Non-Cooperative RF Source Identification for Drone Localization Using SDR-Based System

F. Auguy[1], H. des Dorides[1], D. Petrovic[1] and C. de Loture[1]

[1]Undergraduate Students, ECE Paris School of Engineering, France
(Email: florian.auguy@edu.ece.fr)

***Abstract*:** *In this study a method is presented for detecting and tracking non-cooperative Radio Frequency (RF) sources, within the 2.4 GHz frequency band, in a specific area. The ways in which these signals can be isolated among the heap of other signals is explored, as well as the possibility to locate unidentified radio frequency sources by using various algorithms. The research rests upon the growing potential of Software Defined Radios (SDR) by using the Ettus USRP N210, as well as open source projects for Orthogonal Frequency Division Multiplexing (OFDM) receiver implemented in GNU Radio and the RFtap protocol.*

Keywords: *SDR; Drone Localization; OFDM; RFtap*

1. Introduction

With the recent very fast growing development of flying objects and especially of drones, it becomes urgent for control and safety of this increasing flow, like for regular airplane traffic, to set a reliable recognition system able to identify these objects in real time. Most actions today are based on simple bilateral relations between the flying object and his driver because they are not autonomous and their range is relatively modest for most of them. The identification problem already exists however in a certain number of situations, as well as the determination of flying object trajectory.

The goal of present publication is to propose a system capable of tracking in real-time the position of drones flying over an area. The idea is to isolate emitted signals by the drones, extract position related characteristics from the signal, and use them to estimate a position. To perform the task, the system is composed of four distinct parts: signal acquisition, signal characteristics analysis, sources filtering and localization.

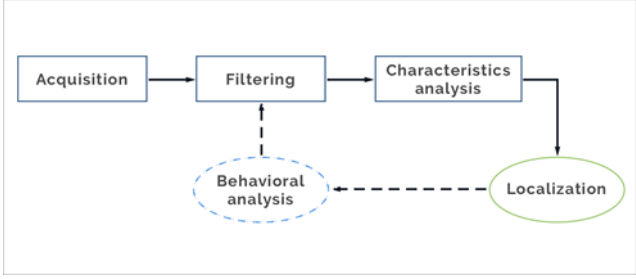

Fig 1 : System Functional Analysis Scheme

The acquisition subsystem is made up of independent modules that have to be gathered. These modules are in charge of intercepting the communication of the WiFi protocol with an USRP. The filtering part is used to eliminate the sources that are not drones. The aim is to focus the localization only on the interesting sources and to find criteria asserting that a specific source is not a drone rather than to look for clues which could prove that the source is definitely a drone. The reasons for this choice are discussed later on. The signal characteristics analysis part is needed to aggregate the collected information and to compute the necessary additional data to locate the drone. Finally, the localization part uses the data measured and computed. This is the reason why it

could be done by using different methods depending on the relevance of measured characteristics as well as previous localization as it is a position tracking.

2. System Identification

Here the behavioral analysis is represented as a closed-loop system, see Figure 1. Sources localization vs time gives valuable information which is used for the filtering part. It could also be interesting to look into the possibility to parallelize computations of the different parts for improving system efficiency.

2.1. Signal Acquisition

From the very principle of wave propagation, each signal is altered when traveling through a medium. The signal takes some time to travel, is attenuated, and its frequency is shifted if the source or receiver is moving. By measuring the Received Signal Strength (RSS), the Frequency Difference of Arrival (FDOA), and/or the Time Difference of Arrival (TDOA) of received signals, and comparing in time and space throughout multiple antennas, one can obtain information about source position and movement.

Drones are in constant communication with their controller, for telemetry or video feed. There thus exists a continuous source of data to analyze for helping in their localization. To exploit it, one needs to be able to differentiate a drone signal from noise, and even other non-drone sources.

2.2. WiFi

The WiFi protocol, specified in the IEEE 802.11 standard, is often used to establish a link between the controller and the drone in many Commercial Off-The-Shelf (COTS) devices. By passively sniffing WiFi frames around signal collecting antennas, those coming from or going to drones can also be received in antenna vicinity. Useful information can then be extracted from the gathered frames.

Communication is often encrypted using protocols like WPA2 to protect packets. This encryption operates on layer 2 so everything on the upper layers is not accessible. The Data Link layer is in present case primordial as it is a definitely accessible one, and readable information is present in these headers regardless of the non-cooperative setting.

