Journal of KIIT. Vol. 24, No. 7, pp. 161-169, Jul. 31, 2026. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2026.24.7.161

레거시 자주포 전술통신 보호를 위한 계류형 UAV 기반 투명 보안 중계 아키텍처 연구

양 시 훈*

A Tethered-UAV-based Transparent Security Relay Architecture for Legacy Self-Propelled Howitzer Tactical Communications

Sihoon Yang*

요 약

자주포 및 자주포 및 사격지휘체계의 임무 데이터 통신은 유선 단절, 지상 무선 차폐, 무선주파수(RF, Radio Frequency) 노출, 레거시 체계 개조 제한이 동시에 작용할 때 보안성과 생존성을 함께 확보하기 어렵다. 본 논문은 계류형 무인항공기(UAV, Unmanned Aerial Vehicle) 공중 중계와 외부 보안 브릿지를 결합한 투명 보안 중계 아키텍처를 제안한다. 공개 기준선 분석에서 제안 UAV 중계 방식의 패킷 전달률(PDR, Packet Delivery Ratio)은 0.5738로 지상 무선 0.1230보다 약 4.7배 높았고, RF 노출 프록시는 15.028에서 3.138로 감소하였다. 추가 민감도 분석은 차폐·단절 스트레스 증가 시 UAV 중계 방식이 지상 무선보다 완만한 PDR 저하를 보이며, 보안 브릿지 처리 오버헤드는 지연 증가를 유발하지만 보완 경로로서의 해석은 유지됨을 보였다.

Abstract

Mission-data communication for self-propelled howitzer and fire-control systems is difficult to secure under cable disruption, terrestrial blockage, Radio-Frequency (RF) exposure, and legacy modification constraints. This paper proposes a transparent security relay architecture that combines a tethered Unmanned Aerial Vehicle (UAV) relay with external security bridges. In a public baseline analysis, the proposed UAV relay achieved a Packet Delivery Ratio (PDR) of 0.5738, about 4.7 times higher than terrestrial wireless communication at 0.1230, while reducing the RF exposure proxy from 15.028 to 3.138. Sensitivity analysis shows that the UAV relay degrades more gradually under disruption and blockage stress, while bridge-processing overhead increases delay but does not change the backup-path interpretation.

Keywords

self-propelled howitzer, tethered UAV, transparent security tunneling, legacy system, tactical communication security

* 육군3사관학교 국방사이버과학과 교수
- ORCID: https://orcid.org/0009-0002-2332-270X

· Received: Jun. 09, 2026, Revised: Jun. 29, 2026, Accepted: Jul. 02, 2026

· Corresponding Author: Sihoon Yang
Dept. of Military Cyber Science, Korea Army Academy at Yeongcheon
495 Hoguk-ro, Gogyeong-myeon, Yeongcheon-si, Gyeongsangbuk-do, [38900] Korea
Tel.: +82-54-330-4813, Email: yangsihun109@gmail.com

Ⅰ. 서 론

1.1 연구 배경

자주포와 사격지휘체계의 데이터 통신은 표적 정보, 사격 명령, 상태보고, 확인 응답을 짧은 시간 안에 교환하기 위한 기반이다. 전술 환경에서는 지휘소와 포대가 분산되고, 임시 진지로 전개되며, 지형 차폐와 전자전 위협이 동시에 작용할 수 있다. 이때 유선 통신은 낮은 지연시간과 안정적 대역폭을 제공하지만 선로 단절, 재설치 부담, 이동 진지 전환 시 운용 부담이 크다. 지상 무선은 기동성이 높지만 가시선 부족, 지형 차폐, RF 노출, 재밍과 감청 위협에 취약하다.

UAV 공중 중계는 지상 장애물 위에 중계 노드를 배치하여 통신 음영을 완화할 수 있는 대안으로 논의되어 왔다[1]. 특히 계류형 UAV는 지상 전원 및 테더 기반 데이터 연결을 활용할 수 있어 일반 배터리형 UAV보다 지속 운용 가능성이 높다[2]. 그러나 UAV를 단순한 RF 중계기로만 취급하면 가짜 노드 참여, 재전송 공격, 키 유출, 펌웨어 변조, 경로 조작과 같은 새로운 공격면이 생긴다. 따라서 공중 중계 구조는 통신 확장 수단이면서 동시에 보안 경계의 일부로 설계되어야 한다.

1.2 문제 정의와 연구 질문

본 논문의 연구 질문은 다음과 같다. 레거시 자주포 및 사격지휘 단말의 내부 소프트웨어와 데이터 포맷을 변경하지 않는 조건에서, 계류형 UAV 공중 중계와 외부 보안 브릿지를 결합하여 임무 데이터의 보안성과 통신 생존성을 동시에 보완할 수 있는가? 이 질문은 새로운 암호 알고리즘이나 최적 라우팅 알고리즘의 제안이 아니라, 공개 가능한 범위에서 보안 아키텍처의 구성요소, 책임 경계, 위협 대응 논리, 후속 검증 지표를 정립하는 문제이다. 특히 본 연구는 레거시 장비의 개조 가능성이 제한되는 운용 환경을 전제로 하므로, 보안 기능의 삽입 위치와 기존 전술통신 절차와의 양립 가능성을 핵심 검토 대상으로 삼는다. 이를 통해 실제 적용 이전 단계에서 아키텍처 수준의 타당성과 검증 우선순위를 제시하고자 한다.

