https://doi.org/10.33778/kcsa.2023.23.2.075

MAVLink 프로토콜 기반 드론 교란 신호 생성 및 송출에 관한 연구★

이 우 진*, 임 창 한**, 이 재 연***

요 약

최근 러시아-우크라이나 전쟁, 북한의 대남 정찰, 육군 Army Tiger 4.0의 드론봇체계 등 군사용 목적으로 드론의 활용도가 증가하고 있기 때문에 각 국에서는 이에 따른 안티드론 기술이 많이 발전하고 있다. 하지만 재래식 무기 또는 전자전 무기를 활용하는 형태의 전통적인 안티드론 기술들은 비용이 비싸다는 단점이 있어 현재는 저비용으로 수행할 수 있는 안티드론 기술도 새롭게 연구되고 있다. 따라서 이러한 안티드론 기술에 대응하여 아군의 생존성을 높이기 위한 노력도 많이 하고 있다. 이러한 흐름에 발맞추어 본 연구에서는 다양한 안티드론 기술들 중 비용이 비싼 재래식 무기 또는 전자전 무기를 활용한 기술이 아닌 저비용으로 수행할 수 있는 사이버영역과 전자전영역 기술이 적용된 가상의 대 드론 체계를 가정하고 이에 대응하여 아군 드론의 생존성을 높일 수 있는 방안에 대해 제시하고자 한다.

A Study on the Generation and Transmission of Drone Jamming Signals Based on the MAVLink Protocol

Woojin Lee*, Changhan Lim**, Jaeyeon Lee***

ABSTRACT

Recently, as the use of drones for military purposes is increasing, such as the Russia-Ukraine War, North Korea's reconnaissance against South Korea, and Army Tiger 4.0's dronebot system, anti-drone technology is developing a lot in each country. However, traditional anti-drone technologies in the form of using conventional weapons or electronic warfare weapons have the disadvantage of being expensive, so anti-drone technologies that can be performed at low cost are currently being newly researched. Therfore, in response to these anti-drone technologies, many efforts are being made to increase the survivability of our allies. In line with this trend, this study assumes a virtual anti-drone system applied with cyber domain and electronic warfare domain technologies that can be performed at low cost, rather than a technique using expensive conventional weapons or electronic warfare weapons among various anti-drone technologies. In response to this, we would like to present a plan to increase the survivability of friendly drones.

Key words : Drone, PX4, MAVLink, Moving Target Defense, MTD, Jamming, Anti-Drone

접수일(2023년 04월 17일), 수정일(2023년 05월 08일), 게재확정일(2023년 05월 16일)

★ 본 논문은 2023년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 미래도전국방기술 연구개발사업임 (No. 915024201).

* 한화시스템(주) 기반기술연구소(주저자)
** 한화시스템(주) 기반기술연구소(공동저자)
*** 한화시스템(주) 기반기술연구소(교신저자)

1. 서 론

현재의 드론은 민간에서 영상 촬영, 곡예비행, 비행 시합과 같은 취미 또는 레저용으로 사용되거나 재난 상황에서의 생존자 수색 및 구출과 같은 구조용으로 사용되는 등 다양한 분야에서 이로운 활용되고 있다. 그러나 과거 1차 세계대전이 발생한 시점부터 드론은 군사적인 목적으로 연구되기 시작하여 1980년대 이스라엘과 레바논 전쟁에서 정찰 및 폭격 유도와 같이 활용되는 형태로까지 발전하였다[1, 2]. 또한 최근 국내에서는 북한 무인기 5대가 약 7시간에 걸쳐 서울, 강화, 파주 일대를 비행하며 정찰하는 동안 격추하거나 나포하지 못한 사건이 벌어지기도 했다. 국외에서는 우크라이나-러시아 전쟁에서 우크라이나가 'TB2', 'Punisher', 'Warmate', 'R-18', 'Switchablade 300·600' 등 10여 종 이상의 공격 드론을 활용하여 러시아를 정밀 타격하고 이에 맞서 러시아도 'Orion-E', 'Forpost-R'과 이란의 'Shahed-136' 등의 공격 드론을 활용하여 전쟁에 참여하는 등 군사 목적의 드론의 활용성[3]이 커지고 있다. 따라서 이러한 군사 목적의 드론에 대한 대응체계의 필요성이 커져 감에 따라 각 군에서는 다양한 영역에서의 드론 무력화 기술을 활용한 대 드론 체계에 대한 연구 개발을 수행하였다. 실제로 앞서 언급한 러시아-우크라이나 전쟁에서 러시아는 우크라이나의 드론에 대응하기 위해 미사일 격추를 활용한 전통적인 방식의 대공 방어 체계인 'Tor M2', 'Pantsir S2'를 운용했으며, 우크라이나도 러시아의 드론에 대응하기 위해 미군의 전통적인 방식의 미사일 격추를 활용한 'Vampire', 'NASAMS'와 같은 대 드론 체계를 활용하였다.[3]

