Communications, Electronics and Sensing Systems
https://ces-systems.org

RIS-Assisted Secure Transmission for Unmanned Aerial Vehicle and Satellite Links Under Hardware Impairments

Joshua Phillips

The Department of Automatic Control and Systems Engineering (ACSE), Faculty of Engineering, The University of Sheffield, Sheffield S10 2TN, UK

Editorial correspondence on behalf of the authors: info@ces-systems.org

Abstract

The integration of satellite networks with unmanned aerial vehicles has emerged as a cornerstone for next-generation communication systems, providing ubiquitous connectivity and expansive coverage. However, the inherent broadcast nature of wireless channels in these open space environments renders them highly susceptible to malicious eavesdropping. Reconfigurable intelligent surfaces have recently been proposed as a revolutionary technology to enhance physical layer security by dynamically altering the propagation environment. Despite their potential, the practical implementation of reconfigurable intelligent surfaces and transceiver modules is inevitably constrained by hardware impairments, such as phase noise, in-phase and quadrature imbalance, and amplifier nonlinearities. This paper provides a comprehensive analysis of secure transmission in a reconfigurable intelligent surface-assisted satellite and unmanned aerial vehicle network subjected to realistic hardware impairments. We formulate a robust optimization problem aimed at maximizing the secrecy rate of the system by jointly designing the active beamforming at the satellite and the passive phase shift matrix at the reconfigurable intelligent surface, while explicitly accounting for the distortion noise introduced by hardware imperfections. Through an alternating optimization framework based on successive convex approximation, we navigate the non-convex nature of the objective function. Extensive theoretical analysis and system-level evaluations reveal that ignoring hardware impairments leads to significant performance degradation, highlighting the necessity of hardware-aware robust designs in practical space-air-ground integrated networks.

Keywords: Reconfigurable Intelligent Surfaces; Physical Layer Security; Hardware Impairments; Satellite Communications

1. Introduction

1.1 Evolution of Space-Air-Ground Integrated Networks

The rapid evolution of wireless communication technologies has catalyzed the transition from purely terrestrial networks to highly complex space-air-ground integrated networks. These architectures are envisioned to satisfy the escalating demands for global coverage, ultra-reliable low-latency communications, and massive connectivity, which are primary objectives for the sixth-generation wireless networks [1]. Space-air-ground integrated networks synergistically combine the expansive footprint of satellite systems, the agility and flexibility of unmanned aerial vehicles, and the high-capacity infrastructure of terrestrial networks [2]. Low Earth orbit satellites, in particular, have garnered immense attention due to their reduced propagation delay and lower path loss compared to their geostationary counterparts. When coupled with unmanned aerial vehicles acting as aerial relays or mobile base stations, the combined network can effectively bridge the digital divide, providing high-quality broadband services to remote, disaster-stricken, or maritime regions where deploying traditional terrestrial infrastructure is either economically unfeasible or physically impossible [3]. The dynamic topology and three-dimensional mobility of unmanned aerial vehicles allow for on-demand deployment and adaptive link configuration, thereby significantly enhancing the overall capacity and resilience of the network infrastructure [4].

1.2 Security Challenges in Non-Terrestrial Networks

Despite the unprecedented advantages offered by non-terrestrial networks, the unique characteristics of the space-air-ground propagation environment introduce profound security vulnerabilities. The predominantly line-of-sight nature of satellite and unmanned aerial vehicle links, combined with their wide geographical coverage, makes the transmitted signals highly susceptible to interception by unauthorized entities [5]. Traditional cryptographic techniques, which operate primarily at the upper layers of the protocol stack, rely heavily on the computational complexity of mathematical algorithms and the secure distribution of cryptographic keys. However, in highly dynamic and decentralized networks involving numerous heterogeneous nodes, key management becomes an exceedingly complex and resource-intensive task. Furthermore, the advent of quantum computing poses a severe threat to classical cryptographic algorithms. Consequently, physical layer security has emerged as a compelling complementary paradigm [6]. Physical layer security exploits the inherent randomness and imperfections of the wireless communication medium, such as fading, noise, and interference, to extract secure transmission rates [7]. By ensuring that the channel capacity of the legitimate receiver strictly exceeds that of the eavesdropper, physical layer security can theoretically guarantee perfect secrecy independent of the computational capabilities of the adversary [8].

