
문제정의서(연구개발계획서)

Project Name	기밀연산 인공위성 시스템 적용
-----------------	------------------

11 조

202002558 조민성
201902711 신희성
201802076 김주호

지도교수: 장진수 교수님 (서명)

Document Revision History

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2023/04/03	문제정의서 양식 초안 작성	조민성, 신희성, 김주호

Table of Contents

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

List of Figure

그림 목차 항목을 찾을 수 없습니다.

1. 연구 개발의 필요성

문제점: 현재 위성통신에서 사용되는 통신링크는 보안이 취약한 부분이 있어 정보 보호 측면에서 위험이 있으므로 보안이 강화된 통신 기술이 필요함.

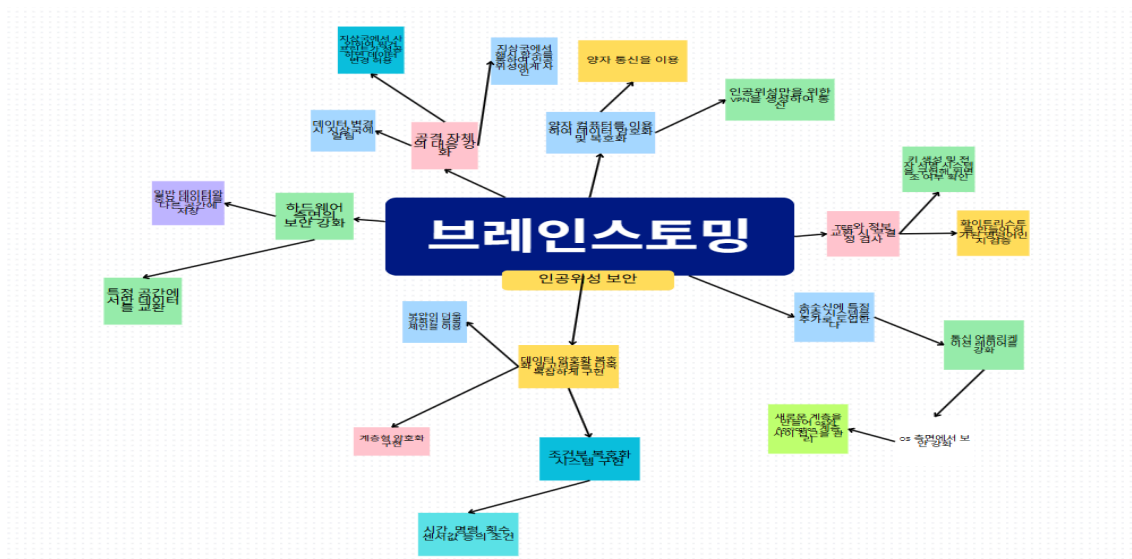
위성 통신에서 보안이 무너지면 국가의 군사 기밀 또는 기업의 중요 정보들, 사용자의 개인 정보들이 노출될 수 있으므로 위성 통신에서의 보안은 매우 중요.

2. 연구 개발의 목표 및 내용

이 프로젝트를 통해 위성 통신에서의 보안을 강화하여 사이버 보안 위협을 줄이고 좀 더 자유로운 데이터 교환을 가능하도록 함.

OP-TEE 기반 기밀연산 프로토콜을 위성 통신에 적용시켜 데이터를 좀 더 안전하게 관리할 수 있도록 함.

사용자들이 클라우드 서버에 정보를 믿고 저장함으로써 정보 활용성을 높임.



3. 이해당사자 인터뷰/ 설문 인사이드

한국항공우주연구원

질문: 인공위성 시스템에서 보안 취약점이 가장 우려되는 부분, 최근 위성 보안과 관련해 주목할 만한 위협 사례나 트렌드는?

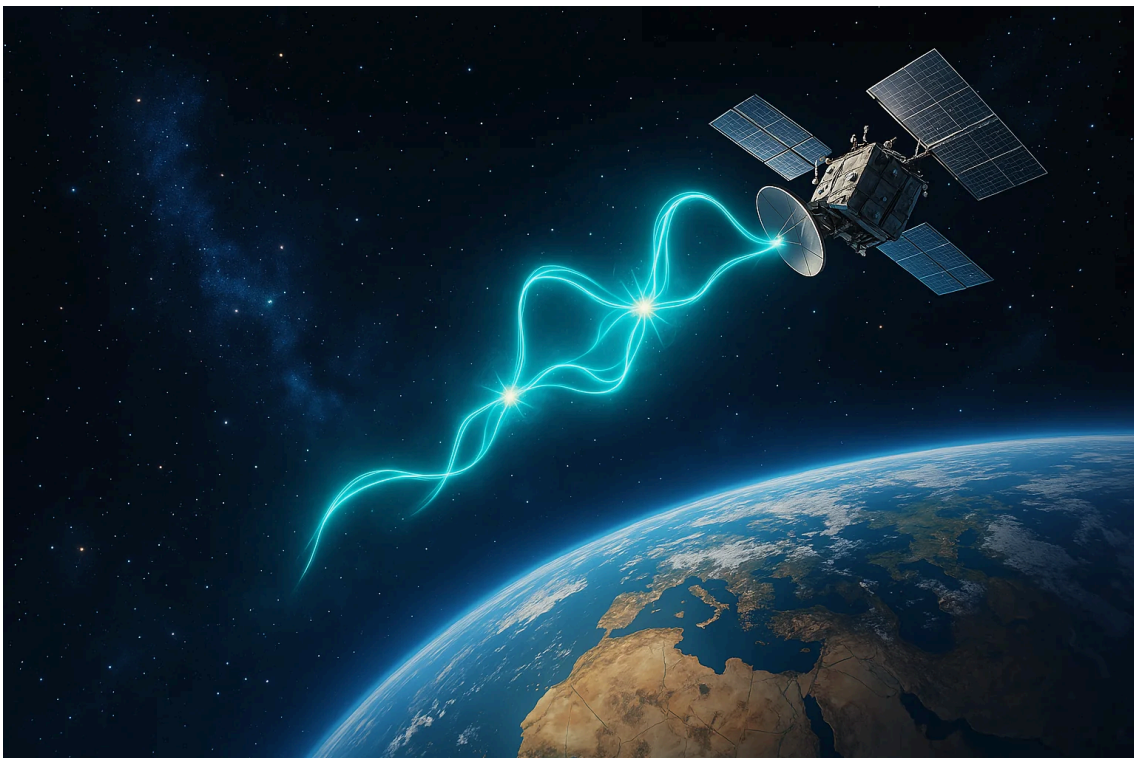
답변: 통신링크, 특히 위성제어용 업링크와 데이터 수신용 다운링크, 위성통신 보안성을 강화하기 위해 양자통신 이용.

