32nd Humantech Paper Awards

Secure Multi-Hop Relaying in Large-Scale Space-Air-Ground-Sea Integrated Networks

(Abstract) We stand at the dawn of ubiquitous connectivity through 6G wireless, but its foundational reliability is threatened by the presence of invisible eavesdroppers (Eves). While the majority of research has relied on the unrealistic assumption of knowing Eve's position and channel state, this study tackles the challenge of secure multi-hop relaying without any Eve channel information. We (i) reformulate the notoriously intractable max-min secrecy-throughput problem into a tractable design, yielding an $\mathcal{O}(1)$ globally optimal radio-resource allocation; (ii) derive a closed-form expression of strictly positive secure connection probability under unknown Eve conditions and validate it across Rayleigh, Rician, and shadowed Rician fading; and (iii) construct the world's first open SAGSIN dataset, integrating SpaceX satellites, Google Loon HAPS, commercial 4G/5G base stations, and maritime vessels to bridge theory with real-world NTNs. This work pioneers a new physical-layer paradigm that guarantees security under uncertainty. It represents a game-changer for secure throughput-aware design in 6G non-terrestrial networks, laying the groundwork for the next era of resilient ubiquitous connectivity. Dataset visualization and appendices are provided in `https://secure-sagsin.github.io/`.

1. INTRODUCTION

The era of hyper-connectivity begins. SpaceX's reusable launch vehicles have paved the way for extending commercial satellite communications to a broader user base [1], and initiatives such as Google's Project Loon [2] and Aerostar's Thunderhead [3] have established the technical foundations for high-altitude platforms (HAPs) networks. Moreover, the advances in sea surface [4] and underwater base stations [5], other forms of borderless networks, signal a big paradigm shift: a global-scale integrated network [6]. NTNs break down national boundaries, lay the groundwork for an interplanetary internet, and provide communication infrastructure across all regions of the Earth. Ubiquitous connectivity in line with this trend has emerged as a primary objective for 6G wireless [7], driving active discussions on standards for non-terrestrial networks [8]–[10]. The integration of these vertical, heterogeneous network layers stands to transcend the limitations of terrestrial networks.

To realize the merits of the space-air-ground(-sea) integrated networks (SAG(S)INs), various technical challenges have been addressed in both industry and academia [11]–[18]. Consequently, numerous techniques have been proposed to combine the complementary strengths of heterogeneous platforms, achieving ubiquitous global coverage and strengthening link reliability [6]. However, the wide communication coverage of SAGSIN and the participation of numerous heterogeneous nodes can intrinsically intensify the possibility of security threat [19], [20]. Safeguarding the integrity and confidentiality of SAGSIN is critical in scenarios where the secrecy requirements are exceptionally high, such as maritime energy transportation and military operations. Moreover, Eves can achieve considerable SNR in SAGSINs as LEO and HAPs emit signals via line-of-sight channels over vast areas, exponentially expanding the attack surface. Therefore, physical-layer security must be employed in SAGSIN to protect information of legitimate users.

Ensuring secrecy for network nodes in SAGSINs presents several technical challenges. Users in the SAGSIN must traverse multiple base station nodes to access the core internet [21]. This indicates that secrecy must be maintained across multiple relay hops, each of which constitutes a potential vulnerability exploitable by adversaries [22]. Numerous studies have explored secure communications in SAGSINs where HAPs serve as intermediate nodes to bridge satellites and ground terminals in two-hop relay systems [11]–[14]. However, ensuring secure communications across multi-hop relays in SAGSINs still needs further investigation.

Delivering high throughput to users while ensuring security presents another significant challenge. In SAGSINs, optimizing radio resources to maximize throughput under security constraints is inherently intractable as acquiring accurate channel state information (CSI) of hidden Eves is practically infeasible [23], [24]. However, many studies focus on optimizing the relay itself for given CSI, while the joint optimization of relay and radio resource management (RRM) in SAGSINs remains an open problem.

These challenges motivate the following research question:

How can high-throughput, secure SAGSIN relay be established without Eve's channel information?

This research question has rarely been addressed within the context of secure SAGSIN research as surveyed in Table 1. Unlike prior works that only optimize secure relaying in NTNs, we introduce a joint optimization framework for multi-hop relaying that maximizes the minimum user throughput while ensuring a prescribed strictly positive secure connection (SPSC) probability against unknown or passive Eves.

The contributions of this work are summarized as follows:

- ***Cross-layer secure relaying framework***: We propose a cross-layer framework for secure multi-hop relaying in large-scale SAGSINs that optimizes the max-min throughput **without Eve's channel information**, bridging two sep-

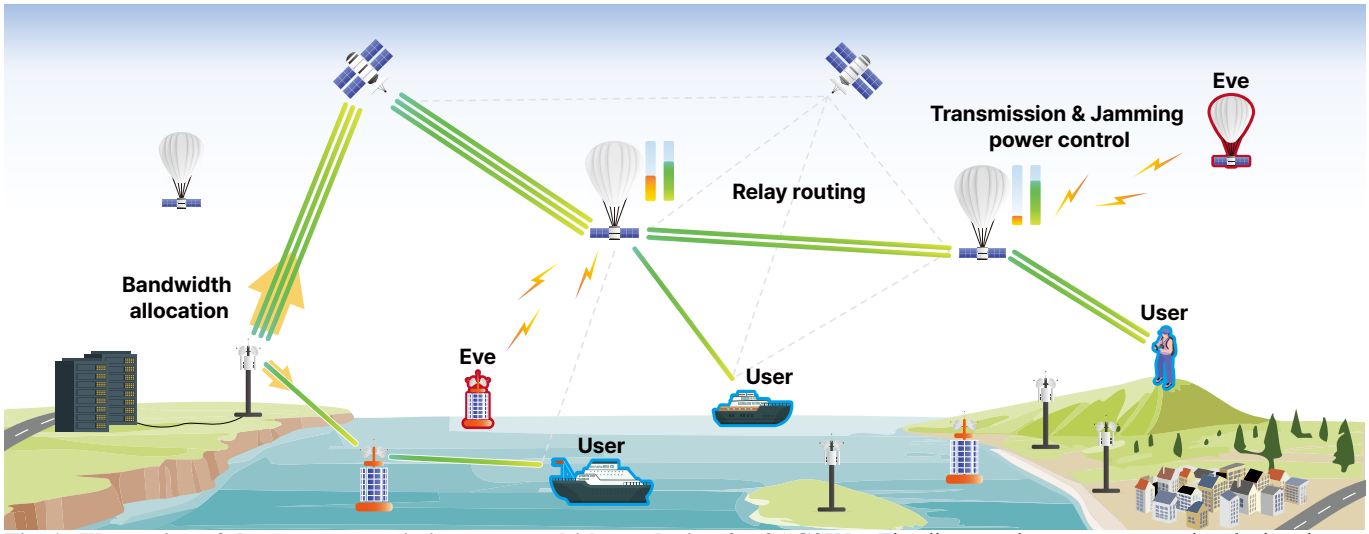


Fig. 1. Illustration of the target scenario in secure multi-hop relaying for SAGSINs. The diagram shows a source node relaying data to multiple users via intermediate nodes. At each relay hop, the nodes transmit both data and predefined jamming signals to degrade the Eves' signal quality, whose locations are modeled as uniformly distributed across the space, air, ground, and sea layer. Each node dynamically allocates bandwidth between data transmission and jamming to maximize the minimum user throughput.

Table 1. Summary of the related works. Appendix A provides further details.

Ref.	Archit.	Eve.	RA	PC	Jamm.	Relay
[11]	SAGIN	Known	✗	✗	✗	Two-hop
[13]	SAGIN	Known	✗	○	○	Two-hop
[15]	SAGIN	Known	✗	○	✗	-
[16]	SAGIN	Known	✗	○	✗	Two-hop
[25]	SAGIN	Unknown	✗	✗	✗	Multi-hop
[26]	UAV net.	Unknown	✗	✗	✗	Multi-hop
[17]	UAV net.	Known	✗	✗	○	Multi-hop
[18]	SGIN	Known	✗	✗	○	Multi-hop
[27]	SGIN	Known	✗	✗	✗	Multi-hop
Ours	SAGSIN	Unknown	○	○	○	Multi-hop

* RA: Resource allocation, PC: Power control, Jamm.: Jamming
S(A)GIN: Space(-air)-ground integrated network.

arate research fields—the secrecy outage probability and radio resource scheduling—with a new form of system model for secure communications that has been previously pioneered. This formulation facilitates the optimization process compared to conventional max-min secrecy rate approaches, while achieving comparable performance to the max-min secrecy problem (Fig. 8).

- ***Analysis for SPSC constraint***: We derive a closed-form approximation for the SPSC probability using stochastic geometry, showing that it can be characterized as a function of Eve density, jamming power, and link distance. This generalizes prior works [28], [29], which obtained closed-form SPSC probability in the absence of jamming. Furthermore, we rigorously analyze the approximation gap and propose a calibration method to mitigate this gap in Figs. 3-5, which has not been addressed in earlier studies.
- ***Efficient solution design***: We develop globally optimal closed-form solutions for radio resource management with $\mathcal{O}(1)$ computational complexity (**Theorem 1**), achieving the optimal frequency allocation, transmission, and jamming power control for a given routing topology. We then propose a Monte-Carlo relay routing algorithm (Alg. 1) with $\mathcal{O}(KN \log N)$ computational complexity for N nodes. Our method consistently achieves a max-min throughput within approximately 5% of the upper bound under various secure SAGSIN simulation settings (Figs. 6-9).
- ***Real-world SAGSIN testbed***: We validate the proposed framework and solver using real-world data of terrestrial, HAPs, LEO satellites, and vessel data. To the best of our knowledge, this is **the first open-source SAGSIN testbed built upon a real-world dataset** including HAPs base stations. The demonstration on the testbeds shows the practicality and superiority of the RRM and routing algorithm (Fig. 10) and illustrates that the framework can immediately adapt to changes in the security environment (Fig. 11).

2. System model

2.1. Scenario Description

This paper aims to construct a secure relaying route in the SAGSIN, with consideration of radio resources, keeping the SPSC probability above a certain threshold in the presence of the hidden Eves. Figure 1 illustrates the target scenario with three control variables. The SAGSIN relay adopts the decode-and-forward scheme [30] and operates in a half-duplex manner, where the throughput is conversely proportional to the number of hops [31]. The nodes transmit predefined jamming signals with data signal to degrade Eve's wiretap ability by reducing the SINR of the wiretap channel [22]. Meanwhile, legitimate nodes recover the original data by cancelling the jamming signals with predefined patterns [32].

