위성 보안 및 서비스 프로토콜

송민호

유튜브 주소: https://youtu.be/eMYwQMwgyWg

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

미래 위성 보안 프로토콜

- 우주 데이터 시스템 자문위원회 CCSDS는 우주 관련 기관들(NASA, ESA 등)이 **데이터 교환과 관련된 표준**을 개발하고 채택할 수 있도록 국제적인 협력을 촉진

- CCSDS의 주요 목표는 우주 탐사와 관련된 데이터의 원활한 교환을 돕는 것
  - 다양한 데이터의 통신 프로토콜과 시스템 표준을 정의
  - 다양한 국가 및 기관 간의 상호운용성을 보장

- CCSDS의 표준은 주로 OSI 모델의 데이터 링크 계층에 중점을 두고 있음
  - 패킷에 포함된 다양한 보조 데이터(시간, 위치 정보 등)를 지원함

  - 이러한 표준화 작업은 우주 탐사 데이터의 **장기적인 보존**과 **관리**에도 기여하며 OAIS 참조 모형에서도 반영됨
    - OAIS 참조모형: 전자 기록의 장기 보존을 위한 시스템의 개념적 기능틀을 제공하는 ISO 표준

Consultative Committee
CCSDS
for Space Data Systems

https://www.3gpp.org
https://www.3gpp.org/specifications-technologies/releases/release-18

미래 위성 보안 프로토콜

- CCSDS는 위성 데이터의 안전한 전송을 위한 다양한 보안 프로토콜 정의하였으며 다음과 같은 기능을 수행함
  - **데이터 링크 계층 표준**: 위성과 지상 간 데이터를 안전하게 송수신할 수 있도록 데이터 링크 계층을 지원하여 패킷 데이터와 동기화 기능을 제공함
  - **텔레커맨드**: 지상에서 위성에 명령을 보내기 위한 프로토콜로 원격 장치와의 통신을 가능하게 함. 이는 위성의 상태 모니터링과 제어에 필수적

- SDLS(Space Data Link Security) 프로토콜
  - 위성과 지구 간 **데이터 링크에서 보안을 강화**하기 위해 설계되었음
  - 위성 데이터 전송 시 기밀성, 무결성, 인증을 제공하며 데이터의 무단 접근을 막고 데이터가 손상되거나 위조되지 않도록 함

- SDLS는 보안 표준을 일관되게 적용해 사용자가 쉽게 적용할 수 있는 형태로 구현됨
  - CYSEC의 ARCA SATLINK는 처음으로 SDLS 프로토콜을 상용화함
    - 이를 통해 **위성 보안의 새로운 표준**을 제시할 수 있음

미래 위성 보안 프로토콜

- CCSDS의 Space Packet Protocol은 SDLS 프로토콜과 연계되어 보안을 지원
  - SDLS 프로토콜은 Space Packet Protocol을 통해 전송되는 데이터의 보안성을 높임
  - 위성 데이터 통신에서 보안을 강화함