1.3 연구 방법과 기여

본 연구는 네 단계로 수행되었다. 첫째, 레거시 전술통신 환경의 제약을 유선 단절, 지상 무선 차폐, RF 노출, 레거시 무개조, UAV 노드 보안의 관점에서 정리하였다. 둘째, 계류형 UAV, 지상 보안 브릿지, 원격 보안 브릿지, 투명 보안 터널링, 키 수명주기 관리 기능을 결합한 참조 아키텍처를 설계하였다. 셋째, 제안 구조가 실측 성능을 보장한다고 주장하지 않도록 공개 가능한 추상 기준선 모델을 별도로 정의하고, 방식 간 상대 경향과 한계를 분석하였다. 넷째, 동일한 추상 모델을 기반으로 차폐·단절 스트레스와 보안 브릿지 처리 오버헤드에 대한 민감도 실험을 수행하여 제안 구조의 해석 범위와 후속 검증 필요성을 구체화하였다.

본 논문의 기여는 다음과 같다. 첫째, 자주포 전술통신 보호 문제를 통신거리 확장 문제가 아니라 레거시 보안 경계 재구성 문제로 재정의한다. 둘째, UAV 노드를 보안 경계 구성요소로 취급하는 투명 보안 중계 아키텍처를 제시한다. 셋째, 위협-통제-요구사항-평가지표의 추적성을 제공하여 후속 구현 및 검증 연구가 활용할 수 있는 기준을 제시한다. 넷째, 기준선 분석의 가정, 계산식, 향후 연구방향을 명시하여 공개 자료 기반 연구의 과도한 성능 주장을 방지한다. 다섯째, 추가 공개 시뮬레이션을 통해 차폐·단절 스트레스와 보안 처리 오버헤드가 PDR과 지연에 미치는 영향을 비교한다.

Ⅱ. 관련 연구

2.1 UAV 공중 중계와 전술통신 적용성

UAV 통신 연구는 UAV가 고도, 이동성, 배치 유연성을 활용하여 지상 통신망의 커버리지와 연결성을 보완할 수 있음을 보여준다[1][2]. UAV는 공중 기지국, 공중 중계, 데이터 수집·전파 노드로 활용될 수 있으며, 통신 성능은 고도, 배치, 가시선 확

률, 채널 상태, 에너지 제약에 영향을 받는다[3]. 전술 환경에서는 이러한 장점이 지형 차폐 완화와 임시 통신 경로 형성에 유용할 수 있으나, 노출성, 회수 위험, 기상 영향, 전자전 위협을 함께 고려해야 한다.

2.2 FANET 보안과 레거시 보호

비행 애드혹 네트워크(FANET, Flying Ad-Hoc Network)는 UAV 노드들이 동적으로 연결되는 네트워크로, 높은 이동성, 빈번한 링크 변화, 제한된 탑재 자원 때문에 일반 이동 애드혹 네트워크(MANET, Mobile Ad-Hoc Network)보다 라우팅 안정성과 보안 설계가 어렵다[4]. FANET 보안 연구는 위장 노드, 내부자 위협, 서비스거부, 재전송, 라우팅 조작을 주요 위협으로 다룬다[5]. 전술통신에서 FANET 또는 UAV 중계망은 단순 전달 경로가 아니라 임무 데이터가 경유하는 보안 경계가 되므로, 링크 품질뿐 아니라 노드 신원, 키 상태, 무결성 상태, 변조 의심 여부를 함께 고려해야 한다.

레거시 체계 보호에서는 내부 응용이나 데이터 형식을 바꾸지 않고 외부 보안 계층을 삽입하는 접근이 중요하다. 본 논문은 외부 보안 브릿지가 원본 메시지를 캡슐화하고 인증 암호 방식(AEAD, Authenticated Encryption with Associated Data)을 적용하여 기밀성과 무결성을 함께 보호하는 방식을 전제로 한다. 이때 암호화는 단순한 알고리즘 적용이 아니라 nonce/IV 관리, 키 생성·보관·회전·폐기, 재전송 방지, 장치 인증을 포함하는 절차적 요구사항으로 해석되어야 한다[6][7].

2.3 본 연구의 위치

기존 연구가 UAV 중계를 주로 커버리지 개선 또는 네트워크 연결성 문제로 다루었다면, 본 논문은 UAV 중계를 레거시 전술통신의 보안 경계 일부로 재해석한다. 또한 본 논문은 실제 군 장비 제원이나 비공개 운용 절차를 공개하지 않는 조건에서, 어떤 아키텍처 요소와 평가 지표가 후속 검증에 필요한지를 정리한다는 점에서 차별성을 갖는다. 특히 UAV 중계 구간을 단순한 전송 경로가 아니라 인증, 암호화, 무결성 검증이 결합되는 보안 통제 지점으로 설정한다는 점에서 기존 중계 중심 연구와 구분된다.

