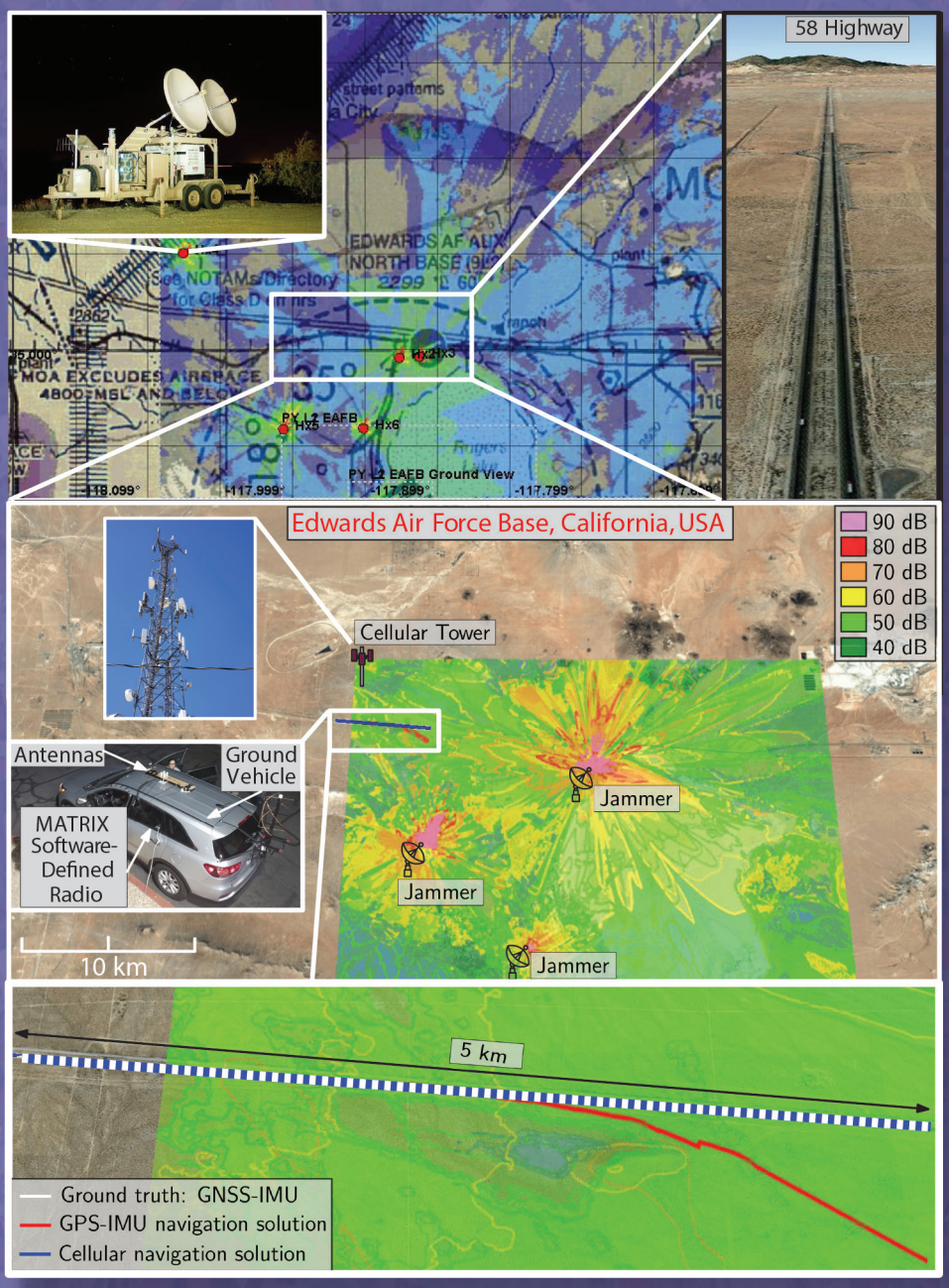
IEEE Aerospace and Electronic SYSTEMS magazine

July 2022
ISSN 0885-8985
Volume 37, Number 7



Feature Article:

DOI. No. 10.1109/MAES.2022.3154110

I Am Not Afraid of the GPS Jammer: Resilient Navigation Via Signals of Opportunity in GPS-Denied Environments

Zaher M. Kassas, Joe Khalife, and Ali A. Abdallah, University of California, Irvine, CA 92697, USA
Chiawei Lee, U.S. Air Force Test Pilot School, Edwards, CA 93524, USA

INTRODUCTION

Global navigation satellite systems (GNSS) are at the heart of numerous technologies that fuel our modern day life. It is estimated that there are currently about 8 billion GNSS devices worldwide, reaching 9 billion by 2025. The economic benefits of GPS to the U.S. private sector between 1984 and 2017 is estimated to be nearly $1.8 trillion, and 15 of the 18 U.S. critical infrastructures rely on GPS. While losing accurate positioning, navigation, and timing (PNT) can be a nuisance in nonsafety critical applications, the impact can be catastrophic in safety-critical applications, such as transportation, aviation, military operations, among others. Over the last few years, GNSS jamming and spoofing incidents have been happening with increasing frequency, exposing the inherent vulnerabilities of GNSS, and rendering them a single point of failure [1]–[4]. GNSS jamming and spoofing have affected hundreds of vessels in South Korea; disrupted navigation over the South China Sea islands; caused chaos on smartphones and rideshares in Moscow; put tens of vessels into disarray in the Black Sea; caused dozens of unmanned aerial vehicles (UAVs) to plummet during a Hong Kong air show, resulting in hundreds of thousands of dollars in damages; are suspected to have been utilized to hijack UAVs and oil tankers in the Persian Gulf; disrupted airport operations around the world; and are becoming commonplace in military conflict [5]. What is particularly alarming is that jamming and spoofing are no longer confined to sophisticated rogue organizations, with jammers being sold online and marketed as personal privacy devices, and hackers publishing spoofing software-defined radio (SDR) code online. Today's navigation systems, particularly those onboard ground, aerial, and surface vehicles, fuse information from a GNSS receiver and an inertial measurement unit (IMU) [6]. The integration of these two systems, typically referred to as a GNSS-aided inertial navigation system (INS), takes advantage of the complementary attributes of each system: the long-term stability of a GNSS navigation solution aids the short-term accuracy of an INS. Sensors (e.g., cameras, lasers, sonar, and odometers) have been commonly adopted to supplement a navigation system for the inevitable event that GNSS signals become unreliable or unavailable. These sensors could be used to extract relative motion information to reduce the INS's error divergence rate. However, they are still dead-reckoning-type sensors; therefore, during prolonged periods of GNSS outage, the error would eventually diverge. Moreover, these sensors only provide local position estimates, may not properly function in all environments (e.g., fog, snow, rain, dust, nighttime, etc.), and are still susceptible to malicious spoofing attacks [7].

Signals of opportunity (SOPs) have been considered to enable navigation whenever GNSS signals become unavailable or unreliable [8]. SOPs are ambient radio signals that are not intended for navigation or timing purposes, such as AM/FM radio [9], [10], WiFi [11], [12], cellular [13]–[16], digital television [17], [18], and low-Earth orbit (LEO) satellite siganls [19]–[21]. In contrast to the aforementioned dead-reckoning-type sensors, absolute position information could be extracted from SOPs to provide bounded INS errors. Moreover, many SOPs are practically unaffected by dense smoke, fog, rain, snow, and other poor weather conditions.

Authors' current addresses: Zaher M. Kassas, Joe Khalife, and Ali Abdallah are with the Department of Mechaincal and Aerospace Engineering, University of California, Irvine, Irvine, CA 92697 USA (e-mails: zkassas@ieee.org; jjkhalife@gmail.com; abdalla2@uci.edu); Chiawei Lee is with the U.S. Air Force Test Pilot School, Edwards, CA 93524 USA (e-mail: chiawei.lee@us.af.mil). *(Corresponding author: Zaher M. Kassas)*.
Manuscript received 8 June 2021, revised 23 October 2021; accepted 2 February 2022, and ready for publication 22 February 2022.
Review handled by Jason Gross.
0885-8985/22/$26.00 © 2022 IEEE

Image licensed by Ingram Publishing

SOPs enjoy several inherently desirable attributes for navigation purposes:

1) abundance in most locales of interest;
2) transmission at a wide range of frequencies and directions;
3) reception at a carrier-to-noise ratio (C/N_0) that is commonly tens of dBs higher than that of GNSS signals;
4) they are free to use, since their infrastructure is already operational.

While SOPs are jammable and spoofable [22]–[24], they are transmitted in multiple frequency bands and are typically received outdoors at high C/N_0. In the case of cellular SOPs, for example, they are received at more than 30 dBs higher C/N_0 than GNSS signals [25]. They also span the 700 MHz to nearly 6 GHz bands, excluding the 5G millimeter wave (mmWave) spectrum, which is envisioned to span several GHz of spectrum, with some bands reaching up to 400 MHz of bandwidth. This makes staging a successful, clandestine attack on cellular SOPs generally challenging, as the attacker would need to target the entire cellular spectrum with very high power. A typical challenge that arises in SOP-based navigation is that unlike GNSS, whose satellite states are transmitted in their navigation message, the states of SOPs, namely their position and clock states, are typically unknown *a priori* and must be estimated. To overcome this challenge, a radio simultaneous localization and mapping (radio SLAM) framework was proposed in which the states of the navigating vehicle are simultaneously estimated with the states of the SOPs [26], while aiding the INS in a tightly coupled fashion [27]. Recent works have demonstrated meter-level-accurate navigation with SOPs on ground vehicles and pedestrians indoors [28], [29] and submeter-level accurate navigation on aerial vehicles [30]. While published results in the literature have demonstrated experimentally the efficacy of SOPs as PNT sources in a standalone fashion (i.e., without fusing SOPs with other signals or sensors) and in an integrated fashion (i.e., fusing SOPs with INS and lidar), experiments were never conducted in actual GNSS-denied environments. These results were achieved by "fictitiously" cutting GNSS signals from the navigation filter. In September 2019, the authors' Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory was invited to participate in live GPS jamming experiments, called Developmental Test Navigation Festival (DT NAVFEST), at Edwards Air Force Base (AFB), California, USA. Experiments with stationary antennas and ground vehicles were conducted to study SOPs for PNT. This article reports findings from these experiments, which represent the first published results evaluating the efficacy of SOPs for PNT in a real GPS-denied environment. In particular, this article analyzes the clock errors of terrestrial cellular long-term evolution (LTE) SOPs located inside the jammed region, showing timing stability over 95 min of GPS jamming. Moreover, this article showcases the efficacy of the radio SLAM approach on a ground vehicle navigating in the jammed environment, while exploiting a terrestrial cellular LTE SOP. The results show the vehicle navigating during GPS jamming for 5 km in 180 s, during which the position root mean-squared error (RMSE) of a traditional GPS-aided INS grew to nearly 238 m. In contrast, the radio SLAM approach with a *single* cellular LTE SOP whose position was poorly known (an initial uncertainty on the order of several kilometers) achieved a position RMSE of 32 m. To the best of authors' knowledge, these are the first published results of navigation with SOPs in real GPS-denied environments, under jamming conditions. Preliminary results of this study were presented in Kassas *et al.*'s work [5]. However, considering the nonpeer reviewed nature of Kassas *et al.*'s work [5], the results therein only focused on showing the navigation solution. In contrast, this article

