J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

객체인식 AI적용 드론에 대응할 수 있는 적대적 예제 기반 소극방공 기법 연구

A Research on Adversarial Example-based Passive Air Defense Method against Object Detectable AI Drone

육 심 언[1] 박 휘 랑[2] 서 태 석[1] 조 영 호[2*]
Simun Yuk Hweerang Park Taisuk Suh Youngho Cho

요 약

우크라이나-러시아 전을 통해 드론의 군사적 가치는 재평가되고 있으며, 북한은 '22년 말 대남 드론 도발을 통해 실제 검증까지 완료한 바 있다. 또한, 북한은 인공지능(AI) 기술의 드론 적용을 추진하고 있는 것으로 드러나 드론의 위협은 나날이 커지고 있다. 이에 우리 군은 드론작전사령부를 창설하고 다양한 드론 대응 체계를 도입하는 등 대 드론 체계 구축을 도모하고 있지만, 전력증강 노력이 타격체계 위주로 편중되어 군집드론 공격에 대한 효과적 대응이 우려된다. 특히, 도심에 인접한 공군 비행단은 민간 피해가 우려되어 재래식 방공무기의 사용 역시 극도로 제한되는 실정이다. 이에 본 연구에서는 AI기술이 적용된 적 군집드론의 위협으로부터 아 항공기의 생존성 향상을 위해 AI모델의 객체탐지 능력을 저해하는 소극방공 기법을 제안한다. 대표적인 적대적 머신러닝(Adversarial machine learning) 기술 중 하나인 적대적 예제(Adversarial example)를 레이저를 활용하여 항공기에 조사함으로써, 적 드론에 탑재된 객체인식 AI의 인식률 저하를 도모한다. 합성 이미지와 정밀 축소모형을 활용한 실험을 수행한 결과, 제안기법 적용 전 약 95%의 인식률을 보이는 객체인식 AI의 인식률을 제안기법 적용 후 0~15% 내외로 저하시키는 것을 확인하여 제안기법의 실효성을 검증하였다.

☞ 주제어 : 객체인식AI 기술 적용 드론, AI드론, 적대적 머신러닝, 군집드론, 방공작전, 기지방호

ABSTRACT

Through the Ukraine-Russia war, the military importance of drones is being reassessed, and North Korea has completed actual verification through a drone provocation towards South Korea at 2022. Furthermore, North Korea is actively integrating artificial intelligence (AI) technology into drones, highlighting the increasing threat posed by drones. In response, the Republic of Korea military has established Drone Operations Command(DOC) and implemented various drone defense systems. However, there is a concern that the efforts to enhance capabilities are disproportionately focused on striking systems, making it challenging to effectively counter swarm drone attacks. Particularly, Air Force bases located adjacent to urban areas face significant limitations in the use of traditional air defense weapons due to concerns about civilian casualties. Therefore, this study proposes a new passive air defense method that aims at disrupting the object detection capabilities of AI models to enhance the survivability of friendly aircraft against the threat posed by AI based swarm drones. Using laser-based adversarial examples, the study seeks to degrade the recognition accuracy of object recognition AI installed on enemy drones. Experimental results using synthetic images and precision-reduced models confirmed that the proposed method decreased the recognition accuracy of object recognition AI, which was initially approximately 95%, to around 0-15% after the application of the proposed method, thereby validating the effectiveness of the proposed method.

☞ keyword : object detectable drone, AI drone, adversarial machine learning, swarm drone, air defense, base defense

1. 서 론

우크라이나-러시아 전은 전쟁사 이래 그 어느 때보다 드론의 군사적 활약상이 돋보이는 전쟁이다. 나날이 전해지는 드론의 효과는 기존의 방공작전 개념과 방공 무기체계의 패러다임을 뒤엎고 있으며, 혹자는 이를 '드론 혁명(Drone revolution)'이라 명명할 만큼 치명적이다[1].