III. 연구 범위와 위협 모델

본 연구는 공개 자료 기반의 보안 아키텍처 연구이며, 실제 장비의 비공개 프로토콜, 주파수, 송신 출력, 암호키, 세부 배치, 운용 절차, 교리 내용을 다루지 않는다. 분석 대상은 지휘소 또는 사격지휘 장비, 외부 보안 브릿지, 계류형 UAV, 공중 중계망, 원격 보안 브릿지, 자주포 또는 말단 단말로 이어지는 추상화된 데이터 경로이다. 레거시 단말은 기존 데이터 포맷을 유지하며, 보안 브릿지는 레거시 단말과 통신장비 사이에 삽입되는 외부 장치로 가정한다. 제안 구조는 기존 유선·지상 무선 수단을 완전히 대체하는 체계가 아니라, 단절·차폐·전자전 압력이 높은 상황에서 임무 데이터 전달 경로의 생존성을 보완하는 구조이다. 정상 유선이 유지되는 상황에서는 유선의 낮은 지연시간과 높은 안정성을 우선하는 것이 타당하며, 계류형 UAV 중계는 대체 경로 또는 보완 경로로 해석해야 한다.

본 논문의 위협 모델은 실제 전술통신 체계의 내부 정보를 모두 가정하지 않고, 공개적으로 논의 가능한 통신 위협을 추상화한 수준에서 설정한다. 공격자는 지상 무선 구간에서 감청, 재전송, 패킷 삽입, 선택적 방해를 시도할 수 있으며, UAV 중계 노드에 대해서는 위장 노드 참여, 링크 상태 조작, 펌웨어 변조, 테더 단선 유발을 시도할 수 있다고 본다. 다만 암호 알고리즘의 수학적 파괴, 비공개 군용 프로토콜의 세부 취약점, 실제 주파수 운용값에 기반한 전자전 효과는 공개 범위에서 제외한다.

이러한 범위 설정은 공개 학술논문에서 검증 가능한 보안 논리를 명확히 하기 위한 것이다. 제안 구조의 핵심 통제는 공격의 완전 제거가 아니라, 레거시 단말 무개조 조건에서 인증된 장치만 임무 데이터 경로에 참여하게 하고, 변조·재전송 패킷을 차단하며, 장애 시 복구 가능한 보완 경로를 제공하는 데 있다.

Ⅳ. 제안 아키텍처

4.1 운용 개념

운용 개념은 지상 레거시 단말과 통신장비 사이에 보안 브릿지를 삽입하고, 이 브릿지에서 원본 임무 데이터를 보안 터널 패킷으로 캡슐화한 뒤 계류형 UAV 중계 노드로 전달하는 방식이다. 그림 1은 제안하려는 아키텍처의 데이터 흐름도를 나타낸다. 지상 장비와 UAV 구간은 전력·데이터 테더를 우선 고려하여 불필요한 지상 무선 노출을 줄이고, UAV 간 또는 UAV-원격 지상 구간은 운용 환경에 따라 RF, 지향성 RF, 광무선 등 다양한 전송 매체로 추상화할 수 있다. 수신 측 보안 브릿지는 패킷 인증, 복호화, 재전송 검사를 수행한 뒤 레거시 단말이 이해할 수 있는 원본 포맷으로 데이터를 전달한다.

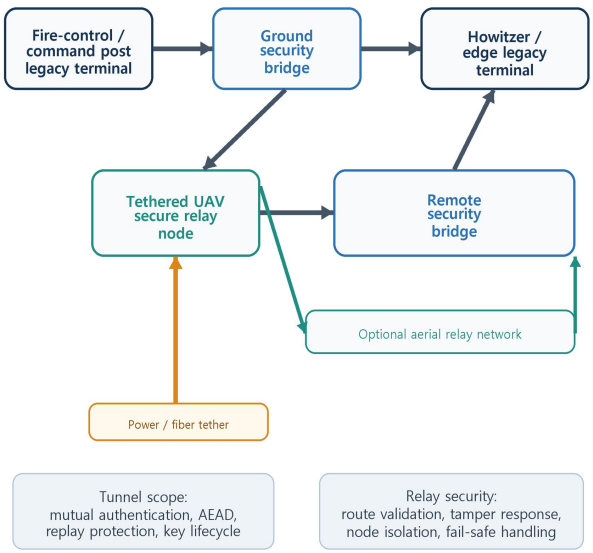

그림 1. 계류형 UAV 기반 투명 보안 중계 아키텍처
Fig. 1. Conceptual architecture of tethered-UAV-based transparent security relay

4.2 구성요소와 책임

구성요소별 책임은 레거시 단말을 수정하지 않는다는 제약을 전제로, 임무 데이터 생성·보호·중계·복원·감사를 어느 경계에서 수행하는지를 명확히 구분하는 데 있다. 우측에 있는 표 1은 각 구성요소가 담당해야 하는 기능과 후속 구현 또는 시험에서 확인해야 할 검증 관점을 정리한 것이다.