The index set of Eves is defined as $\mathcal{M}$. We assume that Eves are present at each network layer to wiretap legitimate communications. The Eves are assumed to be non-colluding

as the SAGSIN's extensive geographic dispersion of nodes makes cooperative wiretap channels logistically unfeasible and the limitations in memory and compute of mobile Eves hinder storing raw I/Q signals. We assume that *the location and channel model of Eves are unknown*, where Eves in each network layer are independently distributed following the homogeneous Poisson point processes (HPPP) with density $\lambda_1, \lambda_2, \lambda_3$, and λ_4 for the space, air, ground, and sea network layers, respectively.

We define the index set of nodes as $\mathcal{I} = \{0, 1, ..., I\}$. A total of U users are served through the multi-hop relays, where the user index set is denoted as $\mathcal{U} = \{1, ..., U\}$. The binary variable $x_{(i,j)} \in \{0, 1\}$ indicates whether there exists a hop between the i-th and j-th nodes. The location of the i-th node and Eve e are denoted as $\boldsymbol{p}_i$ and $\boldsymbol{p}_e$, respectively.

2.2. Propagation Model and Secrecy Metrics

The instantaneous received SNR of the legitimate hop between node i and j, if any, can be given as

$$\mathrm{SNR}^{\mathsf{s}}_{(i,j)} = \frac{\rho_i G_{(i,j)} |h^{\mathsf{s}}_{(i,j)}|^2}{n_0 (d^{\mathsf{s}}_{(i,j)})^{\alpha_i}} \tag{1}$$

where $G_{(i,j)}$ is the antenna gain, $d^{\mathsf{s}}_{(i,j)} = \|\boldsymbol{p}_i - \boldsymbol{p}_j\|_2$ is a distance between; ρ_i is the power density, $h_{(i,j)}$ is small-scale fading, and n_0 is the noise spectral density. The path loss exponent α_i is determined based on the network layer in which node i is located. As nodes can decode and cancel the predefined jamming signal, the SINR of legitimate links are not affected by jamming. Meanwhile, the SNR of wiretap link for node i and Eve k can be defined as

$$\mathrm{SNR}^{\mathsf{e}}_{(i,e)} = \frac{\rho_i G_{(i,j)} |h^{\mathsf{e}}_{(i,e)}|^2 (d^{\mathsf{e}}_{(i,e)})^{-\alpha_i}}{\sigma_i G_{(i,j)} |h^{\mathsf{e}}_{(i,e)}|^2 (d^{\mathsf{e}}_{(i,e)})^{-\alpha_i} + n_0} \tag{2}$$

where σ_i is the power spectral density of the transmitted jamming signal [33], [34]. We consider that Eves have the same receiving capability as the legitimate nodes, assuming the same gain for Eves. For all links, we consider that $|h^{\mathsf{s}}_{(i,j)}|^2$ and $|h^{\mathsf{e}}_{(i,e)}|^2$ are Rayleigh fading channel, following exponential distribution $\mathsf{Exp}(1)$. Adopting the Rayleigh model allows us to analyze the secrecy performance under worst-case conditions, though the LoS nature of SAGSIN channels may be more accurately captured by Rician or Nakagami-m fading. In this sense, the Rayleigh assumption provides a meaningful lower bound on the SPSC probability, as further elaborated in Fig. 3. The entire transmission power density of node i is limited to $P_i^{\max}$; and the minimum transmission power density is defined as $P_i^{\min}$, denoted as

$$\rho_i + \sigma_i \le P_i^{\max},\ \rho_i \ge P_i^{\min}\ \forall i \in \mathcal{I} \tag{3}$$

As the multiple non-colluding Eves can wiretap the legitimate transmission, the secrecy capacity of the link between nodes i and j is defined as

$$C_{(i,j)} = \Big[\log_2\left(1 + \mathrm{SNR}^{\mathsf{s}}_{(i,j)}\right) - \log_2\left(1 + \max_{e \in \mathcal{M}} \mathrm{SNR}^{\mathsf{e}}_{(i,e)}\right) \Big]^+. \tag{4}$$

Then, as introduced in [35], the SPSC probability between node i and j is defined as

$$\mathbb{P}_{(i,j)} = \mathbb{P}(C_{(i,j)} > 0). \tag{5}$$

The closed-form derivation of (5) will be presented in (19).

2.3. Multi-hop Relay Model: Graph-Theoretic Viewpoint

Graph topology. The routing problem is generally considered as finding a sub-graph of directed graph $\mathcal{G}_{\text{all}} = (\mathcal{N}, \mathcal{E})$ where $\mathcal{N} \subset \mathcal{I} \cup \mathcal{U}$ and $\mathcal{E} \subset \{(i,j) | i, j \in \mathcal{N}\}$. This represents that nodes and users are the graph nodes and the relay hops are the graph edges [36], [37].

We assume a spanning tree (ST) topology, which refers to an acyclic graph where all nodes have a single path to the root node [38]. This assumption can be relaxed into a directed acyclic graph (DAG) topology, another topology discussed in the 3GPP standards [39], where nodes can be backhauled by multiple parent nodes. However, the DAG topology requires a sophisticated channel and data management to synchronize and integrate multiple backhaul links, which is not suitable for SAGSINs where node distances can vary significantly.[1]

We define $\mathcal{E}_u$ to denote a relay from node 0 to user u, and

$$x_{(i,j)} = \begin{cases} 1, \text{ if } (i,j) \in \mathcal{E} \\ 0, \text{ otherwise} \end{cases},\ x_{(i,j),u} = \begin{cases} 1, \text{ if } (i,j) \in \mathcal{E}_u \\ 0, \text{ otherwise} \end{cases} \tag{6}$$

to indicate whether edge (i,j) belongs to the edge set of graph $\mathcal{G}$ and edge (i,j) belongs to $\mathcal{E}_u$.[2] There must be no edges entering the root node 0 and every other node should have exactly one entering edge, which can be denoted as

$$\sum_{i \in \mathcal{N}} x_{(i,0)} = 0,\ \sum_{j \in \mathcal{N}} x_{(j,i)} = 1, \forall i \in \mathcal{N} \setminus \{0\} \tag{7}$$

We introduce the *cut-based* constraint, which indicates that graph $\mathcal{G}$ has ST topology. For any non-empty subset $S \subset \mathcal{N} \setminus \{0\}$, there must be at least one selected edge (i,j) with $i \in \mathcal{N} \setminus S$ and $j \in S$, which is denoted as

$$\sum_{i \notin S,\ j \in S} x_{(i,j)} \ge 1, \quad \forall\, S \subset \mathcal{N} \setminus \{0\},\ S \ne \emptyset. \tag{8}$$

This constraint prevents any group of nodes from being disconnected from the root node. Consequently, each node is guaranteed a directed path originating from the root, while satisfying the ST topology.

Relay throughput. The nodes dynamically allocate bandwidth and transmit power on the backhaul link to maximize the network utility. We define $\beta_{(i,j),u}$ to represent the allocated bandwidth of user u at link (i,j); and the spectral efficiency $\gamma_{(i,j)}$ between node i and j as[3]

$$\gamma_{(i,j)} = \log_2\left(1 + \mathrm{SNR}^{\mathsf{s}}_{(i,j)}\right). \tag{9}$$

[1] Nonetheless, the system model can also be applied to the relay with directed acyclic graph topology by changing the graph topology constraints.

[2] The system model considers cross-layer optimization of both network-layer routing and physical-layer resource, so both $x_{(i,j)}$ and $x_{(i,j),u}$ are required to consider the routing and radio resource optimization, respectively.

[3] The ergodic spectral efficiency $\mathbb{E}_{|h^{\mathsf{s}}_{(i,j)}|^2}\left[\log_2(1 + \mathrm{SNR}^{\mathsf{s}}_{(i,j)})\right]$ is approximated as $\log_2\left(1 + \rho_i / [n_0 (d^{\mathsf{s}}_{(i,j)})^{\alpha_i}]\right)$. Appendix C verifies this approximation does not affect to the optimization of decision variables.

The throughput of user u is defined as the minimum throughput divided by the number of hops, denoted as

$$\eta_u = \min_{(i,j)\in\mathcal{E}_u} \frac{\beta_{(i,j),u}\gamma_{(i,j)}}{h_u}, \tag{10}$$

where $h_u = \sum_{(i,j)\in\mathcal{E}} x_{(i,j),u}$. Then, the minimum throughput of the system is defined as $\min_{u\in\mathcal{U}} \eta_u$.

3. Problem Formulation and Proposed Solution

We aim to maximize the minimum throughput across the entire system, ensuring fair service for users accessing the core internet via multiple hops. The problem of guaranteeing a SPSC probability in multi-hop relay terrestrial networks has been studied in [29], [40]. Similarly, the relay routing problem that ensures users' QoS while achieving the optimal secure connection probability has also been investigated [41], [42]. However, there has been no attempt under the SPSC probability constraints in any network settings.

Let $\mathbf{B} = \{\beta_{(i,j),u} : i,j \in \mathcal{N}, u \in \mathcal{U}\}$, $\mathbf{P} = \{\rho_i : i \in \mathcal{N}\}$, and $\mathbf{J} = \{\sigma_i : i \in \mathcal{N}\}$. The max-min throughput problem is formulated as

$$\begin{aligned}
\boldsymbol{\mathcal{P}1}: \max_{\mathcal{G},\mathbf{B},\mathbf{P},\mathbf{J}} \min_{\substack{u\in\mathcal{U},\\(i,j)\in\mathcal{E}_u}} & \frac{\beta_{(i,j),u}\gamma_{(i,j)}}{h_u} && \text{(11a)}\\
\text{s.t. } & \mathbb{P}_{(i,j)} \geq x_{(i,j)}\tau, && \text{(11b)}\\
& (7),\ (8) && \text{(11c)}\\
& \sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}} \beta_{(i,j),u} \leq B, && \text{(11d)}\\
& \rho_i + \sigma_i \leq P_i^{\max}, && \text{(11e)}\\
& \beta_{(i,j),u} \geq 0, \rho_i \geq P_i^{\min}, \sigma_i \geq 0. && \text{(11f)}
\end{aligned}$$

Constraint (11b) represents the threshold of the secrecy connection probability; (11c) is related to the graph topology; (11d) is the frequency resource constraint; (11e) pertains to the transmission and jamming power constraint; and (11f) ensures the positivity of resource variables.

