2017 International Conference on Military Technologies (ICMT)
May 31 – June 2, 2017, Brno, Czech Republic

The Non-destructive Methods of Fight Against UAVs

Miroslav Kratky* and Vaclav Minarik†
* University of Defence, Kounicova 65, Czech Republic, e-mail: *miroslav.kratky@unob.cz*
† University of Defence, Kounicova 65, Czech Republic, e-mail: *vaclavminarik@seznam.cz*

***Abstract*— This article deals with the unmanned aerial vehicles elimination issue using non-destructive methods with focus emphasis on possible electronic warfare capabilities. The main goal is to briefly analyse the known procedures and to focus on ways feasible in the Czech Republic environment, notably its security and military forces. These problems were solved by the analytics, multi-criteria and synthesis methods were used. The output of this work is the possible anti-UAVs defence means summarization, and their potential defence-ability evaluation. The results will be exploited for a more complex work concerning of this problem, which is solved at authors' department. There is an intention to utilize them for doctoral studies program as well.**

Keywords- unmanned aerial vehicle; air defence; electronic warfare; jamming.

I. INTRODUCTION

Thanks to the very dynamic development, which in recent years occurred in the field of UAVs, there is nowadays a necessity to solve their secure operation, possible misuse and also to focus on the use of cyber-attacks capabilities for fight against UAVs. The vast majority of producers are already nowadays trying to use encryption or other methods to secure their products against potential attackers, but relatively large underestimation of this protection in the past has caused a deficit in the present and possibly in the future too.

The attackers or rather defenders can use a wide range of options to defuse UAV or to make impossible to perform its task. The reason is, that there are – for mostly relatively price-affordable civilian UAV - detailed instructions how to attack individual modules of UAVs available, even on the Internet, e.g. [3].

II. PROTECTION AND COMBAT METHODS AGAINST UAV

In the light of these facts, that even the small unmanned systems pose a real security and military threat now, and their potential and frequency of deployment will probably have growth in the future, the responsible bodies should already now plan, take, and particularly implement the relevant counter-measures for an effective defence.

It is obvious, that the most effective way how to prevent any device from an attack is to stop it, even before its deployment for the particular mission. There are some precautions mentioned bellows [2] within the frameworks of security policy:

- **Determent** of possible aggressors, both by revenge and denial; corresponding national/alliance foreign policy should be applied.
- Corresponding **legal environment** within the individual states, or integrative units (i.e. EU in our case). All this should be underline by effective & enforceable laws.
- Particular **organizational-technical precautions** both on external and internal borders (i.e. Schengen Area in our case); at airports, other public transport stations, at high populated places etc.
- **Cooperation** of all Integrated Rescue System components within particular country or in area of operation.
- General **public awareness** creation and its permanent sustentation and improvement.

It means – from the military point of view – the detail intelligence preparation of battlefield ("IPB") in the war-time, or own territory preparation in the case of peace-time, which is the base for any future success. The subsequent operations are performed to eliminate troop's capability for the UAVs attack. These go both for regular or guerrilla enemy forces. Accomplish of these measures practically means to disable their airplanes themselves and the corresponding ground accessories as well, just on the ground. The next possible ways are e.g. to make the land-transportation means useless, or the enemy flight operators elimination.

Now we can discuss, in the wider context, e.g. about the "sensitive" technology embargo to the so called danger regions. But let's face it, the nowadays globalization and widespread technology proliferation make such an attempt, esp. in the case of small UAVs, almost purposeless.

In a case when all the measures mentioned above are depleted and hostile UAV took off for certain combat mission, different procedures has to be used to compromise UAVs tasks, for example by application of passive procedures.

The passive means will not allow the attacking plane to achieve intended goal, or will degrease the effectivity of attack. This means in practise, that the payload (explosive, chemical toxic substance etc.) or the aircraft itself does not hit the target. There are a number of means and measures how to do it: catching nets, safety barriers, reinforced building (incl. bulletproof windows, barring …), sectored endangered areas (e.g. by walls, ramparts ..), anti-aircraft shelters (both deliberately built, and ad-hoc built/found: cellars, land waves …), armoured vehicles, means of personal protection (bullet-proof vests, helmets …), masking equipment, dummy positions prepared for assumed attacked objects, etc. The analysis of these ways of protection is problem on its own and goes beyond of extend of this paper.

We can, in principle, divide the active methods to destructive and non-destructive ones. Both of them have their advantages, disadvantages and particularity when and where a defender can use them. They are all performed in several phases.