  - 위성에서 지상으로 혹은 지상에서 위성으로 전송되는 데이터를 안전하게 전송하기 위해 구조화된 방식으로 설계되어 있음

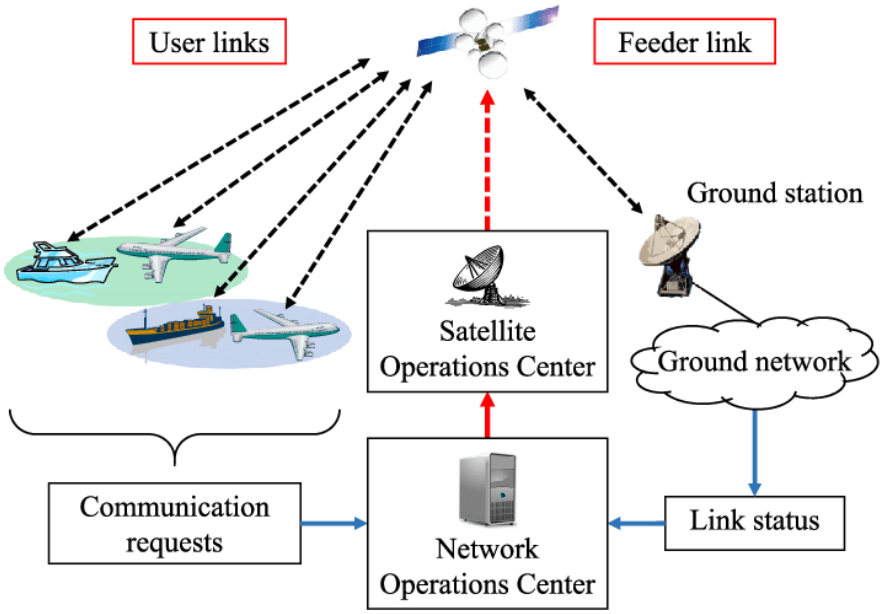
  - Space Packet Protocol 구조
    - **Primary Header**: 데이터 라우팅 정보가 포함되어 정확한 경로로 패킷을 전송. 패킷의 출처 및 목적지를 명확히 하여 인증 과정을 진행함
    - **Secondary Header**: 필요에 따라 데이터 타임스탬프나 메타데이터를 포함해 보안 검증에 유용한 추가 정보 제공
    - **Data Section**: 실질적인 데이터가 담긴 부분으로 SDLS의 암호화 기능이 적용되어 데이터 내용이 안전하게 보호됨

  Space Packet Protocol과 SDLS의 결합은 위성 데이터 통신에서 **안정성**과 **신뢰성**을 크게 높임

https://github.com/KubOS-Preservation-Group/ccsds-spacepacket
https://docs.ccsdspy.org/en/latest/user-guide/ccsds.html

SATCOM

- SATCOM(Satellite Communication)은 위성 통신을 통해 데이터, 음성, 영상 등의 정보를 전송하는 시스템
  - 위성-위성, 위성-지상, 사용자-지상 링크로 구성되어 있음
    - 각 링크는 고유한 통신 특성과 보안 요구사항을 가지고 있음
  - LEO, MEO, GEO 위성 등을 통해 네트워크 형성
    - **네트워크 확장성**, **높은 데이터 전송 속도** 등의 장점 제공
  - 무선으로 데이터를 전송하여 정보 유출, 도청, 재밍 등의 위험이 존재함
    - 이를 해결하기 위해 **다양한 보안 메커니즘** 사용
    - **AES-256**과 같은 강력한 암호 알고리즘을 적용하여 데이터의 기밀성을 보장
    - **안티 재밍** 및 **안티 스푸핑** 기술 적용
    - 전파 환경의 특성을 이용하여 데이터를 보호하기 위해 **물리 계층 보안** 적용



