

연합학습 기반 UAV 이상탐지 및 VC 인증·ChaCha20 기반 보안 세션 아키텍처

박성수, 김기형*
아주대학교, *아주대학교

parky@ajou.ac.kr, *kkim86@ajou.ac.kr

Federated Learning-Based UAV Anomaly Detection and VC Authentication· ChaCha20 Based Secure Session Architecture

SeongSu Park, Ki-Hyung Kim*
Ajou Univ.

요 약

본 논문은 2020 년 CMU 에서 공개한 ALFA Dataset 을 활용하여 무인항공기(UAV) 운영 환경에서의 연합학습(Federated Learning, FL) 이상탐지(Anomaly Detection)용 VC 인증과 ChaCha20 을 활용한 보안 세션 아키텍처를 제안한다. 제안 아키텍처는 각 UAV 가 로컬에서 이상탐지 모델을 학습하고, 중앙 서버는 FedAvg 를 통해 전역 모델을 생성함으로써 데이터 프라이버시를 보호하고 통신 부담을 줄인다. 또한 탐지 결과를 신뢰도 점수(Trust Score)로 변환하여 Verifiable Credential(VC) 형식으로 발급·검증하며, 이를 Noise_XX 키합의와 ChaCha20-Poly1305 세션 암호화에 결합함으로써 UAV 미션 수행 시 강력한 인증·암호화 보안을 제공한다. 실험적으로 ALFA Dataset 의 센서·엔진 이상 로그를 기반으로 한 데모 파이프라인을 구현하였으며, VC 검증·세션 보안·재키잉(re-keying) 정책까지 포함한 결과를 제시한다. 본 연구는 UAV 연합학습 기반 보안 프레임워크 설계에 기여할 수 있다.

I. 서론

최근 UAV(무인항공기)의 활용은 군사·민간 영역에서 빠르게 확산되고 있다. 그러나 분산된 다수 UAV 의 운용은 센서 고장, 엔진 이상, 네트워크 침입 등 다양한 위협에 노출된다. 전통적인 중앙집중식 이상탐지는 데이터 전송 비용과 보안 문제를 유발한다. 따라서 분산 데이터 처리와 보안성 강화를 동시에 만족하는 아키텍처가 필요하다.

본 논문은 UAV 운용 데이터[1]를 활용하여 연합학습 기반 이상탐지를 수행하고, 탐지 결과를 VC 인증 체계[2, 3]와 ChaCha20[4] 기반 보안 세션에 결합하는 방안을 제안한다. 이를 통해 (1) 프라이버시 보존 학습, (2) 권한·정책 기반 인증, (3) 저전력 환경에 적합한 경량 암호 세션을 동시에 달성한다.

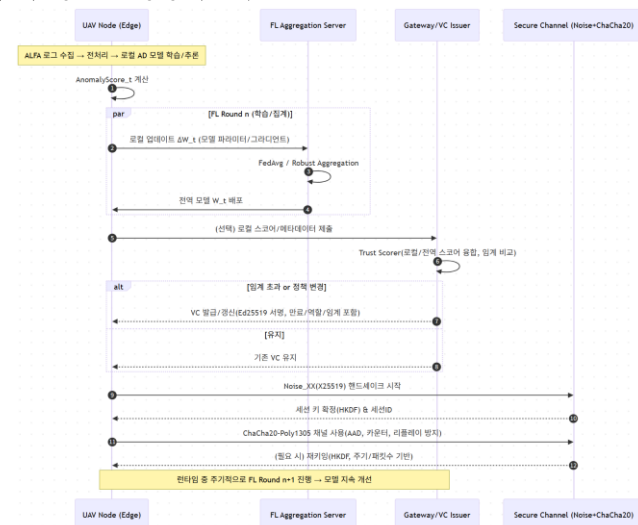
II. 제안 아키텍처

본 논문에서 제안하는 아키텍처는 UAV 운용 환경에서 발생할 수 있는 고장 및 이상 상황을 효율적으로 탐지하고, 그 결과를 결과를 Verifiable Credential(VC) 기반 권한 인증[2, 3]과 ChaCha20 보안 세션에 결합하는 아키텍처를 제안한다. 이를 위해 연합학습(Federated Learning, FL)을 기반으로 한 이상탐지, Verifiable Credential(VC) 인증, 그리고 ChaCha20 세션 보안을 결합하였다.

