저궤도 위성 통신 환경에서의 보안 위협 분석 및 사례 기반 대응 방안에 관한 연구

강희원*, 조가연†, 신원재*,†

*고려대학교 차세대통신학과, †고려대학교 전기전자공학부

{iamheewon811, gayeoncho, wjshin}@korea.ac.kr

A Study on the Security Vulnerabilities of LEO Satellite Communication Systems

Heewon Kang*, Gayeon Cho†, and Wonjae Shin*,†

*Department of Communications Engineering, Korea Univ.,

†School of Electrical Engineering, Korea Univ.

요 약

본 논문은 저궤도(Low Earth Orbit, LEO) 위성 통신 시스템을 위성, 지상 게이트웨이, 사용자 단말로 구성된 지상-비지상 통합 네트워크 구조로 정의하고, 해당 구조적 특성에서 기인하는 보안 위협을 분석한다. 특히 중앙 집중형 지상 인프라 의존 구조, GNSS(Global Navigation Satellite System) 기반 제어 정보의 단일 의존성, 그리고 물리적 접근이 가능한 사용자 단말의 보안 취약성을 핵심 위협 요인으로 식별하였다. 이후 각 취약점에 대응되는 사례 분석을 통해 단말과 지상 인프라 전반으로 공격 표면이 확장될 수 있음을 확인하였다. 분석 결과, 통합적인 보안 체계의 부재가 위성 통신 보안 위협의 핵심 원인으로 도출되었으며, 이에 향후 위성 통신 시스템에는 기술적 대응과 정책 및 표준 체계를 포함한 통합 보안 프레임워크가 요구된다.

Ⅰ. 서론

저궤도(Low Earth Orbit, LEO) 위성은 정지궤도(Geostationary Orbit, GEO) 및 중궤도(Medium Earth Orbit, MEO) 위성과 달리 고도 500 ~ 1,500 km의 비교적 낮은 궤도에서 운용되어 저지연성과 낮은 전파 손실이라는 이점을 제공하며, 차세대 통신 인프라의 핵심으로 자리 잡고 있다. 민간 기업 중심의 우주 산업이 급격히 발전하는 '뉴 스페이스(New Space)' 패러다임 속에서 SpaceX의 Starlink, OneWeb, Amazon의 Amazon Leo 등 대규모 LEO 위성군(Constellation) 기반 통신 서비스가 상용화되고 있다. 이에 따라 전 세계적으로 위성 통신에 대한 의존도가 급격히 증가하고 있다. LEO 위성 통신 기술은 원격지 인터넷 접속, 해양 및 항공 통신, 재난 통신, 군사 작전 지원까지 다양한 영역에서 활용되고 있으며, 특히 2022년 러시아-우크라이나 전쟁에서 Starlink가 우크라이나 군의 핵심 통신 인프라로 활용되면서 그 전략적 중요성이 입증되었다.

그러나 위성 통신의 급격한 기술 도입 속도에 비해, LEO 위성 통신 네트워크에 특화된 보안 설계와 위협 분석에 관한 논의는 상대적으로 미흡한 실정이다. 기존 지상망과 달리, LEO 위성 시스템은 고속 이동성으로 인한 동적인 네트워크 토폴로지와 높은 지상 게이트웨이 의존성을 특징으로 하며, 이는 전통적인 지상망 보안 모델과는 차별화된 위협 분석을 요구한다. 이에 본 논문에서는 LEO 위성 통신 시스템의 구조적 특성으로 인한 보안 취약성을 분석하고, 실제 보안 위협 사례를 기반으로 각 위협 영역에 대한 기술적 대응 방안을 제시하고자 한다.

Ⅱ. LEO 위성 통신 시스템의 특성과 제어 기반 보안 위협

LEO 위성 통신 시스템은 위성과 지상 게이트웨이(Gateway), 사용자 단말(User Terminal, UT)로 구성된 지상-비지상 통합 네트워크 구조를 가진다. 이러한 구조적 특성은 다음과 같은 보안 위협을 내포한다.

첫째, 지상 인프라에 의존적인 제어 구조의 취약성이다. 지상 게이트웨이는 단순 중계 지점을 넘어 무선 자원 관리와 트래픽 라우팅을 수행하는 중앙 집중형 구조로 운용된다. 이러한 구조는 다수의 위성과 사용자 단말을 효율적으로 관리할 수 있는 장점을 제공하지만, 지상 인프라에 장애나 침해가 발생할 경우 단일 실패 지점(Single Point of Failure)으로 작용하여 위성 네트워크 전반에 광범위한 서비스 중단을 초래할 수 있다.

