군용 드론/UAV에 대한 AI 적용과 사이버보안 취약요소에 관한 동향 연구

이형주*, 채웅**, 조영호(교신저자)***
*국방대학교 국방관리대학원 국방과학학부 사이버컴퓨터공학과 석사과정
**국방대학교 국방관리대학원 국방과학학부 사이버컴퓨터공학과 박사과정
***국방대학교 국방관리대학원 국방과학학부 사이버컴퓨터공학과 교수
e-mail: younghocho@korea.kr

A Trend Study on AI Applications and Cybersecurity Vulnerabilities in Military Drones/UAVs

Hyungjoo Lee*, Woong Chae**, Youngho Cho(Corresponding Author)***
*Master's Course, Dept. of Cyber Security and Computer Engineering, Korea National Defense University
**Ph.D. Course, Dept. of Cyber Security and Computer Engineering, Korea National Defense University
***Professor, Dept. of Cyber Security and Computer Engineering, Korea National Defense University

요 약

최근 군용 드론/UAV는 정찰과 감시를 넘어 타격, 자율비행, 군집 운용, 유·무인복합체계로 활용 범위를 빠르게 넓혀가고 있다. 이러한 변화의 중심에는 인공지능(AI)이 있으며, AI는 표적 탐지·식별, 자율기동, 경로계획, 군집 협업 기능을 고도화하면서 드론을 보다 능동적이고 지능적인 전장 자산으로 전환시키고 있다. 그러나 AI의 적용은 성능 향상과 더불어 새로운 보안 문제도 수반한다. 기존 드론 보안이 재밍, GPS 스푸핑, 지상통제체계(GCS) 침해와 같은 통신·항법 중심 위협에 초점을 맞추었다면, 최근에는 적대적 예제, 데이터 중독, 모델 추출, 백도어, 군집 의사결정 교란과 같은 AI 및 협업 구조 기반 위협까지 함께 고려해야 한다. 본 논문은 군용 드론/UAV의 AI 적용 동향을 정리하고, 기본 시스템 아키텍처와 복합 UAV의 기능 계층 구조를 기준으로 계층별 사이버보안 취약요소를 분석하였다. 이를 통해 향후 군용 드론 보안은 개별 구성요소 보호를 넘어 AI 기능과 운용 구조를 함께 고려하는 통합적 접근이 필요함을 제시한다.

1. 서 론

군용 드론/UAV는 전장 속에서 더 이상 보조 전력이 아닌 전투 양상을 바꾸는 핵심 수단으로 인식되고 있다. 러-우 전쟁에서 우크라이나는 '스파이더스 웹(Operation Spider's Web)' 작전을 통해 117대의 드론을 활용하여 4개의 러시아 공군기지를 동시 타격하였다. 또한, 최근 미국-이란 전쟁 국면에서는 전쟁 첫 주에만 1,000대가 넘는 드론이 발사되는가 하면, 저가의 드론을 대량 투입해 고가의 패트리어트 미사일을 소모시키는 공격 양상도 나타났다. 앞선 사례들은 드론이 단순 정찰 자산이 아니라 전략급 장거리 타격 등을 위한 핵심 자산으로 운용되고 있음을 보여주었다.

이와 같이 최근 드론 중심의 전장 변화에는 AI 기술이 중요한 역할을 하였다[1], [2], [4], [5]. 과거 군용 드론이 원격 조종과 영상 전송 중심의 체계였다면, 최근에는 표적을 탐지 및 식별하며, 장애물을 회피하고, 임무 경로를 조정하며, 나아가 군집 드론이 서로 역할을 나누어 효과적으로 임무를 수행하는 형태로 발전하고 있다. 즉, 현대전에서 AI는 드론 운용을 고도화하는 핵심 기술로 이해되고 있다.

그러나 AI 기반 드론의 확산은 새로운 보안 문제를 야기할 수 있다[3], [4], [5]. 기존 드론의 보안 문제가 통신 링크, 항법 신호, 지상통제체계 보호에 집중되었다면, AI 기반 드론에서는 입력 데이터 교란, 학습 데이터 오염 등과 같은 새로운 공격이 가능하다[3], [5], [7]. 또한, 군집드론과 유·무인 복합체계처럼 여러 플랫폼이 연결되는 구조에서는 개별 기체 수준의 오류가 전체 임무에 영향을 미칠 수 있다[6], [7].

