Detection of Secondary Surveillance Radar (SSR) Spoofing using Signal Multilateration

Wang Beini
17S06F
Raffles Institution
Singapore
beiniwang23@gmail.com

***Abstract*—With globalization and increasing interconnectivity, there has been a rapid rise in air traffic flow - there was a 1 million increase in flight count from 36.4 million commercial flights worldwide in 2013 to 37.4 million in 2014. With heavy traffic in the skies, efficient allocation of airspace by reducing separation distances between aircrafts became a rising issue of concern. Thus, Secondary Surveillance Radars (SSR) were deployed, using Automatic Dependent Surveillance-Broadcast (ADS-B) transmissions from commercial aircrafts to augment information provided by the primary radar. However, ADS-B transmissions are unchallenged and unencrypted, making air tracking vulnerable to deliberate false transmissions (spoofing) which may cause ground control to perceive non-existent aircrafts or aircraft at wrong location. The large number of aircrafts which have to be tracked also increases the vulnerability of the airspace. Hence, the positioning of aircrafts should no longer be taken at face value; instead, a check and balance should be developed to ensure the wellbeing of air traffic. In this report, a long-baseline Signal Multilateration (MLAT) system will be presented to counter potential spoofing attacks. The MLAT system works by measuring the Difference Time Of Arrival (DTOA) of an ADS-B signal using at least 3 time-synchronised receivers. The DTOA is used to geolocate the transmitting aircraft, independent of information in the ADS-B message. A small deviation of 1.1132km has been achieved in determining the true position of the aircraft. Such will serve as a precaution in the event of an infringement of air security.**

Keywords-defence; national security; signal; Multilateration

I. INTRODUCTION

In order to address the issue of increasingly heavy air traffic [1], efficient utilisation of airspace is important and has thus been extensively researched. This can be achieved by reducing separation distances between aircrafts, which depends on the timeliness and accuracy of the reported location of the aircraft.

As such, electronic surveillance technology plays a crucial role in Air Traffic Control (ATC). Aircrafts are equipped with transponders designed to respond to Secondary Surveillance Radar (SSR) interrogations with aircraft identification and altitude information via Modes A and C respectively. Some aircrafts are also equipped with Mode S transponders, and thus periodically (at a rate of once per second) broadcast information via Automatic Dependent Surveillance - Broadcast (ADS-B) messages. Information included within an ADS-B message comprises of the aircraft identification, position (latitude, longitude and altitude), velocity, heading of the aircraft, and various other information [2].

However, as ADS-B messages are unencrypted and unchallenged [3], they are vulnerable to deliberate false transmissions (spoofing), potentially causing ATC to perceive aircrafts at locations which deviate from their reported locations, non-existent aircrafts, or the event of overloading of ATC computer systems [4].

Hence, in this project, a long-baseline Signal Multilateration system was established to counter potential spoofing. Based on the Difference Time of Arrival (DTOA) of an ADS-B signal between at least 3 time-synchronised receivers and the known locations of these receivers, the transmitting aircraft could be geolocated using Signal Multilateration, independent of position information transmitted in the ADS-B message. This will serve as a check and balance to the information provided by the ADS-B of each aircraft.

II. HYPOTHESIS

The aircraft can be geolocated by exploiting the ADS-B signal transmission. With the Time Of Arrival (TOA) measured by 3 time-synchronised receivers strategically placed at a sufficient distance apart (>10km between each pair of receivers), the Difference Time Of Arrival (DTOA) may be derived and exploited for geolocation.

III. METHODS AND MATERIALS

A. Systems Set-up

During each trial, 3 sensor stations were deployed across Singapore in the West, South and East areas (Jurong, DSO National Laboratories, SUTD) respectively to achieve the large baseline required for Multilateration. Geographically, Sensor Stations 1 and 2 were placed at a distance of 10km apart, while Sensor Stations 2 and 3 were placed at a distance of 20km apart. The set-up was removed after the required data was collected for each trial. Fig. 1 shows an illustration of the sensor stations position with reference to the Singapore map.

