ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 447-454 (2020)

www.astesj.com

Special Issue on Multidisciplinary Innovation in Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Electronic Warfare Methods Combatting UAVs

Miroslav Kratky[*,1], Vaclav Minarik[1], Michal Sustr[2], Jan Ivan[2]

[1]*University of Defence, Department of Air Defence, 662 10, Czech Republic*

[2]*University of Defence, Department of Fire Support, 662 10, Czech Republic*

ARTICLE INFO

Article history:
Received: 27 August, 2020
Accepted: 15 October, 2020
Online: 20 November, 2020

Keywords:
Unmanned Aerial System – UAS
Unmanned Aerial Vehicle – UAV
Air Defence
Electronic War-fare
Cybernetics
Neural Network

ABSTRACT

This paper describes methods of eliminating Unmanned Aerial Vehicles (UAV) non-destructively, using Electronic Warfare Methods. The aim is to introduce certain methods of UAV detection and elimination in a complex environment and terrain, e.g., in an urban and battlefield environment, that will result in finding the control device position and the UAV itself. Neural networks, cyber penetration elements, and wireless network scanning programs are all used to address this issue. The output of this article is a new concept of a comprehensive solution, which can be implemented into the existing complex system of electronic defence against UAVs, e.g., within the allied base. Conclusions will be also used to further improve the above-mentioned topics at the authors' workplace, within the frame of long-term projects and specifically as a part of solutions applicable to the force protection of combat support units, namely field artillery, which is described here in detail.

1. Introduction

This paper is an extension of the work originally presented in proceedings of the "2019 International Conference on Military Technologies" (ICMT), Brno, Czech Republic [1]. The original material was enriched by the proposed concept applied in the urban area. The whole section proposing a possible concept applicable to artillery units was added.

A very dynamic development of Unmanned Aerial Systems (UASs) is becoming highly visible as they are used in all areas of human activities [2].

With the gradual widening of the UASs complexity and complementing other features, there is a demand for more complex security. The reason is that both military forces and terrorists have increasingly used Unmanned Aircraft Systems to plan, prepare, and execute attacks on ally and partner's forces and on "soft targets" in the civilian sector. Preventing, protecting, and recovering from such attacks require a cross-governmental approach, bridging the different efforts that Allies, partners, NATO, other international organizations, industry, and academia are making on this topic, both in the military and in the civilian domain. The threat description, probable scenarios, and protection models concepts are well described now by several trustworthy documents, e.g., in [3].

In another word, simultaneously with UASs development, we have been witnessing the counter-UAS (C-UAS) systems rapid improvement as well. Moreover, the C-UAS systems development concerns not only the direct defence against flying apparatuses themselves, but this also applies to the whole loop of the air defence system: detection, command-control system and elimination itself. The whole engagement process is now a highly complex, sophisticated, and, from a scientific point of view, multidisciplinary one.

Thus, after transforming from simple radio-controlled machines into sophisticated, "smart", digitally-controlled UAVs, an opportunity was developed to combat the whole UAS not only with standard methods, but – apart from another ones - also with cybernetic methods. Contemporary modern UAV can be seen as a small computer or a mobile phone with the ability to fly. This connects the current IT security issues and air defence issues together with the UAVs.

During the next development, it will be necessary to take into account the possibility of anti-aircraft defence congestion caused by the high availability of micro UAVs at a very low affordable price. Therefore, the developed means should be able to operate a large number of UAVs at the same time and at a minimum cost.

[*]Corresponding Author: Miroslav Kratky, Email: miroslav.kratky@unob.cz

2. Methods of Cyberattack Applied to UAVs

In today's digital age, the growth of cyberattacks can be seen not only on personal computers, servers, and mobile phones, but also with the introduction of "internet of things", on any device that is able to connect and communicate over the network. This opens the possibility of cyberattacks on most types of UAVs too. Cybernetic methods of attack, like conventional methods, can be divided into two basic groups according to the expected effect. These methods are non-destructive and destructive.

2.1. Non-destructive Methods of Cyberattack

Non-destructive cybernetic methods of combat are understood as methods in which there is no direct destruction of any particular component of the affected system. This group includes the most contemporary cyberattacks. We can further divide these attacks into several subareas (in detail: [4]). Graphical representation of non-destructive cyberattack methods on UASs is depicted in Fig. 1.

