Development and Demonstration of a TDOA-Based GNSS Interference Signal Localization System

Jahshan A. Bhatti, Todd E. Humphreys, *The University of Texas at Austin, Austin, TX*
Brent M. Ledvina, *Coherent Navigation, San Mateo, CA*

***Abstract*—Background theory, a reference design, and demonstration results are given for a Global Navigation Satellite System (GNSS) interference localization system comprising a distributed radio-frequency sensor network that simultaneously locates multiple interference sources by measuring their signals' time difference of arrival (TDOA) between pairs of nodes in the network. The end-to-end solution offered here draws from previous work in single-emitter group delay estimation, very long baseline interferometry, subspace-based estimation, radar, and passive geolocation. Synchronization and automatic localization of sensor nodes is achieved through a tightly-coupled receiver architecture that enables phase-coherent and synchronous sampling of the interference signals and so-called reference signals which carry timing and positioning information. Signal and cross-correlation models are developed and implemented in a simulator. Multiple-emitter subspace-based TDOA estimation techniques are developed as well as emitter identification and localization algorithms. Simulator performance is compared to the Cramér-Rao lower bound for single-emitter TDOA precision. Results are given for a test exercise in which the system accurately locates emitters broadcasting in the amateur radio band in Austin, TX.**

I. Introduction

Despite its marvelous success over the last three decades, the Global Positioning System (GPS) has an Achilles' heel: its weak signals are an easy target for jamming. The National Space-Based Positioning, Navigation, and Timing Advisory Board in a recent white paper has concluded that the "United States is now critically dependent on GPS" [1]. The paper notes an alarming increase in the incidence rate of deliberate and unintentional GPS interference, which in some cases renders GPS inoperable for critical infrastructure operations. The white paper also notes the increasing availability of small and cheap GPS jammers known as personal privacy devices (PPDs). Although the advertised jamming coverage radius for these devices is small, typically 10 to 20 meters, their actual range may extend to tens of kilometers [2].

In one recent case of interest, a test version of the GPS ground-based augmentation system (GBAS) at Newark International Airport suffered from periodic interference due to a PPD aboard a truck traveling on a nearby highway [3]. The authorities took four months to track down the jammer. Continued monitoring in the Newark airport area after this incident indicates that during rush hours, there occur 4 to 5 interference events per hour, presumably due to PPDs [4]. GPS-synchronized cellular communications networks also report an increasing rate of periodic GPS outages, most likely due to passing PPDs. Although these networks are designed to fall back to a hold-over mode that is capable of maintaining adequate synchronization for several days, such interference is nonetheless an annoyance for network operators.

Despite a recent effort by the Federal Communications Commission to discourage sale, purchase, and use of PPDs [5], there is reason to believe that they will only become more widespread in the future. The miniaturization and proliferation of GPS trackers will likely lead to an increased use of PPDs, despite their being illegal, as people seek to protect their privacy from invasive tracking [6]. To aid in enforcing laws against PPDs and jamming devices, there is a need for a persistent system capable of detecting and locating sources of jamming.

There is extensive literature on passive geolocation and time difference of arrival (TDOA) estimation. This paper develops an interference localization solution that is based on maximum likelihood TDOA estimation techniques which can be traced back to the 1970s [7–9]. These techniques are based on analysis of the cross-power spectral density (CPSD) of an emitter signal received at two sensors with some differential delay. The very long baseline interferometry (VLBI) community uses similar techniques to estimate the group delay between the received signals at separate reference stations [10].

For single-emitter TDOA estimation, it is often sufficient to choose the delay that maximizes the time-domain cross-correlation function [11–14]. However, for multiple emitters, analysis of the CPSD offers better resolution because powerful subspace methods such as multiple signal classification (MUSIC) can be applied to distinguish the frequency-domain components due to the various emitters [15].

In so-called passive geolocation, where the structure of the interference signals is not known *a priori*, the estimated TDOAs must be associated with emitters. In other words, one must decide from which emitter, if any, a TDOA measurement originated. Previous solutions to the data association problem, which require solving a computationally-demanding high-dimensional assignment problem, are reviewed in [16], and a computationally-efficient "tracking" extension of the problem is introduced. The effect of non-line-of-sight TDOA measurements due to multipath reflections and ways to detect those measurements through consistency checks are considered in [14].

More particularly related to the problem of locating GPS interference sources, the work by Scott (J911) [17], Brown (JLOC) [18], and Chronos Technology (GAARDIAN) [19] focus on building cheap, low-network-throughput jamming-to-

Preprint of the 2012 IEEE/ION PLANS Conference
Myrtle Beach, SC, April 21–23, 2012

noise ratio sensors based on monitoring GPS carrier-to-noise ratio and automatic gain control (AGC) values, making them suited only for triggering and coarse localization. The work by Akos considers a network of sensor nodes using a low-cost Global Navigation Satellite System (GNSS) front end with AGC monitoring capability. Single-emitter interference localization is implemented using AGC values coupled with power-law path loss models for strong sources and cross-correlation-based TDOA estimation coupled with hyperbolic positioning for weak sources [11, 12].

The current paper offers a thorough overview of the emitter localization problem and describes the design and implementation of an operational prototype system targeted to GNSS interference source detection and localization. Theoretical models for received signals from multiple emitters are developed with appropriate assumptions for typical terrestrial emitter localization applications. For improved location precision, the prototype system is implemented with a spatially-distributed array of sensor nodes. The technique of synchronizing sensor nodes by clock-sharing via coaxial cable, as in [13], cannot be applied to this system because the sensors are separated by km-length baselines. Instead, the sensors make use of ambient radio frequency (RF) timing signals such as GPS or cellular code division multiple access (CDMA) to provide timing synchronization [11, 20]. For sensors on moving platforms, a position, velocity, and time solution (commonly obtained from GNSS signals) is required to synchronize the correlator's time and frequency offset.

The current work extends the previous work on TDOA-based GNSS interference source localization in [11, 13] by emphasizing simultaneous localization of multiple emitters. The multiple-emitter problem is addressed under reasonable assumptions about the emitter signal spectral shape, allowing the TDOAs to be detected and estimated in a straightforward subspace and least-squares fitting framework. The problem of TDOA data association is addressed through a simple but effective phase closure consistency check which assumes that the TDOA measurements are not significantly affected by multipath. A simulator developed to provide a testbed for validating theory and refining algorithms is described and both simulated and field-test results for the localization algorithms are provided.

II. Signal Models

The models developed in this section form the basis of the TDOA estimation algorithms. The development is guided by derivations given in the radar literature [21], but adapted for passive geolocation.

A. Received Signal Model

Consider the following model for the signal transmitted by an interference source (hereafter emitter):

$$s(t) = A_s(t)\cos\left(2\pi f_c t + \phi_s(t)\right). \tag{1}$$

Here, $A_s(t)$ is the instantaneous amplitude, f_c is the center frequency, and $\phi_s(t)$ is the transmitted beat carrier phase. For convenience, consider the complex envelope $\tilde{s}(t) = A_s(t)\exp\left(j\phi_s(t)\right)$ and analytic representation $\hat{s}(t) = \tilde{s}(t)\exp\left(2\pi f_c t\right)$ of the transmitted signal $s(t)$. Note that analytic signals are a valid approximation when the complex envelope is slowly varying with respect to the center frequency (i.e. bandpass signals) [21]. Assume that the radio propagation channel induces a non-dispersive delay $\tau_\rho(t)$, an attenuation $A(\bar{\rho})$ that is a function of the average range $\bar{\rho}$ over the time-of-flight interval, and additive white Gaussian noise $n'(t)$. Then the received signal $r'(t)$ at the sensor can be modeled as

$$r'(t) = A(\bar{\rho})\, s\left(t - \tau_\rho(t)\right) + n'(t), \tag{2}$$

or with an analytic representation as

$$\hat{r}'(t) = A(\bar{\rho})\, \hat{s}\left(t - \tau_\rho(t)\right) + \hat{n}'(t), \tag{3}$$

where $\hat{n}'(t)$, the analytic representation of $n'(t)$, is a complex white Gaussian noise process with single-sided power spectral density N_0 in W/Hz. Other propagation effects like multipath and shadowing are not considered in this model.

For electromagnetic waves traveling in a vacuum, the propagation delay $\tau_\rho(t)$ satisfies the implicit relationship

$$c\tau_\rho(t) = \sqrt{\left(\boldsymbol{r}_e\left(t-\tau_\rho\right) - \boldsymbol{r}_s(t)\right)^{\mathrm{T}}\left(\boldsymbol{r}_e\left(t-\tau_\rho\right) - \boldsymbol{r}_s(t)\right)}, \tag{4}$$

where c is the speed of light, $\boldsymbol{r}_s(t)$ is the sensor position vector, and $\boldsymbol{r}_e(t)$ is the emitter position vector [22]. For short propagation distances and electromagnetic wave velocities, (4) can be approximated as

$$c\tau_\rho(t) = \rho(t) = \sqrt{\boldsymbol{r}(t)^{\mathrm{T}}\,\boldsymbol{r}(t)}, \tag{5}$$

where $\boldsymbol{r}(t) = \boldsymbol{r}_e(t) - \boldsymbol{r}_s(t)$ is the relative position vector and $\rho(t)$ is the instantaneous range. The range rate is given by $\dot{\rho}(t) = \boldsymbol{r}(t)^{\mathrm{T}}\,\dot{\boldsymbol{r}}(t)/\rho(t)$. In a further approximation that applies to emitters and sensors with moderate standoff distances and terrestrial velocities, the delay can be modeled linearly as

$$c\tau_\rho(t) = \rho(0) + \dot{\rho}(0)\, t \tag{6}$$

over a small interval of time about $t = 0$.

Let the relationship between the time t_r at the sensor and true time t be given by

$$t = t_r - \tau_r(t_r), \tag{7}$$

where $\tau_r(t_r)$ is the sensor's clock offset from true time. The clock is parametrized by a sensor clock offset bias a_{f0} and clock offset drift or fractional frequency error a_{f1} so that the sensor's clock offset time history $\tau_r(t_r)$ is given by

$$\tau_r(t_r) = a_{f0} + a_{f1} t_r. \tag{8}$$

The linear model is valid for the clocks used in this application over a small interval of time about $t_r = 0$ where small is defined as less than 100 ms for a temperature-compensated crystal oscillator or 10 s for an oven-controlled crystal oscillator.

