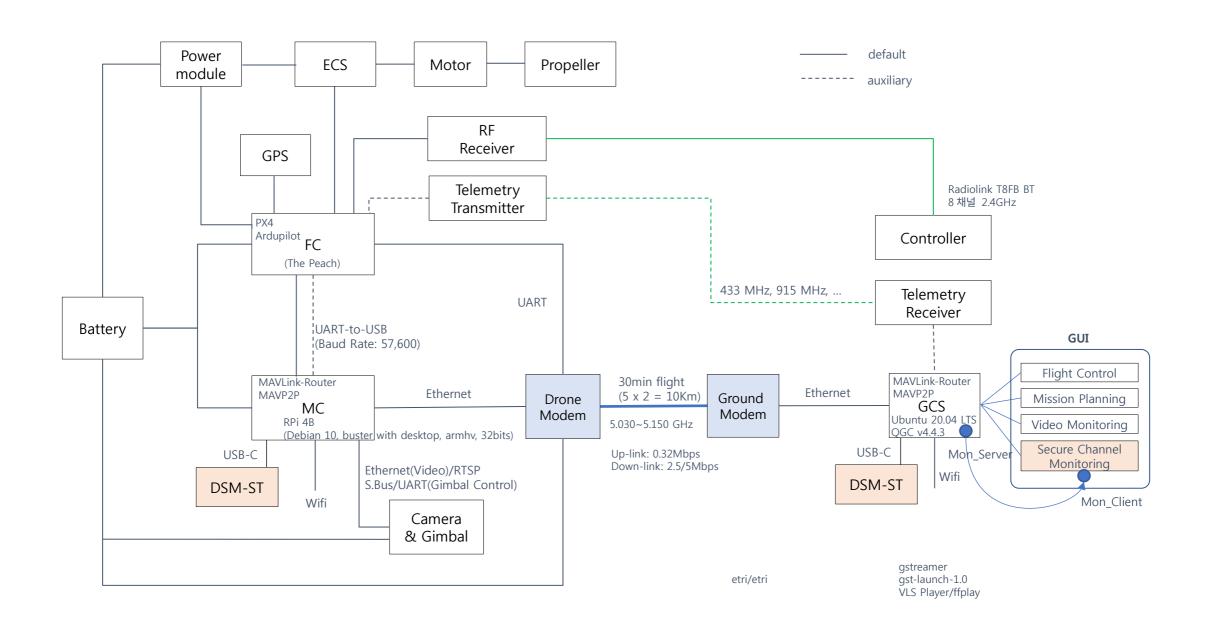
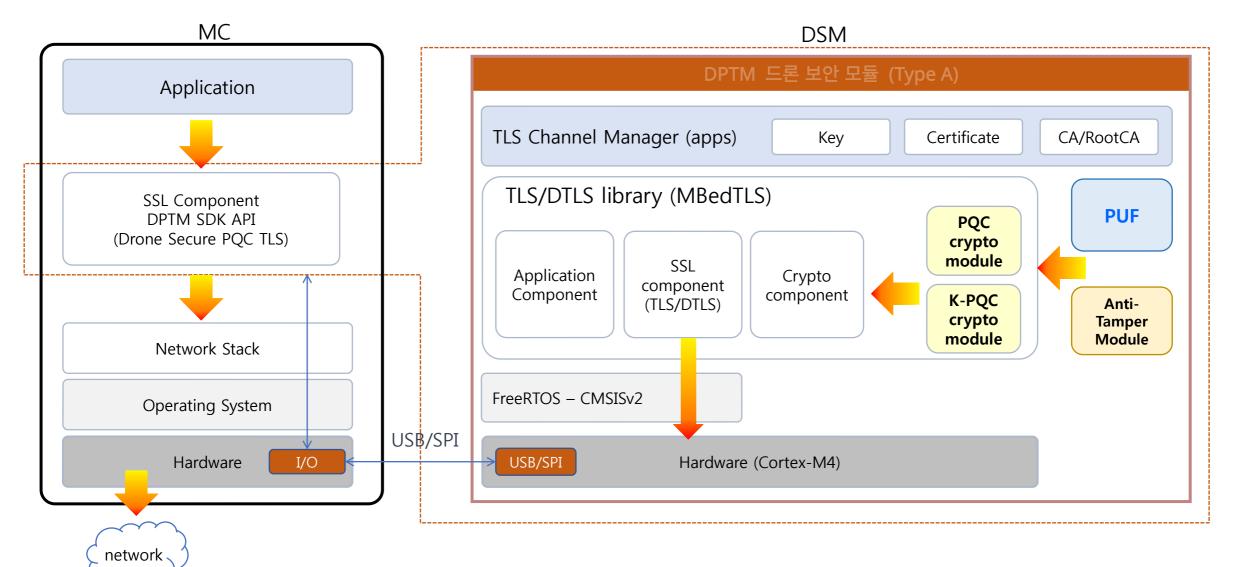
보안채널 모니터링 GUI 설계

