논문 2025-4-17 http://dx.doi.org/10.29056/jsav.2025.12.17

에너지-인식 신뢰 기반 분산 저궤도 위성망 프록시 재암호화 경로 선택 및 보안 연구

김원빈*, 정용준**, 백상현***, 서대희****†

A study on Energy-Aware Trust-Based Proxy Re-Encryption Path Selection and Security in Distributed LEO Satellite Networks

Won-Bin Kim*, Yongjun Chung**, Sanghyun Paek***, Daehee Seo****†

요 약

저궤도(LEO, Low Earth Orbit) 위성망은 지상망을 보완하는 차세대 통신 인프라로 주목받고 있으나, 제한된 온보드 전력과 장기 운용, 위성 장악을 통한 악의적 프록시 공격 등 새로운 보안 위협에 노출되어 있다. 본 논문은 위성이 프록시 재암호화(PRE, Proxy Re-encryption) 노드로 동작하는 환경에서 이러한 제약과 위협을 동시에 고려하기 위해, 에너지-인식 신뢰 점수 기반 프록시/경로 선택 프레임워크를 제안한다. 이를 위해 위성–지상국 네트워크, 태양광 발전과 배터리 소모를 반영한 에너지 모델, 재암호화 결과에 기초한 신뢰 점수 모델을 정의하고, 각 위성의 신뢰도와 에너지 상태를 통합한 점수 및 경로 비용 함수에 기반한 프록시·경로 선택 알고리즘을 설계한다. 또한 재암호화 로그와 이상 행위 관찰값을 사용하는 신뢰 업데이트 및 블랙리스트 메커니즘을 통해 악의적·불안정 위성을 점진적으로 배제하는 구조를 제시하고, 제안 기법이 데이터 기밀성, 정당성, 가용성 요구사항을 충족하는지를 이론적으로 분석한다.

Abstract

Low Earth Orbit (LEO) satellite networks are emerging as a key complement to terrestrial infrastructures, but they face unique security challenges due to limited onboard energy, long operational lifetimes, and the risk of satellite compromise leading to malicious proxy behavior. To address these issues in scenarios where satellites act as proxy re-encryption (PRE) nodes, this paper proposes an energy-aware, trust-based PRE proxy and path selection framework. We define a system model comprising a satellite–ground topology, an energy model capturing solar generation and battery consumption, and a trust model derived from re-encryption outcomes, and design a per-satellite score and path cost function that jointly reflect trust and energy status for proxy/path selection. Furthermore, we introduce trust-update and blacklist mechanisms based on re-encryption logs and anomaly observations to gradually exclude malicious or unstable satellites, and theoretically analyze how the proposed framework satisfies confidentiality, correctness, and availability requirements.

한글키워드 : 우주보안, 저궤도 위성, 프록시 재암호화, 에너지-인식 컴퓨팅, 에너지 관리

keywords : Space Security, LEO, Proxy Re-Encryption, Energy-Aware Computing, Energy Control

* 상명대학교 융합보안연구소
** 상명대학교 자유전공학부 핀테크전공
*** 상명대학교 화학에너지 공학
**** 상명대학교 지능데이터융합학부
† 교신저자: 서대희(email: daehseo@smu.ac.kr)
접수일자: 2025.12.02. 심사완료: 2025.12.13.
게재확정: 2025.12.20.

1. 서 론

저궤도 위성(LEO, Low Earth Orbit) 위성 군집 기반 분산 위성망은 지상망이 닿지 않는 지역을 연결하고, 재난·전쟁 상황에서 백업 통신망으로 활용될 수 있어 차세대 인프라로 주목받고 있다. 그러나 높은 지연과 비트 에러율(BER, Bit Error Rate), 빠르게 변하는 토폴로지, 온보드 전력 제약, 장기간 물리적 접근의 어려움 때문에, 보안 문제가 발생하면 장기적·광범위한 피해로 이어질 수 있다.

이러한 환경에서 민감한 데이터를 안전하게 공유하기 위해, 위성이 프록시 재암호화(PRE, Proxy Re-Encryption) 노드로 동작하는 구조가 유용한 대안으로 떠오르고 있다. PRE를 이용하면 위성은 평문을 보지 않고도 수신자 A용 암호문을 수신자 B용 암호문으로 변환할 수 있어, 키 관리 부담을 줄이면서 유연한 데이터 공유가 가능하다. 하지만 일부 위성이 해킹되거나 수명 종료 후 관리가 소홀해질 경우, 잘못된 재암호화, 비인가 수신자 노출, 서비스 거부 등 공격의 발판이 될 수 있다.

문제는 PRE와 검증 절차를 강화할수록 계산·통신 오버헤드가 증가해 LEO 위성의 제한된 에너지 예산을 빠르게 소모한다는 점이다. 반대로 에너지 절약만 우선하면 검증이 줄어 악의적 프록시를 걸러내기 어렵다. 결국 각 위성의 신뢰도와 잔여 에너지를 함께 고려해 프록시 역할을 맡길 대상을 결정하는 에너지-인식 신뢰 기반 프록시 선택 기법이 필요하다.

본 연구의 구성은 다음과 같다. 2장에서는 관련 연구와 기존 접근의 한계를 분석한다. 3장에서는 시스템 모델과 보안 요구사항을 정의한다. 4장에서는 신뢰·에너지 통합 점수 기반 프록시·경로 선택, 키 위임 절차, 신뢰 점수 업데이트 및 악의적 프록시 대응을 포함한 에너지-인식 프레임워크를 제안한다. 5장에서는 보안 요구사항 충족 여부와 악의적 프록시·공모 공격 대응 능력을 분석한다. 결론에서는 기여를 요약하고 향후 연구 방향을 논의한다. 이를 통해 본 연구는 분산 LEO 위성망에서 신뢰도와 에너지 상태를 통합 반영하는 프록시·경로 선택 프레임워크를 제안하고, 악의적 프록시 존재 하의 보안성과 자원 효율 분석에 기여한다.

