Summer Internship

Internship Period: 13 May – 02 August 2019

Final Internship Report, Part 1 - Theories

Author: Tan Xuan De, Kelvin
kelvin.xuande@u.nus.edu, kelvinxuande@gmail.com

This is the first part of a 2-part report which seeks to address the theories and working principles behind the scope of the project.
Although entire subject(s) were studied, the theories and working principles covered here are only those that are of direct relevance and serves as inspiration to the code produced; and is hence not exhaustive/ the complete picture of the subject(s).

In the second part of the 2-part report 'Final Internship Report, Part 2 – Code Documentation', the python code produced is dissected and documented in detail.

Credits and Acknowledgements:

The Author would like to extend his sincere thanks to the people who contributed to the project, including but not exhaustively:

- junzis/pyModeS for the source code on pyModeS and accompanying materials for reference.
- Oliver Jowett for his invaluable time, advice and assistance rendered.
- Project supervisors for the crucial guidance and required hardware.

Contents

Introduction

It has been widely established how and why the use of multi-lateration can potentially act as a 'validation' method to prevent 'spoofing' – where aircrafts (deliberately or otherwise) report false locations to ground stations that are attempting to track them. This poses an airspace security threat, and such a vulnerability should be rectified.
This report thus aims to explore the feasibility of using/ 'eavesdropping' both mode S and mode A/C aircraft transponder transmissions for the purpose of multi-lateration, and at the same time discuss some considerations that would be required to carry out such an operation.

Literature Review of Relevant Theories

Primary surveillance radar

On the ground, primary surveillance radar transmits a narrow radio frequency (RF) beam using a rotating antenna. Any target in the beam path will reflect some energy. The elapsed time between the transmission and the energy return can then be calculated and by considering antenna position, a precise bearing and distance can be displayed on a two-dimensional radar screen.
This type of surveillance technique is able to detect non-cooperative targets and has a moderate update rate and accuracy.

Secondary surveillance radar

In addition to the primary radar, a secondary surveillance radar (SSR) provides the controller with aircraft identification or altitude information. This is done by either 'actively' interrogating transponders on-board aircrafts, or by passively listening for their 'unsolicited' transmissions (only for mode S). These transmissions come in the form of 'pulse groups', and they either provide aircraft identification data, altitude information, or both.
This allows air traffic controllers to identify and provide guidance to the flight crews and to maintain adequate separation with other aircrafts for safety. More recent versions enable aircraft to recognize other aircraft in the area and subsequently provide alerts to the flight crew so they can avoid potential hazards. This forms the basis for a Traffic Collision Avoidance System (TCAS).
This type of surveillance technique can only detect cooperative targets and has a high update rate and accuracy.

Automatic Dependent Surveillance Broadcast (ADS-B)[1]

Automatic: No pilot input required, no interrogation necessary from the ground.
Dependent: Extremely accurate position and velocity vector from aircraft (e.g. GPS).
Surveillance: Carries comprehensive information such as Aircraft position, altitude, velocity vector, and much more. ADS-B provides automatic, accurate routine reports at a high update rate ~ (e.g. every 0.5 seconds, rate determined by avionics). These reports are visible to other aircraft.

<table>
<tr><th>TCAS</th><th>ADS-B</th></tr>
<tr><td>24 bit code DF11 acquisition squit
<table><tr><td>Control</td><td>24 bit Aircraft Address</td><td>Parity</td></tr></table></td><td><table><tr><td>Control</td><td>24 bit Aircraft Address</td><td>56 bit ADS-B message</td><td>Parity</td></tr></table></td></tr>
</table>

Transponder modes[2]

There are several possible message modes that an on-board aircraft transponder can transmit. This mode depends on the available functional transponder type on-board, and the type of interrogation it receives (which it then responds to with the corresponding mode).

[1] https://www.icao.int/Meetings/AMC/MA/2005/ADSB_SITF4/sp01.pdf
[2] https://en.wikipedia.org/wiki/Aviation_transponder_interrogation_modes

1. **Mode A:**
   When the transponder receives an interrogation request, it broadcasts the configured transponder code (or "squawk code"). This is referred to as "Mode 3A" or more commonly, Mode A.
2. **Mode A with Mode C:**
   Mode A transponder code response can be augmented by a pressure altitude response, which is then referred to as Mode C operation. Pressure altitude is obtained from an altitude encoder, from either a separate self-contained unit mounted in the aircraft or an integral part of the transponder. The altitude information is passed to the transponder using a modified form of the modified Grey code called a Gillham code. Mode A and C responses are used to help air traffic controllers identify an aircraft's position and altitude on a radar screen, in order to maintain separation.
3. **Mode S:**
   Another mode called mode S (Select) is designed to help avoiding over interrogation of the transponder (having many radars in busy areas) and to allow automatic collision avoidance. mode S transponders are compatible with Mode A and Mode C Secondary Surveillance Radar (SSR) systems.
   This is the type of transponder that is used for TCAS or ACAS II (Airborne Collision Avoidance System) functions, and is required to implement the extended squitter broadcast, one means of participating in ADS-B systems. A TCAS-equipped aircraft must have a Mode S transponder, but not all Mode S transponders include TCAS. *Likewise, a Mode S transponder is required to implement 1090ES extended squitter ADS-B Out, but there are other ways to implement ADS-B Out (in the U.S. and China). The format of Mode S messages is documented in ICAO Doc 9688, Manual on Mode S Specific Services.*
   Upon interrogation, Mode S transponders transmit information about the aircraft to the SSR system, to TCAS receivers on board aircraft and to the ADS-B SSR system. This information includes the call sign of the aircraft and/or the aircraft's permanent ICAO 24-bit address (which is represented for human interface purposes as six hexadecimal characters.) One of the hidden features of Mode S transponders is that they are backwards compatible; an aircraft equipped with a Mode S transponder can still be used to send replies to Mode A or C interrogations.