4.3 데이터·제어·보안관리 평면

제안 구조는 데이터 평면, 제어 평면, 보안관리 평면으로 구분된다. 데이터 평면은 원본 임무 데이터를 캡슐화하여 보안 터널 패킷으로 전달한다. 제어 평면은 경로 상태, 링크 상태, 노드 가용성, 정책 상태를 교환한다. 보안관리 평면은 장치 신원, 키 수명주기, 인증서 폐기, 변조 감지 로그, 안전 실패 절차를 관리한다. 세 평면을 구분하면 데이터 전달 성능과 보안 통제의 책임 범위를 분리하여 후속 연구에서 오버헤드와 보안 효과를 독립적으로 평가할 수 있다.

표 1. 제안 아키텍처의 구성요소와 책임
Table 1. Components and responsibilities of the proposed architecture

Component	Primary responsibility	Security and validation perspective
Legacy howitzer and fire-control terminal	Generates and receives mission data without changing the legacy format	No internal modification; format preservation; interface stabilit
Transmitting security bridge	Encapsulates mission messages with session, sequence, and policy metadata	Device authentication; key life-cycle control; replay prevention; processing delay
Tethered power and data segment	Tether-break detection; power stability; physical protection; link reporting	Tether-break detection; power stability; physical protection; link reporting
Tethered-UAV relay node	Relays secure-tunnel packets and reports link/node state	Firmware integrity; anti-impersonation; fail-safe behavior; recovery ris
Remote security bridge	Authenticates, decrypts, checks sequence, and restores the original format.	Integrity verification; abnormal-packet blocking; logging; restoration-error handling
Security management and audit function	Manages keys, certificates, tamper logs, and node-isolation policy.	Audit-log integrity; key disposal; recovery time; operator approval

4.4 투명 보안 터널링 절차

투명 보안 터널링은 레거시 단말의 데이터 형식을 보존하면서 외부 보안 계층에서 보호 기능을 제공하는 방식이다. 송신 측 보안 브릿지는 원본 메시지에 세션 식별자, 시퀀스 번호, 시간 정보, 경로 식별자, 정책 태그를 부여하고 이를 AEAD 방식으로 보호한다. 수신 측은 인증, 시퀀스, 정책 검사를 통과한 패킷만 원본 포맷으로 복원한다.

Ⅴ. 설계 요구사항 및 평가 관점

본 논문은 요구사항을 세부 개발 명세가 아니라 보안 논리의 추적성을 확보하기 위한 압축형 설계 기준으로 제시한다. 요구사항 공학 관점에서는 요구사항이 명확성, 추적성, 검증 가능성을 가져야 하며[7], NIST CSF 2.0의 보호·탐지·대응·복구 관점은 전술통신 보안 요구사항을 검증 가능한 항목으로 정리하는 데 유용하다[8].

첫째, 투명성 요구사항은 레거시 단말의 데이터 포맷, 송수신 순서, 운용 절차를 변경하지 않는 것을 의미한다. 보안 기능은 단말 내부가 아니라 외부 보안 브릿지에서 수행되며, 수신 측에서는 인증과 복호화가 완료된 뒤 원본 포맷으로 복원되어야 한다. 이 요구사항은 레거시 장비 개조 비용과 인증 부담을 줄이는 장점이 있지만, 보안 브릿지의 처리 지연과 장애 시 우회 절차를 별도로 검증해야 한다는 제약도 함께 만든다.

둘째, 보안성 요구사항은 기밀성, 무결성, 인증성, 재전송 방지, 감사 가능성을 포함한다. 임무 데이터는 계류형 UAV 중계 구간을 통과하더라도 평문으로 노출되지 않아야 하며, 수신 측은 장치 신원, 세션 식별자, 시퀀스 번호, 정책 태그를 확인한 뒤 정상 패킷만 레거시 단말로 전달해야 한다. 또한 키 갱신, 인증서 폐기, 로그 무결성 검증 절차가 포함되어야 후속 운용 단계에서 사고 원인 분석과 노드 격리가 가능하다.

셋째, 생존성 요구사항은 단일 통신수단의 성능 우위를 주장하는 것이 아니라, 유선 단절과 지상 무선 음영이 동시에 발생할 때 임무 데이터 전달 경로가 완전히 소멸하지 않도록 하는 데 초점을 둔다. 따라서 평가 지표는 PDR뿐 아니라 경로 가용성, 평균 지연, RF 노출 프록시를 함께 보아야 한다. PDR이 높더라도 지연이 전술적 허용 범위를 넘으면 적용성이 낮아지고, 지연이 낮더라도 RF 노출이 크거나 경로 복구성이 낮으면 생존성 관점의 장점이 제한된다.

넷째, 검증 가능성 요구사항은 본 논문의 수치 결과를 실측 성능 보장으로 오해하지 않도록 하는 장치이다. 공개 기준선 분석은 실제 장비 성능을 대체하지 않으며, 후속 단계에서는 HILS, 제한 야외시험, 키 수명주기 시험, 테더 단선 복구시험, 노드 위장 차단시험을 통해 보안 브릿지와 UAV 중계 노드의 책임 경계를 단계적으로 확인해야 한다. 이처럼 요구사항을 지표와 시험 항목으로 연결해야 심사자가 지적한 '아키텍처 제안과 검증 계획 사이의 간극'을 줄일 수 있다.