1) formulates the mathematical details of radio SLAM by describing the navigator's dynamics model via an INS kinematics formulation versus a dynamics

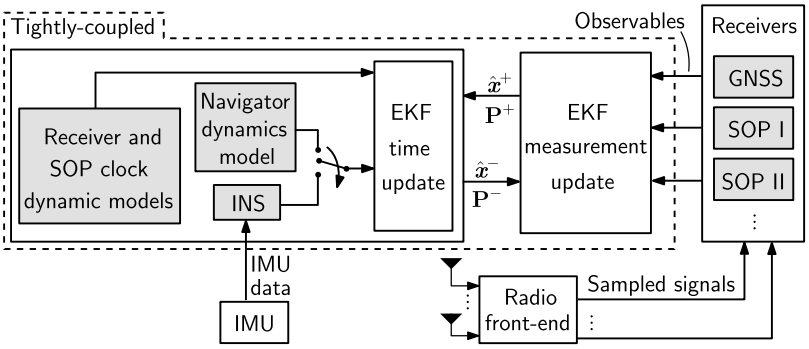


Figure 1.
Overview of a tightly coupled radio SLAM framework. The radio front-end collects signals, which are processed in the navigation receivers. The EKF time update is performed based on the toggling switch: (i) using a dynamical model that describes the navigator's dynamics or (ii) using an INS, when available. The EKF measurement update is performed using navigation observables from received SOP signals and GNSS signals, when available.

model formulation; clock error dynamics model; and SOP measurement model;

2) gives explicit description of the experiments including filter initialization and software and hardware setup;

3) provides further analyses and experimental results of the C/N_0 experienced during jamming as well as the filter's estimation error.

The rest of this article is organized as follows. The section "Radio Slam" provides and overview of the radio SLAM framework. The section "GPS-Jammed Environment and Experimental Setup" describes the GPS-jammed environment and hardware and software setup. "PNT Experimental Results in the GPS-Jammed Environment" presents PNT experimental results. Finally, the "Conclusion" is presented.

RADIO SLAM

This section overviews radio SLAM framework as well as the navigator's dynamics model, clock error dynamics, and SOP measurement models.

FRAMEWORK OVERVIEW

Radio SLAM estimates the states of the navigator-mounted receiver simultaneously with the SOPs' states. Radio SLAM produces an SOP-derived navigation solution in a standalone fashion [26], [31] or an integrated fashion by fusing SOPs with sensors (e.g., IMU, lidar, etc.) and digital maps [32].

Observability of radio SLAM was analyzed in the authors' work [26], [33], leading to establishing the minimal *a priori* knowledge needed about the navigator-mounted receiver's and/or SOP transmitters' states. The most significant conclusion from these observability analyzes is that if a mobile navigator with knowledge of its initial states (position, velocity, clock bias, and clock drift), denoted $\boldsymbol{x}_r$, makes pseudorange measurements to $M \geq 1$ terrestrial SOPs whose states (position, clock bias, and clock drift), denoted $\{\boldsymbol{x}_{s,i}\}_{i=1}^{M}$ are unknown, then the environment is fully observable, i.e., the navigator can estimate its states simultaneously with the states of the SOPs. The conclusions from these observability analyzes will be used in estimating the mobile ground vehicle's and SOP's states in the section "Experiment 2: Mobile Receiver."

A simple, yet effective estimator that could be employed in radio SLAM is the extended Kalman filter (EKF). Here, one could employ a similar architecture to a tightly coupled GNSS-INS. This architecture i) performs the EKF measurement update (yielding the corrected estimate $\hat{\boldsymbol{x}}^{+}$ and corrected error covariance $\mathbf{P}^{+}$) whenever GNSS observables (e.g., pseudorange and carrier phase) are available and ii) performs the EKF time update (yielding the predicted estimate $\hat{\boldsymbol{x}}^{-}$ and prediction error covariance $\mathbf{P}^{-}$) with raw IMU data between GNSS measurement epochs. The added complexity with SOPs is that the EKF state vector is composed of both the navigator's states and the SOPs' states, i.e., $\boldsymbol{x} \triangleq \left[\boldsymbol{x}_r^{\mathsf{T}}, \boldsymbol{x}_{s,1}^{\mathsf{T}}, \ldots, \boldsymbol{x}_{s,M}^{\mathsf{T}}\right]^{\mathsf{T}}$. If no INS is used, then a proper dynamical model for the navigator dynamics can be used for the EKF time update. Of course, this would introduce a mismatch between the true navigator's dynamics and the model used in the EKF; nevertheless, advanced methods such as adaptive filters (e.g., interacting multiple models [34] and noise covariance estimation [35] could alleviate this mismatch.

Figure 1 depicts a high-level block diagram of tightly coupled radio SLAM, which operates in the following two modes.

- **Mapping mode:** GNSS observables are available. Here, GNSS and SOP observables are fused in the EKF to aid the INS (if available), producing a more accurate estimate of $\boldsymbol{x}_r$ while mapping the SOP

radio environment (i.e., estimating the unknown states of the SOPs $\{\boldsymbol{x}_{s,i}\}_{i=1}^{M}$.

- **Radio SLAM mode:** GNSS observables are unavailable. Here, SOP observables aid the INS (if available) to simultaneously estimate the navigator-mounted states $\boldsymbol{x}_r$ while continuing to refine estimates of the SOPs' states.

NAVIGATOR DYNAMICS MODEL

In a tightly coupled radio SLAM framework, either an INS kinematics model or a dynamics model for the navigator is utilized to perform the EKF time update. In what follows, a description of each is discussed.

INS KINEMATICS FORMULATION

Let $\{b\}$ denote a body frame fixed at the navigator, and let $\{g\}$ denote a global frame, e.g., the Earth-centered inertial frame [36]. Moreover, let $\boldsymbol{\theta}_b \in \mathbb{R}^3$ represent the three-dimensional (3-D) orientation vector of the body frame with respect to the global frame and ${}^g\boldsymbol{r}_b \in \mathbb{R}^3$ the 3-D position vector of the navigator expressed in $\{g\}$. Given the INS's true 3-D rotational rate vector ${}^b\boldsymbol{\omega} \in \mathbb{R}^3$ in the body frame and its 3-D acceleration ${}^g\boldsymbol{a}_b \in \mathbb{R}^3$ in the global frame, the standard strapdown kinematics equations can be expressed in continuous time as

$$\dot{\boldsymbol{\theta}}_b(t) = {}^b\boldsymbol{\omega}(t) \tag{1}$$

$${}^g\ddot{\boldsymbol{r}}_b(t) = {}^g\boldsymbol{a}_b(t). \tag{2}$$

The 3-D orientation vector of the body frame with respect to the global frame can be represented by the 4-D quaternion vector ${}^b_g\bar{\boldsymbol{q}} \in \mathbb{R}^4$.

The navigator's IMU is assumed to contain a triad-gyroscope and a triad-accelerometer, which produce measurements $\boldsymbol{z}_{\text{imu}} \triangleq \left[\boldsymbol{\omega}_{\text{imu}}^{\mathsf{T}}, \boldsymbol{a}_{\text{imu}}^{\mathsf{T}}\right]^{\mathsf{T}}$ of the angular rate and specific force, which are modeled as

$$\boldsymbol{\omega}_{\text{imu}}(k) = {}^b\boldsymbol{\omega}(k) + \boldsymbol{b}_{\text{gyr}}(k) + \boldsymbol{n}_{\text{gyr}}(k) \tag{3}$$

$$\boldsymbol{a}_{\text{imu}}(k) = \mathbf{R}\left[{}^b_g\bar{\boldsymbol{q}}(k)\right]({}^g\boldsymbol{a}_b(k) - {}^g\boldsymbol{g}(k)) + \boldsymbol{b}_{\text{acc}}(k) + \boldsymbol{n}_{\text{acc}}(k) \tag{4}$$

where $\mathbf{R}\left[{}^b_g\bar{\boldsymbol{q}}\right]$ is the equivalent rotation matrix of ${}^b_g\bar{\boldsymbol{q}}$; ${}^g\boldsymbol{g}$ is the acceleration due to gravity acting on the navigator in the global frame; $\boldsymbol{b}_{\text{gyr}} \in \mathbb{R}^3$ and $\boldsymbol{b}_{\text{acc}} \in \mathbb{R}^3$ are the gyroscope and accelerometer biases, respectively; and $\boldsymbol{n}_{\text{gyr}}$ and $\boldsymbol{n}_{\text{acc}}$ are measurement noise vectors, which are modeled as zero-mean white noise sequences with covariances $\mathbf{Q}_{\boldsymbol{n}_{\text{gyr}}}$ and $\mathbf{Q}_{\boldsymbol{n}_{\text{acc}}}$, respectively. Integrating IMU specific force data to perform a time update of the position and velocity in a rotating coordinate frame introduces a centrifugal and Coriolis term due to the rotation rate of the Earth [37]. However, a short integration interval is considered in this article, where the variation of the Coriolis force was considered negligible for simplicity. Further details about neglecting the Coriolis force over short integration intervals can be found in Morales and Kassas [27].