Depending on the message's downlink format, the ADS-B message may contain different information:

1.1.1. Message structure

An ADS-B message is 112 bits long, and consists of 5 parts.

```
+--------+--------+-----------+--------------------------+---------+
|  DF 5  |  ** 3  |  ICAO 24  |          DATA 56         |  PI 24  |
+--------+--------+-----------+--------------------------+---------+
```

Any ADS-B must start with the Downlink Format 17, or 18 in case of TIS-B message. They correspond to 10001 or 10010 in binary for the first 5 bits. Bits 6-8 are used as an additional identifier, which has different meanings within each ADS-B subtype.

In following Table 1.1, the key information of a ADS-B message is listed.

Table 1.1. Structure of ADS-B messages

nBits	Bits	Abbr.	Name
5	1 - 5	DF	Downlink Format
3	6 - 8	CA	Capability (additional identifier)
24	9 - 32	ICAO	ICAO aircraft address
56	33 - 88	DATA	Data
	[33 - 37]	[TC]	Type code
24	89 - 112	PI	Parity/Interrogator ID

To identify what information is contained in an ADS-B message, we need to take a look at the `Type Code` of the message, indicated at bits 33 - 37 of the ADS-B message (or first 5 bits of the `DATA` segment).

In following Table 1.2, the relationships between each `Type Code` and its information contained in the `DATA` segment are shown.

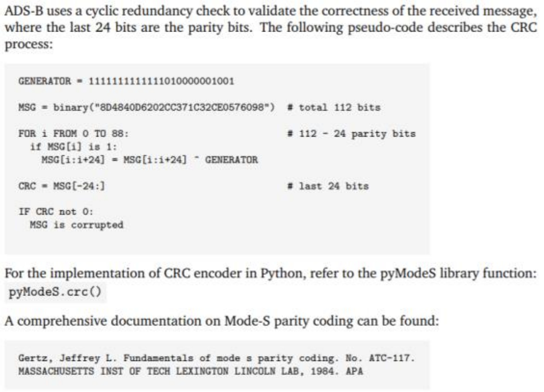
Type Code	Content
1 - 4	Aircraft identification
5 - 8	Surface position
9 - 18	Airborne position (w/ Baro Altitude)
19	Airborne velocities
20 - 22	Airborne position (w/ GNSS Height)
23 - 27	Reserved
28	Aircraft status
29	Target state and status information
31	Aircraft operation status

There is no message format for Mode AC. The payload will either be the Squawk code or Altitude.

For more information on ADS-B mode S messages, review the resources in the Literature review appendix.

Issues with transponders

1. An issue with Mode A/C messages is that they lack the capability/ bits to do cyclic redundancy checking (CRC), as compared to their mode S counterparts. This may potentially compromise their integrity and trustworthiness; and was brought up as a concern by Oliver.



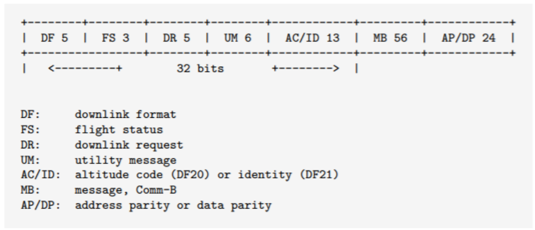
ADS-B uses a cyclic redundancy check to validate the correctness of the received message, where the last 24 bits are the parity bits. The following pseudo-code describes the CRC process:

```
GENERATOR = 1111111111111010000001001

MSG = binary("8D4840D6202CC371C32CE0576098")  # total 112 bits

FOR i FROM 0 TO 88:                           # 112 - 24 parity bits
  if MSG[i] is 1:
    MSG[i:i+24] = MSG[i:i+24] ^ GENERATOR

CRC = MSG[-24:]                               # last 24 bits

IF CRC not 0:
  MSG is corrupted
```

For the implementation of CRC encoder in Python, refer to the pyModeS library function: `pyModeS.crc()`

A comprehensive documentation on Mode-S parity coding can be found:

```
Gertz, Jeffrey L. Fundamentals of mode s parity coding. No. ATC-117.
MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, 1984. APA
```



```
+--------+--------+--------+--------+-----------+---------+-----------+
|  DF 5  |  FS 3  |  DR 5  |  UM 6  |  AC/ID 13 |  MB 56  |  AP/DP 24 |
+-----------------+--------+--------+-----------+---------+-----------+
|  <---------+        32 bits       +--------->  |


DF:     downlink format
FS:     flight status
DR:     downlink request
UM:     utility message
AC/ID:  altitude code (DF20) or identity (DF21)
MB:     message, Comm-B
AP/DP:  address parity or data parity
```

Abstracts on mode S data structure from
"The 1090MHz riddle, an open-access book about decoding Mode-S and ADS-B data" – Junzi Sun
CRC appears to be absent from Mode A/ C

2. An issue with mode S transponders arises when pilots enter the wrong flight identity code into the mode S transponder. In this case, the capabilities of ACAS II and mode S SSR can be degraded.