There are two main challenges in Problem $\boldsymbol{\mathcal{P}1}$. First, The formulated problem is a mixed-integer non-convex problem due to the ST topology assumption and max-min throughput objective. Specifically, the tight coupling between graph and radio resource variables in the objective makes it challenging to search the optimal solution. Finding the exact form of the SPSC probability is another challenge. Numerical computation of (11b) may result in significant computational overhead and restrict finding feasible solutions under tight compute budgets. This paper tackles the challenges above by separating the graph optimization from RRM; and by deriving the exact form of the SPSC probability.

3.1. Closed-form Derivation of SPSC Probability

For a hop between node i and j, the SPSC probability is defined from (4) as

$$\begin{aligned}
\mathbb{P}_{(i,j)} &= \mathbb{P}\left(\log_2\left(\frac{1+\mathrm{SNR}^{\mathsf{s}}_{(i,j)}}{1+\max_{e\in\mathcal{M}}\mathrm{SNR}^{\mathsf{e}}_{(i,e)}}\right) > 0\right) && \text{(12)}\\
&= \mathbb{P}\big(\mathrm{SNR}^{\mathsf{s}}_{(i,j)} > \max_{e\in\mathcal{M}} \mathrm{SNR}^{\mathsf{e}}_{(i,e)}\big) && \text{(13)}\\
&= \mathbb{E}_{|h|^2,\mathcal{M}}\Big[\prod_{e\in\mathcal{M}} \mathbb{P}\big(\mathrm{SNR}^{\mathsf{s}}_{(i,j)} > \mathrm{SNR}^{\mathsf{e}}_{(i,e)}\big)\Big]. && \text{(14)}
\end{aligned}$$

Equation (14) is derived from the property of HPPP and $\mathbb{P}(C > \max\{\gamma_1,...,\gamma_n\}) = \mathcal{P}(C > \gamma_1, ..., C > \gamma_n)$.

We define $\lambda_i \in \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ as the Eve density of the network layer that node i belongs to. The probability generating functional of HPPP [28] results in $\mathbb{E}_{\mathcal{M}}[\prod_{e\in\mathcal{M}} f(\boldsymbol{p}_e)] = \exp\big(-\lambda_i \int_{\mathbb{R}^2} 1 - f(\boldsymbol{p}_e) d\boldsymbol{p}_e\big)$. Then, $\mathbb{P}_{(i,j)}$ becomes

$$\begin{aligned}
\mathbb{P}_{(i,j)} &= \mathbb{E}_{|h|^2}\Big[\exp\Big[-\lambda_i \int_{\mathbb{R}^2} \mathbb{P}\big(\mathrm{SNR}^{\mathsf{s}}_{(i,j)} < \mathrm{SNR}^{\mathsf{e}}_{(i,e)}\big)\, d\boldsymbol{p}_e\Big] && \text{(15)}\\
&= \mathbb{E}_{|h|^2}\Big[\exp\Big[&& \text{(16)}\\
&-\lambda_i \int_{\mathbb{R}^2} \mathbb{P}\Big(\underbrace{\frac{|h^{\mathsf{s}}_{(i,j)}|^2 (d^{\mathsf{e}}_{(i,e)})^{\alpha_i} n_0}{(d^{\mathsf{s}}_{(i,j)})^{\alpha_i} n_0 - \sigma_i G_{(i,j)} |h^{\mathsf{s}}_{(i,j)}|^2}}_{\textbf{(a)}} < |h^{\mathsf{e}}_{(i,e)}|^2\Big) d\boldsymbol{p}_e\Big]\Big].
\end{aligned}$$

From $|h^{\mathsf{e}}_{i,e}| \sim \mathrm{Exp}(1)$, (15) simplifies to

$$\mathbb{P}_{(i,j)} = \mathbb{E}_{|h|^2}\Big[\exp\Big[-\lambda_i \underbrace{\int_{\mathbb{R}^2} \exp\big(-\textbf{(a)}\big)\, d\boldsymbol{p}_e}_{\textbf{(b)}}\Big]\Big]. \tag{17}$$

Direct integral of (17) results in

$$\textbf{(b)} = \frac{2\pi}{\alpha_i}\Gamma\Big(\frac{2}{\alpha_i}\Big)(d^{\mathsf{s}}_{(i,j)})^2 \left(\frac{|h^{\mathsf{s}}_{(i,j)}|^2}{1 - \frac{\sigma_i G_{(i,j)}}{(d^{\mathsf{s}}_{(i,j)})^{\alpha_i} n_0}|h^{\mathsf{s}}_{(i,j)}|^2}\right)^{-\frac{2}{\alpha_i}}. \tag{18}$$

Using the Jensen's inequality, this can be further derived as

$$\begin{aligned}
\tilde{\mathbb{P}}_{(i,j)} &\approx \exp\Big[\mathbb{E}_{|h|^2}\big[-\lambda_i \textbf{(b)}\big]\Big] = && \text{(19)}\\
&\exp\left[-\kappa_i\left[\Gamma\Big(1-\frac{2}{\alpha_i}\Big) - \frac{2\sigma_i G_{(i,j)}}{\alpha_i (d^{\mathsf{s}}_{(i,j)})^{\alpha_i} n_0}\Gamma\Big(2-\frac{2}{\alpha_i}\Big)\right](d^{\mathsf{s}}_{(i,j)})^2\right]
\end{aligned}$$

for $\kappa_i = \lambda_i \frac{2\pi}{\alpha_i}\Gamma(\frac{2}{\alpha_i})$. Equation (19) diverges when $\alpha_i = 2$, indicating mathematically guaranteed secure connection in the free-space cannot be achieved. When $\sigma_i = 0$, (19) reduces to closed-form expression from a previous study [28] which does not consider jamming, confirming its well-definedness.

The approximation gap $\mathbb{P}_{(i,j)} - \tilde{\mathbb{P}}_{(i,j)}$ is bounded by the variance of $-\lambda_i$**(b)**, as the Jensen approximation of moment generating function is bounded by $\frac{1}{2}\lambda_i^2 \mathrm{Var}(\textbf{(b)})$.

Then, the approximation gap is bounded as

$$\mathbb{P}_{(i,j)} - \tilde{\mathbb{P}}_{(i,j)} \leq \frac{\lambda_i^2 \pi^3}{2C}\Big(\ln R - \frac{\pi}{4}\Big) \tag{20}$$

for $C = \big((d^{\mathsf{s}}_{(i,j)})^{\alpha_i} n_0 - \sigma_i G_{(i,j)} |h^{\mathsf{s}}_{(i,j)}|^2\big)^{-1}$ and sufficiently large maximum eavesdropping range R. Rigorous derivations for (19) and (20) are provided in Appendices D and E.

3.2. Optimal Frequency Resource Allocation

We first look into how the optimal $\mathbf{B}$ is obtained for given $\mathcal{G}, \mathbf{P}, \mathbf{J}$. Adopting auxiliary variable η, $\boldsymbol{\mathcal{P}1}$ with fixed $\mathcal{G}, \mathbf{P}, \mathbf{J}$ can be considered as

$$\boldsymbol{\mathcal{P}2}: \max_{\mathbf{B},\eta} \eta \qquad \text{(continued)} \tag{21a}$$

$$\text{s.t. } \beta_{(i,j),u}\gamma_{(i,j)}h_u^{-1} \geq x_{(i,j),u}\eta \tag{21b}$$

$$\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\beta_{(i,j),u} \leq B. \tag{21c}$$

The Lagrangian function of $\mathcal{P}\mathbf{2}$ is

$$\mathcal{L}(\mathbf{B},\eta,\boldsymbol{\lambda},\mu) = \frac{1}{\eta} + \sum_{\lambda_{(i,j),u}\in\boldsymbol{\lambda}} \lambda_{(i,j),u}\Big(x_{(i,j),u}\eta - \frac{\beta_{(i,j),u}\gamma_{(i,j)}}{h_u}\Big) + \mu\big(\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\beta_{(i,j),u} - B\big) \tag{22}$$

for $\boldsymbol{\lambda} = \{\lambda_{(i,j),u} : i,j \in \mathcal{N}, u \in \mathcal{U}\}$. The first-order optimality condition on (22), $\delta\mathcal{L}/\delta\eta = 0,\ \delta\mathcal{L}/\delta\beta_{(i,j),u} = 0$, gives

$$\eta = \big(\sum \lambda_{(i,j),u}x_{(i,j),u}\big)^{-\frac{1}{2}},\ \lambda_{(i,j),u} = \frac{\mu h_u}{\gamma_{(i,j)}}. \tag{23}$$

The optimal resource allocation $\beta^*_{(i,j),u}$ occurs when all frequency resources are fully utilized, which corresponds to the equality condition of (21c). Otherwise, we have $\mu = \lambda_{(i,j),u} = 0$ and η in (23) is not defined according to complementary slackness of the KKT conditions. Similarly, the equality condition of (21b) should be satisfied as well.

This can be expressed mathematically as

$$x_{(i,j),u}\eta - \frac{\beta^*_{(i,j),u}\gamma_{(i,j)}}{h_u} = 0,\ \sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\beta^*_{(i,j),u} = B. \tag{24}$$

Solving the above equations with respect to $\beta^*_{(i,j),u}$ results in

$$\beta^*_{(i,j),u} = B\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}}\Big(\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}}\Big)^{-1}. \tag{25}$$

3.3. Optimal Power Allocation

For fixed $\mathcal{G}$, we can reformulate $\mathcal{P}\mathbf{1}$ by plugging in (25) and introducing an auxiliary variable η as

$$\mathcal{P}\mathbf{3}: \max_{\mathbf{P},\mathbf{J},\eta}\ \eta \tag{26a}$$

$$\text{s.t. } \eta\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}} \leq B, \tag{26b}$$

$$(11b),\ (11e),\ \rho_i \geq P_i^{\min},\ \sigma_i \geq 0. \tag{26c}$$

We rigorously prove the following argument by exploring KKT conditions: *The optimal throughput is attained at the maximum transmission power allowed by the system*. We first simplify the constraints and then demonstrate that the maximum achievable transmission power is determined by the minimum jamming power density.