1.3 The Role of Reconfigurable Intelligent Surfaces

To further bolster physical layer security in environments where the legitimate channel conditions are severely degraded or heavily correlated with the eavesdropper's channel, reconfigurable intelligent surfaces have been introduced as a disruptive technology. A reconfigurable intelligent surface comprises a massive array of low-cost, passive reflecting elements, each capable of independently manipulating the phase and amplitude of the incident electromagnetic waves [9]. By judiciously controlling these elements via a smart controller, the reconfigurable intelligent surface can dynamically reshape the wireless propagation environment, creating favorable channel conditions for the intended user while simultaneously suppressing the signal strength at the eavesdropper. In the context of space-air-ground integrated networks, deploying a reconfigurable intelligent surface on an unmanned aerial vehicle offers exceptional benefits. The mobility of the aerial vehicle allows the surface to be strategically positioned to bypass blockages and establish strong line-of-sight links with both the satellite and the ground terminals. This aerial reconfigurable intelligent surface paradigm essentially establishes a highly flexible, proactive, and smart radio environment that can significantly enhance both the spectral efficiency and the secrecy performance of the network [10].

1.4 The Reality of Hardware Impairments

While theoretical studies on reconfigurable intelligent surface-assisted networks often assume ideal hardware components, practical implementations are inevitably plagued by various hardware impairments. High-frequency communication systems, particularly those operating in the millimeter-wave or terahertz bands often envisioned for satellite links, are highly sensitive to imperfections such as phase noise in local oscillators, quantization errors in low-resolution analog-to-digital converters, in-phase and quadrature imbalances, and nonlinearities in high-power amplifiers. In the context of reconfigurable intelligent surfaces, the phase shift elements are typically controlled by discrete diodes, leading to phase quantization errors and amplitude-phase coupling effects [11]. When the network operates under these non-ideal conditions, the hardware impairments manifest as additive distortion noise that scales with the signal power, fundamentally limiting the channel capacity and altering the spatial directivity of the synthesized beams. Ignoring these practical constraints during the system design phase leads to an overly optimistic estimation of the secrecy performance and can result in severe vulnerability gaps in actual deployments.

2. Literature Review and Background

2.1 Advancements in Satellite and Aerial Communications

The integration of non-terrestrial elements into cellular networks has been extensively studied over the past decade. Initial research primarily focused on addressing the fundamental challenges of satellite communications, such as compensating for large Doppler shifts and mitigating the severe path loss over extensive propagation distances [12]. Researchers have proposed various beamforming and resource allocation schemes to optimize the throughput of multi-beam satellite systems. Simultaneously, the deployment of unmanned aerial vehicles as communication relays has seen a surge in research interest. The ability to optimize the three-dimensional trajectory of the aerial vehicle provides an additional degree of freedom to enhance communication metrics [13]. Studies have demonstrated that by jointly optimizing the flight path and the communication scheduling, the system can significantly improve the energy efficiency and the coverage probability for ground users. The convergence of these two domains has led to the conceptualization of satellite-aerial collaborative networks, where unmanned aerial vehicles serve as intermediate nodes to relay signals between low Earth orbit satellites and terrestrial devices, effectively overcoming shadowing effects caused by urban structures or rugged terrain [14].

2.2 Physical Layer Security in Wireless Networks

The concept of physical layer security, originally introduced by Wyner in his seminal work on the wiretap channel, has evolved into a robust field of research. In conventional terrestrial networks, physical layer security techniques typically involve artificial noise injection, cooperative jamming, and secure beamforming [15]. Artificial noise injection, for instance, deliberately transmits interfering signals into the null space of the legitimate user's channel to degrade the eavesdropper's decoding capability without affecting the intended receiver. However, applying these techniques to satellite and unmanned aerial vehicle networks introduces new challenges [16]. The power constraints of aerial vehicles and the long propagation delays of satellite links make traditional cooperative jamming highly inefficient. Moreover, the strong line-of-sight channels characteristic of aerial networks often result in highly correlated channels for receivers located in close proximity, making it difficult to find a null space that isolates the legitimate user from the eavesdropper [17]. This channel correlation bottleneck necessitates the development of novel approaches to manipulate the spatial signatures of the communication links.

