2025년도 한국통신학회 하계종합학술발표회

Secure Radio Resource and Routing Optimization in Multi-Hop Space-Air-Ground-Sea Integrated Networks

Lyu Hyeonsu[1], Noh Hyeonho[2], Yang Hyun Jong[2,*]
[1]POSTECH, [2]Seoul National University
hslyu4@postech.ac.kr, {hyeonho, hjyang}@snu.ac.kr

다중 홉 우주-공중-지상-해양 통합 네트워크에서의 보안 무선 자원 및 라우팅 최적화 기법에 관하여

류현수 [1] 노현호 [2], 양현종 [2,*]
[1] 포항공과대학교, [2] 서울대학교

Abstract

This paper addresses secure radio resource and routing optimization in multi-hop space-air-ground-sea integrated networks (SAGSINs). We formulate a cross-layer optimization problem that maximizes the minimum user throughput while guaranteeing a strictly positive secure connection (SPSC) probability on each hop. A closed-form expression for the single-hop SPSC probability is derived, enabling efficient enforcement of security constraints. An optimal power and frequency allocation strategy and a Monte-Carlo based relay routing algorithm are proposed. Simulation results show that the framework achieves robust secrecy and high throughput even under dense eavesdropper distributions.

Ⅰ. Introduction

Space-air-ground-sea integrated networks (SAGSINs) are a key enabler of future 6G wireless systems, offering ubiquitous and seamless connectivity [1,4]. However, their multi-tiered, large-scale nature significantly amplifies the risk of passive eavesdropping, making end-to-end secure communication across multi-hop relays a major challenge. Existing studies mostly address two-hop scenarios or assume partial knowledge of eavesdropper (Eve) channels, limiting their applicability to practical SAGSIN environments [5]. In this paper, we formulate a cross-layer optimization framework that jointly designs multi-hop relay routing and radio resource allocation under a strictly positive secure connection (SPSC) probability constraint. Our framework maximizes the minimum user throughput while ensuring physical-layer security against randomly distributed Eves, without requiring Eve's channel state information (CSI).

Ⅱ. Problem Formulation and Proposed Solution

We consider a multi-hop SAGSIN where users connect to a core gateway node via satellite, high-altitude platform, ground, and maritime relays. Each relay operates in half-duplex decode-and-forward mode and can split its transmit power between data transmission and cooperative jamming to degrade eavesdropper channels. Passive eavesdroppers are spatially distributed following a Poisson point process. To ensure security without Eve's CSI, we introduce the strictly positive secure connection (SPSC) probability, defined as the probability that the secrecy capacity of a link is positive.

Our goal is to maximize the minimum user throughput under SPSC constraints. The throughput for a user is determined by the bottleneck hop along its multi-hop path. The joint optimization variables include routing (link selection), bandwidth allocation, and power splitting between data and jamming.

Let $\mathcal{N}$ be the set of relay nodes and $\mathcal{U}$ the set of users. Each link between nodes i and j is denoted by (i,j), with corresponding link capacity $\gamma_{(i,j)}$ and bandwidth allocation $\beta_{(i,j),u}$ for user u. The total power at node i is split into data transmission power ρ_i and cooperative jamming power σ_i. The relay path for each user u is composed of a set of links $\mathcal{E}_u$, with the number of hops denoted by h_u.

The main problem is formulated as

$$\textbf{Problem 1: } \max_{\mathcal{G},\mathbf{B},\mathbf{P},\mathbf{J}} \min_{\substack{u\in\mathcal{U}\\(i,j)\in\mathcal{E}_u}} \frac{\beta_{(i,j),u}\gamma_{(i,j)}}{h_u}$$
$$s.t.\ x_{(i,j)}\mathbb{P}_{(i,j)} \geq \tau,$$
$$\Sigma_{j\in\mathcal{N}}\Sigma_{u\in\mathcal{U}}\beta_{(i,j),u} \leq B,\ \rho_i+\sigma_i \leq P,$$
$$\beta_{(i,j),u} \geq 0, \rho_i \geq P_i, \sigma_i \geq 0,$$

for $\mathbf{B}=\{\beta_{(i,j),u}: (i,j)\in\mathcal{N}, u\in\mathcal{U}\}$, $\mathbf{P}=\{\rho_i: i\in\mathcal{N}\}$, and $\mathbf{J}=\{\sigma_i: i\in\mathcal{N}\}$.

The secure connection probability $\mathbb{P}_{(i,j)}$ of a link (i,j) is defined as the probability that the legitimate channel's instantaneous secrecy capacity is positive, i.e., the signal-to-noise ratio (SNR) at the legitimate receiver exceeds that at any eavesdropper. Assuming that the eavesdroppers are randomly distributed according to a homogeneous Poisson point process (HPPP) with a given density, we derive a closed-form expression for $\mathbb{P}_{(i,j)}$ as

Disclaimer:
This work is based on partial results from a manuscript currently under review for possible publication in IEEE.

$$\mathbb{P}_{(i,j)} = \exp\left[-\pi\lambda_i \sin^{-1}\left(\frac{2\pi}{\alpha_i}\right)\left(\frac{n_0}{\sigma_i + n_0}\right)^{\frac{2}{\alpha_i}} d_{(i,j)}^2\right],$$

where λ_i is Eve density, α_i is pathloss exponent of node i, and $d_{(i,j)}$ is distance of a link (i,j) [1].

