Interference Detection and Mitigation Workshop

Dr. T.D. Powell
Dr. M.A. Jeffris
Rick Hamilton
8 June 2012

Outline

- Discussion of Proposed Spectrum Protection Efforts
- Case Study: Newark Airport (EWR) Event
  - Detection
  - Analysis
  - Testing
  - More Testing
  - Even More Testing
  - Findings
- Additional IDM and Test Events
- Conclusions

Interference Detection & Mitigation (IDM) per NSPD 39

- Identify
- Analyze
- Locate
- Attribute
- Mitigate

U.S. SPACE-BASED POSITIONING, NAVIGATION, AND TIMING POLICY

December 15, 2004

FACT SHEET

The President authorized a new national policy on December 8, 2004 that establishes guidance and implementation actions for space-based positioning, navigation, and timing programs, augmentations, and activities for U.S. national and homeland security, civil, scientific, and commercial purposes. This policy supersedes Presidential Decision Directive/National Science and Technology Council-6, U.S. Global Positioning System Policy, dated March 28, 1996.

I. Scope and Definitions

This policy provides guidance for: (1) development, acquisition, operation, sustainment, and modernization of the Global Positioning System and U.S.-developed, owned and/or operated systems used to augment or otherwise improve the Global Positioning System and/or other space-based positioning, navigation, and timing signals; (2) development, deployment, sustainment, and modernization of capabilities to protect U.S. and allied access to and use of the Global Positioning System for national, homeland, and economic security, and to deny adversaries access to any space-based positioning, navigation, and timing services; and (3) foreign access to the Global Positioning System and United States Government augmentations, and international cooperation with foreign space-based positioning, navigation, and timing services, including augmentations.

For purposes of this document:

- "Interoperable" refers to the ability of civil U.S. and foreign space-based positioning, navigation, and timing services to be used together to provide better capabilities at the user level than would be achieved by relying solely on one service or signal;
- "Compatible" refers to the ability of U.S. and foreign space-based positioning, navigation, and timing services to be used separately or together without interfering with each individual service or signal, and without adversely affecting navigation warfare; and
- "Augmentation" refers to space and/or ground-based systems that provide users of space-based positioning, navigation, and timing signals with additional information that enables

- Maintain the Global Positioning System as a component of multiple sectors of the U.S. Critical Infrastructure, consistent with Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003;
- Encourage foreign development of positioning, navigation, and timing services and systems based on the Global Positioning System. Seek to ensure that foreign space-based positioning, navigation, and timing services are interoperable with the civil services of the Global Positioning System, and that operations in civil, commercial, and scientific users worldwide;
- Ensure that the utility of civil services exceeds, or is at least equivalent to, those routinely provided by foreign space-based positioning, navigation, and timing services;
- Promote plans to modernize the U.S. space-based positioning, navigation, and timing infrastructure, including: (1) development, deployment, and operation of new and/or

Existing and Emerging Threats

1,978,000 hits on “GPS Jammer”

Critical Infrastructure Key Resource Sectors (CIKR)


