Localization of intruder UAV operator using Unmanned Aerial Vehicles

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

Abstract. *The paper presents the results of an experiment where multiple Unmanned Aerial Vehicles (UAVs) were used to locate intruder UAV operator. UAVs were equipped with hardware of such dimension and weight that can be mounted on them. The hardware is then used to detect, identify, and track UAV signal to enable localization of intruder UAV operator. The measured signal strength is used to calculate distance between UAVs and intruder UAV operator to determine its exact location. Several problems need to be overcome to achieve that and they are addressed in the paper.*

Keywords. Localization, Unmanned Aerial Vehicles, UAV

1 Introduction

In many countries, there exist regions where the operation of Unmanned Aerial Vehicles (UAVs) is prohibited. These regions may include, but are not limited to, airspace above airports, military installations, and government buildings. Enforcing flight restrictions in these areas, particularly with respect to UAVs, presents a significant challenge. One major obstacle is the difficulty in identifying the location of the UAV operator, who may be concealed several hundred meters away. While it is possible to remotely disable a UAV, for instance by emitting a strong electromagnetic pulse that induces short circuits, this does not reveal the location of the operator. In this paper, we refer to a UAV engaged in unauthorized activities as an "intruder UAV", and the individual controlling it as the "intruder UAV operator".

Our proposed approach involves locating the intruder UAV operator by measuring the strength of their wireless control signal at multiple locations simultaneously and using this data to trilaterate their position. To accomplish this, we employ UAVs equipped with specialized hardware. This approach offers several advantages, including rapid adaptability to changing conditions on the ground and the ability to move our UAVs closer to the intruder UAV operator's location for more accurate positioning. However, there are also limitations to our approach, including the short battery life of our UAVs and hardware, as well as constraints on antenna size and processing power.

The remainder of this paper is organized as follows: Chapter 2 presents related work; Chapter 3 describes our proposed method for localizing intruder UAV operators using UAVs; Chapter 4 details our initial experiment; and the final section discusses our findings, conclusions, and directions for future work.

2 Related work

Localization of signal sources by measuring signal strength is not novel and it is used for military purposes long ago. Signal strength was used in (Kokić, 2017) to introduce secondary information source for enhanced GPS positioning, thus reducing GPS error. Signal strength was converted to distance between UAVs. Their GPS location was corrected to accommodate calculated distances of complex UAV constellations. In the terms of multipaths authors state that this is not an issue because UAVs were operating in clear line of sight, as this is usual UAV application.

In another research (Tomaš, 2013) author used similar technique to localize sources of the signal in urban environments. Sources of information were moving vehicles. Experiment conducted has managed to introduce less than 5m precision of localization of signal sources. This result is significant considering urban environments and multipathing.

To detect and identify intruder UAV operator we have to intercept communication between him and his UAV. (Jawhar, 2017) and (Hayat, 2016) provide an overview of the communications and architectures used in UAVs. It was described in the papers that a smaller number of UAVs use the pure IEEE 802.11 standard for communication, while most UAVs use their own modified version of the IEEE 802.11 standard. We single out (Bisio, 2018) and (Ezuma,

2020) that deal with the detection and classification of UAVs with regard to information available from captured communication between the UAV and the UAV-controlling system. One approach to locate UAV is described in detail in (Ezuma, 2020). The equipment used is 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.

What is common to those approaches is the usage of large equipment that is stationary or mounted on vehicles. Such equipment is not ideal for the hunt of small and fast UAVs. That's way we decided to take an alternative approach and use UAVs.

3 Localization of intruder UAV operator using UAVs

Our approach to localizing the intruder UAV operator is illustrated in Figure 1. The first step involves visually identifying the intruder UAV, after which several of our UAVs are dispatched to its vicinity to measure the strength of its radio signal, which should be the strongest in the area. The next step entails searching for a signal with the same pattern, or in our case, the same MAC address, as that of the intruder UAV operator. The final step involves calculating the position of the intruder UAV operator based on these measurements.

