Secrecy Enhancement and Distributed Architectures in LEO Satellite Networks: A Survey on AN-Assisted Scheduling and SUSDA Design

Md Sakil Hasan
Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
30224028@o365.hanbat.ac.kr

Md Gulam Ishak
Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
30251284@o365.hanbat.ac.kr

Jihwan Moon
Dept. Mobile Convergence Engineering
Hanbat National University
Daejeon 34158, the Republic of Korea
anschino@staff.hanbat.ac.kr

***Abstract*—The rapid deployment of low Earth orbit (LEO) satellite constellations has created new opportunities for high-capacity, low-latency global communication services. However, the broadcast nature of wireless links and the constraints of satellite hardware present unique challenges for ensuring physical-layer security (PLS). At the same time, emerging distributed satellite architectures promise unprecedented flexibility and scalability in cooperative transmission. This survey highlights two complementary research directions that exemplify these trends. First, we review a secrecy outage analysis that introduces an artificial-noise (AN) assisted scheduling strategy in multi-satellite networks. Second, we examine the Spatial Ultra-Sparse Distributed Antenna (SUSDA) architecture in distributed satellite clusters, which leverages laser inter-satellite links, coherent arraying, and adaptive beam synthesis to deliver large-aperture gains, interference suppression, and reconfigurable transmission.**

***Index Terms*—low Earth orbit (LEO), physical-layer security (PLS), artificial noise (AN), secrecy outage probability(SOP), channel state information (CSI), artificial noise-assisted satellite scheduling (ANSS), user scheduling, distributed antenna, Distributed Satellite Clusters (DSCs),**

I. Introduction

The emergence of large-scale low Earth orbit (LEO) satellite constellations has reshaped the landscape of global communications. Compared with traditional geostationary systems, LEO satellites offer lower latency, higher spatial reuse, and seamless integration with terrestrial networks. These advantages make LEO constellations an attractive platform for supporting broadband Internet access, Internet-of-Things (IoT) connectivity, and mission-critical applications [1]. However, the open nature of wireless propagation combined with the limited hardware resources of small satellites introduces significant challenges in ensuring secure and reliable communications.

Physical-layer security (PLS) has attracted increasing attention as a complementary approach to cryptographic methods. By exploiting channel characteristics such as fading, interference, and noise, PLS enables information-theoretic secrecy without relying solely on computational complexity [2]. Among existing techniques, artificial noise (AN) injection and cooperative transmission have shown promise in improving secrecy performance under adversarial conditions [3]. Nevertheless, the effectiveness of these methods in LEO satellite networks is shaped by unique factors, including dynamic topology, time-varying channels, and resource constraints.

Covert communication seeks to conceal the presence of a transmission from external detectors, providing low-probability-of-detection protection in addition to confidentiality. This concept has seen growing use in modern wireless systems [4]. A widely used technique hides the information signal under AN, allowing the intended receiver to recover it, while NOMA is employed to support covert communications [5].

Parallel to security considerations, distributed satellite architectures have emerged as a transformative design paradigm. In particular, spatial ultra-sparse distributed antenna (SUSDA) systems harness multiple satellites flying in close formation to emulate a large-aperture antenna array. Through coherent combining and advanced beam synthesis, SUSDA architectures enhance link quality, suppress interference, and enable flexible reconfiguration [6]. These capabilities naturally complement PLS strategies by providing new degrees of freedom for secure transmission.

This survey examines two representative research directions that address these issues from complementary perspectives: (i) AN-assisted satellite scheduling for secrecy outage minimization [7], and (ii) SUSDA architectures for distributed cooperative transmission [8]. The scope of the survey is twofold: first, to review the models, assumptions, and findings of each approach; and second, to explore potential synergies and open

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2021R1I1A3050126). This research was partially supported by the MSIT(Ministry of Science and ICT), Korea, under the ICAN(ICT Challenge and Advanced Network of HRD) support program(IITP-2025-RS-2022-00156212) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation). This work was partially supported by the IITP(Institute of Information & Coummunications Technology Planning & Evaluation)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2025-RS-2024-00437886, 33%).

problems at the intersection of physical-layer security and distributed satellite architectures. By consolidating insights from both works, this survey aims to outline a research agenda for secrecy-aware cooperative transmission in next-generation LEO satellite networks.