Suppose that a mixing signal with nominal center frequency f_c is generated with the sensor's clock. The mixing signal's phase $\phi_r(t_r)$ is related to t_r by

$$\phi_r(t_r) = 2\pi f_c t_r + \phi_{r,0}, \tag{9}$$

where $\phi_{r,0}$ is the initial phase of the oscillator. Let the mixing operation be modeled such that the resulting baseband signal $\tilde{r}'(t)$ is given by

$$\begin{aligned}\tilde{r}'(t) &= \hat{r}'(t)\exp(-j\phi_r(t_r)) \\ &= A(\bar{\rho})\,\tilde{s}(t-\tau_\rho(t))\exp(-j\phi'(t,t_r)) + \tilde{n}'(t),\end{aligned} \tag{10}$$

where

$$\phi'(t,t_r) = 2\pi(t_r - t + \tau_\rho(t))f_c + \phi_{r,0} \tag{11}$$

and $\tilde{n}'(t) = \hat{n}'(t)\exp(-j\phi_r(t_r))$ is a zero-mean baseband complex Gaussian process. The sensor clock model in (7) is used in (10) to express $\tilde{r}'(t)$ in the sensor's time base, denoted $\tilde{r}(t_r)$. The noise-free baseband received signal $\tilde{s}_r(t_r)$ is given by

$$\tilde{s}_r(t_r) = A(\bar{\rho})\,\tilde{s}(t_r - \tau_m(t_r))\exp(-j\phi_m(t_r)), \tag{12}$$

with the apparent delay $\tau_m(t_r)$ defined as

$$\tau_m(t_r) = \tau_r(t_r) + \tau_\rho(t_r - \tau_r(t_r)) \tag{13}$$

and the received beat carrier phase $\phi_m(t_r)$ given by

$$\phi_m(t_r) = 2\pi f_c \tau_m(t_r) + \phi_{r,0}. \tag{14}$$

The full expression for the baseband received signal $\tilde{r}(t_r)$ is given by

$$\tilde{r}(t_r) = \tilde{s}_r(t_r) + \tilde{n}(t_r), \tag{15}$$

where $\tilde{n}(t_r) = \tilde{n}'(t_r - \tau_r(t_r))$ is still a zero-mean baseband complex Gaussian process. Given the aforementioned linear approximations for the clock and range delays, the apparent delay can be approximated by linear parameters $\tau_{m,0}$ and $\dot{\tau}_m$ as

$$\tau_m(t_r) \approx \tau_{m,0} + \dot{\tau}_m t_r. \tag{16}$$

Assuming a nominal sampling rate T_s, the digital representation of the signal $\tilde{r}(t_r)$ is given by $\tilde{r}[k] = \tilde{r}(kT_s)$. The noise $\tilde{n}(t_r)$ is generated at each sensor based on the noise power density N_0 in W/Hz over the single-sided noise-equivalent bandwidth B_n in Hz. Therefore, the noise power σ_n^2 in Watts is given by

$$\sigma_n^2 = N_0 B_n. \tag{17}$$

The complex noise time series $\tilde{n}[k]$ is a scaled and filtered version of a sequence of random samples whose real and imaginary components are independent and normally distributed. The noise samples are scaled so that

$$E[\tilde{n}[k]\tilde{n}^\star[k]] = 2\sigma_n^2. \tag{18}$$

The emitter has an average transmitted power density P_s in W/Hz over the single-sided noise-equivalent bandwidth. The spreading loss $L(\bar{\rho})$ is given by

$$L(\bar{\rho}) = \frac{\lambda_c^2}{4\pi^2\bar{\rho}^2}, \tag{19}$$

where $\lambda_c = c/f_c$ is the nominal wavelength of the signal. Isotropic transmit and receive antennas and no cable loss are assumed. The received signal power σ_s^2 in Watts is given by

$$\sigma_s^2 = L(\bar{\rho})\,P_s B_n. \tag{20}$$

The signal component of the received signal $\tilde{s}_r[k] = \tilde{s}_r(kT_s)$ is scaled so that

$$E[\tilde{s}_r[k]\tilde{s}_r^\star[k]] = 2\sigma_s^2, \tag{21}$$

which constrains $A(\bar{\rho})$ in (2) appropriately.

Finally, the received signal $\tilde{r}_i(t_r)$ at sensor i from M emitters can be modeled as a sum of components of the form in (15):

$$\begin{aligned}\tilde{r}_i(t_r) = \sum_{l=1}^{M} A(\bar{\rho}_i^l)\,\tilde{s}^l\left(t_r - \tau_{m_i}^l(t_r)\right) \\ \times \exp\left(-j\left[2\pi f_c \tau_{m_i}^l(t_r) + \phi_{r_i,0}\right]\right) + \tilde{n}_i(t_r),\end{aligned} \tag{22}$$

where the apparent delay for emitter l and sensor i is defined as a specialization of (13):

$$\tau_{m_i}^l(t_r) = \tau_{r_i}(t_r) + \tau_{\rho_i}^l(t_r - \tau_{r_i}(t_r)). \tag{23}$$

B. The Cross-Ambiguity Function

Consider the following narrowband cross-ambiguity function $S_{\tilde{z}_i\tilde{z}_k}(\tau, f_D)$, which has been adapted from the radar literature [21], for a pair of complex baseband signals $\tilde{z}_i(t)$ and $\tilde{z}_k(t)$:

$$S_{\tilde{z}_i\tilde{z}_k}(\tau, f_D) \triangleq \frac{1}{T}\int_{-T/2}^{T/2} \tilde{z}_i(t)\,\tilde{z}_k^\star(t+\tau)\,e^{-j2\pi f_D t}dt, \tag{24}$$

where T is the length of the integration interval, τ is the delay, and f_D is the Doppler frequency. The forthcoming equations will be simplified by using the difference operator $\Delta_{ik}(\cdot) = (\cdot)_k - (\cdot)_i$, that is, the placement of a Δ_{ik} in front of a quantity indicates a difference of that quantity between sensors i and k. The cross-ambiguity function $S_{\tilde{r}_i\tilde{r}_k}(\tau, f_D)$ for a pair of signals $\tilde{r}_i(t)$ and $\tilde{r}_k(t)$ from receivers i and k, respectively, using the single-emitter propagation model in (15) and linearized apparent delay is approximately given by

$$\begin{aligned}S_{\tilde{r}_i\tilde{r}_k}(\tau, f_D) \approx \alpha_{ik} S_{\tilde{s}\tilde{s}}(\tau - \Delta_{ik}\tau_{m,0}, f_D - \Delta_{ik}\dot{\tau}_m f_c) \\ + N_{ik}(\tau, f_D),\end{aligned} \tag{25}$$

where the complex attenuation factor α_{ik} is defined as

$$\alpha_{ik} = A(\bar{\rho}_i)\,A(\bar{\rho}_k)\,e^{j[2\pi\Delta_{ik}\tau_{m,0}f_c + \Delta_{ik}\phi_{r,0}]} \tag{26}$$

and $N_{ik}(\tau, f_D)$ is the noise function, which includes all correlation terms involving the noise signal $\tilde{n}(t)$. In (25), it is assumed that the apparent range rate $\dot{\tau}_m$, which is

related to the velocity of the emitter and oscillator clock drift rate, is small and has negligible impact on the correlation over the integration interval. The impact is negligible if the bandwidth of the baseband signal $\tilde{s}(t)$ is small with respect to the carrier frequency f_c. This is known as the narrowband approximation [21]. The delay and Doppler that maximize the magnitude of the ambiguity function, denoted respectively as $\hat{\tau}_{ik}$ and $\hat{f}_{D,ik}$, are the corresponding time and frequency difference of arrival (T/FDOA) measurements between sensors i and k for a single emitter [21].

Again, invoking the narrowband approximation, the cross-ambiguity function $S_{\tilde{r}_i\tilde{r}_k}(\tau, f_D)$ can be written for M emitters in terms of the auto-ambiguity terms $A_{ik}(\tau, f_D)$, the cross-ambiguity terms $C_{ik}(\tau, f_D)$, and the noise terms $N_{ik}(\tau, f_D)$, as

$$S_{\tilde{r}_i\tilde{r}_k}(\tau, f_D) \approx A_{ik}(\tau, f_D) + C_{ik}(\tau, f_D) + N_{ik}(\tau, f_D). \quad (27)$$

The auto-ambiguity terms are of most interest and can be written as

$$A_{ik}(\tau, f_D) = \sum_{l=1}^{M} \alpha_{ik}^{l} S_{\tilde{s}^l\tilde{s}^l}\left(\tau - \Delta_{ik}\tau_{m,0}^{l}, f_D - \Delta_{ik}\dot{\tau}_m^{l} f_c\right), \quad (28)$$

where the complex attenuation factor α_{ik}^{l} is defined as

$$\alpha_{ik}^{l} = A\left(\bar{\rho}_i^{l}\right) A\left(\bar{\rho}_k^{l}\right) e^{j\left[2\pi\Delta_{ik}\tau_{m,0}^{l} f_c + \Delta_{ik}\phi_{r,0}\right]}. \quad (29)$$

The cross-ambiguity terms are generally small in the delay-Doppler range of interest provided that there is no strict coordination between emitters.

III. Synchronization And Signal Excision

A. Tightly-Coupled Sensor Architecture

"Tightly-coupled" refers to an RF receiver architecture in which emitter signals and reference signals are down-converted with the same oscillator and sampled in such a way that a nanosecond-accurate correspondence can be made between the two sampled signal streams (coherent signal conditioning and sampling). Fig. 1 shows one straightforward tightly-coupled sensor architecture. Tight coupling between the emitter and reference data enables the data streams from two separate sensors to be synchronized to within nanoseconds and for clock variations over the cross-correlation interval to be estimated and compensated at the carrier-phase level. The tightly-coupled sensor architecture draws from the success of ongoing work in opportunistic navigation at the University of Texas at Austin [20, 23, 24]. Experience with GNSS signals, terrestrial signals of opportunity such as cellular CDMA, and Iridium signals suggests that an emitter localization system could exploit any instance of these three signal types as a reference.