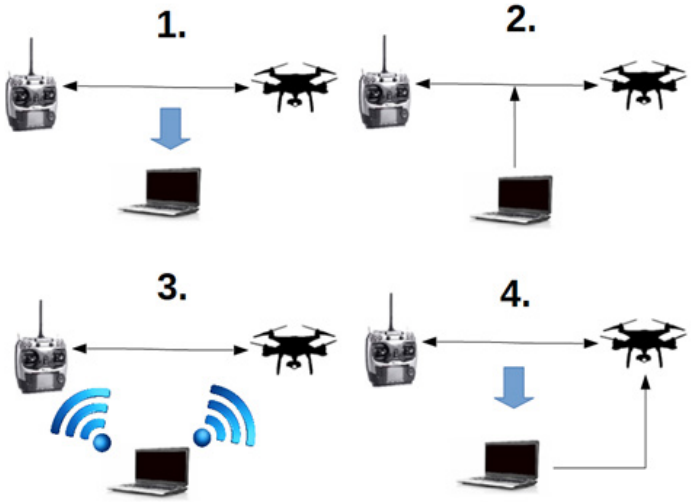

Figure 1: Graphical representation of non-destructive cyberattack methods applied to UAV´s

1) Leakage of Information

This type of attack results in disclosure or leakage of protected information. The advantage is its detection difficulty and in most cases the speed of attack. In UAVs, this attack is about getting the downlink channel information providing the UAV's mission or about getting the data to find the password for Wi-Fi communication.

2) Disturbance of Integrity

This subgroup includes attacks where the UAV's data are destroyed, damaged, or changed. This type of attack is very well detectable, but in most cases until after its accomplishment.

3) Denial of Service

Denial of Service (DOS) attacks make it impossible to use a particular service or system of UAS. The C-UAS defender will focus on a particular access channel or a specific service and will disable real-time activity by systematically sending requests (see DoS attack below). This attack is very visible and is usually suppressed quite quickly.

4) Unlawful Use of Information

These attacks focus on using the obtained information to access non-public parts of the system or to use certain services without authorization. In UAVs, for example, the acquired password can be used to decrypt the intercepted communication or to take over its control.

2.2. Destructive Methods of Cyberattack

The destructive C-UAS cybernetic methods of combat have a direct impact on the part of the attacked system that is physically irreversibly damaged as a result of this activity. These methods mainly use the vulnerability in the lower layers of the OSI (Open Systems Inter-connection) model and focus primarily on individual hardware components that are used in multiple systems. The operation of these methods is primarily based on a mechanical damage. For example: the cybernetic attack induces a collision of mechanically moving components or the cybernetic attack forces a battery or some other component to overheat and thus damage themselves.

3. Signal Detection of the UAV

When combatting mini and micro UAVs, one of the biggest problems is the detection and identification of the UAS itself, especially in an urban densely built area. Using radar or other detection methods with optical equipment (in the visible or IR optical band) is often considerably complicated by many fixed obstacles [5]. Methods using specific acoustic characteristics of the UAVs are also limited due to the interfering ambient noise [6].

The best choice in such environments is, therefore, the detection and localization of signals transmitted by the UAV itself or its control station.

These signals can be relatively well detected and identified due to their known specific transmission frequencies and known encoding.

However, this detection becomes considerably harder if the UAV is managed only by Wi-Fi in an electronically complex environment. Contemporary modern cities are full of devices that use the same Wi-Fi standards, and that hides the UAV' control signal among the other Wi-Fi networks within its range [7].

3.1. Localization Position of the remote control station or UAV

An UAV recognition method can be used, utilizing the MAC address to locate the position of the control station or the Wi-Fi standard to locate the position of the connected UAV itself. Each producer has a certain range of initial MAC address characters, which makes it uniquely identifiable. However, a problem occurs when the Wi-Fi module is modified or if the UAV MAC address is changed by software. Both of these methods are realizable by at least an average capable IT man.

3.2. Analysis of Data Flow Using Neural Network

One of the progressively evolving technologies is the technology of neural networks (NN). The main domain of these networks is their relatively rapid analysis of a large volume of data and the data subsequent evaluation. Neural networks, unlike algorithmic solutions, do not use serial computations. The task is solved simultaneously with several layers of neurons that interact

with each other. Neural network inputs can also be parameters of the UAS Wi-Fi traffic, such as the number of frames, their size, and generally the data flow over time.

Thanks to NN advantages, especially in the field of data processing, i.e., their ability to take in a lot of inputs, process them to infer hidden as well as complex, nonlinear relationships, NNs are playing a big role in signal characteristic recognition. Based on these features, the NN should be able to recognize which device it is both the UAV itself and the control station as well. Thus, the next part is devoted the NN application to the UAS detection and identification.

4. The UAS Signal Detection Using Neural Network

Neural networks can be used in the process of data mining. This is currently an increasingly inflected term. In general, it can be understood as a process aimed at discovering dependencies or finding the required information in a large volume of usually experimentally obtained data. The output is a certain knowledge that can be used in solving a decision problem, predicting values for other new data, or simply understanding a certain phenomenon or context. [8]

In principle, three methods can be used to identify UASs using 802.11 standards. UAS can be identified by the SSID, which is the name of the access point. However, this can be changed very easily. Furthermore, we can use the identification according to the MAC (Media Access Control) address, because in the MAC address the first six characters identify the manufacturer. This method is already suitable for use, but the MAC address can also be changed. The third method is based on the analysis of the data flow and the creation of the so-called fingerprint. For this purpose, a neural network can be successfully used, which has the task of analysing the data flow to decide whether it is intercepted traffic originating from UAS communication or not.

