Week 2 Theoretical

The goal for this week is to ultimately create a decoder for the signals capture by the 1090 filtered SDR (Software-Defined Radio). We can break this down into multiple "layers"

Layer 1

In our current air space, every plane that's equipped with a modern transponder (receives signals and transmits a new signal), is periodically "shouting" in the air on a frequency of 1090 MHz. This is why we connected a 1090 SDR (Software-Defined Radio) filter specifically.

Every time the plane "shouts", it transmits a radio frequency about 120 µs . Inside this shout contains two things

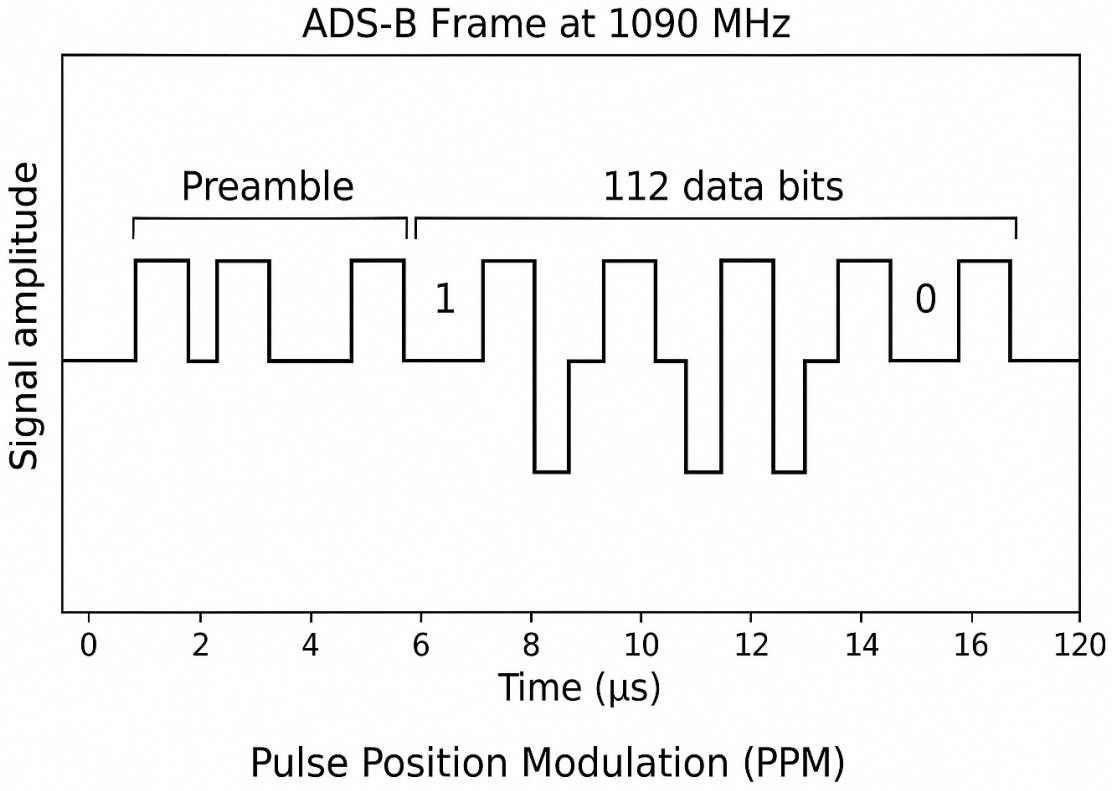
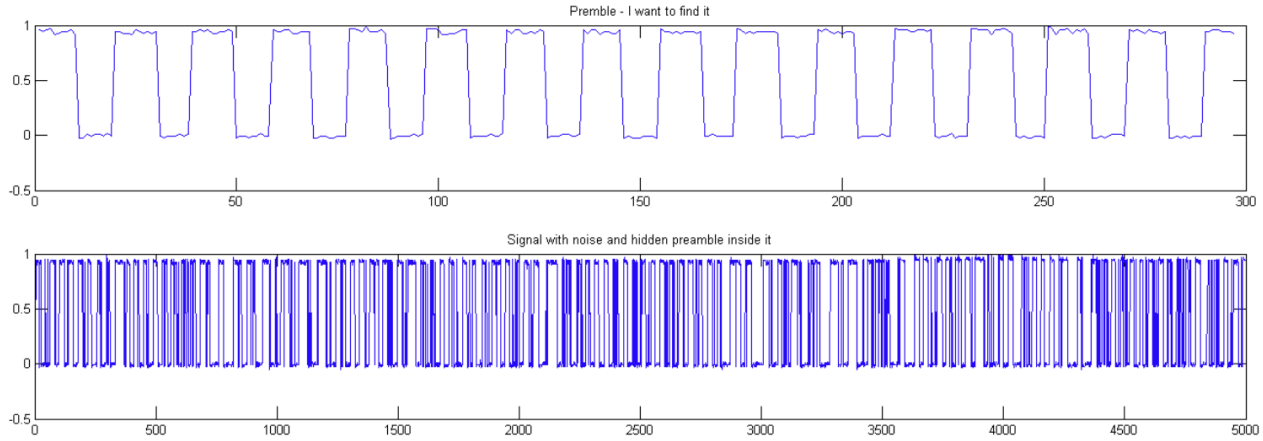


