특집 04

FHSS 기반의 드론 무선통신 취약점 연구*

강재구 · 최병철 (한국전자통신연구원)

목 차

1. 서 론

반도체 집적 기술과 배터리, 무선조종 및 제어 기술이 발전하면서 해당 기술들을 기반으로 하는 무인기의 일종인 멀티콥터/드론이 보편화 되었다. 상당히 가볍고 작은 크기이지만 전문 장비 못지않은 고해상도/고배율 카메라를 장착하고, 적게는 수십분에서 많게는 수시간까지 비행이 가능해진 현대의 드론들은, 그 운용의 편리성과 원격지 정보 취득의 용이성이 더해져 개인의 사생활 침해뿐만 아니라 공항과 같은 비행 금지 구역의 허가되지 않은 비행으로 많은 재산 피해를 발생시키고 있다. 이뿐만 아니라, 살상을 위한 자폭용 드론 무기체계까지 개발되어 실전에 사용되는 사례(2022년 러시아-우크라이나 전쟁)까지 발생 되고 있다. 크기가 워낙 작고 빠르게 움직이는 드론의 특성상 탐지와 탈취, 무력화가 상당히 난해하다. 그러나 이러한 피해를 줄이기 위한 안티드론(Anti-Drone) 기술은 꾸준히 개발되어 오고 있으며, 시장의 크기도 계속하여 증가하고 있는 추세이다[1].

안티드론 기술은 크게 탐지와 무력화의 두가지 범주로 요약 할 수 있다. 탐지의 경우 적외선/가시광선등을 사용하는 전자광학적탐지 방법과, 드론 비행시 발생되는 특유의 소리를 탐지하는 음파탐지 방법, 전통적인 레이더를 사용하는 방식 그리고 드론 혹은 드론 조종자가 발생시키는 통신용 전자파를 탐지하는 RF스캔방식 등으로 구분할 수 있으며 한가지 방식만으로는 탐지에 어려움이 있으므로 보통 2개 이상의 방법을 동시 혹은 순차적으로 사용한다. 무력화의 경우 초기에는 물리적 접촉을 통한 무력화 또는 드론에서 사용하고 있는 같은 주파수 대역에 방해전파(RF Jamming)를 송출하여 드론을 추락시키거나 조종 불능 상태를 유도하였으나, 최근에는 GPS 기만 기법을 사용하거나 해당 드론에 직접 조종 신호를 송출하여 드론의 조종 권한의 탈취를 통해 안전한 장소로 이동시켜 착륙을 유도하는 무력화 기술도 개발이 진행되고 있다. 드론 조종권 탈취 방식의 경우 전자파 방해 방식에 비해 주변 통신 장비들의 광범위한 잠정적인 피해를 최소화할 수 있고, 무력화 대상

※ 국방기술진흥연구소, "사이버 무력화 정밀 타격 기술 개발", KRIT-CT-22-074

드론만을 목표로 하므로 유사 주파수 대역을 사용하는 아군 통신 장비의 피해도 최소화할 수 있다. 뿐만 아니라, 추락으로 인한 추가 피해를 방지할 수도 있다는 장점이 있어 기술에 주목을 받고 있다.

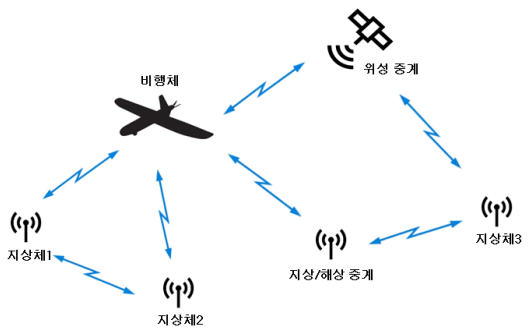
3G혹은 LTE통신의 변형된 방식을 사용하는 것으로 추정되는 DJI사의 드론 대상 안티드론과 관련된 연구로는, 드론과 조종기에서 발신하는 Drone-ID 무선 패킷을 해석[2][3]하는 최근의 연구를 비롯하여 탑재 펌웨어 조작을 위한 dji-firmware-tools[4] 그룹 등이 있고, DJI 드론 조종권의 직접 탈취가 가능한 이스라엘의 D-Fend Solution[5]과 Eclips[6]가 존재한다. 다만 DJI 드론 조종권 탈취 솔루션의 경우 어떠한 방식으로 탈취가 가능한지에 대해서는 현재까지 알려진 바가 없다. DJI를 제외한 나머지 드론들은 대부분 FHSS(Frequency Hopping Spread Spectrum) 혹은 DSSS(Direct Sequence Spread Spectrum) 다중접속방식을 주로 적용하고 있으며, 본 연구에서는 안티드론 기술개발 관점에서의 FHSS 무선통신 방식의 취약점에 대한 연구 결과를 제시하고자 한다.

