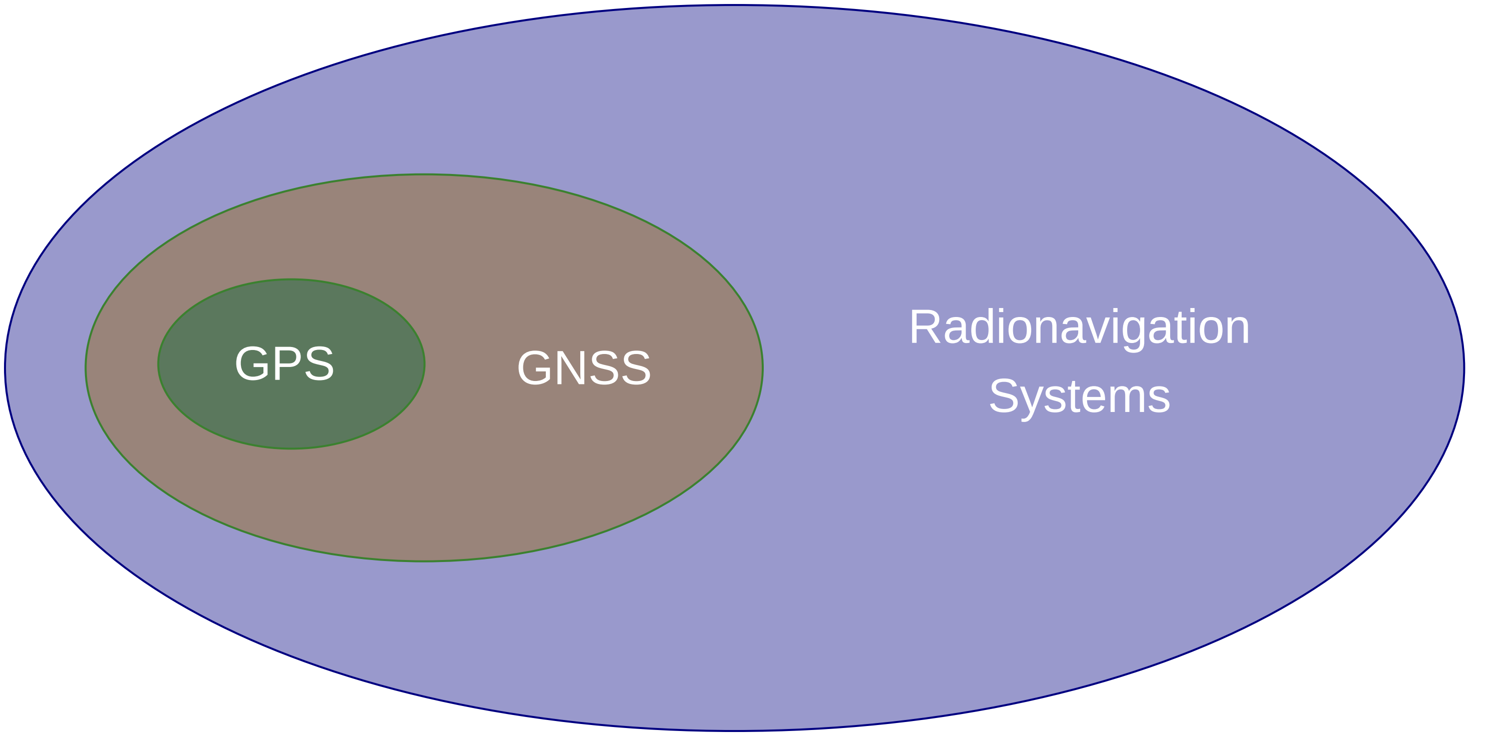
THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Radionavigation Integrity and Security

Dr. Todd E. Humphreys

CSR Seminar, April 6, 2010

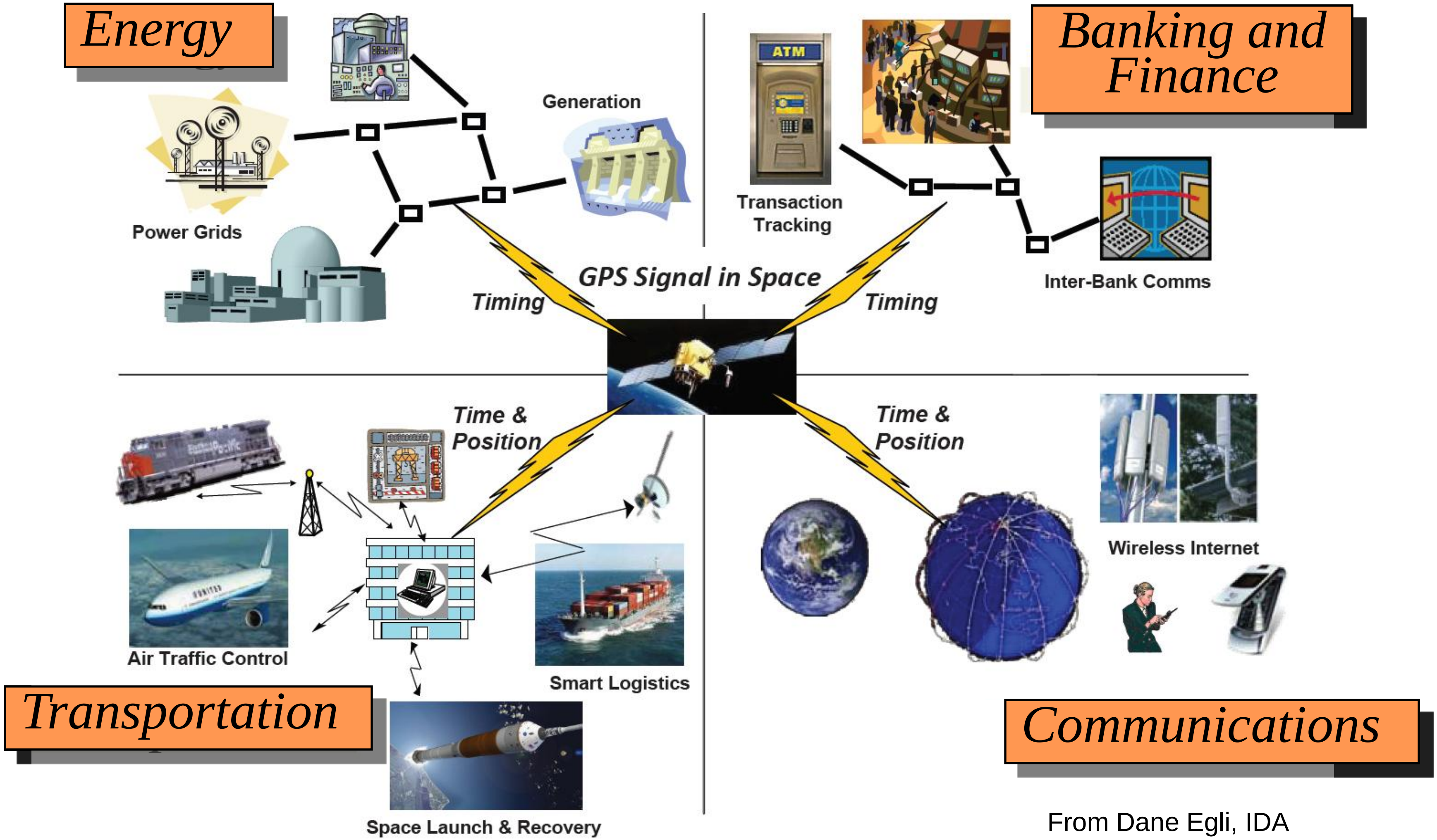
Radionavigation



GPS: The Achilles' Heels

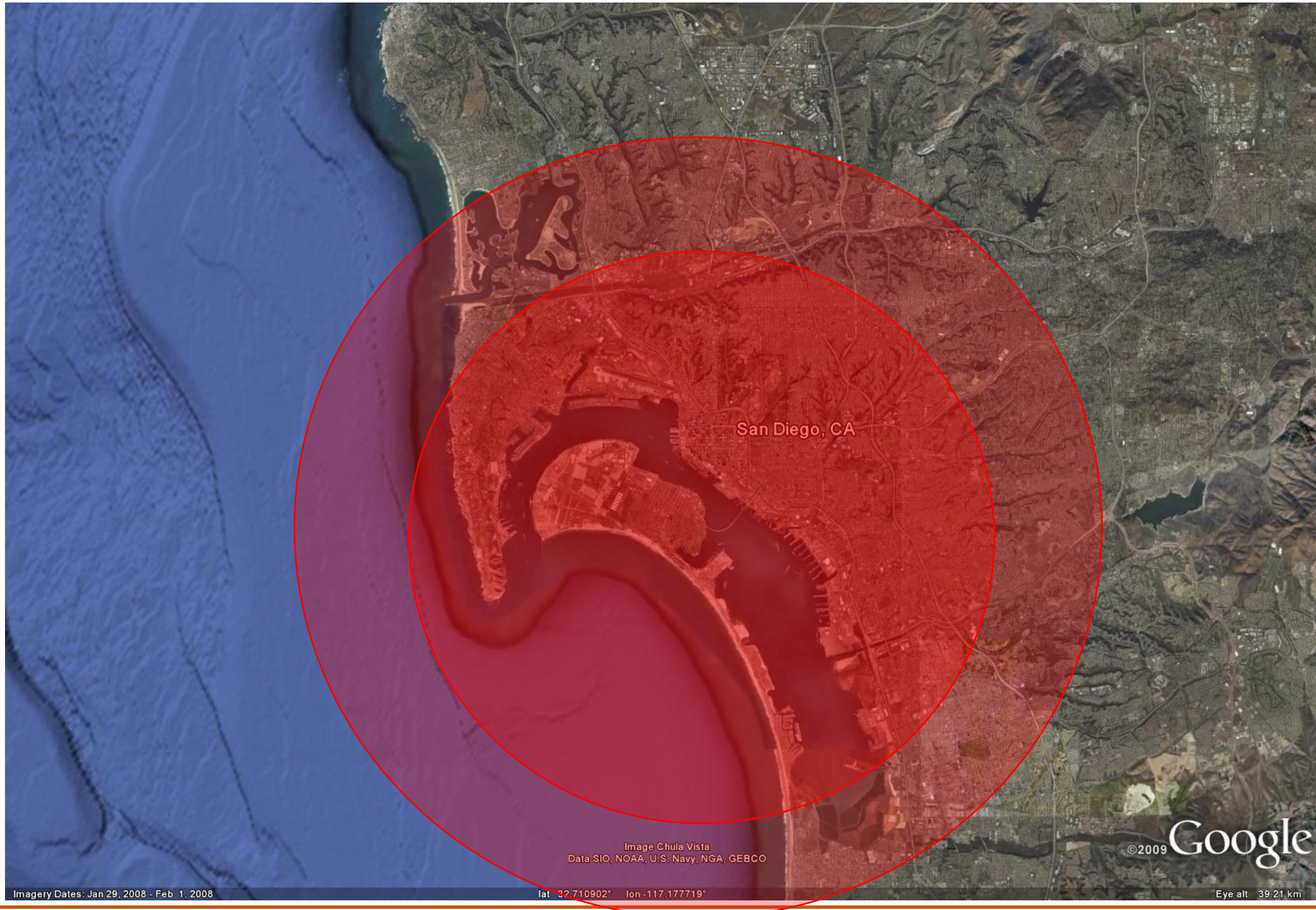
- **Weak GPS Signals**
  - Like a 30-Watt lightbulb held 4000 km away
  - GPS does not penetrate well indoors
  - GPS is easy target for jamming
  - GPS is vulnerable to natural interference (e.g., solar radio bursts and ionospheric scintillation)
- **Unauthenticated Civil GPS Signals**
  - Civil GPS broadcast "in the clear"
  - Makes civil GPS vulnerable to spoofing

