Sensor Deception Detection and Radio-Frequency Emitter Localization

Jahshan Bhatti

Department of Aerospace Engineering
The University of Texas at Austin

August 19, 2015

Table of Contents

Secure Control of Autonomous Systems

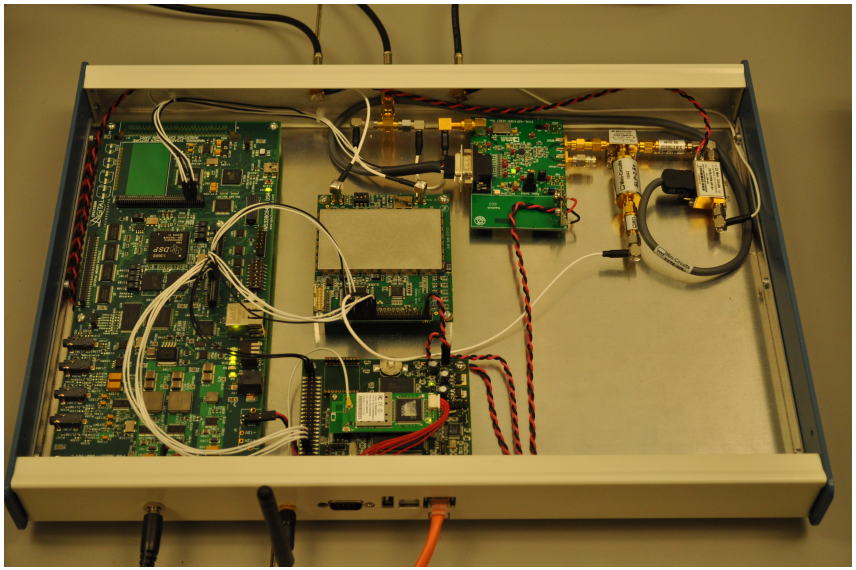
Security researcher Charlie Miller attempts to extract a Jeep Cherokee from a ditch after its brakes were remotely disabled by a cyber attack in a controlled test (Andy Greenberg/Wired).

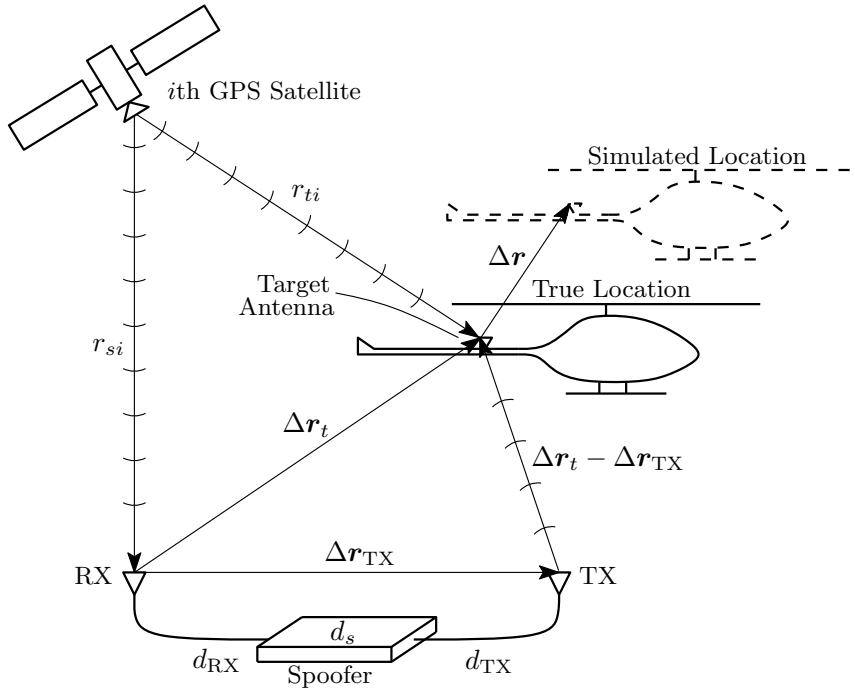
Secure Control of Autonomous Systems

Security researcher Jahshan Bhatti examines the wreckage of an autonomous helicopter after its GPS receiver was captured and manipulated by a field attack in a slightly less-controlled test.

What are Field Attacks?

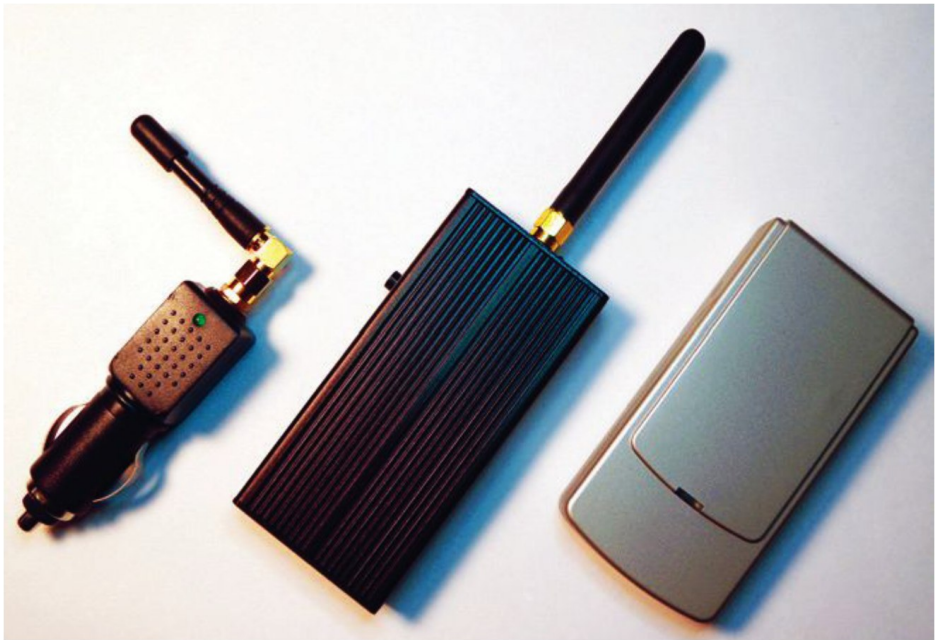
GPS Spoofing

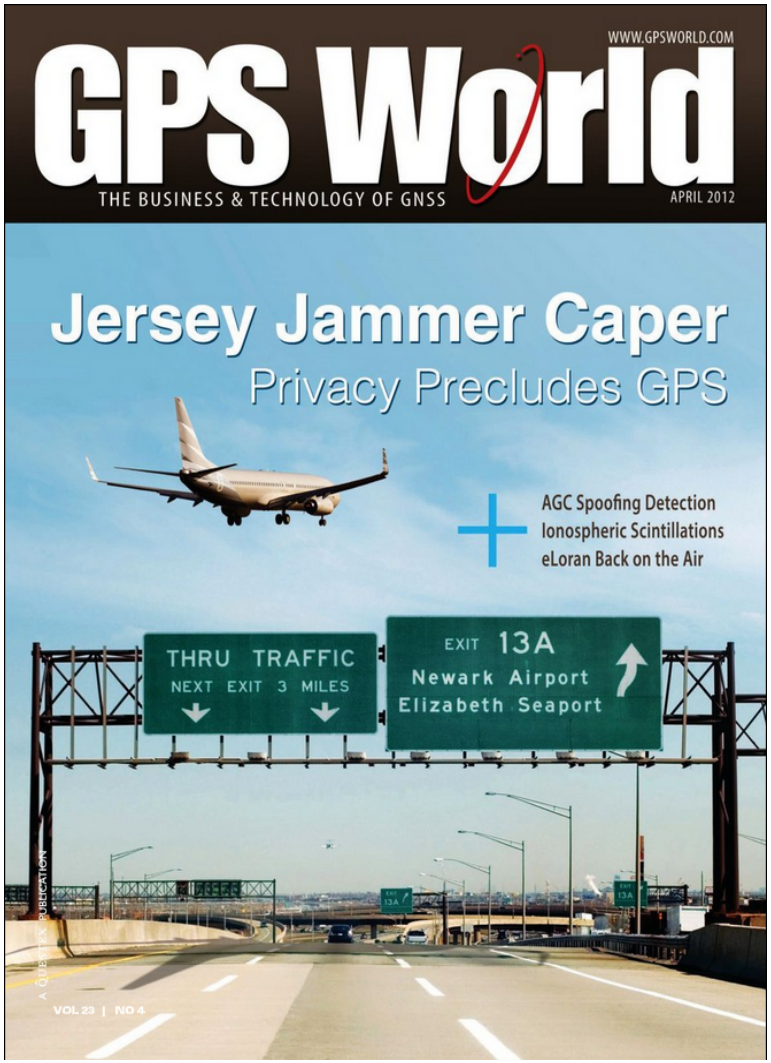




- GPS spoofing has been demonstrated against
  - (i) an autonomous helicopter,
  - (ii) a phasor measurement unit, and
  - (iii) a 65-meter superyacht.

GPS Jamming




WWW.GPSWORLD.COM
GPS World
THE BUSINESS & TECHNOLOGY OF GNSS
APRIL 2012
Jersey Jammer Caper
Privacy Precludes GPS
AGC Spoofing Detection
Ionospheric Scintillations
eLoran Back on the Air
THRU TRAFFIC
NEXT EXIT 3 MILES
EXIT 13A
Newark Airport
Elizabeth Seaport
VOL 23 | NO 4

Published Works (Journal) I

1. K. B. Deshpande, G. S. Bust, C. R. Clauer, H. Kim, J. E. Macon, T. E. Humphreys, J. A. Bhatti, S. B. Musko, G. Crowley, and A. T. Weatherwax, "Initial GPS scintillation results from CASES receiver at South Pole, Antarctica," *Radio Science*, vol. 47, no. 5, 2012
2. C. R. Clauer, H. Kim, K. Deshpande, Z. Xu, D. Weimer, S. Musko, G. Crowley, C. Fish, R. Nealy, T. E. Humphreys, J. A. Bhatti, and A. J. Ridley, "Autonomous adaptive low-power instrument platform (AAL-PIP) for remote high latitude geospace data collection," *Geoscientific Instrumentation, Methods and Data Systems*, vol. 3, pp. 211–227, 2014
3. E. G. Lightsey, T. E. Humphreys, J. A. Bhatti, A. J. Joplin, B. W. O'Hanlon, and S. P. Powell, "Demonstration of a space capable miniature dual frequency GNSS receiver," *Navigation, Journal of the Institute of Navigation*, vol. 61, no. 1, pp. 53–64, 2014

Published Works (Journal) II

4. M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013
5. B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, J. A. Bhatti, and D. P. Shepard, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation, Journal of the Institute of Navigation*, vol. 60, no. 4, pp. 267–278, 2013
6. A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014

Published Works (Journal) III

7. J. Bhatti and T. Humphreys, "Covert control of surface vessels via GPS spoofing," *Navigation, Journal of the Institute of Navigation*, 2015, (In preparation.)
8. J. Bhatti, B. Ledvina, and T. Humphreys, "Analysis and experimental results of direct geolocation techniques," *Navigation, Journal of the Institute of Navigation*, 2015, (In preparation.)

Published Works (Selected Conference)

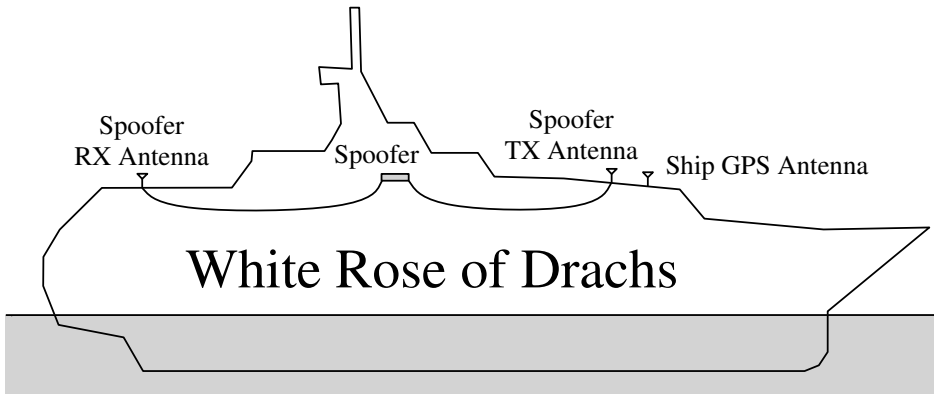
1. T. E. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proceedings of the ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2009, pp. 326–338
2. J. A. Bhatti, T. E. Humphreys, and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Proceedings of the IEEE/ION PLANS Meeting*, April 2012, pp. 1209–1220

Dissertation Contributions

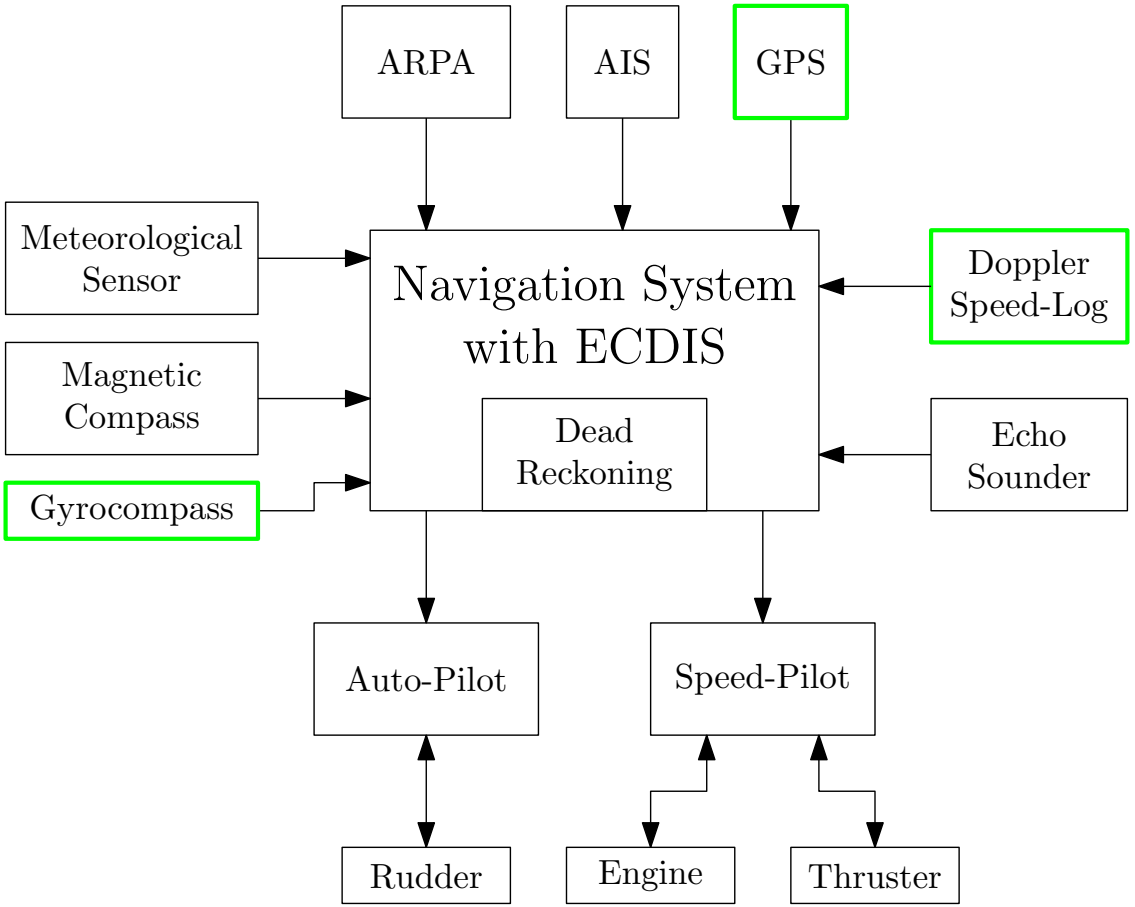
- The underlying theme of this dissertation is the detection and localization of GNSS-based field attacks.
- To that end, this dissertation makes two primary contributions:
  1. a novel GNSS deception detection technique that operates at the sensor fusion level, and
  2. estimation algorithms using Monte-Carlo sampling methods for direct geolocation of radio-frequency emitters.