(Secure Channel Monitoring)

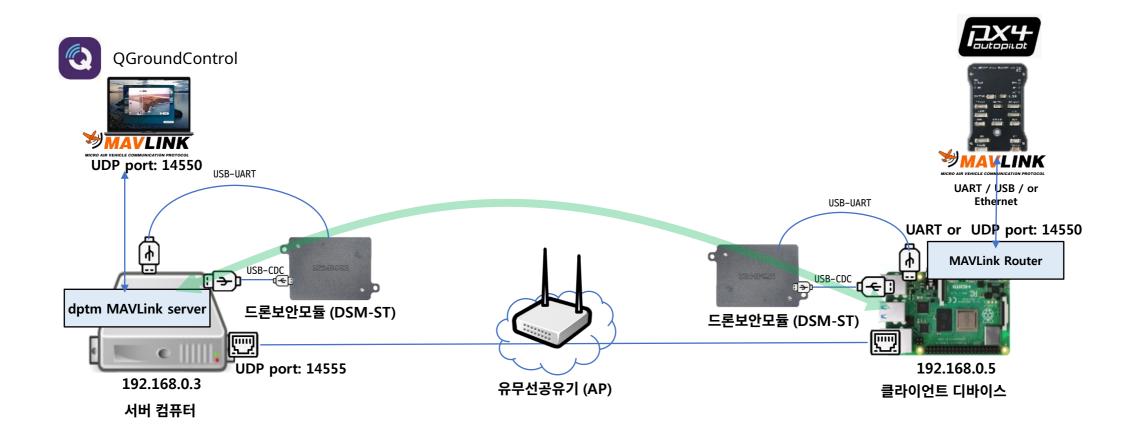
국방 드론 시스템 구조도 (DSM-ST 연동)