GPS: Dependency Begets Vulnerability

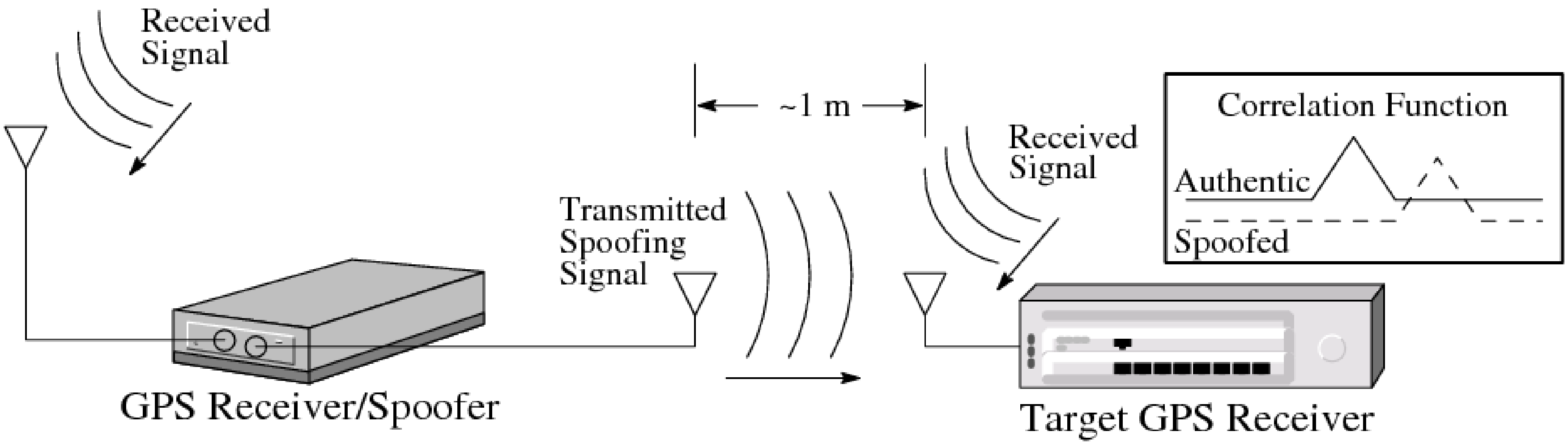


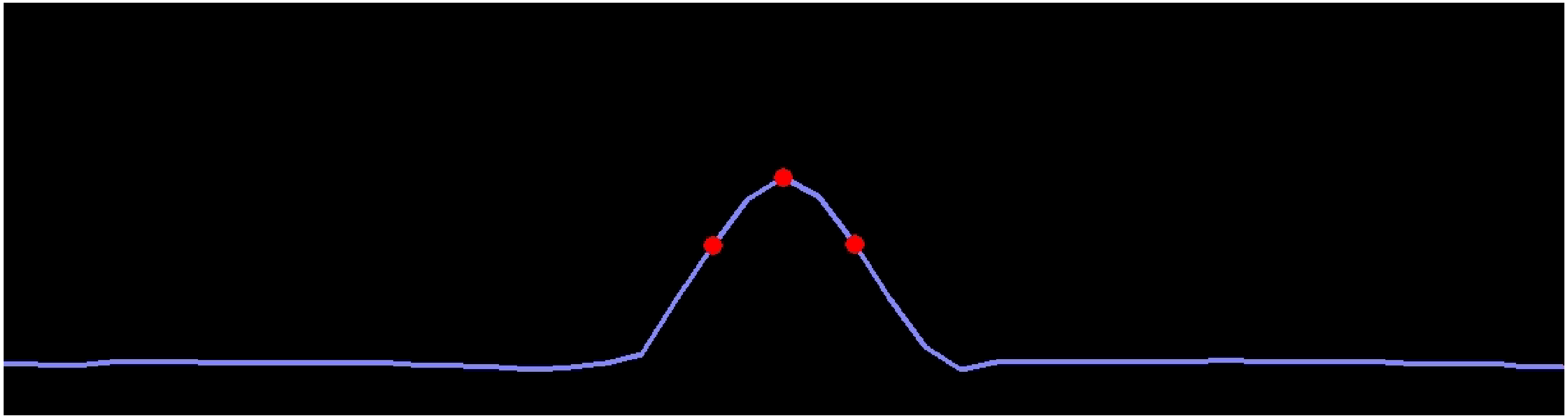
From Dane Egli, IDA

Civil GPS Jamming Event



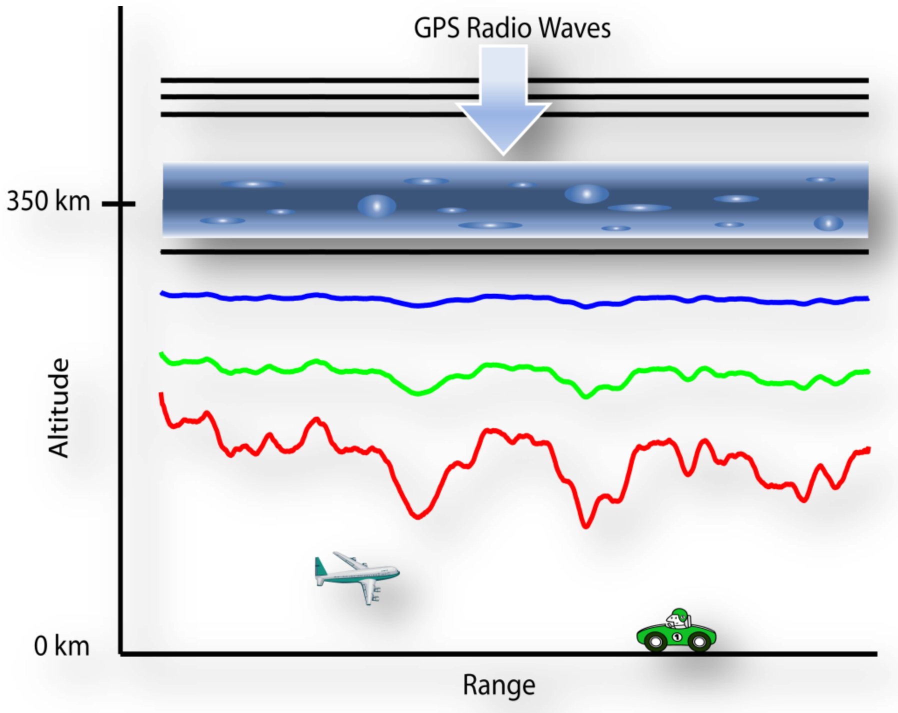
Civil GPS Spoofing

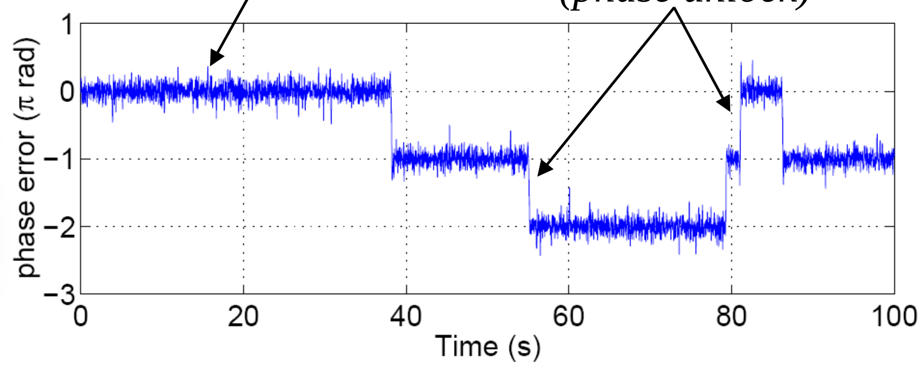


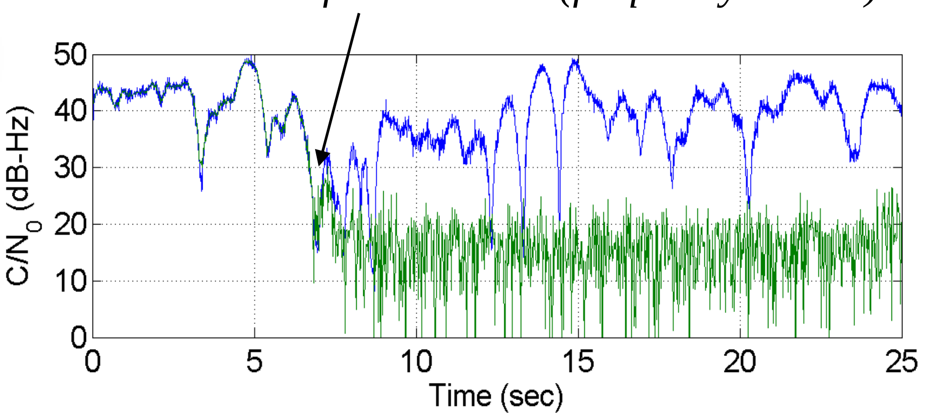


Civil GPS Spoofing (cont'd)