SATCOM 시스템의 다이어그램

https://www.sciencedirect.com/science/article/pii/S138912862200319X

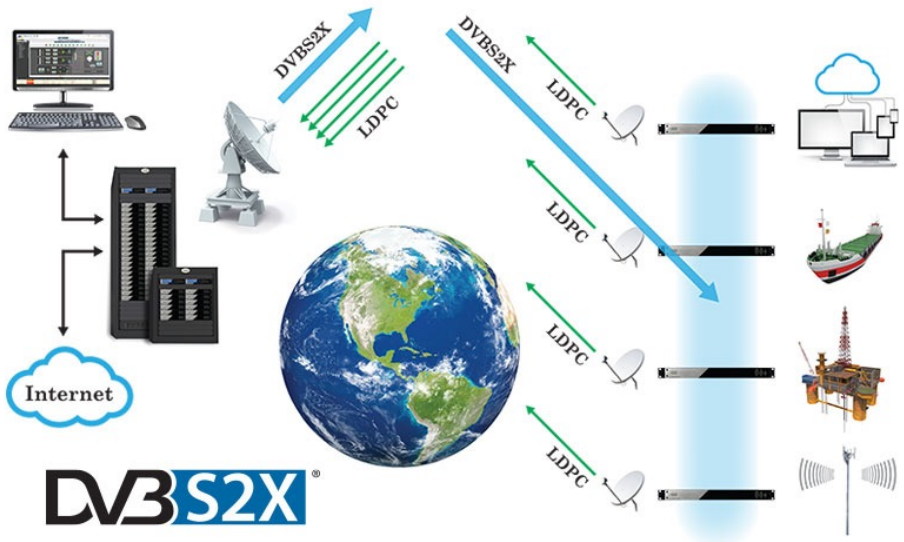
SATCOM – DVBS2X 프로토콜

- SATCOM에서 사용하는 서비스 프로토콜은 다양한 위성 기반 서비스의 신뢰성과 효율성을 향상시키기 위해 설계되어 있음

- DVB-S2X 전송 표준 프로토콜
  - 위성 통신에서 널리 사용되며 **데이터 전송 효율성**을 높이고 다양한 서비스 환경에 대응할 수 있도록 설계되어 있음
  - 새로운 변조 및 코딩 방식을 통해 높은 스펙트럼 효율성을 제공

  - **물리 계층 보안을 강화**하는데 중요한 역할을 함
    - SATCOM 링크에서 도청 및 재밍 방지와 같은 위협을 줄이는데 중점을 두고 있음
    - 암호화 기술이 더해져서 기밀성 보안을 강화하며 특정 SATCOM 링크에 대해 보다 강력한 보안을 제공함

  - 위성 방송뿐만 아니라 원거리 인터넷 연결, IoT 지원, 원격 감시 등 **다양한 상용 및 군사 목적으로 활용 가능**



DVB-S2X 네트워크의 다이어그램

SATCOM – 5G/6G 프로토콜

- SATCOM의 5G/6G 연동 프로토콜은 위성과 지상 네트워크를 통합하여 광범위한 연결성과 높은 데이터 전송 속도를 제공함
  - 5G와 6G의 초고속, 초저지연, 초연결성을 제공함
  - 위성 통신을 이용하여 다양한 지역에서도 5G 및 6G 네트워크를 활용할 수 있도록 SATCOM과의 연동이 필요함
    - 지상 통신망은 산악 지대, 해양, 항공 등 물리적으로 접근하기 **어려운 지역에서 한계**가 있기 때문
    - 5G/6G-SATCOM 연동은 IoT, 스마트 시티, 재난 관리, 항공 및 해양 통신 등 다양한 분야에서 중요한 역할을 함
  - 3GPP(3rd Generation Partnership Project)는 5G/6G와 SATCOM의 연동을 위한 표준을 정의하고 있음
    - **네트워크 아키텍처 통합**: 위성-기지국 간 통신을 위한 인터페이스와 프로토콜을 정의하여 지상과 위성 네트워크 간 원활한 통합이 가능하도록 함
    - **주파수 대역 최적화**: 위성 통신은 지상 통신과는 다른 주파수 대역을 사용하며 간섭을 최소화하기 위한 주파수 분배 및 조정이 필요함. 5G/6G의 밀리미터파와 위성의 Ku, Ka 대역 등의 주파수를 효율적으로 활용함
    - **핸드오버 지원**: 이동 중인 사용자가 위성과 지상 네트워크 사이를 원활하게 오갈 수 있도록 핸드오버를 지원함. 이를 통해 항공기, 선박 등에서의 끊김 없는 연결이 가능함

https://www.3gpp.org
https://www.3gpp.org/specifications-technologies/releases/release-18

5G와 LEO 통신을 위한 보안 프로토콜

- 5G와 저궤도 위성(LEO, Low Earth Orbit) 통신을 위한 보안 프로토콜은 지상 네트워크와 위성 네트워크 간의 안전한 데이터 전송을 보장하기 위해 설계되었음

  - 5G와 LEO 위성 간의 연동은 광범위한 연결성을 제공하는 동시에 공중에서 데이터가 전송되므로 보안 위험이 존재하기 때문에 **높은 수준의 보안이 요구됨**
    - 도청, 재밍, 스푸핑, 물리적 보안 문제 등의 위험에 노출되어있음

