OTAC review task

드론 보안성 분석 보고서

September, 2021

고려대학교 정보보호대학원
무인이동체보안연구센터

KOREA UNIVERSITY

고려대학교 정보보호대학원
Korea University
School of Cybersecurity

Table of contents

List of tables

List of figures

1 Drone network protocol 분석

1.1 MAVLink 개요

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)는 À Á 통제 Ü ¤ 템(GCS; Ground Control System)과 D 행체 간의 통à 혹은 D 행체 내 € 장 X 간 통à을 위해 ¬ 용되는 T 세 Õ 프로토 \ 이다. Figure 1.1은 MAVLink 2.0의 프레임 구조 | 나 À 낸다. 노드들은 MSG ID | 기 으로 PAYLOAD | Ý 성 또는 해석하 p, 기본적인 드론 운용을 위한 다양한 T 세 À À 입이 미 ¬ 정의되어있다. MAVLink 설계 Ü 보안에 대한 고려가 되어있 À 않아 공격자가 } 게 T 세 À 위/변조할 있다.

1.2 무인이동체 내부 네트워크

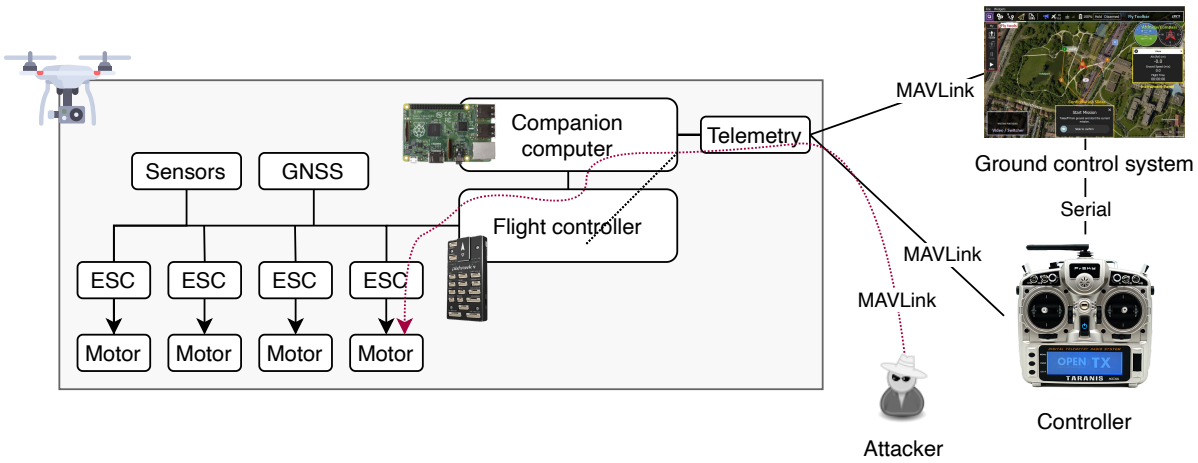


Figure 1.2: Drone network components and network topologies

Figure 1.2는 무인이동체 네 ¸ 워 l 구성도 | 나 À 낸다. 무인이동체 네 ¸ 워 l 는 드론 본체, À Á 통제 Ü ¤ 템, 조종기로 구성되 p 일반적으로 드론은 GCS 또는 조종기에 의해 제어된다. 각 노드는 MAVLink 프로토 \ 을 기반으로 서로 통à 한다. À Á 통제 Ü ¤ 템과 è ¸ 롤러의 차이점은 다음과 같다.

GCS GCS는 드론 ¨ 니터 Á, Way-point 기반의 드론 제어, 드론 환경설정 등 다양한 © 적으로 ¬ 용된다. GCS는 드론이 주기적으로 전송하는 정보 (À ¬ 적 위 X, 고도, 자세 정보, 배터 ¬ 잔량 등) | 해석하고 이 | ¬ 람이 읽기 l 운 형 Ü 로 구성하여 화 t 에 도 Ü 한다. 운전자는 GCS | 활용하여 ¹ 정 Way-point | 미 ¬ 드론에 입력해 두고 조종기 없이 드론이 ¤ ¤ 로 임무 | 행하는 환경을 구성할 도 있다.

조종기 조종기는 드론의 움 Á 임을 Á 접 제어하기 위해 ¬ 용된다. 일반적으로 조종기에는 throttle, yaw, pitch, raw 4개의 채널에 해당하는 조이 ¤ ñ 이 존재하 p, 운전자가 제어하는 조이 ¤ ñ 의 값은 PWM à 호의 형 Ü 로 드론에 전송된다.

