OTAC review task

Drone Security Analysis Report

September, 2021

Center of Security Primitives for Unmanned Vehicles
School of Cybersecurity, Korea University

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

Table of contents

List of tables

List of figures

1 Analysis of drone network protocol

1.1 MAVLink

STX (`0xFD`)	LEN	INC FLAGS	CMP FLAGS	SEQ	SYS ID	COMP ID	MSG ID 3 bytes	PAYLOAD 0–255 bytes	CHECKSUM 2 bytes

Figure 1.1: Structure of MAVLink 2.0 frame

MAVLink (Micro Air Vehicle Link) is a messaging protocol used for communication between ground control systems (GCS) and aircraft, or between devices within a aircraft. Figure 1.1 shows the MAVLink 2.0 frame structure. Nodes interpret PAYLOAD based on MSG IDs, and various message types for basic drone operations are predefined. Unfortunately, some attackers can generate false messages because security is not considered in the MAVLink design.

1.2 Communication of unmanned vehicles

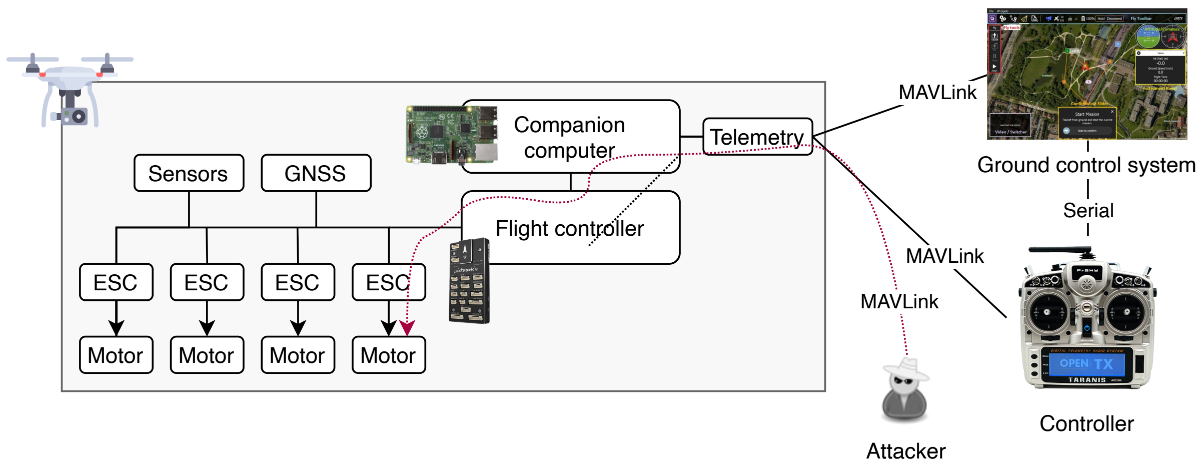


Figure 1.2: Drone network components and network topology

Figure 1.2 shows a network topology of the unmanned mobile network. The network consists of a drone body, a ground control system, and a controller, typically controlled by a GCS or a controller. Each node communicates with each other based on the MAVLink protocol. The differences between ground control systems and controllers are as follows.

GCS The GCS is used for various purposes such as drone monitoring, way-point-based drone control, and drone configuration. The GCS interprets the information (geographical position, altitude, attitude, battery remaining capacity, etc.) that the drone periodically transmits and displays on the screen in an easy-to-read form. The driver can also use the GCS to configure an environment in which a drone performs its own mission without a controller while inputting a specific way-point into the drone in advance.

Controller The controller is used to control the drone's movement instantly. Typically, the controller has a joystick corresponding to four channels: throttle, yaw, pitch, raw, and the value of the joystick controlled by the driver is transmitted to the drone in the form of a PWM signal.