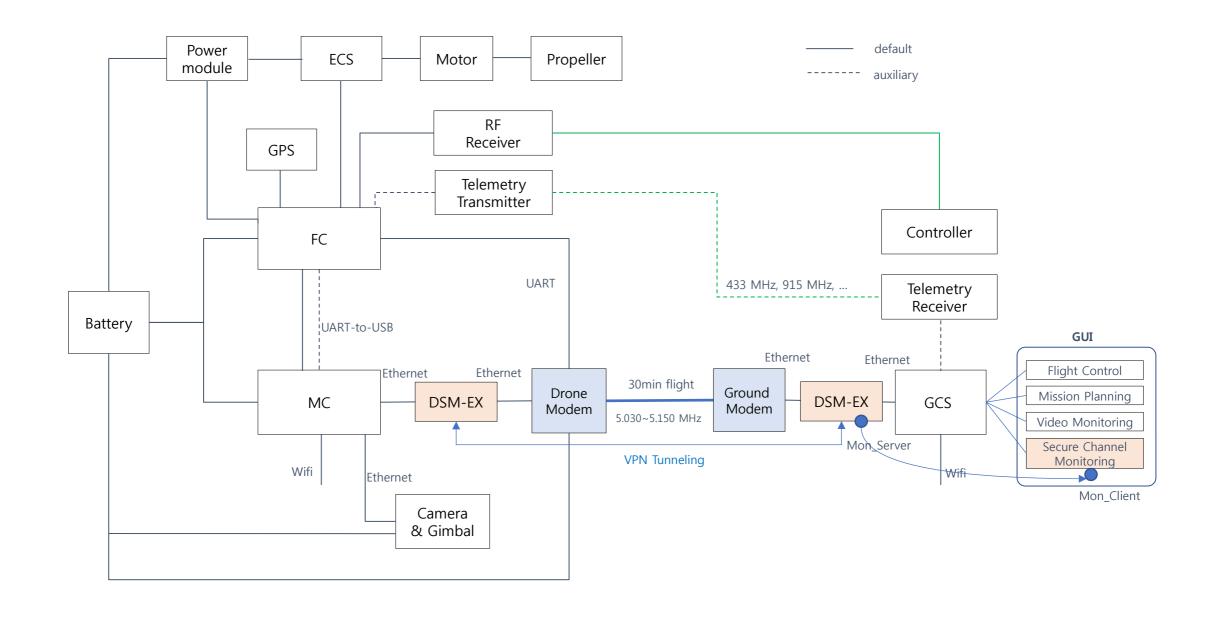
DSM-ST



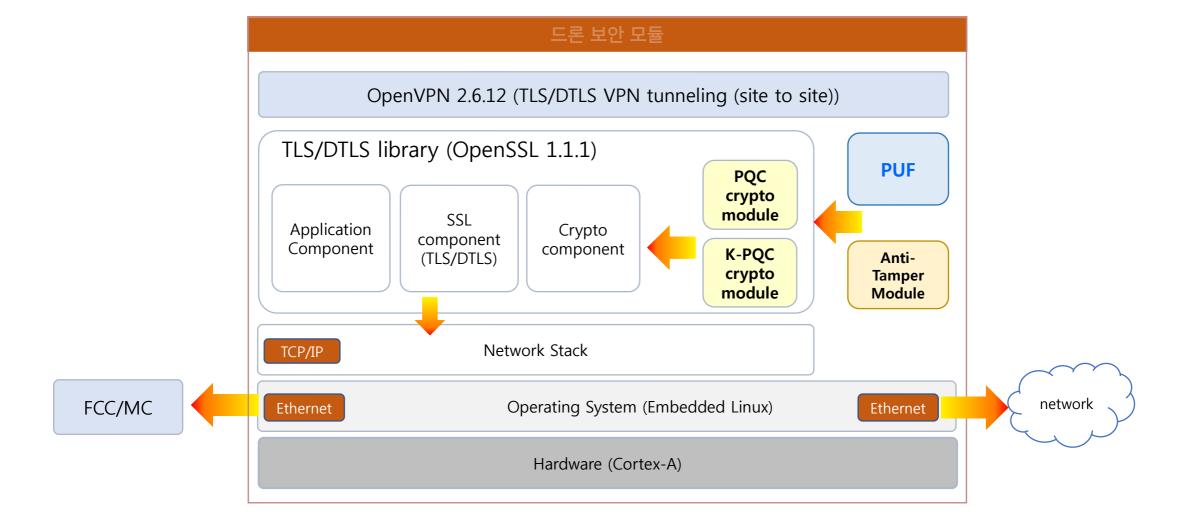
DSM-ST - 네트워크 구성도



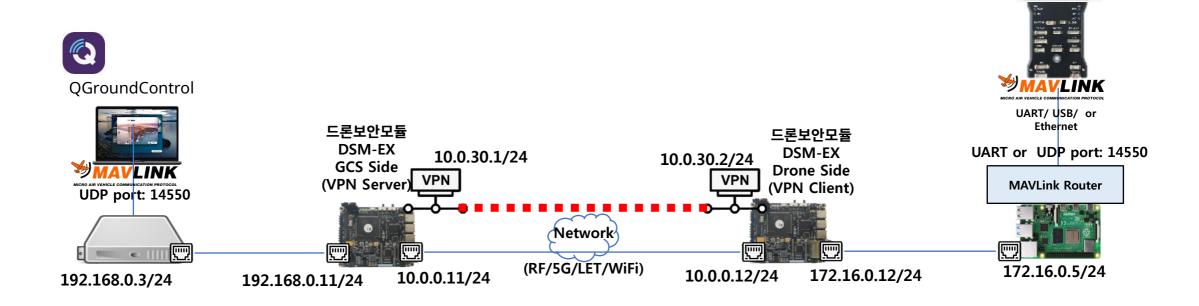
국방 드론 시스템 구조도 (DSM-EX 연동)



DSM-EX



DSM-EX - 네트워크 구성도



State Information

cmd: 16

State: ConnectedProtocol: TLSv1.2KEM: Kyber512DSA: Dilithium2

Ciphersuite: AES_256_GCM_SHA384

Tx Packets: 0Rx Packets: 0Tx Bytes: 0Rx Bytes: 0

Data Monitoring: FCC → GCS

cmd(DSM-ST): 2 cmd(DSM-EX): 6

Ciphertext (Encrypted Data)	Plaintext (Decrypted Data)	MAVLink (Flight & Sensing)

- 암호화 데이터와, 복호화 데이터 터미널 출력을 GUI 텍스트 박스에 출력
- MAVLink 파싱은 네트워크 프로토콜 분석기 Wireshark 이용

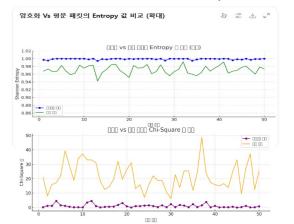
ile Edit View W	rindow Help		Erronesp			••••
X E1	미래암호공학				₹ ETRI-UAV-1	₽ DIM
^^	126.7675, 35.7937	ETRI-UAV-1 Cocryption Encryption	Authentication ■ MAVLink TLS Client ■	ETRI-UAV-1:	-71 dBm 223.171.56.36	AD SKY
		Encrypted Packet	Decrypted Packet	MAVLin ETRI-UAV-2 : [3	192.168.88.49	,
+		F7 AE 51 C6 FC E1 EC D5 5E 16 44 40 E7 BE CF FF 1E 73 0A 2E	0xFE225112A7089EE 0xFE227112A702D9			
•		+ Received Data Length: 39 Received message from fc with ID #42 (sys:1 c MAVLink Buffer: 0xfE28C112A701E4A + Received Data: 17 03 03 00 3C 00 00 00 00 00 00 00 00	0xFE92811000102CS133E7F0 0xFE94FF100000003C0409000 0xFE229112A70235F 0xFE22A112A7040F7	Payload: MISSION_CURRE seq (uint16): 7 Message CRC: 0xa71a MAVLink Protocol (10) Header	NI (42)	
