

위성-지상-위성 링크에서 릴레이 수 증가가 보안 성능에 미치는 영향 분석

손정민, 고영채
고려대학교

<jmson0307, koyc>@korea.ac.kr

Effect of Relay Number on Security Performance in Satellite-Ground-Satellite Links

Jung-Min Son, Young-Chai Ko
Korea Univ.

요 약

본 논문은 위성-지상간 통신 시스템에서 지상 중계기(릴레이)의 수가 보안 성능에 미치는 영향을 분석한다. RF 기반 위성 통신의 도청 취약성을 보완하기 위해 물리 계층 보안(PLS) 기법이 활용되며, 디코드-포워드(DF) 방식의 중계 구조를 기반으로 보안 성능을 평가한다. 비밀률 기반 보안 성능 지표(PNZSC, SOP, ASC)를 사용하였으며 몬테카를로 시뮬레이션을 통해 릴레이 수(1 개, 2 개, 3 개)에 따른 보안 성능 변화를 분석하였다.

I. 서 론

LEO(Low Earth Orbit) 위성 통신은 넓은 커버리지와 낮은 지연 시간 등의 장점이 있으나, RF 기반 통신 특성상 도청과 같은 보안 위협에 취약하다. 이를 보완하기 위해 인공 잡음, 빔포밍, 전력 제어 등 물리계층 보안(PLS) 기법이 활용되며, 최근에는 좁은 빔 전송으로 도청을 어렵게 하는 무선 광통신(FSO)이 보안성 향상 대안으로 주목받고 있다[1][2]. 본 논문은 RF 기반 위성-지상-위성 링크에서 지상 게이트웨이 수 변화에 따른 보안 성능을 시뮬레이션으로 분석하여, 향후 FSO 기반 시스템의 적용 가능성을 평가하기 위한 기초 연구를 수행한다.

II. 본론

1) 시스템 모델

본 논문에서는 RF 기반 위성-지상-위성 링크에서의 보안 성능을 분석한다. 송신자(Alice)로부터 수신자(Bob)까지의 데이터 전송은 두 개의 위성과 지상 게이트웨이를 거치는 구조이며, 각 구간은 도청자(Eve)에 의해 공격당할 수 있다고 가정한다. 중계 방식은 디코드-포워드(Decode-and-Forward, DF) 방식으로, 각 홉에서 수신된 신호는 복호화 및 재암호화를 거쳐 다음 구간으로 전달된다. 이때 전체 링크의 보안 성능은 가장 취약한 홉의 영향을 받으므로, 다운링크 중 최소 보안 성능을 기준으로 시스템을 평가한다. 본 연구는 지상 게이트웨이 수가 증가할수록 보안 성능에 어떤 영향을 미치는지를 분석하기 위한 모델을 구성하고 시뮬레이션을 통해 그 변화를 관찰한다.

2) 채널 모델

위성 통신 환경에서 물리 계층 보안 성능을 분석하기 위해 빔 이득(beam gain)을 고려한다. SISO 기반 시스템에서의 beam gain은 다음과 같이 표현된다[3].

$$b(\varphi) = \left(\frac{J_1(u)}{2u} + 36 \frac{J_3(u)}{u^3} \right)^2 \quad (1)$$

여기서 u 는 다음과 같이 정의된다.

$$u = 2.07123 \frac{d}{R} \quad (2)$$

R 은 빔 반지름, d 는 빔 중심과 수신기 간 거리이다. 위의 빔 이득을 기반으로 신호의 공간 감쇠를 모델링할 수 있다. 또한 채널의 페이딩 특성을 정밀하게 반영하기 위해 시뮬레이션에는 Shadowed-Rician (SR) 채널 모델을 사용한다. SR 모델은 위성 링크의 특성을 잘 설명하며, 다양한 주파수 대역에 적용 가능하다. 채널 벡터의 구성은 다음과 같다.

$$\mathbf{g} = \bar{\mathbf{g}} + \tilde{\mathbf{g}}, \mathbf{g} \sim SR(\Omega, b, m) \quad (3)$$

