



Received: 2026/07/28
Revised: 2026/08/10
Accepted: 2026/08/25
Published: 2026/09/30

***Corresponding Author:**

Myunghoon Park

333 Pangyo-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 13488, Republic of Korea

Tel: +82-31-5179-7267

Fax: +82-31-5179-7086

E-mail: pmh604god@gmail.com

위협평가 기반 Counter-UAS 대응 의사결정 프레임워크

Threat Assessment-Based Counter-UAS Response Decision-Making Framework

박명훈*, 김정, 이성균, 고진용, 장재덕

LIG 디펜스&에어로스페이스 M&S팀 수석연구원

Myunghoon Park*, Jeong Kim, Sungkyun Lee, Jinyong Go, Jaedeok Jang

Chief research engineer, M&S Team, LIG Defense&Aerospace

Abstract

최근 비인가 무인기에 의한 위협이 증가함에 따라 counter-UAS 체계에서는 탐지 및 식별뿐만 아니라 위협평가와 대응 의사결정의 중요성이 더욱 커지고 있다. 그러나 기존 연구는 탐지 성능 향상이나 위협평가 기법에 주로 초점을 두고 있어, 위협평가 결과를 실제 대응수단 선택으로 연결하는 통합적인 의사결정 프레임워크는 상대적으로 부족하다. 본 논문에서는 다중센서 정보와 운용환경 정보를 기반으로 위협을 평가하고, 대응 권한 및 안전성을 함께 고려하는 위협평가 기반 counter-UAS 대응 의사결정 프레임워크를 제안하였다. 또한 대표 운용 시나리오를 통해 제안 프레임워크의 적용 절차와 활용 방안을 제시하여 실제 counter-UAS 운용환경에서의 적용 가능성을 설명하였다.

As threats posed by unauthorized unmanned aerial systems (UASs) continue to increase, counter-UAS systems require not only reliable detection and identification but also effective threat assessment and response decision making. However, existing studies have primarily focused on improving detection performance or threat assessment methods, while integrated decision-making frameworks that connect threat assessment results to response selection remain limited. This study proposes a threat-assessment-based counter-UAS decision-making framework that integrates multi-sensor information, operational context, response authority, and safety constraints. Representative operational scenarios are presented to illustrate the application procedure and potential utilization of the proposed framework in practical counter-UAS environments.

Keywords

무인기 대응(Counter-UAS),
위협평가(Threat Assessment),
대응 의사결정(Response Decision Making),
다중센서 융합(Multi-Sensor Fusion),
의사결정 프레임워크(Decision-Making Framework)

1. 서론

최근 상용 무인항공기의 보급과 운용 범위 확대에 따라 공항, 군사시설, 국가 중요시설 및 대규모 행사장 주변에서 발생하는 비인가 무인기 위협이 증가하고 있다. 소형 무인기는 낮은 고도에서 비행하고 레이더 반사면적이 작아 탐지가 어려우며, 감시, 정보수집, 시설 교란 및 직접적인 공격 수단으로 활용될 수 있다. 이에 따라 비인가 무인기를 탐지·식별·추적하고 적절한 대응수단을 적용하기 위한 counter-unmanned aircraft system(counter-UAS)의 중요성이 지속적으로 증가하고 있다.

Counter-UAS 체계는 일반적으로 레이더, 무선주파수, 전자광학·적외선 및 음향센서를 이용한 탐지·식별 단계와 전파방해, 포획 및 물리적 무력화 등을 이용한 대응단계로 구성된다[1-3]. 기존 연구는 주로 소형 무인기의 탐지확률과 분류 정확도를 향상하고, 다중센서 융합을 통해 단일 센서의 제한을 보완하는 데 중점을 두어 왔다. 그러나 실제 운용환경에서는 무인기가 탐지되었다는 사실만으로 즉각적인 대응을 수행할 수 없다. 탐지된 표적의 비행승인 여부, 보호대상에 대한 접근 의도와 공격능력, 대응수단 적용에 따른 공역 안전 및 부수피해 가능성을 함께 고려해야 하기 때문이다.

JAPCC는 counter-UAS 운용을 억제, 회피, 탐지, 의사결정 및 무력화가 연계된 단계적 절차로 제시하였다[4]. 또한 remote ID 및 UAS traffic management 정보를 이용하여 탐지 표적의 적법성을 추가로 확인하는 연구가 수행되었으며[5] 표준화된 위협 시나리

오와 성능지표를 이용하여 counter-UAS 체계의 성능을 평가하려는 연구도 진행되고 있다[6,7]. 최근에는 이질적인 센서정보와 운용정보를 퍼지 추론으로 결합하여 무인기의 위협수준을 정량적으로 평가하려는 연구가 제안되었다[8].

그러나 기존 연구는 탐지·식별 성능이나 위협수준 산정에 비해, 산정된 위협도를 실제 대응수단 선택으로 연결하는 의사결정 구조를 충분히 제시하지 못하고 있다. 특히 위협도가 높더라도 대응 권한이 없거나 전파간섭 및 부수피해 위험이 큰 경우에는 강제 대응을 제한해야 한다. 반대로 위협도가 중간 수준이더라도 보호대상의 중요도가 높고 접근시간이 짧다면 신속한 대응이 필요하다. 미국 연방항공청과 국제민간항공기구 역시 counter-UAS 운용에서 위협평가뿐 아니라 공역 안전성, 운용 권한, 지역별 비상대응계획 및 대응절차를 함께 고려해야 함을 제시하고 있다[9,10].

따라서 counter-UAS 대응 의사결정은 탐지 결과를 대응수단으로 직접 연결하는 방식이 아니라, 센서 불확실성과 상황정보를 이용한 위협평가, 합법성·안전성 검토 및 대응수단 선택이 순차적으로 연계된 구조로 설계되어야 한다.