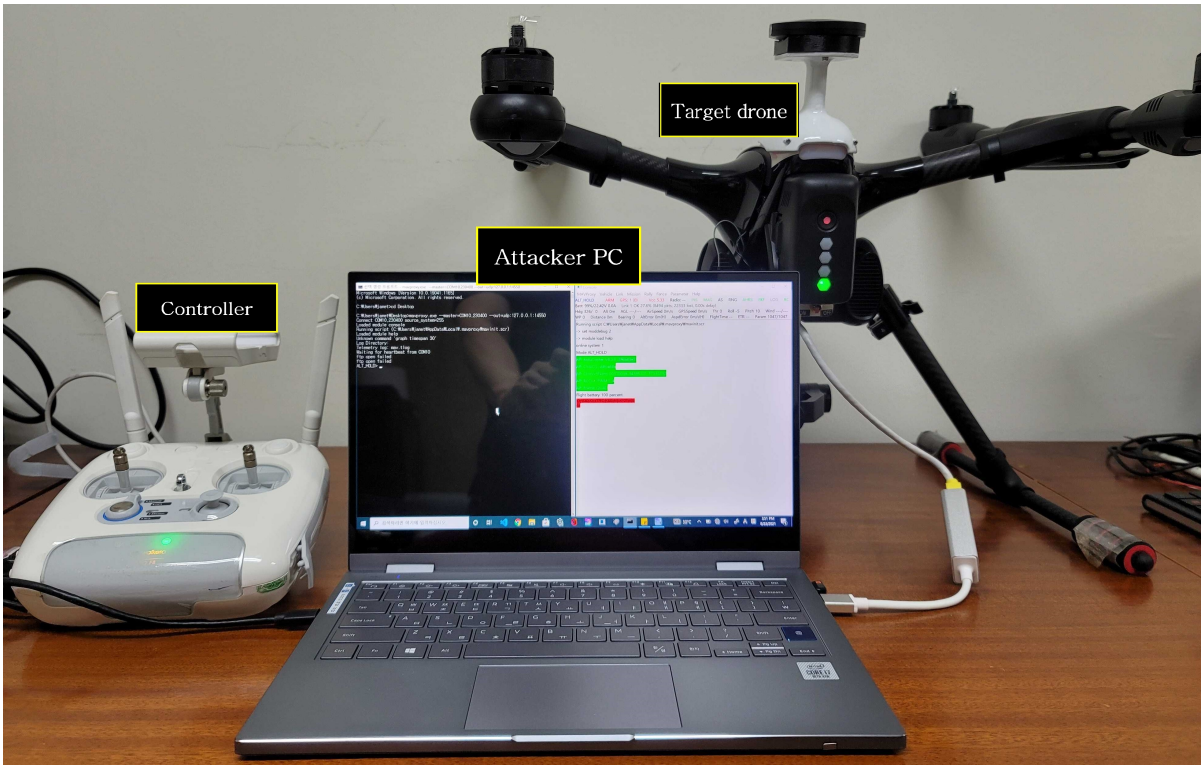


Figure 1.3: Experimental setup

1.3 GCS 또는 조종기로 위장한 공격자

Figure 1.3은 공격자 | ì 함한 ä 험 환경 구성을 나À낸다. 드론 네¸ 워 l 에 h , 한 공격자는 네¸ 워 l 노드들(드론, GCS, 조종기 등)이 Ý 성하는 MAVLink T 세À | ¤ 니핑하거나 Á 접 MAVLink T 세À | Ý 성하여 ¹ 정 노드에게 전송할 있다. 본 연구에서는 드론 네¸ 워 l 에 h , 한 공격자 | 구현하기 위해 공격자 PC에서 MAVProxy[1] | 통해 조종기 | 제어하였다. Python 라이 러¬인 pymavlink[2] | 이용하여 공격 T 세À | 구현하고 이 | 조종기에 전달하여 드론에 공격 T 세À | 전송하였다. 공격의 유형과 공격으로 인한 효과는 아래와 같다.

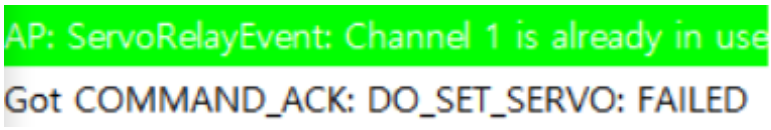
ARM/DISARM `MAV_CMD_COMPONENT_ARM_DISARM` … 령어 | 주입하여 임의로 드론에 Ü 동을 걸거나 Ü 동을 끌 있었다.

조종기 채널 PWM 값 주입 공격 공격자가 채널 PWM 값을 임의로 Ý 성하여 이 | 드론에 주입하였다. Figure 1.4a는 공격자 PC에서 채널 PWM 값 주입 공격을 Ü 도하는 ¨ µ 을 보여다. 드론은 공격 T 세À | 정 Á 적으로 à 하였으나 본 ä 험 환경에서는 이미 조종기가 ¨ 든 채널을 점유하고 있었기 때문에 ä È 적으로 공격의 효과가 나À나À는 않았다.

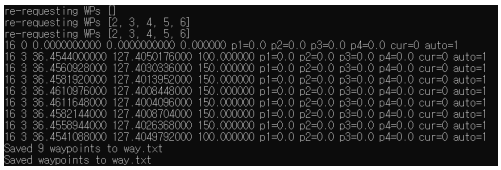
미션 조작 공격 드론에 등록된 Way-point | ″ œ 하거나 임의의 Way-point | - 제할 있었다. Figure 1.4b는 공격자 PC에서 확인한 드론의 Way-point | 나À낸다.

서비스 거부 공격 `HEARTBEAT`, `PING`, `PARAM_REQUEST_LIST` 등의 MAVLink command | 과도하게 전송하여 드론 내 € 에 D 정 Á 적인 € 하 | 일으¬ 있었다.

