# RTL-SDR Plane Spotting

Using a Realtek RTL2382U-based DVB-T USB Dongle

John DeGood
Princeton ACM/IEEE-CS Joint Chapter
Thu 18 Feb 2016

# Outline

- Introduction to Plane Spotting
- SDR Software
- SDR Hardware
- Reception Statistics
- Reception Examples
- Security Considerations

# Introduction to Plane Spotting

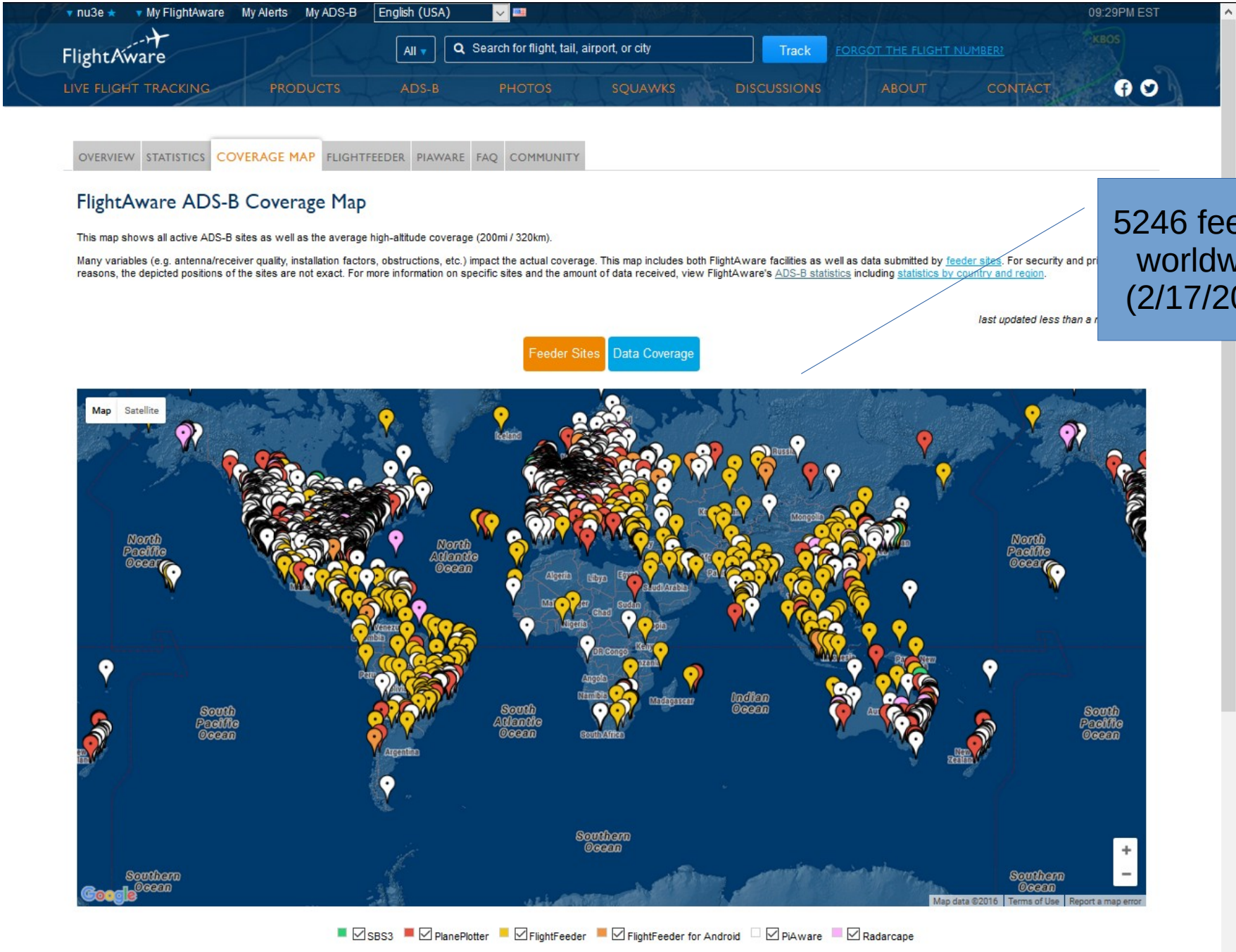
# Plane Spotting Jargon

- Mode A
  - Transponder “squawk” code (4-digit, octal)
  - 1030 MHz interrogation; 1090 MHz response
- Mode C
  - Barometric pressure altitude
- Mode S (Select)
  - Makes the ACAS II (Airborne Collision Avoidance System) and the ADS-B systems function
- 1090 MHz Extended Squitter
  - Extends Mode S
  - Unsolicited 1090 MHz downlink
- ADS-B – Automatic Dependent Surveillance-Broadcast
  - Uses a certified, high-integrity GPS
  - Specifies both ADS-B Out and ADS-B In
  - ADS-B Out required by January 1, 2020 in non-general aviation airspace
- UAT – Universal Access Transceiver
  - General aviation / flights below 18,000 feet
  - 978 MHz downlink
  - Relieves congestion on 1090 MHz
  - Supports ADS-B, but also Flight Information Service – Broadcast (FIS-B) and Traffic Information Service – Broadcast (TIS-B)
- MLAT – Multilateration
  - Determines the aircraft's location by using time difference of arrival (TDOA) when an aircraft is detected across three or more receivers/ground stations

# Example ADS-B Tracker Websites

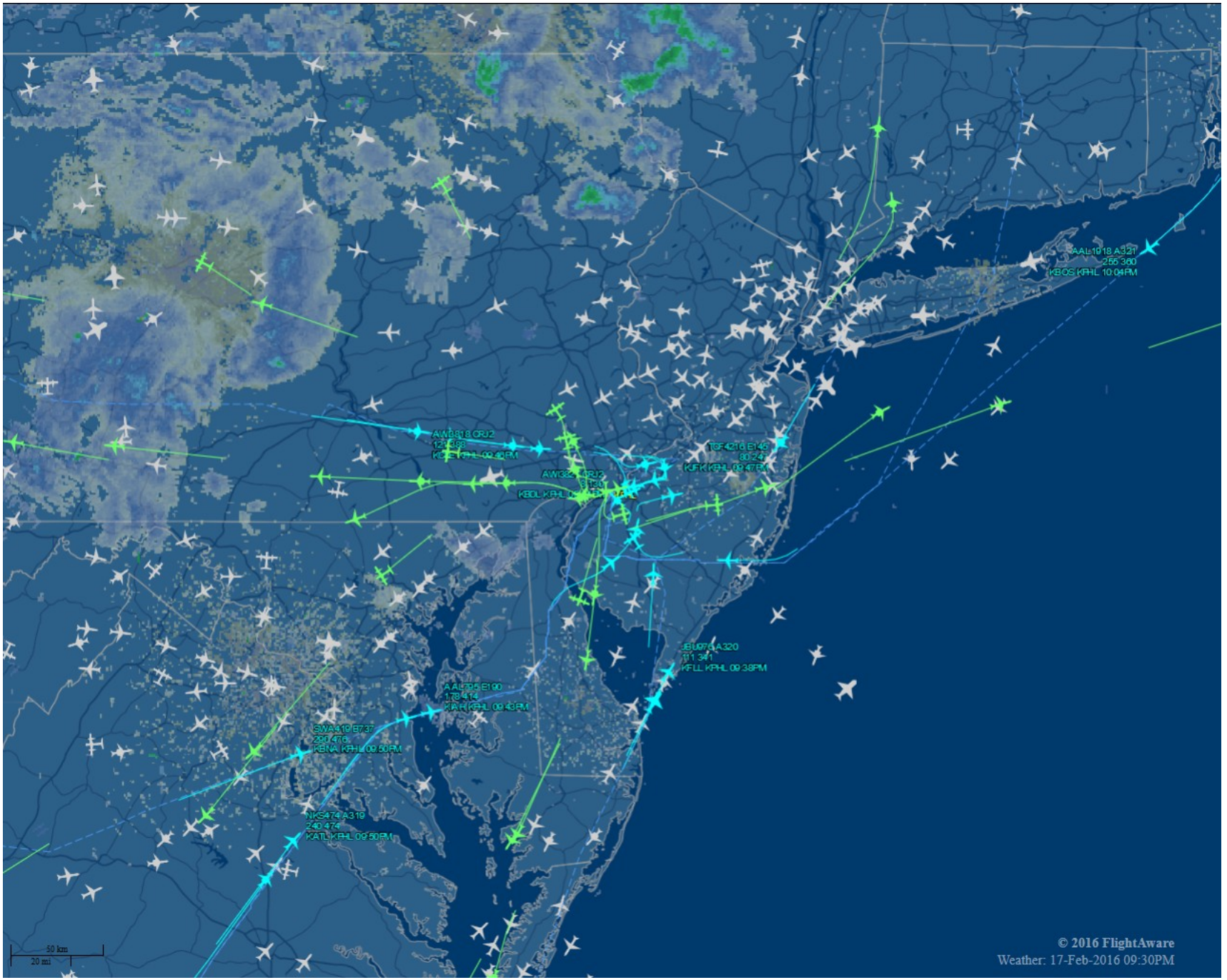
- FlightAware (commercial)
  - Unique trilateration capability
  - Free Enterprise Account ($89.95/month value) to feeders
  - https://www.flightaware.com/
- FlightRadar24 (commercial)
  - Free Premium Account ($35.88/year value) to feeders
  - https://www.flightradar24.com/
- ADS-B Exchange (community co-op)
  - http://www.adsbexchange.com/

