인공위성 RF 신호 생성 통한 오픈소스 지상국 시스템 취약점 연구*

오경제*, 장대희**

*경희대학교 컴퓨터공학과(대학원생), **경희대학교 컴퓨터공학과

Vulnerability Analysis of Open-Source Ground Station Systems Using Artificial Satellite RF Signal Generation

Gyeong-Je Oh*, Dae-Hee Jang**

*Department of Computer Engineering, Kyung Hee University (M.S.),
**Department of Computer Engineering, Kyung Hee University

요 약

현대 사회가 뉴스페이스 시대에 접어들면서 위성과 지상국 소프트웨어 및 통신 프로토콜의 보안 중요성이 대두되고 있다. 본 논문에서는 오픈소스 지상국인 TinyGS 시스템과 LoRa 프로토콜을 분석하고, SDR 장비(USRP B210)를 활용하여 RF 위성 신호를 생성·송신하는 테스트베드를 구축하였다. 이를 바탕으로 Sniffing을 통한 패킷 도청, Spoofing 신호를 통한 악성 RF 신호 송신 취약점을 실증적으로 분석하였으며, TM/TC 프로토콜 기반 자동화된 RF Fuzzing 시스템을 구축하여 체계적인 보안 검증 방법론을 제시한다. 또한 확인된 취약점에 대한 연구 연계와 상용 지상국으로의 확장 가능성을 논의한다.

I. 서론

뉴스페이스 시대의 도래와 함께 저비용 소형 위성과 오픈소스 지상국 시스템의 활용이 빠르게 증가하고 있다. TinyGS와 같은 오픈소스 지상국 플랫폼은 낮은 비용으로 위성 신호를 수신·공유할 수 있도록 지원하지만, 이러한 개방성은 동시에 새로운 공격 표면을 제공한다. 지상국은 RF 신호 수신, 디코딩, 서버 연동, 원격 설정 및 네트워크 통신이 결합된 복합 시스템이므로, 단일 취약점이 전체 서비스 신뢰성에 영향을 미칠 수 있다.

본 논문의 기여는 다음과 같다. 첫째, TinyGS 지상국을 대상으로 RF 계층과 네트워크 계층이 결합된 복합 공격 표면을 실제 테스트베드 환경에서 종합적으로 분석하였다. 둘째, NORBI 위성 beacon 설정과 동일한 LoRa 위조 신호를 생성하여 Sniffing 및 Spoofing 취약점을 실증하였다. 셋째, TM/TC 프레임 기반 자동화 RF Fuzzing 시스템을 구축하고, MQTT Welcome 패킷 기반 크래시 탐지 방법론을 제시하였다. 넷째, 확인된 취약점의 재밍 연계 가능성, 상용 시스템으로의 확장성까지 함께 논의하였다.

II. 관련 연구

기존 위성 보안 연구는 주로 폐쇄형 시스템이나 특정 프로토콜의 구조 분석에 집중되어 왔다. 위성 통신 시스템 보안 Survey[3]와 위성 스푸핑 연구[4]에서는 저비용 SDR과 오픈소스 소프트웨어만으로 위성 시스템을 교란할 수 있음이 제시·입증되었고, LoRa 프로토콜 연구[7]에서는 Jamming, Replay 공격 가능성이

* "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 융합보안핵심인재양성사업의 연구 결과로 수행되었음" (IITP-2025-RS-2023-00266615)
* "이 논문은 2025년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임" (KRIT-CT-24-001, 국방우주보안특화연구실)

실험적으로 확인되었다. 네트워크 계층에서는 IoT MQTT 공격 모델링[5]과 GAN 기반 MQTT Fuzzing[6] 연구를 통해 보안 위협이 분석되었다. 그러나 이들 연구는 RF 계층 또는 네트워크 계층을 개별적으로 다루는 데 그치고 있으며, 오픈소스 지상국에서 두 계층이 결합된 복합 공격 표면을 실제 테스트베드에서 종합 분석하고 자동화 RF Fuzzing 체계까지 구축한 연구는 수행된 사례가 없다.