2. 드론 무선통신 체계

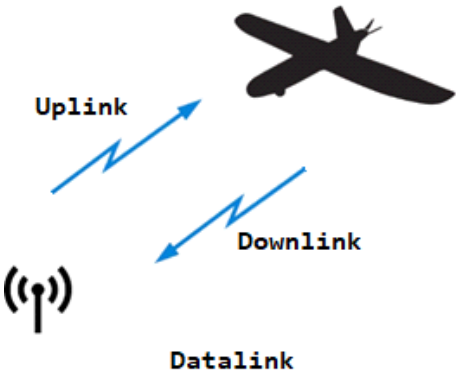
일반적인 드론은 (그림 1)과 같이 지상체 혹은 조종자에 의해 원격으로 조종되며 지상중계, 해상중계 혹은 위성중계 장비등을 체계에 추가 적용하여 그 임무 범위의 확장이 가능하다. 또한 한 개의 지상체/조종자가 아닌 다수의 지상체/조종자가 드론을 통제할 수 있는 복수통제 개념과 한 개 이상의 지상체에서 다수의 비행체를 통제하는 복수기체통제 개념도 존재 한다.

드론과 지상체 혹은 중계기간 통신을 '데이터링크' 라고도 하며 이 데이터링크는 (그림 2)와 같이 비행체로 데이터를 올려 보내는 상향 링크(Uplink)와 비행체로부터 데이터를 수신하는 하향 링크(Downlink)로 구성된다. 이때 상향 링크는 보통 C2(Command & Control), TC(Tele-Command) 혹은 RC(Radio/Remote Control) 신호 라고도 부르며, 이름에서도 알 수 있듯이 주로 비행체의 제어와 통제를 위한 지상체의 명령 데이터를 담고 있다. 하향 링크는 비행체에 대한 원격계측정보(Telemetry)와 EO/IR(Electro-Optical/Infra-Red), SAR(Synthetic Aperture Radar)등과 같은 임무장비의 데이터를 지상체로 내려 보내준다.

전통적인 민수용 무선 조종 주파수는 초기에 AM 변조 방식의 27 MHz 대역을 사용하였으며, FM 변조 기술이 적용되면서 40 MHz와 72 MHz 대역을 사용해 왔다. 디지털 신호처리 기반의 변/복조 기술이 주로 적용되는 최근에는 2.4 GHz 혹은 5.8 GHz의 ISM(Industry Science Medical) 대



(그림 1) 드론 무선통신 체계



(그림 2) 데이터링크 구성

역을 사용한다. 변/복조에는 FSK(Frequency Shift Keying) 혹은 PSK(Phase Shift Keying)가 주로 사용되며 이때 이 ISM 대역을 사용하기 위해서는 같은 대역을 사용하는 다른 기기와의 간섭 회피를 위해 다중접속기술중 하나인 주파수 확산 기법을 적용하게 되는데 대표적으로 주파수도약확산기법과(FHSS - Frequency Hopping Spread Spectrum) 직접확산기법(DSSS - Direct Sequence Spread Spectrum) 두가지가 사용된다.

DSSS 방식의 경우 데이터신호와 확산코드 혹은 의사잡음코드(PN Code - Pseudo Random Noise Sequence)의 배타적 논리합(XOR) 신호를 반송파에 담아 송출하는 방식으로 이 의사잡음코드를 알지 못하면 도감청이 원칙적으로 불가능 하다. 반면 FHSS 방식의 경우 ISM 대역 내에서 일정 간격으로 할당된 채널을 송신기와 수신기만이 알 수 있는 도약 순서로 초당 수~수십회 도약해 가며 송수신을 하는 방식으로, 이 도약 순서를 알지 못하면 역시 신호 도감청이 불가능하다는 특징이 있다. 3G 혹은 LTE의 변형을 사용하는 것으로 추정되는 DJI사의 드론을 제외한 현재 시장에서 판매중인 ISM 대역의 드론 혹은 드론 조종용 송수신기의 경우 대부분 FHSS와 DSSS 방식중 하나이며, DSSS 방식의 Near-Far 문제로 인해 DSSS 방식보다는 FHSS 방식을 주로 선호하는 편이다.