The gyroscope and accelerometer biases in (3) and (4) are dynamic and stochastic; hence, they must be estimated in the EKF as well. As such, the INS 16-state vector is given by

$$\boldsymbol{x}_{\text{ins}} = \left[\begin{array}{cccc} {}^b_g\bar{\boldsymbol{q}}^{\mathsf{T}}, & {}^g\boldsymbol{r}_b^{\mathsf{T}}, & {}^g\dot{\boldsymbol{r}}_b^{\mathsf{T}}, & \boldsymbol{b}_{\text{gyr}}^{\mathsf{T}}, \quad \boldsymbol{b}_{\text{acc}}^{\mathsf{T}} \end{array}\right]^{\mathsf{T}}$$

where $\dot{\boldsymbol{r}}_b \in \mathbb{R}^3$ is the 3-D velocity of the navigator.

The INS states evolve in time according to

$$\boldsymbol{x}_{\text{ins}}(k+1) = \boldsymbol{f}_{\text{ins}}\left[\boldsymbol{x}_{\text{ins}}(k), {}^b\boldsymbol{\omega}(k), {}^g\boldsymbol{a}_b(k)\right]$$

where $\boldsymbol{f}_{\text{ins}}$ is a vector-valued function of standard strapdown kinematic equation [38], which discretizes (1) and (2) by integrating ${}^b\boldsymbol{\omega}$ and ${}^g\boldsymbol{a}_b$ to produce ${}^b_g\bar{\boldsymbol{q}}(k+1)$, $\boldsymbol{r}_b(k+1)$, and $\dot{\boldsymbol{r}}_b(k+1)$, and uses a velocity random walk model for the biases, which is given by

$$\begin{aligned} \boldsymbol{b}_{\text{gyr}}(k+1) &= \boldsymbol{b}_{\text{gyr}}(k) + \boldsymbol{w}_{\text{gyr}}(k) \\ \boldsymbol{b}_{\text{acc}}(k+1) &= \boldsymbol{b}_{\text{acc}}(k) + \boldsymbol{w}_{\text{acc}}(k) \end{aligned}$$

where $\boldsymbol{w}_{\text{gyr}}$ and $\boldsymbol{w}_{\text{acc}}$ are process noise vectors that drive the in-run bias variation (or bias instability) and are modeled as white noise sequences with covariance $\mathbf{Q}_{\boldsymbol{w}_{\text{gyr}}}$ and $\mathbf{Q}_{\boldsymbol{w}_{\text{acc}}}$, respectively.

DYNAMICS MODEL FORMULATION

Generally, the navigator's dynamics can be described as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{f}[\boldsymbol{x}(t), \boldsymbol{u}(t), t] + \boldsymbol{w}(t)$$

where $\boldsymbol{x}$ is the navigator's state vector, $\boldsymbol{u}$ represents known exogenous inputs, and $\boldsymbol{w}$ is the process noise. Depending on the navigator's platform (pedestrian or ground, aerial, or maritime) and motion, different dynamic models can be used to describe the navigator's dynamics, such as polynomial (e.g., white noise acceleration and Wiener process acceleration), singer acceleration, mean-adaptive acceleration, semi-Markov jump process, circular motion, curvilinear motion, coordinated turn, among others [39].

A simple, yet effective dynamical model that has been successfully employed for navigators with "low dynamics," which sufficiently captures the dynamics between EKF measurement updates is the white noise acceleration, given by

$$\dot{\boldsymbol{x}}_{\text{pv}}(t) = \mathbf{A}_{\text{pv}}\,\boldsymbol{x}_{\text{pv}}(t) + \mathbf{D}_{\text{pv}}\tilde{\boldsymbol{w}}_{\text{pv}}(t) \tag{5}$$

$$\mathbf{A}_{\text{pv}} = \begin{bmatrix} \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \end{bmatrix}, \quad \mathbf{D}_{\text{pv}} = \begin{bmatrix} \mathbf{0}_{3\times3} \\ \mathbf{I}_{3\times3} \end{bmatrix}$$

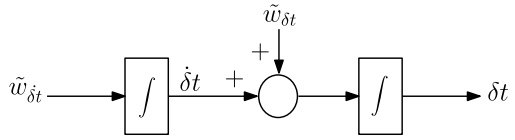


Figure 2.
Clock error states dynamics model.

where $\boldsymbol{x}_{\text{pv}} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}\right]^{\mathsf{T}}$, $\boldsymbol{r}_r \triangleq [x_r, y_r, z_r]^{\mathsf{T}}$ is the 3-D position of the navigator-mounted receiver, and $\tilde{\boldsymbol{w}}_{\text{pv}} = \left[\tilde{w}_x, \tilde{w}_y, \tilde{w}_z\right]^{\mathsf{T}}$ is the process noise vector, whose elements of are modeled as zero-mean, mutually independent white noise processes with power spectral densities $\tilde{q}_x$ $\tilde{q}_y$, and $\tilde{q}_z$, respectively. Note that here, the superscript g is dropped and the subscript r is used to denote the navigator-mounted receiver's position instead of b, since the navigator in this case is not relying on an INS and the orientation of its body is not estimated.

Discretizing the navigator's dynamics (5) at a constant sampling period T yields the discrete-time model

$$\boldsymbol{x}_{\text{pv}}(k+1) = \mathbf{F}_{\text{pv}}\, \boldsymbol{x}_r(k) + \boldsymbol{w}_{\text{pv}}(k), \quad k = 0, 1, 2, \ldots$$
$$\mathbf{F}_{\text{pv}} = \begin{bmatrix} \mathbf{I}_{3\times 3} & T\mathbf{I}_{3\times 3} \\ \mathbf{0}_{3\times 3} & \mathbf{I}_{3\times 3} \end{bmatrix}$$

where $\boldsymbol{w}_{\text{pv}}$ is a discrete-time zero-mean white noise sequence with covariance $\mathbf{Q}_{\text{pv}}$ given by

$$\mathbf{Q}_{\text{pv}} = \begin{bmatrix} x\frac{T^3}{3} & 0 & 0 & \tilde{q}_x\frac{T^2}{2} & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^3}{3} & 0 & 0 & \tilde{q}_y\frac{T^2}{2} & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^3}{3} & 0 & 0 & \tilde{q}_z\frac{T^2}{2} \\ \tilde{q}_x\frac{T^2}{2} & 0 & 0 & \tilde{q}_x T & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^2}{2} & 0 & 0 & \tilde{q}_y T & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^2}{2} & 0 & 0 & \tilde{q}_z T \end{bmatrix}.$$

CLOCK ERROR DYNAMICS MODEL

GNSS satellites are equipped with atomic clocks, are synchronized, and their clock errors are transmitted in the navigation message along with the satellites' positions. Therefore, in GNSS-based navigation, only the receiver's clock error is estimated. In contrast, SOPs are equipped with less stable oscillators than GNSS satellites, are typically roughly synchronized to GNSS, and their clock error states (bias and drift) are mostly unknown. As such, the SOP clock errors must be simultaneously estimated with the receiver's clock error. To facilitate this estimation in the radio SLAM framework, the clock error state dynamics must be specified. To this end, a typical model for the dynamics of the clock error states is the so-called two-state model, composed of the clock bias δt and clock drift $\dot{\delta t}$, as depicted in Figure 2.

Table 1.

Typical h_0 and h_{-2} Values for Different TCXO and OCXO Oscillators [41]

Oscillator	h_0	h_{-2}
TCXO	2.0×10^{-19}	2.0×10^{-20}
TCXO	1.0×10^{-21}	2.0×10^{-20}
TCXO	9.4×10^{-20}	3.8×10^{-21}
TCXO	3.9×10^{-22}	2.4×10^{-22}
TCXO	3.5×10^{-20}	8.5×10^{-22}
TCXO	1.9×10^{-21}	2.5×10^{-23}
OCXO	2.6×10^{-22}	4.0×10^{-26}
OCXO	8.0×10^{-20}	4.0×10^{-23}
OCXO	3.4×10^{-22}	1.3×10^{-24}

The clock error states evolve according to

$$\dot{\boldsymbol{x}}_{\text{clk}}(t) = \mathbf{A}_{\text{clk}}\, \boldsymbol{x}_{\text{clk}}(t) + \tilde{\boldsymbol{w}}_{\text{clk}}(t)$$

$$\boldsymbol{x}_{\text{clk}} = \begin{bmatrix} \delta t \\ \dot{\delta t} \end{bmatrix}, \quad \tilde{\boldsymbol{w}}_{\text{clk}} = \begin{bmatrix} \tilde{w}_{\delta t} \\ \tilde{w}_{\dot{\delta t}} \end{bmatrix}, \quad \mathbf{A}_{\text{clk}} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{6}$$

where the elements of $\tilde{\boldsymbol{w}}_{\text{clk}}$ are modeled as zero-mean, mutually independent white noise processes, and the power spectral density of $\tilde{\boldsymbol{w}}_{\text{clk}}$ is given by $\tilde{\mathbf{Q}}_{\text{clk}} = \text{diag}\left[S_{\tilde{w}_{\delta t}}, S_{\tilde{w}_{\dot{\delta t}}}\right]$. The power spectra $S_{\tilde{w}_{\delta t}}$ and $S_{\tilde{w}_{\dot{\delta t}}}$ can be related to the power-law coefficients $\{h_\alpha\}_{\alpha=-2}^{2}$, which have been shown through laboratory experiments to be adequate to characterize the power spectral density of the fractional frequency deviation $y(t)$ of an oscillator from nominal frequency, which takes the form $S_y(f) = \sum_{\alpha=-2}^{2} h_\alpha f^\alpha$[40]. It is common to approximate the clock error dynamics by considering only the frequency random walk coefficient h_{-2} and the white frequency coefficient h_0, which lead to $S_{\tilde{w}_{\delta t}} \approx \frac{h_0}{2}$ and $S_{\tilde{w}_{\dot{\delta t}}} \approx 2\pi^2 h_{-2}$[34].

Many SOPs of interest, particularly cellular transmitters, are equipped with oven-controlled crystal oscillators (OCXOs). On the other hand, many receivers are equipped with less stable oscillators, e.g., temperature-compensated crystal oscillator (TCXO). Typical TCXO and OCXO values for h_0 and h_{-2} are given in Table 1.