2.3 Reconfigurable Intelligent Surfaces in Modern Communications

Reconfigurable intelligent surfaces have gained immense traction as a viable solution to the limitations of traditional physical layer security techniques. Early studies on these surfaces focused on fundamental capacity limits and channel estimation strategies. Subsequent research explored their application in various network configurations, including multi-user multiple-input multiple-output systems and cognitive radio networks. In the realm of physical layer security, researchers have demonstrated that a strategically placed reconfigurable intelligent surface can dynamically adjust its reflection coefficients to align the reflected signals constructively at the legitimate receiver and destructively at the eavesdropper [18]. This capability is particularly advantageous in scenarios where the direct link between the transmitter and the legitimate user is blocked or severely attenuated. The integration of these surfaces with unmanned aerial vehicles has further expanded the design space, allowing for the joint optimization of the surface's passive beamforming matrix and the aerial vehicle's spatial location [19]. This aerial surface configuration has been shown to provide superior performance compared to static terrestrial surfaces, primarily due to the enhanced probability of establishing line-of-sight links and the ability to adapt to user mobility.

2.4 Hardware Impairments in High-Frequency Communications

Despite the theoretical promise of these advanced communication architectures, the impact of hardware impairments remains a critical bottleneck. In practical systems, the transceiver modules at the satellite, the aerial vehicle, and the ground terminals suffer from residual hardware imperfections that cannot be completely eliminated by calibration algorithms. These imperfections create distortion noise that degrades the signal-to-noise-plus-interference ratio. Furthermore, the reflecting elements of the reconfigurable intelligent surface are typically constructed using inexpensive components, such as PIN diodes or varactors, which exhibit non-ideal behaviors [20]. Phase quantization errors arise when the continuous phase shifts are mapped to discrete values due to limited control bits. Additionally, recent experimental studies have revealed that the reflection amplitude is often coupled with the phase shift, contradicting the common assumption of constant amplitude reflection. Several researchers have attempted to model these impairments mathematically and investigate their impact on system performance [21]. However, the vast majority of existing literature on reconfigurable intelligent surface-assisted secure transmission assumes ideal hardware. There is a conspicuous lack of comprehensive studies that jointly address the challenges of physical layer security, aerial-satellite integration, and realistic hardware impairments, a gap that this paper systematically addresses.

3. System Architecture and Hardware Impairments Model

3.1 Network Topology and Channel Models

We consider a secure communication scenario within a space-air-ground integrated network consisting of a low Earth orbit satellite, an unmanned aerial vehicle equipped with a reconfigurable intelligent surface, a legitimate ground user, and a malicious terrestrial eavesdropper. The satellite is equipped with a massive antenna array, while the ground user and the eavesdropper are equipped with single antennas. The reconfigurable intelligent surface consists of a large uniform planar array of passive reflecting elements. Due to severe terrain blockages and heavy shadowing, we assume that the direct links from the satellite to both the legitimate user and the eavesdropper are completely obstructed. Consequently, all communication must be relayed through the aerial reconfigurable intelligent surface. The aerial vehicle is positioned strategically to maintain strong line-of-sight connections with both the satellite and the ground nodes. The channels are modeled using a combination of large-scale path loss and small-scale fading. Given the high altitude of the satellite and the aerial vehicle, the satellite-to-surface link and the surface-to-ground links are dominated by line-of-sight components and are thus modeled using Rician fading distributions.

