International Conference on Military Technologies (ICMT) 2019
May 30 – 31, 2019, Brno, Czech Republic

Cybernetics Fight against the UAV

Vaclav Minarik and Miroslav Kratky
Department of Air Defence, Faculty of Military Technology, University of Defence, Czech Republic
e-mail: *minarikvaclav@seznam.cz, miroslav.kratky@unob.cz*

Abstract— **This article deals with the problem of the elimination of Unmanned Aerial Vehicles (UAV) by non-destructive methods, especially in the area of cyberspace. The aim is to introduce certain methods of detection and elimination in complex environment and terrain e.g. in the urban environment, with the possibility of finding the position of the control device and the UAV itself. The neural network, cyber penetration elements and the wireless network scanning program are used to address this problem. The output of the article is the creation of a concept of a comprehensive solution, which can be implemented into a complex system of electronic defence against UAV. Conclusions will be further used for a comprehensive solution of the above issues at the authors' workplace within the framework of the long-term project and the elaboration of the related work of the students of the doctoral study program.**

Keywords: Unmanned Aerial System – UAS, Unmanned Aerial Vehicle – UAV, air defence, electronic warfare, cybernetics, neural network.

I. Introduction

The very dynamic development of Unmanned Aerial Systems (UAS) is now highly visible and they are used in all sectors of human activity [1].

With the gradual widening of their complexity and complementing other features, there is a demand for more complex security. After transforming from simple radio-controlled machines to sophisticated "smart" digitally controlled UAVs, there has started an opportunity to act against the whole UAS, not only with standard methods but also with using cybernetic methods. Today's modern UAV can be seen as small computer or mobile phone with the ability to fly. This connects IT security and air defence issues with the UAV and has a lot in common with them. During the development it is necessary to take into account possible congestion of anti-aircraft defence due to presence of high amount of micro UAV with very low purchase price. Therefore, the developed means should be able to operate at the minimum cost to a large number of UAVs at the same time.

II. Methods of cyberattack applied to UAVs

In today's digital age, we can see the growth of cyber-attacks not only on personal computers, servers and mobile phones, but also with the advent of "Internet of Things", the attacks spread to any device able to connect and communicate over the network. This opens the possibility of cyber-attacks 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.

A. *Non-destructive methods of cyberattack*

Non-destructive cybernetic methods of combat are understood as methods in which there is no direct destruction of a particular component of the affected system. This group includes most contemporary cyber-attack. We can further divide these attacks into several sub-areas (see in [2]).

1) Leakage of Information

This type of attack results in disclosure or leakage of protected information. An advantage is the difficulty of detection and in most cases the speed of the attack. Concerning to the UAV, it is about to get downlink channel information, which give us the goals of the UAVs mission or about to get data needed to find a password for Wi-Fi communication.

2) Disturb of Integrity

This subgroup depicts attacks where the UAVs data are destroyed, damaged or changed. This type of attack is already very well detected, but mostly after its successful execution.

3) Denial of Service

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

4) Unlawful Use of Information

These attacks focus on using the information obtained to access non-public parts of the systems or the use of certain services by unauthorized entities. In the UAV issue, for example, the usage of the acquired password can be used to decrypt the intercepted communication or take control itself.

Graphical representation of cyber-attack non-destructive methods on UAS is demonstrated by Fig. 1.

B. *Destructive methods of cyberattack*

Destructive 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 Interconnection) 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 basis. For example: a cybernetic attack induces a collision of mechanically moving components or on a heat base

978-1-7281-4593-8/19/$31.00 ©2019 IEEE

– a cybernetic attack forces the battery or some components to overheat and thereby damage it.

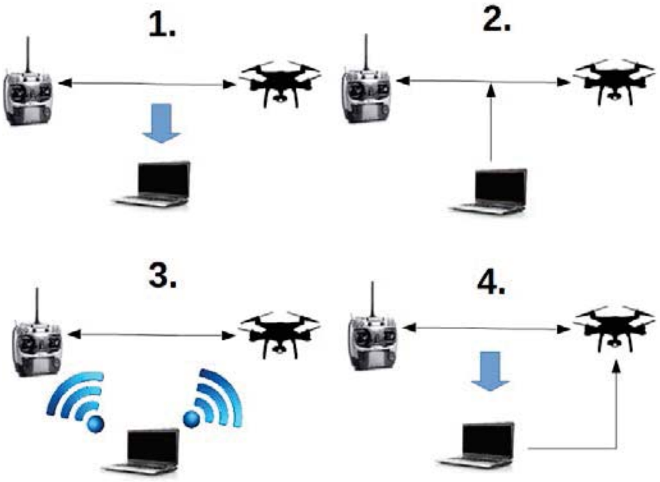

Figure 1 Graphical representation of non-destructive methods of cyberattacks applied to UAV´s

III. Signal detection of the UAV

In the fight with mini and micro UAVs, one of the biggest problem is the detection and identification of UAS itself, especially in the urbanely densely built area. The use of radar or another detection method using optical equipment (in visible or IR optical band) is considerably complicated due to frequent fixed obstacles [3]. Methods using the specific acoustic characteristics of the UAV are considerably problematic due to ambient noise [4].