Discretizing dynamics (6) at a sampling interval T yields the discrete-time-equivalent model

$$\boldsymbol{x}_{\text{clk}}(k+1) = \mathbf{F}_{\text{clk}}\, \boldsymbol{x}_{\text{clk}}(k) + \boldsymbol{w}_{\text{clk}}(k)$$

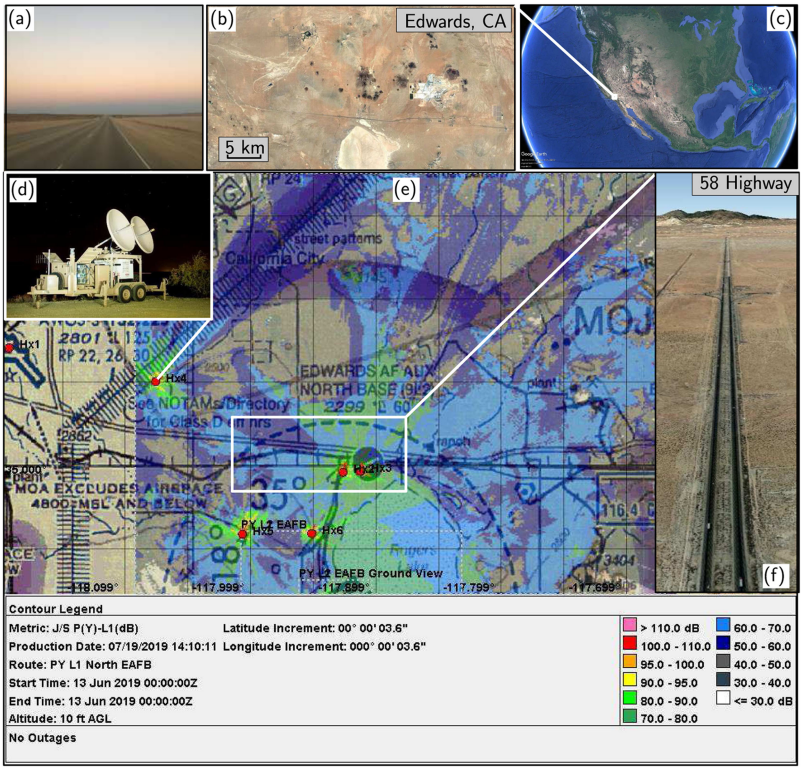


Figure 3.
DT NAVFEST GPS jamming laydown: (a) highway taken toward Edwards AFB, (b) photo of Edwards AFB, CA, (c) location of the experiment, (d) photo of one of the jammers used in the experiment, (e) heat map showing the jamming power and jammers' location, (f) photo of the 58 Highway, where the ground vehicle experiment was performed. Map data: Google Earth.

where $\boldsymbol{w}_{\text{clk}}$ is a discrete-time zero-mean white noise sequence with covariance $\mathbf{Q}_{\text{clk}}$, and

$$\mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Q}_{\text{clk}} = \begin{bmatrix} S_{\tilde{w}_{\delta t}} T + S_{\tilde{w}_{\delta t}} \frac{T^3}{3} & S_{\tilde{w}_{\delta t}} \frac{T^2}{2} \\ S_{\tilde{w}_{\delta t}} \frac{T^2}{2} & S_{\tilde{w}_{\delta t}} T \end{bmatrix}. \tag{7}$$

SOP MEASUREMENT MODEL

A specialized receiver could produce a pseudorange measurement to an SOP, which after discretization and mild approximations discussed in the work of Kassas and Humphrey [26], can be modeled as

$$\rho(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_s\|_2 + c \cdot [\delta t_r(k) - \delta t_s(k)] + v_\rho(k) \tag{8}$$

where c is the speed of light and v_ρ is a DT zero-mean white Gaussian sequence with variance $\sigma_\rho^2(k)$.

Another, more precise navigation observable that can be produced is the carrier phase, which can be modeled as

$$\lambda\phi(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_s\|_2 + c[\delta t_r(k) - \delta t_s(k)] + \lambda N + v_\phi(k) \tag{9}$$

where λ is the wavelength of the carrier signal, N represents the carrier phase ambiguity (namely, the initial phase difference between the receiver and the SOP), and $v_\phi(k)$ is the measurement noise, which is modeled as a discrete-time zero-mean white Gaussian sequence with variance $\sigma_\phi^2(k)$.

Note that the term N in (9) is not necessarily an integer [42]. Single- or double-difference carrier phase measurements will have integer ambiguities. If the SOP carrier phase measurements are used in a differential framework, the Least-squares AMBiguity Decorrelation Adjustment (LAMBDA) method [43], or its variants, e.g., the modified LAMBDA method [44], could be used to resolve the integer ambiguities. If SOP carrier phase measurements are used in a nondifferential framework, the carrier phase ambiguity is treated as a real-valued constant offset that can be assimilated into the SOP's initial clock bias [45]. In both differential and nondifferential frameworks, cycle slips in carrier phase tracking may occur, which could introduce integer "jumps" in N. In such cases, cycle slip detection and mitigation methods may be used to reduce their effects on carrier phase measurements [46]. The rest of this article focuses on a pseudorange-based navigation solution.

RADIO SLAM EKF FORMULATION

The observables to all SOPs in the environment, whether pseudoranges and/or carrier phases are augmented into

Table 2.

Jammer Laydown

Site	Latitude (N)	Longitude (W)	Terrain height (ft MSL)	Antenna height (ft AGL)	Antenna azimuth true (deg)	Antenna elevation (deg)	Antenna gain (dBi)		EIRP (dBm)		Waveform
							L1	L2	L1	L2	
Hx1	35° 04′ 12.4″	118° 08′ 41.82″	2769	10	57	15	24.2	24.5	83.8	84.1	CW, BBN
Hx2	34° 59′ 43.52″	117° 52′ 42.35″	2313	10	15	15	24.2	24.5	83.8	84.1	CW, BBN
Hx3	34° 59′ 45.57″	117° 51′ 52.65″	2289	10	13	15	24.2	24.5	83.8	84.1	CW, BBN
Hx4	35° 02′ 59.59″	118° 01′ 40.87″	2528	10	43	15	24.2	24.5	83.8	84.1	CW, BBN
Hx5	34° 57′ 29.35″	117° 57′ 31.78″	2429	10	24	15	24.2	24.5	83.8	84.1	CW, BBN
Hx6	34° 57′ 30.83″	117° 54′ 12.65″	2441	10	17	15	24.2	24.5	83.8	84.1	CW, BBN
Nx1	34° 54′ 42.45″	117° 54′ 5.5″	2309	29	49	-30	14.1	12.9	-12.4	-13.6	CW, BBN

MSL: Mean sea level; AGL: Above ground level; dBi: Decibel isotropic; dBm: Decibel referenced to 1 mW; EIRP: Equivalent, isotropically radiated power (EIRP) values accounted for estimated 1.5 dB line loss between amplifier and antenna; CW: Continuous wave; BBN: Broad-band noise

the measurement vector z, which is used to estimate $\boldsymbol{x} \triangleq \left[\boldsymbol{x}_r^{\mathsf{T}}, \boldsymbol{x}_{s,1}^{\mathsf{T}}, \ldots, \boldsymbol{x}_{s,M}^{\mathsf{T}}\right]^{\mathsf{T}}$, where $\boldsymbol{x}_{s,i} \triangleq \left[\boldsymbol{r}_{s_i}^{\mathsf{T}}, \boldsymbol{x}_{\mathrm{clk},s_i}^{\mathsf{T}}\right]^{\mathsf{T}} \in \mathbb{R}^5$ is the state of the ith SOP. If an INS is used as discussed in the section "INS Kinematics Formulation," $\boldsymbol{x}_r \triangleq \left[\boldsymbol{x}_{\mathrm{ins}}^{\mathsf{T}}, \boldsymbol{x}_{\mathrm{clk},r}^{\mathsf{T}}\right]^{\mathsf{T}} \in \mathbb{R}^{18}$. If the white noise acceleration model is used as discussed in the section "Dynamics Model Formulation," $\boldsymbol{x}_r \triangleq \left[\boldsymbol{x}_{\mathrm{pv}}^{\mathsf{T}}, \boldsymbol{x}_{\mathrm{clk},r}^{\mathsf{T}}\right]^{\mathsf{T}} \in \mathbb{R}^8$.

GPS-JAMMED ENVIRONMENT AND EXPERIMENTAL SETUP

This section overviews the GPS-jammed environment during DT NAVFEST live GPS jamming at Edwards AFB, as well as the hardware and software setup.

JAMMING LAYDOWN

From the information made available to the participants, six high-powered jammers (HPJ) and one portable box jammer (PBJ) were spread over an area of approximately 50 miles north of Edwards AFB, as shown in Figure 3. The term "Hx" denotes an HPJ, one of them seen in Figure 3, and "Nx" denotes a PBJ. The initial locations and characteristics of the jammers are summarized in Table 2. The experiments conducted by the ASPIN team took place just outside the perimeters of Edwards AFB, mainly on the 58 Highway pictured in Figure 3 and near the Mojave Airport.

SOP LTE ENODEB LAYOUT

An SOP radio mapping campaign with the cognitive SDR Multichannel Adaptive TRansceiver Information eXtractor (MATRIX), discussed in the section "MATRIX Cognitive SDR," was conducted a month before DT NAVFEST to survey available LTE eNodeBs in the area. Since Edwards AFB is largely unpopulated, only two LTE eNodeBs (SOP 1 and SOP 2) were hearable in the scheduled jamming area and were located at the same site, as shown in Figure 4. The eNodeBs were transmitting at high power to service large macrocells in the sparsely populated area. The eNodeBs corresponded to two U.S. cellular providers (Verizon Wireless and T-Mobile), and they were

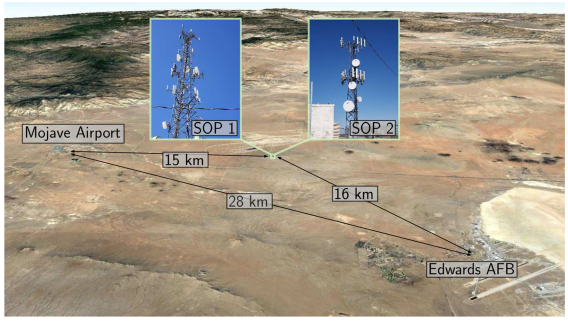


Figure 4.
SOP LTE eNodeB layout. Map data: Google Earth.

transmitting on dual frequencies. The characteristics of the two eNodeBs are summarized in Table 3.