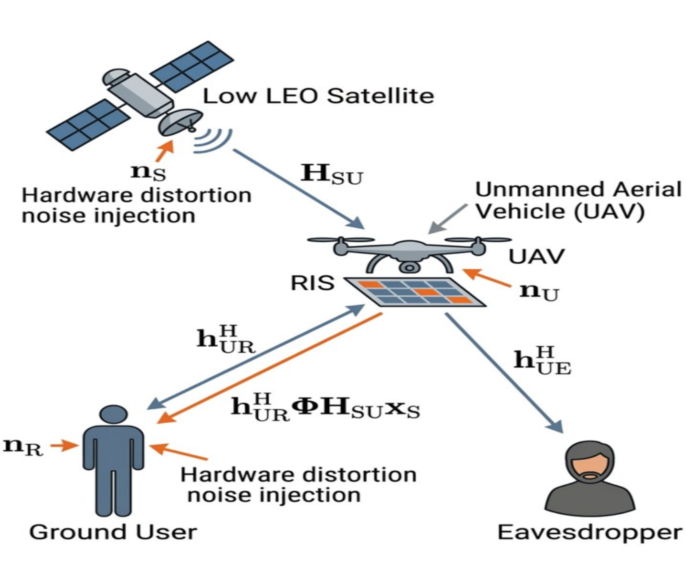

Figure 1: Comprehensive Schematic of RIS

3.2 Mathematical Modeling of Hardware Impairments

To accurately reflect real-world constraints, we incorporate a comprehensive hardware impairment model into our system. The impairments manifest at three primary stages: the satellite transmitter, the reconfigurable intelligent surface, and the ground receivers. At the satellite, phenomena such as digital-to-analog converter quantization errors, power amplifier nonlinearities, and local oscillator phase noise result in a mismatch between the intended baseband signal and the actual transmitted waveform. This mismatch is commonly modeled as an additive distortion noise. Let the intended transmit signal vector be denoted by the corresponding spatial precoding matrix applied to the data symbol. The actual transmitted signal incorporates an independent distortion vector whose covariance matrix is proportional to the power of the intended signal. The proportionality constant represents the error vector magnitude, a metric commonly used to quantify transceiver quality.

Similarly, the reflection process at the reconfigurable intelligent surface is imperfect. The phase shift applied by each element deviates from the ideal intended value due to phase quantization and continuous phase noise. Furthermore, the structural characteristics of the reflecting elements cause the reflection amplitude to vary depending on the applied phase shift. We model these surface imperfections by defining an actual reflection matrix that incorporates both the amplitude degradation and a random phase error term for each diagonal element. The phase error is typically assumed to follow a Von Mises or zero-mean Gaussian distribution. Finally, the receivers at the legitimate user and the eavesdropper introduce their own distortion noise, modeled analogously to the transmitter distortion, capturing the effects of imperfect analog-to-digital conversion and low-noise amplifier nonlinearities.

When combining all these non-ideal factors, the received signal at the legitimate user can be formulated as a complex mathematical expression. To illustrate the core mathematical structure of the impairment integration, we provide the formulation for the effective received signal-to-interference-plus-noise ratio under hardware impairments.

$$\gamma_u = \frac{|h_u^H \, Theta \, G \, w|^2}{kappa_t^2 |h_u^H \, Theta \, G|^2 + kappa_r^2 |h_u^H \, Theta \, G \, w|^2 + \sigma_u^2}$$

In this formulation, the term in the numerator represents the power of the desired signal, where the channel vectors and matrices are combined with the phase shift matrix and the active beamforming vector. The denominator encapsulates the aggregate negative effects, including the transmitter hardware distortion scalar, the receiver hardware distortion scalar, and the additive white Gaussian noise variance.

3.3 Eavesdropper Model and Secrecy Rate Formulation

The eavesdropper in our model is assumed to be a sophisticated adversary capable of intercepting the signals reflected by the aerial surface. We operate under a worst-case security assumption, meaning that the eavesdropper has full knowledge of the transmission protocols and possesses high-quality receiving equipment, resulting in a lower receiver distortion parameter compared to the legitimate user. However, the eavesdropper still suffers from the cascaded hardware impairments originating from the satellite and the reconfigurable intelligent surface. The signal-to-interference-plus-noise ratio at the eavesdropper is formulated similarly to that of the legitimate user, utilizing the specific channel vector from the aerial surface to the eavesdropper's location.

The fundamental metric for evaluating physical layer security in this configuration is the achievable secrecy rate. The secrecy rate defines the maximum rate at which information can be reliably transmitted to the intended user such that the eavesdropper is unable to decode any meaningful data. According to information-theoretic principles, the achievable secrecy capacity is derived from the difference between the channel capacity of the legitimate link and the channel capacity of the wiretap link. Taking into account the complex hardware impairment models and the signal-to-interference-plus-noise formulations discussed previously, the objective function representing the achievable secrecy rate is formally expressed below.

$$C_{sec} = max\left(0, \log_2\left(1+\gamma_u\right) - \log_2\left(1+\gamma_e\right)\right)$$

Here, the variables embedded within the logarithmic functions represent the respective signal quality metrics at the user and the eavesdropper, heavily penalized by the distortion noise parameters defined in the previous subsection. The maximization operator ensures that the secrecy rate cannot be negative; if the eavesdropper's channel quality exceeds that of the legitimate user, the system halts secure transmission, yielding a secrecy rate of zero.