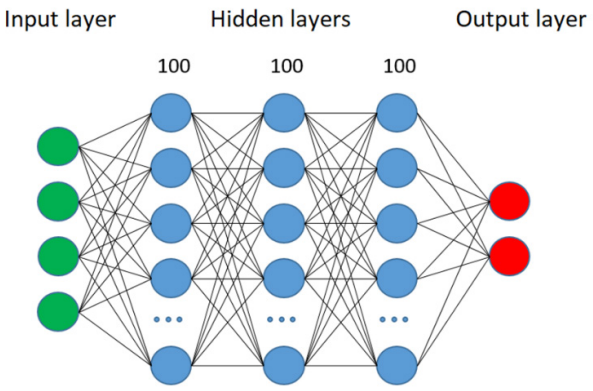

Figure 2: Topology of the created neural network

Input data is a key element in training neural networks. The ability of the network to learn and evaluate, or rather to evaluate with sufficient accuracy, depends on the appropriate selection of individual parameters and the input data set.

The selection of input parameters was made on the basis of knowledge obtained by analysis of data flows originating from the tested UAS and several other applications (e.g. Skype, YouTube). Analysis of data streams revealed that one of the determining parameters is the number of unique frame sizes in a given sample. This is due to the nature of the transmitted stream, where certain activities or communications create a larger number of unique frame sizes than others. The second determining parameter is the number of frames transmitted per second. This is mainly related to the overall data flow, but it also in some way represents the disposition of the intercepted communication. The average frame size was chosen as the third parameter. It expresses whether the captured traffic contains rather smaller or larger frames. The size of the frames is affected by the disposition of the transmitted data. The last parameter was the ratio of the number of frames with a size greater than 100 B and less than 100 B. This value was chosen mainly based on the analysis of all data streams, where different operations have this ratio different. The topology of created neural network is depicted in the Fig. 2.

Based on these parameters, the neural network can distinguish whether it is UAS operation even when masking the SSID or changing the MAC address of the transmitted frames.

5. Possibilities for UAS Elimination Using EW Methods

5.1. Possibilities of Penetration into the UAV Communication Channel

In general, the resilience of security depends on several factors, of which the quality of the encryption used and the length of the password usually have the greatest influence. Specifically, WPA2 security uses the CCMP (Counter Cipher Mode Protocol) algorithm based on the Advanced Encryption Standard (AES) encryption algorithm. The length of the password that can be used with WPA2 is between 8-63 characters. Security resilience depends not only on the length of the password, but also on the character set used. It is also advisable to choose passwords that are not contained in dictionaries, or that do not contain word forms or diminutives [7].

Brute force Attack and Dictionary Attack by Cloud Computing

Brute force Attack and Dictionary Attack can be amplified by using Cloud Computing. In the case of a brute force attack, it is necessary to test all possible combinations in the set given by the specified parameters. Any known information about password parameters significantly speeds up the successful use of this attack. Brute force Attack will certainly find a password in the future, but it is better to use a dictionary attack first. Dictionary attack is based on creating as big as possible a dictionary of known words, which increases the chance of an earlier password being discovered. Commonly used high-performance computer sets can test even with a GPU (Graphic Processor Unit) of only 400 KHps (Kilo Hash per second) when used for WPA2 encryption. The way to amplify computing power is called Cloud Computing. With these services, it is possible under certain circumstances to break relatively long passwords in short or real time. These services can be rented from technology companies such as Google or Amazon, from 10 minutes for the duration of the rental [9].

Rainbow Table

In some cases, the "Hashing Function" format is used for encrypted communication. This function recalculates the password entered by the user and the output is "Hash", which is a transformation of a string to a given number of characters. These

hashes are precalculated within the "Rainbow Table" to make it easier to crack the password [10].

DoS Attack

Denial of Service attack is an attack which transmits recurring deauthentication frames that result in disconnection of communicating devices on 802.11 [11].

KRACK Method

The Key Reinstallation Attack (KRACK) method is one of the relatively newly discovered methods focusing on a certain vulnerability of the Wi-Fi standard. It uses a four-way authentication process, in which communication is established between the AP (Access point) and the client. Simply put, it works on the principle of delaying the response to the third message during the four-way authentication sent to the access point. As a result, the AP sends a new 3rd message with an increased "counter number". When it receives the 3rd message for the first time, the client installs the GTK (Group Transient key) and PTK (Pairwise Transient Key) keys and sends the 4th message, which is then held. Upon receiving a retransmitted 3rd message with an increased counter number, the client reinstalls the previously installed GTK and PTK keys and resends the 4th message. Subsequently, both 4th messages are left to pass to the AP. Knowledge of changing the original and later reinstalled GTK and PTK keys can then be used to decrypt the communication [12].

