JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 27, No. 7, pp. 1953-1963, Jul. 2026

Check for updates

# UAV 군집 환경에서 제로트러스트 기반 PUF 경량 상호인증 프로토콜

백 두 현[1] · 손 태 식[2*] · 정 찬 기[3]
[1]아주대학교 국방디지털융합학과 석사과정
[2]아주대학교 사이버보안학과 교수
[3]아주대학교 국방디지털융합학과 교수

# Lightweight PUF-Based Mutual Authentication Protocol for Zero-Trust UAV Swarm Environments

**Duhyun Baek[1] · Taeshik Shon[2*] · Chanki Jeong[3]**

[1]Master's Course, Department of Military Digital Convergence, Ajou University, Gyeonggi-do 16499, Korea
[2]Professor, Department of Cyber Security, Ajou University, Gyeonggi-do 16499, Korea
[3]Professor, Department of Military Digital Convergence, Ajou University, Gyeonggi-do 16499, Korea

**[요 약]**

무인항공기(UAV) 군집은 IoBT(Internet of Battlefield Things) 환경에서 정찰·감시 등 군사 임무 수행의 핵심 요소로 활용되고 있으나, 개방된 무선 채널의 특성상 위장 공격, 재전송 공격, 물리적 포획 등 다양한 보안 위협에 노출된다. 이를 해소하기 위해 PUF(Physical Unclonable Function) 기반 경량 인증 기법들이 제안되어 왔으나, 기존 기법들은 초기 인증 시점에만 신원 검증을 수행하여 세션 탈취, 내부자 위협, 물리적 포획 후 위장 공격에 구조적으로 대응하지 못하는 한계를 가진다. 본 논문은 PUF의 경량 인증 특성과 제로 트러스트(Zero Trust)의 지속적 검증 원칙을 결합한 상호인증 프로토콜을 제안한다. 제안 기법은 기존 1:1 기반 기법 대비 군집 규모 확장성을 확보하고, 5개 보안 항목을 추가로 충족하면서도 UAV 실시간 운용에 영향을 주지 않음을 확인한다.

**[Abstract]**

UAV swarms are key elements in military missions, such as reconnaissance and surveillance in IoBT environments; however, they are exposed to various security threats, including impersonation and replay attacks and physical capture, due to the nature of open wireless channels. Physical unclonable function (PUF)-based lightweight authentication schemes have been proposed to address these threats. However, existing schemes only perform identity verification during the initial authentication phase and are structurally unable to respond to session hijacking, insider threats, and post-capture impersonation. This study proposes a mutual authentication protocol that combines the lightweight authentication properties of PUFs with the continuous verification principle of zero trust. The proposed scheme achieves swarm-level scalability beyond existing one-to-one-based schemes and satisfies five additional security properties unmet by previous works, while having a negligible impact on real-time UAV operations.

**색인어 :** 무인 항공기, 물리적 복제 방지 기능, 상호 인증, 제로 트러스트, 지속적 검증
**Keyword :** UAV, Physical Unclonable Function (PUF), Mutual Authentication, Zero Trust, Continuous Verification

**http://dx.doi.org/10.9728/dcs.2026.27.7.1953**



**Received** 27 April 2026; **Revised** 15 May 2026
**Accepted** 18 May 2026

***Corresponding Author; Taeshik Shon**

**Tel:** +82-31-219-3321
**E-mail:** tsshon@ajou.ac.kr

## Ⅰ. 서 론

최근 무인항공기(Unmanned Aerial Vehicle, UAV) 군집 기술은 IoBT(Internet of Battlefield Things) 환경에서 정찰, 감시, 타격 등 다양한 군사 임무 수행의 핵심 수단으로 부상하고 있다. UAV 군집은 다수의 UAV가 협력하여 단일 UAV로는 수행이 어려운 광역 임무를 효율적으로 달성할 수 있으며, 일부 노드의 손실에도 임무를 지속할 수 있는 구조적 강건성을 제공한다. 그러나 UAV는 개방된 무선 채널을 통해 통신하며, 배터리 전력, 처리 능력, 메모리 등 온보드 자원이 제한적이라는 특성을 갖는다. 이러한 환경적 특성은 위장 공격(Impersonation Attack), 재전송 공격(Replay Attack), 중간자 공격(Man-in-the-Middle), 물리적 포획(Physical Capture) 등 다양한 보안 위협에 UAV 군집을 노출시킨다[1].

이러한 위협에 대응하기 위해, PUF(Physical Unclonable Function)의 하드웨어 기반 복제 불가 특성을 활용한 경량 인증 프로토콜이 다수 제안되었다. PUF는 반도체 제조 공정에서 발생하는 물리적 변동성을 이용하여 각 칩마다 고유한 시도-응답 쌍(Challenge-Response Pair, CRP)을 생성한다. 장점으로는 비밀 키를 별도로 저장하지 않아도 하드웨어 수준의 신뢰 근거(Root of Trust)를 확보할 수 있다[2]. Wazid 등은 IoD 환경에서 해시함수와 XOR 연산 기반의 AKA 방식[3]을, Srinivas 등은 임시 자격 증명 기반의 TCALAS[4]를, Bansal 등은 V2G 시스템을 위한 PUF 기반 SUKA 프로토콜[5]을, Alladi 등은 PUF를 활용한 UAV-지상기지국 환경에 특화된 SecAuthUAV[6]를 각각 제안하였다. 기존의 PUF 기반 인증 기법들은 초기 등록 및 접속 시점에 한 번 인증을 수행한 이후 세션이 유지되는 동안 해당 노드를 지속적으로 신뢰하는 경계 기반 보안 모델을 따르고 있어, 비행 중 UAV가 물리적으로 포획된 후 공격자가 추출한 자격증명으로 정상 노드를 위장하는 공격이나, 세션 키 탈취를 통한 내부자 위협을 탐지할 수 없다.

한편, 차세대 보안 패러다임 제로트러스트(Zero Trust)는 “절대 신뢰하지 말고 항상 검증하라(Never Trust, Always Verify)”는 원칙에 기반한다. NIST SP 800-207[7]에서 정책결정지점(PDP), 정책집행지점(PEP)으로 구성되는 논리적 아키텍처와 신뢰 점수 기반 동적 위험 평가를 체계화하였다. 미 국방부는 제로트러스트 참조 아키텍처 v2.0[8]을 발표하고, 국내에서도 과학기술정보통신부가 제로트러스트 가이드라인 2.0[9]를 통해 군사 시스템을 포함한 고신뢰 환경에의 적용 기준을 제시하였다.

이에 본 논문은 PUF의 경량 인증 특성과 제로트러스트의 지속적 검증 원칙을 결합한 UAV 군집 환경 경량 상호인증 프로토콜을 제안한다. 제안 시스템 모델은 지상기지국(PDP)-클러스터 헤더(PEP)-멤버 UAV(PUF 탑재 노드)의 3계층 구조로 설계되었으며, 초기 상호인증 이후에도 신뢰 점수 기반 정책 판단을 통한 주기적 PUF 재인증을 수행한다. 이를 통해 기존 기법이 대응하지 못하는 세션 탈취, 포획 후 위장 공격, 내부자 위협에 추가적으로 대응하면서도, 재인증 연산을 경량화하여 UAV 실시간 운용에 영향을 주지 않는 수준의 오버헤드만을 요구한다.

본 논문의 구성은 다음과 같다. 2장에서는 PUF, 제로트러스트를 소개하고 UAV 군집 보안 위협에 대한 관련 연구를 소개한다. 3장에서는 시스템 모델과 제안 프로토콜을 기술하며, 4장에서는 보안성 분석과 성능 검증을 수행한다. 마지막으로 5장에서 결론 및 향후 연구 방향을 제시한다.