Another consideration of the choice of location is the line of sight between the antenna and the aircraft. To the best of ability, sensor station antennas were placed on higher grounds where the view around the vicinity was unblocked. However, due to resource constraints, Sensor Station 1 does not have as good a line of sight as compared to Sensor Stations 2 and 3. The repercussion of such a constraint will be further analyzed in the later part of this report.

This project was done at DSO National Laboratories, Singapore, under the Research@YDSP Programme 2016

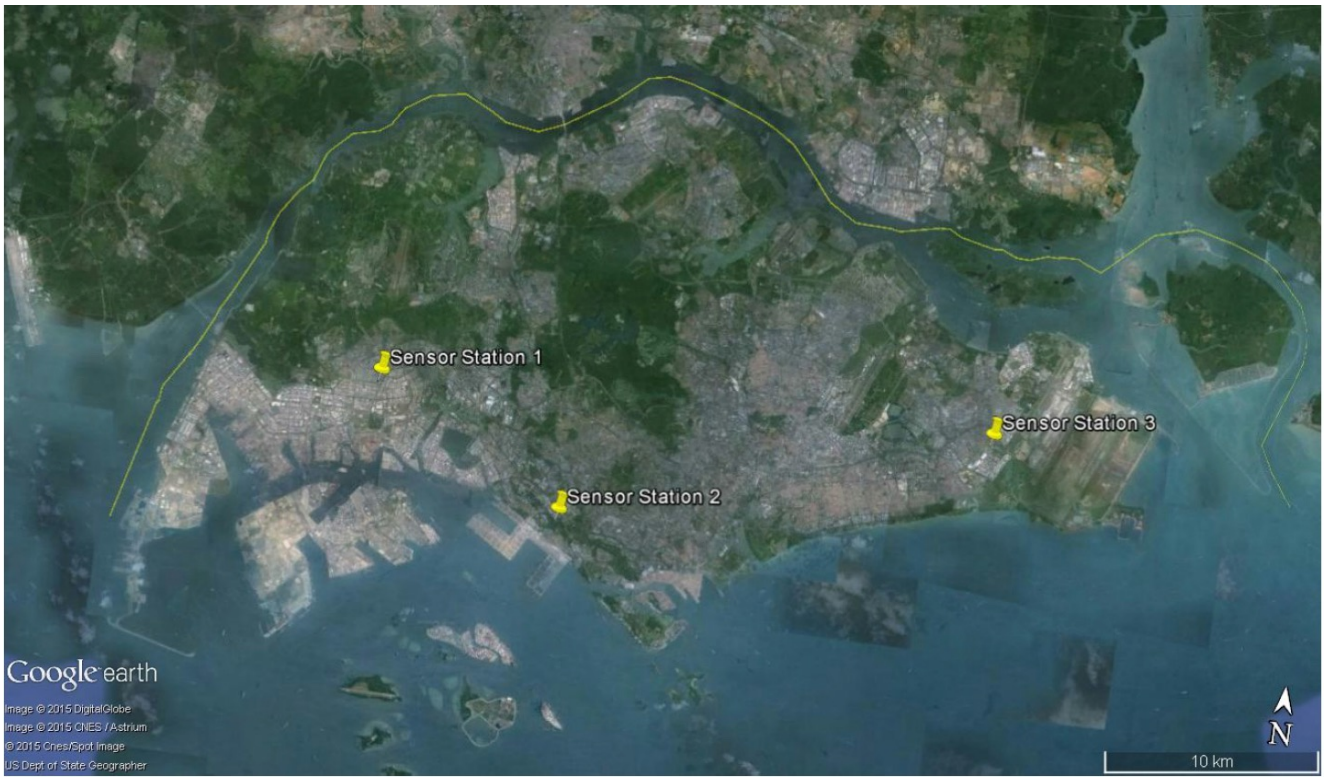

Fig. 1: Locations of Sensor Stations (Map of receivers). Map retrieved from Google Earth.