II. Background

A. Physical-Layer Security in LEO Satellite Networks

Fifth-generation (5G) and emerging sixth-generation (6G) networks aim to deliver higher data rates, ultra-low latency, and massive connectivity across heterogeneous smart devices while maintaining strong user-data security [9].

To protect user and control traffic, the RAN employs standardized ciphering and integrity suites—for example, AES-based 128-EEA2 (LTE) and 128-NEA2 (5G) for encryption, together with integrity algorithms 128-EIA2 (LTE) and 128-NIA2 (5G)—at the appropriate protocol layers, ensuring confidentiality and integrity against interception and eavesdropping [10]. Among alternative approaches, physical-layer security (PLS) has attracted growing interest. By leveraging intrinsic channel characteristics, PLS exploits propagation randomness and structure to prevent unauthorized access and reduce susceptibility to eavesdropping [11].

Recently, satellite-communications research and development have seen renewed focus. As satellite-based wireless services expand, security concerns have intensified because large-scale space information networks are vulnerable to adversarial eavesdropping. Over the past decade, PLS has matured into a complementary protection layer for satellite communications [12]. In [13] investigated PLS for the Low Earth Orbit (LEO)-enabled IoT uplink using a stochastic-geometry framework. It emulated a multi-tier, multi-operator constellation in which satellites acted as legitimate receivers or potential eavesdroppers and incorporated an artificial-noise (AN) scheme via power allocation to quantify the security gains.

Recent studies have examined the secrecy performance of systems that employ a friendly-jammer satellite transmitting AN, while limiting leakage to the legitimate ground user [14]–[16]. For example, the authors investigated the secrecy performance of a LEO satellite communication system under Nakagami-m fading and proposed a scheme in which a friendly jammer satellite transmits AN toward the eavesdropper while limiting leakage to the legitimate ground user [14]. In [15] a robust secure precoding algorithm for multi-beam satellite non-orthogonal multiple access(NOMA) maximizes the secrecy rate by employing Unmanned Aerial Vehicles (UAVs) transmitting AN to protect legitimate users against eavesdropping. In [16] the authors proposed a secure user-scheduling scheme for multiuser single-input multiple-output (SIMO) wiretap networks that improved secrecy-outage performance (SOP) and derived closed-form SOP expressions under maximum-ratio combining (MRC) at both the desired receiver and eavesdropper, while operating without instantaneous eavesdropper channel state information (CSI).

We survey the SOP of multi-satellite networks (e.g., LEO constellations) under eavesdropping by jointly scheduling satellites for data transmission and AN injection.

B. Distributed Satellite Architectures and SUSDA

Distributed Satellite Clusters (DSCs) have emerged as a promising architecture for next-generation non-terrestrial networks (NTNs), addressing the inherent limitations of single-satellite platforms in antenna performance and in-orbit reconfiguration [2]. Building on this concept, the Spatial Ultra-Sparse Distributed Antenna (SUSDA) enables multiple small satellites to form a virtually large, distributed antenna array, thereby enhancing system capacity, strengthening anti-interference capabilities, supporting integrated sensing and communication (ISAC), and relying on enabling technologies such as inter-satellite links, precise synchronization mechanisms, and advanced interference management strategies. Future research is expected to focus on optimizing the performance, efficiency, and scalability of DSC- and SUSDA-based systems.

Beyond terrestrial networks, multi-antenna techniques plays a critical role in satellite communications also, where advanced beamforming enhances link robustness and capacity by precisely directing signals toward targeted regions on Earth [17]–[19]. These technologies are additionally essential in specialized applications, including radar and navigation for aerospace and maritime sectors, as well as in improving safety for autonomous vehicles and aircraft systems [20], [21].

III. Secrecy in LEO via AN-Assisted Scheduling

AN has been widely studied as an effective tool for physical-layer security, particularly in multi-antenna terrestrial networks. Extending this concept to satellite networks, the recent work [7] has investigated the use of coordinated satellites to transmit data and AN simultaneously. The key idea is to leverage the constellation-wise inherent spatial diversity by assigning one satellite to deliver confidential data while another transmits artificial noise to confuse potential eavesdroppers.

A. System Model

The considered scenario is illustrated in Figure 1. A LEO satellite transmits data to the ground base station (GBS), while a malicious UAV attempts to eavesdrop on the satellite-to-ground signal. The network comprises a cluster of M LEO satellites, a single GBS, and the UAV eavesdropper. Each satellite is equipped with a single antenna, whereas the GBS and the UAV employ antennas.