The simplest approach to a tightly-coupled sensor architecture is to use GNSS signals as the reference signals. This approach allows one to exploit the well-known, clean, and stable signal characteristics of GNSS signals. GNSS signal processing can be done within the sensor to minimize network throughput requirements. For example, consider using GNSS

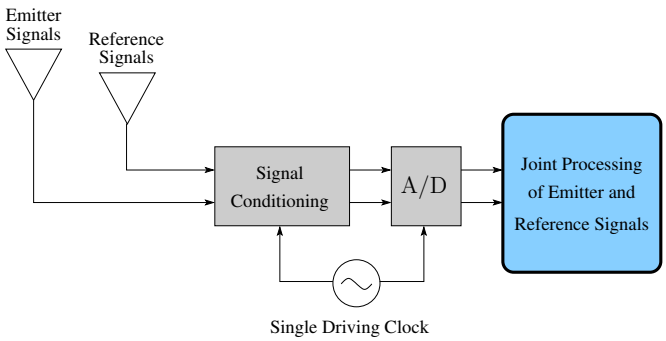


Figure 1: Basic tightly-coupled sensor architecture.

timing to synchronize stationary sensors in known locations. A typical GNSS navigation solution will provide estimates of the receiver clock offset $\tau_{r,0}$ and offset rate $\dot{\tau}_r$. For some sufficiently small time window, a linear model can be applied to the clock offset $\tau_r(t_r) = \tau_{r,0} + \dot{\tau}_r t_r$. Then, (7) can be solved for receiver time in terms of true time as

$$t_r(t) = \frac{t + \tau_{r,0}}{1 - \dot{\tau}_r} = \alpha + (1 + \beta)\, t, \quad (30)$$

where $\alpha = \frac{\tau_{r,0}}{1-\dot{\tau}_r}$ and $\beta = \frac{\dot{\tau}_r}{1-\dot{\tau}_r}$. Invoking the narrowband signal assumption, the baseband synchronized signal $\tilde{r}_s(t)$ is given by

$$\tilde{r}_s(t) \approx \tilde{r}(t + \alpha) \exp(j2\pi\beta f_c t). \quad (31)$$

Therefore, for small clock offset rates, the operations required for synchronization are simply a delay and complex mixing operation.

One might naturally question the wisdom of using GNSS signals as reference signals by pointing out that the emitter to be located may be broadcasting a strong interfering signal within GNSS frequency bands. In this case, the received GNSS carrier-to-noise ratios might be too low to support making reliable timing estimates. This paper addresses this concern in several ways.

First, significant frequency diversity is offered by the combined spectrum assets of modern GNSS systems like GPS, Galileo, GLONASS, and Compass. If any one of the many signal bands within these separate systems is free of interference, then signals from this band can be taken as reference signals. An in-house software-defined radionavigation processing engine, named "GRID," can be embedded for execution on the sensors themselves and is currently capable of acquiring and tracking GPS L1 C/A and GPS L2C signals [20, 25–28]. With some fairly straightforward extensions, the GRID engine is capable of acquiring and tracking all CDMA-based GNSS signals, including GPS L5, GPS L1C, Galileo, Compass, and future CDMA versions of GLONASS signals.

Another approach to mitigating the effects of interference on reference signals drawn from GNSS bands is to draw the reference signals in via a directional antenna. For stationary sensors, a single GNSS signal is all that is required to provide the benefits of a tightly-coupled sensor architecture. Hence, if each sensor is equipped with a directional antenna that

can recover sufficient signal power from just one GNSS satellite (not necessarily the same satellite at each sensor), then the requisite synchronization between the two sensors' data streams can be established. For example, an inexpensive helical antenna pointed toward zenith would have a good chance of capturing the requisite GNSS signal and suppressing a surface-based interference signal.

A third option for dealing with the in-GNSS-bands interference scenario is to capture non-GNSS signals that could be exploited in the same way as GNSS signals to synchronize and stabilize the recorded emitter data. Research at the University of Texas at Austin has shown that forward-link CDMA cellular pilot signals are an excellent reference for tightly-coupled receivers [20, 23, 24]. Typical CDMA cellular base stations transmit signals that arrive with 40 dB greater power than GPS signals, are synchronized to GPS time to within a few microseconds, and offer coherence times at L-band in excess of 100 s [20]. Periodic calibration of forward-link signals during times of GNSS availability can reduce CDMA signals' timing uncertainty to nanoseconds. Thus, for applications where CDMA cellular signals are available—for example, within the US—they represent an excellent backup to GNSS signals for tightly-coupled emitter localization. The GRID software-defined radionavigation processing engine is capable of acquiring and tracking forward-link CDMA cellular pilot signals (see Fig. 2). As with GNSS signals, this processing can be executed onboard the sensors.

```
============ GRID: General Radionavigation Interfusion Device =============
 Receiver time:    0 weeks    160.0 seconds        Build ID:        1379
 GPS time:      1614 weeks 420784.0 seconds
-------------------------------------------------------------------------
CH  TXID    Doppler       BCP           PR      C/N0     Az     El   Status
             (Hz)       (cycles)     (meters)  (dB-Hz)  (deg)  (deg)
-----------------------GPS_L1_CA Channels--------------------------------
 1    1u     430.75     -76149.17  20972555.14  46.3    301.7   12.9    6
 2    2    -2337.63     372213.50  20793027.57  44.1     93.0   10.8    6
 3    5    -2814.11     449035.30  19188750.37  52.3     42.0   32.0    6
 4   15     2229.20    -362763.30  17919804.83  53.6    149.9   48.9    6
 5   18     2228.97    -360186.88  19526452.99  48.6    243.3   29.8    6
 6   21     2027.74    -324302.89  19403848.18  51.0    306.8   34.8    6
 7   25    -2734.77     436530.00  20267387.49  47.7    218.6   19.7    6
 8   26      410.60     -75412.16  17644648.06  54.0     88.4   47.0    6
 9   29      398.14     -71226.59  16810240.92  52.1    287.2   79.5    6
10   30     -731.36     110014.30  20121635.88  46.5    282.3   18.5    6
11   --   ---------  ------------  -----------  ----   ------  -----    -
12   --   ---------  ------------  -----------  ----   ------  -----    -
-----------------------CDMA_UHF_PILOT Channels---------------------------
 1    1       -0.59         91.58   7622658.88  62.0      0.0    0.0    5
------------------------------Navigation Data-----------------------------
 X:  -745467.86   Y: -5462657.31   Z:  3196401.16   deltRx:  -3464962.30
 Xvel:     0.03   Yvel:    -0.04   Zvel:     0.01   deltRxDot:      0.12
=========================================================================
```

Figure 2: Screen output of the GRID software-defined radionavigation engine showing simultaneous tracking of 10 GPS L1 C/A signals and 1 CDMA cellular forward-link pilot signal.

B. Reference Signal Excision

If the emitter and reference signal band are the same, then the ambient reference signals will cross-correlate in the same way as the emitter signals. Therefore, to improve sensitivity to the emitters of interest, it is advantageous to track and remove the ambient reference signals if they have high enough carrier-to-noise ratios before cross-correlation. In CDMA systems, the loss of sensitivity to weak emitters in the presence of strong emitters is known as the near-far effect, and interference cancellation is a commonly-used technique to solve this problem [29, 30]. In addition, the technique was used in [31] to crack the Galileo test codes using the L1-band signals received from a patch antenna, where a software GPS receiver was used to acquire, track, and remove the nuisance GPS/SBAS signals. Ref. [12] considers the same issue when trying to locate weak emitters in the GPS band and solves the problem by using a notch filter to remove the ambient GPS signals before cross-correlation. However, the notch filtering technique is suboptimal and reduces the available emitter signal power that could be used in cross-correlation.

IV. TDOA Estimation

Many parallels can be drawn between VLBI, active radar, and passive geolocation. In the 1970s, high resolution time delay estimation techniques were developed [7, 8] using delay-parameterized models of the phase of the cross-power spectrum (e.g. a linear model for non-dispersive delays). Similarly, in the VLBI community, the group delay estimate is typically couched in terms of a least-squares fit to the slope of the phase of the cross-power spectrum (see Appendix 12.1 of [10]). It has been shown in [32] that this least-squares approach is equivalent to the maximum likelihood estimator developed in [7, 8].

Traditional radar techniques use matched filtering (MF) to determine the delay and Doppler of targets, which is analogous to examining the cross-ambiguity function in passive geolocation as in [12–14]. However, MF is limited by the support of the ambiguity function of the transmitted waveform. As a result, its delay resolution tends to be on the order of the inverse of the bandwidth of the transmitted waveform, and its Doppler resolution tends to be on the order of the temporal support of the transmitted waveform [21, 33]. Therefore, the ability of MF-based methods to distinguish between two closely-spaced targets is severely limited in the delay-Doppler space. In addition, the output of the matched filter leads to peaks that are not centered at the true targets for a majority of the targets due to the superposition of interfering ambiguity functions. Ref. [33] provides a framework for "super-resolution" radar that bypasses the aforementioned limitations for MF by parametrization of the response with a finite set of delays and Doppler-shifts and application of parametric estimation techniques like subspace methods. Non-parametric estimation techniques discretize the delay and Doppler space into a grid and determine if a target is present at each grid point. Given the limitations of non-parametric estimation especially under multiple targets, a parametric approach to estimating the TDOA of emitters is developed in the subsequent subsection.

A. A Parametric Approach to TDOA Estimation

Consider the following model for the CPSD between a pair of sensors,

$$Y_{\tilde{r}_i\tilde{r}_k}(f) = \sum_{l=1}^{M} \alpha_{ik}^{l} Y_{\tilde{s}^l\tilde{s}^l}(f)\, e^{-j2\pi f \tau_{ik}^{l}} + N_{\tilde{r}_i\tilde{r}_k}(f), \quad (32)$$

where α_{ik}^l and τ_{ik}^l are respectively the complex scale factor and the TDOA between sensors i and k of emitter l, $Y_{\tilde{s}^l\tilde{s}^l}(f)$ is the normalized power spectral density of emitter l, and $N_{\tilde{r}_i\tilde{r}_k}(f)$ contains terms due to noise and cross-correlation between the emitter waveforms. Note that the CPSD could be estimated by the discrete Fourier transform of a Doppler cut at some f_D of an estimate of the ambiguity function $R_{\tilde{r}_i\tilde{r}_k}(\tau) = S_{\tilde{r}_i\tilde{r}_k}(\tau, f_D)$. Note that in the case of synchronized sensors and stationary emitters and sensors, $f_D = 0$. The ambiguity function should be windowed appropriately so that only delays of interest, which are driven by the sensor pair's baseline or known emitter waveform repetition rate, are considered. Assuming that the emitter waveforms have normalized, wide, flat frequency spectra ($Y_{\tilde{s}^l\tilde{s}^l}(f) = 1$) and are uncorrelated ($E[N_{\tilde{r}_i\tilde{r}_k}(f)] = 0$), then the measurement model for the power spectral density is given by

$$Y_{\tilde{r}_i\tilde{r}_k}(f) = \sum_{l=1}^{M} \alpha_{ik}^l \exp\left(-j2\pi f \tau_{ik}^l\right) + N_{\tilde{r}_i\tilde{r}_k}(f). \quad (33)$$

The problem is now in terms of parametric estimation of complex exponentials in noise, a well-studied problem [15, 34]. First, guesses for the TDOAs and the number of emitters are initialized using subspace methods like MUSIC [15]. Then, estimates of the power and TDOAs are iterated in a least-squares fitting algorithm until a convergence condition is met. The complex scale factors are estimated using linear least squares fitting (note that α_{ik}^l appears linearly in $Y_{\tilde{r}_i\tilde{r}_k}(f)$) and the TDOAs are updated using an iteration of nonlinear least squares fitting.