Table of Contents

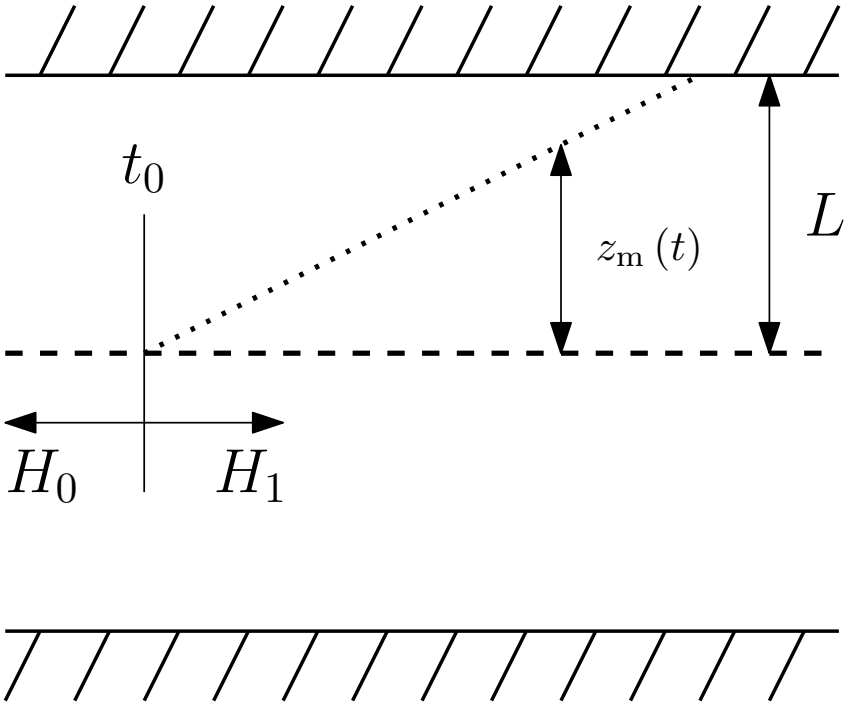
GPS Spoofing Against a Maritime Surface Vessel



Modern Integrated Bridge System

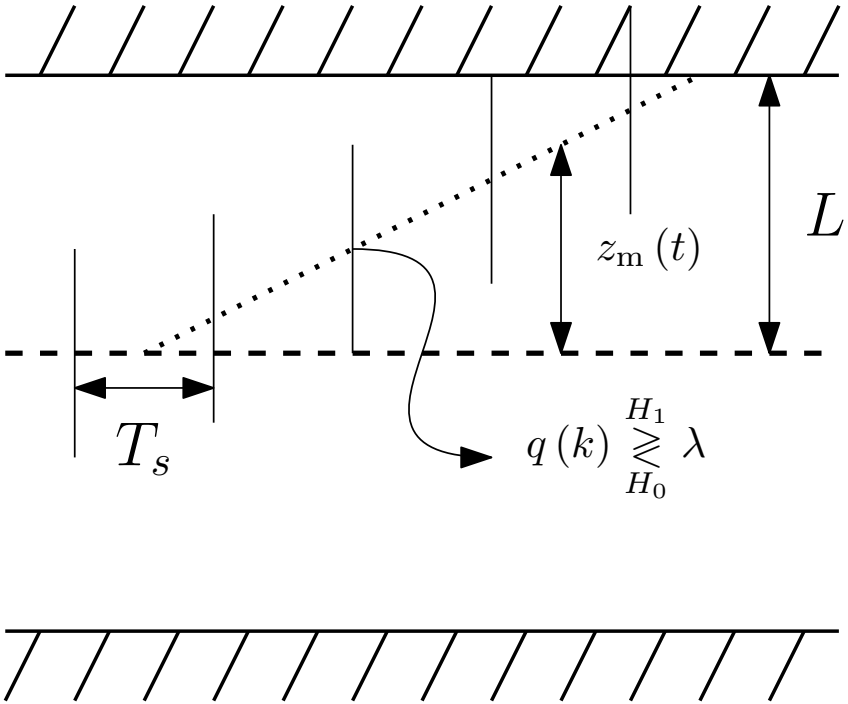


Detection Problem



- What is the optimal detection test for fixed time-to-detect
  - if t_0 and $z_{\mathrm{m}}(t)$ are known?
  - if only $z_{\mathrm{m}}(t)$ is known?
  - if only t_0 is known?

Detection Problem



- What are near-optimal detection procedures for unknown t_0 and $z_{\mathrm{m}}(t)$? (Willsky, 1976)
- What detection procedures take into account integrity risk? (Joerger and Pervan, 2013; Khanafseh et al., 2014)

Integrity Risk

- A hazardously misleading information (HMI) event is defined as

$$E = \bigvee_{t \geq t_0} \left(\|z_{\mathrm{m}}(t)\| > L \wedge \left(\bigwedge_{t_0 < kT_s < t} q(k) < \lambda \right) \right)$$
$$= \bigwedge_{t_0 < kT_s \leq t_L} q(k) < \lambda,$$

  where

  - $q(k)$ is a test statistic that monitors the presence of spoofing,
  - t_0 is the start time of the spoofing attack, and
  - t_L is the first time hazardous conditions are encountered.

- The mean integrity risk of the detection framework is given by

$$I_R = \int_0^1 P(E|t_0 = \beta T_s)\, d\beta.$$

Framework Optimization

- The optimal sampling time $T_s^\star$ minimizes the worst-case integrity risk $I_R^\star$.
- $T_s^\star$ and $I_R^\star$ are the solution to the optimization problem given by

$$\begin{aligned} \min_{T_s} \max_{v_{\max}} \quad & I_R \\ \text{s.t.} \quad & a \leq v_{\max} \leq b \end{aligned}$$

Ship Dynamics Model

The continuous-time ship dynamics model is given by

$$\dot{\eta}(t) = A\eta(t) + Bu(t) + E\tilde{v}(t),$$

where

$$\eta = \begin{bmatrix} x & y & d_x & d_y \end{bmatrix}^{\mathrm{T}} \text{ is the state vector,}$$

$$A = \begin{bmatrix} 0 & I \\ 0 & -\frac{1}{T_d} I \end{bmatrix}, \; B = \begin{bmatrix} I \\ 0 \end{bmatrix}, \; E = \begin{bmatrix} 0 \\ I \end{bmatrix},$$

$$u = U \begin{bmatrix} \sin\psi & \cos\psi \end{bmatrix}^{\mathrm{T}} \text{ is the control, and}$$

$$\tilde{v} = \begin{bmatrix} v_x & v_y \end{bmatrix}^{\mathrm{T}} \text{ is AWGN with intensity } Q_c = \sigma_d^2 I.$$

GPS Measurement Model

The GPS measurement model for sampling time T_s is given by

$$z(k) = H\eta(kT_s) - z_{\mathrm{m}}(kT_s) + w(k),$$

where

$$\begin{aligned} z_{\mathrm{m}}(t) &\text{ is the spoofer-induced modulation,} \\ H &= \begin{bmatrix} I & 0 \end{bmatrix}, \\ w(k) &\sim \mathcal{N}(0, R), \text{ and} \\ R &= \sigma_p^2 I. \end{aligned}$$

Estimation Error

- The optimal sequential estimator for the system model under deception-free conditions (i.e. $\forall t \;\; z_{\mathrm{m}}(t) = 0$) is the Kalman filter.
- The *a posteriori* estimation error and innovation are defined as

$$\hat{\epsilon}(k) \triangleq \eta(kT_s) - \hat{\eta}(k)$$
$$\nu(k) \triangleq z(k) - H\bar{\eta}(k).$$

- The expected value of the estimation error and innovation are given by (in steady state)

$$\mathbb{E}[\hat{\epsilon}(k)] = (I - KH)F\mathbb{E}[\hat{\epsilon}(k)] - Kz_{\mathrm{m}}(kT_s)$$
$$\mathbb{E}[\nu(k)] = HF\mathbb{E}[\hat{\epsilon}(k)] - z_{\mathrm{m}}(kT_s),$$

  where $F = e^{AT_s}$ and K is the Kalman gain.
- The estimation error and innovation are clearly biased under a spoofing attack.

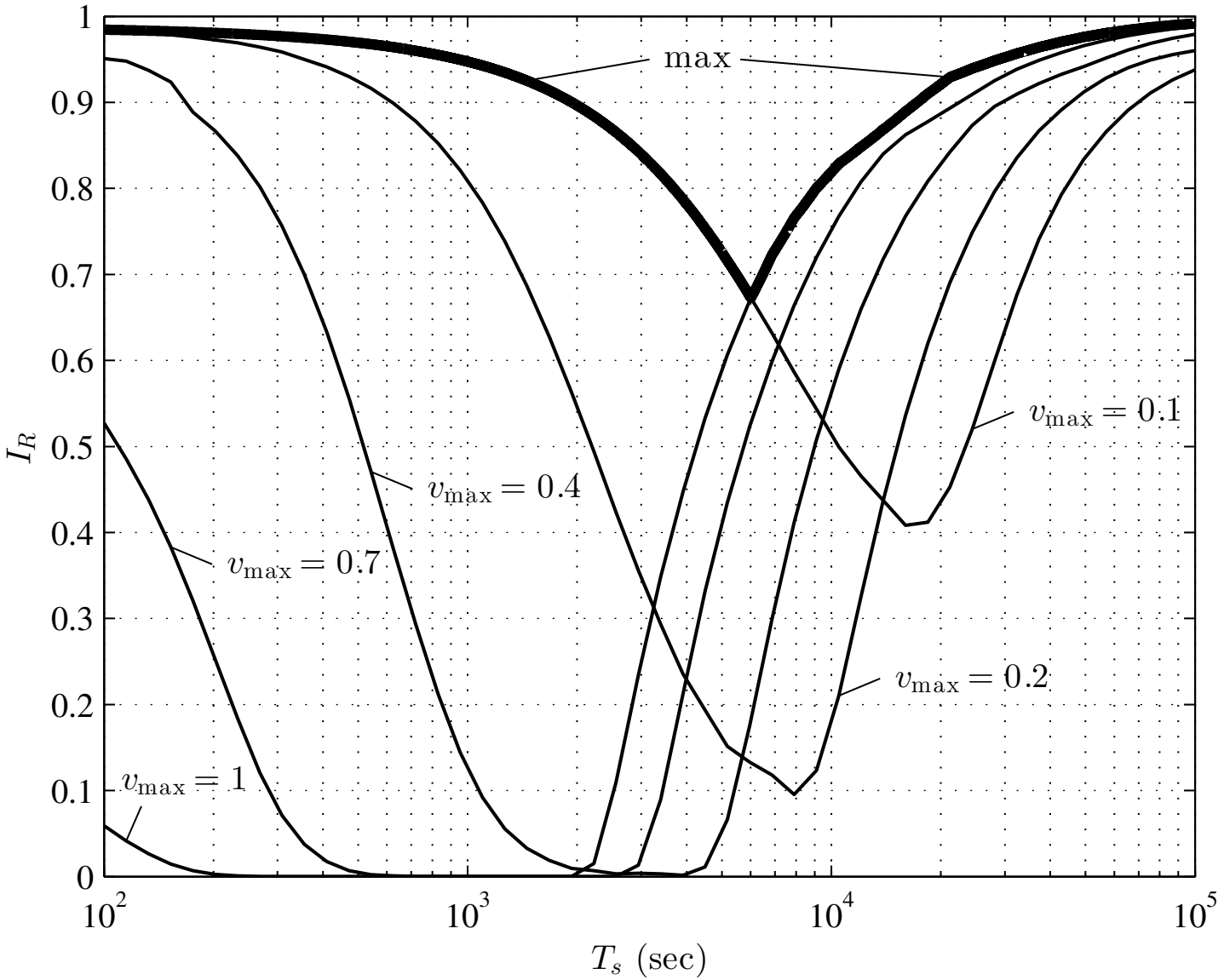
Detection Statistic

- For an arbitrary spoofing profile, the optimal statistic (for a generalized likelihood ratio test) has the form

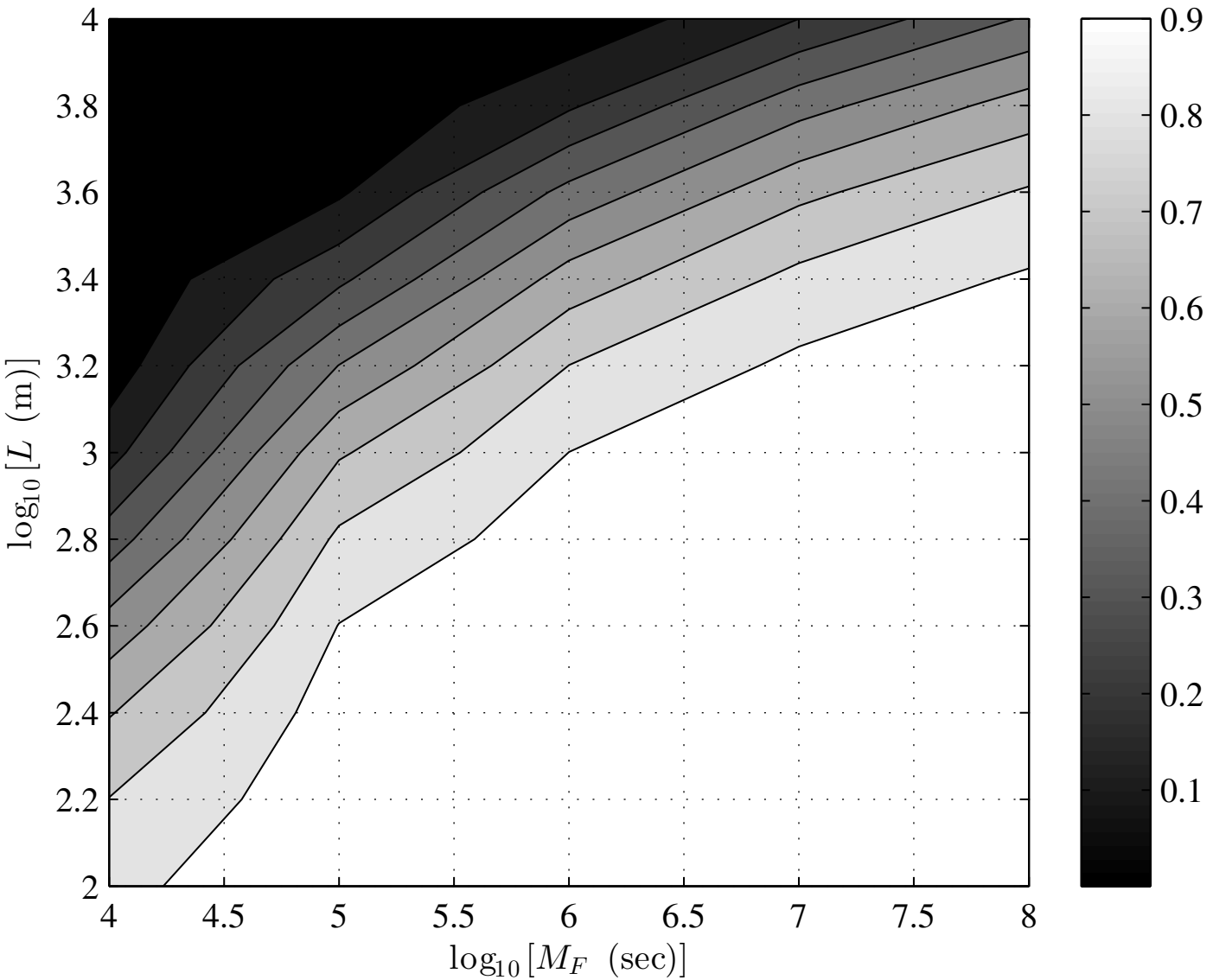
$$q(k) = \nu(k)^T S^{-1} \nu(k) \sim \chi^2 \left(n_z, \mathbb{E}[\nu(k)]^T S^{-1} \mathbb{E}[\nu(k)] \right),$$

  and is typically used for innovations-based fault detection.
- No claims of optimality of the normalized innovation squared (NIS) detection statistic with respect to the current framework are made.

