

문제정의서(연구개발계획서)

Project Name	인공위성 통신 보안 시뮬레이터
-----------------	------------------

13 조

202002561 조영민

202002546 임우진

202002493 박민서

Document Revision History

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2023/04/02	보고서 초안 작성	박민서
2	2023/04/03	1, 2, 4, 6 항목 작성	조영민
3	2023/04/04	3, 5 항목 작성	임우진
4	2023/04/05	문서 검토 및 수정	임우진

Table of Contents

1. 연구 개발의 필요성	4
2. 연구 개발의 목표 및 내용	5
3. 이해당사자 인터뷰/ 설문 인사이트	7
4. 기대 효과 및 향후 확장 가능성	8
5. 연구 개발의 추진전략 및 방법	10
6. AI 도구 활용 정보	11
7. 참고문헌(REFERENCE)	12

1. 연구 개발의 필요성

현재 위성 통신은 상업적, 국방적 측면에서 핵심 인프라로 자리잡고 있다. 상업 분야에서는 글로벌 인터넷 서비스, IoT, 드론 통신, 해상 및 원격지 통신 등 다양한 응용 분야에서 위성 통신 기술이 필수적인 요소로 작용하며, 기술 발전과 함께 그 활용 범위가 지속적으로 확장되고 있다.

기존의 위성 통신 시뮬레이터는 실제 통신환경에서 발생하는 전파지연, 도플러 효과 등 다양한 물리적 현상을 반영하지 못하는 경우가 많다. 또한 사이버 보안 측면에서도 보안 모듈 및 공격 시나리오 검증이 외부 라이브러리에 의존하는 경우가 많아 적용 측면에서 여러 어려움이 존재한다.

본 시뮬레이터는 단순한 사용자 교육을 넘어, 위성 통신 환경에 실제 사이버 공격(예: 재밍, 스푸핑, 중간자 공격 등)을 적용하고, 이에 따른 보안 검증을 수행할 수 있는 시나리오를 구현하는 데 초점을 맞추고 있다. 이를 통해 사용자들이 위성 통신 시스템의 보안 취약점을 직접 체험하고 분석할 수 있도록 하며, 실제 위성 운용 환경에서 발생할 수 있는 보안 위협에 효과적으로 대응할 수 있는 능력을 배양하는 데 기여할 것으로 기대된다.

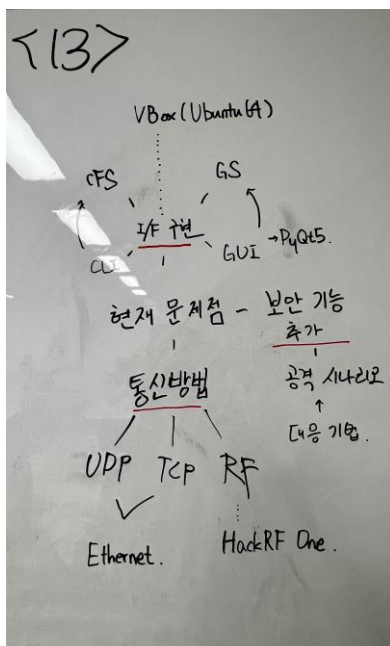
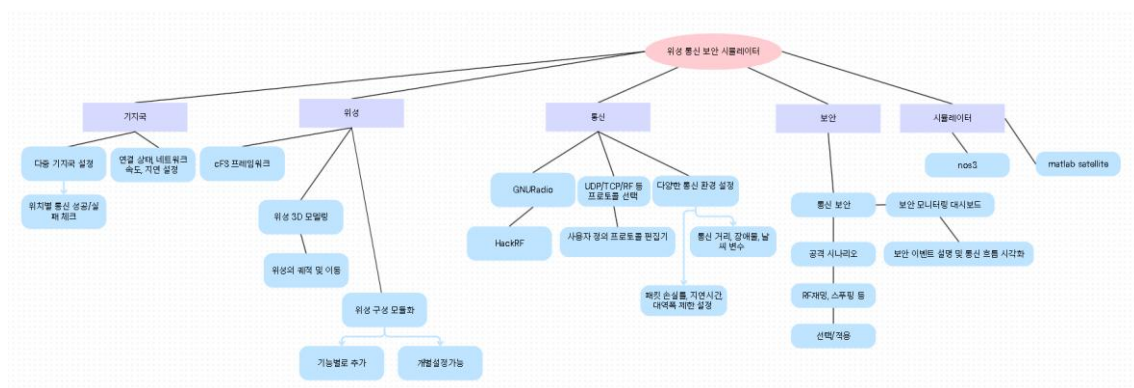
미래 먹거리로 떠오르는 위성 통신 분야에서, 본 접근은 보안 대응력 제고는 물론, 교육과 연구 전반에 걸쳐 실질적이고 지속 가능한 효과를 창출할 수 있는 핵심 기반이 될 것이라 생각한다.

