GPS VULNERABILITY IN MOBILE NETWORKS

Marc A. Weiss, Ph.D.
NIST Time & Frequency Division
303-497-3261
mweiss@nist.gov

Outline:
GPS Vulnerability in Mobile Networks

- Generally, what is the problem?
- What are the tight timing requirements?
- How serious are the risks?
- What are the timing alternatives?
- Conclusions

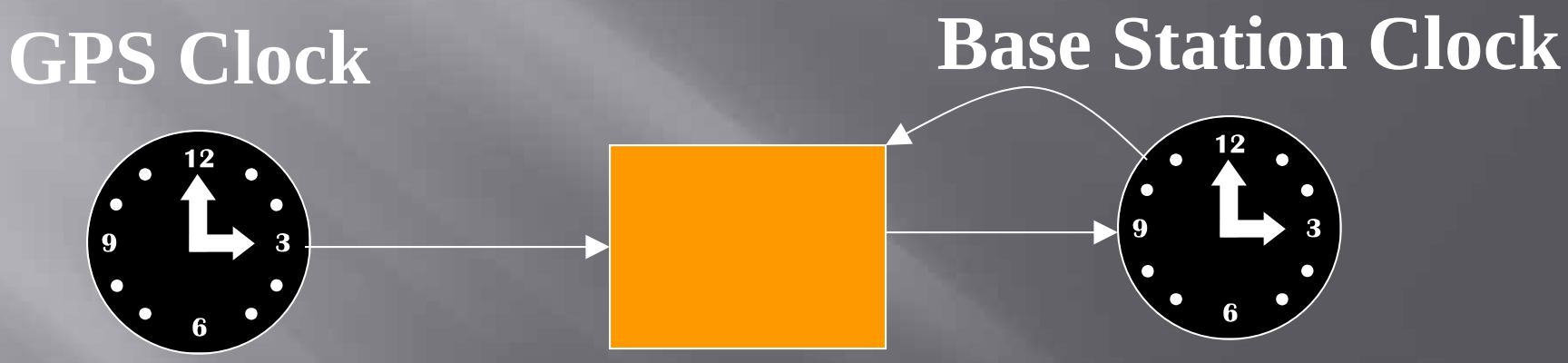
The Problem: GPS Vulnerability in Mobile Networks

- Mobile networks have increasingly tight timing requirements
  - Time, frequency, phase
  - Timing generally optimizes bandwidth
  - Different services have different requirements
- Most timing is dependent on GPS (or GNSS)
  - GPS is extremely accurate, reliable, and virtually free
  - This is perhaps the best and worst aspect of GPS
- GPS (and all GNSS) signals are extremely vulnerable to interference

Evolving Telecom Sync Requirements: Time, Phase, Frequency, and UTC

- Until the last few years, most precision telecom sync requirements were for **Frequency**
  - Directly from a clock, usually one locked to a master
- More recently, largely to optimize mobile bandwidth, requirements are needed for **Phase** and **Time**
  - Phase must be transferred between clocks
  - **UTC or TAI Time** must come from a national lab, generally from GNSS
  - These are generally **harder to hold-over**

Sync from GPS



GPS Clock Systematics and Noise

Lock Loop Systematics and Noise: Contributions from Measurement Noise and Path Perturbations

User Clock Systematics and Noise

Outline: GPS Vulnerability in Mobile Networks

- Generally, what is the problem?
- What are the tight timing requirements?
- How serious are the risks?
- What are the timing alternatives?
- Conclusions

Summary of Some Timing Requirements

Standard	Timing Accuracy	Frequency Accuracy
CDMA2000	10 µs	100 ppb
GSM	–	100 ppb
WiMAX	1 µs (TDD)	8 ppm
LTE	3 µs (TDD)	250 ppb
WCDMA	2.5 µs (TDD)	250 ppb
TD-SCDMA	2.5 µs	100 ppb

Outline: GPS Vulnerability in Mobile Networks

- Generally, what is the problem?
- What are the tight timing requirements?
- How serious are the risks?
- What are the timing alternatives?
- Conclusions