본 논문에서는 다중센서 탐지정보와 운용환경 정보를 이용하여 무인기의 위협수준을 평가하고, 이를 적절한 대응수단 선택으로 연결하는 위협평가 기반 counter-UAS 대응 의사결정 프레임워크를 제안한다. 제안 프레임워크는 무인기의 의도, 능력, 보호대상 접근성 및 시간적 긴급성을 평가하는 위협평가 계층과 비행승인 여부, 대응 권한, 공역 안전 및 부수피해 가능성을 검토하는 대응 게이트로 구성된다. 이후 평가된 위협수준과 대응 제약조건에 따라 관찰, 추가확인, 봉쇄 및 무력화 등 적절한 대응단계를 결정한다.

제안 방법의 주요 특징은 다중센서의 신뢰도와 상황정보를 결합하여 위협수준을 평가하고, 위협평가와 대응수단 사이에 합법성·안전성 검토단계를 적용하며, 대응결과를 설명할 수 있는 규칙기반 구조를 제공한다는 점이다. 또한 표준화된 위협 시나리오를 기반으로 위협평가 정확도뿐 아니라 의사결정 지연시간, 과잉대응률 및 대응누락률을 이용하여 제안 방법의 성능을 평가한다.

본 논문의 구성은 다음과 같다. 제2장에서는 counter-UAS 대응 의사결정의 요구사항을 분석하고, 제3장에서는 제안하는 위협평가 및 대응수단 선택

프레임워크를 설명한다. 제4장에서는 시뮬레이션 환경과 성능평가 방법을 제시하며, 제5장에서는 시뮬레이션 결과를 분석한다. 마지막으로 제6장에서 결론을 제시한다.

2. Counter-UAS 대응 의사결정 요구사항

2.1 Counter-UAS 체계의 구성과 운용절차

Counter-UAS는 비인가 무인기를 탐지하고 적절한 대응을 수행하기 위한 통합 방어체계로, 일반적으로 탐지(detection), 식별(identification), 추적(tracking), 위협평가(threat assessment), 대응(neutralization) 단계로 구성된다[1-4]. 초기 counter-UAS 연구에서는 각 단계를 독립적인 기능으로 다루는 경우가 많았으나, 최근에는 탐지부터 대응까지의 과정을 하나의 의사결정 체계로 통합하는 방향으로 발전하고 있다[2,4].

탐지 단계에서는 레이더, RF 수신기, EO/IR 카메라 및 음향센서와 같은 이질적인 센서를 이용하여 무인기의 존재를 탐지한다. 각 센서는 운용환경에 따라서 다른 장단점을 가지므로 단일 센서만으로 모든 상황에서 안정적인 탐지 성능을 확보하기 어렵다. 따라서 최근 counter-UAS 체계는 복수 센서의 정보를 융합하여 탐지 신뢰도를 향상시키는 다중센서 구조를 기본적으로 적용하고 있다[1-3].

탐지된 표적은 식별 및 추적 단계를 거쳐 항적정보와 비행특성을 생성한다. 이 과정에서는 위치, 속도, 고도 및 접근방향과 같은 운동학 정보뿐 아니라 RF fingerprint, EO/IR 특징량, radar cross section(RCS) 및 분류기의 신뢰도 등이 함께 추출된다. 이러한 정보는 단순한 표적 추적을 넘어 무인기의 의도와 위협도를 판단하기 위한 기초자료로 활용된다[1,2].

그러나 실제 counter-UAS 운용에서 가장 중요한 단계는 탐지 이후의 위협평가와 대응결정이다. 동일한 탐지 결과라도 보호대상과의 거리, 접근속도, 비행패턴 및 운용환경에 따라 실제 위협수준은 크게 달라질 수 있다. 또한 허가된 무인기와 비인가 무인기를 구분하지 못한 상태에서 즉각적인 대응을 수행할 경우 불필요한 임무중단이나 안전사고를 초래할 수 있다. 따라서 최근 연구에서는 탐지결과 자체보다 이를 이용한 위협평가와 대응 의사결정의 중요성이 더욱

강조되고 있다[4,5].

FAA와 ICAO는 counter-UAS 운용 시 탐지결과만으로 대응수단을 결정해서는 안 되며, 비행승인 여부, 공역 안전성, 대응 권한 및 운용환경을 종합적으로 고려하도록 권고하고 있다[9,10]. 이는 counter-UAS 체계가 단순한 감시장비가 아니라 상황인식과 지휘결심을 포함하는 운용체계임을 의미한다.

따라서 본 연구에서는 기존 counter-UAS 운용절차를 기반으로 탐지, 식별 및 추적 결과를 이용하여 위협수준을 평가하고, 합법성과 안전성을 검토한 후 적절한 대응수단을 선택하는 의사결정 프레임워크를 제안한다.

2.2 무인기 위협평가 요소

Counter-UAS 체계에서 위협평가는 탐지된 무인기의 위협도를 정량적 또는 정성적으로 평가하여 적절한 대응 수준을 결정하는 과정이다. 동일한 무인기라 하더라도 운용 목적, 접근 경로 및 주변 환경에 따라 실제 위협 수준은 크게 달라질 수 있으므로 단순한 탐지 여부만으로 대응을 결정하는 것은 적절하지 않다. 따라서 최근 counter-UAS 연구에서는 센서에서 획득한 다양한 정보를 종합하여 위협도를 산정하는 방법이 활발히 연구되고 있다[5,8].

