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 13, 2004

FACT SHEET

The President authorized a new national policy on December 13, 2004 that establishes and implements actions for space-based positioning, navigation, and timing programs, and activities for U.S. national and homeland security, civil, commercial, and non-commercial purposes. This policy supersedes Presidential Decision Directive/National Security and Technology Council, U.S. Global Positioning System Policy, dated March 24, 1996.

I. Scope and Definitions

This policy provides guidance for: (1) development, acquisition, operation, maintenance, and modernization of the Global Positioning System (GPS) and U.S.-developed, owned, and/or operated systems used to augment or otherwise improve the Global Positioning System and/or its space-based positioning, navigation, and timing capabilities; (2) development, deployment, installation, modernization, and redeployment of systems and components to protect U.S. and allied access 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 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.

• "Comparable" 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 ground-based systems that provide users of space-based positioning, navigation, and timing signals with additional information that enables a system to support the user's mission capabilities.

The IDM Policy expands and enhances the IDM Policy guidance by introducing the following:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

II. Identify

The IDM Policy identifies the following components of the IDM Policy:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

III. Analyze

The IDM Policy analyzes the following issues:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

IV. Locate

The IDM Policy locates the following systems and services:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

V. Attribute

The IDM Policy attributes the following:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

VI. Mitigate

The IDM Policy mitigates the following:

1. Interoperable developments for the Global Positioning System to and with foreign, commercial, and other space-based positioning, navigation, and timing services.

2. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

3. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

4. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.

5. Interoperable systems and services for the Global Positioning System and other space-based positioning, navigation, and timing services.
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

GPS Supporting Power Grid Systems
- Power Grids
- Substation
- Energy Plants
- Rail Yards
- Switching Towers & Signals
- Air Traffic Control

GPS Supporting Transportation Systems
- C² Centers
- Ship Routing

GPS Supporting Banking Operations
- ATM Networks
- Stock Exchanges
- Internet Banking
- Banks/Nodes

GPS Supporting Communications Systems
- GIS / Map
- Access
- Comms Networks
- GPS Time & Position
- Relay Position To 911 Dispatch

GPS Supporting Power Grid
- GPS Time

GPS Supporting Transportation Systems
- GPS Time & Position

GPS Supporting Communications Systems
- GPS Time & Position

GPS
- GPS Supporting Power Grid
- GPS Supporting Banking Operations
- GPS Supporting Communications Systems
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

Monitoring & Collection

AFRL

Smart Phone Crowd Sourcing

Fleet Management “WebTech”

FCC/FAA Receiver/ Sensors

Iridium

UNITRAC

FAA MINNOW February 2012

FAA PNTIP SETS

Analysis & Evaluation

SECURE NETWORK CONNECTION

USER

USER

USER
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
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.
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

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

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

**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

DCP: Differential Correction Processor
RPDP: Robust Power Distribution Panel
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
  - 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
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

<table>
<thead>
<tr>
<th>Hit Times</th>
<th>Duration (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25-Mar-2010 11:55:34</td>
<td>4</td>
</tr>
<tr>
<td>25-Mar-2010 18:53:42</td>
<td>4</td>
</tr>
<tr>
<td>25-Mar-2010 18:59:51</td>
<td>7</td>
</tr>
<tr>
<td>25-Mar-2010 19:05:47</td>
<td>7</td>
</tr>
<tr>
<td>25-Mar-2010 19:21:44</td>
<td>7</td>
</tr>
<tr>
<td>25-Mar-2010 20:10:48</td>
<td>4</td>
</tr>
<tr>
<td>25-Mar-2010 20:30:07</td>
<td>7</td>
</tr>
<tr>
<td>25-Mar-2010 21:16:08</td>
<td>22</td>
</tr>
<tr>
<td>25-Mar-2010 21:24:07</td>
<td>8</td>
</tr>
<tr>
<td>25-Mar-2010 21:37:03</td>
<td>4</td>
</tr>
<tr>
<td>25-Mar-2010 21:43:23</td>
<td>10</td>
</tr>
</tbody>
</table>

### Mobile DACU

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

Correlated but non-coincident times imply a moving interferer.
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 x 45 x 20 mm
  - 0.3 Ounces
  - Rechargeable battery rated for up to 42 hrs
- Cost: $100 (amazon.com)
C/N₀ Sensor: Laydown
Analytical Pattern

Idealized Pattern of Low Power Jammer
C/N₀ Sensor: Results: Wednesday 23 Mar 2010, 20:51:00 GMT

Dropout time progression indicates a moving interference source traveling at ~60 mph.
C/N₀ 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
New Jersey Turnpike Overpass Point
Sample Measured Data

Date: 04/15/2010 03:29:16 PM
GPS Position: 40° 41' 17.774" N - 74° 9' 49.636" W
User Name: James S. Aviles
Note: EWR GBAS Interference measured at MP103 Overpass same suspect truck detected in the AM.
Difficulties

Potential Culprits License Plates
Many vehicles to separate the actual Culprit
Strategy became a challenging task
Another Strategy: Closer Observation
Implementation Reality: Traffic

Traffic Buildup
Challenge the Strategy
Interference: Hot Pursuit

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

Home of Security Information Network

Welcome to HSN

User Name:
Password:
Login

You are accessing a U.S. Government information system, which includes (1) this computer, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transmitted or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transmitted or stored on this information system. The government may disclose or use any communications or data transmitted or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes. You are NOT authorized to process classified information on this system.

DO NOT PROCESS CLASSIFIED INFORMATION ON THIS SYSTEM

U.S. Department of Homeland Security

PNT Application Login Page

Login Email:
Password:

Logon to PNTIP  Reset

Change password?  Lost password?

Warning: This is a Federal Aviation Administration (FAA) computer system. 18 U.S.C.

This computer system, including all the related equipment, networks and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. FAA computer systems may be monitored for all lawful purposes, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify the security of this system.

During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this FAA computer, authorized or unauthorized, constitutes consent to monitoring of this system.

Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adversarial action. Use of this system constitutes consent to monitoring for these purposes.
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