안전한 UAM 통신을 위한 DLT 기반 PKI 및 Privacy Management System

강상위, 정경헌, 박홍근, 권태경

서울대학교

swkang@mmlab.snu.ac.kr, ghjeong@mmlab.snu.ac.kr, hgpark@mmlab.snu.ac.kr, tkkwon@snu.ac.kr

DLT-based PKI and Privacy Management System for Secure UAM Communications

Sang Wi Kang, Gyeong Heon Jeong, Hong Geun Park, Ted "Taekyoung" Kwon

Seoul National Univ.

요 약

본 논문은 빠르게 증가하고 있는 UAM의 수요에 따라 향후 활성화 될 UAM 통신 환경에서 안전한 보안 통신을 위한 통신 기법을 제안한다. DLT의 분산 합의와 분산 보장이라는 특성을 이용하여 UAM 통신에 적합한 PKI 구조를 제시하였고, UAM 비행 상황에서 발생할 수 있는 Privacy 침해 상황을 상정하여 Privacy Management System을 제시하였다.

Ⅰ. 서 론

최근 도시의 지상교통혼잡 문제, 교통의 확장, 군사적 목적 등으로 UAM (Urban Air Mobility)의 필요성이 대두되고 있다. 대한민국 국토교통부에 따르면, 2030~2035년 UAM 운용 활성화를 목표로 하고 있고, 관련 분야 세계 시장규모는 2040년까지 총 731조 원 규모로 전망하고 있다.[1] UAM 운용 활성화를 위해서는 다양한 요소를 고려해야 하며, 특히 비행하는 UAM의 특성상 안전하고 안정적인 통신이 필요하다.

UAM-Base Station 혹은 UAM-UAM 간 안전한 통신 및 인증을 위해서는 PKI (Public Key Infrastructure) [2] 기법을 사용할 수 있지만, 전통적인 PKI 기법은 인증을 위한 CA (Certificate Authority)와의 통신, 인증서 유효성 검사를 위한 CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol)의 사용 등 상대적으로 안정적인 통신 환경을 기반으로 동작하기에 UAM 등 비행 상황에서의 안정적인 보안 통신 요구사항을 만족시키기 어렵다.

또한, 안전한 통신과 더불어 Privacy 보호 문제도 고려되어야 한다. 예를 들면, UAM 자체의 촬영 장치 혹은 UAM 탑승객의 촬영 장치를 통해 외부를 촬영하게 될 경우, 사생활 침해가 발생할 수 있으며 기업 시설이나 국가 보안 시설에 대해서는 심각한 기업 보안, 국가 안보 위협 문제가 발생할 수 있다. UAM에는 다양한 센서가 탑재되기 때문에 촬영뿐만 아니라 다양한 종류의 정보를 무단으로 획득할 수 있고, 이는 Privacy 보호 문제를 심화시킬 수 있다. 따라서 공공 보안을 위해 UAM에 적합한 능동적 실시간 항공 프라이버시/보안 통합 관제 시스템이 필요하다.

이러한 통신 환경에 대응하기 위하여 DLT (Distributed Ledger Technology) [3] 플랫폼을 고려할 수 있다. 분산 원장의 다양한 요소를 관리자가 직접 조정할 수 있는 DLT 플랫폼이 일반화되면서 DLT를 다양한 분야 접목하기 위한 연구들이 진행되고 있다. [4], [5]에서는 드론 및 UAV의 인증 정보를 저장 및 관리하기 위해 DLT 플랫폼을 사용하였고, [6]에서는 Vehicle을 위한 DLT 기반 PKI 연구를 수행하였다. 따라서 DLT를 UAM 통신 환경에 적용하는 것은 안정적인 통신을 위해 고려할 수 있으며, 본 논문에서는 불안정한 UAM 통신 상황에서의 보안 통신 문제와 Privacy 보호 문제를 해결하기 위해 DLT 기반 PKI 및 Privacy Management System을 제안한다.