HARDWARE SETUP

The ground vehicle was equipped with hardware setup shown in Figure 5, which was comprised of i) Septentrio GNSS-INS system and ii) LTE front-end. The hardware setup is described in the following.

SEPTENTRIO GNSS-INS SYSTEM

The Septentrio GNSS-INS system consists of the following: a multifrequency GNSS AsteRx-i V receiver, a tactical-grade Vectornav VN-100 microelectromechanical system IMU, and a dual-GNSS antenna system. AsteRx-i V processes the dual antenna multifrequency GNSS signals with IMU measurements to generate an accurate and reliable position and orientation solution. Multi-GNSS

Table 3.

eNodeBs' Characteristics			
eNodeB	Carrier frequency [MHz]	$N_{\mathrm{ID}}^{\mathrm{Cell}}$	Cellular provider
1	751 / 2125	377	Verizon
2	731.5 / 2145	491	T-Mobile

antennas 1 and 2 were mounted on a wooden board that was mounted on the roof of the vehicle and aligned with the vehicle's main axis. Antenna-1, i.e., the main antenna, was toward the back of the vehicle. Antenna-2, i.e., the auxiliary antenna, was toward the front of the vehicle. The VN-100 IMU was mounted on the wooden board as well, with its x-axis pointing toward the front of the vehicle, the y-axis pointing to the right of the vehicle (as seen from behind the vehicle), and the z-axis pointing downward. It is worth noting that only GPS was jammed, while signals from other GNSS constellations (Galileo and GLONASS) were available. The GNSS-INS system was used to obtain the vehicle's ground truth trajectory by using signals from the nonjammed GNSS constellations.

LTE FRONT-END

The LTE front-end comprised of the following:

1) a quad-channel universal software radio peripheral (USRP)-2955;

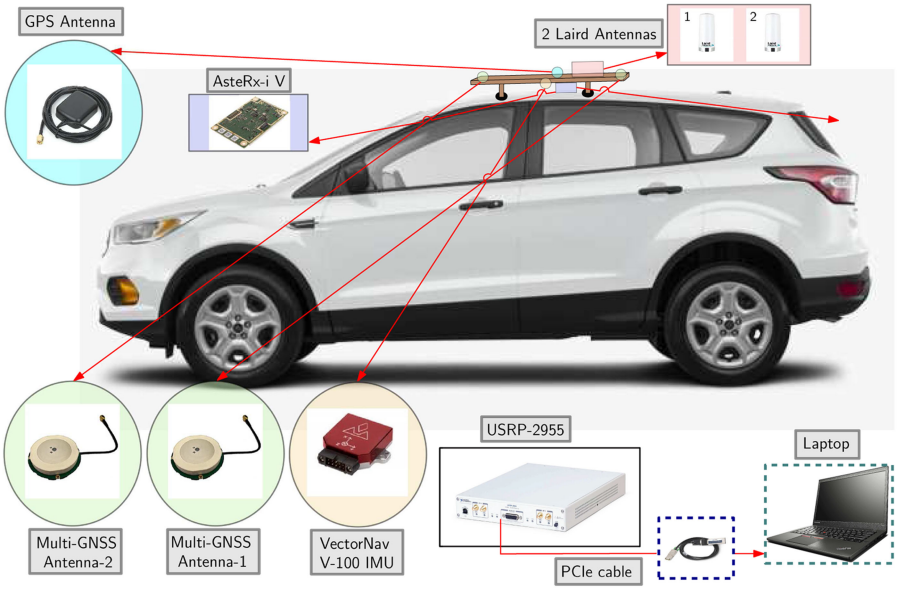


Figure 5.
Ground vehicle and hardware setup.

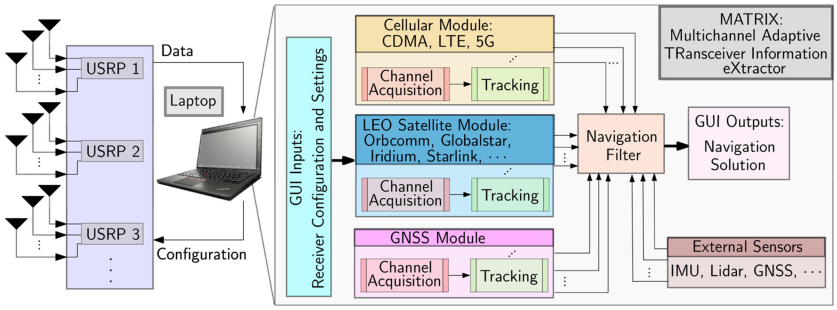


Figure 6.
MATRIX cognitive SDR architecture. The SDR consists of the following: (i) USRPs to collect different radio signals, (ii) various modules to produce navigation observables from different types of signals (e.g., cellular, LEO satellites, etc.), (iii) external sensors (e.g., IMU, lidar, GNSS receivers, etc.), whose measurements can be fused with the navigation observables produced by the signal modules, and (iv) navigation filter that fuses all measurements to produce a navigation solution.

2) two consumer-grade 800/1900 MHz Laird cellular antennas;
3) a PCIe cable;
4) a laptop;
5) a consumer-grade GPS antenna to discipline the USRP's onboard GPS-disciplined oscillator (GPSDO).

The two Laird antennas were connected to the USRP to capture impinging LTE signals, and the USRP was tuned to listen to two carrier frequencies corresponding to the eNodeBs in Table 3.

SOFTWARE SETUP

The software setup used in the performed experiment included the following: i) Septentrio's postprocessing software development kit and ii) MATRIX, which are described in the following.

SEPTENTRIO POSTPROCESSING SOFTWARE DEVELOPMENT KIT (PPSDK) TOOL

Septentrio's PP-SDK was used to process GNSS observables collected by the AsteRx-i V to obtain a GNSS-INS navigation solution. This integrated GNSS-INS system was used to produce the ground truth results with which the produced navigation solution was compared.

MATRIX COGNITIVE SDR

MATRIX is a state-of-the-art cognitive SDR, developed at the ASPIN Laboratory, for navigation with terrestrial and space-based SOPs [47]–[51]. MATRIX continuously searches for

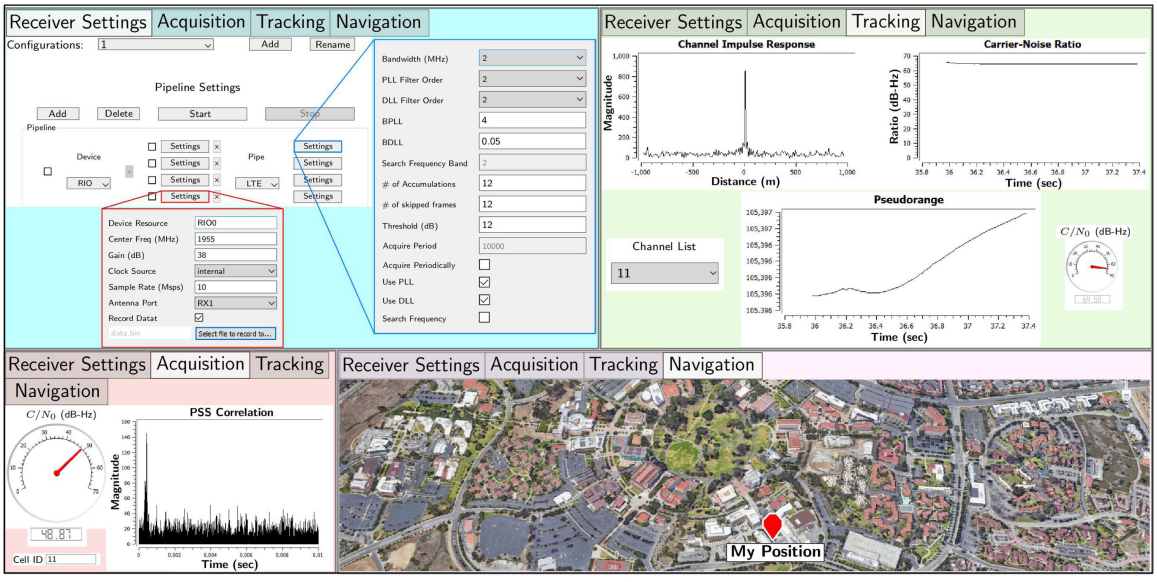


Figure 7.
GUI of the LTE module of the MATRIX SDR. The interface has four main windows: (i) Receiver Settings: to be set by the user; (ii) Acquisition and (iii) Tracking: show the resulting signals in real-time; and (iv) Navigation: plots the navigation solution.

opportune signals from which it draws navigation and timing information, employing signal characterization on-the-fly as necessary. MATRIX could produce a navigation solution in a standalone fashion or by fusing SOPs with sensors (e.g., IMU, lidar, etc.), digital maps, and/or other signals (e.g., GNSS). Figure 6 shows MATRIX's architecture. The conducted experiment used MATRIX's carrier-aided code phase-based LTE module [48] to produce LTE navigation observables. Figure 7 shows the graphical user interface (GUI) front panel of the LTE module of MATRIX.

PNT EXPERIMENTAL RESULTS IN THE GPS-JAMMED ENVIRONMENT

Two experiments were conducted to study the behavior of SOPs in the presence of real GPS jamming and to assess their potential as PNT sources. The results from each experiment are presented as follows.

EXPERIMENT I: STATIONARY RECEIVER

Cellular SOPs are typically equipped with GPSDOs to meet the synchronization requirements set by the 3rd Generation Partnership Project (3GPP). Some opportunistic navigation frameworks exploit the resulting stability of cellular SOPs' clock [30], making it important to evaluate the clock stability of cellular SOPs under GPS jamming to determine their suitability in radio SLAM.