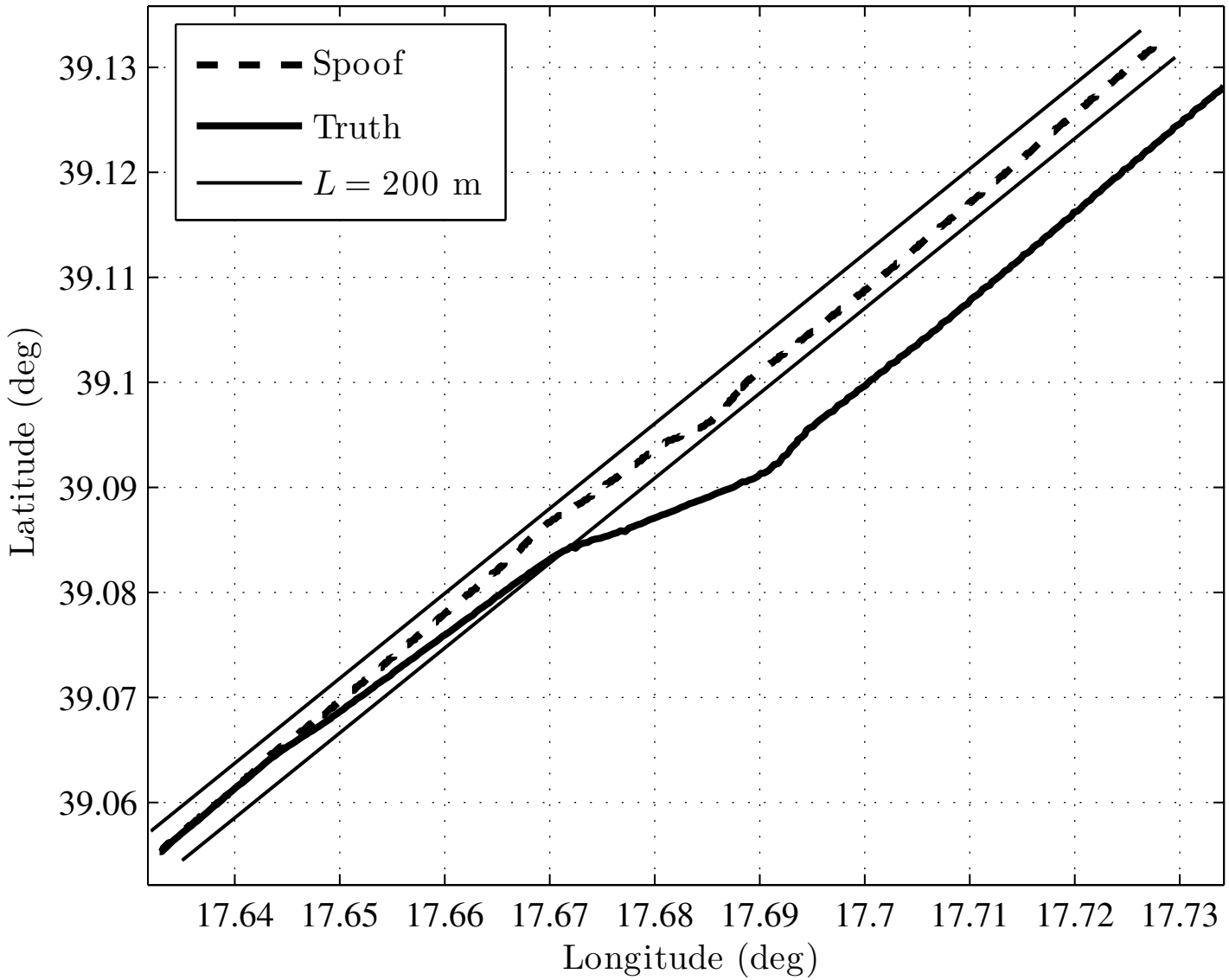
Integrity risk I_R vs. sampling time T_s



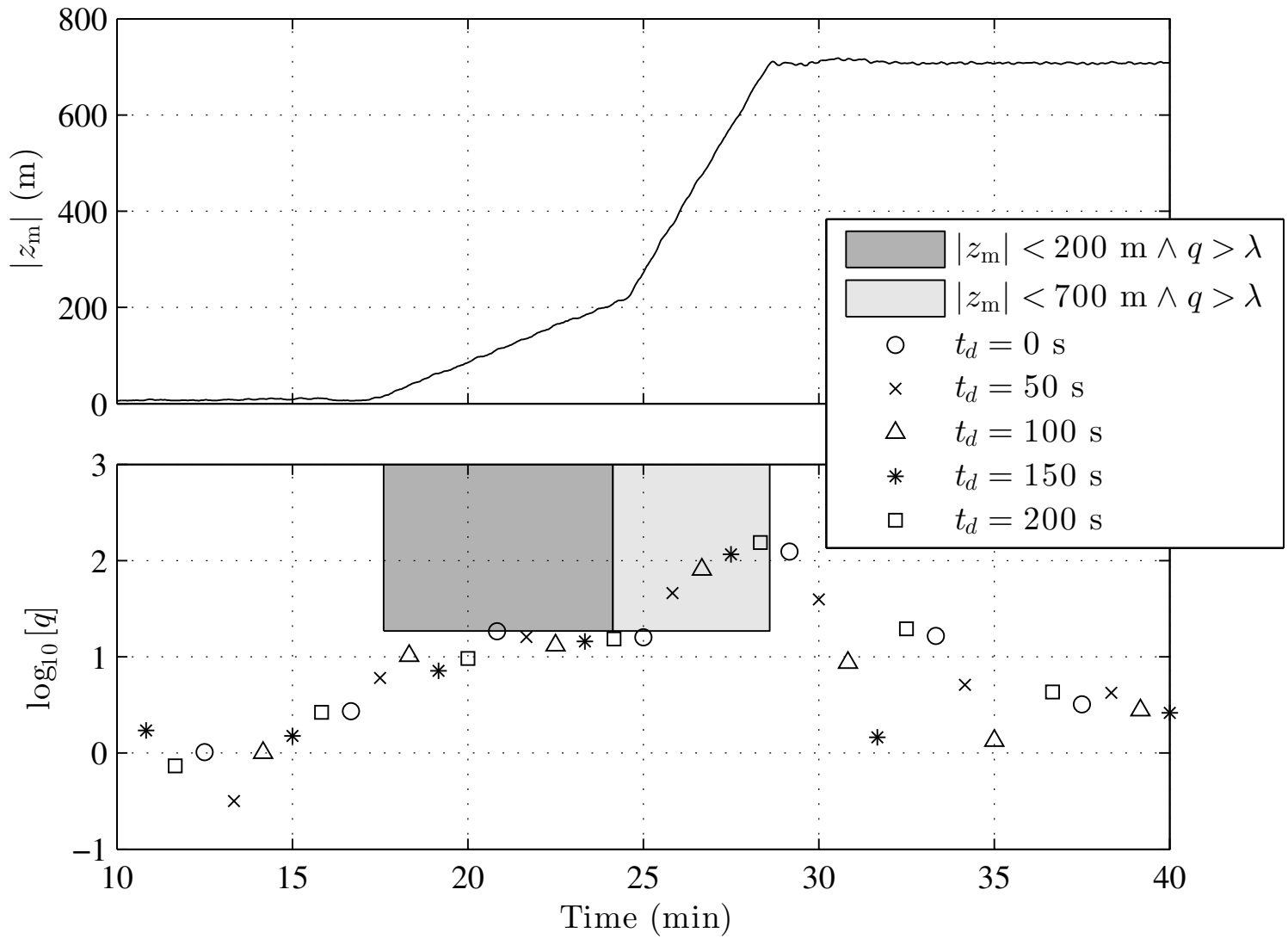
Minimax integrity risk $I_R^\star$ vs. L and M_F



Experimental Results



NIS Time History for $T_s = 250$ s



Open Questions

- Some open questions remain:
  - Can the framework be applied to an inertial measurement unit or clock model, which both have drift parameters governed by Gauss-Markov processes?
  - Can the integrity risk optimization problem be recast so that the detection statistic and attack profile are free parameters?

Table of Contents

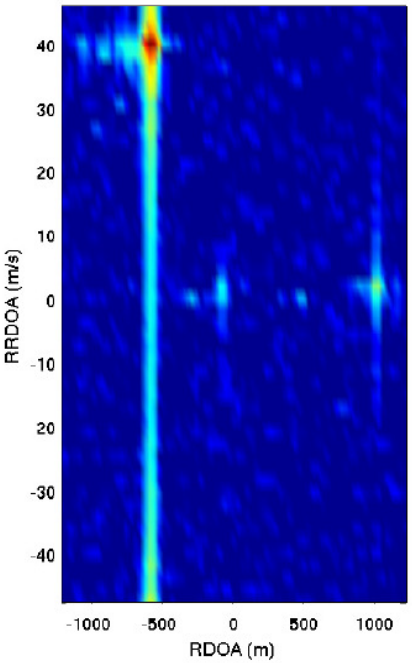
Table : Strengths and weaknesses of different measurement types.

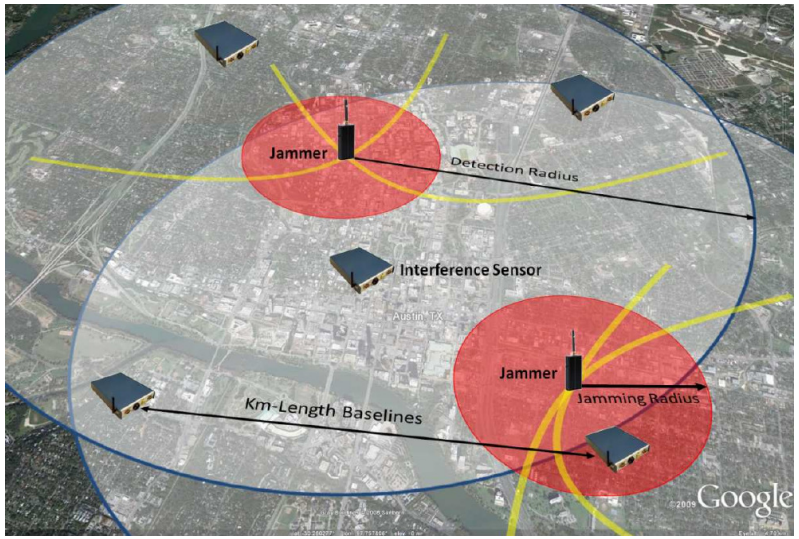
	RSS	AOA	T/FDOA
Antenna and RX complexity	Low	High	Medium
Localization accuracy	Low	Medium	High
Time synchronization	ms	ms	ns
Network throughput	Low	Low	High

Two-Step Emitter Geolocation

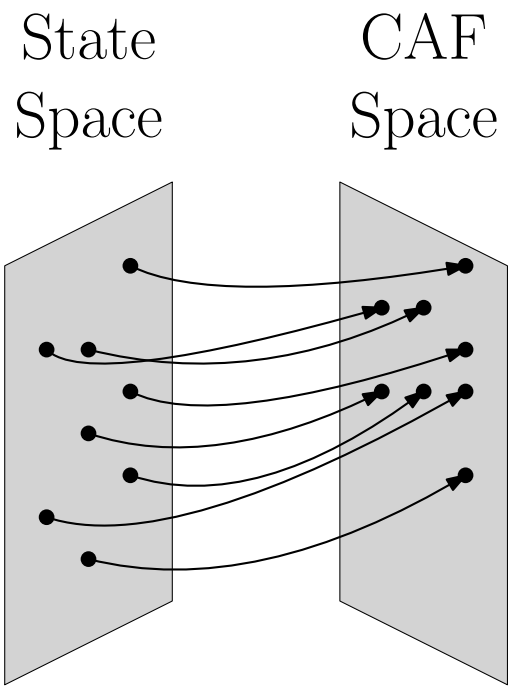
- Traditional two-step geolocation approach (Stein, 1981).

Raw Data → CAF → T/FDOA → Geolocation





Direct Emitter Geolocation



(Sidi and Weiss, 2014)

- The dissertation extends the prior art in the following ways:
  - Theory
    - Relaxed constant Doppler assumption.
    - Developed hybrid Monte-Carlo sampling Kalman filter.
    - Used path-constrained dynamic models.
  - Practice
    - Conducted three experiments.
    - Elucidated important implementation details.
    - Used CDGNSS to extend coherent integration time.

Emitter Dynamics Model

Table : Description of three different types of emitter dynamics models.

Type	State Space	Time History
NS	$\eta = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$	$x(t) = x_0$ $y(t) = y_0$
NCV	$\eta = \begin{bmatrix} x_0 \\ \dot{x} \\ y_0 \\ \dot{y} \end{bmatrix}$	$x(t) = x_0 + \dot{x}t$ $y(t) = y_0 + \dot{y}t$
NCVP	$\eta = \begin{bmatrix} s_0 \\ \dot{s} \end{bmatrix}$	$x(t) = T_x(s_0 + \dot{s}t)$ $y(t) = T_y(s_0 + \dot{s}t)$

Emitter Dynamics Model

Table : Description of three different types of emitter dynamics models.

Type	Update	Matrix Definitions
NS	$\eta(k+1) = F_0\eta(k) + v(k)$ $v(k) \sim \mathcal{N}(0, Q_0)$	$F_0 = I_{2\times 2}$ $Q_0 = q_0 I_{2\times 2} T$
NCV	$\eta(k+1) = F_1\eta(k) + v(k)$ $v(k) \sim \mathcal{N}(0, Q_1)$	$F_1 = \begin{bmatrix} F_2 & 0 \\ 0 & F_2 \end{bmatrix}$ $Q_1 = q_1 \begin{bmatrix} Q_{cv} & 0 \\ 0 & Q_{cv} \end{bmatrix}$
NCVP	$\eta(k+1) = F_2\eta(k) + v(k)$ $v(k) \sim \mathcal{N}(0, Q_2)$	$F_2 = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}$ $Q_2 = q_2 Q_{cv}$ $Q_{cv} = \begin{bmatrix} \frac{1}{3}T^3 & \frac{1}{2}T^2 \\ \frac{1}{2}T^2 & T \end{bmatrix}$

Likelihood Function

- Consider the simplified signal model for the ith receiver

$$r_i = \alpha_i H_i(\eta)\, s + n_i,$$

where s and $n_i \sim \mathcal{CN}\left(0, \sigma_n^2 I\right)$ are the complex baseband emitter signal and noise vectors, respectively, α_i is the complex path attenuation, and $H_i(\eta)$ is a complex matrix that time and phase shifts the signal vector.

- The likelihood function is given by

$$L''(\eta, s, \alpha | z) \propto \exp\left(-\frac{1}{\sigma_n^2} \sum_{i=1}^{N_r} \|r_i - \alpha_i H_i(\eta)\, s\|^2\right).$$

Likelihood Function

- In passive geolocation, α and s are nuisance parameters. A reasonable approach is to replace them with their maximum likelihood estimates as in (Sidi and Weiss, 2014), i.e.

$$L\left(\eta|z\right) = \max_{s,\alpha} L''\left(\eta, s, \alpha|z\right).$$

- After some algebra,

$$L\left(\eta|z\right) \propto \exp\left(\frac{1}{\sigma_n^2}\lambda_{\max}\left(\bar{D}\left(z,\eta\right)\right)\right),$$

where

$$\bar{D}_{i,j}\left(z,\eta\right) = r_i^{\mathrm{H}} H_i\left(\eta\right) H_j^{\mathrm{H}}\left(\eta\right) r_j.$$

Generalized Cross-Correlation Function

- Recall the familiar cross-correlated complex ambiguity function (CAF)

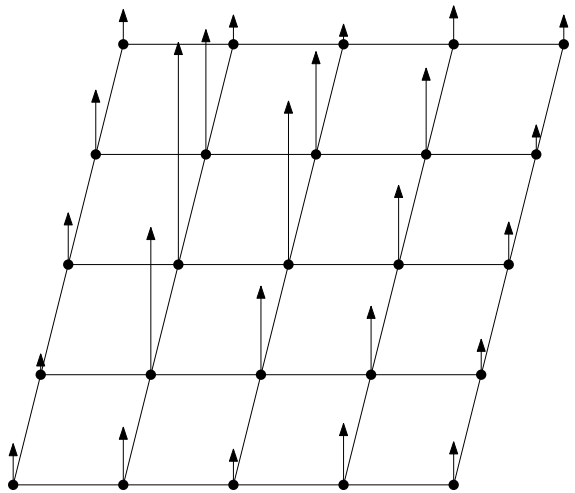
$$S'\left(\tilde{z}_1\left(t\right),\tilde{z}_2\left(t\right),\tau_0,f_D\right)\triangleq\int_0^T\tilde{z}_1\left(t\right)\tilde{z}_2^{\star}\left(t+\tau_0\right)e^{-j2\pi f_D t}dt,$$

  where τ_0 is a constant delay and f_D is the Doppler frequency.
- Now, consider the GCCF for signals $\tilde{z}_1\left(t\right)$ and $\tilde{z}_2\left(t\right)$

$$S\left(\tilde{z}_1\left(t\right),\tilde{z}_2\left(t\right),\tau_1\left(t\right),\tau_2\left(t\right)\right)\triangleq$$
$$\int_0^T\tilde{z}_1\left(t+\tau_1\left(t\right)\right)\tilde{z}_2^{\star}\left(t+\tau_2\left(t\right)\right)e^{j2\pi f_c[\tau_1(t)-\tau_2(t)]}dt,$$

  where $\tau_i\left(t\right)$ is the delay time history for received signal $i\in\{1,2\}$ and T is the length of the integration interval.