Sensor Station 2 was then designated as the base station where the compilation and analysis of data was done, whereas Sensor Stations 1 and 3 were designated as remote stations. In order for the data from the 2 other sensor stations to be compiled in real time, internet access is required. All 3 sensor stations were given internet access in order for the base station to receive, and the remote stations to transmit data. Internet access is provided using a 4G modem, coupled with a data plan subscription from the local network service provider.

The use of virtual control hence enables data from all 3 stations to be analysed simultaneously. Detailed layout of the sensor stations and base station are illustrated in the subsequent subsections.

1) Sensor Station

At each sensor station, an antenna was set up at a location with the best possible reception to receive ADS-B signals from the aircraft flying within the region. These signals were received using a Commercial Off-The-Shelf (COTS) product: Radarcape. Radarcape, is a passive ADS-B receiver [5] which is capable of time-stamping received ADS-B messages with GPS time of accuracy up to +/-50 nanoseconds (ns) for each received signal. The data was fed into the computer (PC) at the sensor station connected using ethernet. A block diagram of the sensor station setup is shown in Fig. 2.

In order for the base station to gain access to and remotely control the remote sensor stations, TeamViewer software was preinstalled in all the remote stations. As a form of security, remote stations are password locked, and preset to display a black screen whenever the base station is gaining access to them. This prevents unauthorized monitoring of the visuals, should there be any attempt to do so.

In addition, Visual Basic software was also installed in order for the Radarcape runner (an in-house developed graphical user interface (GUI)) to be functional.

Radarcape drivers are then installed in order for the sensor stations to gain access to the information received by the Radarcape units.

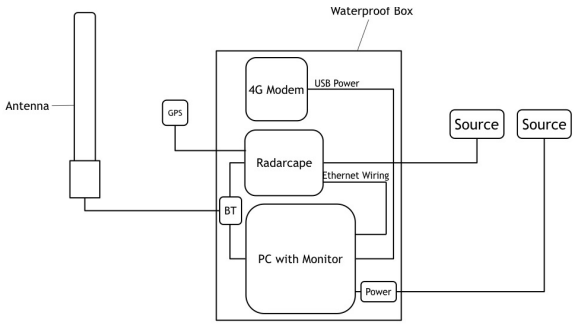

Fig. 2: Block Diagram of Sensor Station

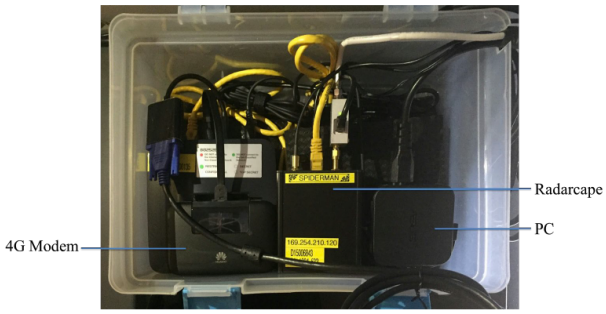

Fig. 3: Photograph of remote station set-up, excluding antenna. Box dimensions: 22cm x 32cm

2) *Base Station*

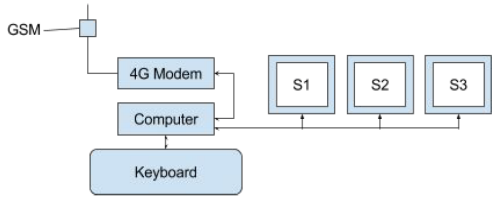

Fig. 4: Block Diagram of Base Station

At the base station, a central processing unit (CPU) is connected to 3 monitors to display the datas received from the 3 sensor stations. This allows for all 3 sensor stations data to be analysed simultaneously.

B. Data Collection

ADS-B signals are received via the 3 antennas at the 3 respective sensor stations. With the aid of the Radarcape and Radarcape runner, the time-stamp of each received signal is documented. All 3 sets of time-stamp data are then collated, via TeamViewer, at the base station for further analysis.