# FlightAware.com

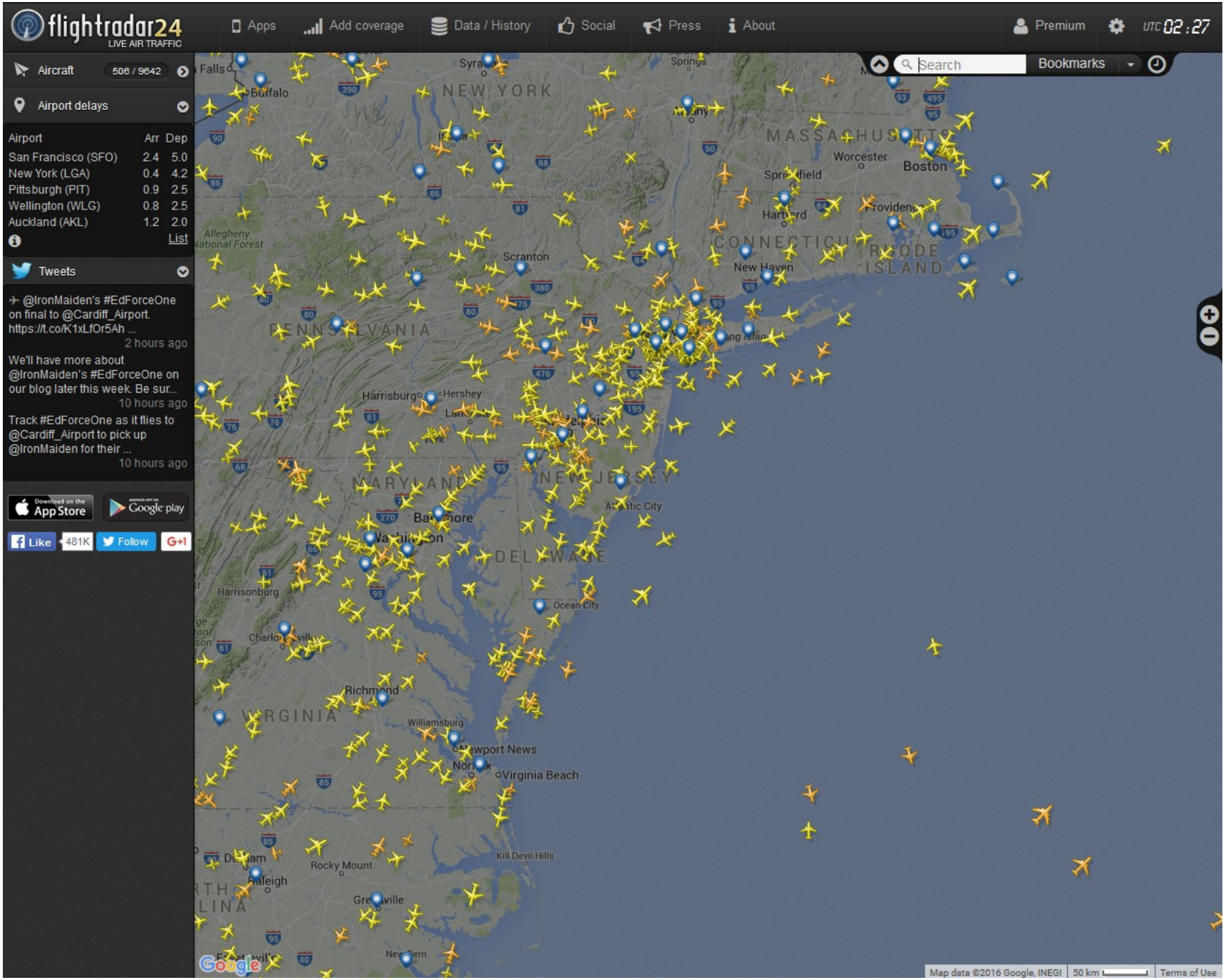



5246 feeders worldwide (2/17/2016)

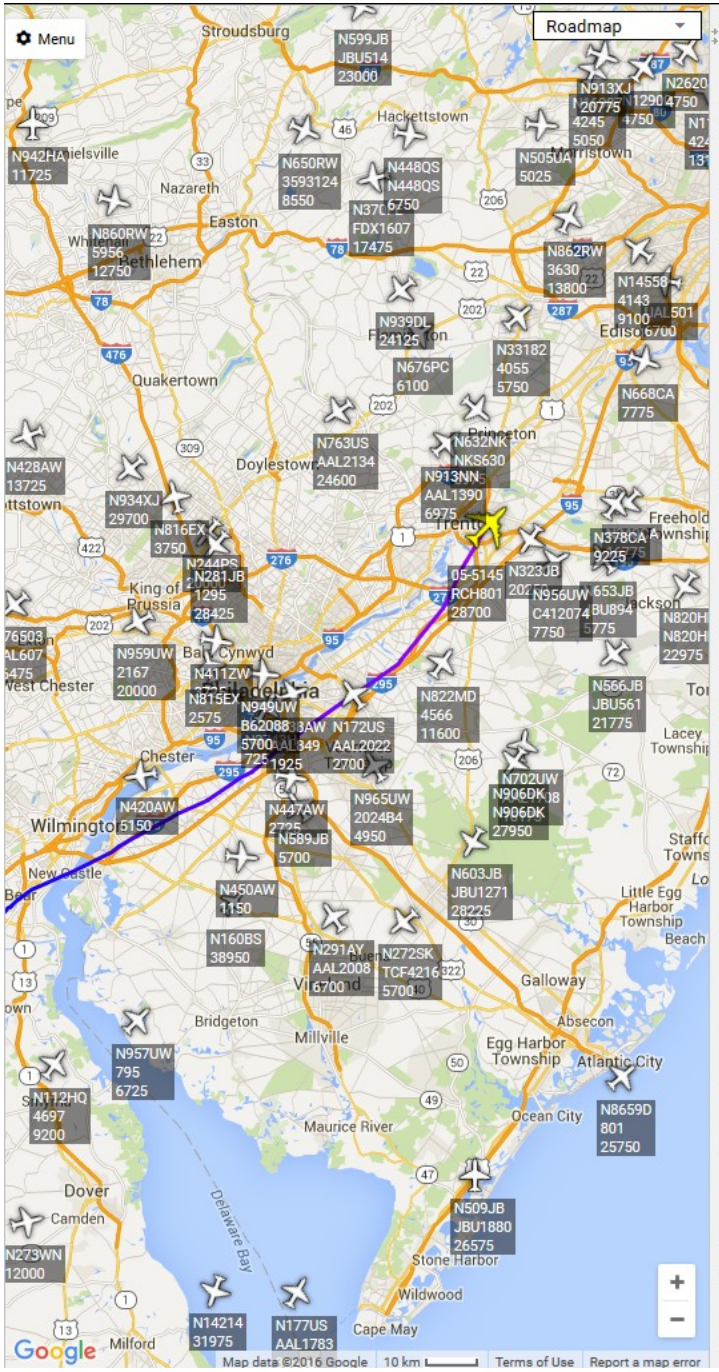
# FlightAware.com Live Display



# FlightRadar24.com Live Display



# ADSBexchange.com Live Display




**05-5145** AE144F
**United States Air Force** RCH801
**United States** Military
**Boeing C-17A Globemaster III** C17

| Altitude: | Speed: | Heading: | Vertical Speed: | Squawk: | Species: | Transponder: | Latitude: | Longitude: |
|---|---|---|---|---|---|---|---|---|
| 28700 ft | 457.6 kts | 46.3° | 576 ft/m | 3673 | Landplane | ADS-B | 40.21159° | -74.69480° |

**Route:**
Route not known

| Interesting: | User Tag: | Flights Count: | Receiver: | MLAT: | Message Count: | Time Tracked: | Avg. Signal Level: |
|---|---|---|---|---|---|---|---|
| No | | 28 | From Consolidator | Yes | 978 | 20:00 | 183 |

**Operator Code:**
RCH

Image Search : : Airliners.Net : : FlightAware : : airport-data.com : : airframes.org
Show on map : : Enable auto-select

Tracking 63 aircraft (out of 2,761) Pause

| ICAO | Callsign | Reg. | Model | Altitude | Speed | Interesting | Squawk | Receiver |
|---|---|---|---|---|---|---|---|---|
| AB318C | N820HB* | N820HB | 1999 GULFSTREAM AEROSPACE G-V | 22975 ft | | Yes | 1754 | From Cons |
| A07792 | | N12900 | 2001 EMBRAER EMB-145LR | 4750 ft | 221.6 kts | No | 6240 | From Cons |
| A0ACB6 | | N14214 | 1998 BOEING 737-824 | 31975 ft | 449.8 kts | No | 1110 | From Cons |
| A0F1D8 | | N160BS | Bombardier Learjet 60 | 38950 ft | 511.8 kts | No | 6043 | From Cons |
| A24031 | | N244PS | 2004 BOMBARDIER INC CL-600-2B19 | 20000 ft | 373.8 kts | No | 7336 | From Cons |
| A288E4 | | N26208 | 2000 BOEING 737-824 | 4750 ft | 254.1 kts | No | 3703 | From Cons |
| A2B3A2 | | N273WN | 2007 BOEING 737-7H4 | 12000 ft | 453.1 kts | No | 1523 | From Cons |
| A37A3F | | N323JB | 2010 EMBRAER ERJ 190-100 IGW | 20250 ft | 259.3 kts | No | 1511 | From Cons |
| A3BD81 | | N340CA | 2002 BOMBARDIER INC CL-600-2C10 | 16775 ft | 223.0 kts | No | 3330 | From Cons |
| A44570 | | N3743H | 2001 BOEING 737-832 | 725 ft | 142.0 kts TAS | No | 5750 | From Cons |
| A451B6 | | N378CA | 2003 BOMBARDIER INC CL-600-2C10 | 9225 ft | 466.9 kts | No | 5644 | From Cons |
| A4DA2B | | N411ZW | 2001 BOMBARDIER INC CL-600-2B19 | 3725 ft | 306.0 kts | No | 5727 | From Cons |
| A4FBB4 | | N420AW | 2002 BOMBARDIER INC CL-600-2B19 | 5150 ft | | No | 3040 | From Cons |
| A5196C | | N428AW | 2002 BOMBARDIER INC CL-600-2B19 | 13725 ft | 200.5 kts | No | 1535 | From Cons |
| A564B3 | | N447AW | 2003 BOMBARDIER INC CL-600-2B19 | 2725 ft | 291.5 kts | No | 2147 | From Cons |
| A57231 | | N450AW | 2003 BOMBARDIER INC CL-600-2B19 | 1150 ft | 291.2 kts | No | 6673 | From Cons |
| A64E46 | | N505UA | BOEING 757-222 | 5025 ft | 272.3 kts | No | 6264 | From Cons |
| A79821 | | N589JB | 2004 AIRBUS A320-232 | 5700 ft | 236.8 kts | No | 7453 | From Cons |
| A8D224 | | N668CA | 2004 BOMBARDIER INC CL-600-2C10 | 7775 ft | 330.2 kts | No | 5661 | From Cons |
| A8F34A | | N676PC | 2005 PILATUS AIRCRAFT LTD PC-12/45 | 6100 ft | 338.2 kts | No | 3621 | From Cons |
| AB1C69 | | N815EX | 1992 DEHAVILLAND DHC-8-102 | 2575 ft | | No | 1652 | From Cons |
| AB2020 | | N816EX | 1992 DEHAVILLAND DHC-8-102 | 3750 ft | | No | 4257 | From Cons |

# SDR Software

# Plane Spotting Ground Station Software

- DUMP1090 Mutability (SDR Mode S Decoder)
  - Oliver Jowett, Cambridge, UK
  - Open source, forked from MalcolmRobb/dump1090
  - https://github.com/mutability/dump1090
- FlightAware PiAware (Web Flight Tracker)
  - Includes multilateration client
  - https://flightaware.com/adsb/piaware/
- FlightRadar24 Raspberry Pi (Web Flight Tracker)
  - https://www.flightradar24.com/raspberry-pi
- Collectd (database of local statistics)
  - https://github.com/mutability/dump1090-tools