4. Secure Transmission Optimization Methodology

4.1 Problem Formulation

The primary objective of our proposed methodology is to maximize the achievable secrecy rate of the space-air-ground network by jointly designing the variables under our control, specifically the active transmit beamforming vector at the satellite and the passive phase shift matrix at the aerial reconfigurable intelligent surface. This optimization must be performed subject to several stringent practical constraints. Firstly, the transmit power of the satellite is strictly limited by an upper bound to prevent overwhelming adjacent frequency bands and to comply with regulatory standards. Secondly, the reflecting elements on the surface are subject to unit modulus constraints in the ideal case, but under our hardware impairment model, they are bounded by a maximum reflection amplitude and constrained by discrete phase configurations.

The resulting mathematical optimization problem is highly non-convex. The non-convexity arises from multiple sources: the logarithmic nature of the objective function, the strong coupling between the active beamforming vector and the passive phase shift matrix in both the signal and the distortion noise terms, and the non-convex constraints associated with the hardware elements. Because the variables are deeply intertwined, standard convex optimization solvers cannot be directly applied to find a globally optimal solution. Therefore, we must rely on advanced transformation and decoupling techniques.

Table 1: Optimization Parameters and Algorithmic Thresholds

Parameter Description	Notation	Baseline Value
Maximum Satellite Transmit Power	P_max	46 dBm
Number of RIS Elements	N_ris	256
Convergence Tolerance	Epsilon	0.0001
Maximum Iterations	Iter_max	100
Transmitter Distortion Coefficient	Kappa_t	0.1

4.2 Alternating Optimization Framework

To overcome the inherent intractability of the joint formulation, we propose an efficient alternating optimization framework. The core principle of alternating optimization, also known as block coordinate descent, involves dividing the complex multi-variable problem into several manageable subproblems. In each iteration, we optimize one block of variables while holding the other blocks fixed. By iteratively solving these subproblems, the algorithm monotonically increases the objective function value until convergence to a stationary point is achieved. In our specific architecture, we decompose the primary problem into two distinct subproblems: the active beamforming optimization at the satellite and the passive phase shift optimization at the reconfigurable intelligent surface.

This decoupling strategy significantly simplifies the mathematical structure. When the phase shift matrix is fixed, the effective cascaded channels from the satellite to the ground terminals become constant, transforming the first subproblem into a more traditional secure beamforming design. Conversely, when the transmit beamforming vector is fixed, the problem reduces to a reflection optimization task, albeit complicated by the complex distortion noise terms introduced by the hardware impairments.

4.3 Active Beamforming Optimization at the Satellite

Let us first examine the subproblem of optimizing the satellite's active beamforming vector for a given phase shift matrix. Even with fixed reflection coefficients, the objective function remains non-convex due to the fractional structure of the signal-to-interference-plus-noise ratio and the presence of the beamforming vector in both the numerator and the distortion noise terms of the denominator. To tackle this, we employ the widely utilized Charnes-Cooper transformation combined with a semi-definite relaxation approach.

By defining a new positive semi-definite matrix that represents the outer product of the beamforming vector, we can recast the fractional terms into a linear matrix inequality format. We apply a first-order Taylor series expansion to the non-convex parts of the objective function, essentially utilizing the successive convex approximation technique. In each iteration of the successive convex approximation, we replace the original non-convex function with a tight convex lower bound, thereby allowing us to solve the subproblem using standard interior-point methods available in off-the-shelf optimization software. The semi-definite relaxation process involves dropping the rank-one constraint on the newly defined matrix. If the resulting optimal matrix yields a rank greater than one, standard Gaussian randomization techniques are applied to extract a feasible, high-quality rank-one solution.

4.4 Passive Beamforming Optimization at the RIS

The second subproblem, optimizing the phase shift matrix while keeping the satellite beamforming fixed, presents a formidable challenge. The phase shifts are embedded within the cascaded channel matrices, and under the hardware impairment model, the distortion noise power scales directly with the specific alignment of the phase shifts. This means that maximizing the signal power at the user might inadvertently amplify the distortion noise, leading to diminishing returns.

