Potential Threats of UAS Swarms and the Countermeasure's Need

Laurent Beaudoin, Antoine Gademer, Loïca Avanthey, Vincent Germain, Vincent Vittori

▶ **To cite this version:**

Laurent Beaudoin, Antoine Gademer, Loïca Avanthey, Vincent Germain, Vincent Vittori. Potential Threats of UAS Swarms and the Countermeasure's Need. European Conference on Information Warfare and Security (ECIW), 2011, Tallinn, Estonia. hal-01132236

HAL Id: hal-01132236
https://hal.science/hal-01132236

Submitted on 17 Mar 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Potential Threats of UAS Swarms and the Countermeasure's Need

Laurent Beaudoin, Antoine Gademer, Loica Avanthey, Vincent Germain and Vincent Vittori
ESIEA, ATIS Dept., Paris, France
beaudoin@esiea.fr
gademer@esiea.fr

Abstract: The rising capabilities and growing accessibility of recent Unmanned Aerial Systems (UAS) widen the risks of success of a terrorists attack through the current aerial defence systems. We will examine first the complexity of the threats from a single unmanned vehicle, to a team of unmanned vehicles and finally to a swarm of unmanned vehicles (and any other association of these three combinations). Then, from an operational point of view, we will see that early detection of danger - a critical stage in the development of counter-attacks - has become very difficult because small unmanned vehicles like UASs precisely possess the ability to take off directly within the sphere of attack. The next stage, equally critical, consists in elaborating the response that best fits the attack. We distinguish three general categories of active and passive countermeasures: destruction, incapacitation and jamming of the enemy UASs. We will then study several possible countermeasures appropriate to the type of attack (enemy's formation: isolated drone, team, swarm; weapon type: bomb, kamikaze, bacteriological etc.). We first present countermeasures that are rather conventional (they usually come from air defense systems) and others specific to the UAS case. We will finish by a case study in which we will tackle the use of simplified physical models for calculating positions in real time in an optimized way in a UAS swarm under constraints.

Keywords: unmanned aerial system, swarms, countermeasure, terrorism

1. Introduction

We previously presented the risks presented by the use of single micro-UAS by terrorist groups given the current flaws in the aerial defence systems (Beaudoin & Gademer, 2010). This scenario is nowadays more than conceivable considering the rising capabilities of recent UASs and their growing accessibility. This perspective thus opens new breaches, even more dangerous than the previous ones, and renders obsolete most of the existing solutions.

This article deals with the potential threats related to the use of micro UASs, which weigh less than 5 kilograms, for terrorist purposes in two ways: the increasing level of automation of these systems and their new capacity for collaboration. In a second step, we will discuss the current counter measures to prevent or fight such situations. Then we will widen the debate with a case study that includes the prospects offered by collaborative systems in terms of counter-measures.

2. Technological abilities for new threats

2.1 Unmanned Vehicle Systems (UVSs) and level of automation

Automated unmanned vehicles are robots of different sizes (Abatti et al., 2005), carrying no human on board, but designed to fulfil various types of missions known as the three "Ds" (Dull, Dirty or Dangerous). They can be remotely controlled or follow a predetermined plan or react to their environment, or even use a combination of the three previous situations. In the literature (Christ, 2007, Singer, 2009), robots are often spoken about, and you can find a lot of autonomy scales. But more than the autonomy (which is a bit anthropomorphic) we prefer to define an automation scale.

We will distinguish several levels of automation:

- Level 1: Slave (assisted piloting, disturbance compensation)
- Level 2: Automated (maintains its orders and takes high level orders)
- Level 3: Automatic Navigation (a priori mission plan)
- Level 4: Response from contextual data (dodging) without human intervention
- Level 5: Decision-maker (expert system) from contextual data (navigation in unknown environment, realization of complex missions, coordination)

Levels 1 and 2 require the intervention of a pilot during the mission and therefore a continuous communication link between himself and the UVS during the attack.

At level 3, the system is independent of the pilot and knows how to place itself in its environment. For this, it relies on passive sensors (AHRS, GPS, clock…) and blindly follows the mission plan that has been given to it beforehand. This involves a detailed knowledge of the place in which the mission will take place to make sure everything goes smoothly.

At level 4, the system has a minimum knowledge of its surrounding environment and can react to events such as performing collision avoidance. To do this it uses a number of active sensors (distance measurement, short range communications, etc.), but the establishment of an accurate mission plan beforehand remains a fundamental element.

Level 5 introduces concepts of artificial intelligence and decision-making that require significant computing power. To take full advantage of these new features, many perceptive sensors are usually added, as well as a large storage capacity that allows the robot to make inferences from the state of its environment, both in space and time. These robots are able to realize complex missions in unexplored environments, to interact with them in a meaningful way, or to reschedule an ongoing mission because of encountered events.