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

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

However, a considerable aggravation will occur if the UAV is managed only by Wi-Fi. Today's modern cities are full of devices that use this standard, resulting in hiding the UAV' control signal between other Wi-Fi networks within range [5].

C. Localization Position of the RC or UAV

You can use the UAV recognition method using the MAC address to locate the position of the control station or the UAV itself, which is connected by the Wi-Fi standard. Each producer has a certain range of initial MAC address characters, which makes it uniquely identifiable. However, the problem occurs when the Wi-Fi module is modified or the UAV MAC address is changed by software.

D. Analyse Fata Flow Using Neural Network

One of the progressively evolving technologies is the technology of neural networks. The main domain of these networks is a relatively rapid analyse of large volumes of data and their 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 input can also be the parameters of Wi-Fi traffic, such as the number of frames, their size, and generally the data flow over time. Based on these parameters, the neural network should be able to recognize which device it is.

IV. Possibilities of penetration into the UAV communication channel

Wi-Fi penetration capabilities when using WPA2 encryption are very limited. As a rule, the success mostly depends on the complexity and length of the password used or on the knowledge of its parameters.

E. Dictionary Attack

This type of attack uses the creation of vocabulary of directly defined word sets and their individual testing when data stream is decrypted. In general, generic information about the password-maker, at least its nationality and linguistic equipment, is used to generate the dictionary. Publicly generated dictionaries with a particular focus or character set are publicly available. The main advantage of using a „Dictionary Attack“ is a significant limitation of the number of passwords tested, but there is a chance of a password failure even after the selected dictionary has been searched completely [6].

F. Brute force Attack

In the case of a brute force attack, all possible combinations of characters are tested according to the specified parameters. The difficulty of this type of attack depends primarily on the known facts about the used password. Any information about the length, structure, or type of characters will greatly speed up the subsequent password-finding process. Nowadays, commonly used powerful computer assemblies, even though they use the GPU (Graphic Processor Unit), can test only 400 KHps (Kilo hash per second) when using WPA2 encryption. This speed is insufficient in time to break the commonly used 8-digit passwords that contain both uppercase and lowercase characters. Partial assistance in solving this problem is the use of the Cloud computing or Rainbow tables, which are explained below [6].

G. Cloud Computing

The branch of Cloud Computing is growing thanks to increasingly available semiconductor com-ponents, more stable information networks, and growing demand for computing performance. The main advantage is lower costs, when high computing power is used abruptly. Technology companies such as Google or Amazon offer an online rental of relatively large computing power with the shortest rental times for as long as 10 minutes. These services open up space for breaking long-passwords with WPA2 encryption and give them the chance to do this in relatively short time or real time.

H. Rainbow Table

A form called "Hashing Function" is used for some types of encrypted communications nowadays. The password entered by the user is recalculated by this function and the resulting communication is encrypted with the resulting of „Hash”, which is a character string transformation to the unified word.

„Rainbow Table“ works on the principle of pre-counting these hash values to facilitate subsequent password breaks. [7]

I. DoS Attack

Denial of Service attack is an attack to impair service availability by sending meaningless or constantly repeating requests, resulting in overloading the line or system capability to address relevant requirements. The same type of attack performed from multiple locations is called DDoS Attack (Distributed). [2]

J. KRACK Method

The Key Reinstallation Attack method is one of the relatively new methods that focuses on a particular vulnerability of the Wi-Fi standard. It uses the "4-way handshake" process, which establishes the communication between "Access Point" - "AP" and the client – in this case the UAV. In simple terms, it works on the principle of delaying the third message response for a 4-way handshake sent by AP. As a result, the AP sends a new third message with an increased "counter number". The first time you receive the third message, the client installs the Group Temporary Key (GTK) and Pairwise Transient Key (PTK) and sends the fourth message, which is then held back. Upon the receipt of the retrieved third message with the elevated counter number, client reinstalls the previously installed GTK and PTK keys and the fourth message is sent again. Subsequently, both messages are left to go to the AP. Knowledge of changes to original and later reinstalled GTK and PTK keys can be used to decrypt communications. The entire procedure and possibilities of penetration of individual operating systems are described in detail in [9].

V. Options after successful penetration into the UAV system

After successful penetration into the system, there are several possible activities depending on the potential of the cyber attacker and the desired goals.

K. Secret Observation

The least noticeable is the hidden observation of the telemetry data or the video stream sent to the UAS control station. This enables you to identify, for example, the area of interest of the operator or his particular sensory (measuring, recording optical / acoustic, etc.) device.

