Analysis of Control Channel Cybersecurity of the Consumer-Grade UAV by the Example of DJI Tello

M.V. Mamchenko

1 V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Profsoyuznaya str. 65, 117342 Moscow, Russia

E-mail: markmamcha@gmail.com

Abstract. This paper presents the assessment of cybersecurity of the non-industrial unmanned aerial vehicle (UAV; using DJI Tello as an example) wireless control channel, implemented on the basis of Wi-Fi Wireless Local Area Network technology. As a result of the research, a model of an adversary conducting a cyberattack on the UAV communication channel was developed, and scenarios of an intruder’s actions (aimed at taking control of the UAV or disabling it) were considered. Relevant block diagrams of the actions of an adversary were also developed. Based on the results of the analysis, a security strategy is proposed. It provides the maximum possible protection (based on the technical characteristics of the drone) and comprises not only passive protection in the form of setting a tough password, but also active actions – deploying a system to monitor the injections of deauthentication/dissociation frames and/or the creation of duplicate wireless networks.

1. Introduction

With the widespread use of drones, particular attention is paid to the UAVs’ overall cybersecurity and protection of their subsystems, including the control systems and channels.

Currently, consumer-grade UAV control and communication systems are mainly implemented using Wi-Fi Wireless Local Area Network (WLAN) technology with WPA2 (AES/TKIP) security protocols. This wireless communication technology is widespread, Wi-Fi access points are miniaturized, and their deployment on drones is well established.

The aim of the work is to analyze and assess the security of a non-industrial UAV’s control channel, identify vulnerabilities, consider scenarios of an adversary’s course of action to hijack the UAV or disable it, and develop recommendations to enhance the cybersecurity of the consumer-grade UAV (by the example of the DJI Tello).

1.1. Brief Description of the Control System of DJI Tello UAV

DJI Tello is controlled by an operator using a proprietary application installed on smartphones running the iOS 9.0 and above or Android 4.4.0 and above operating systems (OS). With power on, the UAV deploys a Wi-Fi Access Point (AP) based on the 802.11n standard at a frequency of 2.4 GHz, unencrypted (open wireless AP) and WPA2-PSK encryption modes are available. The UAV’s AP allows only one client to be connected – the operator’s smartphone [1].
2. The Model of an Adversary Conducting a Cyberattack on the Communication Channel of the UAV

2.1. Assumptions and Limitations
In order to analyze the scenarios of cyberattacks on the wireless control channel and the AP of the UAV, the following assumptions will be introduced:

1. The operator controls the DJI Tello UAV with a smartphone; the maximum flight time of the drone is 13 minutes. The operator enables the WPA2-PSK encryption mode on the AP of the UAV. The length and complexity of the password are unknown to the attacker.

2. The attacker is within the range of the UAV’s Wi-Fi access point, has a personal computer running Kali Linux OS, several external Wi-Fi adapters, and a smartphone running Android 9.0 or higher with a pre-installed drone control application and available Internet access. The attacker starts to act immediately after the drone is activated by the operator.

3. The intruder cannot gain physical access to the drones.

4. The aim of the attacker may be to hijack the drone, while preventing the operator from regaining control of the UAV, or to disable the drone by performing a denial of service (DoS) attack on the UAV’s Wi-Fi AP.

2.2. Types of Possible Cyberattacks
For all of the following attacks, there is the same sequence of preliminary actions that the attacker needs to perform: switch the external Wi-Fi adapter into a monitoring mode (e.g., by using the iwconfig utility), acquire the basic service set id (BSSID) of the target network (BSSID is the MAC address of the UAV’s AP), MAC address of the operator’s device on the target network, the type of encryption used and the number of the wireless channel [2]. It is assumed that the intruder performs these preliminary actions by default in the following attacks.

2.2.1. Deauthentication Attack. The deauthentication attack is carried out by continuously sending frames to disconnect clients from the AP (in this case – to remove the operator’s device from the wireless network deployed by the UAV’s access point). It should be noted that the attacker can conduct the deauthentication attack both continuously and periodically.

However, in the case of a successful deauthentication attack, the intruder cannot immediately connect to the UAV access point due to the presence of a password of unknown complexity and length. Thus, this type of attack is relevant to the attacker in the following cases:

- to remove the operator’s device from the network and gain control of the UAV (if the WLAN password is obtained);
- as an auxiliary stage of DoS or hijack attacks on the UAV [3].

2.2.2. Authentication Flooding DoS Attack. The attack consists in sending multiple authentication and association frames to the AP of the UAV. The attacker may permanently change the MAC address of their external Wi-Fi adapter, and this gives a false sense of sending frames from numerous unique clients. The increase in the number of "clients" awaiting the authentication results in consuming the memory of the AP and decreasing the speed of processing the query frames, and this eventually leads to the disconnection of the operator’s device and the DoS of the drone’s AP [4].

