Swarm of Networked Drones for Video Detection of Intrusions

Mustapha Bekhti[1(✉)], Nadjib Achir[1], and Khaled Boussetta[1,2]

[1] Université Paris 13, Sorbonne Paris Cité – L2TI (EA 4303), Villetaneuse, France
{bekhti.mustapha,nadjib.achir,khaled.boussetta}@univ-paris13.fr
[2] Inria URBANET, INSA Lyon, 69621 Villeurbanne, France

Abstract. Border control, sensitive area monitoring and intrusion detection are surveillance problems of practical import that are well suited to wireless sensor networks. In this paper, we study the application of a swarm of Unmanned Aerial Vehicles to an intrusion detection and tracking problem. We introduce the Boids scheme to maintain the drones team formation in order to deal with coverage issue and collision problem. A contribution of our work is that we do not assume a ground centralized control of the drones; on the contrary, the swarm is considered as a set of autonomous and self organized entities.

Keywords: UAV · Swarm · Intrusion · Detection · SINR · Coverage

1 Introduction

Unmanned aerial vehicles, shortly named UAVs are defined as autonomous entities with no pilot on board. They are a part of a global system called Unmanned System which also includes elements such as a control station, relays etc.

Due to them flexibility and mobility, these flying machines become the ideal tool for carrying out technical inspections of constructions, buildings, industrial sites, highway structures in a fast but also at low-cost way. Capable of going in places difficult of access or simply wide area, the drone allows a simplified but a precise technical inspection. With the aerial shots taken by a drone, it is possible to obtain a precise image of the building and thus allows to localize and to diagnose the defects of constructions. In another hand, borders and sensitive area control and monitoring is a key issue that every state is considering carefully, whether for security or economic reasons. The main challenge is to control borders and areas outside regulated zone crossings, which are always considered as open doors for intrusion. Thus, in order to improve the time and the quality of the response, the UAV could allow a rapid assessment of the situation but also to contribute to the processing of the operational information concerning the threats.

Basically, these flying machines are designed to fulfill the requirements of assigned missions individually or among a set of drones, called swarm. Since complex mission cannot be accomplished with a single entity, the use of a set

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 221–231, 2018.
https://doi.org/10.1007/978-3-319-90802-1_19

of drones is required. Thus, the drones forming the swarm have to cooperate in order to achieve the global mission and to avoid collision with each others. Thus, the main objective of flight in formation is to make a link between the decisional and functional level, in other words, to produce a configuration of formation based on the constraints of the mission. However, such cooperation requires robust communications and a good strategy to avoid obstacles and collision between the drones as well.

Different control strategies have been presented in robotics to control the movement of entities among a swarm, such the ones based on the potential field presented by [2,5,6]. Other visual methods have been developed for mobile robots on the ground, but it is difficult to transpose them to the three-dimensional environment of drones with a much faster dynamics [4].

However, simple target tracking is not sufficient to ensure the stability of the swarm. This requires closing the loop by slaving the drones one against the others. Thus, three behaviors are sought, namely intruder localizing, collision avoidance and configuration compliance. The effectiveness of this control depends on the possibility at which the position of the drones can be obtained.

When flying at high speed in formation with small spacing, the safety of the flight becomes difficult to guarantee, especially in events related to communication systems failures. In fact, communications are the major problems of unmanned aircraft. In order to ensure the safety of the flight, the data must be exchanged continuously between drones themselves and the ground control station, thus excluding the radio silence is more than necessity [1].

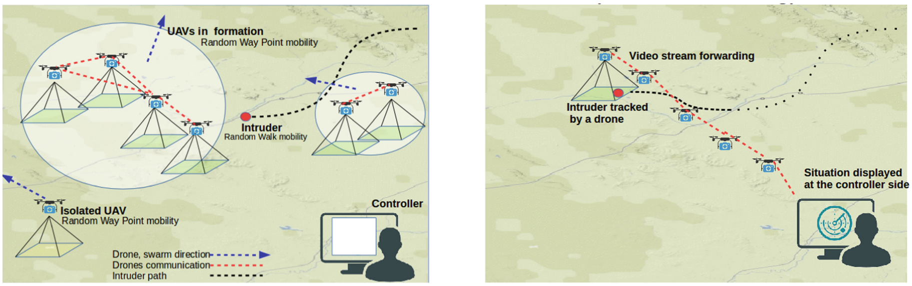
Our current research is mainly motivated by emerging applications such as border surveillance, reconnaissance, environmental monitoring and search-and-rescue tasks in areas without a permanent communication infrastructure. In this paper, we present a deployment strategy of a fleet of quad-copters for area monitoring, intrusion detection and video stream reporting. It is evident that the drones should not collide and keep a safety distance from each other during the mission. Thus, our solution is based essentially on the well known model proposed by [7] where the movement of the swarm is inspired from the motion of a flock of birds.

