

# GPS WORLD

GNSS  
POSITION  
NAVIGATION  
TIMING

**Innovation**

Real-Time GPS  
Orbits for LEOs

WWW.GPSWORLD.COM

GNSS + INS

Cellular + INS (No GNSS)

INS Only

## OPPORTUNITY SIGNALS

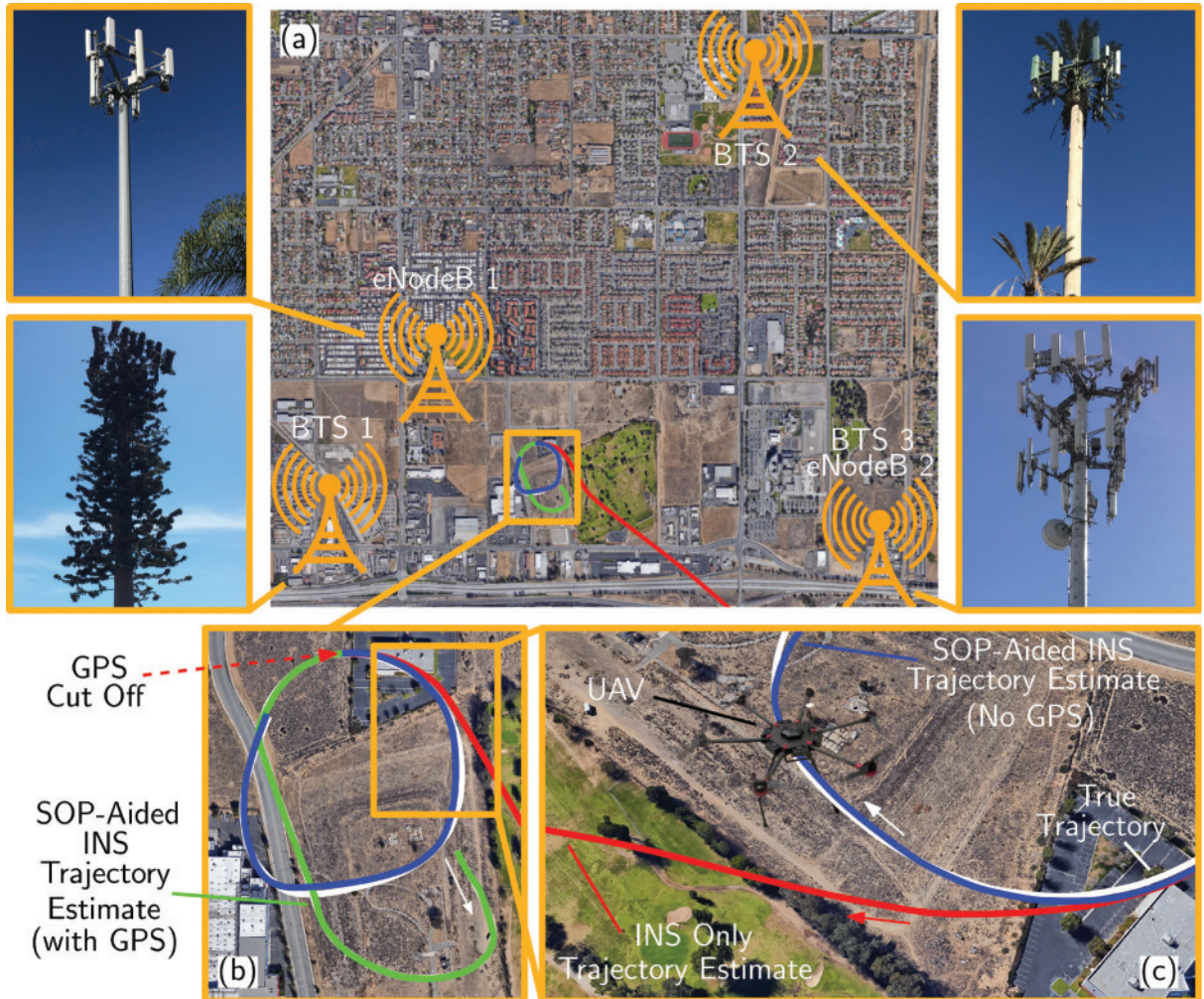
LTE  
NAVIGATES  
UAV

+  
UAV STATE  
OF THE  
INDUSTRY

MOBILE WORLD  
CONGRESS

EYES IN THE SKY  
REMOTE SENSING

GPS IIR-Ms POWER UP



# LTE STEERS UAV

No GPS? No Problem! Signals of Opportunity Work in Challenged Environments

**LONG-TERM EVOLUTION CELLULAR SIGNALS** can be exploited for accurate and resilient autonomous vehicle navigation in the absence of clear GNSS signals. Simulation and experimental results demonstrate that GPS-like performance can be achieved in the absence of GPS signals when cellular pseudoranges aid an inertial navigation system.