기존 연구에서는 위협평가를 위해 표적의 운동학적 특성, 표적 특성, 운용환경 정보를 주로 활용한다. 운동학적 특성에는 위치, 속도, 고도, 접근방향 및 예상 도달시간 등이 포함되며, 이는 보호대상에 대한 접근 가능성과 시간적 긴급성을 판단하는 핵심 요소이다. 표적 특성은 RF fingerprint, radar cross section(RCS), EO/IR 영상 특징 및 센서 분류 신뢰도 등을 포함하며, 탐지된 객체가 실제 위협 표적인지 판단하는 근거로 활용된다[1,2].

최근에는 보호대상의 중요도와 비행승인 여부 등 상황정보(context information)의 중요성이 강조되고 있다. Remote ID와 UTM 정보를 이용하면 허가된 비행인지 여부를 확인할 수 있으며, 공항·군사시설·국가 중요시설과 같은 보호대상 정보는 동일한 비행행위라도 서로 다른 위협수준으로 평가될 수 있음을 의미한다[5,9,10].

위협평가 알고리즘으로는 규칙기반(rule-based), 베이저안 네트워크(bayesian network), 퍼지 추론

(fuzzy inference) 등이 대표적으로 사용된다. 규칙기반 방법은 구현이 단순하고 설명가능성이 높지만 복잡한 운용환경을 반영하기 어렵다. 베이저안 기반 방법은 센서 불확실성과 조건부 확률을 효과적으로 처리할 수 있으나 사전확률 설정에 따라 결과가 달라질 수 있다. 퍼지 추론은 다양한 센서정보와 운용정보를 연속적인 위험도로 표현할 수 있어 최근 counter-UAS 위협평가분야에서 활발히 적용되고 있다[8].

그러나 대부분의 연구는 위협수준을 산정하는 단계까지를 주요 연구범위로 설정하고 있으며, 산정된 위협도를 실제 대응수단 선택으로 연결하는 의사결정 구조는 상대적으로 제한적으로 다루고 있다. 따라서 counter-UAS 대응체계에서는 위협평가 정확도뿐 아니라 위협평가 결과를 실제 운용결심으로 연결하는 체계적인 의사결정 절차가 함께 요구된다.

2.3 대응결심 시 고려해야 할 운용 및 법적 제약

Counter-UAS 운용환경에서는 위협도가 높다고 판단되더라도 모든 상황에서 동일한 대응수단을 적용할 수 있는 것은 아니다. 대응 과정에서는 기술적 성능뿐 아니라 법적 권한, 공역 안전성 및 부수피해 가능성을 동시에 고려해야 하며, 이러한 제약조건은 실제 운용결심에 직접적인 영향을 미친다.

FAA는 무인기 탐지 및 대응체계의 운용에서 탐지 기술과 대응기술을 구분하여 관리할 필요가 있으며, 대응수단 적용 시에는 항공안전, 전파간섭 및 제도적 권한을 함께 검토해야 함을 제시하였다[9]. ICAO 역시 민간항공 기반시설 보호를 위해 위협평가, 대응승인 및 사후조치가 연계된 위협기반 대응절차를 권고하고 있으며, 지역별 비상대응계획과 정보공유 체계를 포함한 운용절차를 제시하고 있다[10].

또한 remote ID와 UTM 정보는 탐지된 무인기의 비행승인 여부를 확인할 수 있는 중요한 정보원이다. 허가된 무인기를 비인가 표적으로 오인하여 대응하는 경우 불필요한 운용중단과 사회적 비용이 발생할 수 있으므로, 최근 연구에서는 센서 탐지결과와 비행관리 정보를 함께 활용하여 대응의 적법성을 확인하는 절차가 제안되고 있다[5].

이와 함께 보호대상의 중요도와 주변 운용환경도 대응수단 선택에 영향을 미친다. 예를 들어 동일한 위협수준이라 하더라도 군사시설, 공항 및 국가 중요시

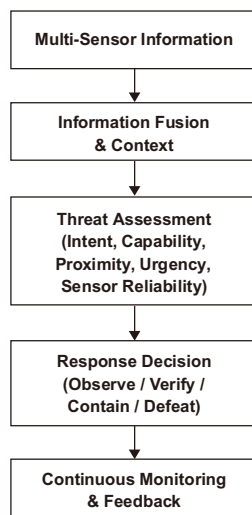


Fig. 1. Proposed threat assessment-based Counter-UAS decision-making framework

설에서는 보다 신속한 대응이 요구될 수 있으며, 반대로 도심지역에서는 전파방해나 물리적 무력화로 인한 부수피해 가능성을 우선적으로 고려해야 한다. 따라서 대응수단은 위협도만을 기준으로 선택하는 것이 아니라 임무 중요도, 시간적 긴급성 및 안전성을 함께 고려하는 다기준 의사결정 과정으로 수행되어야 한다.

이상의 분석을 통해 기존 counter-UAS 연구는 탐지기술과 위협평가 방법은 지속적으로 발전하였으나, 위협평가 결과를 운용환경과 법적 제약을 반영한 대응결심으로 연결하는 통합 의사결정 프레임워크는 아직 충분히 제시되지 않았음을 확인할 수 있다. 따라서 본 논문에서는 다중센서 정보와 상황정보를 기반으로 위협도를 산정하고, 합법성·안전성 검토를 거쳐 대응수단을 선택하는 위협평가 기반 counter-UAS 대응 의사결정 프레임워크를 제안한다.