개전초 우크라이나는 튀르키예산 군사용 드론(TB-2,

1 Integrated System Operation Squadron, Air Operation Group, 17th Fighter Wing, Republic of Korea Air Force, Cheongju, 28152, Korea.
2 Department of Defense Science (Computer Engineering and Cyberwarfare Major), Graduate School of Defense Management, Korea National Defense University, Nonsan, 33021, Korea.
* Corresponding author (youngho@kndu.ac.kr)
[Received 10 October 2023, Reviewed 24 October 2023(R2 27 November 2023, Accepted 4 December 2023]

Bayraktar 社)과 중국산 저가 상용드론(Mavic 등)으로 하여금 러시아군의 주요 기계화 전력(T-90M 전차 등)을 효과적으로 파괴 및 저지하여 단기전을 계획하였던 러시아의 의도를 막아내고 전쟁초기 주도권을 회복하였다[2, 3]. 또한, 러시아 공군의 고가치 전략자산인 공중조기경보기(AWACS, A-50U)를 자폭드론 공격으로 운용 중단시키고[4], 골판지로 만든 종이드론 16기로 러시아 공군의 주력 전투기(Mig-29 1대, Su-30 4대)와 방공 시스템(S-300 지대공 미사일)을 파괴하기도 하였다[5]. 소형 폭탄을 장착하여 만든 자폭 드론은 정밀 유도무기처럼 활용할 수 있으며, 비용적 이점으로 방공유도탄 기반의 방공체계에 비대칭적 방어비용을 강요한다. 설령 막대한 방어비용을 감내하더라도 더욱 많은 수량으로 운용하여 적의 방공능력을 소진시켜버린다. 이러한 막강한 효율성으로 드론은 '빈자의 공군력(Poor man's air force)'이라 불린다[6].

한편, 북한은 무인기를 군사분계선 이남으로 남하시켜 우리 영공을 불법적으로 침범하는 고강도 도발을 '14년 이후 8년 만인 '22년 12월에 감행한 바 있다. 아산정책연구원은 해당 도발을 우-러 전의 드론 효과에 자극받은 의도적인 도발로 평가한 바 있다. 북한은 이미 매울 수 없을 만큼 커져버린 재래식 전력의 격차를 극복하기 위해 화학·생물학 무기, 핵무기와 같은 대량살상 무기(Weapon of Mass Destruction, WMD)와 사이버 무기와 같은 비대칭 전력 확보에 집중해왔다. 드론은 우크라이나-러시아 전을 통해 차세대 비대칭 전력으로 평가되고 있는데, 북한은 이러한 드론의 효과를 실제 도발로 하여금 검증까지 마친 것이다. 즉, 북한의 드론 위협은 이미 현실이 되었으며, 향후 더욱 강대해질 것이라 전망할 수 있다.

여기서 더 나아가 북한은 드론에 인공지능(Artificial Intelligence, AI) 기술 적용을 추진하고 있는 것으로 보인다. '19년 스톡홀름 국제평화연구소(SIPRI)는 북한이 AI 기술에 상당한 투자와 노력을 기울이고 있으며, 무인항공기 역량개선에 이 기술을 활용할 것임을 경고한 바 있다[7]. 이후 김일성대와 김책공대와 같은 북한의 학술연구기관들은 AI연구 개발 성과를 지속적으로 선전해왔다[8]. 올해 9월 우리 정부는 북한 AI 개발업체 '류경 프로그램 개발회사'와 관계자들을 대북제재 대상에 올렸는데, 이 업체 산하의 '기능정보기술 연구소'는 드론에 적용하기 위한 AI기술을 연구해온 것으로 드러났다[9].

드론에 AI기술을 적용하는 주요 목적 중 하나는 '군집(Swarm)' 운용을 가능케 하는 것이다. 드론의 비용적 이점을 극대화하여 많은 개체를 동시에 운용하면 방어자로 하여금 표적포화(Saturation)를 일으켜 소수를 운용할 때보다 훨씬 강력해진다. 우수한 방공능력으로 '신의 방패'라 불리우는 이지스(Aegis) 구축함을 대상으로 美 해군대학원에서 실시한 군집드론 대응 모의실험 결과는 단 8대의 드론만으로 이지스함의 방공망을 뚫고 타격에 성공하는 결과를 보여준 바 있다[10].