Figure 1 below illustrates the process of interrogation:

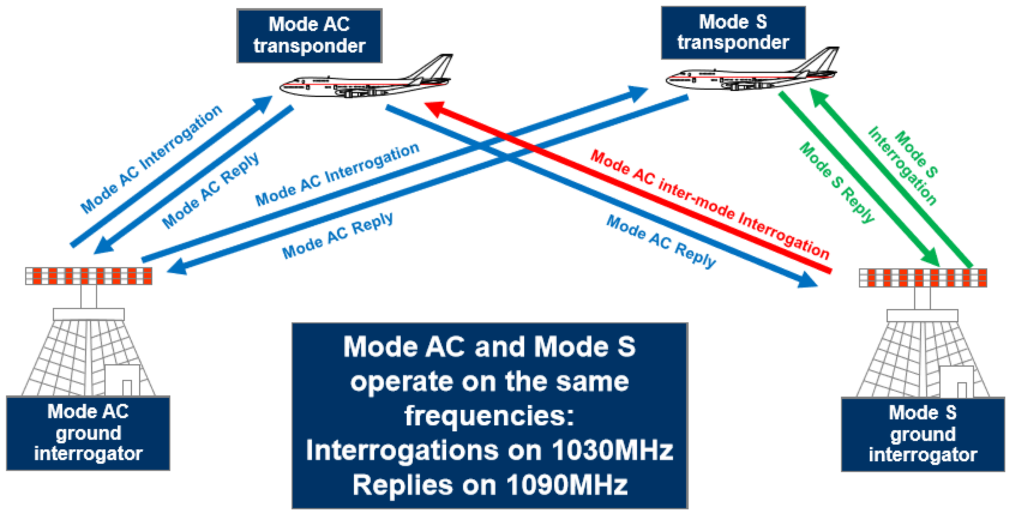


Figure 1: Interrogation in different modes

Key points:

1. We cannot assume that mode S transponders only reply in mode S format. If interrogated by a mode AC ground interrogator, they will reply in mode AC format.
2. By extension, squawk codes that previously appeared in mode S format may also be subsequently be found appearing in mode AC format.

ICAO address vs Squawk code:

ICAO Address[3]:

A unique ICAO address is assigned to each Mode-S transponder of an aircraft. Thus, this is a unique identifier for each aircraft. You can use the query tool (World Aircraft Database) from mode-s.org to find out more about the aircraft with a given ICAO address. For instance, using the previous ICAO 4840D6 example, it will return the result of a Fokker 70 with registration of PH-KZD.

Squawk codes:

Codes distinguish each aircraft. They are typically assigned prior to flight and entered in the transponder control head by a flight crewmember. Certain codes are used when an aircraft is in distress such as 7700 or 7777, and 1200 represents that the aircraft is flying using Visual Flight Rules (VFR). This is recognized by the ground-based equipment and is then highlighted on the air traffic controller's screen making them aware of the situation.

Key points:

1. ICAO address can only be extracted from mode S messages.
2. There are several companies that specialise and offer multilateration capabilities e.g. Flightaware, Flight Radar 24. However, they only work with mode S messages. Reasons cited include:
    a. the large number of messages in mode AC format
    b. The difficulty in determining whether the message in mode AC format refers to Squawk code or the altitude.
    c. Noise and errors – these are issues when working with mode AC messages because it does not include CRC parity bits for error checking.
3. However, if we capture and decode the messages that are being transmitted at any point in time; it can be observed that many of these messages are in mode AC format.
4. This would suggest that there are many aircrafts which utilises mode AC format for transmitting messages that are not being tracked.

Interrogations

Most systems contain added protection that would prevent excessive interrogations. This means the transponder will reply to a maximum of 2,000 requests per second. The normal interrogation rate is about 400 per second[4].

1. The *rate of TCAS interrogations to a Mode S aircraft* depends on the range and the closure rate. Between 1 interrogation every 5 seconds and 1 interrogation per second[5].