Ionospheric Scintillation

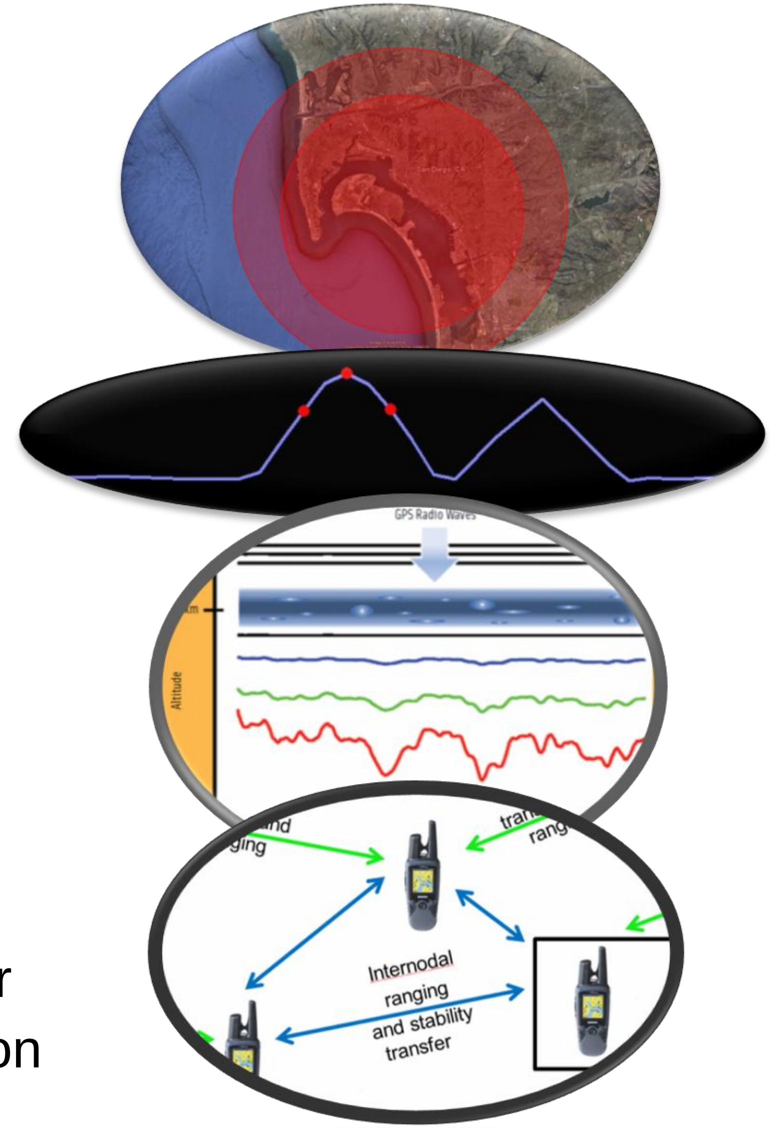






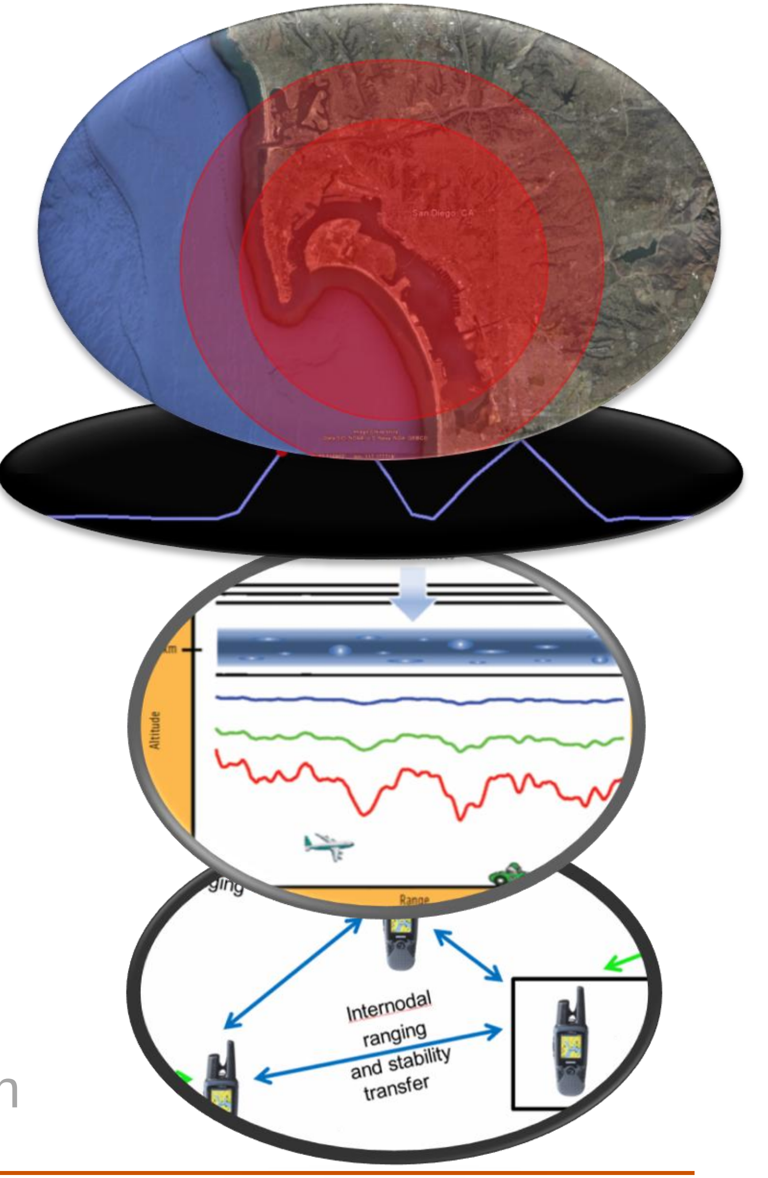
Research Agenda

- **GPS Jamming**
  - Locate jamming sources by combining data from a network of receivers
  - Develop augmentation-based defenses
- **GNSS Spoofing**
  - Characterize spoofing signatures
  - Develop receiver-autonomous defenses
  - Develop augmentation-based defenses
- **Natural GNSS Interference**
  - Improve tracking loop robustness to scintillation
- **Network-Centric Navigation**
  - Establish theory for time stability transfer
  - Opportunistic and collaborative navigation