2. 관련 연구

2.1 분산 LEO 위성망 및 자원 관리 연구

LEO 위성망에서는 급격히 변하는 토폴로지와 제한된 무선·연산 자원을 고려한 자원 관리 및 라우팅 기법이 연구되어 왔다. Hu 등은 스펙트럼 효율, 에너지 효율, 차단율을 고려한 자원 할당 문제를 정의하고, 심층 강화학습 기반 채널·전력 공동 할당으로 자원 활용도를 향상시켰다[1]. Xiu 등은 LEO 위성과 모바일 엣지 컴퓨팅(MEC, Mobile Edge Computing)을 결합해 계산 오프로딩과 자원 할당을 공동 최적화함으로써 지연·에너지·자원 효율 개선 가능성을 보였다[2]. Di 등은 인지 - 예측 결합 보상(Awareness - Prediction Joint Compensation) 기반 동적 자원 할당을 제안해 트래픽 변화에 적응적인 자원 관리 방식을 제시하였다[3].

이들 연구는 대역폭·전력·처리 자원의 효율을 목표로 지연·혼잡·차단율 등을 지표로 삼지만, PRE 수행 노드 배치나 보안적 신뢰도, 악의적 위성을 포함한 위협 모델은 거의 고려하지 않는다.

2.2 프록시 재암호화(PRE)

프록시 재암호화(PRE, Proxy Re-Encryption)는 제3의 프록시가 평문을 알지 못한 채, 특정

송신자의 공개키로 암호화된 암호문을 다른 수신자의 공개키에 대응하는 암호문으로 변환하는 공개키 암호 기법이다. Nuñez 등은 주요 PRE scheme들을 정리하고 단·양방향성, 단일·다중사용자 지원, CCA 보안, 키 노출 저항성 등으로 비교·분석하였다[4].

Zhang 등은 클러스터형 연합학습 환경에서 조건부 PRE 기반 키 공유 메커니즘을 설계하고 효율성과 보안성을 분석하였다[5]. 국내에서도 송유진 등은 모바일 클라우드 환경에서 PRE 기반 안전한 데이터 관리 구조를 제시하였다[6].

하지만 이들 연구는 지상 클라우드·데이터 센터를 반신뢰(semi-trusted) 또는 정직하지만 호기심 많은(honest-but-curious) 프록시로 가정하는 경우가 많아, 프록시 장악에 따른 재암호화 생략·변조·오용, 신뢰도 변화의 동적 반영, 에너지 제약·위성 환경을 함께 고려한 PRE 설계는 충분히 연구되지 않았다.

2.3 신뢰 점수 기반 네트워크 보안 및 경로 선택

이동 애드혹 네트워크(MANET, Mobile Ad-Hoc Network)나 무선 센서 네트워크(WSN, Wireless Sensor Network)에서는 일부 노드의 악의적 동작으로 기존 라우팅 프로토콜이 취약해질 수 있어, 패킷 전달 이력·이웃 평가·행위 관찰로 신뢰 점수를 계산해 경로 선택과 포워딩에 반영하는 신뢰 기반 라우팅이 제안되었다. Djenouri 등은 MANET 분야의 신뢰 기반 라우팅 프로토콜을 비교·분석하였다[7]. Bai 등은 WSN에서 TSRP(Trust-Based and Energy-Aware Secure Routing Protocol)를 제안해 보안성 향상과 성능 영향을 분석하였다[8]. 다만 이들 연구는 주로 MANET/WSN/사물인터넷(IoT, Internet of Things)에 한정되며, PRE와 결합된 프록시 수행 노드 선택 문제나 고비용 암호 연산(PRE) 배분까지는 확장되지 않는다. 본 연구는 신뢰 기반 경로 선택을 프록시 노드 및 경로 선택 문제로 확장한다.

2.4 에너지-인식(energy-aware) 보안/통신 프로토콜

배터리로 구동되는 WSN·IoT 환경에서는 에너지 효율이 시스템 수명과 직결되므로, 에너지-인식(energy-aware) 라우팅·클러스터링 ·MAC 프로토콜이 핵심 연구 주제로 다루어져 왔다. Liu 등은 EAP(Energy-Aware Routing Protocol)에서 에너지 상태 기반 클러스터 헤드 선택·라우팅으로 네트워크 수명 연장을 보였고[9], 또한 S-FEAR(Secure-Fuzzy Energy Aware Routing)[10], TEAHR(Trusted Energy-Aware Hierarchical Routing)[11], Barari 등의 IoT 에너지 효율적 보안 프로토콜[12]처럼 보안 요구를 결합한 연구도 제안되었다. 다만 이들 연구는 주로 패킷 포워딩·클러스터링·MAC 계층에 초점을 두어, PRE처럼 연산 비용이 큰 암호 연산을 어떤 노드가 수행할지 에너지와 신뢰를 함께 고려해 결정하는 프레임워크는 충분히 탐구되지 않았다. 본 연구는 LEO 환경에서 이를 에너지-인식·신뢰 기반 프록시 선택 문제로 재구성해 암호 프로토콜 설계로 확장하는 것을 목표로 한다.

3. 시스템 모델

본 장에서는 제안하는 에너지-인식 신뢰 기반 프록시 선택 프레임워크의 분석을 위해 시스템 모델을 정의한다.

3.1 네트워크 모델

본 연구에서 고려하는 시스템은 다음과 같은 엔티티로 구성된 분산 LEO 위성망이다.

① **위성**($S=\{S_1,S_2,\cdots,S_N\}$): 동일/유사 궤도면에 배치된 LEO 위성으로, 위성 - 위성 링크(ISL)와 위성 - 지상국 링크로 통신한다.