2. The Mode S transponder outputs an unsolicited transmission once per second to enable ACAS to acquire Mode S equipped aircraft[6].

    a. The so-called 56-bit Short Squitter (SS), which is transmitted once per second. This short squitter is used for surveillance, where the 24-bit MODE S ADDRESS field embodies the selective interrogation of aircraft addresses consisting of 2 sub-fields, a 9-bit sub-field that identifies the country, and a 15-bit sub-field the identifies the aircraft. Each ES transmission contains the aircraft address, which permits an unequivocal association between the data in the various squitter formats and the originating aircraft.
    b. The 112-bit Extended Squitter (1090 ES), in addition to the 56 bits of the SS, contains the 56-bit ADS-B message. There are three standards for the ES: RTCA/DO260, RTCA/DO-260A

[3] The 1090MHz riddle, an open-access book about decoding Mode-S and ADS-B data – Junzi Sun
[4] https://www.aviationpros.com/home/article/10386629/transponders-they-make-the-whole-system-work
[5] https://www.icao.int/MID/Documents/2019/MICA/MICA-MID%20-%20WP%2002%20-%20Mode%20S%20Surveillance%20Principle.pdf
[6] https://www.sigidwiki.com/images/1/15/ADS-B_for_Dummies.pdf

and RTCA/DO-260B. These standards correspond, respectively, to Versions 0, 1 and 2, to ICAO Doc 9871.

3. Broadcast of parameters, per aircraft:

    a. DF17 Extended Squitter (long Mode S message) on 1090MHz. When aircraft is airborne, it typically transmits airborne position – 2 per second and Airborne Velocity – 2 per second.
    b. ACID – 1 every 5 seconds
    c. Max 6.2 extended squitter per second

Abstract from European Technical Standard Order, European Aviation Safety Agency[7]:

> *Reply Rate Control.*
>
> *A sensitivity-reduction type reply rate control must be provided. The range of this control must permit adjustment of the reply rate to any value between 500 replies per second and the maximum rate of which the transponder is capable, or 2,000 replies per second, whichever is the lesser, without regard to the number of pulses in each reply. Sensitivity reduction in excess of 3 dB must not take effect until 90 percent of the selected reply rate is exceeded. The sensitivity must be reduced by at least 30 dB when the rate exceeds the selected value by 50 percent. The reply rate limit must be set at 1,200 replies per second or the maximum value below 1,200 replies per second of which the transponder is capable.*
>
> *Transponder Reply Rate Capability.*
>
> *For equipment intended for installation in aircraft that operate at altitudes above 15,000 feet, the reply rate capability must be a least 1,200 reply groups per second for a 15 pulse coded reply. For equipment intended for installation in aircraft that operate at altitudes not exceeding 15,000 feet, the reply rate capability must be at least 1,000 reply groups per second for a 15 pulse coded reply.*

Key points:

1. Transponders will reply when solicited/ interrogated, if the total number of such interrogations do not exceed a maximum of 2,000 requests per second. It is assumed that this is also applicable for mode AC transponders.
2. Minimum number of transmissions does not appear to be of importance here. Regardless of the minimum, the server should be prepared for the maximum number of transmissions.

Literature review appendix:

For more information, consider reviewing the following documents on addition to the sources cited in the footnotes of each page:

1. Aeronautical Telecommunications, Volume IV: Surveillance and Collision Avoidance Systems

2. Jetvision/ Radarcape's overview on Aircraft modes:
   What actually is Mode-A/C, Mode-S and ADS-B? A brief overview.

[7] https://www.easa.europa.eu/download/etso/ETSO-C74d_CS-ETSO_0.pdf

Multilateration[8]

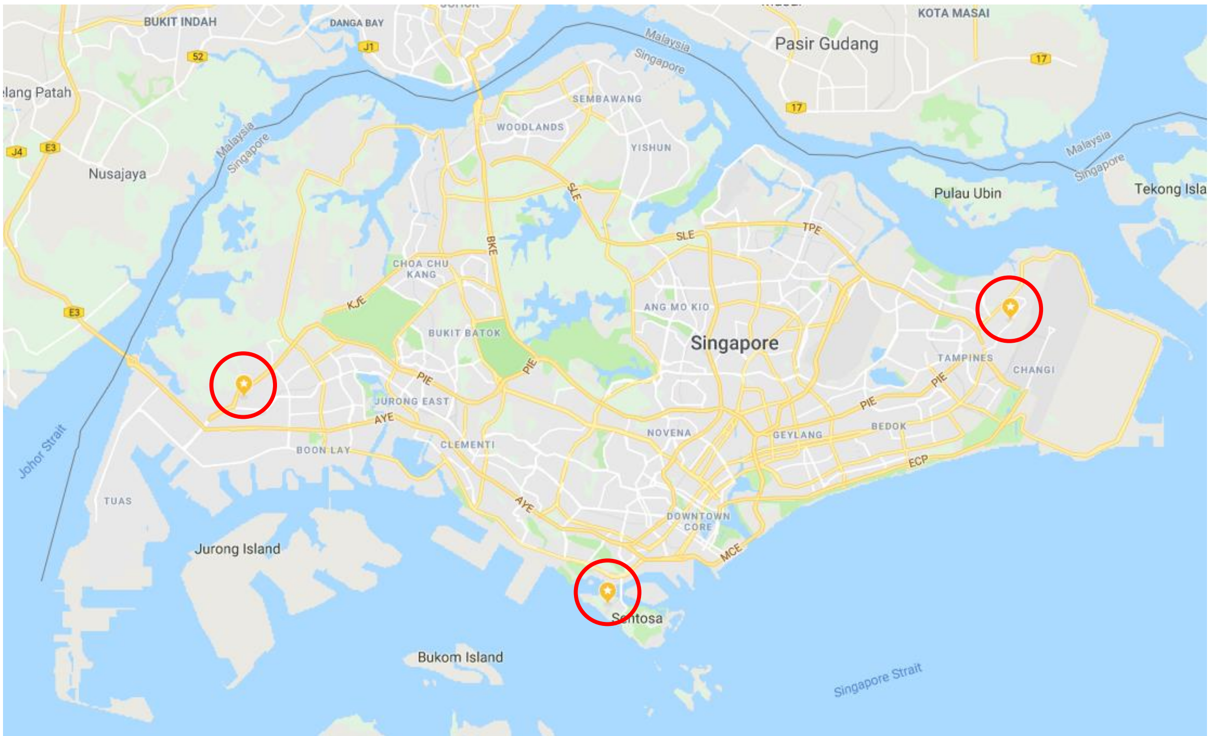
Multilateration is a time-tested technology that was developed for military purposes to accurately locate aircraft. It works by utilising Time Difference of Arrival (TDOA) and is effective in tracking aircraft that do not wish to be "seen".