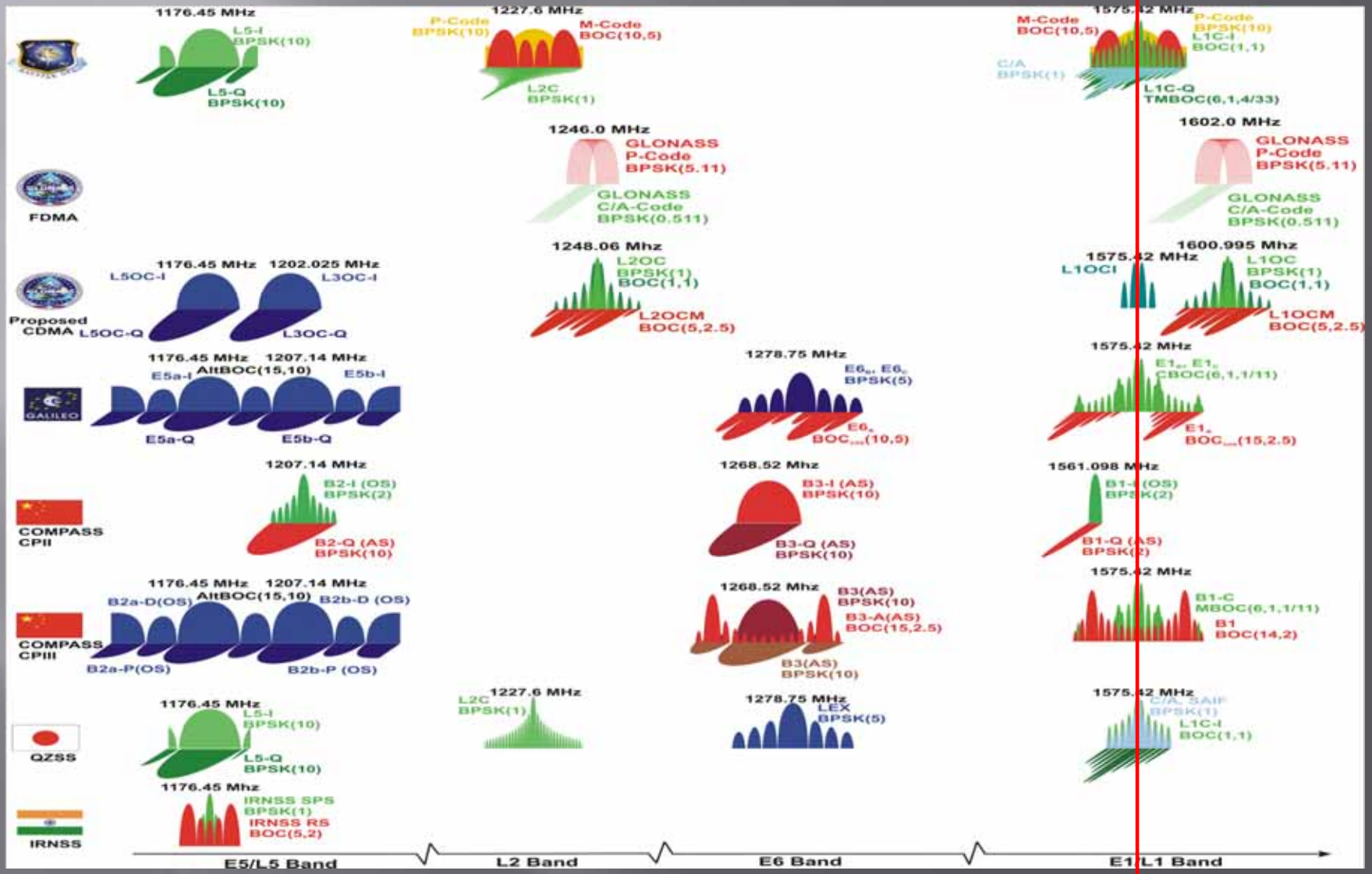
Civil GPS Vulnerabilities

	Attack	Description
Jamming	Unintentional	Solar radio bursts
	Intentional	Denial of service via RF noise
Spoofing	Meaconing	Record and playback of entire RF spectrum
	Security Code Estimation and Replay	Estimate security code on-the-fly and playback with estimated value to defeat security enhanced GPS (not publically available)
	Data Bit Forgery	Alter ephemeris or leap second indicators