Grid Search

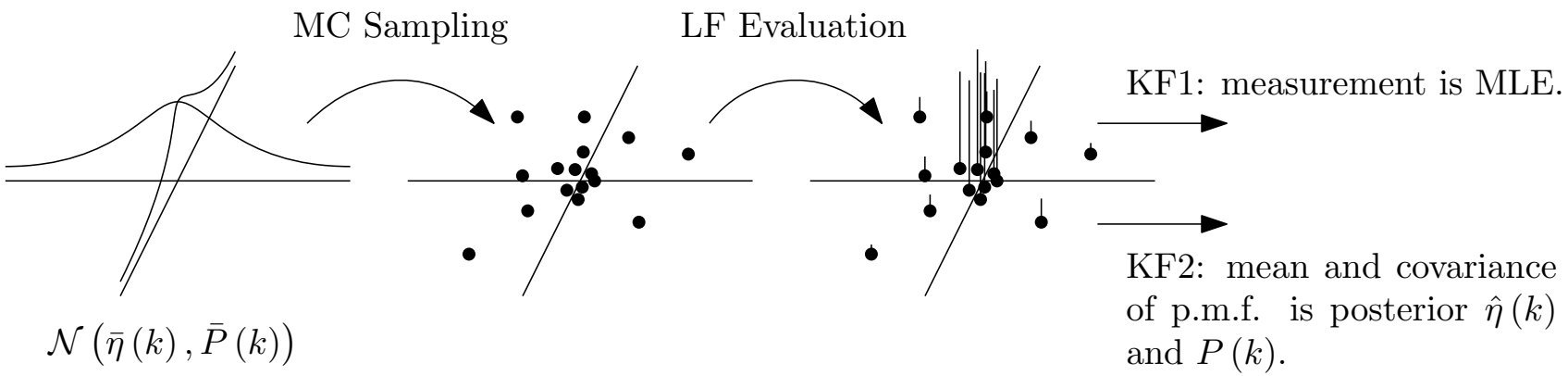


(Weiss, 2011)

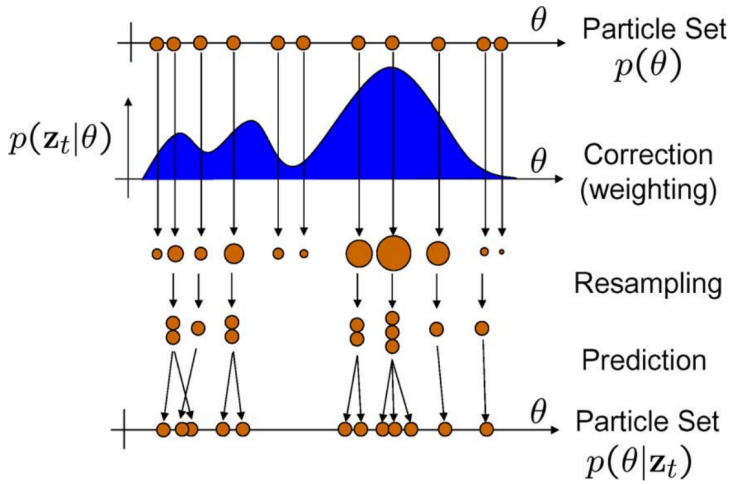
- Naive grid search is appropriate for the 2-D NS model; however,
  - the state space is evaluated inefficiently with a fixed grid,
  - the search space can become unwieldy for the 4-D NCV model, and
  - the dynamical constraint between position and velocity over time in both the NCV and NCVP model is not enforced.

Hybrid Kalman Filter with Monte-Carlo Sampling

- A Kalman filter approach has two advantages over GS:
  - KF allows smoothing the measurement information with the dynamical constraints, and
  - *a priori* emitter state and covariance can be used constrain the search space to a smaller region.
- Hybrid measurement sampling approach:



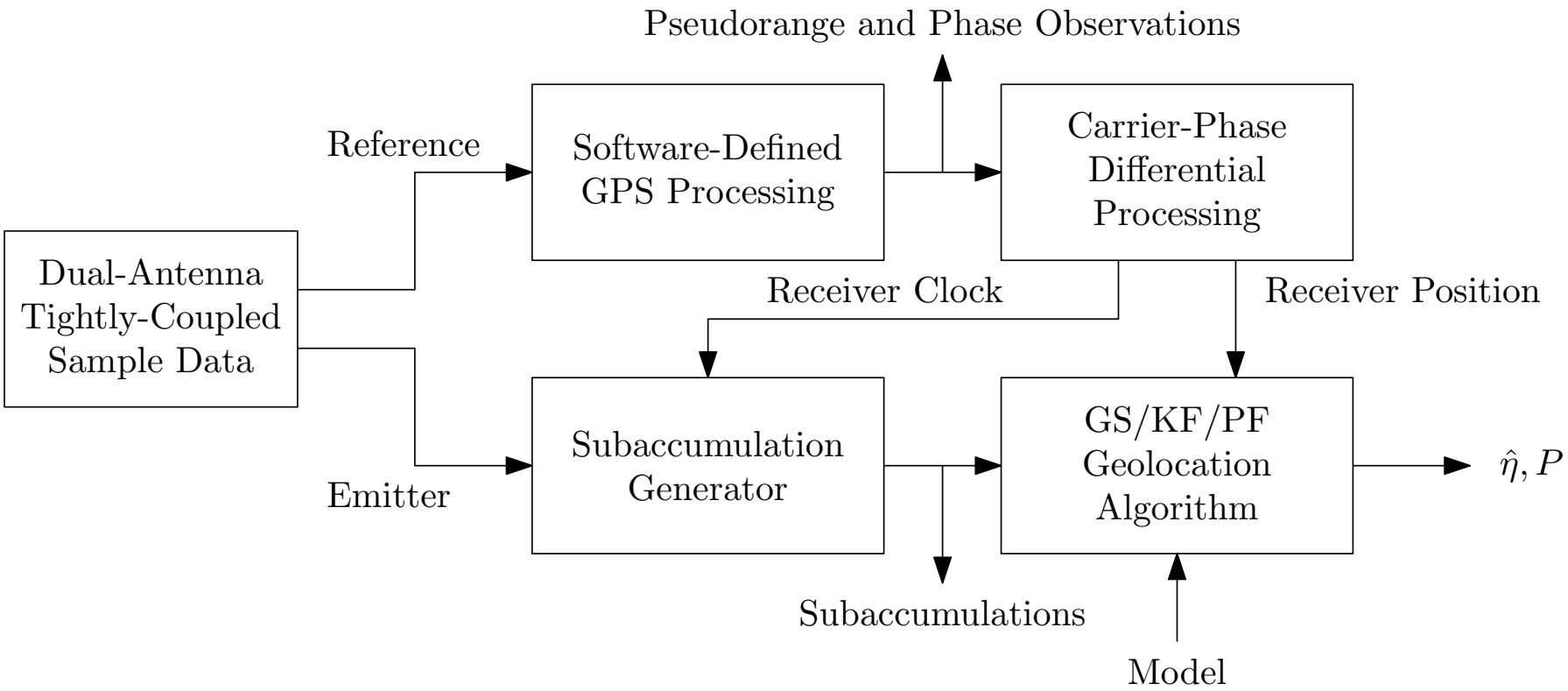
Particle Filter



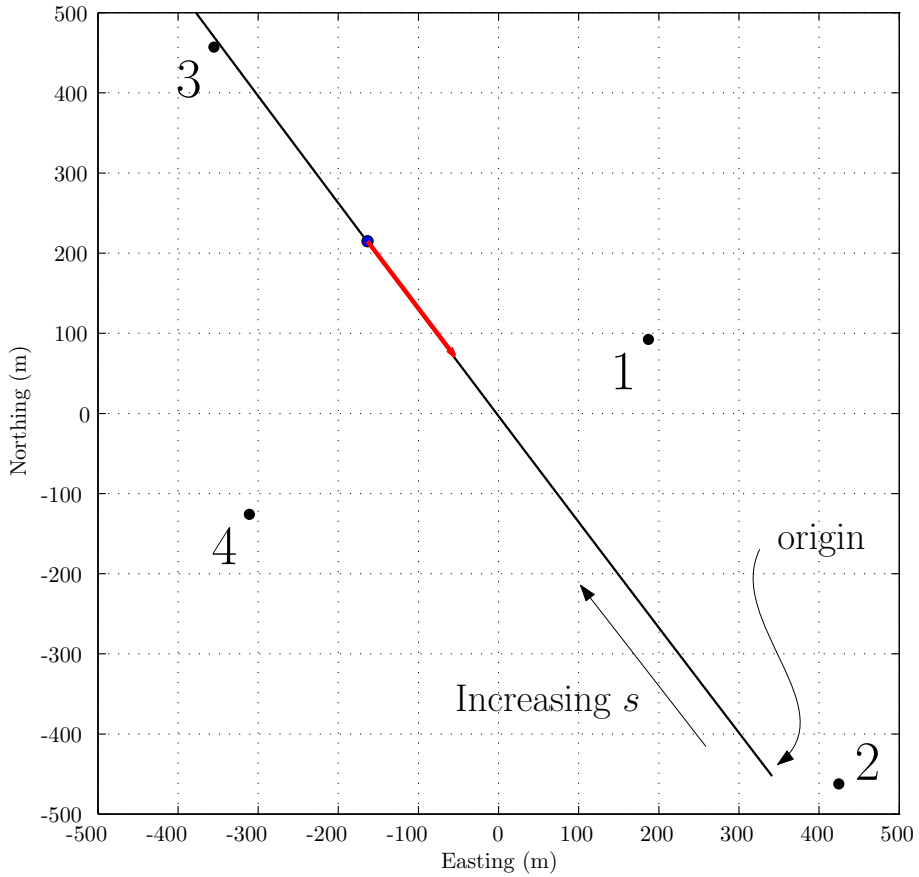
(Gordon et al., 1993)

- The PF provides the same improvements over GS as KF, but has two advantages over KF:
  - no initial guess required, so that a uniform sampling over state space can be used, and
  - can propagate non-Gaussian pdf for emitter state, which can help prevent divergence due to transient multipath.

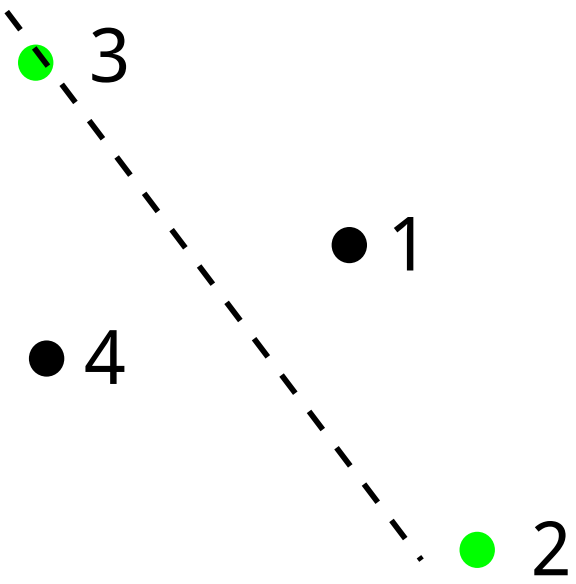
Emitter Localization Post-Processing Workflow

