Mode-S Receiver and ADS-B Decoder

Sean Koceski, Long Lam, and Michael Vose

Dept. of Electrical Engineering and Computer Science, University of Central Florida, Orlando, Florida, 32816-2450, U.S.A.

***Abstract* — National airspace systems around the world are undergoing infrastructure upgrades to aging systems. New technologies like the Automatic Dependent Surveillance - Broadcast (ADS-B) are a part of these upgrades. By using ADS-B, an aircraft broadcast its position by GPS coordinates which in turn allowing it to be tracked by air traffic control stations. However, the ADS-B data is not encrypted and represents an exposure of aircraft information. The objective of this project is to show a possible solution to this issue by developing a system to obtain the ADS-B data and using encryption methods on incoming signals.**

***Index Terms* — ADS-B, Air-Traffic Control, Binary Phase Key Shifting, Manchester Coding, Format-Preserving Encryption, FFX Algorithm.**

I. Introduction

With aging radar systems and the growth of new technologies, ADS-B is quickly replacing traditional primary and secondary radar systems. However, ADS-B data is not encrypted and represents an exposure of highly precise and potentially exploitable commercial aircraft tracking information [1][2]. Military aircraft transponders and ground stations already have the option to use an encrypted digital protocol to address this concern referred to as Mode-5.

The application of encryption (where law and treaty permit) to the non-military Mode-S protocol, a protocol which allows the participation of civilian aircraft and ground support in its use, can protect the tracking data of commercial aircraft and general aviation from being misused. This motivation was behind the creation of this project as the transition to ADS-B continues. The primary purpose of the project is to obtain an ADS-B signal, decode the signal, and display the data retrieved to a medium that the user can see. In addition, this project will simulate the broadcast of an encrypted ADS-B transponder in software, as an actual ADS-B broadcast would be forbidden. Bypassing our Mode-S receiver, our enhanced ADS-B decoder would then decrypt the signal and demonstrate the receipt of the simulated communication. Meanwhile a standard ADS-B decoder would not be able to determine the aircraft's location.

II. ADS-B

ADS–B is a key element of the U.S. Next Generation Air Transportation System as well as being a key upgrade in every other National Airspace System around the world. Avionics equipment for ADS-B is often classified by whether it transmits (ADS-B OUT) or receives (ADS-B IN). Using ADS-B OUT, an aircraft determines its position by GPS coordinates and broadcasts it every second, enabling it to be tracked by any ADS-B IN receiver, including air traffic control ground stations and other ADS-B IN equipped aircraft. Allowing aircraft to both transmit and receive ADS-B provides situational awareness to help avoid collisions in the air and on the runway. It costs much less to build and operate an ADS-B transceiver than a traditional two-story radar complex, and it does the job faster, with greater precision, and with little restriction to the placement of ground stations. ADS-B promises even more benefits in the future. Once everyone is using ADS-B, the current 80-miles-apart safety margin for aircraft in flight can be reduced. This will result in fuel savings, fewer airport delays and fewer diverted flights [1]. The advantages of this new technology are compelling and profitable [3].

However, the move from radar, a costly and somewhat exclusive technology, to ADS-B, a relatively inexpensive digital technology, has had unintended consequences. Not everyone could successfully build a two-story radar complex, but a few engineers could design an inexpensive digital radio receiver to monitor aircraft – a receiver which millions of enthusiasts could then use to monitor their local airspace. Vast networks of such monitoring stations operating over the Internet now exist and the aircraft tracking information they provide matches or exceeds the precision and timeliness of that used by the Federal Aviation Administration in the United States. Flightaware.com, and flightradar24.com are two such examples, [4][5].