SETUP

The setup described in the sections "Hardware Setup" and "Software Setup" was deployed outside the jamming area to listen to two LTE eNodeBs (SOP 1 and SOP 2) located in an area affected by jamming. The jamming-to-signal (J/S) at the eNodeBs was around 60 dBs. During this experiment, the jammers were periodically turned on for 10 min, then turned off for 2 min. The MATRIX SDR sampled LTE signals synchronously at 10 Msps for 95 min on carrier frequencies 751 MHz and 731.5 MHz, which are frequencies allocated to U.S. cellular providers Verizon Wireless and T-Mobile, respectively. Figure 8 shows the setup of the first experiment.

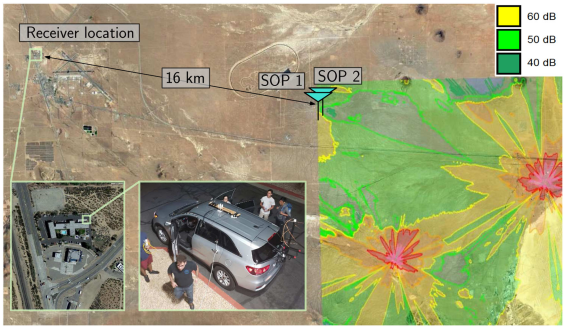


Figure 8.
Experiment 1 setup. The setup discussed in sections "Hardware Setup" and "Software Setup" was deployed outside the GPS-jammed area to listen to two SOPs located in an area where J/S was around 60 dB. Map data: Google Earth.

RESULTS

The LTE signal samples were processed by the LTE module of MATRIX to produce pseudorange observables to the two eNodeBs. The two LTE eNodeBs as well as the receiver were stationary and at known locations. The true range between the receiver and each eNodeB was subtracted from the corresponding pseudorange measurements [cf. (8)]. Figure 9(a) shows the time history of the remaining term (after subtracting the initial pseudorange values). Note that a 5-min dataloss occurred around the 35th minute due to a hardware malfunction. Recalling that the measurement noise is appropriately modeled as white, the trend in the variations, as shown in Figure 9(a) is mainly due to the relative clock biases between the eNodeBs and the receiver. After a short initial transient due to the receiver's GPSDO, the clock biases seem to stabilize. Moreover, both clock biases appear to be driven by a common term, which is likely to be the receiver's bias. To evaluate the relative

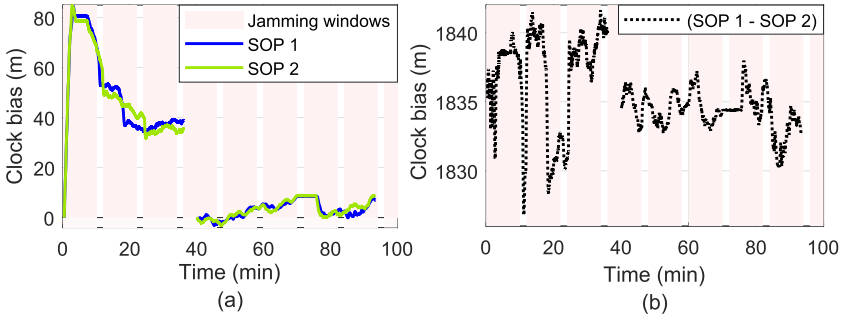


Figure 9.
Experiment 1 results. (a) Time history of clock biases corresponding to SOP 1 and SOP 2. The initial pseudorange values were subtracted. A hardware malfunction around the 35th min caused a 5-min dataloss. (b) Clock bias difference between SOP 1 and SOP 2, without subtracting the initial pseudoranges. The stable difference shows that the relative stability between LTE SOPs is maintained for a period of over 95 min during GPS jamming.

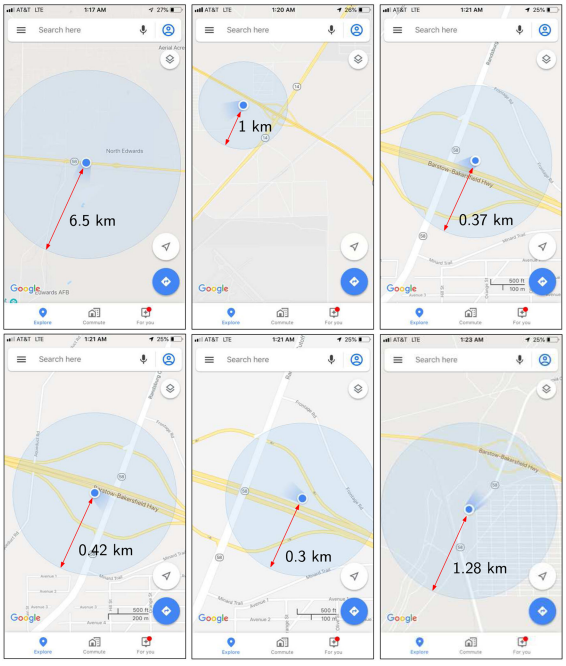


Figure 10.
Screenshots from Google Maps on an iPhone 8 during Experiment 2. The uncertainty grew to a radius over 6 km.

stability between the SOP biases, the difference of the biases (without subtracting their initial values) is plotted in Figure 9(b), which shows a stable difference hovering around 1835 m. Figure 9 does not show significant correlation between the stability of the clock biases and the jamming window, leading to the conclusion that the LTE SOPs' relative stability is maintained for a period of over 95 min during GPS jamming. This could be attributed to either: i) the oscillators equipped on the eNodeBs are disciplined by other GNSS constellations or ii) the free-running oscillators remained stable during the jamming period.

EXPERIMENT 2: MOBILE RECEIVER

Another experiment was conducted to demonstrate the radio SLAM framework with LTE SOPs under real GPS jamming. The experimental setup and results are discussed as follows.

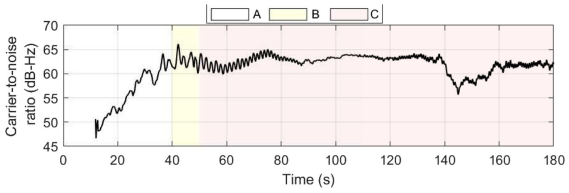


Figure 11.
C/N_0 to the LTE SOP as measured by the ground vehicle. The experiment consists of three time segments: (A) GPS signals available, (B) GPS signals intermittent, and (C) GPS signals were unavailable.

SETUP

In this experiment, a ground vehicle was driven in the east direction along the 58 Highway, as shown in Figure 3. Over the course of the experiment, only one LTE eNodeB (SOP 1) was hearable at 751 MHz. LTE samples were collected at 10 Msps for 8 min. The vehicle started west of the jamming area. The experiment was composed of the following three segments:

1) GPS signals were available (0–40 s);
2) GPS signals were intermittent (40–50 s);
3) GPS signals were not available (50–180 s).

During this experiment, the jammers were operating continuously. The SOP pseudorange measurements were fed to the tightly coupled radio SLAM framework depicted in Figure 1 to estimate the states for two scenarios:

Scenario 1: SOP position was assumed to be *fully known* (from the prior mapping campaign). Here, the estimated state vector in the EKF was $\boldsymbol{x}_r \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, c \cdot (\boldsymbol{x}_{\mathrm{clk},r}^{\mathsf{T}} - \boldsymbol{x}_{\mathrm{clk},s}^{\mathsf{T}})\right]^{\mathsf{T}}$.

Scenario 2: SOP position was assumed to be *unknown*, (a prior with a large uncertainty was used). Here, the estimated state vector in the EKF was $\boldsymbol{x}_r \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \boldsymbol{r}_s^{\mathsf{T}}, c \cdot (\boldsymbol{x}_{\mathrm{clk},r}^{\mathsf{T}} - \boldsymbol{x}_{\mathrm{clk},s}^{\mathsf{T}})\right]^{\mathsf{T}}$.

Table 4.

Experiment 2 Results			
Framework	Position RMSE (m)	Final error (m)	SOP final error (m)
Scenario 1: Radio SLAM with known SOP position	29.4	69.4	–
Secnario 2: Radio SLAM with unknown SOP position	32.2	84.5	5.5
GPS-IMU	237.9	766.0	–

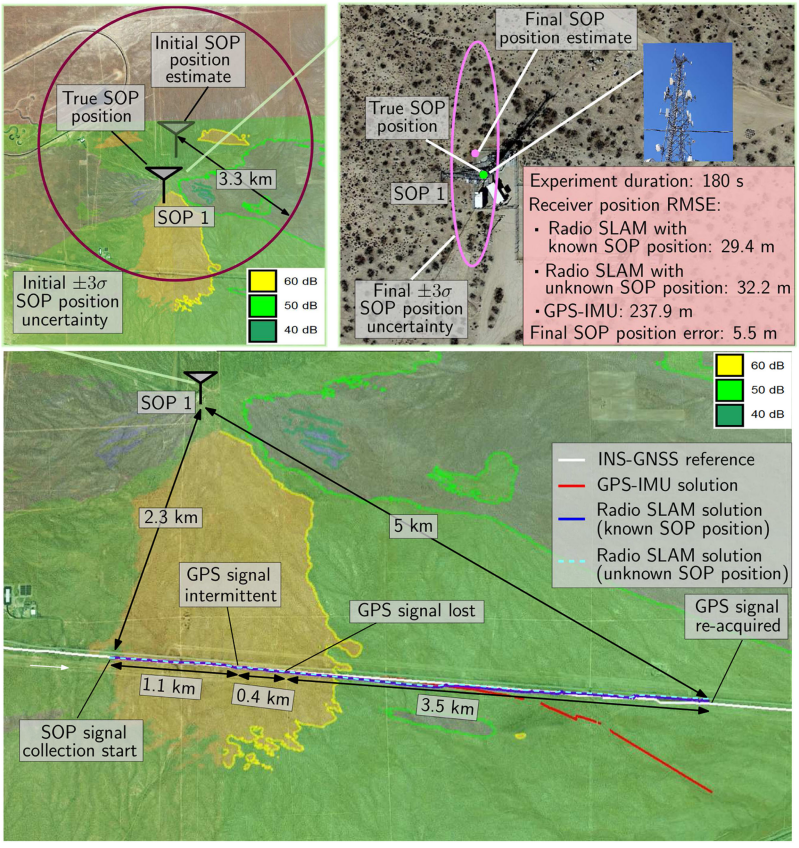


Figure 12.
Experiment 2 results for both scenarios. Map data: Google Earth.