B. Subspace Methods for TDOA Estimation

A brief description of subspace methods is provided. Consider a tapped delay line of length $K > M$ that uniformly samples $Y_{\tilde{r}_i\tilde{r}_k}(f)$ with sampling interval Δf. The data model for the tapped delay line is given in (34) on the next page, where $f_k = f_0 + k\Delta f$, or, in vector form,

$$\mathbf{Y} = \mathbf{E}\mathbf{A} + \mathbf{N}, \quad (35)$$

where $\mathbf{A} \in \mathbb{C}^{M\times 1}$ is a vector of complex scale factors, $\mathbf{E} \in \mathbb{C}^{K\times M}$ is a matrix composed of mode vectors $\boldsymbol{e}(\tau) \in \mathbb{C}^{K\times 1}$, and $\mathbf{N} \in \mathbb{C}^{K\times 1}$ is a complex noise vector, with real and imaginary parts distributed normally $\mathcal{N}\left(\mathbf{0}, \sigma_n^2\mathbf{I}\right)$ and uncorrelated with the parameters. The mode vector $\boldsymbol{e}(\tau)$ is given by

$$\boldsymbol{e}(\tau) = \begin{bmatrix} \exp(-j2\pi f_1\tau) \\ \exp(-j2\pi f_2\tau) \\ \vdots \\ \exp(-j2\pi f_K\tau) \end{bmatrix}. \quad (36)$$

Let the $K \times K$ covariance matrix $\mathbf{S}$ be defined as

$$\begin{aligned} \mathbf{S} &= E\left[\mathbf{Y}\mathbf{Y}^{\mathrm{H}}\right] \\ &= \mathbf{E}E\left[\mathbf{A}\mathbf{A}^{\mathrm{H}}\right]\mathbf{E}^{\mathrm{H}} + \sigma_n^2 E\left[\mathbf{N}\mathbf{N}^{\mathrm{H}}\right] \\ &= \mathbf{E}\mathbf{P}\mathbf{E}^{\mathrm{H}} + \sigma_n^2\mathbf{I}, \end{aligned} \quad (37)$$

where $\mathbf{P}$ is the covariance of the complex scale factors. Given a single, uniformly sampled observation of $Y_{\tilde{r}_i\tilde{r}_k}(f)$ of length P with sampling interval Δf, $x[k]$, the covariance matrix can be estimated using the "forward-backward" averaging method [35] as

$$\hat{\mathbf{S}} = \mathbf{X}^{\mathrm{H}}\mathbf{X}, \quad (38)$$

where

$$\mathbf{X} = \begin{bmatrix} x[K+1] & \cdots & x[1] \\ \vdots & \ddots & \vdots \\ x[P-K] & \cdots & x[K+1] \\ \vdots & \ddots & \vdots \\ x[P] & \cdots & x[P-K] \\ x^\star[1] & \cdots & x^\star[K+1] \\ \vdots & \iddots & \vdots \\ x^\star[K+1] & \cdots & x^\star[P-K] \\ \vdots & \iddots & \vdots \\ x^\star[P-K] & \cdots & x^\star[P] \end{bmatrix}. \quad (39)$$

The K eigenvectors $\boldsymbol{v}_i$ and eigenvalues λ_i of $\mathbf{S}$ must satisfy $\mathbf{S}\boldsymbol{v}_i = \lambda_i\boldsymbol{v}_i$, for $i = 1, 2, \ldots, K$. Assuming that all the mode vectors are linearly independent (i.e. $\mathbf{E}$ has full rank), then for $M < K$, the matrix $\mathbf{E}\mathbf{P}\mathbf{E}^{\mathrm{H}}$ is singular and it can be shown that $\mathbf{S}$ has $K-M$ eigenvalues equal to σ_n^2. In fact, an estimate of M can be computed by subtracting the multiplicity of σ_n^2 in the eigenvalues of $\mathbf{S}$ from K. Since $\mathbf{S} = \mathbf{E}\mathbf{P}\mathbf{E}^{\mathrm{H}} + \sigma_n^2\mathbf{I}$, then $\mathbf{E}\mathbf{P}\mathbf{E}^{\mathrm{H}}\boldsymbol{v}_i = \left(\lambda_i - \sigma_n^2\right)\boldsymbol{v}_i$ is true. Note that for each eigenvalue $\lambda_i = \sigma_n^2$, $\mathbf{E}^{\mathrm{H}}\boldsymbol{v}_i = \mathbf{0}$, i.e. the "signal" subspace $\mathbf{E}$ (spanned by the mode vectors) is orthogonal to the "noise" subspace $\mathbf{E}_N$ (spanned by the eigenvectors associated with $\lambda_i = \sigma_n^2$) [15].

Note that in practice, only estimates of $\mathbf{S}$ are available, and the aforementioned conditions are only approximately satisfied. Therefore, the eigenvalues associated with the noise subspace are not exactly σ_n^2, and instead are clustered about σ_n^2 (and the spread of the cluster decreases with more averaging) [15]. Estimating M can be particularly difficult when the gap between the eigenvalues associated with the signal and noise subspace is not clear. Hypothesis tests for estimating M were developed using matrix perturbation theory in [35]. However, for ease of implementation and prototyping, the present algorithms require *a priori* knowledge of M and/or subjective analysis of the eigenvalues of $\mathbf{S}$ (or equivalently the singular values of $\mathbf{X}$). The MUSIC cost function is given by

$$J_{MU}(\tau) = \boldsymbol{e}^{\mathrm{H}}(\tau)\,\mathbf{E}_N\mathbf{E}_N^{\mathrm{H}}\boldsymbol{e}(\tau), \quad (40)$$

which for uniformly sampled signals, can be minimized using Root-Music [36, 37].

The above algorithms are limited in that the data model assumes flat emitter frequency spectra. The performance of the algorithms degrade with model mismatch, and in particular, simulation results indicate MUSIC makes biased or spurious TDOA estimates when the flat spectra assumption is relaxed. Also, the resolvability of two closely-spaced TDOAs decreases as their separation decreases in the presence of noise.

$$\begin{bmatrix} Y_{\tilde{r}_i\tilde{r}_k}(f_1) \\ Y_{\tilde{r}_i\tilde{r}_k}(f_2) \\ \vdots \\ Y_{\tilde{r}_i\tilde{r}_k}(f_K) \end{bmatrix} = \begin{bmatrix} \boldsymbol{e}(\tau_{ik}^1) & \boldsymbol{e}(\tau_{ik}^2) & \cdots & \boldsymbol{e}(\tau_{ik}^M) \end{bmatrix} \begin{bmatrix} \alpha_{ik}^1 \\ \alpha_{ik}^2 \\ \vdots \\ \alpha_{ik}^M \end{bmatrix} + \begin{bmatrix} N_{\tilde{r}_i\tilde{r}_k}(f_1) \\ N_{\tilde{r}_i\tilde{r}_k}(f_2) \\ \vdots \\ N_{\tilde{r}_i\tilde{r}_k}(f_K) \end{bmatrix} \tag{34}$$

The mode vectors associated with closely-spaced TDOAs are nearly linearly dependent, which causes the one of the eigenvectors in the signal subspace to have a small eigenvalue. In the presence of noise, the eigenvector can not be distinguished from the noise subspace if the associated eigenvalue is too small, hence the loss of resolution.

V. Emitter Identification and Localization

In passive geolocation, the estimated TDOAs between all possible pairs of sensors must be associated with possible emitters. Sathyan and others have proposed algorithms to solve this data association problem inherent in passive geolocation [16]. However, the currently implemented algorithm uses the principle of phase closure to verify that a triad of TDOA measurements can be associated with the same emitter. The closure-based algorithm is a simple and effective prototype but more sophisticated methods may be implemented if they prove to be more effective. Consider three true (noise-free) times of arrival (TOAs) of an emitter signal τ_i, τ_j, and τ_k to sensors i, j, and k, respectively. The sensors can be paired in three ways, forming three true TDOAs: $\tau_{ij} = \tau_j - \tau_i$, $\tau_{ik} = \tau_k - \tau_i$, and $\tau_{jk} = \tau_k - \tau_j$. The TDOA measurements

$$\hat{\tau}_{ij} = \tau_{ij} + n_{ij} \tag{41}$$

are assumed to be corrupted by zero-mean noise n_{ij} with covariance given in [13, p. 64]. The TDOA closure metric is defined as

$$\tau_c = \hat{\tau}_{ij} - \hat{\tau}_{ik} + \hat{\tau}_{jk}. \tag{42}$$

Under the hypothesis that the TDOA measurements are associated with an emitter, then $E[\tau_c] = 0$ and $E\left[\tau_c^2\right] = E\left[(n_{ij} - n_{ik} + n_{jk})^2\right]$. A test can be constructed in which a threshold $\tau_{c,th}$ is chosen such that $\tau_c^2 < \tau_{c,th}^2$ indicates that the TDOA measurements under test can be associated with the same emitter for a certain probability of false alarm, although this paper does not carry out the entire analysis of the detection statistic. If a triplet of TDOA measurements "close," then, geometrically, the three hyperbolas intersect at a single point on a plane. However, ambiguities arise when different combinations of TDOA measurements could result in the same TDOA measurement between a pair of sensors. Geometrically, the ambiguity can be interpreted as a single hyperbola being intersected by other pairs of hyperbolas at more than one point as shown in Fig. 3. Information from other sensor triads, if available, must be used to resolve the ambiguity. Also note that additional TDOA measurements caused by multipath reflections will possibly close, yielding extraneous position solutions.

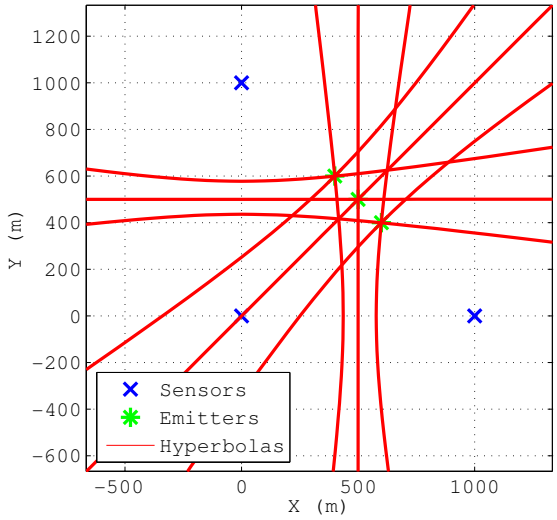


Figure 3: TDOA hyperbola map for a three-emitter scenario in which there are ambiguous phase closures. Note that there are five 3-way intersections of hyperbolas, but only three emitters.