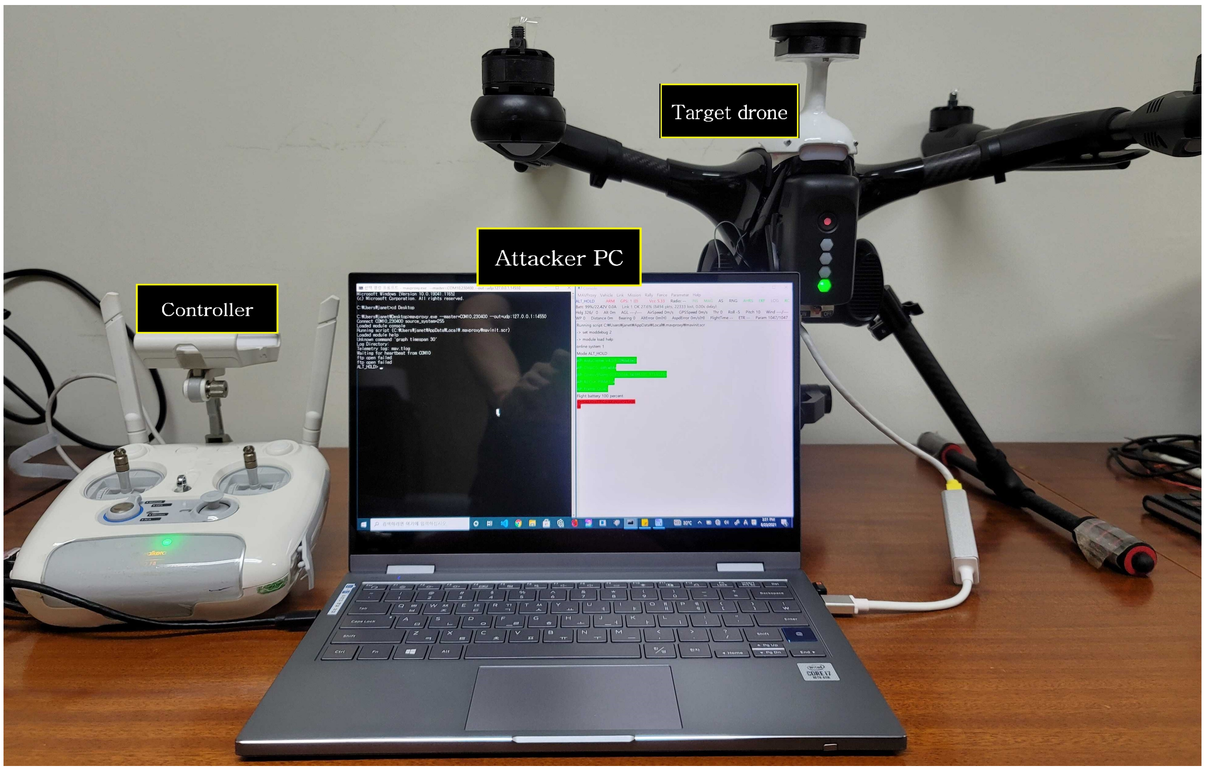


Figure 1.3: Experimental setup

1.3 Attackers disguised as GCS or controls

Figure 1.3 shows the composition of the experimental environment, including attackers. Attackers who have access to the drone network can sniff MAVLink messages generated by network nodes (drone, GCS, controller, etc.) or directly generate MAVLink messages and send them to specific nodes. In this work, the controller was controlled via MAVProxy[1] on the attacker PC to implement attackers infiltrating the drone network. Using python library pymavlink[2], the attack message was implemented and delivered to the controller to send the attack message to the drone. The type of attack and the effect of the attack are as follows.

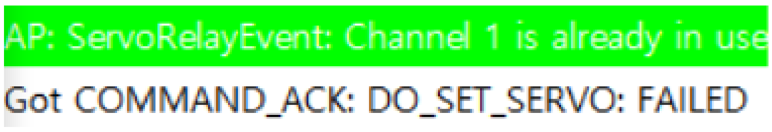
ARM/DISARM We injected the `MAV_CMD_COMPONENT_ARM_DISARM` command and confirmed that the drone could be started or powered off at random.

PWM Value Injection We randomly generated channel PWM values and injected them into drones. Figure 1.4a shows an attacker attempting a channel PWM value injection attack on his PC. The drone normally received an attack message, but in this experimental environment, the effect of the attack was not substantial because the controller already occupied all the channels.

