TBAD Mode-S Upgrade

2014.11.13

Introduction

The TBAD (Transponder-Based Aircraft Detector) system firmware has until recently only decoded Mode-A and Mode-C style transmissions, corresponding to temporarily-assigned identity and altitude, respectively. This 12-bit pattern encapsulates 4096 possible identities and maps to 1280 altitudes at 100 ft spacing.

Not all transmissions from aircraft at TBAD's 1090 MHz frequency are Mode-A and Mode-C signals. Mode-S and some DME (distance-measuring equipment) transmissions occur in this band as well, but with pulse patterns that differ from the Mode-A/C template. The default (original) TBAD firmware is timed specifically to decode Mode-A/C patterns by looking for pulse transitions (causing machine interrupts) at designated times. While unable to decode Mode-S transmissions, characteristic patterns could be observed and noted in the computer log—also applying to DME signals.

By 2020, Air Traffic Control (ATC) will increasingly rely on a new communication protocol from aircraft in order to determine location. This system, ADS-B, involves aircraft broadcasting their GPS-derived positions using a message format adhering to the Mode-S rubric.

Mode-S Upgrade

This motivated development of a new capability for TBAD: to be able to capture Mode-S data packets accurately, for subsequent unpacking/interpretation by the logging computer. TBAD can now scan for the characteristic Mode-S preamble (four pulses differing from Mode-A/C pattern) and either enter a sampling campaign at 1.0 μs cadence for Mode-S or resume interrupt-driven Mode-A/C decoding. The result is that Mode-A/C codes appear as they always did (same message format), but Mode-S packets are sent to the logging computer in hexadecimal format consisting of either 7 or 14 bytes (14 or 28 characters in place of the four octal digits from Mode-A/C).

Example Mode-S Airplane Signals

A sample data capture sequence (redacted to highlight variety of signals) appears below for an airplane responding to Mode-S interrogations from the ground and other aircraft (this is not ADS-B, but standard Mode-S, for which most commercial aircraft are equipped).

```
2014-10-14 16:59:30.764 s3512.D.LF.FE4 107300
2014-10-14 16:59:30.776 s6460.D.LF.FE9   7600
2014-10-14 16:59:30.776 s2000053A12E2C8.D.LF..01 DF-04
2014-10-14 16:59:30.819 s6460.D.LF.FE9   7600
2014-10-14 16:59:30.839 s3512.D.LF.FE4 107300
2014-10-14 16:59:30.877 s28001A2608C05B.D.LF..01 DF-05
2014-10-14 16:59:31.550 s6460..BLF.FE7   7600
2014-10-14 16:59:31.586 s00A1853936D064..BLF..FF DF-00
2014-10-14 16:59:31.619 s3512..BLF.FE2 107300
2014-10-14 16:59:31.669 s59A5F2081980CC..BLF..FF DF-11
```

This is an airplane that: according to Mode-A, is using temporarily assigned ID 3512; and according to Mode-C, is at 7600 feet. The packets appear exactly as they normally do for TBAD, and include only the space-separated field starting with 's' in the examples above. Everything else is added by the logging computer for time-stamping and human readability/interpretation. Note that the squawk ID code, 3512, maps to altitude 107300 ft. In this case, context allows us to understand which is the altitude and which is the ID. But it is not always so easy.

The Mode-S packets adhere to normal TBAD conventions, except that the 4-digit octal code is replaced with 14-character hex codes representing 7 bytes, or 56 bits. The first five bits of each code convey a packet type (DF, or data format), which relates to the information contained in the transmission. In 30 minutes over San Diego, 1250 out of 1500 Mode-S codes received were one of the four types represented above (the other 17% were DF-17 latitude/longitude, discussed below). DF-00 corresponds to an air-to-air surveillance mode, as part of TCAS (traffic collision avoidance system). DF-04 is a surveillance altitude reply, DF-05 is a surveillance identity reply, and DF-11 is an "All-Call" reply. So all of these are interrogated responses. For this flight, in the course of 60 seconds, TBAD recorded 1948 Mode-A (ID), 549 Mode-C (altitude, going from 7800 to 7200 ft), and 174 Mode-S (92 DF-00; 42 DF-04; 32 DF-11; and 8 DF-05).