2. 연구 개발의 목표 및 내용

본 프로젝트의 궁극적인 목표는 위성 통신 보안 시뮬레이터를 통해 현실 위성 통신 환경의 핵심 요소를 경량화된 방식으로 재현하고, 사이버 보안 공격 및 대응 시나리오를 구현하는 것이다.

이를 통해 사용자는 위성 통신 시스템의 보안 취약점을 직접 체험하고 분석할 수 있으며, 본 시스템은 미래 위성 통신 분야에서 필수적인 교육 및 연구 도구로 활용될 수 있을 것이다.

아래는 2차례 진행된 브레인스토밍 결과이다.



다음으로 연구개발 주요 내용은 다음과 같다:

- HackRF 기반 RF 통신 환경을 활용한 위성-지상국 시뮬레이터 구현
두 대의 HackRF 장비를 사용하여, 하나는 cFS 기반 인공위성 역할, 다른 하나는 지상국(Ground Station) 역할을 수행하게 된다. 두 장치는 Ubuntu 기반 가상머신 (VM) 환경에서 운용되며, 가상 환경은 VBox를 활용하여 구성된다.

- 현실 기반 통신 프로토콜 구현
위성과 지상국 간 통신을 위해 UDP, TCP, RF, Ethernet 등 다양한 통신 방식 실험이 가능하도록 설계한다. 이를 통해 현실에서의 다양한 물리적 조건 및 네트워크 특성을 반영할 수 있다.
- 채널 모델링
gr-leo 모듈을 활용하여 도플러 효과, 경로 손실, 대기 감쇠 등 위성 통신 환경의 주요 특성을 반영한 경량 채널 모델링을 수행한다. 이로써 시뮬레이션의 현실성을 높이고, 다양한 조건에서 통신 성능을 검증할 수 있다.
- 보안 기능 시뮬레이션 및 테스트
통신 보안 기능(암호화, 인증, 이상 탐지 등)을 구현하고, 다양한 공격 시나리오에 대한 시뮬레이션 및 대응 실험을 지원한다. 주요 공격 유형으로는 재밍, 스푸핑, 중간자 공격(MITM) 등이 있으며, 각 시나리오에 대한 대응 기법 평가도 가능하도록 설계된다.
- 통합 보안 시뮬레이션 플랫폼
기존 시뮬레이터들이 외부 보안 라이브러리에 의존하는 구조에서 벗어나, 보안 검증 및 반응 시나리오를 시뮬레이터 내부에 통합함으로써 자체 보안 실험 환경을 제공한다. 이를 통해 보다 체계적이고 반복적인 보안 테스트가 가능하다.
- 사용자 시점의 통신 흐름 시각화 기능
GUI(PyQt5) 및 CLI 기반의 이중 인터페이스를 제공하여, 사용자가 통신 흐름, 패킷 전송/응답, 오류 상태 등을 직관적으로 확인할 수 있는 시각화 기능을 지원한다. 이는 학습자와 연구자 모두에게 높은 접근성과 이해도를 제공하는 데 기여할 것이다.