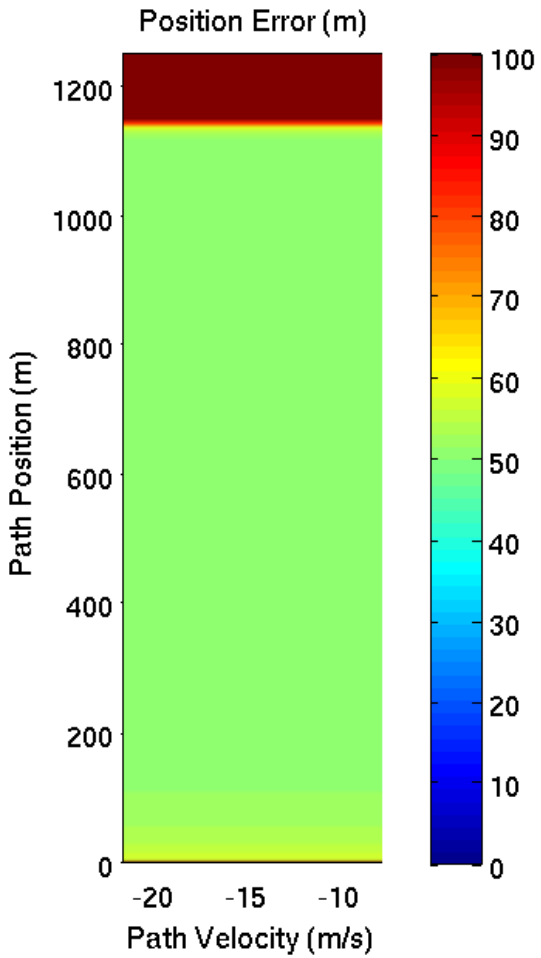


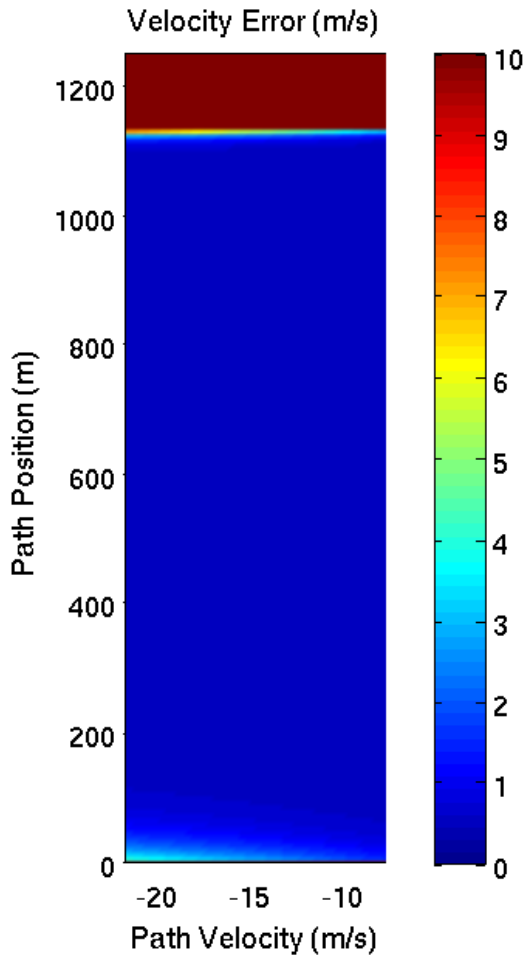
White Sands Missile Range Experiment



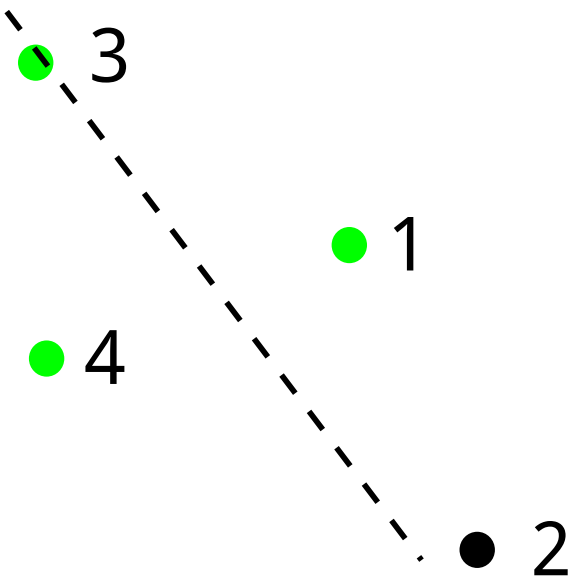
Two-Receiver NCVP Estimability

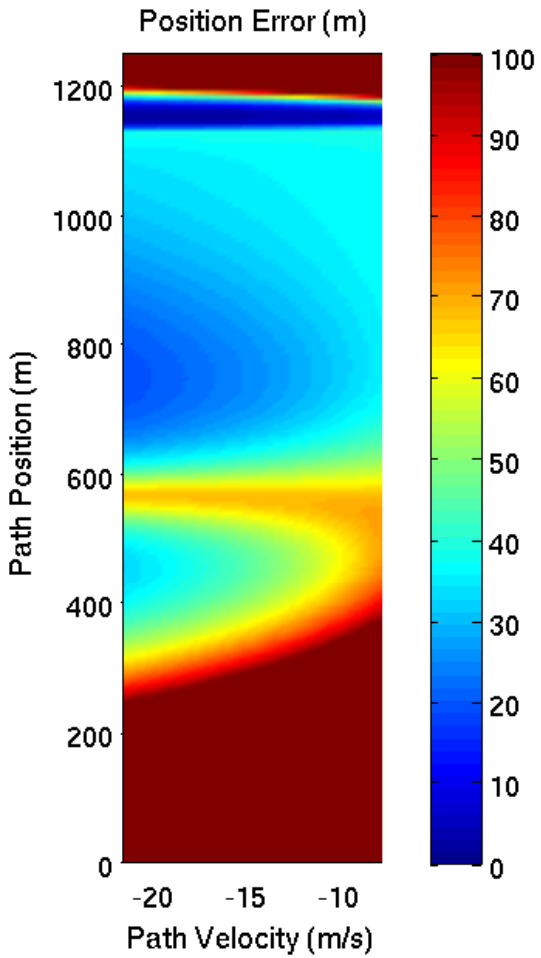


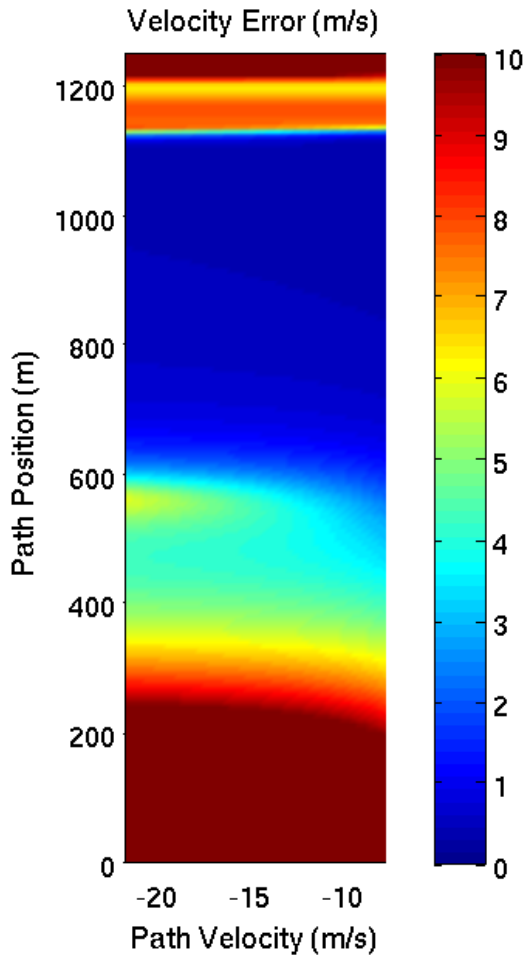




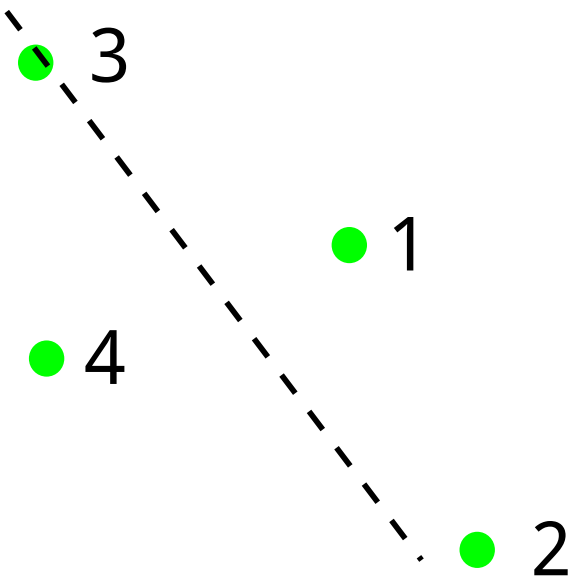
Three-Receiver NCVP Estimability

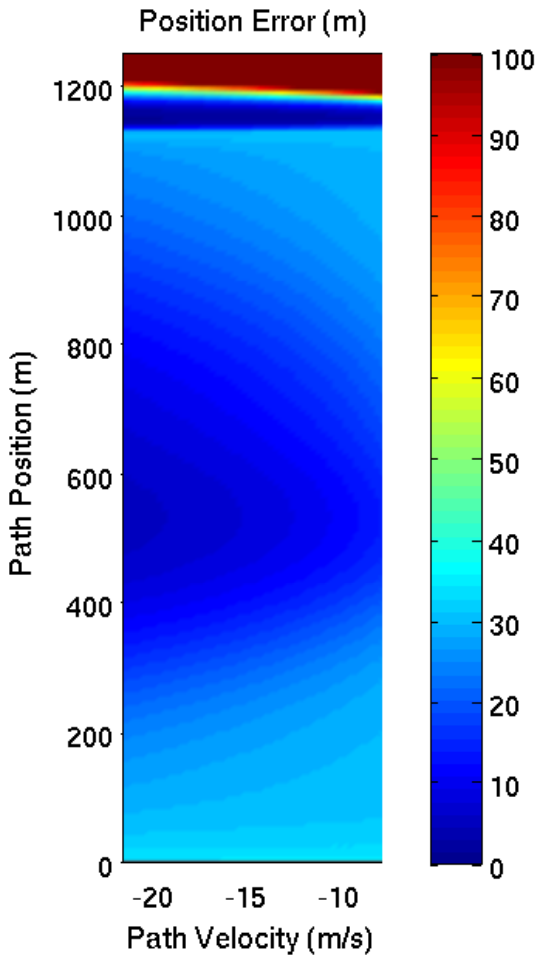


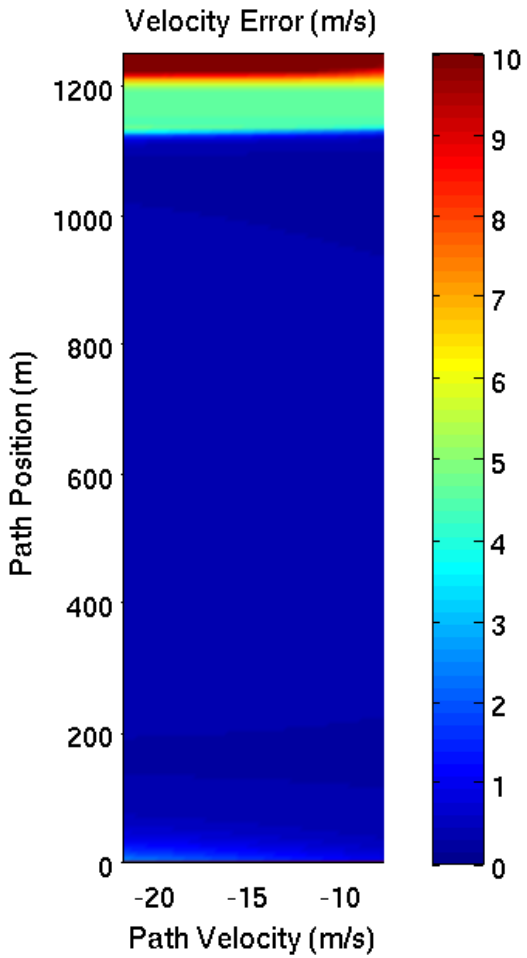




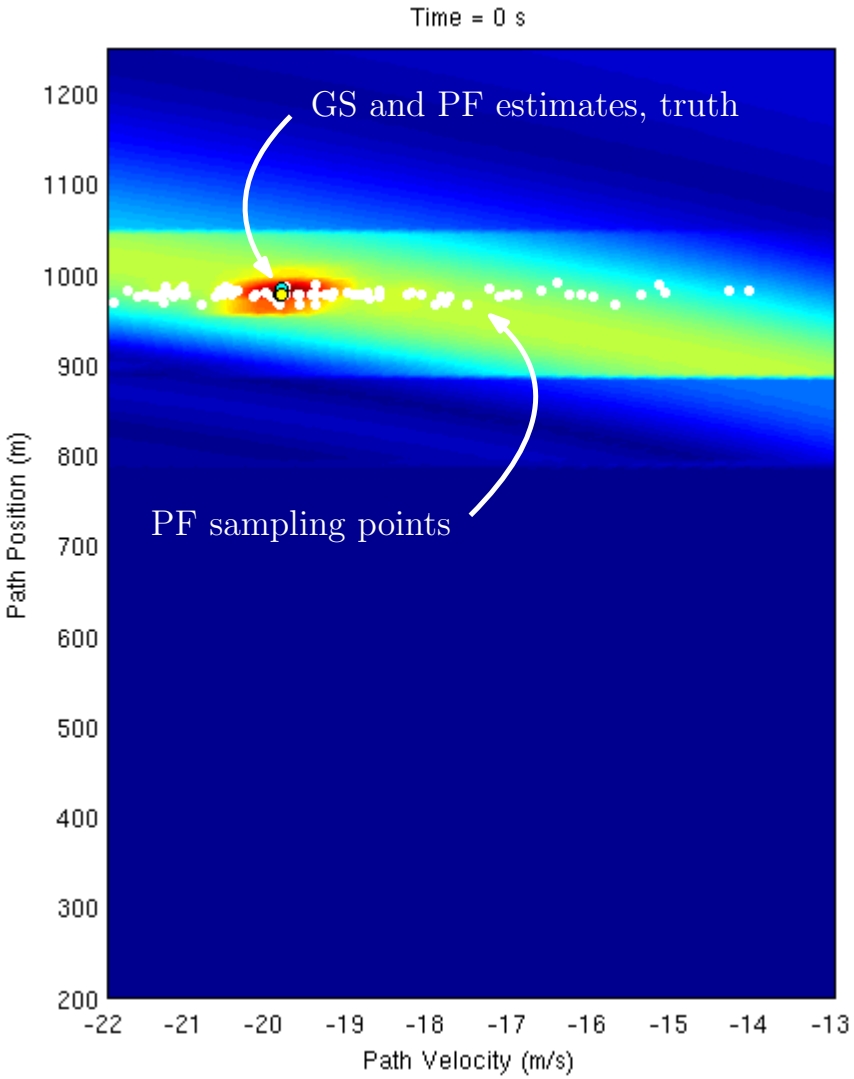
Four-Receiver NCVP Estimability

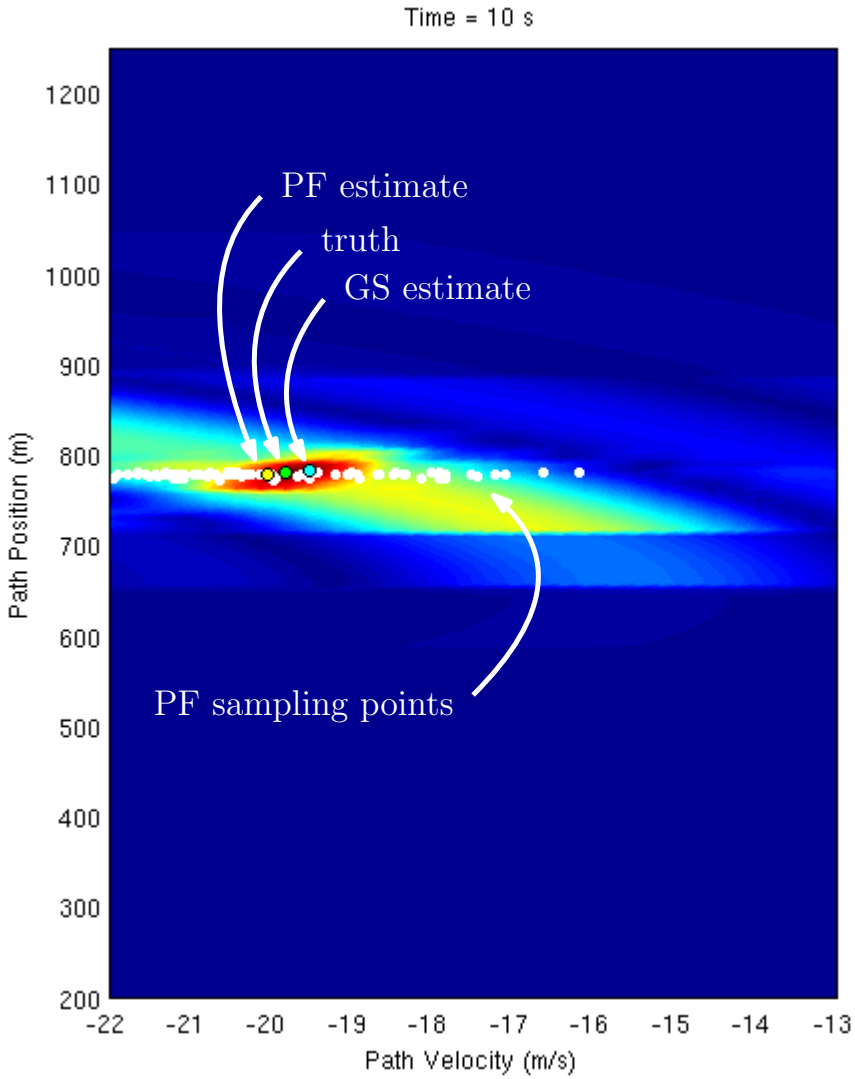




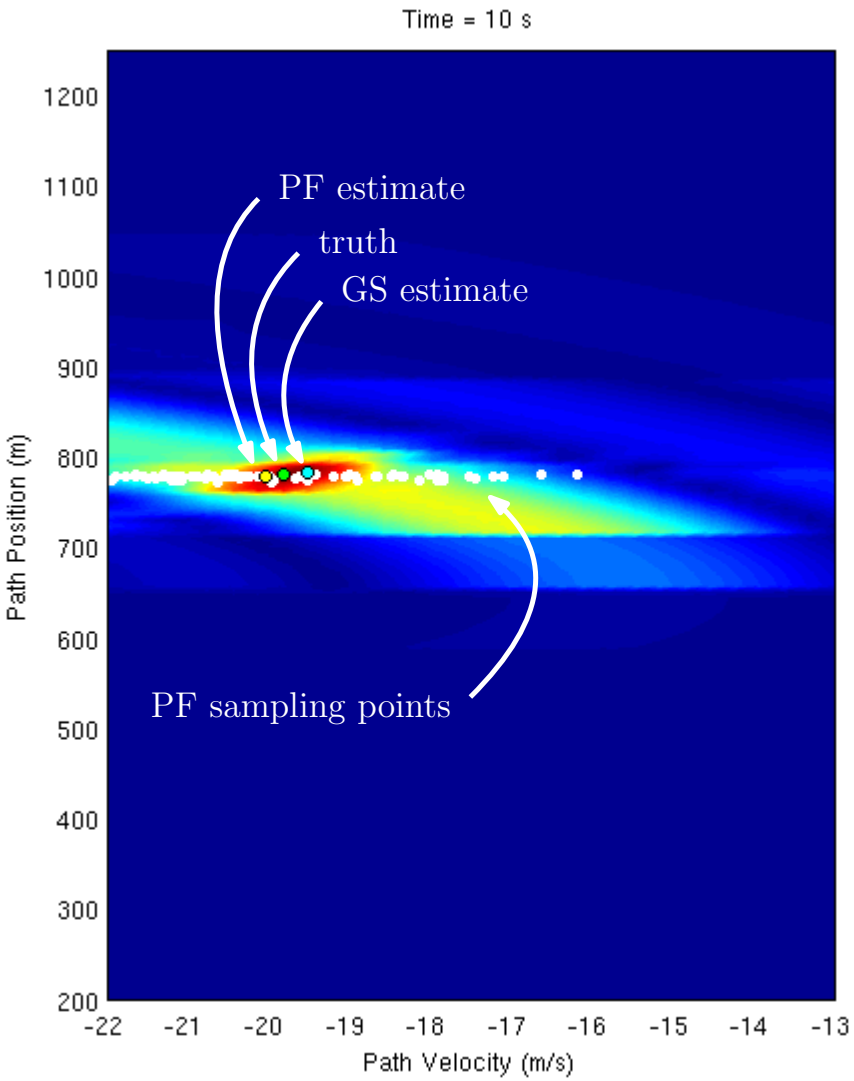


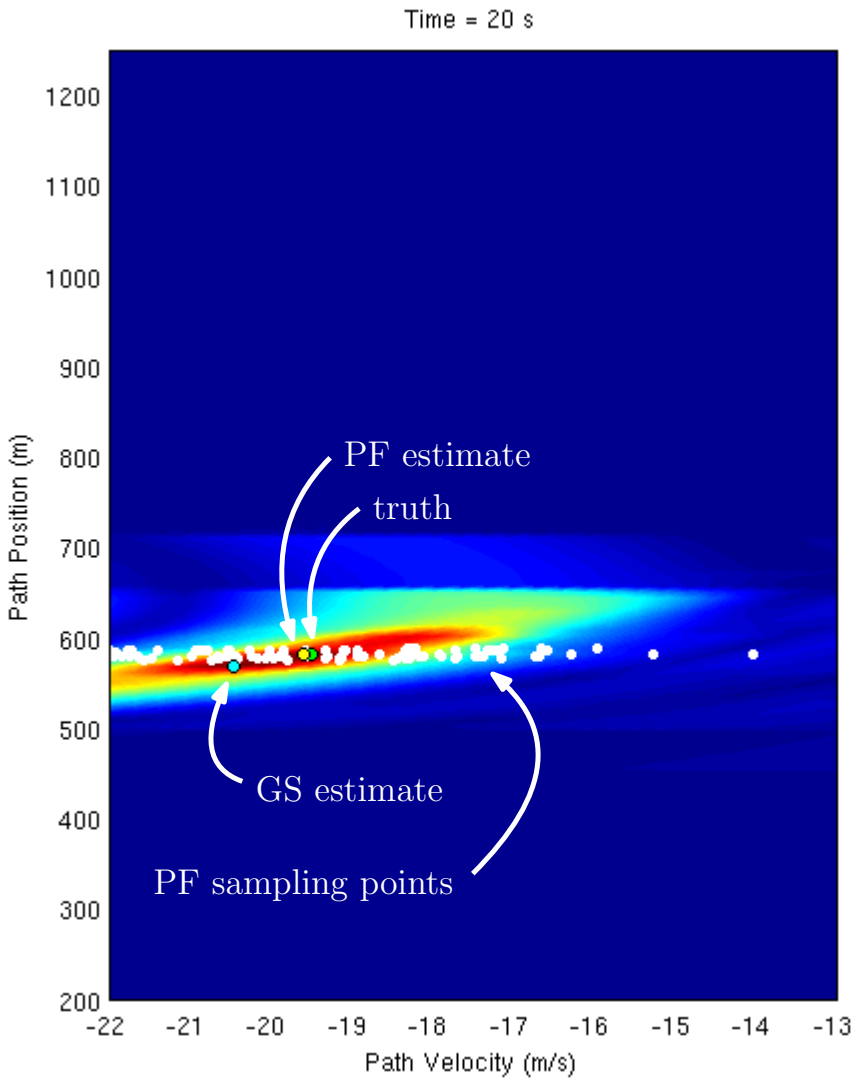
GS and PF Algorithms in NCVP State Space