III. TinyGS 시스템 구조 및 공격 표면

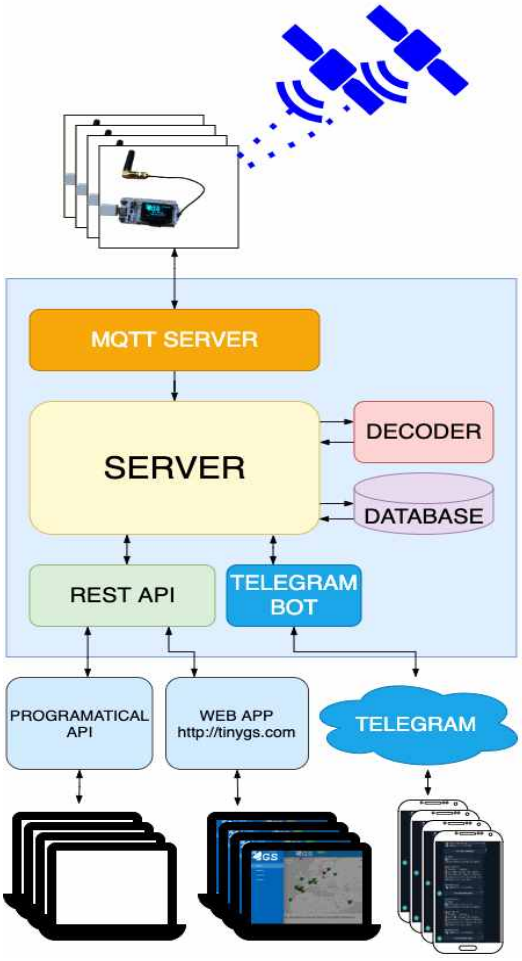

그림 1. TinyGS network architecture

TinyGS는 그림 1와 같이 서버, 브로커, ESP32 수신 보드로 구성된다[1]. 사용자는 펌웨어를 보드에 플래싱한 뒤 서버와 연동한다. 지상국은 수신 위성 목록과 파라미터를 MQTT로 전달받아 RF 신호를 수신하며, LoRa 칩으로 복조된 데이터는 MQTT를 통해 서버에 전달되어 웹사이트 및 텔레그램 채널로 공개된다.

그림 2. TinyGS Setup 모습

이러한 구조는 다양한 공격 표면을 포함한다. 초기 설정 페이지를 통한 네트워크 기반 입력 조작, MQTT 브로커 위·변조, RF 계층에서의 위조 신호 송신 가능성이 존재하므로, TinyGS는 프로토콜·펌웨어·네트워크·RF 계층을 아우르는 통합적 보안 분석이 필요하다.

IV. 테스트베드 기반 취약점 분석

4.1 테스트베드 구성

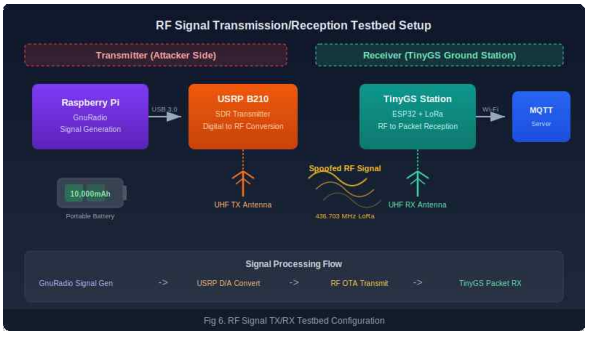

그림 3. RF 신호 송수신 테스트베드 구성도

그림 3과 같이 GnuRadio로 생성한 LoRa 디지털 신호를 USRP B210을 통해 RF 신호로 변환하고, UHF 대역 안테나를 통해 OTA 방식으로 송신하는 환경을 구축하였다[2]. 주파수 및 변조 파라미터는 기존 beacon 설정을 그대로 유지하였다. 상세 구성은 표 1과 같다.

구성 요소	세부 사항
SDR 장비	Ettus USRP B210
신호 생성	GnuRadio + Raspberry Pi
지상국 보드	Heltec WiFi LoRa 32 (ESP32)
대상 위성	NORBI (436.703 MHz)
LoRa 파라미터	SF: 8, BW: 62.5 kHz, CR: 4/6
전원	10,000 mAh 보조배터리(이동형)
안테나	UHF 대역TX/RX 안테나