② **지상국**($G=\{G_1,G_2,\cdots\}$): 데이터 소유자·서비스 운영자 역할을 수행하며, PRE 환경에서 송신자·수신자 역할을 가질 수 있다.

③ **사용자 단말**($U=\{U_1,U_2,\cdots\}$): 이동 단말·센서·지상 시스템 등으로, 지상국을 통해 키를 관리받고 위성을 통해 데이터를 수신한다.

시간 t에서 위성망의 논리적 토폴로지는 수식 (1)과 같은 그래프로 표현된다:

$$G(t)=(V,E(t)) \tag{1}$$

여기서 $V=S\cup G$ 는 노드 집합, $E(t)$ 는 가시성, 링크 상태, 궤도 위치에 따라 변하는 링크 집합이다. 링크 $(i,j)\in E(t)$에 대해서는 지연 $d_{ij}(t)$, 대역폭 $b_{ij}(t)$, 패킷 손실률 등을 추상화된 파라미터로 사용한다.

데이터 전달 경로는 일반적으로 수식 (2)와 같은 형태를 따른다:

$$G_{src}\rightarrow S_{i1}\rightarrow S_{i2}\rightarrow\cdots\rightarrow S_{ik}\rightarrow G_{dst} \tag{2}$$

이 중 하나 이상의 위성이 프록시 역할을 수행하며, 본 연구는 경로 상에서 어떤 위성이 PRE를 수행할지 선택하는 문제에 초점을 둔다.

3.2 에너지 모델

각 위성 S_i는 태양광 발전과 배터리 저장에 기반한 제한된 에너지 예산을 가진다. 시간 t에서 위성 S_i의 가용 에너지는 $E_i(t)$로 표기하며, 이는 발전, 소비, 배터리 용량에 의해 다음과 같이 개념적으로 표현된다.

- **발전 에너지** $P_i^{gen}(t)$: 태양광 패널을 통해 단위 시간당 생성되는 에너지
- **소비 에너지** $P_i^{cons}(t)$: 통신(송·수신), PRE 연산, 기타 온보드 시스템 동작에 사용되는 에너지
- **배터리 상태** $B_i(t)$: 저장된 에너지 양, $0\le B_i(t)\le B_i^{\max}$

에너지 상태의 천이는 수식 (3)과 같은 형태로 추상화할 수 있다.

$$B_i(t+1)=\min\left\{B_i^{\max},B_i(t)+P_i^{gen}(t)\Delta t-P_i^{cons}(t)\Delta t\right\} \tag{3}$$

실제 수식의 정밀 형태는 분석 목적에 따라 단순화하거나 확장할 수 있으며, 본 연구에서는 PRE 연산 수행 가능 여부와 선택 정책에 영향을 줄 수 있는 수준의 모델링에 집중한다.

본 연구에서 에너지 상태는 단일 스칼라 값 $E_i(t)$로 표현하며, 이는 배터리 잔량과 향후 단기 발전 가능성을 반영한 지표로 간주한다. 예를 들어 $E_i(t)$가 특정 임계값 이하로 떨어지면 높은 비용의 PRE 연산을 피하고, 여유 구간에서는 보다 적극적으로 PRE를 수행하도록 정책을 설계한다.

3.3 신뢰 모델 및 신뢰 점수 정의

각 위성 S_i에 대해서, 프록시로서의 행위가 얼마나 신뢰할 수 있는지를 나타내는 신뢰 점수 $T_i(t)$를 정의한다. 신뢰 점수는 0과 1 사이의 실수 값으로 두며, 값이 클수록 "정상적·협조적일 가능성이 높다"는 의미를 갖는다. 신뢰 점수는 다음과 같은 요소를 종합하여 정의한다.

- 과거 재암호화 결과의 검증 이력 (정상/오류 여부)
- 재암호화 지연, 응답 누락 등 비정상 행위의 빈도
- 주변 노드 또는 지상국에서 보고된 이상 행위 정보

예를 들어, 단순한 형태로는 지수 가중 이동 평균을 사용하여 수식 (4)와 같이 정의할 수 있다:

$$T_i(t+1) = \lambda T_i(t) + (1-\lambda) R_i(t) \qquad (4)$$

여기서 $0 \le \lambda \le 1$ 은 과거 이력의 영향도, $R_i(t)$는 시점 t에서의 관측 결과(정상 동작이면 1, 명백한 악의적 행위가 탐지되면 0 등)이다.

본 연구에서 에너지-인식 신뢰 기반 선택은 주로 수식 (5)와 같은 형태의 통합 점수를 통해 이루어진다:

$$S_i(t) = f(T_i(t), E_i(t)) \qquad (5)$$

$f(\cdot)$는 정책 파라미터에 따라 신뢰와 에너지의 상대적 중요도를 조정하는 함수이며, 예를 들어 선형 결합, 가중 최소값, 계단형 정책 등 다양한 형태를 취할 수 있다.

3.4 PRE 환경 및 키 관리 모델

본 연구에서의 PRE 환경은 다음과 같은 키 구조를 가진다.

① 각 지상국/사용자 $X \in \{G, U\}$
- 공개키 PK_X, 비밀키 SK_X를 가짐

② 송신자 A가 수신자 B에게 데이터를 공유하기 위해 필요
- 전역 또는 도메인별 신뢰 기관(TA, Trusted Authority)을 통해 PRE에 필요한 시스템 파라미터를 초기화
- 자신과 관련된 재암호화 키 $RK_{A \to B}$를 생성

③ 위성 S_i가 프록시가 되기 위해 필요
- 사전에 또는 필요 시 지상국/TA로부터 해당 재암호화 키를 안전 채널을 통해 전달
- 위성은 재암호화 키 $RK_{A \to B}$를 이용해 A의 암호문을 B용 암호문으로 변환할 수 있으나, 평문은 복구할 수 없다고 가정

PRE scheme의 알고리즘 집합은 일반적으로 수식 (6)과 같이 표현된다:

$$(Setup, KeyGen, RKGen, Enc, ReEnc, Dec) \qquad (6)$$

본 연구는 이 중 특히 $ReEnc$ 연산이 어느 위성에서 수행되는지, 어떤 위성에게 재암호화 키를 위임할 것인지에 대한 정책을 설계한다.