As $d^{\mathsf{s}}_{(i,j)}$ are fixed for given $\mathcal{E}$, the SPSC probability (19) can be viewed as a function of σ_i, denoted as $\mathbb{P}_{(i,j)}(\sigma_i)$. As $\mathbb{P}_{(i,j)}(\sigma)$ is a monotonically increasing function, the constraint (11b) can be redefined as

$$\sigma_i \geq \mathbb{P}^{-1}_{(i,j)}(\tau) = \frac{\alpha_i(d^{\mathsf{s}}_{(i,j)})^{\alpha_i}n_0}{2G_{(i,j)}\big(1-\frac{2}{\alpha_i}\big)}\Big[1 + \frac{\alpha_i\sin\big(\frac{2\pi}{\alpha_i}\big)}{2\pi^2\lambda_i(d^{\mathsf{s}}_{(i,j)})^2}\ln\tau\Big]. \tag{27}$$

We remark that σ_i is bounded by the maximum of the $\mathbb{P}^{-1}_{(i,j)}(\tau)$, which is determined by the farthest link from node i. Combined with $\sigma_i \geq 0$, the constraint can be given by

$$\sigma_i \geq \tau_i = \frac{\alpha_i(d_i^{\max})^{\alpha_i}n_0}{2G_{(i,j)}\big(1-\frac{2}{\alpha_i}\big)}\Big[1 + \frac{\alpha_i\sin\big(\frac{2\pi}{\alpha_i}\big)}{2\pi^2\lambda_i(d_i^{\max})^2}\ln\tau\Big] \tag{28}$$

where $d_i^{\max} = \max_{j:(i,j)\in\mathcal{E}} x_{(i,j)}d^{\mathsf{s}}_{(i,j)}$.

Then, Problem $\mathcal{P}\mathbf{3}$ can be simplified as

$$\mathcal{P}\mathbf{3}: \max_{\mathbf{P},\eta}\ \eta \tag{29a}$$

$$\text{s.t. } \eta\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}} \leq B, \tag{29b}$$

$$\rho_i + \sigma_i \leq P_i^{\max},\ \rho_i \geq P_i^{\min},\ \sigma_i \geq \tau_i. \tag{29c}$$

With $A_i = \sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}}$, the Lagrangian of $\mathcal{P}\mathbf{3}$ is

$$\mathcal{L}(\mathbf{P},\eta,\boldsymbol{\lambda},\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\xi}) = \eta - \sum_{i\in\mathcal{I}}\lambda_i(B-\eta A_i) - \sum_{i\in\mathcal{I}}\xi_i(\sigma_i-\tau_i) - \sum_{i\in\mathcal{I}}\mu_i(P_i^{\max}-\rho_i-\sigma_i) - \sum_{i\in\mathcal{I}}\nu_i(\rho_i - P_i^{\min}). \tag{30}$$

Then, the derivatives of Lagrangian function are provided as

$$\frac{\partial\mathcal{L}}{\partial\eta} = 1 - \sum_{i\in\mathcal{I}}\lambda_i\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}}\frac{x_{(i,j),u}h_u}{\gamma_{(i,j)}} = 0, \tag{31}$$

$$\frac{\partial\mathcal{L}}{\partial\rho_i} = -\lambda_i\eta\frac{\partial A_i}{\partial\rho_i} - \mu_i + \nu_i = 0,\ \frac{\partial\mathcal{L}}{\partial\sigma_i} = -\mu_i + \xi_i = 0. \tag{32}$$

Then, the complementary slackness condition trivially implies $\nu_i = 0$ and $\sigma_i > 0$ as nodes transmit signal.

Suppose $\sigma_i > \tau_i$ for all $i \in \mathcal{I}$, meaning that we allocate more jamming power than the threshold. Then, we have $\xi_i = \mu_i = 0$ by the complementary slackness condition. Plugging $\mu_i = 0$ into $\frac{\partial\mathcal{L}}{\partial\rho_i}$ yields $\nu_i = -\lambda_i\eta\frac{\partial A_i}{\partial\rho_i} \geq 0$ as $\frac{\partial A_i}{\partial\rho_i} < 0$. If $\nu_i > 0$, then $\rho_i = P_i^{\min}$ by complementary slackness. Then, $\rho_i + \sigma_i < P_i^{\max}$ since $\mu_i = 0$, so decreasing σ_i and increasing ρ_i keeps feasibility, strictly decreases A_i allows a larger η, which is a contradiction. Thus, $\sigma_i = \tau_i$ holds at optimum.

Constraint (29c) now can be viewed as $\rho_i \leq P_i^{\max} - \tau_i$. If we assume $\rho_i < P_i^{\max} - \tau_i$ for $i \in \mathcal{I}$, then $\mu_i = 0$ to satisfy the complementary slackness condition. Again, we obtain $\lambda_i = 0$ to meet the optimality condition $\frac{\delta\mathcal{L}}{\delta\rho_i}$, which contradicts $\frac{\delta\mathcal{L}}{\delta\eta}$.

Combining the above conditions, the optimal transmission and jamming power, ρ_i^* and σ_i^*, are given as

$$\rho_i^* = P_i^{\max} - \tau_i,\ \sigma_i^* = \tau_i,\ \forall i \in \mathcal{I}, \tag{33}$$

for τ_i in (28). We correspondingly denote the optimal spectral efficiency as $\gamma^*_{(i,j)}$ by putting ρ_i^* into (9).

The following theorem guarantees that the RRM in (25) and (33) is optimal for the given graph $\mathcal{G}$:

Theorem 1 (Global optimality of RRM). *Let $\mathcal{G}$ be a fixed network topology. Then, the solution $(\beta^*_{(i,j),u}, \rho_i^*, \sigma_i^*)$ obtained by solving $\mathcal{P}\mathbf{1}$ under the given $\mathcal{G}$ is globally optimal.*

Proof. The objective in $\mathcal{P}2$ is convex for $\eta > 0$, and the constraints (21b) and (21c) are affine. Thus, the KKT conditions serve as both necessary and sufficient conditions, guaranteeing $\beta^*_{(i,j),u}$ is a global optimum solution of $\mathcal{P}2$. Similarly, in $\mathcal{P}3$, the objective function is convex, and all constraints including (29c) are affine. Thus, KKT conditions are necessary and sufficient, and (ρ_i^*, σ_i^*) is globally optimal for $\mathcal{P}3$.

Then, from (25), $\beta^*_{(i,j),u}$ can be expressed as an explicit function of (ρ_i^*, σ_i^*). Therefore, combining these yields the full set of decision variables for $\mathcal{P}1$ under fixed $\mathcal{G}$ in the max-min throughput problem [43]. □

3.4. Monte-Carlo Relay Routing

Problem formulation. We have analytically found the optimal $\beta^*_{(i,j),u}$, ρ_i^*, and σ_i^* for given graph $\mathcal{G}$. Then, the problem can be reformulated as

$$\max_{\mathcal{G}} \min_{\substack{u\in\mathcal{U},\\ (i,j)\in\mathcal{E}_u}} B\Big(\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}} \frac{x_{(i,j),u}h_u}{\gamma^*_{(i,j)}}\Big)^{-1} \text{ s.t. (11b), (11c).} \quad (34)$$

The SPSC constraint (11b) can be converted into an explicit link-distance constraint in the routing graph. This transformation is necessary because SPSC probability does not directly indicate how the graph topology is constrained. Specifically, the SPSC constraint determines the maximum link distance,

$$d^{\mathsf{s}}_{(i,j)} \le D_i^{\max}, \quad \forall j \in \mathcal{N} \quad (35)$$

where $D_i^{\max}$ indicates the farthest allowable distance from node i at the maximum jamming power density $P_i^{\max} - P_i^{\min}$. As the SPSC approximation in (19) decreases monotonically in terms of $d^{\mathsf{s}}_{(i,j)}$, $D_i^{\max}$ can be determined by applying the bisection method to (19) for the given τ and $\sigma_i = P_i^{\max} - P_i^{\min}$.

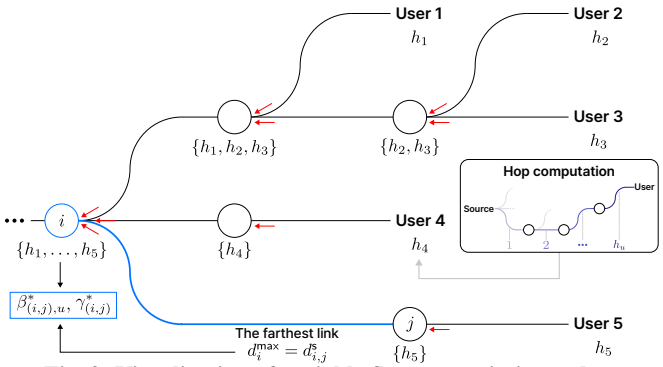


Fig. 2. Visualization of variable flows to optimize node i.

Solving Problem (34) is challenging, as the objective cannot be computed before the graph is completed. As depicted in Fig. 2, determining $\beta^*_{(i,j),u}$, ρ_i^*, and σ_i^* requires h_u and $x_{(i,j),u}$ from the child nodes. These variables can be computed only after the complete routing graph $\mathcal{G}$ is established. This interdependence between routing and resource allocation significantly complicates the routing optimization.

Routing algorithm. This challenge motivates the Monte-Carlo relay routing (MCRR) in Alg. 1, which builds the relay graph $\mathcal{G}$ by sequentially adding source-to-user paths. When a new user path is added to the graph, the MCRR algorithm propagates the user information from the user node back to the source node, as illustrated in Fig. 2. MCRR then exclusively updates the throughput for nodes along this path. Nodes outside this path remain unaffected and thus do not require update, making Alg. 1 node-specific and computationally efficient. Leveraging the low computational complexity of the throughput calculation, MCRR iteratively swaps candidate user paths to construct a graph that yields the highest throughput.