전통적인 방식의 대 드론 체계는 값싼 공격 드론을 저지하기 위해 값비싼 지대공 미사일을 대량으로 사용하여 비용이 많이 드는 단점을 가지고 있으므로 새로운 방식의 드론 무력화 기술을 활용한 대 드론 체계 개발에 대한 수요가 커지고 있다. 전통적인 방식이 아닌 새로운 유형의 드론 무력화 기술에는 소리 신호를 통해 센서 오류를 유발하는 기술[4, 5], 전자기장 신호 주입을 통해 통신채널 오작동을 유발하는 기술[6], 전자전 영역에서 RF(Radio Frequency) 신호 분석 및 재밍 신호 송출을 통해 드론을 저지하는 기술[7]과 사이버 영역에서 드론 통신 프로토콜 취약점을 이용한 악성 코드 주입 및 제어권 탈취 기술[8, 9]이 주로 연구되고 있다. 또한 최근에는 사이버 영역과 전자전 영역을 융합하여 RF 신호 분석부터 드론에서 사용하는 데이터들에 대한 조합 및 악성 코드 주입 및 제어권 탈취 기술에 대한 사이버 전자전 기술 연구[10]가 국내 여러 기관에서 시작되고 있다.

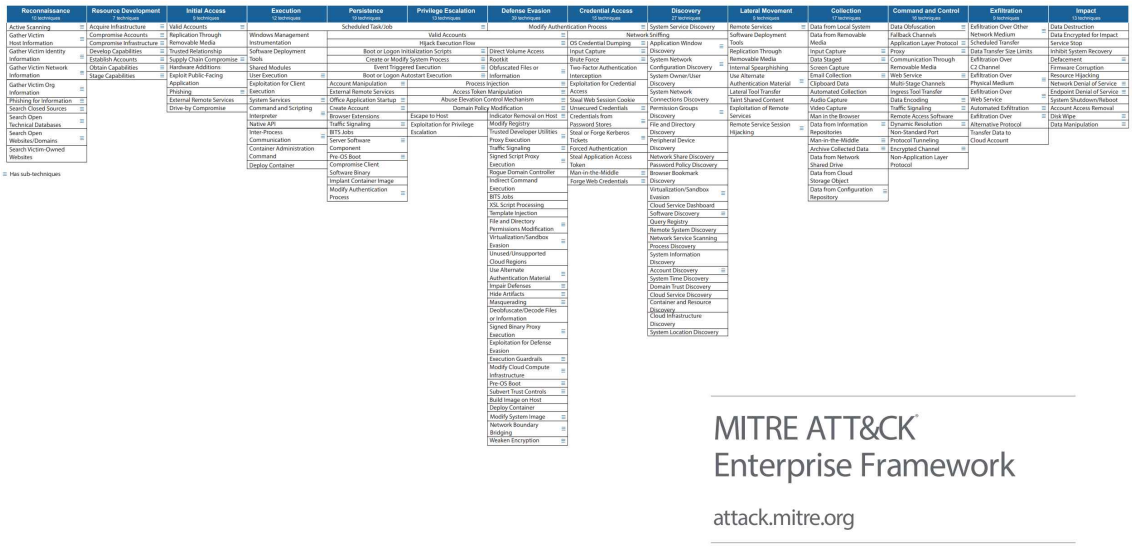
이러한 드론 무력화 기술이 적용된 대 드론 체계에 대비하여 아군의 운용 드론에 대한 생존 가능성을 향상하는 것은 현재 드론을 실전 배치[11]하고자 하는 군에게 중요한 기술이다. 따라서 본 논문에서는 다양한 드론 무력화 기술 중 비교적 저비용으로 드론을 저지할 수 있고 가장 최근에 연구가 시작된 사이버 전자전 기술이 적용된 대 드론 체계에 대비하여 통신 프로토콜의 교란 신호 생성 및 송출을 통해 아군 드론의 생존 가능성을 높이는 방안에 대해 제시하고 연구 결과를 소개하고자 한다.

2. 관련 연구 및 사례

2.1 Moving Target Defense 기술

사이버 영역에서의 Moving Target Defense (이하, MTD)라고 불리는 기술은 일반적으로 공격 대상인 Target의 위치를 바꾸어 공격자가 공격할 수 있는 공격 표면(Attack Surface)을 늘리고, Target을 식별하여 공격이 성공하더라도 위치가 변경되기 때문에 공격 지속성이 떨어지는 효과를 보이는 기술이다. 이는 MITRE 기관의 ATT&CK Matrix로 표현되는 사이버 공격 전술(Tactic) 중 정찰(Reconnaissance) 단계와 지속(Persistence) 단계를 방해하여 사이버 생존 가능성을 높일 수 있는 기술이라 이해할 수 있다.

전통적으로 MTD 기술은 유선 네트워크상에서 디지털 자산의 네트워크 주소에 해당하는 IP 또는



(그림 1) MITRE ATT&CK 프레임워크[20]

Port를 변이하여 공격자를 기만하는 형태의 연구[12, 13, 14, 15, 16, 17]가 활발히 진행됐으며 각 MTD 기술들에 대한 평가 및 특성이 연구[18, 19]되었다. 본 연구에서는 이러한 전통적인 MTD 기술에 대한 연구내용을 바탕으로 드론에서 사용하는 별도의 텔레메트리(RF) 통신에서의 프로토콜에 MTD 개념을 확장하여 적용하였기 때문에 IP, Port 이외의 항목에 대해서 자가 변이를 수행하는 방안을 제시하고자 한다.

