Spoofer Analysis

The spoofer takes a number of drones and a starting location as input. Locations of drones are calculated from this starting location. Instances of drones have **random Mac addresses and operator IDs** so no simple filtering based on identificators is possible.

Metadata

Mac address always starts with a zero, it is random after 1st character. **RSSI** probably depends on the device used for spoofing or is null. **Timestamp** is counted from a constant starting date in the year 2022.

Data

The majority of data fields in messages are constant default values.

```
location_data->Status             = ODID_STATUS_UNDECLARED; // 0
location_data->SpeedVertical      = INV_SPEED_V;
location_data->HeightType         = ODID_HEIGHT_REF_OVER_TAKEOFF;
location_data->HorizAccuracy      = ODID_HOR_ACC_10_METER;
location_data->VertAccuracy       = ODID_VER_ACC_10_METER;
location_data->BaroAccuracy       = ODID_VER_ACC_10_METER;
location_data->SpeedAccuracy      = ODID_SPEED_ACC_10_METERS_PER_SECOND;
location_data->TSAccuracy         = ODID_TIME_ACC_1_5_SECOND;
```

Some values are random or are generated in a randomized way with some seed value. **Operator id** contains random characters, so also numbers in country code. Fields that change are:

- location, heading, speed, altitude
- number of satellites, not used in Remote ID
- timestamp

Location

The initial location of the drone is the starting location with an offset of -0.0005 to 0.0004 degrees.

```
utm_data.base_latitude = latitude + (float) (rand() % 10 - 5) / 10000.0;
utm_data.base_longitude = longitude + (float) (rand() % 10 - 5) / 10000.0;
```

After each update, there is a delay of `200 / num_spoofers ms`. On update, the new location is calculated from the randomly generated speed. Acceleration is in the range of -10 m/ms^2 to 10 m/ms^2

```
speed_m_x += float(rand % int(2 * max_accel) - max_accel) / 1000.0 - 0.05 * x;
speed_m_y += float(rand % int(2 * max_accel) - max_accel) / 1000.0 - 0.05 * y;
```

```
// compute the heading based on speed
double heading_rads = atan2(speed_m_y, speed_m_x);
int heading_degs = int(heading_rads * angle_rad2deg);
utm_data.heading = heading_degs % 360;

// calculate the new x, y
x += speed_m_x * time_elapsed_secs;
y += speed_m_y * time_elapsed_secs;

// update the lat long degrees
utm_data.latitude_d  = utm_data.base_latitude  + (y / m_deg_lat);
utm_data.longitude_d = utm_data.base_longitude + (x / m_deg_long);
```

Proposed methods for filtering spoofed data

Analysing single container

When a new message container arrives to the flutter-opendroneid, it should undergo a series of tests designed to determine if data may or may not be spoofed. Not all messages may be available at the time in a container.

There would be several tests, each would respond if data may be spoofed, are probably not spoofed or no decision could be made. For example, if Mac does not start with 0, it suggests that data are not spoofed. On the other hand, numbers in country code of Operator ID would suggest data are spoofed. Another type of test would be to check if messages contain default values. Keep count of how many of these tests suggested data may be spoofed and if this count reaches some threshold, consider data spoofed and filter out. The downside is that these filters could be easily passed by changing constants in spoofer code.

Data	Spoofed	Real
mac address	starts with 0	any mac
satellites - not useful	min 8	
operator id	any	first 3 letters are capital
aut/loc/system timestamp	started 16.12.2022	actual timestamp
messages	mainly default values	real values

Analysing data series

Analysis of a whole set of received data, not just one container enables more in-depth analysis but is much more demanding.

Analyse location data

Analyse the movement of drones to find irregularities. Also, the location may be too far from the phone location (if available).

Analyse RSSI

Compare RSSI with a location to see if changes in RSSI and location correspond to each other and make sense, e.g. it would be suspicious if RSSI was the strongest when the device is further away.