To a large degree, this represents a loss of control of local airspace information. Granted, ADS-B broadcast is strictly regulated, but this would not deter a dedicated attacker. And, unrestricted reception of ADS-B empowers everyone with a dark motive to contemplate how easy it might be to engage the system in subversive ways. Too much is at stake to dismiss the potential for abuse. It has been demonstrated in other research [2] that unauthorized ADS-B broadcast could be used to spoof the presence of a phantom aircraft or to flood the local airspace with many

such phantoms. Could the resulting confusion create an exploitable vulnerability in the air traffic control system? Could ADS-B tracking information be used to target an anti-aircraft weapon? The worldwide adoption of ADS-B needs complementary security protocols to minimize such attack vectors. Global leaders have recognized the need to act, and experts in aviation and related fields have been carefully considering this issue. In his 2013 State of the Union Address, President Barack Obama said, "America must also face the rapidly growing threat from cyber-attacks… our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." [6]. The American Institute of Aeronautics and Astronautics (AIAA) has made specific recommendations to harden our aviation infrastructure against cyber-attack [7]. Likewise, the International Civil Aviation Organization (ICAO), and the Air Force Institute of Technology (AFIT) have published specific recommendations to harden, (e.g. improve the security of,) ADS-B [8][9]. Among the AFIT recommendations is the use of a NIST draft standard encryption algorithm named FFX [10]. The FF in the FFX acronym denotes a (F)ormat-preserving (F)eistel-based cryptographic algorithm. Without addressing the obviously larger issues regarding
encryption key management and distribution across international airspace, this project attempts an implementation of FFX on the ADS-B messages to the explore the difficulties this may present. In turn, this requires that we decode the structure and contents of key ADS-B messages from the radio frequencies, modulation, and line coding in which they are transmitted.

The subset of ADS-B messages that contain the relevant data for this project are known as Extended Squitters (ES). The relationship between the ES subset and the scope of encryption can be visualized as in Table 1.

The ES messages we need occupy the extended data field one by one. They are known by the names:

- Airborne Position Squitter
- Surface Position Squitter
- Airborne Velocity Squitter
- Aircraft Identification Squitter
- DO-260A State and Status

III. Signal Encryption and Decryption

ADS-B messages are not presently encrypted. The intent is to add such a cryptographic scheme without breaking ADS-B message integrity. Format-Preserving encryption (FPE) based on the FFX algorithm has been recommended by AFIT and will be used in this project to protect key data within the ADS-B messages without changing the overall structure of the messages. FFX is especially suited to this scenario because it encrypts encrypted data to compensate for the inherent weakness of matching input and output data size.

The idea of encrypting encrypted data requires further explanation. The FFX algorithm specifies a variable number of rounds of encryption (and therefore also decryption) using other known encryption algorithms [10]. The FFX documentation illustrates its operation using the Advanced Encryption Standard (AES) as this underlying algorithm. However, FFX itself could theoretically use a different underlying encryption algorithm depending on the need at hand.

Figure-1 illustrates four rounds of FFX using what is termed the 'left' method. The input data, shown as the block labeled A0 followed by B0 is an unspecified fixed length n. The B0 portion is encrypted with algorithm F and XORed with the A0 portion to create a new encrypted message fragment C0. This is prefixed with the prior B0 portion to complete one round. The partially encrypted message is logically repartitioned for the next round. Note that the input data and the output data are exactly the same size after every round. This would be an exploitable

<table>
<tr><td>Message Type</td><td colspan="2">Surveillance-Control</td><td>Extended Data*</td><td>ICAO Code +</td></tr>
<tr><td>5-bits</td><td colspan="2">27-bits</td><td>56-bits
(Format depends on message type).</td><td>24-bits</td></tr>
<tr><td></td><td>Capability 3-bits</td><td colspan="3">Largest Possible Encryption Target
104-bits</td></tr>
</table>

Table 1. ADS-B Extended Squitters

weakness in most symmetric algorithms – but not in FFX. All this is undone in reverse for the decryption side of the operation.

