안전한 위성간 통신을 위한 샤미르 시크릿 쉐어링 기반 주파수 호핑 기법

김수경[1], 김소연[2], 이일구[3]
[1]성신여자대학교 융합보안공학과 학부생
[2]성신여자대학교 미래융합기술공학과 박사과정
[3]성신여자대학교 융합보안공학과, 미래융합기술공학과 교수
{20220115, 220237014, iglee}@sungshin.ac.kr

Shamir's Secret Sharing-Based Frequency Hopping Technique for Secure Inter-Satellite Links

Su-Kyoung Kim[1], So-Yeon Kim[2], Il-Gu Lee[1,2]
[1]Dept. of Convergence Security Engineering, Sungshin Women's University
[2]Dept. of Future Convergence Technology Engineering, Sungshin Women's University

요 약

최근 광역 네트워크의 신속·안전성이 중요해지면서 위성간 통신이 다양한 산업의 필수 인프라로 자리 잡았다. 그러나 위성통신은 넓은 지역에 전파가 확산되므로 재밍·도청 공격에 취약하고, 하드웨어적 제약으로 고성능 보안 기법을 적용하기 어렵다는 한계가 있다. 본 논문에서는 위성통신 환경에서 데이터의 기밀성과 무결성을 높이면서도 복잡한 연산을 요구하지 않는 샤미르 시크릿 쉐어링 기반 주파수 호핑 기법을 제안한다. 실험에 따르면, 제안 방식은 재밍 강도가 증가할수록 종래 방식 대비 약 9.5% 높은 데이터 복원율을 보였으며, 재밍 발생 확률 70% 구간에서 종래 방식과 달리 100%의 복원율을 유지했다. 또한 종래 방식 대비 도청 성공률이 평균 30.6% 낮았다.

1. 서론

최근 위성통신은 기존 지상망의 지리적 한계를 넘어 전 지구적 커버리지를 제공하면서, 6세대 이동통신의 핵심 인프라로 주목받고 있다. 모건스탠리에 따르면 세계적 위성통신 시장 규모는 2040년에 약 456조 원에 달할 것으로 전망된다[1]. 그러나 위성통신은 넓은 지역에 전파가 확산되므로 재밍 및 도청 공격에 취약하다. 이를 해결하기 위해 Wang 외 2인 [2]은 위성의 전파 방향을 분석하여 재밍 신호를 탐지하는 방법을 제안했으나, 해당 방법은 신호를 지속적으로 추적해야 하므로 전력이 제한된 위성통신 환경에 적용하기 어려웠다. 이러한 문제를 해결하기 위해 Yuan 외 5인 [3]은 일정한 주기로 주파수를 전환하며 데이터를 전송하는 FHSS (Frequency Hopping Spread Spectrum) 기반 보안 기법을 제안했다. 이 방식은 연산 부담이 적으나, 도약 패턴이 노출되면 보안성이 저하되는 문제가 있었다.

이에 본 논문에서는 SSS (Shamir's Secret Sharing)로 데이터를 분할한 후 분할 데이터마다 FHSS 전송하는 방식을 제안한다. 분할 데이터는 서로 다른 주파수 경로로 전송되므로 전체 데이터가 재밍·도청될 확률이 낮으며, 고성능 보안 기법 대비 연산량이 적어서 자원 효율적이다.

본 논문의 주요 기여점은 다음과 같다.

- 위성통신 환경의 제약을 고려하면서도 보안성을 강화하는 SSS 기반 주파수 도약 전송 기법을 제안했다.
- 제안 방식은 종래 FHSS 방식 대비 약 30.6% 낮은 도청 성공률을 보였으며, 재밍 환경에서 약 9.5% 높은 복원율을 보였다. 특히, 재밍 발생 확률 70% 구간에서 100%의 복원율을 유지했다.

3. 제안 방식

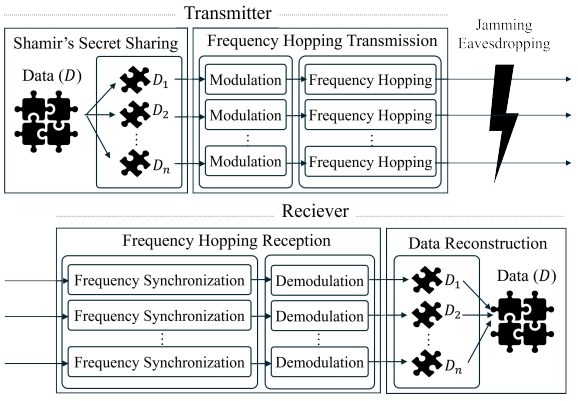

그림1. 제안 방식의 구조도

그림 1은 제안하는 방식의 동작 과정을 나타낸

다. 먼저, 데이터를 여러 개의 조각으로 분할한 뒤 이를 각각 다른 주파수로 전송함으로써 전체 데이터가 단일 경로에서 노출되지 않도록 한다. 각 조각은 위상 신호로 변조된 후, 주파수 도약을 통해 각각 다른 주파수 채널로 전송한다. 수신 측에서는 도약 주파수를 동기화하고 데이터 조각들을 재조합하여 원본 데이터를 복원한다.