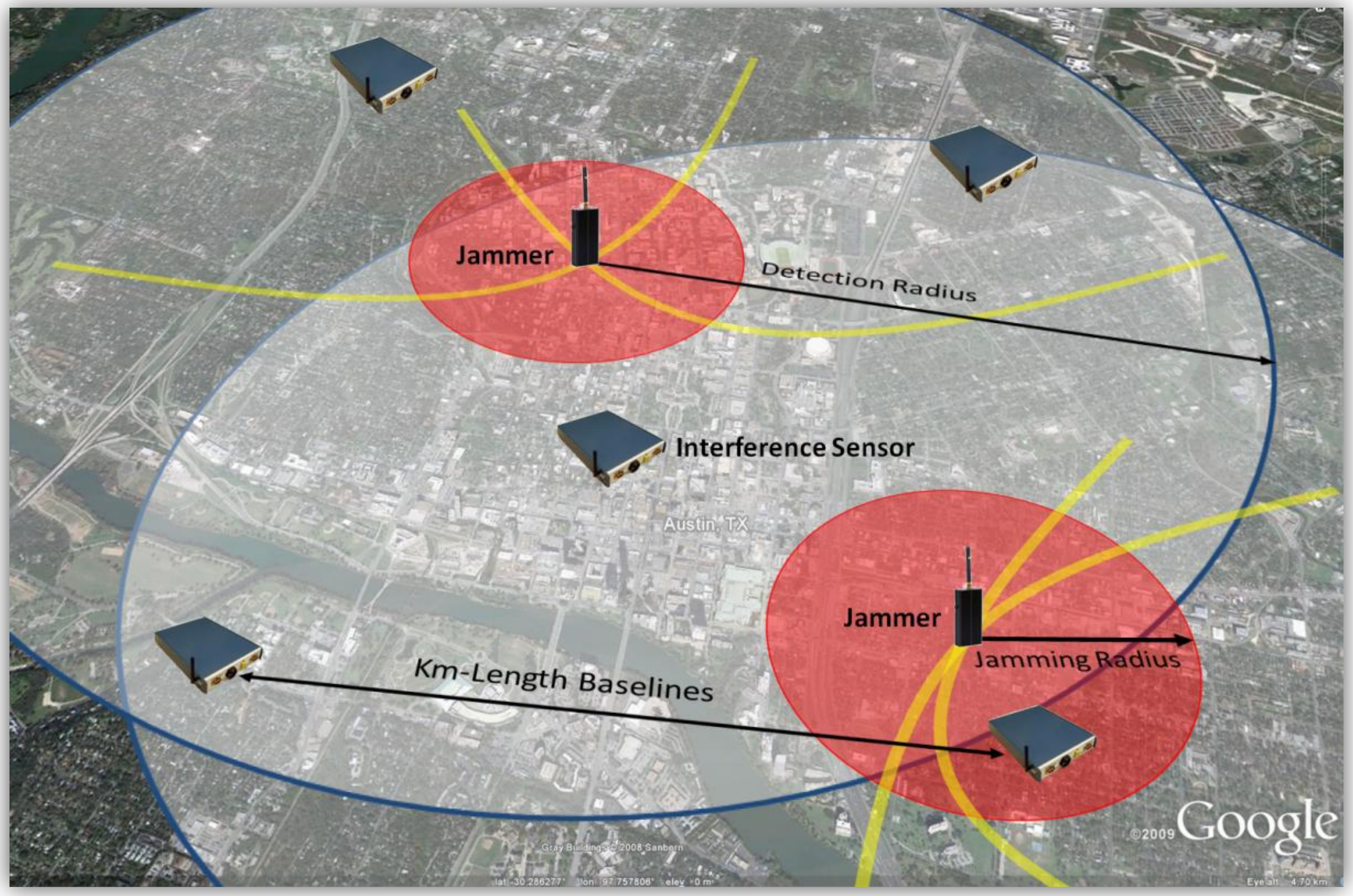


Research Agenda

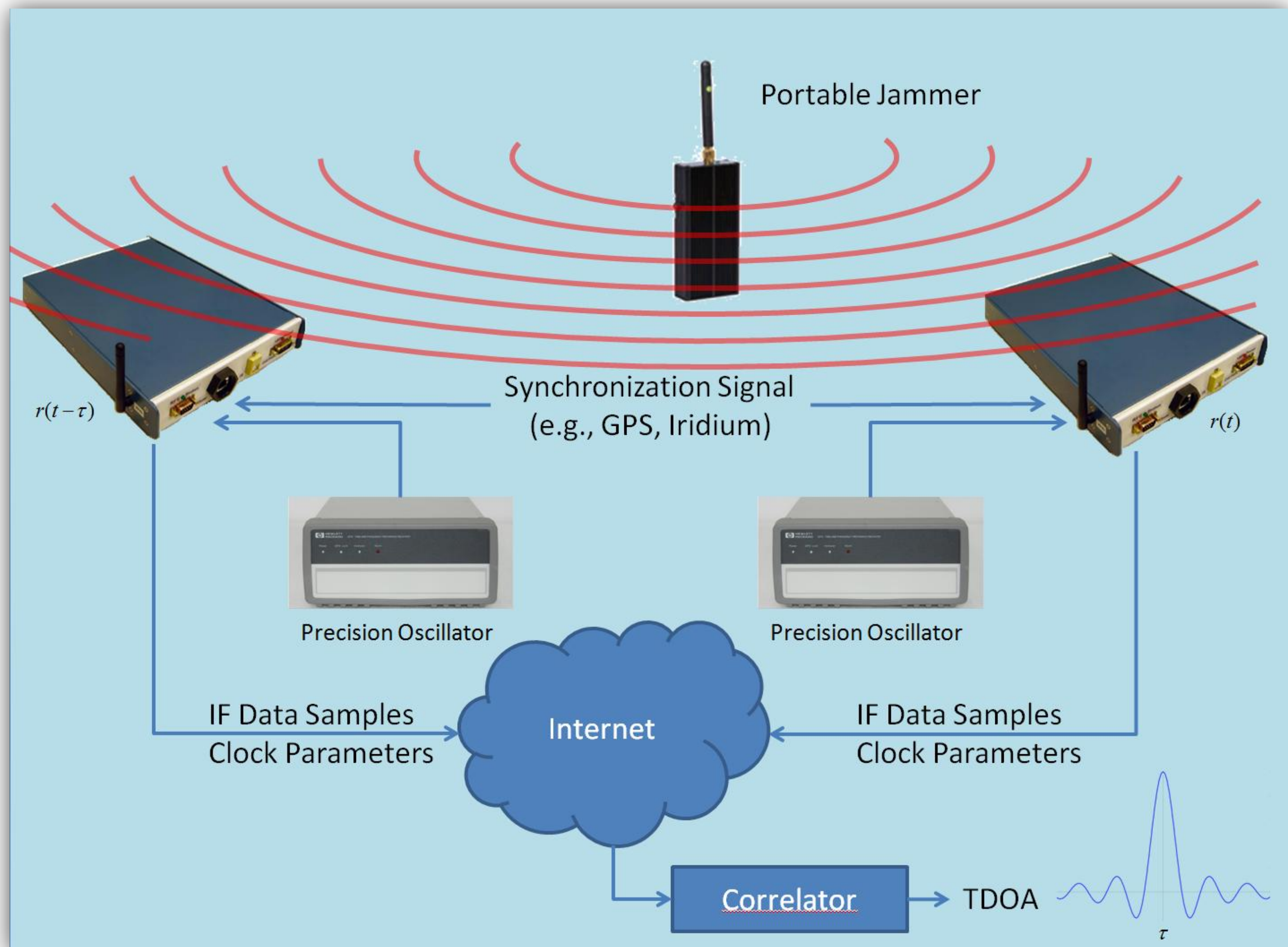
- **GPS Jamming**
  - Locate jamming sources by combining data from a network of receivers
  - Develop augmentation-based defenses
- **GNSS Spoofing**
  - Characterize spoofing signatures
  - Develop receiver-autonomous defenses
  - Develop augmentation-based defenses
- **Natural GNSS Interference**
  - Improve tracking loop robustness to scintillation
- **Network-Centric Navigation**
  - Establish theory for time stability transfer
  - Opportunistic and collaborative navigation