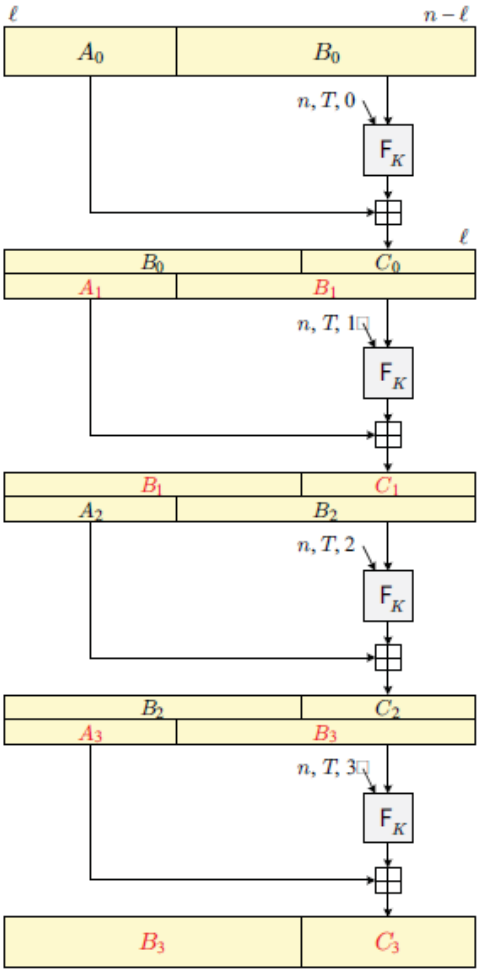


Figure 1. FFX Encryption

IV. Systems Specifications

When design this project, there was a set of specifications that we expected to achieve:

- The antenna shall collects the signal from the source via the two frequency bands used by ADS-B without interfering with NTIA restrictions.
- The receiver will be housed in a weather resistant radome made of a rigid plastic tubing that will not interfere with the signal's reception.
- Once the signal is collected, extraneous noise is removed via bandpass filters designed for the UHFs involved.
- The receiver will be using a rechargeable battery with an estimated time of more than one hour of current use.
- The receiver is expected to continuously decoded/decrypted aircraft position and altitude information with minimal delay.

V. System Concepts

To gain a better understanding of the system as a whole, Figure 2 show the overall design from when an ADS-B signal is received to when the user can view the signal.

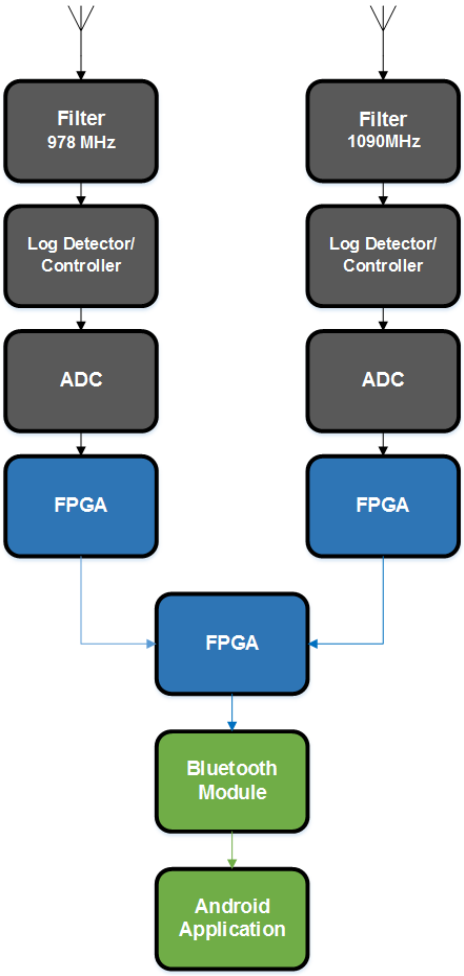


Figure 2. Complete System Concept

From the figure, the signal from the two frequencies will be initially obtained separately. After signal conversion and decoding, the two signals are then merged and are sent to a Bluetooth module. Finally, the ADS-B data is processed by the Android application for use of the user.

VI. Hardware Components

In general, the design of the project can be broken down into multiple components, from hardware to software. In this section, an overview will be given to each hardware component.