3. 이해당사자 인터뷰/ 설문 인사이드

인터뷰 및 설문 계획

기간	상시
대상	관련 연구실 석사, 교수님, 테스터
목적	위성 통신 시뮬레이터의 필요성, 기존 시뮬레이터의 한계, 사용자 요구사항 파악
방법	온라인 설문조사 및 개별 인터뷰 병행
도구	Google Forms(설문조사)

주요 질문 항목

1	기존 위성 통신 시뮬레이터를 사용해보신 경험이 있으신가요? 있다면, 어떤 제품을 사용하셨나요?
2	기존 시뮬레이터 사용 시 불편했던 점이나 개선이 필요하다고 느낀 부분은 무엇인가요?
3	위성 통신 시뮬레이터에 어떤 보안 기능이 추가되기를 원하시나요?
4	시뮬레이터의 사용자 인터페이스(UI)에서 가장 중요하게 고려해야 할 요소는 무엇이라고 생각하시나요?
5	시뮬레이터를 통해 어떤 종류의 보안 공격 시나리오를 실험해보고 싶으신가요?
6	시뮬레이터가 현실적인 물리적 현상(예: 도플러 효과, 경로 손실 등)을 얼마나 정확하게 반영해야 한다고 생각하시나요?
7	추가로 시뮬레이터에 포함되었으면 하는 기능이나 개선 사항이 있으시면 자유롭게 말씀해주세요.

예상 분석 방법

- 응답 데이터 분석: 설문 및 인터뷰 응답을 수집하여 빈도 분석 및 내용 분석 실시
- 공통 주제 도출: 응답 내용에서 공통적으로 나타나는 요구사항 및 개선점을 도출
- 시각화: 키워드 클라우드, 그래프 등을 활용하여 결과를 시각적으로 표현

4. 기대 효과 및 향후 확장 가능성

위성 통신 보안 시뮬레이터를 개발함으로써, 사용자는 cFS/GS 프레임워크 기반 통신 프로토콜 구현을 통해 실제 위성 운용 환경에 적용 가능한 보안 검증 체계를 구축할 수 있으며, 이를 통해 위성 통신 시스템의 보안 취약점을 사전에 진단하고 대응 전략을 수립하는 기반을 마련할 수 있다.

본 시뮬레이터는 사용자가 직접 재밍, 스푸핑, 중간자 공격 등 다양한 사이버 공격 시나리오를 실험함으로써, 위성 통신 환경에서 발생 가능한 보안 문제에 대한 직접적 체험 및 분석이 가능하도록 설계되었다. 이는 교육 및 연구 도구로서의 실효성을 확보하는 데 중요한 역할을 한다.

또한, gr-leo 모듈을 통해 도플러 효과, 경로 손실, 대기 감쇠 등의 필수적인 물리 현상을 반영하여 실제와 유사한 채널 모델링이 가능하며, 현실성을 반영한 시뮬레이션 환경을 제공함으로써 기술적 정합성도 확보하였다.

구체적인 기대 효과는 다음과 같다:

- 보안 대응 역량 향상
 - 다양한 공격 시나리오에 대한 보안 대응 실습 및 전략 수립이 가능하여, 보안 전문가 및 연구자들의 훈련 효과를 극대화할 수 있다.
- RF 통신 실험 확장성
 - HackRF를 활용하여 다양한 주파수 대역에서의 실험을 진행할 수 있으며, 실제 위성 통신 환경에서 발생할 수 있는 다양한 조건을 반영할 수 있다.
- 교육 활용도 증가
 - GUI(PyQt5) 및 CLI를 동시에 제공함으로써 사용자 편의성과 통신 흐름 시각화가 용이하며, 이는 교육적 효과를 크게 높이는 데 기여한다.
- 향후 확장 가능성
 - 시뮬레이터는 이후 다음과 같은 방향으로의 확장이 가능하다:
 - 궤도 데이터 연동을 통한 현실적인 운용 시나리오 구성
 - 실시간 트래픽 분석 및 이상 탐지 모듈과의 통합
 - 인터페이스 플러그인 시스템 도입으로 사용자 정의 기능 강화
 - AI 기반 이상 징후 탐지 시스템과의 연계

이처럼 본 프로젝트는 기술적·교육적·보안적 측면에서 다양한 가치와 파급력을 제공할 수 있으며, 향후 위성통신 보안 기술 발전을 위한 핵심 도구로 발전할 수 있을 것이다.