This choice is motivated by the simplicity and robustness of the method. Moreover, it does not increase the use of bandwidth for communications, considering that drones must only exchange their positions to maintain the swarm formation, to cover a large area and to avoid collision as well.

2 Scenario

We address the problem of mobile target localizing and tracking by the use of a fleet of drones. Our goal is to determine the intruder position, to keep the fleet in a certain formation in order to avoid collision between drones and to forward video situation to the controller side. To this end, a behavioral approach based on the quality of signal between drones of the same swarm is proposed. In addition, we deal with one of the assumption commonly made about wireless networks that says that the signal strength is just a simple function of distance, which is not always the case.

The following scenario provides the motivation of this work. We consider a sensitive area to monitor. A set of ground detectors is deployed at the border of the area. In the case of intrusion, the ground sensors send an alarm to the security forces in charge of the area surveillance. The security forces need to localize the intruder and to get a real time video of the situation for a better threat evaluation. To this end, the security forces resort to the use of a set of small scale drones equipped with cameras and wireless communications devices. The Figs. 1a and b give an overview of the scenario and illustrate the drone's behavior during the different phases of the mission.



(a) UAVs fleet for intruder localizing

(b) UAVs fleet for video stream reporting

Fig. 1. Intruder search and report scenario

3 Problem Formulation

3.1 Problem Statement and System Description

As mentioned earlier, we are dealing with a sensitive area surveillance. The main objective of this paper is to localize the intruder and to report the situation to the security forces in the shortest possible time in order to evaluate the threat and to deploy the adequate forces. Basically, this mission is given to a set of autonomous small scale drones, denoted by $D = \{D_1, D_2, \ldots, D_n\}$. Each drone D_i is equipped with a camera and wireless devices to communicate with the other drones and the base station BS situated at the controller side. We assume that all the communication devices have the same characteristics and have a short sensing range compared to the size of the region of interest. In addition all the cameras have the same field of view that we denote by FoV. We also consider that the drones have a limited flight autonomy Υ. Finally, we assume that the intruder is localized once it is within the FoV of any drone D_i.

In this frame, the system is modeled as 2D area A without any obstacle since the drones are flying at the same altitude h. The projection of the flying area is represented by a rectangular with length of x_{max} and a width of y_{max}.

Our goal is to present a solution that minimize the search localization, optimize the number of the used drones for a given mission. Moreover, during the mission, and in no cases, the drones must not collide with each other. Furthermore, and in order to cover a large area, drones shall flight in formation and maintain the maximum distance possible between the rest of drones of the same swarm. For this purpose, we assume that after each period P drone generates a message of size D bits containing its identification, its position and speed. The on-board wireless interface tries to send each generated message to the other UAVs. For some reasons, a message can be corrupted or lost due to possible interference and collisions. The opportunity to transmit also depends on the radio coverage, the capacity of the related wireless technology and the drone's location.

The following is how the mobile target search problem is resolved. A swarm of mini drones with autonomous behaviors is capable of performing low cost and distributed sensing functions such as the one described in the preceding scenario. A first drone is sent to the direction where the attacker was initially reported by the ground detectors that are deployed at the border of the area. After a period time p, and if the situation is not received at the controller side, another drone takes off and moves towards a random position looking for the intruder. This step is repeated after each period p, until the intruder is localized or the maximum number of the drones is reached. In the case where the drone identification and position message D is received by one or different drones, the sender and the receivers drones create a new swarm. The cohesion of this swarm is a function of the signal quality of the wireless network created by the swarm drones. Thus, the drones forming a swarm maintain the largest distance between them in order to cover a large area. In this case, a low signal strength could guarantee the position messages exchange in the network. Whereas, a high data rate is needed to report the video situation to the controller. However, a good quality of signal should be assured when the drones are being closer enough.