MAC addresses of communicating actors are present in the readable header. The main use of this MAC address is to identify the unique sources of frames, and thus signals. One can easily find all the sources talking or being talked to, and have a way to aggregate and bundle frames from a unique source together.

2.3. OFDM Demodulation

While sniffing WiFi frames is possible by using a wireless network interface card, the static nature of the hardware will mean that its behavior cannot be modified to fit present needs. Specifically, although many different WiFi protocols (eg. b/a/g/nc) can be demodulated and read, only sent data vector can be extracted. By doing the demodulation, more control on the processing chain can be gained, and RF information can be added using digital processing, see Figure 2.

The OFDM Receiver project [3] allows demodulate OFDM WiFi frames from the 802.11 a/g/p protocol using the USRP. Even though using only one type of modulation can limit the functionality of the system, it is worth noting that OFDM is widely used because of its spectral efficiency. The AR Parrot drone on which tests have been performed, has a network interface compatible with b/g WiFi, 802.11g using the OFDM modulation.

OFDM has many interesting characteristics which can be used to extract reliable position related parameters. The known preamble allows easily find the start of a received frame with a correlation, thus giving the signal reception time and fixing the start of the data frame. The four pilot subcarriers at known frequency, meant to allow frequency offset correction for the OFDM demodulation, provides a measurement of the frequency offset, and thus the target velocity. Also, the cyclic prefix of each symbol, in addition of helping with channel estimation, gives a guard time for multipath propagation interference.

This solution has its limitation. A bandwidth of 20MHz is needed to monitor a whole WiFi channel. With the maximum 25MHz bandwidth of the used Ettus N210 USRP, frequency hopping is needed if all channels need to be covered. Otherwise, some sources will be ignored. Furthermore, the pipeline will ignore preamble arriving shortly after the previous one, so some frames are missed. Finally, having only a SBX Rev. 2 daughterboard for the Ettus N210, the tests are only performed on the 2.4 GHz frequency spectrum, thus using only the 802.11g WiFi protocol.

2.4. RFtap

The PDU (Protocol Data Unit) traveling across the GNU Radio demodulation chain carries the information between the different demodulation blocks, along with other characteristics such as the nominal frequency, the frequency offset and the signal-to-noise ratio (SNR). Those information are present in a header used by the different GNU Radio blocks, and is discarded at the end of the chain when the final data frame is created.

The RFtap protocol adds an additional header to the standard WiFi frame data vector, adding those RF information that would be otherwise be ignored. Additional parameters can easily be computed by Digital Signal Processing and added to the RFtap header, if needed.