표 1. 테스트베드 실험 환경 구성

4.2 Sniffing을 통한 위성 패킷 도청

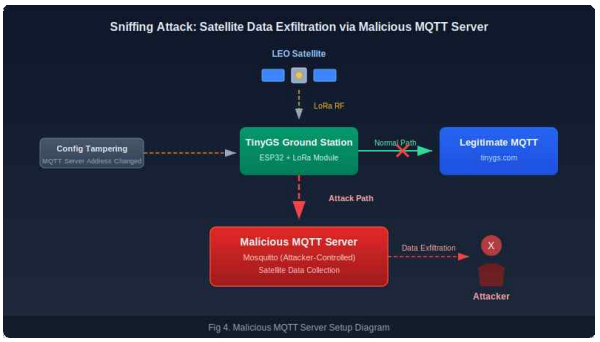

그림 4. 악성 MQTT Server 구축 개념도

TinyGS 지상국은 초기 설정 시 MQTT 서버 주소·포트·사용자명·비밀번호를 입력받아 서버와 연동된다. 공격자가 제어하는 MQTT 서버를 입력하도록 유도하면 수신된 위성 데이터가 공격자 서버로 전달될 수 있다. Mosquitto 기반 MQTT 서버를 구축하고 TinyGS 지상국 서버 설정을 변경한 결과, 위성 관련 텔레메트리가 공격자 서버로 지속 전달되는 것을 검증하였다. 해당 취약점은 초기 설정 단계 개입이 필요하지만, 한 번 설정이 변경되면 후속 RF 공격을 위한 사전 정찰 수단으로 활용될 수 있다.

4.3 Spoofing 신호를 통한 악성 RF 송신

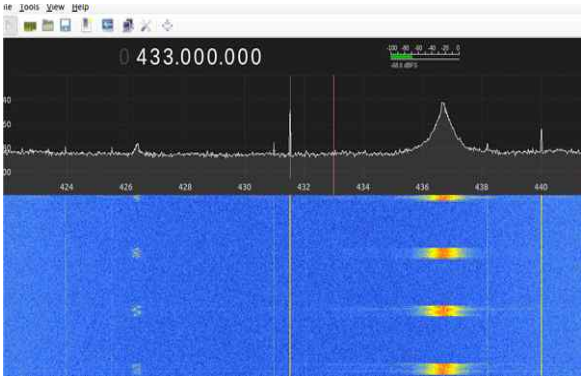

그림 5. 스푸핑 beacon 신호 Gqrx 수신 모습

TinyGS가 특정 위성 신호를 수신하는 과정에서, 동일한 주파수와 LoRa 파라미터를 갖는 위조 RF 신호를 외부에서 송신할 경우 이를 정상 패킷으로 처리하는지 분석하였다. 근거리 OTA 환경에서 30회 스푸핑 신호를 송신한 결과는 표 2와 같다.

항목	스푸핑 신호	정상 위성 신호
RSSI	-26 dBm	-120 ~ -130 dBm
SNR	11.75 dB	-5 ~ 5 dB
Freq. Error	-2841.64 Hz	+/- 5000 Hz
Packet Size	39 bytes	20 ~ 255 bytes
수신 성공률	100% (30/30)	가변적(패스 의존)
서버 정상 처리	100%	100%

표 2. 스푸핑 신호 수신 테스트 결과

스푸핑 신호의 RSSI는 -26 dBm으로 정상 위성 신호 대비 약 100 dB 이상 강하고, SNR 역시 11.75 dB로 높은 수신 품질을 보였다. 30회 전송 모두 지상국이 정상 수신하여 100% 성공률을 기록하였고, 수신된 패킷은 TinyGS 서버에서도 정상 위성 텔레메트리로 처리되었다. 이는 TinyGS가 RF 계층에서 수신 신호의 출처를 검증하지 못하여 위조 신호가 실제 위성 데이터처럼 처리될 수 있음을 실증적으로 보여준다.

4.4 RF Fuzzing 자동화 테스트베드

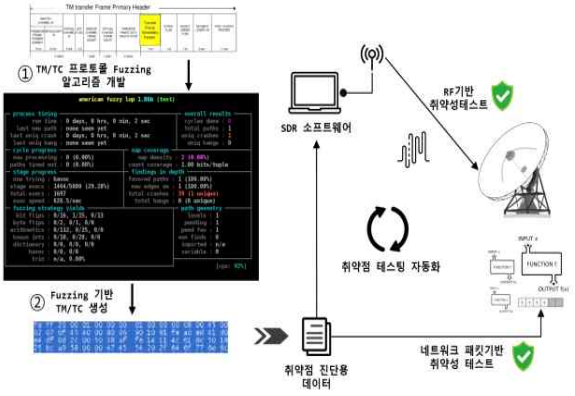

그림 6 RF Fuzzer 테스트베드 구축

앞서 확인한 취약점 분석을 체계화하기 위해 그림 6과 같이 TM/TC 프로토콜 기반 자동화 Fuzzing 시스템을 구축하였다. 기존 MQTT Fuzzing 연구[6]가 네트워크 계층에 집중한 것과 달리, 본 시스템은 RF 계층에서 악성 페이로드를 자동 생성·송신하고 지상국의 상태 변화를 관찰하는 방식으로 동작한다. 본 시스템의 세부 방법론은 다음 세 단계로 구성된다.