The optimal solution of **Problem 1** then can be obtained from the Karush-Kuhn-Tucker conditions as

$$\beta^*_{(i,j),u} = B\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}}\left(\sum_{\substack{j\in\mathcal{N},\\ u\in\mathcal{U}}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}}\right)^{-1},\ \rho_i = P - \tau_i,\ \sigma_i = \tau_i$$

for $\tau_i = n_0\left(\frac{\pi\lambda_i \sin^{-1}\left(\frac{2\pi}{\alpha_i}\right)d^2}{-\ln\tau}\right)^{\alpha_i/2} - n_0$ and $d = \max x_{(i,j)}d_{(i,j)}$.

To efficiently solve the routing problem under the SPSC constraint, we propose a Monte-Carlo based relay routing strategy. The algorithm constructs multiple random relay paths for each user by sequentially selecting feasible links that satisfy the SPSC condition. For each sampled path, optimal bandwidth and power allocations are computed in closed form. Among the sampled paths, the one achieving the highest minimum user throughput is selected. This randomized approach significantly reduces complexity while achieving near-optimal performance compared to exhaustive search.

Table I. Simulation Parameters

Parameter (Unit)	Ground (G), Maritime (M), HAPs (H)	LEO
Carrier frequency (GHz)	14	20
Total bandwidth (MHz)	250	400
Tx power (dBm)	30	21.5
Tx antenna gain (dBi)	43.2 (G,M,H→LEO), 25 (G,M,H→G,M,H)	38.5
Rx antenna gain (dBi)	39.7 (G,M,H→LEO), 25 (G,M,H→G,M,H)	38.5
Antenna gain to noise temperature (dB/K)	1.5 (H→LEO), 16.2 (H→G,M,H), 1.2 (G,M→LEO), 15.9 (G,M→G,M,H)	13
Pathloss exponent	2.8 (G), 2.7 (M), 2.6 (H)	2.4

III. Problem Formulation

The simulations are conducted based on a realistic SAGSIN with randomly located users. The physical-layer parameters in Table I are configured following 3GPP standards [2] and existing literature [3, 4]. The SPSC probability threshold is set to 99.99%.

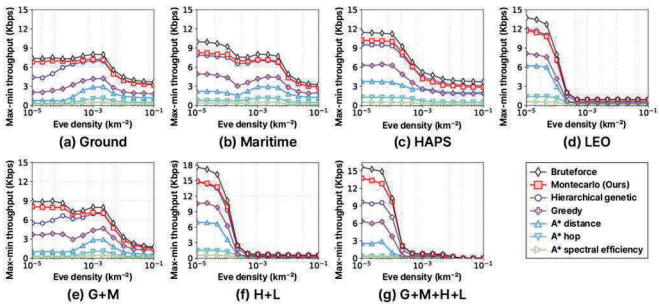

Fig. 1. Max-min throughput versus Eve density for various SAGSIN scenario. Each graph reports the max–min throughput while varying the Eve density of the infrastructure layer indicated in the caption, with the other layers fixed at $(\boldsymbol{\lambda_1, \lambda_2, \lambda_3, \lambda_4}) = (\mathbf{10^{-3}, 2\cdot 10^{-3}, 3\cdot 10^{-4}, 10^{-4}})$. Notations **G+M**, **H+L**, and **G+M+H+L** in (e), (f), and (g) correspond to ground and maritime; HAPs and LEO; and ground, maritime, HAPs and LEO, respectively.

We evaluate the proposed framework through simulations in a multi-layer SAGSIN environment with randomly distributed users and eavesdroppers. The results demonstrate that the proposed cross-layer optimization significantly improves the minimum user throughput while ensuring a high SPSC probability under varying eavesdropper densities. As shown in Fig. 1, the throughput increases notably when the density of eavesdroppers in the high-altitude layers, such as HAPs and LEO satellites, is reduced. This indicates that securing long-distance links in higher layers has a critical impact on overall network performance. Furthermore, the Monte-Carlo based relay routing approach achieves near-optimal throughput performance with substantially lower computational complexity compared to exhaustive search. Overall, the proposed solution provides an effective and scalable framework for ensuring secure and efficient communications in future large-scale integrated networks.

IV. Problem Formulation

Overall, the proposed cross-layer framework ensures secure and efficient multi-hop communications in large-scale SAGSINs. By optimally combining resource allocation and Monte-Carlo based routing, it achieves high throughput while satisfying stringent secrecy requirements. This highlights its scalability and effectiveness for future 6G integrated networks.

ACKNOWLEDGMENT

This research was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-2021-0-02048) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), in part the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2025-2023-00250191), and in part by IITP grant funded MSIT (No. RS-2025-2024-00404972, Development of 5G-A vRAN Research Platform).

REFERENCE

[1] H. Lyu, H. Noh, H. J. Yang, and K. Chowdhury, "Secure Multi-Hop Relaying in Large-Scale Space-Air-Ground-Sea Integrated Networks," arXiv preprint arXiv:2505.00573, May 2025.

[2] 3GPP, "Solutions for NR to support Non-Terrestrial Networks (NTN) - Enhancements in Release 18," 3GPP, Technical Report 3GPP TR 38.821, February 2024.

[3] D. Liu, J. Zhang, J. Cui, S.-X. Ng, R. G. Maunder, and L. Hanzo, "Deep learning aided routing for space-air-ground integrated networks relying on real satellite, flight, and shipping data," IEEE Wireless Commun., vol. 29, no. 2, pp. 177-184, 2022.

[4] M. Vondra, M. Ozger, D. Schupke, and C. Cavdar, "Integration of satellite and aerial communications for heterogeneous flying vehicles," IEEE Netw., vol. 32, no. 5, pp. 62-69, 2018.

[5] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-airground-sea integrated network security in 6G," IEEE Commun. Surveys Tuts., vol. 24, no. 1, pp. 53-87, 2022.