Ⅱ. 본론

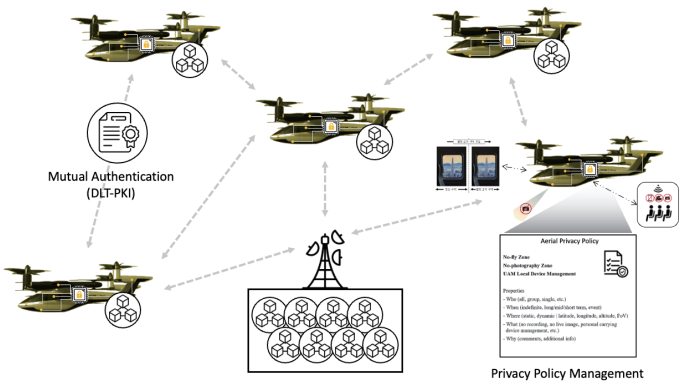

그림 1. DLT-based PKI & Privacy Management System

그림 1은 본 논문에서 제안하고자 하는 통합 시스템의 전체적인 구조를 나타낸 그림이다. 해당 시스템에서는 DLT 플랫폼을 사용하여 PKI 역할 수행을 위한 인증서와 Privacy 보호 기능 수행을 위한 Policy를 저장 및 관리한다. 각 UAM은 DLT의 노드로서의 역할을 수행하며 인증서와 Privacy Policy를 저장하고 있다. UAM이 새로운 인증서와 Policy를 Patch하기 위해 인접 UAM 노드와 통신할 수 있다. 이때, 지연을 최소화하기 위해 가장 가까운 UAM 노드부터 통신을 시도한다. 단순한 정보 Patch가 아닌 새로운 정보를 DLT에 배포하기 위해서는 Base Station을 통해 정보를 갱신하고 각 UAM 노드로 배포한다.

DLT 플랫폼에서는 SPOF (Single Point of Failure)가 존재하지 않기 때문에, 주변 노드(UAM)의 응답 불능으로 인한 Patch 실패의 경우가 사라진다. 따라서 불안정한 UAM 통신 환경에서 안정적인 통신이 가능하게

된다.

또한, 모든 Transaction을 공개하는 투명성과 기록 조작이 불가능한 불변성은 UAM 비행에 도움을 줄 수 있다. 인증 이력, 비행 정보 등 안전한 데이터 로깅이 가능해 감사 및 사고 조사에 활용할 수 있고, 통신 참여 노드들이 인증 정보 및 프라이버시 보호 정책을 열람할 수 있어 신뢰성과 책임성이 향상된다.

DLT 플랫폼 구현에는 Enterprise 수준에서 사용 가능한 Open-Source Permissioned DLT 플랫폼인 Hyperledger [7]를 사용할 수 있다. 이를 통해 PKI 및 Privacy Policy Management에 적합한 유연한 설계가 가능하다.

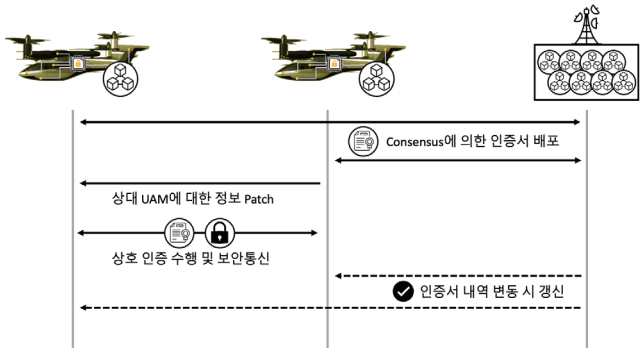

그림 2. DLT를 적용한 UAM 통신 환경에서의 PKI 동작 흐름

그림 2는 DLT를 적용한 UAM 통신 환경에서의 PKI를 나타낸 그림이다. 전통적 PKI에서는 루트 CA와 후속 인증서 Chain을 검증하는 방식으로 인증이 수행된다. 하지만 DLT 기반 PKI에서는 암호학적 증명과 분산 합의를 통해 인증서 유효성 검증이 가능하다. 즉, DLT를 거치게 되면 단일 CA의 보장이 아닌 전체 네트워크 합의에 의한 분산된 보장이라는 개념이 되고, 이 합의 기록이 불변성과 투명성이라는 특성을 지니게 된다. 이러한 특성은 단일 신뢰 보장 기관이 없거나 바람직하지 않은 환경에 적합하다.