> *Multilateration requires no additional avionics equipment, as it uses replies from Mode A, C and S transponders, as well as military IFF and ADS-B transponders. Furthermore, while the radar and multilateration "targets" on a controller's screen are identical in appearance, the very high update rate of the multilateration-derived targets makes them instantly recognizable by their smooth movement across the screen. A screen displaying multilateration information can be set to update as fast as every second, compared with the 4 - 12 second position "jumps" of the radar-derived targets.*

<u>Working principle:</u>

Multilateration requires several ground stations - at least 3, or at least 4 if altitude information is desired[9]; to be positioned in strategic locations that are as far apart as possible as one another.

Figure 2 illustrates how the positioning of these ground stations can be done for Singapore, with ground station locations denoted by the *red circles*.



Station:	**Location:** *Postal, Latitude, Longitude*
Singapore Discovery Centre **(A)**	*638365, 1.3285491,103.674149*
Sentosa Merlion **(B)**	*099958, 1.2532208,103.8185307*
Changi Museum **(C)**	*507707, 1.3493771,103.9581887*

Figure 2: Positioning of Entities for multilateration

[8] http://multilateration.com/surveillance/multilateration.html
[9] Further Elaborated in 'Calculations'

Table 1 details the distances between the positioned ground stations - **A, B** and **C**.

Ground station-Ground station:	**Distance:**
A – B	*17.89 km*
A – C	*32.97km*
B – C	*21.07km*

Table 1: Distances between the positioned ground stations

These ground stations listen for "replies" which Aircrafts would transmit, typically in response to interrogation signals from the local airspace controller.

Since 'target' aircrafts would be at different distances from each of the ground stations that we have positioned, the 'same' reply transmitted by a 'target' aircraft would be received by each of the positioned ground stations (ideally all of them) at different times.

We can then visualise this as a message set, where within each message set, there are ideally **n** number of timestamps, where **n** is the number of positioned ground stations.

<u>Calculations for Emitter Location[10]:</u>

Suppose the emitter is an unidentified airplane (or an airplane transmitting messages in mode-a/c) at an unknown location (x, y, z) that we wish to locate. There are primarily 2 methods to resolve the complicated simultaneous equations problem; either *graphically* or *resolving the equations directly*.

Graphical Approach[11]:

This approach requires at least 3 receivers at known locations and in return provides the (x, y) coordinates of the emitter's location.

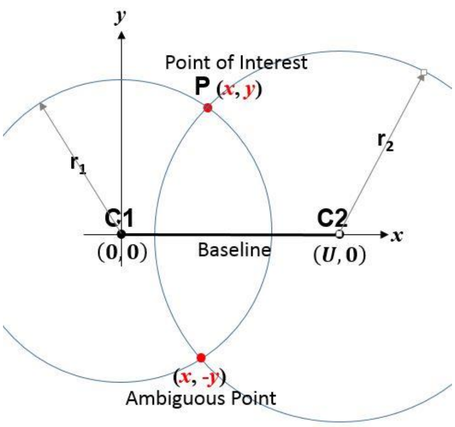


Figure 3: Cartesian true range multilateration (trilateration) scenario. **C1** and **C2** are centres of circles having known separation. **P** is point whose (x, y) coordinates are desired based on U (separation between the 2 receivers) and measured ranges r1 and r2.

Consider first, two circle centres (which are also our receiver stations) **C1** and **C2** in *Figure 3*, which have known (x, y) locations.

Information on their locations also allow us to find U – the distance of separation between these 2 receiver stations.

We wish to find the (x, y) coordinates of P, our point-of-interest. This can be done with Pythagoras's theorem as shown below:

$$r_1^2 = x^2 + y^2$$

$$r_2^2 = (U - x)^2 + y^2$$

$$x = \frac{r_1^2 - r_2^2 + U^2}{2U}$$

$$y = {}^{+}/_{-} \sqrt{r_1^2 - x^2}$$

However, this calculation would give us two possible points; the actual (x, y) coordinates of our point-of-interest, and the (x, y) coordinates of an Ambiguous point. To determine the actual (x, y) coordinates of our

[10] http://wiki.gis.com/wiki/index.php/Multilateration
[11] https://en.wikipedia.org/wiki/True_range_multilateration#Solution_methods

point-of-interest from the two possible points, we can utilise a third receiver station which mathematically 'confines' the y-axis to 1 possible plane and hence the solution.