Overriding mission We have confirmed that we can extract way-points registered in drones or delete arbitrary way-points. Figure 1.4b shows pre-defined way-points extracted from the target drone.

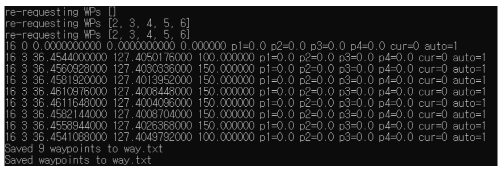
Denial-of-service attack By flooding MAVLink command such as `HEARTBEAT`, `PING`, and `PARAM_REQUEST_LIST` commands, we have confirmed that drones could be overloaded by the flooding. If a drone is overloaded, it can lead to the denial of service.

[1] https://ardupilot.org/mavproxy/
[2] https://github.com/ArduPilot/pymavlink



```
AP: ServoRelayEvent: Channel 1 is already in use
Got COMMAND_ACK: DO_SET_SERVO: FAILED
```

(a) Channel PWM injection attack



```
re-requesting WPs []
re-requesting WPs [2, 3, 4, 5, 6]
re-requesting WPs [2, 3, 4, 5, 6]
16 0 0.0000000000 0.0000000000 0.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4544000000 127.4050176000 100.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4560928000 127.4030336000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4581920000 127.4013952000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4610976000 127.4008448000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4611648000 127.4004096000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4582144000 127.4008704000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4558944000 127.4026368000 150.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
16 3 36.4541088000 127.4049792000 100.000000 p1=0.0 p2=0.0 p3=0.0 p4=0.0 cur=0 auto=1
Saved 9 waypoints to way.txt
Saved waypoints to way.txt
```

(b) Way-point disclosure attack

Figure 1.4: Simulation results of the attacks.

1.3.1 Analysis result

This study confirmed that an attacker could gain various means of controlling Remocopter 500 drones if the attacker has access to the drone network and is able to inject MAVLink commands. The experiment shows that the attack can arm and disarm drones, manipulate way-points, and cause overloads.

2 OTAC Security Analysis

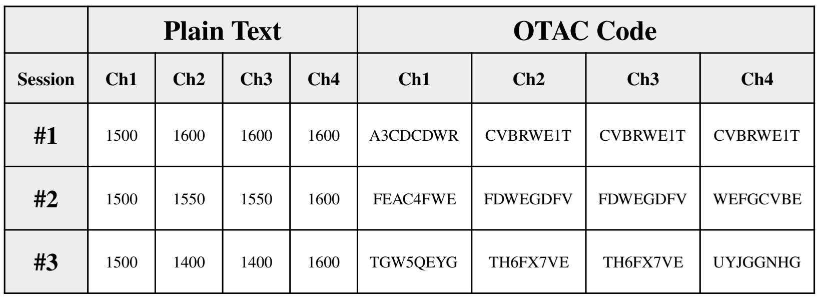
2.1 OTAC Packet Analysis

2.1.1 Packet Analysis

OTAC code generation algorithm transforms 16bit length plain text into 80bit length OTAC code. The plain text corresponds to a command used for flight control and 2 bytes from 80 bit OTAC code have 0x0000 as prefixed value. As a result of parsing pairs of plain text and OTAC code, commands from a controller are sent via 4 channels and all the channels generate OTAC code by using a same seed. In other words, OTAC code C correspond to plain text M was identical over all 4 channels in the code update period. In addition to this, we could confirm OTAC code C correspond to plain text M has a prefixed value over the code update period. However, due to the short code update period, it is hard for an attacker to inject a meaningful attack message into the drone. Figure 2.1a shows plain text and corresponding OTAC code.

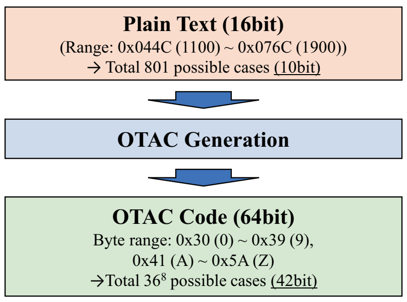
A drone's control command with plain text ranges from 1100 to 1900 with a decimal value; thus control command can be varied by 801 different ways.