AI기술이 적용되지 않은 드론은 각 개체마다 개별적인 조종사가 요구되며, 조종기술 숙련도에 성패가 좌우된다. 사전에 좌표를 입력하는 방식으로 운용할 경우에는 조종사 없이도 다수 개체 운용이 가능하지만, 이동표적 및 시한성표적의 타격은 제한되는 한계가 있다.

그러나 AI기술을 적용하면 이러한 제한사항들의 극복이 가능해진다. 표적의 이미지를 딥러닝(Deep learning) 기반의 AI기술로 학습시켜 드론이 체공상태에서 표적을 스스로 탐지 및 인식, 추적, 타격하도록 운용할 수 있다. 이러한 드론을 수백, 수천 대를 동시에 체공시켜 군집의 형태로 운용한다면 현존하는 어떠한 방공수단으로도 이를 100% 방어하는 것은 불가능할 것이다[11].

북한의 도발 이후 우리 군은 적 드론 위협에 대응하기 위해 고출력 레이더와 전자기파를 활용한 신규 무기체계는 물론 재래식 방공전력을 포함한 대 드론 체계를 다방면으로 개발 및 도입하고 있다[12]. 그러나 타격체계 일변도의 전력구축은 군집 드론 대응에 명백한 한계가 존재한다. 더욱이 주 전장이 야전이나 해상인 육·해군과는 달리, 도심에 인접한 공군 비행단은 민가 피해와 아 항공기에 대한 물리적 피해, 전자적 영향이 우려되어 더더욱 가용한 드론 대응 수단이 제한되는 실정이다.

이에 본 연구에서는 AI기술이 적용된 적 군집드론의 공격으로부터 아 항공기의 생존성을 향상시키기 위해, 적 드론에 탑재된 객체인식 AI의 탐지를 회피하는 목적으로 적대적 머신러닝 기술(Adversarial Machine Learning) 중 하나인 적대적 예제(Adversarial Example)를 활용한 소극방공 기법을 제안하였고, 실험을 통해 검증하였다.

본 논문의 이후 구성은 다음과 같다. 2장에서는 배경지식과 관련 연구를 소개한다. 3장에서는 제안기법과 실제 적용 시의 양상을 시나리오 기반으로 기술한다. 4장에서는 실험결과를 통해 제안기법의 실효성을 검증하고 5장에서 결론을 맺고 향후 연구방향을 제시한다.

2. 배경지식 및 관련 연구

2.1 대 드론 체계 구분과 방공작전 유형

대 드론 체계는 드론을 식별하는 '탐지체계'와 탐지한

드론을 파괴 또는 무력화하는 '타격체계'로 구분할 수 있으며, 타격체계는 물리적 피해 유무에 따라 소프트킬(Soft kill)과 하드킬(Hard kill)로 다시 구분된다(표 1).

(표 1) 대 드론 체계 구분
(Table 1) Classification of anti-drone system

구분		세부체계		
탐지 체계		• 레이다, RF신호, EO/IR(열화상/광학), 음향 기반 드론 식별 및 추적		
타격 체계	소프트킬	전파교란(신호재밍)	스푸핑(기만)	
		• 주파수 교란으로 드론 제어 상실 유도	• 의도적 오동작신호, 오착륙 및 추락 유도	
	하드킬	고출력레이저	전자기파	재래식방공무기
		• 타격점 용융 및 파괴	• 내부 전자회로 및 부품 파괴	• 유도탄/분산탄