따라서, 본 논문은 먼저 군용 드론/UAV의 AI 적용 동향을 조사하여 소개한 후, 드론의 기본 시스템 아키텍처와 복합 UAV의 기능 계층 구조를 기준으로 사이버보안 취약요소를 분석하고자 한다. 특히, 기존 드론 체계의 구조적 취약성, AI 적용에 따라 새롭게 부각되는 위협, 그리고 군집·유무인복합 운용 환경에서의 위협 확산 문제를 종합적으로 분석하여 향후 군용 드론 보안을 계층·운용 연계 관점에서 이해할 필요가 있음을 제시한다.

본 연구는 서울경제진흥원 '인공지능(AI) 기술사업화 지원사업'의 지원을 받아 수행된 연구임.(과제번호: CY250284_1_1)

2. 군용 드론/UAV의 AI 적용

2.1 전장 환경 변화와 AI 도입

최근 전장은 감시·정찰 정보가 폭증하고, 표적 식별과 결심 속도가 짧아지며, 통신 교란과 GPS 장애가 빈번하게 나타나는 환경으로 변화하고 있다. 여기에 병력 감소와 저비용 무인체계 확대까지 겹치면서 군용 드론은 단순 원격 비행체가 아니라 일정 수준의 자율성과 판단 능력을 갖춘 체계로 발전할 필요가 커졌다[1], [2]. 특히, AI 기반 공격용 드론 연구는 미래 전장에서 드론이 단순 보조 수단이 아니라 유·무인복합체계의 핵심 전력이 될 가능성을 강조했다[1].

이와 같은 변화는 단순히 드론의 성능이 향상된다는 의미로 끝나지 않는다. 과거 군용 드론이 영상 수집과 원격조종 중심의 보조 자산으로 인식되었다면, 최근에는 표적 탐지·식별, 자율기동, 임무 경로 수정, 군집 협업과 같은 기능을 통해 전장 의사결정 과정의 일부를 직접 담당하는 방향으로 발전하고 있다. 다시 말해, AI의 도입은 군용 드론을 단순한 비행 플랫폼이 아니라 "전장 정보를 수집·해석하고 이에 반응하는 지능형 작전 자산"으로 전환시키고 있다.

또한, 이러한 변화는 전장 운영 방식 자체에도 영향을 미친다. 감시·정찰 자산이 수집한 정보를 인간 운용자가 일일이 분석하고 결심하던 구조에서, 앞으로는 드론이 전장 상황을 선별적으로 인식하고 우선순위를 판단해 운용자의 부담을 줄이는 방향으로 발전할 가능성이 크다. 따라서, 군용 드론에 AI를 적용한다는 것은 비행 자동화 수준의 문제가 아니라, 전장 인식 속도와 작전 지속성을 동시에 높이는 문제로 이해할 필요가 있다[4], [5].

2.2 군용 드론의 주요 AI 적용 영역

AI 기술의 군용 드론 적용 영역은 [표 1]에서와 같이 크게 **인식, 기동, 협업**으로 나눌 수 있다.

첫 번째는 **인식 영역**이다. 전장에서는 무엇을 탐지하고 어떻게 분류하며 어떤 표적을 우선시할 것인가가 중요하므로, 컴퓨터 비전 기반의 표적 탐지, 객체 식별, 영상 분류, 이동 표적 추적 기능이 핵심으로 부각된다. [1]은 전자광학/적외선 기반 정찰장비에서 객체 추적, 객체 식별, 형상 인식 기술이 AI 공격용 드론의 핵심 기술이라고 설명하였다.

두 번째는 **기동 영역**이다. 군용 드론은 통신 두절, GPS 오차, 전파 교란, 복잡한 지형 속에서도 임무를 지속해야 하므로, 자율비행, 경로계획, 장애물 회피, 충돌 방지 기능이 중요하다. 예를 들어, [2]는 지능화 전장에서 드론 운용을 위해 충돌 감지, 거리 유지, 경로 원복 기능을 포함한 안전 비행 알고리즘이 필요하다고 제시하였다.

마지막은 **협업 영역**이다. 최근 군용 드론은 한 대의 기체가 모든 기능을 수행하기보다, 다수의 드론이 역할을 분담하는 방향으로 발전하고 있다. 이를 위해, [2]는 탈중앙식 지휘통제, 드론 간 임무 분석과 재할당, 통신 보안 강화를 군집드론 운용의 핵심 과제로 제시하였다.