키 관리와 관련하여 다음과 같은 가정을 둔다.

TA 또는 상위 키 관리 기관은 신뢰할 수 있는 엔티티로 가정하며, 키 생성·배포는 안전한 채널을 통해 수행된다.

일부 위성은 공격자에 의해 장악될 수 있으며, 이 경우 장악된 위성은 자신에게 부여된 재암호화 키와 해당 시점 이후 수신하는 암호문을 임의로 조작할 수 있는 악의적 프록시로 모델링한다.

3.5 보안 요구사항

제안하는 에너지-인식 신뢰 기반 프록시 선택 프레임워크가 만족해야 할 주요 보안 요구사항은 다음과 같다.

① 기밀성(Confidentiality)
- 악의적 위성을 포함한 공격자가 위성 프록시를 장악하더라도, 평문 데이터나 다른 사용자의 비밀키를 획득할 수 없어야 함

② 가용성(Availability)
- 일부 위성이 공격으로 사용 불능이 되더라도 다른 위성을 통해 PRE 경로를 재구성하여 서비스 중단을 최소화해야 함
- 에너지 상태를 고려한 선택 정책은 에너지 고갈로 인한 기능 상실을 줄여 네트워크 전체 가용성을 향상시켜야 함

③ 신뢰 기반 프록시 선택(Trust-Based Proxy Selection)
- 신뢰·에너지 기반 선택 알고리즘은 악의적 행위가 탐지된 위성의 신뢰

점수를 낮춰 PRE 역할에서 배제해야 함
- 공격자의 신뢰 점수 조작·위장 행위를 어렵게 하거나 최소한 탐지·완화할 수 있어야 함

④ 에너지-보안 균형(Energy - Security Trade-off)
- 에너지 제약을 이유로 보안 수준이 과도하게 낮아지지 않도록 정책 파라미터(가중치, 임계값 등)를 설계해야 함
- 지나친 보안 요구로 에너지 고갈이 발생해 위성이 장기간 활용 불가능해지는 상황도 지양해야 함

4. 제안 방식

4.1 시스템 파라미터

본 장에서 사용되는 시스템 파라미터들은 다음 표 1과 같다.

표 1. 시스템 파라미터
Table 1. system parameters

기호	설명
i	위성 인덱스 (위성 S_i)
j	경로 상에서의 위성 순서 인덱스 (i_j)
t	시간 인덱스 (슬롯 또는 연속 시간)
S_i	i번째 LEO 위성
$S=\{S_1,...,S_N\}$	LEO 위성 집합
G_k	k번째 지상국
$G=\{G_1,...,G_{N_G}\}$	지상국 집합
U_l	l번째 사용자 단말
$U=\{U_1,...,U_{N_U}\}$	사용자 단말 집합
TA	Trusted Authority, 시스템 파라미터/키 발급 기관
$V=S\cup G$	위성 + 지상국 노드 집합
$E(t)$	시간 t에서 존재하는 링크 집합
$G(t)=(V,E(t))$	시간 t에서의 위성망 그래프
$(u,v)\in E(t)$	노드 u,v 사이의 링크
$d_{uv}(t)$	링크 (u,v)의 지연(latency)
$b_{uv}(t)$	링크 (u,v)의 대역폭(bandwidth)
$\ell_{uv}(t)$	링크 (u,v)의 손실률(loss rate)
$C(t)$	시간 t에서 프록시 후보 위성 집합
$P=(i_1,i_2,...,i_k)$	위성 인덱스로 표현한 경로 P
$P(t)$	시간 t에서 고려하는 후보 경로 집합
$delay_{i_j}(t)$	경로 상 위성 S_{i_j}를 지날 때의 지연 기여도
$B_i(t)$	시간 t에서 위성 S_i 배터리에 저장된 에너지
$B_i^{\max}$	위성 S_i 배터리 최대 용량
$P_i^{gen}(t)$	시간 t에서 위성 S_i의 발전 전력
$P_i^{cons}(t)$	시간 t에서 위성 S_i의 소비 전력 (통신, 연산 등)
Δt	시간 슬롯 길이
$E_i(t)$	시간 t에서 위성 S_i의 에너지 상태 지표
$E_i^{\max}$	에너지 상태 정규화 상한 기준값
$E_i^{norm}(t)=E_i(t)/E_i^{\max}$	정규화된 에너지 상태 (0~1 범위)
$T_i(t)$	시간 t에서 위성 S_i의 신뢰 점수 (0~1)
$R_i(t)$	시간 t에서 위성 S_t에 대한 관찰 결과
λ	신뢰 점수 업데이트 가중치 $(0\le\lambda\le1)$
λ_{good}	정상 동작 시 신뢰 업데이트 계수
λ_{bad}	악의적/오류 동작 시 신뢰 업데이트 계수
$T_{\min}$	프록시 후보로 인정하기 위한 최소 신뢰 임계값
T_{block}	이 값 이하로 떨어지면 블랙리스트에 넣는 임계값
$S_i(t)$	위성 S_i의 신뢰·에너지 통합 점수
α,β	통합 점수에서 신뢰/에너지 가중치 $(\alpha,\beta\ge0)$
$i^*(t)$	시간 t에 선택된 프록시 위성 인덱스
C(P)	경로 P에 대한 비용 함수 값
w_1,w_2,w_3	경로 비용에서 신뢰 부족, 에너지 부족, 지연에 대한 가중치
$P^*(t)$	시간 t에 선택된 최적 경로
(PK_X,SK_X)	사용자/지상국 X의 공개키/비밀키 쌍
$C_A=Enc(PK_A,m)$	송신자 A의 공개키로 평문 m을 암호화한 암호문
$RK_{A\to B}$	송신자 $A\to$ 수신자 B 재암호화 키
$C_B=ReEnc(RK_{A\to B},C_A)$	프록시가 재암호화한 암호문
$m=Dec(SK_B,C_B)$	수신자 B가 비밀키로 복호화한 평문

