전자통신동향분석, 41권 5호 2026, 51-60

저궤도 위성통신 환경에서의 보안 위협 및 대응 기술 동향

Technology Trends in Security Threats and Countermeasures in Low Earth Orbit Satellite Communications

조성민 (S.M. Cho, smcho3315@etri.re.kr) 융합보안연구실 연구원
김영호 (Y.H. Kim, wtowto@etri.re.kr) 융합보안연구실 책임연구원
이미숙 (M.S. Lee, lms@etri.re.kr) 융합보안연구실 책임연구원
손선경 (S.G. Sohn, sgsohn@etri.re.kr) 융합보안연구실 책임연구원
이시하 (S.H. Lee, sh.lee@etri.re.kr) 융합보안연구실 학생연구원
이윤경 (Y.K. Lee, neohappy@etri.re.kr) 융합보안연구실 책임연구원/실장

ABSTRACT

Low Earth Orbit (LEO) satellite communications are central to integrated terrestrial and non-terrestrial networks. However, dynamic topologies, large constellations, open radio links, cloud-based ground systems, and commercial supply chains create security challenges that conventional terrestrial defenses do not fully address. This article reviews attack surfaces across the space, ground, user, and link segments. It examines jamming, spoofing, replay, routing manipulation, compromised terminals, software supply-chain attacks, and coordinated multi-stage attacks, and assesses layered cryptography, scalable key management, anti-jamming, resilient routing, zero-trust architecture, secure software updates, and artificial intelligence-based anomaly detection. It compares Third Generation Partnership Project and Consultative Committee for Space Data Systems standards with United States, European, and Korean guidance. The review shows that no single defense secures all segments, highlighting the need for layered, standards-aligned protection and coordinated research priorities for resilient LEO communications.

KEYWORDS CCSDS, Cybersecurity, LEO satellite communication, Non-Terrestrial Network

* DOI: https://doi.org/10.22648/ETRI.2026.J.410505
* 이 논문은 2026년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임[No. RS-2026-25523535, 저궤도위성 통신 네트워크 신뢰성 보장을 위한 보안기술 개발].

본 저작물은 공공누리 제4유형
출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.
©2026 한국전자통신연구원

I. 서론

저궤도(LEO: Low Earth Orbit) 위성통신은 지상망의 음영지역을 보완하는 수단을 넘어, 5G-Advanced와 6G의 비지상 네트워크(NTN: Non-Terrestrial Network)의 핵심 인프라로 발전하고 있다. 다수의 소형 위성, 위성 간 링크(ISL: Inter-Satellite Link), 재생형 탑재체, 지상 코어망 및 클라우드 운영 플랫폼이 결합되면서 서비스 범위와 처리 능력도 빠르게 확대되고 있다[1,2]. 이와 함께 상용 부품, 오픈소스 소프트웨어, 외부 클라우드 서비스와 일반 사용자 단말의 활용이 늘면서 저궤도 위성통신은 폐쇄형 전용 시스템에서 여러 사업자와 기술이 연결된 개방형 디지털 인프라로 변화하고 있다[3].

이러한 변화는 공격자가 노릴 수 있는 지점, 즉 저궤도 위성통신 시스템의 공격 표면을 확대시킨다. 위성 링크는 본질적으로 개방된 무선 채널이며, 저궤도 위성은 빠른 이동으로 인해 빔 전환과 핸드오버를 반복한다. 군집 규모가 수백에서 수천 기로 증가하면 식별자, 인증서, 암호 키, 소프트웨어 버전 및 보안 정책을 자동으로 관리해야 한다. 반면, 궤도상의 장비는 물리적으로 접근하기 어렵고 연산 · 전력 · 저장 공간이 제한되어, 취약점이 발견되어도 지상 장비처럼 즉시 회수하거나 교체하기 어렵다. 공격자는 지상 시스템이나 사용자 단말의 한 취약점을 비교적 적은 비용으로 공략할 수 있지만, 방어자는 위성 · 지상국 · 링크 · 단말의 전체 수명주기를 보호해야 한다는 비대칭성도 존재한다[4]. ENISA는 이러한 특성 때문에 저궤도 위성통신의 사이버 위험 노출과 사고 영향이 지상 이동통신보다 클 수 있으며, 지상망 수준을 넘어서는 보호 체계가 필요하다고 분석하였다[5].

본고에서는 저궤도 위성통신 시스템을 우주, 지상, 사용자 및 링크 부문으로 구분하여 보안 특성과 주요 위협을 살펴본다. 이어 보안 위협 대응 기술인 암호 · 인증, 항재밍, 안전한 라우팅, 제로트러스트, 공급망 보안 및 AI 기반 탐지 기술의 연구 동향을 정리하고, 3GPP 및 CCSDS와 주요국 가이드라인이 저궤도 위성통신 보안에 주는 시사점을 제시한다.