[표 1] 군용 드론/UAV의 주요 AI 적용 영역

구 분	주요 기능	군사적 의미
인 식 영 역	표적 탐지, 객체 식별, 영상 분류, 이동 표적 추적	정찰·감시 효율 향상, 표적 획득 및 타격 정확도 향상
기 동 영 역	자율비행, 경로계획, 장애물 회피, 충돌 방지	조종 부담 감소, 생존성 향상, 임무 지속성 확보
협 업 영 역	군집 제어, 임무 재할당, 탈중앙 지휘통제	다수 플랫폼 운용, 유·무인 복합체계, 분산형 공격·정찰

2.3 AI 적용에 따른 드론 운용구조와 보안위협의 변화

AI가 적용된 군용 드론은 단순히 "더 편하게 조종되는 드론"이 아니라 임무 수행 구조 자체를 바꾸고 있다. 인식 영역에 적용되는 AI의 발전은 드론을 단순 영상 수집 장비에서 표적획득 수단으로 전환시키고 있으며, 기동 영역의 AI의 발전은 드론을 원격조종 장비에서 부분 자율형 비행체로 변화시키고 있다. 협업 영역의 AI의 발전은 군집드론과 유·무인복합체계와 같은 새로운 전투개념을 실제 운용 가능하게 만든다.

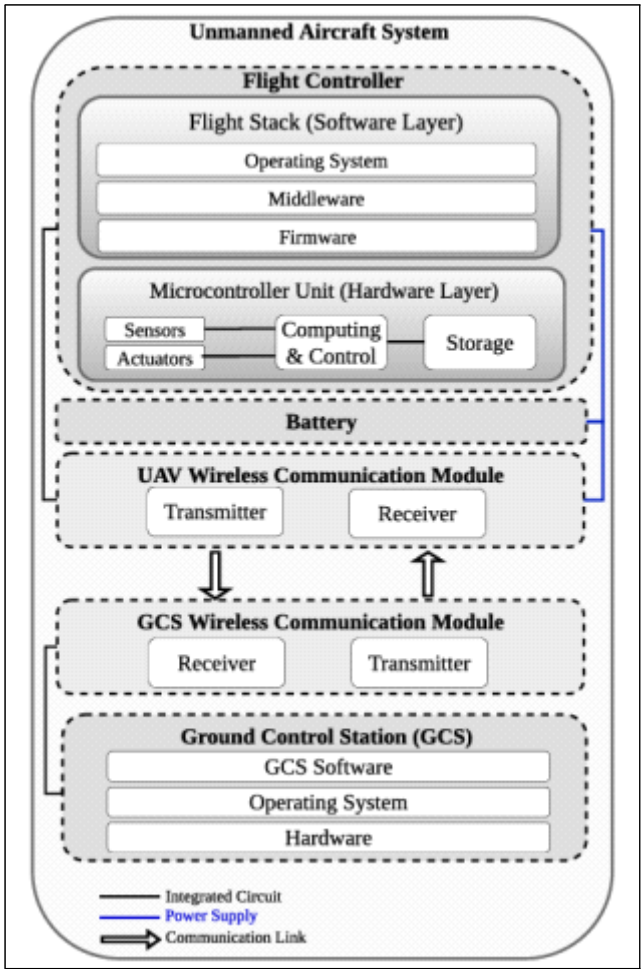
이러한 변화는 전장 운용의 기본 전제를 바꾸고 있다는 점에서 중요하다. 과거에는 드론 운용의 핵심이 "어떻게 안전하게 띄우고 조종할 것인가"에 있었다면, 이제는 "드론이 전장 상황을 어떻게 인식하고 어떤 방식으로 반응할 것인가"가 더 중요한 문제로 부상하고 있다. 즉, AI 적용은 개별 기체의 기능 향상을 넘어서 전장 인식, 기동, 협업 구조 전체를 재편하고 있다.

더 나아가 AI 적용은 보안 문제의 성격도 바꾸고 있다. 기존 드론 보안이 통신 링크 보호, 항법 신호 교란 방지, 지상통제체계 침해 방지와 같은 개별 기능 보호에 가까웠다면, AI 적용 이후에는 입력 데이터의 신뢰성, 학습 과정의 무결성, 모델의 검증 가능성, 협업 알고리즘의 안정성까지 함께 고려해야 하는 문제로 범위가 넓어졌다[3], [5]. 다시 말해, 운용구조가 복합화될수록 보안 역시 개별 장비 보호 수준이 아니라 체계 수준에서 재정의될 필요가 있다.