Each byte from OTAC uses a value between 0 and 9 from ASCII code and capitalized alphabet character between A to Z. OTAC code. Each byte of the OTAC code has 36 cases and 8 bytes excluding prefixed 2 bytes can have 36^8 cases. Figure 2.1b shows OTAC code generating process obtained by the packet analysis.



	Plain Text				OTAC Code			
Session	Ch1	Ch2	Ch3	Ch4	Ch1	Ch2	Ch3	Ch4
#1	1500	1600	1600	1600	A3CDCDWR	CVBRWE1T	CVBRWE1T	CVBRWE1T
#2	1500	1550	1550	1600	FEAC4FWE	FDWEGDFV	FDWEGDFV	WEFGCVBE
#3	1500	1400	1400	1600	TGW5QEYG	TH6FX7VE	TH6FX7VE	UYJGGNHG

(a) Example of captured packets


Plain Text (16bit)
(Range: 0x044C (1100) ~ 0x076C (1900))
→ Total 801 possible cases (10bit)
OTAC Generation
OTAC Code (64bit)
Byte range: 0x30 (0) ~ 0x39 (9),
0x41 (A) ~ 0x5A (Z)
→Total 36^8 possible cases (42bit)

(b) Overall OTAC generation process

Figure 2.1: Packet analysis result

Plain text inputs are represented by 801 decimal numbers in the range of 1100 to 1900, which shows a 10 bit level of diversity. Each byte of OTAC code uses one of the 36 ASCII codes to be represented. As a result, an 8 byte OTAC code has 36^8 possible cases. This refers to 8 byte OTAC code has a 42bit level of output diversity.

2.1.2 Randomness Assessment based on entropy

In this study, randomness evaluation is performed based on the entropy of the OTAC code. Specifically, the randomness is analyzed by measuring the entropy of the 64-bit OTAC code generated in each session. For this, OTAC codes corresponding to the same plaintext were collected during 425 OTAC code update cycles. Specifically, the OTAC code corresponding to plaintext 1500, which is the command corresponding to the initial value, among the entire range of commands that the manipulator can transmit was collected. Table 2.2 shows the

Table 2.1: Entropy-based randomness test result per sample

	Approximate Entropy Test	Cumulative Sums (Cusum) Test
Mean	1.00E+00	5.15E-01
TRUE	425	425
FALSE	0	0

bit values for each index of the OTAC code collected during the 425 OTAC code conversion cycles used in this analysis. The entropy-based randomness evaluation consists of the Approximate Entropy Test and the Cumulative Sums (Cusum) Test. Table 2.1 shows the entropy evaluation result. Mean of Table 2.1 is the average of individual randomness test output values, and True/False shows whether OTAC codes judged based on the output value passed entropy-based randomness.

As a result of entropy-based randomness test, OTAC was analyzed to have sufficient randomness in terms of entropy.

Table 2.2: An OTAC code sequence during 425 code update periods corresponding to the plain text ‘0x05DC’