II. 저궤도 위성통신 시스템과 보안 특성

1. 시스템 구성 및 공격 가능 지점

저궤도 위성통신 시스템은 일반적으로 우주, 지상, 사용자 부문과 이들을 연결하는 통신 링크로 구성된다. 우주 부문에는 위성 본체(Bus), 통신 탑재체(Payload), 위성 탑재 컴퓨터(OBC: On-Board Computer), 자세 · 궤도 제어 장치(AOCS: Attitude and Orbit Control System) 등이 포함된다. 지상 부문은 게이트웨이, 관제 및 TT&C(Telemetry, Tracking and Command) 시설, 네트워크 운영센터, 관리 시스템 등으로 구성된다. 사용자 부문에는 고정형 · 이동형 위성 단말, 스마트폰 직접접속 단말, 선박 · 항공 · 군용 단말 및 IoT 장치가 포함된다[6]. 통신 링크에는 위성과 사용자 간 통신을 지원하는 서비스 링크, 위성-지상국 간 관제 및 제어 명령 · 데이터 전송을 위한 피더 링크, 위성 간 통신을 지원하는 ISL이 있다.

저궤도 위성은 고도 약 500~2,000km에서 지구를 초속 약 7.5km/s로 공전하며, 신호를 단순 증폭 · 중계하는 Transparent 방식과 온보드에서 신호를 복조 · 처리 · 재생성하는 Regenerative 방식으로 구분된다. Transparent 방식 위성은 수신 신호를 증폭하고 주파수를 변환하여 지상 게이트웨이로 중계하므로 대부분의 제어와 보안 기능이 지상에 집중된다. 반면, Regenerative 방식 위성은 신호를 복조 · 처리하고 기지국 또는 라우터 기능을 수행하며, 여러 위성을 거치는 다중 홉(Multi-Hop) 경로로 트래픽을 전달할 수 있다. 이 구조는 지연과 지상국 의존도를 줄

이는 장점이 있지만, 위성 내부의 운영체제, 가상화 기능, 라우팅 소프트웨어와 관리 인터페이스가 새로운 공격 대상이 된다. 특히 일부 코어망 또는 엣지 기능이 위성에 배치되면 한 위성의 침해가 단순히 링크 장애를 넘어 인증, 세션 제어 및 서비스 분리 실패로 이어질 수 있다.

지상 부문은 기존 인터넷과 기업망, 클라우드에 연결되므로 계정 탈취, 랜섬웨어, 원격접속 취약점과 같은 일반적인 IT 공격에 노출된다. 우주 부문과 지상 부문을 연결하는 통신 링크 부문은 도청(Eavesdropping), 재밍(Jamming), 스푸핑(Spoofing)과 재전송 공격의 영향을 받을 수 있다. 특히 ISL은 광학 또는 RF 방식으로 위성 간 직접 데이터 중계를 가능하게 하며, 지상국 의존도를 낮추는 동시에 침해된 위성이 다른 위성으로 악성 트래픽이나 잘못된 경로 정보를 확산시키는 통로가 될 수 있다.

2. 저궤도 환경의 보안 특성

첫 번째 특성은 동적 토폴로지이다. 위성과 단말의 상대 위치가 지속적으로 변하므로 서비스 링크, 피더 링크 및 ISL 경로가 빈번하게 재구성된다. 이 과정에서 핸드오버 정보와 라우팅 상태가 변조되면 서비스 단절이나 비정상 경로 우회가 발생할 수 있다.

두 번째 특성은 대규모 군집 위성군과 운용 자동화이다. 수천 기의 위성을 수작업으로 관리할 수 없어 중앙 관제, 소프트웨어 배포, 인증서 발급 및 정책 설정이 중앙 관리 시스템에 의존하며, 관리 계층의 단일 취약점이 군집 전체로 전파될 가능성이 크다.

세 번째 특성은 제한된 유지보수성과 자원 제약이다. 위성은 장기간 운용되고 지상 장비와 달리 현장 수리가 불가능하다. 보안 패치의 검증 실패나 업데이트 중 장애는 임무 손실로 이어질 수 있으므로 안전한 부팅, 서명된 업데이트, 복구용 이중 이미지와 안전 모드가 요구된다.

표 1 저궤도 위성통신 특성과 보안 요구사항

저궤도 특성	보안 영향 및 핵심 요구사항
동적 토폴로지	• 빈번한 핸드오버와 경로 변경으로 인증 지연, 라우팅 변조 위험 증가 • 상태정보 무결성, 빠른 재인증, 경로 검증 필요
대규모 군집	• 식별자, 암호화 키, 정책, 패치의 자동 관리가 필수 • 중앙 관리 침해와 일괄 업데이트 실패의 파급 효과 최소화 필요
개방 무선 링크	• 도청, 재밍, 스푸핑, 재전송 및 트래픽 분석에 노출 • 암호화, 인증, 항재밍, 간섭원 추적 필요
궤도상 유지보수	• 현장 수리와 물리적 격리가 곤란 • 보안 부팅, 원격 검증, 안전한 업데이트, 복구 이미지 및 점진적 배포 필요
다기관 공급망	• 위성, 지상국, 클라우드, 단말 간 보안 수준이 상이 • 제로트러스트, SBOM(Software Bill of Materials), 계약 기반 통제 및 인터페이스 보안 필요

네 번째 특성은 다기관 공급망이다. 위성체, 탑재체, 발사 서비스, 지상국, 클라우드, 단말 및 통신 서비스가 서로 다른 기관과 국가에 의해 제공될 수 있어 신뢰 경계와 보안 책임을 명확히 정의하기 어렵다[7,8]. 표 1은 저궤도 위성통신 특성별 해당하는 보안 영향 및 핵심 보안 요구사항을 보여준다.