		F7 AE 65 C3 E1 6C A6 12 27 D2 5D 49 66 6D 7E 63 09 05 5C BF 01 90 F5 10 CD 41 36 F8 BF 50 2A E0 D2 E9 A1 EE DC 09 A9	0xFE228112A709868 0xFE2CC112A7080AF 0xFE1C2D111EA81930EA2C4A8CD094DE387AE2613F8CD7 0xFE2ZE112A703898	Magic value / vers Payload length: 2 Packet sequence: 1 System id: 0x01		
		B2 + Received Data Length: 65 Received message from fc with ID #30 (sys:1 c	0xFE22F112A70EE7 0xFE230112A7003AB	Component id: 0x01 Message id: 0x0000		
		MAVLink Buffer: 0xFE1C8D111E21D93083AD438C9C: + Received Data:	0x 0xFE93411000102C5133EA3A 0xFE95FF10000068C04077A5	Payload: MISSION_CURRE seq (uint16): 7 Message CRC: 0x38cf		
		17 03 03 00 22 00 00 00 00 00 00 00 00 F7 AE 51 C6 FC 5A D8 68 08 1C 8C 81 98 88 C8 BE A1 6A 71 88	0xFE2035118DC91F463E200067963426796342221F2348 0xFE1E3611189729453E200031C05916181A984B8FEFCF 0xFE237112A70C86C	MAVLink Protocol (10) Header Magic value / vers	day Orfo	
		+ Received Data Length: 39 Received message from fc with ID #42 (sys:1 c	0xFE238112A703F75 0xFE239112A70EAEA	Payload length: 2 Packet sequence: 1		
		MAVLink Buffer: 0xFE28E112A70A57D + Received Data: 17 03 03 00 22 00 00 00 00 00 00 00 F7 AE 51 C6 FC 8F 44 BE 77 20 0E E3 1A	0xFE23A112A788442 0xFE23B112A7951D0 0xFE1C3C111E995930882488C3271DC385688613F1D8D6 0xFE23D0112A799C85	System id: 0x01 Component id: 0x01 Message id: 0x0000	1/2a	
025		3	0xFE23E112A70F22D	Payload: MISSION_CURRE seg (uint16): 7	NI (42)	