2.2.3. Capturing the Handshakes and Brute Force Dictionary Attack. Handshakes are data packets that the AP and the client exchange during the process of connection. They confirm that the client and the access point have correct credentials and agree on a new encryption key to protect traffic. The attacker carries out the deauthentication attack and waits for the operator to reconnect to the UAV’s AP. When the operator reconnects, the attacker captures the handshakes, saves them in a separate file, and then carries out the dictionary brute force attack [2, 5].
There are two outcomes of such an attack: an attacker may get the password in less than the drone’s flight time (if the password is simple and can be obtained from the dictionary), or the attack will fail (if the password is complicated and cannot be obtained by the dictionary brute force attack). In the first case, the attacker, having obtained the password, conducts the deauthentication attack, connects to the drone’s AP and hijacks the UAV. However, the probability of the presence of a simple password to be obtained in less than 13 minutes is rather low. Therefore, the intruder needs to carry out the attack that has the highest chance of success in the absence of information about the length and complexity of the password.

Figure 1 shows the block diagram of the handshake capture and the dictionary attack.

![Fig. 1. Block diagram of handshake capture and dictionary attack.](image)

2.2.4. "Evil Twin" Attack – Creating the False AP and Jamming the Target One. Suppose that the password disclosure from the captured handshake via the dictionary attack failed, or the attacker initially assumes that the password cannot be obtained by the dictionary attack.

In this case the most effective for the adversary is the "Evil Twin" attack: jamming the target AP (from the first wireless adapter) and simultaneously creating a false one with the same SSID, MAC address and encryption type (from the second wireless adapter). The operator may assume that the UAV has inadvertently disconnected, and attempt to reconnect to the AP using valid password of the target access point. But in fact, they will reconnect to a false AP. The software of the intruder will automatically attempt to enter the real wireless network using the intercepted password. If successful, the attacker stops jamming the target AP and maintaining the false one. The intruder then carries out the deauthentication attack, connects to the drone’s AP using the valid intercepted password, and gains accesses to the UAV [6, 7].

This attack can be both difficult and easy for the attacker. If the operator tries to reconnect to the "false" AP by entering the valid password from the target wireless network, the further steps to hijack the control will be simple. However, it is possible that the operator will not yield to the used social engineering methods and will not reconnect to the false AP, then the attack will fail. Figure 2 shows the block diagram of the "Evil Twin" attack with the subsequent deauthentication attack.
2.2.5. **KRACK.** The Key Reinstallation Attack (KRACK) is based on the identified vulnerability of the four-phase handshake of the WPA2 protocol. During the 4-way handshake exchange between the AP and the client, the attacker can force them to reset the encryption keys (that protect the WPA2 traffic) to zero values, eavesdrop the Wi-Fi traffic, and even inject frames into the victim’s data (if WPA-TKIP or GCMP is used). Thus, KRACK is a classic man-in-the-middle attack and leads to decryption of the transmitted traffic [8].

Despite the particular danger of the attack, exploited vulnerability can be eliminated by patching the client’s firmware/software. Google is known to have already patched the Android Open Source Project, so that versions of Android 5.0.2 and higher are not affected by this vulnerability. In addition, Apple’s iOS 11.1 and higher versions are also patched to exclude the possibility of the KRACK attacks [9].

The probability of the operator using a smartphone with older versions of Android or iOS to control the drone is very low. Thus, assume that this type of attack is not effective and will not be used by the attacker.

---

**Fig. 2.** Block diagram of the "Evil Twin" attack with the subsequent deauthentication attack.
3. Malicious Attack Scenarios

3.1. Hijacking the Drone’s Control

Since the attacker does not know the length and complexity of the password, they cannot rely solely on the capture of the handshake and the dictionary attack. On the other hand, the intruder also has to take into account that the "Evil Twin" attack will not succeed if the operator realizes that the target AP is being jammed. In addition, the duration of the attack is limited to a maximum of 13 minutes. In this case, the most optimal scenario for the attacker will be combining the dictionary attack and the "Evil Twin".

The attacker conducts the deauthentication attack and waits for the operator to reconnect to the AP of the UAV, then intercepts the handshake, and attempts to obtain the password via the dictionary brute force attack.

Then the attacker carries out the "Evil Twin" attack (simultaneously with the start of the dictionary attack). Thus, the chances of success increase: two processes – waiting for the operator to reconnect to the "false" AP to capture the valid password, and processing the captured handshake – run in parallel. If the password is simple, it will be gained via the dictionary attack; the intruder stops the "Evil Twin" attack, deauthenticate the operator from the drone’s WLAN, and connects to the AP of the UAV to hijack it. If the password is complicated, the dictionary attack will fail, but the operator may reconnect to the "false" AP and enter a valid password. In this case the intruder stops both attacks, carries out the deauthentication attack, connects to drone’s AP and gains control of the UAV [10].

Such an attack algorithm is the most appropriate one and gives the best chance of success. Figure 3 shows the block diagram of the combined attack to gain control of the UAV.