유럽 사이버보안청(ENISA: European Union Agency for Cybersecurity)은 이러한 특성 때문에 저궤도 위성통신 시스템에는 지상망 위협뿐만 아니라 우주 부문 특유의 위협까지 함께 고려한 맞춤형 보안 접근이 필요하다고 지적하였다. 그 대응 사례로는 유럽 우주국(ESA: European Space Agency)의 SPACE-SHIELD를 들 수 있다[9].

III. 저궤도 위성통신 보안 위협 동향

1. 주요 보안 위협

1.1 무선 및 물리 계층 위협

대표적인 무선 위협으로는 도청, 재밍, 스푸핑 및 재전송 공격이 있다. 암호화가 적용되지 않

거나 잘못 구성된 다운링크에서는 사용자 데이터뿐만 아니라 접속 시간, 빔 운용 정보 및 트래픽 패턴이 노출될 수 있다. 재밍은 정상 신호보다 강한 간섭 신호를 주입하여 서비스 링크나 TT&C 링크의 가용성을 저하시킨다. 스푸핑은 위조된 GNSS 신호, 접속 신호 또는 원격명령(TC: Telecommand)을 전송하여 단말이나 위성의 판단을 교란하는 공격으로, 재전송 방지(Anti-Replay) 기능이 없는 경우 과거에 수집한 정상 명령을 다시 보내 위험한 동작을 반복시킬 수 있다[10].

저궤도 위성은 빠르게 이동하고 빔을 자주 전환하므로 간섭의 위치와 영향 시간이 계속 달라진다. 공격자가 공개 궤도 정보와 빔 패턴을 이용하면 특정 위성이 보이는 짧은 시간대에 맞춰 간헐적인 재밍을 수행할 수도 있다. 광 ISL은 좁은 빔을 사용해 도청 가능성이 낮지만, 광학 단말의 정밀 조준 및 추적 정보 교란 혹은 광학 센서를 포화시키는 위협을 고려해야 한다. 채널 특성을 활용하는 물리 계층 보안 기술은 도청 가능성을 낮추는 보조 수단이며, 암호 기반 인증과 키 관리를 대체하지는 못한다.

1.2 네트워크 및 제어평면 위협

Regenerative 위성군에서는 각 위성이 라우터나 기지국 역할을 수행하므로 라우팅 경로 조작, 악성 경로 삽입, 패킷 삭제와 선택적 전달 공격이 가능하다. 공격자가 위성 한 기의 라우팅 소프트웨어를 장악하면 정상 위성으로 위장하여 트래픽을 감청하거나 지연시키고, 위험 지역을 우회하도록 설정된 경로를 의도적으로 통과시킬 수 있다. 동적 토폴로지에서는 정상적인 경로 변화와 공격에 의한 변화가 유사하게 보이므로 단순 임곗값만으로는 탐지와 원인 분석이 어렵다.

소프트웨어 정의 네트워크와 중앙집중형 군집 관리는 운용 효율을 높이지만, 컨트롤러 및 정책 저장소가 공격자가 우선 노릴 핵심 표적이 된다. 컨트롤러 대상 서비스 거부 공격, 잘못된 경로 규칙 삽입 또는 인증되지 않은 관리 API 호출은 광범위한 서비스 장애를 유발할 수 있다. 저장 및 전달(S&F: Store and Forward) 통신에서는 메시지가 위성에 일정 시간 보관되므로 저장 중 기밀성 · 무결성, 유효 기간, 재전송 방지 및 최종 수신자 검증이 추가로 요구된다.

1.3 지상·사용자·공급망 위협

실제 침입 경로는 궤도상의 위성보다 접근하기 쉬운 지상망이나 사용자 단말일 가능성이 높다. 게이트웨이와 관제센터는 인터넷, 기업망, 클라우드 및 협력기관망에 연결되므로 계정 탈취, 랜섬웨어, 웹 취약점, 원격 접속 오용 및 내부자 위협에 노출된다. 지상 관리 시스템이 침해되면 원격명령 생성, 위성 소프트웨어 배포, 키 관리 및 가입자 데이터가 함께 영향받을 수 있다. 사용자 단말에서는 하드코딩된 비밀번호, 불필요하게 열린 관리 포트, 취약한 부트로더(Bootloader) 및 변조 가능한 펌웨어가 주요 위험요소이다[5,8].

뉴스페이스 환경에서는 개발 도구, 오픈소스 라이브러리, FPGA 비트스트림, 상용 부품 펌웨어, 클라우드 서비스와 여러 협력업체가 단일 공급망을 이룬다. 공격자는 보안이 약한 조직이나 업데이트 서버를 먼저 침해해 악성코드를 전체 위성군으로 확산시킬 수 있다. 따라서 구성품 출처와 버전, 빌드 환경, 서명 키 및 배포 이력을 임무 수명주기 전체에서 추적하고, 소프트웨어 자재명세서(SBOM)를 활용해 영향 범위를 신속히 확인해야 한다[3,4].