For the purpose of this report, analysis of the results are based on the assumption that the position information provided by the decoded ADS-B signal are true and accurate. As such, to serve as a comparison to the derived geolocated position, Kinetic SBS-3 receiver is used. With the aid of the Kinetic SBS-3 receiver, the ADS-B signals are decoded to provided the position information transmitted by the aircraft.

C. Data Processing and Analysis

The area of the map in consideration is first divided into pre-defined grids. The distance of each grid point from the sensor stations was computed with the aid of the spherical Law of Cosines formula [6] as shown below:

$$D = acos(sin(lat1) \times sin(lat2) + cos(lat1) \times cos(lat2) \times cos(long2 - long1)) \times r \quad (1)$$

where, D = Distance between 2 points in km

$lat1$ = Latitude of position 1 in radians

$lat2$ =Latitude of position 2 in radians

$long1$ = Longitude of position 1 in radians

$long2$ = Longitude of position 2 in radians

r = Earth's radius (6378.137km at the equator)

With the distance between each grid to the respective sensor, the time needed for the signal to travel the required distance can be computed using the following formula:

$$t = \frac{d}{c} \quad (2)$$

where, t = time taken for signal to travel in seconds

d = distance in km

c = speed of light (299792.458km/s)

As such, the DTOA for each grid to the respective sensor stations can then be computed by finding the difference between the time needed for the signal to travel to each sensor station as follows:

$$DTOA = (t_2 - t_1) \times 10^9 \quad (3)$$

where, $DTOA$ = difference time of arrival in nanoseconds

t_2 = time taken for signal to travel to sensor 2 in seconds

t_1 = time taken for signal to travel to sensor 1 in seconds

This generates a table of map positions with corresponding DTOA between the respective sensors as shown in Fig. 5.

To derive each location of the aircraft, the obtained time of arrival (TOA) from the Radarcape is to be utilized to obtain the DTOA between each sensor station. However, the TOA at each sensor station from the same signal has to first be determined from the long list of acquired data. With reference to the distance between the sensor stations, it is deduced that the DTOA between each sensor station should be in that of the nanosecond region. As such, a Matlab script is written to filter and group the TOA datas from each sensor station by grouping TOAs that are less than time taken between baseline (approximately 100000ns), as TOA from the same ADS-B signal.

With the filtered results, each set of result is then compared to the DTOA table as illustrated in Fig. 5. However, in view of slight deviations due to computation or data error, a tolerance value is defined, such that any value that falls within the range is acceptable. Each possible DTOA match is then marked out on the map as shown in Fig. 6. The matches marked will form a line for each set of DTOA sensor stations, contributing to 3 lines formed for the 3 set of differences as illustrated in Fig. 5. The point of coincidence of the 3 lines, marked with E in Fig. 6, is the computed geolocated location of the aircraft.

TABLE 1: GENERATED DTOA

Position	DTOA (Sensor 1, Sensor 2)	DTOA (Sensor 1, Sensor 3)	DTOA (Sensor 2, Sensor 3)
1	t_1	t_2	t_3
2	t_4	t_5	t_6
3	t_7	t_8	t_9