We let $\alpha^\star$ and $\beta^\star$ denote the scheduled-satellite indices for data and AN transmission, respectively. Using linear receive weight vectors, the achievable rates at the GBS and the malicious UAV are given by [7]:

$$r_g = \log_2\left(1 + \frac{\|\mathbf{w}_g^{\mathrm{H}}\mathbf{h}_{\alpha^\star}\|^2}{\|\mathbf{w}_g^{\mathrm{H}}\mathbf{h}_{\beta^\star}\|^2 + 1/\rho_g}\right), \tag{1}$$

$$r_u = \log_2\left(1 + \frac{\|\mathbf{w}_u^{\mathrm{H}}\mathbf{s}_{\alpha^\star}\|^2}{\|\mathbf{w}_u^{\mathrm{H}}\mathbf{s}_{\beta^\star}\|^2 + 1/\rho_u}\right). \quad (2)$$

Here, ρ_g and ρ_u denote the transmit signal-to-noise ratio (SNR), defined as $\rho_g \triangleq \frac{P_T}{\sigma_g^2}$ and $\rho_u \triangleq \frac{P_T}{\sigma_u^2}$, respectively The GBS knows the instantaneous CSI via channel estimation, whereas the CSI between the satellite and the UAV is unavailable at the GBS—a realistic assumption under passive eavesdropping [7]. Hence, the authors in [7] evaluated secrecy using the SOP rather than the instantaneous secrecy rate, defined as

$$P_{\mathrm{so}}(\tau) \triangleq \Pr\{\, r_g - r_u < \tau \,\}. \quad (3)$$

where r_g and r_u are given in (1)-(2), and τ denotes the secrecy rate threshold.

B. AN-Assisted Satellite Scheduling

The GBS exploits pilot-based downlink CSI to select (i) a data satellite with a strong channel and (ii) an AN satellite whose interference can be mitigated via linear weight vectors at the GBS. Secrecy performance is analyzed under Nakagami-m fading for both single- and multi-antenna receivers at the GBS and a UAV eavesdropper. An algorithm to select the best transmit and AN satellites and optimize the beamforming vector was provided by [7]. Meanwhile, an alternative algorithm to solve the optimization problem can be designed as in Algorithm 1.

Algorithm 1 Artificial Noise-Assisted Satellite Scheduling

Input: $\{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_M\}$ //a set of channel vectors
Output: $\alpha^\star \leftarrow 0$, $\beta^\star \leftarrow 0$, $\mathbf{w}_g \leftarrow 0$, $\mu \leftarrow 0$
for $i \in \{1, \ldots, M\}$ **do**
  $i^\star = \arg\min \|\mathbf{h}_i\|$ //pick AN satellite candidate
  Calculate $\mathbf{P}_{i^\star} = \frac{\mathbf{h}_{i^\star}\mathbf{h}_{i^\star}^{\mathrm{H}}}{\|\mathbf{h}_{i^\star}\|^2}$ // Projection matrix
  Set $\mathbf{w}_{i^\star} \in svd(\mathbf{P}_{i^\star})$ // Nullspace of $\mathbf{h}_{i^\star}$
  for $j \in \{1, \ldots, M\} \setminus \{i^\star\}$ **do**
    if $\left\|\mathbf{w}_{i^\star}^{\mathrm{H}}\mathbf{h}_j\right\| > \mu$ **then**
      Update $\alpha^\star \leftarrow j$
      Update $\mu \leftarrow \left\|\mathbf{w}_{i^\star}^{\mathrm{H}}\mathbf{h}_j\right\|$
      $\mathbf{w}_g \leftarrow \mathbf{w}_{i^\star}$
      $\beta^\star \leftarrow i^\star$;
    end if
  end for
end for

In [7], Algorithm 1 achieves optimal pair selection for the stated metric at the expense of an $M-$fold increase in nullspace computations and a quadratic inner-product complexity $\mathcal{O}(M^2 n)$, yielding higher latency; by contrast,the above Algorithm1 is a greedy, low-complexity scheduler with per-decision complexity $\mathcal{O}(n^3) + \mathcal{O}(Mn)$, equires minimal CSI/signaling, and attains lower latency.