A. Antenna

Imperative to the overall design is the basis of receiving the desired signals. Accurate collection and of the 1090 MHz and the 978 MHz is performed by two individual antennas each designed specifically for one frequency. The antenna type selected is a coaxial collinear design. This design holds the benefit of having an omni-directional collection pattern, allowing for the design to rely on its radiation pattern to collect signals surrounding it rather than needing to be directed at the signals source of transmission for reception.

Implementation of this design was created with RG-213/U 50-Ohm coaxial cable. The segments of the antenna are designed to receive signals of the desired frequency by having their length a fraction of the wavelength determined by the velocity factor of the cable using equation (1). In the case of ADS-B this resulting in length of 90.75mm and 101.15mm for the lengths of each segment. The use of segments designed in half-wavelengths allows for a relatively large gain by alternating the segments allowing each segment to be driven and become cophasal. At the end of each antenna is an additional whip which is composed of just an exposed segment of wire set to a quarter wavelength.

$$\lambda \div 2 = 300 \div f \div 2 \times V \quad (1)$$

f is the frequency in megahertz
V is the velocity factor of the coax cable, in the case of our cable 66% of the speed of light

Challenges with this design is the fact that there is no true ground plane on the feed-line. To perform this a balun was necessary to cancel out the signal traveling on the outside of the coax cable. This was implemented by designing a sleeve balun to be placed at top of the feedline's connection to the antenna. Length of the sleeve of copper tubing is determined using a similar equation to that used for finding the length of the segments, equation (2).

$$\lambda \div 4 = 300 \div f \div 4 \times V \quad (2)$$

V is the velocity factor of the copper tubing, 95% of the speed of light

To further remove undesired signals on the outside of the cable ferrite beads are placed on the feedline cable with their location adjusted to maintain a SWR (Standing Wave Ratio) as close to 1 as can be managed. Following the feedlines, the signal is then passed to the receiver box where it travels first to the filters.

B. Filters

A pair of band-pass hairpin filters is used to shed unwanted signals and noise outside our two target frequencies. The filter for 1090 MHz filter is the MiniCircuits CBP-1090C+. This is based on ceramic resonator technology. The reason for purchasing the filter from a vendor allowed for greater reliability for the project. We implemented our own microstrip hairpin filter design for the 978 MHz frequency. This filter was designed using Keysight Genesys software.

Figure 3. 978MHz Hairpin Filter on PCB

The bandwidth of the filter was designed to be 75 MHz due to the fact that the design is formed around parameters that are outside of our control, such as the dielectric constant of our FR4-type PCB laminate material. To minimize this uncertainty we used hyper-accurate measurements of the dielectric constant and loss-tangent for FR4 laminate at 1081 MHz. These measurement, as show in table 2, were provided by research completed at the University of Missouri-Rolla [11]. Figure 4 shows the frequency response for the 978MHz filter.