BY ZAHER M. KASSAS, JOSHUA J. MORALES, KIMIA SHAMAEI, AND JOE KHALIFE

**N**avigation systems onboard today's vehicles mainly rely on integrating global navigation satellite system (GNSS) receivers with an inertial navigation system (INS). As vehicles approach full autonomy, requirements on the accuracy and resiliency of the

vehicle's navigation system become ever more stringent. Besides the known limitations of GNSS indoors and in deep urban canyons, recent cyber attacks on GNSS signals (jamming and spoofing) are exposing an alarming vulnerability, necessitating alternative and complementary navigation systems when GNSS signals become unavailable or untrustworthy. When GNSS signals become unavailable,



the errors of the INS's navigation solution diverge, and the divergence rate is dependent on the quality of the inertial measurement unit (IMU). Such diverging errors compromise the required safe and efficient operation of autonomous vehicles (AVs).

Two conflicting considerations arise in the design of an AV's integrated navigation system: high accuracy and low size, weight, power and cost (SWaP-C). Current trends to supplement an autonomous vehicle's navigation system in the inevitable event when GNSS signals become unusable are traditionally sensor-based, such as cameras and lasers. However, such sensors could violate SWaP-C constraints and may not function properly all the time, in all weather conditions. Recently, research in navigation via signals of opportunity (SOPs) has revealed their potential as an attractive source for navigation in GNSS-challenged environments. SOPs are ambient radio signals, which are not intended as positioning, navigation and timing sources: cellular, Wi-Fi, AM/FM, digital television, Iridium satellites and so on. SOPs are practically free to use and could alleviate the need for expensive and bulky aiding sensors.

Among different SOPs, cellular signals are particularly attractive due to their inherent characteristics:

- **Abundance:** Cellular signals base transceiver stations (BTSs) are plentiful.
- **Geometric diversity:** The cellular system configuration by construction yields favorable BTS geometry, unlike certain terrestrial SOPs such as digital television, which tend to be co-located.
- **Large bandwidth:** Cellular signals have a bandwidth up to 20 MHz, yielding accurate time-of-arrival (TOA) estimation.
- **High received power:** The received carrier-to-noise ratio ( $C/N_0$ ) from nearby cellular BTSs is commonly tens of dBs higher when compared to GNSS signals.

	Positions	Clock Errors	Oscillators	Signal Structure	Typical $C/N_0$
GNSS SVs	Known	Known	Atomic	Known	37–45 dB-Hz
Cellular BTSs	Not always known	Unknown	OCXO	Known	35–70 dB-Hz

**TABLE 1** GNSS SVs vs. Cellular BTSs.

While cellular SOPs are lucrative to exploit for navigation purposes, a number of challenges must be first addressed, since such signals were never intended for navigation purposes. **TABLE 1** compares GNSS space vehicles (SVs) and cellular BTSs with respect to relevant navigation attributes. Unlike GNSS SVs whose positions and clock errors are transmitted to the receiver in the navigation message, cellular BTSs do not transmit such information. Therefore, the receiver must either estimate these quantities in a stand-alone fashion or have access to a database (cloud-hosted) that is crowdsourcing this information from multiple nearby receivers.

The first strategy is analogous to the simultaneous localization and mapping (SLAM) problem in robotics, while the second strategy could be achieved by deploying multiple receivers, whether vehicle-mounted or affixed on dedicated stations.

This article discusses relevant cellular code division multiple access (CDMA) and long-term evolution (LTE) signals that could be exploited for navigation. The article also presents a specialized software-defined receiver (SDR) called Multichannel Adaptive Transceiver Information eXtractor (MATRIX), developed at the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory at the University of California, Riverside. MATRIX is capable of producing pseudorange observables to cellular CDMA and LTE BTSs. We also present a radio SLAM approach for AV navigation via a tightly-coupled cellular-aided INS framework. Simulation and experimental results demonstrate ground vehicles and unmanned aerial

vehicles (UAVs) navigating with cellular signals in the absence of GNSS signals.

