Localization of drone operator using Unmanned Aerial Vehicles: Preliminary research

Ivan Magdalenić, Neven Vrček, Boris Tomaš
Faculty of Organization and Informatics
University of Zagreb
Varaždin, Pavlinska 2
{ivan.magdalenic, neven.vrcek, boris.tomas}@foi.unizg.hr

Karl Sölvi Guðmundsson
Faculty of Electrical and Computer Engineering
University of Iceland
Sæmundargötu 2, 102 Reykjavík
karlsg@hi.is

***Abstract**. The paper presents the results of a preliminary study of the localization of drone operator using other multiple Unmanned Aerial Vehicles. The emphasis is put on hardware testing, to be mounted on UAVs, in order to detect, identify and track drone signal and to enable localization of drone operator. Since UAVs can carry limited cargo mass, the challenge is to find optimal hardware in terms of ratio of mass and receiving signal capabilities and processing power. The paper describes results of the experiment where hardware, to be mounted on UAVs, is used to measure the signal strength of the intruder drone operator.*

Keywords. Localization, UAV, drone

1 Introduction

The popularity of drones is growing day by day and more and more drones of different sizes and capabilities are filling the sky above us. The main difference between Unmanned Aerial Vehicles (UAVs) and drone is that UAV needs to have autonomous flight capabilities, whereas drones do not. In addition to business and recreation, drones could be used for illegal activities such as unauthorized entry into prohibited airspace and for invading privacy. In the rest of the paper, a drone that does illegal activities will be called an intruder drone and the person who controls it will be called the intruder drone operator. Although the intruder drone itself is visible in the sky, it is difficult to locate the intruder drone operator to prevent him to continue or repeat illegal activities.

The idea of our research is to locate a drone operator by measuring the strength of its wireless signal at several locations at the same time and using the obtained data to calculate its location. There are several challenges that need to be addressed. The first challenged is to identify the right wireless signal. The radio frequency spectrum is often saturated and it is not clear which signal belongs to the intruder drone and its operator. The situation is particularly pronounced in urban areas. The second challenge is to track the intruder drone as it is very fast and can change its location quickly. Our answer to both challenges is to use several UAVs (swarm) to get close to the intruder drone, track it and to catch the strongest signal in the area. Once the signal emitted by the intruder drone is identified, the next step is to identify the intruder drone operator signal by searching the same pattern in other signals in the same frequency band. The other advantage of this approach is to have multiple measured values of signal power on different location which makes it easier to calculate the exact location of the intruder drone operator, which moves significantly slower than drone

The paper is organized as follows: the second chapter brings related work, the third chapter describes our proposal of drone localization using UAVs, followed by a description of the first experiment, and the last part brings discussion, conclusion and future work.

2 Related work

Localization of signal sources by measuring signal strength and calculating position is not new and has been used for decades especially for military purposes. (Jawhar, 2017) and (Hayat, 2016) provide an overview of the communications and architectures used in UAVs. It was pointed out in the papers that a smaller number of drones use the pure IEEE 802.11 standard for communication, while most drones use their own modified version of the IEEE 802.11 standard. We single out here two papers (Bisio, 2018) and (Ezuma, 2020) dealing with the detection and classification of drones, based on information available from captured communication between the drone and the drone-controlling system. Learning techniques were used to identify and classify drones. The paper (Ezuma, 2020) lists the equipment used: 6 GHz bandwidth Keysight MSOS604A oscilloscope with a maximum sampling frequency of 20 GSa / s, 2 dBi omnidirectional antenna (for short-range detection), and 24 dBi Wi-Fi network antenna (for detection) at greater distances). Antennas are used in the 2.4 GHz spectrum. Common to both approaches is the use of stationary equipment of large dimensions and mass. Such approach is not practical nor suited for real life situations. That is why our approach is based on small, lightweight and fast constellation of drones controlled by only one operator who is driving entire swarm by the software we developed as a part of our research.

Similar research to our approach was conducted by usage of fixed-wing unmanned aerial vehicles (UAVs) and described in (Frey et all. 2008) and (Fray, 2008) were different flight parameters were investigated to locate a moving target. Our approach differs in that we use UAVs with multiple rotors that do not have the ability to stay in the air for a long time and that cannot carry more additional weight. Therefore, flight parameters and detection algorithms must be adapted specifically for such equipment. Compared to fixed-wing, multirotor UAVs have a greater manoeuvrability, thus allowing more flexibility in terms of constellation design and search patterns.

3 Localization of drone operator using UAVs

The basic idea of localization of the intruder drone operator is shown in Figure 1. Several UAVs need to approach the intruder drone as shown in Figure 2.