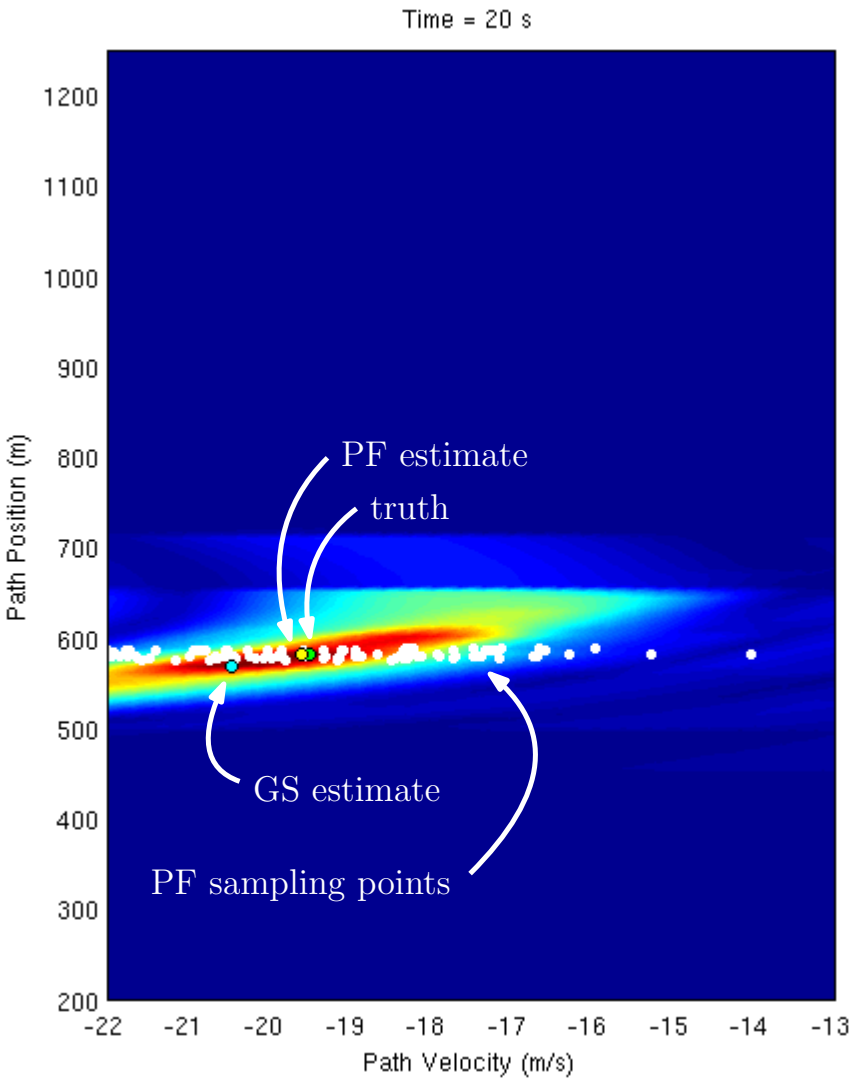


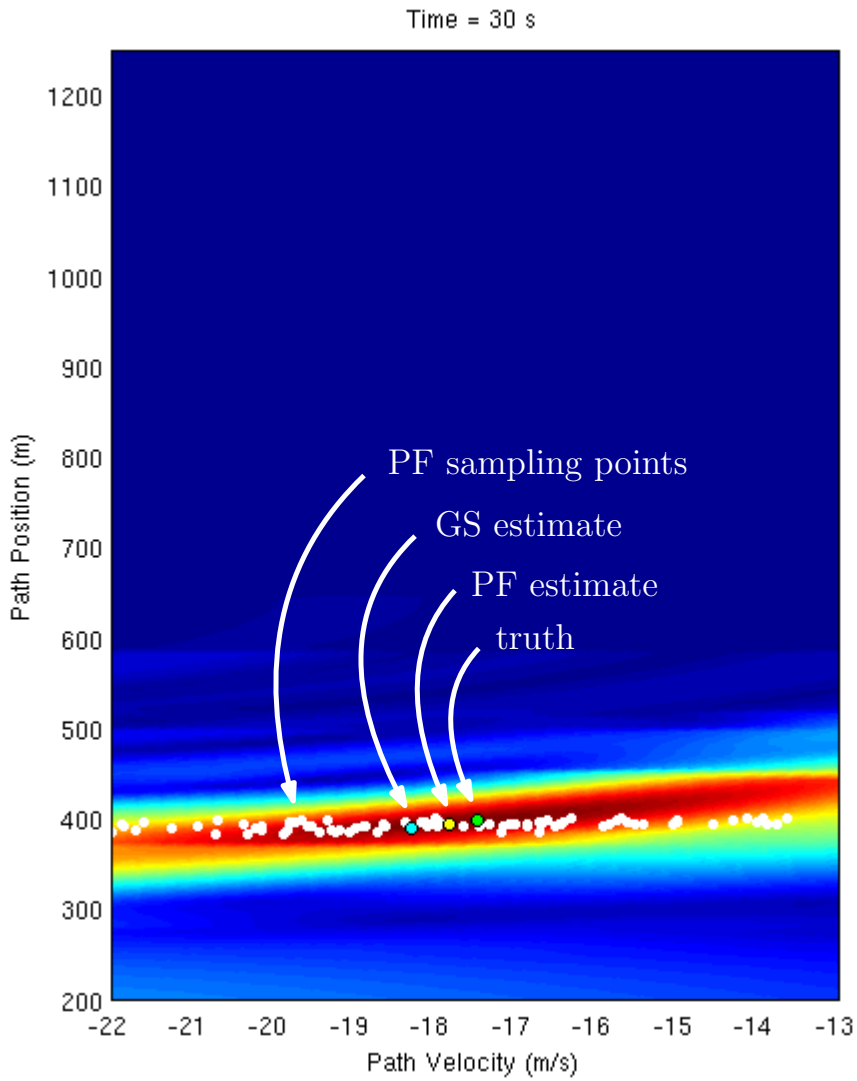
GS and PF Algorithms in NCVP State Space