# SDR Hardware

# RTL-SDR USB Dongle

USB 2.0 Digital DVB-T SDR+DAB+FM HDTV TV Tuner Receiver Stick RTL2832U+R820T2 D9

**$6.95**

From Hong Kong

Buy It Now

**Free shipping**

- RLT2382U DVB-T Demodulator
  - 7-bit ADC
  - outputs 8-bit I/Q samples (in-phase/quadrature)
  - highest theoretically possible sample-rate is 3.2 MS/s
  - highest sample-rate without lost samples is ~2.8 MS/s
  - Dump1090 uses 2.4 MS/s
- R820T tuner
  - frequency range = 24-1850 MHz

# RTL-SDR Receiver in Attic

# Bill of Materials

| | |
|---|---|
| $35 | Raspberry Pi 2 |
| $10 | Cables, connectors, adapters |
| $7 | RTL-SDR USB dongle |
| $6 | 16GB Micro SD card |
| $2 | Wi-Fi USB dongle |
| free | 5 V @ 1 A Cell Phone Charger |
| $60 | TOTAL |

Optional:

$20 – 1090 MHz bandpass filter, or

$3 – satellite TV diplexer used as highpass filter

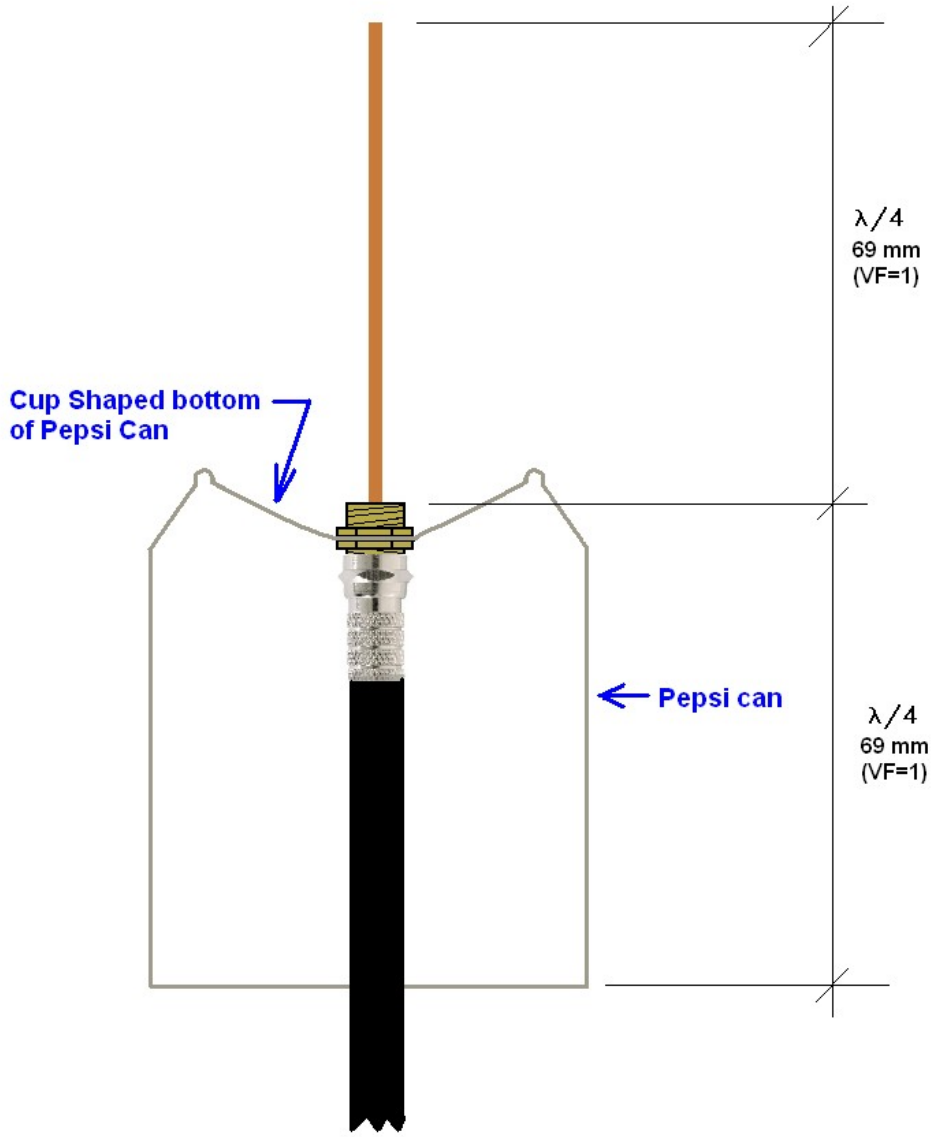
Prevents receiver desense from nearby radio transmitters, e.g. cell tower, pager tower, ham radio, etc.

# OEM Monopole on Ground Plane

# 4-element Coaxial Collinear Antenna

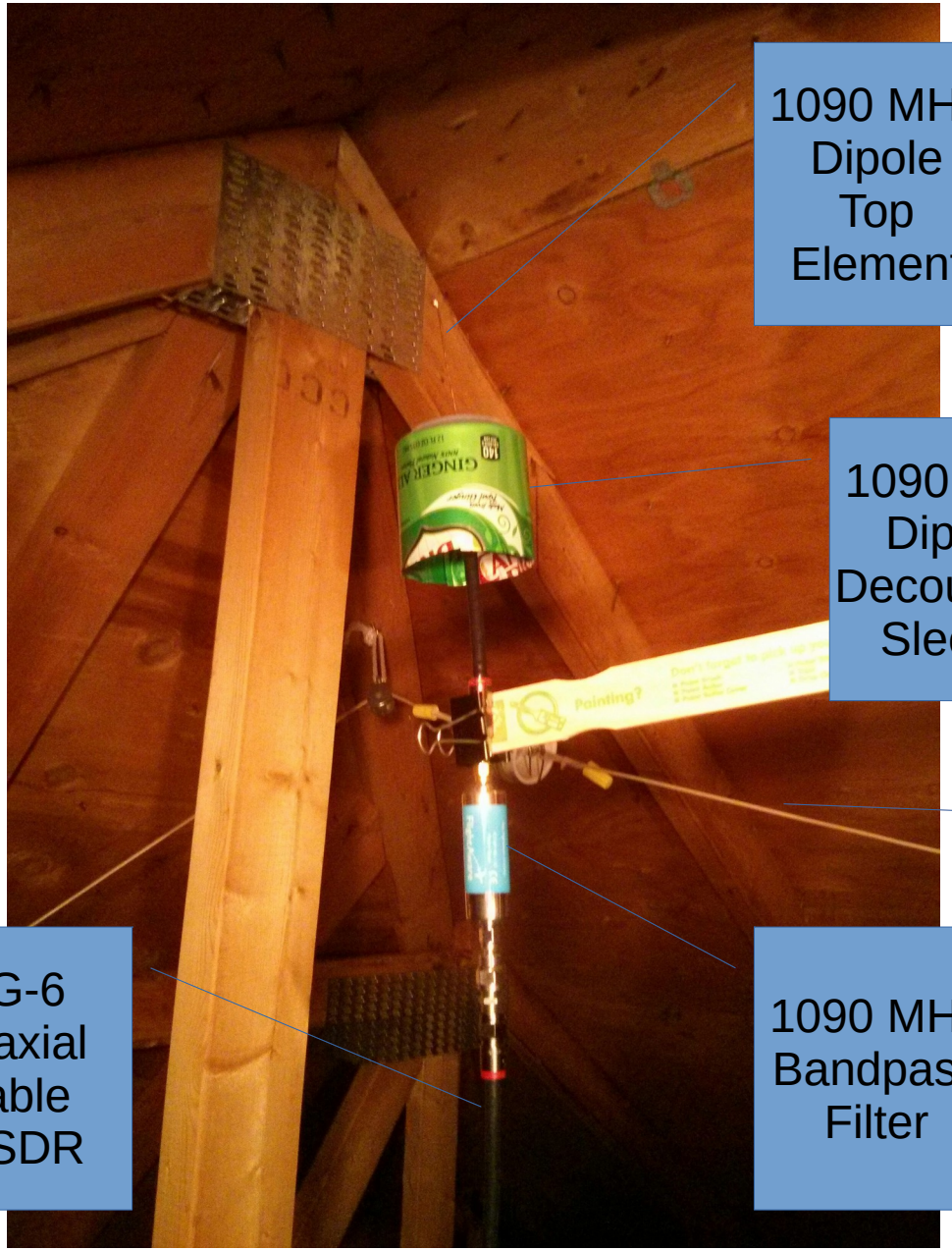
- Provides excellent gain vs. monopole
- Made from RG-6U satellite TV cable
- Unreliable due to connections between copper-plated steel center conductor and aluminum braid/foil shield

# “Cantenna” Construction Details




From FlightAware
user abcd567

# “Cantenna” Sleeve Dipole in Attic

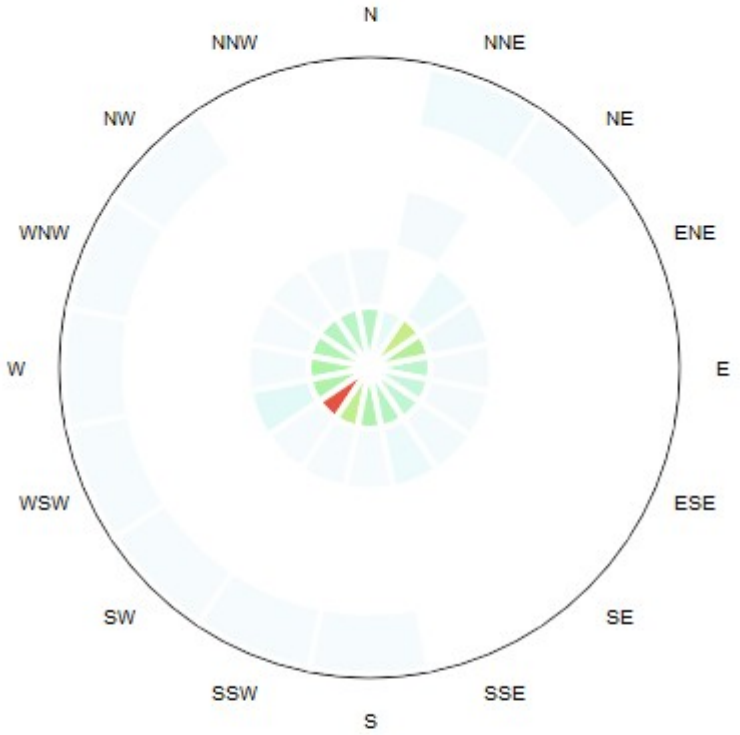


# Reception Statistics

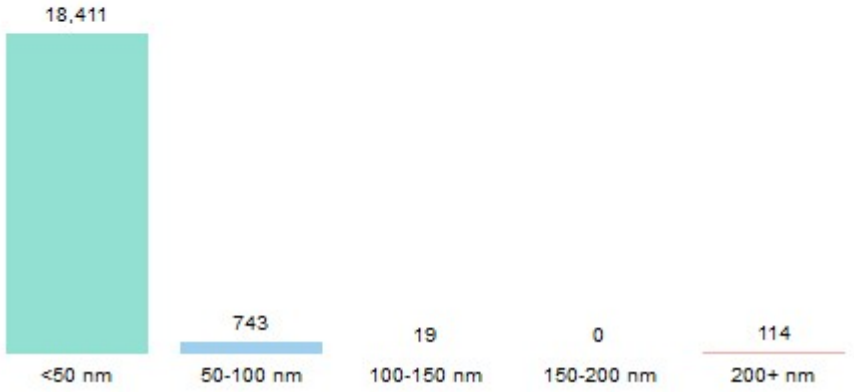
# Monopole @ 1.5 meters (1st floor table)