f0 (GHz)	εr	tanδ	Effective conductivity at f0 (S/m)
1.0185	4.47	0.01646	0.004168

Table 2. Measurements

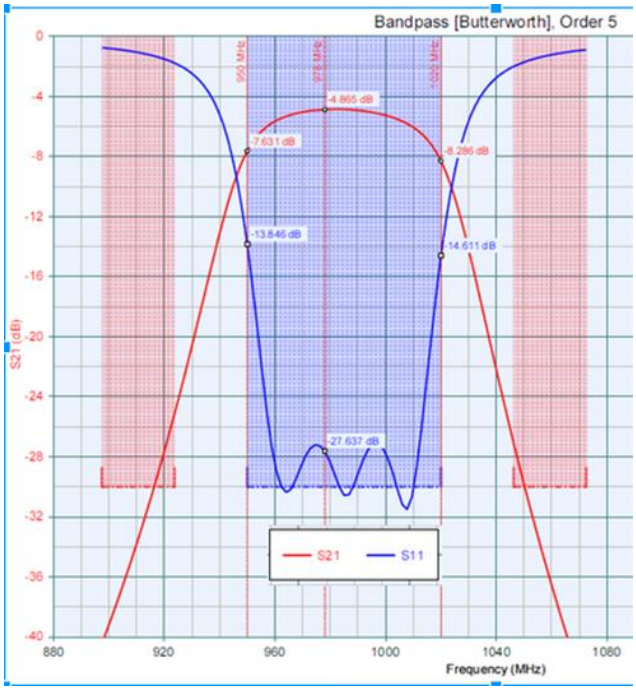


Figure 4. 5th Order Frequency Response of 978 MHz Filter

C. RF Detector

Before signal conversion from analog to digital, the filtered signal is converted to a signal that is more suited for the analog to digital converter. For this process, the Analog Devices AD8319 was selected. The AD8319 is a demodulating logarithmic RF power detector made to converts a wide-range (45dB), low-power RF input signal to a smaller-scale DC output. By using this component, it allows us to convert the AC signal from the antenna to a DC voltage. The AD8319 achieves this conversion by employing a progressive compression technique through a cascade of small signal op-amps. The resulting logarithmic slope is −22 mV/dB. Figure 5 shows the functional diagram of the component and how this is implemented.

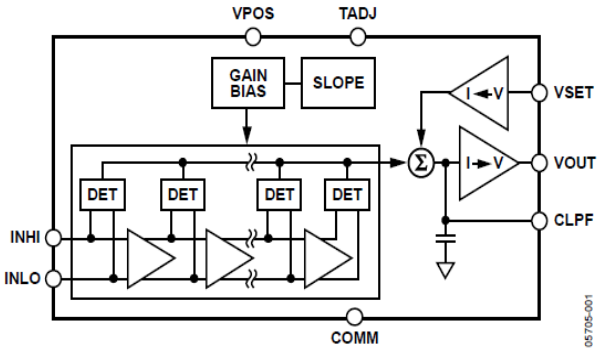


Figure 5. AD8319 Functional Diagram, Copyright Analog Devices [12]

As shown from the figure, the AC signal is obtain by INHI, afterwards the signal is processed through a series of Op-Amp and detectors. The values obtained from the detectors are summed and then offset by VSET. The calculated voltage will be sent to VOUT.

D. Analog to Digital Converter

After the signal conversion from an AC to a DC voltage, the analog to digital converter is the next part in the receiver. For this part, the MAX1192 from Maxim Integrated was selected. The MAX1192 uses a pipeline architecture for its conversion method and have two channels for inputs. The ADC features three power saving modes that can really help when it comes to conserving power. Under normal operations, the converter has a sampling rate of 22 mega-samples per second (MSPS) with a power consumption of 27.3mV [13]. This is quite impressive to get this kind of performance for so little power. The signal to noise ratio and signal to noise and distortion ratio is 48.6 dB which is high enough to support this application [13]. The converter outputs the analog signal as an 8-bit digital signal by a parallel CMOS interface which allows fast transfer of data to the decoder [13]. When not in use, the MAX1192 can consume as little 1.8µV when in shutdown mode. The operating voltage for the MAX1192 is from 2.7V to 3.6V [13]. In addition, the reference voltage can be set internally or externally.

E. FPGA

We believe that hardware-based decryption will be possible in later iterations of this project, but our intent is to only execute the Manchester decode for each frequency and then digitally merge the two. Separate clock oscillators are needed for these two functions. Consequently, a two-tiered FPGA architecture will be employed to create a large reserve capacity for experimentation with hardware-based decryption and to separate the essential Manchester decoding from later functions like the merge of the ADS-B data streams from the two frequencies being received. Why a merge? Because there is no tuner or "frequency-hopping" circuit to limit the inbound data to a single channel at a time. The signals remain separate and simultaneous thru the RF portion of the design.

In detail, the first tier is comprised of two small FPGAs; one for each ADC. The 8-bit output of each ADC dictates these FPGAs accept 8-bits. Manchester decoding then takes place. Ideally, these two FPGAs will run at eight times the clock speed of the ADCs, but variation is possible. Faster than five times the incoming bit rate will correctly detect the next bit transition, and less than twelve times the incoming bit rate will suppress any between-bit transition. The second tier of this FPGA cascade takes

both decoded ADS-B data streams and merges them together. Unlike the first two FPGAs doing the Manchester decode, this one needs at least 16 GPIO and enough logic space to emulate a small buffer in which to combine and order the results. To satisfy this design, we are using Xilinx XC2C64 devices for tier-1 and Xilinx Spartan-6 for tier-2.