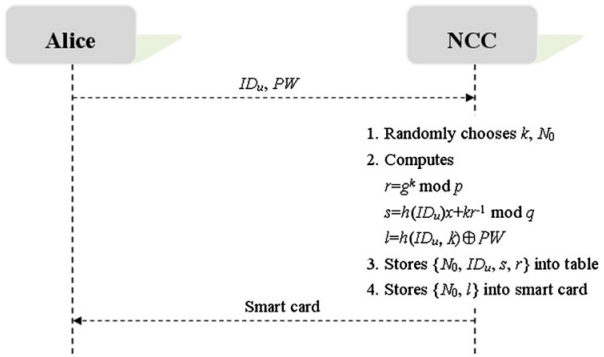
  - 5G와 LEO 위성을 연동하기 위해서는 데이터 기밀성, 무결성, 인증을 보장하는 보안 프로토콜이 필요함
    - **EAP-AKA**: 5G에서 사용자 인증을 위해 사용하는 프로토콜. LEO 위성 네트워크와 연동 시에도 사용될 수 있음. 사용자와 네트워크 간 상호 인증을 수행하며 인증 이후 키를 생성하여 데이터 전송 시 기밀성을 보장함. 이를 통해 네트워크에 접속하는 사용자가 신뢰할 수 있는지 확인하며 세션 동안 암호화 키를 생성하여 데이터의 안전한 전송을 보장함.
    - **IPsec**: IP 계층에서 데이터 암호화 및 인증을 제공하는 프로토콜로 LEO 위성과 지상 네트워크 간 데이터 전송 시 보안을 강화함. IPsec은 데이터 패킷을 암호화하고 데이터 무결성을 보장하며 네트워크를 통한 안전한 연결을 제공함.
    - **물리 계층 보안**: 위성 통신의 특성을 활용하여 물리 계층에서 보안을 제공하는 기술. 예를 들어, 신호 대 잡음비(SNR) 차이를 활용해 신호가 정당한 수신자에게만 수신되도록 함. 이러한 방식은 기존의 암호화 방식보다 경량화 되어서 위성의 제한된 자원을 절약할 수 있음.

위성 보안 프로토콜

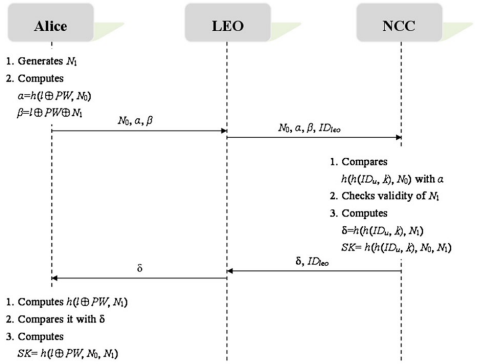
- 위성 통신에서의 인증 및 키 합의 프로토콜 연구

  - 제안된 인증 및 키 합의 프로토콜
    - **디지털 서명 방식**(ElGamal 서명)을 사용하여 불법적인 삽입 공격 방어
    - **서버와 사용자의 상호 인증**을 통해 인증된 사용자만 서비스에 접근할 수 있도록 하며 매 세션마다 **임시 ID**를 갱신해 사용자 추적을 어렵게 함
    - **세션 키**를 사용하여 통신 내용을 암호화하며 이전 및 이후 세션의 키가 독립적으로 작동하도록 해 해킹이 발생해도 다른 세션에 영향을 주지 않도록 보장함

  - 이 프로토콜은 **일회용 해시 함수**와 **비밀 키**를 사용하여 재전송 공격, 위장 공격, 스마트 카드 분실 시 보안 위협 등 다양한 공격에 대해 강한 방어력을 가짐



등록 과정



인증 과정

Chang, Chin-Chen, Ting-Fang Cheng, and Hsiao-Ling Wu. "An authentication and key agreement protocol for satellite communications." *International Journal of Communication Systems* 27.10 (2014): 1994-2006.