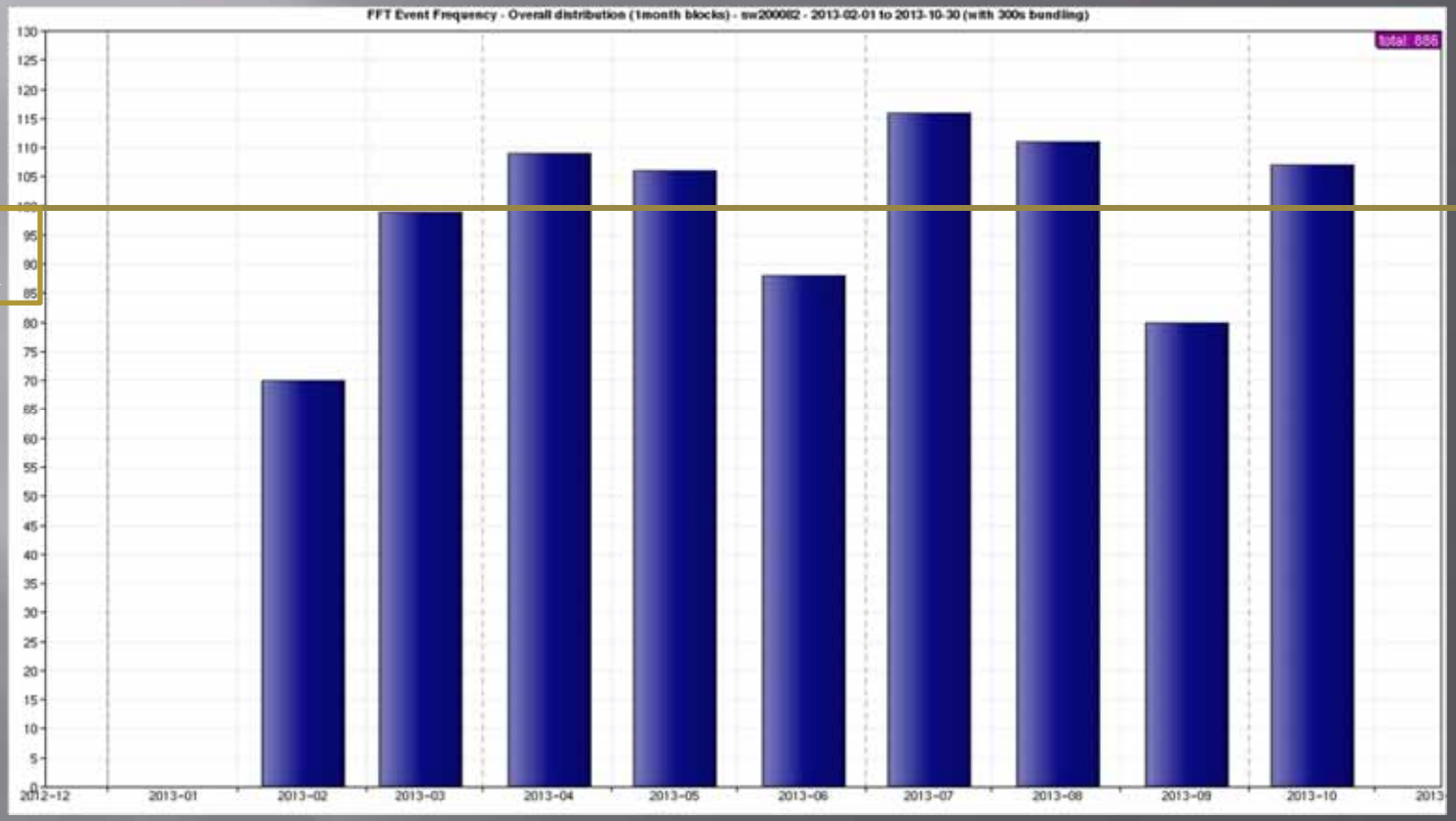
GNSS Vulnerability

- GNSS best feature and worst problem: it is extremely reliable
- Jamming Power Required at GPS Antenna
  - On order of a Picowatt (10^{-12} watt)
- Many Jammer Models Exist
  - Watt to MWatt Output – Worldwide Militaries
  - Lower Power (<100 watts); "Hams" Can Make; Easily Available on the Internet