F. Bluetooth Module

After the processing of the ADS-B signal is complete, this data will be sent to an application for viewing. With some deliberations, it was decides to transfer the data to an Android application via a Bluetooth signal. To accomplish this task, the Digilent PmodBT2 was selected. The Digilent PmodBT2 is a Bluetooth interface module that is compatible with the Spartan 6 FPGA that is being used for signal merging. This module employs a Microchip RN42 Class 2 Bluetooth radio. The RN42 supply the PmodBT2 with a built-in antenna which allows for distances from up to 20 meters. In terms of Bluetooth support, the PmodBT2 supports the following standards: 2.1, 2.0, 1.2, and 1.1. When it comes to communication, this module uses a simple 8-bit UART interface to receive data from the FPGA and has a baud rate of 115.2 kbps for data transfer. In addition to its built-in antenna, this module has a small form factor (0.8" x 1.5"), and a variety of modes (Slave, Master, Trigger Master, and Auto-Connect Master). To enter these modes, the PmodBT2 can be switch to a command mode where it can customized to work with certain applications.

VII. SOFTWARE COMPONENTS

This section will cover the software components of the project.

A. Manchester Encoding/Decoding

The program that are be used in the FPGAs implements a method called Manchester encoding / decoding. This is a widely used and standardized scheme where both the data and the clock can be recovered from the same signal. It is considered a binary form of phase-shift keying, [14].

When it comes to Manchester code, it is a self-clocking code with a minimum of one and a maximum of two level transitions per bit. A Zero is encoded as a Low-to-High transition, a One is encoded as a High-to-Low transition. Between two identical bits of data there is an extra level transition which must be ignored by the decoder. The decoder, therefore, needs some information about the bit timing. Typically, the decoder has a clock with timing that is a known multiple of the encoding clock.

The decoder clock can be asynchronous to the incoming data, but must be faster than five times the incoming bit rate (in order to detect the next bit transition), and slower than 12 times the incoming bit rate (in order to suppress the between-bit transition). The nominal decode clock frequency should, therefore, be eight times the incoming data rate. After detecting a valid transition, the circuit ignores further transitions for six clock periods.

With that, every ADS-B message begins with an 8-microsecond preamble of four pairs of on-pulse/off-pulse with specific inter-pulse timing followed by 56 or 112 microseconds of Manchester coded data (which translates to 56 or 112 bits of data due to the fixed time nature of this scheme.). The 56-bit portion is a datagram and is formatted using table 3:

Message Type	Surveillance-Control	ICAO (Aircraft) Code + Parity
5-bits	27-bits	24-bits

Table 3. Short Squitter Format

The 112-bit portion is also a datagram and is formatted with an additional 56-bit field inserted in the datagram as shown in table 4:

Message Type	Surveillance -Control	Extended Data	ICAO Code +
5-bits	27-bits	56-bits	24-bits

Table 4. Extended Squitter Format

Specifically, the following ADS-B message types, [Köllne], [Radar] will be decoded for further processing:

- DF0 (56-bit) Generally referred to as the ACAS message.
- DF4 (56-bit) Rollcall reply: Altitude - resolution to 100ft.
- DF17 (112-bit) Extended Squitter: Contains ADS-B data (position, heading, etc.)
- DF18 (112-bit) Extended Squitter: Same as DF17 but from ground traffic.
- DF20 (112-bit) Rollcall reply: Altitude - resolution to 25ft. Uses EHS/BDS registers.
- DF21 (112-bit) Rollcall reply: Identity. Uses EHS/BDS registers.

With these formats, the tier-1 FPGAs are in charge of processing the signals and the tier-2 FPGA is in charge of merging the signals and sending them to the Bluetooth module.