## Ⅱ. 관련 연구

### 2-1 PUF(Physical Unclonable Function)

PUF(Physical Unclonable Function)는 반도체 제조 공정에서 발생하는 미세한 물리적 변동성을 이용하여 각 칩마다 고유한 응답을 생성하는 하드웨어 보안 기술이다. 동일한 설계를 적용한 두 칩이라도 제조 과정에서의 공정 편차로 인해 동일한 챌린지(Challenge)에 대해 서로 다른 리스폰스(Response)를 출력한다. 이러한 챌린지-리스폰스 쌍(CRP)은 칩의 고유한 “물리적 지문”으로 기능한다. PUF는 비밀 키를 메모리에 별도로 저장할 필요가 없으므로, 물리적 포획을 통한 키 추출 공격에 대한 본질적 저항성을 제공한다. 해시 및 XOR 연산과 결합하여 경량 인증 프로토콜을 구성할 수 있어 UAV와 같은 자원 제약 환경에 적합하다[2]. PUF의 이러한 경량성과 복제 불가 특성은 제로트러스트 환경에서 하드웨어 수준의 신뢰 근거(Root of Trust)를 확보하는 핵심 수단이 된다.

### 2-2 제로트러스트(Zero Trust) 보안 모델

제로트러스트는 “절대 신뢰하지 말고 항상 검증하라”는 원칙에 기반한 보안 모델로, 네트워크 내부와 외부를 구분하지 않고 모든 접속을 지속적으로 검증하는 접근 방식이다. 제로트러스트의 핵심 원칙은 세션 유지 중에도 신원과 행위를 반복 확인하는 지속적 검증, 업무 수행에 필요한 최소한의 권한만을 부여하는 최소 권한, 그리고 네트워크가 이미 침해되었을 수 있다는 전제 하에 피해 확산을 최소화하는 침해 가정이다. NIST SP 800-207은 제로트러스트 아키텍처의 논리적 구성요소로 정책결정지점(Policy Decision Point, PDP)과 정책집행지점(Policy Enforcement Point, PEP)을 정의한다[7].

#### 1) PDP(Policy Decision Point)

PDP는 접근 요청에 대한 허용 또는 차단을 판단하는 중앙 결정 기능을 수행하는 정책 결정 지점이다. 사용자 신원, 기기 상태, 환경 컨텍스트 등 다양한 속성을 종합하여 정책을 평가한다.

#### 2) PEP(Policy Enforcement Point)

PEP는 PDP의 판단 결과를 실제 네트워크에서 집행하는

정책 이행 지점이다. PEP에서는 접근 허용, 제한, 차단 등의 조치를 수행한다. 또한 제로트러스트는 접근 통제 시 단일 인증 결과에만 의존하지 않고, 신뢰 점수(Trust Score) 기반의 동적 위험 평가를 수행하여, 인증된 주체라 하더라도 세션 유지 중 컨텍스트가 변화하면 접근 권한을 실시간으로 재조정할 수 있다. 이는 기존의 이분법적(허용/차단) 접근 통제와 근본적으로 차별화된다.

#### 3) 군사분야에서의 제로트러스트

미 국방부는 제로트러스트 참조 아키텍처 v2.0[8]을 발표하고 국내에서는 과학기술정보통신부가 2024년 제로트러스트 가이드라인 2.0[9]를 발표하여 군사 시스템을 포함한 고신뢰 환경에의 적용 기준을 제시하였다. 또한 오충만 등이 사이버전자전 환경에서 무선 통신 위협에 대한 제로트러스트 기반 대응 방안[10]을 제시하였으며, 강대영 등은 제로트러스트 2.0 가이드라인을 기반으로 한국군 C4I체계에 속성기반 접근통제(ABAC)를 적용한 계층형 보안정책 구조를 설계[11]하였다. 그러나 UAV 군집과 같이 자원 제약이 심한 무인체계 환경에 대한 제로트러스트 적용 연구는 아직 초기 단계에 있다. 특히 제로트러스트의 PDP-PEP 구조와 신뢰 점수 기반 동적 위험 평가를 UAV 군집에 적용하기 위해서는 경량화된 인증 수단이 반드시 수반되어야 한다.

### 2-3 UAV 군집 환경에서의 보안 요구사항

UAV 군집은 공중 무선 환경에서 다수의 노드가 동적으로 통신하는 특성상 다양한 보안 위협에 노출된다. 본 절에서는 인증 프로토콜이 충족해야 할 주요 보안 요구사항을 분석한다.

#### 1) 상호 인증

통신에 참여하는 양측이 서로의 신원을 검증하는 절차이다. UAV 군집 환경에서는 UAV와 지상기지국 간, 그리고 UAV 상호 간에 정당한 노드임을 확인하는 과정이 선행되어야 안전한 데이터 교환이 가능하다.

#### 2) 위장 공격

공격자가 정상 UAV 또는 GCS의 신원을 위조하여 네트워크에 접근하는 공격이다. 특히 UAV가 물리적으로 포획된 후 추출된 자격증명으로 정상 노드를 위장하는 포획 기반 위장 공격(Post-Capture Impersonation)은 초기 인증만으로는 탐지가 불가능하다.

#### 3) 재전송 공격

공격자가 정상적으로 송수신된 인증 메시지를 가로채어 저장한 후, 이를 나중에 재전송함으로써 인증 절차를 우회하는 공격이다. 타임스탬프나 난수(nonce)를 검증하지 않는 경우 발생할 수 있다.

#### 4) 중간자 공격

악성 노드가 정상적인 통신을 하는 두 노드 사이에 위치하면서, 송수신되는 메시지와 패킷을 가로채거나 변조하는 공격이다.

#### 5) 물리적 포획 공격

공격자가 비행 중이거나 착륙한 UAV를 물리적으로 탈취하여, 내부에 저장된 암호 키, 인증 정보 등을 추출하는 공격이다. PUF는 하드웨어의 물리적 특성에 기반하여 키를 생성하므로, 칩을 분해하더라도 동일한 값을 복제할 수 없어 이에 대한 저항성을 제공한다.

#### 6) 세션 탈취 및 내부자 위협

초기 인증이 완료된 이후 유지되는 세션을 공격자가 가로채거나, 인가된 내부 노드가 악의적으로 행동하는 경우이다. 기존의 경계 기반 보안 모델에서는 초기 인증 이후 노드를 신뢰하므로 이러한 위협에 대응하기 어렵다. 제로트러스트의 지속적 검증 원칙은 세션 유지 중에도 주기적으로 노드의 신원을 재확인함으로써 이에 대응할 수 있는 구조적 기반을 제공한다.

#### 7) 기기 복제 불가 보장

각 노드가 고유한 신원을 가지며, 이를 물리적으로 복제할 수 없음이 보장되어야 한다. PUF는 제조 공정의 물리적 변동성에 기반하여 각 칩마다 고유한 응답을 생성하므로, 하드웨어 수준에서 기기 복제 불가성을 보장한다.