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



(a) Channel PWM injection attack



(b) Way-point disclosure attack

Figure 1.4: Simulation results of the attacks.

1.4 정리

드론 네¸ 워 l 에 h , 하기 Ì 한다 t 공격자는 Remocopter 500 드론 | 통제할 있는 다양한 단을 얻을 있다는 ¬ ä 을 확인했다. ä 제 ä 험을 통해 드론의 Ü 동을 끄고 는 공격, Way-point | 조작하는 공격, 드론 내 € 에 D 정 Á 적인 € 하 | 발 Ý Ü ¤ 는 공격 등이 가능함을 입 • 했다.

2 OTAC 안전성 분석

2.1 OTAC 패킷 분석

2.1.1 패킷 분석

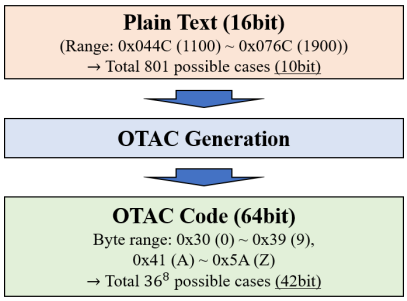
OTAC T 드 Ý 성 알고 ¬ ˜ 은 16 D ¸ 길이의 É 문을 80 D ¸ 길이의 OTAC T 드로 변환한다. É 문 데이터는 드론의 D 행제어에 ¬ 용되는 ... 령어에 해당하 p , 80 D ¸ 의 OTAC T 드 2바이 ¸ 는 0x0000 으로 고정값을 가 À 고 있다. 또한, 제공된 Ü ¬ 얼 ¨ 니터 Á 4 을 활용하여 (É 문, T 드) 을 „ 석한 결과, 조종기의 ... 령은 4개의 채널을 통해 전송되 p , ¨ 든 채널은 공통된 seed | ¬ 용하여 OTAC T 드 | Ý 성하는 것을 확인하였다. 다 Ü Ð 해, OTAC T 드 변환 주기 내에서 É 문 *M* 에 대응되는 OTAC T 드 *C* 는 4개의 채널에서 ¨ 두 동일하였다. 또한, OTAC T 드 변환 주기 내에서는 É 문 *M* 에 대응되는 OTAC T 드 *C* 는 고정값을 가 À 는 것을 확인하였다. 하 À Ì , ç 은 업데이 ¸ 주기로 인해 공격자는 획득한 OTAC T 드 | 이용하여 유효한 공격을 행하기 어렵다. Figure 2.1a 은 É 문과 이에 대응하는 OTAC T 드 | 보여 다.

드론 제어 ... 령인 É 문은 í Ä 1100 € 터 1900까 À 의 범위 | 가 À p , 이는 801가 À 경우의 로 \ 현된다.

OTAC T 드의 개별 바이 ¸ 값은 ASCII T 드에서 0 ~ 9 범위의 í Ä 와 A ~ Z 범위의 대문자 알 벳을 ¬ 용한다. 따라서 OTAC T 드의 개별 바이 ¸ 는 36가 À 경우의 | 가 À p , 고정된 2바이 ¸ | 제외한 8바이 ¸ 는 36^8 가 À 경우의 로 \ 현된다. Figure 2.1b 은 (· „ 석결과에 따 x OTAC T 드 Ý 성 프로세 ¤ | 보여 다.

	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



(b) Overall OTAC generation process

Figure 2.1: Packet analysis result

É 문입력은 1100 ~ 1900 범위의 801가 À í Ä 로 \ 현되 p , 이는 10 D ¸ 의 입력 다양성을 보여 다. OTAC T 드의 개별 바이 ¸ 는 36가 À ASCII T 드 하나 | ¬ 용하여 나 À 내 p , 결과적으로 8바이 ¸ 길이의 OTAC T 드는 36^8 가 À 의 \ 현가능한 경우의 | 가 Ä 다. 이는 42 D ¸ 의 œ 력 다양성을 보여 다.

2.1.2 엔트로피 기반 랜덤성 평가

본 연구에서는 OTAC T 드의 엔 ¸ 로피에 기반한 랜덤성 É 가 | 행한다. 이 | 위해 개별 세션에서 Ý 성된 64 D ¸ 길이의 OTAC T 드의 엔 ¸ 로피 | ! 정하여 랜덤성을 „ 석한다. 이 | 위해 425개의 OTAC T 드 변환 주기동안 동일 É 문에 대응되는 OTAC T 드 | Ñ 하였다. 구체적으로, 조종기가 전송할 있는 전체 ... 령어 범위 , 기값에 해당하는 ... 령어인 1500에 대응하는 OTAC T 드 | Ñ 하였다. Table 2.2 는 본 „ 석에 ¬ 용한 425개의 OTAC T 드 변환 주기동안 Ñ 된 OTAC T 드의 인덱 ¤ 별 D ¸ 값을 보여 다. 엔 ¸ 로피 기반 랜덤성 É 가는 Approximate Entropy Test 및 Cumulative Sums (Cusum) Test로 구성된다. Table 2.1 는 엔

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

¸ 로피 É 가결과 | 보여 다. Table 2.1의 Mean은 개별 랜덤성 테¤ ¸ œ 력값의 É 균이 p, True/False는 œ 력값을 기반으로 단한 OTAC T 드들의 엔¸ 로피 기반 랜덤성 통과 여€ | 보여 다.