## Coverage Distribution

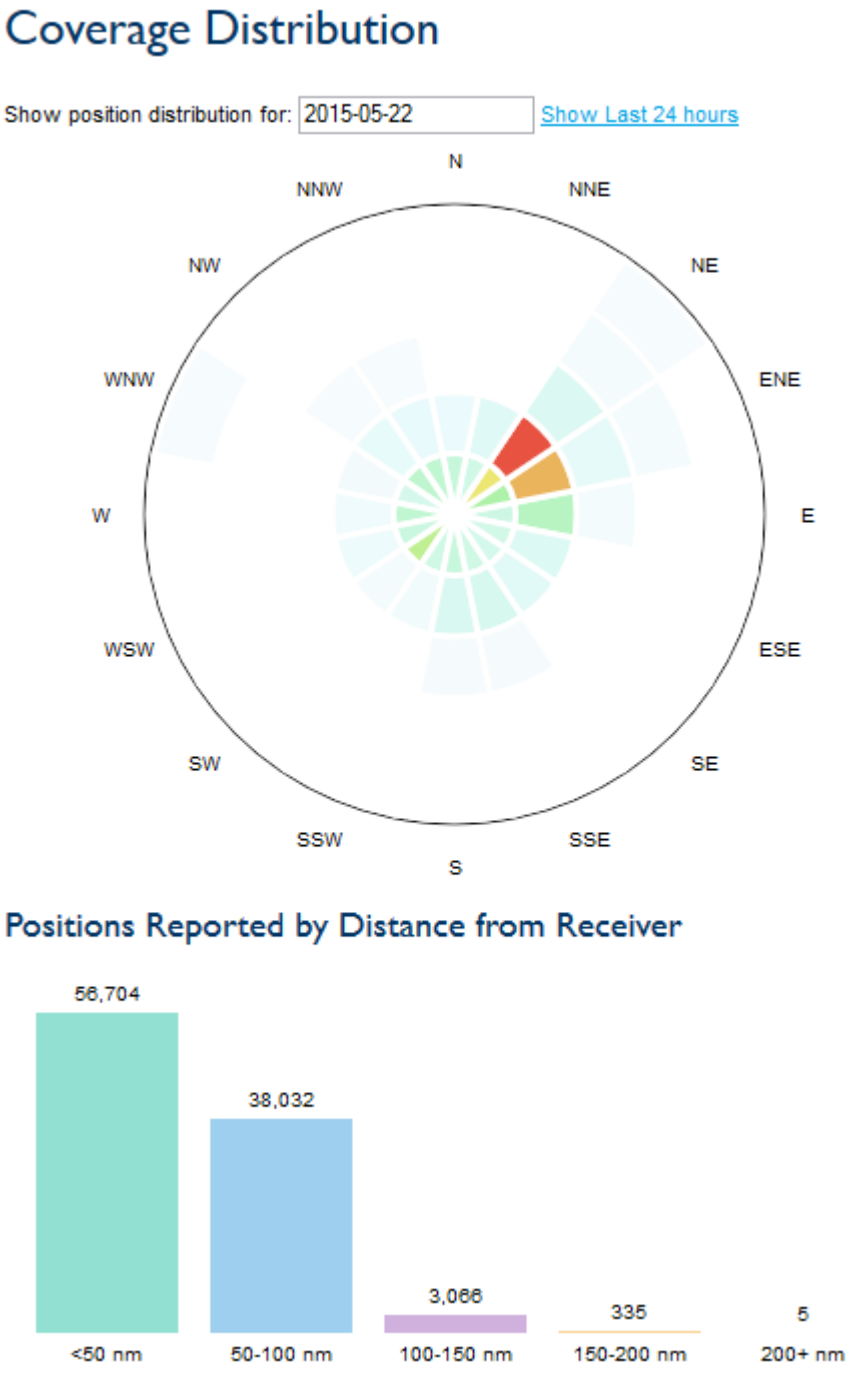
Show position distribution for: 2015-04-22 Show Last 24 hours



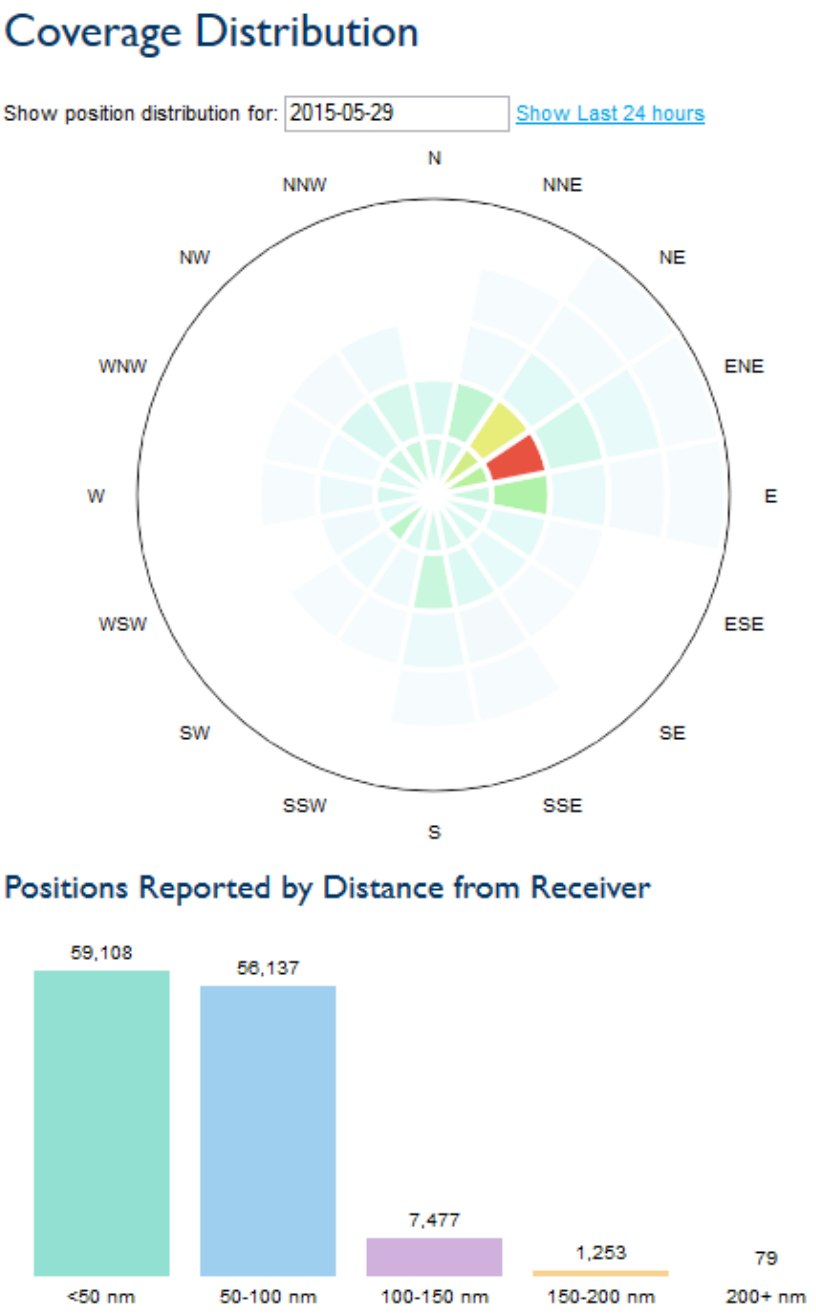

## Positions Reported by Distance from Receiver



# Monopole @ 5 meters (2nd floor ceiling)



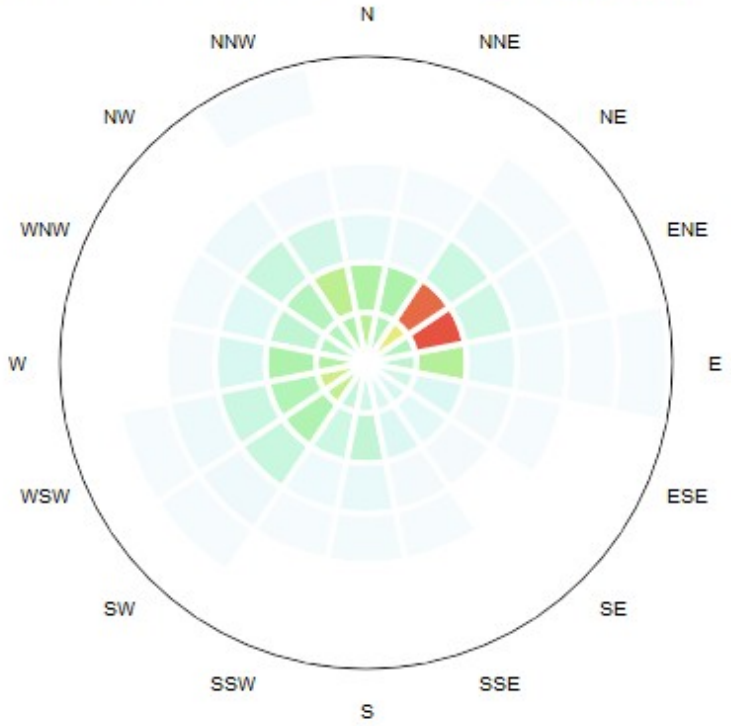
# Collinear @ 8 meters (2nd Floor Ceiling)