우선 데이터 계층에서는 UAV 단말이 ALFA Dataset 과 같은 실제 운용 로그를 로컬에서 수집한다[1]. 각 단말은 센서·엔진·조종면 데이터를 윈도우 기반으로 전처리하고, median 및 MAD(Median Absolute Deviation)를 활용한 로컬 이상탐지 모델을 학습한다[5]. 이러한 접근은 데이터가 중앙 서버로 전송되지 않고 각

단말 내부에 머무르도록 하여 프라이버시와 통신 효율성을 동시에 확보한다.

모델 계층에서는 중앙 서버가 각 UAV 에서 전송된 모델 파라미터를 FedAvg 방식으로 집계하여 전역 모델을 생성한다. 필요 시 Median-Krum Aggregation 과 같은 Byzantine-robust 기법[6]을 적용하여 악의적 업데이트나 노이즈에 강건하게 동작할 수 있다. 생성된 전역 모델은 다시 각 UAV 에 배포되어 탐지 성능을 향상시킨다.



<그림 1:운용 시퀀스(FL+ 런타임 인증/세션)>

정책 계층에서는 각 UAV 가 산출한 이상탐지 점수를 기반으로 신뢰도(trust score)를 계산하고, 이를 임계값과 비교하여 허용(allow), 2 단계 인증(2FA), 거부(deny)의 정책을 결정한다. 이 결과는 Verifiable Credential(VC) 형태로 발급된다. VC 는 Ed25519 서명을 통해 위·변조를 방지하며, 기체 DID, 미션 식별자, 신뢰도

점수, 정책 및 만료 시간 등을 포함한다. VC 는 네트워크 단절 상황에서도 자율적으로 검증 가능하도록 설계되며, revocation epoch 를 통해 최신 상태 동기화가 가능하다.

보안 계층에서는 VC 와 Noise_XX 키합의를 결합하여 세션 보안을 수립한다[7]. 키합의 시 HKDF 의 info 필드에 VC Digest, 미션 ID, UAV DID 를 포함시켜 세션 키가 권한·미션·디바이스와 강하게 결속되도록 한다. 이후 ChaCha20-Poly1305 AEAD (Authenticated Encryption with Associated Data) 암호화를 통해 UAV 와 서버 간의 통신을 보호하며, Nonce 는 세션 ID 와 카운터로 구성된다[4, 7]. AAD (Additional Authenticated Data)에는 VC Digest 와 미션, 프레임 헤더를 포함시켜 맥락 무결성을 보장한다[2]. 또한 리플레이 방지와 주기적 재키잉 정책을 통해 장기 세션에서도 안전성을 유지한다.

III. 실험 및 데모

실험은 ALFA Dataset 과 합성 데이터를 사용하여 제한한 아키텍처의 동작을 검증하였다. 세 개의 UAV 노드를 가정하여 각 노드가 로컬 robust anomaly detector 를 학습하고, FedAvg 를 통해 전역 모델을 산출하였다. 데이터 전처리 과정에서는 센서 로그를 윈도우 단위로 분할하여 이상 상황이 반영된 부분과 정상 구간을 비교하였다.

이상탐지 결과를 통해 전역 모델은 정상 데이터에 비해 엔진 고장 및 조종면 이상 데이터에서 유의미하게 높은 anomaly score 를 산출하였으며, 이를 바탕으로 trust score 가 산출되었다. 예를 들어 정상 로그에서는 높은 신뢰도가 유지되었으나, 이상 로그에서는 임계값 미만으로 떨어져 deny 정책이 실행되도록 했다.

발급된 VC 에는 UAV 의 DID, 미션 ID, 신뢰도, 정책, 만료 시간, revocation epoch 등이 포함되었으며, 서버는 이를 Ed25519 기반으로 검증하였다. 실험에서는 정상 로그의 경우 “allow” 정책이 적용되어 VC 가 발급되었고, 이상 로그의 경우 “2FA” 또는 “deny”가 적용됨을 확인하였다.