Agriculture and Food


Banking and Finance *


Chemical


Commercial Facilities


Communications *


Critical Manufacturing


Dams


Defense Industrial Base


Emergency Services


Energy *


Government Facilities


Healthcare and Public Health


Information Technology *


National Monuments and Icons

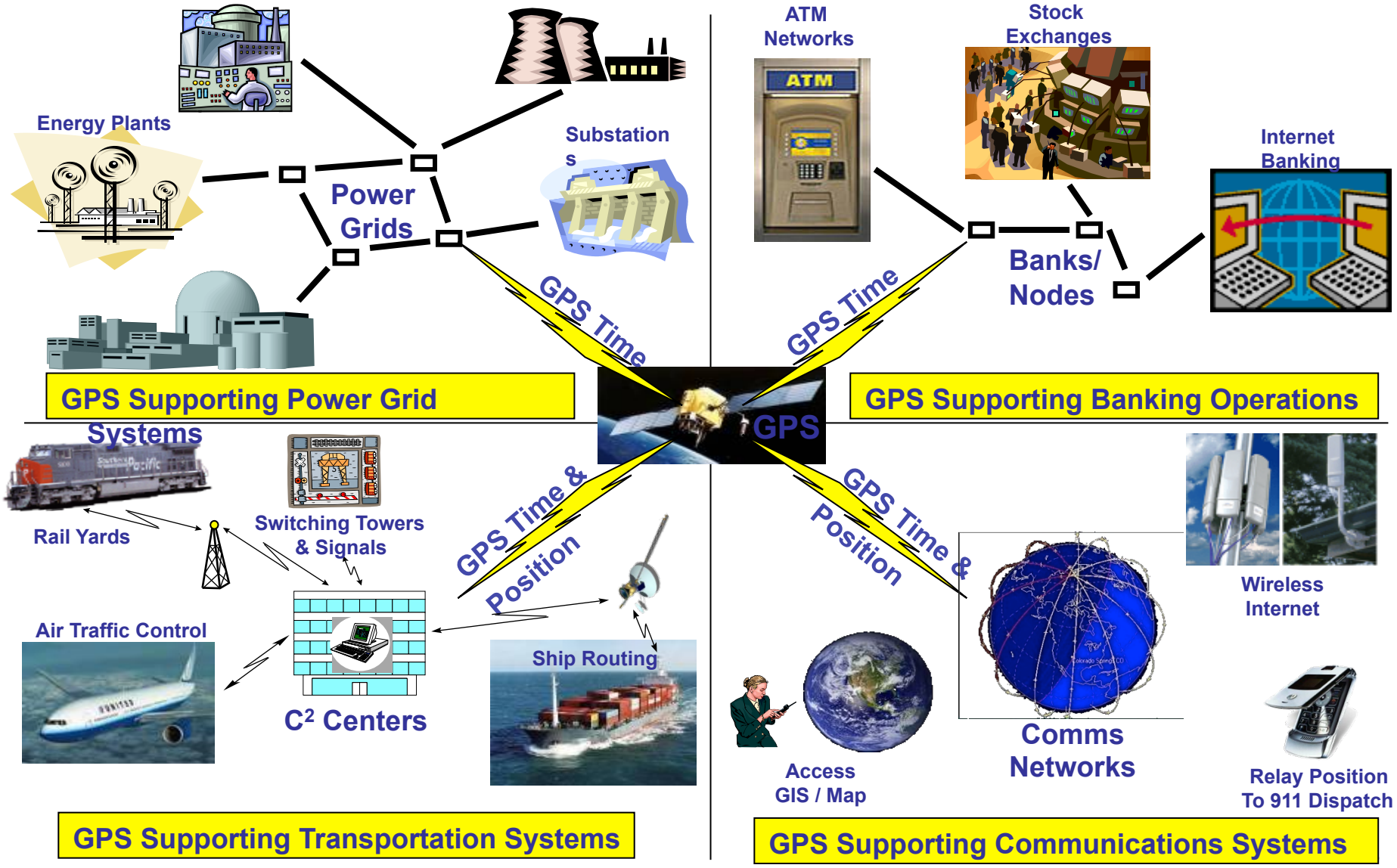

Nuclear Reactors, Materials and Waste


Postal and Shipping


Transportation Systems


Water

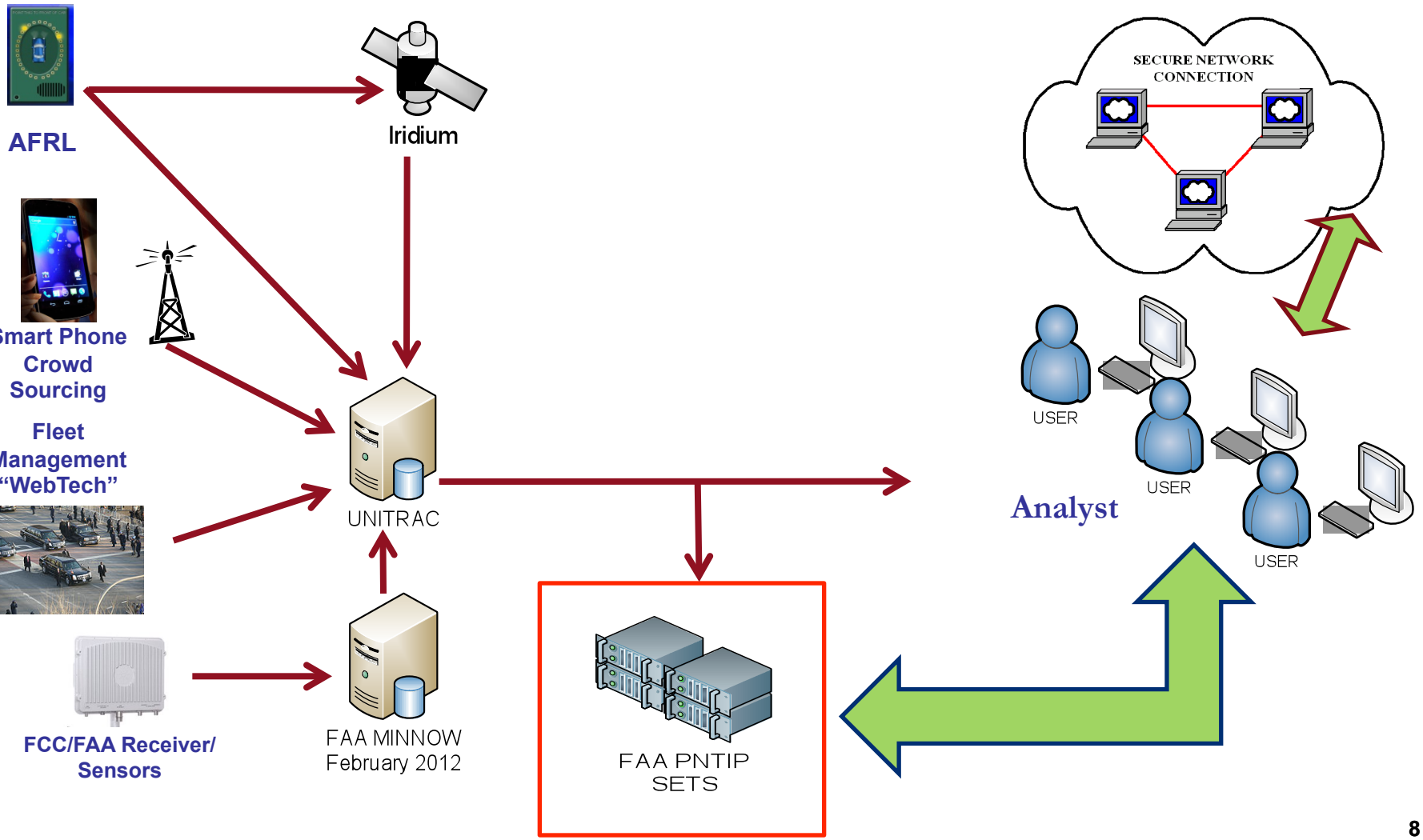
Extent of GPS Dependencies



U.S. Initiative

- **Protect the Nation's 18 Critical Infrastructure & Key Resource Sectors (CIKR)**
- **System-of-Systems, Open Architecture, Multi-Phased/Multi-Layered Approach**
- **Near Real-Time Situational Awareness of Position Navigation and Timing (PNT) Interference**
  - **Leverage Existing mature capabilities & focus on the data, less on system/device**
  - **Common Data Structure for Information Sharing**
  - **Persistent Monitoring for Situational Awareness**

Proposed Architecture



Outline

- Discussion of Proposed Spectrum Protection Efforts
- Case Study: Newark Airport (EWR) Event
  - Detection
  - Analysis
  - Testing
  - More Testing
  - Even More Testing
  - Findings
- Additional IDM and Test Events
- Conclusions

The Threat

- GPS Privacy Jammers
  - Marketed to consumers
    - Honest people who fear the loss of privacy
    - Criminals / dishonest people who want to evade law enforcement, employers, etc …
  - Power: milliwatts to watts
    - Many devices are battery powered
  - Effective Radius:
    - Advertised: meters to tens of meters
    - Potentially 100s to 1000s of meters
  - Cost: $25 to $300 USD
- During the week of April 26, 2010
  - Commuter on NJ Turnpike was found by the FAA/FCC with GPS Privacy Jammer


FOX NEWS .com Fair & Balanced

Search

Full Coverage | Private Property Rights | Job Hunt | Road to Recovery

Watch Live | Shuttle Discovery | Energy Conference

GPS Jammers Illegal, Dangerous, and Very Easy to Buy

By John Brandon - FOXNews.com

An electronic device small enough to fit in a shirt pocket and big enough to conceivably bring down an airplane can be easily purchased over the Internet. All a terrorist needs is a credit card and $49.

PRINT | EMAIL | SHARE | RECOMMEND (5) | AAA

Despite being illegal and potentially dangerous, GPS jammers like this model (designed to fit a car cigarette lighter) are cheap and readily available online.

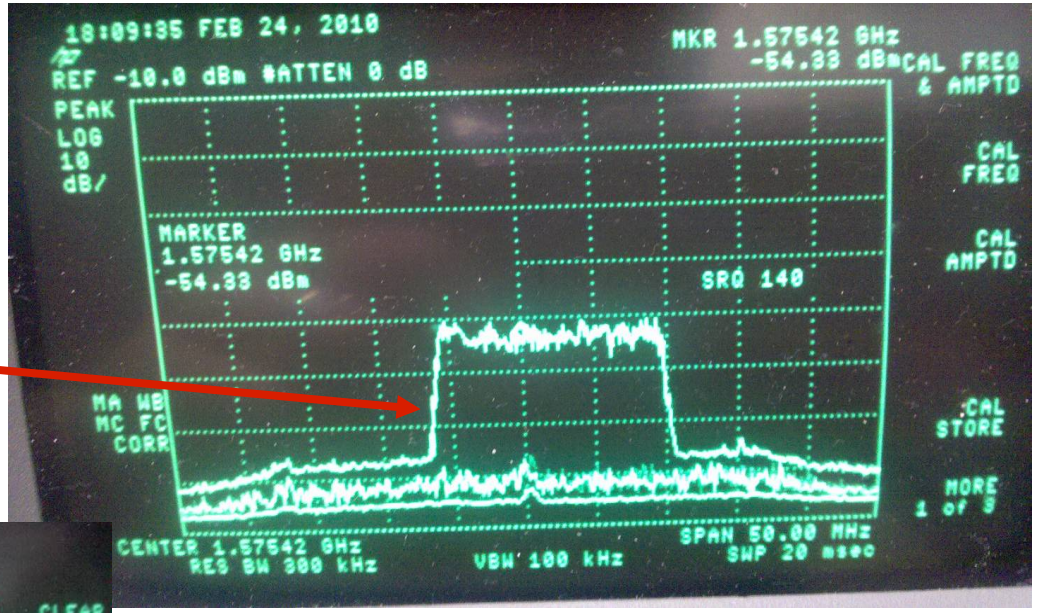
With car thieves in the United Kingdom using GPS jammers to aid their getaways, experts say it's only a matter of time until crooks -- and, ominously, terrorists -- in the United States catch on.

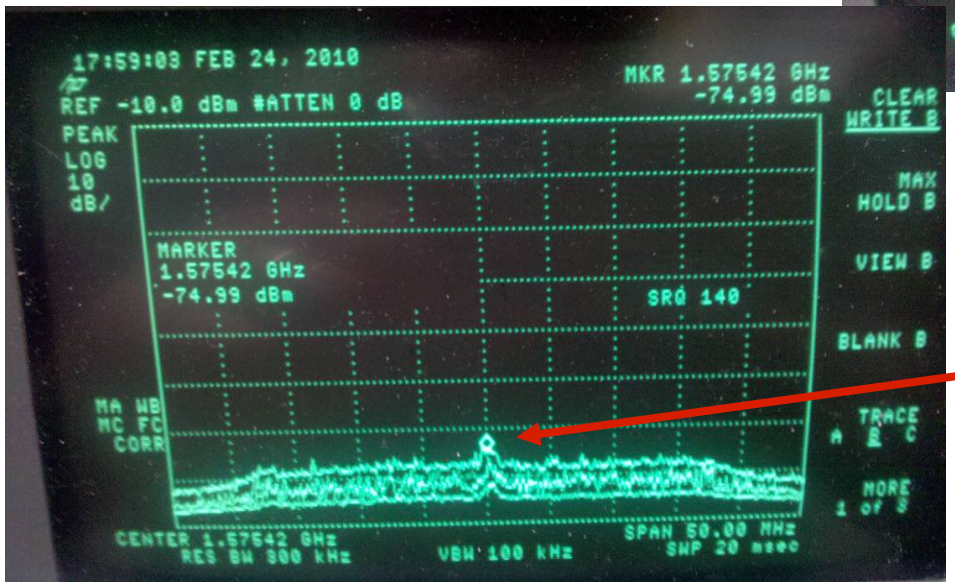
Jammers transmit a low-power signal that creates signal noise and fools a GPS receiver into thinking the satellites are not available. They can be used to confuse police and avoid toll charges, and some pranksters

Device Found at EWR

FAA Spectrum Measurements

- Wideband Intermittent Source detected in December 2011 occupying approx – 20 MHz
- 5 MHz below and 15 MHz above L1.