GNSS Spectrum



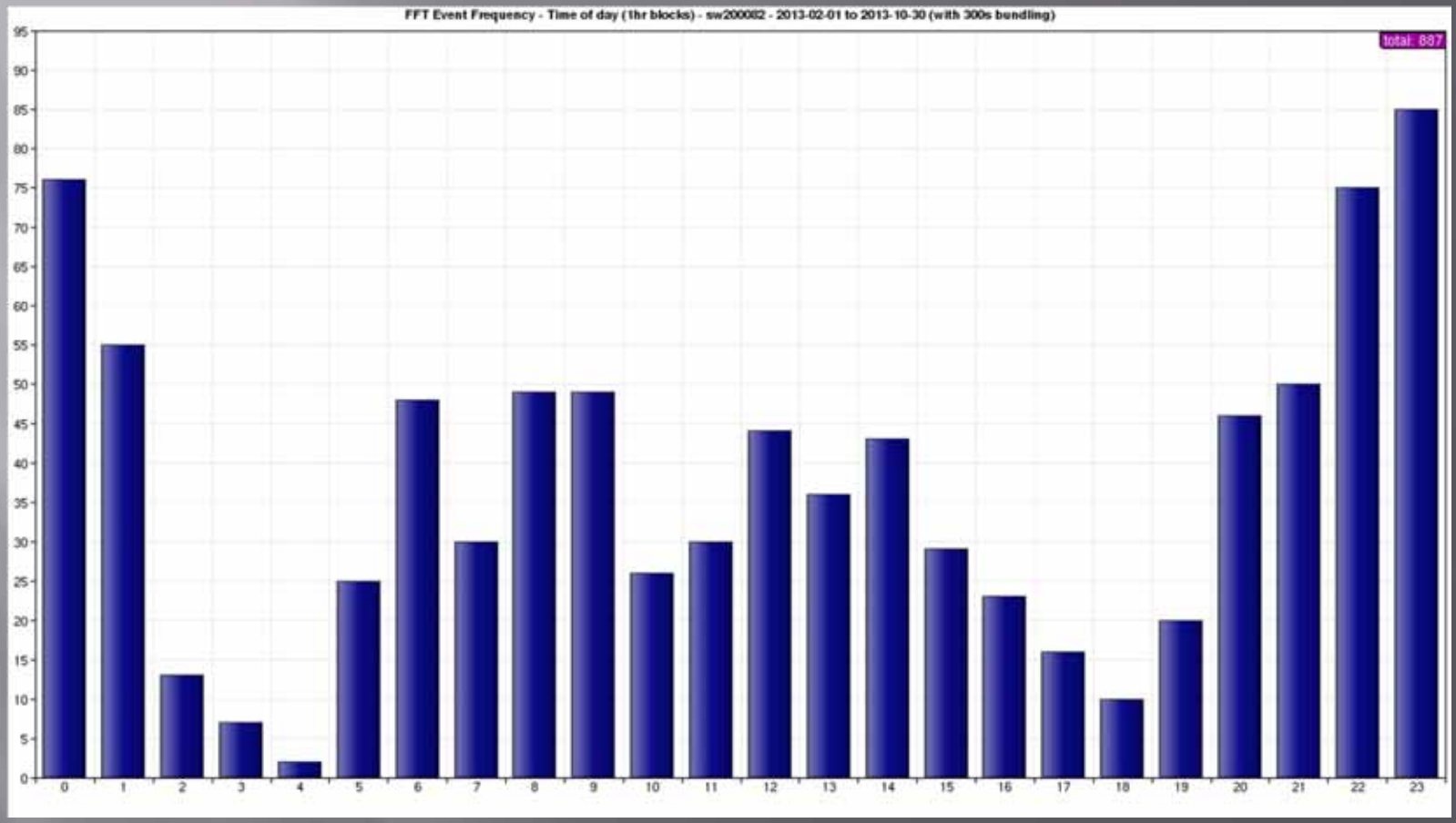
Jamming Events Each Month, Feb – Oct 2013: London Financial District