INTERLOC:
Network-based Interference Location

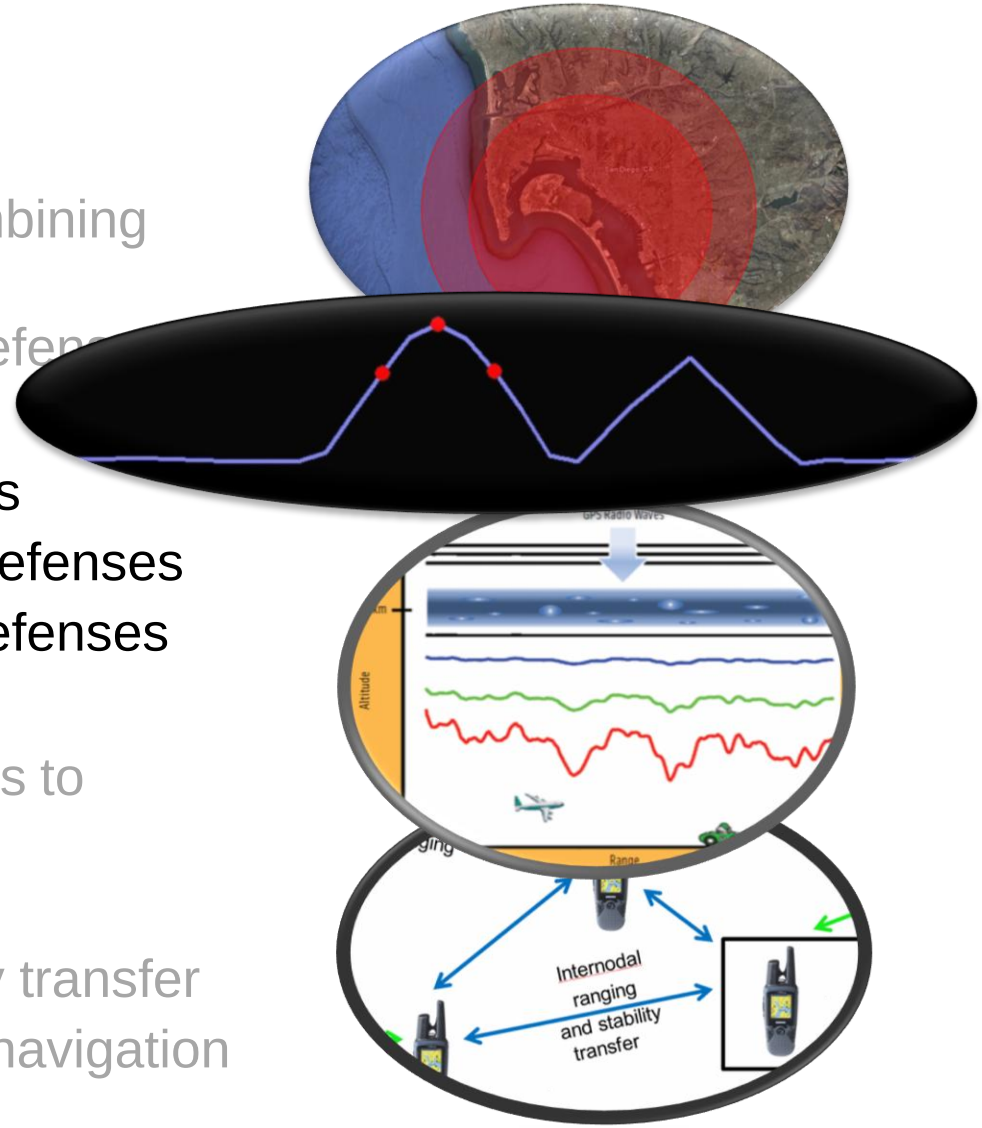


INTERLOC Functional Diagram



Research Agenda

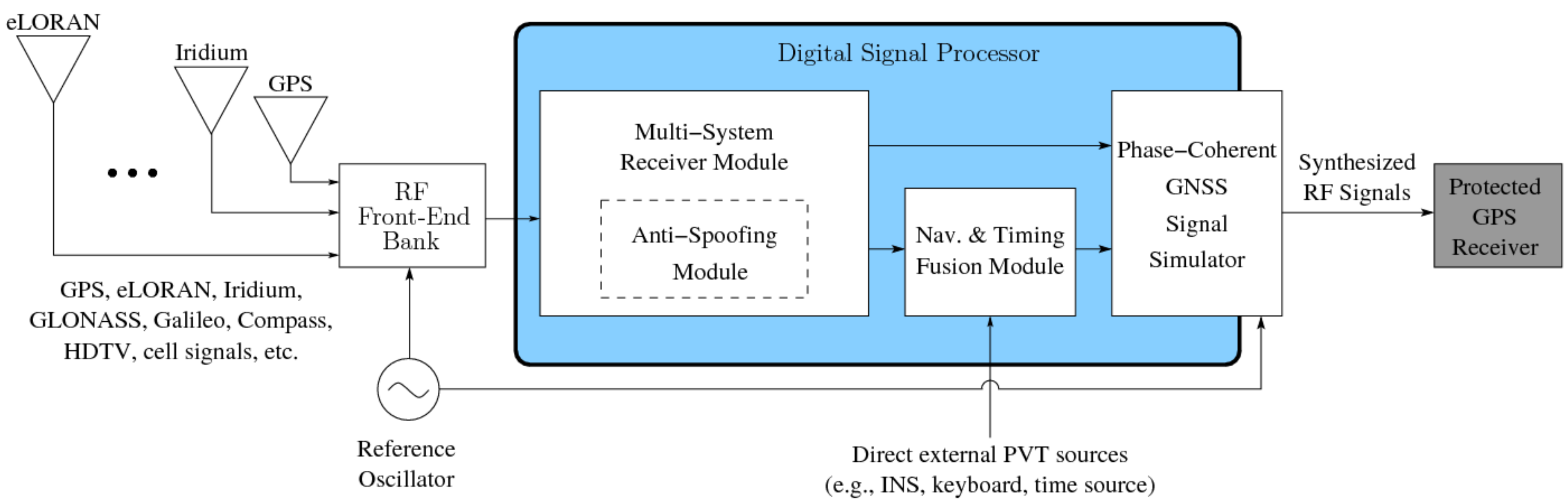
- **GPS Jamming**
  - Locate jamming sources by combining data from a network of receivers
  - Develop augmentation-based defen…
- **GNSS Spoofing**
  - Characterize spoofing signatures
  - Develop receiver-autonomous defenses
  - Develop augmentation-based defenses
- **Natural GNSS Interference**
  - Improve tracking loop robustness to scintillation
- **Network-Centric Navigation**
  - Establish theory for time stability transfer
  - Opportunistic and collaborative navigation



GRID Software-Defined Radio

Flexible software-defined radio platform enables:
GPS Assimilator
Spoofing characterization
GPS-based scientific research
Collaborative navigation research

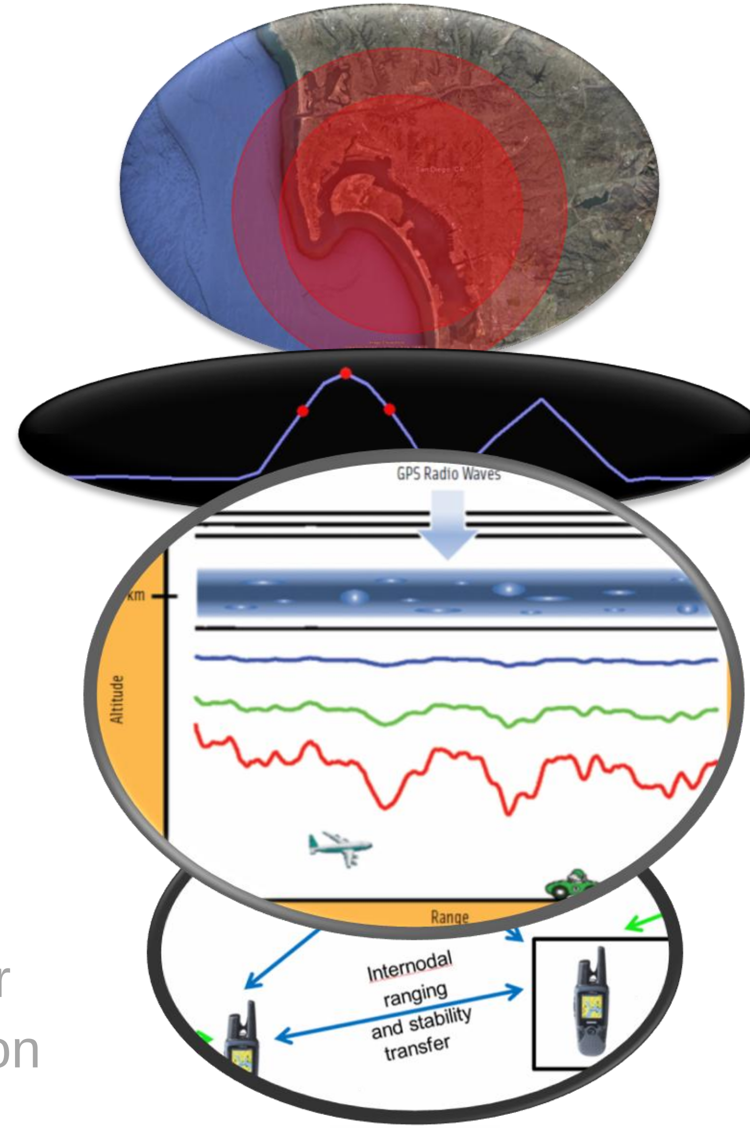
The GPS Assimilator



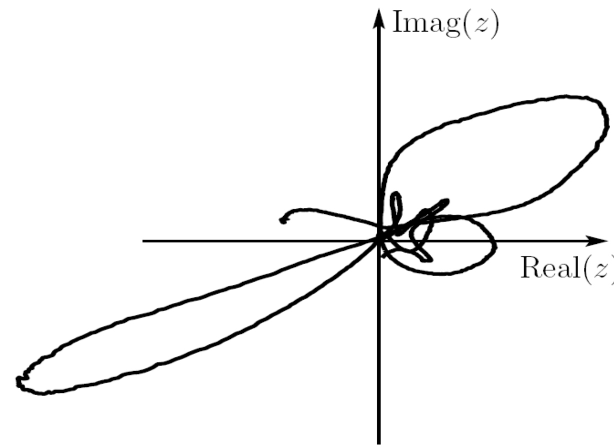
The GPS Assimilator modernizes and makes existing GPS equipment resistant to jamming and spoofing without requiring hardware or software changes to the equipment

Research Agenda

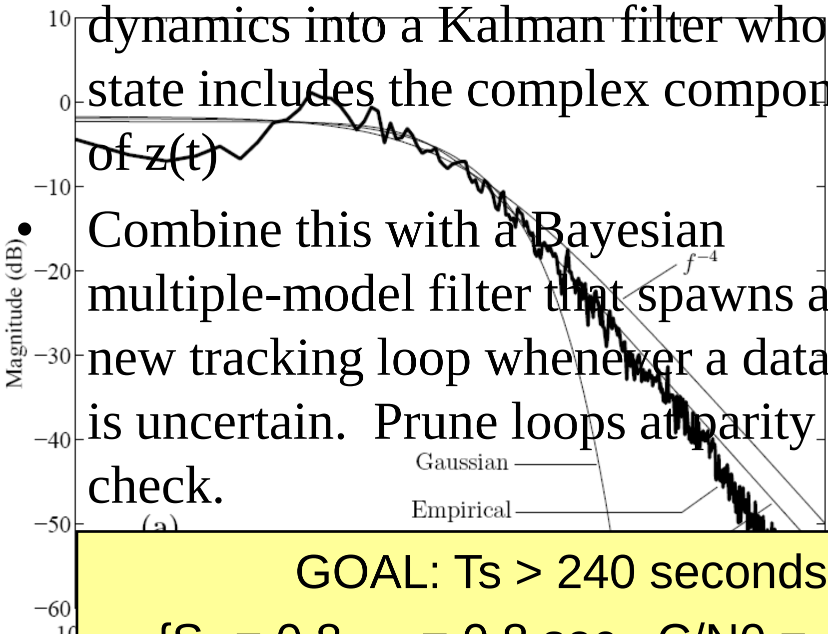
- **GPS Jamming**
  - Locate jamming sources by combining data from a network of receivers
  - Develop augmentation-based defenses
- **GNSS Spoofing**
  - Characterize spoofing signatures
  - Develop receiver-autonomous defenses
  - Develop augmentation-based defenses
- **Natural GNSS Interference**
  - Improve tracking loop robustness to scintillation
- **Network-Centric Navigation**
  - Establish theory for time stability transfer
  - Opportunistic and collaborative navigation



Scintillation-hardened Tracking Loops



- Straightforward approach: navigation data bit prediction
- Incorporate the observed second-order dynamics into a Kalman filter whose state includes the complex components of z(t)
- Combine this with a Bayesian multiple-model filter that spawns a new tracking loop whenever a data bit is uncertain. Prune loops at parity check.