1.4 복합 공격과 프라이버시 위협

저궤도 위성통신 공격은 단일 기법보다 여러 부문을 연계한 공격 과정으로 나타날 수 있다. 예를 들어, 지상 운영자의 계정을 탈취한 뒤 관리 API를 악

용하고, 변조된 업데이트를 단말 또는 위성에 배포하여 장기적인 접근 권한을 확보한 다음, 라우팅을 조작하거나 서비스를 마비시킬 수 있다. 공개 궤도 정보, 단말 접속 시간, 빔 전환 및 트래픽량을 결합하면 특정 조직의 위치와 활동을 추정할 수도 있다. 따라서 보안 목표에는 기밀성 · 무결성 · 가용성뿐만 아니라 임무 안전, 서비스 연속성, 위치 프라이버시 및 공급망 신뢰까지 포함해야 한다[11].

또한, 우주 환경에 따른 장비 오류나 운용자의 설정 실수는 공격과 비슷한 현상을 만들 수 있다. 원인 규명이 늦어지면 정상 위성을 불필요하게 격리하거나, 반대로 공격을 단순 고장으로 오인할 수 있다. 대응 체계는 위성 상태정보와 통신 로그, 명령 이력, 지상 시스템의 보안 이벤트를 시간 기준으로 연계하고, 사고 정보를 사업자와 관계기관이 공유할 수 있도록 설계할 필요가 있다[3,4].

2. 저궤도 위성 대상 주요 공격 사례

2022년 Black Hat USA에서는 약 25달러 부품으로 제작된 모드칩을 이용하여 Starlink 단말에 전압 오류를 주입하여 보안 부팅 절차를 우회하고 관리자 권한을 획득하는 공격이 시연되었다[12]. SpaceX는 이후 UART 디버그 인터페이스를 비활성화함으로써 대응하였다. 해당 사례는 위성 링크의 암호화가 안전하더라도 사용자 단말의 하드웨어 신뢰점과 디버그 인터페이스가 취약하면 전체 서비스의 신뢰가 무너질 수 있음을 보여준다. 특히 이미 배포된 단말의 하드웨어 결함은 소프트웨어 패치만으로 완전히 해결하기 어렵기 때문에 설계 단계의 위협 분석과 물리적 변조 방지가 중요하다. 또한, 러우전쟁에서는 Viasat 네트워크 운용센터의 잘못 구성된 VPN 어플라이언스를 통해 신뢰 관리망이 침투되었다. SentinelLabs의 분석 및 Viasat 확인에 따르면 우크라이나 내 수천 대와 유럽 전역 수만 대의 모뎀이 영향받았으며, Viasat은 복구를 위해 약 30,000대의 신규 모뎀을 배포하였다[13].

2023년에는 ESA의 저궤도 실험 나노 위성인 OPS-SAT을 대상으로 취약한 운영 인터페이스와 탑재 소프트웨어를 악용해 위치 정보, 자세제어와 카메라 기능에 접근하는 공격이 시연되었다[14]. 이는 위성에 소프트웨어를 원격으로 올리고 임무 기능을 재구성하는 능력이 운용 유연성을 높이는 동시에, 코드 서명, 권한 분리, 업데이트 검증이 미흡할 경우 직접적인 공격 경로가 될 수 있음을 보여준다. 같은 해 Hack-A-Sat에서는 저궤도 큐브샛 Moonlighter를 실제 궤도상 보안시험 플랫폼으로 활용하였다[15]. 이러한 시험은 실제 위성을 무분별하게 공격하자는 것이 아니라, 격리된 시험 자산에서 취약점과 대응 절차를 반복 검증할 수 있는 환경이 필요하다는 점을 보여준다. 국내에서도 소형위성 실증을 연계하여 보안 기능이 통신 지연, 전력과 임무 안전에 미치는 영향까지 평가할 필요가 있다.

IV. 보안 대응 기술 및 연구 동향

1. 계층형 암호화·인증 및 키 관리

저궤도 위성통신은 단일 계층의 암호화에만 의존하기보다 링크, 네트워크, 전송 및 응용 계층의 보안 기능을 조합하는 계층형 보안 기술이 바람직하다. 3GPP 기반 NTN에서는 5G-AKA(Authentication and Key Agreement) 또는 EAP-AKA(Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement) 기반 가입자 상호인증이 기본이 되며, 지상 백홀에는 IPsec과 같은 네트워크 보호 기술을 적용할 수 있다[16]. CCSDS SDLS(Space Data Link Security Protocol)는 TM, TC, AOS 및 USLP 프레

임에 인증, 무결성, 재전송 방지 및 선택적 기밀성을 제공한다[17,18]. 중요 명령과 임무 데이터는 응용 계층 서명이나 종단 간 암호화를 추가하여 중간 노드가 침해되더라도 내용이 보호되도록 해야 한다[19,20].

대규모 위성군에서는 키를 안전하게 생성 · 주입 · 갱신 · 폐기하고 침해된 장치를 신속히 제외하는 절차가 핵심이다. 여러 위성이 같은 장기 키를 공유하면 한 기의 침해가 전체 군집에 영향을 줄 수 있으므로 장치별 하드웨어 기반 신뢰점과 계층형 키 구조가 필요하다. 지상 연결이 끊긴 상황에서는 짧은 수명의 인증서, 사전에 배포한 비상 키와 오프라인으로 검증할 수 있는 권한 정보를 조합할 수 있다. 키 갱신과 폐기 절차는 위성 핸드오버와 독립적으로 동작하고, 단말-위성-게이트웨이 사이에서 신뢰가 어떻게 이어지는지 명확히 검증해야 한다.