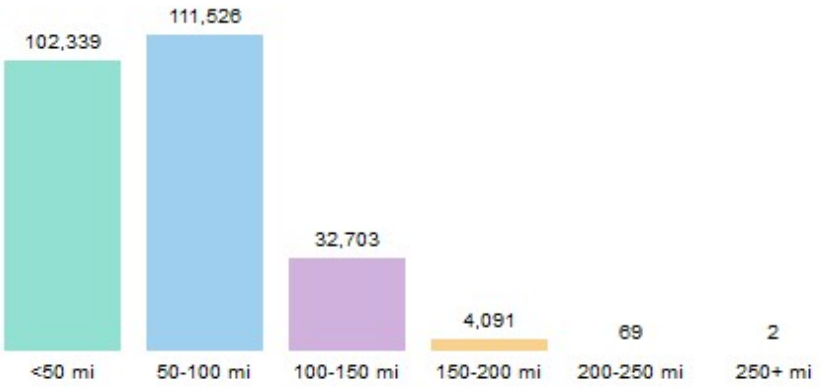
# “Cantenna” @ 8 meters (attic ridge)

## Coverage Distribution

Show position distribution for: 2016-02-12 Show Last 24 hours

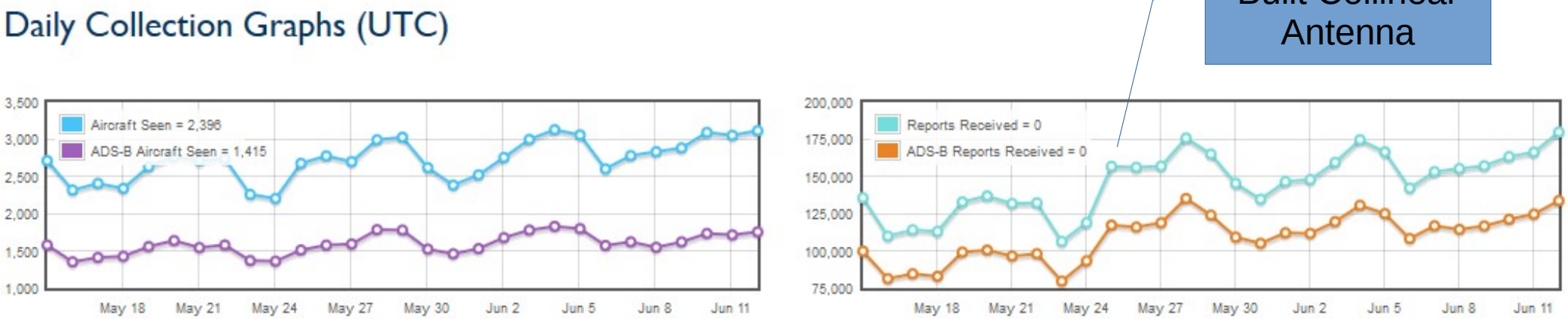



## Positions Reported by Distance from Receiver



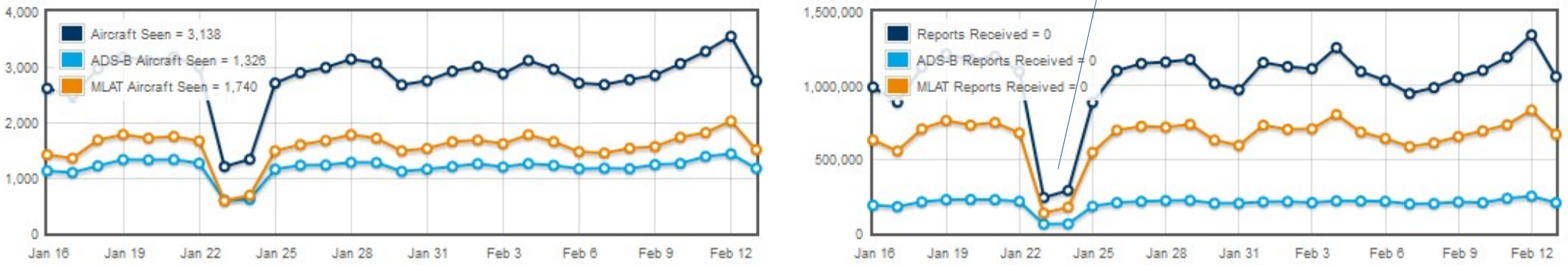
# 30-Day Collection Statistics

Built Collinear Antenna




2nd Floor Bedroom Antenna: May 15 – Jun 12, 2015

January 2016 Blizzard




Attic Antenna: Jan 16 – Feb 13, 2016

# FlightAware.com 30-Day Ranking

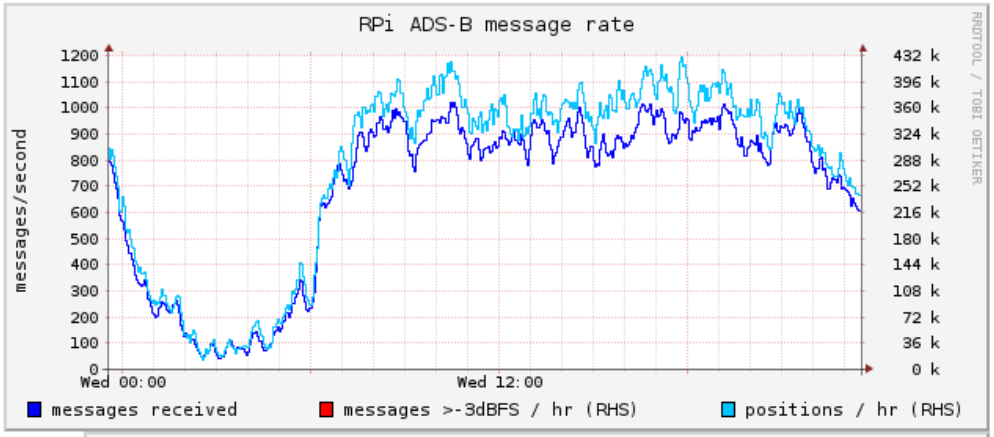
30 Day Ranking

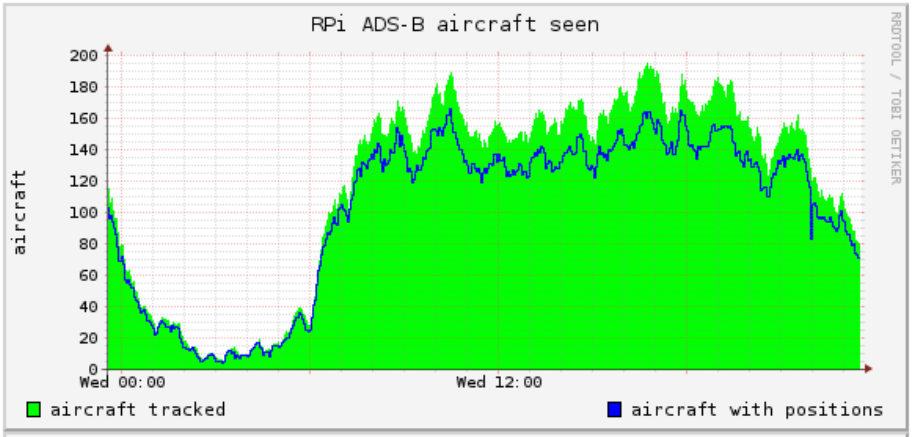
| Rank | | Username | Joined | Last Seen | Days Feeding | ADS-B Aircraft Seen Total | ADS-B Aircraft Seen Daily Average | ADS-B Positions Reported Total | ADS-B Positions Reported Daily Average | MLAT Aircraft Seen Total | MLAT Aircraft Seen Daily Average | MLAT Positions Reported Total | MLAT Positions Reported Daily Average | Nearest Location |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | ↑ | djs | 07-Mar-2015 | Live | 30 | 32,653 | 1,088 | 5,872,279 | 195,742 | 48,108 | 1,603 | 20,334,456 | 677,815 | Madison, WI, United States (KMSN) |
| 32 | ↑ | phillip wolford ★ | 11-May-2015 | Live | 30 | 31,038 | 1,034 | 4,172,847 | 139,094 | 48,969 | 1,632 | 13,159,568 | 438,652 | Galesburg, IL, United States (KGBG) |
| 33 | ↑ | John DeGood ★ | 21-Apr-2015 | Live | 30 | 34,763 | 1,158 | 5,902,650 | 196,755 | 45,690 | 1,523 | 18,826,572 | 627,552 | Wrightstown, NJ, United States (KWRI) |
| 34 | ↑ | lk2855 | 10-Sep-2015 | Live | 30 | 31,043 | 1,034 | 3,790,508 | 126,350 | 48,981 | 1,632 | 9,897,899 | 329,929 | College Park, MD, United States (KCGS) |
| 35 | ↑ | brant | 29-Sep-2015 | Live | 30 | 27,473 | 915 | 2,531,670 | 84,389 | 48,888 | 1,629 | 11,280,473 | 376,015 | Toccoa, GA, United States (KTOC) |

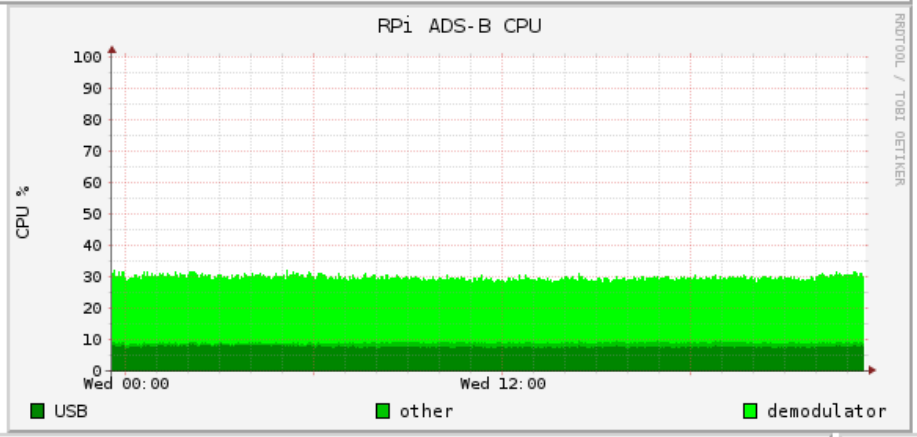
I am ranked #33 of 5246 feeders worldwide

