UAV 네트워크에서 경로 프라이버시 강화를 위한 블록체인 기반 가명 교체 메커니즘

최빈, 허가빈, 도인실

이화여자대학교

chlqls@ewhain.net, gjrkqls@ewhain.net, isdoh1@ewha.ac.kr

A Blockchain-based Pseudonym Change Mechanism for Enhancing Path Privacy in UAV Networks

Been Choi, Gabin Heo, Inshil Doh

Ewha Womans Univ.

요 약

최근 FANET의 확산으로 UAV의 경로 정보 노출 등 프라이버시 침해 우려가 커지고 있다. 기존 시스템은 자원 제약적 환경에서의 과도한 에너지 소모와 중앙 집중식 구조의 보안 취약점이라는 한계를 지닌다. 본 연구에서는 이를 해결하기 위해 격자 기반의 믹스 존(Mix-Zone) 전략과 블록체인을 결합한 탈중앙화 가명 교체 메커니즘을 제안한다. 격자 구조를 통해 연산 효율을 높이고, 블록체인으로 가명 관리의 무결성과 사후 추적성을 확보하여 자원 최적화된 경로 프라이버시 보호를 보장한다.

Ⅰ. 서론

최근 다양한 분야에서 FANET(Flying Ad-hoc Network)의 활용이 확대되고 있으나, 이는 동적인 토폴로지 변화와 개방된 무선 채널 의존성의 특성으로 인해 도청 및 데이터 가로채기에 매우 취약하다. 특히 UAV (Unmanned Aerial Vehicle)의 고유 식별자가 노출될 경우 비행경로 및 위치 정보가 실시간으로 추적되는 심각한 프라이버시 침해 문제가 발생한다. 이에 따라 UAV의 이동 궤적을 보호하기 위한 가명(Pseudonym) 기술을 활용한 경로 프라이버시 강화 메커니즘이 필수적으로 요구된다. 하지만 기존 시스템은 대량의 인증서 관리에 따른 자원 소모와 희소 네트워크에서의 낮은 익명성이라는 문제를 가지고 있다. 또한 중앙 집중식 구조는 단일 장애점(Single Point of Failure, SPoF) 및 DoS(Denial-of-Service) 공격에 취약하며 데이터 무결성 검증이 어렵다는 보안상 한계가 있다[1]. 본 연구에서는 이를 해결하기 위해 믹스 존(Mix-Zone)과 블록체인 기술을 결합한 탈중앙화 가명 교환 메커니즘을 제안한다. 이를 통해 효율적이면서도 가명 관리의 무결성과 강건한 익명성을 보장하는 실용적인 프라이버시 보호 프레임워크를 제시하고자 한다.

Ⅱ. 관련 연구

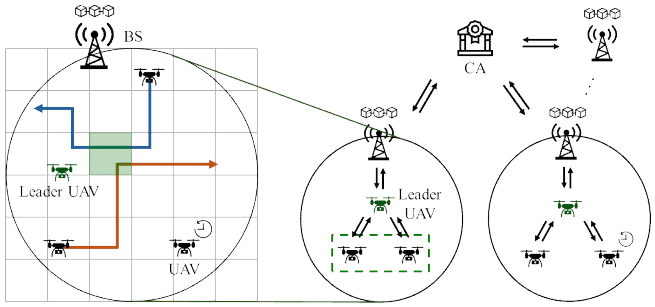
가명 교환은 노드의 식별자를 주기적으로 교체하여 추적 가능성을 차단하고 익명성을 확보하는 기술이다. 대표적 전략인 믹스 존(Mix-zone)은 다수의 노드가 특정 구역에서 동시에 가명을 변경하여 공격자의 추적을 혼란시키는 보호 구역을 의미하며, 고정 장치를 활용하는 인프라 방식과 노드 간 그룹을 형성하는 애드혹(Ad-hoc) 방식으로 구분된다. 이 외에도 단일 노드의 시간 기반 교체나 전력 제어를 통한 도청 범위 축소 등 다양한 전략이 연구되고 있다[2].

최근 UAV 환경에서는 생체 모방 기술을 활용해 드론 교통량에 따라 믹스 존 위치를 실시간 변경하는 BioMixD 전략이 제안되었다[3]. BioMixD는 동적 믹스 존과 경로 전환을 결합하여 높은 추적 저항성을 제공한다. 그러나 이러한 방식은 프라이버시 강화를 위해 의도적인 경로 우회를 수반함으로써 에너지 소모와 임무 지연을 초래하며, 이는 자원이 제한적인 UAV 환경에서 서비스 품질을 저하시키는 한계를 지닌다.