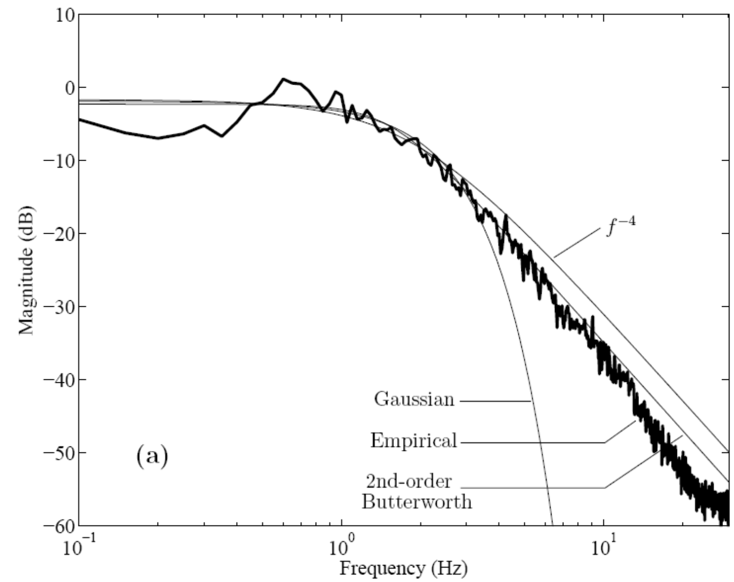
GOAL: Ts > 240 seconds for

{S_4 = 0.8, τ_0 = 0.8 sec., C/N0 = 43 dB-Hz}

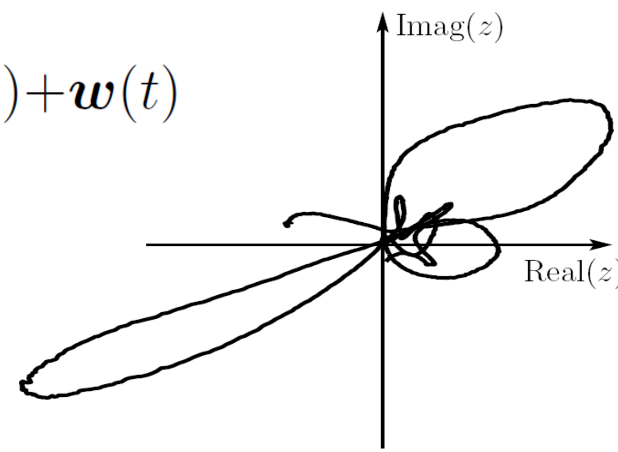
(a factor of 10 longer than current best)

A New Approach to Carrier Modeling

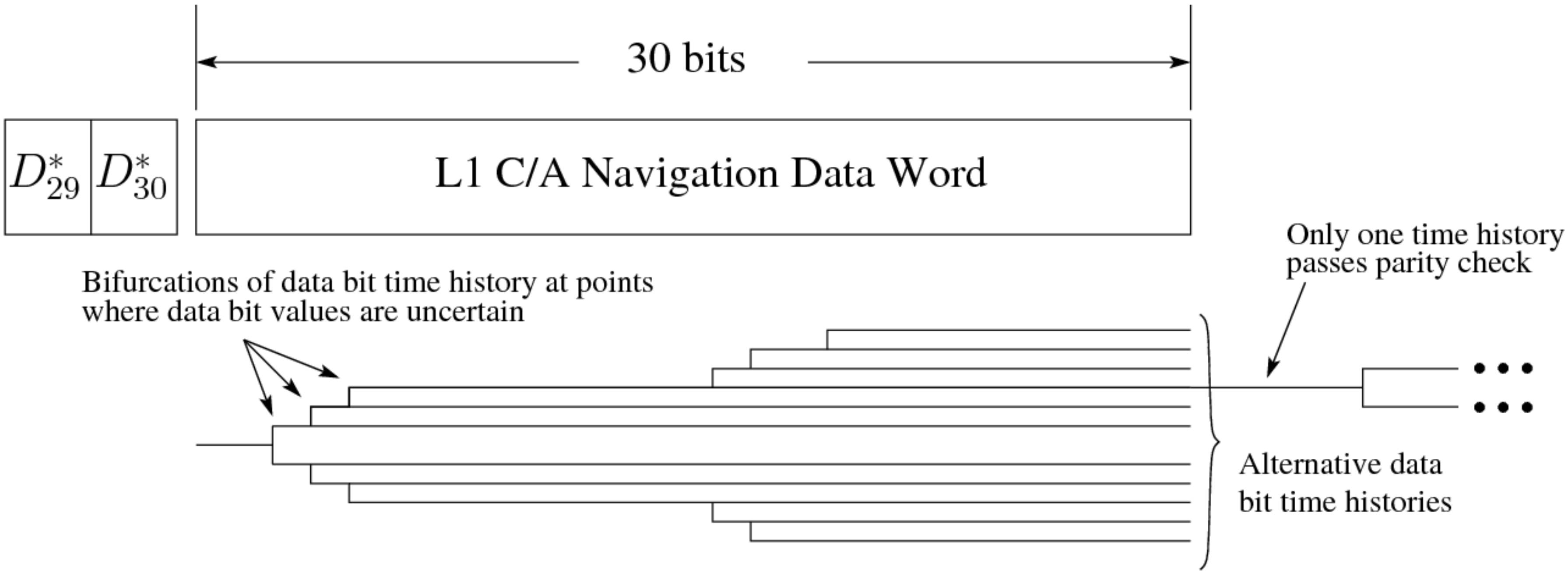
$$\boldsymbol{x} = \begin{bmatrix} I_p \\ \dot{I}_p \\ Q_p \\ \dot{Q}_p \end{bmatrix}$$



$$\begin{bmatrix} \dot{I}_p \\ \ddot{I}_p \\ \dot{Q}_p \\ \ddot{Q}_p \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} I_p \\ \dot{I}_p \\ Q_p \\ \dot{Q}_p \end{bmatrix} + \boldsymbol{f}(\omega_{NCO}) + \boldsymbol{w}(t)$$

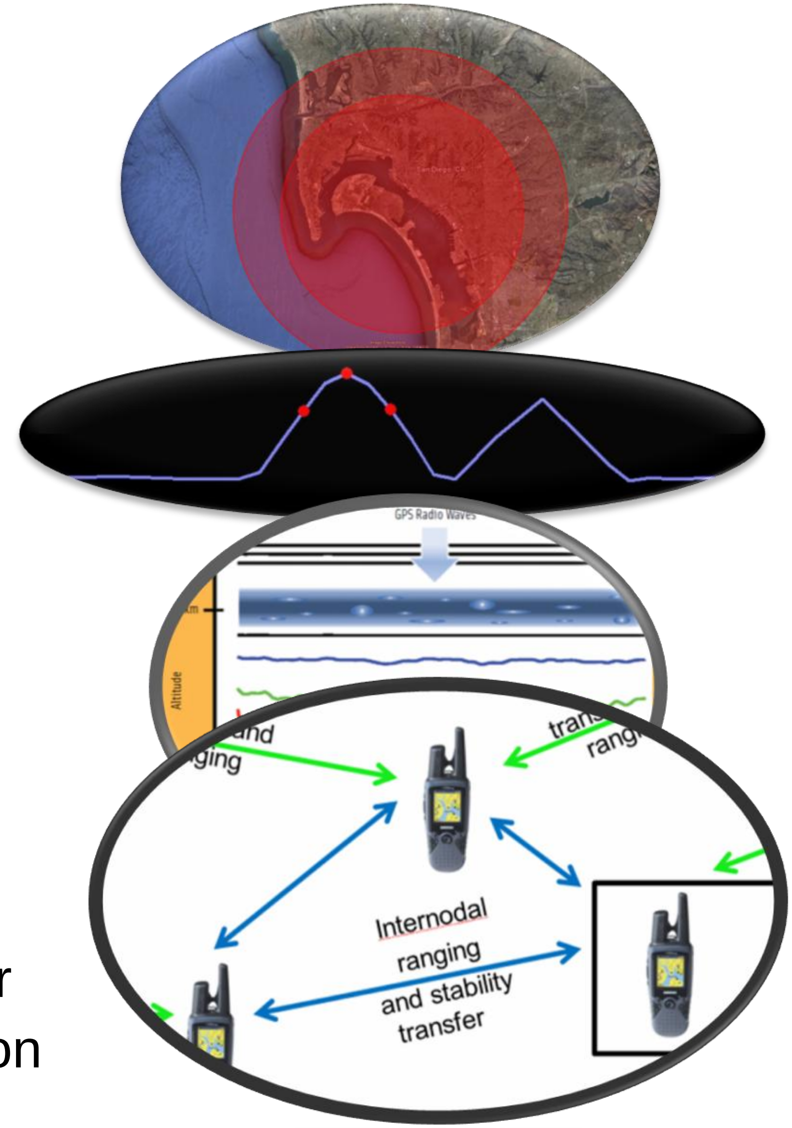


A Multiple-Model Approach to Data Bit Estimation



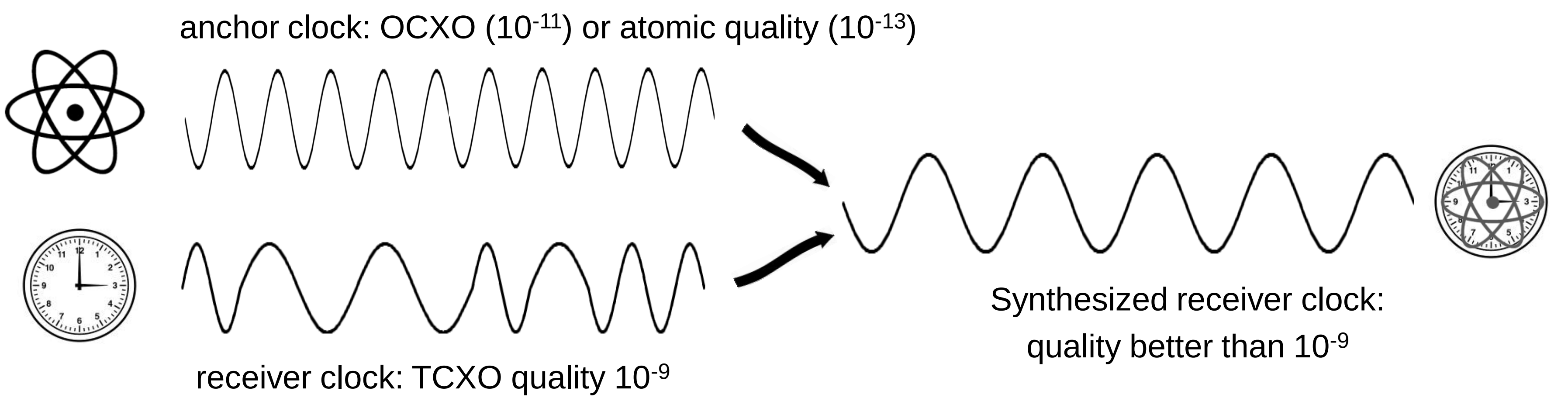
Research Agenda

- **GPS Jamming**
  - Locate jamming sources by combining data from a network of receivers
  - Develop augmentation-based defenses
- **GNSS Spoofing**
  - Characterize spoofing signatures
  - Develop receiver-autonomous defenses
  - Develop augmentation-based defenses
- **Natural GNSS Interference**
  - Improve tracking loop robustness to scintillation
- **Network-Centric Navigation**
  - Establish theory for time stability transfer
  - Opportunistic and collaborative navigation