Bit index	Bit sequence
0	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
1	11011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111
2	00100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000
3	00101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011
4	00010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000
5	01001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111
6	00010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011
7	10111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100
8	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
9	1111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111
10	0000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
11	1111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
12	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000
13	1011010101110010000001100000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111110011101111011010101110010000001100000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111110011101111011010101110010000001100000
14	0100101010001101111110111111111111111111111111111111111111111110011101111011010101110010000001111111111111111111111111111111111111111111111111111111111111111111111111111110011101111011010101110010000001111110011101111011010101110010000001100001100010000100101010001101111110111111111111111111111111111111111111111110011101111011010101110010000001111111111111111111111111111111111111100001100010000100101010001101111110011110
15	0100101010001101111110011110011101111011010101110010000001100001100010000100101010001101111110011110011101111011010101110010000001111110011101111011010101110010000001100001100010000100101010001101111110000001100010000100101010001101111110000001100010000100101010001101111110011110011101111011010101110010000001100001100010000100101010001101111110011110011101111011010101110010000001100001100010000100101010001101111110000001
16	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
17	01111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101011111001111010111011111111111000101
18	10000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010100000110000101000100000000000111010
19	10111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110101011110111111101100000000001111110
20	00010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000010110000010010000010011101010011000
21	10000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100000101110000100111001010111100100100
22	11100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101111110011100000011111000001000100101
23	00100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111000100100100010100111110010011101111
24	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
25	1111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111010100000110000101000100100000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111
26	0000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000101011111001111010111011011111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
27	0000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000101011111001111010111011011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
28	0000000000000000000000111010100000110000101000100100000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000101011111001111010111011011111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
29	1111111111111111111111000101011111001111010111011011111111111010100000110000101000100100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111010100000110000101000100100000000111111 1
30	1111111111111111111111000101011111001111010111011011111111000101011111001111010111011011111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111010100000110000101000100100000000111010100000110000101000100100000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000101011111001111010111011011111111 1000000
31	1000010100010010000000000101011111001111010111011011111111000101011111001111010111011011111111111010100000110000101000100100000000111010100000110000101000100100000000111111111111111111111111111111111111000101011111001111010111011011111111000101011111001111010111011011111111111010100000110000101000100100000000111010100000110000101000100100000000111010100000110000101000100100000000000101011111001111010111011011111111 1111010
32	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
33	10111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110101111110111111101100110101001111110
34	01000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001010000001000000010011001010110000001
35	11000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011110000111000101010111101010110111011
36	00110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100010011000110010101010100000000011100
37	10011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100001110110011110010001001000011100100
38	10000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000101010010000010101100111011111100000
39	00011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011001011100011000001111000111010101011
40	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
41	1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
42	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
43	1111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111
44	1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
45	0000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111
46	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111 1
47	0000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000 0
48	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
49	11111111011001000010011111111011111111111111101100100001001111111101111111111111110110010000100111111110111111111111111011001000010011111111011111111111111101100100001001111111101111111111111110110010000100111111110111111111111111011001000010011111111011111111111111101100100001001111111101111111111111110110010000100111111110111111111111111011001000010011111111011111111111111101100100001001111111101111111111111110110010000100111111111
50	00000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000100000000000000100110111101100000000
51	11000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001110000111000100010111111110110111001
52	01010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111000010001010011101000110100000000111
53	10100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010011011010100011000010001000011111010
54	00111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111010101100111101010011000000000011111
55	01011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010001011101011000001111010011010101010
56	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
57	1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000001000000001000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
58	0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111110111111110111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
59	1111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111110111111110111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111
60	0000000000000000000000111110111111110111111111111111111111111111111111111111111111111111111111000001000000001000000000000000000000000001000000001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111110111111110111111111111111111111000000000000000000000000000000000000000000
61	1111111111111111111111000001000000001000000000000000000000000000000000000000000000000000000000000001000000001000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111000001000000001000000000000000000000111110111111110111111111111111111111111111 1
62	1111111111111111111111000001000000001000000000000000000000111111111111111111111111111111111111000001000000001000000000000000000000000001000000001000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111110111111110111111111111111111111111111111111111111111111111111111111111111111110111111110111111111111111111111000001000000001000000000000000000000000001000000001000000000000000000000000000 0
63	1011111111111111111111000001000000001000000000000000000000111110111111110111111111111111111111000001000000001000000000000000000000000000000000000000000000000000000000111110111111110111111111111111111111111110111111110111111111111111111111000001000000001000000000000000000000111110111111110111111111111111111111000001000000001000000000000000000000000001000000001000000000000000000000000001000000001000000000000000000000 1111101

2.2 Code predictability analysis

2.2.1 Attack Model

Since the relationship between the plain text and the OTAC code is maintained only within the code update period, the attacker performs the analysis based on the OTAC code pair with the given plain text within the code update period. The attacker then uses the OTAC codes collected from the new code update period to generate valid OTAC codes for the same code update period. Figure 2.2 shows an attack process suggested in this paper. **In summary, the attacker aims to generate new valid OTAC codes within the code update period by exploiting the given OTAC codes.**

The goal of an attacker assumed in this study is generating a valid OTAC code C' within the code update period, using a given OTAC code C. The attacker can inject a valid control command into the target drone during the code update period by using a valid OTAC code of C'. Through the attack, the attacker can increase $\frac{2^{10}}{2^{42}} = \frac{1}{2^{32}} \approx 2.32 \times 10^{-10}$ which is probability of finding a valid control command in the OTAC code space via random guessing.