2.2 국외 드론 무력화 제품 사례

기존 드론 무력화 기술은 앞서 서론에서 언급하였듯이 정말 다양한 영역에서 탐지 기술과 공격 기술로 나뉘어 발전하고 있다. 네덜란드에서는 Robin Radar System 사에서 'ELVIRA'라는 장비[21]와 Thales 사의 Squire[22]를 개발하였으며 레이더를 활용하여 드론을 탐지한다. 영국에서는 MGT Europe의 DroneRANGER[23]를 개발하여 레이더와 광학장비를 이용해 무인비행체를 검출하고 상업용 민간 드론의 주파수 및 GNSS(Global Navigation Satellite System)를 교란하는 제품이 존재한다. 또한 앞서 설명한 영국, 네덜란드의 제품 사례뿐만 아니라 스페인 Advanced Radar Technology 사의 'Drone Sentinel', 독일 Aaronia 사의 'Advanced Automatic RF Tracking and Observation Solution', 프랑스 Cebair 사의 'Anti-Drone Solution', 이스라엘 RADA 사의 'RPS-42', 미국 SpotterRF 사의 'Radar'와 Black Sage Technology 사의 'A2000', Harrier 사의 'DSR-200d', Gryphon Sensor 사의 'SkyLight', Kelvin Hughes 사의 'SMS-D', DMT Security Radar Solutions 사의 'c-UAS' 등의 제품[7]이 있다. 대부분의 드론 무력화 제품들이 이와 같은 레이더, EO/IR(Electro-Optical/Infra-Red) 광학장비를 이용해 드론을 식별하고 있으며, 식별 후 드론을 저지하는 방법으로는 주파수 전파 방해 또는 GNSS 교란 장비를 활용하여 드론을 저지하는 방식을 활용하고 있다.

하지만 이러한 방식의 드론 무력화 시스템의 드론 저지방식은 주파수 전파 방해 또는 GNSS 재밍 방식으로써 주파수가 공개되지 않고 레이더의 탐지 범위를 넘어 운용되는 군용 드론의 경우 동작하지 못할 수 있으며 재밍 시 민간 전자장비 또는 아군의 전자장비에 피해를 줄 수 있다. 이뿐만 아니라 재밍으로 인한 드론의 추락과 같은 위험 요소 때문에 인명 피해가 발생할 수도 있다는 단점이 있다. 또한 전파 출력의 통달 거리를 늘리

기 위해서는 비용이 많이 들기도 하며 단순 무력화가 아닌 정교한 공격을 수행하기에 제한적이다. 따라서 최근에는 단순 전자전 영역의 드론 무력화 기술뿐만 아니라 사이버 영역의 데이터를 삽입하여 악성 코드를 주입하고 제어권 탈취를 하는 형태의 드론 무력화 기술과 관련된 연구가 수행되고 있다.

2.3 사이버 영역 드론 무력화 기술 연구

현재까지 연구되고 있는 드론 무력화 기술들에 대한 일반적인 분류는 <표 1>과 같다.

<표 4> 드론 무력화 기술 분류

구분	기술	단점
물리	미사일	비용이 많이 듦
	요격 드론	효율성이 낮음
	그물	정확도가 낮음
	고출력레이저	비용이 많이 듦
전자전	GPS 재밍	전자장비 피해
	전자기장 교란	전자장비 피해
	RF 신호 재밍	전자장비 피해
사이버	Wifi 해킹	제한적인 대상
	블루투스 해킹	제한적인 대상
	SW 취약점 해킹	제한적인 대상
	GPS 스푸핑	정상 GPS 방해