4. 실험 및 결과

본 실험은 위성간 통신의 송수신 환경을 모델링하여 시뮬레이션했다. 제안 기법의 성능을 검증하기 위해 재밍 및 도청 상황을 구현하여 종래의 FHSS 방식과 비교하였다. 전송 데이터는 총 9개의 조각으로 분할되며, 복원에 필요한 최소 조각 수는 3개이다. 주파수 도약에 사용된 주파수 슬롯은 총 10개이며, 각 실험은 10,000회 반복 수행하였다.

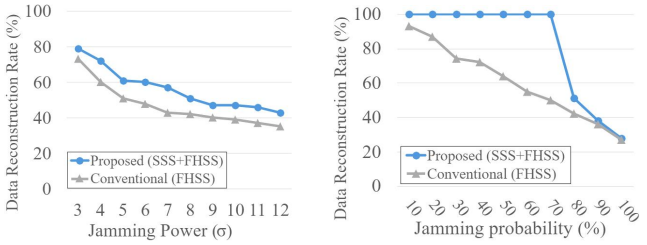

그림 2. 재밍 강도·발생 확률에 따른 데이터 복원율

그림 2는 제안 방식과 종래 방식을 재밍의 강도·발생 확률에 따른 데이터 복원율을 비교한 결과이다. 위성간 통신에 미치는 재밍 효과는 주파수 슬롯에 가우시안 잡음을 주입하는 방식으로 모델링하였으며, 재밍 발생 확률은 재밍을 가한 주파수 슬롯 수를 전체 주파수 슬롯 수로 나눈 비율로 정의했다. 그리고 재밍 발생 확률을 80%로 고정하고 재밍 강도에 따른 데이터 복원율 평가했다. 실험 결과에 따르면 재밍 강도가 3 σ에서 12 σ까지 증가할 때, 제안 방식은 종래 방식 대비 복원율이 평균 9.5% 높았다. 재밍 발생 확률에 따른 데이터 복원율 평가에서는 재밍 강도를 8 σ로 고정하였다. 종래 방식 대비 제안 방식의 복원율이 전반적으로 높았으며, 특히 재밍 발생 확률 70% 구간에서 종래 방식은 51%의 복원율을 보였지만, 제안 방식은 100% 복원했다.

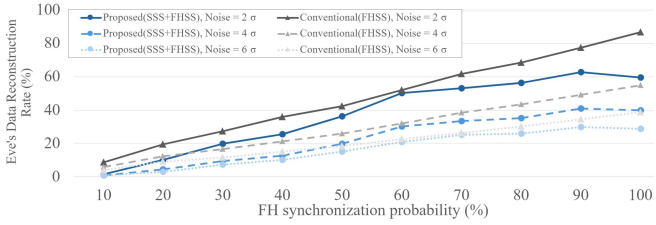

그림 3. 주파수 동기화 성공률에 따른 도청 성공률

그림 3은 도청자의 주파수 동기화 성공률에 따른 도청자의 데이터 복원율을 비교한 결과이다. 위성통신 환경을 반영해 잡음을 추가하였으며, 잡음 세기는 각각 약한 환경(2 σ), 중간 환경(4 σ), 강한 환경(6 σ)으로 설정하였다. 주파수 동기화 성공률은 주파수 동기화된 슬롯 대 전체 슬롯의 비율로 정의했다. 실험 결과에 따르면, 제안 방식의 도청 성공률은 종래 방식과 비교하여 잡음이 약한 환경에서 평균 약 29%, 중간 수준 환경에서 약 33.5%, 강한 환경에서 약 29.3% 낮았다.

4. 결론

장거리 무선 환경의 위성 간 통신은 재밍·도청 공격에 취약하고, 열악한 채널 품질과 하드웨어적 제약으로 고성능 보안 기법을 적용하기 어렵다. 이를 보완하기 위한 종래의 FHSS 방식은 주파수 도약 패턴의 노출 여부에 따라 보안 수준이 좌우된다는 문제가 있었다. 본 연구에서는 보안성을 더욱 높이기 위해, SSS 기반의 주파수 도약 전송 방식을 제안했다. 실험 결과에 따르면, 제안 방식은 종래 FHSS 방식 대비 약 30.6% 낮은 도청 성공률을 보였으며, 재밍 환경에서 약 9.5% 높은 복원율을 보였다. 특히, 재밍 발생 확률 70% 구간에서 100%의 복원율을 유지했다. 향후에는 테스트 베드를 구현하여 다양한 위협 환경에서 제안한 SSS 기반 FHSS 전송 기법의 성능과 보안을 최적화하는 연구를 수행할 계획이다.

ACKNOWLEDGMENT

본 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2025-00518150)과 과학기술정보통신부 및 정보통신기획평가원의 ICT혁신인재4.0 사업의 연구결과로 수행되었음 (No. IITP-2022-RS-2022-00156310)

참고문헌

[1] Aguilar, A. et al. “Tradespace Exploration of the Next Generation Communication Satellites”. AIAA Scitech Forum. 2019

[2] Wang, H et al. “Deception Jamming Detection Based on Beam Scanning for Satellite Navigation Systems”. IEEE Communications Letters. Cancun, Mexico. 2021

[3] Yuan, E et al. “Satellite navigation method based on high-speed frequency hopping signal”. China Communications. 2023