C. Secrecy Outage Analysis

The authors derived a closed-form expression for the SOP under the proposed scheme in the single-antenna case. Using (1) and (2), the final SOP in (2) is rewritten as

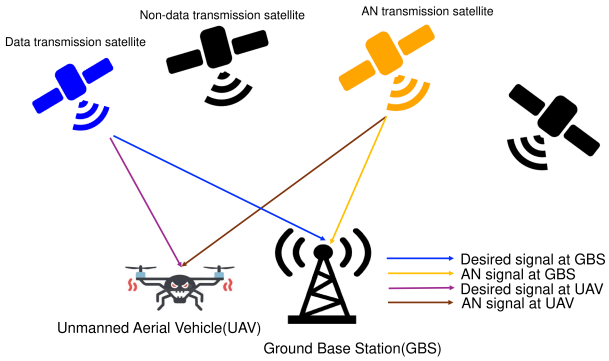

Fig. 1: System model in [7]

$$p_{\mathrm{so}}(\tau) = M\left(\frac{m^m}{\Gamma(m)}\right)^3 \sum_{a=0}^{M}\sum_{b=0}^{M}\sum_{d=0}^{M}\sum_{e=0}^{b}\sum_{i=0}^{m}\sum_{p=0}^{b}\sum_{v=0}^{p-m-i} \times \sum_{q=0}^{\infty} e^{m\sigma^2(a-\lambda)}(-1)^{a+b-p+q}\binom{M}{a}\delta_{b,a}\,\beta_t \times a^{b+d}\sigma^{2(e+m-i)}\binom{b}{e}\binom{m}{i}\binom{p-m-i}{v} \times \binom{j+q-1}{q}2^{\tau v}A^{-j-v}\lambda^v\Gamma(m+d+b-e) \times \Gamma(m+i)\frac{\Gamma(m+v+q)}{(m\sigma^2(\lambda+1))^{m+v+q}} \quad (4)$$

where $j = a + d + b - e$, $\lambda = a\,2^\tau$, $A = M - a + \lambda$ and $\sigma^2 = \sigma_g^2 = \sigma_u^2$

The authors in [7] assumed that each channel coefficient follows Nakagami-m fading. The same shape parameter m is used for both the GBS-satellite and UAV-satellite links, while allowing the scale parameter to differ across the two links. Coefficients within each vector are independent and identically distributed (i.i.d), and the same assumptions apply to all satellites.

D. Key Findings and Limitations

In [7] the authors proposed an ANSS scheme that jointly selects one satellite for data transmission and another for artificial-noise injection in LEO networks under Nakagami-m fading. They further derived a closed-form SOP for the single-antenna case. As future work, one may develop real-time, low-complexity variants of AN-assisted scheduling that scale to large constellations. The findings also suggest practical applications, such as a military defense.

IV. SUSDA: Capabilities and Challenges

Distributed satellite architectures have emerged as a promising solution to overcome the size, weight, and cost limitations of single large-aperture antennas. Among them, the SUSDA concept represents a paradigm shift in constellation design, enabling multiple satellites to operate cooperatively as a large, reconfigurable antenna array.