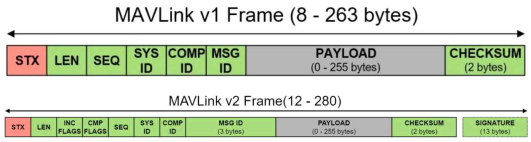
<표 1>에서 분류한 드론 무력화 기술 중 물리, 전자전 영역은 비용이 많이 드는 경향이 있으며 항재밍 기술이 탑재되지 않은 아군의 드론과 전자장비 또는 민간 상용 드론과 장비에 피해를 줄 수 있다는 제한사항이 있으므로 단점으로 볼 수 있으며 아군에 피해를 줄 가능성이 있으므로 본 연구에서는 공격 대상은 제한적이지만 피해를 주지 않는 사이버 영역의 드론 무력화 기술이 활발하게 사용될 것이라 가정하고 이에 대한 대응 방안을 중점적으로 다룰 예정이다. 특히 Wifi, 블루투스를 이용한 공격은 해당 통신 모듈에 제한적이므로 범용적으로 쓰일 수 있는 기술 연구를 위해 SW 취약점 해킹에 대응할 수 있는 방어 기술에 관해 연구한다. 사이버 영역에서 SW 취약점 공격을 이용한 무력화를 수행하기 위해서는 공격하고자 하는 대상에서 사용하는 SW의 취약점을 찾아 공격하기 위한 페이로드를 구성하여 대상의 네트워크 주소를 목적지로 악성 코드를 전송하여 제어권을 탈취하거나 서비스 거부 공격을 수행한다. 일반적으로 SW 취약점 공격은 암호화[24], 시큐어 코딩[25], 퍼징[26, 27]을 이용한 취약점 검증 등과 같은 기존의 방어 기술들이 있지만 본 연구에서 제시하고자 하는 방어 기술은 이러한 기존 방어 기술들이 무력화되었을 때를 대비한 방어 기술이며 SW의 취약점 공격은 주로 외부와의 접점이 있는 통신 프로토콜을 통해 발생하므로 통신 프로토콜을 활용한 공격에 대응하여 생존 가능성을 보장하는 방안을 연구하였다. 특히 본 논문에서는 오픈소스 통신 프로토콜인 MAVLink 통신 프로토콜 메시지의 취약점을 공격하여 드론을 무력화하는 기술 및 시나리오[28]를 활용한 대 드론 체계에 대한 아군 드론의 생존 가능성을 높일 수 있는 대응 방안을 제시하고자 한다. MAVLink 통신 프로토콜은 공식적으로 현재 우리 군에서 활용하고 있는 통신 프로토콜이 아니며 군이 현재 운용 중인 군용 드론은 별도의 정립된 표준 통신 프로토콜이 없는 상황이지만 25년까지 기반 체계 구축, 27년까지 주요 부대 전력화, 30년까지 전 부대 전력화를 위해 추진 중인 육군의 드론봇 전투체계의 구축 방안을 보면 320여억 원의 예산을 활용하여 상용 드론을 도입[29]하려고 하고 있다. 따라서 본 논문에서는 민간 상용 드론에서 주로 사용하고 있는 오픈소스 통신 프로토콜인 MAVLink 통신 프로토콜을 선정하였다.

3. MAVLink 기반 교란 신호 생성

3.1 MAVLink 메시지 분석

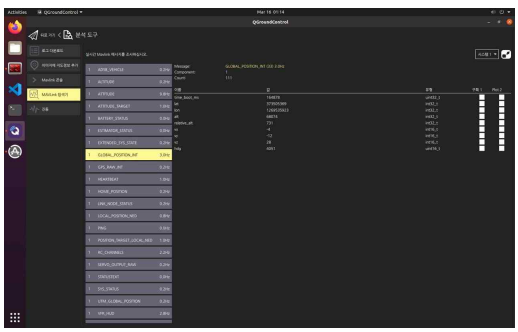
MAVLink 메시지는 소형 비행체에 사용하기 적합하도록 디자인된 경량 메시지 프로토콜이다.[30] MAVLink 메시지의 구조는 아래 (그림 2)와 같이 구성되며 SYSID와 COMPID를 이용해 MAVLink 메시지를 사용하는 시스템 및 컴포넌트를 식별한다. 예를 들어 각각의 드론은 서로 다른 SYSID를 가지며 이는 일반 유선 네트워크 환경에서의 IP와 같은 구실을 한다. COMPID는 하나의 드론 기체에 적재될 수 있는 미션 컴퓨터, 카메라 등 부가적인 컴포넌트에 대한 식별자로 일반 유선 네트워크 환경에서의 Port와

같은 구실을 한다.



(그림 2) MAVLink 프로토콜 구조

MSG ID는 MAVLink 메시지의 식별자로써 PX4 시스템의 동작을 위한 각 메시지를 구분하는 역할을 한다. 기체의 종류별로 사용하는 MAVLink 메시지가 다른데 공통으로 사용되는 메시지의 경우 mavlink 오픈소스 프로젝트 내에 common.xml[31, 32]의 형태로 정의되어 있다. 2.1절에서 설명한 바와 같이 본 연구에서는 유선 네트워크 상의 IP, Port를 변이하는 형태의 MTD를 MAVLink 환경에서 그와 유사한 SYSID, COMPID를 변이하는 형태로 확장 적용하여 네트워크 기반 교란 신호를 생성하고 정의된 MAVLink 메시지 중 MSGID가 33번인 GLOBAL_POSITION_INT 메시지, 0번인 HEARTBEAT 메시지, 4번인 PING 메시지에 대해 호스트 기반 교란 신호를 생성한다. 이는 실제 드론이 운용 중일 때 (그림 3)과 같이 GCS(Ground Control System)로 전달하는 메시지를 확인하여 드론 식별에 중요하다고 판단되는 메시지를 우선으로 선별한 결과이며, 추후 더 다양한 메시지에 대한 교란 신호를 생성할 수 있도록 메시지 별 교란 신호가 대 드론 체계의 공격 성공 및 실패에 미치는 효과도 분석을 수행하여 교란 신호로 송출할 메시지를 식별하여야 한다.



(그림 3) GCS에서 수신받은 MAVLink 메시지

3.1.1 GLOBAL_POSITION_INT 메시지

GLOBAL_POSITION_INT 메시지는 MSGID가 33번이며 드론에서 GPS 센서 및 가속도 센서를 통해 들어오는 위치 값을 조합한 위치 정보를 GCS로 전달하기 위한 메시지이다. 실제 GCS에서는 해당 메시지를 수신받고 해석하여 지도에 현재 연결된 드론의 위치를 표시하며 <표 2>와 같은 필드를 가진다.