4.2 신뢰 · 에너지 통합 점수 함수 설계

각 위성 S_i에 대해, 3장에서 정의한 신뢰 점수 $T_i(t)$와 에너지 상태 $E_i(t)$를 이용해, 프록시 후보로서의 적합도를 나타내는 통합 점수 $S_i(t)$를 정의한다. 기본적인 형태로는 수식 (7)과 같은 선형 결합을 사용할 수 있다.

$$S_i(t)=\alpha\cdot T_i(t)+\beta\cdot E_i^{norm}(t) \qquad (7)$$

정규화는 예를 들어 수식 (8)과 같이 정의할 수 있다.

$$E_i^{norm}(t) = E_i(t) / E_i^{\max} \quad (8)$$

($E_i^{\max}$ 는 위성 S_i의 가용 에너지 상한 또는 공통 기준값)

보다 보수적인 정책을 위해, 수식 (9)과 같이 신뢰가 충분히 높지 않으면 프록시에서 제외하는 임계값 기반 함수도 사용할 수 있다.

$$S_{i(t)} = \begin{cases} 0 & (T_i(t) < T_{\min}) \\ \alpha \cdot T_i(t) + \beta \cdot E_i^{norm}(t) & (T_i(t) \geq T_{\min}) \end{cases} \quad (9)$$

이와 같이 정의하면, 신뢰 점수가 일정 임계값 $T_{\min}$미만인 위성은 에너지가 아무리 충분하더라도 프록시 후보에서 사실상 제외된다.

통합 점수 함수 $f(\bullet)$의 구체적인 형태(선형, 비선형, 계단 함수 등)는 네트워크 운영 정책에 따라 달라질 수 있으며, 5장과 6장에서는 $\alpha, \beta, T_{\min}$을 변화시키면서 보안 - 에너지 trade-off를 분석한다.

4.3 프록시/경로 선택 알고리즘

통합 점수 $S_i(t)$를 바탕으로, 특정 통신 세션에 대해 프록시 위성과 경로를 선택하는 알고리즘을 설계한다. 기본적으로 두 단계로 나눌 수 있다.

① 후보 위성 집합 선정

- 현재 시점 t에서, 토폴로지와 링크 상태를 고려하여 송신자 - 수신자 경로 상에 존재하는 위성 집합 $C(t)$를 구함
- $C(t)$는 경로 상 위성들 중 PRE를 수행할 수 있는 잠재적 프록시 집합

② 프록시 선택 규칙 적용

가장 단순한 형태의 단일 프록시 선택은 수식 (10)과 같이 정의할 수 있다.

$$i^*(t) = \arg\max_{i \in C(t)} S_i(t) \quad (10)$$

즉, 후보 집합 $C(t)$ 중에서 통합 점수 $S_i(t)$가 가장 큰 위성 $S_i^*(t)$ 에게 PRE 연산을 맡긴다.

여러 위성이 연쇄적으로 PRE를 수행하는 경로 기반 선택을 고려하려면, 경로 $P = (i_1, i_2, \ldots, i_k)$에 대해 수식 (11)과 같은 비용 함수를 정의할 수 있다.

$$C(P) = \sum_{j=1}^{k} (w_1 \cdot (1 - T_{i_j}(t)) + w_2 \cdot (1 - E_{i_j}^{norm}(t)) + w_3 \cdot delay_{i_j}(t)) \quad (11)$$

이때 최적 경로 선택은 수식 (12)와 같이 정의할 수 있다.

$$P^*(t) = rg\max_{P \in P(t)} C(P) \quad (12)$$

($P(t)$ 는 시점 t에서 가능한 경로 집합)

실제 구현에서는 계산 복잡도를 줄이기 위해, 전체 경로 최적화 대신 경로가 주어져 있을 때 그 중 PRE 수행 노드만 선택하거나, 상위 몇 개의 후보 위성만 고려하는 휴리스틱을 사용할 수 있다.

4.4 키 위임 및 프로토콜 메시지 흐름

본 절에서는 선택된 프록시 위성에 재암호화 키를 위임하고, 실제 통신 시에 메시지가 어떻게 흐르는지를 단계별로 기술한다. 기본적인 시나리오는 다음과 같다.

① 시스템 초기화 (오프라인 단계)

(a) 신뢰 기관(TA)이 $Setup$을 수행하여 시스템 파라미터를 배포한다.

(b) 각 지상국/사용자는 $KeyGen$으로 (PK_X, SK_X) 를 생성한다.

(c) 위성 S_i에 대한 초기 신뢰 점수 $T_i(0)$와 에너지 상태 $E_i(0)$ 를 설정한다.

② 재암호화 키 생성 및 위임
(a) 송신자 A가 수신자 B와의 데이터 공유를 허용하기로 하면 $RKGen$을 통해 $RK_{A\to B}$ 를 생성한다.
(b) TA 또는 A는 프록시 후보 위성 집합에 대해, 정책에 따라 필요한 위성에만 $RK_{A\to B}$를 안전 채널로 전달한다.
(c) 이때, 신뢰·에너지 조건을 만족하는 위성 집합에 한정하여 키를 배포하는 방식도 가능하다.