100 Events/Month

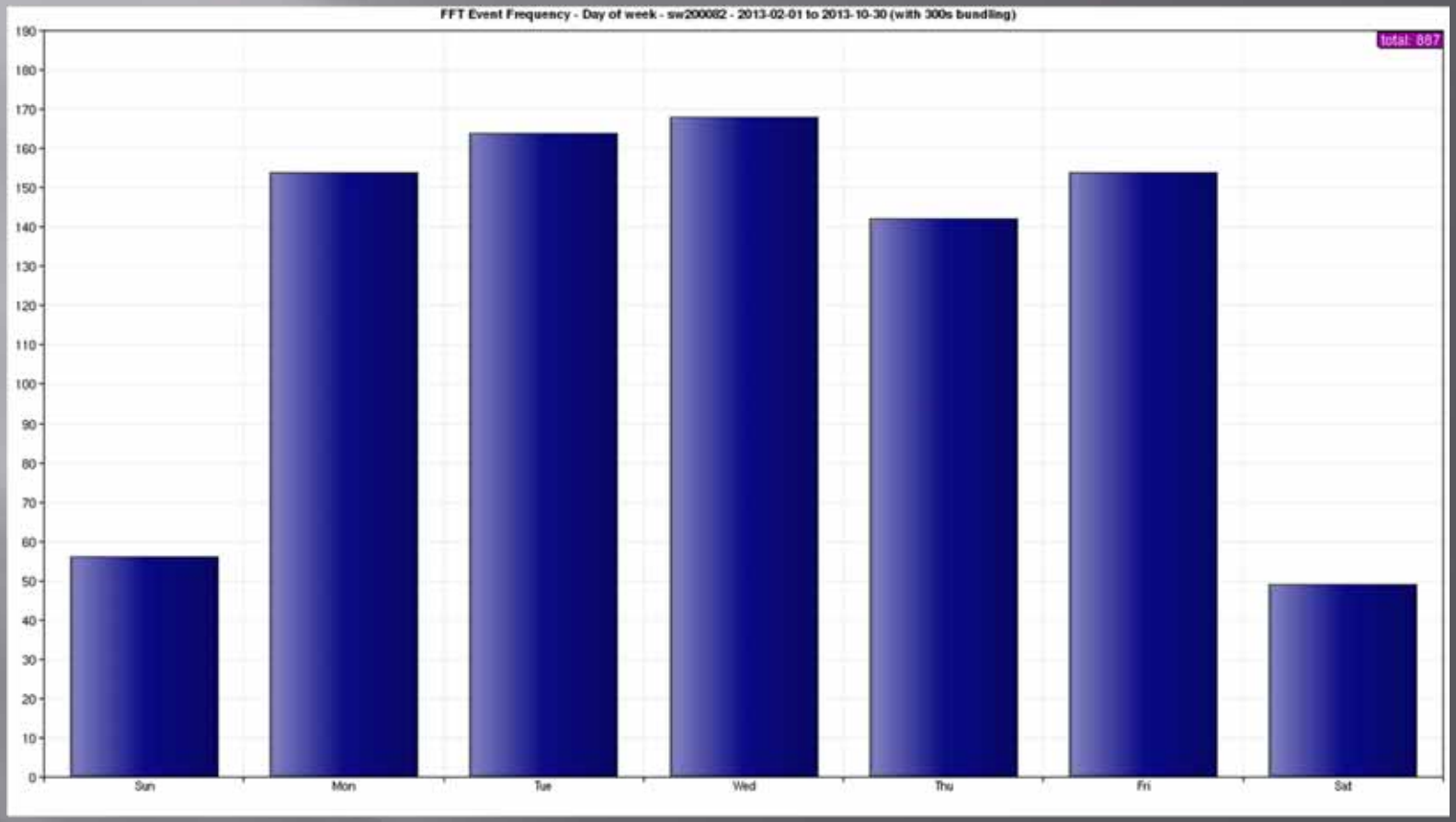
Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project

Jamming Events Each Hour, Feb – Oct 2013: London Financial District



Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project

Jamming Events Day of Week, Feb – Oct 2013: London Financial District



Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project

ENFORCEMENT BUREAU
SIGNAL JAMMER ENFORCEMENT INITIATIVE

Education and Outreach Efforts

Coupled with increasingly aggressive enforcement action, the FCC Enforcement Bureau (EB) continues to educate the public, coordinate with other USG agencies, and form international partnerships. For example, EB has:

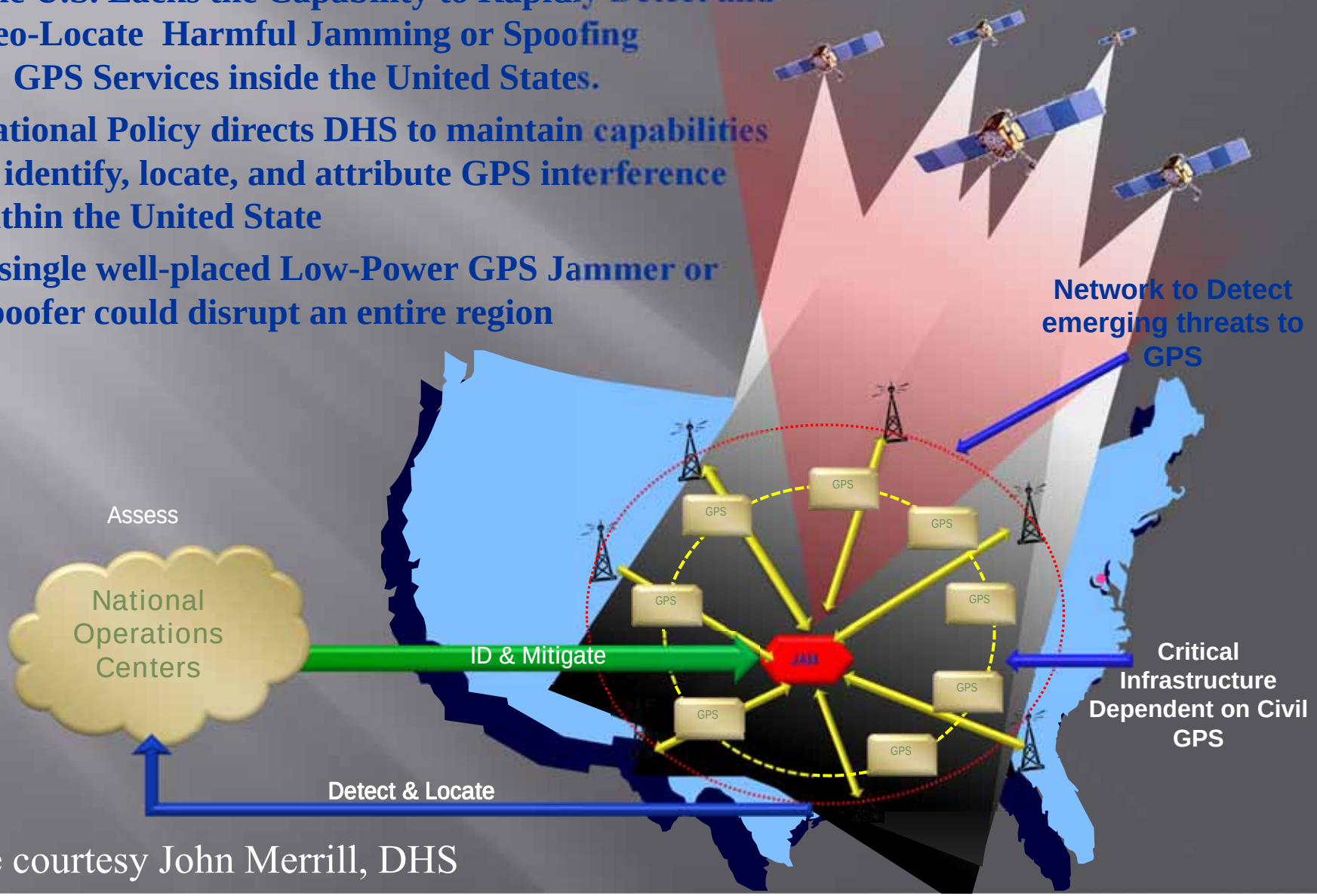
- released three Enforcement Advisories (one of which was translated into Spanish and Mandarin) designed to (i) educate retailers and consumers, (ii) emphasize that jammers are illegal, and (iii) note that violators risk substantial civil and criminal penalties;
- launched a webpage focused on jammer enforcement (**http://www.fcc.gov/jammers**);
- developed and released detailed Frequently Asked Questions on signal jamming devices;
- created **jammerinfo@fcc.gov**, a one-stop shop for consumer questions regarding jammers;
- instituted a dedicated tip line for jammers: **1-855-55NOJAM (1-855-556-6526)**;
- issued a downloadable poster highlighting the jamming prohibition and describing how to file a complaint; and
- developed jammer-related reference bulletins for law enforcement officers and other critical audiences.

Slide courtesy John Merrill, DHS

1-855-55NOJAM (1-855-556-6526) – jammerinfo@fcc.gov – http://www.fcc.gov/jammers

DHS Patriot Watch Overview

- **The U.S. Lacks the Capability to Rapidly Detect and Geo-Locate Harmful Jamming or Spoofing of GPS Services inside the United States.**
- **National Policy directs DHS to maintain capabilities to identify, locate, and attribute GPS interference within the United State**
- **A single well-placed Low-Power GPS Jammer or Spoofer could disrupt an entire region**