The information in the Mode-S transmissions above is as follows.

- The DF-04 message says the plane is at 7650 ft (carries 25 ft resolution), and has international airframe ID A5F208 (mixed into three parity bytes at end). This can be looked up on `airframes.org` and in this instance corresponds to the U.S.-registered plane with tail number N482WN—a Boeing 737 operated by Southwest Airlines. The DF-04 codes over one minute steadily descend from 7725 ft to 7250 ft, consistent with the Mode-C trend and limits.
- The DF-05 message says the assigned identity code is 3512 (matching the Mode-A transmission), and is airframe A52F08 (mixed into parity bytes).
- The DF-00 message says the airplane is at 7625 ft, and is airframe A5F208 (mixed into parity). The DF-00 codes over one minute encompass altitudes from 7750 ft to 7100 ft—again consistent with the trajectory of this aircraft.
- The DF-11 message says the airplane is registered as A5F208 (visible directly in the code), this time with parity uncorrupted by other information. In some instances, the last several bits of the parity field contain an identifier for the source of the request—generally one of a handful of ground stations visible to the airplane. By this means, one can generate statistics for how many ground stations are visible to airplanes over the site.

Here we have an example of how useful Mode-S information can be to building a picture of a TBAD event. Any ambiguity over altitude vs. ID are resolved by the ubiquitous DF-00 and DF-04 transmissions—and the DF-05 codes are icing on the cake. Also, the unique identification of the airframe (and associated operator) can help resolve which flight is being tracked (e.g., in reference to Flight Aware or Flight Explorer, etc.). Note that the behavior of Mode-S with respect to beam and saturation flags mirrors that of the Mode-A/C data, cementing further the association between the two.

Example ADS-B Airplane Signals

It gets even better for airplanes equipped with ADS-B equipment (a number that is set to increase). In this case, DF-17 transmissions can encode aircraft position (to 5 meters) and altitude (to 25 ft) in one shot (other DF-17 formats communicate velocity info and other useful bits). Consider this example from 2014.10.14.

```
17:15:40.888 s7624..BLF.FEA  40000
17:15:40.891 s2457..BLF.FE9  -----
17:15:40.908 s2457..BLF.FE9  -----
17:15:40.923 s8DAA77C0601BD57F4011546D5E0A...LF..EB DF-17
17:15:40.943 s4320...LF.FCC   4500
17:15:41.013 s7303...LF.FD0  -----
17:15:41.023 s8D4CA4B560CD85726018DE5F582E..BLF..FF DF-17
```

We have two airplanes simultaneously detected. In this case, squawk-ID codes do not map to altitudes, and one airplane is tripping the 'B' in-beam condition while the other is not. So the separation is clear in this case (not always so): we have a plane with ID 2457 at 40,000 ft triggering in-beam, while a lower airplane at 4,500 ft with ID 7303 is not in the beam.

Note the long-format DF-17 ADS-B codes. One triggers as in-beam while the other does not. The first is airframe AA77C0 (seen "in the clear" in the code), which according to `airframes.org` is registered as N7739A, a Boeing 737 operated by Southwest Airlines. It is at 4525 ft altitude, and at position 32.79214 N, 117.302371 W. The other airplane is 4CA4B5, registered as EI-DRC (registered in Ireland): a Boeing 737 operated by AeroMexico, flying at 40,000 ft at position 32.71542 N, 117.194189 W. Indeed, not only do the DF-17-reported altitudes match those in Mode-C, but which one is "in-beam" also makes sense.