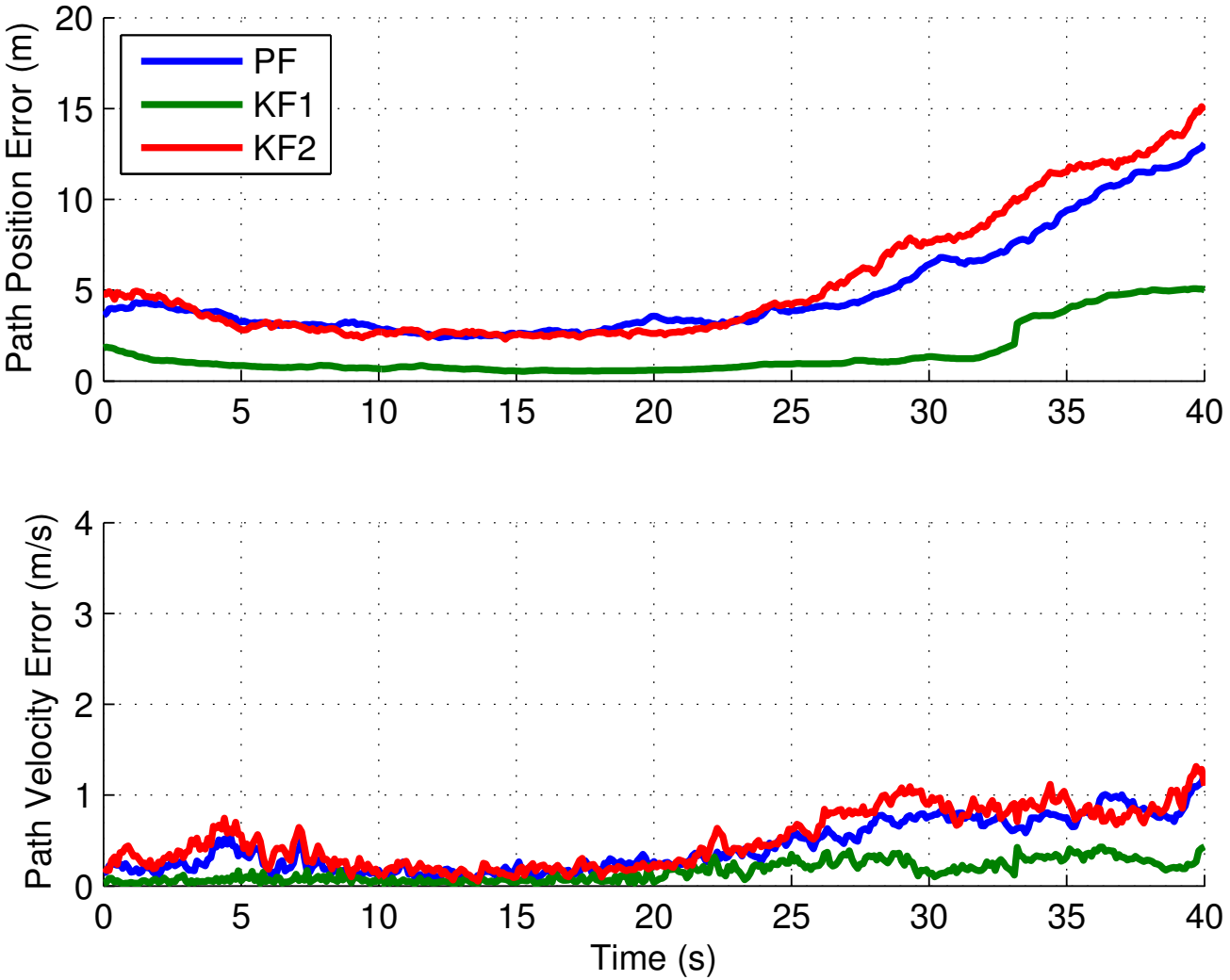


GS and PF Algorithms in NCVP State Space

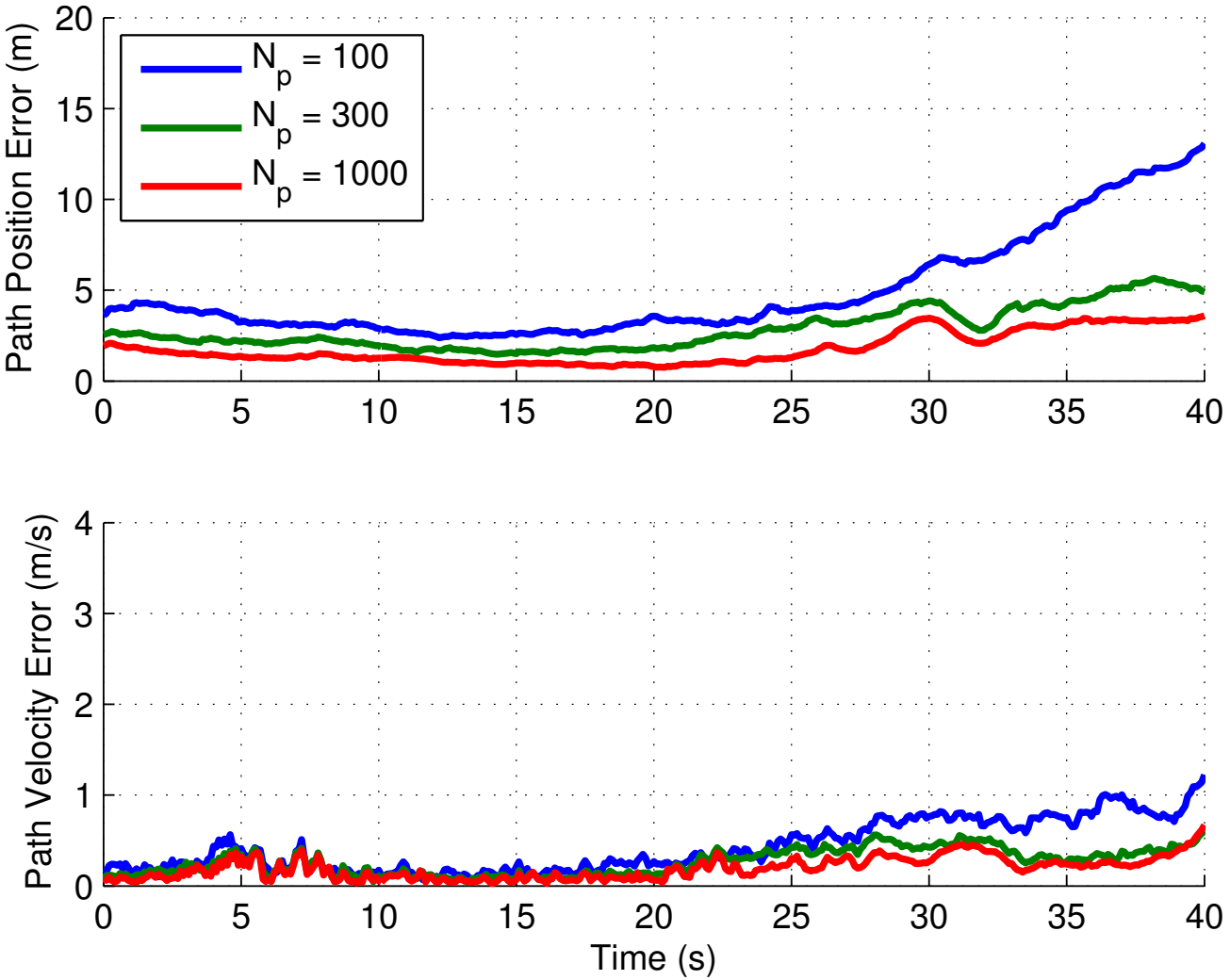




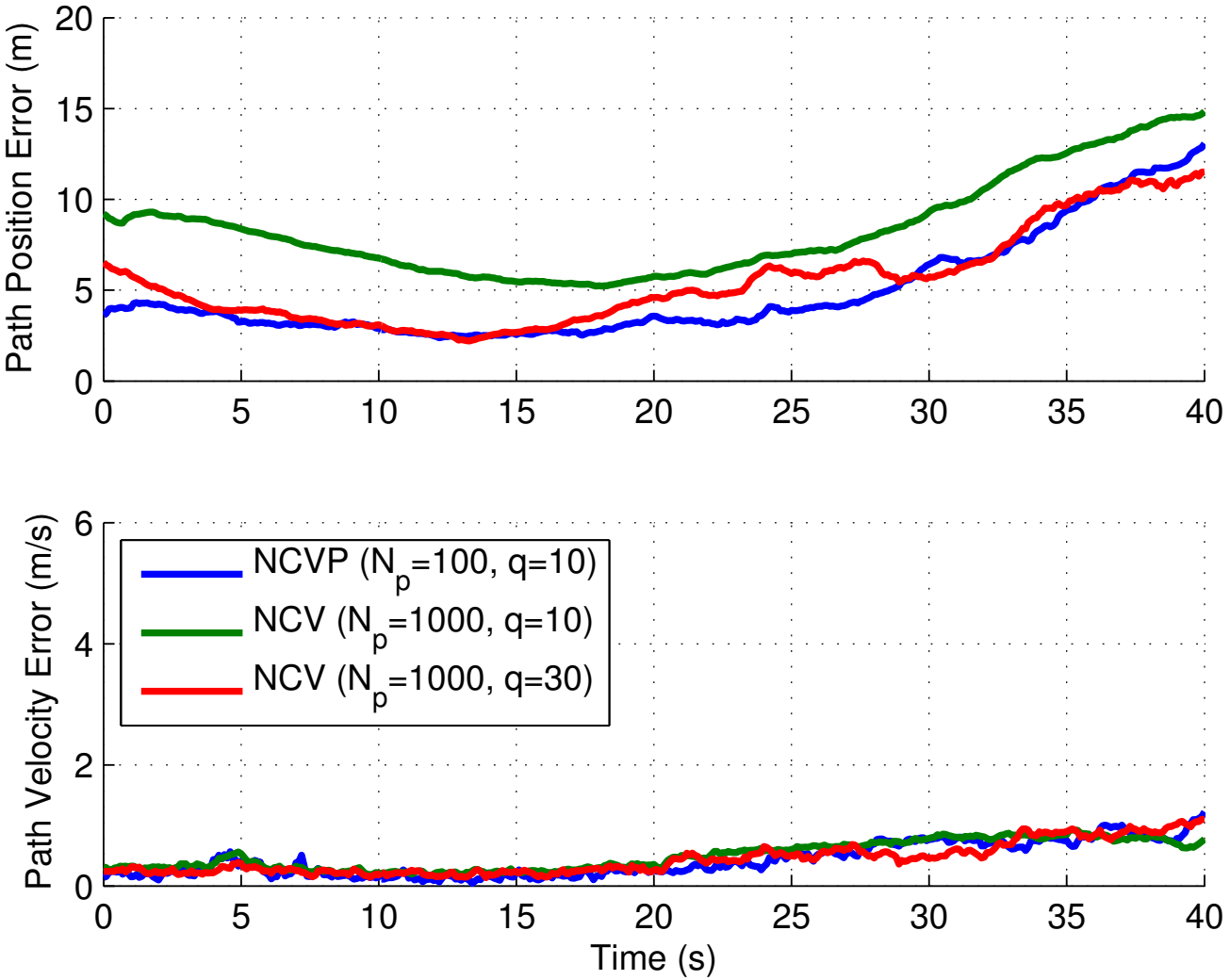
PF, KF1, KF2 Algorithm Performance



PF Performance with Varying Number of Particles

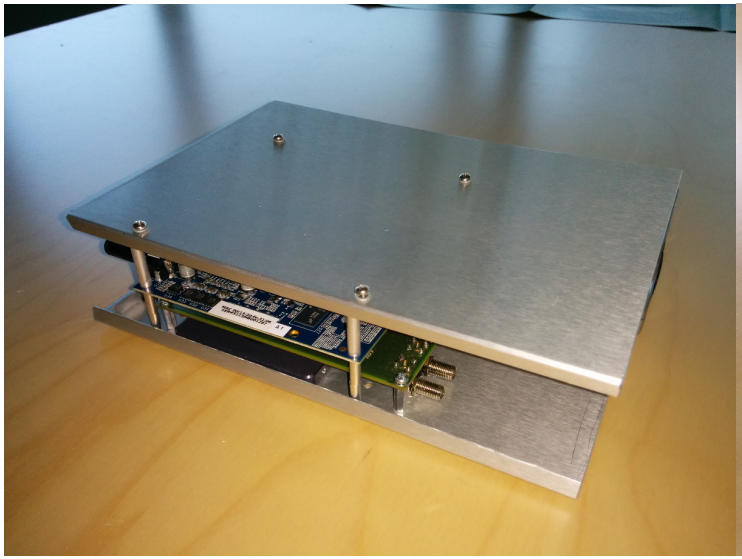


PF Performance Comparing NCVP and NCV Model

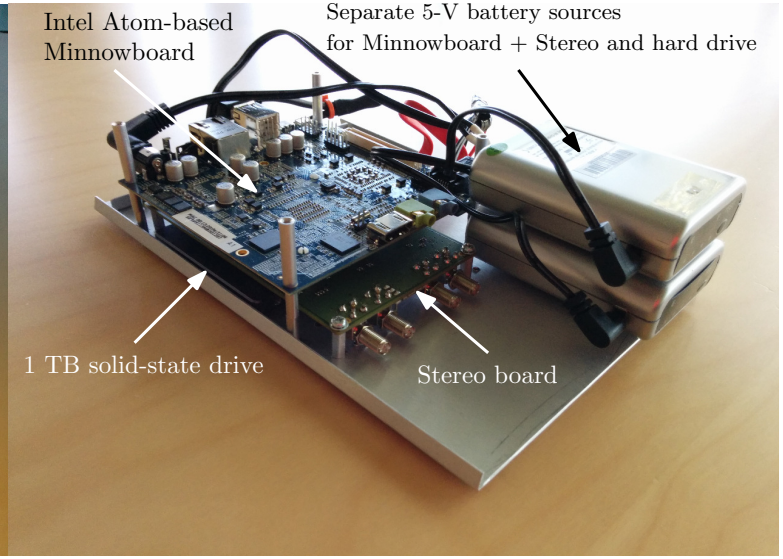


UAV Experiment

- The UAV experiment was designed to mimic applications where a stationary base and dynamic rover platform work together to locate a target.

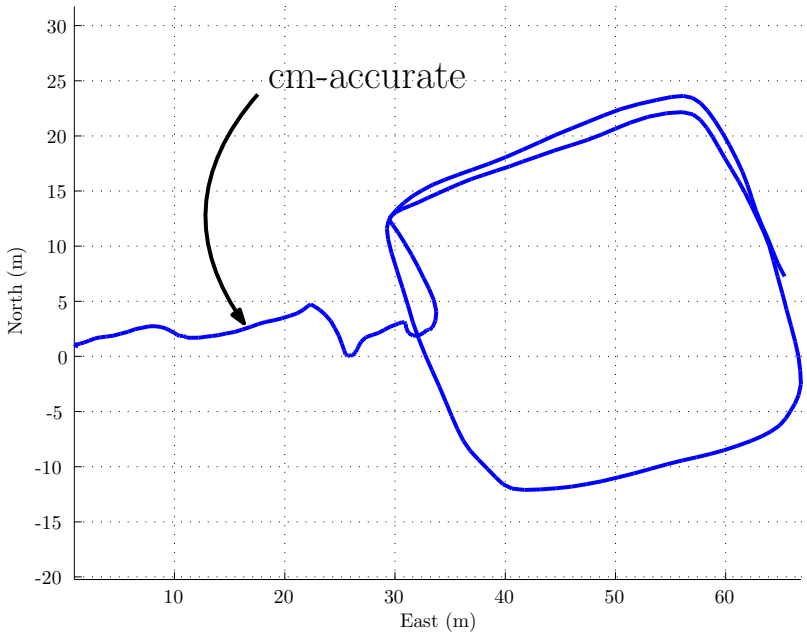


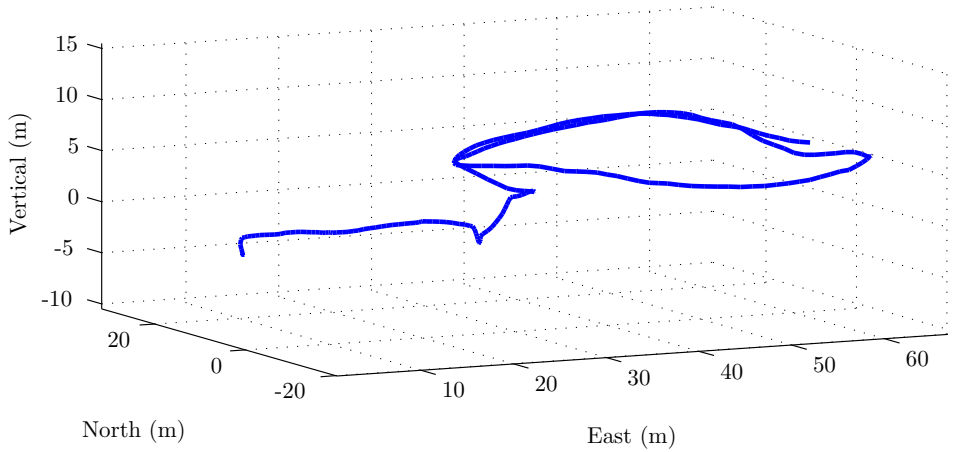
Fully-assembled Stereo-based EMLOC sensor



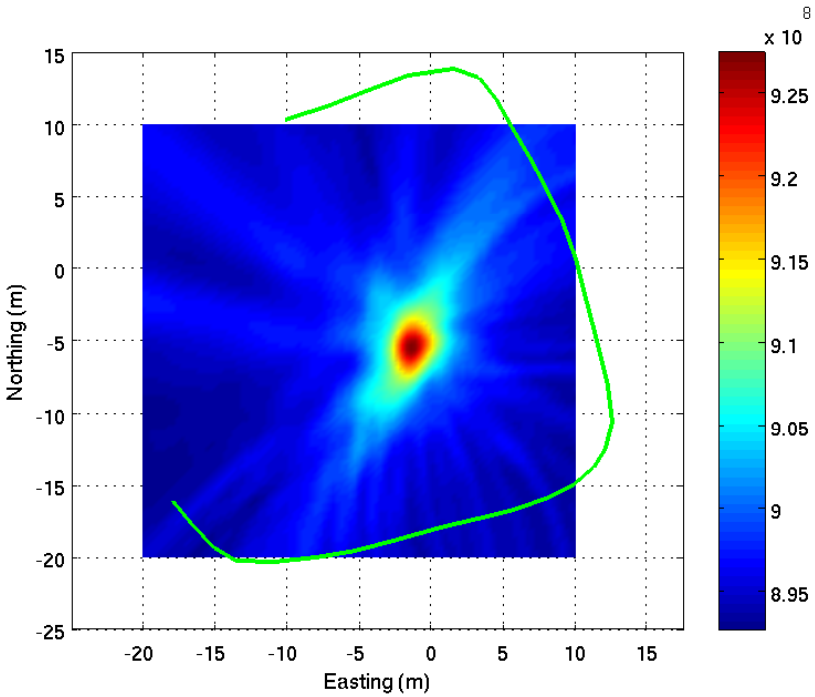
Stereo-based EMLOC sensor with top cover removed

UAV Experiment

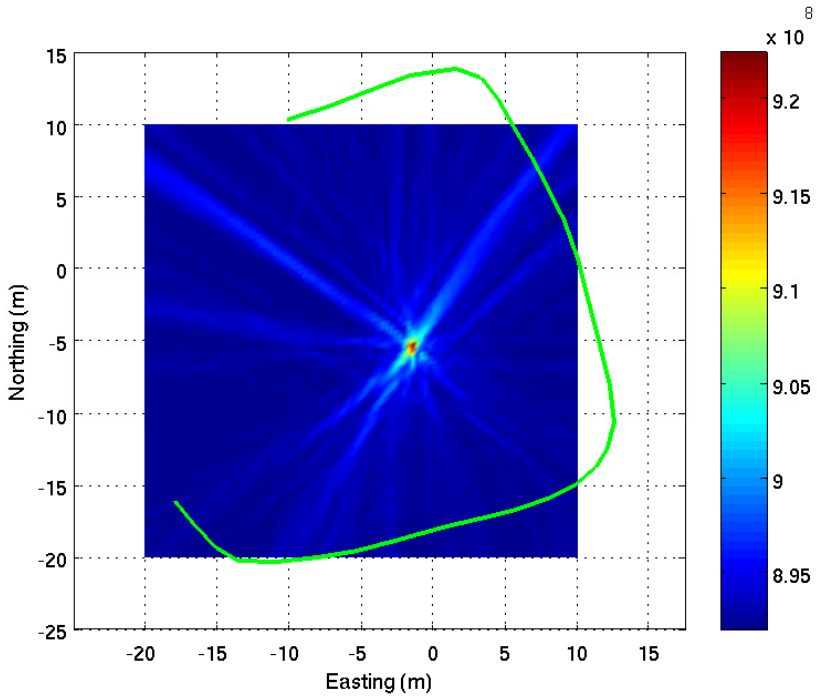




GS with Non-Coherent Averaging

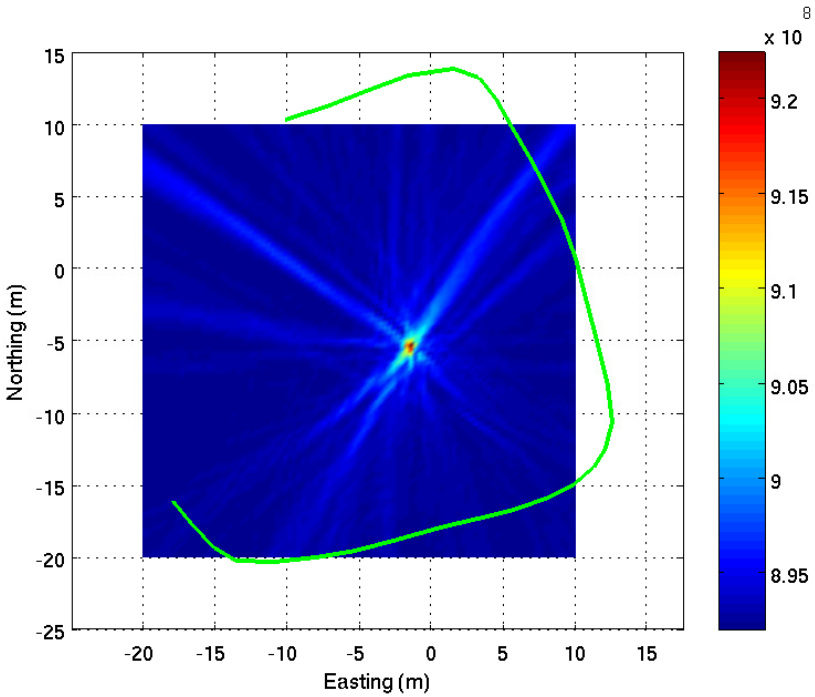


$T = 1\,\mathrm{s}$

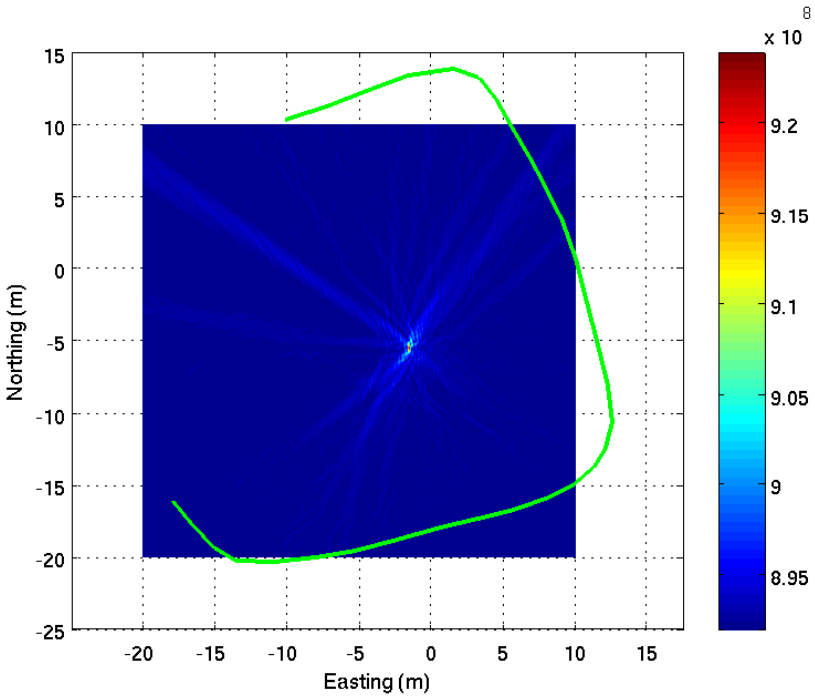


$T = 5\,\mathrm{s}$

GS with Non-Coherent Averaging

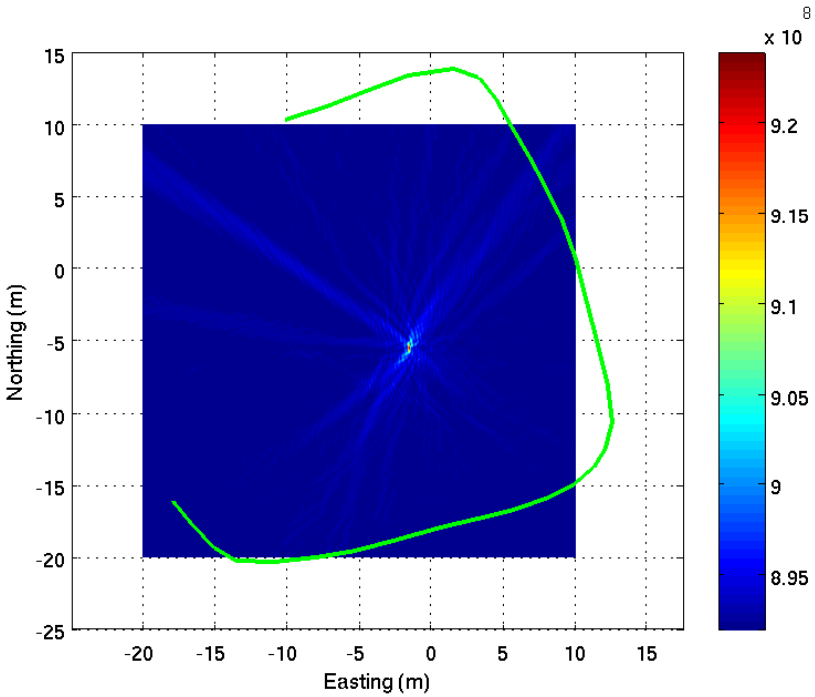


$T = 5\,\mathrm{s}$

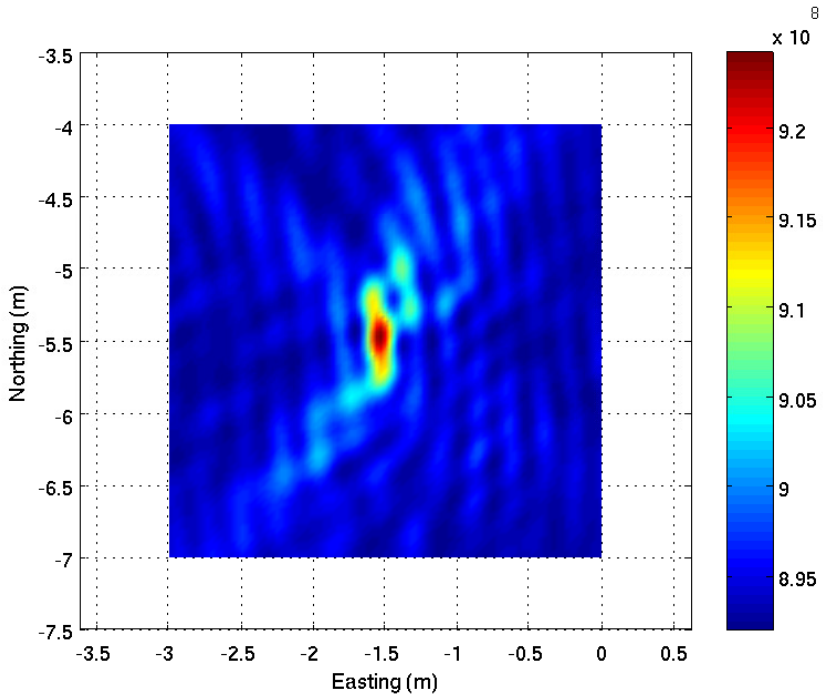


$T = 15\,\mathrm{s}$

GS with Non-Coherent Averaging



$T = 15\,\mathrm{s}$



$T = 15\,\mathrm{s}$ (zoomed in)

Open Questions

- What are the implications of multiple emitters on the estimation architecture in terms of computational and algorithmic complexity?
- How can motion planning algorithms for dynamic receiver platforms based on an information-seeking control law be applied to direct emitter geolocation? (Hoffmann and Tomlin, 2010).