### 2-4 관련 연구 분석 및 한계

UAV의 자원 제약사항을 고려하여 여러 경량화 인증 프로토콜이 제안되었다. Wazid 등은 드론과 사용자 간의 인증을 위해 해시함수와 XOR 연산 기반의 AKA 방식[3]을 제안하였으며, Srinivas 등은 IoD 환경에서 임시 자격 증명 기반의 TCALAS[4]를 제안하였다. Bansal 등은 V2G 시스템을 위한 PUF 기반 SUKA 프로토콜[5]을 제안하여, PUF를 사용한 2단계 상호 인증을 달성하였다. Alladi 등은 UAV-지상기지국 환경에 특화된 PUF 기반 인증 기법 SecAuthUAV[6](이하 “PUF Only”로 표기)를 제안하여, 해시, XOR, PUF 연산만을 사용한 경량 상호인증과 세션키 생성을 달성하였다. 그러나 PUF Only 역시 초기 인증 이후 세션 동안의 지속적 검증 메커니즘은 제공하지 않으며, UAV-GS 간 1:1 통신만을 전제로 하고 있다.

위의 기존 연구들은 공통적으로 두 가지 구조적 한계를 가진다. 첫째, 대부분의 PUF 기반 인증 기법은 UAV와 지상기지국 간의 1:1 통신을 전제로 하며, CRP를 지상기지국의 데이터베이스에 저장하는 방식을 취한다. Swarm 환경에서 클러스터 헤더 역할을 하는 드론이 탈취될 경우, 해당 군집의 인증 과정은 정상적으로 수행될 수 없다. 또한 [5]의 SUKA는 V2G 환

경을, [6]의 PUF Only는 UAV-GS 1:1 환경을 전제로 설계되어 있어, UAV 군집의 계층적 구조와 확장성을 반영하지 못한다. 둘째, 기존 기법들은 초기 인증 이후 세션 동안 해당 노드를 신뢰하는 경계 기반 보안 모델을 따르고 있다. 이는 비행 중 UAV가 물리적으로 포획된 후 공격자가 추출한 자격증명으로 정상 노드를 위장(Post-Capture Impersonation)하거나, 세션 키가 탈취되어 내부자 위협이 발생하는 상황에 대응할 수 없다는 근본적 한계를 갖는다. NIST SP 800-207[7]에서 정의한 제로트러스트의 핵심 원칙인 지속적 검증과 신뢰 점수 기반 동적 위험 평가가 이러한 한계를 해소할 수 있는 대안으로 주목되고 있으나, 기존의 [3], [4], [5], [6] 어느 기법도 이를 반영하지 않고 있다.

본 논문에서는 이러한 한계를 동시에 해소하기 위해, PUF 기반 인증에 제로트러스트의 지속적 검증 원칙을 결합한 경량 상호인증 프로토콜을 제안한다. 제안 기법은 GCS(PDP)-클러스터 헤더(PEP)-멤버 UAV의 3계층 구조와 신뢰 점수 기반 정책 판단을 통해, 기존 기법이 대응하지 못하는 세션 탈취, 포획 후 위장 공격, 내부자 위협에 추가적으로 대응하며, 재인증 과정은 해시 및 XOR 연산 중심의 경량 설계를 통해 UAV 실시간 운용에 영향을 주지 않는 수준으로 억제하였다.

## Ⅲ. 제안 기법

본 장에서는 UAV 군집 환경에서 제로트러스트 원칙을 적용한 PUF 기반 경량 상호인증 프로토콜을 제안한다. 먼저 시스템 모델과 위협 모델을 정의한 후, 사전 등록, 초기 상호인증, 지속적 재인증의 3단계로 구성되는 프로토콜을 기술한다.

### 3-1 시스템 모델 및 위협 모델

본 논문에서는 중앙 지상기지국(GCS)에 연결된 유한 개수(N)의 UAV로 구성된 군집 시스템을 고려한다. UAV는 주변 환경의 모니터링 및 감시 데이터를 수집하며, 수집된 데이터는 클러스터 헤더 UAV를 통해 GCS로 전송된다. UAV는 배터리 전력, 처리 능력, 메모리와 같은 온보드 자원이 제한적이며, GCS는 풍부한 컴퓨팅·메모리·에너지 자원을 갖춘 안전하고 보호된 지상 위치에 있다고 가정한다.

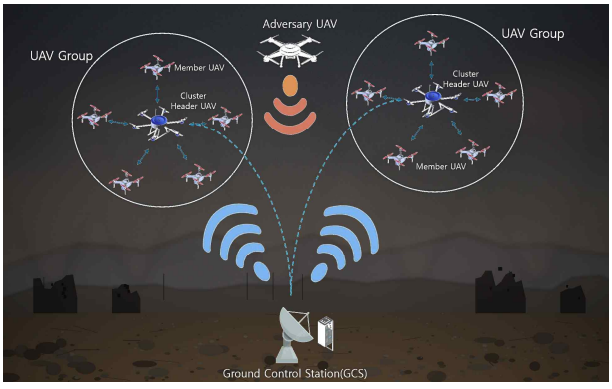


**그림 1.** 시스템 모델
**Fig. 1.** System model

제안하는 시스템 모델은 제로트러스트 아키텍처의 논리적 구성요소를 UAV 군집 환경에 매핑하여, 다음과 같이 세 가지 역할 계층으로 구성된다. 제안된 시스템 모델의 개략도는 그림 1에 나타낸다.

#### 1) 지상기지국(GCS)

제로트러스트 아키텍처의 정책결정지점(PDP) 역할을 수행한다. 모든 UAV의 PUF CRP 데이터베이스를 보유하며, 초기 등록 및 인증뿐 아니라 세션 유지 중 발생하는 재인증 요청에 대한 정책 판단을 담당한다.

#### 2) 클러스터 헤더 UAV (CH)

군집 내에서 GCS와 직접 통신하는 대표 UAV로, 정책집행지점(PEP) 역할을 수행한다. GCS의 정책 판단 결과를 수신하여 멤버 UAV에 대한 접근 통제를 실행하며, 주기적 PUF 재인증 요청을 중계한다.

#### 3) 멤버 UAV ($U_i$)

PUF 칩을 탑재하고 있으며, 초기 군집 합류 시 CH를 통해 GCS에 등록·인증된다. 이후에도 CH로부터 주기적인 PUF 챌린지를 수신하고 리스폰스를 반환하여 신원을 재검증받는다.

위협 모델 측면에서는 적대적 UAV 노드의 존재를 가정한다. 공격자는 정상 UAV를 물리적으로 탈취하거나 악성 노드로 교체할 수 있으며, 군집에 합류하여 내부 통신을 교란하거나 허위 데이터를 주입하려 시도할 수 있다. 지상기지국은 물리적으로 보호된 환경에서 운용되므로 신뢰할 수 있는 노드로 가정한다[1]. 특히 본 논문에서는 2-3절에서 정의한 위장 공격 중에서도, 비행 중 정상 UAV가 물리적으로 포획된 후 공격자가 추출한 자격증명을 이용해 정상 노드로 위장하는 포획 기반 위장 공격(Post-Capture Impersonation) 시나리오를 명시적으로 위협 모델에 포함한다.

### 3-2 주요 표기법

제안 프로토콜에서 사용되는 주요 표기법은 표 1과 같다.

### 3-3 사전 등록 단계(Registration)

사전 등록 단계는 UAV가 군집에 배치되기 전, 물리적으로 안전한 환경에서 수행되는 일회성 절차이다.

Step R1. GCS는 각 UAV $U_i$에 대해 고유 식별자 IDi를 할당한다.