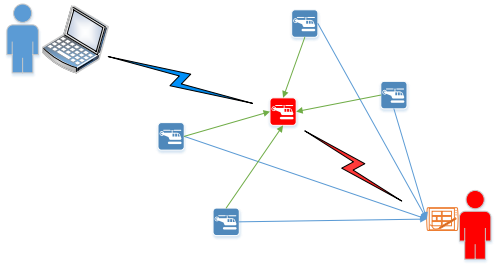

Figure 1. Localization of the intruder UAV operator

In Figure 2 is shown one of the UAVs with scanning equipment mounted and the intruder UAV.

One challenge we faced was developing hardware that was both lightweight and compact enough to be mounted on a UAV. Our initial setup consisted of a Raspberry Pi 4 Model B with 8 GB RAM, an Alfa AWUS036ACH wireless network adapter, a Ublox NEO M8U GPS module, and a HUAWEI E3372 LTE modem (as shown in Figure 2). However, after conducting several experiments, we determined that this hardware was not suitable for our approach due to two main issues: high power consumption, which significantly reduced the UAVs' flight time, and communication problems resulting from insufficient data transmission from the UAVs. We hypothesized that these issues were caused by mechanical vibrations affecting the components and wiring. As a result, we decided to switch to an integrated hardware solution (shown in Figure 3).

Figure 2. UAV with mounted hardware and the intruder UAV

The specification of the hardware are as follows: LoRa and WiFi packet capturing (3 devices): LILYGO TTGO T-Beam v1.1 ESP32 868 MHz, 0,96“ OLED screen, SSD 1306 driver, battery holder for Li-Ion 18650, MCU: ESP32, 8 MB PSRAM, 4 MB flash, LoRa: Semtech SX1276 14 dBm, NEO-6M (GPS) modul, WiFi/Bluetooth antenna 3D WiFi + IPEX. The transmission rate is 300 kb/s, and the radio signal strength sensitivity is up to -148 dBm.

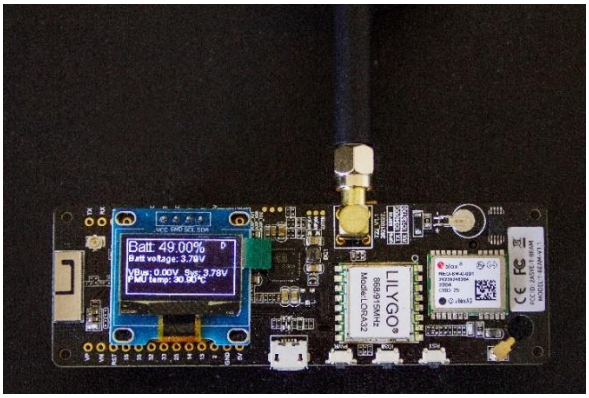

Figure 3. Hardware for intruder UAV operator detection and communication with home operator

In Figure 4 is presented a block diagram of the firmware used on each hardware mounted on UAVs. The firmware is developed that it captures all Wi-Fi packets on specific channel and every second it send the data with measured signal strength together with its present GPS coordinates to base station.

In Figure 5 is shown a block diagram of the firmware at the base station. The role of the base station is to collects data of all UAVs and to forward those data to server where all data are used to calculate the location of the intruder UAV operator. Our algorithm uses all collected data to determine with certain probability the location of the intrude UAV operator.