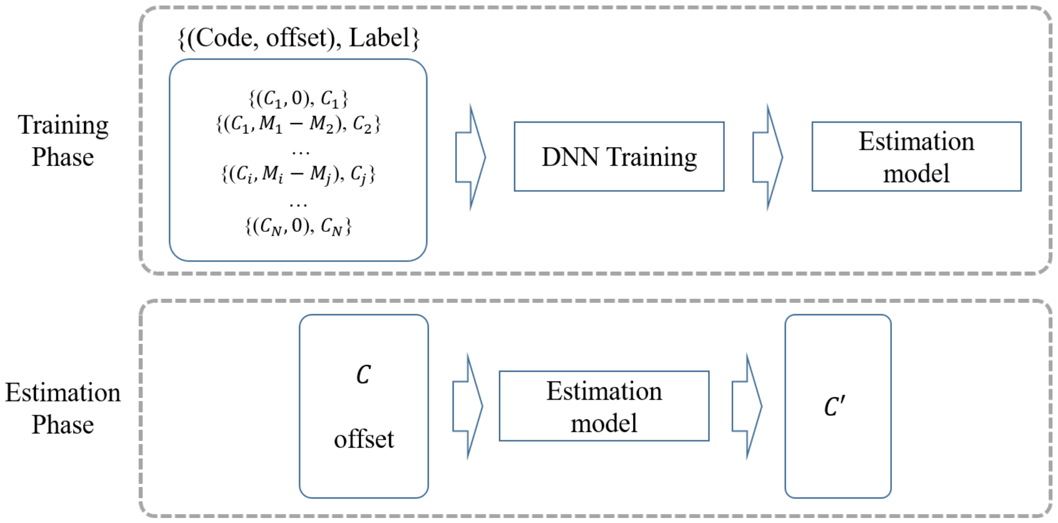


Figure 2.2: Training and estimation process

2.2.2 Analysis Method

Given the OTAC code c_i corresponding to the plain text m_i in code update period S_i, if c'_i corresponding to m'_i is generated, an attacker can send commands to the drone corresponding to m'_i. Therefore, to learn the relationship between the offset of the plain text and the code change, we train a DNN model that outputs c'_i by taking m_i, offset of m'_i, and c_i as input. Various plain texts are required for learning code change using offset and data is collected through as many manipulations as possible during the code update period. Since the code generation method changes from code update period to code update period, the offset is only calculated within the code update period by segmenting the data into code update periods. Within a single code update period, multiple identical commands are included. Since the offset and code change from the identical plain text are the same, we perform a redundancy check to use only different plain texts. For the entire code update period, we collect training data from each code update period by calculating offset and 64 bit binary codes by 1 by 1 matching, and we earn a total number of 189,596 training data pairs. Figure 2.3 shows distributions of plaintext control commands and offsets corresponding to used codes while training the DNN model.