장기 운용 위성은 양자컴퓨터 등장 이전에 발사되어 이후까지 운용될 수 있으므로 암호 민첩성(Crypto-Agility)이 중요하다. NIST는 2024년 ML-KEM[21], ML-DSA[22] 및 SLH-DSA[23]를 양자내성암호 표준으로 제정하였다. 위성 환경에서는 공개키와 서명 크기, 인증 지연, 메모리 사용량 및 방사선 내성 구현 비용을 함께 고려해야 하므로 기존 알고리즘과 양자내성 알고리즘을 병행하는 하이브리드 방식부터 단계적으로 적용하는 것이 현실적이다.

2. 항재밍 및 물리계층 보안

재밍 대응에는 주파수 도약, 확산대역, 적응형 부호화 · 변조, 송신전력 조절 및 간섭원 위치추정 기술을 함께 사용한다. 특정 링크가 방해받을 때 다른 위성, 게이트웨이 또는 궤도 경로로 우회하면 한 지역의 재밍이 군집 전체 장애로 확산되는 것을 줄일 수 있다. 다만, 우회 경로는 혼잡과 지연을 증가시킬 수 있으므로 보안 위험과 서비스 품질을 함께 고려해야 한다.

물리계층 보안 연구는 위성과 단말이 관측하는 채널 차이를 이용한 비밀 키 생성, 인공 잡음(AN: Artificial Noise), 방향성 빔포밍 및 도청 확률 분석으로 확장되고 있다. 최근 저궤도 위성 기반 IoT 연구에서는 합법 위성과 잠재적 도청 위성이 혼재하는 환경에서 인공 잡음과 빔 제어의 효과를 분석하였다[24]. 이러한 기술은 도청 위험을 낮추는 보조수단으로 활용하되, 인증된 암호 프로토콜과 결합해야 한다.

3. 안전한 라우팅과 분산 제어

군집 라우팅은 단순히 가장 짧은 경로만 선택하지 않고 노드의 보안 상태, 경로가 통과하는 관할지역, 링크 품질 및 임무 중요도를 함께 고려해야 한다. 패킷에 경로 정보를 안전하게 기록하거나 중계 노드가 전달 사실을 증명하도록 하면 실제 전달 경로가 정책을 지켰는지 확인할 수 있다. Gu 등은 동적으로 중계 위성을 선택하면서 저궤도 라우터의 암호 연산 부담을 줄이는 경량 경로 검증 방법을 제시하였다[25]. 실제 적용을 위해서는 경로 증명 메시지 자체의 위조 방지, 위성 시간 동기 및 토폴로지 변화에 따른 오탐 제어가 필요하다.

컨트롤러와 게이트웨이를 분산 배치하고 중요 트래픽을 우선 처리하며 장애 영역을 논리적으로 분리하면 서비스 복원력을 높일 수 있다. 침해가 의심되는 위성은 군집에서 즉시 완전 제거하기보다 단계적으로 권한을 줄이고 제한된 안전 명령만 받아들이도록 격리할 수 있다. 저장-전달 서비스에는 메시지별 유효기간, 발신자 서명, 중복 식별자 및 저장 데이터 암호화를 적용해 과거 메시지가 무제한 재생되지 않도록 해야 한다.

4. 제로트러스트와 공급망 보안

제로트러스트는 위성, 게이트웨이, 운영자와 단말을 네트워크 위치나 소유기관만으로 신뢰하지 않고, 신원 · 장치 상태 · 임무 역할 · 시간과 위험도를 바탕으로 접근 권한을 계속 확인하는 원칙이다. 위성 내부에서도 통신 탑재체, 플랫폼 제어, 관리 기능과 임무 소프트웨어를 분리하고, 구성요소 간 호출을 인증하여 한 기능의 침해가 전체 시스템으로 확산되지 않도록 해야 한다.

설계 단계에서 적용할 기술로는 하드웨어 기반 신뢰점, 부팅 과정의 무결성 측정, 원격 상태 검증, 서명된 펌웨어, 이전 취약 버전으로의 되돌림 방지, 복구용 이중 이미지, 디버그 포트 잠금과 감사로그 보호가 있다. 업데이트는 먼저 소수 위성에 적용해 이상 유무를 확인한 뒤 전체 군집으로 확대하는 단계적 배포가 바람직하다. NASA의 우주 보안 모범사례는 임무 수명주기 전반의 소프트웨어 보증, 다중요소 인증, 코드 저장소 접근통제 및 공급망 제한을 강조한다[26]. 공급망에서는 SBOM, 재현 가능한 빌드, 코드와 펌웨어 서명, 외부 개발환경 접근통제와 공급 업체별 보안 책임을 계약에 반영해야 한다.