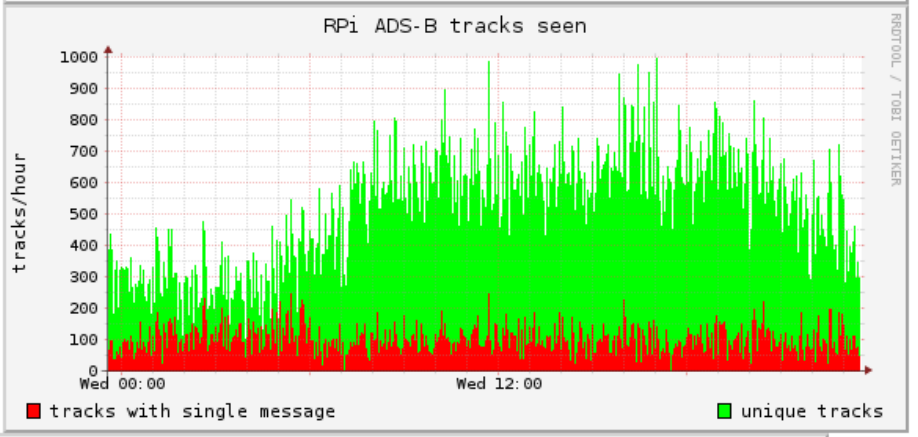
# Collectd: local SDR statistics

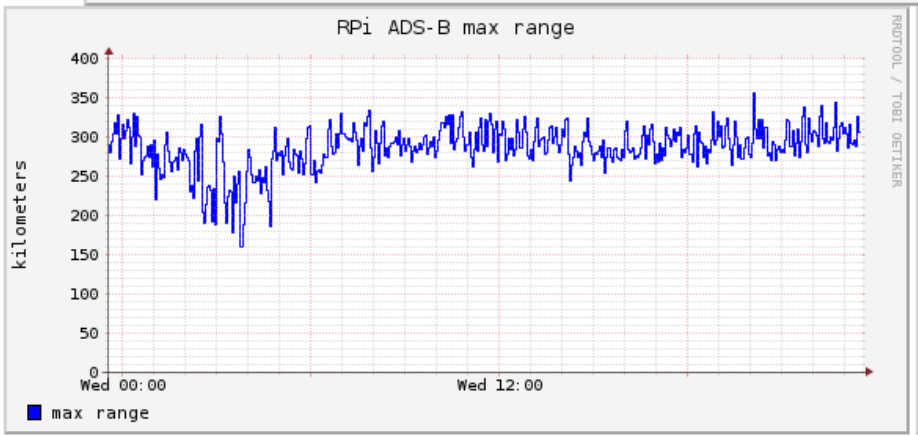
[ day ] [ week ] [ month ] [ year ]