Ⅲ. UAV 네트워크에서 경로 프라이버시 강화를 위한 블록체인 기반 가명 교체 메커니즘

3.1. 메커니즘 개요 및 핵심 전략

본 연구에서 제안하는 가명 교체 메커니즘은 자원 제약적인 FANET 환경을 고려하여 격자 기반 가명 교환과 유효기간 기반 자가 갱신 전략을 채택한다. 격자 기반 가명 교환은 3차원 공간을 격자 단위로 분할하여 믹스 존을 형성하고 가명을 교환하는 방식이다. 이는 UAV의 고이동성에 따른 실시간 거리 계산을 최소화하고, 무분별한 교환을 방지하여 연산 오버헤드와 익명성 사이의 최적의 상충 관계를 제공한다. 유효기간 기반 자가 갱신은 주변에 교환할 노드가 없는 고립 상황에서 수행된다. UAV가 외부 통신 없이 독립적으로 가명을 생성하여 인프라와의 통신 오버헤드를 줄이고 프라이버시 보호의 연속성을 보장한다.



[그림 1] 블록체인 기반 격자형 가명 교체 메커니즘 구성도

3.2. 메커니즘 구성요소 및 역할

- Certificate Authority (CA): 신뢰 기관으로서 UAV 등록 및 인증서 (Certificate) 발급을 담당한다. 실제 신원과 가명 매핑 정보를 보유하

며, 악성 노드 발생 시에만 신원을 복구하여 사후 조치를 취한다.

- Base Station (BS): 관할 구역 격자를 관리하며 블록체인 풀 노드 역할을 수행한다. 가명 변경 이력을 기록하여 무결성을 유지하고, CA와 UAV 간의 통신을 중계한다.
- Leader UAV: 격자 내 가명 교환 절차를 주도하는 관리자이다. 활성화된 가명 목록을 관리하고 교환 프로세스를 조정하며, 해당 지역 이탈 시 임시 데이터를 폐기한다.
- UAV: 임무 수행 노드로, 상황에 따라 자가 가명 갱신을 수행하고 주변 노드의 악성 행위를 모니터링하여 BS에 보고한다.

3.3. 단계별 상세 프로세스

① UAV 등록 및 초기 가명 발급

UAV가 네트워크에 최초 진입하거나 지역을 이동할 때, BS는 CA에 검증을 요청한다. CA가 UAV의 정당성 확인 후 인증서($Cert$)를 발급하면, BS는 식 (1)과 같이 초기 가명(PID)을 생성하여 블록체인에 기록한다.

$$PID = H(BS_{ID} \parallel Timestamp \parallel Cert) \quad (1)$$

BS_{ID}와 $Timestamp$는 기록 주체와 생성 시점의 유일성을 보장하며, $Cert$는 향후 추적 시 실제 신원과 첫 가명을 연결하는 기초 데이터가 된다. 이후 BS는 UAV에 PID와 임무를 할당한다. 이때 BS는 각 UAV의 비행 경로를 분석하여 경로가 중첩될 것으로 예측되는 격자 구역을 미리 파악하고, 해당 구역의 리더 UAV에게 중첩 정보를 사전에 공유한다.

② 믹스 존 가명 교환 및 트랜잭션 기록

특정 격자 내에 2대 이상의 UAV가 동시에 존재할 경우, 리더 UAV는 활성화된 가명 목록을 통해 노드 신뢰성을 검증한다. 검증이 완료되면 리더는 라운드 로빈(Round Robin) 방식으로 격자 내 각 UAV에게 교체할 타 노드의 PID 정보를 암호화하여 전달한다. 이러한 리더를 통한 교환 방식은 노드 간 직접 통신의 복잡도를 줄이고 가명 관리의 일관성을 확보한다. 가명 변경이 완료되면 리더 UAV는 교체 성공 메시지를 BS에 전송하고, 메시지를 수신한 BS는 변경 이력에 대한 트랜잭션을 생성하여 블록체인에 기록한다.

③ UAV 자가 가명 갱신 및 Silent Period

주변 노드가 없는 상황에서 가명이 만료되면 UAV는 식 (2)를 통해 자가 갱신을 수행한다.

$$PID_{i+1} = H(UID \parallel PID_i \parallel Timestamp) \quad (2)$$

실제 신원(UID)과 이전 가명(PID_i)을 해시 값에 포함함으로써, 악성 노드 적발 시 블록체인에 기록된 이력을 바탕으로 과거 가명들과의 상관관계를 추적하여 일괄적인 대응 조치가 가능하다. 가명 전환 시에는 일정 시간 동안 메시지 전송을 중단하는 Silent Period를 적용한다. 이는 물리적 경로의 불연속성을 확보하여 공격자가 노드를 추적하는 것을 차단한다[2]. 통신 중단으로 인해 발생 가능한 안전 문제는 BS가 사전에 파악된 비행 경로 정보를 활용하여 혼선 없이 개체를 관리함으로써 해결한다.