5. AI 기반 탐지와 보안 검증

대규모 군집에서는 RF 스펙트럼, 패킷 흐름, 라우팅 상태, 위성 상태정보 및 사용자 행위를 동시에 분석해야 하므로 AI 기반 이상탐지가 유용하다. 위성 탑재용 경량 모델은 지상 연결이 끊긴 상황에서도 비정상 명령, 센서 간 불일치 및 트래픽 급증을 탐지할 수 있다. 여러 게이트웨이나 위성이 원시 데이터를 직접 공유하지 않고 탐지 모델을 공동 학습하는 연합학습도 민감정보 보호 측면에서 연구되고 있다. 소프트웨어 정의 저궤도 네트워크의 성능 예측

표 2 주요 위협과 대응 기술의 연계

주요 위협	대응 기술
재밍·스푸핑·재전송	적응형 빔/주파수, 간섭원 추적, 상호인증, 시각·순서번호 기반 재전송 방지, 다중경로 우회
명령·업데이트 변조	종단 간 전자서명, 보안 부팅, 원격 상태 검증, 서명 이미지, 이전 버전 복귀 방지, 단계적 배포
라우팅 조작·노드 침해	경로 검증, 노드 상태 평가, 다중경로, 컨트롤러 분산, 의심 위성의 단계적 격리
DDoS·자원 고갈	입력 검증, 속도 제한, 서비스 분리, 우선순위 큐, 분산 게이트웨이와 이상탐지
단말·지상망 침해	다중요소 인증, 제로트러스트, 네트워크 분리, 키 보호와 보안 업데이트
공급망·공통 취약점	SBOM, 공급자 보증, 재현 빌드, 코드서명, 소수 위성 선적용 후 단계적 확대

값과 실제 측정값의 차이를 이용해 알려지지 않은 공격을 탐지한 연구도 보고되었다[27].

다만, 실제 위성 공격 데이터가 적고 정상 동작도 궤도, 트래픽 및 소프트웨어 버전에 따라 달라져 오탐이 발생하기 쉽다. 공격자가 입력 데이터를 조작해 탐지 모델을 속이는 문제도 고려해야 한다. 따라서 AI의 판단은 규칙 기반 점검, 설명 가능한 근거와 운영자 승인 절차와 결합하고, 디지털 트윈과 하드웨어-인-더-루프 시험에서 반복 검증해야 한다. 평가 지표도 탐지 정확도뿐만 아니라 탐지 지연, 전력 소모, 링크 오버헤드 및 임무 영향까지 포함해야 한다. 표 2는 위성통신 환경에서의 주요 위협 및 그에 대한 대응 기술을 보여준다.

V. 표준화 및 정책 동향

1. 3GPP NTN 보안 표준화

3GPP Release 17은 NR-NTN과 IoT-NTN을 규격화하면서 기존 5G 보안 구조를 위성 접속으로 확장하였다. 가입자 인증, NAS · AS 보안, 로밍 및 코어망 보호는 지상 5G의 기본 절차를 활용하지만, 긴 지연과 불연속 커버리지, 위성 위치정보 및 서비스

가용성 정보의 신뢰성이 추가 검토 대상이 되었다. Release 18의 TR 33.700-28은 불연속 위성 커버리지를 지원하는 구조에서 단말 보호와 보안 · 프라이버시 문제, 위성 커버리지 가용성 정보의 신뢰 문제를 분석하였다[28].

Release 19의 TR 33.700-29는 재생형 탑재체, 저장-전달 서비스 및 위성을 통한 단말 간 통신 등 5G 위성 접속 Phase 3의 보안 문제를 다룬다[29]. 핵심 쟁점은 지상 코어망에 즉시 연결되지 않는 상황에서의 인증과 권한 확인, 위성 내부 기능 간 신뢰, 저장 메시지 보호 및 로컬 통신 권한이다. Release 20의 TR 33.700-30은 Phase 4 구조의 추가 보안 문제를 연구하고 있어, 향후 다중 위성 환경의 신뢰 연계와 대규모 키 관리가 더욱 구체화할 것으로 보인다[30].

2. CCSDS 보안 표준

CCSDS 355.0-B-2 SDLS는 TM, TC, AOS와 USLP 데이터 링크 프레임에 인증 · 무결성, 재전송 방지와 선택적 기밀성을 제공한다[17]. 355.1-B-1은 키와 보안연관(SA: Security Association)의 관리 및 상태 감시 절차를 보완한다[18]. CCSDS 352.0-B-2는 권고 암호 알고리즘과 운용 방식을 제시하고[19], 356.0-B-1은 IP 기반 임무를 위한 IPsec 적용 방식을 제공한다[31]. 또한, CCSDS는 352.0-B-2의 개정 작업을 통해 최신 알고리즘, 경량 암호 및 양자내성 전환을 검토하고 있다.

CCSDS 표준은 TT&C와 임무 데이터 보호에 적합하지만 5G 코어망, 클라우드 관리 API, 가입자 프라이버시와 상용 단말 생태계를 모두 포괄하지는 않는다. 따라서 3GPP와 CCSDS 보안을 경쟁 관계로 보기보다 적용 구간이 다른 보완체계로 설계해야 한다. 예를 들어, 3GPP는 사용자 접속과 코어망 보안을, CCSDS는 위성 제어와 우주 데이터링크를 보호하고, 양쪽의 키 수명주기와 사고 대응 정책이 서로 연결되도록 해야 한다.