- Normal L1 Pass Band Spectrum when Interference Source is Not Present.

FAA Minnow System

- November 23, 2009 during initial SLS-4000 stability testing the Station Faulted and Reference Receiver Satellite Tracking was Interrupted.

SLS-4000 Components

GPS Antenna (RRA)
- Multipath Limiting design
- Sharp cutoff/rejection at horizon

GPS Receiver (RSMU)
- 48-channel, L1 C/A GPS
- Signal Deformation Monitoring (SDM) capable

Processor HW (DCP)
- Pentium M, 1.8 GHz CPU
- Hosts integrity monitoring software

Processor SW (DCP)
- Real time monitoring for GPS failure modes, local error sources
- Differential correction determination
- User interface via Maintenance Data Terminal

VHF Radios (VDB)
- D8PSK modulation, TDMA
- Nav band, 108-118 MHz

VHF Antenna
- Horizontal (HPOL) or Elliptical (EPOL) polarized signal

DCP: Differential Correction Processor
RPDP: Robust Power Distribution Panle
VHF: Very High Frequency
VDB: VHF Data Broadcast
HW: Hardware
RRA: Reference Receiver Antenna
RSMU: Remote Satellite Measurement Unit

FAA / FCC Investigation

- **Government and Contractor Teams convened in Newark on February 24 – 26, 2010 in an attempt to locate the direction toward the source of the observed interference events.**
- **The Teams on site for the first time had a "Learning Curve" experience and effective data could not be obtained.**
  - **Three (3) Radio Frequency Interference (RFI) events were observed and measured, but not by all on-site teams.**
- **The same Teams participated again during March 22 – 25, 2010 in an attempt to draw accurate and more conclusive simultaneous lines of bearing.**
  - **Measurements and data analysis reveal interference source was MOBILE at slow and fast rates.**

Testing Summary

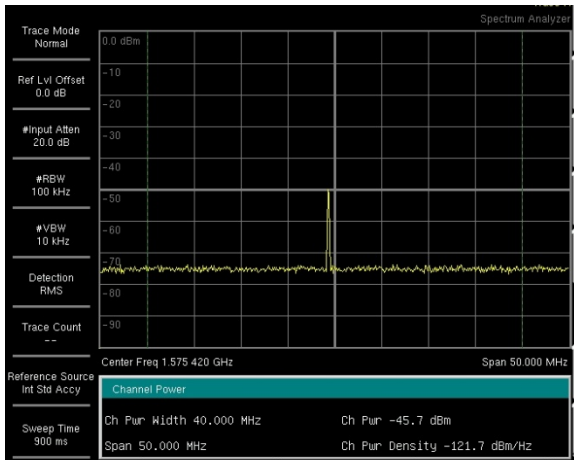
- Jammer Characterization
  - Attempt to build library of jammer signatures
  - Testing is ongoing
- EWR Field Test #1
  - Overview
    - Single Sensor
    - C/N_0 sensors placed on ground
  - Successes
    - Proved sensor could detect the threat
  - Lessons Learned:
    - C/N_0 sensors of limited use when placed on the ground
    - Coordination among stakeholders critical
- EWR Field Test #2
  - Overview
    - Dual sensors
    - Repositioned C/N_0 sensors above ground
    - Utilized MITRE built data to capture interference time series
    - Automated spectral recording w
  - Successes
    - Sensors again successfully detected interference and data implies a moving interferer
    - C/N_0 sensor data conclusively shows moving interference

Jammer Characterization

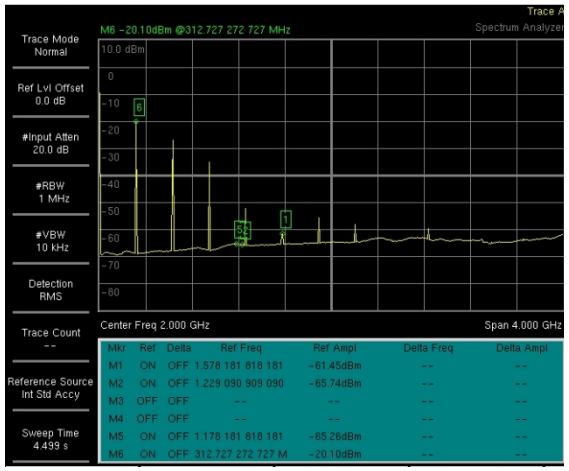
- MITRE purchased 12 GPS privacy jammers for signal characterization
- Results:
  - Very dirty outside the intended GPS bands thus capable of causing additional, collateral damage
  - Testing of EP5000 jammer similar to EWR jammer reveals an L1 tone jammer
    - Other broadband jamming waveforms observed at EWR
    - Most likely indicates there are more jammers out there