위성 보안 프로토콜

- ECC를 활용한 위성 통신의 인증 및 키 합의 프로토콜
  - 기존 위성 통신 보안 프로토콜은 여러 취약점이 존재하여 이러한 문제를 해결하기 위해 ECC를 사용한 3단계 인증 및 키 합의 프로토콜을 제안함

  - **3단계 인증**
    - 사용자는 스마트 카드나 모바일 장치를 통해 본인 인증을 진행
    - **무작위 난수**를 사용하여 매 세션마다 새로운 암호화 키를 생성하여 보안성을 높이고 이 과정에서 ECC를 사용하여 효율적이면서도 강력한 암호화 기능을 구현함
    - 사용자와 네트워크 제어 센터(NCC)는 각각의 신원을 확인하는 과정에서 도청자가 이를 추적하거나 역추적하여 사용자의 정보를 탈취하지 못하도록 설계되어 있음

  - 세션 키 합의
    - 사용자가 NCC와 세션 키를 합의할 때 ECC를 통해 생성된 **일회용 암호화 키**를 이용. 이는 세션 간 보안이 강화되어 이전 세션의 정보가 노출되더라도 새로운 세션에는 영향을 미치지 않도록 보장함
    - **에포크(ephmeral secret)** 보호 기능이 적용되어 일회용 암호화 키가 노출되더라도 이전이나 이후의 세션에 영향을 미치지 않게 하는 완벽한 순방향 비밀성을 보장함

기존 방식에서 부족했던 **사용자 익명성**, **데이터 무결성** 및 **재전송 공격 방어**와 같은 중요한 보안 기능들을 강화함

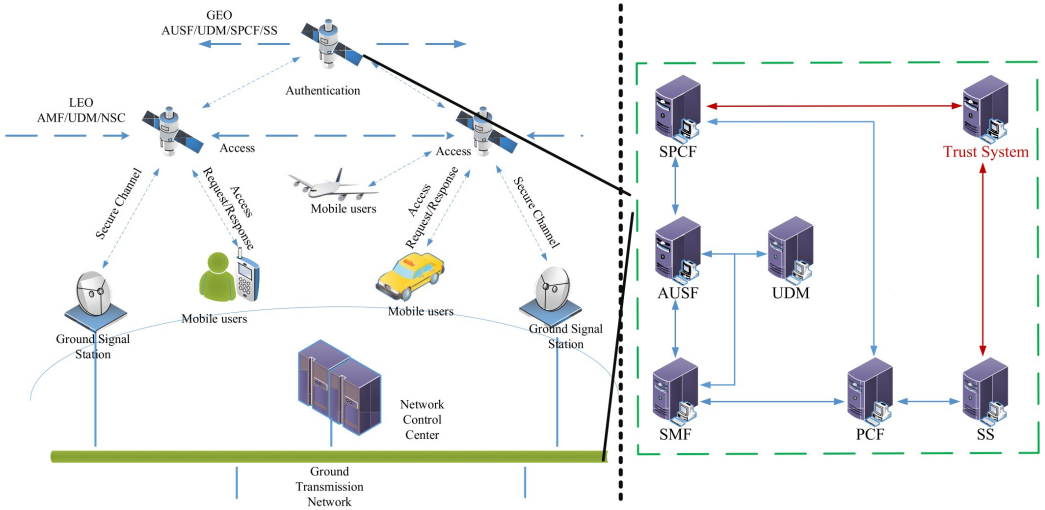
Ostad-Sharif, Arezou, Dariush Abbasinezhad-Mood, and Morteza Nikooghadam. "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications." *Computer Communications* 147 (2019): 85-97.

위성 보안 프로토콜

- 신뢰 측정 기반 위성 인터넷 자원 접근 인증 프로토콜
  - 신뢰 측정에 기반한 접근 제어 방식을 통해 위성 통신 자원을 효율적으로 관리하고 사용자에게 맞춤형 보안 정책을 제공함

  - 위성 네트워크 자원을 가상으로 나누는 **자원 슬라이싱 기술**을 통해 사용자 필요에 따라 다양한 서비스를 제공할 수 있음
    - 특정 사용자가 필요로 하는 자원을 신속하고 효율적으로 할당함
    - 슬라이싱 기술은 IoT 및 긴급 통신 등의 상황에서 중요한 역할을 하며 5G 및 6G와 같은 최신 통신 기술에 적합한 고속, 저지연, 대역폭 효율성을 제공함