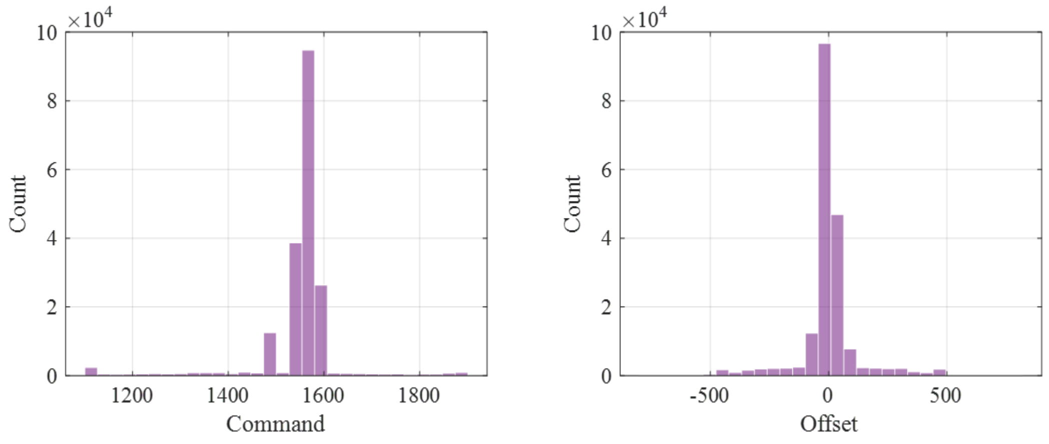


Figure 2.3: Training data distribution

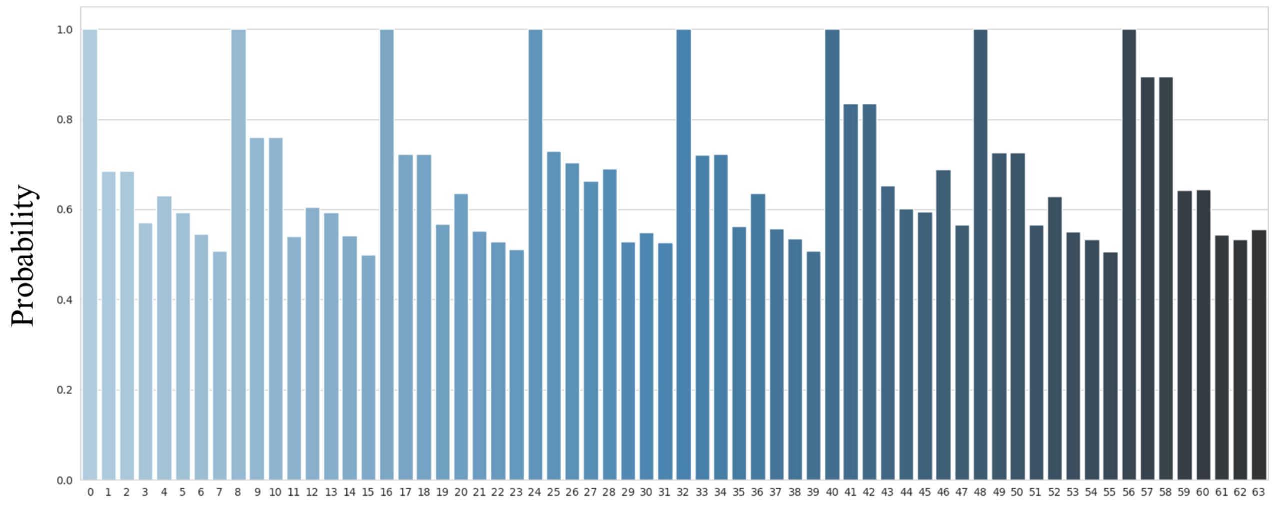


Figure 2.4: Estimation success probability according to bit position

2.2.3 Analysis result

Output values of the DNN model were rounded to be classified into 0 and 1 for the performance evaluation of the DNN model and we evaluated the predictive accuracy of individual bits. Figure 2.4 shows 64 cases of bit-specific prediction accuracy. The prediction accuracy of the top bits of each byte is 1 because the ASCII code range of the OTAC code was limited to numeric and uppercase alphabets. Specifically, the top 4 bits of the ASCII code have 0x3, 0x4, 0x5, so the highest bit is fixed at zero, and the remaining top 3 bits also have a relatively high probability of predictive success because they have low entropy. However, for the lower 4 bits, we expect to the prediction accuracy would have a level of a random guess because the prediction accuracy was near 0.5. Thus, this study confirmed that OTAC code is safe for code predicting attacks based on deep learning.

DNN model succeeded in predicting the portion of entire bits with a relatively high probability because the limited area was used among 64-bit spaces which is the output size of the OTAC code generation algorithm. However, since about half of the bits have predictive accuracy near 0.5 which is corresponding to the level of random guessing, we can expect OTAC code to be safe for code predicting attacks.