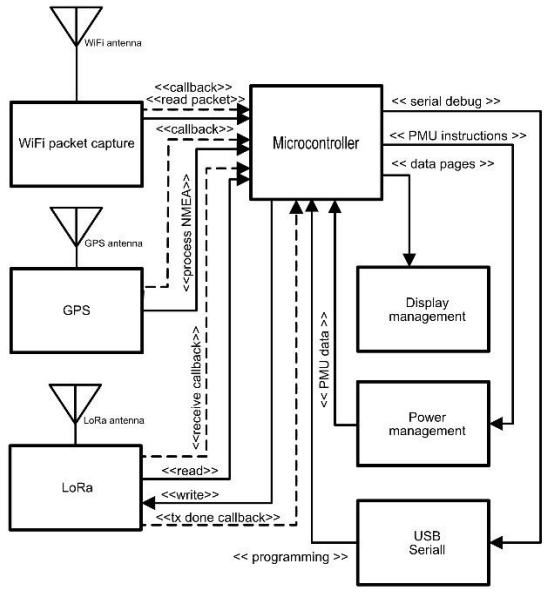

Figure 4. The block diagram of the firmware used on the hardware mounted on UAV

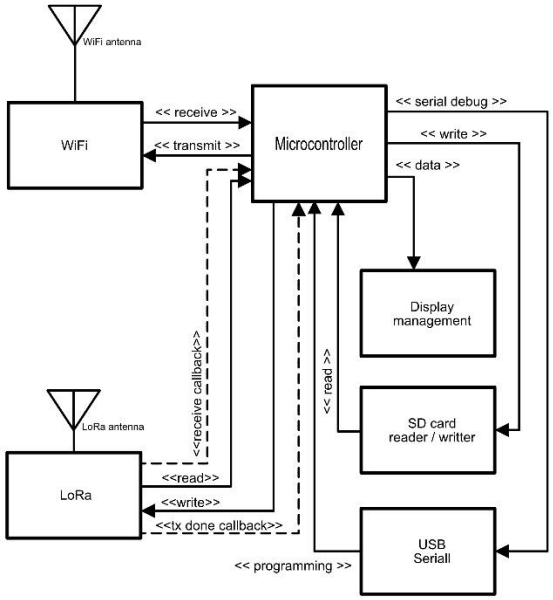

Figure 5. The block diagram of the firmware at the base station

We have divided our project into two phases. In the first phase, we focus exclusively on intruder UAVs that communicate using the standard 802.11 protocol. This phase is elaborated in this paper. In the second phase, we plan to employ machine learning techniques to identify the intruder UAV's signal pattern within the radio spectrum.

During the first phase, both the intruder UAV and its operator can be identified by their respective MAC addresses, which facilitates differentiation of their radio signals. Each of our UAVs can scan a different Wi-Fi channel to expedite the search for the intruder UAV's signal. Once this signal has been identified, all of our UAVs switch to listening on the same Wi-Fi channel and transmit their measurements to a central server.

One challenge we face is determining the optimal constellation of our UAVs to accelerate the search for the intruder UAV's radio signal. Once this signal has been detected and identified, another challenge arises in managing the constellation of our UAVs to move closer to the intruder UAV operator's location.

4 Experiment

The objective of this experiment was to evaluate the equipment and software depicted in Figures 3, in order to assess the viability of our methodology within a controlled environment with a known channel characteristic (center frequency of 2412MHz). The intruder UAV operator utilized an omnidirectional antenna with a constant output power of 20 dBm.

The intruder UAV operator actively controlled the intruder UAV from a fixed location, the GPS coordinates of which were determined at the onset of the experiment for subsequent distance calculations. The equipment and software were activated and gradually moved away from the intruder UAV operator in a linear formation.

The experiment was repeated multiple times, and the relationship between received signal strength and distance is illustrated in Figures 6, 7, and 8.

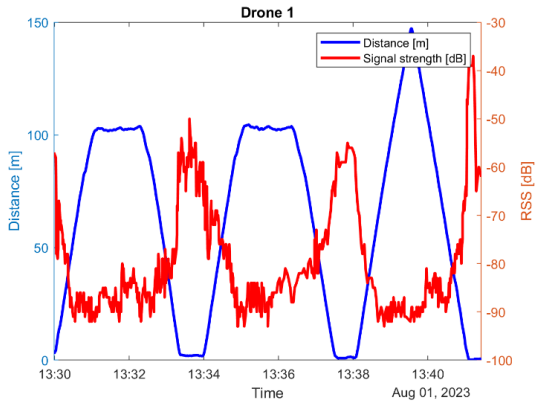

Figure 6. UAV 1 – signal strength/distance dependence

Data was collected at intervals of 1 s from all three UAVs and used to calculate the probability of the intruder UAV operator's location using the Friis transmission equation (Friis, 1946), with the frequency set to the midpoint of channel 1 (2412MHz) and the power component set to a constant value (20dBm) and disregarded due to multiple UAVs receiving the same signal.