우리 군의 합동방공작전 교범에 따르면, 방공작전은 대응방법에 따라 적을 직접 격추 또는 무력화하는 '적극방공'과, 아군 피해를 최소화하기 위해 수행하는 '소극방공'으로 구분된다. 이와 같은 기준에서 표 1의 타격 체계들은 적극방공 수단에 해당된다. 반면에, 소극방공 수단에는 위장, 은폐, 엄폐, 기만, 소산, 시설 견고화, 등화관제 등이 있다. 위장은 적의 시각적 인식을 회피하기 위해 과거부터 전통적으로 적용되어온 소극방공 수단이다. 최근 러시아는 자폭 드론 공격에 대응하기 위해 전략폭격기 Tu-95의 동체와 날개위에 타이어를 쌓아두는 등의 소극방공 수단을 활용하는 양상을 보이기도 하였다(그림 1).

(그림 1) 항공기 소극방공 사례(Mig-29/F-16/Tu-95)
(Figure 1) Passive air defense case of aircraft

2.2 공군의 소극방공 중요성

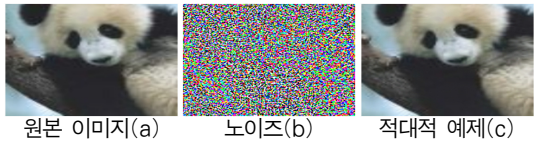
항공기는 구조적 특성상 소규모 자폭드론 타격에도 장기간 동안 가동이 중단되는 피해를 입을 수 있다. 캐노피를 공격하여 시야를 방해하거나, 조종사에 직접 피해를 입히거나, 공기흡입구(Air intake)에 의도적으로 빨려들어가 엔진 파괴를 도모하거나, 랜딩기어나 타이어를 공격하여 이·착륙 간 동체파손을 유도할 수도 있다(그림 2).

(그림 2) 드론 공격 시 예상 타격점
(Figure 2) Expected hit point in case of drone attack

일반적으로 공군의 항공자산들은 체공 중에는 드론의 위협이 그리 크지 않으나, 이·착륙 및 활주로 이동 시에는 적 드론의 공격에 매우 취약하다고 할 수 있다. 따라서 기지에 적 드론활동이 식별되면 신속히 이륙하거나 엄체호 내부로 대피할 때까지 적 드론 피해를 최소화할 수 있는 방공대책이 요구된다. 그러나 공군 비행단의 특성을 고려할 때, 적극방공 수단 운용 시 인접 민가피해 및 민항기 또는 아 항공기 피해 등 부차적 피해의 우려가 있다. 따라서 적 드론 위협에 대한 소극방공 수단의 강구와 활용이 더욱 중요한 의미를 가진다고 볼 수 있다.

2.3 적대적 예제

적대적 예제는 객체인식이 가능하도록 학습된 AI모델이 제대로 기능하지 못하도록 의도적으로 생성된 예제를 말하며, 이안 굿펠로(Ian Goodfellow)가 제안한 적대적 머신러닝 기술 중 하나이다[14]. 그림 3에서 판다 이미지(a)를 정상적으로 판다로 인식하는 AI모델이 있다고 가정할 때, 해당 AI가 제대로 기능하지 못하도록 의도적으로 생성된 노이즈(b)를 합성한 이미지(c)를 만든다. 즉, 사람의 눈에는 동일한 판다로 보이지만 AI모델은 긴팔원숭이로 오인식한다. 이때의 이미지(c)를 적대적 예제라 한다.



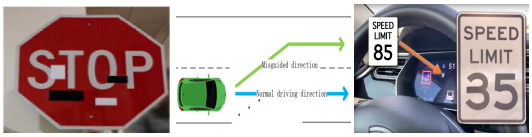
원본 이미지(a) 노이즈(b) 적대적 예제(c)

(그림 3) 적대적 예제 예시
(Figure 3) Examples of adversarial example

적대적 예제를 물리적 공간에서도 구현하고자 하는 후속 연구들이 수행되었다. 케빈(Kevin) 등은 정지(STOP) 표지판에 라벨을 부착, 물리적 노이즈를 가하여 객체인식 AI의 인식률을 저하시킬 수 있다는 점을 보였다(그림 4(a))[15]. 테슬라(Tesla)는 객체인식 AI기반으로 작동하는 자율주행기능인 오토파일럿(Auto pilot) 기능이 유명한데, 이에 대한 적대적 예제 연구사례로 텐센트(Tencent) 연구

