https://doi.org/10.7840/kics.2025.50.11.1730

저궤도 위성 네트워크에서 위장 공격에 따른 핸드오버 실패 확률 분석

하 승 철◆, 이 용 재*,
채 승 호**, 김 태 훈***, 방 인 규°

Analysis of Handover Failure Probability Against Impersonation Attacks in LEO Satellite Networks

SeungCheol Ha◆, Yongjae Lee*,
Seong Ho Chae**, Taehoon Kim***,
Inkyu Bang°

요 약

저궤도 위성(Low Earth Orbit: LEO) 통신은 글로벌 연결성과 낮은 지연 시간 등 향후 6G 비지상 네트워크를 구축하기 위한 핵심 기술로 주목받고 있다. 그러나 위성 네트워크에서는 위성의 빠른 이동으로 인해 빈번한 핸드오버(handover)가 발생하며 이는 다양한 보안 위협으로 이어질 수 있다. 본 논문에서는 위성 네트워크에서 허위 기지국(fake base station)이 위성과 지상국의 핸드오버를 탈취하는 위장 공격의 가능성을 분석하고 핸드오버 실패 확률을 모델링한다. 또한, 핸드오버 실패 확률을 수학적으로 분석하여 위성 네트워크에서의 보안 취약점을 평가하고 저궤도 위성 통신의 보안성을 강화하기 위한 대응 방안을 논의한다.

Key Words : Low Earth orbit (LEO), satellite network, handover, impersonation attack, handover failure probability

ABSTRACT

Low Earth Orbit (LEO) satellite communications have become one of the key technologies for future 6G non-terrestrial networks due to their global connectivity and low latency. However, frequent handovers in LEO satellite networks could initiate severe security threats. In this paper, we investigate the feasibility of the impersonation attack by a fake base station, which hijacks the legitimate handover between a satellite and a ground base station. Further, we analyze a handover failure probability and discuss potential countermeasures to enhance the security of the LEO satellite handover procedure.

Ⅰ. 서 론

저궤도 위성(LEO)은 상대적으로 지구와 가까운 300km~2,000km 궤도 위에서 이동하기 때문에 지연 시간이 짧고 신호 강도가 높아 기존 위성 통신보다 안정적인 통신 성능을 제공할 수 있다. 또한, 저궤도 위성 통신은 기존의 지상 네트워크 기반 통신을 보완하며, 농촌·해양·극지방과 같은 음영 지역에서도 안정적인 연결성을 제공할 수 있어, 6G 이동통신의 핵심 기술로 주목받고 있다[1].

저궤도 위성 네트워크에서는 저궤도 위성의 상대적으로 낮은 고도와 빠른 이동속도로 인해 핸드오버가 빈번히 발생한다. 이러한 핸드오버 과정에서 허위 기지국(fake base station)이 위성을 목표 삼아 정상 지상국을 모방하는 위장(impersonation) 공격을 수행할 경우, 해당 위성은 중간자(MitM) 공격이나 서비스 거부(DoS) 공격 등 다양한 보안 위협에 노출될 수 있다[2,3]. 따라서 저궤도 위성의 핸드오버 과정 중에 발생할 수 있는 보안 위협의 가능성을 분석하고 이를 토대로 위성 통신의 보안성을 강화하는 연구가 필요하다.

※ 이 논문은 2022년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원(KRIT-CT-22-047, 우주계층 지능통신망 특화연구실)과 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. RS-2024-00444170, 6G 개방형 네트워크 환경에서 트러스트 모델 기반 지능형 침해대응 기술 연구 및 국제협력,50%)을 받아 수행된 연구임(IITP-2025-RS-2024-00437886, 50%).
◆ First Author : (ORCID:0009-0006-3019-8902) Hanbat National University, Dept. of Intelligence Media Engineering, scha@edu.hanbat.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0001-7109-1999) Hanbat National University, Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 부교수, 종신회원
* (ORCID:0009-0008-3157-7634) Hanbat National University, Dept. of Intelligence Media Engineering, yjlee@edu.hanbat.ac.kr, 학생회원
** (ORCID:0000-0001-9092-5039) Tech University of Korea, Dept. of Electronics Engineering, shchae@tukorea.ac.kr, 부교수, 종신회원
*** (ORCID:0000-0002-9353-118X) Hanbat National University, Dept. of Computer Engineering, thkim@hanbat.ac.kr, 부교수, 종신회원
논문번호 : 202506-141-B-LU, Received June 18, 2025; Revised July 4, 2025; Accepted July 4, 2025