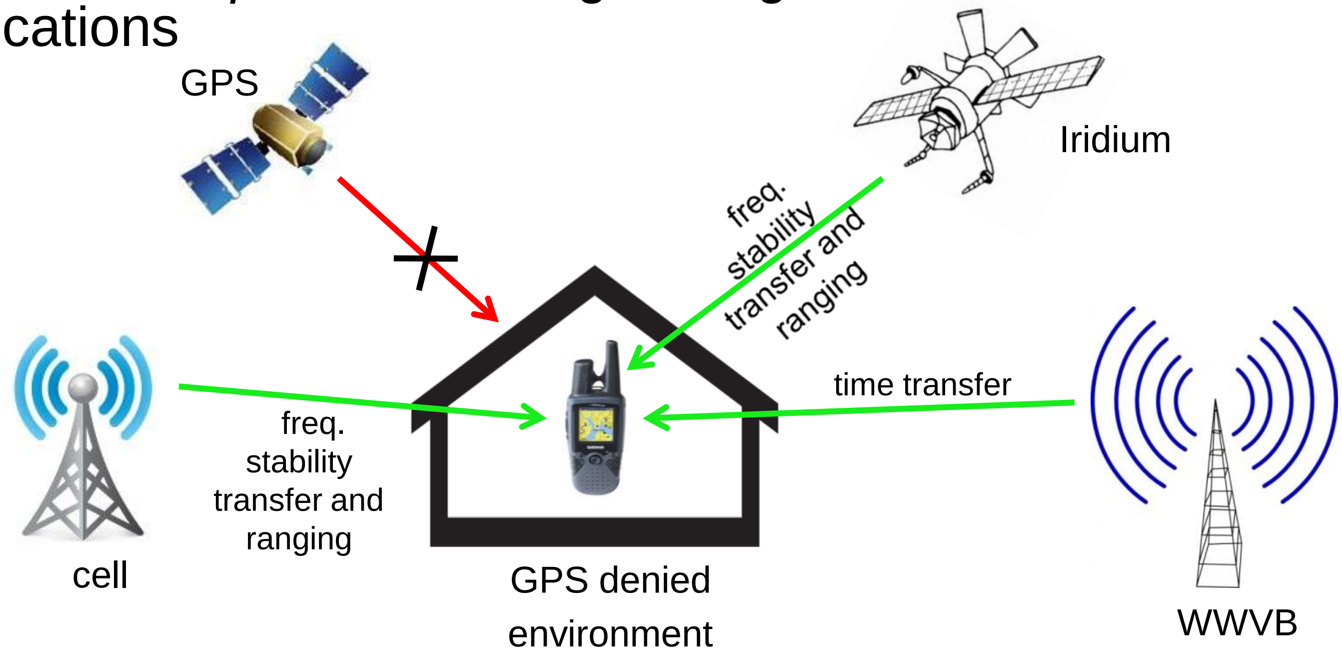
Time Stability Transfer

- Leverage the frequency stability of an "anchor" clock to extend the coherence time of an inexpensive clock
- Allow GPS RX to coherently integrate over several seconds to draw signal from noise



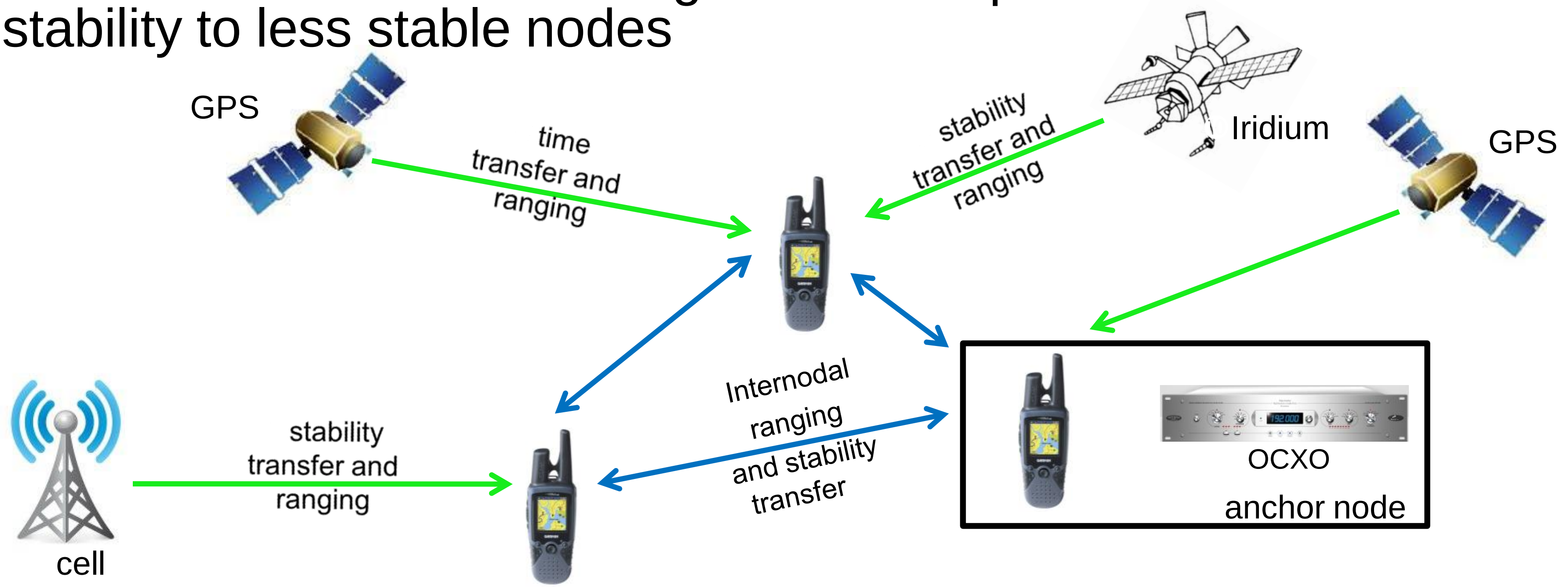
Opportunistic Navigation

- Opportunistic Frequency Stability Transfer: GPS RX clock “leans” on more stable signals of opportunity (cell transmissions, HDTV, WWVB)
- Opportunistic Ranging: Phase locks to one or more non-GPS transmission signals to maintain localization in GPS denied environments (indoors, jamming).
- RX uses *a priori* knowledge of signal standards and base station locations



Collaborative Navigation

- Create a network of GPS receivers capable of operating as GPS, Iridium and spread-spectrum transceivers
- Nodes relay GPS tracking data and range to each other
- Collective navigation solution could achieve greater accuracy than individual solutions
- “Anchor nodes” with OCXO-grade clocks provide time stability to less stable nodes