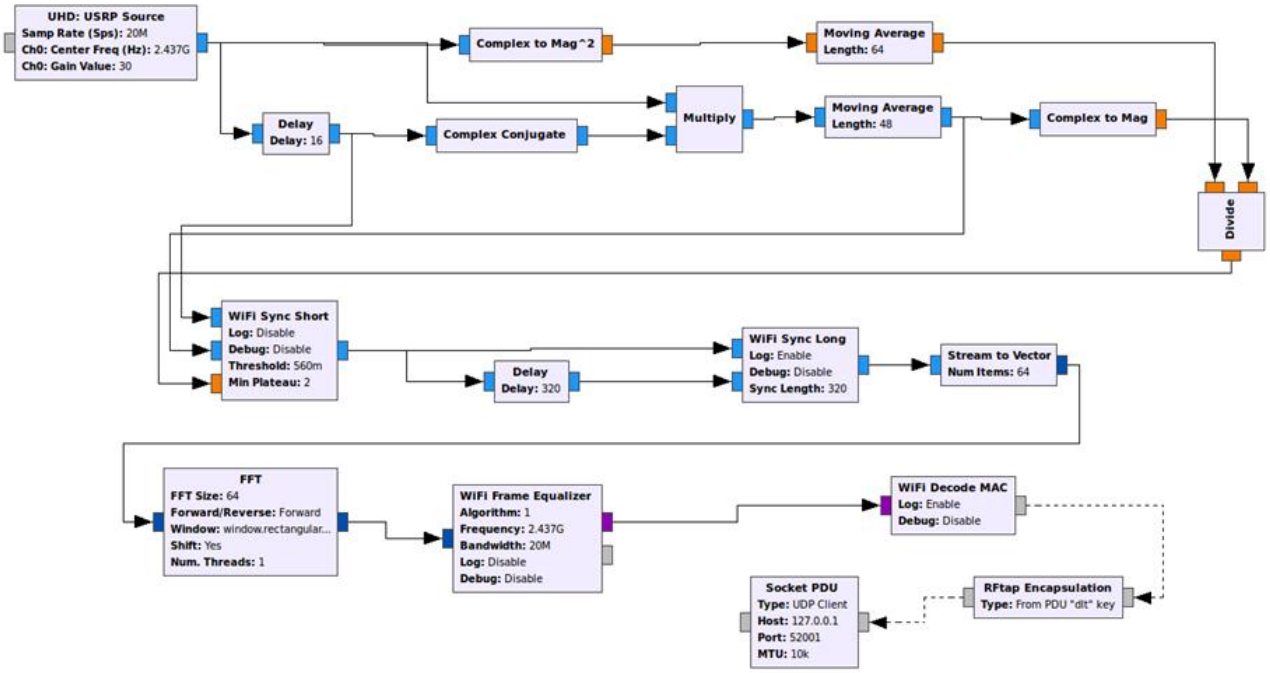

Fig 2 : WiFi Demodulation Chain with RFtap Encapsulation

With the standard frame information obtained by manual demodulation, one can have here not only the same information as by using a wireless interface card, but also additional characteristics related to the signal which can be exploited by the filtering and localization subsystem. The process for getting these RF characteristics occurs in parallel to the frame demodulation, since at this point no information about the source is yet known. Because the modularity of the GNU Radio chain and the flexibility of SDR, one can easily make experiments with the signal processing for chain tuning and calibration to provide accurate data.

The RFtap protocol is integrated in tools such as Wireshark or the command line equivalent Tshark, and can easily be analyzed and manipulated to interface the data with other applications.uy

2.5. Filtering

This subsystem aggregates the frames coming from a same source, filtering and ignoring the sources that do not fit specified criteria. Those frame bundles will be sent to the next subsystem, along with the binary information and the RF characteristics that are present alongside them.

By combining RF and WiFi information in the same binary structure, filtering based on both types of information is enabled. Using tools integrating the RFTap protocol (Wireshark or Scapy for example), one can use any field of the frame as an elimination criteria.

For example, the MAC address can be used for identification if one of the actors of a wireless communication is a drone. Every drone vendor has a MAC addresses range assigned to him. Using a database of MAC addresses ranges per drone constructor, it can easily be asserted if a MAC address belongs to a drone or not.

However, since a non-cooperative situation is assumed, the MAC address could be changed and even randomized. With the access to a wide range of RF metadata about the frames, more complex filtering schemes can be considered using more available variables. For example, frames could exhibit some common spectral signature allowing assert that they are coming from the same source. These spectral signatures may be discovered in a test environment by relying on a known MAC to gather the data from the test source.

Having multiple sources of information allows eliminate more reliably uninteresting sources. This is why a feedback loop from the localization subsystem has been considered here as shown on Figure 1. Once the tracking has been done by the localization subsystem, static or slowly moving targets can be eliminated in order to spare processing power, and further eliminate non-relevant sources.

The goal of the filtering subsystem is to output relevant data points to the next subsystem. These data points are bundled together by source. Each data point is identified with a MAC address, a time of reception and the available RF characteristics. The next subsystem can then analyze the available data, using the fields from the data structure that are useful to it.

In present application, it is used to track the sources, and to pinpoint which ones of them are drones. By relying upon the information of the data link layer to associate signals to potential sources, usual need to do computational complex and intensive plot to track association necessary in radar systems is here completely eliminated. Moreover, by using the already existing communication between drones and their controller, a passive system has been designed without any emission.

3. System Localization

The identification system is compatible with the majority of localization methods, depending on the type of sensors. Thanks to the WiFi demodulation chain, one can localize the identified source. For instance, in the case of packets containing the emitting and received power, with only three sensors, classical trilateration can be used. Specific sensors would allow other techniques: for example, using directional antennas would allow apply triangulation. The localization part has a quite light computational load compared to identification. Implementing an efficient tracking therefore needs a fast identification (helped by the loopback of localization). Moreover, statistic and probabilistic tools will limit the uncertainty coming from interferences or sensors' characteristics. To prove that localization is possible after proposed identification method, a very basic, yet working algorithm needing only received powers has been created.