<표 5> GLOBAL_POSITION_INT 필드

필드명	타입	단위	설명
time_boot_ms	uint32_t	ms	부팅 이후 시간
lat	int32_t	degE7	위도
lon	int32_t	degE7	경도
alt	int32_t	mm	고도
relative_alt	int32_t	mm	MSL 기준 고도
vx	int16_t	cm/s	위도방향 속도
vy	int16_t	cm/s	경도 방향 속도
vz	int16_t	cm/s	고도 방향 속도
hdg	uint16_t	cdeg	방향

해당 메시지의 각 필드 중 lat, lon, alt, relative_alt 필드를 교란하면 대 드론 체계가 RF 신호 수집을 통해 드론을 식별할 때 드론의 위치가 실시간으로 바뀌어 혼란을 겪을 수 있다. 또한 가짜 드론이 식별되어 공격 대상 선정에 어려움을 겪을 것이다.

3.1.2 HEARTBEAT 메시지

HEARTBEAT 메시지는 MSGID가 0번이며 드론에서 현재 시스템 및 컴포넌트의 상태, 타입, 모드, MAVLink 프로토콜 버전 등에 대한 정보를 GCS로 전달하기 위한 메시지이다. 실제 GCS에서는 해당 메시지를 수신받고 해석하여 GCS에 현재 드론 타입, 모드, AUTOPILOT 종류, 상태 등 다양한 정보를 표시하며 <표 3>과 같은 필드를 가진다.

<표 6> HEARTBEAT 필드

필드명	타입	값	설명
type	uint8_t	MAV_TYPE	비행체 및 컴포넌트 타입 (eg. 쿼드콥터, 짐벌 등)
autopilot	uint8_t	MAV_AUTOPILOT	AUTOPILOT 종류(eg. PX4, OrageCube 등)
base_mode	uint8_t	MAV_MODE_FLAG	MAV 모드 (eg. 시동 등)
custom_mode	uint32_t	-	-
system_status	uint8_t	MAV_STATE	시스템 상태
mavlink_version	uint8_t	-	mavlink 버전

해당 메시지의 각 필드는 전반적인 드론 및 컴포넌트의 상태가 담겨있으므로 대 드론 체계가 드론을 식별하고 SW 취약점을 찾을 수 있는 중요한 정보이다. 따라서 MTD 교란 항목으로 선정하였다. RF 신호 및 드론 통신 프로토콜을 분석하는 드론 무력화 기술을 적용한 대 드론 체계가 있다면 해당 필드를 분석하여 각각의 드론을 식별할 것이기 때문에 해당 필드를 교란한다면 공격 표면을 증가시키는 효과를 보일 것으로 기대할 수 있다.

3.1.3 PING 메시지

PING 메시지는 MSGID가 4번이며 드론에서 GCS로의 연결을 유지하기 위한 목적으로 주기적으로 전달되는 메시지이다. 드론에서 GCS로 PING 메시지를 보내면 GCS는 그에 대한 응답 메시지로 PING 메시지를 보내며 GCS 화면에 해당 드론의 SYSID, COMPID를 포함한 메시지 정보를 표시하며 <표 4>와 같은 필드를 가진다.

(표 7) PING 필드

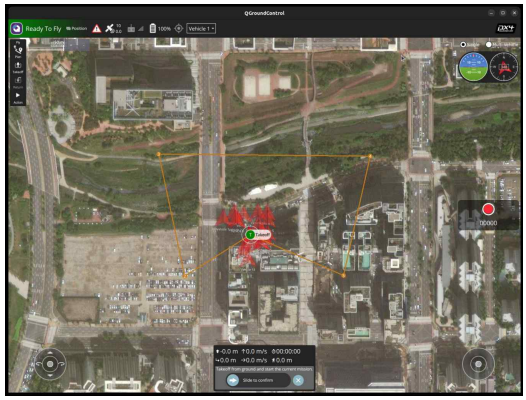
필드명	타입	단위	설명
time_usec	uint64_t	us	부팅 이후 시간
seq	uint32_t	-	시퀀스 넘버
target_system	uint8_t	-	대상 sysid
target_component	uint8_t	-	대상 compid

해당 메시지의 필드 중 target_system과 target_component 항목은 공격자의 관점에서 공격 대상을 식별할 수 있는 중요한 단서이며, GCS에서 각 드론 및 미션 컴퓨터, 짐벌 등 다양한 시스템/컴포넌트로 전달하는 PING 메시지를 통해 공격하고자 하는 시스템 및 컴포넌트를 식별할 수 있으므로 해당 필드를 교란한다면 HEARTBEAT 메시지와 마찬가지로 공격 표면을 증가시키는 효과를 보일 것으로 기대할 수 있다.