## CDMA SIGNALS

CDMA is at the heart of third-generation (3G) wireless communication systems, which use orthogonal and maximal-length pseudorandom noise (PN) sequences to enable multiplexing over the same channel. The sequences transmitted on the forward link channel, from BTS to receiver, are known. By correlating the received cellular CDMA signal with a locally generated PN sequence, the receiver can estimate the TOA and produce a pseudorange measurement. In a cellular CDMA communication system, 64 logical channels are multiplexed on the forward link channel: a pilot channel, a sync channel, seven paging channels, and 55 traffic channels. The receiver uses the pilot signal to detect the presence of a CDMA signal and synchronize its locally-generated short code. The sync and paging channels are used to provide time and frame synchronization to enable the receiver to register in the network. All forward-link signals are spread at 1.2288 MHz by a 32,768-chip PN sequence called the short code. To distinguish the received data from different BTSs, each station uses a shifted version of the short code. This shift, known as the pilot offset, is unique for each sector of each BTS and is an integer multiple of 64 chips; hence, a total of 512 pilot offsets can be realized.

The goal of a cellular CDMA navigation receiver is to acquire and track the signal parameters, namely the code phase and the carrier phase. To this end, such a receiver consists of three main stages: signal acquisition, signal tracking and message decoding.

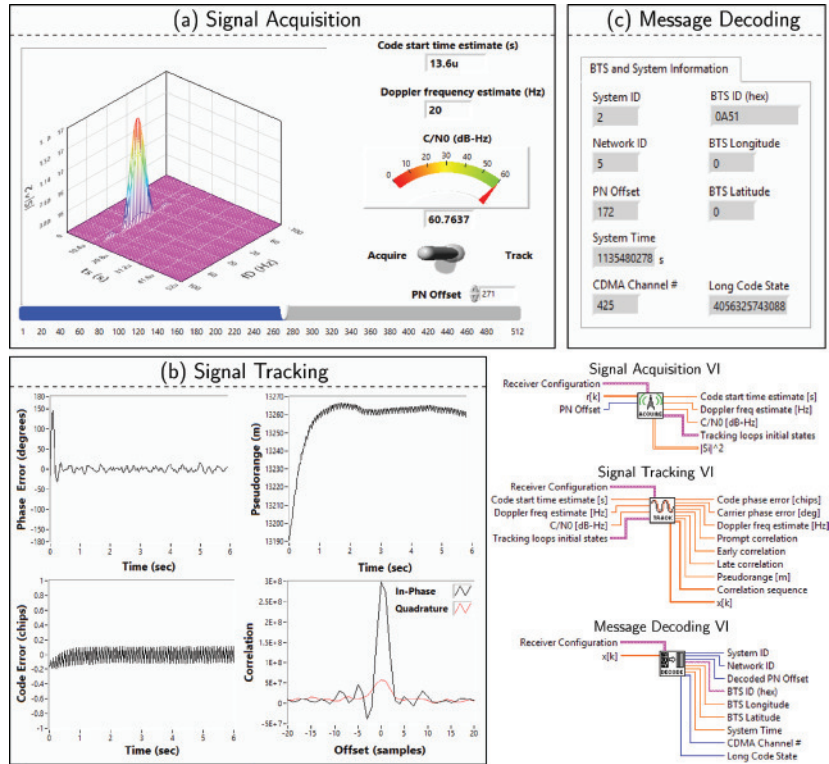


The pilot channel is used for signal acquisition and tracking. In fact, the pilot channel is dataless: only the short code is transmitted. This enables longer integration periods. A search in time and frequency in the acquisition stage obtains a coarse estimate of the TOA and the Doppler frequency. Next, these parameters are tracked and their estimates are refined via tracking loops. Similar to a GPS receiver, a phase-locked loop (PLL) and a carrier-aided delay-locked loop (DLL) are used to track the carrier and code phase, respectively. Finally, the sync and paging channels are decoded for timing and data association purposes. **FIGURE 1** illustrates the three stages of the cellular CDMA module of the MATRIX SDR, implemented as LabVIEW virtual instruments (VIs), and the front panel corresponding to each stage.