5.2. Options after Successful Penetration into the UAV System

From the attacker's point of view, there are several ways to penetrate the system, differing in danger and enabling different goals to be met [1].

Secret Observation

The most inconspicuous way to start a penetration is a simple observation of the video stream or telemetry data, which are received by the UAS control station. This makes it possible to identify the equipment of the UAS with specific sensor (measuring) devices or to identify the operator' area of interest.

Sending Unobtrusive Commands

The operator' control can be affected by sending confusing or conflicting commands. Such an effect on the UAS may lead to the termination of the UAS task, as the operator will think it is a technical fault.

Complete take over the UAS

For the complete takeover of the UAS, it is necessary to disconnect the original RC and prevent it from being reconnected. To do this, you need to know the password and the ability to change it in real time as well. Successful takeover largely depends on the manufacturer of the individual components or the UAS model itself.

6. The Proposed Concept of the EW C-UAS System

6.1. Basic principles and functioning of the proposed concept

The basic principles of system operation are clearly shown in the Figure 3. The whole system is divided into one main and two support sections, each of which brings a different ability, or added value. The proposed concept [6] may represent the addition of another element of complex defence against micro and mini UAS.

The concept includes devices to detect signals and record Wi-Fi data in passive mode and send deauthentication frames in active mode. Within one computer and control centre, information are collected from one or more devices.

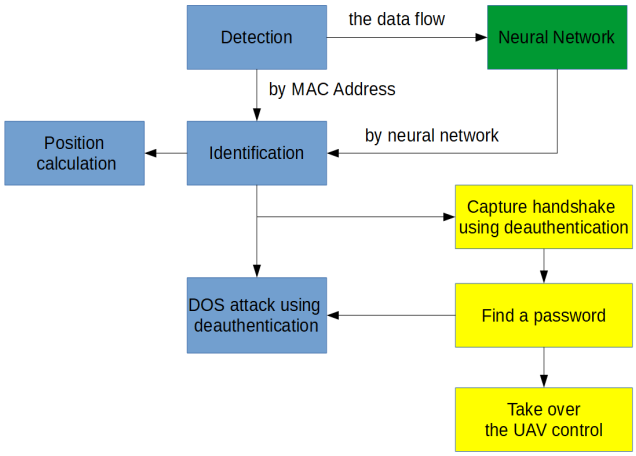

Figure 3: The proposed neural network

Detection, Identification, Position calculation and DoS Attack Using Deauthentication

The main section (shown in blue) provides the basic capabilities of the system and is the only one that can act automatically in a limited way. It contains 4 blocks providing initial signal detection (capture), device identification according to MAC address, position calculation based on information from one or more sensors and, if necessary, the DOS attack itself. Upon successful capture and identification of an unwanted UAS, we are able to send a deautentication frame to the nearest sensor to disconnect communication between the RC and the UAS or between the RC and the display device. After sending only one or a few deauthentication frames, the connection is established automatically, but if the deauthentication frames are still sent, the connection will not be established. [9]

Neural Network

The first support section (shown in green) evaluates the intercepted data stream using a neural network (explained in more detail in Section 4) and, based on the results, identifies the type of device or the type of traffic in the intercepted communication. This information is passed on to the main section for subsequent specification [6].

Possibilities to Find Password

The second support section (shown in yellow) aims to bring the ability to take control of the UAV. The process usually begins by sending a deauthentication frame and then capturing a 4-way handshake. This provides a signal pattern to perform the password retrieval process. After successfully finding the password, it is possible to take over the control, either completely or partially, or penetrate into the communication system. [6]

6.2. The proposed concept applied in the urban area

For practical use in urban areas, e.g., the device *Alfa AWUS036ACM* (see Fig. 4) can be used as a sensor and

transmitter, providing sufficient omnidirectional range, supporting 802.11 a / b / g / n / and ac standards, and operating in the 2.4 GHz and 5 GHz frequency bands, respectively. Another indisputable advantage of this device is its low price in combination with normal commercial availability [6].