In addition, if a drone D_i consumes a 70% of its energy it goes back to the start position. Moreover, if a drone identifies the intruder based on its camera, it reports and notifies the nearby UAVs of its location. The UAVS alter their flight paths and align themselves between the intruder position and the BS at the controller side. As the intruder moves, the drones update them positions to keep the target in sight. Through coordination, the UAVs should be able to complete tasks that each could not have done alone. With these new capabilities, UAVs can plan missions collaboratively and can re-plan adaptively based on real-time changes in UAV availability, camera FoV and target movement. The flow chart in Fig. 4 depicts clearly the different steps of our algorithms, namely, localization, swarming and collision avoidance, and video reporting.

3.2 Problem Formulation

We have n autonomous drones flying at the same altitude h at an instant t. For simplicity we denote the position of a single drone D_i at time step t by the coordinate $(x_{i,t}, y_{i,t})$. The movement of a drone D_i is discretized in space and time allowing the drone to make its own decision to move to adjacent position or to hover at the same position via the information gained from the nearby drones.

Our main objective is to minimize the search time of the intruder:

$$\text{minimize} \sum_{i=1}^{N} t_i x_i \tag{1}$$

subject to:

$$\sum_{i=1}^{N} x_i = 1 \tag{2}$$

where N is the number of UAVs, t is an estimate of the time needed by the drone D_i to intercept the target, and x is an assignment variable that is equal to 1 if the intruder is within the D_i FoV, and zero otherwise.

As we assumed that the drones are flying at a constant altitude h, they therefore have a collision avoidance constraint which can be quantified as

$$(x_{n+1,t}, y_{n+1,t}) - (x_{n,t}, y_{n,t}) > A, n = 1, \ldots, N-1. \tag{3}$$

where A is the minimum safety separation between two drones.

In addition, when performing area coverage for intruder detection and for video stream reporting, it is important to define the range boundary of the drones swarm based on signal-to-noise (SNR) ratio, which is the signal level (in dBm) minus the noise level (in dBm). For example, to maintain the UAV swarm in formation, drones need to know the other nearby drones position, a small SNR and low data rate are enough to guarantee a reliable data exchange. However, a healthy value for wireless network is more than necessary for video streaming.

$$SNR_{n,n+1} < \delta, n = 1, \ldots, N-1. \tag{4}$$

3.3 Communications

Assuming a transmission power P_t for the UAV, the received power P_r is easily calculated using an appropriate propagation model depending on the distance d between UAVs. As we consider an open field area, and UAV to UAV communications, the appropriate model could be the free space model.

$$P_r = Att(d).P_t \tag{5}$$

In the ideal case and in its simplest form, the Friis equation is expressed as the ratio of power available at the input of the receiving antenna P_r, to the output power of the transmitting antenna P_t:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \tag{6}$$

where G_t is the antenna gains of the transmitting antenna, G_r is the antenna gains of the receiving antenna, λ is the wavelength, and R is the distance between the transmitter and the receiver antennas.

Once P_r is determined, the signal-to-noise ratio SNR is computed using the noise/interference power value. In this case, the SNR is equal to:

$$SNR = 10.log\left(\frac{P_r}{P_{Noise} + P_{Interf}}\right) \tag{7}$$

The SNR is an indicator of the quality of transmission of the data. It impacts in a direct manner on the performance of the network. Thus, a lower SNR decreases the throughput and lead the network to operate at a lower data rate with a low throughput. However, a higher SNR value allows a higher data rate, a better throughput and fewer retransmissions [3,8].

The use of a particular SNR value as a requirement for signal coverage, collision avoidance between drones but for keeping the warm in a formation is certainly a difficult choice, and the rule of thumb given in this paper is to test the algorithm with a set of SNR range values.

3.4 Swarm Formation

The basic flocking model presented by [7] consists of three simple steering behaviors. Each behavior is based on the position and the velocity of the nearby agents.

- Cohesion (R1): steer to move toward the average position of local flockmates. The center of the swarm is simply the average position of all the drones. We assume we have N drones in one swarm, then the center c of all N drones is given by:

  $$\text{c} = (D_1.\text{position} + D2.\text{position} + \ldots + D_N.\text{position})/\text{N}$$

  The positions here are vectors, and N is a scalar.