Step R2. GCS는 N개의 챌린지 집합 $\{C_i^1, C_i^2, \cdots, C_i^N\}$을

**표 1.** 주요 표기법
**Table 1.** Notations

| Notation | Description |
|---|---|
| GCS(G) | Ground Control Station (PDP) |
| CH | Cluster Header UAV (PEP) |
| $U_i$ | i-th Member UAV |
| $ID_i$ | Unique Identifier of $U_i$ |
| $ID_{CH}$ | Unique Identifier of CH |
| $PUF_i(\cdot)$ | PUF Function of $U_i$ |
| $C_i$, $R_i$ | Challenge-Response Pair (CRP) of $U_i$ (initial authentication) |
| $C_i^j$, $R_i^j$ | j-th challenge, response for $U_i$ |
| $M_i^j$, $N_i^j$ | Masked challenge and masked response delegated to CH, respectively |
| $C_i^*$ | Masked challenge for $U_i$ |
| $N_x$ | Nonce generated by entity x |
| $T_x$ | Timestamp |
| $T_R$ | Request transmission time recorded by CH |
| $T_R'$ | Response reception time recorded by CH |
| $T_U$ | Response timestamp generated by $U_i$ |
| $V_1$ | Authentication verification value generated by GCS |
| $V_2$ | Authentication verification value generated by $U_i$ |
| $V_R$ | Re-authentication verification value generated by $U_i$ |
| $V_R'$ | Expected re-authentication verification value computed by CH |
| M | Authentication message |
| SK | Session Key: $h(R_i \| \| N_1 \| \| N_2)$ |
| $h(\cdot)$ | One-way Hash Function (SHA-256) |
| $\oplus$ | XOR Operation |
| $\|$ | Concatenation Operation |
| $\tau$ | Re-authentication Period (seconds) |
| K | Number of Re-authentication |
| $TS(U_i)$ | Trust Score of $U_i$ |
| $S_{puf}$ | PUF response integrity score (0 or 1) |
| $S_{time}$ | Response timeliness score (0-1) |
| $S_{beh}$ | Behavioral consistency score (0-1) |
| $\Delta_{max}$ | Maximum allowable response delay threshold |

생성하여 $U_i$에게 전송한다.

Step R3. $U_i$는 탑재된 PUF 칩을 이용하여 각 챌린지에 대응하는 응답 $R_i^j = PUF_i(C_i^j)$를 생성하고, GCS에 반환한다.

Step R4. GCS는 CRP 데이터베이스 $DB_i = \{(ID_i, C_i^j, R_i^j)\}$를 안전한 저장소에 기록한다. UAV 측에는 어떠한 비밀 정보도 저장되지 않으며, PUF 칩 자체가 신뢰 근거로 기능한다.

### 3-4 초기 상호 인증 단계(Authentication)

UAV가 군집에 합류할 때, CH를 통해 GCS와 상호 인증을 수행하고 세션 키를 확립한다. 초기 상호인증의 메시지 흐름은 다음과 같다.

Step A1 ($U_i \rightarrow$ CH). $U_i$는 타임스탬프 $T_1$과 난수 $N_1$을 생성하여, 인증 요청 메시지 $M_1 = \{ID_i, T_1, N_1\}$을 CH에 전송한다.

Step A2 (CH $\rightarrow$ GCS). CH는 $M_1$에 자신의 식별자 $ID_{CH}$와 타임스탬프 $T_2$를 추가하여 GCS로 전달한다: $M_2 = \{ID_i, ID_{CH}, T_1, T_2, N_1\}$.

Step A3 (GCS). GCS는 $DB_i$에서 미사용 챌린지 $C_i$를 선택하고, 해당 $R_i$를 조회한다. 인증 검증값 $V_1 = h(ID_i \| R_i \| N_1 \| T_2)$과 마스킹된 챌린지 $C_i^* = C_i \oplus h(R_i \| N_1)$을 생성하여 CH에 전송한다: $M_3 = \{C_i^*, V_1, T_3\}$.

Step A4 (CH $\rightarrow U_i$). CH는 $M_3$을 $U_i$에게 중계한다.

Step A5 ($U_i$). $U_i$는 $h(R_i \| N_1)$을 계산하여 $C_i = C_i^* \oplus h(R_i \| N_1)$을 복원하고, $R_i' = PUF_i(C_i)$를 계산한다. $V_1' = h(ID_i \| R_i' \| N_1 \| T_2)$가 수신한 $V_1$과 일치하는지 확인하여 GCS를 인증한다. 검증 성공 시, 난수 $N_2$를 생성하고 $V_2 = h(R_i' \| N_2 \| T_4)$을 CH를 통해 GCS에 전송한다: $M_4 = \{V_2, N_2, T_4\}$.

Step A6 (GCS). GCS는 $V_2$를 검증하여 $U_i$를 인증한다. 양방향 인증이 완료되면, 세션 키 $SK = h(R_i \| N_1 \| N_2)$를 계산한다. 이후 다음 K개의 CRP를 XOR 마스킹하여 CH에 위임한다: $M_i^j = C_i^j \oplus h(SK \| j)$, $N_i^j = R_i^j \oplus h(SK \| j \| 1)$로 마스킹하여 $M_5 = \{M_i^j, N_i^j\}$를 CH에 전송한다.

Step A7 (CH). CH는 SK를 독립 계산한 뒤 동일한 방식으로 XOR 역연산하여 CRP를 복원하고, 재인증 단계에서 활용한다.

### 3-5 지속적 재인증 단계(Continuous Re-Authentication)

#### 1) 재인증 프로토콜 흐름

Step C1 (CH). CH는 주기 τ마다 위임받은 CRP 집합에서 다음 챌린지 $C_i^{new}$를 선택하고, 재인증 요청 메시지 $M_R = \{C_i^{new}, N_R, T_R\}$을 $U_i$에게 전송한다.

Step C2 ($U_i$). $U_i$는 $R_i^{new} = PUF_i(C_i^{new})$를 계산하고, 응답 생성 시간 $T_U$를 포함하여 $V_R = h(R_i^{new} \| N_R \| T_R \| T_U)$을 생성하여 CH에 반환한다: $M_R' = \{V_R, T_U\}$

Step C3 (CH). CH는 응답 수신 시간 $T_R'$를 기록하고, 위임받은 예상 응답 $R_i^{new}$을 이용하여 $V_R' = h(R_i^{new} \| N_R \|$

$T_R \| T_U$)을 계산하여 수신한 $V_R$과 비교한다. 다음 세 가지 컨텍스트 조건을 평가하여 신뢰 점수 산출에 활용한다.

- **조건 1 (PUF 응답 무결성):** $V_R = V_R'$ 여부
- **조건 2 (응답 적시성):** $T_R' - T_R \leq \Delta_{max}$ 여부
- **조건 3 (행위 일관성):** 해당 UAV의 이전 통신 패턴 대비 이상 여부

#### 2) 신뢰 점수 기반 정책 판단

CH는 Step C3에서 평가한 세 가지 조건을 종합하여 해당 $U_i$의 신뢰 점수 $TS(U_i)$를 산출한다.

$$TS(U_i) = w_1 \cdot S_{puf} + w_2 \cdot S_{time} + w_3 \cdot S_{beh} \quad (1)$$

여기서 $S_{puf}$, $S_{time}$, $S_{beh}$는 각각 무결성, 적시성, 행위 일관성에 대한 점수(0~1)이며, 가중치 $w_1 = 0.5$, $w_2 = 0.3$, $w_3 = 0.2$로 설정한다. PUF 응답 무결성($w_1$)에 최대 가중치를 부여하는 근거는 PUF 응답 불일치가 하드웨어 수준의 신원 위조를 의미하는 가장 직접적인 증거이기 때문이다. 응답 적시성($w_2$)은 재전송 공격 방어의 핵심 지표이며, 행위 일관성($w_3$)은 네트워크 교란 등에 의한 오탐을 줄이기 위해 보조 지표로서 가장 낮은 가중치를 부여한다.