Figure 4: Device *Alfa AWUS036AC*

Figure 5 shows an object with a marked critical defence point (red circle), access roads (3, 5), high-rise areas (1,2,4), and a low building (6), which poses the greatest risk due to the possibility of direct visibility to defended point

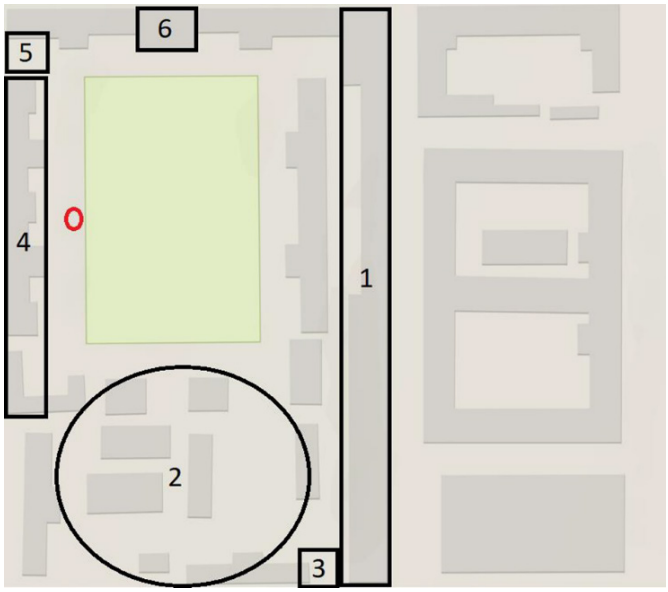

Figure 5: Defended critical point

It is advisable to place the sensors so that they cover most of the area and selected places outside the area from which the UAS control could be performed. The Alfa AWUS036AC device, which is connected to a certain small computer, e.g. *Raspberry Pi*, is taken as a sensor. All sensors would then be connected to a central point where evaluation and control would take place.

Despite of this that the quantity of sensors seems to be a little considerable, by using low-price hardware mentioned above, we are able to cover the protected area completely. Connection to the EW C-UAS system proposed in subsection 6.1 can sustain full control of this defended critical area.

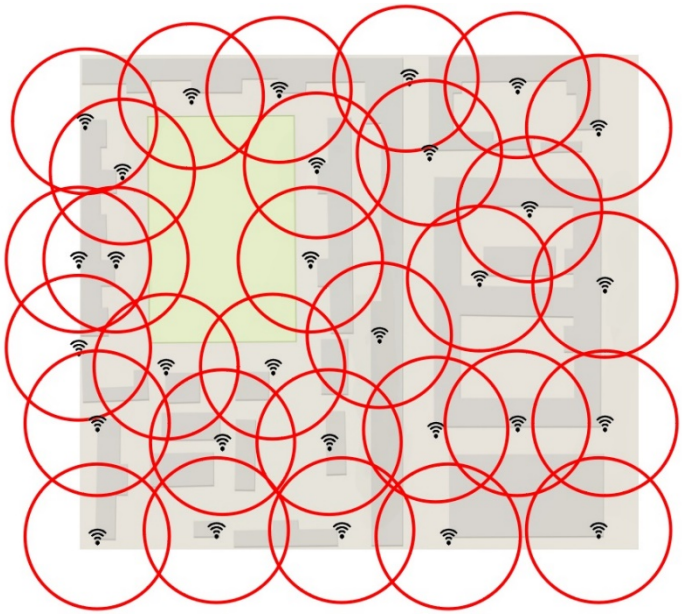

Figure 6: Defended critical point

6.3. Partial conclusion of Section 6

The previous parts described the general principles and division of cyber-attacks and the operation of the 802.11 standard of interest. To detect UAS using this standard was developed by applying the neural network and the concept in which it is embedded. However, instead of a neural network, it would be possible to use other methods of genetic programming, but the use of a neural network is suitable for this task.

Within this theoretical concept, the use of an existing HW and its deployment on the example of a defended object in a non-war area was also proposed. The use of the system in the military field is dealt with in the following section.

7. The proposed concept applied to artillery units

Based on knowledge from current conflicts, especially from the war in Ukraine and Syria, it is clear that UAVs - small, light, and cheap unmanned aerial vehicles pose a great risk to all combat units. The availability of these tools, which are available for small amounts of money, together with their capabilities makes them an ideal means of conducting aerial reconnaissance.

Findings from the conflicts in Ukraine and the Middle East clearly show that these instruments, when applied to fire support units, specifically artillery, can be used very effectively, especially for:

- reconnaissance (uncovering the battle group),
- target acquisition,
- artillery fire control,
- evaluation of the effectiveness of fires,
- perform attacks using explosives,
- perform attacks, using weapons s of mass destruction (chemical, biological, and possibly also radioactive "dirty" bombs).

In recent years, we can find countless combat situations, where small UAVs have successfully performed the tasks mentioned above. To illustrate this, several examples of the use of small UAVs are given in the table No 1.