Ⅵ. 공개 기준선 분석

본 장은 제안 아키텍처의 실제 전술시험 결과를 제시하는 장이 아니다. 군 장비의 비공개 제원과 운용 절차를 배제한 상태에서, 제안 구조가 어떤 지표로 후속 검증될 수 있는지를 보이기 위한 공개 기준선 분석이다. 따라서 수치는 특정 장비의 성능값이 아니라, 동일한 추상 조건에서 방식 간 상대 경향을 비교하기 위한 기준선 결과로 해석해야 한다.

6.1 분석 모델과 변수 정의

시나리오는 지휘소 1개소와 포대 3개소가 임시 진지로 산개한 상황을 가정하고, 방식별 1,500회씩 총 4,500개 표본의 반복 시행으로 비교하였다. 각 시행에서 성공 여부는 링크 상태, 경로 존재 여부, 보안 브릿지 검증 통과 여부를 함께 고려해 결정하였다.

6.2 기준 조건과 해석 기준

본 논문에서 '추상 모델의 상대 비교값'이란 특정 장비의 실측값이 아니라 공개 가능한 가정과 단순화된 상태 변수를 이용해 방식 간 경향을 비교한

기준선 결과를 의미한다. 유선 방식은 정상 고정 유선 링크의 이론적 성능이 아니라, 야전 운용 중 선로 단절, 재설치 지연, 진지 이동 전환 부담이 반영된 '유선 단절 시나리오'로 설정하였다. 따라서 표 2의 유선 PDR 0.6556은 정상 유선 링크의 물리계층 오류율을 의미하지 않으며, 유선 경로가 임무 수행 시점에 실제로 사용 가능한지를 포함한 운용 가용성 기반 성공률이다.

지상 무선 방식은 임시 진지 산개, 지형 차폐, 비가시선 구간, RF 노출에 따른 운용 제약을 반영하여 낮은 PDR을 보였다. 제안 UAV 중계 방식은 공중 중계 노드의 고도 이점으로 지상 차폐를 완화하지만, 공중 중계 구간과 보안 브릿지 검증 절차가 추가되므로 지연은 증가한다. UAV 중계 PDR이 유선 단절 시나리오와 큰 차이를 보이지 않는 이유는 본 기준선이 정상 유선과 비교한 것이 아니라, 유선 선로의 사용 가능성이 낮아진 운용 조건과 비교했기 때문이다. 성공 판정은 단순히 물리 링크가 한 번 연결되었는지를 보는 것이 아니라, 임무 데이터가 송신 측 보안 브릿지에서 캡슐화되고 중계 경로를 거쳐 수신 측 보안 브릿지의 인증·시퀀스·정책 검사를 통과한 뒤 레거시 단말이 이해할 수 있는 원본 포맷으로 복원되는지를 기준으로 한다. 따라서 PDR은 통신 채널 품질과 보안 검증 실패가 결합된 결과이며, 경로 가용성은 해당 시점에 사용 가능한 전달 경로가 존재하는지를 나타내는 운용 지표로 해석한다. 평균 지연은 링크 전송 지연, 공중 중계 지연, 보안 브릿지 처리 지연을 합산한 값으로 본다. RF 노출 프록시는 실제 탐지확률이나 재밍 성공률이 아니라, RF 구간 길이, 송신 지속시간, 노출 계수를 결합한 상대 지표이다. 그러므로 표와 그림의 수치는 특정 장비의 성능을 주장하기보다, 유선 단절, 지상 무선, UAV 보안 중계 방식이 서로 다른 비용과 장점을 갖는다는 점을 설명하기 위한 비교 기준으로 보아야 한다.

6.3 기준선 결과

표 2는 기준 조건에서 유선 단절 시나리오, 지상 무선, 제안 UAV 중계 방식의 PDR, 경로 가용성, 평균 지연, RF 노출 프록시를 비교한 것이다. 그림 2는 이 중 PDR과 경로 가용성을 시각화하여 제안 방식의 전달률 향상과 경로 가용성의 상대적 위치를 함께 보여준다.

표 2. 기준 조건에서 통신 방식별 기초 성능
Table 2. Baseline performance by communication mode

Mode	PDR	Availabilty	Delayed(s)	RF
Wired	0.6556	0.6562	0.001050	0.000
Terr. RF	0.1230	1.0000	0.005050	15.028
UAV relay	0.5738	0.8364	0.006259	3.138

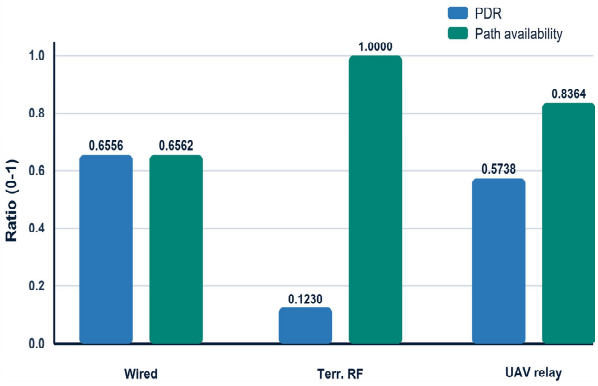

그림 2. 기준 조건에서 통신 방식별 PDR 및 경로 가용성
Fig. 2. Baseline PDR and path availability by communication mode