③ 세션 수립 및 프록시/경로 선택
(a) A가 B에게 데이터를 전송하려 할 때, 현재 시점 t에서 토폴로지/링크 상태를 반영하여 후보 위성 집합 $C(t)$ 와 경로 집합 $P(t)$를 계산한다.
(b) 4.2절의 $S_{i(t)}$와 4.3절의 선택 규칙을 이용해 프록시 위성 $i^*(t)$또는 경로 $P^*(t)$를 결정한다.
(c) 선택 결과는 관련 노드(위성, 지상국)에 통지된다.

④ 데이터 암호화 및 전송
(a) A는 평문 m을 자신의 공개키로 암호화하여 $C_A = Enc(PK_A, m)$을 생성한다.
(b) C_A는 선택된 경로를 따라 위성망으로 전송된다.

⑤ PRE 수행 및 전달
(a) 프록시 위성 $S_i^*(t)$ 는 $RK_{A\to B}$ 와 C_A를 이용해 $C_B = ReEnc(RK_{A\to B}, C_A)$를 계산한다.
(b) 재암호화된 암호문 C_B는 이후 경로를 따라 B또는 B가 속한 지상망으로 전달된다.

⑥ 복호 및 검증
(a) 수신자 B는 SK_B를 사용하여 $m = Dec(SK_B, C_B)$를 계산한다.
(b) 필요 시, 상위 계층에서 MAC, 전자서명, 해시 등을 통해 데이터 무결성과 정당성을 추가로 검증한다.

⑦ 로그 및 모니터링
(a) 각 PRE 수행 결과에 대해 “성공/실패 여부”, “지연”, “오류 발생 여부” 등을 기록하여 이후 신뢰 점수 업데이트에 활용한다.

4.5 신뢰 점수 업데이트 및 악의적 프록시 대응

프록시 선택 기법이 장기적으로 악의적 위성을 배제하고 신뢰 가능한 위성에 PRE 역할을 집중시키기 위해서는, 신뢰 점수 $T_i(t)$를 적절히 업데이트하는 메커니즘이 필요하다.

가장 기본적인 형태의 신뢰 점수 업데이트는 수식 (13)과 같이 정의할 수 있다.

$$T_i(t+1) = \lambda \cdot T_i(t) + (1-\lambda)\cdot R_i(t) \qquad (13)$$

악의적 프록시 대응을 강화하기 위해, 나쁜 행동에 더 민감하게 반응하는 비대칭 업데이트도 사용할 수 있다.

- 정상 동작 시 :
$$T_i(t+1) = \lambda_{good} \cdot T_i(t) + (1-\lambda_{good})\cdot 1 \qquad (14)$$

- 악의적 행위 탐지 시 :
$$T_i(t+1) = \lambda_{bad} \cdot T_i(t) + (1-\lambda_{bad})\cdot 0 \qquad (15)$$

보통 $\lambda_{bad} < \lambda_{good}$ 로 두어, 악의적 행위가 한 번이라도 탐지되면 신뢰 점수가 빠르게 떨어지도록 한다.

또한 일정 임계값 T_{block}이하로 떨어진 위성은 블랙리스트에 등록하여 프록시 후보에서 제외할 수 있다.

- $T_{i(t)} \le T_{block}$ 이 되는 시점부터
- S_i는 프록시 선택 대상에서 제외

종합하면, 본 절에서 정의한 신뢰 점수 업데이트와 블랙리스트 메커니즘을 통해, 시스템은 시간이 지남에 따라 악의적·불안정한 위성을 도태

시키고, 안정적이고 에너지 여유가 있는 위성들에 PRE 역할을 집중시키는 방향으로 결정된다.

5. 제안 방식 분석

5.1 보안 요구사항 분석

3.5절에서 정의한 주요 보안 요구사항(기밀성, 정당성·무결성, 프록시 선택의 안전성, 가용성, 에너지 - 보안 균형)에 대해 제안 방식이 어떻게 부합하는지 분석한다.

① 데이터 기밀성(Confidentiality)

PRE가 IND-CPA 또는 IND-CCA 안전하다고 가정하면, 암호문 C_A 및 C_B, 그리고 재암호화 키 $RK_{A\to B}$만으로는 평문 m이 노출되지 않는다.

위성 S_i가 공격자에 의해 장악되더라도, S_i는 자신에게 위임된 $RK_{A\to B}$와 수신하는 암호문들에 대해서만 재암호화를 수행할 수 있을 뿐, SK_A나 SK_B에 접근할 수 없으므로 다른 세션에 대한 평문 복구는 불가능하다.

프록시 선택 알고리즘은 $ReEnc$의 수행 대상만을 바꾸며, 암호문·키 구조 자체는 변경하지 않으므로, PRE의 기밀성 보장에 영향을 주지 않는다.

② 가용성(Availability)

일부 위성이 블랙리스트에 들어가거나 에너지 부족으로 PRE 수행을 거부하더라도, 다른 후보 위성이 $C(t)$에 존재하는 경우, 프록시 재구성이 가능하다.

이와 같이 에너지 상태 $E_i(t)$를 고려하는 정책은 에너지가 극도로 부족한 위성에 재암호화 부담을 몰아주지 않도록 설계되어, 장기적으로 더 많은 위성이 기능을 유지할 수 있도록 돕는다.

③ 신뢰 기반 프록시 선택 (Trust-Based Proxy Selection)

신뢰 점수 $T_i(t)$와 블랙리스트 임계값 T_{block}을 통해, 악의적 행위가 반복적으로 관측되는 위성은 점차 프록시 후보 집합 $C(t)$에서 배제된다. 통합 점수 $S_i(t)$ 가 낮아진 위성은 $i^*(t)=\arg\max_{i\in C(t)} S_i(t)$ 규칙에 의해 선택될 가능성이 줄어들며, 결국 프록시의 역할에서 도태된다. 이 과정에서 $R_i(t)$의 정의와 λ, λ_{bad}등의 파라미터를 설정하면, 악의적 행위에 대한 대응을 유연하게 할 수 있다.