(1) 입력 생성: 정상 beacon 패킷을 seed로 사용하고, TM/TC 프레임 구조(Primary Header, Packet Data Field)에 대해 bit-flip, field-level mutation, 길이 필드 경계값(boundary value) 변이를 적용하여 악성 페이로드를 자동 생성한다.

(2) 전송: 생성된 페이로드를 GnuRadio flowgraph에서 LoRa 변조한 뒤 USRP B210을 통해 OTA로 송신한다.

(3) 모니터링 및 크래시 탐지: 지상국이 재부팅될 때마다 서버로 전송하는 Welcome MQTT 패킷을 크래시 발생 지표로 활용한다. 즉, 특정 입력 송신 직후 Welcome 패킷이 서버에 수신되면 해당 입력이 펌웨어 크래시/리부팅을 유발한 것으로 자동 기록한다.

Fuzzing 테스트 결과, 실제 지상국 펌웨어에서 비정상 동작(리부팅·행·Heap-overflow)을 유발하는 입력 패턴을 탐지하는 데 성공하였다.

V. 연구 연계 및 확장성 논의

5.1 재밍 연계 가능성

동일한 SDR 환경에서 정상 위성 패스 시간대에 협대역 재밍으로 정상 신호를 억제하고 그 자리에 스푸핑 신호를 주입하는 selective jamming-spoofing 결합 공격이 가능하며, 실제로 RSSI 기반 탐지를 회피하면서 정상 데이터를 위조 데이터로 치환하는 Spoofing 신호를 생성하여 가능성을 입증하였다.

5.2 상용 지상국으로의 확장성

본 연구의 분석 대상은 TinyGS에 국한되지만, ①RF 계층에서 수신 신호 출처를 검증하지 않는 구조, ②네트워크 기반 백엔드 공유 구조라는 두 특성은 SatNOGS 등 타 오픈소스 플랫폼뿐 아니라 TM/TC 프레임을 사용하는 상용 지상국 시스템에도 공통적으로 나타난다. 본 논문에서 제시한 RF Fuzzing 방법론과 재부팅 기반 크래시 탐지 기법은 대상 프로토콜의 프레임 구조와 동일하게 적용 가능하다. 단, 상용 시스템과의 확장성은 오픈소스 대비 낮을 수 있으며, 이는 향후 연구가 필요한 부분이다.

VI. 결론

본 논문에서는 오픈소스 지상국 TinyGS를 대상으로 Sniffing을 통한 패킷 도청과 Spoofing 신호를 통한 악성 RF 송신 취약점을 실증하였다. 또한 TM/TC 프레임 기반 자동화 RF Fuzzing 시스템과 Welcome MQTT 패킷을 활용한 크래시 탐지 방법론을 제시하였다. 또한 확인된 취약점에 대한 재밍 연계 가능성, 상용 시스템 확장성을 종합적으로 논의하였다.

향후 자동화 Fuzzing 시스템을 고도화하여 다양한 프로토콜과 지상국 플랫폼(SatNOGS, 상용 CCSDS 기반 시스템 등)으로 확장하고, selective jamming-spoofing 결합 공격을 포함한 고도 위협 시나리오에 대한 방어 연구를 이어갈 예정이다.

[참고문헌]

[1] TinyGS, "TinyGS Homepage," Available: https://tinygs.com

[2] Ettus Research, "Transmitting DVB-S2 with GNU Radio and a USRP B210," https://kb.ettus.com/

[3] M. Kim, S. Park, and W. Lee, "A Survey on Satellite Communication System Security," Sensors, vol. 24, no. 9, 2897, 2024.

[4] E. Salkield, S. K?hler, and I. Martinovic, "Satellite Spoofing from A to Z: On the Requirements of Manipulating Satellite Systems," in Proc. CCS, 2023.

[5] S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol," in Proc. IEEE iThings, 2017.

[6] Z. Wei et al., "SGANFuzz: A Deep Learning-based MQTT Fuzzing Method using Generative Adversarial Networks," IEEE Access, vol. 12, 2024.

[7] E. Arsas et al., "Exploring the Security Vulnerabilities of LoRa," in Proc. IEEE CYBCONF, 2017.