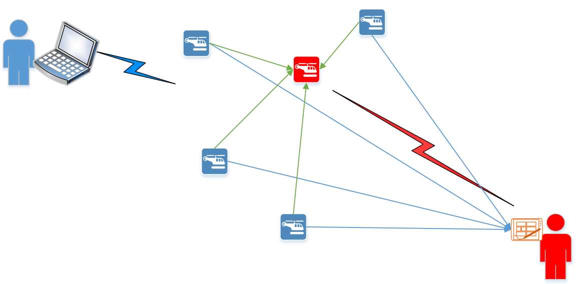

Figure 1. Localization of the intruder drone

We expect to find the intruder drone signal to be the strongest in the vicinity of the drone. The next step is to search the signal of the same pattern that belongs to the intruder drone operator. That signal is received by each UAV and we expect to measure different values of the signal receive power. The final step is to calculate the position of the intruder drone operator based on different location of UAVs and its measured values.

Figure 2. UAV is approaching to intruder drone

Each UAV has equipment mounted for searching and recording of radio signals as shown in Figure 3. The equipment consists of: Raspberry Pi 4 model B with 8 GB RAM, Wireless network adapter Alfa AWUS036ACH, GPS module Ublox NEO M8U and LTE modem HUAWEI E3372. We chose this network adapter because it can be set to monitor mode, which means it can receive all frames on a certain channel. By researching the available technology, we concluded that network adapters that have implemented one of the listed chipsets can be set in monitor mode: Atheros AR9271, Ralink RT3070, Ralink RT3572, Ralink RT5572, Realtek RTL8812AU and Ralink RT5370N. In future research, we plan to acquire other smaller network adapters based on one of the listed chipsets.

We divided our project into two phases. In first phase, we are dealing with intruder drones that are communicating with pure 802.11 protocol. This phase is the proof of concept of our approach and test of our equipment. In the second phase, we plan to use machine learning to find intruder drone signal pattern in radio signal.

For the first phase, we made a software in Python consisting of server part on each drone and desktop application on laptop. Figure 4 shows part of GUI of desktop application. Both, intruder drone and intruder drone operator can be identified by their MAC addresses, which makes it easier to distinguish their radio signal. Each UAV can scan different Wi-Fi channel which speeds up the search for intruder drone signal. After the radio signal is identified, channel is locked and all UAVs are listening to the same Wi-Fi channel.

Figure 3. Equipment for searching and recording of radio signals

Figure 4. Part of GUI of desktop application.

The challenge is to find the best constellation of UAVs in order to speed up the search of radio signal in first step and then to measure the signal strength in the second step. After the measured values are sent to server, the location of the intruder drone operator can be calculated.

Distance will be calculated using the Friis transmission equation (Friss, 1946) where frequency is going to be set to middle of receiving channel, Power component is going to be set to a constant and ignored considering the same signal is received by multiple UAVs. The plan is to use at least four UAVs to exactly calculate the location of the intruder drone. Additional experiments has to be made to determine if more UAVs will increase accuracy and speed of localization.

4 Experiment

The aim of the first experiment was to test equipment and software shown in Figure 3 and to check the feasibility of our approach.

The intruder drone operator is actively operating the intruder drone from its well-known location. GPS coordinates of the intruder drone operator were determined at the start of the experiment for the purpose of later distance calculation. The equipment and software are turned on and are slowly moving away from intruder drone operator. The radio signal is measured until the equipment is so far away that the signal from intruder drone operator is too weak to be received.

The experiment is repeated several times and dependence of received signal strength related to distance is presented in Figures 5, 6 and 7.

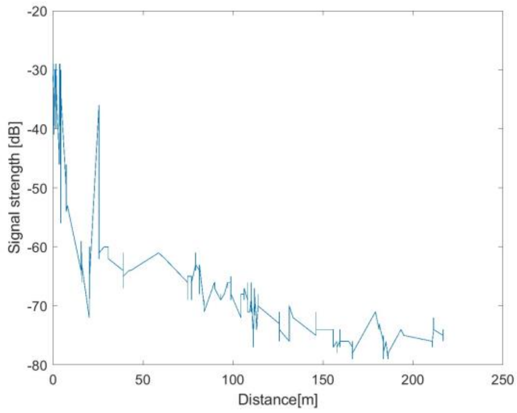

Figure 5. Dependence of received signal strength related to distance – first case

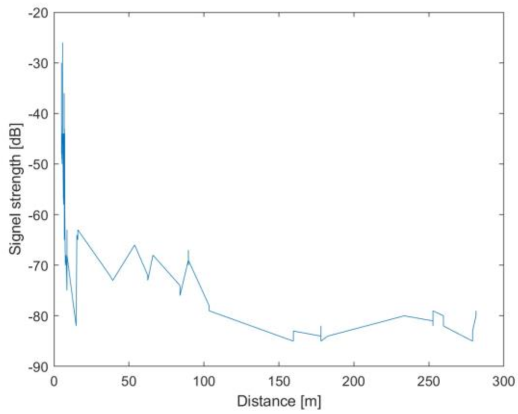

Figure 6. Dependence of received signal strength related to distance – second case