④ 에너지-보안 균형(Energy-Security Trade-off)

$S_i(t)=\alpha\cdot T_i(t)+\beta\cdot E_i^{norm}(t)$와 같은 통합 점수 함수에서 α, β 의 비율을 조절함으로써, 보안(신뢰)과 에너지 효율 사이의 가중치를 조정할 수 있다.

예를 들어 α를 크게, β를 작게 설정하면 신뢰도가 최우선이 되며, 반대로 β를 키우면 에너지 여유가 더 큰 위성이 선호된다.

이는 운영 정책에 따라 “보안 우선 모드”와 “생존성·가용성 우선 모드” 간의 선택을 가능하게 한다.

결과적으로, 제안 방식은 PRE의 기존 보안 특성을 유지하면서, 신뢰·에너지 기반 프록시 선택 계층을 추가하여, 악의적 프록시와 에너지 제약을 동시에 고려하는 보안 아키텍처를 제공한다.

5.2 악의적 프록시 및 공모 공격 대응 분석

본 절에서는 3장에서 정의한 위협 모델에 따라, 제안방식이 악의적 프록시 및 공모 공격에 안전하게 동작함을 확인한다.

① 단일 악의적 프록시 공격

위성 S_a가 장악되어 악의적 프록시로 동작하는 경우를 고려한다. S_a는 자신에게 전달된 암호

문에 대해 다음과 같은 행동을 할 수 있다.

- 재암호화를 생략하거나, 임의의 C_B' 로 대체
- 잘못된 수신자용 재암호화 수행
- 지연을 인위적으로 증가시켜 서비스 품질을 저하시킴

이 경우, 상위 계층의 무결성 검증에서 오류가 반복적으로 관측되거나, 지연·실패율이 특정 위성을 중심으로 비정상적으로 높게 나타나면, $R_a(t)$ 값은 낮게 설정되고, $T_a(t)$는 업데이트 규칙에 따라 지속적으로 감소한다. 일정 시점 이후 $T_a(t) \le T_{block}$ 이 되면, S_a 는 프록시 후보 집합 $C(t)$에서 제외된다.

즉, 단일 악의적 프록시는 단기적으로 서비스 거부나 일부 세션 실패를 유발할 수 있으나, 장기적으로는 신뢰 점수 시스템에 의해 영향을 제한받고, 프록시 역할에서 배제된다.

② 복수 악의적 프록시 및 공모 공격

여러 위성이 동시에 장악되었거나, 특정 수신자와 일부 위성이 공모하는 경우를 고려할 수 있다. 만약 복수 악의적 위성이 다양한 경로에 분포해 있는 경우, 악의적 행동이 더욱 광범위하게 발생할 수 있으나, 동일한 신뢰 업데이트 메커니즘이 적용되면, 다수의 위성에 대해 $T_i(t)$ 가 감소한다.

공모 공격의 경우, 예를 들어 악의적 수신자 B가 자신에게 유리한 방향으로 로그를 조작해 특정 위성의 $T_i(t)$저하를 방해할 수 있는 가능성이 있다. 이 경우 단일 수신자의 보고에만 의존하지 않고, 다수 노드·지상국의 관찰 결과를 집계하는 방식으로 $R_i(t)$를 결정하는 구조를 도입함으로써, 공모 공격의 영향을 완화할 수 있다.

③ 신뢰 점수 시스템에 대한 공격

공격자가 정상적인 동작을 일부 시간 유지하면서 점차 $T_i(t)$를 끌어올린 후, 특정 시점에 집중적으로 악의적 행위를 수행하는 "신뢰 상승 후 배신" 전략도 고려할 수 있다. 이를 완화하기 위해서는 다음과 같은 설계가 가능하다.

- λ_{good} 값은 비교적 크게, λ_{bad}값은 작게 설정하여, 악의적 이벤트가 발생할 때 $T_i(t)$가 급격히 떨어지도록 함
- 최근 관찰에 더 높은 가중치를 부여하는 슬라이딩 윈도우 기반 $R_i(t)$ 정의

이 경우, 공격자는 일시적으로 피해를 줄 수 있지만, 악의적 행위가 포착되는 즉시 신뢰 점수가 급격히 떨어지고, 프록시 후보에서 빠져나가게 된다.

종합적으로, 제안된 신뢰 업데이트 및 블랙리스트 메커니즘은 완전한 공격 불가능성을 보장하지는 않지만, 악의적 프록시의 영향 범위와 지속 시간을 제한하고, 장기적으로는 신뢰도가 높은 위성에 프록시 역할을 집중시키는 방향으로 시스템을 유도한다.

6. 결론

본 연구는 분산 LEO 위성망에서 위성이 PRE 노드로 동작하는 환경을 대상으로, 제한된 온보드 에너지와 악의적 프록시 위협을 함께 고려한 에너지-인식 신뢰 점수 기반 프록시/경로 선택 프레임워크를 제안하였다. 이를 위해 위성 - 지상국 네트워크 구조, 태양광 발전 및 배터리 소모를 반영한 에너지 모델, 재암호화 결과 검증 이력 기반 신뢰 점수 모델, PRE 및 키 관리 구조와 보안 요구사항을 포함한 시스템 모델을 정의하였다.