GP5000 Power Spectra

GPS L1



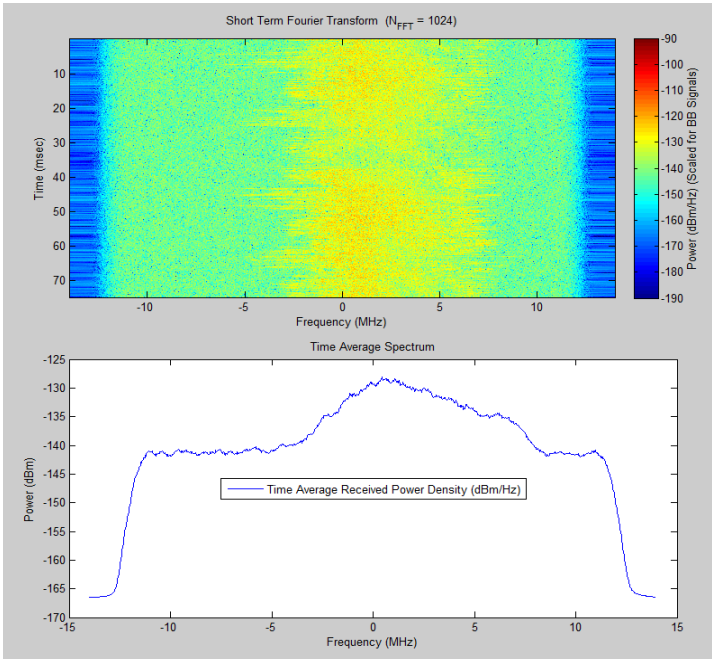
0-4 GHz

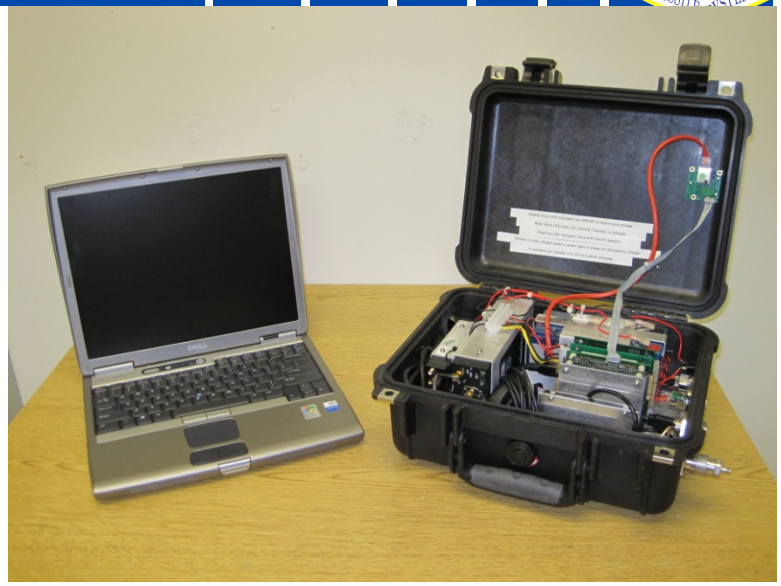


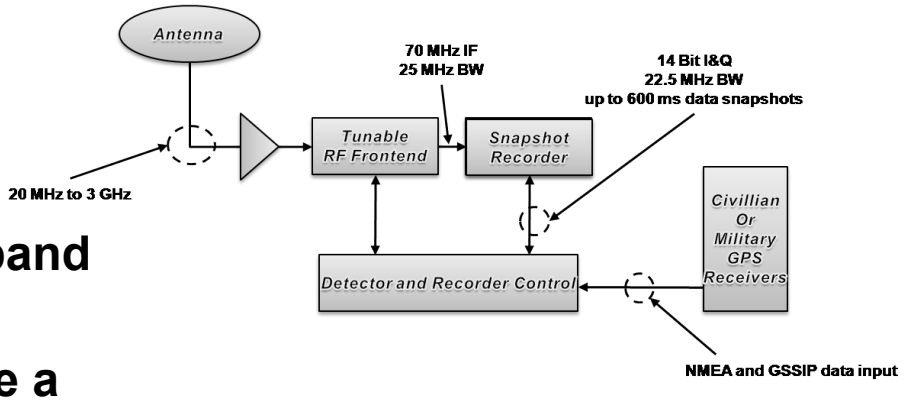
15

Data Recording

- Automatic detection of interference*
- MATLAB analysis toolbox







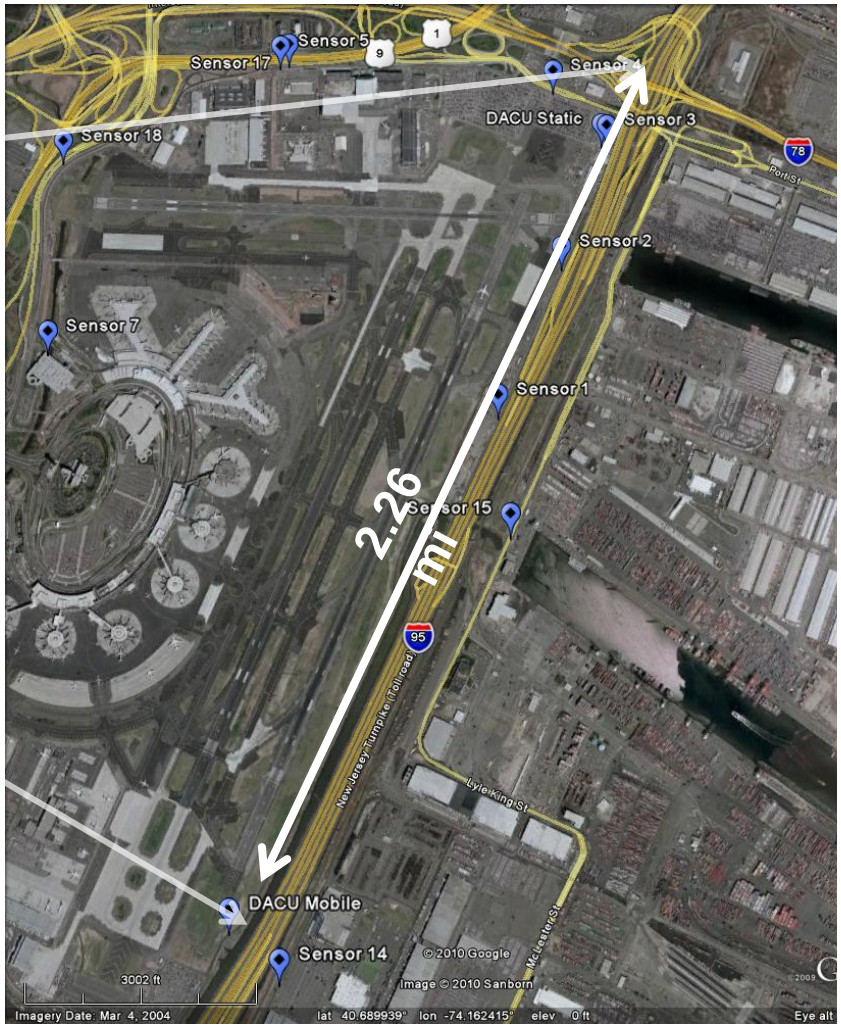
- Data from 24 Mar 2010 shows wideband modulation
- Data hopefully can be used to derive a "signature" for the jammer

Note: automatic detection mode not used at EWR

Dual Sensor Laydown

Static Sensor

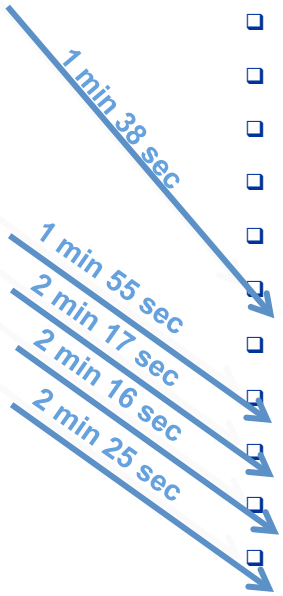
Mobile Sensor



Testing Results

Static DACU

Hit Times	Duration (sec)
25-Mar-2010 11:55:34	4
25-Mar-2010 18:53:42	4
25-Mar-2010 18:59:51	7
25-Mar-2010 19:05:47	7
25-Mar-2010 19:13:28	5
25-Mar-2010 19:21:44	7
25-Mar-2010 20:10:48	4
25-Mar-2010 20:30:07	7
25-Mar-2010 21:16:08	22
25-Mar-2010 21:24:07	8
25-Mar-2010 21:37:03	4
25-Mar-2010 21:43:23	10



Mobile DACU

Hit Times	Duration (sec)
25-Mar-2010 11:47:51	7
25-Mar-2010 12:08:46	6
25-Mar-2010 13:21:09	4
25-Mar-2010 14:46:47	3
25-Mar-2010 14:47:52	3
25-Mar-2010 15:16:22	10
25-Mar-2010 15:21:39	3
25-Mar-2010 18:30:24	3
25-Mar-2010 19:01:29	9
25-Mar-2010 19:03:05	6
25-Mar-2010 20:12:43	3
25-Mar-2010 20:32:24	3
25-Mar-2010 21:18:23	3
25-Mar-2010 21:26:32	10