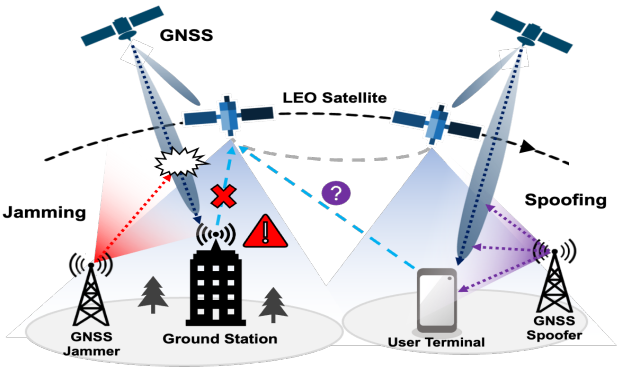

그림 1. LEO 위성 통신 시스템에 대한 GNSS 재밍 및 스푸핑 공격 개념도

둘째, GNSS(Global Navigation Satellite System) 기반 제어 정보의 의존성이다. LEO 위성은 고속 이동 특성상 잦은 핸드오버와 빔 포인팅 보정이 필수적이며, 이 과정에서 GNSS 기반의 위치 결정(Positioning), 항법(Navigation), 시각 동기화(Timing)가 핵심 인프라로 활용된다. NIST IR 8270에서는 상업용 위성 시스템 보안 위협 분류를 통해, GNSS 기반 제어 구조가 센서 데이터 및 유도/제어 시스템에 대한 의도적 재밍(jamming)과 스푸핑(spoofing) 공격에 취약함을 명시하고 있다 [1]. 이러한 공격으로 제어 신호의 무결성이 훼손될 경우, 단순한 위치 정보 상실을 넘어 링크 연결 실패와 시스템 동기화 오류로 직결될 수 있다. GNSS 재밍 공격은 GNSS 수신 주파수 대역에 고출력 간섭 신호를 송출하여 정상적인 위성 신호 수신을 방해하는 기법이다. GNSS 신호는

약 20,000 km 상공의 위성에서 송출되어 지상에 도달할 때 매우 미약해지므로, 지상에서 상대적으로 낮은 출력의 재밍 신호만으로도 쉽게 교란될 수 있다. 재밍 공격이 성공하면 수신기는 위치 및 시간 정보를 획득할 수 없게 되어 항법 기능이 마비된다. GNSS 스푸핑 공격은 재밍보다 정교한 공격 기법으로, 정상 GNSS 신호와 유사한 구조의 위조 신호를 송출하여 수신기를 기만한다. 공격자는 조작된 의사거리(Pseudorange) 정보를 포함한 위조 신호를 통해 수신기가 잘못된 위치나 시간을 계산하도록 유도한다. 이로 인해 오류가 누적되고 결과적으로 시스템 전반의 운용 안정성이 저하된다.

셋째, 사용자 단말의 물리적 노출과 공격 표면 확장이다. LEO 위성 통신 시스템에서 사용자 단말(User Terminal, UT)은 위성과 가시거리(Line of Sight, LoS) 통신을 수행하는 종단 장치로서, 네트워크 보안 경계의 최말단에 위치한다. 단말 보안이 무력화될 경우 인증 정보 노출, 통신 프로토콜 역공학, 세션 하이재킹, 악성 트래픽 주입 등 추가적인 공격 가능성이 확대된다. 특히 사용자 단말에 저장된 암호화 키나 인증 크리덴셜(Authentication Credential)이 유출될 경우, 해당 단말뿐만 아니라 연결된 네트워크 전체의 보안이 위협받을 수 있다.

Ⅲ. 보안 위협 사례 분석 및 기술적 대응 방안

2022년 발생한 Viasat KA-SAT 공격은 위성 자체가 아닌 지상 관리망과 단말 관리 프로토콜의 취약점을 악용한 대표적인 사례이다. 공격자는 잘못 설정된 VPN을 통해 관리망에 침투한 후, TR-069 프로토콜을 악용해 와이퍼(Wiper) 악성코드인 AcidRain을 배포함으로써 단말의 펌웨어 영역을 덮어쓰고 영구적인 기능 불능 상태를 유발하였다 [2]. 이러한 사례는 중앙 집중형 원격 관리 체계가 대규모 서비스 거부(Denial of Service, DoS) 공격의 경로가 될 수 있음을 시사한다. Viasat KA-SAT 사례를 통해 도출된 지상 인프라 보안 강화 방안으로는 지상 관리 인프라에 대한 접근 권한 최소화, 다중 인증(Multi-Factor Authentication, MFA) 적용, 그리고 운영망과 관리망의 물리적·논리적 분리를 통한 횡적 이동 차단 등이 있다. 또한, TR-069와 같은 원격 관리 프로토콜 사용 시 상호 인증 및 명령어 무결성 검증을 의무화하고, 대규모 설정 변경 시도에 대한 이상 징후 탐지 시스템을 도입해야 한다. 아울러, OTAR(Over-The-Air Rekeying)와 같은 무선 기반 키 관리 기술을 적용하여 암호화 키를 주기적으로 갱신함으로써, 키 탈취로 인한 추가 피해 확산을 예방할 수 있다.