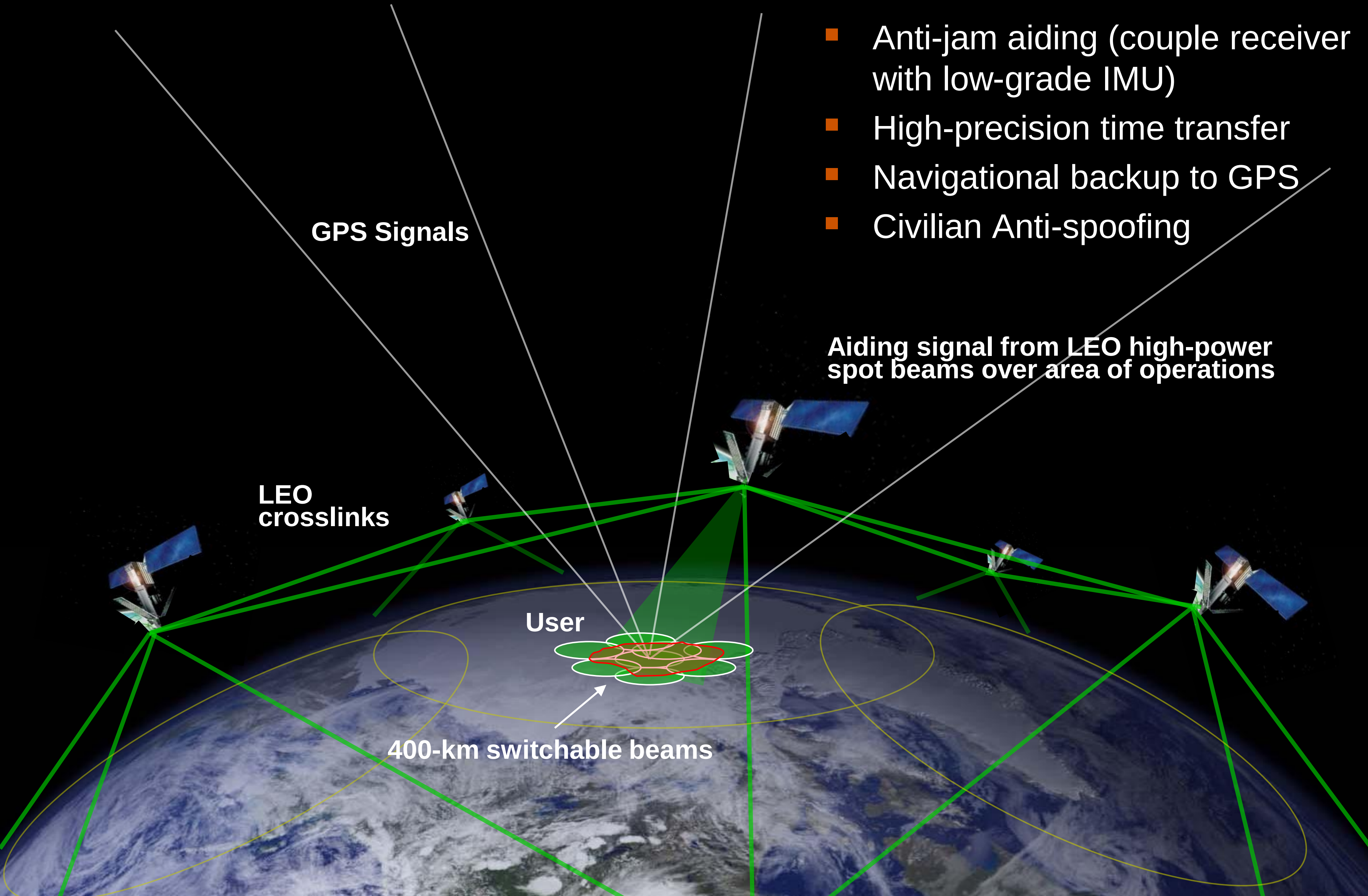
Radionavigation Lab

- Jahshan Bhatti
  - Ph.D.-track, AE
  - INTERLOC, spoofing defenses
- Muthukumar Pasupathy
  - Ph.D.-track, AE
  - Ionospheric effects on SatNav
- Kyle Wesson
  - Ph.D.-track, ECE
  - Collaborative navigation and time stability transfer
- Ken Pesyna
  - Ph.D.-track, ECE
  - Time stability transfer, cell-phone-based opportunistic navigation
- Zach Tschirhart
  - Undergraduate, AE
  - Lab manager/technician

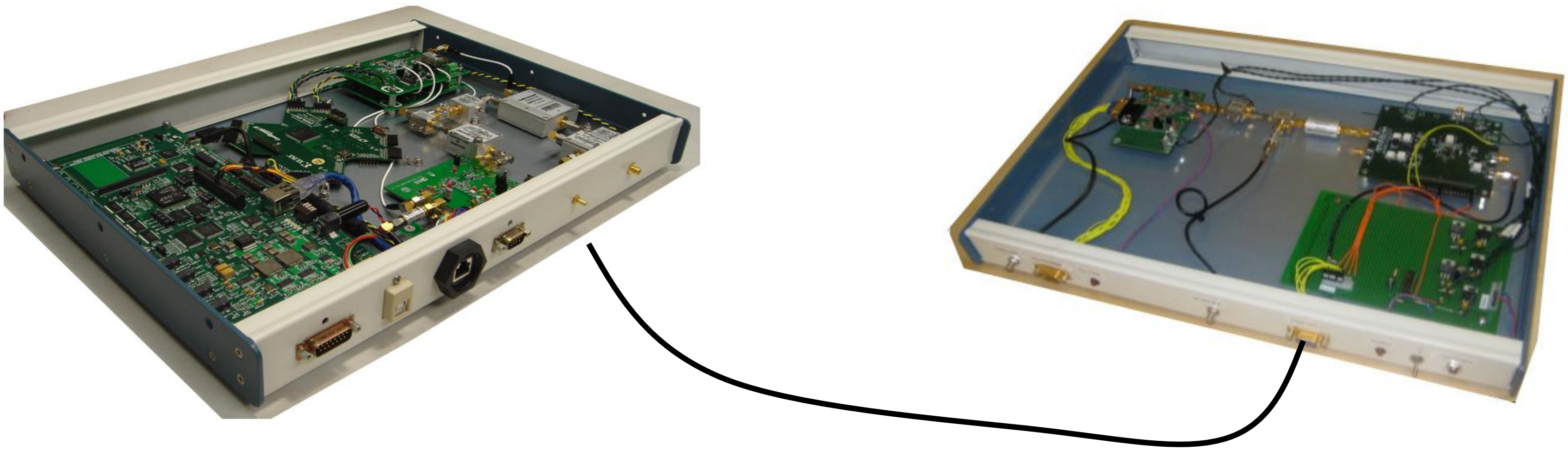
Backup Slides

Iridium-Augmented GPS

- Anti-jam aiding (couple receiver with low-grade IMU)
- High-precision time transfer
- Navigational backup to GPS
- Civilian Anti-spoofing



GPS Assimilator Prototype



- All digital signal processing implemented in C++ on a high-end DSP
- Marginal computational demands:
  - Tracking: ~1.2% of DSP per channel
  - Simulation: ~4% of DSP per channel
- Full capability:
  - 12 L1 C/A & 10 L2C tracking channels
  - 8 L1 C/A simulation channels
  - 1 Hz navigation solution
  - Acquisition in background

Civil GPS Spoofing (cont'd)

Outside Collaboration

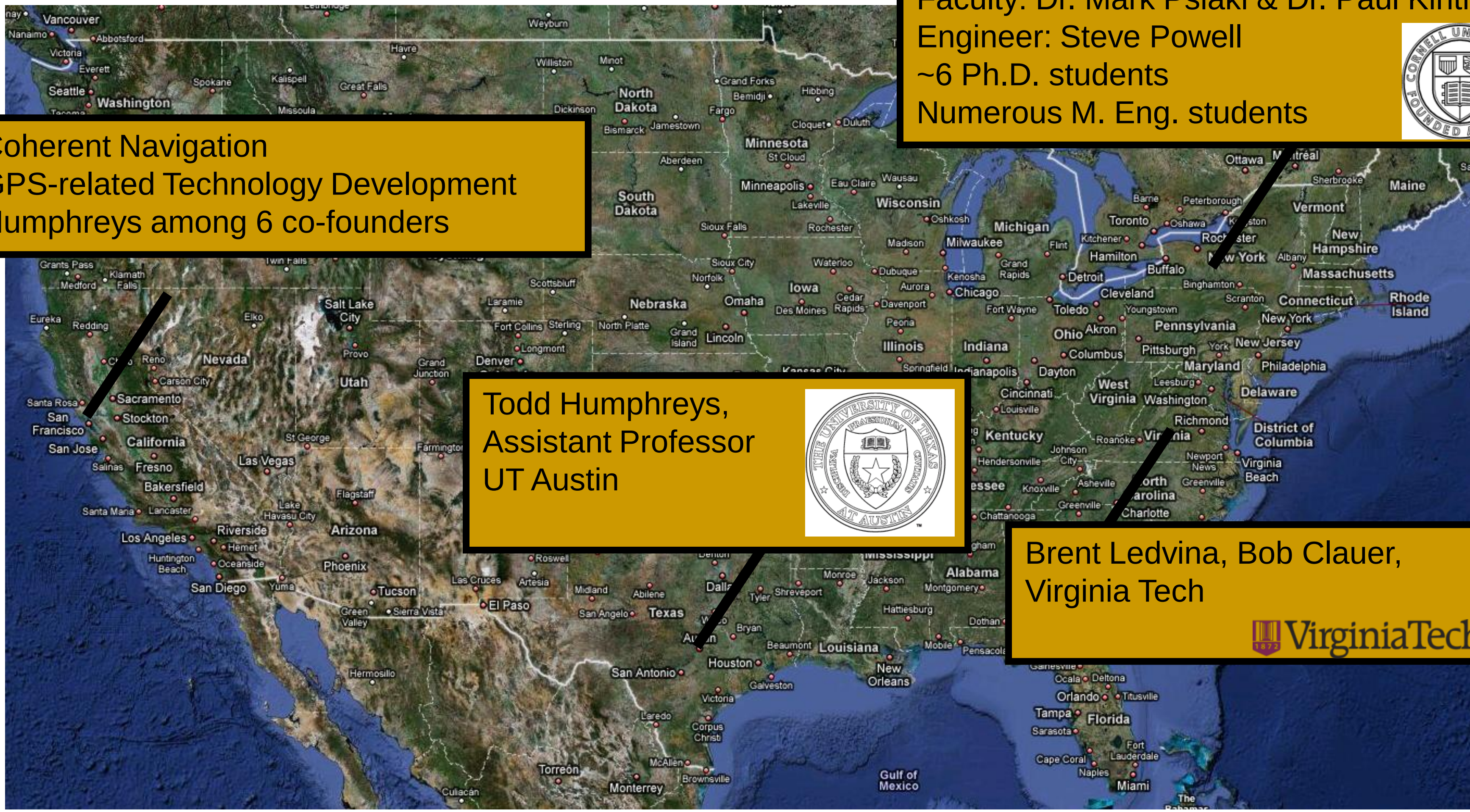
Cornell GPS Group, Ithaca NY:
Faculty: Dr. Mark Psiaki & Dr. Paul Kintner
Engineer: Steve Powell
~6 Ph.D. students
Numerous M. Eng. students

Coherent Navigation
GPS-related Technology Development
Humphreys among 6 co-founders

Todd Humphreys,
Assistant Professor
UT Austin

Brent Ledvina, Bob Clauer,
Virginia Tech

VirginiaTech



THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

THE UNIVERSITY OF TEXAS AT AUSTIN
WHAT STARTS HERE CHANGES THE WORLD

Cockrell School
THE UNIVERSITY OF TEXAS AT AUSTIN
Aerospace Engineering and Engineering Mechanics

Who is Interested in our Work?

- Scintillation-robust software GPS receivers
  - ASTRA (Atmospheric and Space Technology Research Associates LLC)
  - National Science Foundation
- Spoofing characterization and defenses
  - Joint Research Centre, European Commission
  - Office of the Secretary of Defense
  - GPS Wing of the Air Force
- GPS Assimilator
  - DARPA
  - Department of Homeland Security
  - Coherent Navigation