  - 신뢰 기반 인증 모델
    - 사용자의 신뢰 점수를 측정하여 **신뢰 수준에 따라 적합한 보안 정책 적용**
    - 신뢰 점수는 베타 함수, 통신 바이트 변동성, 집중 경향 측정 등의 요소를 활용하여 측정함
    - 신뢰 점수가 높은 경우 더 **빠르고 효율적인 접근** 인증 프로토콜이 제공되며 낮은 신뢰 점수를 가진 사용자는 보다 **높은 보안을 제공하는 접근** 인증 프로토콜을 적용함



접근 인증 시나리오 다이어그램

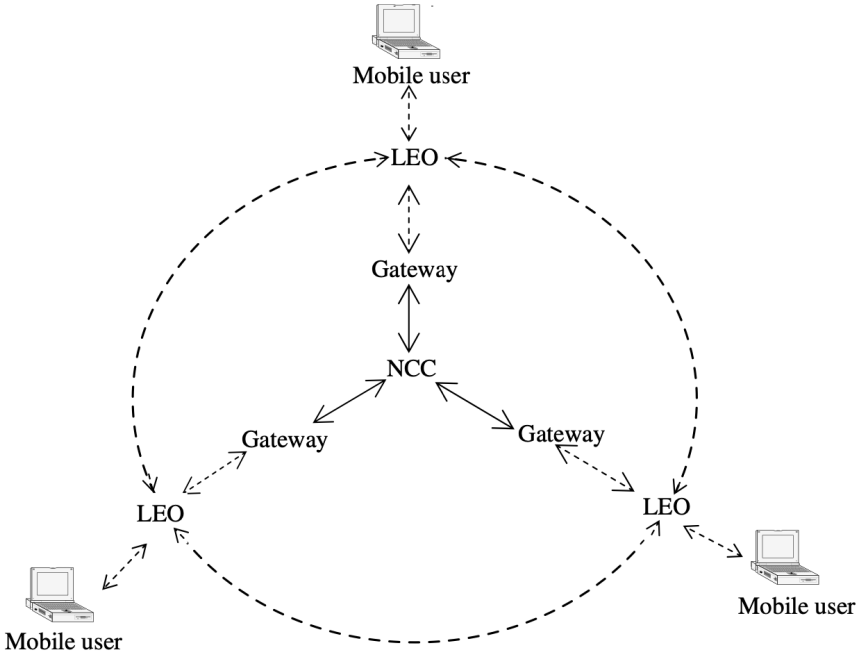
Guo, Chao, et al. "Authentication for Satellite Internet Resource Slicing Access Based on Trust Measurement." *IEEE Internet of Things Journal* (2024).

위성 보안 프로토콜

- 모바일 위성 통신 시스템에서의 사용자 인증
  - 자체 검증 메커니즘을 기반으로 한 인증 프로토콜 제안

  - **상호 인증**과 **통신 기밀성** 유지
    - 기존의 비밀키 기반 인증은 서버가 공격에 취약해지고 공개키 기반은 높은 계산 비용과 복잡한 인증 인프라(PKI) 문제를 가지고 있어 이들을 결합해 단점을 보완함

  - **자체 검증 인증 메커니즘**
    - **자체 검증** 개념을 도입하여 NCC가 생성한 서명을 모바일 사용자가 검증하고 이를 통해 **세션 키**를 상호 설정함
    - 사용자는 NCC의 공개키를 필요로 하지 않으며 서버는 사용자 신원과 관련된 정보를 서버에 명시적으로 저장하지 않아 보안이 강화됨



모바일 위성 통신망
실선: 유선보안망, 점선: 무선망

모바일 위성 통신 시스템 환경에서 **낮은 계산 비용**으로 **보안성**과 **프라이버시 보호**를 제공하며 저전력 모바일 기기에 적합하도록 설계되었음

Chen, Tzung-Her, Wei-Bin Lee, and Hsing-Bai Chen. "A self-verification authentication mechanism for mobile satellite communication systems." *Computers & Electrical Engineering*35.1 (2009): 41-48.

Q & A