Resolving the simultaneous equations directly[12]:

To calculate for the plane's location, we can also deploy a multilateration system that consists of either 3 or 4 receiver site 'ground stations' at known locations: **A**, **B**, **C** and **D**.

- Having a system with 3 receiver site 'ground stations' allows us to derive the (x, y) coordinates of P, our point-of-interest.
- Having a system with 4 receiver site 'ground stations' allows us to derive the (x, y, z) coordinates of P, our point-of-interest. An additional altitude information is obtained.

With 4 receiver site 'ground stations':

The travel time (T) of pulses from the emitter at (x, y, z) to each of the receiver locations is simply the distance divided by the pulse propagation rate (c):

$$T_A = \frac{1}{c}\sqrt{(x-x_A)^2+(y-y_A)^2+(z-z_A)^2}$$
$$T_B = \frac{1}{c}\sqrt{(x-x_B)^2+(y-y_B)^2+(z-z_B)^2}$$
$$T_C = \frac{1}{c}\sqrt{(x-x_C)^2+(y-y_C)^2+(z-z_C)^2}$$
$$T_D = \frac{1}{c}\sqrt{(x-x_D)^2+(y-y_D)^2+(z-z_D)^2}$$

If the site **A** is taken to be at the coordinate system origin, then

$$T_A = \frac{1}{c}\sqrt{x^2+y^2+z^2}$$

Then the **time difference** of arrival between pulses arriving directly at the central site and those coming via the side sites can be shown to be:

$$\tau_C = T_C - T_A = \frac{1}{c}\left(\sqrt{(x-x'_C)^2+(y-y'_C)^2+(z-z'_C)^2} - \sqrt{x^2+y^2+z^2}\right)$$
$$\tau_D = T_D - T_A = \frac{1}{c}\left(\sqrt{(x-x'_D)^2+(y-y'_D)^2+(z-z'_D)^2} - \sqrt{x^2+y^2+z^2}\right)$$

where $(x'_B,\ y'_B,\ z'_B)$ is the location of receiver site *B* with respect to the origin located at site *A*, etc., and c is the speed of propagation of the pulse, often the speed of light. Each equation defines a separate hyperboloid.

The multilateration system must then solve for the unknown target location (x, y, z) in real time with respect to site 'A' as its origin. All the other symbols are known.

With 3 receiver site 'ground stations':

$$\tau_B = T_B - T_A = \frac{1}{c}\left(\sqrt{(x-x'_B)^2+(y-y'_B)^2} - \sqrt{x^2+y^2}\right)$$
$$\tau_C = T_C - T_A = \frac{1}{c}\left(\sqrt{(x-x'_C)^2+(y-y'_C)^2} - \sqrt{x^2+y^2}\right)$$

Source: Multilateration, Wikipedia

For more information, consider reviewing the document 'Aircraft Navigation and Surveillance Analysis for a Spherical Earth, by Michael Geyer'; on addition to the sources cited in the footnotes of each page.

[12] http://wiki.gis.com/wiki/index.php/Multilateration

Estimations:

This section explores a test-case to get a ballpark estimate of the time differences of flight that can be expected. The maximum time difference of flight of the same message to the different receiver site 'ground stations' is also calculated.

Ballpark estimate of time differences of flight

Consider the following scenario:

1. Suppose we have location details for P, our point-of-interest (denoted by the yellow star in *Figure 4* below):

Point-of-Interest (P)	**Location:** *Postal, Latitude, Longitude*
Sembawang God of Wealth Temple	*757611, 1.4496186,103.786974*

2. Positioned receiver site 'ground stations' as before, but in this analysis; we are aware of the distance between each receiver site 'ground station' from P.

Ground station, from P	**Distance:**
Singapore Discovery Centre **(A)**	*20.45 km*
Sentosa Merlion **(B)**	*23.09 km*
Changi Museum **(C)**	*21.17 km*