Table 1: Examples of small UAV attacks

Year	Example
2005	Al-Qaida used Chinese made remote control model airplanes to recon Pakistan security forces prior attacks. It was also weaponized with IED.[13]
2014	Islamic state used small quadcopters for recon missions of Syrian military bases prior to ground attacks. [13]
2015	Drone attacks on military bases in Ukraine. Each drone was equipped with one grenade (ZMG-1 type). [14]
2015	Several attacks on ammunition depots at Svatovo, Ukraine. Drones were equipped with grenades. [14]
2016	Two French Special Forces soldiers were injured and an exploding ISIS drone killed two Kurdish fighters. [14]
2019	Drone attacks struck two key oil installations inside Saudi Arabia [15].
2020	Pro-Kremlin mercenaries use an unmanned aerial vehicle to drop a rocket-propelled grenade on Ukrainian emplacements. [16]

These examples clearly show the possibilities of using small UAVs and their ability to cause significant losses. The use of small commercial UAVs in combat operations can provide the enemy with key information about the positions of our own troops and their manoeuvres. In combination with explosives or weapons of mass destruction, it is possible to cause significant losses in technique and manpower. For this reason, it is necessary to be prepared for this variant and be able to defend effectively against these types of attacks.

7.1. Artillery units in the regular operations and proposed concept of application

In a peer-to-peer war, all kinds of military forces and resources are involved in combat operations. For simplicity, examples of the application of the proposed concept of protection against small UAVs are reduced only to artillery units. However, a similar approach can be used for all types of units and their specializations wherever there is a real possibility of attack by these UAVs.

The artillery battalion (battery) is conducting its operations within a given position area of artillery (PAA) within the zone of attack (defence) of the brigade (task force). Part of this PAA are also battalion (battery) Fire Direction Centres (FDC). Fig. 7 gives an example of PAA [17].

The danger emerging from the use of small UAVs is, in particular, the possibility of uncovering a combat formation and subsequent directing fire on firing units and command posts, and attacks using explosives placed on the UAV or attacks using weapons of mass destruction. Artillery units are usually deployed in a hidden position, outside the firing positions, when they do not conduct fires. Weapon systems occupy firing positions only when they are firing. Firing positions and firing points are usually in the open space. At this point, they are vulnerable and easy targets.

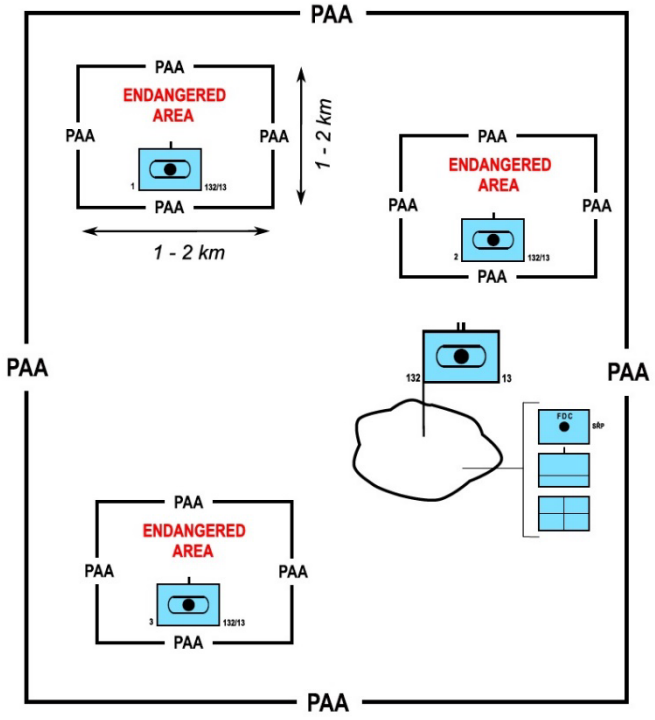

Figure 7: The position area of artillery [18]

One of the main risks the artillery is facing is the counterbattery fires. Artillery units are always priority targets and it is necessary to avoid the risk of detection, which precedes the implementation of counterbattery fire. The tactic of using small UAVs by enemy reconnaissance and diversion groups has always been a danger. In connection with the development of capabilities and possibilities of using not only military, but also small commercial UAVs, new risks are emerging and their frequency may be higher due to their massive spread and availability.

With a standard time of one fire mission and time to leave the firing position, the probability of successful counterbattery fire is low. In the case of proactive counterbattery activity, where artillery units are actively searched for and neutralized without unmasking themselves by firing, the probability of success is much greater than in the case of reactive counterbattery fire when it is reacted to firing artillery. The enemy gains an advantage by knowing the coordinates of the firing positions and starts the fire mission when the cannons are taking up firing points to conduct fire. It is this key information that can be easily obtained using small UAVs. They are able to uncover a combat formation, detect individual artillery weapon sets and already in the phase of the manoeuvre into the firing position, warn the enemy, and provide sufficient information for the preparation and execution of fire. At the same time, they can provide a detailed evaluation of battle damage assessment (BDA) after firing.