  However, the center of swarm is a property of the entire flock; it is not something that would be considered by each drones. Thus, each individual drone moves toward its perceived center, which is the center of all the other drones, not including itself. Thus, for D_i (1 <= i <= N), the perceived center D_ipc is given by:

$$\begin{aligned} D_ipc = (D_1.position + D_2.position + \ldots \\ +D_{i-1}.position + D_{i+1}.position + \ldots \\ +D_N.position)/(N-1) \end{aligned} \tag{8}$$

- Separation (R2): steer to avoid crowding local flockmates
- Alignment (R3): steer towards the average heading of local flockmates

Algorithm 1. Separation

```
Input:
    V                                                        ▷ vector
    D_i                                                      ▷ Drone
    SNR_{i,j}                                                ▷ SNR
function SEPARATION(D_i , SNR_{i,j})
    Vector vector = 0
    for each drone D_j ∈ swarm do
        if thenD_i != D_j
            if SNR_{i,j} > δ then
                vector ← vector − (D_i.position − D_j.position)
            end if
        end if
    end for
    return vector
end function
```

Algorithm 2. Alignment

```
Input:
    V                                                        ▷ vector
    D_i                                                      ▷ Drone
function ALIGNMENT(D_i , SNR_{i,j})
    Vector vector_i = 0
    for each drone D_j ∈ swarm do
        if thenD_i != D_j
            vector_i ← vector_i + D_j.velocity
        end if
    end for
    vector_i ← vector_i/N − 1
    return vector − D_i.velocity
end function
```

3.5 Pattern Formation

The formation pattern is one of the most important coordination issue in swarm formation. The geometric pattern to be formed is a set of points in the plane, represented by the drones cartesian coordinates after messages exchange and computation process. For drones, the suited formation can be one of the following pattern:

- arbitrary pattern where all shapes are allowed.
- circle pattern, in this case drone place themselves on the plane to form a circle.
- line pattern: the drones are required to place themselves on a line.
- V pattern: inspired from V-shaped flight formation of migratory birds.

At the end of the coordination and computation, each drone has to broadcast its new localization to the other drones in the same swarm.

4 Results

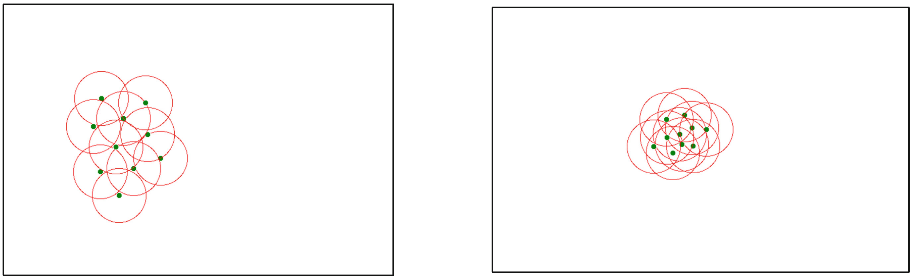
In this section we evaluate our proposed algorithm. Two main objectives were fixed, first, to minimize the intruder localization by the use of less number of drones, while the second one was avoid collision between these drones.

Thus, we assess the algorithm in different scenarios. Using Omnet simulator we generate two traces of the intruder trajectory. Since intruders follows unpredictable path and in order to make it more realistic, we opt for Random Way Point (RWP) mobility model. In addition, as we didn't discretize the area of interest, a drone can move freely to the all adjacent positions. Here again a drone follows a RWP mobility model on its way of intruder localization. Thus, once a set of drones form a swarm, the swarm follows a mobility model resulted of different behaviors, namely separation, cohesion, alignment and the RWP mobility model as well. The Table 1 summarizes the predefined variables.

Table 1. Simulation parameters

Designation	Value
Area	X = Y = 1000 m
Number of drones	1..N
UAV altitude	20 m
D	200 bytes
P_t	20 dBm (100 mW)
Path loss type	Free space
Pnoise + Pinterf	−60 dBm (Constant)
Antennas gains	Ge = Gr = 10 dBi
Carrier frequency	2.4 GHz
Drone' packet sending interval	1 s
Intruder mobility model	RWP
Single drone mobility model	RWP
Swarm mobility model	Cohesion, separation, alignment and RWP

The result of the Fig. 2 shows the influence of the SNR parameter on the swarm connectivity and the area size covered by the swarm. As illustrated in Fig. 2a, a low SNR value allows to cover a larger area and therefore, the drones of the same swarm maintain the maximum distance possible. In the same logic, a higher SNR result a small size area covered by the swarm, since the distances that separate the drones is small. In addition, the Fig. 3a illustrates two separate swarms and having two different bearing. In fact, our algorithm can generate more than one swarm at the same time t. When communication between two different swarms is possible, these latter constitute a single one swarm as depicted