Fig. 5: Illustration of generated DTOA Table

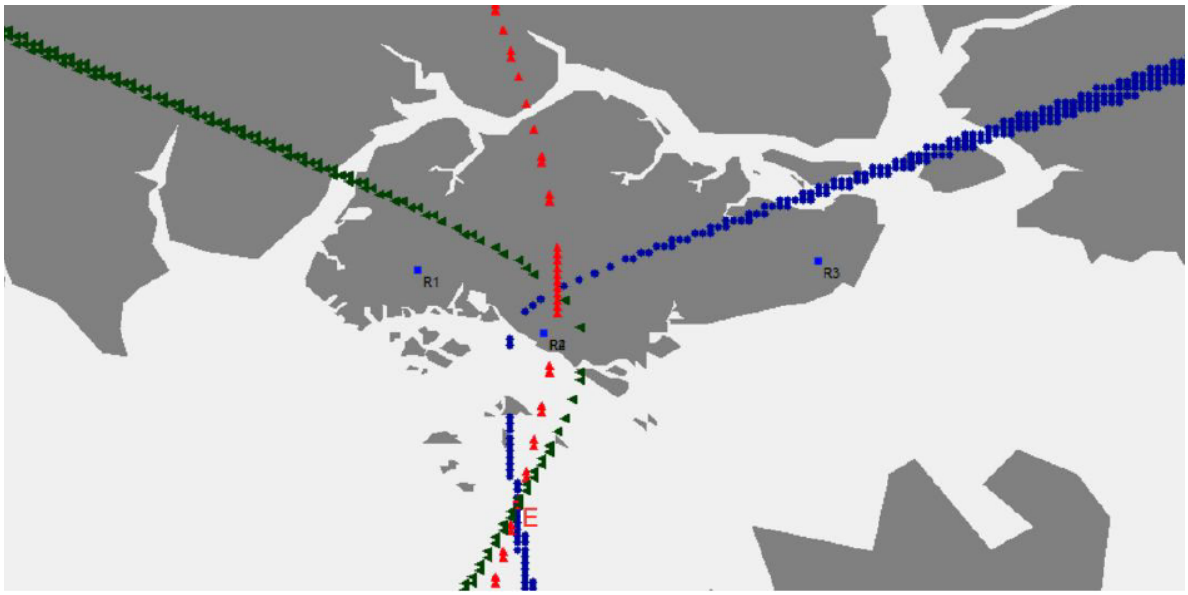

Fig. 6: DTOA match for each location

In order to automate the whole system of filtering and comparison, the above process described is written into a script with the aid of MatLab. Matlab then generates the plots for each set of data, allowing the flight path of the aircraft to be deduced, as shown in Fig. 7 of Results and Discussion. The flight path based on the locations of the aircraft calculated by Multilateration was then plotted against the flight path based on the decoded ADS-B messages.

IV. Results and Discussion

For experimentation, a tolerance of 500ns and a grid size of 0.005 degrees (º) was used.

A trial was done on a live commercial aircraft (SLK435, callsign 0610) on 11 December, 2015. The location of the aircraft was tracked from 09:55:02 UTC to 09:56:26 UTC.

The corresponding results were then analyzed. Using the MatLab script, the matching points were plotted as shown in Fig. 7 and the flight path demarcated in red is being deduced. The ADS-B path as provided by the Kinetic SBS-3 is also plotted for comparison, as shown in brown in Fig. 7.

In order to determine the deviation of the deduced path from the true path, the percentage error of the position in terms of latitude and longitude, and the distance between the flight paths was analyzed.

$$Percentage\ Error = \frac{(Deduced\ Position - True\ Position)}{True\ Position} \times 100\% \quad (4)$$

The smallest error was found where the location obtained by decoding the ADS-B signal was at longitude 103.6º and latitude 1.03º, while the location derived via Multilateration was at longitude 103.6º and latitude 1.04º. This corresponds to a position error of 0.97% (2s.f.) and a distance error of 1.1km (2s.f.).

On the other hand, the largest error was found later, as the plane flew towards the East of Singapore, where the location obtained by decoding the ADS-B signal was at longitude 103.9º and latitude 0.975º, while the location derived via Multilateration was at longitude 103.9º and latitude 1.01º. This corresponds to a position error of 3.6% (2s.f.) and a distance error of 3.9km (2s.f.).

Such large errors observed as the aircraft travelled towards the east of Singapore can be attributed to the positioning of the 3 sensors. A good positioning is one where each pair of sensor stations form a "good triangle" with the position of the emitter source. Such can be observed in the initial part of the flight path, and hence allowing a highly accurate computation of the flight locations. However, towards the later part of the flight, it can be observed that Sensor Stations 1 and 2 form an almost-straight line with the aircraft location. This is detrimental to Multilateration, hence resulting in the large error. This is also known as Geometric Dilution of Precision (GDOP).