The higher the level of automation is, the more the human cost and risk is minimized from the point of view of the attacker and the greater the probability of an unexpected attack increases (because fewer staff are involved upstream and on field). The impact on the financial cost is more complex to measure, because it is much more influenced by the material cost of the device (due to the payload and the number of sensors) than by the embedded intelligence (software part). In what follows, we will apply the previous scale to micro-UASs. Given the current technological breakthroughs available at a lower cost, micro UASs represent new threats. Moreover, the multiplication of supply depots all over the world makes it impossible to survey or to detect suspicious individuals or groups. If you look at what exists today on the market for micro-UASs (less than 5 kg category) and given what we just described, we can distinguish three cases:

- Levels 1 and 2 which are relatively common, with reasonable prices. We find material for flying model aircraft (<500 €) or the first micro-UAS (<1 000 €) as the AR. Drone Parrot, Quad Flyer GAUI or first models from Mikrokopter.
- Level 3 is the standard micro-UAS premium (~ 10 000 €) as the models from Draganfly Innovations Inc.., Microdrone Gmbh or Fly-n-Sense. Note that the models from Mikrokopter offer this capability for less than 2 000€, but need to be assembled by an engineer.
- Levels 4 and 5 are for now confined to laboratories (Valenti et al. 2007, 2007b).

2.2 Unmanned Aerial Systems (UASs) and level of collaboration

After having established the automation scale of UAS, let's talk now about the collaboration scale of UAS among themselves. We will examine the definitions by increasing complexity from the isolated individual, a group of individuals, a team and to finish, a swarm. Through these concepts (see figure 1), we will take the opportunity to note the strengths and weaknesses of these different formations.

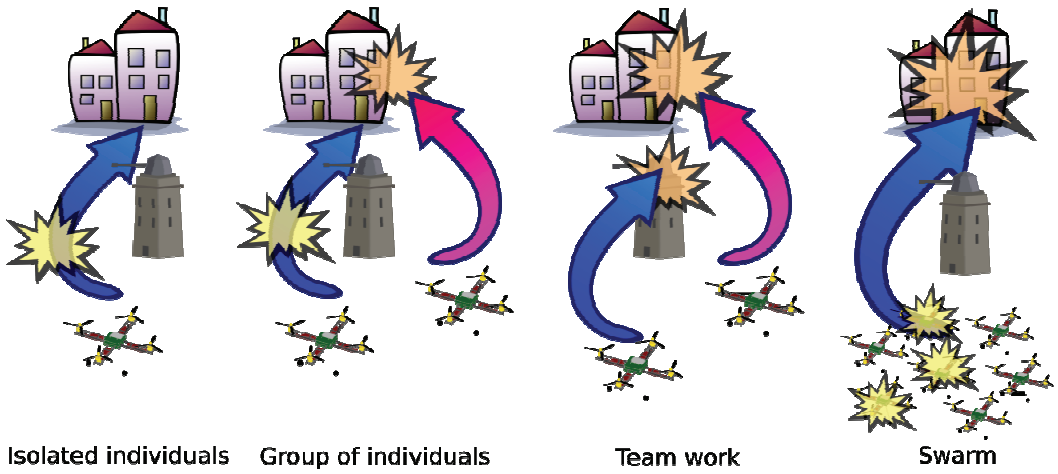

Figure 1: Different levels of collaboration in operation

Isolated individuals

The most basic case is about the isolated individual (Beaudoin & Gademer, 2010). The UAS can be piloted or autonomous and has a specific mission to perform. Small in size, easy to assemble, affordable to fly, some models can even embed a light payload. They have all the assets to be used for terrorists operations in the close future. However, if the pilot or the UAS is stopped, disabled or destroyed, the threat is removed.

A group of individuals

A group of UASs is composed of several isolated individuals, each with their own mission without coordination. Their sphere of action does not necessarily lie on the same location and each unit can be considered as the case described in the previous paragraph. But by increasing the number of individuals, we multiply the probability of a successful attack by trying to saturate the defense's capabilities. The main advantage of the group is that it does not need any collaboration among the individuals and thus does not need advanced collaborative capacity.

Team of UASs

A team of UASs can be seen as a group in which all members are assigned specialized tasks and are usually coordinated by a chief. Team formation is particularly effective: the objectives are divided and each member can focus on achieving its task. With UASs on the third level (automatic navigation) of the automation scale, you will have synchronized action but no possibility to update the mission plan according to what happens on the field. The fourth level (without human intervention) will give you reaction to the surroundings but may lead to a fatal loss of synchronization between the team members, which quickly leads to using UASs of the fifth level. At this step, all members are communicating with each other and the leader chooses what to do next. So the action is fast and has things in common with a commando operation.