**LTE SIGNALS**

LTE has become the prominent standard for fourth-generation (4G) communication systems. Its multiple-input, multiple-output capabilities allow higher data rates compared to previous wireless standards. The high bandwidth and ubiquity of LTE networks make LTE signals attractive for navigation. In LTE Release 9, a broadcast positioning reference signal (PRS) was introduced to enable network-based positioning capabilities within the LTE protocol. However, PRS-based positioning suffers from a number of drawbacks:

- The user’s privacy is compromised since the user’s location is revealed to the network.
- Localization services are limited only to paying subscribers and from a particular cellular provider.
- Ambient LTE signals transmitted by other cellular providers are not exploited.
- Additional bandwidth is required to accommodate the PRS, which caused the majority of cellular



**FIGURE 1** Front panel of the cellular CDMA module of the MATRIX SDR and corresponding LabVIEW VIs. (a) Signal acquisition: the peak indicates the presence of a cellular CDMA signal at a C/N0 of 60.8 dB-Hz, tens of dBs higher than typical received GPS signals. (b) Signal tracking: after a short transient period, the receiver is tracking the code and carrier phase, as seen from the tracking errors. (c) Message decoding: the first three nibbles of the BTS ID are common to all sectors. U.S. providers do not transmit the BTS longitude and latitude.

Bandwidth (MHz)	Total number of subcarriers ( $N_c$ )	Number of subcarriers used ( $N_r$ )
1.4	128	72
3	256	180
5	512	300
10	1024	600
15	1536	900
20	2048	1200

**TABLE 2** Bandwidth and number of allocated subcarriers to LTE signals.

providers to choose not to transmit the PRS in favor of dedicating more bandwidth for traffic channels.

To circumvent these drawbacks, user equipment-(UE)-based positioning approaches, which exploit the existing reference signals in the transmitted LTE signals, have been explored.

**LTE Frame Structure.** LTE uses orthogonal frequency division multiplexing (OFDM) to transmit signals. In OFDM, the transmitted symbols are first parallelized into

groups of length  $N_r$ . Then, to provide a guard band, the resulting signal is zero-padded to a length  $N_c$ , which is set to be greater than  $N_r$ . Finally, an inverse fast Fourier transform (IFFT) is taken, and the last  $L_{cp}$  elements are repeated at the beginning. **TABLE 2** shows the possible values for  $N_r$  and  $N_c$  in an LTE system.

The OFDM signals are arranged into blocks called frames. A frame is composed of 10 ms data, which is divided into either 20 slots or 10 subframes with duration of 0.5 ms



or 1 ms, respectively. A slot can be decomposed into multiple resource grids and each resource grid has numerous resource blocks. Then, a resource block is broken down into the smallest elements of the frame, namely resource elements. The frequency and time indices of a resource element are called subcarrier and symbol, respectively.

**LTE Reference Signals.** There are three possible reference sequences in a received LTE signal that can be exploited for navigation.

**Primary synchronization signal (PSS).** The PSS is transmitted in symbol 7 of slots 0 and 10 of each frame. This signal, which is transmitted on the middle 62 subcarriers, provides symbol timing to the UE. The PSS is expressible in only three different orthogonal sequences, each of which represents a BTS's (also known as eNodeB) sector ID. This presents two main drawbacks: the received signal is highly affected by interference from neighboring eNodeBs with the same PSS sequences, and the UE can only simultaneously track a maximum of three eNodeBs, which is not desirable in an environment comprising more than three eNodeBs.

**Secondary synchronization signal (SSS).** The SSS is transmitted in symbol 6 of slot 0 or 10 of each frame. This signal, which is transmitted on the middle 62 subcarriers, provides frame timing to the user equipment. The SSS is expressible in only 168 different sequences, each of which represents the cell group identifier; therefore, it does not suffer from the aforementioned drawbacks of the PSS. The transmission bandwidth of the SSS is 930 KHz, which is slightly less than the GPS C/A code bandwidth (1.023 MHz). Therefore, navigation with SSS provides comparable results to GPS: low-cost and relatively precise pseudorange information using conventional PLLs and DLLs in an environment without multipath, but

low TOA accuracy in a multipath environment.

**Cell-specific reference signal (CRS).** The CRS is mainly transmitted to estimate the channel between the eNodeB and the UE. Therefore, it is scattered in both frequency and time and is transmitted from

all transmitting antennas. The CRS is known to provide better accuracy in estimating the TOA in a multipath environment due to its higher transmission bandwidth. Since the CRS is scattered across the LTE bandwidth, it is not possible to track the TOA from the CRS using



Photo compliments of Aeyon Labs Inc.