Also, as shown in the plot below, the flight path derived from Multilateration is incomplete, ending before the flight path derived from decoded ADS-B signals. This is because as the aircraft flew towards the East, it exited the line of sight of the antenna at Sensor Station 1. Due to the limitation of resources, sensor station 1 Line Of Sight (LOS) was blocked by the taller buildings that surrounds it. Hence, no more signals were received at Sensor Station 1 as the aircraft flew towards the eastern part of the region, preventing Signal Multilateration from being done due to insufficient data.

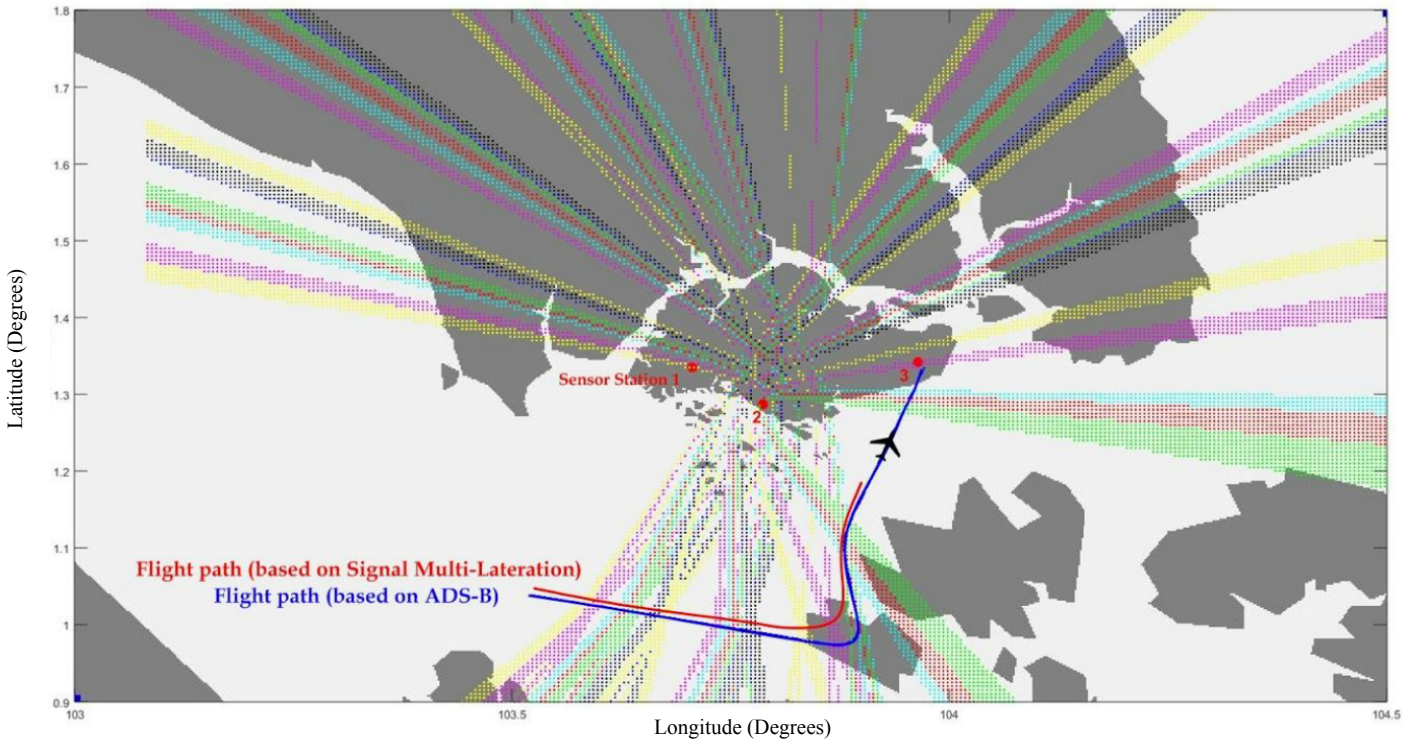

Fig. 7: Comparison of Flight Paths Generated using Multilateration and decoded ADS-B signals