3. 위협평가 기반 Counter-UAS 대응 의사결정 프레임워크

본 장에서는 제안하는 위협평가 기반 counter-UAS 대응 의사결정 프레임워크를 설명한다. 기존 counter-UAS 연구는 탐지 및 식별 성능 향상과 위협수준 평가에 중점을 두었으나, 위협평가 결과를 실제 대응수단 선택으로 연결하는 통합적인 의사결정 구조는 충분히 제시하지 못하였다. 따라서 본 연구에서는 다중센서 정보와 운용환경 정보를 통합하여 위

협수준을 산정하고, 운용 및 법적 제약을 고려하여 대응수단을 선택하는 계층형 의사결정 프레임워크를 제안한다.

3.1 프레임워크 전체 구조

제안하는 프레임워크는 센서 정보 수집, 상황정보 융합, 위협평가, 합법성 및 안전성 검토, 대응수단 결정의 다섯 단계로 구성된다.

먼저 레이더, RF 수신기, EO/IR 및 음향센서로부터 탐지정보를 수집하고, 각 센서의 신뢰도를 고려하여 표적정보를 생성한다. 이후 remote ID, UTM 정보, 보호대상 중요도, 공역 정보 및 운용환경과 같은 상황정보를 함께 융합하여 위협평가에 필요한 입력데이터를 구성한다.

위협평가 단계에서는 표적의 의도(intent), 능력(capability), 접근성(proximity) 및 시간적 긴급성(urgency)을 종합적으로 고려하여 위협수준을 산정한다. 이후 위협평가 결과는 곧바로 대응수단으로 연결되지 않고, 대응 권한, 공역 안전성 및 부수피해 가능성을 검토하는 합법성·안전성 게이트(legality and safety gate)를 통과한다. 마지막으로 위협수준과 운용 제약조건을 함께 고려하여 최종 대응수단을 결정한다.

기존 연구는 위협평가 이후 대응단계를 단순히 연결하거나 독립적으로 수행하는 경우가 많았다. 그러나 실제 운용에서는 동일한 위협수준이라도 운용환경과 대응 권한에 따라 적용 가능한 대응수단이 달라질 수 있다. 따라서 본 연구에서는 위협평가와 대응결정 사이에 합법성 및 안전성 검토 단계를 추가하여 실제 운용환경을 보다 현실적으로 반영하였다.

3.2 위협평가 모델

제안 프레임워크에서는 탐지된 무인기의 위협수준을 의도, 능력, 접근성, 시간적 긴급성 및 센서 신뢰도를 이용하여 평가한다. 각 평가요소는 서로 다른 물리량과 범위를 가지므로, 위협도 산정에 앞서 0에서 1 사이의 값으로 정규화한다. 정규화된 값이 0에 가까울수록 위협 기여도가 낮고, 1에 가까울수록 해당요소가 위협도에 미치는 영향이 큰 것으로 정의한다.

의도 I는 무인기의 비행경로, 보호대상에 대한 접

근방향, 반복 선회 및 체공과 같은 비행행태를 기반으로 적대적 접근 가능성을 나타낸다. 능력 C 는 비행속도, 탑재 가능 중량 및 운용 지속시간 등을 이용하여 무인기가 실제 피해를 유발할 수 있는 정도를 나타낸다. 접근성 P 는 보호대상과 무인기 사이의 거리와 접근속도를 이용하여 목표에 도달할 가능성을 평가한다. 시간적 긴급성 U 는 무인기가 보호대상에 도달하기까지 남은 시간을 기반으로 대응의 시급성을 나타낸다. 센서 신뢰도 R 는 레이더, RF, EO/IR 및 음향센서의 탐지·분류 신뢰도를 융합한 값으로 정의한다.

Table 1. Threat assessment parameters used in the proposed framework

Category	Input variable	Unit	Description
Intent	Flight path, approach angle, loitering pattern	–	Hostile Flight Intent
Capability	Flight speed, payload capacity, endurance	m/s, kg, min	Damage Infliction Capability
Proximity	Distance and closing velocity	m, m/s	Accessibility to Protected Assets
Urgency	Estimated time to target	s	Response Time Urgency
Sensor reliability	Radar, RF, EO/IR, and acoustic confidence	–	Reliability of Threat Assessment Input Information

Table 1은 제안 위협평가 모델에 사용되는 주요 입력요소와 물리적 단위를 나타낸다. 각 입력값은 서로 다른 단위와 범위를 가지므로 위협도 산정 전에 0에서 1 사이의 값으로 정규화한다. 이를 기반으로 최종 위협도는 다음과 같이 계산한다.

$$T = w_I I + w_C C + w_P P + w_U U + w_R R \quad (1)$$

여기서 T 는 최종 위협도로서 무차원 값이며 $0 \leq T \leq 1$ 의 범위를 갖는다. I , C , P , U 및 R 은 각각 정규화된 의도, 능력, 접근성, 시간적 긴급성 및 센서 신뢰도를 나타내며 모두 무차원 값이다. w_I , w_C , w_P , w_U 및 w_R 은 각 위협요소의 상대적 중요도를 나타내는 가중치로서 다음 조건을 만족한다.

$$w_I + w_C + w_P + w_U + w_R = 1 \quad (2)$$

가중치는 방호대상의 특성과 운용환경에 따라 설정할 수 있다. 예를 들어 군사시설이나 국가 중요시설과 같이 표적 접근 자체가 높은 위험을 의미하는 환경에서는 접근성과 시간적 긴급성의 가중치를 상대적으로 크게 설정할 수 있다. 반면 공항이나 도심지역에서는 허가 비행과 비인가 비행의 구분이 중요하므로 의도와 센서 신뢰도의 가중치를 높게 설정할 수 있다. 본 연구의 시뮬레이션에서는 각 평가요소의 영향을 균형 있게 비교하기 위해 동일 가중치를 기본값으로 적용한다.