Algorithm 1 Monte-Carlo Relay Routing (MCRR)

Require: Nodes $\mathcal{N}$
Ensure: Solution graph $\mathcal{G}^* = (\mathcal{N}^*, \mathcal{E}^*)$
1: $\mathcal{E} \leftarrow \{(i,j) | d^{\mathsf{s}}_{(i,j)} \le D_i^{\max}\}$, $\mathcal{N}^* \leftarrow \{\}$, $\mathcal{E}^* \leftarrow \{\}$
2: $\mathcal{G}_{\text{all}} \leftarrow (\mathcal{N}, \mathcal{E})$, $\mathcal{G}^* \leftarrow (\mathcal{N}^*, \mathcal{E}^*)$, $T_{\mathcal{G}^*} \leftarrow 0$
3: **for** user u in $\mathcal{U}$ **do**
4: **for** k in $1, \ldots, K$ **do**
5: $\mathcal{E}_{u,k} \leftarrow$ Biased random walk from node 0 to u in $\mathcal{G}_{\text{all}}$
6: $\mathcal{N}_{u,k} \leftarrow$ nodes in the path $\mathcal{P}_{u,k}$
7: **end for**
8: **end for**
9: **while** $T - T_{\mathcal{G}^*} > \epsilon$ **do**
10: **for** each user u **do**
11: $\mathcal{E}_{-u} \leftarrow \{(i,j) \in \mathcal{E}^* | \sum_{u' \in \mathcal{U}} x_{(i,j),u'} \neq x_{(i,j),u}\}$
12: $\mathcal{N}_{-u} \leftarrow \{i, j \mid (i,j) \in \mathcal{E}_{-u}\}$
13: **for** k in $1, .., K$ **do**
14: $\mathcal{G}_{u,k} \leftarrow (\mathcal{N}_{-u} \cup \mathcal{N}_{u,k},\ \mathcal{E}_{-u} \cup \mathcal{E}_{u,k})$
15: $T_{\mathcal{G}_{u,k}} \leftarrow \min_{i \in \mathcal{N}_{u,k}} B\Big(\sum_{j\in\mathcal{N}}\sum_{u\in\mathcal{U}} \frac{x_{(i,j),u}h_u}{\gamma^*_{(i,j)}}\Big)^{-1}$
16: **end for**
17: $\mathcal{G}^* \leftarrow \text{argmin}_{\mathcal{G} \in \{\mathcal{G}^*, \mathcal{G}_{u,1}, \ldots, \mathcal{G}_{u,k}\}} T_{\mathcal{G}}$, $(\mathcal{N}^*, \mathcal{E}^*) \leftarrow \mathcal{G}^*$
18: $T \leftarrow \min_{\mathcal{G} \in \{\mathcal{G}^*, \mathcal{G}_{u,1}, \ldots, \mathcal{G}_{u,k}\}} T_{\mathcal{G}}$
19: **end for**
20: **end while**

The MCRR in Alg. 1 operates as follows: We first build the initial directed graph $\mathcal{G}_{\text{all}}$ by including all possible edge whose length does not exceed the maximum feasible link distance D_i in Eq. (35) (**Line 1-2**). Then, for each user u, we generate a set of K candidate source-to-user path by collecting a shortest-path on $\mathcal{G}_{\text{all}}$, assigning independent random weights $\mathcal{U}(0,1)$ to edge costs at each iteration (**Line 3-8**). This mechanism thus operates similar to a biased random walk from node 0 toward user u, constructing paths with an proper hop count while exploring topologies that may offer superior performance.

The MCRR refinement process (**Line 9-20**) creates multiple candidate graphs by removing and replacing paths to select the optimal configuration. It begins by temporarily removing the existing path of the user evaluated from the current routing graph (**Line 11-12**). Then, each pre-computed candidate path is inserted once at a time, creating different graph configurations that satisfies ST topology (11c) (**Line 14**). As each change is implemented, its effects immediately propagate through the bandwidth and power allocation equations to upstream nodes (**Line 15**). The algorithm evaluates the minimum throughput of each candidate graph, committing the changes only if the throughput improves; otherwise, it reverts

to the original path (**Line 17-18**). Appendix F visualizes how the Monte-Carlo random walk sampling and step-by-step optimization are performed in the MCRR algorithm.

Computational complexity of MCRR. Let N be the number of nodes, K the number of candidate paths per user, and R the number of refinement rounds. The computational cost of MCRR is decomposed as follows:

- **Path sampling**: K randomized shortest paths takes the complexity of $\mathcal{O}(KN \log N)$.
- **Iterative refinement**: In each of the R rounds, every user examines K candidate paths. For each, the algorithm updates the graph and recomputes throughput by locally propagating changes to relevant upstream nodes, giving total refinement cost $\mathcal{O}(RNK)$.

Then, total complexity of Alg. 1 is $\mathcal{O}(KN(\log N + R)) \approx \mathcal{O}(KN \log N)$ when $N \gg R$.

4. Numerical Experiments

This section addresses the following research questions:
RQ 1. How accurate is the closed-form approximation of the SPSC probability? ➜ Sec. 4.1.
RQ 2. How does the max-min throughput in SAGSIN change when security parameters change? ➜ Sec. 4.2.
RQ 3. How does the proposed framework perform in real-world network deployments? ➜ Sec. 4.3.

Answering the questions, we broadly provide a comprehensive validation from the feasibility of the system model to the effectiveness of the proposed scheme. Numerical experiments and analysis exploring each question are presented in Sec. 4.-A to Sec 4.-C. All simulations are implemented in Python 3.12 on an AMD Ryzen™ 9 5800X processor.

4.1. Analysis on SPSC Probability Approximation

4.1.1. Calibration of the SPSC probability

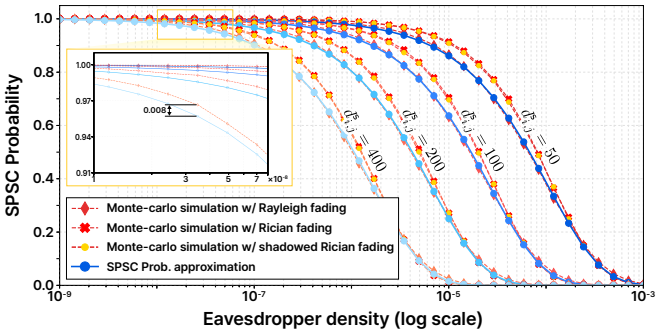


Fig. 3. The SPSC probability versus Eve density for various link distances. Parameters $K_{\text{dB}} = 8$ for a Rician fading and $m = 3$ for a shadowed-Rician fading are adopted as in the 3GPP standard [10].

Figure 3 shows comparisons of the 50,000 Monte-Carlo evaluations of (5) and its closed-form approximation in (19) for four representative link lengths of $\{50, 100, 200, 400\}$ km. We introduced two empirical calibration parameters, a_d and p_d, to compensate for the approximation gap. These factors serve to correct complex, non-ideal effects in the actual environment that the theoretical model may fail to capture. Accordingly, (19) can be calibrated as

$$\hat{\mathbb{P}}_{(i,j)} = \exp\Bigg[- a_d \kappa_i^{p_d} \times \Big[\Gamma\big(1 - \frac{2}{\alpha_i}\big) - \frac{2\sigma_i G_{(i,j)}}{\alpha_i (d^{\text{s}}_{(i,j)})^{\alpha_i} n_0} \Gamma\big(2 - \frac{2}{\alpha_i}\big)\Big] \big(d^{\text{s}}_{(i,j)}\big)^2 \Bigg]. \tag{36}$$

This correction preserves the inherent correlation between distance and SPSC probability while ensuring accurate estimation under varying Eve densities. The (a_d, p_d) pairs used in our experiments are: $(a_{50}, p_{50}) = (0.224, 0.806)$; $(a_{100}, p_{100}) = (0.170, 0.805)$; $(a_{200}, p_{200}) = (0.133, 0.807)$; and $(a_{400}, p_{400}) = (0.102, 0.807)$.

Across the whole distance range, the analytical expression faithfully tracks the Monte-Carlo result; the largest absolute gap occurring in the inset is < 0.008. This indicates that the Rayleigh fading provides worst-case SPSC probability since introducing LoS component helps the legitimate link more than the eavesdropper. (Shadowed) Rician fading disproportionately benefits the short legitimate link, yielding a larger performance gain than for typically distant eavesdroppers.

Moreover, we observe that the change of fading primarily rescales the Eve density and calibration parameters in (36), but preserves the curve' s shape. Equivalently, transitioning from Rayleigh to (shadowed) Rician fading shifts the SPSC curve rightward, effectively resembling a reduction in eavesdropper density. Thus, Rayleigh offers a worst-case guarantee, while (shadowed) Rician represent realistic regimes.

4.1.2. Accuracy of the SPSC probability over link distance

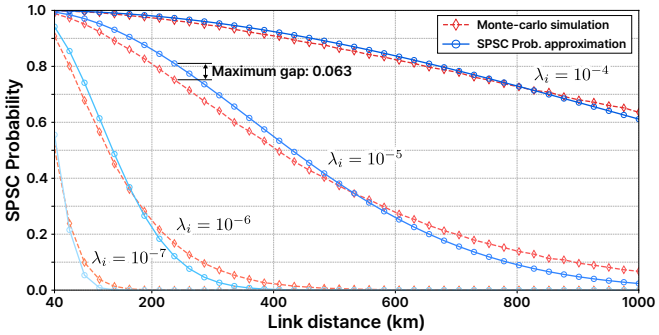


Fig. 4. The SPSC probability versus link distance for various Eve densities.

Figure 4 benchmarks the SPSC probability obtained from 50,000 Monte-Carlo evaluations of (5) against the closed-form approximation (19) for the four Eve densities $\{10^{-4}, 10^{-5}, 10^{-6}, 10^{-7}\}$ km^{-2}. The largest disparity, 0.063, occurs around 320 km of link distance when $\lambda_i = 10^{-5}$. When the link distance increases, the SPSC approximation shows larger degradation than the Monte-Carlo simulation. This is attributed to the assumption that an infinite number of Eves are distributed over an infinite region, whereas in real environments both the number of Eves and the area are finite.

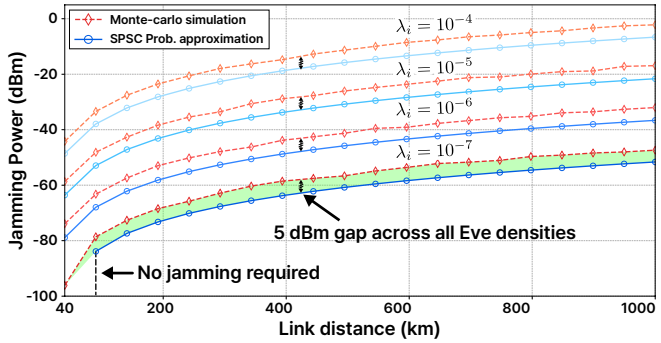


Fig. 5. Required jamming power versus link distance for various Eve densities.

4.1.3. Required jamming power versus link distance

Figure 5 plots the minimum jamming power to guarantee the target SPSC probability threshold $\tau = 0.9999$. The results are obtained (i) numerically from 500,000 Monte-Carlo simulation of (5) and (ii) via the closed-form inversion (28) of the SPSC approximation.[4]

As shown in Fig. 5, the minimum required jamming power computed by the approximation consistently demonstrates a deviation of approximately 5 dBm across all regions. This trend aligns with the over-estimation of the SPSC approximation in Fig. 4 when the link distance is relatively short. Figures 3 and 5 collectively suggest that the SPSC approximation (19) needs to be corrected by the computed offset when determining the minimum jamming power in (28) and the maximum link distance in (35).