$\bar{\mathbf{g}}$ 는 LoS 성분으로 Nakagami- m 분포를 따르며 $\tilde{\mathbf{g}}$ 는 산란 성분으로 Rayleigh fading을 따른다. Ω 는 LoS 성분의 평균 전력, b 는 다중경로 성분의 평균 전력, m 은 Nakagami- m 분포의 심도 파라미터이다. 최종적으로 빔 이득 계수 b 와 채널 벡터 \mathbf{g} 를 결합한 전체 채널 모델 h 와 수신기에서의 SNR은 다음과 같이 정의된다.

$$h = \sqrt{b(\varphi)} \mathbf{g}, \gamma = \frac{P}{\sigma^2} |h|^2 \quad (4)$$

3) 보안 성능 지표 정의

본 논문에서는 RF 기반 위성-지상-위성 시스템의 보안 성능을 평가하기 위해 비밀률(Secrecy Rate), 비영 보안 용량 확률(Probability of Non-Zero Secrecy Capacity, PNZSC), 보안 아웃티지 확률(Secrecy Outage Probability, SOP), 평균 보안 용량(Average Secrecy Capacity, ASC)을 사용한다. Alice-Bob-Eve 구조의 와

이러한 채널에서 비밀율은 다음과 같이 정의된다[3].

$$C_S = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \leq \gamma_E \end{cases} \quad (5)$$

여기서 $C_B = \log_2(1 + \gamma_B)$, $C_E = \log_2(1 + \gamma_E)$ 는 각각 Bob 과 Eve 의 채널 용량을 의미한다. PNZSC 는 비밀 용량이 0 이 아닐 확률을 의미하며, Bob 의 채널 상태가 Eve 보다 좋을 확률이다. 시스템의 보안성 확보 가능성을 평가하는 지표가 된다. Nakagami-m 분포를 따르는 PNZSC 의 이론식은 다음과 같다.

$$PNZSC = Pr(\gamma_B > \gamma_E) = \left[1 - \left(\frac{m/\gamma_B}{m/\gamma_B + 1/\gamma_E} \right)^m \right]^R \quad (6)$$

SOP 는 주어진 목표 비밀율 R_S 보다 실제 비밀 용량이 낮을 확률을 의미한다. 보안 통신 실패 가능성을 나타낸다.

$$SOP = Pr(C_S < R_S) = Pr(C_B - C_E < R_S) \quad (10)$$

$$= 1 - \left[1 - \int_0^\infty F_{\gamma_B}((1 + \gamma_E)2^{R_S} - 1) f_{\gamma_E}(\gamma_E) d\gamma_E \right]^R$$

ASC 평균 비밀 용량으로, 평균적인 보안 전송 성능을 보여준다.

$$ASC = E[C_S] \quad (12)$$

$$= \int_0^\infty \int_0^\infty C_S(\gamma_B, \gamma_E) f_{\gamma_B, \gamma_E}(\gamma_B, \gamma_E) d\gamma_B d\gamma_E$$

4) 시뮬레이션 결과

지상 게이트웨이 수의 변화에 따른 보안 성능을 분석하기 위해 몬테카를로(Monte Carlo) 시뮬레이션을 수행하였다. SR 모델은 이론값 도출이 복잡하므로, 보다 간단한 Nakagami-m 모델을 활용해 이론값을 계산하고, 이를 SR 기반 몬테카를로 결과와 비교하여 성능 차이를 분석하였다. 또한 Nakagami-m 모델에 대해서도 시뮬레이션을 수행하여 이론값과의 일치 여부를 확인하였다. 시뮬레이션에서는 DF 중계 방식을 적용하고, 지상 릴레이 수를 1 개, 2 개, 3 개로 설정하여 각 경우의 보안 성능(PNZSC, SOP, ASC)을 평가하였다.