시간적 긴급성은 보호대상까지의 예상 도달시간을 이용하여 다음과 같이 산정한다.

$$U = \begin{cases} 1 - \frac{t_{arr}}{t_{max}}, & 0 \leq t_{arr} < t_{max} \\ 0, & t_{arr} \geq t_{max} \end{cases} \quad (3)$$

여기서 t_{arr} 은 현재 위치와 접근속도로부터 계산한 예상 도달시간으로 단위는 초(s)이며, t_{max} 는 위협평가에 반영하는 최대 기준시간으로 단위는 초(s)이다. 예상 도달시간이 짧을수록 U 는 1에 가까워지고, 기준 시간보다 긴 경우에는 시간적 긴급성이 없는 것으로 간주하여 0으로 설정한다.

접근성은 보호대상과의 거리가 가까우면서 접근속도가 빠를수록 높은 값을 갖도록 구성한다. 거리와 접근속도를 각각 정규화한 값을 P_d 와 P_v 라 할 때 접근성은 다음과 같이 산정한다.

$$P = \alpha P_d + (1 - \alpha) P_v \quad (4)$$

여기서 α 는 거리와 접근속도의 상대적 영향을 조정하는 계수로 $0 \leq \alpha \leq 1$ 의 범위를 갖는다. 거리 기반 접근성은 보호대상과의 거리 $d[m]$ 가 감소할수록 증가하며, 접근속도 기반 접근성은 보호대상 방향의 방사속도 $v_a[m/s]$ 가 증가할수록 높은 값을 갖는다.

센서 신뢰도는 다중센서의 탐지 및 분류 신뢰도를 결합하여 산정한다. 레이더, RF, EO/IR 및 음향센서의 신뢰도를 각각 r_k 라 할 때, 전체 센서 신뢰도는 다음과 같이 표현한다.

$$R = \sum_{k=1}^{N_s} \beta_k r_k, \quad \sum_{k=1}^{N_s} \beta_k = 1 \quad (5)$$

여기서 N_s 는 사용된 센서의 수, r_k 는 k 번째 센서의 정규화된 신뢰도, β_k 는 해당 센서에 부여된 융합 가중치이다. 센서의 운용상태가 불량하거나 특정 환경에서 탐지성능이 저하되는 경우에는 해당 센서의 β_k 를 낮춰 위협평가 결과에 미치는 영향을 제한할 수 있다.

식 (1)에서 산정된 위협도 T 는 낮음, 보통, 높음 및 치명의 네 단계로 구분하며, 각 위협단계는 이후 대응수단 선택의 기본 입력으로 사용한다. 다만 높은 위협도가 산정되더라도 즉시 강제 대응을 수행하지 않고, 3.3절에서 설명하는 합법성 및 안전성 검토를 통과한 경우에만 최종 대응단계를 결정한다. 따라서 제안 모델은 위협도를 정량화하는 동시에, 평가결과가 대응 의사결정으로 직접 연결될 때 발생할 수 있는 과잉대응을 방지하도록 구성된다.

3.3 대응수단 선택 방법

본 연구에서는 3.2절에서 산정된 위협도 T 를 기반으로 대응수단을 결정한다. 그러나 위협도가 높다고 해서 즉시 강제 대응을 수행하는 것은 적절하지 않다. 실제 counter-UAS 운용에서는 대응 권한, 공역 안전성 및 주변 환경과 같은 운용 제약조건을 함께 고려해야 하므로, 본 연구에서는 위협평가와 대응결정을 분리한 계층형 의사결정 구조를 적용하였다.

먼저 식 (1)을 이용하여 계산된 위협도는 사전에 정의된 기준에 따라 낮음(low), 보통(moderate), 높음(high) 및 치명(critical)의 네 단계로 분류된다. 이후 각 위협단계는 최종 대응수단을 직접 결정하는 것이 아니라 대응결정의 기본 입력값으로 사용된다.

실제 대응단계에서는 위협도와 함께 대응 권한(legality), 공역 안전성(safety) 및 보호대상의 임무 중요도(mission priority)를 추가적으로 검토한다. 대응 권한은 해당 기관이 전자적 또는 물리적 대응수단을 적용할 수 있는 법적 권한의 보유 여부를 의미하며, 공역 안전성은 주변 항공기 운항, 전파간섭 및 부수피해 가능성을 포함한다. 또한 임무 중요도는 군사 시설, 공항, 국가 중요시설 등 보호대상의 특성을 고려하여 동일한 위협도에서도 서로 다른 대응수단을 선택할 수 있도록 한다.

예를 들어 높은 위협도가 산정되더라도 대응 권한이 확보되지 않았거나 공역 안전성이 충분하지 않은 경우에는 강제 무력화를 수행하지 않고 지속 감시 또

는 추가 확인을 수행한다. 반대로 위협도가 보통 수준이라 하더라도 보호대상의 중요도가 높고 예상 도달 시간이 매우 짧은 경우에는 보다 적극적인 봉쇄 대응을 수행할 수 있다. 이러한 계층형 구조는 위협도만을 기준으로 대응을 결정하는 기존 방식보다 실제 운용 환경을 보다 현실적으로 반영할 수 있다.

본 연구에서는 최종 대응수단을 관찰(observe), 추가 확인(verify), 봉쇄(contain) 및 무력화(defeat)의 네 단계로 정의하였다. 관찰 단계는 위협도가 낮거나 대응이 필요하지 않은 경우 지속적인 추적과 상황감시를 수행하는 단계이다. 추가 확인 단계는 탐지 결과의 신뢰도가 낮거나 remote ID 및 비행승인 여부의 확인이 필요한 경우 적용된다. 봉쇄 단계는 보호구역 접근을 제한하거나 관계기관과의 연계를 통해 추가적인 위협 확산을 방지하는 대응을 의미한다. 무력화 단계는 위협도가 매우 높고 대응 권한 및 안전성이 모두 확보된 경우에 한하여 전자적 또는 물리적 대응수단을 적용하는 최종 대응단계이다.