본 논문에서는 허위 기지국이 위성과 지상국의 핸드오버를 탈취하는 위장 공격의 가능성을 분석하고 핸드오버 실패 확률을 모델링한다. 또한, 핸드오버 실패 확률을 수학적으로 분석하여 위성 네트워크에서의 보안 취약점을 평가하고 저궤도 위성 통신의 보안성을 강화하기 위한 대응 방안을 논의한다. 본 논문의 신규성과 주요 기여점을 요약하면 다음과 같다.

① 본 논문에서는 이동통신 네트워크에서 허위 기지국 기반의 핸드오버 실패 공격이 가능하다는 기존의 실험 결과를 바탕으로 위성 네트워크에서 핸드오버 실패 확률을 모델링한다. ② 본 논문에서는 Nakagami-m 채널 모델을 가정했을 때, 가우시안 근사를 활용하여 핸드오버 실패 확률을 분석한다. ③ 본 논문에서는 저궤도 위성 네트워크 환경을 고려한 모의실험을 통해 핸드오버 실패 확률 분석 결과를 검증하고 대응 방안으로 안테나 선택 기법이 사용되는 경우에 대한 결과를 함께 논의한다.

Ⅱ. 시스템 모델

본 장에서는 저궤도 위성, 지상국, 허위 기지국 등을 가정하는 시스템 모델에서 각각의 변수와 허위 기지국에 의한 핸드오버 실패 공격의 과정을 논의한다.

2.1 시스템 환경 변수

본 논문에서는 그림 1과 같이 저궤도 위성, 지상국(Ground Base Station: GBS) 및 허위 기지국(fake BS)이 존재하는 비지상 네트워크에서 저궤도 위성이 핸드오버를 수행하는 상황을 가정한다. 저궤도 위성은 소스 지상국(source GBS)으로부터 서비스를 받으며, 핸드오버를 위해 주변 지상국과의 채널 상태를 측정하고 소스 지상국에게 보고(measurement report: MR)한다. 허위 기지국은 공격 목표인 저궤도 위성이 채널 상태를 측정할 수 있도록 파일럿 신호를 전송한다.

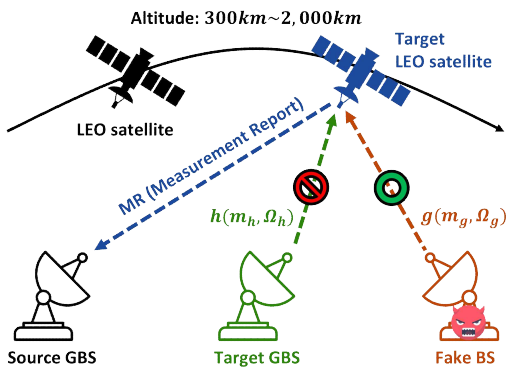

그림 1. 허위 기지국이 존재하는 위성 네트워크 예시
Fig. 1. A satellite network with fake BS

본 논문에서는 위성과 지상국 사이의 채널 계수를 형상(shape) 매개변수 m_h, m_g와 척도(scale) 매개변수 Ω_h, Ω_g를 갖는 Nakagami-m 분포로 가정한다. Nakagami-m 채널 모델은 저궤도 위성 통신 관련 연구에서 많이 사용되고 있는 채널 모델로 형상 매개변수와 척도 매개변수 값을 통해 가시성(LoS)과 비가시성(NLoS)의 영향 및 위성 고도에 따른 대규모 페이딩(Large-scale fading)의 영향을 반영할 수 있다[4],[5]. 본 논문에서 가정하는 저궤도 위성 네트워크 모델의 주요 특징(지상 네트워크 대비 차별점 등) 및 구체적인 변수 값 등은 각 세부 절에서 논의한다.