The missions that a team can perform could be far more complex than the one in the previous case.
The team strength is also its weakness: the more each member is highly specialized, the more the destruction of a key element can jeopardize the whole mission (coordinator UAS, UAS with the lethal load, UAS dedicated to the collection of information...). Survival of team-members is therefore critical and fundamental to the proper performing of the mission.

The enemy can also try to predict the behaviour of a team, in a certain way, because it usually works following a logical reasoning, and so it is possible for him to act accordingly.

Swarm of UASs

A swarm, unlike a team, is made of a uniform mass of undifferentiated individuals (Clough, 2002). The robots forming a swarm are at least of the fourth level on the automation scale. The swarm has no "chief" or "organization". Its efficiency is based on the emergent behaviors related to the large number of individuals and their interactions, that's why they cannot be controlled and need to be automated. The intelligence is decentralized (Frantz, 2005): each individual interacts with others on the same basis of simple rules describing the reactions of individuals to their local environment (like a shoal of fish).

This decentralization, combined with the large number of individuals, allows the swarm to be a highly resistant form (Chaumette et al., 2010). If some individuals disappear, it will have little influence on the conduct of the mission. The resulting action is certainly less efficient, but the mission can still succeed. Similarly, the swarm is resistant to local disturbances or to the addition of new individuals into the system, the overall behaviour is the only one taken into account.

However, the behaviour of the swarm is only based on individuals' reactions. So it is not deterministic (Lamont, 2007, 2008). Then, we can only estimate a probability of success, even in a favourable situation, which is far removed from the optimum way of the team work. The main strength of a swarm, its distributed intelligence and its lack of hierarchical bonds, is also its main weakness, which is its lack of strategic global view.

Finally, the apparence of the swarm itself can fulfil another objective in psychological warfare. Indeed, it can inspire both fear and powerlessness into the collective unconscious as for example in “The Birds” of Hitchcock, or like the killer bees from South America, the ants in Indiana Jones, or grasshopper clouds.

3. The vulnerability of existing defense systems and counter measures

3.1 Vulnerability of present defense systems and attacks by micro-UASs

In practice, defense systems in simplified can be viewed as the achievement of two critical phases: detection and identification of the danger and counteraction through appropriate response while restricting collateral damage.

The traditional tools of detection used by air defence systems can be categorized into two families:

- Active radar surveillance: they generate waves and use the rebound of the echoes on potential flying objects to locate them. From there, it is possible to estimate their distance, their speed of approach, the penetration vector, and even have an idea about their trajectory (at least in the short term) and their size.
- Monitoring by passive observation of the electromagnetic spectrum, either in the visible or thermal infrared or by listening to the radio waves on the common communication channels.

In practice, the data fusion of multiple sensors allows to reduce noise and false alarms to the maximum while maintaining reliability. Except unusual cases, the bigger the device is, the easier it is to notice. Usually the defence systems are optimized to detect aircraft or missiles. They both move at a rather high altitude and reach substantial speeds during the approach stage of the target.

The main problem posed by micro-UASs is that the approach stage can be practically non-existent, because their small size allows them to be launched into action very close by the target (Carnu, 2010 ; Miasnikov, 2005; Gademer, 2009, 2010, 2010a) . This cancels the long range defensive strategies and raises the problem of reactivity from the decision line. Reactivity that has to be all the quicker as we are near the target. Their slow flight at a very low altitude is an aggravating factor that increases the probability of non-detection. Moreover, their electric motors do not leave a thermal signature, which makes their detection extremely difficult.

Finally, the topography of the theatre of war can also be an additional factor of complexity, as in the case of an urban environment. Here, the sphere of attack is limited. Therefore the interception stage inevitably takes place near the target, so probably within the urban environment itself. Thus the risk of collateral damage is much higher.

3.2 Counter-measures against these new threats

Once the danger is detected, it is then necessary to determine according to the context the best adapted countermeasure. There are two big families of countermeasures (Mirkarimi et al., 2003, Haulman, 2003). The first family, the active one, tries to incapacitate or to destroy the threat in a direct way (systems of air-to-ground defence for example). The second, the passive one, tries to protect from the danger in an indirect way (physical protections around the target, the use of decoys, organized by systems of communications or of jamming of the sensors of the aggressor as will be detailed in the practical case part).