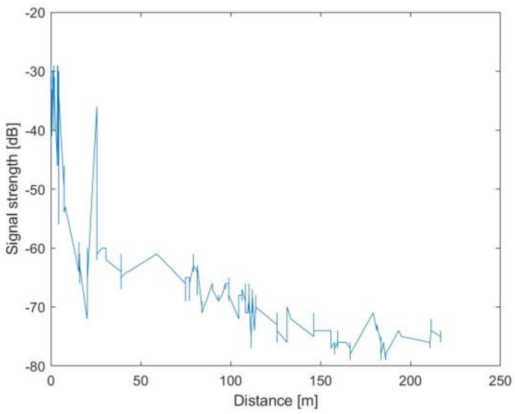

Figure 7. Dependence of received signal strength related to distance – third case

As shown in figures, there is a clear relation between distance of the source of the signal and signal strength and that can be used to determine the location of the source of the signal. In the first 150 meters signal strength is satisfactory and large number of frames are received. After 200 meters, the signal strength is becoming too weak to be received and only a small number of frames are received.

In figures there is a clear limitation of used hardware regarding maximal distance of the receiver from the signal source, and it is about 250 meters. However, it has to be noted that in real scenarios signal might be partially obscured by buildings, trees, etc. This means that this relationship is not that precise. Our future work is directed towards research of such use cases and the development of algorithm capable to compensate eventual signal obstruction.

Since this research is focused on testing the equipment and evaluating the feasibility of our approach, no more experiments were done to determine the ultimate capabilities of radio signal detection. It is planned to do this on equipment mounted on UAVs.

5 Discussion

The advantage of using several UAVs to locate the intruder drone operator, is in short time for identifying and tracking of a target and in flexibility to adopt to the current circumstances in the area. There are also several disadvantages of this approach and the most significant are the short time the drone stays in the air, the size and weight of the signal receiver and the processing power limited by battery power. Although, there are much powerful receivers available on the market, most of them are too big and too heavy to be mounted on a small UAV. The next step is to find an optimal constellation shape of UAVs that will adopt to different scenarios on the ground and that will annul shortcomings of mounted hardware on UAVs by flexible and fast placement in the area.

The conducted experiment has shown some physical and hardware limitations of our equipment. Although the source of our signal in the experiment transmitted packages with constant rate, the rate of the received packages was decreasing with the distance. This means that we received fewer packets with lower power at a greater distance from the source of the radio signal. Although we received packages at distance of 250 meters from the source, we expect that at this distance there will be too few packages received by all four UAVs to calculate intruder drone location. We are planning to mount the equipment used in this experiment on the UAVs and to repeat measurements in order to find exact limitations of our equipment and our approach.

5 Conclusion

The paper presents the results of the experiment where the special hardware is used to measure the signal strength of the intruder drone operator in order to test ability to use those measured values to calculate intruder operator exact location. The experiment shows that it is possible to combine light and small hardware which can be mounted on UAVs and which has enough receiving capabilities and processing power to detect, identify and track radio signal of the intruder drone operator.

The future work is going to follow the next steps on the project and those are mounting the hardware on the UAVs and finding the optimal constellation of UAVs in order to locate the intruder drone operator.

Acknowledgments

This work has been fully supported by Croatian Science Foundation under the project IP-2019-04-4864.

References

Bisio I., Garibotto C., Lavagetto F., A. Sciarrone, and S. Zappatore,. “Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis,” IEEE Commun. Mag., vol. 56, no. 4, pp. 106–111, Apr. 2018.

Ezuma M., Erden F., Kumar Anjinappa C., Ozdemir O. and Guvenc I., "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference," in IEEE Open Journal of the Communications Society, vol. 1, pp. 60-76, 2020, doi: 10.1109/OJCOMS.2019.2955889

Frew E.W., Lawrence D. A., Morris S. Coordinated standoff tracking of moving targets using Lyapunov guidance vector fields. Journal of guidance, control, and dynamics 31 (2), 290-306, 2008.

Frew E.W. Sensitivity of cooperative target geolocalization to orbit coordination. Journal of Guidance, Control, and Dynamics 31 (4), 1028-1040, 2008.

Friis H. T., "A Note on a Simple Transmission Formula," in Proceedings of the IRE, vol. 34, no. 5, pp. 254-256, May 1946, doi: 10.1109/JRPROC.1946.234568

Jawhar I. et al. Communication and Networking of UAV-Based Systems: Classification and Associated Architectures. Journal of Network and Computer Applications · February 2017, DOI: 10.1016/j.jnca.2017.02.008

Hayat S. et al. Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. IEEE Communications Surveys & Tutorials (Volume: 18 , Issue: 4 , Fourthquarter 2016), DOI: 10.1109/COMST.2016.2560343