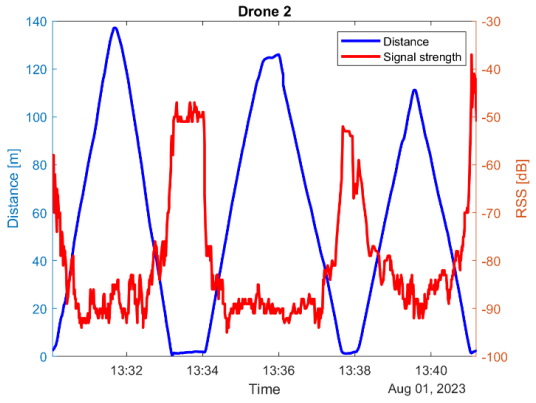

Figure 7. UAV 2 – signal strength/distance dependence

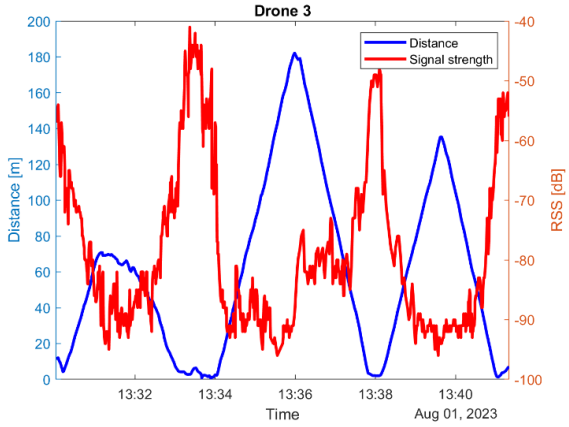

Figure 8. UAV 3 – signal strength/distance dependence

A tool and algorithm were developed to calculate the location of the intruder UAV operator, which computes the probability of location for selected points in space as depicted in Figure 9.

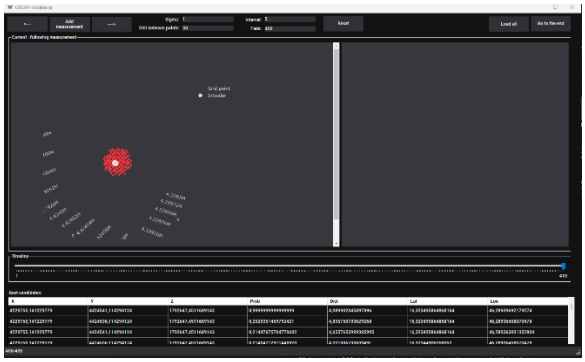

Figure 9. The tool for calculating the location of the intruder UAV operator.

The tool calculates the probability for all points within a defined region of space where the intruder UAV operator is expected to be located, as shown in Figure 10.

Probability for each is calculated based on location estimation using Friis transmission equation for every single measurement. Probability is multiplied from data originating for every UAV that is surveying airspace in real-time.

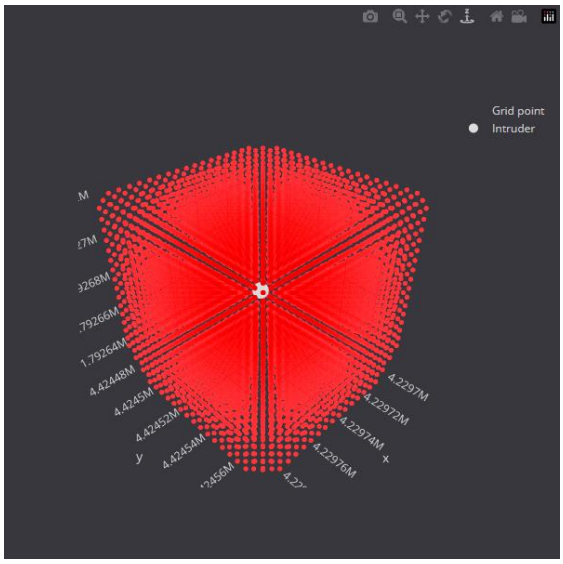

Figure 10. 3D space of localization points

Subsequently, a probability threshold was established so that only points with a probability above a certain value were displayed. Figure 9 displays points with a probability above 80% for the location of the intruder UAV operator. It should be noted that a white dot in the center of Figure 11 represents the actual location of the intruder UAV operator.