Here a non-cooperative RF emitter localization system is proposed. It has been tested under MATLAB simulation. A clear environment is assumed, i.e. with no multipath, no diffraction, so that Friis equation can be applied. This allows simulate the received power by an antenna according to emitter parameters and distance. Waves propagate under Free Space Path Loss (FSPL), having a computable attenuation, thus allowing know the distance to emitter. Being in non-cooperative scenario brings incertitude: the emitting power is ignored,

trilateration is not adapted as one cannot distinguish a far drone emitting at full power from a near one with low power.

The idea is to study the Received Strength in a grid of sensors and look for three similar values. This received power is computed via Friis equation. However, one cannot have the exact same values which would guarantee a maximal precision because it would require a huge number of sensors. Therefore, the minimal difference between sensors is researched with a maximum 1% differential. An important difference allows more localizations with more errors, whereas a small one reduce errors but also the number of localizations. The three selected points allow compute a circle equation with the drone as center, see Figure 3. Additionally, three grids may be used to perform a trilateration or a triangulation of the three estimated positions. However, this would require many sensors as every single grid should have sufficient precision: despite two precise localizations, a third grid with less precision would lead to the very opposite result.

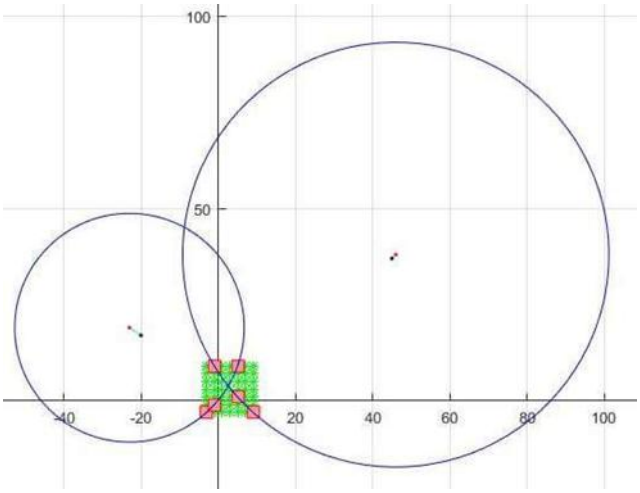

Fig 2 : Localization Concept Scheme

With a single grid of 121 sensors, an average error of 4m at 100m of the drone and 12m at 200m is obtained, see Figure 4. Beyond this range, the results are too variable and the precision is not satisfying. It can be increased to the expense of the number of localizations. However here the error is not constant. Depending on real drone position, similar values of received power cannot be guaranteed depending on whether sensors are suitably placed for a precise position. However, those results have been obtained in simulation by randomly plotting drones.

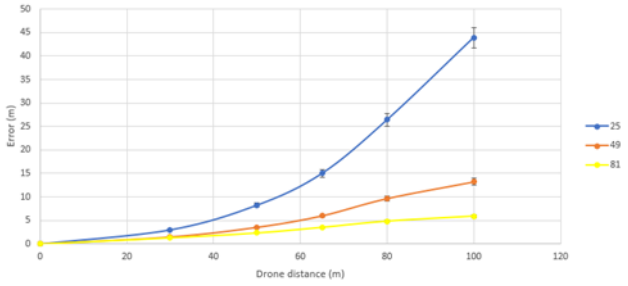

Fig 4: Average Error of Localization System vs.Sensor-Source Distance

Continuous tracking could change this issue. If for instance the targeted drone is detected at 40m of the grid, then at 150m for only a few seconds, the intermediate result can be eliminated. Moreover, here only a squared grid has been tested, and error variation would be more limited with a circled one (the problem being to set such a grid). Again, the results can be improved by increasing the number of sensors.

Virtual sensors can be created to reduce cost. As Friis equation is applied on grid sensors, one can compute a virtual one in the middle of a square formed by four real ones. However this interpolation would create additional incertitude which could be minimized by the FSPL hypothesis. For a more realistic environment, the sensors can be calibrated by creating a fingerprint of RF spectrum, thus building a map of the sources of interference and diffraction in order to minimize errors. Despite mentioned uncertainty issues, present system allows localize non-cooperative drones with modest computational load and acceptable precision, and without any hypothesis on the emitting power or protocol. Finally, probabilistic and statistic tools like Kalman Filter and its derivatives, especially the Unscented Kalman Filter, may allow reduce errors before processing and work on noisy data samples.