3. 군용 드론/UAV의 사이버보안 취약요소 분석

AI 기반 군용 드론의 보안 문제를 이해하기 위해서는 먼저 드론 체계가 어떠한 구조와 기능 계층 위에서 작동하는지를 살펴볼 필요가 있다. 기본적인 UAV 시스템은 비행제어기, 센서와 액추에이터, 저장장치, 무선통신 모듈, 배터리, 지상통제체계(GCS) 등으로 구성되며, 최근 연구는 여기에 자율성, 온보드 지능, 상황인식 기능이 결합되면서 UAV가 복합 사이버-물리 시스템으로 발전하고 있다고 보고 있다[4], [7].

3.1 UAV의 기본 아키텍처와 구조적 취약성



[그림 1] General architecture of an Unmanned Aerial Vehicle[4]

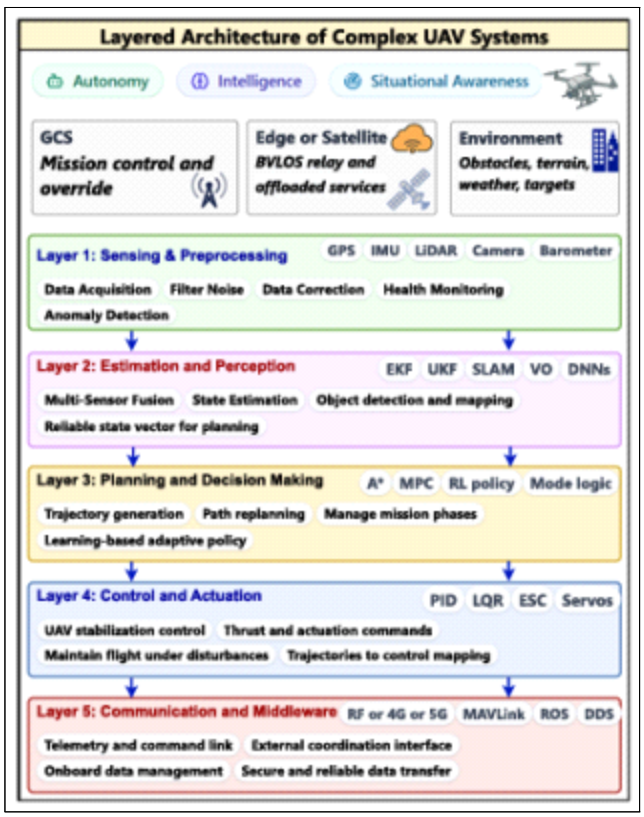
[그림 1]은 UAV 시스템이 비행제어기, 소프트웨어 스택, 마이크로컨트롤러 기반 하드웨어 계층, 무선통신 모듈, 지상 통제체계로 구성된다는 점을 보여준다[4]. 이러한 구조는 다양한 기능을 통합해 주지만, 동시에 각 구성요소가 잠재적 공격표면(Attack Surface)이 될 수 있다.

먼저, 센서와 액추에이터, 저장장치를 포함한 하드웨어 계층은 물리적 변조나 센서 입력 왜곡에 노출될 수 있다. 예를 들어, 센서 데이터가 의도적으로 교란되면 드론은 실제 위치나 자세를 잘못 추정할 수 있으며, 이는 항법 오류나 제어 불안정으로 이어질 수 있다. 또한, 펌웨어, 미들웨어, 운영체제 계층은 취약한 업데이트 절차나 악성코드 주입을 통해 침해될 수 있으며, 이 경우 비행제어 기능 자체가 공격자에게 노출될 가능성도 존재한다[4], [5].

특히, UAV와 GCS 사이의 무선통신 모듈은 군용 드론 보안에서 가장 오래되고도 중요한 취약 지점 중 하나이다. 이 구간은 명령·제어 신호와 텔레메트리 정보를 송수신하므로, 재밍, 도청, 하이재킹, 위조 명령 주입과 같은 전통적 공격에 취약하다[4], [5]. 특히, [5]는 UAV 보안 위협을 물리, 사이버, 사이버-물리 영역으로 구분하면서, 재밍, 가짜 메시지 주입, GPS 스푸핑 등을 대표적 위협 사례로 제시했다. 군용 드론은 민간 드론보다 통신 지속성, 항법 신뢰성, 임무 보안성이 훨씬 더 중요하므로, 이러한 전통적 취약성은 작전 정보 노출, 비행 경로 왜곡, 제어권 상실, 임무 실패로 직결될 수 있다.