A. Defence phases against UAVs – in general

The **first** essential prerequisites for a UAV defeating are the timely disclosure, and the necessary information preparation for the next processing. The reconnaissance process is usually composed by four sequences: detection, recognition, identification, and localization. It is worth to note, that mainly detection – as a key step, and identification of small UAV are very hard esp. in urban and close terrain.

It is necessary in the **second** phase to determine what kind of effector we should use in the view of the fact that the inadequate collateral losses could be caused.

The **final** phase of the defense act is the effector action itself and evaluation of the action.

The active defense is realizable - taking into account the current technological level - as:

- physical aircraft destruction: *physical hard-kill*,
- making aircraft impossible to fly physically, or fly improperly: *physical soft-kill*,
- electronic warfare ("EW") methods application: *electronic soft-kill*.

B. Physical hard-kill and soft-kill methods

These methods are characterized by the direct destruction of the UAV. Physical energy affects to the fuselage, or impacts to some of the vital important parts of the UAV. Weapons that use kinetic energy of projectiles, or the directed-energy weapons ("DEW") are chiefly developed at present days.

Concerning to physical soft-kill methods, there are several means for to affect a physical disability of UAV, or to cause its flight difficult, e.g.: high-velocity stream of water (water cannon), firm articles cluster (granules), cloud of viscous foam, fire curtain etc. But there are several problems with these soft-kill means. Especially their limited range and the high logistic demands for to ensure the needed amount of an active working medium are degrading their ability for wider practical deployment

C. Non-destructive soft-kill methods

These methods and corresponding means are often used within areas, where the destructive weapon engagement could be dangerous for friendly units or some civilian casualties may occur. The non-destructive methods application is often not only more economically efficient, but it enables even to take possession of a hostile UAV in useable condition.

Non-destructive methods belong to the EW domain and their realisation is carryout both by a disruption, or infiltration and modification of:

- control signals used for to guide UAV to its target ("uplink"),
- signals sending from UAV to the ground control point ("downlink"),
- information obtained by UAV and sent to operator/user ("downlink"),
- location reference signals (GPS, GLONAS, GALILEO),
- another signals/information needed for UAV control system,
- SW functionalities of UAV.

General design can be demonstrate by the Figure 1 below.

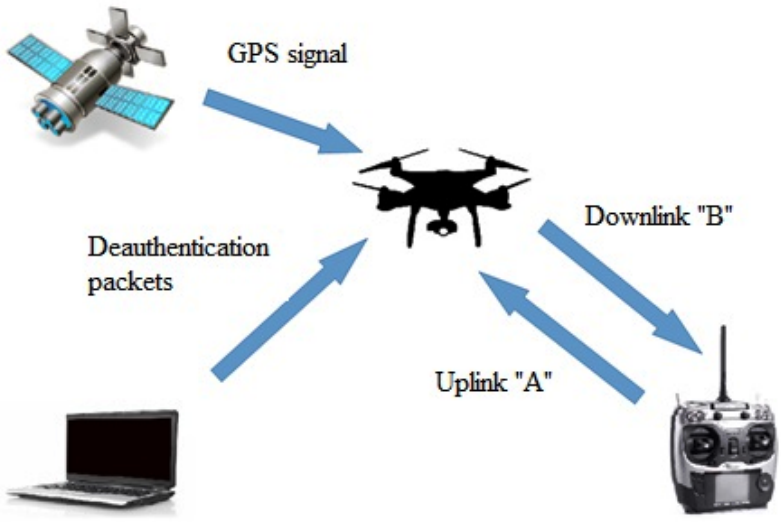

Figure 1. The electronic warfare system for fight against UAV - general chart

From the information flow point of view and with taking into account corresponding signals which pursue methods mentioned above, the issue is about:

- simple jamming of a signal,
- breaking into the unmanned system control loop by defender' EW means,
- consequent flight parameters modification.

This is done either simple for the UAV flight plan corruption only, or for a full take-over of the flying UAV. Afterwards, the overtaken UAV subsequently follows defender' commands.

From the system point of view the UAV flight is realised in the control loop which includes ground control centre (transmitter, receiver, interface etc., in the next "RC" only) data transfer paths and aircraft itself.

Looking to the data flow and corresponding signals which realize the above mentioned methods, we can talk about a simple signal jamming, or an entering into the control loop. This is done for to the UAV flight parameters changing, their modification, or possibly for to take over the UAV as the whole.

III. JAMMING

Jamming can be used to interfere with several signals used by the UAV. This chapter briefly describes the principles, possibilities and reasons for their use.

A. Jamming signals sending from RC to the UAV

The first option of the jamming analyse here is the attack on the signal (control commands) from a RC transmitter to the aircraft - "uplink". In the Figure 1 this is labelled by letter "A". This prevents a direct remote control. If the UAV has a function to automatically switch to an autonomous mode, usually after losing control signal it returns to the take-off position and attempts to land there. Or UAV is guided to the last position, where the proper connection was recorded.