Correlated but non-coincident times imply a moving interferer

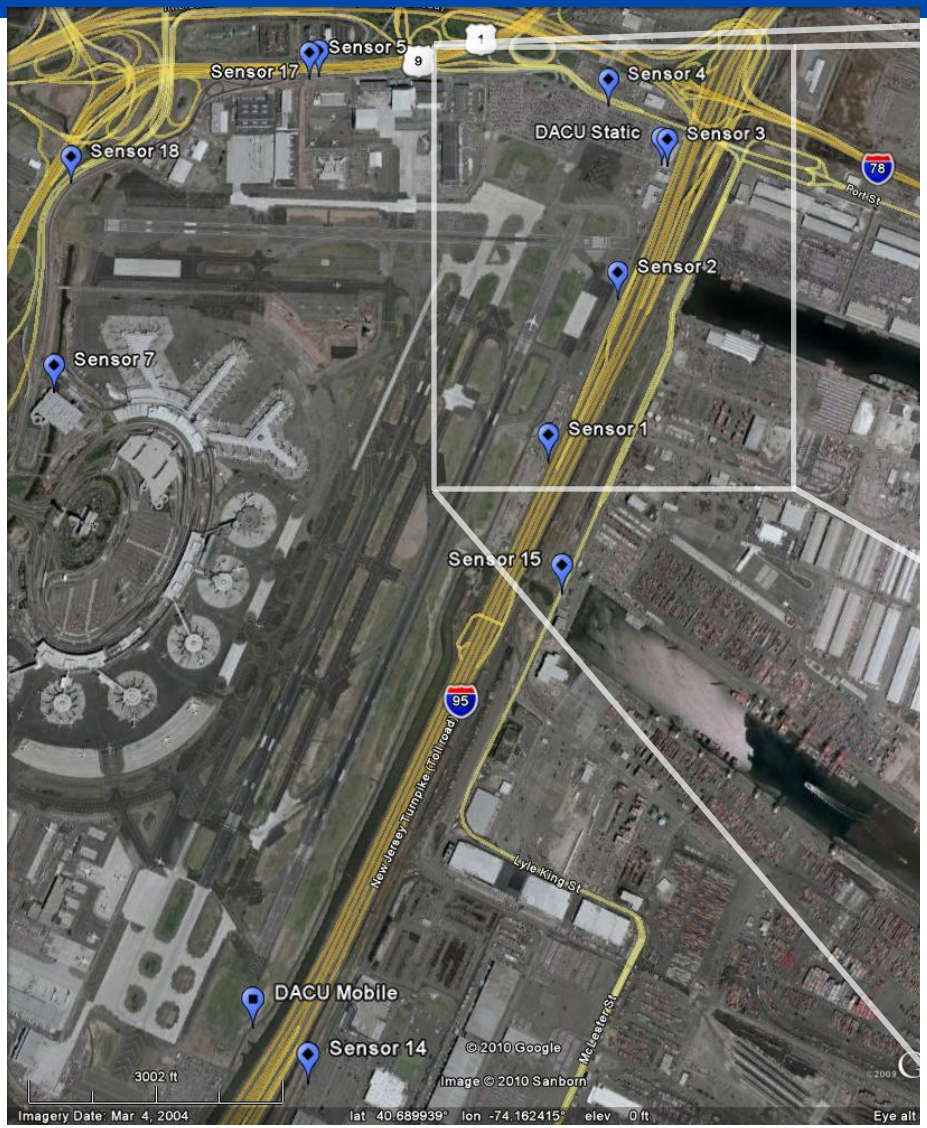
18

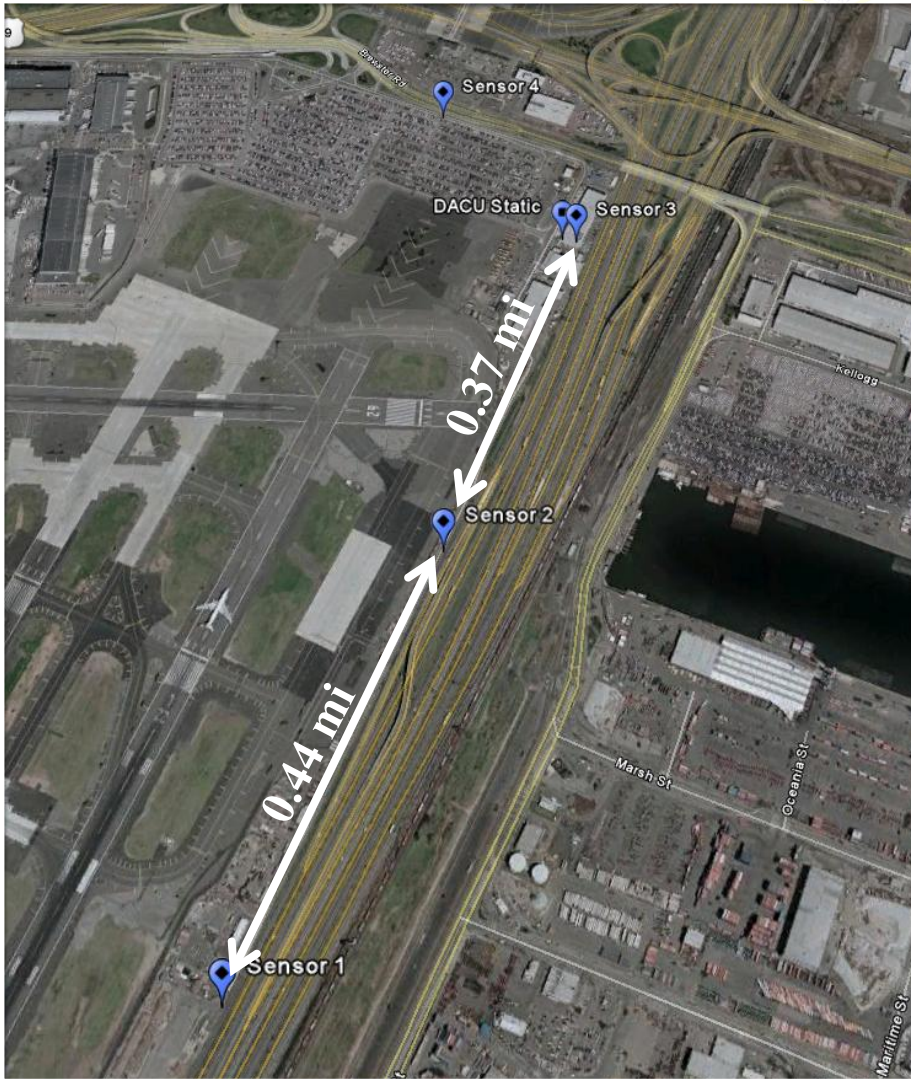
C/N0 Sensor

- Qstarz Q-1000X
  - Affordable, high performance &
    low SWaP integrated GPS receiver plus data logger
  - GPS Receiver
    - 66 Channel, high sensitivity, AGPS
  - Data Logger
    - Records PVT, C/N_0 and more
    - Export to NMEA, CSV, Google Earth
    - 7 hour capacity at 1 Hz
  - Low SWaP
    - 72 x45 x 20 mm
    - 0.3 Ounces
    - Rechargeable battery rated for up to 42 hrs
  - Cost : $100 (amazon.com)