2.2 핸드오버 실패 공격

허위 기지국은 목표 저궤도 위성의 핸드오버 절차를 악용하여 위성과 목표 지상국(target GBS) 사이의 새로운 연결을 방해하고 허위 기지국과 강제로 연결되는 핸드오버 실패 공격을 수행한다. 지상 네트워크에서 3GPP 기반의 핸드오버 절차를 악용하는 공격 사례는 SDR (software-defined radio) 장비를 사용하여 실험적으로 연구된 바 있다[3]. 본 연구에서는 기존 연구의 실험적 결과를 3GPP 기반 비지상 네트워크(즉, 위성 네트워크)로 확장하여 핸드오버 실패 공격에 필요한 절차를 논의한다. 본 연구의 주요 목표는 핸드오버 실패 공격의 수학적 모델링과 이에 대한 대응 방안을 논의하는 것이다.

그림 2는 위성 네트워크에서 3단계로 구성되는 핸드오버 실패 공격 과정의 예시를 나타낸다. 공격의 각 단계에 대한 설명은 다음과 같다.

소스 지상국은 해당 MR 정보와 새로운 지상국의 PCI (physical cell identity)를 확인하고 최종 핸드오버를 결정한다. 이 과정에서 허위 기지국은 기존 지상국으로 위장하여 MR 정보와 PCI 정보를 기만할 수 있다[3]. 소스 지상국은 핸드오버 준비 단계로 RRC (radio resource control) 연결 재설정 절차를 시작한다.

1단계: 허위 기지국은 목표(target) 저궤도 위성이 핸드오버를 준비하는 과정에서 핸드오버 실패 공격을 시작한다. 저궤도 위성은 주변 지상국의 채널 상태를 측정 및 보고(MR)하여 소스 지상국에게 전달한다.

2단계: 허위 기지국은 기존 지상국의 정보를 이용하여 핸드오버 완료를 위해 필수적인 RRC 재설정 요청을 거부하고 RRC 연결 해제 메시지를 위성에 전달하여 최종적으로 핸드오버 실패를 강제한다. RRC 재설정 거부 메시지와 RRC 연결 해제 메시지는 일반적인 핸드오

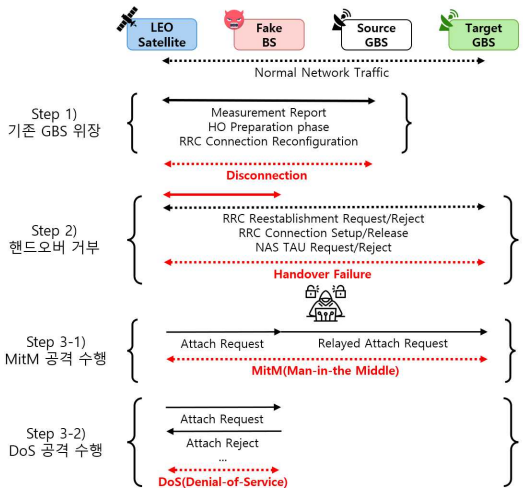

그림 2. 핸드오버 실패 공격 절차 예시
Fig. 2. Handover failure attack procedure

버 실패 과정에서도 발생하기 때문에 핸드오버 프로토콜에서 위성이 해당 메시지의 진위 여부를 구분하는 것은 어려운 상황이다[3].