3.2 MAVLink 메시지 생성 및 송출 결과

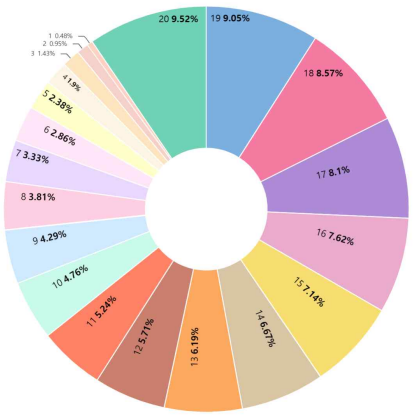
위에서 설명한 공격 대상을 식별할 수 있는 필드가 포함된 3종류의 MAVLink 메시지 각 필드와 SYSID, COMPID를 변이하여 MAVLink 메시지를 생성하고 송출하기 위해서는 각 메시지 필드별 변이 알고리즘을 정해야 한다. MTD 기술을 활용한 필드 변이 알고리즘은 게임이론 기반 변이 알고리즘과 같은 형태로 설계한 연구[33], OSINT(Open Source Intelligence) 정보 기반 변이[34] 등 다양한 형태의 알고리즘이 존재하지만 본 연구에서는 단순 무작위 값으로 변이하는 형태로 구현하였다. 각각의 메시지 필드를 무작위 값으로 변이하기 위해서는 변이 최솟값과 최댓값, 변이 주기를 입력값으로 받는 MTD 정책이 필요하며 이를 받아서 처리하는 MTD 에이전트를 구현하였다. 또한 각 메시지 필드의 값이 정상 드론이 사용하는 메시지 필드의 값과 전혀 다른 값으로 무작위 변이하는 경우 대 드론 체계의 관점에서 정상 타겟과 비정상 타겟의 구분이 명확하여 혼란을 주는 효과가 떨어질 수 있으므로 정상 드론의 신호의 값을 기준값으로 설정하고 최솟값과 최댓값을 더해 무작위 값을 생성하는 형태로 구현하였다.

랜덤 변이 알고리즘을 적용하여 GLOBAL_POSITION_INT, HEARTBEAT, PING 메시지에 대해 무작위 값을 적용한 교란 메시지가 생성되면 오픈소스인 pymavlink 패키지[35]를 사용하여 MAVLink 메시지를 송출하였으며, 그 결과는 대 드론 체계에서 (그림 4)와 같이 드론을 식별하는 식별자인 SYSID가 여러 개로 늘어나고 드론을 식별하기 위한 위치 정보도 교란되어 나타난다. 이에 따라 공격자는 실제 드론을 제외한 가짜 드론을 추가로 식별하게 되며 매초 식별자(SYSID) 및 위치 정보 필드(lat, lon, alt)가 변경되어 공격 표면이 늘어나 공격 대상을 선정하기 어려운 효과를 가져온다. 또한 공격 대상이 선정되더라도 교란 신호로 인해 생성된 가짜 드론을 공격하게 되어 공격이 실패하게 된다.



(그림 4) MAVLink 교란 신호 송출 결과

이처럼 MTD 교란 신호 생성 및 송출을 수행했을 때, 드론 무력화 기술 모의기에서 공격 대상을 선정하기 위해 SYSID를 출력한 결과 아래 (그림 5)와 같이 실제 아군의 SYSID는 1인데 다양한 SYSID가 식별되는 것을 확인할 수 있었다.

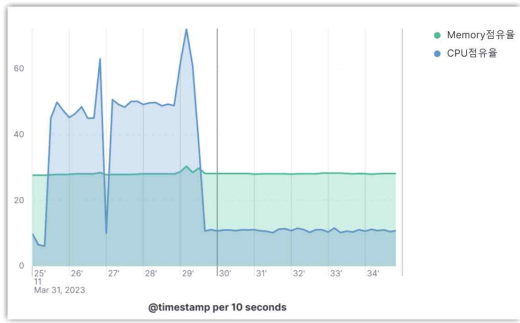


(그림 5) MTD 실행 결과 SYSID 스캔 비율

또한 (그림 5)에서 식별한 드론의 SYSID를 인자로 공격을 시도할 경우 가짜 드론을 포함한 20개의 드론에 공격을 가하면 단순 계산으로는 95%의 공격 방어율을 보장하며 공격에 수행되는 시간 소요도 많이 되어 최종적으로 공격에 실패할 확률이 높아진다.

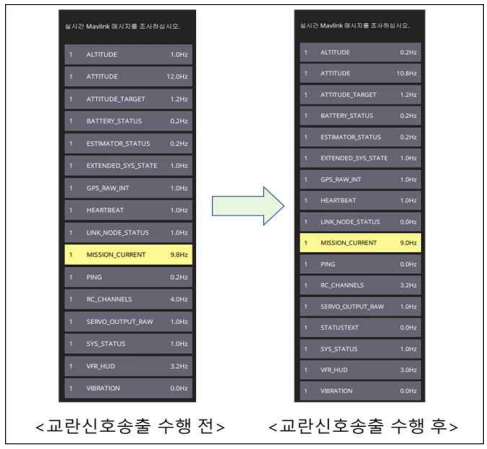
4. 교란 신호 생성 및 송출 성능 분석

메시지별 자가 변이는 필드별로 다르게 설정할 수 있으며 MAVLink 메시지의 송출 주기는 일반적으로 SITL(Software-In-The-Loop) 환경에서 GLOBAL_POSITION_INT 메시지는 약 50Hz, PING 메시지와 HEARTBEAT 메시지는 1Hz로 송출하기 때문에 실제 MTD 기능을 수행하는 에이전트는 1초에 약 52회 이상의 반복문을 수행해야 한다. 따라서 교란할 메시지가 늘어날수록 미션 컴퓨터의 성능이 부족하여 메시지 생성 및 송출 작업을 수행하지 못할 수 있으며 실제 3개의 메시지를 변이 및 송출하는데 소모되는 리소스 사용량은 (그림 6)와 같았다.