B. Disruption of signals sending from UAV to the RC

In connection to the disruption of command – control loop, it is also possible to interfere so-called "downlink", in the Figure 1 marked as "B". By successful disruption of this signal we can compromise transfer of geographic coordination to the command post. In this case UAV must be guided visually or autonomy. This type of disruption is advantageous if there is an effort to disable or disrupt coordination of several UAV commanded by a common ground control station.

C. Disruption of information from UAV to the RC

Some UAVs are used as e.g. "spy" means, and information acquired by them are sent to the ground. Content of this data stream is composed usually by audio and video components and data are obtained by UAV modules or sensors. Disruptions of these signals are possible too.

D. Jamming GPS reference signals

Other signals for possible jamming are GPS signals. If the jamming is successful and we assume that the UAV has GPS positioning only, the UAV is forced to land because it is threatened to collide with uneven terrain or other object. In connection with the GPS jamming it is important to discuss also the possibility to create a false signal of GPS - called "GPS spoofing". This is realized by so called "pseudo satellites". If the UAV catches a false signal, and the GPS sensors on the board of UAV evaluate it as "correct", there is a high probability of an accident due to faulty specified UAV position or a mission failure. At least – this is the desired effect of defence.

E. Disruption the UAV software functionalities

One of the less used, difficulty feasible, but highly effective option is to repeatedly send deauthentication packets (also "Disassociate Package" or known as "Aircrack"), which prevent connection between the UAV and operator. This method, however, can only take place at shorter distances (certain power of jamming signal is needed) and only in the case of certain types of UAVs.

IV. TAKE OVER THE UAV CONTROL

Within the non-destructive methods of combat, as optimal appears an attempt to take control of the adversary UAV. Generally, we can talk about a false signal that the UAV receives and based on this signal it performs actions desired by defender.

A. Options of to take a control

The majority of commercial available communication equipment operates with WiFi technology, specifically at the frequency 2.4 GHz and 5.8 GHz bands. Despite of the use of the high-quality WPA (WiFi Protected Access) encryption, this Wi-Fi technology has some weaknesses. But if a defender would exploit them and hack into the control loop, he must overcome some challenges.

The biggest problem, if defenders would want to take over the UAV control, is that they have to focus on a particular type of UAV. Each producer uses a different security key - both for the different series and for specific products as well. It is necessary to timely identify the type of attacking machine, its capabilities, and the actually used control signal. Basically, the direct correlation is between the dimension (and rather the price of UAV), and the sophistication of the safety features and the given specific security.

B. How to take a control

Possibilities how to take control could be generally divided into several types. It depends on the degree of interference with the data transmission between the UAV and the control station.

The most natural way how to take a control is to induce a situation when defender is able to duplicate control signals from the attacker' control station. After such intervention the attacker may not be able to recognize that the control of the UAV can be transferred to someone else. It can be used in favour of the defender, for example, if causing a subtle correction looks like it is caused by an accident. The attacker can consider this disaster as a self-error or a technical

malfunction of UAV and such a defence action remains hidden for him.

Another option is to focus more (if an attacking UAV has this functionality) on video data transmission and other parameters sent from UAV back to RC centre. This can then determine not only what a particular invader focuses its attention on, but also the UAV position itself or the ground control transmitter / receiver station.

The third type is the complete takeover of UAV control. The attacker' RC is disconnected from his UAV. This allows defender not only to guide the UAV into an area where it is best to eliminate it with respect to collateral losses, but there is also a possibility for to land it safely on our own territory and disarm it. This method is prospective, and analysis will be done in the future.

C. *Taking control – the use and tactical aspects*

The defensive EW equipment can be located both on land and on the flying platforms. Location on earth, of course, assumes a highly mobile and easily transportable means. Modifications and placing of the necessary hardware for to take control on board a defender' UAV can achieve a higher degree of "3D Mobility" and improves conditions for receiving and analyzing signals from opponent streams.

Indisputable advantage of a successful hostile UAV taking control is also psychological, preventive, and propaganda aspects. If an opponent after the failed attack finds out that his UAV was literally "stolen", it will significantly damage his self-esteem and even a motivation for further similar acts. In contrast, appropriate self-promotion such a defense is desirable, and make this act appropriately visible could cause a deterrence of potential attackers. From the perspective of defense forces we can assume their encouragement by the fact that they are able to defend themselves in this way.