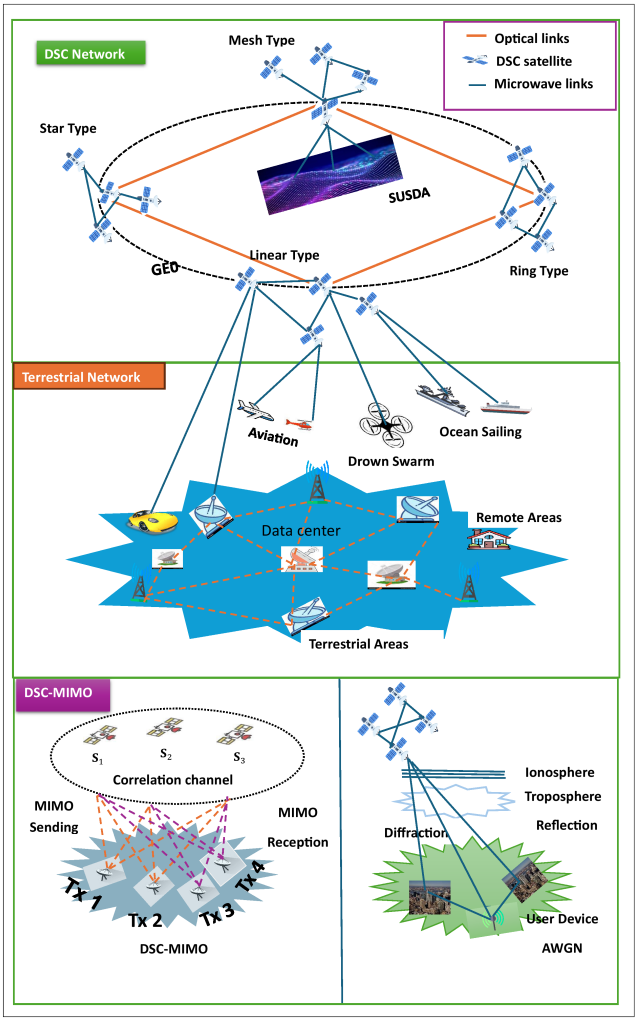

Fig. 2: Architecture of SUSDA satellite-ground collaborative transmission in [8]

A. Architectural Overview

The network architecture appears in Fig. 2. The SUSDA architecture integrates distributed antennas and inter-satellite synchronization to enable coherent multi-satellite beamforming. Small-aperture antennas on DSC satellites form a virtual array, providing high SNR outputs and supporting flexible topologies, including linear, ring, star, or hybrid formations.

In the uplink, ground RF signals are delay-compensated, converted, and shared via inter-satellite links, with cross-correlation ensuring precise synchronization. In the downlink, satellites pre-compensate for geometric delays, allowing ground terminals to recover synchronized signals through phase adjustment and demodulation. This cooperative design enables reliable, high-throughput space-ground connectivity.

B. Key Enabling Technologies

1) Inter-Satellite Links (ISLs): ISLs are crucial for real-time coordination among Distributed Satellite Clusters (DSCs). Optical (laser) ISLs are preferred over microwave due to higher capacity, lower power consumption, and reduced interference; however, challenges such as visibility, connectivity, and antenna size persist. Robust ISLs provide the backbone for delay compensation, synchronization, and distributed processing in SUSDA architectures

2) DSC-MIMO Transmission: DSC-MIMO leverages spatial diversity and multiplexing by employing multiple antennas across satellites and ground stations. In the uplink, ground transmitters apply MIMO encoding, satellites forward the signals, and ground receivers perform decoding. This distributed architecture enhances spectral efficiency and provides improved resilience against fading and interference

3) Synchronization and Delay Compensation: Precise synchronization is essential due to kilometer-scale satellite spacing. Each DSC node calculates and compensates for geometric delays, with results shared via inter-satellite links (ISLs). Cross-correlation is employed to refine timing and support coherent beamforming. In the downlink, phase-aligned transmissions enable reliable signal recovery, preserving array coherence in dynamic orbital environments

C. Challenges and Design Issues

1) Grating Lobes and Sidelobes: As an ultra-sparse array, SUSDA generates strong grating lobes that reduce antenna gain and degrade localization performance. Mitigation requires non-periodic array configurations and intelligent optimization techniques. Sparse array synthesis methods are employed to suppress grating lobes while maintaining safe inter-satellite spacing

2) Channel Modeling: SUSDA channels are affected by mobility-induced fading, multipath propagation, and Doppler shifts. High correlation among satellites constrains both capacity and reliability. Correlated shadowed Rice fading models, along with techniques such as signal diversity, spatial multiplexing, and advanced channel estimation, can be employed to mitigate these effects

3) Adaptive Anti-Interference: Dynamic interference requires adaptive control. SUSDA leverages real-time sensing, beamforming adjustment, and deep reinforcement learning (DRL)-based strategies to optimize anti-interference performance while maintaining service quality, thereby ensuring robust operation under challenging conditions

4) Mobility and Integration: Mobility across orbits introduces challenges in synchronization and channel stability. Extending SUSDA to low Earth orbit (LEO) necessitates precise navigation and alignment, whereas integration with geostationary orbit (GEO) satellites provides redundancy. Coupling SUSDA with multi-access edge computing (MEC) platforms enables distributed computation, thereby reducing latency and enhancing system reliability.

D. Research Opportunities

Future research in satellite communications encompasses several critical areas. Advanced channel modeling and estimation remain essential, as current models cannot fully capture Doppler, multipath, and delay effects in ultra-sparse

constellations. Machine learning-driven prediction and hybrid deterministic-stochastic models for GEO, MEO, and LEO channels represent promising directions. Similarly, intelligent grating lobe and sidelobe suppression is necessary, since ultra-sparse arrays generate strong lobes that degrade performance. AI-assisted array design and real-time reconfigurable synthesis could dynamically mitigate lobes and enhance beamforming. Adaptive anti-interference schemes based on deep reinforcement learning (DRL) also show potential but face scalability challenges; future work may explore multi-agent RL, federated learning, and cross-layer AI models to enable robust interference mitigation. Synchronization and delay compensation at scale remain critical, motivating investigations into quantum clock distribution, GNSS-free timing, and joint communication-sensing synchronization to improve system robustness.