Due to a hardware storage malfunction, the raw IMU data were not properly saved. As such, the radio SLAM with the white noise acceleration dynamical model discussed in the section "Dynamics Model Formulation" was used. The process noise spectral densities were set as $\tilde{q}_x = \tilde{q}_y = 0.01$ m^2/s^3, and $\tilde{q}_z = 0.001$ m^2/s^3 and the receiver's and SOP's oscillators were set to be high quality OCXOs with parameters $h_0 = 2.6 \times 10^{-22}$ and $h_{-2} = 4.0 \times 10^{-26}$. The results are presented as follows.

RESULTS

Results from a smartphone navigation application are provided first to showcase the impact of real GPS jamming on a GPS receiver. Figure 10 shows screenshots from Google Maps running on an iPhone 8 during the ground vehicle's trajectory. Essentially, the navigation solution stopped updating, would sporadically jump around by hundreds of meters, and the blue "halo" representing the estimated position uncertainty grew to a radius over 6 km. Note the time progression shown in the screenshots as the vehicle was driving along the 58 Highway in one direction; nevertheless, the estimated position reported by the iPhone kept jumping around.

In both scenarios, the receiver had access to GPS signals for the first 50 s only. The receiver's last produced GPS navigation solution before GPS signals were

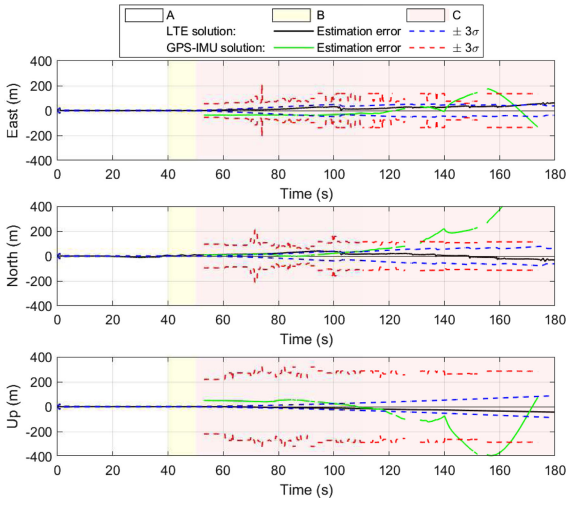


Figure 13.
Experiment 2 EKF results: receiver position error and associated $\pm 3\sigma$ bounds for Scenario 1: assuming *fully known* SOP position. (A) GPS signals available, (B) GPS signals intermittent, and (C) GPS signals unavailable.

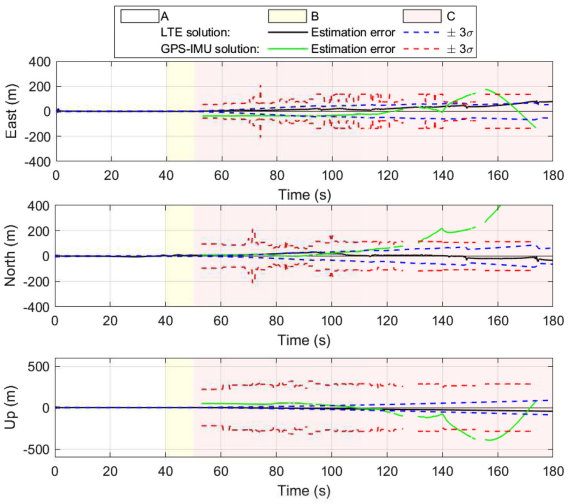


Figure 14.
Experiment 2 EKF results: receiver position error and associated $\pm 3\sigma$ bounds for Scenario 2: assuming *unknown* SOP position. (A) GPS signals available, (B) GPS signals intermittent, and (C) GPS signals unavailable.

lost was used to initialize the position states in both radio SLAM scenarios, and the receiver's and SOP's positions were expressed in an East–North–UP frame, centered at the receiver's initial position. The initial state estimate for Scenario 1 was $\hat{\boldsymbol{x}}^- = \mathbf{0}_{8\times 1}$, while the initial state estimate for Scenario 2 was $\hat{\boldsymbol{x}}^- = [\mathbf{0}_{1\times 6}, 976.9, 3221.3, 58.9, \mathbf{0}_{1\times 2}]^{\mathsf{T}}$. The initial estimation error covariance for Scenario 1 was $\mathbf{P}^- = \mathrm{diag}[1, 1, 1, 10, 10, 10, 1\times 10^9, 45]$, while the initial estimation error covariance for Scenario 2 was $\mathbf{P}^- = \mathrm{diag}[1, 1, 1, 10, 10, 10, 12\times 10^5, 12\times 10^5, 1, 1\times 10^9, 45]$. For Scenario 2, the SOP position was randomly initialized around the true SOP position with an initial 2-D $\pm 3\sigma$ radius of about 3.3 km. For the random realization used in the EKF, the initial SOP position error was 1.07 km. Figure 11 shows C/N_0 as measured by the vehicle-mounted receiver to the LTE SOP.

For Scenario 1, the receiver's 2-D position RMSE was found to be 29.4 m with a final 2-D position error of 69.4 m. For Scenario 2, the receiver's final 2-D position RMSE was found to be 32.2 m with a final 2-D position error of 84.5 m. The SOP's final 2-D position error was 5.5 m. For comparison, a GPS-IMU solution was produced using Septentrio's PPSDK tool for the same trajectory. The receiver's 2-D position RMSE was found to be 237.9 m from the GPS-IMU solution with a final 2-D position error of 766.0 m. Table 4 and Figure 12 summarize the results of Experiment 2.

The EKF position error and associated $\pm 3\sigma$ bounds for Scenario 1 are shown in Figure 13. The EKF position error and associated $\pm 3\sigma$ bounds for Scenario 2 are shown in Figure 14 for the receiver and in Figure 15 for the SOP. It can be seen from these figures that, as expected, the GPS-

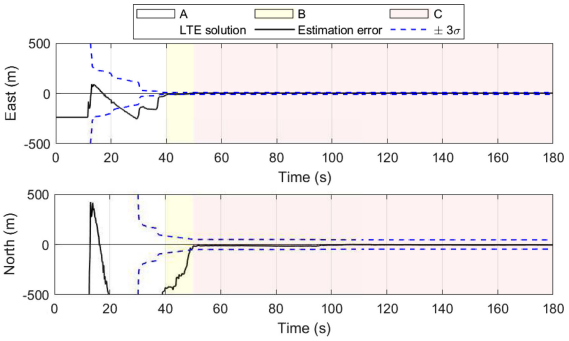


Figure 15.
Experiment 2 EKF results: SOP position error and $\pm 3\sigma$ bounds. (A) GPS signals available, (B) GPS signals intermittent, and (C) GPS signals unavailable.

IMU errors diverge unboundedly in the GPS-jammed region. What appears to be alarming is that these errors are inconsistent with the reported σ-bounds. In contrast, the errors for both Scenarios 1 and 2 in the east and north directions are consistent with the σ-bounds and are drifting at a much lower rate. This drift could be attributed to poor estimability—recall that a *single* SOP is being used and that the vehicle is quickly moving away from the SOP. Of course, using an IMU would reduce this drift as it would provide more precise time updates than the assumed white noise acceleration dynamical model. In fact, this slowly drifting behavior is consistent with the results presented in the work of Morales and Kassas [27] with a single SOP. Using signals from two or more SOPs was shown to alleviate this drift and yield bounded errors. The divergence in the Up direction is simply due to poor geometric diversity in the vertical direction, which could be readily accounted for with an external sensor (e.g., altimeter).

DISCUSSION

The following can be concluded from the aforementioned results. First, Experiment 1 shows that cellular SOP clocks remain relatively stable during the jamming period. This could be attributed to: i) the jamming was intermittent, as shown in Figure 9, which could have allowed the SOPs' on-board GPSDOs to relock to GPS and ii) by design, cellular transmitter clocks are required to maintain $\pm 3\,\mu$s synchronization with GPS time, even after 8 h of GPS signal loss [52]. Future studies could consider longer periods of GPS jamming (more than 8 h), to fully characterize the behavior of cellular SOP clocks in the presence of a persistent GPS jammer.

Second, as expected, the performance of radio SLAM with unknown SOP position is worse than that of radio SLAM with known SOP positions. This is due to the poorer estimability of the state space in Scenario 2, as more states are being estimated from the same pseudorange measurements. The final position errors in Scenarios

1 and 2 highlight this degradation in the performance. However, the EKF error is a random process itself, and can theoretically take arbitrary realizations from an underlying distribution at any point in time. As such, the position RMSE is a more insightful measure of the filter performance. What is interesting is that the degradation of the RMSE performance between Scenarios 1 and 2 is about 3 m, which is on the same order of magnitude as the SOP position estimation error in Scenario 2.

Third, the nature of the experiment makes it difficult to be performed in an urban region. The environment in which the experiment took place was rural, where cellular SOPs tend not to be as abundant as urban regions. Within the same region, one could receive signals from faraway SOPs on an aerial platform compared to a ground platform. As such, future studies could consider conducting the experiments on an aerial platform, which would increase the number of hearable SOPs.

CONCLUSION

This article justified why I am not afraid of the GPS jammer, as long as there are ambient SOPs to exploit in the environment. A radio SLAM approach was presented, which enables the exploitation of SOPs for resilient navigation in environments where GPS signals are challenged or denied. Radio SLAM could produce an SOP-derived navigation solution in a standalone fashion or by fusing SOPs with sensors, digital maps, and/or other signals (e.g., GNSS). This article presented the first published experimental results for navigation with SOPs in a GPS-denied environment. These experiments took place at Edwards AFB, during DT NAVFEST, in which GPS was intentionally jammed with J/S as high as 90 dB. The results analyzed the clock stability of two cellular SOP LTE eNodeBs in the jammed area, showing that the relative stability between the LTE SOPs is maintained for a period of more than 95 min during GPS jamming. Moreover, the results showcased a ground vehicle traversing a trajectory of about 5 km in 180 s in the GPS-jammed environment, during which a GPS-IMU system drifted from the vehicle's ground truth trajectory, resulting in a position RMSE of 238 m. In contrast, the radio SLAM approach with a *single* cellular LTE SOP whose position was poorly known (an initial uncertainty on the order of several kilometers) achieved a position RMSE of 32 m.