기준 조건에서 제안 UAV 중계 방식의 PDR은 0.5738로, 지상 무선 방식의 0.1230보다 약 4.7배 높게 나타났다. 경로 가용성도 제안 방식 0.8364로 지상 무선 1.0000보다는 낮지만 유선 단절 시나리오의 0.6562보다 높았다. RF 노출 프록시는 지상 무선 15.028에서 제안 UAV 중계 3.138로 감소하여 약 79.1% 낮아졌다. 반면 평균 지연시간은 0.006259초로 지상 무선 0.005050초보다 증가하였다. 따라서 기준선 결과는 제안 구조가 모든 성능 지표에서 우월하다는 의미가 아니라, 지상 무선 음영과 RF 노출이 동시에 문제가 되는 조건에서 보안성을 유지한 보완 경로로 검토할 가치가 있음을 보여준다.

6.4 추가 공개 시뮬레이션 실험

기준선 결과만으로는 제안 구조가 어떤 조건에서 유효한지 판단하기 어렵다. 따라서 본 절에서는 동

일한 공개 추상 모델을 사용하여 두 가지 추가 실험을 수행하였다. 첫 번째 실험은 차폐·단절 스트레스 수준을 낮음, 기준, 높음, 심각으로 변화시키며 PDR 변화를 비교하였다. 두 번째 실험은 보안 브릿지의 AEAD 처리 및 세션 검증 오버헤드를 0.2ms, 0.5ms, 1.0ms, 2.0ms로 변화시키며 평균 지연의 민감도를 확인하였다. 두 실험 모두 방식별·조건별 1,500회 반복 시행을 가정한 공개 추상 시뮬레이션이며, 실제 장비 실측값이나 특정 전술환경의 성능 보장을 의미하지 않는다. 표 3은 차폐·단절 스트레스 수준에 따른 방식별 PDR 변화를 정리한 것이며, 표 4는 보안 브릿지 처리 오버헤드가 평균 지연에 미치는 영향을 나타낸다. 그림 3은 표 3과 표 4의 핵심 경향을 함께 보여주어, 제안 구조의 적용 조건과 비용 요소를 시각적으로 비교할 수 있게 한다.

표 3. 차폐·단절 스트레스에 따른 PDR 민감도
Table 3. PDR sensitivity under disruption and blockage stress

Stress level	Wired disruption	Terrestrial wireless	Proposed UAV relay	Interpretation
Low	0.920	0.420	0.780	All modes benefit from mild conditions; wired path remains strongest.
Baseline	0.6556	0.1230	0.5738	Matches the baseline condition in Table 8.
High	0.380	0.070	0.490	UAV relay maintains a higher delivery tendency under blockage.
Severe	0.180	0.030	0.380	All modes degrade, but elevated relay remains a meaningful backup path.

실험 1에서 지상 무선 방식의 PDR은 낮음 0.420, 기준 0.1230, 높음 0.070, 심각 0.030으로 급격히 감소하였다. 제안 UAV 중계 방식도 낮음 0.780에서 심각 0.380으로 저하되지만, 모든 스트레스 단계에서 지상 무선보다 높은 값을 유지하였다. 특히 심각 단계에서는 제안 방식이 지상 무선보다 약 12.7배 높은 PDR을 보였다. 유선 단절 시나리오는 낮음 단계에서 0.920으로 가장 높지만, 심각 단계에서는 0.180까지 낮아져 단절·재설치 지연이 누적되는 운용 조건에서 취약해질 수 있음을 보였다. 이 결과는 제안 구조가 정상 유선을 대체한다는 의미가 아니라, 지상 무선 음영과 유선 단절이 동시에 발생하는 조건에서 보완 경로로서 의미가 있음을 뒷받침한다.

표 4. 보안 브릿지 처리 오버헤드에 따른 지연 민감도
Table 4. Delay sensitivity to security-bridge processing overhead

Security overhead per packet(ms)	Proposed UAV relay delay(ms)	Terrestrial RF baseline delay(ms)	Interpretation
0.2	5.959	5.05	Lower security-processing overhead narrows the delay gap
0.5	6.259	5.05	Baseline condition used in Table 2
1.0	6.759	5.05	Delay increases, but the architecture remains survivability-oriented
2.0	7.759	5.05	Heavy processing overhead requires optimization or acceleration

실험 2는 보안 브릿지 처리 지연이 제안 구조의 주요 비용임을 보여준다. 보안 처리 오버헤드가 패킷당 0.2ms에서 2.0ms로 증가하면 제안 UAV 중계 방식의 평균 지연은 5.959밀리초에서 7.759밀리초로 증가하였다. 같은 조건에서 지상 무선 기준 지연은 0.005050초로 유지되므로 지연 격차는 약 0.909밀리초에서 2.709밀리초로 확대된다. 따라서 실제 구현 단계에서는 암호 연산 가속, 세션 재사용 정책, 키 갱신 주기, 로그 처리 방식을 함께 최적화해야 한다. 다만 본 논문의 주장은 평균 지연 우위가 아니라 단절·차폐 환경에서 보안성을 유지한 전달 경로를 제공하는 데 있으므로, 지연 증가는 제안 구조의 해석 범위를 제한하는 비용 요소로 다루어야 한다.