진은 바닥에 흰색 마커 3개를 부착, 차선으로 오인식을 유도하여 의도하지 않은 차선 변경 수행됨을 보였다[16](그림 4(b)). 또한, 맥아피(McAfee) 연구진은 속도제한 표지판의 '35mph'에 검정 라벨을 부착하여 '85mph'로 오인식하게 함으로써 과속을 유도하였다[17](그림 4(c)).

상기 사례들은 물리적 공간에서 객체에 특정한 시각적 변화를 가하면 적대적 예제로서 작용하여 객체인식 AI의 탐지를 회피, 저하하는 것이 가능하다는 것을 보여준다.



케빈Kevin 등(a) 텐센트(b) 맥아피(c)

(그림 4) 물리적 공간에서 적대적 예제 연구 사례

(Figure 4) Study cases of adversarial example in physical domain

3. 제안기법

3.1 레이저를 활용한 적대적 예제 조사

앞에서 소개한 물리적 공간에서의 적대적 예제 연구사례에 착안하여, 본 연구에서는 이·착륙 및 활주로 상에서 이동하는 아 항공기를 자동으로 인식, 추적 및 타격하도록 학습된 객체인식AI 적용 자폭드론이 아 항공기를 제대로 인식하지 못하도록 항공기의 표면에 적대적 예제로 작용하는 시각적 변화를 일으키는 기법을 제안한다.

일반적으로 특정 객체 표면에 시각적인 변화를 가하려면 도색을 하거나 위장포를 씌우는 등의 물리적 노력이 요구된다. 그러나 이러한 방법을 가동 중인 항공기에 적용하기는 현실적으로 제한되며, 가능하더라도 갑작스런 공격에 신속한 대응이 어렵고, 위협이 제거되었을 때 원상복구도 용이하지 않다. 따라서 본 연구에서는 적대적 예제로서 작용하는 레이저빔을 항공기 표면에 조사(Projection)함으로써 즉각적인 시각적 변화를 달성할 수 있는 방안을 제안한다.

야외 건축물 외부 전체 또는 일부의 광범위한 면적에 레이저빔을 영상의 형태로 조사하는 '미디어 파사드'처럼, 항공기 전체에 레이저빔을 조사한다(그림 5). 단, 주간에는 면이 아닌 점의 형태의 레이저 패턴을 조사하여 시인성 증대를 도모한다.

(그림 5) 레이저 조사 예시

(Figure 5) Examples of laser projection

3.2 제안기법의 실제 적용 시나리오

제안기법의 이해를 돕기 위해 시나리오를 기반으로 실제 적용 양상을 기술한다(그림 6).

첫째, 객체인식 AI기술이 적용된 적 자폭드론이 기지 상공으로 침투한다(a). 둘째, 침투한 드론에 적용된 객체인식 AI가 표적인 아 항공기의 식별을 시도한다(b). 셋째, 아측은 탐지체계로 적 드론위협 상황을 인지한다(c). 넷째, 적대적 예제를 아 항공기에 조사한다(d). 다섯째, 적 드론의 AI는 아 항공기 인식을 실패한다(e). 여섯째, 출동 타격 전력이 적 드론을 제거한다(f).