이 모델 위에서 신뢰도·에너지 통합 점수와 경로 비용 함수를 설계하고, 이를 이용해 단일 프

록시 선택과 다중 위성 경로 선택 알고리즘을 제시하였다. 또한 재암호화 로그와 이상 행위 관찰값을 활용한 신뢰 점수 업데이트 및 블랙리스트 메커니즘을 도입하여, 시간이 지남에 따라 악의적·불안정 위성이 프록시 후보에서 배제되도록 설계하였다. 제안 방식은 기존 PRE의 기밀성과 정당성을 유지하면서 에너지-보안 균형을 고려하는 선택 계층을 추가함으로써, 우주 환경의 제약을 반영한 보안 아키텍처를 제공한다.

본 연구는 (1) LEO 위성망에서 프록시의 신뢰도와 에너지 상태를 통합적으로 반영하는 선택 프레임워크를 제시하고, (2) 악의적 프록시 및 공모 공격을 포함한 위협 모델 하에서 보안 요구사항 충족 여부를 분석했으며, (3) 에너지·연산·통신 오버헤드 관점에서 특성을 논의했다. 이를 통해 에너지 상태에 따른 유연한 경로 설정을 가능하게 하여, 향후 우주 환경에서의 안전한 데이터 전달에 기여할 것으로 기대한다.

본 연구는 2025년도 상명대학교 대학혁신지원사업 연구비를 지원받아 수행하였음

참 고 문 헌

[1] Hu, Yu, et al. “Multi-dimensional resource allocation strategy for LEO satellite communication uplinks based on deep reinforcement learning”, Journal of Cloud Computing, 13(56), pp. 1-15, 2024, DOI : https://doi.org/10.1186/s13677-024-00621-z

[2] Xiu, Qingxiao, et al. “Computation offloading and resource allocation in satellite edge computing networks: A multi-agent reinforcement learning approach”, Computer Networks, 111680, pp. 1-17, 2025, DOI : https://doi.org/10.1016/j.comnet.2025.111680

[3] Di, Hang, et al. “Network Resource Allocation Method Based on Awareness-Prediction Joint Compensation for Low-Earth-Orbit Satellite Networks”, Applied Sciences, 15(10), 5665, pp. 1-22, 2025, DOI : https://doi.org/10.3390/app15105665

[4] Nuñez, David, et al. “Proxy re-encryption: Analysis of constructions and its application to secure access delegation”, Journal of Network and Computer Applications, 87, pp. 193-209, 2017, DOI : https://doi.org/10.1016/j.jnca.2017.03.005

[5] Zhang, Yongjing, et al. “Conditional proxy re-encryption-based key sharing mechanism for clustered federated learning”, Electronics, 13(5), pp. 848, 2024, DOI : ttps://doi.org/10.3390/electronics13050848

[6] Song, You-Jin, and Jeong-Min Do. “Secure Data Management based on Proxy Re-Encryption in Mobile Cloud Environment”, The Journal of Korean Institute of Communications and Information Sciences, 37(4)B, pp. 288-299, 2012, DOI : https://doi.org/10.7840/KICS.2012.37B.4.288

[7] Poonam, Kumkum Garg, and Manoj Misra. “Trust based security in MANET routing protocols: a survey”, Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India, pp. 1-7, 2010, DOI : https://doi.org/10.1145/1858378.1858425

[8] Bai, Yameng, et al. “TSRP: a novel trust-based and energy-aware secure routing protocol for resource-constrained wireless sensor networks”, Journal of The Institution of Engineers (India): Series B, 106(5), pp. 1401-1413, 2025, DOI : https://doi.org/10.1007/s40031-024-01158-0

[9] Liu, Ming, et al. “An energy-aware routing protocol in wireless sensor networks”, Sensors, 9(1), pp. 445-462, 2009,

DOI : https://doi.org/10.3390/s90100445
[10] Almomani, Iman, and Maha Saadeh. “S-FEAR: secure-fuzzy energy aware routing protocol for wireless sensor networks”, KSII Transactions on Internet and Information Systems (TIIS), 12(4), pp. 1436-1457, 2018,
DOI : https://doi.org/10.3837/tiis.2018.04.003
[11] Vikas, et al. “Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks”, Sensors, 25(8), pp. 2519, 2025,
DOI : https://doi.org/10.3390/s25082519
[12] Barari, Malak, and Ramzi Saifan. “Energy - Aware security protocol for IoT devices”, Pervasive and Mobile Computing, 96, pp. 101847, 2023, DOI : https://doi.org/10.1016/j.pmcj.2023.101847

저 자 소 개

김원빈(Won-Bin Kim)

2015.2 순천향대학교 소프트웨어공학과 졸업
2017.2 순천향대학교 컴퓨터학과 석사
2022.2 순천향대학교 SW융합학과 박사
2022.1-2024.5 엘에스웨어(주) 팀장
2024.5-현재 : 상명대학교 연구교수
<주관심분야> 암호프로토콜, 프록시재암호화, 암호학, 우주보안

정용준(Yongjun Chung)

2025.3-현재 : 상명대학교 자유전공학부 핀테크전공 재학 중
<주관심분야> 통계적 모델링, 데이터 마이닝, 금융 정보보호

백상현(Sanghyun Paek)

2007.2 고려대학교 화학과 졸업
2009.2 고려대학교 소재화학 석사
2013.2 고려대학교 태양전지소재 박사
2014.9-2020.2 EPFL 박사후 연구원
2020.3-현재 : 상명대학교 교수
<주관심분야> 에너지, 페로브스카이트 태양전지, 유기합성 재료

서대희(Daehee Seo)

2001.2 동신대학교 전기전자공학부 졸업
2003.2 순천향대학교 전산학과 석사
2006.2 순천향대학교 전산학과 박사
2009.10-2015.3 한국전자통신연구원 선임연구원
2018.8~2020.5 Kennesaw state university Senior researcher
2021.3-현재 : 상명대학교 교수
<주관심분야> 정보보안, 암호학, 융합보안, AI보안, 우주보안