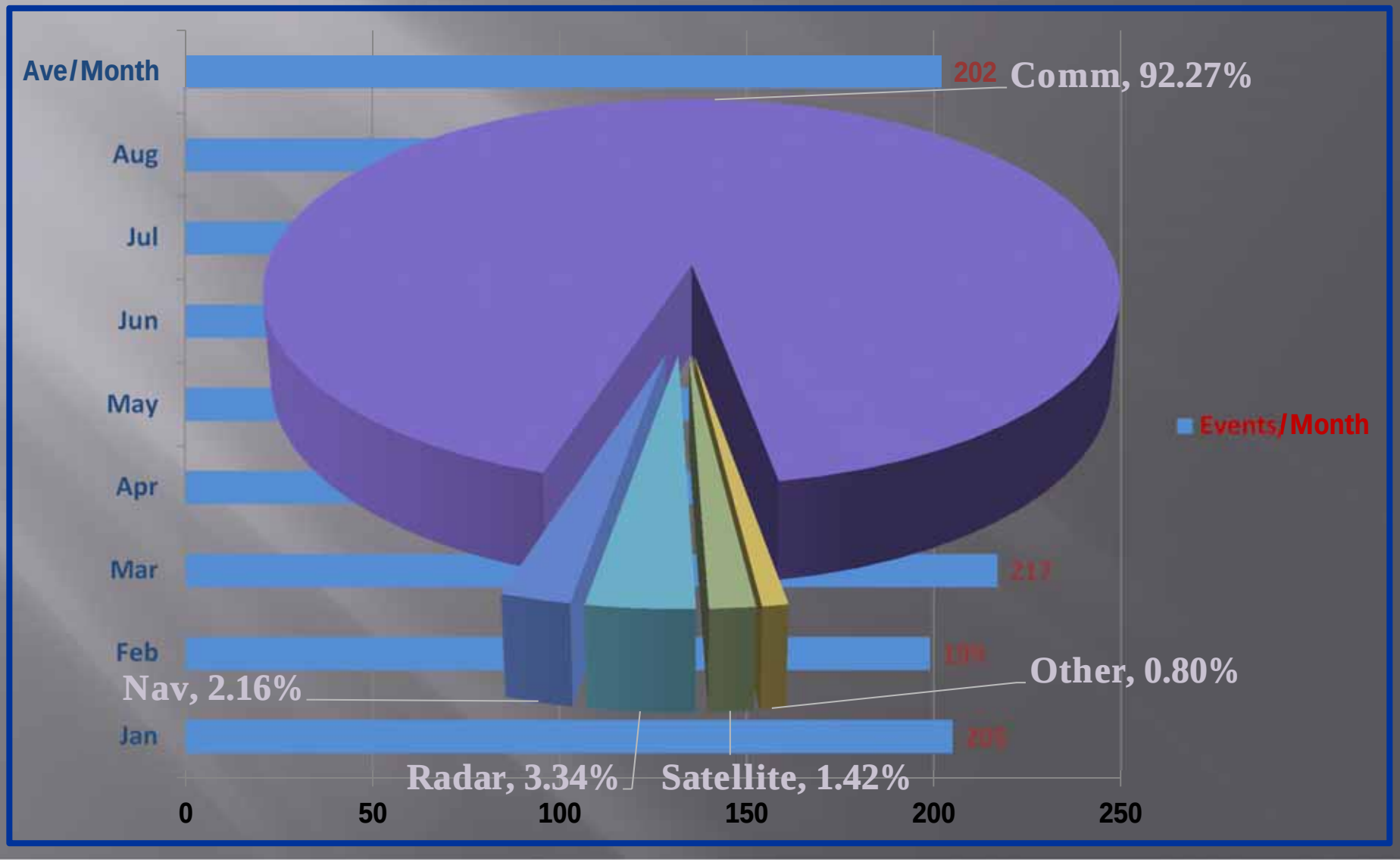


Slide courtesy John Merrill, DHS

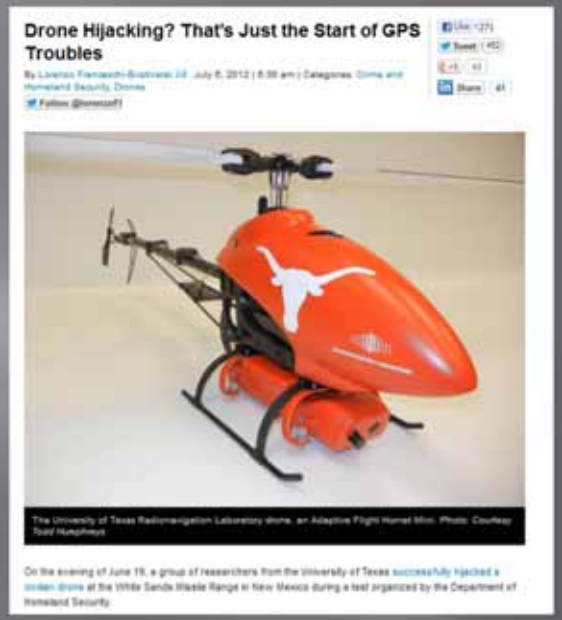
Slide courtesy John Merrill, DHS

2013 FAA RFI Events by Month

Source: August 2013 FAA Spectrum Engineering Office



Spoofing: A Growing Threat

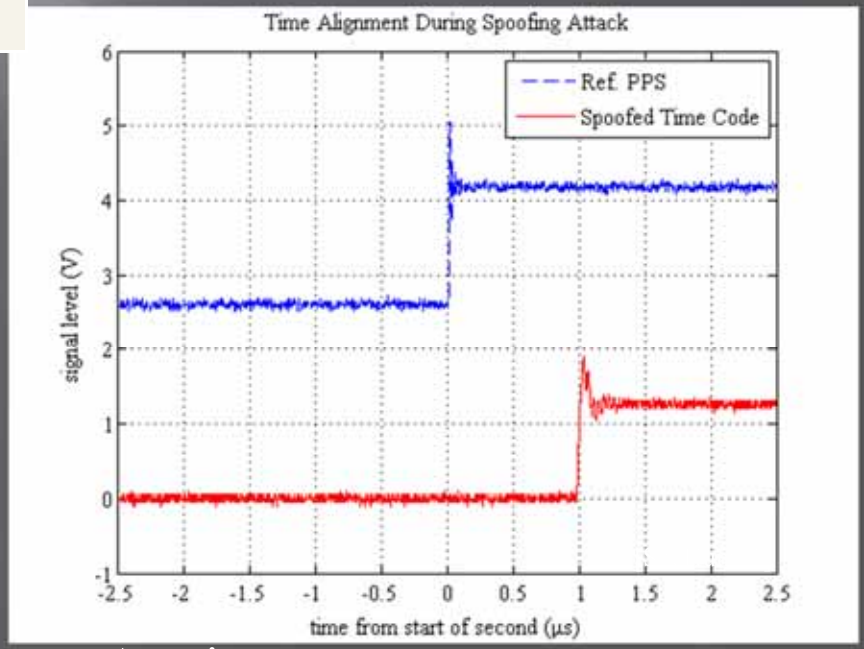


Slide courtesy Kyle Wesson, University of Texas, Austin

Spoofing GPS: Telecom Network Vulnerabilities

Standard	Timing Accuracy	Frequency Accuracy
CDMA2000	10 µs	100 ppb
GSM	–	100 ppb
WiMAX	1 µs (TDD)	8 ppm
LTE	3 µs (TDD)	250 ppb
WCDMA	2.5 µs (TDD)	250 ppb
TD-SCDMA	2.5 µs	100 ppb

[PesWes&11]



In 35 minutes, spoofer can shift time 10 µs, which would disrupt CDMA call hand-off

Slide courtesy Kyle Wesson, University of Texas, Austin

Outline: GPS Vulnerability in Mobile Networks

- Generally, what is the problem?
- What are the tight timing requirements?
- How serious are the risks?
- What are the timing alternatives?
- Conclusions

How long can you hold a microsecond?

- Much harder to hold time / phase than frequency
- Hold-over time depends on many things
  - Type of local oscillator (LO)
  - Initialization of LO
  - Environment: in telecom mostly temperature

Holding a Microsecond

	Temperature Controlled Crystal Oscillator (TCXO)	**Oven Controlled Crystal Oscillator (OCXO)**	**Rb Oscillator** (5E-12/mo. aging)
Range of times to hold a microsecond	10 minutes – 1 hour	1 – 8 hours	8 hours – 3 days