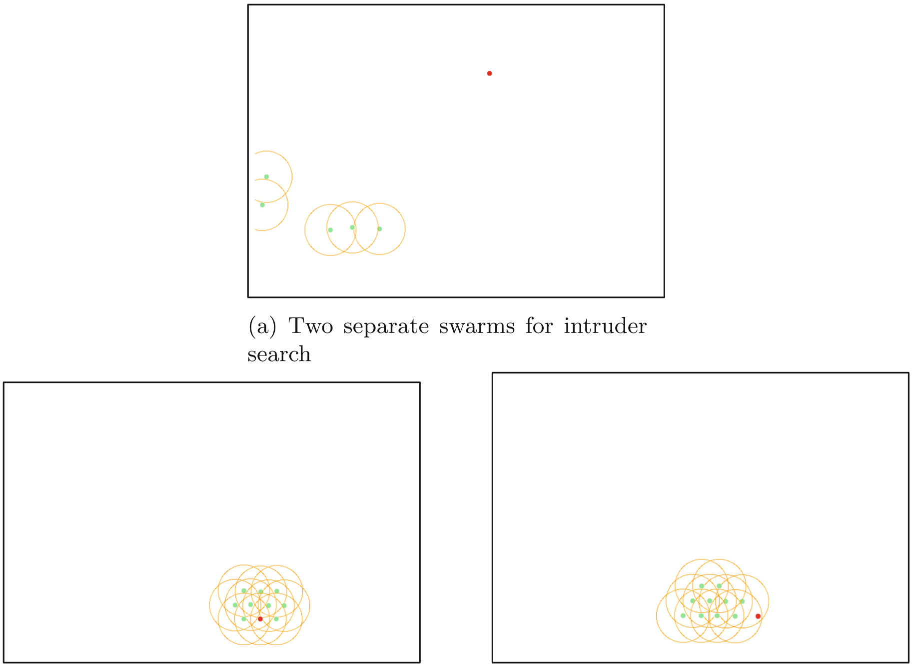


(a) SNR Separation parameter = 10dBm

(b) SNR Separation parameter = 16dBm

Fig. 2. UAVs swarm formation with different SNR separation parameters

in Figs. 2, 3b and c. The intruder localization is illustrated by Fig. 3b and c. Indeed, when an intruder is within one drone camera field of view, the swarm change its topology and the drones become closer to each other in order to ensure a high data rate for video forwarding to the controller side.