3. 드론 FHSS 무선통신 취약점

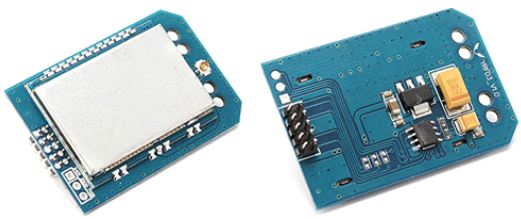
전술한 바와 같이 FHSS 방식은 송신기와 수신기가 사전에 서로 약속된 도약 순서를 따라 주파수 채널을 바꿔가며 통신을 수행하는 방식으로, 해당 채널로의 데이터 전송시 송신기의 가용 전력 스펙트럼을 모두 사용하므로 상대적으로 낮은 전력 스펙트럼 특성을 보이는 DSSS 방식에 비해 Near-Far 문제로부터 자유롭다. 또한 특정 채널 근처의 강한 신호가 나타나더라도 다른 채널로 능동적으로 바꿔가며 통신 연결 유지가 가능하므로, 진보된 적응형 채널 도약 알고리즘을 적용할 경우 전파 간섭 또한 최소화가 가능하다는 장점이 있어 시중에 판매되고 있는 드론과 드론용 무선 송수신기 들은 FHSS 기법이 많이 적용되어 있다.

FHSS 기법이 적용된 드론 혹은 무선 송수신 장치들의 경우 보통 Low-Cost, Low-Power를 강조하는 상용 RF Front-End SoC 혹은 RF Transciever 칩들을 사용하는 경우가 대부분이며 자체 조사를 통해 대표적인 아래 4가지의 SoC가 주로 사용되는 것을 파악 할 수 있었다.

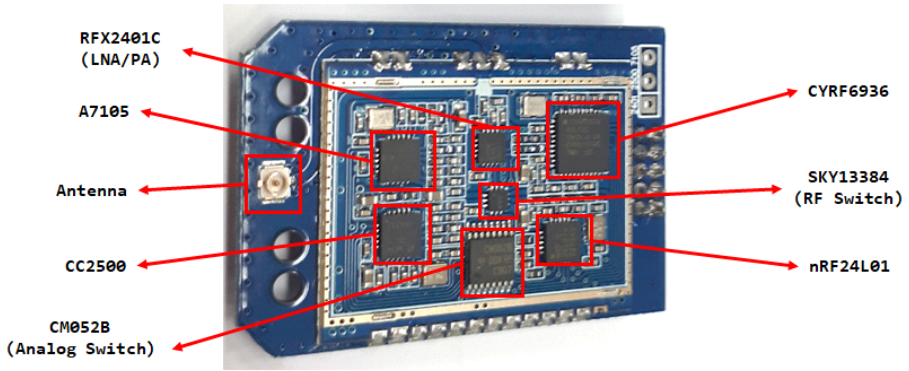
1) **CC2500/CC2510 (Texas Instruments)**
2) **CYRF6936 (Cypress Semiconductor)**
3) **nRF24L01 (Nordic Semiconductor)**
4) **A7105 (AMICCOM)**

대규모 글로벌 반도체 기업에서 판매하는 CC2500/CC2510 및 CYRF6936의 경우 중급기 이상의 제품에 주로 탑재가 되고 상대적으로 비용의 경쟁력을 갖추고 있는 nRF24L01 및 A7105등과 같은 칩셋은 주로 저가 및 보급형 드론과 무선 송수신기에 탑재되어 판매 되고 있는 것을 확인할 수 있었으며, 이 4개의 모든 SoC를 한데 모아 FHSS기반의 많은 프로토콜에 대응이 가능한 4IN1 모뎀[7]을 시장에서 쉽게 구매 가능함을 확인하였다 (그림 3), (그림 4).