V. Conclusion and Recommendations for Future Work

In conclusion, aircrafts can be geolocated by performing Signal Multilateration on ADS-B signal transmissions using the DTOA between strategically-placed time-synchronised receivers. The successful deployment of the system across Singapore as well as the ability to geolocate the positions of a specific aircraft over time to plot its flight path will potentially allow ATC to deploy this system for the confirmation of aircraft locations in our airspace. One key advantage of this set up is the compactness, portability and functionality of the remote stations.

In future, more sensors can be placed in Singapore, even though a minimum of 3 remote stations is required for Signal Multilateration. This will allow the line of sight to be improved as data from different remote stations can be used depending on the location of the plane. The accuracy of the timestamping of signals can also be improved. Instead of relying on COTS receivers such as Radarcape, receivers with higher accuracy may be researched and developed.

One major limitation of Remote Station 1 is that the antenna was placed in a heavily built-up area, which restricts the line of sight of the sensor to the aircraft, due to the existence of taller buildings around it. Therefore, many signals towards the extreme east of the region were blocked and could not be received by the antenna. In future, the antenna can be placed on higher, open-air spaces in order to ensure a better line of sight, and hence a constant stream of reliable data.

In addition, one may also consider fully automating the system, such that signals from all aircrafts can be collected with its timestamps, processed with Multilateration algorithm, and compared against the desired decoded ADS-B messages to highlight any discrepancies in reported locations of aircrafts. This will allow a live analysis of the data and would therefore be more suitable for commercial usage in ATC.

Acknowledgment

I would like to thank Raffles Girls' School as well as DSO National Laboratories for providing the resources necessary to the completion of this project and for giving me this opportunity to undertake this project under the Research@YDSP Programme. Special thanks go to my research mentors, Mr Wong Jit Chin and Mr Frederick Neo of DSO National Laboratories, for their patient guidance and help throughout the course of the project; my teacher-mentors, Mr Yang Kian Hong, Mr Shaun De Souza of Raffles Girls' School and Dr Tan Guoxian of Raffles Institution for their support; as well as International Researchers Club and all co-sponsors for the opportunity to participate in IRC-SET 2016.

References

1. Aviation Benefits Beyond Borders. (2014, April 1). Retrieved December 12, 2015, from http://aviationbenefits.org/media/26786/ATAG__AviationBenefits2014_FULL_LowRes.pdf
2. Guidance Material on Comparison of Surveillance Technologies (GMST) Edition 1.0. (2007, September 1). Retrieved December 12, 2015, from http://www.icao.int/APAC/Documents/edocs/cns/gmst_technology.pdf
3. Finke, C., Butts, J., & Mills, R. (n.d.). ADS-B Encryption: Confidentiality in the Friendly Skies. Retrieved December 15, 2015, from http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/CSIIRW.pdf
4. Exploring Potential ADS-B Vulnerabilities in the FAA's Nextgen Air Transportation System. (2011, June 1). Retrieved December 12, 2015, from http://www.hsdl.org/?abstract&did=697737
5. The Radarcape. (n.d.). Retrieved December 3, 2015, from http://www.modesbeast.com/radarcape.html
6. Veness, C. (2015). Calculate distance, bearing and more between Latitude/Longitude points. Retrieved December 12, 2015, from http://www.movable-type.co.uk/scripts/latlong.html
7. Neven, W., Quilter, T., Weedon, R., & Hogendoorn, R. (2005, August 1). Wide Area Multilateration Report on EATMP TRS 131/04, Version 1.1. Retrieved December 16, 2015, from https://www.eurocontrol.int/sites/default/files/publication/files/surveilllance-report-wide-area-multilateration-200508.pdf