KAIST 인공위성연구소

질문: 위성 보안과 관련된 앞으로의 주요 과제나 기술적 도전, 위성 시스템 보안을 위해 현재 가장 많이 쓰이는 기술은?

답변: 다수 통신위성으로 인터넷 서비스를 하는 위성 시스템의 보안, AES-256 같은 암호화와 표준은 CCSDS

정리 : 데이터 수신용 링크 및 제어용 링크의 보안이 가장 취약하며 고도의 암호화 기술을 필요로 하는 상태



4. 기대 효과 및 향후 확장 가능성

1. 국가 기밀 또는 군사 기밀 보안 강화
-> 국가 안보 강화로 국제적 평화 유지

- 2. 기업의 기밀을 유지
-> 기업의 영리적 피해와 사회적 혼란 감소
- 3. 개인 정보 유출 가능성 감소
-> 클라우드 사용을 통한 정보 활용성 증가

양자 컴퓨터를 개발할 경우 고도화된 암호화 알고리즘 개발로 보안 강화된 위성 통신 가능
HW 기술 개발 시 보안이 강화된 하드웨어 개발로 인공위성에 탑재 가능한 하드웨어 연구 가능

5.연구 개발의 추진전략 및 방법

- 1. OP-TEE 환경 구축
- 2. AES-256 알고리즘 학습
- 3. TEE 환경에서 키 교환 방식 연구
- 4. 인공위성 관련 연구소 인터뷰 조사 지속

6.AI 도구 활용 정보

사용 도구	GPT-4o
사용 목적	인터뷰 질문 초안 작성, 연구 개발 필요성 초안 작성
프롬프트	<ul style="list-style-type: none">인공위성의 보안과 관련되어서 할 수 있는 질문 몇 가지 알려줘인공위성 보안의 필요성에 대해 알려줘인공위성 시각화 자료 만들어줘
반영 위치	<ul style="list-style-type: none">1. 인터뷰 질문 목록 (p.6)2. 연구 개발의 필요성 (p. 5)3. 시각화 자료 (p.6)
수작업 수정	있음(질문 요구사항 교체, 개발 필요성 수정)

질문 리스트에 대한 전문가 선정을 위해 Chat GPT-4o 에 질문한 프롬프트

전문가 대상 (심층 인터뷰)

- 1.인공위성 시스템에서 보안 취약점이 가장 우려되는 부분은 어떤 영역이라고 생각하시나요? (예: 통신 링크, 지상국, 펌웨어 등)
- 2.최근 위성 보안과 관련해 주목할 만한 위협 사례나 트렌드가 있다면 어떤 것이 있을까요?
- 3.위성 시스템 보안 강화를 위해 현재 산업계에서 가장 많이 쓰이는 방법이나 기술이 있다면 무엇인가요?

4. 위성 시스템 보안을 위한 국제적 규제나 협력이 충분하다고 보시나요?
 5. 앞으로 위성 보안과 관련된 주요 과제나 기술적 도전이 있다면 어떤 부분일까요?
 6. 정부나 기업의 대응에서 보완이 필요하다고 느끼는 점이 있다면 무엇인가요?
-

해당 질문에 대해 인터뷰했을 때 적절한 대답을 해줄 수 있는 실제 기관 또는 연구자는 누가 있을까

7. 참고문헌(Reference)

- [1] 서홍석, 인공위성 시스템 암호 통신 향상을 위한 TEE 적용 방안. 충남대학교 대학원 컴퓨터공학과 네트워크 및 보안 전공, 2025.2
- [2] CSSD, “Emerging Threats to Satellite Security and Mitigation Approaches.” Center for Space Security and Diplomacy, Mar. 2024. Available: <https://cssd-ngo.org/emerging-threats-to-satellite-security-and-mitigation-approaches/>