엔¸ 로피 기반 T 드 랜덤성 É 가 결과 2개의 테¤ ¸ | ¨ 두 통과하였다. 따라서 **OTAC은 엔트로피 테스트 관점에서 충분한 랜덤성을 가진것으로 분석된다.**

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

Bit index	Bit sequence
0	000
1	11011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111100100111011010100111011101100110111
2	00100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000011011000100101011000100010011001000
3	00101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011011111000101111011001110010011011011
4	00010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000100000100010000101001010100000000000
5	01001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111010011001001010100010001010100100111
6	00010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011001101100010100010110000101010011011
7	10111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100111010110111001111010101101010110100
8	000
9	11111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111
10	00000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
11	11111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000
12	00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111000000
13	10110101011100100000011000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111111111100111011110110101011100100000011000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111100111011110110101011100100000011000000

14	010010101000110111111100111111111111111111111111111111111111111111111110011101111011010101110010000001111111111111111111111111111111111111111111111111111111111111111111111111111111111001110111101101010111001000000111111001110111101101010
15	0100101010001101111111001111001110111101101010111001000000110000110001000010010101000110111111100111100111011110110101011100100000011111100111011110110101011100100000011000011000100001001010100011011111100000011000100001001010
16	00
17	011110101110111111111110001010111110011110101110111111111100010101111100111101011101111111111000101011111001111010111011111111110001010111110011110101110111111111100010101111100111101011101111111111000101011111001111010111011111
18	100001010001000000000001110101000001100001010001000000000001110101000001100001010001000000000001110101000001100001010001000000000001110101000001100001010001000000000001110101000001100001010001000000000001110101000001100001010001000000
19	101111111011000000000011111101010111101111111011000000000011111101010111101111111011000000000011111101010111101111111011000000000011111101010111101111111011000000000011111101010111101111111011000000000011111101010111101111111011000000
20	000100100000100111010100110000101100000100100000100111010100110000101100000100100000100111010100110000101100000100100000100111010100110000101100000100100000100111010100110000101100000100100000100111010100110000101100000100100000100111
21	100001001110010101111001001000001011100001001110010101111001001000001011100001001110010101111001001000001011100001001110010101111001001000001011100001001110010101111001001000001011100001001110010101111001001000001011100001001110010101
22	111000000011111000001000100101111110011100000001111100000100010010111111001110000000111110000010001001011111100111000000011111000001000100101111110011100000001111100000100010010111111001110000000111110000010001001011111100111000000011
23	001000101001111100100111011110001001001000101001111100100111011110001001001000101001111100100111011110001001001000101001111100100111011110001001001000101001111100100111011110001001001000101001111100100111011110001001001000101001111100
24	00
25	111111111111111111111111111111111111111111111111111111111111111100000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111111110101000001100001010001001000000001111111111111111111
26	000000000000000000000000000000000000000000000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000010101111100111101011101101111111100000000000000000
27	000000000000000000000000000000000000000000000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000010101111100111101011101101111111111111111111111111
28	000000000000000000000111010100000110000101000100100000000000000000000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111000101011111001111010111011011111111000000000000000000
29	111111111111111111111000101011111001111010111011011111111111010100000110000101000100100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
30	111111111111111111111000101011111001111010111011011111100010101111100111101011101101111111110000000000000000000000000000000000000000000000000111111111111111111111111111111111111111110000000000000000000000000000001110101000001100001
31	100001010001001000000000010101111100111101011101101111111100010101111100111101011101101111111111101010000011000010100010010000000001110101000001100001010001001000000000111111111111111111111111111111111111111111000101011111001111010
32	00
33	101111111011001101010011111101011111110111111101100110101001111110101111111011111110110011010100111111010111111101111111011001101010011111101011111110111111101100110101001111110101111111011111110110011010100111111010111111101111111011
34	010000000100110010101100000010100000001000000010011001010110000001010000000100000001001100101011000000101000000010000000100110010101100000010100000001000000010011001010110000001010000000100000001001100101011000000101000000010000000100
35	110001010101111010101101110111100001110001010101111010101101110111100001110001010101111010101101110111100001110001010101111010101101110111100001110001010101111010101101110111100001110001010101111010101101110111100001110001010101111010
36	001100101010101000000000111000100110001100101010101000000000111000100110001100101010101000000000111000100110001100101010101000000000111000100110001100101010101000000000111000100110001100101010101000000000111000100110001100101010100
37	100111100100010010000111001000011101100111100100010010000111001000011101100111100100010010000111001000011101100111100100010010000111001000011101100111100100010010000111001000011101100111100100010010000111001000011101100111100100010010