Table 2. Threat level and response decision rules

Threat level	Basic action	Operational constraints	Final response
Low	Critical	–	Continuous monitoring
Moderate	Verify	Remote ID / Flight authorization	Identification and warning
High	Contain	Legality and safety satisfied	Area isolation and response preparation
Critical	Defeat	Legality, safety, and mission priority satisfied	Electronic or physical neutralization

Table 2는 제안 프레임워크의 대응규칙을 나타낸다. 기존 연구에서는 위협도를 기반으로 대응수단을 직접 선택하는 경우가 많았으나, 본 연구에서는 위협도와 운용 제약조건을 동시에 고려하여 최종 대응단계를 결정하도록 설계하였다. 이를 통해 과잉대응(false escalation)과 대응누락(missed intervention)을 동시에 감소시킬 수 있으며, 운용자가 대응결정의 근거를 명확하게 확인할 수 있는 설명 가능한 의사결정 구조를 제공한다.

제안 방법은 특정 위협평가 알고리즘에 종속되지

않는 구조적 프레임워크라는 장점을 갖는다. 따라서 향후 퍼지 추론, 베이지안 네트워크 또는 인공지능 기반 위협평가 기법을 적용하더라도 위협도 산정 결과를 동일한 대응결정 절차에 적용할 수 있으며, 다양한 counter-UAS 운용환경에 유연하게 확장될 수 있다.

4. 제안 프레임워크 적용 방안

4.1 대표 운용 시나리오

제안 프레임워크의 적용 가능성을 설명하기 위해 counter-UAS 운용환경에서 발생할 수 있는 대표적인 상황을 가정하였다. 본 연구의 목적은 특정 알고리즘의 성능을 정량적으로 비교하는 것이 아니라, 제안한 의사결정 프레임워크가 다양한 운용환경에서 어떠한 절차를 통해 대응수단을 선택하는지를 제시하는 데 있다. 따라서 실제 운용환경을 대표할 수 있는 시나리오를 구성하고, 각 상황에서 프레임워크의 적용 과정을 예시 형태로 설명하였다.

대표 시나리오는 군사시설, 공항, 국가 중요시설의 세 가지 환경을 대상으로 구성하였다. 세 환경은 보호 대상의 특성, 요구되는 안전수준 및 대응 권한이 서로 다르므로 동일한 무인기 위협이라도 서로 다른 의사결정이 이루어질 수 있다. 이를 통해 제안 프레임워크가 위협도뿐만 아니라 운용환경과 제약조건을 함께 고려하는 구조임을 설명하고자 한다.

첫 번째 시나리오는 군사시설 주변으로 비인가 무인기가 접근하는 상황을 가정하였다. 군사시설은 국가 안보와 직결되는 보호대상으로서 비인가 비행에 대한 신속한 대응이 요구된다. 따라서 무인기의 접근 경로, 예상 도달시간 및 비행행태를 종합적으로 고려하여 위협을 판단하고, 대응 권한 및 안전성을 검토한 후 적절한 대응수단을 선택하는 과정을 적용한다.

두 번째 시나리오는 공항 주변에서 무인기가 탐지되는 상황을 가정하였다. 공항은 항공기 운항 안전이 최우선적으로 고려되어야 하는 환경으로, 탐지된 무인기가 실제 위협인지 또는 허가된 비행인지를 우선적으로 확인해야 한다. 따라서 remote ID와 비행승인 정보를 함께 검토하며, 불필요한 대응으로 인해 항공기 운항에 영향을 주지 않도록 단계적인 의사결정을 수행한다.

세 번째 시나리오는 국가 중요시설로 고속 접근하

는 비인가 무인기를 가정하였다. 이 경우에는 보호대상과의 거리, 접근속도 및 예상 도달시간으로 인해 시간적 긴급성이 매우 높으며, 대응 지연 시 시설 피해 가능성이 증가한다. 따라서 제안 프레임워크는 위협평가 결과와 운용 제약조건을 종합적으로 고려하여 신속한 대응 여부를 판단하도록 구성된다.

이와 같이 제안한 시나리오는 counter-UAS 운용환경에서 대표적으로 발생할 수 있는 상황을 기반으로 구성되었으며, 다음 절에서는 각 시나리오에 제안 프레임워크를 적용하는 과정을 예시를 통해 설명한다.

4.2 프레임워크 적용 예시

4.1절에서 제시한 대표 운용 시나리오에 대해 제안 프레임워크를 적용하면 Fig. 2와 같은 절차를 통해 위협평가와 대응 의사결정이 수행된다. 본 절은 제안 프레임워크의 적용 과정을 설명하기 위한 예시이며, 특정 시나리오에 대한 정량적 성능평가 결과를 의미하지 않는다.

먼저 탐지 단계에서는 레이더, RF, EO/IR 및 음향 센서를 이용하여 무인기의 위치, 속도, 비행방향 및 표적 특성 정보를 획득한다. 이후 다중센서 융합을 통해 생성된 표적정보와 remote ID, UTM 정보, 보호대상 중요도 및 운용환경 정보를 통합하여 위협평가의 입력자료를 구성한다.

다음 단계에서는 3.2절에서 제시한 위협평가 모델을 이용하여 의도, 능력, 접근성, 시간적 긴급성 및 센서 신뢰도를 종합적으로 고려한 위협수준을 산정한다. 산정된 위협도는 최종 대응수단을 직접 결정하는 값이 아니라 이후 대응 의사결정을 위한 기준정보로 활용된다.