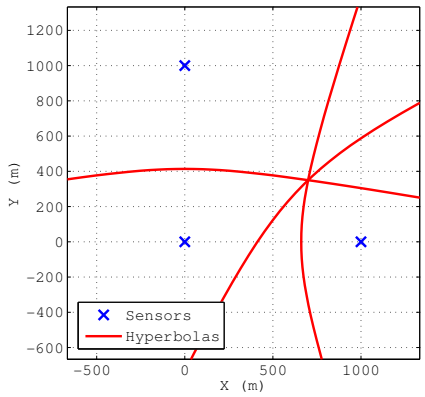
Typically a nonlinear least-squares algorithm is used to locate an emitter given a set of TDOA measurements. Note that a TDOA measurement constrains the emitter position to a hyperbola of revolution. Chan and Ho describe a computationally-efficient estimator for hyperbolic location by using an intermediate variable to reduce the nonlinearities in the problem [38]. However, for simplicity, a standard approach to the problem is implemented. The TDOA measurements that have been associated with a particular emitter are reduced to an independent set of TDOA measurements $\hat{\tau}'_{ik}$, one for each of the sensors involved except for a reference sensor k, using a linear least squares approach [13, p. 63]. This approach exploits the following linear relationship between TDOA measurements,

$$\hat{\tau}_{ij} = \tau_{ik} - \tau_{jk} + n_{ij}, \tag{43}$$

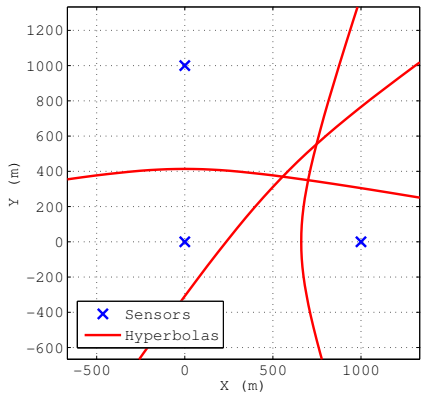
where $\tau_{kk} = 0$. Given N TDOA measurements involving M sensors, N equations of the form in (43) can be stacked so that

$$\boldsymbol{z} = \mathbf{H}\boldsymbol{z}', \tag{44}$$

where $\boldsymbol{z} \in \mathbb{R}^{N\times 1}$ is the vector of TDOA measurements with noise covariance matrix $\mathbf{R} \in \mathbb{R}^{N\times N}$, $\boldsymbol{z}' \in \mathbb{R}^{(M-1)\times 1}$ is the vector of $M-1$ independent TDOA measurements, and $\mathbf{H} \in \mathbb{R}^{N\times(M-1)}$ is the sensitivity matrix governed by the model



(a) "Closed" TDOA hyperbolas.



(b) "Unclosed" TDOA hyperbolas.

Figure 2: Geometric interpretation of TDOA closure metric.

in (43). A least squares solution for $\boldsymbol{z}'$ is given by

$$\hat{\boldsymbol{z}}' = \mathbf{R}'\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\boldsymbol{z} \tag{45}$$

where

$$\mathbf{R}' = \left(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}. \tag{46}$$

Each of the independent $M-1$ TDOA measurements $\hat{\tau}'_{ik}$ in $\hat{\boldsymbol{z}}'$ can be modeled as a nonlinear function of the unknown emitter location and the known sensor locations by

$$c\hat{\tau}'_{ik} = \rho_k - \rho_i + n'_{ik}, \tag{47}$$

where ρ_i is the true range between sensor i and the emitter and n'_{ik} is zero-mean noise. The stacked noise vector $[\cdots, n'_{ik}, \cdots]^{\mathrm{T}}$, arranged in the order of $\hat{\boldsymbol{z}}'$, has covariance $\mathbf{R}'$. A nonlinear least squares search algorithm can be used to estimate the unknown emitter location.

VI. Implementation and Results

A. Theoretical TDOA Estimation Error Bounds

Many derivations of the Cramér-Rao lower bound (CRLB) for single-emitter TDOA precision exist in the literature [9, 10, 13]. One form of the CRLB is given by

$$\sigma^2_{w,\tau_{ij}} \geq \bar{\sigma}^2_{w,\tau_{ij}} = \frac{N_{0,i}N_{0,j}}{8\pi^2 T\alpha_i^2\alpha_j^2\int_{-\Delta f/2}^{\Delta f/2} S_s^2(f)\, f^2 df}, \tag{48}$$

where $\sigma^2_{w,\tau_{ij}}$ is the error variance of the TDOA estimate under a weak received power assumption, $\bar{\sigma}^2_{w,\tau_{ij}}$ is the minimum value this variance can attain (the CRLB), T is the integration time, $S_s(f)$ is the emitter signal power spectral density, Δf is the captured bandwidth, α_i and α_j are the amplitude attenuation of the emitter signal, and $N_{0,i}$ and $N_{0,j}$ are the noise power density, all for the i,jth sensor pair. If, in addition to the received power being weak, the transmitter signal is spectrally flat within the captured band (i.e., $S_i = \alpha_i^2 S_s \ll N_{0,i}$, $S_j = \alpha_j^2 S_s \ll N_{0,j}$), then (48) reduces to

$$\sigma^2_{w,\tau_{ij}} \geq \frac{3N_{0,i}N_{0,j}}{2\pi^2 T S_i S_j \Delta f^3} = \frac{3}{\pi^2 \mathrm{SNR}_p \Delta f^2}, \tag{49}$$

where $\mathrm{SNR}_p = 2T\Delta f\left(\frac{S_i}{N_{0,i}}\right)\left(\frac{S_j}{N_{0,j}}\right)$ is the "passive" cross-correlation signal-to-noise ratio [10]. Relaxing the weak emitter power assumption yields a slightly modified CRLB [9],

$$\sigma^2_{\tau_{ij}} \geq \bar{\sigma}^2_{w,\tau_{ij}}\left(1 + \frac{S_i}{N_{0,i}} + \frac{S_j}{N_{0,j}}\right). \tag{50}$$

Also, [13, p.64] gives expressions for the noise covariance of the TDOA measurement model in (43) as

$$E\left[n_{ij}^2\right] = \sigma^2_{\tau_{ij}}, \tag{51}$$

$$E\left[n_{ij}n_{jk}\right] = \frac{3N_{0,j}}{2\pi^2 T S_j \Delta f^3} = -E\left[n_{ij}n_{kj}\right], \tag{52}$$

$$E\left[n_{ij}n_{kl}\right] = 0. \tag{53}$$

Note that for a fixed number of data samples, or equivalently, constant time-bandwidth product $T\Delta f$, TDOA precision improves only by increasing the captured bandwidth or increasing the emitter power density. In the subsequent subsection, the simulator performance will be compared to the theoretical performance according to the CRLB.

B. Simulated TDOA Estimation Performance

A simulator has been developed to provide guidance and evaluate the performance of the estimation algorithms. The simulator generates the complex baseband samples that would be received at the sensors from any number of emitters using the models and approximations developed in Sec. II. In the simulator, the emitter waveform is oversampled by some integer factor of the receiver sampling rate in order to model the delay with sub-sample resolution using linear interpolation. Currently, the simulator supports generating three types of emitter waveforms: white noise, GPS signals, and continuous

wave signals with linear chirp modulation. The simulated noise time series and emitter waveforms are filtered by a 10th-order Butterworth filter with cutoff frequency B_n to model the sensor front-end filter. The emitter is assumed to be transmitting throughout the duration of the simulation, which lasts from 1–100 milliseconds so that the linear approximations are satisfied.

The TDOA estimation algorithms developed in Sec. IV are verified in a simulation study. The raw samples generated by the simulator are cross-correlated for each sensor pair and the resulting CPSDs are used as inputs to the TDOA estimator. Monte Carlo runs of this configuration yield TDOA estimates whose error variance approaches the theoretical CRLB in (50) for a representative single-emitter scenario. The baseline configuration of the simulator includes one 1 mW white noise emitter that is equidistant from two perfectly synchronized sensors with a 20 km baseline, an integration time of 10 ms, and a captured bandwidth of 500 kHz. The CRLB of the baseline configuration is 10 m. Figs. 4, 5, and 6 show this comparison while varying the parameters T (integration time), Δf (captured bandwidth), and S_s (emitter power density) around the baseline configuration. The red vertical line in the figures indicates when the parameters are equivalent to the baseline scenario. Clearly, the implemented TDOA estimator under single-emitter conditions approaches the CRLB; however, the estimator becomes unreliable for small integration times and weak emitters since SNR_p is below the estimator's detection threshold.

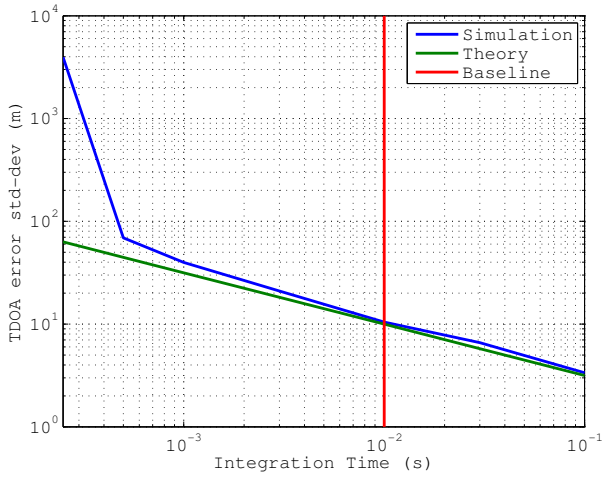


Figure 4: TDOA precision comparison while varying integration time T, holding all other parameters constant.