Figure 1: Example graph of a capture frame in 1090 MHz

1) A known preamble pattern for about 8µs
2) About 112 bits of data that says specific information such as aircraft identity and it's current altitude XYZ

Layer 2: Reality Of What We Receive Without a 1090 Filter



Here's an example signal that we want to capture ADS-B Preamble. This is a signal that is constantly transmitted by a plane's transponder. However in reality, we don't capture this signal by itself. It is usually hidden within a bunch of other signals transmitted(noise in this case).

By using a 1090 MHz band-pass filter, it helps remove signals **outside** the ADS-B (Automatic Dependent Surveillance – Broadcast) band. This doesn't eliminate noises completely but it dramatically reduces irrelevant energy

Through software, we can use techniques such as threshold and pulse detection to further isolate the preamble and extract the actual data bits inside the ADS-B message. When we "capture" a signal, we are storing samples, numbers that represent the plane's radio wave over time. These numbers form a HUGE list, known as IQ samples, representing how radio wave vibrates

In terms of setup, I configured receiver to have a:

Sample rate = 2,000,000 samples per second (2 MHz)
Center frequency = 1,090,000,000 Hz (1090 MHz)

So what do these numbers mean? At 2 MHz sample rate, the SDR record 2 million samples per second, meaning one sample every 0.5 microseconds

These captured numbers in the form of IQ samples, are each represented in the form of I + jQ , a complex number.

I (In-phase) = How much of the signal is aligned horizontally
Q (Quadrature) = How much of the signal is aligned vertically

Combining these two together allows me to obtain:
1) Amplitude – How strong the signal is
2. Phase – Where the wave is in its cycle

Amplitude allows us to detect pulses while Phase helps decode modulation. If we combine the two, it allows digital demodulation such as ADS-B PPM (Pulse Position Modulation) decoding. This is the method planes use to encode simple information such as 1's and 0's into radio pulses.

After we detect and capture the preamble, we can slice the message into bit-sized windows. The windows are based on federal standard layout:

1) Bits 0 to 4 = Downlink Format (df)
2) Bits 5 to 7 = Capability (ca)
3) Bits 8 to 31 ICAO address

These three fields always exist in every ADS-B (Automatic Dependent Surveillance-Broadcast) message, regardless of message type. This is the reason why I focused on decoding them first.

The rest of the ADS-B frame such as the message payload (rawM) and the CRC (cyclic redundancy check) depends on the message type and contains information such as altitude, position, velocity, identification, or status

A good analogy for this in our networking background, when we inspect a packet, we always see a certain header fields such as MAC, IP, and protocol information. The deeper the payload changes depends on the type of packet

Decoding the Payload and CRC is tabled for week 3