3단계: 핸드오버 실패 공격 이후 허위 기지국은 다양한 추가 공격을 수행하여 위성 네트워크에 추가적인 피해를 유발할 수 있다. 대표적으로 다음과 같이 중간자 공격과 서비스 거부 공격을 생각할 수 있다.

3-1) 중간자 공격(MitM): 허위 기지국은 위성과 타겟 지상 기지국 간의 신호를 가로채어 중계함으로써, 위성과 지상국 간의 통신을 감청 및 위조할 수 있다.

3-2) 서비스 거부 공격(DoS): 허위 기지국은 연결 요청(Attach Request)에 대해 연결 거절 응답(Attach Reject)을 반복하여, 위성이 정상적인 네트워크 접속을 하지 못하도록 방해할 수 있다.

Ⅲ. 핸드오버 실패 확률 분석

본 장에서는 핸드오버 실패 공격을 수학적으로 모델링한다. 허위 기지국은 저궤도 위성이 핸드오버 과정 중에 선택하려는 지상국보다 더 좋은 위성과의 채널 상태가 측정되도록 MR 정보를 기만하여 허위 기지국이 더 좋은 핸드오버 후보가 될 수 있도록 한다. 허위 기지국이 PCI 정보 위조에 성공했다고 가정했을 때, 핸드오버 실패는 지상국 신호와 허위 기지국 신호의 유효 SNR (signal-to-noise ration) 차이에 따라 결정된다. 따라서 핸드오버 실패 확률(handover failure probability)을 다음과 같이 정의할 수 있다.

$$p_f = \Pr\left[|g|^2 \frac{P_0}{\sigma^2} \geq |h|^2 \frac{P_t}{\sigma^2} + \delta \right], \quad (1)$$

여기서 P_t와 P_0는 각각 정상 지상국과 허위 기지국의 송신 전력, σ^2은 평균 잡음 전력 그리고 δ은 SNR 차이의 여유 값(margin)을 나타낸다.

수식 (1)의 $|h|^2$와 $|g|^2$는 각각 형상 매개변수 m_h, m_g와 척도 매개변수 Ω_h/m_h, Ω_g/m_g을 갖는 감마(Gamma) 분포를 따른다. 따라서 핸드오버 실패 확률 p_f는 서로 독립인 두 감마 확률 변수의 차의 누적 분포 함수(CDF)로 표현이 된다. 일반적으로 두 감마 확률 변수의 차의 누적분포에 관한 연구가 많이 논의되고 있으나 특정 매개변수 조합을 제외한 경우에 대해서는 해당 CDF를 닫힌 형태(closed-form)로 유도하는 것이 불가능하다고 알려져 있다[6]. 본 연구에서는 이를 근사적으로 해결하고자 가우시안(Gaussian) 근사를 사용한다. m_h, m_g 값이 큰 경우에, 각각의 감마 분포는 평균이 Ω_h, Ω_g이고 분산이 Ω_h^2/m_h, Ω_g^2/m_g인 가우시안 분포로 근사된다. 위성 통신에서는 LoS의 영향이 크기 때문에 m_h, m_g 값이 적당히 큰 상황을 가정할 수 있다. 최종적으로 표준 정규 분포의 CDF를 $\Phi(x)$으로 정의할 때 p_f의 근사 값은 다음과 같다.

$$p_f \approx 1 - \Phi\left(\frac{\frac{\delta}{P_0} - \left(\Omega_h - \frac{P_t}{P_0}\Omega_g \right)}{\sqrt{\frac{\Omega_h^2}{m_h} + \left(\frac{P_t}{P_0}\right)^2 \frac{\Omega_g^2}{m_g}}} \right). \quad (2)$$

Remark 1: 본 논문에서 논의한 핸드오버 실패 확률 분석은 채널 모델 가정에 따라 다양한 상황에서 적용 가능한 분석 방법이다. 그러나 저궤도 위성의 빠른 움직임과 글로벌 커버리지로 인해 핸드오버 실패로 인한 영향은 일반 지상 네트워크에 비해 저궤도 위성 네트워크에서 훨씬 클 것으로 예상된다. 따라서 안정적인 저궤도 위성 네트워크 서비스 제공을 위한 설계 기준으로 핸드오버 실패 확률 분석 결과를 활용할 수 있을 것이다. 또한, 본 논문의 결과를 확장하여 핸드오버 실패 확률이 글로벌 커버리지에 미치는 영향을 종합적 고려한 서비스 중단 확률(outage probability) 등을 분석하는 향후 연구 방향을 생각해 볼 수 있다.