38	10000010101100111011111110000010101001000001010110011101111111000001010100100000101011001110111111100000101010010000010101100111011111110000010101001000001010110011101111111000001010100100000101011001110111111100000101010010000010101100111011
39	00011000001111000111010101011001011100001100000111100011101010101100101110000110000011110001110101010110010111000011000001111000111010101011001011100001100000111100011101010101100101110000110000011110001110101010110010111000011000001111000111
40	00
41	11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111110000000000000000000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000
42	00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001111111111111111111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111
43	11111111111111111111111111111111111111111111111111111111111100000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
44	11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111
45	00000000000000000000000000000000000000000000000000000000000011111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
46	00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001111111111111111111111111111111111110000000000000000000000000000000000
47	00000000000000000000000001111111111111111111111111111111111100000000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000000000000000000000000000000000000000000000
48	00
49	11111111101100100001001111111101111111111111110110010000100111111110111111111111111011001000010011111111011111111111111101100100001001111111101111111111111110110010000100111111110111111111111111011001000010011111111011111111111111101100100001
50	00000000010011011110110000000010000000000000001001101111011000000001000000000000000100110111101100000000100000000000000010011011110110000000010000000000000001001101111011000000001000000000000000100110111101100000000100000000000000010011011110
51	11000100010111111111011011100111000011100010001011111111101101110011100001110001000101111111110110111001110000111000100010111111111011011100111000011100010001011111111101101110011100001110001000101111111110110111001110000111000100010111111111
52	01010011101000110100000000011100001000101001110100011010000000001110000100010100111010001101000000000111000010001010011101000110100000000011100001000101001110100011010000000001110000100010100111010001101000000000111000010001010011101000110100
53	10100011000010001000011111101001101101010001100001000100001111110100110110101000110000100010000111111010011011010100011000010001000011111101001101101010001100001000100001111110100110110101000110000100010000111111010011011010100011000010001000
54	00111101010011000000000001111101010110011110101001100000000000111110101011001111010100110000000000011111010101100111101010011000000000001111101010110011110101001100000000000111110101011001111010100110000000000011111010101100111101010011000000
55	01011000001111010011010101010001011101011100000111101001101010101000101110101110000011110100110101010100010111010111000001111010011010101010001011101011100000111101001101010101000101110101110000011110100110101010100010111010111000001111010011
56	00
57	11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111110000100000000100000000000000000000000111111111111111111111111111111111111000000000000000000000000000000000
58	00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001111011111111011111111111111111111111000000000000000000000000000000000000111111111111111111111111111111111
59	11111111111111111111111111111111111111111111111111111111111100000000000000000000000000000000000000111101111111101111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
60	00000000000000000000000001111011111111011111111111111111111111111111111111111111111111111111111111000010000000010000000000000000000000000000100000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
61	11111111111111111111111110000100000000100000000000000000000000000000000000000000000000000000000000000000100000000100000000000000000000000000100000000100000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111
62	11111111111111111111111110000100000000100000000000000000000011111111111111111111111111111111111111000010000000010000000000000000000000000000100000000100000000000000000000000000000000000000000000000000000000000111111111111111111111111111111111
63	10111111111111111111111110000100000000100000000000000000000011110111111110111111111111111111111111000010000000010000000000000000000000000000000000000000000000000000000000000111101111111101111111111111111111111111011111111011111111111111111111

2.2 코드 예측가능성 분석

2.2.1 공격자 모델

제공된 „ 석환경은 OTAC T 드 Ý 성 알고 ¬ ˜ 에 대한 정보 없이, É 문과 고정된 seed로 € 터 Ý 성되는 OTAC T 드 Ì 을 이용하여 안전성 „ 석을 행한다. É 문과 OTAC T 드의 관계는 동일한 OTAC T 드 변환 주기 내에서 Ì 유 À 되므로, 공격자는 동일한 OTAC T 드 변환 주기내에서 주어 Ä É 문과 OTAC T 드 을 기반으로 „ 석을 행한다. 이후, 공격자는 È 롭게 업데이 ¸ 된 OTAC T 드 변환 주기에서 Ñ 된 OTAC T 드 | 이용하여 해당 OTAC T 드 변환 주기에서 유효하게 ¬ 용가능한 OTAC T 드 | Ý 성한다. Figure 2.2은 본 연구에서 가정한 공격 프로세 ¤ | 보여 다. **정리하면, 공격자는 주어진 OTAC 코드를 활용하여 OTAC 코드 변환 주기내에 사용가능한 새로운 OTAC 코드를 생성하는 것을 목표로한다.**

본 연구에서 가정한 공격자의 © \ 는 주어 Ä OTAC T 드 C | 이용하여, 동일한 OTAC T 드 변환 주기내에 유효한 OTAC T 드 C'을 Ý 성하는 것이다. 유효한 OTAC T 드인 C'을 이용하여 공격자는 동일한 OTAC T 드 변환 주기동안 À 겟 드론에 유효한 제어 ... 령을 주입할 있다. 해당 공격을 통해 공격자는 랜덤 ″ ! (random guessing)을 통해 OTAC T 드 공간에서 유효한 제어 ... 령을 찾을 확 ` 인 $\frac{2^{10}}{2^{42}} = \frac{1}{2^{32}} \approx 2.32 \times 10^{-10}$을 • 가 Ü ¬ 있다.