또한, 이러한 구조적 취약성은 AI 기능이 탑재되었다고 해서 사라지지 않는다. 오히려 센서, 통신, 제어 계층의 불안정성은 상위 인식 및 의사결정 기능의 입력 품질을 저하시켜 AI의 오판단 가능성을 높일 수 있다. 결국, 군용 드론 보안의 출발점은 여전히 플랫폼, 항법, 통신, 제어 구조의 기본적 보호에 있으며, 이는 AI 기반 위협을 논하기 이전에 반드시 전제되어야 하는 기초 보안 영역이라고 할 수 있다.

3.2 복합 UAV의 기능 계층과 AI 기반 위협



[그림 2] Architectural overview of complex UAV system and its functional layers[7]

[그림 2]는 복합 UAV가 센싱 및 전처리, 추정 및 인식, 계획 및 의사결정, 제어 및 작동, 통신의 다섯 기능 계층으로 구성된다는 점을 보여준다[7]. 이 구조에서 AI는 주로 인식, 추정, 경로계획, 정책 선택과 같은 상위 기능을 가능하게 하는 핵심 기술로 작동한다. 문제는 AI 도입이 보안 위협의 범위를 데이터, 학습, 모델, 추론 단계로 확장시킨다는 데 있다.

대표적으로 적대적 예제 공격은 센서 입력이나 영상 데이터에 미세한 교란을 가해 표적을 오인식하게 만들 수 있으며, 이는 통신을 끊지 않고도 드론의 판단을 왜곡시킨다[3], [5], [7]. 예를 들어 [3]은 UAV 대상 AI 보안 공격을 적대적 예제 공격, 데이터 중독 공격, 모델 추출 공격으로 구분했으며, 각 공격이 인식·판단 기능의 신뢰성을 훼손할 수 있음을 정리했

다. 또한, 데이터 오염이나 백도어 공격은 모델의 학습 단계에 악성 데이터를 삽입하여, 특정 조건이 충족될 때만 오작동하도록 만들 수 있다. 즉, 평시에는 정상적으로 보이기 때문에 식별이 어렵고, 실제 작전 환경에서 특정 표적 또는 특정 조건에서만 오작동을 유발할 수 있다는 점에서 치명적이다.

결국 AI 기반 드론 보안은 더 이상 통신 보호만의 문제가 아니다. 입력 데이터의 신뢰성, 학습 데이터의 무결성, 모델의 검증 가능성, 실시간 추론의 안정성을 함께 고려해야 하는 문제로 바뀌고 있다.

3.3 군집·유무인복합 운용 확장에 따른 위협

AI 기반 드론의 보안 문제가 더 복잡해지는 지점은 군집드론과 유·무인복합 형태로 확장된 운용 환경이다. [그림 2]의 계층 구조는 각 기능이 독립적으로 존재하는 것이 아니라 상호 연동된다는 점을 보여준다[7]. 따라서, 센싱 계층에서 발생한 작은 이상은 인식과 추정 계층을 거쳐 계획 및 의사결정에 영향을 주고, 최종적으로 제어와 통신 계층에 누적되어 임무 수준의 실패로 이어질 수 있다. 예를 들어, [7]은 GPS 오염이 상태 추정 오류, 경로계획 왜곡, 제어 불안정으로 연쇄적으로 확산될 수 있음을 설명했다. 또한 [6]은 군집 UAV 네트워크를 centralized, distributed, hybrid architectures로 구분하면서, 중앙집중형 구조의 SPoF(Single Point of Failure) 위험과 군집 네트워크 전반의 데이터 변조, 라우팅 교란, 명령 전달 실패 가능성을 지적했다. 특히 군집 환경에서는 악성 또는 손상된 드론 노드가 허위 위치·상태·표적 정보를 전파하거나 협업 절차를 교란할 경우, 그 영향이 개별 기체에 머무르지 않고 전체 군집의 임무 수행 실패로 확대될 수 있다. [2] 역시 급변하는 전장에서는 이러한 문제에 대응하기 위해 탈중앙 지휘통제와 임무 재할당 기능이 중요하다고 보았다.