그림 3의 (a)는 차폐·단절 스트레스가 증가할수록 세 방식의 PDR이 모두 낮아지지만, 감소 기울기가 서로 다르다는 점을 보여준다. 지상 무선은 낮음 단계에서 0.420이지만 심각 단계에서 0.030까지 감소하므로 음영·차폐 조건에 민감하다. 반면 UAV 중계는 낮음 0.780에서 심각 0.380으로 감소하지만 모든

단계에서 지상 무선보다 높은 값을 유지한다. 유선 단절 시나리오는 낮음 단계에서는 가장 안정적이지만, 심각 단계에서는 단절과 재전개 부담이 누적되어 UAV 중계보다 낮은 PDR을 보인다.

그림 3의 (b)는 보안 기능 삽입이 공짜가 아니라는 점을 보여준다. 유선 단절 시나리오의 기준 지연은 0.001050초 수준으로 가장 낮고, 지상 무선 기준 지연은 0.005050초로 유지된다. 제안 UAV 중계는 보안 브릿지 오버헤드가 증가할수록 5.959밀리초에서 7.759밀리초까지 상승하므로, 지연 민감 응용에서는 암호 처리 가속과 세션 관리 최적화가 필요하다. 그러나 이 증가는 제안 구조의 목적이 저지연 최적화가 아니라, 단절·차폐 조건에서 보안성을 유지한 보완 경로 제공이라는 점과 함께 해석해야 한다.

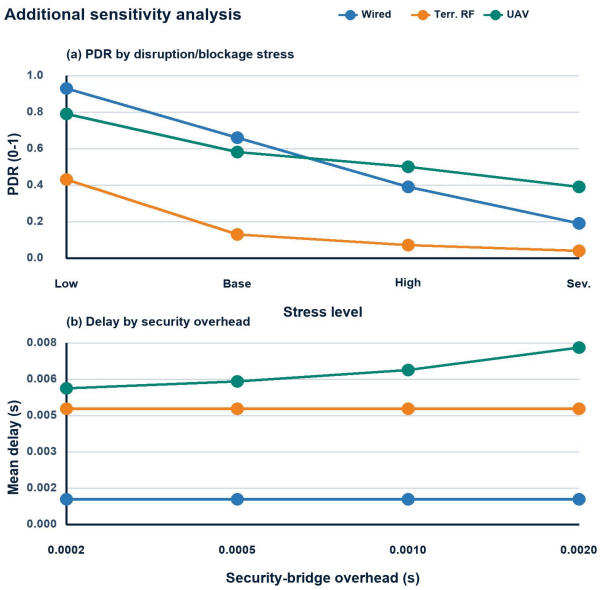

그림 3. 추가 민감도 분석 결과
Fig. 3. Additional sensitivity analysis results

따라서 추가 민감도 분석의 핵심 해석은 'UAV 중계가 항상 우수하다'가 아니라 '적용 조건이 제한적으로 존재한다'는 것이다. 정상 유선이 유지되는 조건에서는 유선 방식이 우선되어야 하며, 지상 무선이 충분히 안정적인 조건에서는 UAV 중계의 추가 지연을 감수할 이유가 작다. 반대로 지상 무선 음영, RF 노출 부담, 유선 단절 또는 재전개 지연이 동시에 커지는 조건에서는 계류형 UAV 기반 보안 중계가 임무 데이터 전달 생존성을 보완하는 후보가 될 수 있다.

6.5 타당성 위협과 후속 검증 계획

후속 연구에서는 UAV 고도, 배치 거리, 차폐 강도, 재밍 압력, 보안 브릿지 처리 지연, 키 갱신 주기를 변화시키는 민감도 분석이 필요하다. 또한 단일 UAV 장애, 테더 단선, 노드 위장, 경로 조작 시나리오를 추가하여 단일 중계 구조와 FANET 기반 우회 구조의 복원성을 비교해야 한다. 마지막으로 HILS(Hardware-in-the-Loop Simulation) 또는 제한 야외시험을 통해 암호화 지연, 로그 무결성, 노드 격리, 경로 복구 특성을 단계적으로 검증해야 한다.

후속 검증은 세 단계로 나누어 수행하는 것이 적절하다. 1단계에서는 공개 시뮬레이션의 파라미터를 확장하여 UAV 고도, 테더 길이, 배치 거리, 차폐 강도, 보안 처리 지연이 PDR과 평균 지연에 미치는 영향을 분리해 확인한다. 2단계에서는 HILS 환경에서 실제 보안 브릿지 소프트웨어 또는 대체 모듈을 연결하여 AEAD 처리 지연, 키 갱신 지연, 로그 생성 부하, 장애 격리 시간을 측정한다. 3단계에서는 제한된 야외 환경에서 테더 단선, UAV 회수, 노드 재인증, 지상 무선 우회 절차를 검증한다.

