frequencies were not directly jammed, it is known that cellular infrastructure timing is disciplined to GPS/GNSS timing. Nevertheless, despite GPS jamming, the cellular signals were profitably exploitable via the proposed receiver, while the timing of each cellular transmitter was estimated via the navigation filter. This enabled the
vehicle to navigate to an unprecedented level of accuracy without GNSS signals. This article justified conclusively, "No GPS, No Problem."

ACKNOWLEDGMENT

The authors would like to thank C. Lee at Edwards AFB for inviting the ASPIN Laboratory to conduct experiments during NAVFEST. The authors would also like to thank S. Shahcheraghi, M. Neinavaie, and J. Khalife for insightful discussions and J. Morales, K. Shamaei, M. Maaref, K. Semelka, M. Nguyen, and T. Mortlock for their help with data collection.

ZAHER (ZAK) M. KASSAS, Senior Member, IEEE
The Ohio State University, Columbus, OH USA

ALI ABDALLAH
University of California, Irvine, CA USA

REFERENCES