결국 군집 환경에서는 개별 드론의 인식 오류나 통신 이상이 충돌 회피, 공격 순서 결정, 편대 유지 실패로 증폭될 수 있으며, 유·무인복합체계에서는 이러한 이상이 유인 플랫폼의 상황인식과 결심에도 영향을 줄 수 있다. 따라서 향후 군용 드론 보안은 개별 취약점 봉합이 아니라, 플랫폼 보호, AI 모델 검증, 협업 알고리즘 안정성, 통신·항법 보안, 이상 전파 통제를 함께 고려하는 통합적 접근이 필요하다.

논의한 계층별 주요 취약요소를 정리하면 [표 2]와 같다.

[표 2] 군용 드론/UAV의 계층별 주요 사이버보안 취약요소

구 분	대표 위협	주요 계층	예상 피해/영향
구조적 취약성	재밍, GPS 스푸핑, 하이재킹, GCS 침해	통신·항법·제어·플랫폼	비행 경로 왜곡, 제어권 상실, 정보 유출
AI 기반 위 협	적대적 예제, 데이터 중독, 모델 추출, 백도어 공격	입력·학습·모델	오인식, 오판단, 은닉된 오작동
운 용 확 장 위 협	군집 의사결정 교란, 임무 재할당 오류, 계층 간 이상 전파	협업·지휘통제·네트워크	편대 붕괴, 임무 실패, 체계 신뢰도 저하

4. 결 론

본 논문은 군용 드론/UAV의 AI 적용 동향을 정리하고, 이를 바탕으로 기본 시스템 아키텍처와 복합 UAV의 기능 계층 구조를 기준으로 계층별 사이버보안 취약요소를 분석하였다. 군용 드론은 정찰과 감시를 넘어 타격, 자율비행, 군집 운용, 유·무인복합체계로 활용 범위를 넓혀가고 있으며, 이 과정에서 AI는 인식, 기동, 협업 기능을 가능하게 하는 핵심 기술로 자리 잡고 있다.

그러나 이러한 발전은 기존의 재밍, GPS 스푸핑, GCS 침해와 같은 전통적 위협 위에 적대적 예제, 데이터 중독, 모델 추출, 백도어와 같은 AI 고유의 위협을 추가하고, 나아가 군집·복합 운용 환경에서는 계층 간 이상 전파와 체계 수준의 임무 실패 가능성을 증폭시킨다. 따라서 향후 군용 드론 보안은 개별 취약점을 분절적으로 보완하는 방식으로는 충분하지 않다. 기본 플랫폼과 통신구조 보호, AI 모델과 데이터 검증, 군집 협업 알고리즘의 안정성 확보, 이상 전파 통제를 하나의 연속된 체계로 통합해 접근해야 한다.

참고문헌

[1] 길병옥, “인공지능(AI) 기반 공격용 드론의 효과적 전력화방안에 관한 연구,” 한국군사학논총, 제12집 제4권, pp. 75-99, 2023년.

[2] 채희, 이경석, 엄정호, “지능화 전장에서 인공지능 기반 공격용 군집드론 운용 방안,” 융합보안논문지, 제23권 제3호, pp. 65-71, 2023년.

[3] 진미리, 최윤성, 이학준, “UAV 대상 AI 보안 공격 현황 및 대응 방안 연구,” 한국산업보안연구, 제14권 제1호, pp. 9-29, 2024년.

[4] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, “A Survey on Security and Privacy Issues of UAVs,” Computer Networks, vol. 224, Art. 109626, 2023년.

[5] Z. Yu, Z. Wang, J. Yu, D. Liu, H. H. Song, and Z. Li, “Cybersecurity of Unmanned Aerial Vehicles: A Survey,” IEEE Aerospace and Electronic Systems Magazine, vol. 39, no. 9, pp. 182-215, 2024년.

[6] X. Wang, Z. Zhao, L. Yi, Z. Ning, L. Guo, F. R. Yu, and S. Guo, “A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures,” ACM Computing Surveys, vol. 57, no. 3, Art. 74, 2024년.

[7] M. I. Umrani, B. Butler, A. O’Driscoll, and S. Davy, “Toward Secure Complex UAV Cyber-Physical Systems: A Unified Threat Taxonomy and Cross-Layer Survey of Cybersecurity Challenges,” Internet of Things, vol. 37, Art. 101902, 2026년.