The first active countermeasures to fight against micro-UASs are inspired by classic anti-aircraft defences. However, if the latter showed their ability on "classic" targets, their efficiency against smaller and more reactive targets is much more mitigated, especially in urban zones with the public at risk. These methods are also difficult to apply against enemies attacking simultaneously on multiple fronts, even if we increase the ability of the defence system to react and make its saturation limit recede. The team mode of operation should besides allow implementing operational strategies (decoys, shields, rams) which complicates at the same time the stage of detection and interception. The swarm, on the other hand, should be easier to detect globally because it is not evident to mask the arrival of a cloud of robot craft, but it should show itself on the other hand much tougher to neutralize.

The passive countermeasures based on the physical protection of the target (installation of nets for example) are last resort solutions. However, within the context of attack by micro-UAS, these solutions can be effective because of the small size of the robots. The use of decoys supposes that we know a

priori the sensors used by the drone to make his kamikaze attack and how this information is used particularly in the final phase. The jamming of communication would appear to be effective against drones of level 1 or 2 which require the control of a pilot. It can also prove interesting to perturb the inter-drones communication required for a team or a swarm. The jamming of the sensors (false GPS information, camera dazzling, magnetic disturbance of the heading sensor) can also be an effective approach, whatever the level of automation.

4. Case study of a UAS swarm

4.1 Operational context

As we have seen previously, there can be a high operational interest to locally jam GPS cover. But a loss of the signal can easily be detected by the attacker who can then activate a ploy like estimating the course, the ground-speed and a timer in order to nonetheless reach the area of the target. More interesting is the case in which we only slightly modify the GPS signal to give false positions to the attackers in order to lure them into a chosen area. For the attacker, this strategy of defence is much more difficult to detect. In every case, this strategy can be complicated to apply on an area with fixed facilities, furthermore if the perimeter of the area to protect is mobile. A possible solution could be to use a swarm of UAS, each of them having an action (eventually mobile) of locally jamming. In this hypothesis, we use the swarm in a situation of defence. As for the aggressor, a solution could be to perform a kamikaze attack in order to create a breach in the defence system in position. In our next section, we will show an example an innovating demonstrator to test scenarios of swarm-based attack and defence in a given operational context.

4.2 Operational modelling of a swarm in defense

To continue working, the swarm will have to respond to the suicide bomber attack. The maneuver that is least costly in human resources will be a dodge to avoid contact with the bomber, but also with other UASs of the swarm. However, in order to have an operational interest, we will have at the same time to minimize the deformation of the network of the UAS swarm. Finally, to check the operational feasibility of these solutions, we want to be able to perform the associated calculations locally and almost instantly, which excludes conventional solutions such as those based on numerical modeling of virtual reality. To accommodate the constraints, we propose to develop a demonstrator adapting a physical library (Chipmunk) mainly used in video games on smart-phones. This pragmatic approach allows us to leverage for our problem all the improvements and developments made by the video game industry for which resource constraints and time calculations are close to what we want. The problem then is to find how to model our problem in the range of tools available in the library. The modelling solution that we propose for the demonstrator is:

- Avoidance of UAS done through a repulsive force like the Coulomb one so as $1 / r^2$, where r is the distance between the UASs.
- Minimizing deformation of the mesh done by linking the UASs with their neighbours in eight connexions by restoring forces in the manner of a spring where the coefficient of stiffness and length at rest reflect the physical reality (UAS's reactivity and inter-UAS distance respectively).

Figure 2 shows the physical network of the modelization. The big square is the attack UAS, and the small ones the defend UAS. The images shows different position of the attack UAS and the re-organized response of the defend UAS.

Figure 2: Modelization

Figure 3 shows screen shots of the demonstrator. This reacts in near real time. The modeling approach shows the desired behavior (deformation of the mesh of the swarm optimized and UAS-UAS avoidance made).

Figure 3: Demonstrator

From this demonstrator, we can draw two initial conclusions:

- The real-time constraints can be totally satisfied on architectures with limited computing power, and therefore be available in operation.
- The modelling shows that it is virtually impossible for the attacker to destroy or disrupt the defender's swarm effectively, unless he develops abilities to move very much faster than those of the defenders.

4.3 Collaboration among UASs in attack

From the perspective of the attacker, since a single attack is not enough, we have explored different scenarios of attacks of the defensive swarm by another offensive group using the demonstrator indicated above.

Among the initial findings, it appears that an attack from a team of UASs that begins by encircling the defensive swarm to limit the operating space increases dramatically the effectiveness of a direct attack, but needs strong coordination to have a maximum effect.

We can reverse the demonstration and say that a UAS swarm in attack would be practically unstoppable unless the defender demonstrates strong collaboration. If we describe a cloud of UAS as graph, we think it will be possible to use graph matching techniques to distort an attacking swarm with amazing efficiency over the defensive swarm.