4.2. Analysis on Max-Min Throughput

We evaluate the max-min throughput by changing the security parameters and compare the proposed scheme with several baselines. The SAGSIN networks are randomly generated using real-world terrain data across diverse latitudes and longitudes.

Baselines. Each baseline employs a different graph-optimization strategy, but they share the same optimal radio resource **B**, **P**, and **J** obtained in Sec. 3.

- **Bruteforce (Naive upper bound):** Exhaustively evaluates all routing graphs to find an upper-bound on minimum throughput. The exhaustive search trial count is set to 5,000.
- **Hierarchical genetic:** Is a canonical genetic algorithm with elitism [44], but operating in two hierarchical steps [45], [46]. In the first step, each node is binary-encoded as a gene to determine the set $\mathcal{N}^*$. The second step determines the set of edges $\mathcal{E}$ by constructing feasible spanning trees among the selected node genes, subject to the graph topology constraints (11c) and the maximum link distance constraint (35). The genetic algorithm is configured as 5,000 generations, 50 populations, 6 elite counts, and 5% mutation probability.
- **Greedy:** Iteratively selects the relay path that maximizes immediate throughput gain of the user.

[4]The minimum jamming power is determined using the bisection method. Due to the high variance of the experiments, the number of simulations is increased tenfold.

- **Variants of A*:** Use fixed link cost metrics in A* search. While these metrics do not exactly optimize $\mathcal{P}$**1** (because the throughput of nodes and edges changes depending on the graph topology), they serve as useful benchmarks for comparing the performance of different schemes. Moreover, graphs generated by A* always have spanning-tree structures [47], ensuring that the graph solutions remain within the feasible domain of $\mathcal{P}$**1**.

  The choice of metrics in A* is motivated by the objective function in $\mathcal{P}$**1**, which is
  - **A* distance:** Minimizes the sum link distance.
  - **A* hop:** Minimizes the number of source-to-user hops.
  - **A* spectral efficiency:** Maximizes the sum spectral efficiency of the source-to-user routes.

Table 2. Simulation Parameters

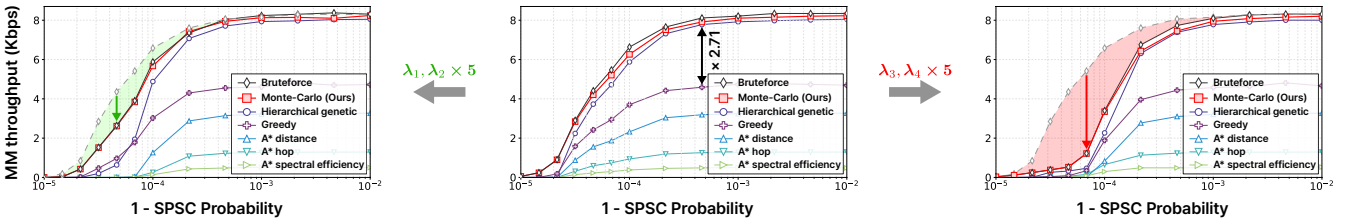
Parameter (Unit)	Ground (G), Maritime (M), HAPs (H)	LEO
Total bandwidth (MHz)	250	400
Tx power (dBm)	30	21.5
Tx antenna gain (dBi)	43.2 (G,M,H→LEO) 25 (G,M,H→G,M,H)	38.5
Rx antenna gain (dBi)	39.7 (G,M,H→LEO) 25 (G,M,H→G,M,H)	38.5
Antenna gain-to-noise temperature (dB/K)	1.5 (H→LEO) 1.2 (G,M→LEO) 16.2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

SAGSIN configurations. The SAGSIN map is generated considering realistic geography as illustrated in Sec. 4.3., randomly placing 150 ground base stations, 150 maritime base stations, 12 HAPs stations, and 10 LEO satellites within longitude 30° and latitude 20° to serve 60 users. The default Eve density is set as $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (10^{-3}, 2{\cdot}10^{-3}, 3{\cdot}10^{-4}, 10^{-4})$ following the literature [48]. Physical layer parameters for SAGSIN, such as carrier frequency, total bandwidth, antenna gain, and antenna gain-to-noise-temperature, are configured as in Table 2, referring to [49], [50] and the 3GPP standard [10].

4.2.1. Impact of the SPSC probability threshold

Figure 6 illustrates how the max-min throughput varies as the SPSC outage probability $(1-\tau)$ increases from 10^{-5} to 10^{-2}. The minimum transmit power P_i for each base station is set to 80% of its total available power. Figures 6a and 6c are obtained by scaling the Eve densities of ground/maritime nodes; and HAPs/LEO nodes fivefold, relative to Fig. 6b.

The minimum throughput of all schemes converges to zero as $1-\tau$ approaches zero. The stricter SPSC threshold τ reduces the maximum link distance (35), making some users unserviceable. Across all subfigures, the **Monte-Carlo** scheme consistently attains throughput levels within ≈5% of the optimal values from the **Bruteforce** method, demonstrating its efficiency and near-optimal performance.



(a) $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (5 \cdot 10^{-3}, 10^{-2}, 3 \cdot 10^{-4}, 10^{-4})$ (b) $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (10^{-3}, 2 \cdot 10^{-2}, 3 \cdot 10^{-4}, 10^{-4})$ (c) $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (10^{-3}, 2 \cdot 10^{-2}, 1.5 \cdot 10^{-3}, 5 \cdot 10^{-4})$

Fig. 6. Max-min throughput versus SPSC outage probability. (a), (b), and (c) measure max-min throughput of SAGSINs in the same environmental settings, except for the Eve densities. The gray dashed lines in (a) and (c) represent the numerical results from the Bruteforce method in (b), illustrating the relative throughput degradation as **green** and **red** areas in (a) and (b). (a) The max-min throughput of **Bruteforce** at $1 - \tau = 5{\cdot}10^{-5}$ decreases from 4.4 kbps in (b) to 2.6 kbps. (c) The performance drop is more pronounced, with the **Bruteforce** throughput at $1 - \tau = 7{\cdot}10^{-5}$ falling from 5.5 kbps to 1.2 kbps.

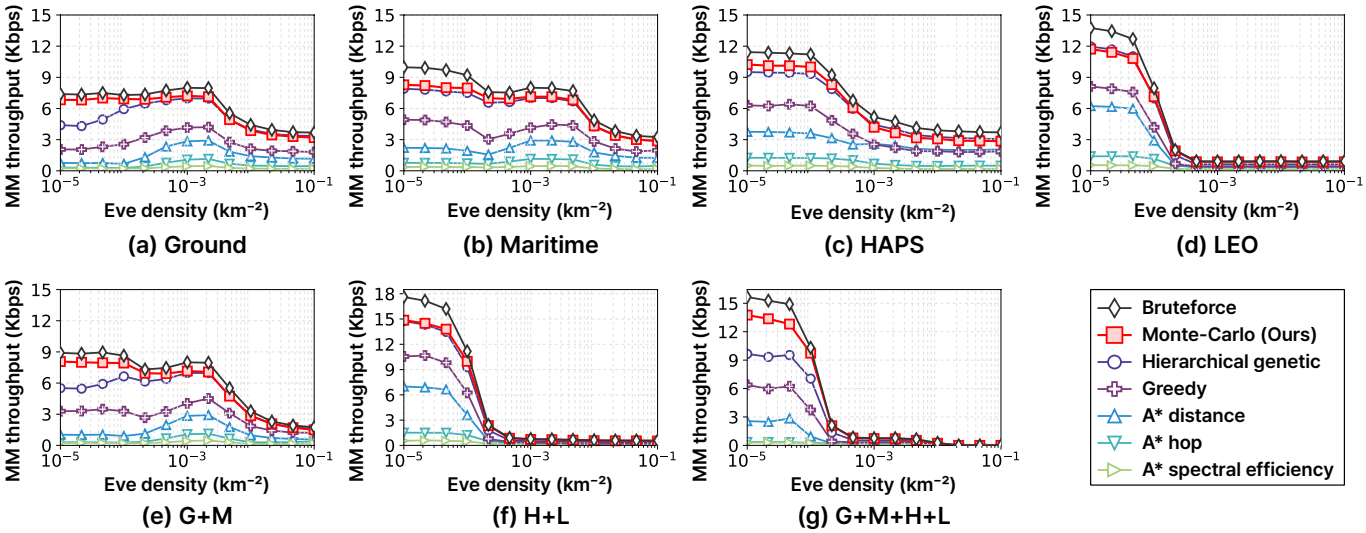


Fig. 7. Max-min throughput versus Eve density for various SAGSIN scenarios. Each graph depicts the max-min throughput while varying the Eve density of the network layer indicated in the caption. The densities of the other layers are fixed to their respective values in the baseline configuration $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (10^{-3}, 2{\cdot}10^{-3}, 3{\cdot}10^{-4}, 10^{-4})$. 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.

In Figs. 6a and 6c, we note that the increase in the Eve density of HAPs and LEO notably deteriorate the max-min throughput, inducing a long tail near zero throughput. This result verifies the critical role of HAPs and LEO nodes in forming secure relays in SAGSINs, as they can establish long-distance connections more easily due to their low path loss and line-of-sight characteristics.

4.2.2. Impact of Eve density

Figure 7 shows how the max-min throughput changes when Eve densities in the various SAGSIN layers vary. The SPSC probability threshold τ is given as 99.99%. In all subfigures, the max-min throughput improves as the Eve density decreases. This improvement is attributed to the expansion of the feasible region defined by the constraints in $\mathcal{P}\mathbf{1}$, providing a broader set of relay options to achieve higher user throughput.

Nevertheless, as shown in Figs. 7a, b, and e, the max-min throughputs of ground and maritime nodes exhibit only modest throughput improvement relative to those of HAPs and LEO nodes. Although the large number of ground and maritime nodes expands the search space and theoretically offers more routing possibilities, it also significantly increases algorithmic complexity and reduces the likelihood of reaching the global optimum. Consequently, the additional computational burden offsets the expected throughput gain due to increased search complexity, leading to only modest improvements. In Figs. 7d, f, and g, the most significant throughput increases are observed when reducing the Eve density at the LEO layer, as LEO nodes enable source-to-user connections with fewer hops and higher spectral efficiency through inter-satellite routes.