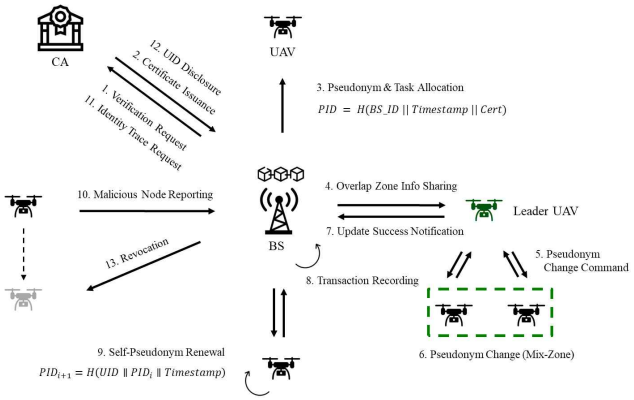
④ 악성 노드 탐지 및 신원 추적

UAV 간 상호 모니터링 중 악성 행위가 탐지되면 BS에 보고되며, BS는 신고 내역을 블록체인에 기록하고 CA에 신원 확인을 요청한다. CA는 블록체인의 가명 이력을 역추적하여 실제 신원을 도출하며, 신고 횟수가 임계치를 초과한 노드는 인증서 폐기 등 제재를 가한다.

⑤ 특수 상황 대응

UAV들이 동일 방향과 속도로 연속된 격자를 통과할 경우, 불필요한 가명 교환이 발생할 수 있다. 이를 방지하기 위해 가변적 교환 전략을 사용한다. 중첩되는 첫 격자에서는 가명을 교환하되, 이후 격자에서는 교환을 건너뛰거나 자가 갱신을 수행하도록 지시한다. 새로운 노드가 진입하여 구성이 변경되면 즉시 일반 교환 프로세스로 회귀하여 익명성 수준을 동적으로 조절한다.

또한 UAV가 동일 격자에 일정 시간 이상 체류하는 경우, 추가적인 가명 교환은 제한되며 가명 유효기간 만료 시 자가 갱신 방식만을 적용하여 과도한 교환으로 인한 에너지 소모를 방지한다.



[그림 2] 단계별 프로세스 다이어그램

Ⅳ. 결론

본 논문은 UAV의 경로 프라이버시를 강화하기 위한 블록체인 기반의 효율적인 가명 교체 메커니즘을 제안하였다. 제안하는 메커니즘은 믹스 존 기반의 가명 교환 전략을 통해 공격자의 추적 가능성을 효과적으로 차단한다. 특히 격자 구조와 자가 발급 방식을 도입함으로써 고이동성 노드의 거리 계산 오버헤드와 외부 인프라 의존도를 낮추어 UAV의 에너지 효율성을 개선하였다. 또한 블록체인을 통해 가명 교체 로그의 무결성을 확보하고, 이상 행위 발생 시 조건부 신원 추적이 가능한 체계를 구축하여 탈중앙화된 환경에서의 신뢰성과 책임성을 동시에 확보하였다.

향후 연구로는 시스템 전반의 경량화 설계를 통해 실시간 운용성을 높이고, 보안 위협 수준에 따른 가명 유효기간 최적화 및 리더 UAV 보호를 위한 보안 체계 고도화 연구를 지속할 계획이다.

ACKNOWLEDGMENT

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (RS-2023-NR076673)
(교신저자: 도인실)

참 고 문 헌

[1] S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun, M. Huth, “Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems,” in IEEE Access, vol. 7, pp. 80390-80403, 2019.

[2] L. Benarous, S. Zeadally, S. Boudjit, A. Mellouk, “A Review of Pseudonym Change Strategies for Location Privacy Preservation Schemes in Vehicular Networks,” ACM Comput. Surv. 57, 8, Article 204, 2025.

[3] Alisson R. Svaigen, Azzedine Boukerche, Linnyer B. Ruiz, Antonio A.F. Loureiro, “BioMixD: A Bio-Inspired and Traffic-Aware Mix Zone Placement Strategy for Location Privacy on the Internet of Drones,” Computer Communications, Volume 195, pp. 111-123, 2022