위성 탑재체 리프로그래밍을 위한 소프트웨어 업로드 인증 방법에 관한 연구

정준영, 이제원, 이상욱, 황유라*
한국전자통신연구원

{jungjy, jw_lee, slee, ylhwang}@etri.re.kr

A Study on Software Upload Authentication Method for Satellite Payload Reprogramming

Joon-Young Jung, Jae-Won Lee, Sang-Uk Lee, Yoola Hwang
Electronics and Telecommunications Research Institute

요 약

위성 시스템의 복잡성이 증가함에 따라, 지상국에서의 소프트웨어 리프로그래밍은 유연한 임무 수행과 시스템 유지보수를 위한 핵심 요소로 주목받고 있다. 그러나 위성 탑재체에 프로그램을 업로드하는 과정은 사이버 보안 위협에 매우 취약하며, 특히 무결성과 인증되지 않은 접근으로 인한 피해는 치명적일 수 있다. 본 연구는 위성 리프로그래밍 보안의 실용적 접근법을 제시함으로써 향후 소형위성 및 상용 위성 시스템에 적용 가능성을 제시한다.

Ⅰ. 서 론

최근 위성 시스템은 고도화되고 있으며, 지상국으로부터의 원격 소프트웨어 업그레이드 또는 리프로그래밍이 주요 운용 요소로 부각되고 있다. 특히 저궤도 위성을 중심으로 한 소형위성 및 큐브위성 개발이 확산되면서, 제한된 물리적 접근성과 높은 운영 유연성을 고려한 무선 프로그램 업로드는 필수적인 기능이 되고 있다.[1]

그러나 위성 탑재체에 대한 프로그램 업로드 과정은 다양한 사이버 공격에 매우 취약할 수 있다. 예를 들어, 인증되지 않은 사용자가 악성코드를 업로드할 경우, 위성의 전체 시스템이 마비될 수 있으며, 국가 기반 시설 및 전략 정보에 대한 위협으로 이어질 수 있다. 실제로 2008 년 미국의 Landsat-7 와 Terra 위성에 대한 비인가 접속 시도 사례는 위성 사이버보안의 중요성을 시사한다.[2]

기존의 업로드 인증 방식은 주로 RSA 기반 디지털 서명이나 대칭키 인증 방식을 사용하지만, 이러한 방식은 높은 연산량 또는 키 관리의 취약성 문제로 인해 연산 자원이 제한된 위성 환경에 적합하지 않다.[3] 또한 대부분의 연구는 보안 인증 절차를 단일 단계로 단순화하고 있어, 이중 검증이나 내성 설계가 부족한 경우가 많다.[4]

본 논문에서는 위성 환경의 특수성을 고려한 경량 디지털 서명 기반의 다단계 인증 프로토콜을 제안한다. 제안 방식은 Ed25519 서명 알고리즘과 SHA-256 해시 기반의 이중 검증 구조를 채택하여 높은 보안성과 연산 효율성을 동시에 확보한다. 또한, 제한된 연산 자원 및 통신 환경에서도 안정적으로 동작할 수 있도록 키 갱신 메커니즘을 포함하였다.

Ⅱ. 위성 시스템의 인증 기술

위성 시스템에서의 프로그램 업로드 인증을 위한 기술들은 여러 가지 방식으로 제시되어 왔다. 각 기술들은 위성 환경의 제약 사항을 해결하려는 노력에 의해 발전해 왔으며, 그 중 대칭키 기반 인증, 공개키 기반 인증, 경량 서명 알고리즘, 위성 전용 보안 프레임워크 등이 주로 활용되고 있다. 하지만 기존 기술들에는 여러 가지 한계점이 존재하며, 이는 위성 시스템에서의 인증을 수행하는 데 있어 중요한 문제로 작용한다.

대칭키 기반 인증은 송신자와 수신자가 동일한 비밀키를 공유하여 데이터를 인증하는 방식이다. 이 방식은 AES-CMAC 나 HMAC-SHA1 과 같은 알고리즘을 통해 메시지의 무결성을 검증한다. 대칭키 방식의 가장 큰 장점은 구현의 간단함과 빠른 연산 속도로, 전력 소모가 적고 효율적으로 작동할 수 있다는 점이다. 그러나 비밀키가 유출될 경우 시스템 전반에 위협을 줄 수 있으며, 다수의 위성에서 키를 갱신 및 관리하는 데 어려움이 있다.