3. 주요국 가이드라인 및 국내 동향

NIST IR 8270은 상용 위성운영에 사이버보안 프레임워크를 적용하는 방법을 제시하며[32], IR 8401은 위성 명령 · 제어를 포함한 지상 부문의 보안에 초점을 둔다[7]. IR 8441은 여러 기관이 소유한 위성, 탑재체, 지상망이 결합한 하이브리드 위성망의 인터페이스 위험을 다룬다[8]. 미국의 우주정책지침-5(SPD-5: Space Policy Directive-5)는 위험 기반 설계, 소유자와 운영자의 통합 보안계획, 정보공유와 임무 특성을 고려한 균형 있는 통제를 강조한다. NASA와 CISA 지침도 설계부터 폐기까지의 수명주기 보안, 소프트웨어 공급망, 강한 인증, 네트워크 분리, 사고대응을 공통으로 요구한다[26,33].

ENISA의 2024년 LEO SATCOM 사이버보안 평가는 사용자 · 지상제어 · 우주 부문의 악의적 위협뿐만 아니라 장비 고장과 구성 오류 같은 비악의적 요인도 함께 다루며, 저궤도 위성통신에 맞춘 보안 요구사항과 전문인력, 정보공유의 필요성을 제시한다[5]. 2025년 Space Threat Landscape에서는 상용 위성의 수명주기와 위협 분류를 확장하였다. ETSI TR 103 958은 중요 인프라 복원력 관점에서 3GPP 위성 보안 연구를 포함한 관련 표준을 정리하였다[34]. 일본은 민간 우주시스템 사이버보안 가이드라인을 통해 민간 사업자가 설계 · 조달 · 운용 단계에서 확인할 기본 조치를 정리하였다[3]. 이러한 흐름은 상용 저궤도 위성망의 보안이 개별 암호 기술만으로 해결되지 않고, 공급망 · 운영절차 · 민관 협력까지 포함하는 위험관리 문제임을 보여준다[3,4].

국내에서는 KISA와 한국항공우주연구원이 2024년 우주항공 보안모델 개발 · 검증, 기업 · 제품 보

표 3 주요 표준 및 가이드라인의 적용 범위

표준 및 가이드	주요 범위 및 최근 동향
3GPP Rel-18~20	불연속 커버리지, 재생형 탑재체, 저장-전달, 위성 단말 간 통신과 확장 구조의 보안·프라이버시
CCSDS 350/352/355/356	우주 데이터링크 보안, 암호 알고리즘, 보안 연관 관리, IPsec 프로파일과 운용 절차
NIST IR 8270/8401/8441	상용 위성운영, 지상 명령·제어, 하이브리드 위성망 인터페이스의 위험관리
NASA·CISA·미국 SPD-5	수명주기 보안, 공급망, 통합 보안계획, 정보 공유, 강한 인증과 사고대응
ENISA·ETSI	저궤도위성 자산·위협·사고 분석, 상용 우주 위협지형, 중요 인프라 복원력 및 표준 연계
KISA·항우연	국내 우주 보안모델, 해설서·사례집, 보안모델 검증과 산업체 지원 기반 마련

안 강화 및 인력양성을 위한 협력을 시작하였다. KISA는 2025년 위성항법 · 위성통신 · 위성방송을 포함한 우주 보안모델을 공개하고, 2026년에는 해설서와 사례집을 발간하여 보안요구사항과 적용사례를 구체화하였다[35,36]. 향후에는 상용 NTN, 군통신, 위성 IoT 및 지상-위성 통합망을 대상으로 표준 간 매핑, 시험 · 인증 기준 및 침해사고 공동대응 체계를 발전시킬 필요가 있다. 표 3은 위성통신 보안에 관한 주요국의 표준 및 가이드와 그에 대한 보안 적용 범위를 보여준다.

VI. 결론

저궤도 위성통신은 지상망의 단순한 보완수단을 넘어 초공간 통신과 국가 핵심서비스를 지원하는 기반으로 발전하고 있다. 그러나 개방형 무선 링크, 동적 토폴로지, 대규모 자동화, Regenerative 탑재체, 클라우드 지상망 및 복합 공급망이 결합하면서 기존 위성 또는 지상 이동통신만을 전제로 한 보안대책으로는 충분하지 않다. 재밍과 스푸핑 같은 신호 공격뿐만 아니라 명령 · 라우팅 변조, 지상망 · 단말 침해, 공급망 공격, 위치정보 추론과 공격 원인 규명의 어려움을 함께 고려해야 한다.

대응을 위해서는 계층형 암호와 상호인증, 자동화된 키 관리, 항재밍과 다중경로 복원력, 안전한 라우팅, 제로트러스트, 설계 단계 보안, 공급망 보증 및 AI 기반 탐지를 하나의 체계로 통합해야 한다. 3GPP와 CCSDS 표준은 적용 구간에 따라 연계하고, NIST · NASA · CISA · ENISA 및 국내 우주 보안모델의 수명주기 위험관리 원칙을 운용 절차에 반영할 필요가 있다.

향후에는 암호 민첩성과 양자내성 전환, 실제 저궤도 환경을 반영한 시험 · 검증, 공통 사고데이터 및 지상-위성 통합 보안 관리를 중심으로 연구와 표준화가 진행될 것으로 전망된다.