Now consider an extension of the baseline scenario in which the single emitter is replaced by two emitters with some separation distance having geometry as shown in Fig. 7. Figs. 8 and 9 highlight the predicted breakdown of the estimator when TDOA separation decreases for several different values of emitter power. The two emitters were assumed to transmit at equal power. Note that to improve the estimator performance slightly, only 80% of the captured bandwidth was

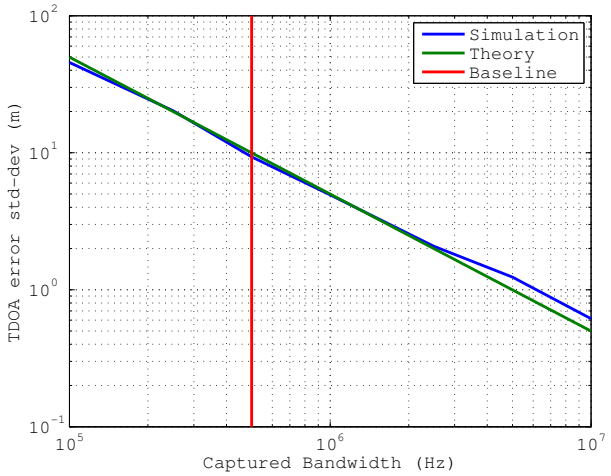


Figure 5: TDOA precision comparison while varying the captured bandwidth Δf, holding the time-bandwidth product and other parameters constant. The time-bandwidth product is held constant to reduce execution times of the simulator and estimation algorithms. Note that it is acceptable to hold the transmitted emitter power density constant because it is assumed that transmitted emitter bandwidth is larger than the captured bandwidth, which is usually the case for GPS jammers [2].

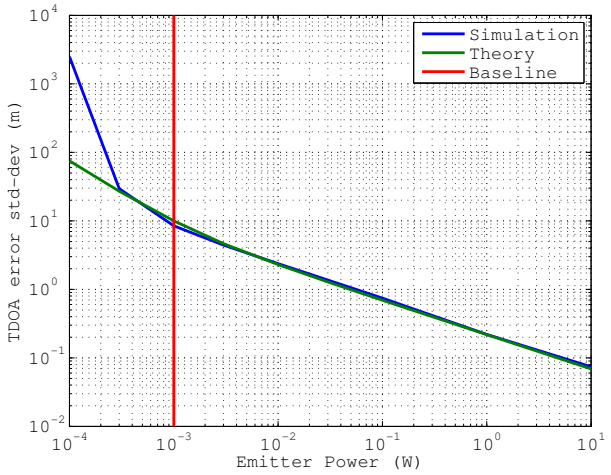


Figure 6: TDOA precision comparison while varying the emitter power density S_s, holding all other parameters constant.

considered so that the spectrum contributing to the CPSD did not contain the edges of the simulated front-end filter. For this simulation, the emitters are considered resolved when the estimated TDOAs are within 50% TDOA separation of the true TDOAs. The gradual increase in error as the TDOA separation decreases is due to the mode vectors becoming correlated (i.e. $\mathbf{E}$ in (37) is nearly singular). The spikes in error at certain TDOA separations are due to the complex attenuation factors of the two signals being almost 180 degrees apart in

phase, causing destructive interference. Note that constructive interference occurs when the TDOA separation is an integer multiple of the transmitted wavelength, which, for GPS L1, is approximately 19 cm. The TDOA resolution offered by the proposed multiple-emitter algorithm is better than matched-filtering (MF) techniques, whose resolution is typically limited by Δf^{-1} [21, 33]. For the baseline scenario, MF resolution is 600 m, which is when the main lobes of the ambiguity functions associated with each emitter begin interfering.

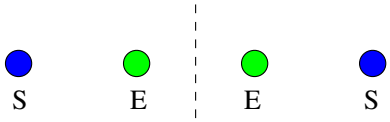


Figure 7: Sensor geometry for multiple-emitter baseline scenario. The sensors and emitters are collinear and symmetric about the dashed line.

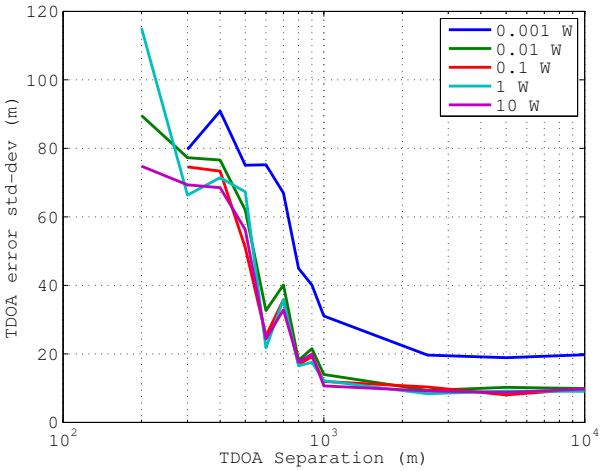


Figure 8: TDOA precision while varying the TDOA separation and emitter power, holding all other parameters constant. The emitters were placed in such a way to keep SNR_p approximately constant for all TDOA separations.

C. Prototype System Performance

1) Prototype Sensor: To support live testing, a small emitter localization network has been implemented in Austin, TX. The network comprises one mobile sensor and two fixed RF sensors. The fixed sensors, located at the University of Texas Center for Space Research and Applied Research Laboratory, straddle a major highway. The fixed sensors are denoted CSR and ARL and the mobile sensor is denoted MBL. A pictorial overview of the network is given in Fig. 10.

Each of the sensors in the network is composed of

- Two Ettus Research Universal Software Radio Peripheral (USRP) N200s.
- One Dell Precision T3500 workstation (fixed sensors) or one Panasonic Toughbook laptop (mobile sensor).

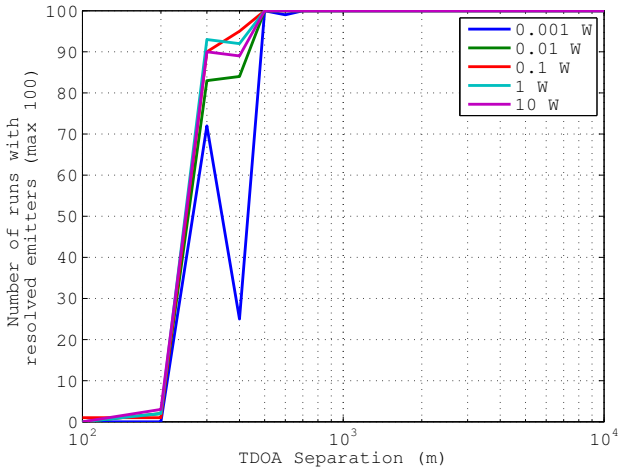


Figure 9: TDOA resolution performance under the same conditions as Fig. 8

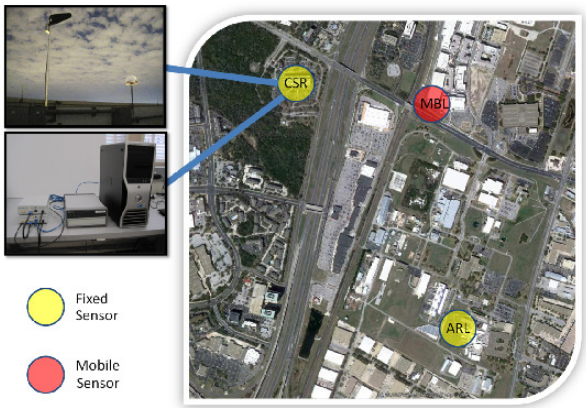


Figure 10: The University of Texas at Austin Prototype Emitter Localization Network.

- One oven-controlled crystal oscillator (OCXO) serving as a local frequency reference.
- Required antennas, amplifiers, and cabling.

The USRP N200 with the DBSRX2 daughterboard, shown in Fig. 10, down-converts and digitizes RF signals between 800 MHz and 2.4 GHz. The USRP N200s are connected together with a MIMO cable so that their clocks are synchronized to within 1 ns. In the fixed stations, the raw complex samples generated by the pair of N200s are sent to the Dell workstation via Gigabit Ethernet. The USRP N200 supports complex sampling rates up to 25 MHz for 16-bit samples and up to 50 MHz for 8-bit samples with experimental firmware. The antenna used for receiving emitter signals is broadband (750–3000 MHz) and directional, with a peak gain of 7 dBi. One USRP is dedicated to sensing the emitter to be tracked and the other is used for receiving timing signals

from GPS or CDMA to synchronize the sensor network. Fig. 10 shows the antenna configuration on the rooftop of the CSR station. GPS signals are received from a separate hemispherical GPS antennas, rather than from the broadband emitter antenna, because the hemispherical antenna has better multipath mitigation properties and more signals in view. The ARL station has a similar configuration.

The MBL station, shown in Fig. 11, is identical to the CSR and ARL stations except that (1) data are collected on a laptop, (2) a narrowband 2300 MHz antenna is used for receiving the emitter signal, and (3) the narrowband antenna gain pattern is azimuthally homogeneous whereas the broadband antenna used at CSR and ARL has a 3-dB beamwidth of approximately 70 degrees.

The network includes a non-real-time MATLAB-based processing center. A web interface has been developed to automate data capture from each of the stationary sensors (CSR and ARL) as shown in Fig. 12. High-resolution data (16-bit quantization) are streamed over the campus network to a central processing computer for after-the-fact processing. Data from the mobile sensor are recorded locally to hard disk and brought back to campus for processing. When all data for a particular capture window have been loaded onto the central processor, an automated sequence of processing steps is executed, with some manual supervision.

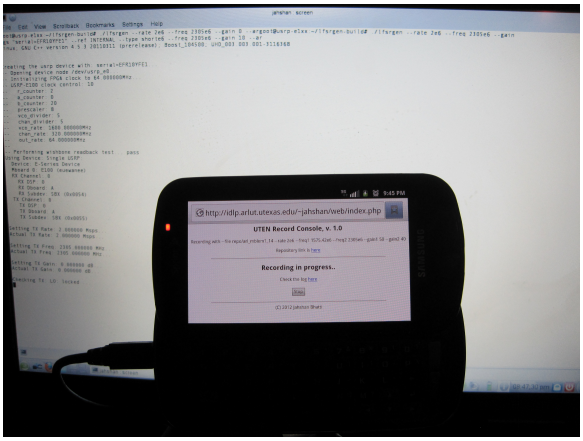


Figure 12: Web recording interface for stationary sensors shown on cell phone browser with laptop controlling USRP E100 emitter in background.

2) Localization: To illustrate the operation of the prototype network, results are offered from a test exercise attempting to locate two emitters placed in the parking lot of a shopping center near the centroid of the sensor network. Two USRP E100s served as emitters. These were programmed to transmit either the GPS L1 C/A chipping sequences for PRN1 or PRN2 at 1 Mcps with carrier frequency of 2.305 GHz, which falls in the US amateur radio band. The emitters transmitted approximately 10 mW of power and were operated under a valid amateur radio license. The sensor's complex sampling rate was set to 2 Msps for the emitter and reference channels. The test exercise's emitter-sensor geometry is shown in Fig. 13.