단, PUF 응답 무결성($S_{puf}$)이 0인 경우, 다른 조건과 무관하게 $TS(U_i) = 0$으로 설정한다. 이는 PUF 불일치가 포획 후 위장 공격의 직접적 증거이므로, 즉시 격리가 필요하기 때문이다. 가중치의 정밀 최적화는 운용 환경과 위협 수준에 따라 조정 가능하며, 시뮬레이션 기반 최적값 도출은 향후 연구 과제로 남긴다.

#### 3) 단계별 대응 메커니즘

군집 내 헤더 드론(CH)은 산출된 신뢰 점수에 따라 표 2와 같이 차등적 정책 대응을 수행한다. 이는 제로트러스트의 최소 권한 원칙을 구현하는 것으로, 획일적인 허용/차단이 아닌 위험 수준에 따른 동적 접근 통제를 가능하게 한다.

**표 2.** 신뢰 점수에 따른 단계별 대응
**Table 2.** Action based on trust score

| Trust Score Range | State | Action |
|---|---|---|
| TS ≥ 0.7 | Normal | Maintain normal communication, apply default period $\tau$ |
| 0.4 ≤ TS <0.7 | Warning | Shorten period to $\tau/2$, restrict high-risk commands, report to GCS |
| TS < 0.4 | Isolation | Block communication, invalidate session key, report anomaly to GCS |

- **정상 상태 (TS ≥ 0.7)**

PUF 응답 무결성, 응답 적시성, 행위 일관성이 모두 양호한 경우이다. CH는 해당 $U_i$의 군집 내 통상 통신을 유지하고, 기본 재인증 주기 $\tau$를 그대로 적용한다. 해당 UAV는 정찰 데이터 송수신, 군집 대형 유지를 위한 좌표 교환, GCS로부터의 임무 명령 수신 등 모든 군집 기능에 제한 없이 참여할 수 있다.

- **주의 상태 (0.4 ≤ TS < 0.7)**

PUF 응답은 일치하나 응답 지연이 임계값에 근접하거나, 행위 일관성 점수가 저하된 경우이다. 이는 네트워크 교란, 일시적 통신 장애, 또는 공격의 초기 징후일 수 있으므로, CH는 다음과 같은 제한적 조치를 수행한다. 첫째, 재인증 주기를 $\tau/2$로 단축하여 해당 노드에 대한 검증 빈도를 높인다. 둘째, 정밀 타격 명령, 군집 대형 변경 등 고위험 명령의 수신 및 실행을 제한한다. 셋째, GCS에 해당 UAV의 주의 상태 전환 이벤트를 보고하여, 군집 전체의 상황 인식을 지원한다. 주의 상태의 UAV가 이후 재인증에서 신뢰 점수가 회복되면 정상 상태로 복귀하며, 지속적으로 점수가 하락하면 격리 상태로 전환된다.

- **격리 상태 (TS < 0.4)**

PUF 응답이 불일치하거나, 복수의 조건에서 동시에 이상이 탐지된 경우이다. 특히 PUF 무결성($S_{puf}$)이 0인 경우, 다른 조건과 무관하게 TS = 0으로 자동 설정되어 즉시 격리가 적용된다. 이는 포획 후 위장 공격의 직접적 증거이기 때문이다. CH는 즉시 다음 절차를 수행한다. 첫째, 해당 $U_i$를 군집 통신에서 격리하여 모든 데이터 송수신을 차단한다. 둘째, 해당 노드와의 세션 키를 무효화하여 이후 통신을 완전히 차단한다. 셋째, GCS에 이상 이벤트를 보고(log: $ID_i$, 실패 유형, TS 값, 시각)한다. 해당 UAV의 군집 재합류 여부는 GCS의 정책 판단에 따라 결정된다. 신뢰 점수 계산은 이미 수행되는 PUF 응답 검증과 타임스탬프 비교 결과를 재활용하는 산술 연산으로 구성되므로, 전체 인증 오버헤드에 미치는 영향은 무시 가능한 수준이다.

## Ⅳ. 보안성 분석 및 성능검증

본 장에서는 제안 기법의 보안성을 정성적으로 분석한 후, 연산 및 통신 오버헤드를 정량적으로 비교한다. 비교 대상은 UAV 환경에서 PUF 기반 인증의 대표 기법인 Alladi 등의 PUF Only[6]와, V2G 환경의 Bansal 등의 SUKA[5]이다.

### 4-1 보안성 분석

보안성 분석은 2장 3절에서 언급한 UAV 군집 환경에서의

보안 요구사항 7개 이외에 제안기법이 달성하는 5개의 항목인 세션 탈취, 내부자 위협, 물리적 포획 후 위장공격, 지속적 검증, 최소 권한 접근통제의 5개 항목을 추가로 비교한다.

#### 1) 상호 인증 및 위장 공격 방어

제안 기법은 초기 상호인증 단계에서 GCS와 $U_i$가 PUF 응답 기반 검증값 $V_1$, $V_2$를 교환하여 양방향 인증을 달성한다. 일반 위장 공격의 경우, 공격자는 $PUF_i(\cdot)$ 함수에 접근할 수 없으므로 $V_1$ 검증 단계에서 탐지된다. 포획 기반 위장 공격(Post-Capture Impersonation)의 경우, 공격자가 자격증명을 추출하더라도 PUF 칩 자체는 물리적으로 복제가 불가능하므로 올바른 응답을 생성할 수 없다. 또한 지속적 재인증을 통해 세션 유지 중에도 주기적으로 새로운 챌린지를 전송하므로, 포획된 자격증명으로 위장한 공격자는 최초 재인증 주기 $\tau$ 이내에 탐지되어 격리된다. 반면 SUKA[5] 및 PUF Only[6]는 초기 인증 시점에만 PUF 검증을 수행하므로, 초기 인증 이후 발생하는 포획 기반 위장 공격에는 대응할 수 없다.

#### 2) 재전송 공격 및 중간자 공격 방어

제안 기법은 매 인증 및 재인증 메시지에 난수와 타임스탬프를 포함하며, 사용된 CRP는 데이터베이스에서 제거되므로 재전송 및 재사용이 불가능하다. 또한 GCS가 PUF 응답을 마스킹($C_i^* = C_i \oplus h(R_i \| N_1)$)하여 전송하므로, 공격자가 메시지를 가로채더라도 $R_i$를 모른 상태에서는 원본 챌린지를 복원할 수 없다. 세션 키 $SK = h(R_i \| N_1 \| N_2)$ 역시 PUF 응답 기반으로 생성되어 복호화·무결성 우회가 불가능하다.

#### 3) 세션 탈취 및 내부자 위협 대응

본 항목은 제안 기법이 기존 기법 대비 가장 차별화되는 보안 특성이다. 기존 기법들은 초기 인증 완료 후 세션 동안 노드를 신뢰하므로, 세션 키 탈취나 내부자의 악의적 행동에 대응할 수 없다. 제안 기법은 제로트러스트의 "무엇도 신뢰하지 말고, 모든 것을 매번 확인하라" 원칙에 따라 재인증 주기 $\tau$마다 PUF 기반 신원 재검증을 수행한다. 그리고 신뢰 점수 기반 정책 판단을 통해 PUF 무결성, 응답 적시성, 행위 일관성을 종합적으로 평가한다. 세션 키가 탈취되었더라도 원본 PUF 칩 없이는 재인증 단계에서 즉시 탐지된다. CH 자체도 GCS로부터 주기적으로 재인증을 받는 대상이므로, CH 탈취에도 구조적으로 대응한다. 또한 신뢰 점수에 따른 "정상(Normal)", "주의(Warning)", "격리(Isolation)" 3단계 차등 대응은 제로트러스트의 최소 권한 원칙과 동적 위험 평가를 구현한 것으로, 기존의 이분법적 접근 통제와 근본적으로 차별화된다.