DLT로 구현된 UAM PKI에서는 신원 정보와 관련 공개키를 분산 원장에 저장하여 관리하게 된다. 처음에는 각 UAM의 정보를 생성하고 이를 Main 노드인 Base Station에 전달한다. DLT의 분산 원장에 이 정보들이 분산 합의에 의해 정상적으로 받아들여지면 이 정보들은 분산 보장 개념에 따라 유효성을 지니게 되고, 해당 분산 원장 네트워크 어디에서도 유효한 정보로 받아들여지게 된다. 상대 UAM과 통신하고자 할 경우, 자신과 상대 UAM 각각 인증서를 인증하고 상호 인증이 가능하게 된다. 유효한 인증서라면 보안 채널을 수립하고 안전한 통신을 시작한다.

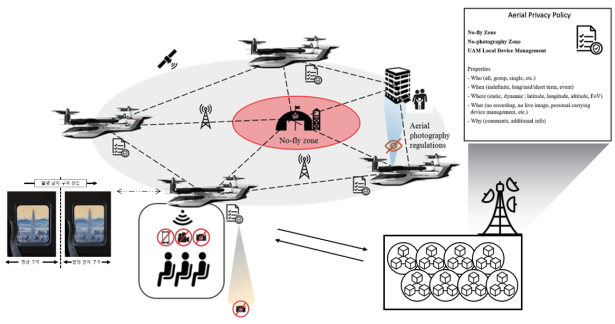

그림 3. DLT를 적용한 Privacy Management System

그림 3은 DLT를 적용한 Privacy Policy Management System을 나타낸 그림이다. DLT로 구현된 Privacy Policy Management System에서는 Policy를 분산 원장에 저장, 관리하기 때문에 유효성이 보장된 Policy를 실행시킬 수 있다. Policy에는 어떤 UAM이, 언제, 어떤 장소에 방문했을 때 어떤 제약사항을 동작시켜야 하는지 명시되어 있다. UAM에 장착된 카메라를 제한하거나 탐승객의 전자기기 사용 제한, UAM에 장착된 다양한 센서를 제한하는 등 Privacy 침해 방지를 위한 다양한 제한 기능이 실행될 수 있다.

Ⅲ. 결론

본 논문에서는 불안정한 UAM 통신 상황에서 안전한 통신을 위해 DLT를 적용한 UAM PKI 및 Policy Management System을 제안하였다. DLT의 분산 합의 및 분산 보장이라는 특성으로 UAM 비행 환경에 맞는 PKI를 구현할 수 있고, UAM 비행 상황에서 발생할 수 있는 Privacy 침해 상황에 대응할 수 있는 Policy 기반 기법을 보였다. 향후 보다 구체적인 구현을 통해 해당 제안을 실증할 예정이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2025-2021-0-02048)

참 고 문 헌

[1] 대한민국 국토교통부, "한국형 도심항공교통(K-UAM) 로드맵," 2020, (https://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95083976).

[2] SSL.com, "What is Public Key Infrastructure (PKI)?," 2024, (https://www.ssl.com/article/what-is-public-key-infrastructure-pki/).

[3] Government Office for Science (UK), “Distributed Ledger Technology: beyond block chain”, January. 2016.

[4] J. C. P. García, A. Benslimane, A. Braeken and Z. Su, "μTesla-Based Authentication for Reliable and Secure Broadcast Communications in IoD Using Blockchain," in IEEE Internet of Things Journal, vol. 10, no. 20, pp. 18400-18413, 2023.

[5] N. Jäger, A. Aßmuth, “An Approach for Decentralized Authentication in Networks of UAVs,” in Proc of the 12th International Conference on Cloud Computing, GRIDs, and Virtualization (Cloud Computing 2021), 2021.

[6] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto and P. Pagano, "IOTA-VPKI: A DLT-Based and Resource Efficient Vehicular Public Key Infrastructure," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pp. 1-6, 2018.

[7] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” In Proceedings of the Thirteenth EuroSys Conference (EuroSys '18), Article 30, 1-15, 2018.