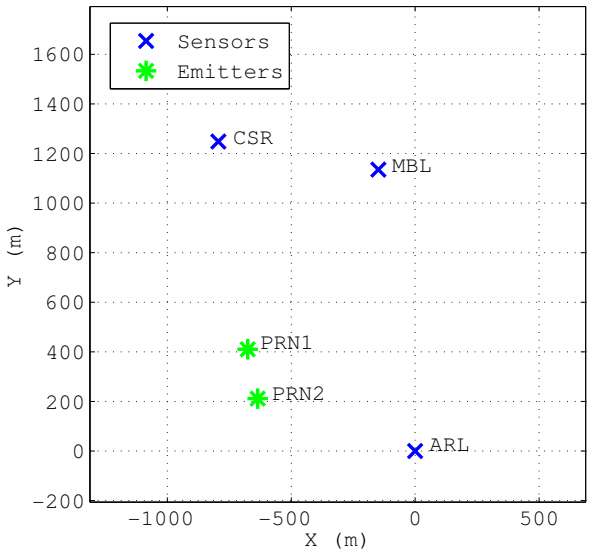


Figure 13: Location of sensors and emitters for test exercise.

Before proceeding with standard cross-correlation techniques for locating the E100 emitters, the emitter data from each sensor were processed in a so-called active tracking mode. In this mode, knowledge of the signal structure is assumed; thus, correlation against a noise-free local signal replica is possible. In typical emitter localization scenarios, active tracking is not possible because one does not know the exact emitter signal structure. Passive tracking based on cross-correlation of data from multiple sensors is used instead. In the test exercise, active tracking was used at first only to get information about the multipath environment and the emitters' relative signal strengths. Active tracking revealed that each sensor received the two emitter signals with comparable signal strength, although the signal from PRN2 was stronger in all cases (Fig. 14), and the ARL station data showed significant multipath distortion in the PRN1 code (Fig. 15).

Emitter data from the three sensor pairs were cross-correlated and estimates of the CPSD are formed. Multiple emitters were manifest in the CPSD as a sum of complex exponentials in the frequency domain. The quasi-sinusoidal patterns in the real and imaginary traces in Fig. 16 are the result of a complex superposition of components from the two emitters sensed by the ARL-MBL sensor pair.

MUSIC separates the signal from the noise subspaces, yielding estimates of the TDOAs. One can either assume knowledge of the number of emitters present or attempt to estimate this number based on the MUSIC singular values. The CSR-ARL pair whose MUSIC singular values are plotted in Fig. 17 shows evidence of three possible emitters of comparable strength due to the multipath corruption that was noted in connection with Fig. 15. Fig. 17 highlights the fact that MUSIC can be used to estimate the number of emitters (or, in reality, the number of strong RF propagation paths) present. For the test exercise,

(a) The GPS and 2300 MHz antenna are placed on top of the vehicle.

(b) The USRP N200 RF recording equipment, power supply, and OCXO are placed inside the vehicle.

Figure 11: The MBL station is parked on top of a tall, nearby parking garage to ensure line-of-sight view of the emitters.

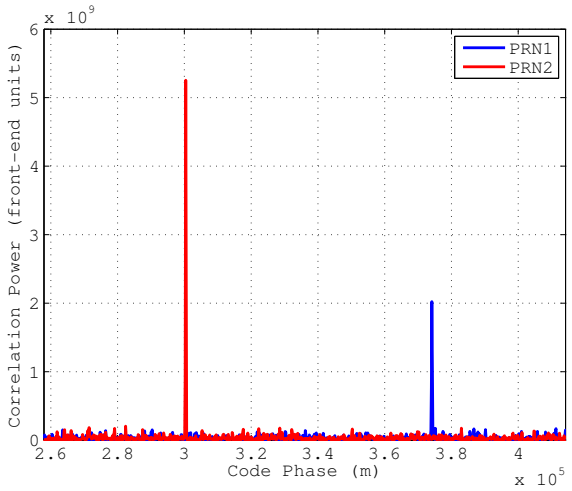


Figure 14: Active tracking of GPS L1 C/A PRN codes in CSR data reveals the presence of the two emitter signals.

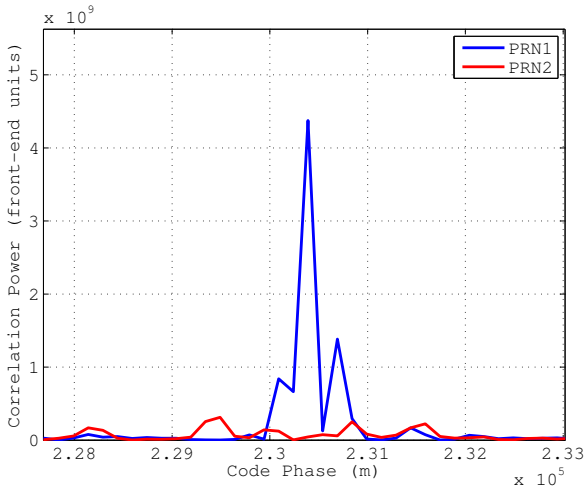


Figure 15: Active tracking of GPS L1 C/A codes in ARL data shows significant multipath distortion of the PRN1 code. The peak of the PRN2 code is outside the code phase window.

it was assumed that the CSR-ARL and ARL-MBL sensor pair detected three emitters and the CSR-MBL pair detected only one emitter, which seemed to best fit the data. Note that in the CSR-MBL pair, the TDOAs associated with the two emitters were too closely spaced to be resolved given the SNR_p in this test exercise.

The estimated TDOAs must each be associated with a particular emitter. This is done by examining the TDOA closure metric which should be small when emitters are correctly associated. For the exercise, the closure threshold was subjectively chosen to be 100 m. Once a TDOA 3-tuple has been associated, emitters can then be precisely located at 3-way hyperbolic intersection points. Hyperbolic trace estimates from five independent data segments are overlaid in Fig. 18 with 1 s integration time. Fig. 19 shows the corresponding emitter location estimates, but because of the multipath corruption, three possible emitter locations are shown. Note that the TDOA measurement resulting from the CSR-MBL sensor pair closes more than one 3-tuple of TDOAs, so it was assumed that there could be an emitter at each of those intersections.

The location precision is about 20 m and the mean of one cluster of position estimates is within 10 m of a true emitter (PRN2). It is not known whether the other position clusters are associated with the other emitter (PRN1) or multipath. The absolute location accuracy is limited by not accounting for the antenna heights of the sensors and emitters and the differential delay between the reference and emitter channel due to 100s of feet of coaxial cable at the fixed sensors and frequency-dependent biases in the USRP front end.

Note that if only one emitter is assumed to be present in the received data, then the TDOA estimates become biased and jump between different emitters as their strength varies as shown in Figs. 20 and 21. Clearly, multiple-emitter TDOA

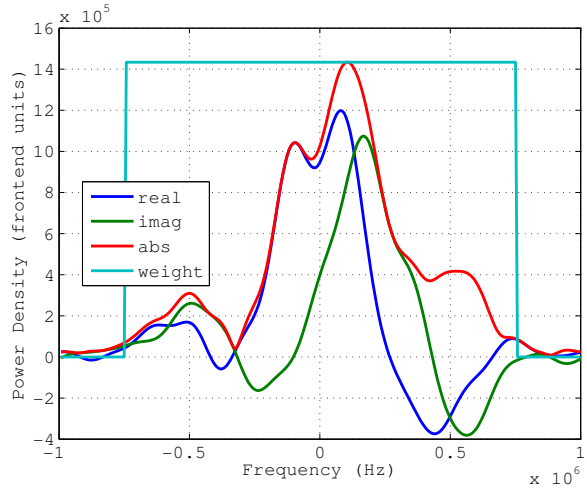


Figure 16: Cross power spectral density estimate for ARL-MBL pair based on 1 s of coherent averaging. Multiple emitters are manifest as a sum of complex exponentials in the frequency domain. The light blue line indicates the boxcar frequency weighting applied when estimating TDOAs for each emitter.

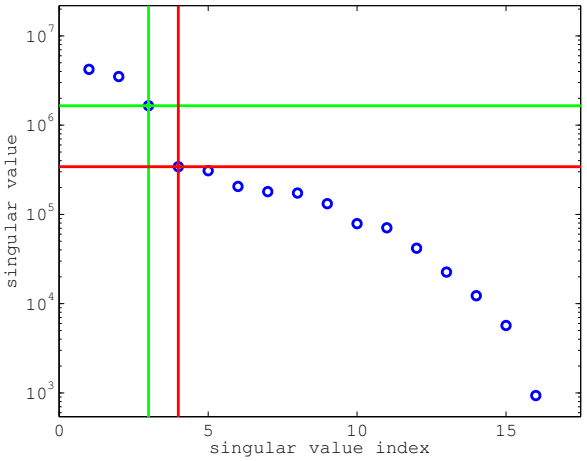


Figure 17: Singular values produced by the MUSIC algorithm for the CSR-ARL pair. Assuming three emitters, the green lines indicate the boundary of the signal subspace and the red lines indicate the boundary of the noise subspace. Note that there is a clear separation between the strongest noise singular value and the weakest signal singular value.

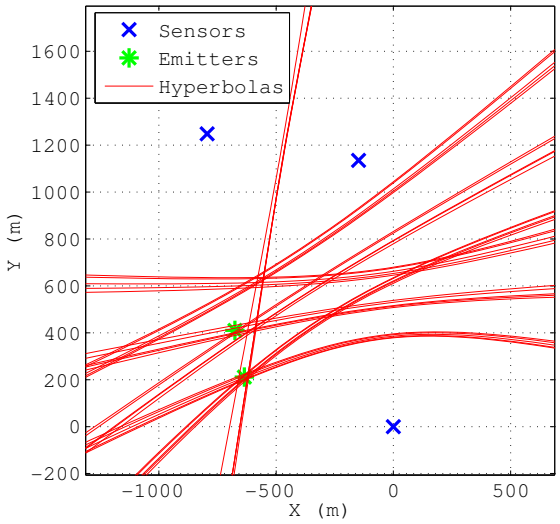


Figure 18: TDOA hyperbola map for the amateur band test exercise with an effective captured bandwidth of 1.5 MHz and integration time of 1 s.