**When precision matters**, you need a precise, non-magnetic GNSS antenna. Tallysman offers a range of economical lightweight antennas like the TW1721, TW4421, TW3865 and others, providing:

- High multi-path signal rejection for improved accuracy and
- Tight Phase Centre Variation for precision systems

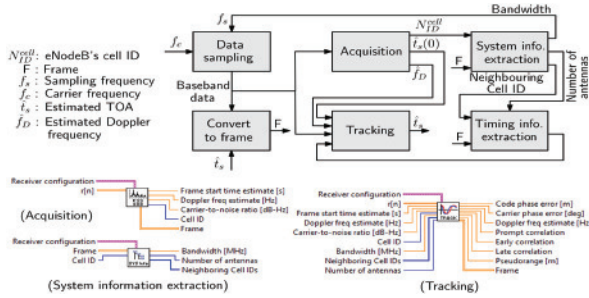
Please visit: [www.tallysman.com/index.php/gnss/applications](http://www.tallysman.com/index.php/gnss/applications)



CONTACT US TODAY:  
[info2@tallysman.com](mailto:info2@tallysman.com)  
[www.tallysman.com](http://www.tallysman.com)



When precision matters...™



**FIGURE 2** LTE module of the MATRIX SDR and corresponding LabVIEW VIs.

conventional low-complexity DLLs. Several methods can be used to estimate the channel parameters, including the TOA: multiple signal classification (MUSIC), estimation of signal parameters via rotational invariance techniques (ESPRIT) and space-alternating generalized expectation-maximization (SAGE) algorithms.

**LTE Receiver Structure.** The LTE navigation receiver exploits SSS, PSS and CRS, and consists of four stages.

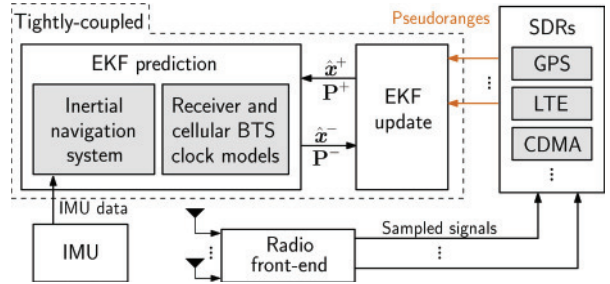
**Acquisition.** In this step, the received signal is correlated with the locally generated PSS and SSS signals to obtain the frame start time estimate, Doppler frequency estimate and the eNodeB's cell ID.

**System information extraction.** In LTE systems, the bandwidth can be assigned to different values. The actual value of the bandwidth is provided to the UE by the eNodeB in a block called master information block (MIB). When user equipment enters an LTE network, it starts receiving signals with the lowest possible bandwidth. After obtaining the frame start time, it is possible to convert the LTE signals into frame structure by executing the steps discussed in the LTE Frame Structure section in reverse order. Then, the UE decodes the MIB and obtains the actual bandwidth. The UE can then increase the sampling rate to as high as the signal bandwidth.

Due to the near-far effect on the PSS signal, it is not possible to acquire all the available eNodeBs in the environment. Each eNodeB provides the list of its neighboring cell IDs to the UE in the system information block (SIB). After obtaining the frame start time and the actual transmission bandwidth, the UE can decode the SIB to obtain the neighboring cell IDs.

**Tracking.** The receiver starts tracking the SSS using components of the tracking loop: a frequency-locked loop (FLL)-assisted PLL to track the carrier phase and a carrier-aided DLL to track the code phase.

**Timing information extraction.** To overcome the error due to multipath in tracking the SSS, the CRS is used. For this purpose, by knowing the CRS sequence and the received signal, the channel frequency response is first estimated. Then, the channel impulse response is obtained by taking an IFFT of the channel frequency response. Finally, the first



**FIGURE 3** Tightly coupled cellular-aided INS framework.

peak of the channel impulse response is detected, which represents the line-of-sight TOA.

**FIGURE 2** illustrates the block diagram of the LTE module of the MATRIX SDR and the corresponding LabVIEW VIs.

### CELLULAR-AIDED INERTIAL NAVIGATION

To correct INS errors using cellular pseudoranges, an extended Kalman filter (EKF) framework similar to a traditional tightly coupled GNSS-aided INS integration strategy is adopted, with the added complexity that the cellular BTSs' states (position and clock error states) are simultaneously estimated alongside the navigating vehicle's states (position, velocity, attitude, IMU measurement error states and receiver clock error states). This framework is composed of two modes.