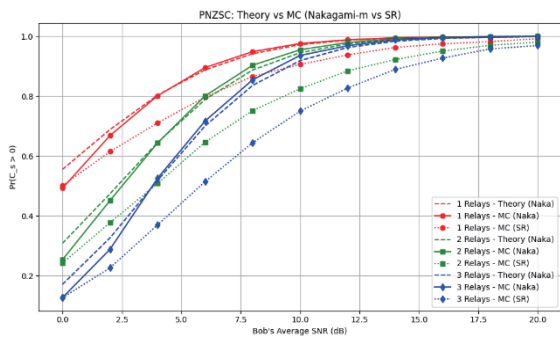


그림 1 PNZSC 시뮬레이션 결과

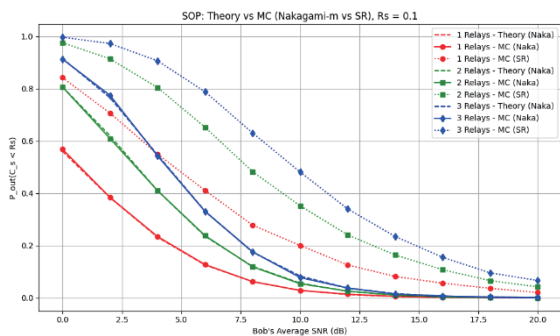


그림 2 SOP 시뮬레이션 결과

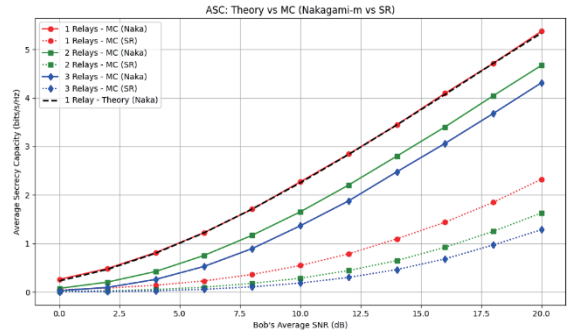


그림 3 ASC 시뮬레이션 결과

각 그래프(그림 1~3)는 표 1의 파라미터를 기반으로 생성되었으며, Nakagami-m 모델을 활용한 이론값과 동일 모델 및 SR 모델 기반 몬테카를로 시뮬레이션 결과가 유사함을 확인하였다. 세 그래프 모두 Bob의 평균 SNR이 증가할수록 보안 성능이 향상되었고, 릴레이 수가 많을수록 성능은 저하되었다. 이는 중계 구간 증가에 따른 보안 취약 구간 확대로 해석된다. 또한 SR 모델 결과는 Nakagami-m과 유사한 경향을 보였으나 전반적으로 낮은 성능을 나타냈으며, 이는 산란 성분으로 인한 불확실성 증가에 기인한 것으로 판단된다.

파라미터	기호	값
Nakagami	m	2
수평 거리	d	1000 [m]
위성 코드 [LEO]	R	500 [km]
SOP 임계치	R_S	0.1 [bits/s]
SR LoS 성분	Ω	8.97×10^{-4}
SR 산란 강도	b	0.063
Eve 평균 세기	$\bar{\gamma}_E$	0 [dB]

표 1 시뮬레이션 파라미터 값

III. 결론

본 논문에서는 RF 기반 위성-지상-위성 통신 시스템에서 지상 릴레이 수가 보안 성능에 미치는 영향을 분석하였다. 시뮬레이션 결과, Bob의 평균 SNR이 증가할수록 보안 성능은 향상되었으며, 릴레이 수가 많아질수록 보안 취약 구간이 늘어나 PNZSC는 감소하고 SOP는 증가하는 경향을 보였다. 이는 홉 수 증가가 전체 링크의 보안 성능을 저하시킬 수 있음을 보여준다. 본 연구는 릴레이 구성에 따른 보안 성능 변화를 정량적으로 분석하였으며, 향후 FSO 링크를 포함한 멀티 홉 구조에서의 보안 성능을 평가하고, 보다 효율적인 릴레이 배치 전략 도출을 목표로 한다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2021-0-00260, 저궤도 군집 소형 위성 간 통신 기술 개발)

참고 문헌

- [1] J. Lei, Z. Han, M. A. Vázquez-Castro, and A. Hjørungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.
- [2] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, 2016.
- [3] K. An, T. Liang, X. Yan, and G. Zheng, "On the secrecy performance of land mobile satellite communication systems," *IEEE Access*, vol. 6, pp. 39 606–39 620, Aug. 2018.