용어해설

공격 표면(Attack Surface) 공격자가 시스템에 접근하거나 영향을 줄 수 있는 장비, 통신 경로, 소프트웨어, 계정과 관리 인터페이스의 전체 범위

암호 민첩성(Crypto-Agility) 위협과 표준의 변화에 따라 암호 알고리즘, 키 길이와 인증 방식을 안전하게 교체할 수 있는 능력

제로트러스트(Zero Trust) 네트워크 위치나 소속만으로 신뢰하지 않고 사용자와 장치의 신원·상태·권한을 지속적으로 확인하는 보안 원칙

참고문헌

[1] 신재승 외, “셀룰러 기반 저궤도 위성통신 기술 동향,” 전자통신동향분석, 제38권 제2호, 2023. 4., pp. 1-11.

[2] 최가은, 송영근, “저궤도 위성통신의 활용과 주요 사업자의 서비스 전개 현황,” 전자통신동향분석, 제39권 제3호, 2024. 6., pp. 36-47.

[3] 김다혜 외, “주요국 우주(Space) 사이버시큐리티 정책 동향 조사·분석,” KISA Insight, vol. 4, 2024. 3., pp. 1-24.

[4] 윤정현, “우주 사이버 위협의 난제와 한국의 대응 방안,” INSS 전략보고, no. 290, 2024. 11., pp. 1-23.

[5] ENISA, “Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment,” Feb. 2024.

[6] 3GPP TR 38.821, “Solutions for NR to Support Non-Terrestrial Networks (NTN),” Release 16, 2021.

[7] NIST IR 8401, “Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control,” Dec. 2022.

[8] NIST IR 8441, “Cybersecurity Framework Profile for Hybrid Satellite Networks,” Sep. 2023.

[9] ENISA, “Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment,” Feb. 2024.

[10] M. Kang et al., “A survey on satellite communication system security,” Sensors, vol. 24, no. 9, 2024, 2897.

[11] ENISA, “ENISA Space Threat Landscape 2025,” Mar. 2025.

[12] L. Wouters et al., “Glitched on Earth by Humans: A black-box security evaluation of the SpaceX Starlink user terminal,” in Proc. Black Hat USA 2022, (Las Vegas, NV, USA), Aug. 2022.

[13] J.A. Guerrero-Saade and M. van Amerongen, “AcidRain: A modem wiper rains down on Europe,” SentinelLabs, 2022.

[14] ESA, “ESA oversees in-orbit cybersecurity demonstration,” CYSAT 2023, 2023.

[15] The Aerospace Corporation, “Aerospace at DEF CON 31: Moonlighter and Hack-A-Sat 4,” Aug. 2023.

[16] 3GPP TS 33.501, “Security Architecture and Procedures for 5G System,” Release 15, 2018.

[17] CCSDS 355.0-B-2, “Space Data Link Security Protocol,” Blue Book, Issue 2, Aug. 2022.

[18] CCSDS 355.1-B-1, “Space Data Link Security Protocol—Extended Procedures,” Blue Book, Issue 1, Feb. 2020.

[19] CCSDS 352.0-B-2, “CCSDS Cryptographic Algorithms,” Blue Book, Issue 2, Aug. 2019.

[20] CCSDS 350.0-G-3, “The Application of Security to CCSDS Protocols,” Green Book, Issue 3, Mar. 2019.

[21] NIST FIPS 203, “Module-Lattice-Based Key-Encapsulation Mechanism Standard,” Aug. 2024.

[22] NIST FIPS 204, “Module-Lattice-Based Digital Signature Standard,” Aug. 2024.

[23] NIST FIPS 205, “Stateless Hash-Based Digital Signature Standard,” Aug. 2024.

[24] A. Talgat et al., “Enhancing physical-layer security in LEO satellite-enabled IoT network communications,” IEEE Internet Things J., vol. 11, no. 20, 2024, pp. 33967-33979.

[25] C. Gu et al., “STARVERI: Efficient and accurate verification for risk-avoidance routing in LEO satellite networks,” in Proc. IEEE 32nd Int. Conf. Netw. Protoc., (Charleroi, Belgium), Oct. 2024, pp. 1-11.

[26] NASA, “Space Security: Best Practices Guide,” SS BPG Rev. B, Jan. 2024.

[27] D. Agnew et al., “Detection of zero-day attacks in a software-defined LEO constellation network using enhanced network metric predictions,” IEEE Open J. Commun. Soc., vol. 5, 2024, pp. 6611-6634.

[28] 3GPP TR 33.700-28, “Study on Security Aspects of Satellite Access,” Release 18, 2023.

[29] 3GPP TR 33.700-29, “Study on Security Aspects of 5G Satellite Access in the 5G Architecture Phase 3,” Release 19, 2025.

[30] 3GPP TR 33.700-30, “Study on Security Aspects of Satellite Access in 5G Phase 4,” Release 20, work in progress, 2026.

[31] CCSDS 356.0-B-1, “Network Layer Security Adaptation Profile,” Blue Book, Issue 1, June 2018.

[32] NIST IR 8270, “Introduction to Cybersecurity for Commercial Satellite Operations,” July 2023.

[33] CISA, “Recommendations to Space System Operators for Improving Cybersecurity,” June 2024.

[34] ETSI TR 103 958 V1.1.1, “Cyber Security (CYBER): Study Implementation of the Resilience of Critical Entities Directive,” Mar. 2025.

[35] 한국인터넷진흥원, “우주 보안모델,” 2025. 2.

[36] 한국인터넷진흥원, “우주 보안모델 해설서 및 사례집,” 2026. 2.