Other research directions include the integration of non-terrestrial networks with multi-access edge computing (MEC) and edge intelligence, mobility management in LEO and multi-orbit systems, and the development of novel modulation schemes. Lightweight MEC nodes on satellites possess limited computing power, necessitating energy-aware task scheduling strategies across satellites, GEO relays, and ground stations. LEO expansion further requires stable swarm formation and cross-orbit integration, which may be enabled through swarm intelligence algorithms and standardized multi-orbit protocols. Finally, orthogonal time-frequency space (OTFS) modulation offers strong Doppler resilience but must be integrated with MIMO and multiple access schemes; combining OTFS with NOMA or SCMA may unlock new capabilities for high-mobility 6G non-terrestrial networks.

V. Joint Design Opportunities

The two research directions reviewed in this survey—AN-assisted scheduling for secrecy enhancement and SUSDA-based distributed architectures—approach the problem of secure LEO communication from complementary perspectives. While the former develops analytical tools and scheduling strategies to minimize secrecy outage, the latter provides a cooperative physical infrastructure capable of amplifying such techniques. Their integration offers several promising opportunities.

A. Distributed Artificial-Noise Beamforming

AN-assisted scheduling has demonstrated that even a single AN-transmitting satellite can significantly improve secrecy. Within a SUSDA architecture, multiple satellites could jointly transmit AN in a phase-coherent manner, effectively shaping interference patterns. This would allow the constellation to direct AN energy toward potential eavesdroppers while nulling it at legitimate receivers, thereby extending single-satellite AN strategies into constellation-scale beamforming.

B. Secrecy Outage with Correlated Channels

The secrecy outage analysis in current AN-assisted schemes assumes independent fading channels. In contrast, SUSDA emphasizes channel correlation across closely spaced satellites. Incorporating correlated fading into secrecy outage probability analysis would yield more realistic performance bounds and could inform optimal satellite spacing and formation design for secrecy enhancement.

C. Robust Scheduling under Synchronization and Delay Constraints

The AN-assisted scheduling framework assumes perfect CSI at the GBS and negligible coordination delay. SUSDA architectures, however, must contend with synchronization errors, ISL latency, and Doppler dynamics. Extending secrecy-aware scheduling to account for delayed or imperfect CSI would make the framework more robust and practical in distributed satellite clusters.

D. Joint Array Pattern and Security Optimization

SUSDA research has highlighted the need to suppress grating lobes and optimize sparse array layouts. By integrating secrecy objectives, array synthesis could be extended to jointly minimize sidelobe leakage and maximize secrecy capacity. This would enable simultaneous optimization of communication performance and physical-layer security, aligning with the broader trend of multi-objective constellation design.

E. Learning-Based Security Adaptation

Both AN-assisted secrecy schemes and SUSDA anti-interference strategies can benefit from machine learning. Reinforcement learning could be applied to dynamically allocate satellites for data versus AN roles, adapt beam patterns under adversarial conditions, and balance tradeoffs between throughput, interference suppression, and secrecy performance.

VI. Conclusion

This survey has reviewed two complementary research directions addressing these challenges. The first was AN assisted scheduling, which leverages cooperative satellites to minimize secrecy outage probability and demonstrates the potential of constellation-scale diversity for physical-layer security. The second was the SUSDA architecture, which exploits tightly coordinated satellite clusters to emulate large-aperture arrays, enabling coherent combining, interference suppression, and flexible reconfiguration. Together, these approaches highlighted the dual importance of secrecy strategies and distributed architectures in shaping the future of secure LEO networks. Their integration offered promising opportunities such as distributed AN beamforming, secrecy-aware array synthesis, and learning-enabled adaptive security. At the same time, several open problems remain, including multi-antenna secrecy analysis under correlated channels, robust scheduling under imperfect CSI, and geometry-aware secrecy optimization. Looking ahead, the convergence of physical-layer security and distributed cooperative architectures will play a pivotal role in the design of next-generation satellite communication systems. By unifying secrecy objectives with constellation-scale cooperation, future LEO networks can achieve both high capacity and strong resilience against

eavesdropping, advancing toward secure and intelligent global connectivity.