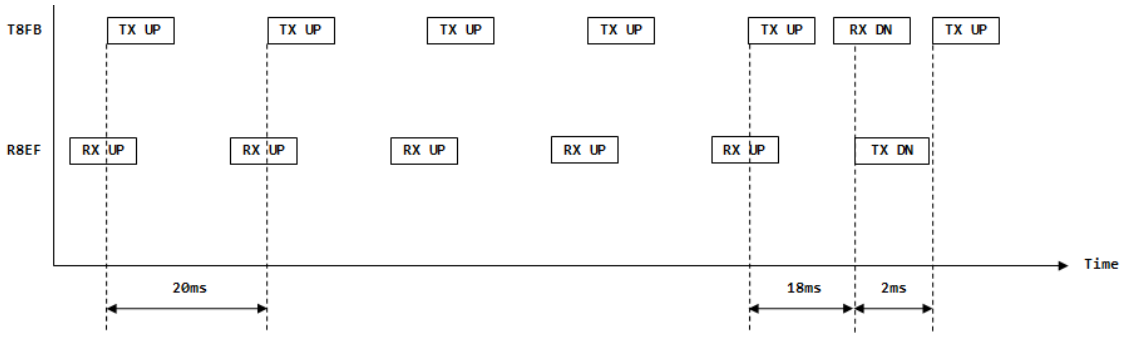
FHSS 패킷 스케쥴링은 각 제조사와 모델마다



(그림 3) 4IN1 모뎀



(그림 4) 4IN1 모뎀 내부 구성



(그림 5) 상용 송수신기(T8FB/R8EF) RF 패킷 스케쥴링 예시

조금씩 차이는 있으나, 대부분 (그림 5)와 같이 수신기의 수신여부와 상관 없이 송신기는 일정 주기로 조종명령(TX UP) 패킷을 보내고, 수신기는 송신기와 바인딩(Binding)시 주고받은 정보를 기반으로 수신 채널을 변경해 가며 송신기의 C2 패킷을 기다리고 수신(RX UP)하는 구조 이다. 이때 송신기는 일정 패킷 송신 횟수(예, 5회)에 다다르면, 수신기에 Telemetry 패킷을 요구하게 되며 수신기는 C2 패킷 중간에 텔레매트리(Telemetry) 패킷을 발신한후(TX DN) 다음 C2 수신 채널로 복귀하여 C2 신호를 수신하는 방식으로 구현된 프로토콜이 상당수 인것으로 파악 되었다.

(그림 6)은 패킷 스캐쥴링 역공학 대상의 RadioLink사의 상용품으로, T8FB 송신기와 R8EF 수신기의 패킷 스캐쥴링 역공학 결과 (그림 5)와 같음이 파악 되었다.

FHSS 기법이 적용된 송수신장치의 경우 송수신기간 정의된 도약 순서를 알지 못하면 도감청이 원칙적으로 불가능하지만, 시장에 판매되고 있는 모델들의 경우 그 구현의 특성상 다음 몇가지 취약점이 존재하는 것을 파악 할 수 있었으며, 해당 취약점을 활용하여 제 3자에 의한 패킷의 수신과

(그림 6) 패킷 스케쥴링 역공학 대상 모델 (좌 송신기 T8FB, 우 수신기 R8EF)

송신이 가능함도 확인 하였다.

1) 대부분의 FHSS 드론 무선 패킷의 데이터가 암호화 되어 있지 않음

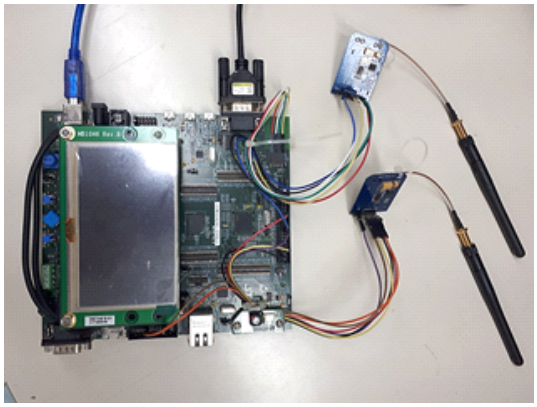
2) 제조사별 FHSS 도약 알고리즘의 상당수가 공개정보[7]로 취득 가능