Cost Range	$5-25	$50-150	$500-1500

Alternative Time Transfer

- Through the Network
  - SONET has frequency sync, but is being phased out
  - Modern native packet networks need special equipment to pass sync
  - Synchronous Ethernet (SyncE) can provide excellent frequency sync
  - Precise Time Protocol (PTP) can provide sub – us time sync over a few hops with special equipment
- Over Air
  - Signals from other wireless base-stations ("macrosniff")
  - PTP over microwave
- eLORAN Could be a Complete Backup Including UTC
  - Currently towers are being taken down

Conclusions: GPS Vulnerabilities

- GPS has been extremely reliable, yet is highly vulnerable to attack
  - So far, GPS interference has been incidental
  - Much like the internet started with no viruses or attacks, GPS could become a target
  - Telecom has accepted the current risk level
- Very dangerous scenarios are possible
  - GPS could be denied, impacting first responders
  - Could be part of a larger attack
  - Removing a GPS attack could take more than a day, for example if done with multiple mobile intermittent jammers

Overall Conclusions

- GNSS provides very accurate and free all three types of sync: Time and Frequency and Phase
- Mobile sync specs are getting tighter
- GNSS are vulnerable, best feature and worst problem: extremely reliable
- Backup options: good LO, other transfer source

For More About Sync

http://www.atis.org/wsts/

Thank you for your interest!