Based on the antenna pointing (172° azimuth, 36.5° elevation, at 32.87415 N, 117.23928 W, we can construct the 3-D geometry to realize that the in-beam aircraft is 5.2° from boresight at a slant-range distance of 21.9 km, while the other is 47° away at a distance of 11.0 km.

The DF-17 transmission has several formats besides airborne position. Heading information (together with vertical rate) is often communicated. An 8-character text message is also common, usually containing flight number, like `UAL1462`.

Impact on Operations

The primary functioning of TBAD is not very much impacted by addition of the Mode-S data sampling technique. All in-beam, saturation, etc. performance is unchanged. Shutter decisions will be made the same as before. The only two impacts anticipated are:

1. Paying attention to longer transmission packets opens up more chances of tripping shutter closure conditions. In the past, if the Mode-S pulses did not trip a beam or saturation condition in the first 25 μs, what happened in the remaining 35–90 μs could not contribute (while the TBAD unit ignored the sky during serial transmit). Now, the entire packet is considered. On the one hand, this is safer. On the other hand, it is more vulnerable to nuisance conditions. Of particular note is signal collision: other codes falling on top of the Mode-S packet causing signal interference that can sometimes lead to false in-beam assertions[1]. The effect should be minor: Mode-S codes are not the bulk of activity, and even over San Diego the total duty cycle is still low. In remote locations this should be of little consequence.

2. The maximum practical capture rate (250 Hz before) is somewhat reduced by the fact that TBAD spends more time transmitting larger packets. What was 16 characters becomes 26 or 40 characters for the different formats. But given that Mode-S signals occupy a minor portion of the total, the impact on speed should be modest (200 Hz)[2]. For remote locations, this is not an issue.

The TBAD logging software requires only a few tweaks to accommodate the interspersed longer-format data blocks. Likewise, any post-analysis code relying on the nominal format is easily modified to either ignore or utilize the new data blocks. The examples above illustrate typical patterns that can be expected from Mode-S.

Optionally, one could integrate decoding of the Mode-S packets into the logging software, or rely on external post-analysis programs to accomplish this task. Because the entire packet is recorded, any detail present in the transmissions may be investigated at a later date with no loss.

This upgrade was put into service at the Apache Point Observatory on 2014.10.24, and has been working without incident. In 12 nights of dome-open operation (totaling 130 hours of on-sky time), TBAD accumulated 370,000 Mode-A/C transmissions and 12,400 Mode-S or ADS-B transmissions. Of the Mode-S types, 31% were DF-00, 10% DF-04, 31% DF-11, and 25% DF-17.

Summary

Mode-S decoding adds a substantial dimension to TBAD logging and analysis. Unlike Flight Explorer and similar products, the data are real-time, higher-cadence, and integrated with the TBAD log. It is not a complete replacement to flight tracking services, because it cannot report on unseen airplanes. It *can*, however, add significant power to interpretation and analysis—removing key uncertainties and providing critical linkages between TBAD data and other resources (otherwise the only linkage between datasets is altitude).

The upgrade package can be provided for a price $750 per operational unit. Included will be the assembly and HEX codes for reprogramming the PIC microcontroller, and support in affecting the program transfer, if needed. Also provided will be Python code used to unpack the Mode-S transmission data, as well as support to add to this library as new message formats are encountered/decoded.

Contact Tom Murphy (`tom@aircraft-avoid.com`) or visit `aircraft-avoid.com` for more information. Phone: 858.232.2668.

[1]While it is also possible for pulses to interfere in such a way as to defeat a legitimate in-beam pulse, there is an important asymmetry: all it takes is a *single* pulse in the train to *not* be trampled in order to cause shutter closure (an unlikely conspiracy of timing), while a single false in-beam pulse will trigger a false in-beam condition. Thus the collision failure mode is unlikely to mask a true threat.

[2]ADS-B will become more prevalent over time, but Mode-A/C should become less prolific. Indeed, the FAA is implementing ADS-B in part to mitigate clutter in the 1090 MHz time domain.