19

C/N_0 Sensor: Laydown

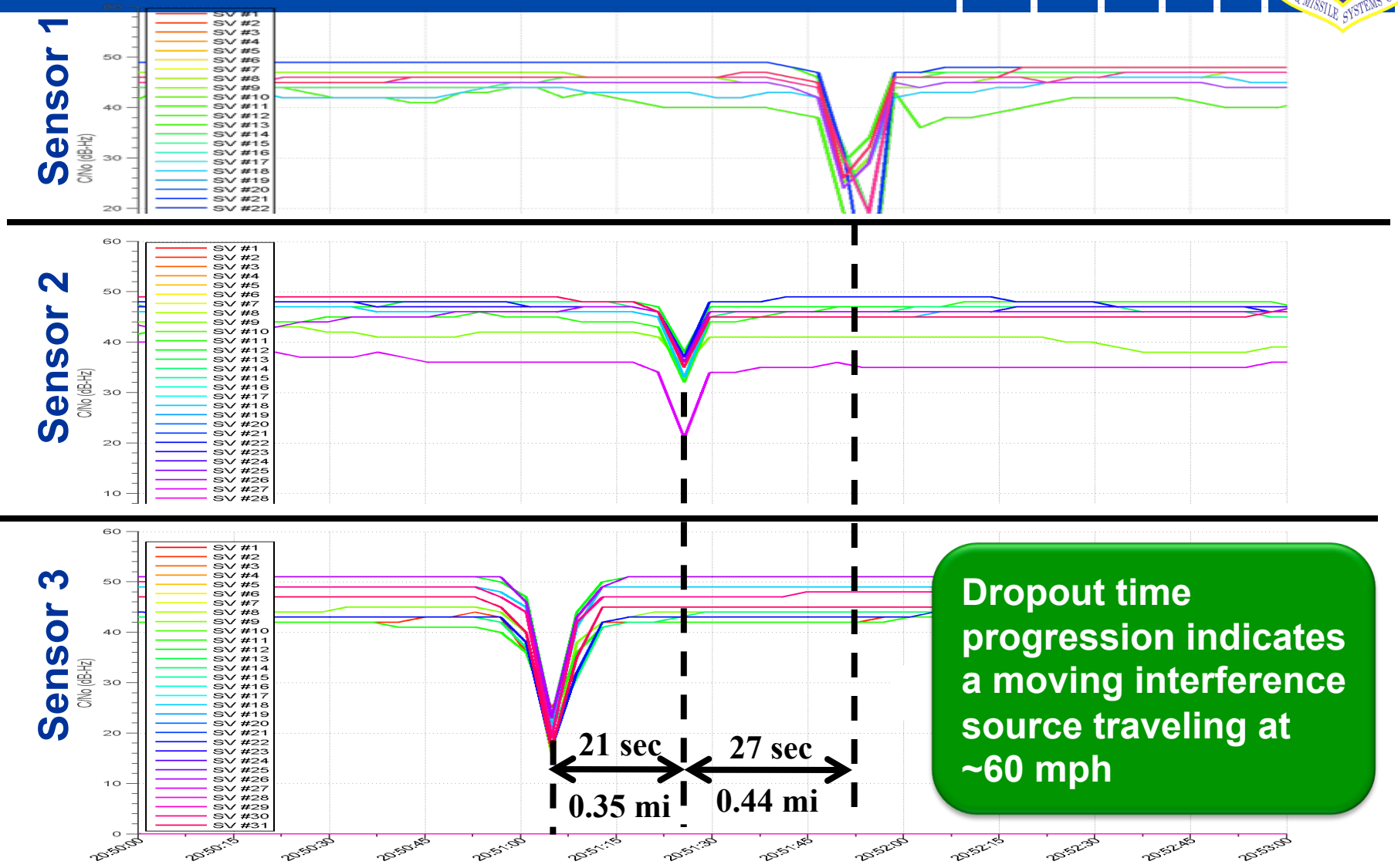




20

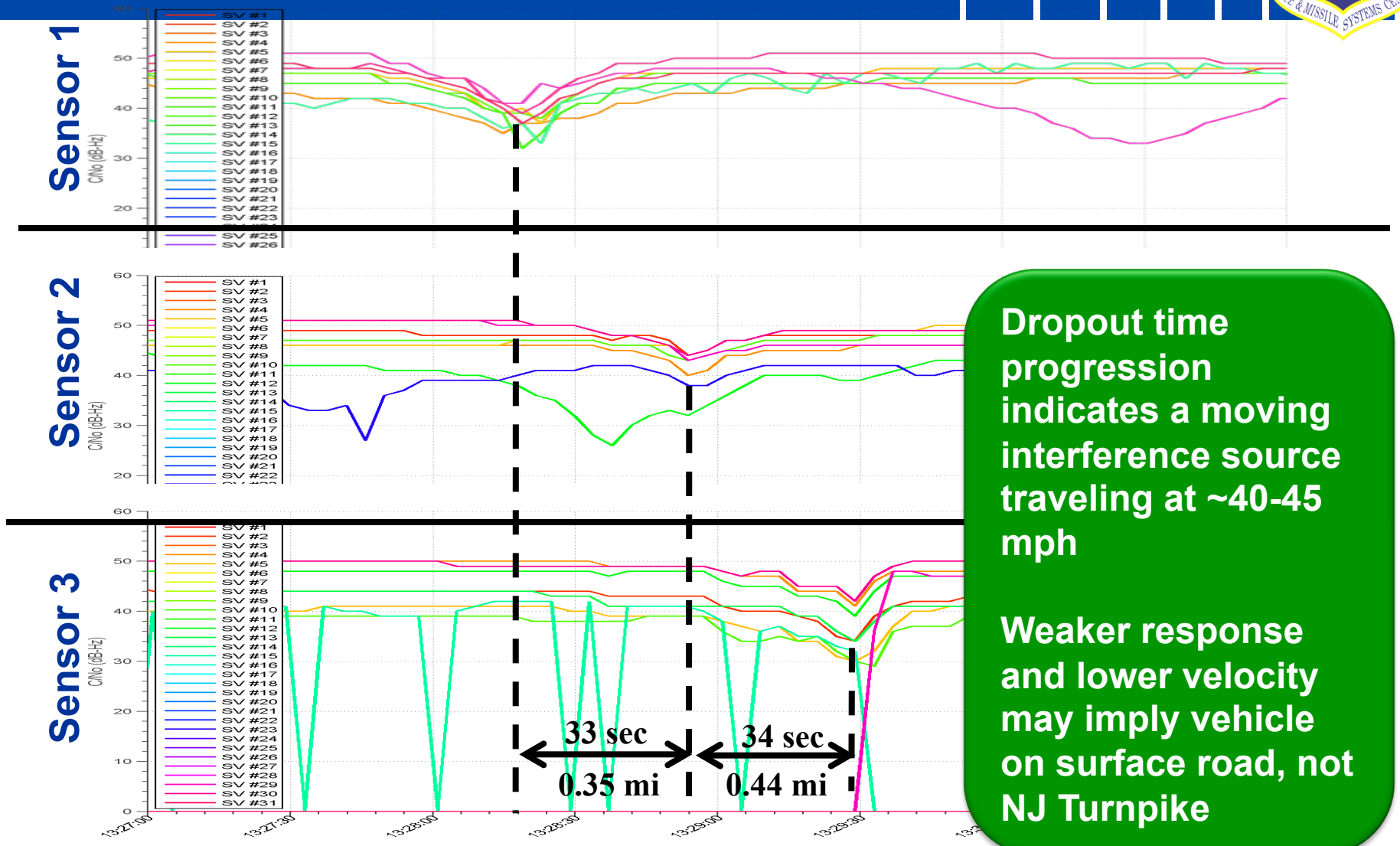
Analytical Pattern

C/N_0 Sensor: Results: Wednesday 23 Mar 2010, 20:51:00 GMT



22

C/N_0 Sensor: Results: Wednesday 23 Mar 2010, 13:28:00 GMT

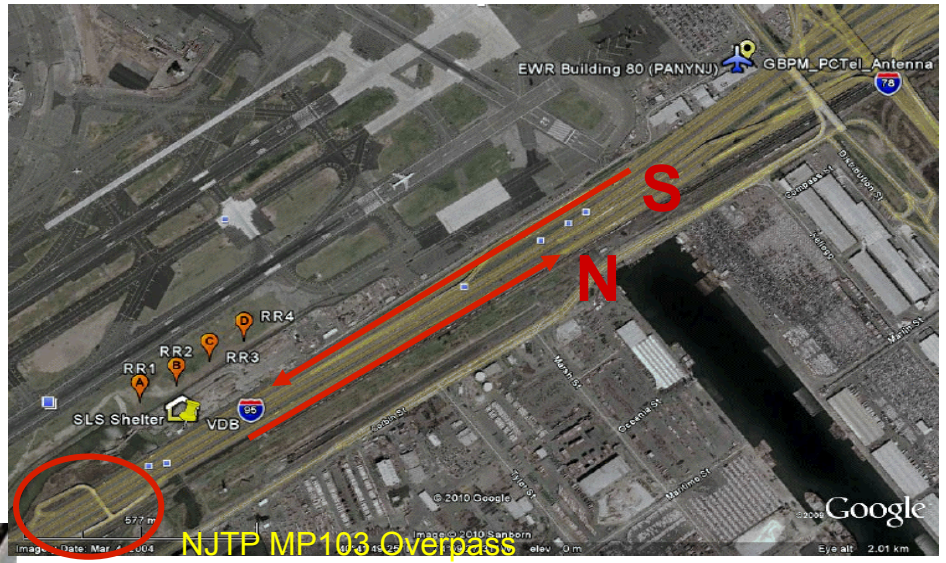


Dropout time progression indicates a moving interference source traveling at ~40-45 mph

Weaker response and lower velocity may imply vehicle on surface road, not NJ Turnpike