Remark 2: 본 논문에서 논의한 핸드오버 실패 공격은 핸드오버의 측정보고(MR) 단계에서 위성에서 측정되는 지상국 신호의 유효 SNR (effective SNR) 값에 영향

을 받는다. 따라서 안테나 다양성(antenna diversity)을 활용한 기술을 이용하여 측정보고 단계에서 측정되는 유효 SNR 값을 증가시킬 경우 핸드오버 실패 확률을 줄일 수 있을 것이다. 예를 들어, 다중 안테나 탑재를 가정할 경우, 안테나 선택(antenna selection) 기법 등을 적용하여 MR 단계에서 유효 SNR 값을 증가시킬 수 있을 것이며[6], 이 경우 수식 (1)의 핸드오버 실패 확률은 다음과 같이 표현된다.

$$p_f = \Pr\left[|g|^2 \frac{P_0}{\sigma^2} \geq \max|h_i|^2 \frac{P_t}{\sigma^2} + \delta\right], \qquad (3)$$

여기서 h_i는 다중 안테나 탑재를 가정했을 때 안테나 인덱스 i의 채널 계수를 의미한다.

Ⅳ. 모의실험

본 장에서는 모의실험을 통해 수식 (2)의 분석 결과를 검증한다. 모의실험에서는 표 1의 변수 값을 사용한다. 또한, 허위 기지국의 핸드오버 실패 공격에 대해서 핸드오버 실패 확률을 줄이기 위한 대응 방안으로 안테나 선택 기법이 사용되는 경우에 대한 모의실험 결과를 함께 논의한다.

그림 3은 저궤도 위성과 허위 기지국 사이의 SNR이 10 dB일 때, 위성과 지상국 사이의 SNR 값 변화에 따른 핸드오버 실패 확률을 나타낸다. Ω_h과 Ω_g은 10 dB로 설정했으며, m_h, m_g은 동일하게 1, 5, 10의 값으로 설정했다. 논의한 바와 같이 m_h, m_g의 값이 클수록 근사의 정확도가 높아진다. 위성과 지상국 사이의 SNR 값이 증가할수록 핸드오버 실패 확률이 감소하는 것을

표 1. 모의실험 관련 변수
Table 1. Simulation Parameters

Parameter	Value
Carrier frequency f_c (GHz)	30
Transmit power P (dBm)	30
Path-loss exponent α	2
Nakagami shape parameter m	1, 2, 5, 10
LEO orbit altitude h (km)	600
Noise spectral density N_0 (dBm/Hz)	-174
Speed of light c (m/s)	3×10^8
Maximum antenna gain $G = G_t = G_r$ (dBi)	40
EIRP (dBW)	40

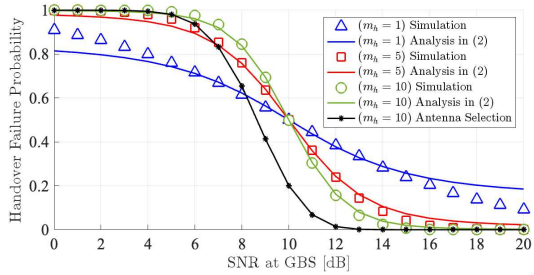

그림 3. GBS의 SNR 변화에 따른 핸드오버 실패 확률
Fig. 3. Handover failure probability with SNR

확인할 수 있다. 핸드오버 실패 공격의 대응 방안을 논의하기 위해 안테나 선택 기법(4개)을 추가적으로 실험하였다. 안테나 다양성으로 인해 핸드오버 실패 확률이 감소하는 것을 확인할 수 있다.