To reformulate this subproblem, we isolate the phase shift variables by rewriting the cascaded channel matrices as functions of a diagonal matrix containing the phase shifts. We then extract the diagonal elements into a single vector. To handle the unit-modulus or bounded amplitude constraints, which form a non-convex feasible set, we utilize the penalty-based successive convex approximation method. We introduce auxiliary variables to decouple the complex constraints and apply a penalty term to the objective function that heavily penalizes any deviation between the optimization variables and the auxiliary variables. The objective function is again linearized using Taylor series expansions around the local point obtained from the previous iteration. This rigorous mathematical procedure ensures that the phase shifts are optimized not only to direct the main lobe of the signal toward the legitimate user but also to actively suppress the leakage toward the eavesdropper, all while carefully managing the amplification of hardware-induced distortion noise.

5. Experimental Results and Discussion

5.1 Simulation Environment Setup

To validate the theoretical analysis and demonstrate the efficacy of the proposed alternating optimization methodology, we conduct extensive Monte Carlo simulations. The simulation environment models a space-air-ground integrated network operating at an altitude appropriate for a low Earth orbit satellite, approximately six hundred kilometers above the Earth's surface. The unmanned aerial vehicle is deployed as a quasi-stationary aerial platform at an altitude of two hundred meters, hovering over a designated coverage area. The legitimate ground user and the eavesdropper are distributed randomly within the terrestrial footprint of the aerial vehicle. We utilize standard 3GPP channel models for non-terrestrial networks to generate the large-scale path loss and small-scale fading coefficients. The hardware distortion parameters are meticulously selected based on empirical data from contemporary millimeter-wave transceiver datasheets, providing a realistic representation of current technological limitations.

Table 2: Simulation System Parameters

Component	Parameter Name	Specified Value
Satellite Array	Number of Antennas	64
Environment	Noise Power Spectral Density	-174 dBm/Hz
Distances	UAV to Ground User	500 meters
Distances	UAV to Eavesdropper	450 meters
Hardware	Receiver Distortion Coefficient	0.05

5.2 Impact of Hardware Impairments on Secrecy Rate

The foremost objective of our numerical evaluation is to explicitly quantify the degradation caused by hardware impairments. We evaluate the achievable secrecy rate as a function of the satellite's total available transmit power. In scenarios where ideal hardware is assumed, the secrecy rate scales logarithmically with increasing transmit power, as the optimization algorithm effectively nulls the signal at the eavesdropper while maximizing the array gain toward the legitimate user. However, when practical hardware impairments are introduced into the simulation, a striking paradigm shift occurs.

As the transmit power increases, the performance under hardware impairments initially follows the ideal curve but quickly diverges. At high transmit power regimes, the secrecy rate begins to saturate, hitting a strict performance ceiling. This ceiling effect is a direct manifestation of the multiplicative nature of the distortion noise. Because the distortion noise variance scales proportionally with the transmit signal power, increasing the satellite power beyond a certain threshold simultaneously increases the noise floor at the receivers. Consequently, the signal-to-interference-plus-noise ratio becomes dominated by the distortion parameters rather than the thermal noise, rendering further power investments entirely ineffective. This critical finding underscores the severe peril of neglecting hardware impairments during the network planning phase; relying on ideal assumptions leads to grossly overestimated security metrics and potentially vulnerable deployments in the field.

5.3 Performance Evaluation of the Proposed Algorithm

We subsequently benchmark the performance of our proposed robust alternating optimization algorithm against several baseline schemes. The primary baselines include a non-robust design that optimizes the system assuming ideal hardware but operates in the impaired environment, a random phase shift scheme where the reconfigurable intelligent surface elements are assigned random phases, and a conventional amplify-and-forward relaying scheme replacing the intelligent surface.

Table 3: Performance Comparison of Optimization Schemes

Optimization Scheme	Secrecy Rate at 30 dBm	Secrecy Rate at 40 dBm
Proposed Robust Algorithm	4.15 bps/Hz	5.82 bps/Hz
Non-Robust Ideal Design	3.20 bps/Hz	4.10 bps/Hz
Random Phase Shift Baseline	1.15 bps/Hz	1.45 bps/Hz
Amplify-and-Forward Relay	2.85 bps/Hz	3.55 bps/Hz

The data presented in the performance comparison table unequivocally demonstrates the superiority of the proposed robust methodology. By explicitly incorporating the hardware distortion mathematical models into the optimization constraints and the objective function, our algorithm intelligently balances the raw signal gain with the detrimental noise amplification. The non-robust design performs adequately at low transmit powers where thermal noise is dominant but fails spectacularly at higher powers because its aggressive beam steering strategies inadvertently maximize the hardware distortion leakage toward the user. Furthermore, the immense gap between the proposed algorithm and the random phase shift baseline highlights the critical necessity of smart, active reconfiguration of the intelligent surface. Without optimized phase control, the surface merely acts as a passive scatterer, offering negligible security benefits. The comparison with the active amplify-and-forward relay demonstrates that the reconfigurable intelligent surface, despite being entirely passive and suffering from component impairments, can achieve superior secrecy performance due to the massive degrees of freedom provided by its numerous reflecting elements.