2022년 2월 러시아의 우크라이나 침공 이후, 분쟁 지역에서 관측된 GNSS 재밍 및 스푸핑 사례는 위성 통신 및 유도 무기 체계의 정확도를 현저히 저하시켰다. 이는 LEO 통신의 필수 제어 요소인 PNT(Position, Navigation, and Timing) 정보의 가용성을 위협한다. 이에 대응하기 위해, GPS, GLONASS, Galileo 등 복수의 GNSS 신호를 동시에 수신하여 가용성을 확보하고, OSNMA(Open Service Navigation Message Authentication)와 같은 신호 인증 기술을 통해 스푸핑 공격을 탐지해야 한다. 또한, CRPA(Controlled Reception Pattern Antenna)와 같은 적응형 배열 안테나는 재밍 신호가 유입되는 방향으로 null을 형성하여 간섭을 효과적으로 억제할 수 있다. 이러한 안테나 기술은 군용 시스템에서 이미 활용되고 있으며, 핵심 민간 인프라에도 확대 적용이 필요하다. 더불어 GNSS 단일 의존 구조에서 벗어나 관성항법시스템(Inertial Navigation System, INS) 등 비위성 기반의 대체 PNT와의 센서 융합을 통해, GNSS 교란 상황에서도 제어 안정성을 유지할 구조가 필요하다.

2022년 Black Hat USA 컨퍼런스에서 KU Leuven 대학의 연구원 Wouters는 SpaceX Starlink 사용자 단말기를 대상으로 한 전압 결함 주입(Voltage Glitching) 기반의 물리적 공격을 통해, 단말의 부트 로더 검증 단계를 우회하고 임의 코드를 실행이 가능함을 실증하였다 [3]. 공격자는 SoC(System-on-Chip)의 전압 강하를 유도하여 서명 검증 로직을 무력화하고 루트 권한을 획득하였으며, 이는 물리적 접근이 가능한 단말이 네트워크 전반에 대한 추가적인 공격 경로로 악용될 수 있음을 입증하였다. 지상 단말 보안성을 강화하기 위한 방안으로는 먼저 하드웨어 기반 보안 부팅(Secure Boot) 강화를 고려할 수 있다. 이를 위해 SoC 내 변조가 불가능한 하드웨어 신뢰점을 기반으로 부팅 전 단계의 무결성을 검증하고, 결함 주입 시도를 하드웨어적으로 탐지해 시스템을 락다운(lockdown)하는 보호 회로를 설계해야 한다. 더 나아가, 보안 요소를 활용하여 암호화 키 등 민감 정보는 물리적 복제가 방지된 별도의 보안 칩에 저장하여 추출을 방지해야 한다. 마지막으로, 네트워크 접속 시 단말의 하드웨어 및 소프트웨어 상태를 암호학적으로 검증하여, 변조된 단말의 네트워크 접근을 원천 차단해야 한다.

Ⅳ. 결론

본 논문에서는 LEO 위성 통신 시스템을 위성, 지상 게이트웨이, 사용자 단말로 구성된 지상-비지상 통합 네트워크 구조로 정의하고, 해당 구조적 특성에서 기인하는 보안 위협을 분석하였다. 각 취약점에 대응되는 실제 보안 위협 사례를 통해 도출된 핵심 취약점은 지상-단말-우주 구간을 포괄하는 통합적인 보안 체계의 부재이다. 특히 중앙 집중형 지상 관리 구조에 대한 의존, GNSS 기반 제어 정보의 단일 의존성, 그리고 물리적 접근이 가능한 사용자 단말의 보안 취약성은 상호 결합되어 공격 표면을 확장시키며, 이는 시스템 전반의 무결성 저해 및 대규모 통신 장애로 이어질 수 있다.

이에 따라 향후 6G 이동통신 환경에서 비지상 네트워크(Non-Terrestrial Network, NTN)의 핵심 요소로 활용될 LEO 위성 통신 시스템은 OSNMA, Secure Boot, OTAR 등과 같은 기술적 대응책을 도입함과 동시에, 국가적 보안 표준과 운영 가이드라인, 기간 간 협력 체계가 결합된 통합 보안 프레임워크를 바탕으로 설계·운용되어야 한다. 이러한 다각적인 보안 접근은 LEO 위성 통신 시스템의 신뢰성을 확보하고 차세대 통신 인프라의 안정적인 활용을 가능하게 할 것이다.

ACKNOWLEDGMENT

본 연구는 고려대학교 차세대통신학과 ACSESS 진리장학 프로그램의 지원을 받아 수행되었습니다.

참 고 문 헌

[1] NIST, “Introduction to Cybersecurity for Commercial Satellite Operations,” NIST Interagency Report 8270, Oct. 2020.

[2] Viasat, “KA-SAT Network Cyber Incident Overview”, Viasat Technical Report, Mar. 2022.

[3] Wouters, L., “Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal”, Black Hat USA 2022, Las Vegas, NV, Aug. 2022.