보안 세션 검증 단계에서는 Noise_XX 기반 키합의로 생성된 세션 키가 VC Digest, 미션 ID, UAV DID 에 바인딩되었다. 이후 ChaCha20-Poly1305 암호화 채널을 통해 UAV 명령 메시지를 보호하였으며, Replay 공격 시도는 카운터 검증을 통해 차단되었다. 또한 패킷 전송 횟수와 시간 기준으로 재키잉이 수행되어 장기간 세션에서도 안정적인 보안을 유지할 수 있었다.

또한, VC Digest 와 미션 ID, UAV DID 가 Noise_XX 키합의 및 ChaCha20-Poly1305 세션 암호화에 바인딩되어, anomaly detection 결과가 보안 세션까지 연계됨을 검증하였다. 데모에서는 (1) VC 발급 및 검증, (2) Noise 핸드셰이크 성공 및 세션키 확정, (3) ChaCha20 암호화 명령 전송 및 리플레이 공격 차단, (4) 패킷·시간 기준 재키잉이 성공적으로 수행되는 것도 모두 확인되었다.

이러한 데모를 통해 본 연구의 아키텍처는 (1) 분산 데이터 기반 이상탐지, (2) 정책·신뢰도 기반 VC 인증, (3) 경량 암호 기반 세션 보안을 효과적으로 결합할 수 있음을 검증하였다. 이는 UAV 운용 환경에서 프라이버시, 신뢰성, 보안성을 동시에 확보할 수 있는 실질적인 프레임워크임을 보여준다.

IV. 결론 및 향후 연구

본 연구는 ALFA Dataset 을 기반으로 UAV 연합학습 이상탐지와 VC 인증, ChaCha20 보안 세션을 통합한 아키텍처를 제시하였다. 이는 UAV 운용의 데이터 프라이버시·인증 보장·세션 보안을 동시에 만족시키는 프레임워크로 활용될 수 있다. 이 연구를 기반으로 향후 (1) GRU/TCN/AE 기반 시계열 모델 확장, (2) Byzantine-robust FL 알고리즘 확장, (3) VC 폐기 메커니즘 (비트맵·Accumulator) 구현, (4) 수시로 Offline 되는 네트워크 환경에서의 안정적인 운영에 대해 연구할 것이다.

ACKNOWLEDGMENT

이 논문은 2025 년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행되었고(KRIT-CT-23-041), 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었고(IITP-2025-RS-2021-II211835), 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 (2021-0-00590, RS-2021-II210590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발)

참 고 문 헌

- 1 Keipour, A., Mousaei, M., and Scherer, S.: ‘ALFA: A dataset for UAV fault and anomaly detection’, The International Journal of Robotics Research, 2021, 40, (2-3), pp. 515-520
- 2 Chadwick, D.W., and Burnett, D.C.: ‘Verifiable credentials’, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials, 2021, pp. 126
- 3 Park, S., and Kim, K.-H.: ‘Leveraging Digital Twins for ON/OFF-LINE Blockchain Networks: A Resilient Framework for Drone and IoT Communication’, in Editor (Ed.)^(Eds.): ‘Book Leveraging Digital Twins for ON/OFF-LINE Blockchain Networks: A Resilient Framework for Drone and IoT Communication’ (IEEE, 2025, edn.), pp. 426-430
- 4 Bernstein, D.J.: ‘ChaCha, a variant of Salsa20’, in Editor (Ed.)^(Eds.): ‘Book ChaCha, a variant of Salsa20’ (Lausanne, Switzerland, 2008, edn.), pp. 3-5
- 5 Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A., and Seth, K.: ‘Practical Secure Aggregation for Privacy-Preserving Machine Learning’. Proc. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, Texas, USA2017 pp. Pages
- 6 Colosimo, F., and De Rango, F.: ‘Median-krum: A joint distance-statistical based byzantine-robust algorithm in federated learning’, in Editor (Ed.)^(Eds.): ‘Book Median-krum: A joint distance-statistical based byzantine-robust algorithm in federated learning’ (2023, edn.), pp. 61-68
- 7 Perrin, T.: ‘The noise protocol framework’ (2018. 2018)