**Mapping Mode.** The EKF produces estimates and associated estimation error covariances of both the navigating vehicle and the cellular BTSs' states (augmented in  $x$ ) using both GNSS SV and cellular BTS pseudoranges. Between aiding corrections, the EKF produces the state prediction  $\hat{x}^-$  and prediction error covariance  $P^-$  using INS model and receiver and cellular BTS clocks models. When an aiding source is available, either a GNSS SV or cellular BTS pseudorange, the EKF produces a state estimate update  $\hat{x}^+$  and associated estimation error covariance  $P^+$ .

**SLAM Mode.** The cellular-aided INS framework enters a SLAM mode when GNSS pseudoranges become unavailable. In this mode, INS errors are corrected using cellular BTS pseudoranges and the cellular BTSs' state estimates provided from the mapping mode. As the autonomous vehicle navigates, it simultaneously continues to refine the BTSs' state estimates. **FIGURE 3** illustrates a high-level diagram of the cellular-aided INS framework.

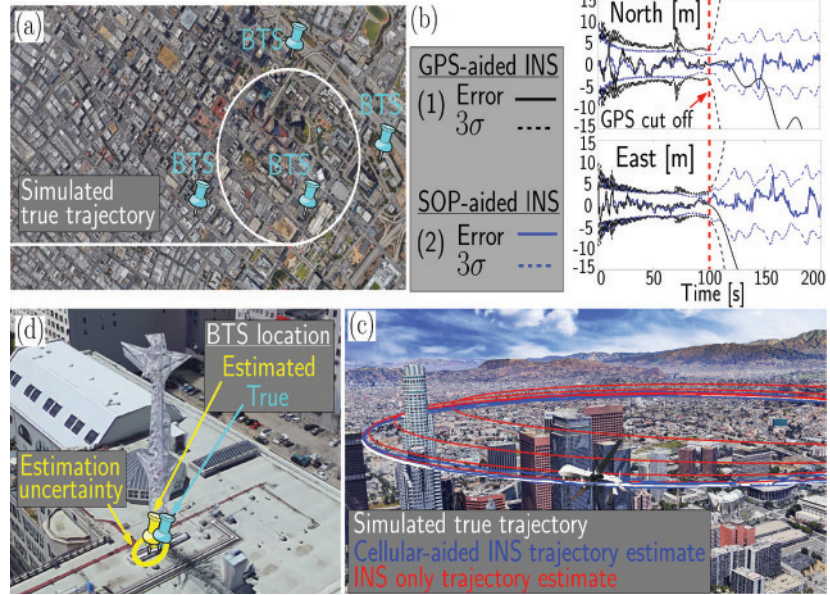
### SIMULATION RESULTS

To evaluate the performance of this cellular-aided INS framework presented, simulations were conducted of a UAV equipped with the MATRIX SDR, navigating in downtown Los Angeles, while exploiting ambient cellular signals. Two navigation systems were employed to estimate the trajectory of the UAV: a traditional tightly-coupled GPS-aided INS

with a tactical-grade IMU; and the cellular-aided INS discussed here with a consumer-grade IMU.

A simulator generated the true trajectory of the UAV and clock error states of the UAV-mounted receiver, the cellular BTSs' clock error states, noise-corrupted IMU measurements of specific force and angular rates and noise-corrupted pseudoranges to multiple cellular BTSs and GPS SVs.

The IMU signal generator models a triad gyroscope and a triad accelerometer, each with time-evolving biases that provided sampled data at 100 Hz. GPS L1 C/A pseudoranges were generated at 1 Hz using SV orbits produced from receiver independent exchange files downloaded Oct. 22, 2016, from a continuously operating reference station server. The GPS L1 C/A pseudoranges were set to be available for only the first 100 seconds of the 200-second simulation. Cellular



**FIGURE 4** Illustration of simulation results for a UAV flying over downtown Los Angeles, California. (a) Simulated true trajectory (white curve) and cellular BTS tower locations (blue pins). (b) EKF estimation errors and corresponding three standard deviation bounds ( $3\sigma$ ) of the North and East position states of the UAV. (c) Unaided INS navigation solution (red curve), and cellular-aided INS navigation solution (blue curve) during the GPS outage. (d) True and estimated BTS location and estimation uncertainty ellipse. Simulator developed with Paul Roysdon at UCR.