Table of Contents

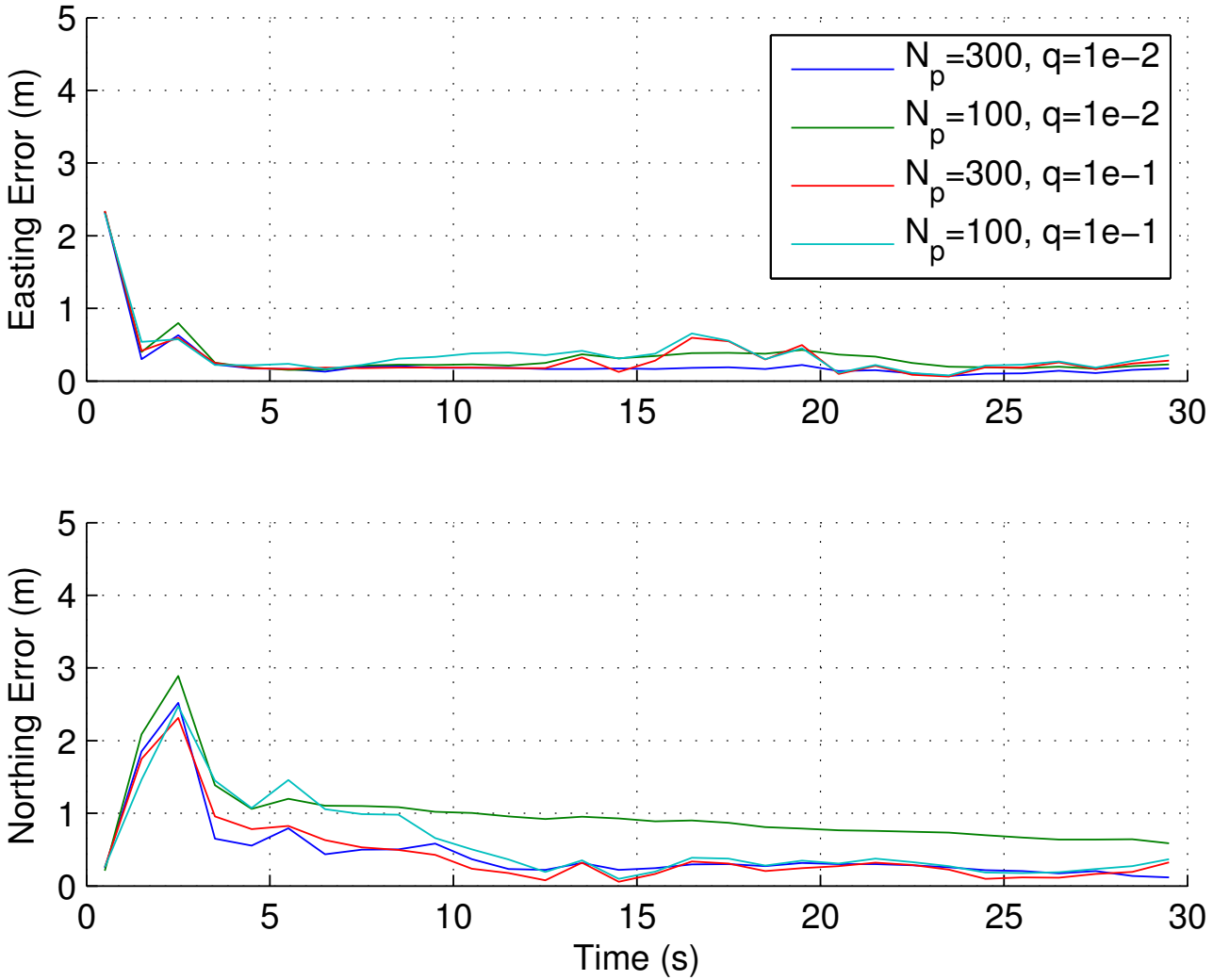
Conclusion

- A detection framework has been developed to detect spoofing attacks in maritime environments based solely on Doppler log, gyrocompass, and potentially-spoofed GPS measurements.
- The worst-case integrity risk of the detection framework was minimized by optimizing the sampling time of the GPS measurements.
- A passive RF emitter localization system has been developed and analyzed thoroughly with multiple experiments.
- The system employed direct geolocation and long coherent integration techniques, thus improving the system's estimation performance with weak emitters and multipath.

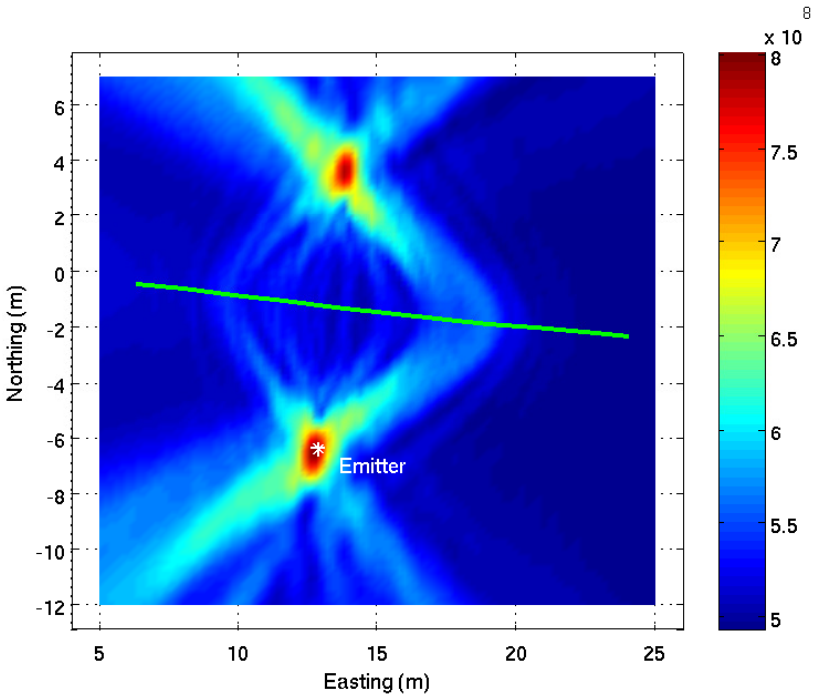
Conclusion

Security researcher Jahshan Bhatti gazes toward the empty horizon, observing the bent wake caused by the captain steering the yacht to keep the spoofed GPS position, so easily trusted yet so easily manipulated, within a carefully charted corridor.

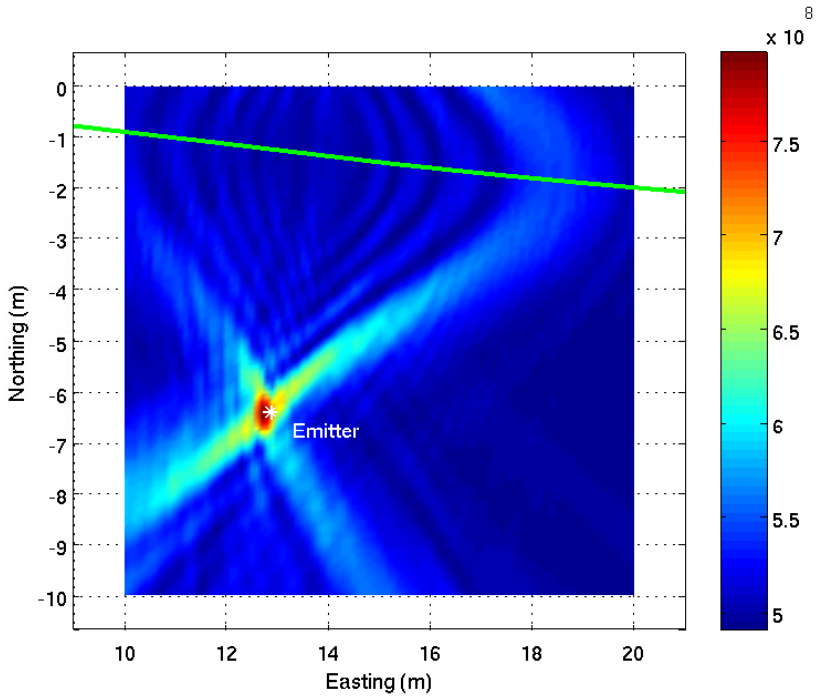
PF Performance for UAV Experiment



UAV on Roof Experiment

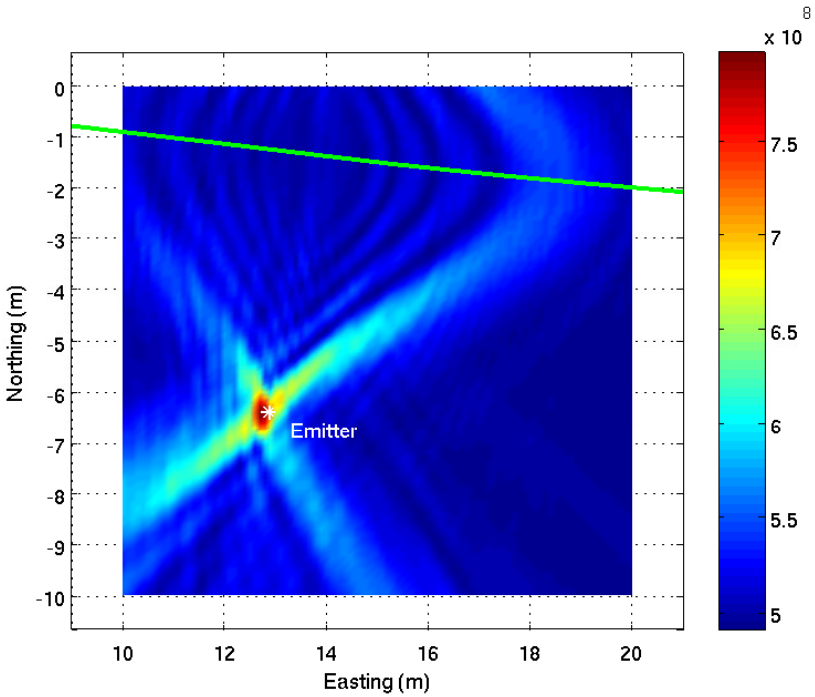


$T = 2\,\mathrm{s}, \epsilon = 11.5\,\mathrm{cm}$

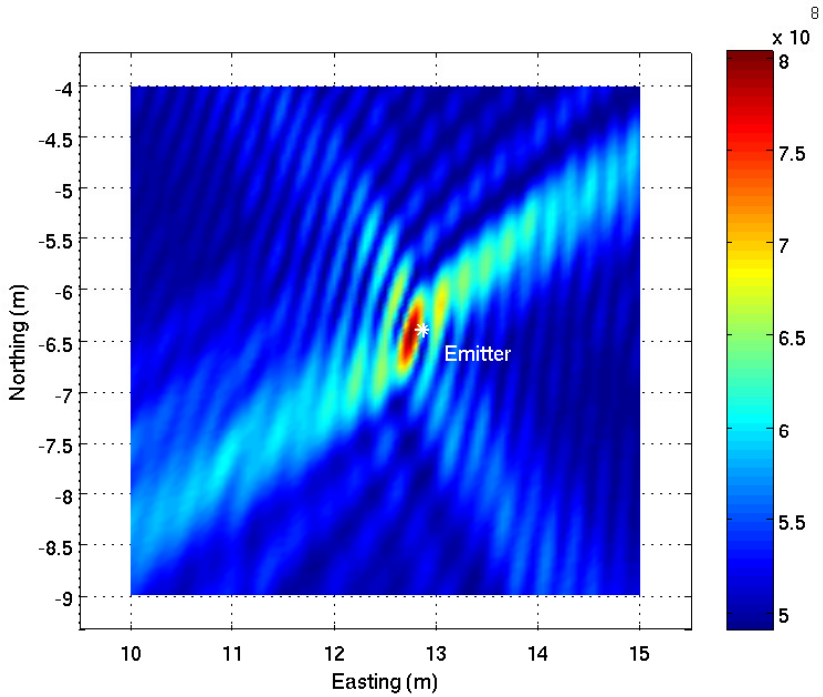


$T = 5\,\mathrm{s}, \epsilon = 16.7\,\mathrm{cm}$

UAV on Roof Experiment



$T = 5\,\mathrm{s}, \epsilon = 16.7\,\mathrm{cm}$



$T = 10\,\mathrm{s}, \epsilon = 12.9\,\mathrm{cm}$

For Further Reading I

K. B. Deshpande, G. S. Bust, C. R. Clauer, H. Kim, J. E. Macon, T. E. Humphreys, J. A. Bhatti, S. B. Musko, G. Crowley, and A. T. Weatherwax, "Initial GPS scintillation results from CASES receiver at South Pole, Antarctica," *Radio Science*, vol. 47, no. 5, 2012.

C. R. Clauer, H. Kim, K. Deshpande, Z. Xu, D. Weimer, S. Musko, G. Crowley, C. Fish, R. Nealy, T. E. Humphreys, J. A. Bhatti, and A. J. Ridley, "Autonomous adaptive low-power instrument platform (AAL-PIP) for remote high latitude geospace data collection," *Geoscientific Instrumentation, Methods and Data Systems*, vol. 3, pp. 211–227, 2014.

E. G. Lightsey, T. E. Humphreys, J. A. Bhatti, A. J. Joplin, B. W. O'Hanlon, and S. P. Powell, "Demonstration of a space capable miniature dual frequency GNSS receiver," *Navigation, Journal of the Institute of Navigation*, vol. 61, no. 1, pp. 53–64, 2014.

For Further Reading II

M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, J. A. Bhatti, and D. P. Shepard, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation, Journal of the Institute of Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

J. Bhatti and T. Humphreys, "Covert control of surface vessels via GPS spoofing," *Navigation, Journal of the Institute of Navigation*, 2015, (In preparation.).

For Further Reading III

J. Bhatti, B. Ledvina, and T. Humphreys, "Analysis and experimental results of direct geolocation techniques," *Navigation, Journal of the Institute of Navigation*, 2015, (In preparation.).

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, pp. 326–338.

J. A. Bhatti, T. E. Humphreys, and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Proceedings of the IEEE/ION PLANS Meeting*, April 2012, pp. 1209–1220.

A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, no. 6, pp. 601–611, 1976.

For Further Reading IV

M. Joerger and B. Pervan, "Kalman filter-based integrity monitoring against sensor faults," *Journal of Guidance Control Dynamics*, vol. 36, pp. 349–361, 2013.

S. Khanafseh, N. Roshan, S. Langel, F. Cheng-Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

S. Stein, "Algorithms for ambiguity function processing," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 29, no. 3, pp. 588–599, June 1981.

A. Sidi and A. Weiss, "Delay and doppler induced direct tracking by particle filter," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 50, no. 1, pp. 559–572, January 2014.

A. Weiss, "Direct geolocation of wideband emitters based on delay and doppler," *Signal Processing, IEEE Transactions on*, vol. 59, no. 6, pp. 2513–2521, June 2011.

For Further Reading V

N. Gordon, D. Salmond, and A. Smith, "Novel approach to nonlinear/non-gaussian bayesian state estimation," *Radar and Signal Processing, IEE Proceedings F*, vol. 140, no. 2, pp. 107–113, Apr 1993.

G. Hoffmann and C. Tomlin, "Mobile sensor network control using mutual information methods and particle filters," *Automatic Control, IEEE Transactions on*, vol. 55, no. 1, pp. 32–47, Jan 2010.