We can conclude this part by saying that countering a swarm (in defence or attack) is very expensive because it seems necessary to have high level collaboration on the defence group side. Costs are an additional vulnerability factor for aerial security against a collaborative UAS attack.

5. Conclusion

We started this article by defining the new levels of automation and collaboration that the current UAS technology can offer. We then presented how these new capacities could increase the potential menace of a terrorist attack using simple short-range flying robots and why it seems necessary to start thinking

about appropriate responses to this particular problem. In the last part we have shown with a simplified demonstrator that some basic rules could give a UAS swarm a strong endurance to kamikaze attack, which can be used in a defensive way to maintain a local jamming on an area or in an offensive way to overwhelm the enemy. Against collaborative UASs, it seems that the only solution would be smarter and more numerous UASs. To conclude, our numerical approach has shown its value to estimate the behaviour and interactions of an UAS swarm. Nevertheless these results should be consolidated by practical tests; which will need to integrate the physical constraints of the robots and their sensors, as the reacting time, the measurements errors including the positioning error, the processing and synchronization capacities. Another way of extending this work could be 3D simulations, with remarkable increase in complexity with both attack and defence strategies.

References

Abatti, J. M. and AL, A., "*Small power: the role of micro and small UAVs in the future*.", Research report, Air Command and Staff College, Air University, Maxwell Air Force Base, 2005.

Beaudoin, L. and Gademer, A., "Towards symmetrization of asymmetric air dominance : the potential key role playing by home-made low cost Unmanned Aerial Systems", in *European Conferences on Information Warfare and Security, ECIW'10*, 2010.

F. Carnu, "The new face of air oriented terrorism and air defence systems vulnerabilities", in *Romanian Military Thinking*, p. 108-112, 2010.

Chaumette, S., Laplace, R., Mazel, C. and Godin, A., "Secure cooperative ad hoc applications within UAV fleets position paper", in *Military Communications Conference, MILCOM 2009. IEEE*, p. 1-7, 2009.

Chipmunk game Dynamics, http://code.google.com/p/chipmunk-physics/

Clough, B. T., "UAV swarming? So what are those swarms, what are the implications, and how do we handle them?", 2002.

Christ, R. D., Wernli Sr, R. L., "The Rov Manual : a user guide for observation-class remotely operated vehicles", Butterwsorth-Heinemann, Chapter 2 : ROV Design, 2007

Frantz, N. R., "*Swarm Intelligence for Autonomous UAV Control"*, Thesis, Naval Postgraduate School, Dept. of Electrical and Computer Engineering, 2005.

Gademer, A., Vittori, V. and Beaudoin, L., "*From light to ultralight UAV*", in *International Conference Unmanned Aircrafts System Forum,* Eurosatory, 2010.

Gademer, A., "*Réalité Terrain Étendue : une nouvelle approche pour l'extraction de paramètres de surface biophysiques et géophysiques à l'échelle des individus"*, PhD Thesis, ParisEst University, 2010a.

Gademer, A., Chéron, C., Monat, S., Mainfroy, F. and, Beaudoin,L., *"A low cost spying quadrotor for global security applications using hacked digital cameras*", in *DEFCON 17*, 2009.

Haulman, D. L., "*US unmanned aerial vehicles in combat, 1991-2003*", Research Paper, Air Force Historical Research Agency Maxwell Air Force Base, 2003.

Lamont, G.B., "*UAV Swarm Mission Planning Development Using Evolutionary Algorithms-Part I*", Research Paper, NATO, SCI-195, 2007,

Lamont, G.B., "*UAV Swarm Mission Planning Development Using Evolutionary Algorithms and Parallel Simulation-Part II",* Research Paper, NATO, SCI-195, 2008.

Miasnikov, E., "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", Technical Repport, Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology, 2005.

Mirkarimi, D. B. and Pericak, C., "Countering the tactical UAV Threat", *Armor*, vol. 112, n°. 1, p. 43, 2003.

Valenti, M., Bethke, B., How,J. P., de Farias, D. P. and Vian, J., "Embedding health management into mission tasking for UAV teams", in *American Control Conference, 2007. ACC'07*, p. 5777-5783, 2007.

Valenti, M., Dale, D., How, J. and Vian, J. , "Mission health management for 24/7 persistent surveillance operations", in *AIAA Guidance, Navigation and Control Conference and Exhibit,* 2007.

Singer, P. W., "Wired for War : the robotics revolution and conflict in the 21st century", Chapter 3 : Robotics for dummies,The penguin press, New-York, 2009