그림 4은 저궤도 위성과 허위 기지국 사이의 SNR 및 위성과 지상국 사이의 SNR 값 변화에 따른 핸드오버 실패 확률을 나타낸다. Ω_h과 Ω_g은 10 dB로 설정했으며, m_h, m_g은 동일하게 2의 값으로 설정했다. 지상국에서 수신되는 SNR이 높고 허위 기지국의 SNR이 낮은 경우(오른쪽 하단 영역)에는 핸드오버 실패 확률이 0에 가까운 값으로 수렴하고 허위 기지국의 SNR이 지상국보다 상대적으로 높은 상황(왼쪽 상단 영역)에서는 핸드오버 실패 확률이 1에 근접하는 것을 확인할 수 있다. 또한, 두 SNR이 유사한 상황에서는 핸드오버 실패 확률이 0.5 값을 지니는 것을 확인할 수 있다. 모의실험 결과를 활용하여 위성 네트워크 설계 단계에서 핸드오버 실패의 위협성을 분석하고 이를 토대로 핸드오버 실패 공격을 예방하기 위해 지상국에서 필요한 최소 수신 SNR을 정략적으로 계산할 수 있다.

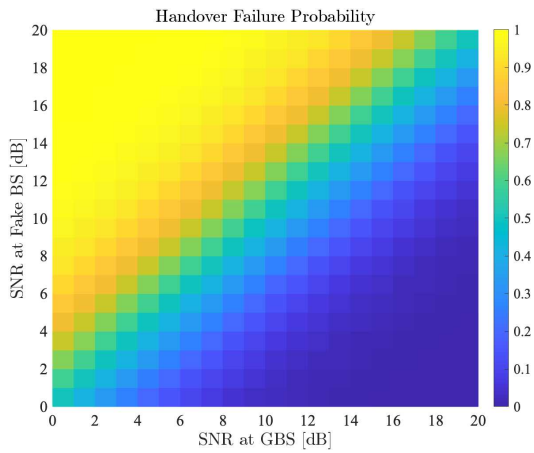

그림 4. SNR 변화에 따른 핸드오버 실패 확률
Fig. 4. Handover failure probability with SNR

V. 결 론

본 논문에서는 허위 기지국의 위장 공격에 기반한 핸드오버 실패 공격을 조사하고 핸드오버 실패 확률을 수학적으로 모델링하고 분석하였다. 또한, 다중 안테나 기술이 하나의 대응 방안으로 사용될 수 있다는 것을 모의실험을 통해 확인하였다.

References

[1] Z. Xiao, et al., "LEO satellite access network (LEO-SAN) toward 6G: Challenges and approaches," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 89-96, Apr. 2024.

[2] P. Yue, et al., "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE Commun. Surv. & Tuts.*, vol. 25, no. 3, pp. 1604-1652, Thirdquarter 2023.

[3] E. Bitsikas and C. Pöpper, "Don't hand it over: Vulnerabilities in the handover procedure of cellular telecommunications," *ACSAC*, 2021.

[4] J. Park, et al., "A tractable approach to coverage analysis in downlink satellite networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 793-807, Feb. 2023.

[5] A. Ospanova, et al., "Delay-outage analysis of multi-LEO satellites communication system," *IEEE Access*, vol. 11, pp. 124509-124523, Nov. 2023.

[6] P. J. Forrester, "On the gamma difference distribution," in *ELSEVIER Statistics and Probability Lett.*, vol. 211, pp. 1-7, Aug. 2024.

[7] M. Can, et al., "Joint transmit and receive antenna selection in MIMO-NOMA-based uplink satellite networks," in *IEEE Sensors J.*, vol. 24, no. 15, pp. 24841-24850, Aug. 2024.