Fig. 3. Block diagram of the combined attack to gain control of the UAV.
3.2. Drone’s Control System Denial of Service

When the aim of the attacker is to deliberately cause the DoS of the UAV (resulting in the failure of the drone’s flight missions), they may resort to sequential authentication flood and deauthentication attacks, until the goal is reached. The presence, complexity and length of the AP (network) password are irrelevant [11]. Figure 4 shows the block diagram of the combined DoS attack on the AP of the drone.

![Block Diagram of Combined DoS Attack](image)

**Fig. 4.** Block diagram of the combined DoS attack on the AP of the drone.

4. Protection Strategy

Based on the scenario analysis, the following protection strategy is proposed:

1. Given the minimum and the maximum password length of 8-63 characters, the password should consist of 16 and more characters, including lowercase and uppercase Latin letters, numbers and special characters. The use of a complex password minimizes the probability of a successful dictionary attack and ensures maximum resistance to brute force cracking.

2. When operating the UAVs, it is recommended to deploy a workstation running Linux OS and installed Waidps-type software capable of identifying duplicate wireless networks with the same BSSID, as well as mass injection of dissociation/authentication/deauthentication frames into the protected WLAN. The deployed software should be able to promptly notify the drone’s operator of all such cases. The use of such workstations will leave no opportunity to conduct the "Evil Twin" attacks, and will prevent and/or reduce the possible damage during DoS attacks on the UAV’s AP [12, 13].

3. The operator’s smartphone used to control the drone must operate under the latest versions of the OS (Android or iOS). It is also recommended to install officially distributed patches and updates that address newly identified vulnerabilities.

5. Conclusion

The paper considered the main attack scenarios aimed at gaining control of a consumer-grade unmanned aerial vehicle (such as DJI Tello) or cause its denial of service. Based on the results of the analysis, a protective strategy has been proposed. It provides the maximum possible security (based on the drone’s...
technical characteristics) and involves both passive actions (strong Wi-Fi password), and active measures (monitoring the injection of deauthentication/authentication flooding frames and the creation of duplicate networks).

Acknowledgement

The reported study was partially funded by RFBR, project number 19-08-00331.

References

[1] DJI Ryze Tello UAV User Manual 2018 Available from https://dl-cdn.ryzerobotics.com/downloads/Tello/20180404/Tello_User_Manual_V1.2_EN.pdf

[2] Ghanem M C and Ratnayake D N 2016 Enhancing WPA2-PSK Four-way Handshaking after Re-authentication to Deal with De-authentication Followed by Brute-Force Attack a Novel Re-authentication Protocol 2016 Int. Conf. On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA) (London) (IEEE) p 1–7

[3] Agarwal M, Biswas S and Nandi S 2015 Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach 2015 IEEE Int. Conf. on Systems, Man, and Cybernetics (Kowloon) (IEEE) p 246–251

[4] Elhigazi A, Razak S A, Hamdan M, Mohammed B, Abaker I and Elsafi A 2020 Authentication Flooding DOS Attack Detection and Prevention in 802.11 2020 IEEE Student Conf. on Research and Development (SCoReD) (Batu Pahat) (IEEE) p 325–329

[5] Chang T, Lin J, Chen C and Lai G 2018 The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual? 2018 IEEE Conf. on Dependable and Secure Computing (DSC) (Kaohsiung) (IEEE) p 1–4

[6] Asaduzzaman M, Majib M S and Rahman M M 2020 Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack 2020 IEEE Region 10 Symposium (TENSYMP) (Dhaka) (IEEE) p 1704–1707

[7] Juhász K, Póser V, Kozlovzsky M and Bánáti A 2019 WiFi Vulnerability Caused by SSID Forgery in the IEEE 802.11 Protocol 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI) (Herlany) (IEEE) p 333–338

[8] Fehér D J and Sandor B 2018 Effects of the WPA2 KRACK Attack in Real Environment 2018 IEEE 16th Int. Symposium on Intelligent Systems and Informatics (SISY) (Subotica) (IEEE) p 000239–000242

[9] Vanhoef M and Piessens F 2017 Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 CCS '17: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security (Dallas) (New York: Association for Computing Machinery) p 1313–1328

[10] Liu Y, Jin Z and Wang Y 2010 Survey on Security Scheme and Attacking Methods of WPA/WPA2 2010 6th Int. Conf. on Wireless Communications Networking and Mobile Computing (WiCOM) (Chengdu) (IEEE) p 1–4

[11] Abo-Soliman M A and Azer M A 2017 A Study in WPA2 Enterprise Recent Attacks 2017 13th Int. Computer Engineering Conf. (ICENCO) (Cairo) (IEEE) p 323–330

[12] Noh J, Kim J, Kwon G and Cho S 2016 Secure Key Exchange Scheme for WPA/WPA2-PSK Using Public Key Cryptography 2016 IEEE Int. Conf. on Consumer Electronics-Asia (ICCE-Asia) (Seoul) (IEEE) p 1–4

[13] Wang S-L, Wang J, Feng C, Pan Z-P 2016 Wireless Network Penetration Testing and Security Auditing ITM Web Conf. 7 03001 p 1-5