(그림 6) 교란 신호 생성 및 송출 리소스 사용량

(그림 6) 기준 25분부터 교란 신호 생성 및 송출하기 시작하였고 30분부터 중단하였을 때, 리소스 사용량을 보면 CPU 사용량이 평균적으로 40~60%인 것을 알 수 있었지만, 실제 GCS에서 MAVLink 메시지 수신 주기를 비교해본 결과 아래 (그림7)과 같이 큰 차이가 없는 것을 확인할 수 있었으며 이는 교란 신호 생성 및 송출이 드론의 실시간 비행 중 통신 문제가 없음을 나타낸다.



(그림 7) 교란신호송출 전/후 통신 주기

그러나 본 연구에서 제안하는 교란 신호 생성 및 송출 기술은 성능이 좋은 서버나 데스크탑 PC에서 동작하는 것이 아닌 임베디드 장비인 드론 또는 드론에 장착되는 임베디드 보드 탑재체에 적용되는 기술로써 전력 소모량, 성능이 중요하게 작용하므로 추후 리소스 사용량을 줄이는 방안에 관해 연구가 필요하다.

5. 결 론

본 연구에서는 아직 잘 알려지지 않은 드론 무력화 기술이 적용된 대 드론 체계에 대응하기 위해 상용 통신 프로토콜 기반 MTD 기술을 적용하여 공격 표면을 늘리는 효과로 인해 드론의 생존 가능성을 향상하는 방안을 제시하였다. 아직 연구의 시작 단계로 성능 최적화, 드론 무력화 기술의 운용개념 적용, MTD 변이 알고리즘의 다양화, RF 신호 특성 변이, 암호화 통신에서의 적용 방안 등 고려해야 할 요소들이 많다. 하지만 해외 NATO(North Atlantic Treaty Organization)의 STANAG(Standardization Agreement) 4586 통신 프로토콜과 같이 실제 국내 우리 군에서 운용 및 개발 중인 드론의 통신 프로토콜이 정립된다면 본 연구에서 수행한 MTD 자가 변이 기술을 적용한 드론 탑재체를 개발하고 미래 육군에서 운영 예정인 드론봇 전투체계에 탑재하여 미상의 대 드론 체계로부터 임무 수행을 보장하고 생존 가능성을 향상할 수 있을 것으로 생각된다. 또한 본 연구에서 제시한 기술은 드론에 해당 기능이 탑재되는 형태로 개발되어 활용할 수도 있지만 드론이 표준 인터페이스만 따른다면 정찰 드론, 공격 드론, 통신 드론, 수송 드론 등 드론의 종류에 구애받지 않고 MTD 통신 기능 탑재체만 단순 장착하면 되므로 군에서 활용하기 유용한 형태로 발전이 가능할 것으로 생각된다. 따라서 추후 이와 관련하여 군에서 사용하고 있는 표준 프로토콜에 적용할 수 있는 형태의 연구를 수행하여 실제 군에서 활용할 수 있도록 개선할 예정이다.

참고문헌

[1] 정지훈, “드론의 발전현황과 향후 시장전망”, 광학세계, 제158권, pp.40-47, 2015.

[2] 이건영, “드론, 우리 곁으로 성큼 다가온다.”, 전기의 세계, 제65권, 제1호, pp.17-24, 2016.

[3] 서강일, 김기원, 김종훈, 조상근, 박상혁, “우크라이나-러시아 전쟁에서 나타난 다영역 대드론체계 연구”, 국방로봇학회논문집, 제2권, 제1호, pp.25-32, 2023.

[4] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, Yongdae Kim, “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors”, USENIX Conference on Security Symposium, 2015.

[5] Jinseob Jeong, Dongkwan Kim, Joonha Jang, Juhwan Noh, Changhun Song, Yongdae Kim, “Un-Rocking Drones: Foundation of Acoustic Injection Attacks and Recovery Thereof”, Network and Distributed Systems Security Symposium, 2023.

[6] Joonha Jang, ManGi Cho, Jaehoon Kim, Dongkwan Kim, Yongdae Kim, “Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels”, Network and Distributed Systems Security Symposium, 2023.

[7] 최상혁, 채종석, 차지훈, 안재영, “안티 드론 기술 동향”, 정보통신동향분석, 제33권, 제3호, pp.78-88, 2018.

[8] 이우진, 서경덕, 채병민, “오픈소스 활용 드론에 대한 보안 위협과 Telemetry Hijacking을 이용한 군용 드론 공격 시나리오 연구”, 융합보안논문뫂ㅅ지, 제20권, 제4호, pp.103-112, 2020.