By having access to information of the localization as well as the speed and motion pattern, an additional method of finding out the type of a source is obtained. With a multitude of estimators, each tuned to a different behavior, we may make hypothesis and validate or reject them according to the measurements, and make predictions when some frames are not captured.

4. Conclusion

From the flexibility of SDR and the very active open source community tools exist for building a system isolating signals coming from drones, for extracting interesting characteristics using digital signal processing, and for using them in a direct application such as localization. By combining the physical and data link layers of WiFi frames, it has been shown that identifiers can be added to raw signals which can then be grouped together by source and filtered using relevant criteria. Using data collected by an antenna is simple. This system thus opens up the way to multiple interesting projects that only need an USRP to start.

The next step is experimenting with the signal characteristics extraction process, tuning and calibrating it. Then, the collected data can be used to build up sources profile by looking at their spectral signature, perform a localization of the sources. Finally, the filtering criteria has be devised to fit the objective of the end-system for best accuracy.

5. Acknowledgment

The authors are very much indebted to ECE Paris School of Engineering to have provided the necessary setup for the development of the project. They would like to thank Dr F. Saidi for helpful critical view, Dr. V. Nuzzo and Pr. M. Cotsaftis for guidance throughout the research community, and Dr. R. Zitouni for lending them the USRP and introduction to the endless possibilities of SDR.

6. References

[1] P.~Nguyen,M.~Ravindranathan, and A.~Nguyen, “Investigating Cost-effective RF-based Detection of Drones”, DroNet 16, June 26 2016, Singapore, Singapore\hskip 1em plus 0.5em minus 0.4em\relax Olson M.V., Title of Chapter of a book, in Classic Sciences. A. Editor \& B. Editor, Publisher City: Publisher Name, pp. 212-213 \(1999).

[2] S.Gezici, A Survey on Wireless Position Estimation, Springer Science+Business Media, LLC. 2007.

[3] B.Bloessl, M.Segata, C.Sommer and F.Dressler, “An IEEE 802.11a\/g\/p OFDM Receiver for GNU Radio”, SRIF 13 - Software radio implementation forum (p 9-16)..

[4] B.Bloessl, M.Segata, C.Sommer and F.Dressler, “Towards an Open Source IEEE 802.11p Stack: A Full SDR-based Transceiver in GNU Radio”, DOI: 10.1109 - Conference: IEEE Vehicular Networking Conference (VNC 2013) (pp. 143 - 149).

[5] N.N. Okello, F. Fletcher, D. Musicki, et al., “Comparison of Recursive Algorithms for Emitter Localization and TDOA Measurements From a Pair of UAVs”, in IEEE Transactions on Aerospace and Electronic Systems 47(3):1723 - 1732, August 2011.

[6] K.A.Gotsis, I. Kyriakides, J.N. Sahaloss, "3D Localization and Frequency Band Estimation of Multiple Unknown RF Sources Using Particle Filters and a Wireless Sensor Network," Springer Science+Business Media - New York 2016.

[7] M. Jakubiak, "Cellular Network Coverage Analysing using UAV and SDR", Master of Science Thesis, Tampere University of Technology, 2014.

[8] Sathyan T., Sinha A., Kirubarajan T., "Passive Geolocation and Tracking of an Unknown Number of Emitters," IEEE Transactions on Aerospace and Electronic Systems 42(2):740 - 750, May 2006.

[9] Alyafawi I., Dimitrova D.C., Braun T., "SDR-based Passive Indoor Localization System for GSM," SRIF 14 - August 18, 2014, Chicago, IL, USA.

[10] Sun M., Ho K. C., "An Asymptotically Efficient Estimator for TDOA and FDOA Positioning of Multiple Disjoint Sources in The Presence of Sensor Location Uncertainties," in IEEE Transactions on Signal Processing 59(7):3434 - 3440, August 2011.

[11] Vesely J., "Differential Doppler Target Position Fix Computing Model. In Proceedings of the International Conference on Circuits," Systems, Signals, pages 284-287. WSEAS Press.

[12] Wang W.D. and Zhu Q.X., "RSS-based Monte Carlo localisation for mobile sensor networks," in IET Communications 2(5):673 - 681, June 2008.