Another variant is the use of UAVs as carriers of explosive devices, which can be used to destroy targets. In the case of artillery, a suitable target are FDCs. Destruction of them will

eliminate the entire firing battery from combat for a period of time. Alternatively, it is possible to destroy individual artillery weapon sets, which cause a deficiency in fire support.

Based on these findings, the proposed concept of detection and neutralization of UAVs is a very effective tool for reducing the risk of detection by these means and the subsequent elimination of artillery units by enemy counterbattery fire, or explosive devices. From the point of view of the effective use of the proposed concept, it is necessary that the established measures reflect the tactics and procedures of artillery fire units. The biggest restrictions will be mainly area requirements. The firing battery of self-propelled cannon howitzers is deployed in the area of firing positions, usually 1 - 2 x 1 - 2 km, depending on the position conditions and the combat task [19]. This space must be covered with the ability to neutralize the UAV - this can be achieved by using a directional antenna with sufficient gain or power, which will ensure the required range. The individual antennas should be connected to an automated system, from which their focus and modes of operation will be controlled.

Firing units are most exposed to observation at the moment of performing fire missions, when they are deployed in firing positions. A suitable variant is the placement of equipment for neutralization of UAVs on vehicles of artillery reconnaissance/survey units, or on artillery weapons sets [20]. To a minimal extent, it would be sufficient to place this device on the lead gun of fire platoons, or vehicle of the platoon commander. However, this depends on the possibility of increasing the scope of the opportunity of neutralizing the enemy UAV within the proposed solution. At command points (FDCs), it would be sufficient to place the equipment on one vehicle of FDC.

7.2. Artillery units in asymmetric operations and proposed concept of application

The use of artillery in an asymmetric conflict has its specifics. Firing units are usually located on permanent or forward operational bases and provide fire support to units performing framework operations in the area of responsibility. They do not manoeuvre and are constantly at the firing points. In an asymmetrical operation, the risk of counterbattery fire is minimal according to current experience. However, commercially available UAVs can radically change this state if used correctly [21]. The danger of the UAV being used by the enemy lies mainly in the possibility of uncovering the combat formation, finding out the position of the firing point of individual artillery weapon sets, and possibly leading an attack on them using explosives placed on the UAV. In an asymmetrical environment, this way of conducting combat is one of the few ways to put the fire units located in the base area in danger. A coordinated attack can cause significant technical losses and limit the ability to provide artillery fire support in the area of operations. It is therefore appropriate to consider how to defend against such an attack and to provide protection for the artillery fire support units and other base personnel. Placing the defence EW device on the base in such a way, which achieves coverage of the base perimeter, is a suitable variant of solving the problem. In the event of a breach of the base perimeter, the operator is able to ensure the protection of base members and prevent the UAV from flying over the base within the proposed method.

7.3. Partial conclusion of Section 7

This concept of protection against small UAVs will ensure that units are not attacked or uncovered and the risk of losing artillery fire support will not increase. At the same time, the simplicity of the proposed solution will not place excessive demands on interventions in the construction of vehicles or buildings. The solution can be applied to all types of troops and its specialization, wherever the risk of using small UAVs in the combat activities of the enemy can be assumed.

8. Conclusion

UAV defence in a cyber environment combines elements of cyber security and air defence. The development of new methods for attack and defence is necessary due to the dynamics of the development of these areas, which is confirmed by current knowledge from the fighting in Nagorno-Karabakh, where unmanned aerial vehicles and artillery play a major role. One of the possible ways is the proposed solution for penetration into UAS control systems.

The methods described in this article focus on supplementing and extending existing complex solutions of UAV defence models. Their application clearly achieves an increase in capability in the implementation of defensive measures and the fight against the UAV opponent. Simplicity and ease of materials and new inexpensive technical means represent an advantage for application in practice, e.g. in the military environment, as described and suggested by the examples of artillery units.

As the main achievement, authors consider a practical demonstration of the possibility for identifying the device based on the characteristics of the data frames. For this purpose, a neural network was developed which, based on the entered parameters, can evaluate whether the intercepted traffic comes from UAV communication.

As all the UAS defence systems are usually aimed at a certain type of opponent, this concept is not universal. It focuses on complementing the existing comprehensive defence model with more options, thus creating the ability for the defence institutions to fight more effectively with highly sophisticated adversary means.

Subsequent research in this area could be aimed at expanding the input parameters of the neural network and output neurons. The neural network should then be able to identify not only the device or the type of data stream transmitted during UAV operation, but also other types of operation. The whole system could then be used for overall monitoring - for the purpose of using Wi-Fi networks in the area of interest. However, extending this system to such a level could mean a significant intrusion on the privacy of individual users. If implemented in practice, this problem would be forced by the author to solve both at the technical and legal level.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This work was performed as a part of the project "PROKVES" for Development of Electro – Military Departments at Faculty of Military Technology and "SPECIFIC RESEARCH" at Faculty of Military Leadership, University of Defence in Brno. They have been financed from the Institutional Support Department funded by the Ministry of Defence Czech Republic.