ACKNOWLEDGMENTS

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-19-1-2511 and Grant N00014-19-1-2613, in part by the National Science Foundation (NSF) under Grant 1929965, and in part by part by the U.S. Department of Transportation (USDOT) under Grant 69A3552047138 for the CARMEN University Transportation Center (UTC). The authors would like to thank Edwards AFB for inviting the ASPIN Laboratory to conduct experiments during DT NAVFEST. The authors would also like to thank J. Morales, K. Shamaei, M. Maaref, K. Semelka, M. Nguyen, and T. Mortlock for their help with data collection.

Distribution Statement A. Approved for public release; Distribution is unlimited 412TW-PA-20399.

REFERENCES

[1] D. Borio, F. Dovis, H. Kuusniemi, and L. Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233–1245, Feb. 2016.

[2] M. Psiaki and T. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[3] R. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Feb. 2016.

[4] C. Hegarty, D. Bobyn, J. Grabowski, and A. Van Dierendonck, "An overview of the effects of out-of-band interference on GNSS receivers," *NAVIGATION, J. Inst. Navigat.*, vol. 67, no. 1, pp. 143–161, Mar. 2020.

[5] Z. Kassas, J. Khalife, A. Abdallah, and C. Lee, "I am not afraid of the jammer: Navigating with signals of opportunity in GPS-denied environments," in *Proc. 33rd Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2020, pp. 1566–1585.

[6] D. Gebre-Egziabher, "What is the difference between 'loose', 'tight', 'ultra-tight' and 'deep' integration strategies for INS and GNSS," *Inside GNSS*, 2007, pp. 28–33.

[7] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, 2015.

[8] J. Morton, F. van Diggelen, J. Spilker Jr., and B. Parkinson, Eds., "Position, navigation, and timing technologies in the 21st century," in *Part D: Position, Navigation, and Timing Using Radio Signals-of-Opportunity*, vol. 2. Berlin, Germany: Wiley, 2021, ch. 35–43, pp. 1115–1412.

[9] 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, OH, USA, 2006.

[10] X. Chen, Q. Wei, F. Wang, Z. Jun, S. Wu, and A. Men, "Super-resolution time of arrival estimation for a symbiotic FM radio data system," *IEEE Trans. Broadcast.*, vol. 66, no. 4, pp. 847–856, Dec. 2020.

[11] R. Faragher and R. Harle, "Towards an efficient, intelligent, opportunistic smartphone indoor positioning system," *NAVIGAT., J. Inst. Navigat.*, vol. 62, no. 1, pp. 55–72, 2015.

[12] A. Makki, A. Siddig, M. Saad, and C. Bleakley, "Survey of WiFi positioning using time-based techniques," *Comput. Netw.*, vol. 88, pp. 218–233, 2015.

[13] C. Gentner, T. Jost, W. Wang, S. Zhang, A. Dammann, and U. Fiebig, "Multipath assisted positioning with simultaneous localization and mapping," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6104–6117, Sep. 2016.

[14] J. del Peral-Rosado, R. Raulefs, J. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1 G to 5 G," *IEEE Commun. Surv. Tut.*, vol. 20, no. 2, pp. 1124–1148, Apr.–Jun. 2018.

[15] Z. Kassas, "Navigation With Cellular Signals of Opportunity," in *Position, Navigation, and Timing Technologies in the 21st Century*, vol. 2, J. Morton, F. van Diggelen, J. Spilker Jr., and B. Parkinson, Eds. Berlin, Germany: Wiley, ch. 37, pp. 1171–1223, 2021.

[16] A. Abdallah and Z. Kassas, "UAV navigation with 5 G carrier phase measurements," in *Proc. ION GNSS Conf.*, 2021, pp. 3294–3306.

[17] C. Yang, T. Nguyen, and E. Blasch, "Mobile positioning via fusion of mixed signals of opportunity," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 29, no. 4, pp. 34–46, Apr. 2014.

[18] L. Chen, O. Julien, P. Thevenon, D. Serant, A. Pena, and H. Kuusniemi, "TOA estimation for positioning with DVB-T signals in outdoor static tests," *IEEE Trans. Broadcast.*, vol. 61, no. 4, pp. 625–638, Dec. 2015.

[19] T. Reid, A. Neish, T. Walter, and P. Enge, "Broadband LEO constellations for navigation," *NAVIGAT., J. Inst. Navigat.*, vol. 65, no. 2, pp. 205–220, 2018.

[20] 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 Mag.*, vol. 14, no. 3, pp. 56–64, May 2019.

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

[22] M. Lichtman, R. Jover, M. Labib, R. Rao, V. Marojevic, and J. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, Apr. 2016.

[23] A. Gupta, R. Jha, P. Gandotra, and S. Jain, "Bandwidth spoofing and intrusion detection system for multistage 5 G wireless communication network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 618–632, Jan. 2018.

[24] W. Xu, C. Yuan, S. Xu, H. Ngo, and W. Xiang, "On pilot spoofing attack in massive MIMO systems: Detection and countermeasure," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1396–1409, 2021, doi: 10.1109/TIFS.2020.3036805.

[25] A. Abdallah, J. Khalife, and Z. Kassas, "Experimental characterization of received 5 G signals carrier-to-noise ratio in indoor and urban environments," in *Proc. IEEE Veh. Technol. Conf.*, 2021, pp. 1–5.

[26] Z. Kassas and T. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 260–273, Feb. 2014.

[27] J. Morales and Z. Kassas, "Tightly-coupled inertial navigation system with signals of opportunity aiding," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 3, pp. 1930–1948, Jun. 2021.

[28] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular position tracking using LTE signals," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3376–3391, Apr. 2017.

[29] A. Abdallah and Z. Kassas, "Deep learning-aided spatial discrimination for multipath mitigation," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, 2020, pp. 1324–1335.

[30] J. Khalife and Z. Kassas, "Precise UAV navigation with cellular carrier phase measurements," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, 2018, pp. 978–989.

[31] C. Yang and A. Soloviev, "Simultaneous localization and mapping of emitting radio sources-SLAMERS," in *Proc. ION GNSS Conf.*, 2015, pp. 2343–2354.

[32] Z. Kassas, M. Maaref, J. Morales, J. Khalife, and K. Shamaei, "Robust vehicular localization and map matching in urban environments through IMU, GNSS, and cellular signals," *IEEE Intell. Transp. Syst. Mag.*, vol. 12, no. 3, pp. 36–52, Jun. 2020.

[33] J. Morales and Z. Kassas, "Stochastic observability and uncertainty characterization in simultaneous receiver and transmitter localization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 2, pp. 1021–1031, Apr. 2019.

[34] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation With Applications to Tracking and Navigation*. New York, NY, USA: Wiley, 2002.

[35] J. Dunik, O. Kost, O. Straka, and E. Blasch, "State and measurement noise in positioning and tracking: Covariance matrices estimation and gaussianity assessment," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, 2018, pp. 1326–1335.

[36] M. Shuster, "A survey of attitude representations," *J. Astronautical Sci.*, vol. 41, no. 4, pp. 439–517, Oct. 1993.

[37] P. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed. Norwood, MA, USA: Artech House, 2013.

[38] M. Braasch, "Inertial navigation systems," in *Aerospace Navigation Systems*. Hoboken, NJ, USA: Wiley, 2016.

[39] X. Li and V. Jilkov, "Survey of maneuvering target tracking. Part I: Dynamic models," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 4, pp. 1333–1364, Oct. 2003.

[40] A. Thompson, J. Moran, and G. Swenson, *Interferometry and Synthesis in Radio Astronomy*, 2nd ed. New York, NY, USA: Wiley, 2001.

[41] J. Curran, G. Lachapelle, and C. Murphy, "Digital GNSS PLL design conditioned on thermal and oscillator phase noise," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 1, pp. 180–196, Jan. 2012.

[42] M. Psiaki and S. Mohiuddin, "Modeling, analysis, and simulation of GPS carrier phase for spacecraft relative navigation," *J. Guid., Control, Dyn.*, vol. 30, no. 6, pp. 1628–1639, Nov./Dec. 2007.

[43] P. Teunissen, "The least-squares ambiguity decorrelation adjustment: A method for fast GPS integer ambiguity estimation," *J. Geodesy*, vol. 70, no. 1, pp. 65–82, Nov. 1995.

[44] X. Chang, X. Yang, and T. Zhou, "MLAMBDA: A modified LAMBDA method for integer least-squares estimation," *J. Geodesy*, vol. 79, no. 9, pp. 552–565, 2005.

[45] J. Khalife and Z. Kassas, "Opportunistic UAV navigation with carrier phase measurements from asynchronous cellular signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 4, pp. 3285–3301, Aug. 2020.

[46] K. Shamaei and Z. Kassas, "Sub-meter accurate UAV navigation and cycle slip detection with LTE carrier phase," in *Proc. ION GNSS Conf.*, 2019, pp. 2469–2479.

[47] J. Khalife, K. Shamaei, and Z. Kassas, "Navigation with cellular CDMA signals—Part i: Signal modeling and software-defined receiver design," *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2191–2203, Apr. 2018.

[48] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *NAVIGAT., J. Inst. Navigat.*, vol. 65, no. 4, pp. 655–675, Dec. 2018.

[49] K. Shamaei and Z. Kassas, "Receiver design and time of arrival estimation for opportunistic localization with 5G signals," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4716–4731, Jul. 2021.

[50] M. Orabi, J. Khalife, and Z. Kassas, "Opportunistic navigation with Doppler measurements from Iridium Next and Orbcomm LEO satellites," in *Proc. IEEE Aerosp. Conf.*, 2021, pp. 1–9.

[51] J. Khalife, M. Neinavaie, and Z. Kassas, "The first carrier phase tracking and positioning results with starlink LEO satellite signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 2, pp. 1487–1491, Apr. 2022, doi: 10.1109/TAES.2021.3113880.

[52] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0010-E, Mar. 2014. [Online]. Available: http://www.arib.or.jp/english/html/overview/doc/STD-T64v7_00/Specification/ARIB_STD-T64-C.S0010-Ev2.0.pdf