위협평가가 완료되면 대응 권한, 공역 안전성 및 부수피해 가능성을 검토하는 합법성·안전성 검토 단계가 수행된다. 이 단계에서는 해당 기관의 대응 권한 여부와 주변 운용환경을 함께 고려하여 적극적인 대응이 가능한지를 판단한다. 따라서 높은 위협수준이 산정되더라도 대응 권한이 확보되지 않았거나 공역 안전성이 충분하지 않은 경우에는 지속 감시 또는 추가 확인 절차를 우선 수행하도록 구성하였다.

모든 검토가 완료되면 위협도와 운용 제약조건을 종합적으로 고려하여 관찰(observe), 추가 확인(verify), 봉쇄(contain) 또는 무력화(defeat) 중 적절

한 대응수단을 선택한다. 또한 대응 이후에는 운용 결과를 기록하고 후속 상황을 지속적으로 감시함으로써 추가적인 위협 발생 여부를 확인하고, 필요시 새로운 센서정보를 반영하여 위협평가를 반복 수행할 수 있도록 하였다.

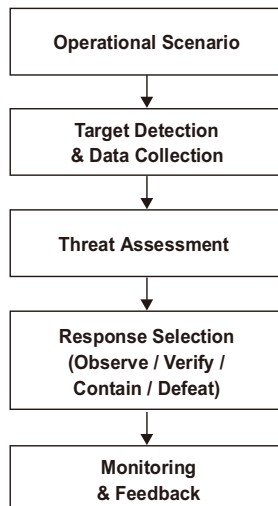


Fig. 2. Application procedure of the proposed threat assessment-based Counter-UAS decision-making framework

Fig. 2는 제안 프레임워크의 전체 적용 절차를 나타낸다. 기존 counter-UAS 연구는 탐지 결과를 기반으로 위협을 평가하거나 대응수단을 선택하는 과정에 중점을 두는 경우가 많았으나, 제안 프레임워크는 위협평가, 운용 제약 검토 및 대응결정을 하나의 연속된 의사결정 절차로 통합하였다. 특히 위협평가와 대응결정 사이에 합법성 및 안전성 검토 단계를 추가함으로써 기술적 판단뿐 아니라 실제 운용환경에서 요구되는 법적·운용적 제약을 함께 반영할 수 있도록 구성하였다. 이러한 구조는 다양한 센서 융합기법이나 위협평가 알고리즘과 독립적으로 적용될 수 있으며, 향후 counter-UAS 운용환경 변화에도 유연하게 확장 가능한 프레임워크를 제공한다.

4.3 활용 방안

제안한 위협평가 기반 counter-UAS 대응 의사결정 프레임워크는 특정 탐지장비나 위협평가 알고리즘에 종속되지 않는 구조를 가지므로 다양한 counter-UAS 운용환경에 적용할 수 있다. 또한 위협평가

와 대응결정을 하나의 절차로 통합함으로써 군사 및 민간 환경에서 요구되는 운용 특성을 유연하게 반영할 수 있다.

군사 분야에서는 군사기지, 지휘소 및 주요 방호시설에 대한 비인가 무인기 대응체계에 적용할 수 있다. 특히 다수의 센서에서 획득한 정보를 기반으로 위협을 평가하고, 임무 중요도와 대응 권한을 함께 고려하여 대응수단을 결정함으로써 지휘관의 의사결정을 효과적으로 지원할 수 있다. 또한 기존 감시체계나 지휘통제체계와 연계할 경우 탐지부터 대응까지의 절차를 일관된 형태로 운용할 수 있을 것으로 기대된다.

민간 분야에서는 공항, 발전소, 항만 및 국가 중요 기반시설과 같이 안전성이 우선되는 환경에 활용할 수 있다. 이러한 시설에서는 탐지 성능뿐만 아니라 허가 비행 여부, 공역 안전성 및 부수피해 가능성을 함께 고려해야 하므로, 제안 프레임워크의 단계적 의사결정 구조를 통해 불필요한 대응을 줄이고 운용의 신뢰성을 향상시킬 수 있다. 또한 remote ID 및 UTM과 같은 무인기 운용정보와 연계할 경우 적절한 비행과 비인가 비행을 보다 효과적으로 구분할 수 있다.

제안 프레임워크는 향후 인공지능 기반 위협평가 기법이나 다양한 다중센서 융합기술과도 쉽게 결합될 수 있다. 위협평가 알고리즘이 변경되더라도 의사결정 절차는 동일하게 유지되므로, 새로운 탐지기술이나 운용환경 변화에 유연하게 대응할 수 있는 확장성을 가진다. 또한 counter-UAS 체계의 운용개념(CONOPS) 수립, 운용 절차 개발 및 교육·훈련 시나리오 작성에도 활용될 수 있어 실무적인 활용 가능성이 높다.

종합하면, 제안 프레임워크는 단순히 무인기의 위협수준을 평가하는 데 그치지 않고, 위협평가 결과를 실제 대응 의사결정으로 연결하는 절차를 체계화하였다는 점에서 기존 counter-UAS 연구와 차별성을 가진다. 특히 다중센서 정보, 운용환경 및 법적·안전성 제약을 통합적으로 고려함으로써 실제 운용환경에 적용 가능한 의사결정 구조를 제시하였으며, 향후 다양한 counter-UAS 체계의 기본 프레임워크로 활용될 수 있을 것으로 기대된다.