5. 연구 개발의 추진전략 및 방법

주차	보고서	활동
1	디자인 개요서	프로젝트 계획 수립, 문헌 조사
2	문제점 목록	문헌 조사, 인터뷰 계획 수립
3	브레인스토밍	기술 요소 정의, 페이퍼 프로토타이핑
4	문제 정의서	GUI 프로토타이핑, 이더넷 통신 환경 구축
5	유스케이스명세서	보안 환경 분석, HackRF 학습
6		RF 통신 환경 구축
7	시퀀스 다이어그램	채널 모델링 및 통신 프로토콜 구현
8		보안 공격 시나리오 설계 및 구현
9	테스트 계획서	전체 테스트 계획 수립
10		테스트 환경 구현
11	테스트케이스 설계서	테스트케이스 설계
12		상세 테스트 환경 구현 및 시나리오 실행
13	테스트 결과 보고서	테스트 수행, 데이터 수집
14		테스트 결과 분석 및 시각화 준비
15	최종 발표 보고서	프로토타입 완성, 결과 시각화 및 발표 자료 작성
16		마무리 점검 및 제출 준비

6.AI 도구 활용 정보

사용 도구	GPT-4o, Claude 3.7 Sonnet, Perplexity
사용 목적	인터뷰 질문 초안 작성, 문장 흐름 정리, 사례 리서치 보조
프롬프트	<ul style="list-style-type: none">● 사용자 경험 중심으로 문제정의서 예시를 보여줘● 디자인 브레인스토밍 아이디어 10개 제안해줘● 관련 논문, 기사 탐색
반영 위치	<ol style="list-style-type: none">1. 인터뷰 질문 목록 (p.6)2. 아이디어 설명 문단 정리 (p.7)
수작업	있음(논리 보강, 사례 교체 등)
수정	

7. 참고문헌(Reference)

위성 통신 보안 위협 및 해결책에 대한 종합적 조사

- M. Marchese et al., "Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges," *Computer Networks*, vol. 198, 2021. [Online].
- Available: <https://www.sciencedirect.com/science/article/pii/S138912862200319X>

HackRF One의 소프트웨어 정의 라디오(SDR) 기술 활용

- N. C., "HackRF One - Software Defined Radio," *Total Cyber*, 2023. [Online].
- Available: <https://training.totalcyber.com/hackrf-one-software-defined-radio/>

gr-leo: GNU Radio 기반의 우주 채널 시뮬레이터

- Libre Space Foundation, "Gr-leo: A GNU Radio Open-Source Space Channel Simulator," *Libre Space*, 2020. [Online].
- Available: <https://libre.space/2020/07/30/gr-leo-a-gnu-radio-open-source-space-channel-simulator/>

위성 통신 네트워크 시뮬레이션에 대한 연구

- Y. Wang et al., "Research on Simulation of Satellite Communication Networks," *Proceedings of the 2023 International Conference on Communications, Computing, and Networking*, 2023. [Online].
- Available: <https://dl.acm.org/doi/10.1145/3654446.3654492>

위성 해킹 워크숍: HackRF와 GNU Radio를 활용한 고급 기법 탐구

- Tonex, "Workshop on Hacking a Satellite with HackRF and GNU Radio: Exploring Link Budget and Advanced Techniques," *Tonex Training*, [Online].
- Available: <https://www.tonex.com/training-courses/workshop-on-hacking-a-satellite-with-hackrf-and-gnu-radio-exploring-link-budget-and-advanced-techniques/>

위성 소프트웨어 분석

- The Core Flight System github
- <https://github.com/nasa/cFS>

위성 통신 시뮬레이터 분석

- NASA Operational Simulator for Small Satellites
- <https://github.com/nasa/nos3>