6. Conclusion and Future Work

6.1 Summary of Contributions

In this comprehensive study, we have addressed the critical challenge of securing space-air-ground integrated networks by leveraging unmanned aerial vehicles equipped with reconfigurable intelligent surfaces, specifically under the restrictive and realistic conditions of hardware impairments. We formulated a rigorous mathematical model that captures the complex multiplicative distortion noise originating from practical transceiver limitations and imperfect intelligent surface components. To maximize the achievable secrecy rate of the system, we developed a sophisticated alternating optimization framework based on successive convex approximation and semi-definite relaxation techniques. This methodology effectively navigates the highly non-convex landscape of the joint active and passive beamforming problem. Through extensive numerical simulations and theoretical analyses, we established that hardware impairments impose a fundamental capacity ceiling on the secrecy rate, a limitation that cannot be overcome simply by increasing the transmission power. Our proposed robust algorithm successfully mitigates these detrimental effects, consistently outperforming non-robust designs and conventional relaying architectures, thereby validating the necessity of impairment-aware optimization in next-generation wireless deployments.

6.2 Future Research Directions

While this paper establishes a strong foundation for secure transmission in realistic aerial-satellite networks, several promising avenues for future research remain open. The current optimization framework relies heavily on the availability of perfect, or near-perfect, channel state information at the centralized controller. In highly dynamic non-terrestrial environments characterized by massive mobility and long propagation delays, acquiring accurate channel state information is immensely challenging. Future studies should investigate robust beamforming designs under bounded channel uncertainty or statistical channel models. Furthermore, the exploration of terahertz frequency bands for satellite-to-aerial links will introduce new forms of hardware limitations, such as severe oscillator phase noise and molecular absorption fading, requiring novel compensatory algorithms. Finally, the integration of advanced machine learning paradigms, particularly deep reinforcement learning and federated learning, offers a powerful alternative to traditional mathematical optimization. These data-driven approaches could potentially learn the highly nonlinear impairment patterns directly from environmental interactions, enabling real-time, adaptive configuration of the reconfigurable intelligent surface in complex, time-varying adversarial scenarios.