References

[1] V. Minařík a M. Krátký, "Cybernetics fight against the UAV". 2019 International Conference on Military Technologies (ICMT), Brno, Czech Republic: Institute of Electrical and Electronics Engineers Inc., 2019, 8870103.

[2] M. Kratky and J. Farlik "Countering UAVs – the Mover of Research in Military Technology". Defence Science Journal 2018, **68**(5), 460-466. https://doi.org/10.14429/dsj.68.12442.

[3] NATO C-UAS Working Group, "NATO Countering Class I Unmanned Aircraft Systems (C-UAS) Handbook". Version 1.8. Brussels, BEL 2020.

[4] J. Kolouch, "Kybernetické útkoy" 2019. https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[5] T. Kornelly, J. Casar, V. Stary and J. Farlik, "Mobile phone optical sensor usage for navigation tasks" 2017 International Conference on Military Technologies (ICMT), Brno, 2017, 671-675. doi: 10.1109/MILTECHS.2017.7988842.

[6] V. Minařík, "Elektronický boj v obraně proti bezpilotním prostředkům". Brno, 2019. Ph.D. exam thesis. University of Defence.

[7] V. Minařík a M. Krátký, "The Non-destructive Methods of Fight Against UAVs". 2017 International Conference on Military Technologies (ICMT), Brno, 2017, 690-694. doi: 10.1109/MILTECHS.2017.7988845.

[8] M. Lastovka, "Data mining jako moderní prostředek analýzy dat a možnosti jeho uplatnění v podmínkách AČR". Brno, 2015. Diploma thesis. University of Defence.

[9] "Ethical Hacking and Countermeasures v10". EC-council, 2019. https://iclass.eccouncil.org/.

[10] "Rainbow tables tajemství zbavené" [Online article]. 2015 [cit. 2019-01-5]. Available from: https://www.soom.cz/clanky/1165--Rainbow-tables-tajemstvi-zbavene.

[11] J. Kolouch, P. Bašta, "CYBERSECURITY". Praha: CZ.NIC, z. s. p. o, 2019. ISBN 978-80-88168-34-8.

[12] M. Vanhoef, F. Piessens, „Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2" [Online article]. 2017 [cit. 2019-01-5].

[13] J. R. Bunker, Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications. Carlisle, Pennsylvania: US Army war college press, 2005.

[14] Russian Drone With Thermite Grenade Blows Up a Billion Dollars of Ukrainian Ammo. Popularmechanic [online]. 2017, 27. 7. 2017, [cit. 2020-08-13]. Dostupné z: https://www.popularmechanics.com/military/weapons/news/a27511/russia-drone-thermite-grenade-ukraine-ammo/.

[15] Donbas: Russian militants use drone to attack Ukrainian positions. 112UA [online]. 1. 6. 2020, [cit. 2020-08-13]. Dostupné z: https://112.international/conflict-in-eastern-ukraine/donbas-russian-militants-use-drone-to-attack-ukrainian-positions-51819.html

[16] J. Ivan, K. Šilinger, L. Potužák. "Target acquisition systems suitability assessment based on joint fires observer mission criteria determination". In: Madani K., Gusikhin O. ICINCO 2018 - Proceedings of the 15th International Conference on Informatics in Control, Automation and Robotics. Portugal: SciTePress, 2018, roč. 1, 397-404. ISBN 978-989-758-321-6.

[17] B. Čermák, R. Hegyi, L. Potužák, M. Kalina, "Bojové použití dělostřelectva", Military publication Pub-35-14-01, TRAIDOC Vyškov, 2013.

[18] J. Ivan, "Situační značky a zkratky pro dělostřelectvo: (vojenská symbolika a taktické značky pro dělostřelectvo dle APP-6)". University of Defence in Brno. ISBN 978-80-7582-122-5.

[19] M. Bláha, K. Šilinger, "Application support for topographical-geodetic issues for tactical and technical control of artillery fire". In: International Journal of Circuits, Systems and Signal Processing, **12**, 48-57. ISSN 1998-4464.

[20] IVAN, Jan and Jan POTUŽÁK, Jiří ŠOTNAR. Dělostřelecká rekognoskace pro zabezpečení činnosti autonomních zbraňových systémů a základní požadavky na rekognoskační jednotky. *Vojenské rozhledy*. 2019, **28** (4), 063-077. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.

[21] KARBER, Phillip A. Lessons Learned from the Russo-Ukrainian War: Personal Observations [online]. 8 July 2015. Available at: https://www.researchgate.net/publication/316122469_Karber_RUS-UKR_War_Lessons_Learned.