5. 결론

최근 무인항공기의 활용이 증가함에 따라 공항, 군

사시설 및 국가 중요기반시설을 대상으로 하는 비인가 무인기 위협이 지속적으로 증가하고 있으며, 이를 효과적으로 대응하기 위한 counter-UAS 체계의 중요성이 더욱 커지고 있다. 그러나 기존 counter-UAS 연구는 탐지 및 식별 성능 향상이나 위협평가 알고리즘 개발에 중점을 두는 경우가 많았으며, 위협평가 결과를 실제 대응 의사결정으로 연결하는 통합적인 운용 프레임워크에 관한 연구는 상대적으로 부족하였다.

본 논문에서는 이러한 한계를 보완하기 위해 위협평가 기반 counter-UAS 대응 의사결정 프레임워크를 제안하였다. 제안 프레임워크는 다중센서 정보를 기반으로 무인기의 의도, 능력, 접근성, 시간적 긴급성 및 센서 신뢰도를 종합적으로 평가하여 위협수준을 산정하고, 대응 권한, 공역 안전성 및 보호대상의 중요도를 함께 고려하여 최종 대응수단을 선택하도록 구성하였다. 또한 위협평가와 대응결정을 하나의 연속적인 절차로 통합함으로써 실제 운용환경에서 요구되는 법적·운용적 제약을 반영할 수 있도록 설계하였다.

제안 프레임워크는 특정 센서나 위협평가 알고리즘에 종속되지 않는 구조를 가지므로 다양한 counter-UAS 체계에 유연하게 적용할 수 있다. 특히 다중센서 융합, remote ID 및 UTM과 같은 운용정보를 함께 활용하여 위협을 평가하고, 단계적인 대응 의사결정을 수행함으로써 기존의 위협도 중심 대응방식보다 운용 현실성을 향상시킬 수 있을 것으로 기대된다. 또한 설명 가능한 규칙 기반 구조를 적용하여 대응결정의 근거를 명확하게 제시할 수 있으며, 향후 새로운 센서나 위협평가 기법이 도입되더라도 동일한 의사결정 절차를 유지할 수 있는 확장성을 제공한다.

본 연구는 실제 counter-UAS 운용에서 활용 가능한 개념적 의사결정 프레임워크를 제안하는 데 중점을 두었으며, 정량적인 성능평가보다는 운용 절차와 의사결정 구조를 체계화하는 것을 연구 범위로 설정하였다. 따라서 향후 연구에서는 다양한 위협 시나리오를 기반으로 제안 프레임워크를 적용하고, 위협평가 알고리즘과의 연계, 시뮬레이션 기반 성능검증 및 실제 운용환경에서의 적용 가능성을 분석함으로써 프레임워크의 실효성을 보다 객관적으로 검증할 필요가 있다.

종합하면, 본 연구에서 제안한 위협평가 기반 counter-UAS 대응 의사결정 프레임워크는 탐지-위

협평가-대응결정을 하나의 연속된 절차로 통합하고, 기술적 요소와 운용적 제약을 함께 고려하는 구조를 제시하였다. 이를 통해 기존 counter-UAS 연구에서 상대적으로 부족했던 대응 의사결정 체계를 보완하고, 향후 군사 및 민간 분야에서 활용 가능한 counter-UAS 운용 프레임워크의 기초 모델로 활용될 수 있을 것으로 기대된다.

참고문헌

- [1] Honggu Kang, Jingon Joung, Jinyoung Kim, Joonhyuk Kang, & Yong Soo Cho, 'Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems,' IEEE Access, VOL. 8, 2020, pp. 168671–168710.
- [2] Jian Wang, Yongxin Liu, & Houbing Song, 'Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends,' IEEE Aerospace and Electronic Systems Magazine, VOL. 36, NO. 3, 2021, pp. 4–29.
- [3] Seongjoon Park, Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, & Hwangnam Kim, 'Survey on Anti-Drone Systems: Components, Designs, and Challenges,' IEEE Access, VOL. 9, 2021, pp. 42635–42659.
- [4] Andre Haider, 'A Methodology for Countering Unmanned Aircraft Systems,' in A Comprehensive Approach to Countering Unmanned Aircraft Systems, Joint Air Power Competence Centre (JAPCC), 2021, pp. 75–86.
- [5] Abdulhadi Shoufan & Ernesto Damiani, 'Contingency Clarification Protocols for Reliable Counter-Drone Operation,' IEEE Transactions on Aerospace and Electronic Systems, VOL. 59, NO. 6, 2023, pp. 8944–8955.
- [6] Konrad D. Brewczyński, Marek Życzkowski, Krzysztof Cichulski, Kamil A. Kamiński, Paraskevi Petsioti, & Geert De Cubber, 'Methods for Assessing the Effectiveness of Modern Counter Unmanned Aircraft Systems,' Remote Sensing, VOL. 16, NO. 19, 2024, Article 3714.
- [7] Geert De Cubber, Daniela Doroftei, Paraskevi Petsioti, Alexios Koniaris, Konrad D. Brewczyński, Marek Życzkowski, Razvan Roman, Silviu Sima, Ali Mohamoud, Johan van de Pol, et al., 'Standardized Evaluation of Counter-Drone Systems: Methods, Technologies, and Performance Metrics,' Drones, VOL. 9, NO. 5, 2025, Article 354.
- [8] Fani Arapoglou, Paraskevi Zacharia, & Michail Papoutsidakis, 'Intelligent Counter-UAV Threat Detection Using Hierarchical Fuzzy Decision-Making and Sensor Fusion,' Sensors, VOL. 25, NO. 19, 2025, Article 6091.
- [9] Federal Aviation Administration, Unmanned Aircraft Systems Detection and Mitigation Systems Aviation Rulemaking Committee Final Report, 2024.
- [10] International Civil Aviation Organization, Protection of Civil Aviation Infrastructure Against Unmanned Aircraft, 2023.