4.2.3. Throughput-secrecy gap

Figure 8 presents a comparative analysis between the max-min secrecy rate and the max-min throughput across SPSC probability thresholds. As the threshold τ increases, the two metrics exhibit a strong convergence, highlighting their equivalence under stringent security constraints. In contrast, in the regime of low SPSC thresholds, a noticeable performance gap occurs, primarily because the max-min throughput formulation does not intrinsically incorporate relay security considerations. However, maintaining a high SPSC probability (e.g., > 0.95) is imperative to effectively mitigate the risk of eavesdropping by adversarial nodes such as Eve [29]. Under the high-security regime, where the SPSC probability exceeds

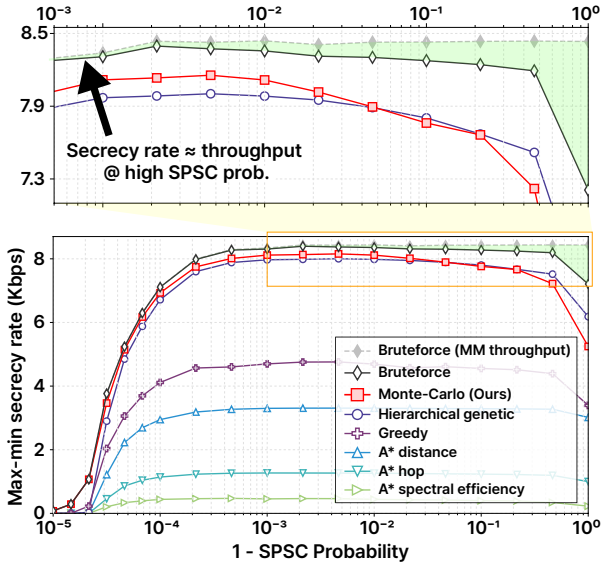


Fig. 8. Comparison of max-min throughput and secrecy rate versus SPSC outage probability. The lower graph plots the max-min secrecy rates across the SPSC probabilities, while the upper graph magnifies the gap (**Green area**) between the max-min throughput and secrecy rate for the Bruteforce solution.

a predefined reliability threshold, the maximum throughput-secrecy gap is approximately 0.38% at $1-\tau = 10^{-3}$, which is marginal enough to justify the use of max-min throughput metric in highly secure scenarios.

4.2.4. Impact of minimum transmit-power constraint

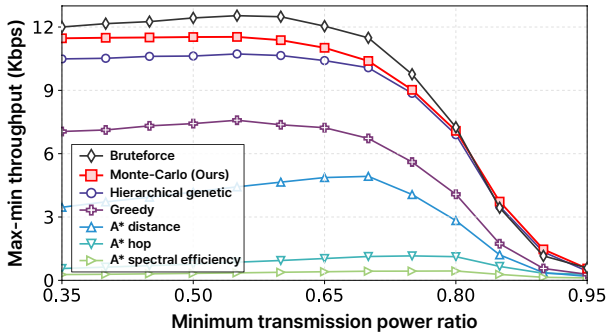


Fig. 9. Max-min throughput versus minimum transmit power ratio. The SPSC probability is set as $\tau = 0.9999$ and the Eve density is fixed as $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (10^{-3}, 2{\cdot}10^{-3}, 3{\cdot}10^{-4}, 10^{-4})$.

Figure 9 examines how the max-min throughput varies as the minimum transmission power ratio $P_i^{\min}/P_i^{\max}$ changes. For $P_i^{\min}/P_i^{\max} < 0.65$, each node can flexibly allocate its transmission and jamming powers according to (33), thereby maintaining a nearly constant achievable throughput.

This finding suggests a practical design guideline as follows: As $P_i^{\min}$ increases, the maximum available jamming budget gradually decreases, which shortens the admissible link distance under the SPSC constraint and excessively limits the feasible graph domain. Selecting $P_i^{\min}/P_i^{\max}$ within the range of 0.6-0.7 ensures adequate jamming capability while eliminating non-promising links, thereby reducing the search space without compromising performance.

4.3. Demonstrations on Real-World Data Testbeds

We evaluate and visualize the framework in testbeds built from real-world base station data to understand scheme operations and framework behavior under secure environment changes. We construct two testbeds in the Mozambique-Madagascar Channel and Southern North America. This work is the first to establish **a SAGSIN testbed with a real-world dataset** integrating HAP base stations. These testbeds reflect the large-scale HAP mobility patterns [2].[5]

Data preparation. The testbeds incorporate various network elements from multiple data sources, as detailed below:

- **Ground.** Ground node positions are extracted from the open source project OpenCellID database, using a network snapshot at 2025-04-22 13:00 UTC.
- **Maritime.** Maritime nodes for the Mozambique-Madagascar testbed are parsed from the MarineTraffic database at 2025-04-22 13:00 UTC.
- **HAPs.** HAPs node positions are derived from the non-profit organization Stratocat database based on data provided by Google's Project Loon [2]. Snapshots at 2020-09-28 10:00 UTC for Mozambique-Madagascar; and at 2020-07-29 00:00 UTC for Southern North America are used to represent HAPs deployments.
- **LEO satellites.** LEO node coordinates are extracted from the non-profit organization CelesTrak repository, parsing Starlink satellites at 2025-04-22 13:00 UTC.

From the positional information obtained from the dataset, we generate channels as described in the system model using the simulation parameters in Table 2.

4.3.1. Mozambique-Madagascar Testbed

Figure 10 overlays the secure routes selected in the Mozambique-Madagascar testbed. In Fig. 10b, the **Monte-Carlo** scheme consistently finds the "sweet-spot" of two or three hops of a few hundred kilometers each, balancing the throughput penalty of extra relay hops with the signal loss incurred on longer links.

The three A* metrics provide useful insights, but optimizing only one axis inevitably violates the inherent multi-dimensional trade-offs. **A* hop** forces overly long links that suffer severe SNR penalties, while **A* spectral efficiency** fragments the path into many short hops and incur excessive scheduling overhead. These observations reveal that effective secure routing in SAGSIN must jointly account for hop count, link distance, and hop capacity.

4.3.2. Southern North America testbed

Figure 11 shows how the proposed MCRR adapts to varying Eve distributions in the Southern North America region. By computing each link's maximum allowable distance from

[5]Since no operational datasets for HAP base stations are currently available, the HAP nodes were synthesized with temporal adjustments.

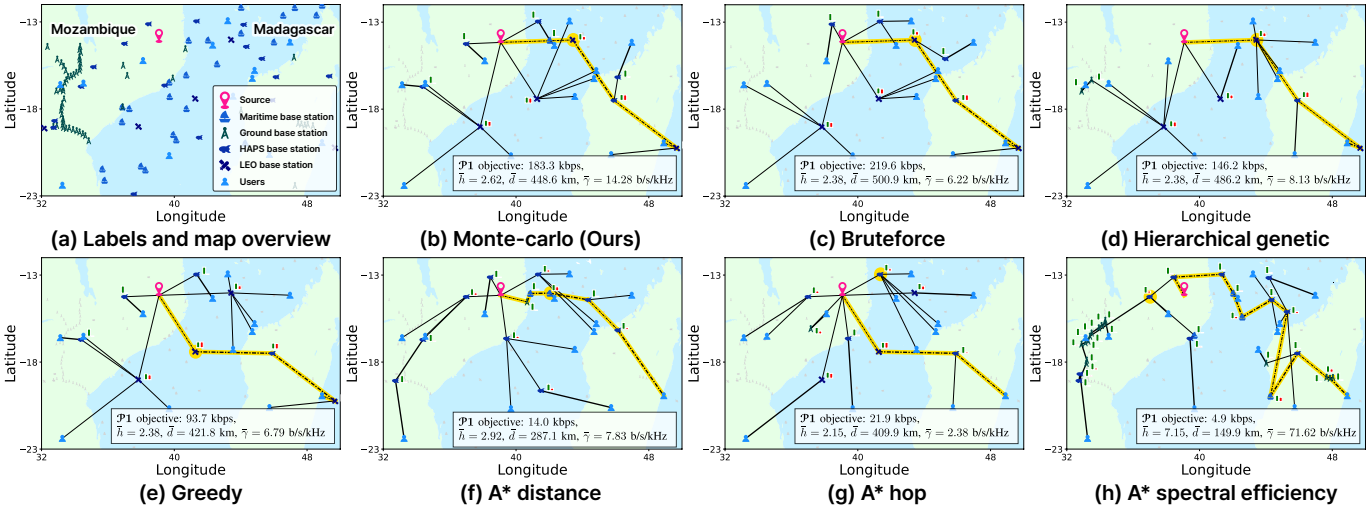


Fig. 10. Secure routing examples on the Mozambique-Madagascar testbed. The highlighted dashed line represents the longest path. The highlighted node represents the min-throughput node. $\bar{h}$, $\bar{d}$, and $\bar{\gamma}$ represent average hop, link distance, and link spectral efficiency, respectively. The green and red bars adjacent to each node indicate the normalized transmission and jamming power allocated under the minimum transmission power ratio $P_i/P = 0.8$. The line width of each link represents the amount of allocated bandwidth.

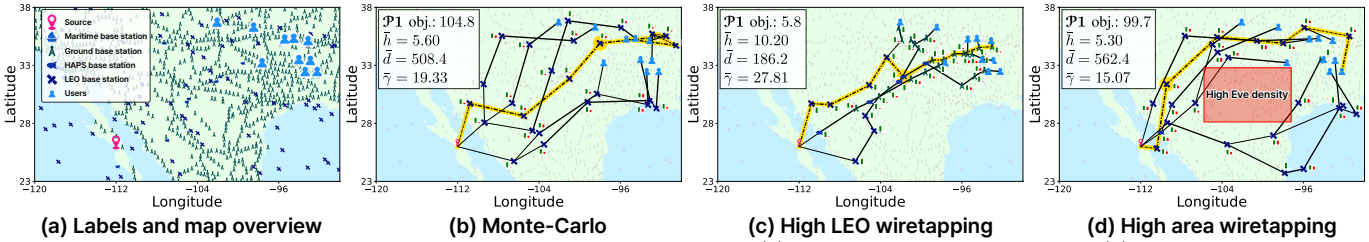


Fig. 11. Secure routing solutions on the Southern North America testbed. (a) Moderate uniform Eve density; (b) High Eve density in the LEO layer; (c) Localized high-density region (**red area**). Eve density in (b) and (c) is increased tenfold.

Eve density and the SPSC threshold, the framework automatically adjusts routing when (i) density increases on a particular network layer (Fig. 11c) and (ii) Eves concentrate in a specific geographic area (Fig. 11d). Thus, we can observe:

- **Fig. 11b:** When Eve density is moderate across all layers, the **Monte-Carlo** scheme adopts inter-satellite paths that maintain throughput in the hundreds of kbps.
- **Fig. 11c:** If Eve density increases in a LEO network, the links in the network become infeasible. Then Alg. 1 detours through ground and HAPs nodes.
- **Fig. 11d:** When Eves concentrate in the shaded area, links crossing that region are automatically excluded and replaced by detours around the area.

