P R O J E C T D O C U M E N T

Usecase Specification Document

Project Name	인공위성 통신 보안 시뮬레이터

13 조

202002561 조영민
202002546 임우진
202002493 박민서

Document Revision History

Rev#	Date	Affected Section	Author
1	2023/04/19	문서 작성	임우진

Table of Contents

List of Figure

1. Introduction

1.1. Objective

이 명세서는 위성 통신 환경의 핵심 요소를 경량화된 방식으로 재현하고, 다양한 사이버 보안 공격 및 대응 시나리오를 구현하기 위한 **'인공위성 통신 보안 시뮬레이터'** 개발의 필요성과 방향성을 제시하는 데 그 목적이 있습니다.

현재 위성 통신은 상업 및 국방 분야의 핵심 인프라로 자리잡고 있으나, 기존 시뮬레이터들은 실제 통신환경의 전파지연, 도플러 효과 등 물리적 현상을 제대로 반영하지 못하고, 보안 측면에서도 외부 라이브러리에 의존하는 한계가 있습니다. 이 명세서는 HackRF 기반 RF 통신 환경과 gr-leo 모듈을 활용하여 실제 위성 통신 환경의 물리적 특성을 반영하고, 재밍, 스푸핑, 중간자 공격 등 다양한 보안 공격 시나리오를 구현하여 통합된 보안 시뮬레이션 환경을 제공하는 시스템 개발 계획을 담고 있습니다.

이를 통해 사용자들이 위성 통신 시스템의 보안 취약점을 직접 체험하고 분석할 수 있는 교육 및 연구 도구를 개발하는 것이 궁극적인 목표입니다. **명세서는 이러한 시스템의 구체적인 기능 요구사항, 개발 전략, 이해관계자 니즈, 기대효과 등을 포괄적으로 정의하고 있습니다.**

2.Usecase Diagram

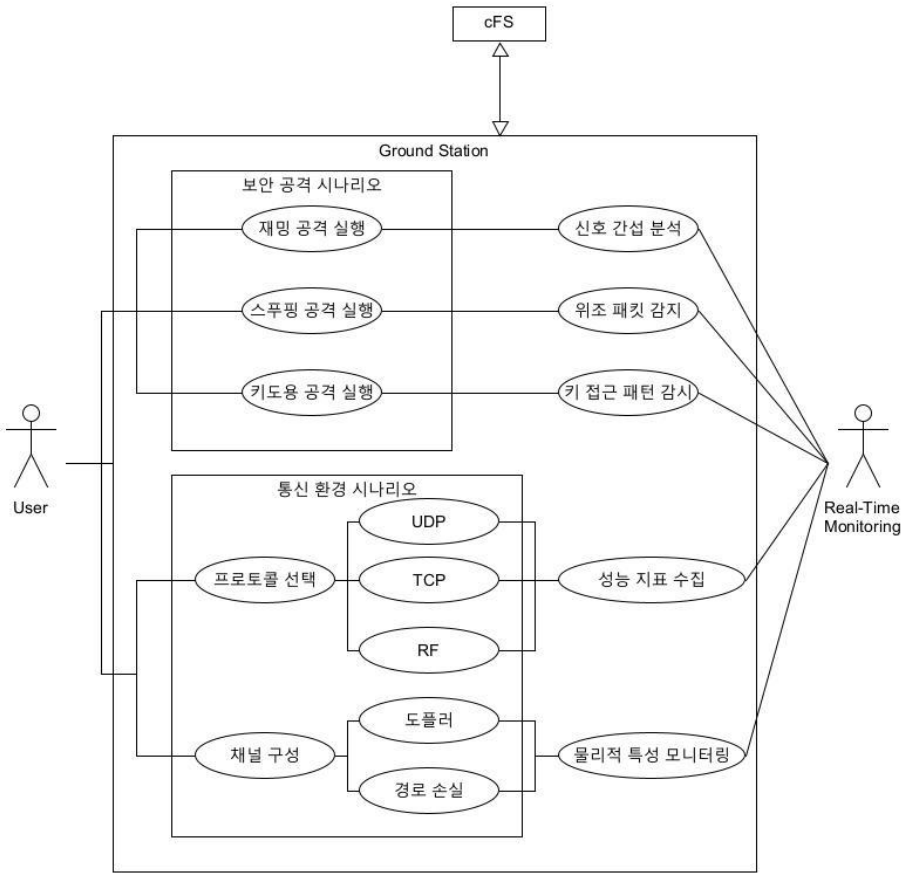

그림 1

- 재밍 공격 실행
- 스푸핑 공격 실행
- 키 도용 공격 실행
- 프로토콜 선택
- 채널 구성

모든 시나리오는 일반 사용자에 의해 실행되며, 실시간 모니터링 시스템을 통해 결과를 관찰하고 분석할 수 있습니다. 시스템의 핵심은 cFS와 지상국(Ground Station) 컴포넌트로, 이들이 시뮬레이션 환경의 기반을 제공합니다.