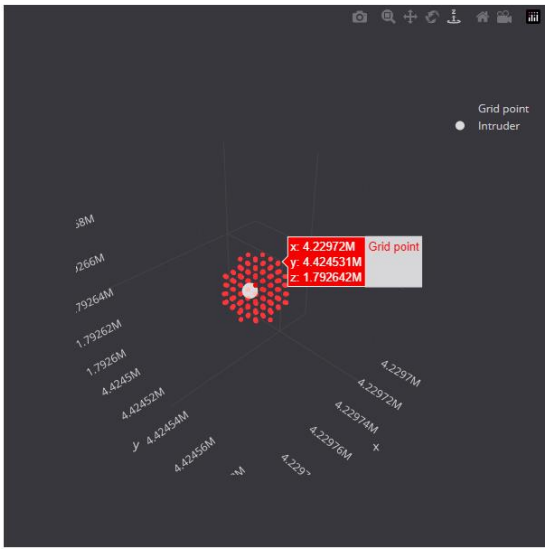

Figure 11. 3D visualization of the calculated probability of the location of the intruder UAV operator with threshold set 80%

Under ideal conditions, with measurements taken in open space with clear line-of-sight between our hardware and the radio signal source, our experiment achieved an accuracy within one meter for locating the intruder UAV operator, which is a highly satisfactory result.

5 Discussion

The utilization of multiple UAVs to locate the intruder UAV operator offers several advantages, including rapid target identification and tracking, as well as the flexibility to adapt to changing conditions within the area. However, this approach also presents several disadvantages, including limited flight time for the UAVs, the size and weight of the signal receiver, and processing power constrained by battery capacity. While more powerful receivers are available on the market, many are too large and heavy to be mounted on a small UAV.

The experiment demonstrated the feasibility of measuring distance using RF signal attenuation. However, challenges remain in terms of proper parameter setup and potential environmental influences on the radio signal. GPS error is another potential source of issues that will be addressed in future work. The effects of RF noise and GPS error may be mitigated by the open space of the experimental setup and multiple measurements that could theoretically minimize errors over time.

Similar to RF noise, different shapes and antenna power outputs could be mitigated by multiple measurements from various locations. Indeed, radiation patterns could be shaped like triangled torus, system could be capable of localizing the sources.

It should be noted that in real-world scenarios, signals may be partially obstructed by buildings, trees, and other obstacles. This introduces imprecision into the relationship between actual distance and that calculated using the Friis transmission equation. Even multipath scenarios might not pose significant challenge to constellation of rapidly moving aerial signal scanners as depicted in this research. Future work will focus on investigating such use cases and enhancing the algorithm capable of compensating for signal obstruction and multipaths.

There is also a clear limitation in terms of the maximum distance between the receiver and signal source imposed by the hardware used, which is approximately 250 meters. Additionally, in the initial phase of our project, only UAVs utilizing pure Wi-Fi protocol can be detected.

6 Conclusion

This paper presents the results of an infield initial experiment in which specialized hardware was utilized to measure the signal strength of an intruder UAV operator, with the aim of assessing the feasibility of using these measurements to determine their precise location. The results of the experiment demonstrate that the hardware mounted on the UAVs functioned as intended, exhibiting sufficient reception and processing capabilities to detect, identify, and track the radio signal emitted by the intruder UAV operator.

Future work on this project will focus on several key areas: i) real-time calculation of the intruder UAV operator's location; ii) investigation of the impact of environmental factors and GPS errors; iii) evaluation and benchmarking of the system against various radiation patterns emitted by intruder UAV controllers; and iv) determination of the optimal constellation and flight path of UAVs for efficient localization of the intruder UAV operator.

Acknowledgments

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

References

Kokić P., Tomaš B. (2017) Enhanced drone swarm localization using GPS and trilateration based on RF propagation model. *Central European Conference on Information and Intelligent Systems.* Varaždin, 2017. pp. 259-264

Tomaš B. (2013) Wifi roaming access point optimum assignment in urban multi-sensor. *Research papers Faculty of Materials Science and Technology Slovak University of Technology in Trnava*, pp 109-115

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

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

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

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

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