#### 4) 보안 기능 비교

이상의 분석을 종합한 보안 기능 비교는 표 3과 같다.

**표 3.** 보안 기능 비교
**Table 3.** Security feature comparison

| Security Property | PUF Only[6] | SUKA[5] | Proposed |
|---|---|---|---|
| Mutual Authentication | O | O | O |
| Impersonation Attack | O | O | O |
| Replay Attack | O | O | O |
| MITM Attack | O | O | O |
| Physical Capture | O | O | O |
| Device Unclonability | O | O | O |
| Session Abuse | X | X | **O** |
| Insider Threat | X | X | **O** |
| Post-Capture Impersonation | X | X | **O** |
| Continuous Identity Verification | X | X | **O** |
| Least Privilege Access Control | X | X | **O** |

제안 기법은 기존 기법이 충족하는 7개 기본 보안 요구사항을 모두 충족함과 동시에, 제로트러스트 원칙에 기반한 5개 항목을 추가로 충족한다.

### 4-2 성능 분석

본 논문에서 경량성은 기존 1:1 초기 인증 기법보다 모든 연산 항목이 감소한다는 의미가 아니라, UAV의 제한된 연산 자원과 실시간 통신 주기 내에서 추가 보안 기능을 수행할 수 있을 정도로 인증 및 재인증 비용이 낮다는 의미로 정의한다. 따라서 제안 기법의 성능은 초기 인증 1회 비용뿐 아니라, 세션 유지 중 반복 수행되는 재인증 비용과 추가로 충족되는 보안 요구사항을 함께 고려하여 평가한다.

#### 1) 실험 환경

공정한 비교를 위해 초기 인증단계에서 PUF 인증방식을 1회 사용하는 Alladi 등의 PUF Only[6]와 동일한 실험 환경을 채택하였다. 프로세서는 Raspberry Pi 3B(C 언어)이며, 해시 함수는 SHA-256을 모든 비교 기법에 일괄 적용하였다. 단위 연산 비용은 표 4와 같다.

**표 4.** 단위 연산 비용(Raspberry Pi 3B, C언어)
**Table 4.** Unit operation cost (Raspberry Pi 3B, C language)

| Operation | Symbol | Unit Cost (μs) |
|---|---|---|
| Hash(SHA-256) | $T_h$ | 6.5 |
| PUF Challenge-Response | $T_p$ | 0.4 |
| XOR | $T_x$ | 1.26 |
| RNG | $T_n$ | 0.253 |
| Concat | $T_c$ | 0.587 |

#### 2) 초기 인증 연산 비용 비교

세 기법의 초기 상호인증(UAV 1대당 1회)에 소요되는 연산량은 표 5와 같다.

**표 5.** 초기 인증 연산 비용 비교
**Table 5.** Computation cost comparison for initial authentication

| Operation | PUF Only[6] | SUKA[5] | Proposed |
|---|---|---|---|
| Hash($T_h$) | 3 | 6 | 9 |
| PUF($T_p$) | 2 | 1 | 1 |
| XOR($T_x$) | 8 | 6 | 3 |
| RNG($T_n$) | 2 | 2 | 1 |
| Concat($T_c$) | 11 | 4 | 6 |
| Time | 37.34 μs | 49.81 μs | 66.46 μs |

제안 기법의 초기 인증 소요시간은 66.46 μs로 PUF Only[6] 대비 약 78% 증가한다. 이는 GCS-CH-UAV의 3계층 구조에서 세션 키 확립뿐 아니라, 이후 재인증에 사용될 CRP 위임 정보를 생성·검증하기 위한 추가 해시 연산이 포함되기 때문이다. 따라서 제안 기법의 초기 인증 비용은 단순한 1:1 초기 인증 비용이 아니라, 지속적 재인증을 가능하게 하기 위한 초기 설정 비용으로 해석하는 것이 타당하다.

다만 초기 인증 1회 비용 단독 비교는 기능적으로 등가가 아니다. PUF Only[6]가 동일하게 K회의 신원 검증을 수행하려면 초기 인증을 K회 반복해야 하므로, K=3 기준 누적 비용은 37.34×3 = 112.02 μs인 반면 제안 기법은 66.46 + 14.83×3 = 110.95 μs이다. 즉 분할상환비용(amortized cost) 관점에서 환산한 평균 인증 비용은 제안 기법이 27.74 μs로 PUF Only(37.34 μs) 대비 약 26% 감소하며, 이는 78% 증가분이 K회 재인증을 위한 1회성 setup 비용임을 정량적으로 뒷받침한다.

반면, 세션 유지 중 반복적으로 수행되는 재인증 비용은 14.83 μs로 초기 인증 비용의 약 22% 수준에 불과하다. 즉, 제안 기법은 초기 단계에서 제한적인 추가 비용을 부담하는 대신, 이후 세션 유지 단계에서는 낮은 비용으로 지속적 검증을 수행하는 구조이다.

이러한 구조는 초기 인증 이후 노드를 계속 신뢰하는 기존 기법과 달리, 세션 탈취, 포획 후 위장 공격, 내부자 위협 등 세션 유지 중 발생 가능한 위협을 탐지할 수 있다는 점에서 보안 기능 향상과 연산 비용 증가 간의 합리적인 trade-off를 제공한다.

#### 3) 재인증 오버헤드

제안 기법만이 갖는 재인증 1회당 연산은 Hash 2회, PUF 1회, RNG 1회, Concat 2회로, 총 14.83 μs이다. 이는 초기 인증의 약 22% 수준의 경량 연산으로, 제로트러스트의 지속적 검증을 자원 제약 환경에서 실현 가능하게 한 핵심 설계이다. 본 논문에서의 경량성은 기존 1:1 초기 인증 기법보다 모든 연산 항목이 감소한다는 의미가 아니라, UAV의 제한된 연산 자원과 실시간 통신 주기 내에서 지속적 재인증을 반복 수행할 수 있을 정도로 인증 비용이 낮다는 의미이다. 따라서 제안 기법의 성능은 초기 인증 1회 비용뿐 아니라, 세션 유지 중 반복 수행되는 재인증 비용과 추가로 충족되는 보안 요구사항을 함께 고려하여 평가되어야 한다. 이러한 관점에서 제안 기법은 초기 단계에서 CRP 위임을 위한 추가 비용을 부담하지만, 이후 세션 유지 단계에서는 14.83 μs의 낮은 비용으로 지속적 검증을 수행할 수 있다.

#### 4) K(재인증 횟수)값에 따른 민감도 분석

재인증 횟수 K가 증가함에 따라 총 소요시간이 선형적으로 증가하지만, K=3 기준 약 110.95 μs는 UAV C2 링크 성능 평가에서 활용되는 단방향 지연 기준 50 ms[13]의 약 0.22% 수준으로 매우 작은 값이다. K값에 따른 총 소요시간은 표 6과 그림 2에 나타내었다.