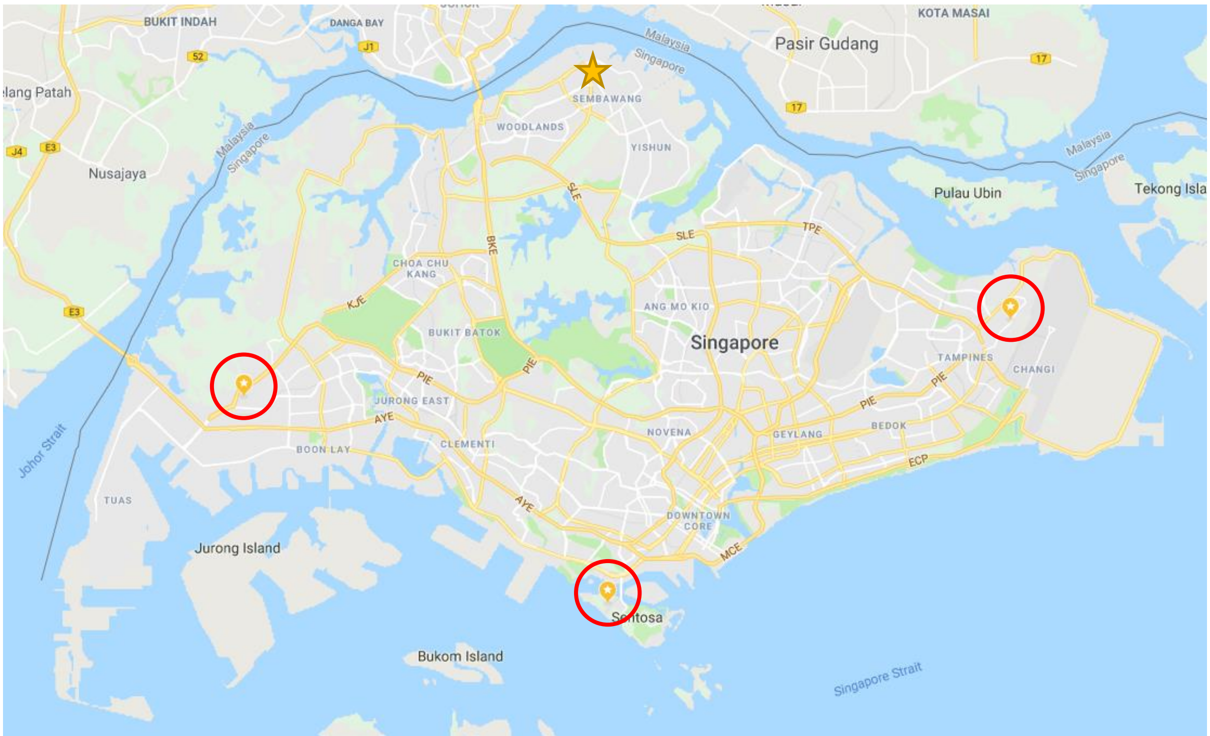


Figure 4: Distances between the positioned ground stations

Radio waves travel at the speed of light, and hence the time taken for the signals broadcasted by the Airplane (at point P) to reach our individual receiver site 'ground stations' can be computed with the following formula:

$$t = \frac{d}{c}$$

Where, t = time taken for the signal to travel in seconds,

d = distance in km

c = speed of light (299792.458km/s)

With the formula, we construct *Table 2*, which shows the time taken for the signals to travel from point P to our ground stations, as well as the time difference of flight:

Ground station, from P:	**Distance:**
Singapore Discovery Centre **(A)**	$6.8213857\ x\ 10^{-5}\ s$
Sentosa Merlion **(B)**	$7.701994958\ x\ 10^{-5}\ s$
Changi Museum **(C)**	$7.06155\ x\ 10^{-5}\ s$
Ground station – Ground station:	**Time difference of flight:**
B – A	$0.880609\ x\ 10^{-5}\ s$
B – C	$0.640445\ x\ 10^{-5}\ s$
C – A	$\underline{0.240164\ x\ 10^{-5}\ s}$

Table 2: Time taken and time difference of flight

Maximum time difference of flight

This section explores estimating the maximum time difference of flight to different receiver site 'ground stations' for a single valid message.

Consider the following scenario:

1. We have deployed several receiver site 'ground stations', 2 of which are at the maximum possible distance from each other (for Singapore). 2 of such possible positions have been circled in red, with a red double-headed arrow between them, as shown in *Figure 5* below.
2. To estimate for the maximum time difference of flight to these two receivers, we consider the 'target' emitter aircraft to be somewhere along the blue dotted line, outside the airspace of Singapore.
3. We can then estimate the maximum time difference of flight to be:

Side – Station name	**Distance separation, Maximum difference in Time difference of flight:**
Left – Singapore Discovery Centre	*32.96km,*
Right – Changi Museum	$1.0994\ x\ 10^{-4}$ *s for signal to travel*

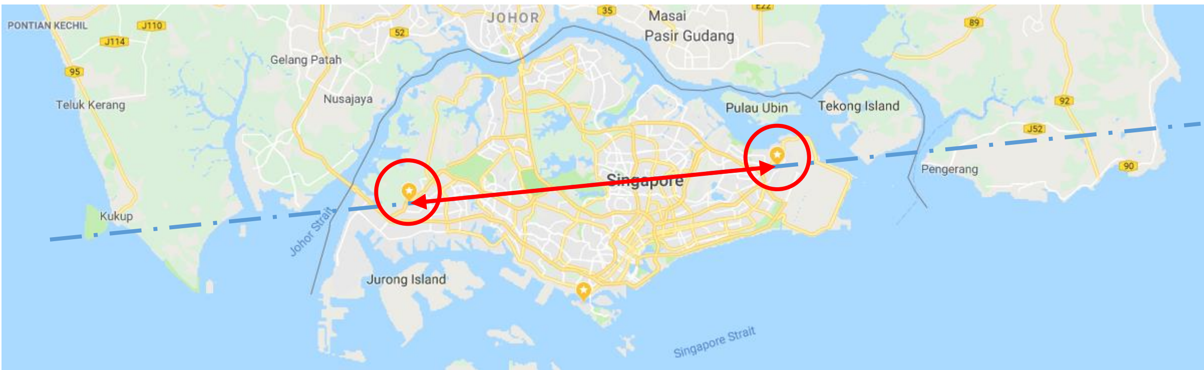


Figure 5: Calculation of maximum time difference of flight

Designs

Having covered the fundamentals via a literature review of materials that are directly relevant to the code, this section shares some insights into the designed solution, using some of the proposed hardware and software (discussed at a higher level).