## MEMS Inertial Navigation Systems



Booth #731



The best accuracy/weight ratio

**NEW**

**ELLIPSE**



- 0.1° Roll & Pitch
- 2 m Position
- Single-frequency GNSS
- 47 g, 12 g (OEM)

**NEW**

**EKINOX**



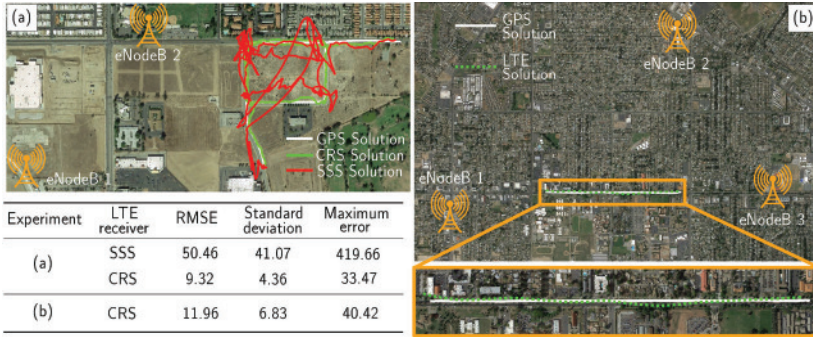
- 0.02° Roll & Pitch
- 2 cm Position
- Bi-frequency GNSS
- 600 g

**APOGEE**



- 0.008° Roll & Pitch
- < 1 cm Position
- Tri-frequency GNSS
- 900 g

Performance in real-time



**FIGURE 5** Experimental results for standalone LTE navigation. (a) Comparative experimental results in a semi-urban environment for an SSS-based and a CRS-based receiver. The results show the importance of using CRS to alleviate the multipath effects. (b) Experimental results for a CRS-based receiver in an urban environment with severe multipath.

pseudoranges were generated at 5 Hz to four BTS locations, which were surveyed from real tower positions in downtown Los Angeles.

The UAV’s true trajectory included a straight segment followed by two banked orbits in the vicinity of the four cellular BTSs, shown in **FIGURE 4(a)**. The resulting EKF estimation errors and corresponding three standard deviation bounds for the north and east position of the UAV are plotted in **FIGURE 4(b)**. The navigation solution from using the cellular-aided INS and navigation solution from using only an INS during the 100 seconds GPS pseudoranges were unavailable appear in **FIGURE 4(c)**. The final BTS estimated position and corresponding 95th percentile estimation uncertainty ellipse is shown in **FIGURE 4(d)**.

We can conclude that when GPS pseudoranges become unavailable at 100 seconds, the estimation errors associated with the traditional GPS-aided INS integration strategy begin to diverge, as expected, whereas the errors associated with the cellular-aided INS are bounded within this 100-second duration of GPS unavailability. Second, when GPS was still available during the first 100 seconds, the cellular-

aided INS with a consumer-grade IMU almost always produced lower estimation error uncertainties when compared to the traditional GPS-aided INS integration strategy with a tactical-grade IMU.

### EXPERIMENTAL RESULTS

To evaluate the standalone LTE navigation performance, two field tests were conducted with real LTE signals in semi-urban and urban environments. In both tests, a ground vehicle was equipped with LTE and GPS antennas and universal software radio peripherals (USRPs). LTE signals were simultaneously downmixed and synchronously sampled via a dual-channel USRP driven by a GPS-disciplined oscillator. The GPS navigation solution served as ground truth. **FIGURE 5(a)** shows experimental results for a CRS-based and an SSS-based receiver in a semi-urban environment with moderate multipath. The table, **FIGURE 5(b)**, demonstrates the importance of exploiting CRS to alleviate multipath effects. Figure 5(b) shows the experimental results for a CRS-based receiver in an urban environment with severe multipath.

To evaluate the performance of cellular-aided inertial navigation, a field test

	2D RMSE (m)	3D RMSE (m)	Final 3D error (m)
INS-only	>100	>100	>100
SOP-aided INS	4.68	7.76	4.92

**TABLE 3** UAV’s RMSEs and final errors after GPS cut off.

was conducted with real cellular signals and an IMU-equipped UAV. The UAV was equipped with three antennas to acquire and track:

- GPS signals
- LTE signals from nearby eNodeBs
- cellular CDMA signals from nearby BTSs.