**표 6.** K값에 따른 총 소요시간(UAV 1대당)
**Table 6.** Total cost by re-authentication count K

| K | Total Cost (μs) | vs PUF Only[6] |
|---|---|---|
| 1 | 66.46 + 14.83 × 1 = 81.29 | +118% |
| 3 | 66.46 + 14.83 × 3 = 110.95 | +197% |
| 5 | 66.46 + 14.83 × 5 = 140.61 | +277% |

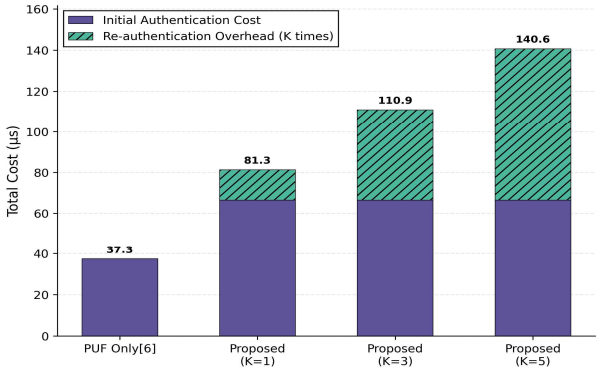


**그림 2.** K값에 따른 총 소요시간 그래프(UAV 1대당)
**Fig. 2.** Total cost comparison by re-authentication (K=1,3,5)

#### 5) 군집 규모 확장성 분석

UAV 군집 규모 N에 따른 전체 인증 소요시간은 표 7과 같다(재인증 횟수 K=3 기준).

N=100 기준 제안 기법의 총 소요시간은 약 11.1 ms로, UAV C2 링크 성능 평가에서 활용되는 단방향 지연 기준 50 ms[13]의 약 22% 수준이다. PUF Only[6] 대비 약 2.97배이나, PUF Only가 동일하게 K=3회의 신원 검증을 수행하려면 매회 초기 인증을 반복해야 하므로 3,734×3 = 11,202 μs

가 소요되어, 제안 기법(11,095 μs)과 거의 동등한 수준이다. 즉, 제안 기법은 PUF Only와 사실상 동등한 연산 비용으로 세션 탈취 및 내부자 위협 탐지 기능을 추가로 제공한다. 모든 기법이 선형적 증가만을 보이며, 실제 운용에서는 UAV별 재인증이 병렬 수행되므로 체감 지연은 이보다 작다. 군집 규모에 따른 소요시간 비교는 그림 3에 나타내었다.

**표 7.** 군집 규모별 총 소요시간(K=3)
**Table 7.** Total cost by swarm size N (K=3)

| UAV (N) | PUF Only[6] | SUKA[5] | Proposed |
|---|---|---|---|
| 5 | 186.7 | 249.1 | 554.8 |
| 10 | 373.4 | 498.1 | 1,109.5 |
| 20 | 746.8 | 996.2 | 2,219.0 |
| 30 | 1,120.2 | 1,494.3 | 3,328.5 |
| 50 | 1,867.0 | 2,490.5 | 5,547.5 |
| 75 | 2,800.5 | 3,735.8 | 8,321.3 |
| 100 | 3,734.0 | 4,981.0 | 11,095.0 |

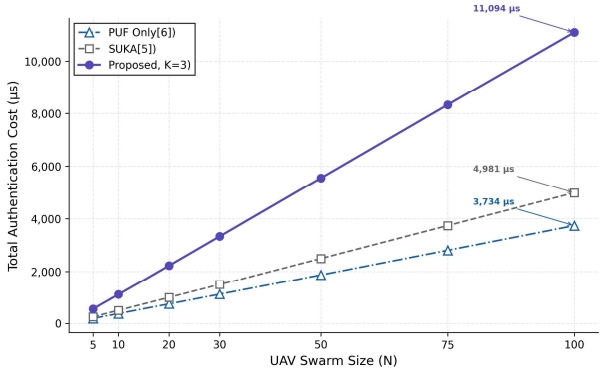


**그림 3.** 군집 규모 N에 따른 세 기법의 인증 소요시간 그래프
**Fig. 3.** Total cost comparison by swarm size N

다만 이 결과는 연산 비용 중심의 이론적 분석이며, 실제 무선 채널에서 발생하는 RTT, 패킷 손실, 멀티홉 라우팅 지연은 포함하지 않는다. 실시간 UAV 군집 협조 운용에서 통신 지연이 핵심 제약 요인으로 작용함[14]을 고려할 때, 본 결과는 제안 기법이 CH의 연산 자원 측면에서 군집 규모 증가를 수용할 수 있음을 보이기 위한 것이며, 실제 UAV 군집 환경에서의 최적 재인증 주기 τ는 네트워크 지연을 함께 고려하여 설정되어야 한다. 특히 N대의 UAV를 순차적으로 재인증하는 경우 τ는 최소한 N대의 재인증 연산시간과 각 노드 간 통신 지연을 모두 포함할 수 있도록 설정되어야 하며, 이에 대한 정밀 평가는 NS-3 기반 네트워크 시뮬레이션을 통해 후속 연구에서 수행할 필요가 있다.

#### 6) 통신 비용 비교

해시 다이제스트 256 bit, PUF 응답 256 bit, 난수 128 bit, 식별자 64 bit 기준 UAV 1대당 통신 비용은 표 8과 같다.

제안 기법은 PUF Only 대비 약 60% 통신량 증가를 보이나, 이는 3회의 재인증 메시지를 포함한 값이다. 재인증 1회당 추가 통신량은 약 256 bit(32 Bytes)로, UAV 표준 통신 프로토콜인 MAVLink v1.0의 최대 패킷 길이인 263 Bytes[12]의 약 12.2% 수준에 해당한다. 따라서 제안 기법의 재인증 메시지는 일반적인 UAV 제어·텔레메트리 트래픽 대비 제한적인 추가 통신 오버헤드로 해석할 수 있다.

**표 8.** UAV 1대당 통신 비용 (K=3)
**Table 8.** Communication cost per UAV (K=3)

| Item | PUF Only[6] | SUKA[5] | Proposed |
|---|---|---|---|
| Number of Messages | 4 | 3 | 10 |
| Total Communication (bits) | ~1500 | 1600 | ~ 2400 |

### 4-3 분석 종합

이상의 보안성 및 성능 분석 결과를 종합하면, 제안 기법은 기존 기법 대비 5개 보안 항목을 추가로 충족하면서도, 세션당 평균 인증 비용, 즉 분할상환비용(amortized cost) 관점에서 PUF Only[6] 대비 약 26% 감소하였으며(동일 검증 횟수 K=3 기준 누적 비용도 거의 동등 수준), 재인증 연산은 14.83 μs(초기 인증의 22%)로 경량화되었고, 100대 규모 군집에서도 총 약 11.1 ms의 소요시간만을 요구한다. 이는 앞서 4-2절에서 언급한 UAV C2 링크 단방향 지연 기준 50 ms 대비 약 22% 수준에 해당하여 실시간 운용에 영향을 주지 않는 범위에 있다. 한편 실시간 UAV 군집 협조 운용에서 통신 지연이 중요한 제약 요인으로 작용하므로[14], 제안 기법의 연산 오버헤드는 네트워크 지연과 함께 통합적으로 평가할 필요가 있다. 따라서 제안 기법은 보안성의 상당한 향상을 달성하면서도, 연산 비용 측면에서 실시간 운용 적용 가능성을 갖는 합리적 트레이드오프를 제공한다.

## V. 결 론

본 논문은 IoBT UAV Swarm 환경에서 제로트러스트 기반 PUF 경량 상호인증 프로토콜을 제안하였다. 기존의 PUF 기반 UAV 인증 기법들은 물리적 포획 공격에 대한 저항성을 확보하였으나, 초기 인증 시점에만 신원 검증을 수행하는 경계 기반 보안 모델에 의존하여 세션 탈취, 내부자 위협, 포획 후 위장 공격에 구조적으로 대응할 수 없었다. 또한 1:1 통신 기반으로 설계되어 UAV 군집의 계층적 구조와 확장성을 반영하지 못하는 한계를 가졌다.