3 Assess the possibility of network-level attacks after applying OTAC

3.1 OTAC message analysis

The Remocopter 500 drone prototype analyzed in this study communicates with the controller based on the OTAC ciphertext. To do this, OTAC developers newly defined customized MAVLink messages with MSG ID values of 1050. The structure of the Customized MAVLink message is shown in Table 3.1. The fields ch1, ch2, ch3, and ch4 contain raw PWM values generated by joystick of the controller. The fields rollstream, pitchstream, throttlstream, and yawstream contain ciphertexts of PWM values for each channel with OTAC technology. When enabling encryption mode, the controller and drone communicate based on encrypted control commands.

Table 3.1: Structure of customized OTAC MAVLink message

Field name	validotacmodecmd	otacmodecmd	ch1	ch2	ch3	ch4	ch5	ch6	ch7	ch8	reserved	controlcameramode	rollstream	pitchstream	throttlestream	yawstream
Byte index	0	1	2	4	6	8	10	12	14	16	18	20	22	32	42	52
Type	byte	byte	uint16	uint16	uint16	uint16	uint16	uint16	uint16	uint16	uint16	uint16	byte array	byte array	byte array	byte array
Example value (Hex)	0x01	0x02	0x044C	0x05DC	0x05DC	0x05DC	0x05DC	0x05DC	0x0100	0x0000	-	0x0001	0x3736384B343836390000	-	-	-
Example value (Integer)	1	2	1100	1500	1500	1500	1500	1500	256	0	-	1	-	-	-	-
Example value (ASCII)	-	-	-	-	-	-	-	-	-	-	-	-	768K4869	-	-	-

3.2 Evaluating the OTAC-based MAVLink communications

We attempted a replay attack to verify the security of the OTAC technology applied to the customized MAVLink messages. The reply attack is an attack that pre-collects and copies a number of ciphertexts from a benign stream and then retransmits them to the target node to obtain the validity of the cipher data without trying to decode them. Each attack was attempted before and after activation of encryption mode, and the drone was observed.

The replay attacks did not affect the drone's operation regardless of encryption mode was enabled or not. Given that the message generated by the replay attack was not observed in the communication channel between the controller and the drone, the replay message did not successfully reach the drone due to the limitations of the drone network environment configured in this study.

The controller generates ten customized MAVLink messages per second and updates the OTAC seed every 10 seconds. An attacker cannot collect enough ciphertexts to affect the operation of the drone, as only data observed for up to 10 seconds can be utilized for the retransmission. Therefore, OTAC can be an effective defense against replay attack.

3.3 Analysis result

We confirmed that the attacker could not affect the drone by retransmitting a message protected by the OTAC and that the OTAC was effectively protecting the control command. However, as shown in Section 1.3, it was confirmed that functions not protected by OTAC could be easily affected by attackers disguised as controllers.Therefore, the scope of OTAC should be extended across drone network communication. If OTAC is applied to all kinds of MAVLink messages, it will significantly improve the security of internal and external communication of drones.

4 Conclusion

This report discussed whether OTAC-based encryption communication technology, which was applied in the MAVLink protocol-based wireless communications between a GCS/controller and a drone, can improve security in inter-vehicle communications. MAVLink is used not only for open-source drones but also for various commercial vehicles as it includes various functions for unmanned vehicles. However, it is vulnerable from a security perspective and is unprotected in attacks such as arbitrary command injection, message forgery and reuse. To overcome these limitations, OTAC technology is applied to MAVLink message payload for drones and pilots to be analyzed in this report.

In order to analyze the OTAC-enabled MAVLink communication, this report evaluated MAVLink packet analysis with OTAC, entropy-based randomness, code predictability, and message re-usability. If the attack model exploits the MAVLink command function without OTAC, we confirmed that attacks can turn off and on drones, manipulate way-points, and attacks that cause abnormal loads inside drones are possible. However, for PWM values between pilots and drones protected by OTAC, it was impossible to falsify or replay messages through the proposed attack model.

The encryption code (i.e., the OTAC command) provides the following security improvements:

High-entropy randomness We confirmed that OTAC messages have sufficient randomness from an entropy test perspective.

Code unpredictability We confirmed that OTAC messages are unpredictable.

Unreusable message We confirmed that OTAC messages can prevent replay attacks.

In conclusion, replacing the existing MAVLink control commands with OTAC-based commands can provide security improvements and thus prevent network-level drone hijacking.