3. Usecase Specification

3.1 재밍 공격 실행

Usecase 이름	재밍 공격 실행
ID	SA-01
간략 설명	RF 신호 간섭을 통한 통신 차단 효과 분석
Actor	일반 사용자
Pre-Conditions	HackRF One 장비 2세트 정상 연결 상태 Ubuntu 22.04 LTS 기반 가상머신 2대 구성 완료 GNU Radio 및 gr-leo 모듈 설치 완료 기본 통신 세션 수립 확인
Main Flow	1) 사용자가 GUI에서 '재밍 공격' 옵션 선택 2) 공격 파라미터 설정 3) '공격 실행' 버튼 클릭 4) 실시간 스펙트럼 분석기 모니터링 5) 패킷 손실률 및 신호 대잡음비(SNR) 변화 기록 6) 공격 종료 후 통신 복구 시간 측정
Post-Conditions	공격 영향도 보고서 자동 생성 방어 메커니즘 효과 측정 데이터 저장
Alternative Flow	A1: 공격 실패 시 → 전력 레벨 5dBm 단위 증량 A2: 위성 측 오작동 발생 → cFS 프로세스 재시작

3.2 스푸핑 공격 실행

Usecase 이름	스푸핑 공격 실행
ID	SA-02
간략 설명	위성 신호를 위조하여 지상국 속임
Actor	일반 사용자
Pre-Conditions	cFS 텔레메트리 패킷 구조 분석 완료 기본 통신 세션 정상 작동 확인 SYNC 마커 0x1ACFFC1D 패턴 인식 가능
Main Flow	1) 사용자가 GUI에서 '스푸핑 공격' 옵션 선택 2) 위성 ID 및 위조할 명령 유형 설정 3) 위조 패킷 생성 옵션 선택 4) 신호 전력 조정 옵션 설정 5) '공격 실행' 버튼 클릭 6) 지상국 반응 모니터링 7) 명령 수락/거부 결과 기록
Post-Conditions	스푸핑 성공/실패 보고서 생성 방어 메커니즘 개선 권장 사항 도출
Alternative Flow	B1: 위조 패킷 거부 시 → 체크섬 알고리즘 자동 조정 B2: 통신 두절 발생 → 원래 신호 특성으로 복구

3.3 키 도용 공격 실행

Usecase 이름	키 도용 공격 실행
ID	SA-03
간략 설명	암호화 키 탈취를 통한 세션 장악 시나리오 실행
Actor	일반 사용자
Pre-Conditions	핸드셰이크 프로토콜 설정 완료 암호화 키 교환 세션 활성화 실시간 키 모니터링 도구 구성 완료
Main Flow	1) 사용자가 '키 도용 공격' 메뉴 선택 2) 공격 대상 키 유형 선택(세션 키/인증 키) 3) 공격 방식 선택 4) 키 유출 임계값 설정 5) '공격 실행' 버튼 클릭 6) 키 탈취 시도 과정 모니터링 7) 탐지시스템반응관찰
Post-Conditions	키 사용 패턴 분석 리포트 생성 키 라이프사이클 관리 효율성 평가 데이터 저장
Alternative Flow	C1: 키 교환 시간 초과 → 자동 키 재생성 트리거 C2: 비정상 키 접근 패턴 감지 → 보안 경고 발생

3.4 통신 프로토콜 선택

Usecase 이름	통신 프로토콜 선택
ID	COM-01
간략 설명	다양한 프로토콜 환경에서 통신 품질 평가
Actor	일반 사용자
Pre-Conditions	네트워크 스택 초기화 완료 테스트 파일 준비 프로토콜별 기준 성능 데이터 수집 완료
Main Flow	1) 사용자가 ' 통신 프로토콜' 메뉴 선택 2) 프로토콜 유형 선택(UDP/TCP/RF) 3) 패킷 크기 설정(512B-2048B) 4) 대역폭 제한 설정(1-20MHz) 5) '테스트 시작' 버튼 클릭 6) 실시간 처리량 및 지연 시간 모니터링 7) 패킷 손실률 계산 및 표시 8) 테스트 완료 후 성능 요약 리포트 생성
Post-Conditions	프로토콜별 성능 비교 차트 생성 최적 프로토콜 추천 결과 도출
Alternative Flow	D1: TCP 연결 실패 → 3-way 핸드셰이크 재시도 D2: 버퍼 오버플로우 → 윈도우 크기 자동 조정

3.5 채널 모델링

Usecase 이름	채널 모델링
ID	COM-02
간략 설명	gr-leo 모듈 활용한 도플러 효과/경로 손실 시뮬레이션
Actor	일반 사용자
Pre-Conditions	gr-leo 모듈 설치 및 구성 완료 궤도 요소 입력 완료(이심률, 경사각) 참조 안테나 이득 설정(위성, 지상국)
Main Flow	1) 사용자가 '채널 모델링' 메뉴 선택 2) 궤도 고도 설정(300-1000km) 3) 주파수 대역 선택(UHF/VHF/S-Band) 4) 시뮬레이션 시간대 설정(UTC 기준) 5) 채널 모델 활성화 (도플러 효과, 경로 손실, 대기 감쇠) 6) '시뮬레이션 실행' 버튼 클릭 7) 실시간 신호 강도 히트맵 관찰 8) 주파수 편이 값 모니터링
Post-Conditions	채널 특성 검증 리포트 출력 궤도별 통신 품질 예측 데이터 생성
Alternative Flow	E1: 모델 불일치 발생 → 자동 보정 알고리즘 실행 E2: 계산 오류 발생 → GNU Radio 플로우그래프 재컴파일

4. AI 도구 활용 정보

사용 도구	GPT-4.0, Claude 3.7 Sonnet, Perplexity
사용 목적	문장 흐름 정리, 사례 리서치 보조, 유스케이스 명세서 구조화 지원
프롬프트	● "유스케이스 명세서 템플릿과 작성 방법 제안" ● "사용자 경험 중심으로 시나리오 예시를 보여줘" ● "위성 통신 보안 시뮬레이터 관련 논문 및 기사 탐색"
반영 위치	1. 유스케이스 다이어그램 구조화 (p.6) 2. 유스케이스 명세 템플릿 적용 (p.7)
수작업 수정	• 프로젝트 특성에 맞게 용어 조정 • 기술적 정확성 검증 및 보완