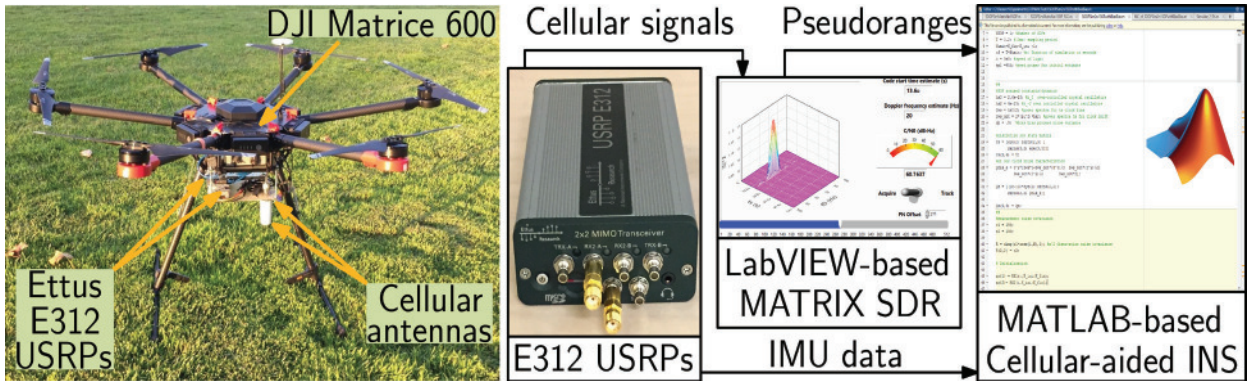
Samples of the received signals were stored for off-line post-processing. The LTE and CDMA signals were processed by the MATRIX SDR. **FIGURE 6** depicts the experimental hardware setup.

Experimental results are presented for two scenarios: the cellular-aided INS described in this article, and for comparative analysis, a traditional GPS-aided INS using the UAV’s IMU. The true trajectory traversed by the UAV is plotted in the **OPENING FIGURE (b)-(c)**, which consists of a GPS unavailability run of 50 seconds, starting at a location marked by the red arrow. The north-east root mean squared errors (RMSE) of the GPS-aided INS’s navigation solution after GPS became unavailable was more than 100 meters. The UAV also estimated its trajectory using the cellular-aided INS framework using signals from the two eNodeBs and three cellular BTSs illustrated in **OPENING FIGURE (a)** to aid its onboard INSs. The north-east RMSEs of the UAV’s trajectory after GPS became unavailable was 4.68 meters with a final error of 4.92 meters. **TABLE 3** summarizes the UAV’s RMSEs and final errors.

### CONCLUSION

Cellular signals can be exploited to navigate in the absence of GNSS signals. Experimental results demonstrated a UAV navigating with a cellular-aided INS using two LTE eNodeBs and three cellular CDMA BTSs achieving GPS-like performance in the absence of GNSS signals. This article is based on IEEE/ION PLANS, ION GNSS+ and ION ITM papers by the authors; see online version. This work is supported by grants from the Office Naval Research (ONR)





**FIGURE 6** Experimental hardware setup.

under Grant N00014-16-1-2305 and the National Science Foundation (NSF) under Grant 1566240.

### MANUFACTURERS

Cellular antennas used were consumer-grade 800/1900-MHz cellular omnidirectional antennas. The UAV and GPS antenna used were DJI with the A3 flight controller. The cellular signals were simultaneously down-mixed and synchronously sampled via two Ettus E-312 USRPs tuned to 1955 MHz (AT&T) and 882.75 MHz (Verizon) carrier frequencies. 🌐

**JOSHUA J. MORALES** is a Ph.D. student at the University of California, Riverside and a member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) laboratory.

**KIMIA SHAMAEI** is a Ph.D. candidate at the University of California, Riverside and a member of the ASPIN Laboratory.

**JOE KHALIFE** is a Ph.D. student at the University of California, Riverside and a member of the ASPIN Laboratory.

**ZAHER (ZAK) M. KASSAS** is an assistant professor at the University of California, Riverside and director of the ASPIN Laboratory. He received a Ph.D. in electrical and computer engineering from the University of Texas at Austin.

**One team with one goal:  
accurate and reliable GNSS positioning anywhere**