제안 프로토콜은 이러한 한계를 해소하기 위해 PUF의 경량 인증 특성과 제로트러스트의 지속적 검증 원칙을 결합하였다. PUF 응답 무결성, 응답 적시성, 행위 일관성을 종합한 신뢰 점수 기반 정책 판단을 통해 “정상(Normal)”, “주의

(Warning)", "격리(Isolation)"의 3단계 차등 대응을 구현함으로써, 제로트러스트의 최소 권한 원칙과 동적 위험 평가를 UAV 군집 환경에 실질적으로 적용하였다.

보안성 분석 결과, 제안 기법은 Alladi 등의 PUF Only[6]와 Bansal 등의 SUKA[5]가 충족하는 7개 기본 보안 요구사항을 모두 충족한다. 동시에 세션 탈취, 내부자 위협 탐지, 포획 후 위장 공격 탐지, 지속적 신원 재검증, 최소 권한 접근 통제의 5개 항목을 추가로 충족하였다. 성능 분석 결과 [5], [6]과 동일한 환경에서 재인증 연산은 14.83 μs로 초기 인증(66.46 μs)의 약 22% 수준으로 경량화되었으며, K=3 재인증 기준 100대 규모 군집에서도 총 약 11.1 ms의 소요시간만을 요구하였으며, 이는 UAV C2 링크 성능 평가에서 활용되는 50 ms 수준의 단방향 지연 기준보다 낮은 값이다. 따라서 제안 기법의 성능은 초기 인증 비용만으로 평가하기보다, 초기 단계에서 CRP 위임을 위한 제한적인 추가 비용을 부담하는 대신 세션 유지 단계에서 반복적인 경량 재인증을 수행하고 추가 보안 요구사항을 충족하는 보안성 향상과 연산 비용 증가 간의 합리적인 trade-off로 해석할 수 있다.

본 논문의 한계와 향후 연구방향은 다음과 같다. 첫째, 정성적 보안성 분석과 이론적 연산 비용 분석에 초점을 맞추었으며, 실제 UAV 하드웨어 플랫폼을 활용한 구현 및 실증 실험은 향후 과제로 남긴다. 둘째, 재인증 주기 τ와 재인증 횟수 K의 최적값은 임무 특성과 위협 수준에 따라 동적으로 조정될 필요가 있다. 셋째, BAN Logic이나 ProVerif 등 형식 검증 도구를 활용한 프로토콜의 형식적 안전성 증명이 필요하다. 넷째, 제안 기법을 한국군 C4I 체계 및 IoBT 운용 환경에 실제 적용하기 위한 통합 보안정책 프레임워크와의 연계 방안에 대한 후속 연구가 요구된다.

## 참고문헌


[1] M. S. Alkatheiri, S. Saleem, M. A. Alqarni, A. O. Aseeri, S. H. Chauhdary, and Y. Zhuang, "A Lightweight Authentication Scheme for a Network of Unmanned Aerial Vehicles (UAVs) by Using Physical Unclonable Functions," *Electronics*, Vol. 11, No. 18, 2921, September 2022. https://doi.org/10.3390/electronics11182921

[2] X. Zhao, Q. Zhao, Y. Liu, and F. Zhang, "An Ultracompact Switching-Voltage-Based Fully Reconfigurable RRAM PUF with Low Native Instability," *IEEE Transactions on Electron Devices*, Vol. 67, No. 7, pp. 3010-3013, July 2020. https://doi.org/10.1109/TED.2020.2996181

[3] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet of Things Journal*, Vol. 5, No. 1, pp. 269-282, February 2018. https://doi.org/10.1109/JIOT.2017.2780232

[4] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," *IEEE Transactions on Vehicular Technology*, Vol. 68, No. 7, pp. 6903-6916, July 2019. https://doi.org/10.1109/TVT.2019.2911672

[5] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar and M. Guizani, "Lightweight Mutual Authentication Protocol for V2G Using Physical Unclonable Function," *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 7, pp. 7234-7246, July 2020. https://doi.org/10.1109/TVT.2020.2976960

[6] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication," *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 12, pp. 15068-15077, December 2020. https://doi.org/10.1109/TVT.2020.3033060

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST, Gaithersburg: MD, NIST Special Publication 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207

[8] U.S. Department of Defense and Department of Defense Chief Information Officer. Department of Defense Zero Trust Reference Architecture v2.0 [Internet]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[9] Ministry of Science and ICT, Korea Internet & Security Agency. Zero Trust Guideline 2.0 [Internet]. Available: https://www.kisa.or.kr/2060204/form?postSeq=18&page=1.

[10] C. M. Oh and S. Kang, "A Study on the Application of Zero Trust in Cyber Warfare Electronic Environment," *Journal of the Korea Society of Information Technology Policy & Management*, Vol. 17, No. 2, pp. 3833-3839, 2025.

[11] D. Kang, S. Park, Y. Jeong, and T. S. Shon, "Designing a Security Policy Framework for the Republic of Korea Military C4I System Based on Zero Trust Architecture," *Journal of Defense and Security*, Vol. 7, No. 1, pp. 183-207, 2025.

[12] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro Air Vehicle Link (MAVLink) in a Nutshell: A Survey," *IEEE Access*, Vol. 7, pp. 87658-87680, 2019. https://doi.org/10.1109/ACCESS.2019.2924410

[13] R. Amorim, I. Z. Kovács, J. Wigard, G. Pocovi, T. B. Sørensen, and P. Mogensen, "Improving Drone's Command and Control Link Reliability Through

Dual-Network Connectivity," in *Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, pp. 1-6, 2019. https://doi.org/10.1109/VTCSpring.2019.8746579

[14] R. Vera-Amaro, A. Luviano-Juárez, M. E. Rivero-Ángeles, D. Márquez-González, and D. P. Suárez-Ángeles, "Measurement-Informed Latency Limits for Real-Time UAV Swarm Coordination," *Drones*, Vol. 10, No. 4, 310, 2026. https://doi.org/10.3390/drones10040310

**백두현(Duhyun Baek)**

2020년 : 아주대학교 정보통신대학 국방디지털융합학과 졸업(학사)

2022년～현 재: 아주대학교 국방디지털융합학과 석사과정

※관심분야 : 사이버 보안, UAV/IoT 보안, 경량 인증, 제로트러스트

**손태식(Taeshik Shon)**

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)

2002년 : 아주대학교 정보통신전문대학원 졸업(석사)

2005년 : 고려대학교 정보보호대학원 졸업(박사)

2004년～2005년: University of Minnesota 방문연구원

2005년～2011년: 삼성전자 통신·DMC 연구소 책임연구원

2017년～2018년: Illinois Institute of Technology 방문교수

2011년～현 재: 아주대학교 정보통신대학 사이버보안학과 교수

※관심분야 : Digital Forensics, ICS/Automotive Security

**정찬기(Chanki Jeong)**

1986년 : 공군사관학교 전자공학과 졸업(학사)

1994년 : 플로리다공대 컴퓨터공학과 졸업(석사)

2001년 : 플로리다공대 컴퓨터공학과 졸업(박사)

1986년～2007년: 공군 정보통신장교

2008년～2014년: 국방대학교 컴퓨터공학과 교수

2016년～현 재: 아주대학교 소프트웨어융합대학 국방디지털융합학과 교수

※관심분야 : Enterprise Engineering, Cloud Computing, AI Cybersecurity