REFERENCES

[1] O. Kodheli, E. Lagunas, N. Maturo, and S. K. Sharma, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys and Tutorials*, vol. 23, pp. 70 – 109, 2021.

[2] P. Devi, M. R. Bharti, and D. Gautam, "A Survey on Physical Layer Security for 5G/6G Communications over Different Fading Channels: Approaches, Challenges, and Future Directions," *Vehicular Communications*, vol. 53, June 2025.

[3] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[4] M. S. Hasan and J. Moon, "Detection Error Probability Maximization for Relay-Based Covert Communications," *The Journal of Korean Institute of Communications and Information Sciences*, 2024.

[5] X. Chen, J. An, Z. Xiong, C. Xing, N.Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, April 2023.

[6] Y. He, P. Yang, Y. Man, C. Wang, and C. Qi, " Spatial Ultra-Sparse Array Formation on LEO Distributed Satellite Cluster: An Enhanced Hybrid Particle Swarm Method," *IEEE Journal of Selected Topics in Signal Processing*, vol. 19, no. 5, pp. 447 – 460, March 2025.

[7] Y. Lee, T. Kim, and I. Bang, "Secrecy Outage Probability of Secure Transmission with Artificial Noise in Low Earth Orbit Satellite Networks," *Proc. ICC 2025 - IEEE International Conference on Communications, Montreal, Canada*, pp. 1–6, 8–12 June 2025.

[8] Y. He, C. Wang, C. Qi, and Z. Feng, "Spatial Ultra-Sparse Distributed Antenna Satellite-Ground Cooperative Transmission Architecture: Challenges, Key Technologies, and Trends," *IEEE Commun. Mag.*, vol. 62, no. 9, pp. 136–143, September 2024.

[9] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G Security Threat Assessment in Real Networks," *Communications Security in Wireless and Mobile Networks*, August 2021.

[10] P. Scalise, M. Boeding, M. Hempel, H. Sharif, and J. Reed, "A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas," *5G Security: Challenges, Opportunities, and the Road Ahead*, February 2024.

[11] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An Overview of Key Technologies in Physical Layer Security," *Entropy Reviews*, November 2020.

[12] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet of Things Journal*, vol. 7, pp. 33–52, January 2020.

[13] A. Talgat, R. Wang, M. A. Kishk, and M. S. Alouini, "Enhancing Pysical Layer Security inn LEO Satellite-Enabled IoT Network Communications," *IEEE Internet of Things Journal*, vol. 11, pp. 33967 – 33979, October 2024.

[14] D. Na, K. H. Park, Y. C. Ko, and M. S. Alouini, "Physical Layer Security for LEO Satellite Communication Systems with Friendly Jamming Satellite," *IEEE Transactions on Wireless Communications*, pp. 1–1, May 2025.

[15] M. Huang, G. Li, F. Gong, Z. Yin, X. Li, A. Nallanathan, and Z. Ding, "Robust Secure Precoding for UAV-Aided multi-beam Satellite NOMA Communications," *EEE Transactions on Vehicular Technology*, vol. 73, pp. 8069 – 8082, June 2024.

[16] I. Bang, S. M. Kim, and D. K. Sung, "Artificial Noise-Aided User Scheduling from the Perspective of Secrecy Outage Probability," *EEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7816 – 7820, JAugust 2018.

[17] L. You, K.-X. Li, J. W. X. Gao, X.-G. Xia, and B. Ottersten, " Massive MIMO transmission for LEO satellite communications ," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1851–1865, 2020.

[18] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, and S. K. et al., " Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 1, pp. 70–109, 2020.

[19] J. Heo, S. Sung, H. Lee, I. Hwang, and D. Hong, " MIMO satellite communication systems: A survey from the PHY layer perspective," *IEEE Commun. Surv. Tutorials*, vol. 25, pp. 1543 – 1570, July 2023.

[20] J. Li and P. Stoica, " MIMO radar with colocated antennas," *IEEE Signal Process Mag.*, vol. 24, no. 5, pp. 106–114, 2007.

[21] J. Li and P. Stoica, " MIMO radar with colocated antennas," *IEEE Signal Process Mag.*, vol. 24, no. 5, pp. 106–114, 2007.