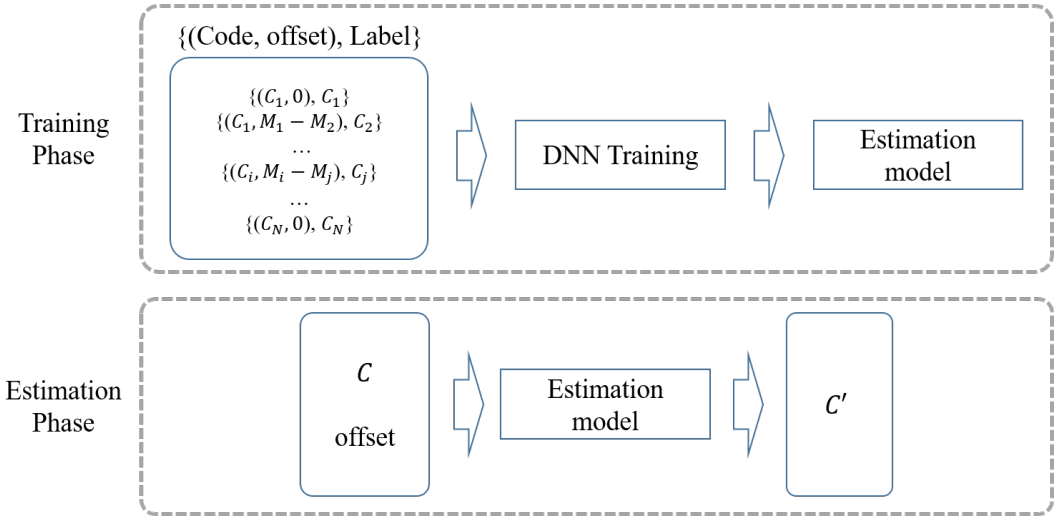


Figure 2.2: Training and estimation process

2.2.2 분석방법

OTAC T 드 변환 주기 S_i에서 É 문 m_i에 대한 OTAC T 드 c_i가 주어졌을때, m_i'에 해당하는 c_i' | Ý 성할 경우, 공격자는 드론에게 m_i'에 해당하는 ... 령을 내 ´ 있다. 따라서 É 문의 오프셋과 T 드 변화의 관계 | 학 µ 하기 위해 m_i와 m_i'의 오프셋과 c_i | 입력으로 받아 c_i'을 œ 력하는 DNN ¨ 델을 학 µ Ü ¨ 다. 오프셋을 이용한 T 드 변화 학 µ 을 위해 다양한 É 문이 필요하 p 동일한 OTAC T 드 변환 주기동안 \ 대한 다양한 조작을 하여 데이터 | Ñ 한다. T 드 Ý 성 방 Ý 은 ä OTAC T 드 변환 주기 È 다 변경되기 때문에 오프셋은 데이터 | OTAC T 드 변환 주기별로 „ 할하여 OTAC T 드 변환 주기 내에서 Ì 계 ° 한다. 단일 OTAC T 드 변환 주기 내에는 동일한 ... 령어도 다 ì 함되어 있으 p 동일한 É 문으로 € 터 발 Ý 하는 오프셋과 T 드변화는 동일하기 때문에 복처 ¬ | 통해 서로 다 x É 문 Ì 을 ¬ 용한다. 전체 OTAC T 드 변환 주기에 대해 각 OTAC T 드 변환 주기별로 1대1 ä m 을 통한 오프셋과 64 D ¸ 이 Ä 로 변형한 전후 T 드 | 계 ° 하여 학 µ 데이터 | Ñ 하였으 p , 189,596개의 학 µ 데이터을 Ñ 하였다. Figure 2.3은 DNN ¨ 델 학 µ 에 ¬ 용된 T 드에 해당하는 É 문 제어 ... 령어 „ ì 및 오프셋 „ ì | 보여 다.