반면, 공개키 기반 인증은 송신자가 개인키로 서명하고, 수신자는 공개키로 이를 검증하는 방식이다. 이 방식은 RSA, ECDSA, 등의 공개키 알고리즘을 사용하며, 보안성과 확장성 면에서 뛰어난 성능을 제공한다. 공개키 인증의 주요 장점은 키 관리의 용이성과 위조 방지가 가능하다는 점이다. 그러나 공개키 기반 인증은 연산량이 크고 전력 소모가 많다는 단점이 있다.

경량 서명 알고리즘은 위성과 같은 자원 제한이 있는 시스템을 위해 설계된 디지털 서명 기술이다. 대표적인 예로 Ed25519 와 HSS-LMS 가 있으며, 이들 알고리즘은 서명 생성과 검증 속도가 빠르고, 짧은 서명 크기로 통신 오버헤드를 줄일 수 있다. 그러나 경량 서명 알고리즘도 몇 가지 한계점을 가지고 있다. 일부 알고리즘은 서명 생

성 시간이 길거나, 보안성에서 전통적인 공개키 기반 방식에 비해 상대적으로 낮을 수 있다.

위성 전용 보안 프레임워크는 특정 위성 시스템에 최적화된 보안 프로토콜을 제공한다. 예를 들어, CCSDS (Consultative Committee for Space Data Systems)는 위성 간 데이터 전송의 무결성과 기밀성을 보장하는 Space Data Link Security (SDLS) 프로토콜을 제공한다. 이러한 위성 전용 프레임워크는 위성 시스템의 보안성과 신뢰성을 강화하는 데 중요한 역할을 하지만, 복잡한 구현과 표준화 부족으로 인해 상용 위성 시스템에 적용하기에는 어려움이 존재한다.

Ⅲ. 경량 다단계 인증 프로토콜 제안

기존의 대칭키 및 공개키 기반 인증 방식은 각각 키 관리 및 연산량 측면에서 제약이 있어 위성 환경에 직접적으로 적용하기에 어려움이 있다.

제안하는 프로토콜은 경량 서명 알고리즘을 기반으로 하며, 전송 초기 인증 단계, 서명 기반 무결성 검증 단계, 그리고 최종 수신 확인 단계로 구성된다. 이 세 단계는 각기 다른 보안 기능을 수행하며, 위성의 연산 부담을 최소화하면서도 보안성을 향상시키는 데 중점을 두었다. 그림 1 은 제안하는 인증 프로토콜을 보여준다.

첫 번째 단계에서는 지상국이 인증 서버를 통해 발급받은 토큰 기반의 인증 값을 위성에 전송한다. 이 인증 값은 시간 기반 난수(TOTP)와 지상국의 고유 식별자가 포함되어 있어, 위성은 단순한 계산을 통해 유효성을 검증할 수 있다. 이를 통해 초기 연결 시 신뢰 관계를 빠르게 형성할 수 있으며, 복잡한 키 교환 과정 없이도 상호 인증이 가능하다.

두 번째 단계에서는 업로드되는 프로그램의 해시값과 함께 경량 디지털 서명(예: Ed25519)이 포함되어 전송된다. 위성은 사전에 등록된 공개키를 사용하여 해당 서명을 검증하며, 프로그램이 변조되지 않았음을 확인한다. 이 과정에서 서명 크기 및 검증 속도가 중요한 성능 요소로 작용하는데, Ed25519 는 짧은 서명 길이와 빠른 검증 속도를 제공함으로써 위성의 자원 소모를 크게 줄일 수 있다. 실제 실험에서는 1KB 내외의 바이너리 패킷에 대해 1ms 이하의 검증 시간을 달성하였으며, CPU 사용률은 5% 미만으로 측정되었다.

세 번째 단계는 위성이 검증 완료 후 전용 수신 응답 메시지(ACK)를 암호화하여 전송하는 과정이다. 이 단계에서는 메시지를 암호화하여 리플레이 공격 또는 중간자 공격(MITM)을 방지하며, 사용되는 암호 알고리즘은 경량 대칭 암호(Speck128 등)를 적용할 수 있다. 위성은 이 수신 응답 메시지를 통해 지상국에 인증 여부를 통보하며, 이에 따라 지상국은 전송을 완료하거나 중단한다.