(a) Two separate swarms for intruder search

(b) Intruder localized by the swarm

(c) UAVs fleet for video stream reporting

Fig. 3. Intruder search and report scenario

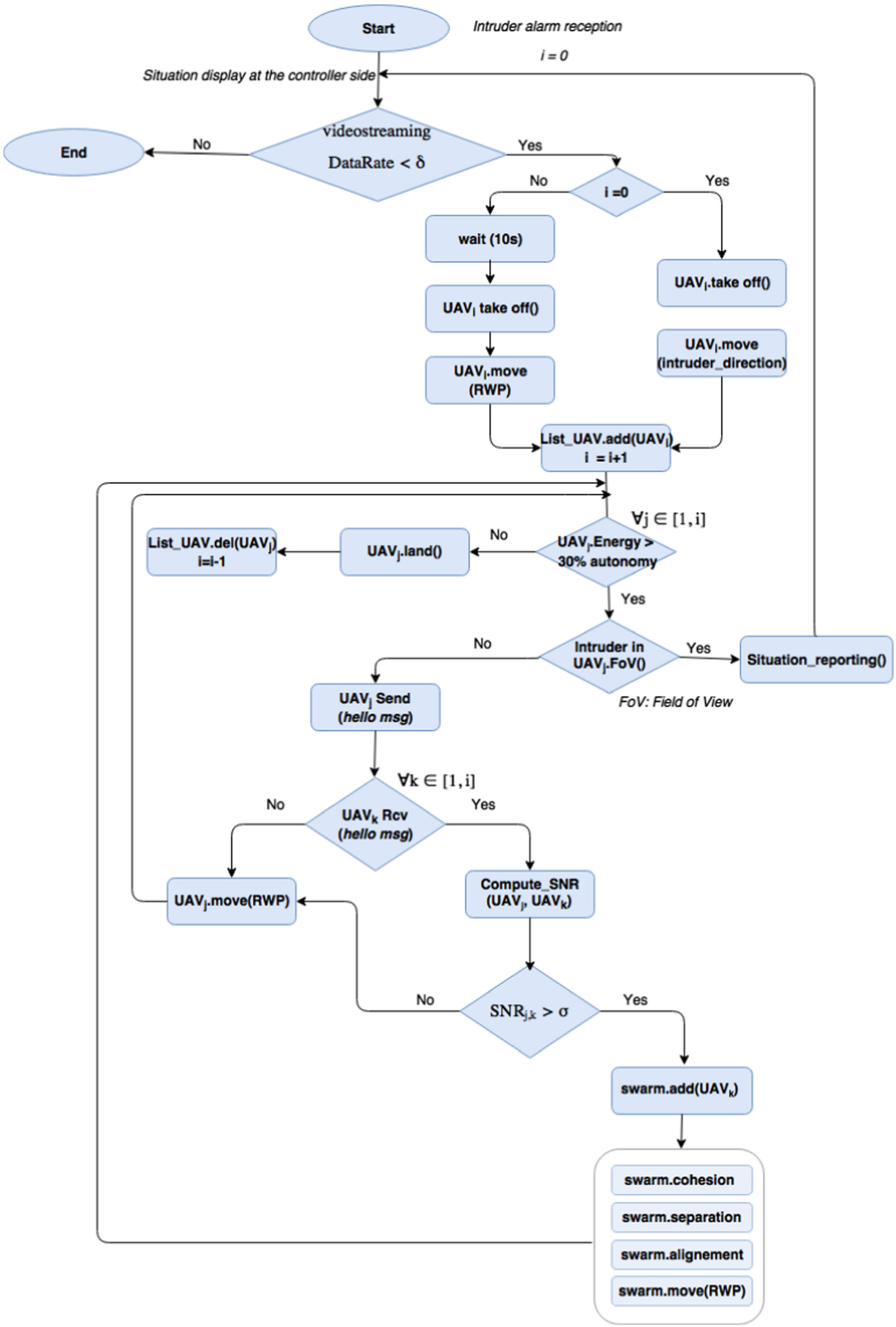


Fig. 4. UAVs swarm intruder tracking and video stream reporting flow chart

5 Conclusion

We propose a comprehensive solution for borders and sensitive areas control and monitoring through the use and the exploitation of the communications and imaging capabilities of a team of drones. The proposal should improve the response time between intruder detection and interception, and thus allows to better compare the nature and level of the threat, and consequently yield to optimize the deployment of resources and enhance their values. We showed the flocking scheme based on the quality of the received signal between drones of the same swarm enable to avoid collision end to cover a large area.

Nevertheless other methods deserve to be explored for faster execution, in particular the potential field, only the solution mentioned above has been tested. In addition, the video stream reporting needs to be evaluated, either by simulation or with experiments to assess the influence of multi hops video forwarding on the quality of the situation displayed at the controller side and the. This is left for future work.

References

1. Bekhti, M., Abdennebi, M., Achir, N., Boussetta, K.: Path planning of unmanned aerial vehicles with terrestrial wireless network tracking. In: Wireless Days (WD), pp. 1–6. IEEE (2016)
2. Gazi, V., Passino, K.M.: Stability analysis of swarms. IEEE Trans. Autom. Control **48**(4), 692–697 (2003)
3. Geier, J.: How to: Define Minimum SNR Values for Signal Coverage (2008). http://www.wi-fiplanet.com/tutorials/article.php/3743986
4. Hattenberger, G.: Vol en formation sans formation: contrôle et planification pour le vol en formation des avions sans pilote. Ph.D. thesis, Université Paul Sabatier-Toulouse III (2008)
5. Khatib, O.: Real-time obstacle avoidance for manipulators and mobile robots. In: Cox, I.J., Wilfong, G.T. (eds.) Autonomous Robot Vehicles, pp. 396–404. Springer, New York (1986). https://doi.org/10.1007/978-1-4613-8997-2_29
6. Leonard, N.E., Fiorelli, E.: Virtual leaders, artificial potentials and coordinated control of groups. In: Proceedings of the 40th IEEE Conference on Decision and Control, vol. 3, pp. 2968–2973. IEEE (2001)
7. Reynolds, C.W.: Flocks, herds and schools: a distributed behavioral model. ACM SIGGRAPH Comput. Graph. **21**(4), 25–34 (1987)
8. Techaccess. Pre-installation Wi-Fi Site Survey Report. https://www.techaccess.be/wp-content/uploads/2013/10/Pre-Installation-WLAN-Site-Survey-Report-VOORBEELD-BE.pdf