V. MULTICRITERIA EVALUATIONS OF COMBAT AGAINST UAV

Multi-criteria evaluations are used in situations where it is necessary to choose between several alternatives. To evaluate the combat utility against UAV, the method of scoring was chosen. This method was selected not only because of a relative simplicity, but also efficiency. Based on the weight determination and expert assessment of the number of points, we can obtain various ways of fighting. When applying this method, one should select individual parameters, determine their priority and assign the appropriate weight.

Example realized here assumes an offense UAV "mini" category and defence against it in a densely populated, urban area. Expert analysis is shown in TABLE I. Consider, for example, an UAV attack on gathering of people at a festive occasion, at the sports stadium, the central node of public transport etc.

For multi-criterial evaluation of the effectivity of such scenario and when the defence EW means were applied, the first parameter **effectiveness** was chosen – describing the capability to disable a UAV fulfil its task. This parameter has the highest priority, and he was assigned a value of 0.3. The second criterion is a **collateral effect** of our activity on the opponent's UAV. Assuming that the attack is carried out on our own territory, it is desirable to minimize this effect. Next parameter is within **range**, but it was valued 0.1 only – more precisely because of the assumption that the defence is applied in urban areas. The penultimate parameter is **technical complexity** and applicability of the particular method. Due to differences in a UAV security measures and technical solutions for each individual UAV its quantification is considerably generalized. The final factor is labelled as **scale of possible use**. It qualifies the methods of fight variability. Due to the frequent combination of a several UAV management systems it is desirable to thwart the UAV attack using a combination of two or more methods of struggle.

TABLE I.

	Value	Jamming uplink		Jamming downlink		GPS jamming		GPS spoofing		Deauthentication packets	
		Points	*Result*	*Points*	*Result*	*Points*	*Result*	*Points*	*Result*	*Points*	*Result*
Effectiveness	0.3	2	0.6	2	0.6	2	0.6	3	0.9	3	0.9
Collateral effect	0.2	2	0.4	2	0.4	2	0.4	2	0.4	3	0.6
Range	0.1	3	0.3	3	0.3	3	0.3	2	0.2	1	0.1
Technical complexity	0.2	2	0.4	2	0.4	3	0.6	2	0.4	3	0.6
Scale of possible use	0.2	2	0.4	2	0.4	2	0.4	2	0.4	1	0.2
Summary	1	**2.1**		**2.1**		**2.3**		**2.3**		**2.4**	

The TABLE I. shows that the top-rated method of combat is sending deauthentication packets, mainly due to high efficiency, small collateral effect and relatively low technical difficulty.

VI. CONCLUSION

To manage a problem arising with the numbers of UAVs operating worldwide is now more than desired. An array of laws, regulations and instructions, e.g. from safety, military and transport domains, are trying to put legal frameworks for the UAVs' operational rules. Problems concerning defence against hostile, or misused small aircraft are analysed as well.

Applying electronic warfare means into anti-UAV defence systems appear to be a quite promising way. Analysing the feasible methods how to stop, or divert a UAV from its intended goal. Authors have decided that some methods are more suitable for use in security sector, another for military use, and some for both areas.

Example given in chapter V shows a typical security problem situation. Especially collateral effects should be taken into account – thanks to the action within an urban area.

The multi-criteria evaluations results are different if EW means were used it in other conditions, or for military purposes on battlefield.

ACKNOWLEDGMENT

This work was performed as part of the project for development of electro - military departments of Faculty of Military Technology of the University of Defence in Brno – "PROKVES" when financing from institutional support paid by the Ministry of Defence. For students the support was provided from the University Specific Research funds paid by the Czech Ministry of Education, Youth and Sports of the Czech Republic.

REFERENCES

[1] FARLÍK, Jan; ČASAR, Josef. Application of Multi-Agent principles for operational centres procedural modelling. In: *RECENT ADVANCES in CIRCUITS, SYSTEMS and AUTOMATIC CONTROL*. Budapest, Hungary: WSEAS Press, 2013, p. 383-386. ISSN 1790-5117. ISBN 978-960-474-363-6.

[2] KRÁTKÝ, Miroslav. Today's toys – tomorrows' threats - Countering UAVs as the Air-Defenders' Challenge. Main paper at *Integrated Air & Missile Defence* conference workshop, Hamstad, Sweden. Producer: IQPC Ltd, International Quality & Productivity Center, London, UK, 2014, 55 p.

[3] AMP Security. *WiFi Crack WPA Handshake* [online]. Last rev.: 8. 12. 2016. Available at http://airdump.cz/wifi-crack-wpa-handshake.

[4] NCC Group. *Drones: Detect, identify, intercept and hijack* [online]. London, [UK]. Last rev.: 1. 12. 2016. Available at https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/december/drones-detect-identify-intercept-and-hijack.