[9] 김명수, 유일선, 임강빈, “무인이동체 드론의 취약점분석 및 대응기술 연구 동향”, 정보보호학회지, 제30권, 제2호, pp.49-57, 2020.

[10] 김선웅, 강승민, 이원준, 전준, 김봉연, “한국군 사이버·전자전 발전방향 제언 : 미 사이버·전자전 무기 조직체계 강화방안을 중심으로”, 국방과 기술, 제514호, pp64-71, 2021.

[11] 류창수, 김명환, 정영진, “드론봇 전투부대 편성 및 운용개념에 관한 연구”, 국방과 기술, 제480호, pp.70-81, 2019.

[12] 우사무엘, 박경민, 문대성, 김익균, “네트워크 주소 변이 기반 Moving Target Defense 연구 동향”, 정보보호학회지, 제28권, 제2호, 2018.

[13] Justin Yackoski, Peng Xie, Harry Bullen, Jason Li, Kun Sun, “A Self-shelding Dynamic Network Architecture”, Military Communications Conference, 2011.

[14] Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan, Proceedings of the first workshop on Hot topics in software defined networks, pp.127-132, 2012.

[15] Jafar Haadi H.Jafarian, Ehab Al-Shaer, Qi Duan, “Spatio-temporal Address Mutation for Proactive Cyber Agility against Sophisticated Attackers”, Proceedings of the First ACM Workshop on

Moving Target Defense, pp.69-78, 2014.
[16] Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan, “An Effective Address Mutation Approach for Disrupting Reconnaissance Attacks”, IEEE Transactions on Information Forensics and Security, pp. 2562-2577, 2015.
[17] Jianhua Sun, Kun Sun, “DESIR: Decoy-enhanced seamless IP randomization”, IEEE INFOCOM, 2016.
[18] Gui-lin CAI, Bao-sheng WANG, Wei HU, Tian-zuo WANG, “Moving target defense: state of the art and characteristics”, Frontiers of Information Technology & Electronic Engineering, pp.1122-1153, 2016.
[19] Lei, Cheng, et al. "Moving target network defense effectiveness evaluation based on change-point detection." Mathematical Problems in Engineering 2016 (2016).
[20] MITRE ATT&CK Enterprise Framework, “https://attack.mitre.org/docs/attack_matrix_poster_2021_june.pdf”, 2021.
[21] ELVIRA, “https://www.robinradar.com/elvira-anti-drone-system”.
[22] SQUIRE, “https://www.thalesgroup.com/en/squire-ground-surveillance-radar”.
[23] DRONERANGER, “https://scgroup-ltd.com/ droneranger/”.
[24] Allouch, Azza, et al. "MAVSec: Securing the MAVLink protocol for ardupilot/PX4 unmanned aerial systems." 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019.
[25] 안준선, 이은영, 창병모, “SW 개발보안을 위한 보안약점 표준목록 연구”, 정보보호학회지, 제 25권, 제 1호, 2015.
[26] 오상환, 김태은, 김환국, “SW 보안 취약점 자동 탐색 및 대응 기술 분석”, 한국산학기술학회논문지, 제 18권, 제 11호, 2017.
[27] Domin, Karel, Iraklis Symeonidis, and Eduard Marin. "Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol." (2016).
[28] 이우진, 서경덕, 채병민, “오픈소스 활용 드론에 대한 보안 위협과 Telemetry Hijacking 을 이용한 군용 드론 공격 시나리오 연구” 융합보안논문지 20.4, pp.103-112, 2020.
[29] 대한민국 육군, “https://www.army.mil.kr/webapp/mbshome/mbs/newmobile/subview.do?id=newmobile_030102000000”.
[30] MAVLink, “https://mavlink.io/”
[31] MAVLink Common Message Set XML, “https://github.com/mavlink/mavlink/blob/master/message_definitions/v1.0/common.xml”.
[32] MAVLink Common Message Set, “https://mavlink.io/en/messages/common.html”.
[33] 서상, 문해은, 이선호, 이재연, 김병진, 이우진, 김도훈, “무인기동체계 사이버 생존성 보장을 위한 게임이론 기반 능동적 이동 변이 연구”, 군사과학기술학회 종합학술대회, pp.1207-1208, 2022.
[34] Seo Sang, Dohoon Kim. “OSINT-based LPC-MTD and HS-decoy for organizational defensive deception.” Applied Sciences 11.8, 2021.
[35] pymavlink 패키지, “https://github.com/ArduPilot/pymavlink”

〔저자소개〕

이 우 진 (Woojin Lee)
2018년 7월 부산대학교 학사
現, 한화시스템(주) 기반기술연구소
email :
holinder4s@hanwha.com

임 창 한 (Changhan Lim)
2022년 2월 영남대학교 학사
現, 한화시스템(주) 기반기술연구소
email :
ckdglsdl@hanwha.com

이 재 연 (Jaeyeon Lee)
2002년 2월 가톨릭대학교 학사
2004년 2월 광주과학기술원 석사
現, 한화시스템(주) 기반기술연구소
email:
jaeyeon46.lee@hanwha.com