References

1. Li, X., Hu, J., & Liu, X. (2020). Harmonic Distortion Optimization for Sigma-Delta Modulators Interface Circuit of TMR Sensors.Sensors,20(4), 1041.
2. Yang, Z., Ji, W., Guo, Q., & Wang, Z. (2023, October). Javp: Joint-aware video processing with edge-cloud collaboration for dnn inference. In Proceedings of the 31st ACM International Conference on Multimedia (pp. 9152-9160).
3. Yang, Z., Ji, W., & Wang, Z. (2024). Adaptive joint configuration optimization for collaborative inference in edge-cloud systems. Science China Information Sciences, 67(4), 149103.
4. Tian, Y., & Yang, Z. (2026, May). SAEC: scene-aware enhanced edge-cloud collaborative industrial vision inspection with multimodal LLM. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 19747-19751). IEEE.
5. Xia, L., Yang, M., Wang, J., Yan, Z., Ren, Y., Yu, G., & Lei, K. (2025, September). Mamba4Net: Distilled Hybrid Mamba Large Language Models For Networking. In2025 IEEE 33rd International Conference on Network Protocols (ICNP)(pp. 1-10). IEEE.
6. Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. IEEE internet of things journal, 8(23), 16779-16786.
7. Luo, H., Li, Q., Cheng, H., Li, W., Sun, W., Zhao, W., & Liu, Z. (2025). A²Tformer: Addressing temporal bias and non-stationarity in transformer-based IoT time series classification. IEEE Internet of Things Journal, 12(20), 42198–42213.
8. Zhang, W., Li, M., & Chen, X. (2026). Distributed Edge-Fog-Cloud Architecture for Intelligent Fault Diagnosis of Permanent Magnet Synchronous Motors Using Temporal Fusion Transformers and Federated Learning. Fundamental Scientific Reports in Multidisciplinary Areas, 2 (02), 121-131.
9. Hu, Y., Yang, Z., Zhao, C., & Ji, W. (2026, May). Adaptive guidance semantically enhanced via multimodal llm for edge-cloud object detection. In ICASSP 2026-2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 12962-12966). IEEE.
10. Li, X., Wang, P., Li, G., Ni, L., & Zhang, Y. (2023). Design of interface circuits and lightweight PUF for TMR sensors. IEEE Sensors Journal, 23(11), 11754-11761.
11. Zhao, Q., & Huang, Y. (2026). DAREA: A Dynamic AI-Driven Architecture for Real Estate Asset Tokenization on Blockchain.Fundamental Scientific Reports in Multidisciplinary Areas,2(02), 182-192.
12. Xu, C., Wang, C., & Li, Z. (2026). H2-LBM: A Hierarchical Hybrid Deep Reinforcement Learning Framework for L7 Load Balancing and Global Traffic Scheduling in Multi-Cloud LLM Serving. Fundamental Scientific Reports in Multidisciplinary Areas, 2 (02), 109-120.
13. Corbett, J. C., Dean, J., Epstein, M., Fikes, A., Frost, C., Furman, J. J., et al. (2013). Spanner: Google’s globally-distributed database. ACM Transactions on Computer Systems, 31(3), Article 8.
14. Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. Communications of the ACM, 59(5), 50–57.
15. Yao, Y., Sun, J., Miao, P., Chen, G., & Tafazolli, R. (2026). Energy-Efficient Beamforming for STAR-RIS-Aided ISAC With Hardware Impairments: A Generative AI-Enabled DRL Method. IEEE Transactions on Wireless Communications.
16. Yang, W., Qin, Y., Jiang, Z., & Chu, X. (2021, June). Traffic Management for Distributed Machine Learning in RDMA-enabled Data Center Networks. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.
17. Li, Y., Zhou, Y., Zhang, Y., Wang, P., Zhang, Y., Li, X., & Zhang, X. (2025). Nonvolatile Optical Switch With a Programmable pn Heterojunction.IEEE Transactions on Electron Devices,72(8), 4030-4035.
18. Yang, W., Qin, Y., & Yang, Z. (2022). A reinforcement learning based data storage and traffic management in information-centric data center networks. Mobile Networks and Applications, 27(1), 266-275.
19. Long, J., Xu, Z., Jiang, T., Yao, W., Jia, S., Ma, C., & Chen, X. (2025, April). Robust SAM: on the adversarial robustness of vision foundation models. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 39, No. 6, pp. 5775-5783).
20. Yao, Y., Lu, Z., Chen, G., Huang, C., Feng, C., & Quek, T. Q. (2026). Interference Management in ISAC-SAGINs Based on Transformer-Enabled Mean-Field Reinforcement Learning Method. IEEE Transactions on Wireless Communications.
21. Wan, H., Zhang, Y., Wang, J., Wu, D., Li, M., Chen, X., ... & Ji, X. (2025). Toward universal embodied planning in scalable heterogeneous field robots collaboration and control. Journal of Field Robotics, 42(5), 2318-2336.
22. Ren, S., Li, X., Shao, Z., Gong, M., & Ren, M. (2025). A Hybrid Structure Noise Shaping SAR ADC.Journal of Circuits, Systems and Computers,34(05), 2550135.
23. Xiao, W., Tan, Q., Chen, M., Yao, Y., & Shu, F. (2026). Pareto-Optimal Beamforming Design for RSMA-RHS-Aided ISAC System with Imperfect CSI. IEEE Transactions on Vehicular Technology.
24. Yang, Y., Ma, X., Li, C., Zheng, Z., Zhang, Q., Huang, G., ... & Zhao, Q. (2021). Believe what you see: Implicit constraint approach for offline multi-agent reinforcement learning. Advances in Neural Information Processing Systems, 34, 10299-10312.
25. Wang, S., Zhang, X., Wang, P., & Li, X. (2026). Design of Magnetic Sensor Array-Based PUFs for IoT Security. IEEE Transactions on Instrumentation and Measurement, 75, 1-9.