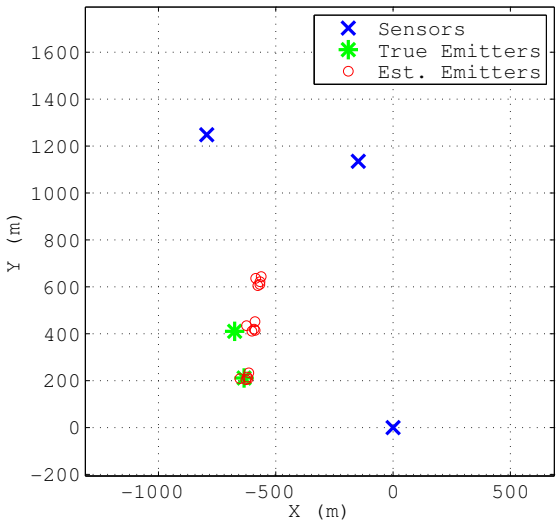


Figure 19: Estimated emitter locations for five independent runs with 1 s coherent integration.

estimation techniques are required for accurate emitter localization.

VII. Conclusions

A full picture, from theory to hardware implementation with field experiments, of a multiple-emitter localization system is offered. A novel multi-reference synchronization strategy based on a tightly-coupled sensor architecture is adopted. A focus on multiple emitters (as opposed to the single-emitter focus of prior work on interference localization) leads to a TDOA estimation strategy based on parametric estimation

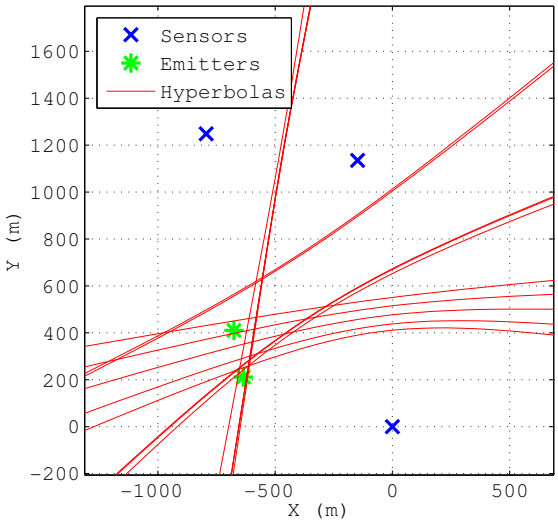


Figure 20: Hyperbolas generated by estimated TDOAs with the single-emitter assumption and an integration time of 1 s.

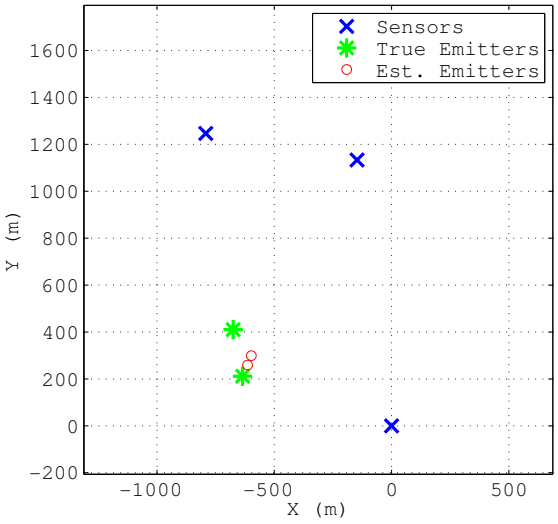


Figure 21: Estimated emitter locations with the single-emitter assumption and 1 s coherent integration.

techniques. The precision of the proposed TDOA estimator approaches the CRLB in a simulated representative scenario. Although the estimator becomes unreliable at low SNR_p or for closely-spaced emitters, it outperforms non-parametric matched-filtering-based techniques. Field tests show 20 m localization precision for five independent runs. Multipath is a significant challenge because it introduces false TDOA measurements that are consistent, leading to false emitter location estimates. Future work will configure the prototype system to detect and localize emitters in the GNSS bands, explore UAV-based platforms to mitigate multipath and allow feedback-based, adaptive sensor network geometries, and modify the processing algorithms to jointly estimate TDOA and FDOA in order to localize moving emitters.

Acknowledgment

This work was generously supported by Coherent Navigation through a sponsored research agreement. The authors also thank the members of the UT Radionavigation Laboratory.

References

[1] National PNT Advisory Board, "Jamming the Global Positioning System - A national security threat: Recent events and potential cures," Nov. 2010.

[2] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphrys, "Signal characteristics of civil GPS jammers," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.

[3] S. Pullen and G. Gao, "GNSS jamming in the name of privacy," *Inside GNSS*, vol. 7, Mar./Apr. 2012.

[4] Department of Homeland Security official. private communication, Sept. 2011.

[5] Federal Communications Commission, "Public Notice DA-05-1776," June 2005.

[6] T. E. Humphreys, "The GPS dot and its discontents: Privacy vs. GNSS integrity," *Inside GNSS*, vol. 7, Mar./Apr. 2012.

[7] B. Hamon and E. Hannan, "Spectral estimation of time delay for dispersive and non-dispersive systems," *Applied Statistics*, pp. 134–142, 1974.

[8] E. Hannan and P. Thomson, "Estimating group delay," *Biometrika*, vol. 60, no. 2, p. 241, 1973.

[9] C. Knapp and G. Carter, "The generalized correlation method for estimation of time delay," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 24, no. 4, pp. 320–327, 1976.

[10] A. Thompson, J. Moran, and G. Swenson, *Interferometry and Synthesis in Radio Astronomy*. Wiley, 2001.

[11] O. Isoz, A. T. Balaei, and D. Akos, "Interference detection and localization in the GPS L1 band," in *Proceedings of the ION ITM*, (San Diego, CA), pp. 925–929, Institute of Navigation, Jan. 2010.

[12] J. Lindstrom, D. M. Akos, O. Isoz, and M. Junered, "GNSS interference detection and localization using a network of low-cost front-end modules," in *Proceedings of the ION GNSS Meeting*, Institute of Navigation, 2007.

[13] K. G. Gromov, *GIDL: Generalized Interference Detection and Localization System*. PhD thesis, Stanford University, March 2002.

[14] M. B. Montminy, "Passive geolocation of low-power emitters in urban environments using TDOA," Master's thesis, Air Force Institute of Technology, Mar. 2007.

[15] R. Schmidt, "Multiple emitter location and signal parameter estimation," *Antennas and Propagation, IEEE Transactions on*, vol. 34, pp. 276 – 280, Mar. 1986.

[16] T. Sathyan, A. Sinha, and T. Kirubarajan, "Passive geolocation and tracking of an unknown number of emitters,"

Aerospace and Electronic Systems, IEEE Transactions on, vol. 42, pp. 740–750, April 2006.

[17] L. Scott, "J911: Fast Jammer Detection," *GPS World*, vol. 21, no. 11, pp. 32–37, 2010.

[18] A. Brown, D. Reynolds, D. Roberts, and S. Serie, "Jammer and interference location system," in *Proceedings of the ION GPS Meeting*, (Nashville, TN), pp. 137–142, Institute of Navigation, Sept. 1999.

[19] A. Proctor, C. Curry, J. Tong, R. Watson, M. Greaves, and P. Cruddace, "Protecting the UK infrastructure," *Inside GNSS*, vol. 6, Sep./Oct. 2011.

[20] K. Pesyna, Z. Kassas, J. Bhatti, and T. E. Humphreys, "Tightly-coupled opportunistic navigation for deep urban and indoor positioning," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.

[21] A. Rihaczek, *Principles of high-resolution radar*. McGraw-Hill, 1969.

[22] M. Psiaki and S. Mohiuddin, "Modeling, analysis, and simulation of GPS carrier phase for spacecraft relative navigation," *Journal of Guidance Control and Dynamics*, vol. 30, no. 6, p. 1628, 2007.

[23] K. M. Pesyna, Jr., K. Wesson, R. W. Heath, Jr., and T. E. Humphreys, "Extending the reach of GPS-assisted femtocell synchronization and localization through tightly-coupled opportunistic navigation," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011.

[24] K. Wesson, K. Pesyna, J. Bhatti, and T. E. Humphreys, "Opportunistic frequency stability transfer for extending the coherence time of GNSS receiver clocks," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2010.

[25] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and P. M. Kintner, Jr., "GNSS receiver implementation on a DSP: Status, challenges, and prospects," in *Proceedings of the ION GNSS Meeting*, (Fort Worth, TX), Institute of Navigation, 2006.

[26] B. W. O'Hanlon, M. L. Psiaki, P. M. Kintner, Jr., and T. E. Humphreys, "Development and field testing of a DSP-based dual-frequency software GPS receiver," in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), Institute of Navigation, 2009.

[27] T. E. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), Institute of Navigation, 2009.

[28] B. O'Hanlon, M. Psiaki, S. Powell, J. Bhatti, T. E. Humphreys, G. Crowley, and G. Bust, "CASES: A smart, compact GPS software receiver for space weather monitoring," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.

[29] A. Duel-Hallen, J. Holtzman, and Z. Zvonar, "Multiuser detection for CDMA systems," *Personal Communications, IEEE*, vol. 2, pp. 46–58, April 1995.

[30] P. Madhani, P. Axelrad, K. Krumvieda, and J. Thomas, "Application of successive interference cancellation to the GPS pseudolite near-far problem," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 39, pp. 481–488, April 2003.

[31] M. L. Psiaki, T. E. Humphreys, S. Mohiuddin, S. P. Powell, A. P. Cerruti, and J. Paul M. Kintner, "Searching for Galileo: Reception and analysis of signals from GIOVE-A," *GPS World*, vol. 17, pp. 66–72, June 2006.

[32] Y. Chan, R. Hattin, and J. Plant, "The least squares estimation of time delay and its use in signal detection," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 26, pp. 217–222, June 1978.

[33] W. Bajwa, K. Gedalyahu, and Y. Eldar, "Identification of parametric underspread linear systems and super-resolution radar," *Signal Processing, IEEE Transactions on*, vol. 59, pp. 2548 –2561, June 2011.

[34] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 37, pp. 984–995, July 1989.

[35] J.-J. Fuchs, "Estimating the number of sinusoids in additive white noise," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 36, pp. 1846–1853, Dec. 1988.

[36] A. Barabell, "Improving the resolution performance of eigenstructure-based direction-finding algorithms," in *Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '83.*, vol. 8, pp. 336–339, April 1983.

[37] B. Rao and K. Hari, "Performance analysis of root-music," *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 37, pp. 1939–1949, Dec. 1989.

[38] Y. Chan and K. Ho, "A simple and efficient estimator for hyperbolic location," *Signal Processing, IEEE Transactions on*, vol. 42, pp. 1905–1915, Aug. 1994.