In summary, incorporating distance constraints computed from the Eve density and SPSC threshold into the optimization process enables routing decisions to promptly adapt to variations in node-specific and geographical secure threats.

5. Discussion

Conclusion. This work demonstrates that secure and high-performance multi-hop communication can be achieved even in the presence of unknown eavesdroppers across large-scale SAGSINs. This achievement is made possible by deriving a closed-form expression for the SPSC probability and integrating it into a cross-layer optimization framework that jointly optimizes radio resources and relay routes. This framework features an $\mathcal{O}(1)$-complexity frequency allocation and power splitting strategy, along with a Monte-Carlo relay routing algorithm that ensures a minimum throughput for each user under security constraints. The proposed framework was validated through a real-world testbed incorporating ground, maritime, HAP, and LEO nodes, marking the first SAGSIN testbed which includes HAP base stations. This validation narrows the gap between theoretical models and practical deployment, offering promising insights into the realization of secure communication in future 6G integrated networks.

Limitations and Future Work. While this paper proposes a novel approach to physical-layer secure routing in SAGSINs, several challenges remain open. First, the closed-form derivation of the SPSC probability in (19) assumes Rayleigh fading. As links in SAGSINs can be LoS, particularly in the space and aerial layers, a derivation under Rician or Nakagami-m fading models would be more appropriate, but remains an unsolved problem. Furthermore, challenges involving cross-layer or active attacks in SAGSINs, such as satellite jamming or ship-to-air interception, still need to be addressed. Although this work establishes a new paradigm for secure routing against unknown passive eavesdroppers, the system model remains limited to this threat type. Thus, designing robust protocols against active and mobility-driven attacks in SAGSINs remains a key open problem.

REFERENCES

[1] Kodheli, O. et al. Satellite communications in the new space era: A survey and future challenges. *IEEE Commun. Surveys Tuts.*, **23**(1), 70–109 (2021)

[2] Bellemare, M. G. et al. Autonomous navigation of stratospheric balloons using reinforcement learning. *Nature*, **588**(7836), 77–82 (2020)

[3] Elamassie, M. et al. FSO-based multi-layer airborne backhaul networks. *IEEE Trans. Veh. Technol.*, **73**(10), 15004–15019 (2024)

[4] Li, Y. et al. Implementation of an ieee 802.11ax-based maritime mesh network in the red sea. arXiv: 2502.13559 (2025)

[5] Zhang, J. et al. Long-term and real-time high-speed underwater wireless optical communications in deep sea. *IEEE Commun. Mag.*, **62**(3), 96–101 (2024)

[6] Meng, S. et al. Semantics-empowered space-air-ground-sea integrated network: New paradigm, frameworks, and challenges. *IEEE Commun. Surveys Tuts.*, **27**(1), 140–183 (2025)

[7] ITU-R WP5D. M.2160: framework and overall objectives of the future development of IMT for 2030 and beyond. ITU-R recommendations, ITU Radiocommunication Sector (ITU-R) (2023)

[8] 3rd Generation Partnership Project (3GPP). Study on 5GC Enhancements for Non-Terrestrial Networks (NTN). Technical Report 3GPP TR 23.700-10, 3GPP (2023)

[9] 3rd Generation Partnership Project (3GPP). 5G Media Streaming – Support for Non-Terrestrial Networks (NTN). Technical Specification 3GPP TS 26.501, 3GPP (2024)

[10] 3rd Generation Partnership Project (3GPP). Solutions for NR to support Non-Terrestrial Networks (NTN) - Enhancements in Release 18. Technical Report 3GPP TR 38.821, 3GPP (2024)

[11] Wang, Q. et al. Aerial bridge: A secure tunnel against eavesdropping in terrestrial-satellite networks. *IEEE Trans. Wireless Commun.*, **22**(11), 8096–8113 (2023)

[12] Han, C. et al. Joint UAV deployment and power allocation for secure space-air-ground communications. *IEEE Trans. Commun.*, **70**(10), 6804–6818 (2022)

[13] Zhang, Y. et al. Joint UAV trajectory and power allocation with hybrid FSO/RF for secure space–air–ground communications. *IEEE Internet Things J.*, **11**(19), 31407–31421 (2024)

[14] Li, H. et al. UAV-assisted secure communication for coordinated satellite-terrestrial networks. *IEEE Commun. Lett.*, **27**(7), 1709–1713 (2023)

[15] Wang, Z. et al. Label-free deep learning driven secure access selection in space-air-ground integrated networks. In *IEEE Global Commun. Conf. (GLOBECOM)*, 958-963 (2023)

[16] Kakati, A. et al. Toward proactive, secure and efficient space-air-ground communications: Generative AI-based DRL framework. *IEEE Open J. Commun. Soc.*, *6*, 1284–1298 (2025)

[17] Sun, G. et al. Secure and energy-efficient UAV relay communications exploiting collaborative beamforming. *IEEE Trans. Commun.*, **70**(8), 5401–5416 (2022)

[18] Nguyen, T. N. et al. Security-reliability tradeoffs for satellite–terrestrial relay networks with a friendly jammer and imperfect CSI. *IEEE Trans. Aerosp. Electron. Syst.*, **59**(5), 7004–7019 (2023)

[19] Guo, H. et al. A survey on space-air-ground-sea integrated network security in 6G. *IEEE Commun. Surveys Tuts.*, **24**(1), 53–87 (2022)

[20] Reus-Muns, G. et al. Flying among stars: Jamming-resilient channel selection for UAVs through aerial constellations. *IEEE Trans. Mobile Comput.*, **22**(3), 1246–1262 (2023)

[21] Xu, P. et al. Deep learning driven buffer-aided cooperative networks for B5G/6G: Challenges, solutions, and future opportunities. *IEEE Wireless Commun.*, **31**(4), 215–222 (2024)

[22] Dong, L. et al. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Processing*, **58**(3), 1875–1888 (2010)

[23] Su, Y. et al. A secure transmission scheme with energy-efficient cooperative jamming for underwater acoustic sensor networks. *IEEE Sensors J.*, **22**(21), 21287–21298 (2022)

[24] Abdalla, A. S. et al. UAV trajectory and multi-user beamforming optimization for clustered users against passive eavesdropping attacks with unknown CSI. *IEEE Trans. Veh. Technol.*, **72**(11), 14426–14442 (2023)

[25] Eiza, M. H. et al. A hybrid SDN-based architecture for secure and QoS aware routing in space-air-ground integrated networks (SAGINs). In *IEEE Wireless Commun. Networking Conf. (WCNC)*, 1-6 (2023)

[26] Sbeiti, M. et al. PASER: Secure and efficient routing approach for airborne mesh networks. *IEEE Trans. Wireless Commun.*, **15**(3), 1950–1964 (2016)

[27] Guo, K. et al. Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling. *IEEE Access*, *6*, 55815–55827 (2018)

[28] Yao, J. et al. Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying. *IEEE Trans. Commun.*, **64**(2), 753–764 (2016)

[29] Yao, J. et al. Secure transmission in linear multihop relaying networks. *IEEE Trans. Wireless Commun.*, **17**(2), 822–834 (2018)

[30] Cover, T. et al. Capacity theorems for the relay channel. *IEEE Trans. Inform. Theory*, **25**(5), 572–584 (1979)

[31] Gupta, P. et al. The capacity of wireless networks. *IEEE Trans. Inform. Theory*, **46**(2), 388–404 (2000)

[32] Goel, S. et al. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.*, **7**(6), 2180–2189 (2008)

[33] Lv, L. et al. Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay. *IEEE Trans. Commun.*, **68**(3), 1698–1715 (2020)

[34] Mao, Y. et al. Joint transceiver optimization for CJ-aided security communication systems with frequency mismatch. *IEEE Wireless Commun. Lett.*, **13**(6), 1631–1635 (2024)

[35] Jameel, F. et al. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surveys Tuts.*, **21**(3), 2734–2771 (2019)

[36] Pagin, M. et al. Resource management for 5G NR integrated access and backhaul: A semi-centralized approach. *IEEE Trans. Wireless Commun.*, **21**(2), 753–767 (2022)

[37] Yin, H. et al. Routing and resource allocation for IAB multi-hop network in 5G advanced. *IEEE Trans. Commun.*, **70**(10), 6704–6717 (2022)

[38] 3rd Generation Partnership Project (3GPP). NG-RAN; Architecture description. Technical Report TS 38.401, 3rd Generation Partnership Project (3GPP) (2023)

[39] 3rd Generation Partnership Project (3GPP). NR; Integrated Access and Backhaul (IAB) architecture and procedures. Technical Report TS 38.340, 3rd Generation Partnership Project (3GPP) (2023)

[40] Thapar, S. et al. Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users. *IEEE Trans. Veh. Technol.*, **69**(11), 13259–13272 (2020)

[41] Xu, Y. et al. Security/QoS-aware route selection in multi-hop wireless ad hoc networks. In *IEEE Int. Conf. on Commun. (ICC)*, 1-6 (2016)

[42] Xu, Y. et al. SOQR: Secure optimal QoS routing in wireless ad hoc networks. In *IEEE Wireless Commun. Netw. Conf. (WCNC)*, 1-6 (2017)

[43] Boyd, S. et al. *Convex Optimization*. Cambridge University Press (2004)

[44] Weise, T. Global optimization algorithms-theory and application. *Self-Published Thomas Weise*, *361* (2009)

[45] Schaefer, R. et al. Genetic search reinforced by the population hierarchy. In *Foundations of Genetic Algorithms 7*, 383–399. Morgan Kaufmann Publishers (2003)

[46] Ciepiela, E. et al. Hierarchical approach to evolutionary multi-objective optimization. In Bubak, M. et al. (Eds.), *Int. Conf. Comput. Sci. (ICCS)*, 740–749. Springer Berlin Heidelberg (2008)

[47] Cormen, T. H. et al. Dijkstra's algorithm. In *Introduction to Algorithms* (3rd ed.). chapter 24.3, 658–664. MIT Press (2009)

[48] Zou, Y. et al. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE*, **104**(9), 1727–1765 (2016)

[49] Liu, D. et al. Deep learning aided routing for space-air-ground integrated networks relying on real satellite, flight, and shipping data. *IEEE Wireless Commun.*, **29**(2), 177–184 (2022)

[50] Vondra, M. et al. Integration of satellite and aerial communications for heterogeneous flying vehicles. *IEEE Netw.*, **32**(5), 62–69 (2018)