(a) 적 드론 침투 (b) 표적 객체 인식 시도

(c) 적 드론 위협 식별 (d) 적대적 예제 조사

(e) 적 드론 인식 실패 (f) 적 드론 위협 제거

(그림 6) 제안기법 적용 시나리오

(Figure 6) Scenario of the proposed method

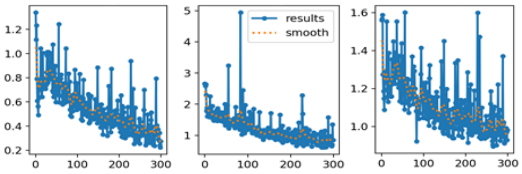
4. 구현 및 실험

본 제안의 실현 가능성 검증을 위한 실험을 수행하였다. 실제 항공기를 대상으로 하는 실험은 제한되기에 가상의 실험환경을 구축하였으며, 합성 이미지를 활용한 실험과 정밀 축소모형을 활용한 실험을 각각 실시하였다. 적대적 예제 적용여부에 따른 인식률 감소를 확인할 객체인식 AI모델은 웹기반 환경인 로보플로우(Roboflow)에

서 제공하는 YOLOv7모델을 활용하였다.

4.1 합성 이미지를 활용한 실험 결과

인터넷 공간에서 수집한 F-35A 항공기 이미지를 공개 이미지셋(MS COCO)을 활용하여 사전훈련(pre-trained)된 YOLOv7 모델을 298 에포크(epoch)로 전이학습하여 사용하였다. 훈련데이터 33개, 검증데이터 3개, 테스트데이터 1개의 총 37개 이미지를 사용하였으며, 훈련 과정의 로스(loss) 그래프는 다음과 같다(그림 7). 세로축은 로스율, 가로축은 에포크 수를 의미한다.



(a) localization (b) classification (c) confidence

(그림 7) 훈련과정에서의 로스(loss) 그래프
(Figure 7) Loss graph in training

해당 학습모델에서 원본 이미지의 인식률은 98%로 나타났다(그림 8(a)). 해당 원본 이미지에 적대적 예제를 레이저로 조사했을 경우를 가정하여 녹색의 점을 항공기 부분에 합성한 이미지를 생성하였고, 인식률을 확인할 결과 16%로 감소함을 확인할 수 있었다(그림 8(b)).

다른 이미지를 대상으로 진행한 반복 실험에서도 인식률은 96%(그림 8(c))에서 8%(그림 8(d))로 감소함을 보였다. 본 실험을 통해 적대적 예제 적용 전후의 객체인식 정확도의 감소를 확인하였다.

(a) 원본 이미지 A (b) A에 적대적 예제 적용

(c) 원본 이미지 B (d) B에 적대적 예제 적용

(그림 8) 합성 이미지를 활용한 실험 결과
(Figure 8) Experimental result using synthetic images

4.2 정밀 축소모형을 활용한 실험 결과

보다 더 현실적인 검증을 위해 1/72 비율의 F-35A 항공기 축소모형을 제작하여 실험을 수행하였다. 전이학습에 사용된 데이터는 항공기 축소모형을 직접 촬영하여 훈련데이터는 48개, 검증데이터 4개, 테스트데이터 3개를 활용하였으며, 훈련은 4.1과 같은 조건으로 수행하였다.

주간과 야간의 상황을 가정하여 각각 수행하였으며, 먼저 주간을 가정하여 그린 레이저 포인트를 활용하여 점 형태의 레이저빔을 조사하였다. 조사되는 레이저빔의 밀도와 유형을 변화시키며 인식률의 변화를 확인하였다. 적대적 예제를 레이저로 조사하기 전의 인식률은 약 95%를 보였으나, 조사 후에는 약 0~15%로 감소하는 결과를 보였다. 특히 모형 항공기에 조사되는 레이저빔의 밀도가 높을수록 인식률 감소폭이 증가하였다(그림 9).

(a) 최소 밀도 (b) 중간 밀도 (c) 최고 밀도

(그림 9) 정밀 축소모형을 활용한 실험 결과(주간)
(Figure 9) Experimental result using scale model(Day)

다음으로, 야간을 가정하여 면 형태의 레이저를 빔프로젝터를 활용하여 조사하였다. 인터넷 공간에서 수집한 미군의 위장 패턴과 임의의 기하학 패턴들을 적대적 예제로 활용하였다. 레이저 조사 전 인식률은 약 95%로 높게 나타났으나, 조사 후에는 0~12%로 감소함을 확인하였다. 또한, 적용 패턴에 따라 인식률 감소의 정도가 상이함을 확인하였다(그림10 (a)는 12%, (b)와(c)는 0% 내외).