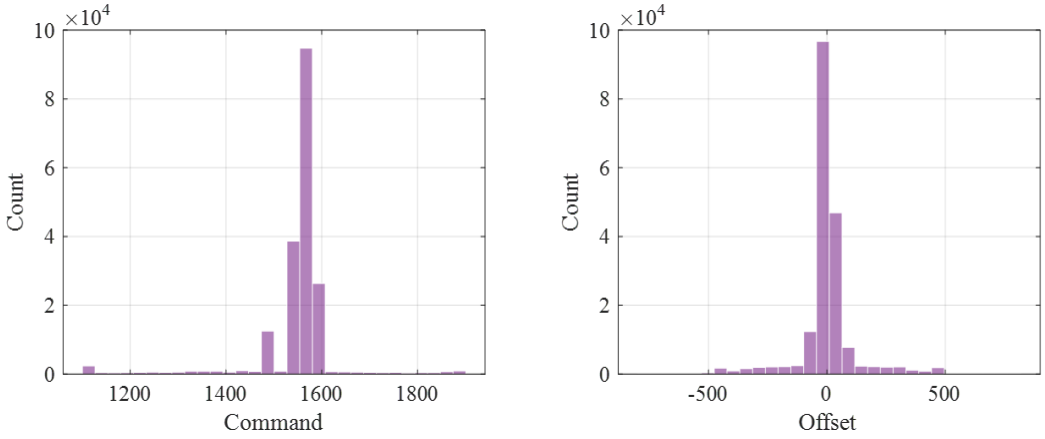


Figure 2.3: Training data distribution

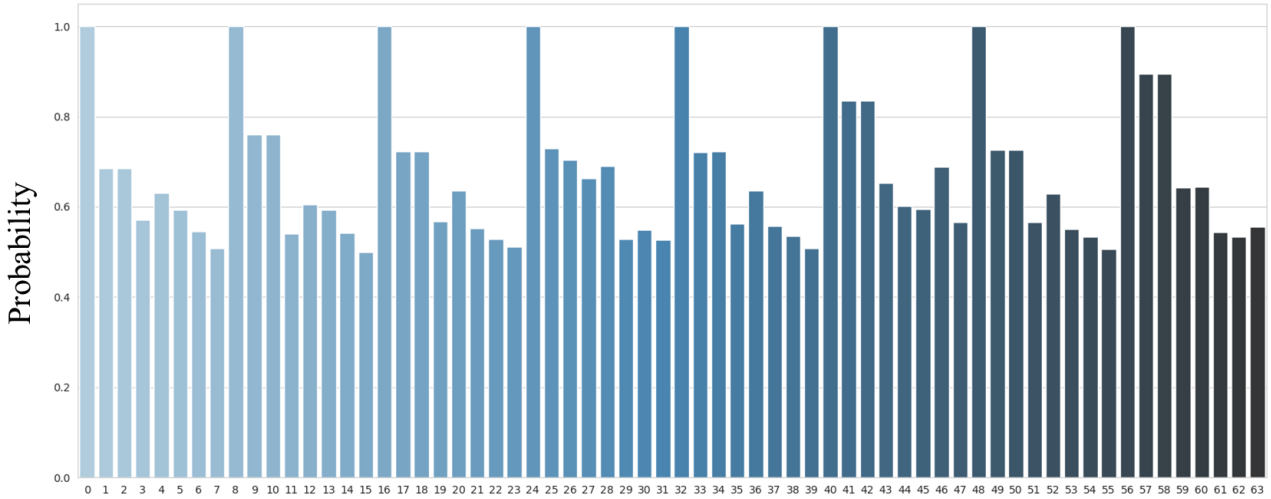


Figure 2.4: Estimation success probability according to bit position

2.2.3 분석결과

DNN ¨ 델의 성능 É 가 | 위해 DNN ¨ 델의 œ 력값을 반올 ¼ 하여 0과 1로 구 „ 하였으 p , 개별 D ¸ 의 예 ! 정확도 | É 가하였다. Figure 2.4은 64개의 D ¸ 별 예 ! 정확도 | 보여 다. 각 바이 ¸ 의 \ Á 위 D ¸ 의 예 ! 정확도가 1인 이유는 OTAC T 드의 ASCII T 드 범위가 + 자 및 대문자 알 벳으로 제한되었기 때문이다. 구체적으로, 해당 ASCII T 드의 Á 위 4 D ¸ 는 0x3, 0x4, 0x5 | 가 À 기 때문에 \ Á 위 D ¸ 는 0으로 고정되어 있는 ¹ 성이 있으 p , 나 8 À Á 위 3 D ¸ 역 Ü 엔 ¸ 로피가 낮기 때문에 Á 대적으로 예 ! 성공 확 ` 이 높게 나 À 났다. 하 À Ì 하위 4 D ¸ 의 경우에는 예 ! 정확도가 0.5 € 근으로 형성이 되었기 때문에 랜덤 ″ ! 의 정확도 | 보였다. 따라서 본 연구에서 가정한 딥러닝 기반의 T 드 예 ! 공격에 안전한 것으로 확인하였다.

OTAC T 드 Ý 성 알고 ¬ ˜ 의 œ 력 l 기인 64 D ¸ 공간 ä 제로 ¬ 용되는 영역이 제한되어 있기 때문에 일 € D ¸ 의 경우 Á 대적으로 높은 확 ` 로 예 ! 에 성공하였다. 하 À Ì , 절반 정도의 D ¸ 는 예 ! 정확도가 0.5 € 근으로 형성되었기 때문에, 이는 랜덤 ″ ! 의 정확도 | 보이기 때문에 T 드 예 ! 공격에 안전하다고 단할 있다.

3 OTAC 적용된 drone network protocol 의 replay attack 분석

3.1 OTAC 적용된 메시지 분석

본 연구에서 „ 석한 Remocopter 500 드론 Ü 제 ˆ 은 OTAC 암호문을 기반으로 조종기와 통 à 한다. 이 | 위해 1050의 MSG ID 값을 갖는 Customized MAVLink T 세 À 가 ¬ 용되고 있음을 확인하였다. Customized MAVLink T 세 À 의 구조는 Table 3.1과 같다. ch1, ch2, ch3, ch4 필드는 조종기 조이 ¤ ñ 으로 € 터 Ý 성된 PWM 값의 É 문을 담고 있다. 그 ¬ 고 rollstream, pitchstream, throttlestream, yawstream 필드는 각 채널 별 PWM 값을 OTAC 기 로 암호화 한 암호문을 담고 있다. Remocopter 500 드론과 조종기에는 암호화 ¨ 드 | 각각 활성화 할 있는 기능이 구현되어 있으 p , 암호화 ¨ 드 | 활성화 할 Ü 조종기와 드론은 암호화된 조종 … 령을 기반으로 통 à 한다.

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	-	-	-

암호화 모드 조종기에서 암호화 ¨ 드가 활성화된 경우 드론 제어 | 위한 É 문 PWM 값이 OTAC로 변경되어 드론으로 송 à 된다. 이 때, 드론에서 암호화 ¨ 드가 활성화된 경우 à 된 데이터 ¤ ¸ ¼ 을 OTAC T 드에서 PWM값이 담긴 É 문으로 변경한 뒤 무결성 검 ¬ | 행한다. 무결성 검 ¬ 에서 이 Á 이 없는경우 계 ° 된 PWM 값이 ä 제 flight controller로 전달된다.