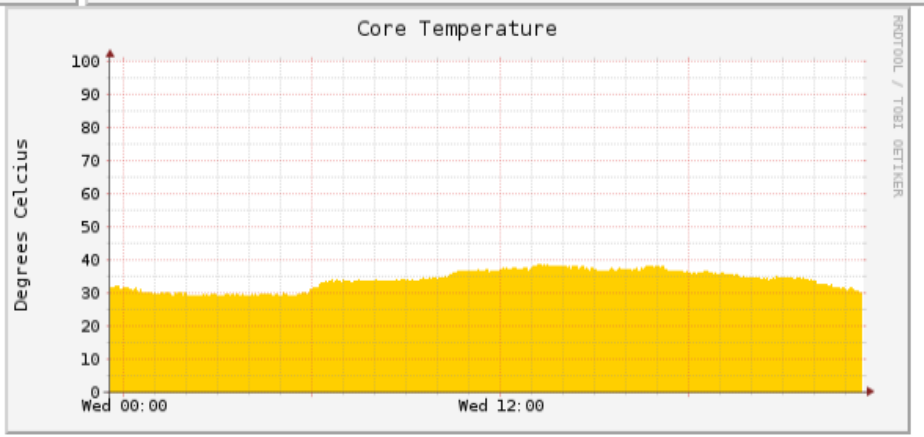


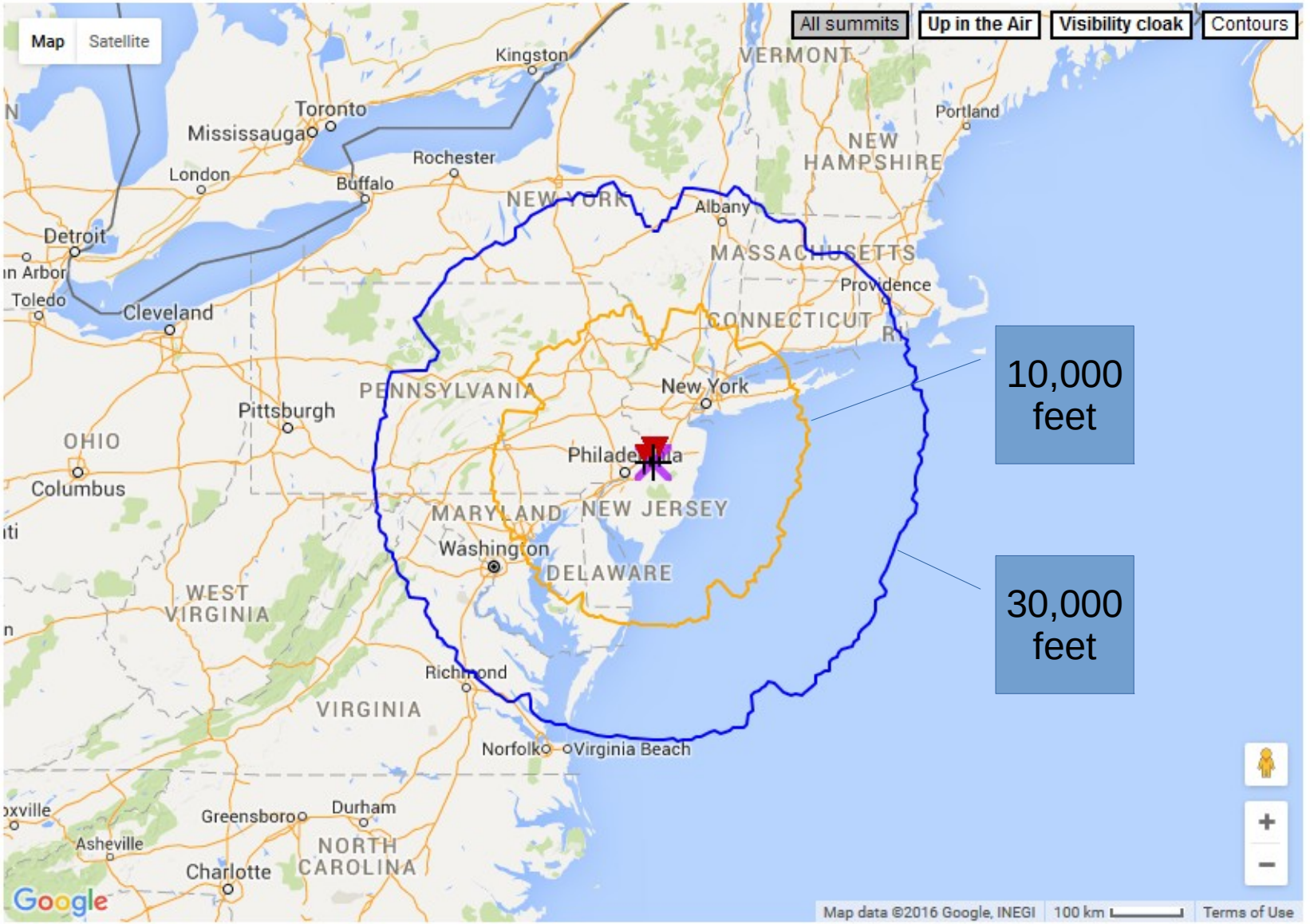



# Reception Examples

# Maximum Line-of-Sight Range

http://heywhatsthat.com/

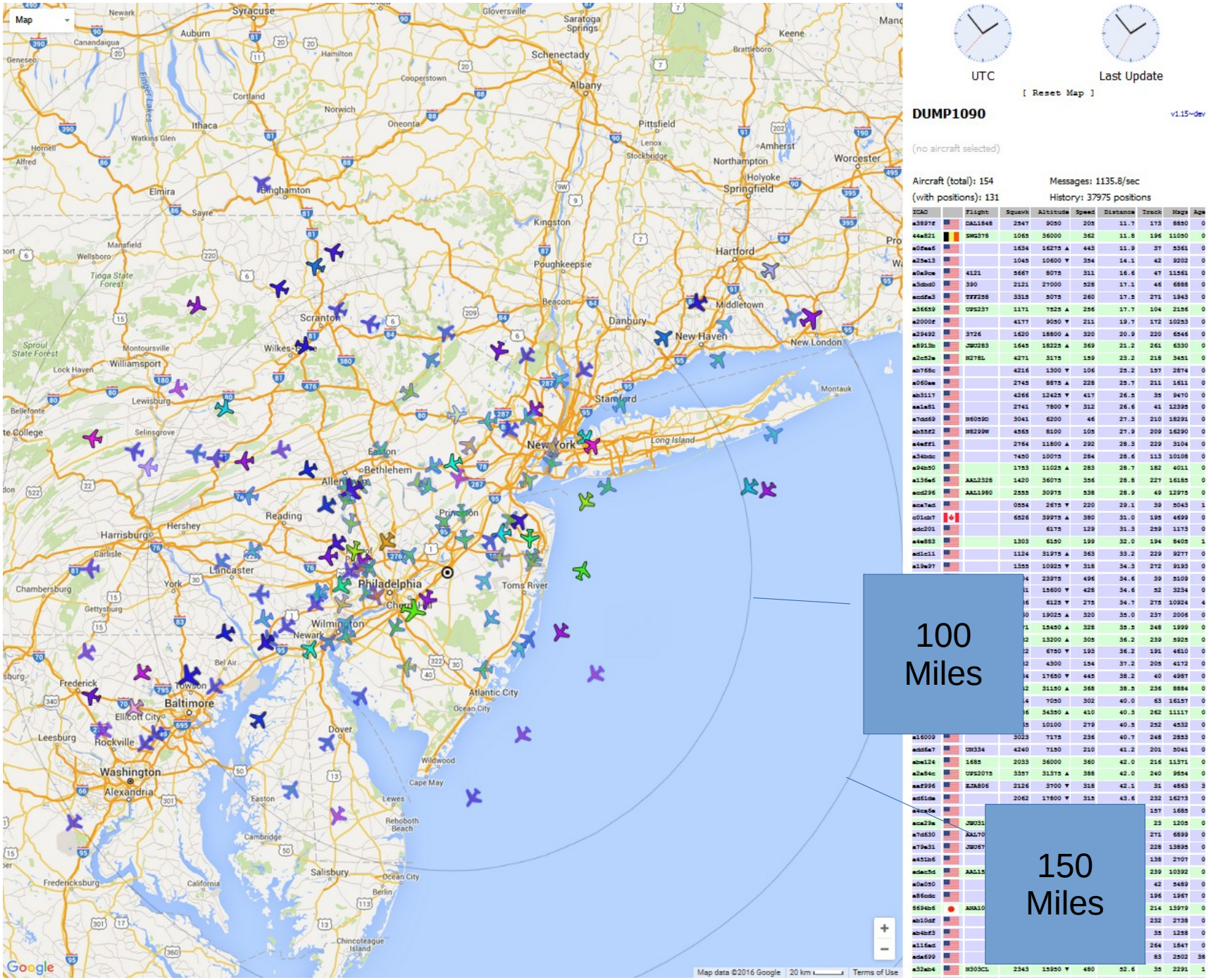



40.0692 N 74.7409 W 92 ft

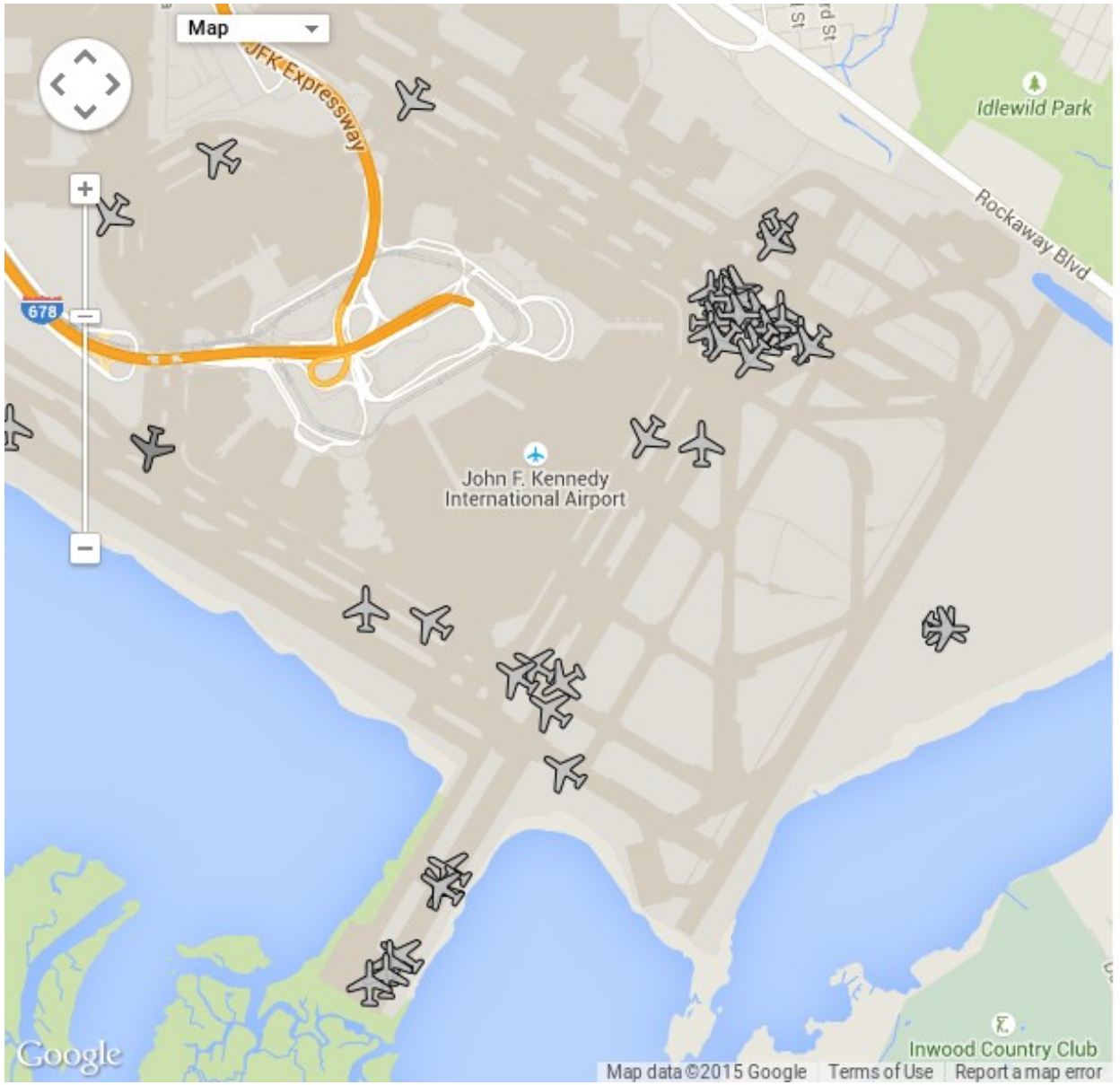
*Click here to re-center map on Home Attic Max Range*

The layers of air cause refraction of radio waves. As a result, radio line-of-sight may extend beyond optical line-of-sight by as much as 50 to 100 nautical miles.

# DUMP1090 Web Display



# JFK Ground via Reflection or Ducting




UTC

Last Update

[ Reset Map ]

**DUMP1090** v1.14

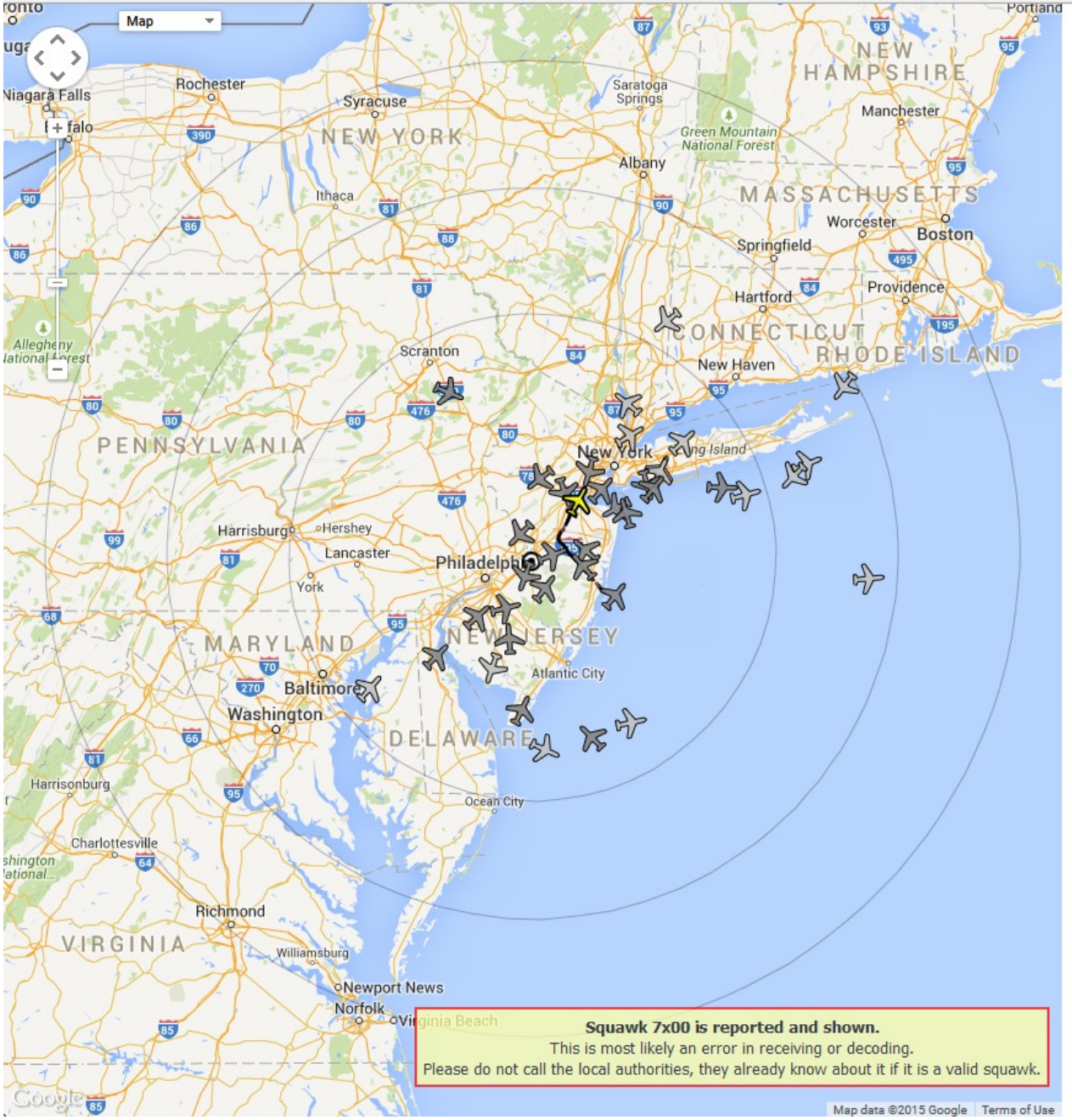
(no aircraft selected)

Aircraft (total): 95 Messages: 252.0/sec

(with positions): 70 History: 4093 positions

| ICAO | Flight | Squawk | Altitude | Speed | Distance | Track | Msgs | Age |
|---|---|---|---|---|---|---|---|---|
| a168f5 | 1507 | 1513 | 20000 | | | | 4580 | 0 |
| ab0405 | 3392 | 2125 | 25000 | | | | 627 | 0 |
| ab2474 | 4677 | 2415 | 29000 | | | | 5201 | 32 |
| a0a053 | 6180 | 2460 | 7775 | | | | 1960 | 4 |
| abd57e | 619 | 3641 | 37000 | 440 | 38.7 | 17 | 4961 | 0 |
| a299c8 | 952 | 1602 | 31000 | | | | 404 | 1 |
| a36553 | 985 | 1555 | 12650 | | | | 2394 | 0 |
| a1682c | AAL2254 | 2116 | 14000 ▼ | 372 | 36.5 | 40 | 3295 | 1 |
| 4ca938 | AZA611 | 3311 | 19475 ▲ | 361 | 67.6 | 111 | 1782 | 1 |
| ab766a | DAL1109 | 3633 | 11575 ▼ | 289 | 46.4 | 148 | 5090 | 0 |
| a406be | FDX1276 | 1505 | 9550 ▲ | 290 | 39.1 | 212 | 1309 | 0 |
| a87c4f | JBU384 | 1601 | 19475 ▼ | 402 | 42.2 | 33 | 1705 | 0 |
| a00054 | N1DG | 4060 | 41000 | 485 | 25.3 | 63 | 1503 | 0 |
| a65451 | N507DW | 3512 | 36225 ▼ | 496 | 128.0 | 215 | 537 | 0 |
| 06a07b | QTR734 | 0552 | 31000 | 503 | 97.2 | 75 | 3161 | 8 |
| 740822 | RJA262 | 1654 | ground | 12 | 55.3 | 194 | 15 | 4 |
| ae0505 | TOPCAT6 | 7067 | 1500 | | | | 5327 | 0 |
| a51ede | UPS1075 | 1752 | 8450 ▲ | 285 | 33.7 | 305 | 508 | 1 |
| a2badf | UPS1083 | 1716 | 26050 ▲ | 460 | 30.9 | 252 | 3740 | 0 |
| a51770 | UPS1125 | | 25 | | 55.1 | | 13 | 45 |
| a533ca | UPS1191 | | 10300 ▲ | 303 | 33.5 | 342 | 156 | 0 |