(a) 미 육군위장 (b) 미 해군위장 (c) 기하학 패턴

(그림 10) 정밀 축소모형을 활용한 실험 결과(야간)
(Figure 10) Experimental result using scale model(night)

5. 결론 및 향후 연구

본 연구는 객체인식 AI가 적용되어 표적을 스스로 탐지하고 공격하는 적 자폭드론으로부터 아 항공기의 생존

성을 높일 수 있는 수단으로, 적대적 예제를 레이저로 조사하여 적 AI의 객체 인식률을 감소시키는 소극방공 기법을 제안하였다. 합성 이미지와 정밀 축소모형을 활용한 실험을 통해 실현 가능성을 검증하였고, 적대적 예제의 유형에 따라 인식률 저하정도가 상이함을 확인하였다.

제안기법이 객체인식 AI의 인식률을 저하하는 효과가 존재한다는 점은 확인하였지만, 실제 항공기의 구조적 특성을 반영한 피해 감소율과 생존성 향상 정도를 정량화하지는 못하였다. 그러나 이러한 정보들은 적에게 이로운 방향으로 악용될 우려가 있기에 군사보안의 측면에서 국방분야 공개 연구가 가진 일반적인 한계로 볼 수 있다.

실제 환경에서는 적의 AI기술 수준에 대한 합리적인 가정과 평가가 선행되어야 할 것이며, 적의 기술 수준 향상에 대응하기 위한 지속적인 추가 연구가 필요하다. 예를 들어, 적대적 예제가 어떠한 형태와 패턴으로 조사되었을 때 더 효과적인지, 대상 항공기의 형상이나 외부 도색의 색상, 주변 조도나 기상환경이 어떠한 영향을 미치는 지와 같은 다양한 후속 연구들이 요구된다.

본 연구는 기존의 타격체계와는 다른 시각에서 효과적인 대 AI 드론 방어수단을 제공하였다는 점에서 가장 큰 기여가 있다. 효과적인 드론 대응을 위해서는 적극방공과 소극방공 수단이 복합적으로 활용되어야 하는바, 우리 군의 드론 대응 능력 향상에 도움이 되길 기대한다.

참고문헌(Reference)

[1] Kunertova, Dominika, “Drones have boots: Learning from Russia’s war in Ukraine,” Contemporary Security Policy, 1-16, 2023. https://doi.org/10.1080/13523260.2023.2262792

[2] Borger, Julian, “The drone operators who halted Russian convoy headed for Kyiv,” The Guardian 28.03, 2022. https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv

[3] Kunertova, Dominika, “The war in Ukraine shows the game-changing effect of drones depends on the game,” Bulletin of the Atomic Scientists, 79.2, 95-102, 2023. https://doi.org/10.1080/00963402.2023.2178180

[4] Mia Jankowicz, “Ukraine claims it damaged prized Russian jets using ’cardboard’ drones from Australia in a daring raid,” Business insider, 30 Aug 2023. https://www.businessinsider.in/international/news/ukraine-claims-it-damaged-prized-russian-jets-using-cardboard-drones-from-australia-in-a-daring-raid/articleshow/103178331.cms last access: 10 Oct 2023)

[5] Don Shift, Poor Man’s Air Force: A guide to how small drones might be used in domestic unrest or low intensity conflicts, Independently published, 2023.

[6] Beuben johnson, “Why drones targeted a Russian A-50U, vital for hypersonic Kinzhal strikes,“ Breaking Defense, 2023. https://breakingdefense.com/2023/03/why-drones-targeted-a-russian-a-50u-vital-for-hypersonic-kinzhal-strikes

[7] Boulanin, Vincent, et al., “Artificial intelligence, strategic stability and nuclear risk,” 2020. CID: 20.500.12592/z6tfzg.