Data Monitoring: GCS → FCC

cmd: 1 cmd: 5

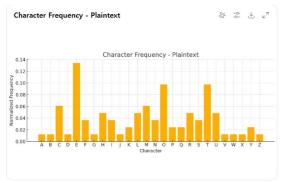
MAVLink (Command & Control)	Plaintext (Decrypted Data)	Ciphertext (Encrypted Data)

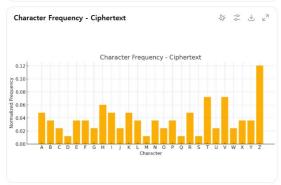
• 그래프를 이용한 시각화 (if possible)

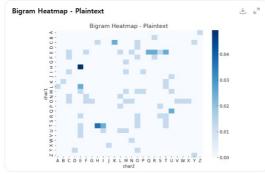


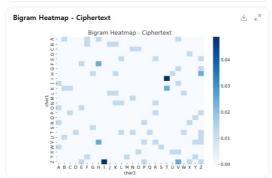
시각화 요약 그래프 구성 아이디어

분석 종류	Plaintext 예시	Ciphertext 예시
문자 빈도 히스토그램	불균형한 분포	균등 분포
bigram 히트맵	특정 조합이 빈번	무작위
엔트로피 수치	낮음 (4~5)	높음 (7~8)
chi-square 값	작음	큠