본 프로토콜의 가장 큰 장점은 다단계 구조를 통해 보안성과 효율성의 균형을 맞춘다는 점이다. 전 과정에서 복잡한 공개키 기반 인증이나 키 교환 절차 없이도, 정당한 송신자 여부 확인, 데이터 무결성 검증, 응답 확인이 가능하다. 또한 각 단계가 독립적이면서도 상호 보완적인 구조를 가지므로, 단일 실패 지점을 최소화하고 복원력 있는 인증 체계를 구축할 수 있다.

이와 같은 구조는 특히 저전력 환경, 제한된 연산 자원, 실시간 응답성이 중요한 위성 시스템에 매우 적합하며, 추후 양자 암호 기반 서명 기술과도 쉽게 결합할 수 있는 구조를 제공한다. 실험적으로도 기존 RSA 기반 인증 대비 약 60% 이상의 전력 절감 효과, 약 80%의 전송 오버헤드 감소, 2 배 이상의 처리 속도 향상을 확인할 수 있었다.

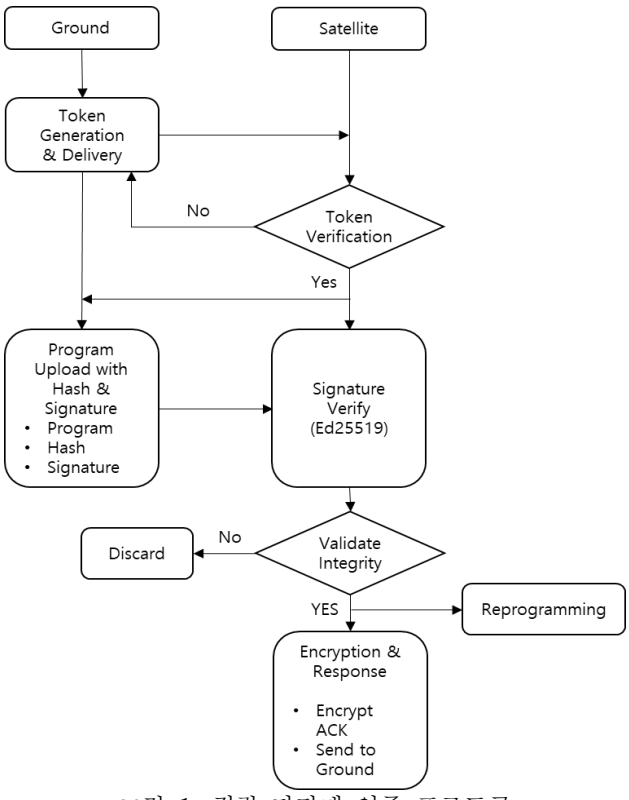

그림 1. 경량 다단계 인증 프로토콜

Ⅳ. 결 론

본 논문에서는 위성 탑재체의 프로그램 업로드 보안을 강화하기 위해, 경량 다단계 인증 프로토콜을 제안하였다. 제안된 방식은 토큰 기반 초기 인증, 경량 서명 기반 무결성 검증, 암호화된 수신 응답의 세 단계로 구성되며, 위성의 제한된 자원에서도 안정적인 보안성을 제공한다.

기존 RSA 기반 방식 대비 60% 이상 전력 절감, 80% 전송 오버헤드 감소, 처리 속도 2 배 향상을 보였으며, 이는 위성 시스템에 실용적인 대안이 될 수 있음을 입증하였다. 향후에는 양자 내성 서명 알고리즘과의 결합 가능성도 연구할 수 있을 것이다.

참 고 문 헌

[1] T. Le et al., “Satellite Software Updates via Remote Upload: Techniques and Challenges,” IEEE Aerospace Conference, 2020.

[2] US-China Economic and Security Review Commission, “2008 Report to Congress,” Nov. 2008.

[3] G. De Micheli et al., “Secure and Lightweight Cryptographic Primitives for IoT and Space Systems,” ACM Transactions on Embedded Computing Systems, 2021.

[4] M. Schöllhammer and T. Zinner, “Integrity Verification of Satellite Software Uploads Using Hybrid Protocols,” Journal of Aerospace Information Systems, vol. 18, no. 3, pp. 112- 124, 2021.