[8] Lim, Tai Wei, “North Korea’s artificial intelligence (AI) program,” North Korean Review, 15.2, 97-103, 2019. https://www.jstor.org/stable/26915828

[9] Si-young choi, “S. Korea sanctions N. Korean drone maker,” The Korea Herald, 1 Sep 2023. https://www.koreaherald.com/view.php?ud=20230901000529

[10] Pham, Loc V., et al., “UAV swarm attack: protection system alternatives for destroyers. Diss. Monterey,” California: Naval Postgraduate School, 2012. https://apps.dtic.mil/sti/citations/ADA573999

[11] Seungjoung Song, “Implications of drone warfare in the Ukraine War for future warfare,” Implications of the Ukraine War and Korea’s Defense Innovation, Royal company, 2023.

[12] Yonhap, S. Korea to introduce anti-drone defense system at key military, govt. facilities, the Korea Herald, 6 July 2023. https://www.koreaherald.com/view.php?ud=20230706000217&ACE_SEARCH=1

[13] Wonjin Jin, “A Review of Aircraft Camouflage Techniques to Reduce Visual Detection,” Journal of the Korea Academia-Industrial cooperation Society, Vol.21, No. 5, pp.60-636, 2020. https://doi.org/10.5762/KAIS.2020.21.5.630

[14] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy, “Explaining and harnessing adversarial examples,” arXiv preprint arXiv:1412.6572. 2014. https://doi.org/10.48550/arXiv.1412.6572

[15] Eykholt, Kevin, et al., “Robust physical-world attacks on deep learning visual classification,” Proceedings of the IEEE conference on CVPR, 2018. https://doi.org/10.1109/CVPR.2018.00175

[16] Tencent Keen Security Lab, “Experimental Security Research of Tesla Autopilot.” 2019. https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/

[17] McAfee “Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles,” 2020. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/)

◐ 저 자 소 개 ◑

육 심 언(Simun Yuk)
2010년 한국교원대학교 컴퓨터교육전공(교육학사)
2013년 아주대학교 정보통신대학원 정보보호/C4I전공(공학석사)
2023년 국방대학교 국방관리대학원 컴퓨터공학전공(군사학박사)
2023년~현재 공군 제17전투비행단 항공작전전대 통합체계운영대대 운영통제실장
관심분야 : 적대적 머신러닝 기술의 군사적 활용, 은닉통신(스테가노그래피), 사이버보안 등
E-mail : 6simun@gmail.com

박 휘 랑(Hweerang Park)
2010년 전남대학교 물리학전공(이학사)
2022년~현재 국방대학교 국방관리대학원 컴퓨터공학/사이버전협동전공(공학석사)
관심분야 : 스테가노그래피, 디지털포렌식, IoT보안, 사이버보안, 적대적 머신러닝 등
E-mail : sharku@mnd.go.kr, sharku7@gmaiil.com

서 태 석(Taisuk Suh)
2006년 공군사관학교 전산과학전공(공학사)
2020년 국방대학교 국방관리대학원 컴퓨터공학/사이버전협동전공(공학석사)
2020년~현재 공군 제17전투비행단 항공작전전대 통합체계운영대대 대대장
관심분야 : WSN보안, 사이버보안, 적대적 머신러닝 등
E-mail : corneli1202@gmail.com

조 영 호(Youngho Cho)
1998년 공군사관학교 산업공학전공(공학사)
2006년 연세대학교 컴퓨터산업시스템공학전공(공학석사)
2013년 University of Maryland, College Park, Electrical and Computer Engineering 전공(공학박사)
2017년~현재 국방대학교 국방관리대학원 컴퓨터공학 및 사이버전협동전공 교수
2022년~IEEE Senior Member
관심분야 : WSN보안, 신뢰메커니즘, 스테가노그래피 봇넷, 디지털포렌식, AI 보안, 적대적 머신러닝 등
E-mail : youngho@kndu.ac.kr, yhcho94@gmail.com