3) 일부 모델의 경우 C2 패킷에 다음 도약 채널을 연산 할 수 있는 정보를 담고 있음

해당 취약점들을 직접 확인하고 검증하기 위해 (그림 7)과 같이 임베디드시스템 평가보드와 4IN1 모듬을 연동하여 간단한 도구를 구성해 위 3가지

〈표 1〉 Multiprotocol TX Module github를 통해 파악 가능한 프로토콜 일부

Name	Sub 0	Sub 1	Sub 2	Sub 3	Sub 4	Sub 5	Sub 6	Sub 7
Assan	ASSAN							
Bayang	Bayang	H8S3D	X16_AH	IRDRONE	DHD_D4	QX100		
Bugs	BUGS							
BugsMini	BUGSMINI	BUGS3H						
Cabell	Cabell_V3	C_TELEM					F_SAFE	UNBIND
CFlie	CFlie							
CG023	CG023	YD829						
Corona	COR_V1	COR_V2	FD_V3					
CX10	GREEN	BLUE	DM007		J3015_1	J3015_2	MK33041	
Devo	Devo	8CH	10CH	12CH	6CH	7CH		
DM002	DM002							
DSM	DSM2_1F	DSM2_2F	DSMX_1F	DSMX_2F	AUTO			
E010 R5								
E016H v2								
E01X	E012	E015	E016H					
E129								
ESky	ESky	ET4						
ESky150	ESKY150							
ESky150V2								
Flysky	Flysky	V9x9	V6x6	V912	CX20			
Flysky AFHDS2A	PWM_IBUS	PPM_IBUS	PWM_SBUS	PPM_SBUS	PWM_IBUS16	PPM_IBUS16		
FQ777	FQ777							
FrSkyD	D8	Cloned						
FrSkyL	LR12	LR12_6CH						
FrSkyR9	R9_915	R9_868	R9_915_8CH	R9_868_8CH	R9_FCC	R9_FCC_8CH		
FrSkyV	FrskyV							
FrSkyX	CH_16	CH_8	EU_16	EU_8	Cloned	Cloned_8		
FrSkyX2	CH_16	CH_8	EU_16	EU_8	Cloned	Cloned_8		



(그림 7) FHSS 무선통신 취약점 분석용 간이 도구

취약점을 모두 확인 하였다.

Multiprotocol TX Module[7] 단체에서 공개한 자료들의 경우 시중에 판매되는 약 170여가지의 FHSS 통신 프로토콜과 관련된 정보를 소스코드 수준에서 취득할 수 있으며, 연구[8]에서는 FHSS 기반 드론의 조종권 탈취를 직접적으로 수행한 결과를 보여 주고 있다. 주파수 도약 방법이 바인딩 시 상수로 고정되는 드론의 경우 SDR(Software Defined Radio)과 같은 장치들을 활용하여 손쉽게 도약 정보를 파악 할 수 있으며, 위 1)의 취약점과 같이 패킷에 암호화가 되어 있지 않으므로 시행착오 방법 혹은 Multiprotocol TX Module github에 공개된 패킷 포맷에 따라 비행제 조종명령을 만들어 송신하게 되면 원 조종자와 경쟁상태에서 드론의 조종권 일부 획득이 가능하다. 또한 위 취약점 3)과 같이 무선 패킷에 다음 도약 정보가 포함된 FHSS 프로토콜의 경우 원 조종자와 상이한 다음 도약정보 패킷을 만들어 송신하게 되면 좀더 개선된 조종권 탈취가 가능해짐을 보여주고 있다.

FHSS에서의 도약 방법은 가능한 난수에 가까울 수록 간섭이 최소화 되므로, 각 드론 및 송수신기 제조사들은 보다 진보된 도약 알고리즘들을 개발 하고 있으며, 패킷에 도약과 관련된 정보가 없는 모델이거나, 도약을 위한 난수 발생 알고리즘을 알 수 없는 경우 FHSS 특성에서 설명한 바와 같이 FHSS 조종명령을 통한 조종권 탈취는 쉽지 않다.

<표 1>은 Multiprotocol TX Module github에서 확인 가능한 170여가지 FHSS 통신 프로토콜 중 일부 항목의 예시를 보여주고 있다.