# Squawk 7700 – General Emergency




UTC Last Update

[ Reset Map ]

**UAL1107** ⇒ A146F9 **Squawking: General Emergency** [FR24] [FlightStats] [FlightAware]

Altitude: ▼ 3550 ft / 1081 m
Squawk: 7700
Speed: 217 kt / 402 km/h
RSSI: -26.4 dBFS
Track: 29° (Northeast)
Last seen: now
Position: 40.468°, -74.336° (59.4s)
Distance from Site: 30.3 NM / 56.1 km

| ICAO | Flight | Squawk | Altitude | Speed | Distance | Track | Msgs | Age |
|---|---|---|---|---|---|---|---|---|
| c0404e | SWG604 | 3632 | 35975 | 449 | 7.1 | 200 | 8973 | 0 |
| 3c4b27 | DLH419 | 2160 | 33000 | 530 | 8.2 | 69 | 4007 | 0 |
| ad03ee | 901 | 1645 | 1800 ▲ | 205 | 11.8 | 225 | 155 | 0 |
| a2c44b | AAL754 | 2776 | 15125 ▲ | 403 | 12.5 | 37 | 2968 | 0 |
| a41e94 | UAL1484 | | 5975 | 260 | 20.8 | 319 | 997 | 0 |
| c07e62 | WJA2739 | 6052 | 40000 | 411 | 21.9 | 312 | 8545 | 1 |
| a1a2b6 | AAL750 | | 11950 ▲ | 367 | 22.7 | 76 | 1477 | 0 |
| a146f9 | UAL1107 | 7700 | 3550 ▼ | 217 | 30.3 | 29 | 5867 | 1 |
| 4cc2a6 | | | 4600 ▼ | 229 | 31.0 | 161 | 3 | 12 |
| a8e4e9 | UAL936 | | 33525 ▲ | 475 | 32.6 | 48 | 905 | 0 |
| a97310 | JBU1579 | | 27975 | 429 | 33.6 | 232 | 577 | 0 |
| acfa13 | AAL878 | | 7050 ▼ | 261 | 34.1 | 356 | 4767 | 14 |
| a874e1 | JBU1202 | 3661 | 11300 ▼ | 410 | 37.1 | 39 | 6845 | 0 |
| a65408 | AAL1860 | 1546 | 9950 ▲ | 283 | 40.3 | 241 | 2947 | 0 |
| acd5ad | AAL2182 | 0522 | 6100 ▼ | 253 | 40.4 | 42 | 6723 | 0 |
| ab5383 | AAL2362 | 3743 | 4325 ▼ | 261 | 42.7 | 344 | 3540 | 0 |
| a445cd | UAL1111 | 3351 | 10150 ▲ | 293 | 43.1 | 196 | 724 | 0 |
| c0787b | TSC810 | 6267 | 36000 | 453 | 47.6 | 199 | 9825 | 20 |
| a1f557 | UAL950 | | 28400 ▲ | 507 | 55.9 | 45 | 313 | 0 |
| a82aac | VRD406 | 7325 | 12375 ▼ | 327 | 55.9 | 165 | 6289 | 0 |
| aa4d77 | JBU1152 | 0707 | 27000 | 509 | 57.4 | 40 | 11780 | 0 |
| a6a00b | JBU84 | 1020 | 31025 ▼ | 466 | 62.2 | 26 | 1281 | 0 |
| ad27f3 | | 2272 | 10375 ▲ | 267 | 63.2 | 26 | 122 | 4 |
| abedc8 | | | 6575 ▲ | 267 | 63.8 | 26 | 34 | 31 |
| 3c4b31 | DLH403 | | 13650 ▲ | 313 | 64.5 | 59 | 91 | 12 |
| 868e7c | ANA1009 | 1147 | 16975 ▲ | 403 | 74.3 | 310 | 1289 | 0 |
| ad1927 | | | 25275 ▼ | 491 | 76.3 | 113 | 99 | 0 |
| a1a66d | AAL837 | | 15975 | 369 | 77.2 | 315 | 494 | 0 |
| a96577 | DAL194 | 7130 | 35000 | 490 | 78.3 | 47 | 11118 | 2 |
| 71005f | SVA038 | | 31000 | 522 | 78.7 | 78 | 3255 | 3 |
| ad08ef | AAL1752 | 6137 | 24775 ▲ | 475 | 79.0 | 115 | 1129 | 0 |
| 4caafb | EIN11C | 3016 | 14450 ▲ | 378 | 82.9 | 92 | 1715 | 6 |
| aacd50 | | 2140 | 26950 | 467 | 85.5 | 42 | 212 | 1 |
| 44007c | AUA94 | 5646 | 35000 | 524 | 91.2 | 75 | 13304 | 3 |
| a895eb | | | 32000 | 438 | 110.9 | 231 | 225 | 3 |
| a67181 | | | 36000 | 432 | 112.3 | 224 | 301 | 55 |
| 44ccda | BEL516 | 2171 | 36975 | 507 | 118.6 | 68 | 13210 | 2 |
| 4951eb | TAP204 | 7601 | 32675 ▲ | 518 | 138.4 | 85 | 9891 | 42 |
| aaee43 | | | 22850 ▼ | 415 | 145.4 | 217 | 205 | 44 |
| a2e9fd | | 3436 | 40000 | | | | 14266 | 1 |

# Security Considerations

# Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
*Network and Security Department*
*EURECOM*
*Sophia-Antipolis, France*
*Email: andrei.costin@eurecom.fr, aurelien.francillon@eurecom.fr*

***Abstract*—In this paper we investigate (in)security aspects of Automatic Dependent Surveillance-Broadcast (ADS-B) protocol. ADS-B is intended to be widely deployed in Air Traffic Management (ATM) Surveillance systems by 2020. One of the goals of ADS-B is to increase safety of air traffic. While the security of ADS-B was previously questioned, in this paper we demonstrate that attacks are both easy and practically feasible, for a moderately sophisticated attacker. Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying of injection).**

**The attacks have been implemented using an Universal Software Radio Peripheral (USRP), a widely available Software-Defined Radio (SDR). for which we developed an ADS-B receiver/transmitter chain with GNURadio. We then present and analyze the results of the implemented attacks tested against both USRP-based and commercial-off-the-self (COTS) radio-enthusiast receivers. Subsequently, we discuss the risks associated with the described attacks and their implication on safety of air-traffic, as well as possible solutions on short and long terms. Finally, we argue that ADS-B, which is planned for long-term use, lacks the minimal and necessary security mechanism to ensure necessary security of the air traffic.**

***Keywords*-Architecture and Design Air Traffic Control, Air Traffic Management, Automatic Dependent Surveillance-Broadcast, ADS-B, message injection, message replay, wireless security, privacy.**

## I. Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) is an Air Traffic Management and Control (ATM/ATC) Surveillance system that is intended to replace traditional radar based systems and is expected to become an essential part of the Next Generation Air Transportation System (NextGen)-like systems. Figure 1 shows an envisioned by [4], and already partially deployed, architecture for the NextGen-like systems, along with ADS-B as part of it.

The concept behind ADS-B is quite simple and can be summarized as follows: ADS-B avionics broadcast a plain text, unencrypted, error-code protected messages over radio transmission links, approximately once per second. Those messages contain the aircraft's position, velocity, identification, and other ATC/ATM-related information.

For the spatial position derivation, ADS-B is designed to use mainly GPS, though GPS is prone to GPS-derived

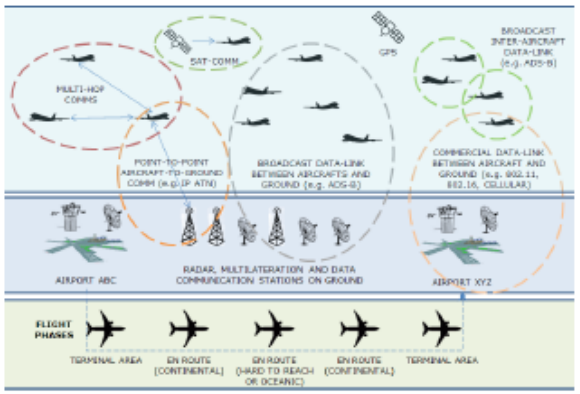



Figure 1. Envisioned NextGen airspace system with ADS-B and e-enabled aircrafts according to [4].

attacks [53], [54]. However, these GPS-oriented attacks are out of scope of this paper, Tippenhauer et al. provides more details on GPS spoofing in [32]. On the other hand, GPS sensors used in ADS-B devices must comply with ADS-B requirements, specifically with RTCA/DO-229C TSO-C145a [24] (e.g. Garmin GDL 90 [59], Freeflight 120x [60] and others). Those standards specify the requirements for integrity checks on GPS signals, hence allowing ADS-B to withstand most GPS-related attacks. On top, [33] suggests inclusion of spatial accuracy parameters in ADS-B messages to enable GPS error computation by the receiver, while [34] proposes the use of Ground-Based Augmentation System (GBAS) to add resilience to unintentional or intentional GPS errors.

ADS-B can be used for several purposes and has the following intended benefits :

- increased safety of the air-traffic management and control. It is intended to dramatically improve situational awareness of pilots, by providing them access to the same kind of real-time air-traffic information as ATC controllers. For example, will receive information from other aircrafts and information about weather and terrain.

Black Hat 2012
Las Vegas, NV
July 25, 2012

Includes a good summary of related work.

# Cited Vulnerabilities

- Disruption of GPS Readings
- Wireless Jamming, Exploitation, Manipulation
- Aircraft Reconnaissance
- Ground Station Flood Denial
- Ground Station Target Ghost Inject
- Ground Station Multiple Ghost Inject
- Aircraft Flood Denial
- Aircraft Target Ghost Inject

# Example ADS-B Attacks

- Replay attack
  - Difficulty: easy
  - Danger: low-moderate
  - Possible Mitigations: radar, multilateration, track discontinuity, group verification
- Synthetic packets
  - Difficulty: moderate-high
  - Danger: moderate-high
  - Possible Mitigations: radar, multilateration, track discontinuity, group verification

Always trust your instruments, son