Problem Recap:

There are many aircrafts which utilises mode AC format for transmitting messages; that are not being tracked.

Objectives:

To investigate the feasibility of capturing both mode s and mode a/c signals, and thereafter use the time difference of flight of these signals to determine aircraft locations (multi-lateration).

Required hardware:

1. Radarscope BEAST:
    a. ADS-B receiver capable of timestamping received ADS-B messages with a GPS time accuracy of +/- 50 nanoseconds (ns) for each signal
    b. Datasheet and documentation: https://wiki.jetvision.de/wiki/Radarcape:Contents
    c. Specifications: DC 5V/ 1A, Manufacturer: jet vision
2. BUNDLE:
    a. "Active Diapason" Antenna (1090 MHz)
    b. 20 m Antenna Cable
    c. Specifications: 1090 MHz, Manufacturer: jetvision
3. Bias Tee:
    a. Specifications: 0.1 - 2 GHz, DC 5V – 12V/ 200mA

Available data streams from Radarcape:

Extracted from Radarcape manual:

Data Streaming to Network (TCP and UDP)

- *TCP or UDP port 10002:* This is a CRC-checked mirror of the data as it comes from the FPGA, DF-11, DF-17 and DF-18. Includes Mode-A/C data with respect to the configuration setting.
- *TCP or UDP port 10003:* Binary formatted raw data with all Modes-S data formats CRC-prechecked (eliminates transmission of the erroneous frames, reduces load on the network). All data from the FPGA is disassembled into messages and verified if correct.
- *TCP or UDP port 10004:* Binary formatted raw data, pre-checked DF-11, DF-17 and DF-18 only: minimum load for the transmission path but contains most information. No Mode-A/C data.
- *TCP or UDP port 10005:* Binary formatted raw data, only raw data frames of those aircraft where the location (latitude and longitude) is unknown. Used for special MLAT purposes. No Mode-A/C data.

The binary and AVR raw data formats are identical to those of the Mode-S Beast and documented in *Mode-S_Beast:Data_Output_Formats*. For the Radarcape, there is one additional message that contains timestamp and FPGA configuration information, which is triggered by each 1PPS from the GPS module.

Port 30003 Service (TCP, UDP, and USB-serial)

Port 30003 style output (e.g., for use with SBS Plotter) can be provided without the need of an additional application on your PC.

The Radarcape provides this data stream on TCP port 30003, UDP port 30003, and the serial USB interface.

The format of the data output can be found in this document

The *date* in Port 30003 messages is always the *Linux system date*.

The *timestamp* instead is a *GPS timestamp* when the configuration is set to GPS timestamps and system time when the Radarcape operates in legacy 12 MHz time stamp mode.

Due to the low efficiency and high processor load caused by this protocol, please do not use Port 30003 unless really necessary.

A better way of getting the same data is the deltaDB service.

On Linux, a very simple method how to access the TCP stream of Port 30003 is socat:

```
socat - TCP:radarcape:80
```

USB Serial Port Data Access

The Radarcape supports one selectable data stream out of following sources on a virtual serial port via the back side USB port:

- Raw FGPA data - including Mode-A/C data
- CRC pre-checked Mode-S with Mode-A/C data
- Mode-S Frame types DF-11, DF-17 and DF-18 only
- Mode-S Frames of all aircraft without a known location
- Port 30003 format

The output can be selected in the configuration menu. Due to processor load, it is recommended to keep this feature disabled when not required.

Output Settings

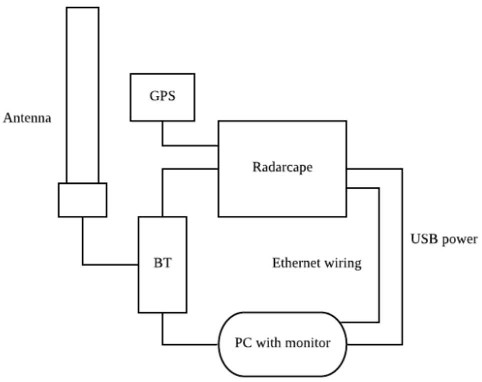
Data Stream on USB Serial Interface (Mode-S Beast compatibility)

- ○ disabled
- ◉ Raw FPGA data with Mode-A/C
- ○ Mode-S CRC pre-checked with Mode-A/C
- ○ DF11,17,18
- ○ Non ADS-B Aircraft
- ○ Port 30003

radarcape_manual.pdf

RCport_30003.pdf

Proposed hardware set-up:



Software Design (high level)