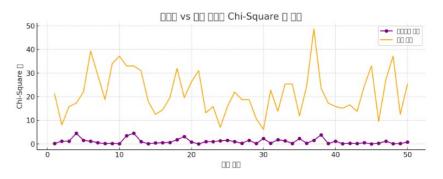


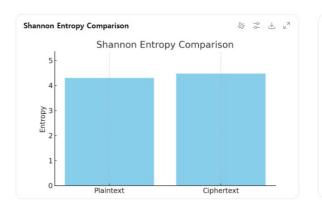


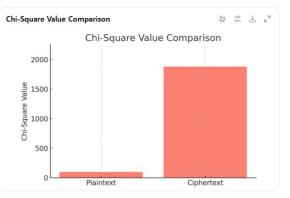










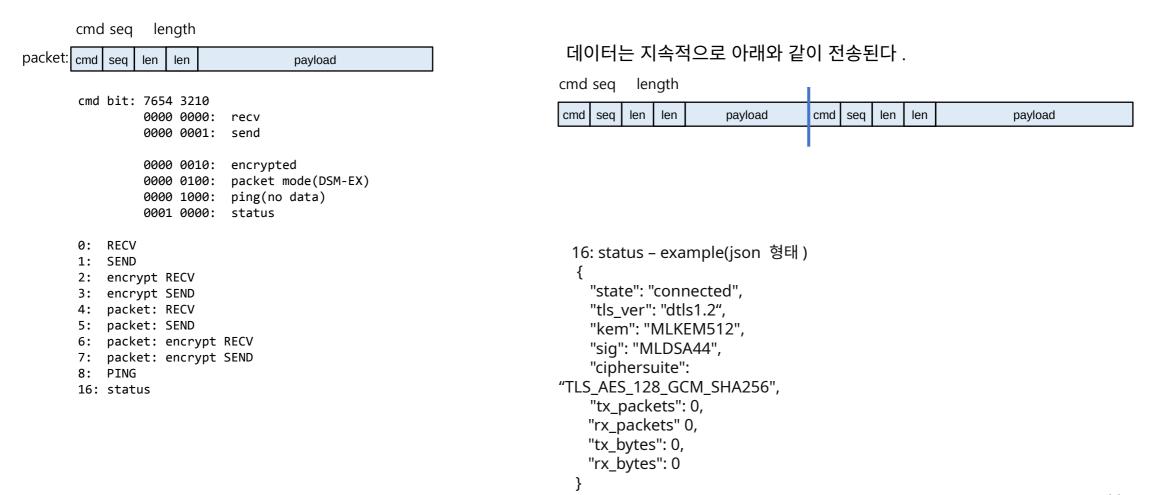


DSM-TLS 모니터링 프로토콜

- connection 실패 시 : 경량형 세션 없음 , 고속형 치명적 오류 (무조건 connection 은 가능해야함)
- TCP port: 14445
- 세션 상태 표시 : 모니터 서버에 연결 후 수초 마다 전송됨 .
- 모니터 client 는 지속적으로 수신 해야 하며 , 수신을 일정 시간 하지 않으면 세션이 끊어진다 . 세션이 끊어지면 처음부터 다시 tcp connet 를 해야 한다 .
- Mavlink packet plain-text encrypt data decoding 모니터 client 는 아래 4 곳 (dsm-st, dsm-ex 의 서버측 / 클라이언트측) 에 접속 가능하다 * 현재 서버측 (1 번 , 3 번) 만 사용 유력 Send plain-text Send:encrypted CMD 에 따라 아래로 표시 모니터 프로그램 모니터 packet 수신 Recv:encrypted Recv:plain-text Mavlink packet encrypt data plain-text decoding QGroundContr ₩<mark>MAV</mark>LINK QGroundCont UDP port: 14550 드론보안모듈 드론보안모듈 DSM-EX 10.0.30<u>.2/24</u> DSM-EX 10.0.30.1/24 UART or UDP port: Drone Side GCS Side (MPN Client VPN UDP port: 14550 otm MAVLink serve DSM-ST DSM-ST (경량형 드론보안모듈) (RF/5G/LET/ T, z.16.0.12/2 192.168.0.3/ 192.168.0.11/ 172.16.0.5/24 WiFi) 10.0.0.12/24 10.0.0.11/24 192.168.0.5 RF 모뎀 / 5G/LTE/ WiFi/ 드론 미션 컴퓨터 (라즈베리파이 4) 유무선공유기 (AP) 서버 컴퓨터 10 DSM-EX (고속형 드론 보안 모듈) DSM-ST (경량형 드론 보안 모듈)

TLS 모니터링 프로토콜

- 프로토콜은 아래와 같다 .(IP/TCP)
- 4byte head 를 먼저 수신 한다.
- head 에서 length(16bit, big-endian) 를 얻어 , 길이가 0 이 아니면 , 해당 길이 만큼 무조건 수신 (읽어야) 한다 .



TLS 모니터링 서버 구조