이러한 단계적 검증 계획은 본 논문의 한계를 보완하는 동시에 공개 가능성과 군사 보안 요구를 함께 만족시키기 위한 절충안이다. 실제 장비 제원과 운용 절차를 공개하지 않더라도, 보안 브릿지의 처리 지연, 키 관리 절차, 장애 복구 시간, 감사 로그 무결성은 재현 가능한 시험 항목으로 정의할 수 있다. 따라서 본 논문의 기여는 완성된 실전 체계의 성능 보장이 아니라, 향후 실증 연구가 따라야 할 아키텍처 수준의 책임 경계와 검증 우선순위를 제시하는 데 있다.

Ⅶ. 결 론

본 논문은 자주포 전술통신의 생존성과 보안성을 보완하기 위해 계류형 UAV 중계와 투명 보안 터널링을 결합한 참조 아키텍처를 제안하였다. 제안 구조는 UAV를 단순 중계기가 아니라 인증, 키 관리, 경로 검증, 변조 대응, 안전 실패 절차를 포함하는 보안 경계 구성요소로 설정한다.

제안 구조는 지상 안테나 간 가시선 제약을 완화하고, 레거시 장비 내부 개조 없이 암호화, 무결성, 인증, 재전송 방지 기능을 외부에서 제공할 수 있다. 또한 UAV 노드를 보안 경계로 포함함으로써 단순 중계 구조에서 누락되기 쉬운 장치 신뢰, 키 관리, 변조 대응 요구사항을 명시할 수 있다. 기준선 분석 결과, 제안 UAV 중계 방식은 지상 무선 방식보다 높은 PDR과 낮은 RF 노출 프록시를 보였으나 보안 터널링 처리에 따른 지연 증가도 확인되었다. 따라서 제안 구조는 정상 유선을 대체하기보다, 유선 단절 또는 지상 무선 음영 상황에서 보안성을 유지한 보완 경로로 해석해야 한다.

향후 연구에서는 본 논문의 기준선 결과를 바탕으로 지형 차폐, 전파 방해, 유선 단절, UAV 고도 변화 등 다양한 운용 조건에서 PDR, 지연, 경로 가용성, RF 노출 프록시를 정량적으로 비교할 필요가 있다. 또한 암호화 처리 지연, 키 갱신, 재전송 방지, 노드 인증 실패가 임무 데이터 전달률에 미치는 영향을 분석하고, 테더 단선, 위장 노드, 패킷 재전송 및 변조 시나리오를 포함한 복원성 평가로 확장해야 한다. 최종적으로는 공개 가능한 테스트베드 또는 HILS 환경에서 레거시 장비 무개조 조건의 보안성 보완과 통신 생존성 향상 효과를 검증할 필요가 있다.

References

[1] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges", IEEE Communications Magazine, Vol. 54, No. 5, pp. 36-42, May 2016. https://doi.org/10.1109/MCOM.2016.7470933.

[2] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems", IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, pp. 2334-2360, Mar. 2019. https://doi.org/10.1109/COMST.2019.2902862.

[3] Q. Song, Y. Zeng, J. Xu, and S. Jin, "A Survey of Prototype and Experiment for UAV Communications", Science China Information Sciences, Vol. 64, Art. no. 140301, Feb. 2021. https://doi.org/10.1007/s11432-020-3030-2.

[4] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A Survey", Ad Hoc Networks, Vol. 11, No. 3, pp. 1254-1270, May 2013. https://doi.org/10.1016/j.adhoc.2012.12.004.

[5] O. Ceviz, S. Sen, and P. Sadioglu, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions", IEEE Communications Surveys & Tutorials, Vol. 27, No. 5, pp. 3227-3265, Oct. 2025. https://doi.org/10.1109/COMST.2024.3515051.

[6] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, pp. 1-31, Nov. 2007. https://doi.org/10.6028/NIST.SP.800-38D.

[7] NIST, "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms", NIST Special Publication 800-175B Rev. 1, pp. 1-83, Mar. 2020. https://doi.org/10.6028/NIST.SP.800-175Br1.

[8] ISO/IEC/IEEE, "ISO/IEC/IEEE 29148:2018 Systems and Software Engineering - Life Cycle Processes - Requirements Engineering", ISO/IEC/IEEE, 2018.

[9] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0", NIST Cybersecurity White Paper 29, pp. 1-27, Feb. 2024. https://doi.org/10.6028/NIST.CSWP.29.

저자소개

양 시 훈 (Sihoon Yang)

2017년 2월 : 육군사관학교 컴퓨터공학과(이학사)
2026년 1월 : 국방대학교 컴퓨터공학과(이학석사)
2026년 1월 ~ 현재 : 육군3사관학교 국방사이버과학과 강사
관심분야 : 강화학습, 무기표적할당, 인공지능