B. Android Application

Users will be able to view the ADS-B data via an Android Application. This application shall display information from the aircraft by a graphical user interface. This interface will display markers of aircraft on a map that are picked up by the receiver and are within the current GPS position of the Android device. From this map, the user can view information for each individual aircraft from traveling speed, current altitude, to the type of plane by selecting its marker. As this process occurs, all aircraft information shall be updated in real-time. In addition, the application shall be able to decode any encrypted information that is sent to the mobile device. Figure 6 shows the general process of how the application run.

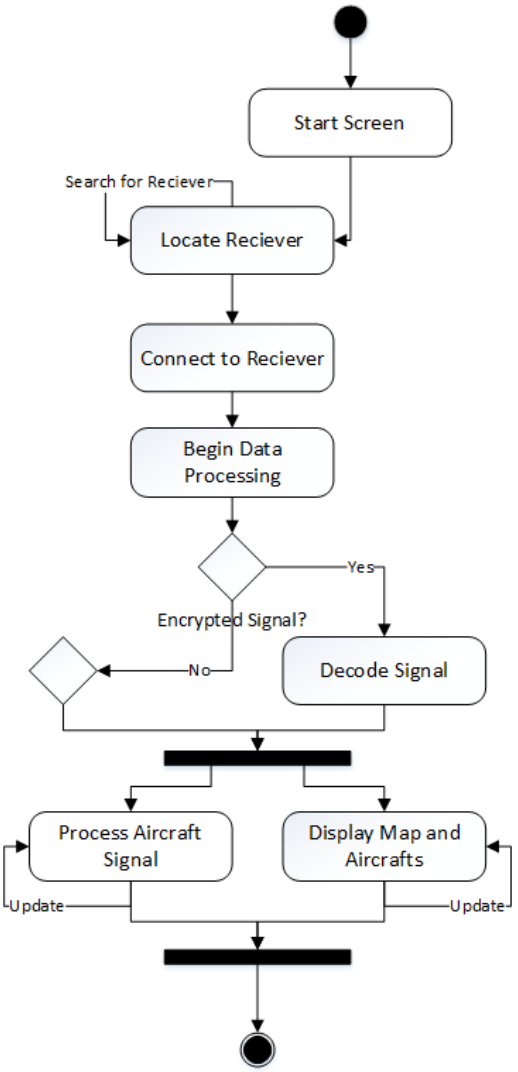


Figure 6. Android Application Flowchart

When the applications begins, a menu screen will appear asking the user to enable their Bluetooth Adapter. Should the current device does not have an adapter, a message will appear warning the user of this issue. Once the adapter is on, a list of possible Bluetooth devices will be display. The user will then select the receiver from this list and the application will connect to the device. After connecting, the application will begin to process data. As this occurs, the map's initial location will be set to the user's smartphone GPS location. During processing if the signal is encrypted, decode the data and then display it to the screen. If not, display the data straight to the screen for the user to view. As the user view the aircraft information, the program will continuously update the information while updating the user's view. Having to deal with a large amount of data, the general interface for the application is quite simple.

VIII. Conclusion

The Mode-S receiver and ADS-B decoder project has allow us to gain valuable experience that will be useful for our future careers. This experience includes working as a group, reading and understanding technical documents, and writing professional technical documents as well.

From the beginning, this project had each member use what we learned to create a system that can be used in the real world. From that, we learned the importance of proper research, as it was needed to give the project a chance to succeed. As work continued, we had encountered many real world issues when it came to implementation. Coming up with solutions to these issues shows us that even the simplest component can make a big difference in an application.

Acknowledgement

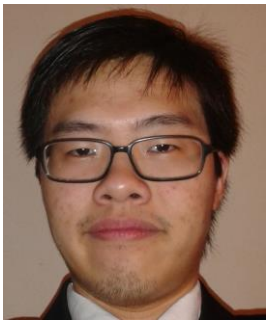
The authors wish to acknowledge the sponsorship and special contributions of the following corporations and individuals whose support has been invaluable:

- Boeing
- Harris
- Keysight Technologies
- Epec Engineered Technologies
- Dr. S. M. Richie, Faculty Advisor
- Dr. Gong
- Nathan Bodnar
- Chris Faehnel
- Bud Simciak

BIOGRAPHY

Michael Vose, a senior student at the University of Central Florida computer engineering department. Transitioning from legacy systems programming to modern methods and architectures with a special concentration in secure computing technologies.