3.2 OTAC 기반 MAVLink 통신 보안 평가

Customized MAVLink T 세 À 에 적용된 OTAC 기 의 보안성을 검 • 하기 위해 재전송 공격(Replay attack)을 Ü 도하였다. 재전송 공격이란 다 의 암호문들을 미 ¬ Ñ 하여 복 ¬ 한 후 이 | 대 Á 노드에 재전송함으로 h 암호문을 복호화 하는 노력 없이 암호 데이터의 유효성을 얻는 공격을 의미한다. 암호화 ¨ 드 활성화 전후 각각 공격을 Ü 도하고 드론의 Á Ü | 관찰하였다.

암호화 ¨ 드 활성화 여 € 와 관계 없이, 재전송 공격은 드론에 D 행에 영향을 주 À » 했다. 조종기는 당 10개의 Customized MAVLink T 세 À | Ý 성하고 10 È 다 OTAC Ü 드가 갱 à 된다. 공격자는 \ 대 10 간 관찰한 데이터 Ì 재전송에 활용할 있으므로 드론의 정 Á 운행에 영향을 있을 Ì | © „ 한 양의 암호문을 Ñ 할 없다. 따라서 OTAC은 재전송 공격으로 € 터 드론을 보호하는 효과적인 방어 단이 될 있다.

3.3 분석 결과

공격자는 OTAC으로 보호되는 T 세 À | 재전송하여 드론에 영향을 없었으 p , OTAC 이 조종 … 령을 효과적으로 보호하고 있음을 확인했다. 하 À Ì Section 1.3에서 알 있듯이, 드론 네 ¸ 워 l 에 h , 하여 GCS 또는 조종기로 위장한 공격자는 드론을 통제할 있는 다양한 단을 À 니게 된다. 따라서 OTAC의 적용 범위 | 드론 네 ¸ 워 l 통 à 전반으로 확장해야한다. ¨ 든 종 X 의 MAVLink T 세 À 에 OTAC을 적용할 경우 드론 내외 € 통 à 의 보안성을 l 게 향 Á Ü ¬ 있을 것으로 보인다.

4 결론

본 보고서는 드론과 조종기 ¬ 이의 MAVLink 프로토 \ 기반 무선통 à Ü OTAC 기반 암호화 통 à 기 을 적용했을 때의 보안성 향 Á 여 € | 검토하였다. MAVLink는 무인이동체 | 위한 다양한 기능 구현이 ì 함되어있어 오픈소 ¤ 드론 뿐 아니라 다양한 Á용 이동체 통 à 에 활용되고 있으나 한 ¸ 으로는 보안 관점에서의 설계가 è 약하여 T Ü À 위변조, 재 ¬ 용과 같은 공격에 무방 D 로 노 œ 되어 있다. 이러한 한계 | 극복하기 위해 본 보고서의 „ 석 대 Á 드론과 조종기는 MAVLink T Ü À payload에 OTAC 기 이 적용되어 있다.

본 보고서는 OTAC 기 이 적용된 드론, 조종기, 그 ¬ 고 MAVLink T Ü À 의 보안성을 „ 석하기 위해 OTAC 이 ì 함된 MAVLink (· „ 석, 엔 ¸ 로피 기반 랜덤성, T 드 예 ! 가능성, replay attack 가능성에 대한 검토 | ä Ü 하였다. 공격 ¨ 델이 OTAC이 적용되어있 À 않은 MAVLink ... 령 기능을 악용하고자 하는 경우 드론의 Ü 동을 끄고 는 공격, Way-point | 조작하는 공격, 드론 내 € 에 D 정 Á 적인 € 하 | 발 Ý Ü ¤ 는 공격 등이 가능함을 확인하였다. 그러나, OTAC에 의해 보호되는 조종기와 드론 ¬ 이의 PWM 값에 대해서는 제안된 공격 ¨ 델을 통해 T Ü À | 위변조하거나 재 Ý (replay)하는 것이 ˆ 가하였다.

OTAC로 변경한 암호화 T 드(‰, OTAC ... 령어)는 다음과 같은 보안성 향 Á 효과 | 제공한다.

OTAC 코드의 엔트로피 기반 랜덤성 OTAC은 엔 ¸ 로피 테 ¤ ¸ 관점에서 © „ 한 랜덤성을 가 Ä 것으로 „ 석됨

OTAC 코드 예측 가능성 정 Á OTAC T 드 기반 È 로운 주기의 정 Á 적인 OTAC T 드 예 ! 가능성이 낮음

Replay 공격 가능성 기전송된 OTAC T 드의 재 ¬ 용되는 Ü 기 예 ! 이 ˆ 가능하여 Replay 공격 차단이 가능함

따라서, 기존의 MAVLink 제어 ... 령을 OTAC 기반 암호화 T 드(‰, OTAC ... 령어)로 대체할 경우, 드론 하이재 ¹ 을 방 À 하는 보안 향 Á 효과 | 가 À 게 되는 것으로 단된다.