L. Sending Unobtrusive Commands

Sending conflicting or confusing commands may result in an operator's attempt to change this behaviour. Eventually, this may be considered by the operator as a technical defect and then interrupts the performance of the UAV task.

M. Complete take over the UAV systems

For a successful overall takeover, it is desirable to disconnect the original RC management capabilities or downlink transfer capabilities - such as video and other signal information. This requires not only the access password from communication, but also the ability to change it as quickly as possible. The use of the full takeover option depends largely on the producer and the UAV model used.

VI. The proposed concept of cyber defence against the UAS

The overall concept of the proposed cyber defence system against UAS in the future is, in principle, based primarily on originally developed application using the "aircrac-ng" software tool.

The hardware configuration consists of devices that allow not only to detect signals and capture Wi-Fi data, but also to transmit deauthentication frames. Information from one or more devices is sent to a common evaluation, computing, and control centre.

N. Software for Detection and Identification

Detection and identification software performs space scanning as far as possible and creates a list of found devices. Based on the detected MAC addresses, it assigns performers' names to individual devices and captures the data stream streaming on their channels.

O. Neural Network

The input of the neural network is the captured data stream parameters. Based on these input parameters, the probable type of device interpreted by the captured data stream is evaluated.

P. Position calculation

The calculation of the position depends on the amount, distance and characteristics of the sensors used. Using more than 2 sensors, a triangulation method can be used to calculate the signal strength and position of the source of signal. Depending on the signal strength, the distance of the source can also be determined and azimuth can be determined precisely using the directional antennas. Desirably, a combination of more omnidirectional and several appropriately positioned directional sensors appears.

Q. DoS Attack Using Deauthentication

When successfully capturing and identifying an undesired UAS, we are able to send a deauthentication frame using the closest sensor to disconnect the RC and UAV communication between the RC and the display device. After sending only one or several deauthentication frames, the connection is re-established automatically, but the deauthentication frames cannot be established when the connection is in progress [4].

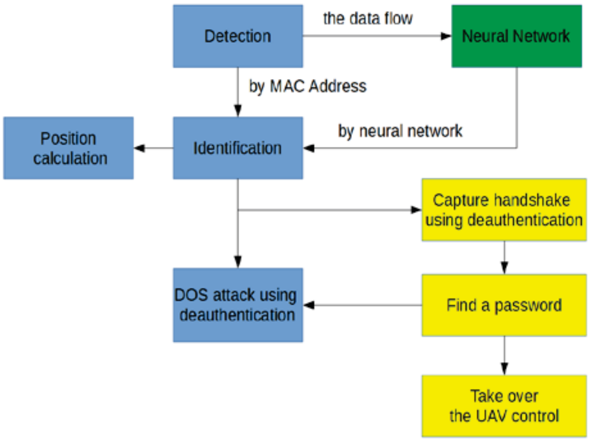

Figure 2: The proposed concept of cyber defence against the UAS

R. *Possibilities to Find Password*

For Wi-Fi with WPA2 encryption, communication is established by 4-way handshake authentication. When capturing a data stream containing a 4-way handshake, it is then possible to try to find a password. It is not necessary to locate the password on the capture site, but it is desirable to send it as soon as possible to a better-equipped processing facility. To get a quick search, use as many computing units as possible with the highest possible power. As previously described in the "Possibilities of penetration into the UAV," an optimal way to get a great computing power is to use cloud computing [6].

VII. Conclusion

Cybernetic counter-UAV defence is a combination and application of cyber security and air defence against UAV. Due to the tremendous dynamics of development in both areas, it is still necessary to create new methods and applications for both attack and defence. Moreover, in the area of cyber-attacks, we find ourselves in a situation where much information and "know-how" are classified because of illegality and competitive advantage. Literature generally describes general principles on the basis of which it is necessary to develop its own tools for penetration into the UAS control systems.

The concept described in this article was created by combining several general knowledge, supplemented by a part of the latest "know-how" that authors have created over the past few years.

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

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 and from the University Specific Research funds paid by the Ministry of Education, Youth and Sports of the Czech Republic.

References

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

[2] J. Kolouch, “*kybernetické útkoy”* [online]. [cit. 2019-01-5]. Available from: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[3] 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, pp. 671-675. doi: 10.1109/MILTECHS.2017.7988842

[4] V. Minařík “*Elektronický boj v obraně proti UAV”*. Brno, 2017. Ph.D. exam. thesis. University of Defence.

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

[6] “Ethical Hacking and Countermeasures v10”. EC-council, 2018. [online] [cit 2019-02-14]. Available from: https://iclass.eccouncil.org/

[7] *“Rainbow tables tajemství zbavené”* [online]. 2015 [cit. 2019-01-5]. Available from: https://www.soom.cz/clanky/1165--Rainbow-tables-tajemstvi-zbavene

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

[9] M. Vanhoef, F. Piessens „*Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”* [online]. 2017 [cit. 2019-01-5].