Sean Koceski, a senior student at the University of Central Florida computer engineering department. Planning to pursue a working career in the computer engineering profession.



Long Lam, senior student at the University of Central Florida studying Computer Engineering. Currently working as an intern at Computing System Innovation.

REFERENCE

[1] McCallie, Donald. “EXPLORING POTENTIAL ADS-B VULNERABILITIES IN THE FAA’s NEXTGEN AIR TRANSPORTATION SYSTEM.” AIR FORCE INSTITUTE OF TECHNOLOGY, 1 June 2011. Web. 10 Nov. 2014. <http://apps.fcc.gov/ecfs/document/view.action?id=7021694523>.

[2] Magazu III, Domenic. “EXPLOITING THE AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST SYSTEM VIA FALSE TARGET INJECTION” AIR FORCE INSTITUTE OF TECHNOLOGY, 1 March 2012. Web. 10 Nov. 2014. <http://www.dtic.mil/dtic/tr/fulltext/u2/a561697.pdf>.

[3] Nickels, Robert. "Virtual Radar from a Digital TV Dongle." ARRL, The National Association for Amateur Radio. American Radio Relay League, 1 Jan. 2014. Web. 1 Dec. 2014. <http://www.arrl.org/files/file/QST/This Month in QST/January 2014/VirtualRadarJan2013QST.pdf>.

[4] FlightAware Live Flight Tracking. FlightAware. Web. 1 Dec. 2014. <http://flightaware.com/>.

[5] Flightradar24 Live Air Traffic. Flightradar24. Web. 1 Dec. 2014. <http://www.flightradar24.com/>.

[6] Obama, Barack. "President Barack Obama's State of the Union Address -- As Prepared for Delivery." The White House. Office of the Press Secretary, 12 Feb. 2013. Web. 1 Dec. 2014. <http://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address>.

[7] AIAA, "A Framework for Aviation Cybersecurity." The American Institute of Aeronautics and Astronautics, 1 Aug. 2013. Web. 1 Dec. 2014. <https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf>.

[8] CAO, "SECURITY ISSUES OF ADS-B OPERATIONS." International Civil Aviation Organization, 1 Apr. 2014. Web. 1 Dec. 2014. <http://www.icao.int/APAC/Meetings/2014 ADSBSITF13/WP19_India AI.7 - Security Issues of ADS-B operations.pdf>.

[9] Finke, Cindy, Jonathan Butts, Robert Mills, and Michael Grimaila. "Evaluation of a Cryptographic Security Scheme for Air Traffic Control’s Next Generation Upgrade." Air Force Institute of Technology. Web. 2 Dec. 2014. <http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/ICIWedit2.pdf>.

[10] Bellare, M., Rogaway, and P., Stegers, T. (2010) The FFX mode of operation for format-preserving encryption. <http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf>.

[11] Wang, “Determining Dielectric Constant and Loss-Tangent in FR-4”, UMR EMC Laboratory Technical Report TR-00-1-041, March, 2000. <http://test-fixture.wikispaces.com/file/view/TR00-1-041.pdf>.

[12] Analog Devices, Inc. AD8319 (Rev. C) (n.d.): n. pag. Analog Devices, Inc. Web. <http://www.analog.com/media/en/technical-documentation/evaluation-documentation/AD8319.pdf>.

[13] "MAX1192 Ultra-Low-Power, 22Msps, Dual 8-Bit ADC." Maxim Integrated. N.p., n.d. Web. 15 Nov. 2014.

[14] Tanenbaum, Andrew. (2002). Computer Networks (4th Edition). Prentice Hall. pp.