4. 결론 및 향후 연구

안티드론 기술개발의 관점에서 드론의 무선 조종에 많이 사용되는 ISM 대역의 FHSS 확신기법에 대한 취약점 연구를 수행하였다. 그 결과 대부분의 FHSS 무선 패킷은 암호화가 되어있지 않으므로 대표적인 4가지 RF SoC인 CC2500/CC2500, CYRF6936, nRF24L01, A7105의 데이터시트를 참고하여 임의의 주파수 채널을 통해 목표 드론에 송신되는 패킷을 수신하여 그 내용을 분석할 수 있었으며, 공개된 정보를 기반으로 송신기의 복제와 수신기의 복제도 가능함을 확인 할 수 있었다. 또한 초기 바인딩과정에서 상수로 고정되는 도약 알고리즘들의 경우 전술한 취약점의 활용과 더불어 SDR과 같은 도구를 활용해 그 도약 정보를 쉽게 유추해 낼수 있으며, 드론 조종패킷을 기반으로 다음 도약 채널을 연산해 낼수 있는 프로토콜의 경우 해당 연산 알고리즘이 확보된다면 역시 도약 정보의 취득이 가능함을 확인 하였다. 다만, 어떠한 방법으로든 도약 정보를 확인할 수 없는 기종의 경우 해당 FHSS 패킷으로의 조종권 탈취는 거의 불가능하며, 연구[8]에서와 같이 취약점을 이용해 조종권한을 탈취하더라도 원 조종자의 조종신호가 공존하는 한 영구적 혹은 장시간 드론 조종권 탈취는 쉽지 않다.

향후에는 본 연구를 통해 확인된 FHSS 취약점과 더불어 다수의 모뎀을 활용하여 원 조종자의

조종신호를 무력화시키는 방법을 동원, 좀더 진보된 드론 조종권 탈취를 위한 연구를 진행할 계획이다.

참 고 문 헌

[1] Grand View Research, Anti-drone Market Size, Share & Trends Analysis Report By Component, By Type, By Range, By Technology, By Mitigation Type, By Defense Type, By End-use, By Region, And Segment Forecasts 2023-2030, 2023.

[2] Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars , Thorsten Eisenhofer, Tobias Scharnowski, Felix Domke, Lea Schönherr, Thorsten Holz, Drone Security and the Mysterious Case of DJI's DroneID, Network and Distributed System Security Symposium, Feb. 2023.

[3] Bender, C. DJI drone IDs are not encrypted. arXiv 2022, arXiv:2207.10795. [Google Scholar].

[4] dji-firmware-tools, Available online: https://github.com/o-gs/dji-firmware-tools, accessed on 6 Dec. 2023.

[5] D Fend Solutions, Available online: https://d-fendsolutions.com, accessed on 6 Dec. 2023.

[6] NSO Group Eclips, Available online: https://www.nsogroup.com/Newses/nso-group-launches-drone-defense-system-eclipse, accessed on 6 Dec. 2023.

[7] Multiprotocol TX Module, Available online: https://github.com/pascallanger/DIY-Multiprotocol-TX-Module (accessed on 6 Dec. 2023).

[8] Sebastian Plotz, Frederik Armknecht, Christian Bunse, How to Take Over Drones, Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, Pages 526–536, May 2021.

저 자 약 력

강 재 구

이메일 : kangjaegu@etri.re.kr

- 2004년 전북대학교 전자제어계측공학 (학사)
- 2003년-2005년 KEC-메카트로닉스연구소 연구원
- 2007년 과학기술연합대학원대학교 HCI 및 로봇응용공학 (석사)
- 2007년~2010년 한국로봇융합연구원 연구원
- 2010년~2012년 (주)한화종합연구소 연구원
- 2012년~2022년 (주)대한항공 항공기술연구원 연구원
- 2023년~현재 한국전자통신연구원 연구원

최 병 철

이메일 : corea@etri.re.kr

- 1999년 서울시립대학교 제어계측공학과 (학사)
- 2001년 서울시립대학교 전자전기공학부 (석사)
- 2012년 충남대학교 컴퓨터공학 (박사)
- 2019년~2022년 한국전자통신연구원 보안취약점분석연구실 실장
- 2001년~현재 한국전자통신연구원 책임연구원
- 2020년~현재 한국정보보호학회 이사
- 관심분야 : 사이버보안, 사이버전, 사이버전자기전