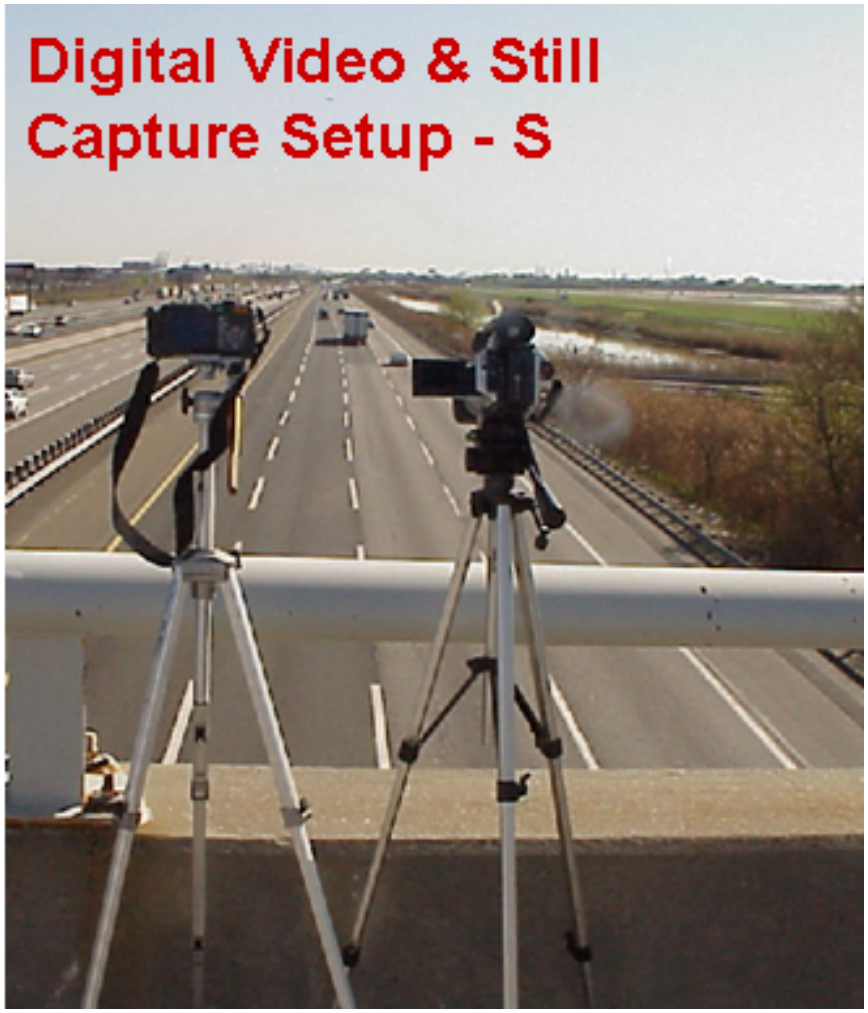
23

New Jersey Turnpike Overpass Point

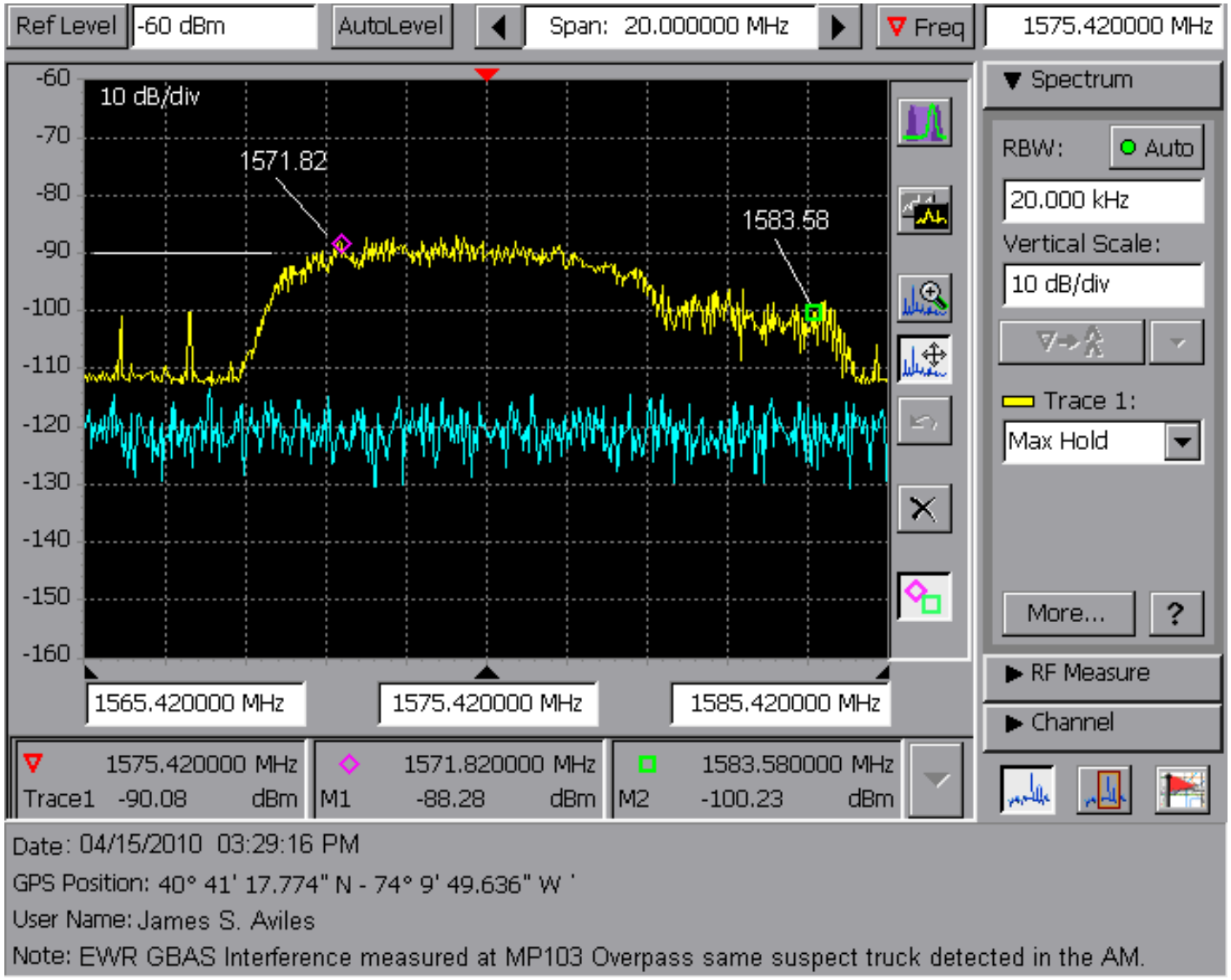


NJTP MP103 Overpass

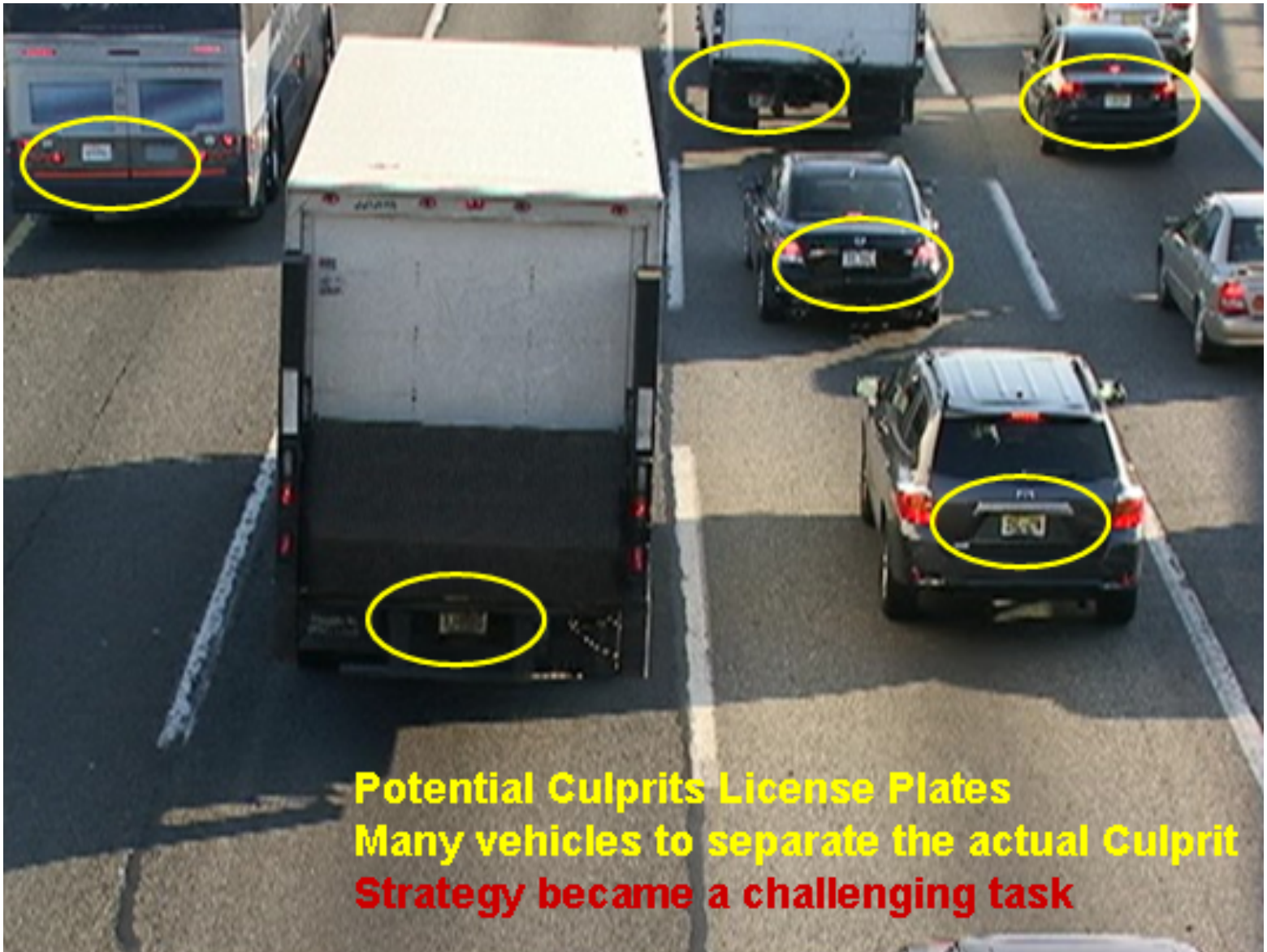
Equipment Capture Setup



Sample Measured Data



Difficulties



Another Strategy: Closer Observation

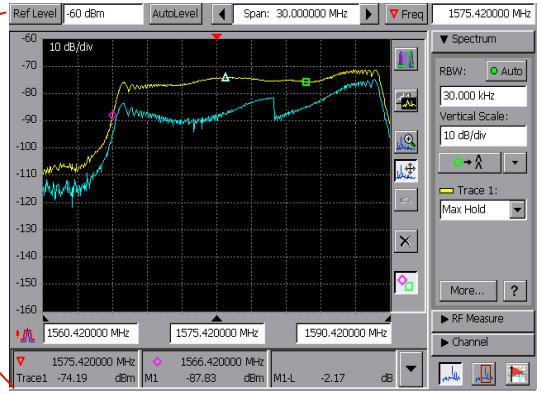
Implementation Reality: Traffic

Interference: Hot Pursuit

FCC Equipment

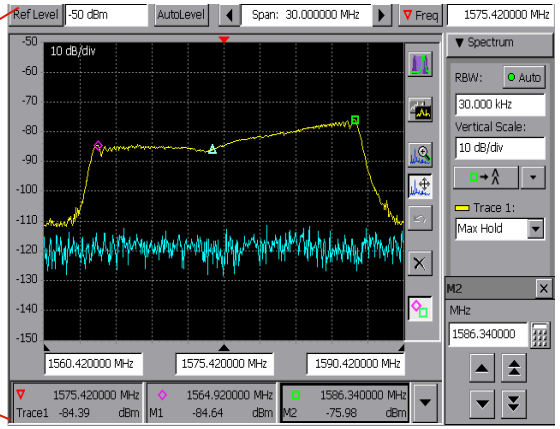
FAA Equipment

FAA “Tip OFF”



RFI source “Locked-on” and pursued until vehicle stop at traffic light further south

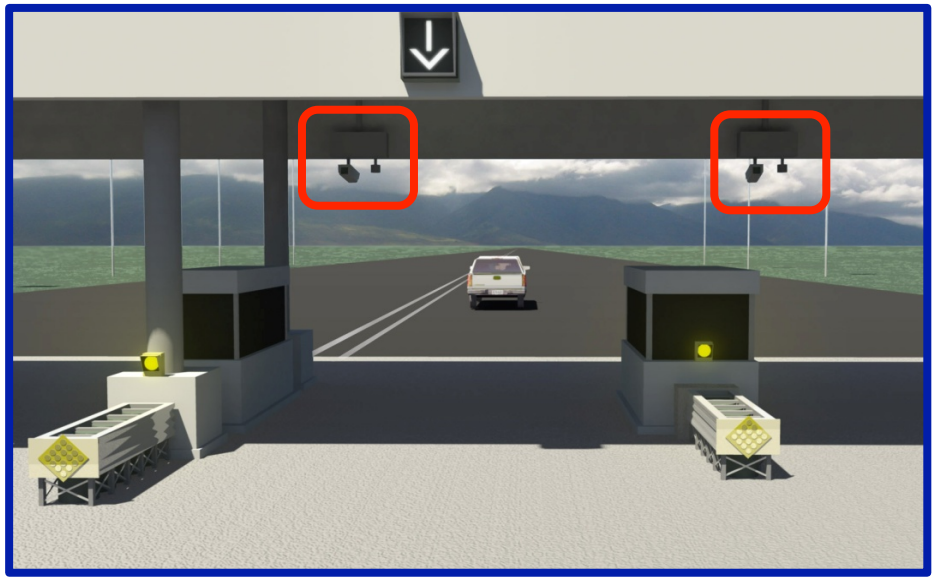
Interference Source Revealed

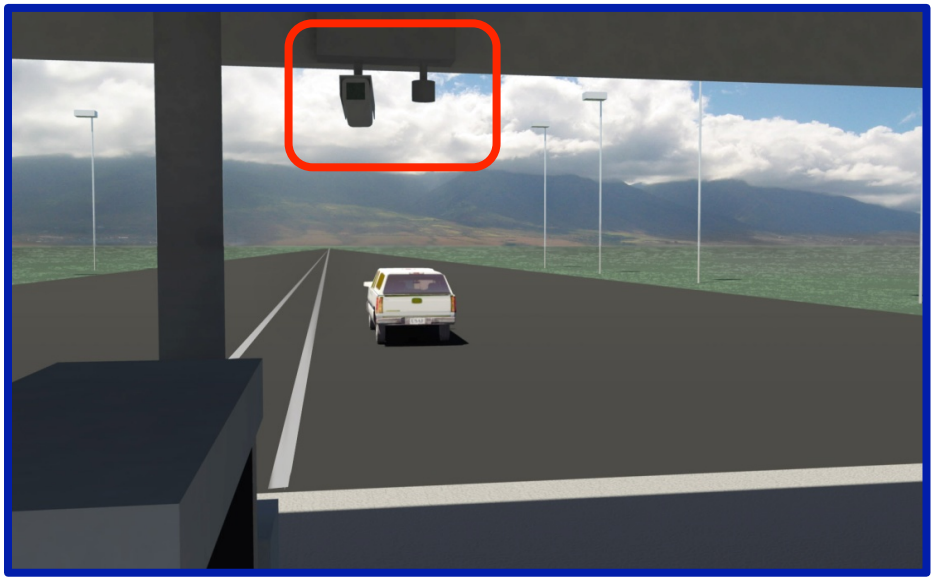


On Site ON-OFF tests confirm surrendered GPS RFI source on April 29, 2010

Period of several months to locate 1 GPS jammer!

Additional IDM Concepts





- Integrated with Camera System
- Alert Enforcement Personnel to Jammer Presence
- Detect & Track Jammers Approaching Entry Point
- Multi-Lane Distinction
- UNITRAC Database Connection

Outline

- Discussion of Proposed Spectrum Protection Efforts
- Case Study: Newark Airport (EWR) Event
  - Detection
  - Analysis
  - Testing
  - More Testing
  - Even More Testing
  - Findings
- Additional IDM and Test Events
- Conclusions

Additional Test Events

- **Civil Focus, Test/Training; June 18 – 22, 2012**
- **746th Test Squadron Support**
- **1st open air transmission using Commercial Jammers**
- **Training Opportunity**
- **Capability Testing**
- **Encourage participant collaboration**
- **Multiple scenarios, moving targets**
- **Jammer Characterizations**

PNT Collaboration Sites

Conclusions

- US is actively pursuing threat monitoring
  - Open Architecture
  - Scalable
  - Crosses Organizational Boundaries

- Recent real-world case study
  - Highlight difficulties in observation and attribution
  - Demonstrates success

- This is just the beginning