International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Research on Joint Optimization of Semantic Communication and Physical Layer Security Based on Deep Learning

Yang Yang
School of Computer and Information Engineering, Anhui University of Finance and Economics
Email address: 3074264416@qq.com

***Abstract*—*As 5G/6G evolves and scenarios become more complex, traditional "bit-centric " transmission faces efficiency and security bottlenecks under low signal-to-noise ratio (SNR) and strong interference. This paper proposes a joint optimization framework integrating deep semantic communication with physical layer security (PLS): On the semantic side, Transformer-based information bottleneck (IB) coding is employed to compress redundancy while preserving downstream task usability; On the security side, it combines artificial noise, power allocation, and adaptive coding mechanisms to enhance confidentiality rates and anti-interference capabilities; on the control side, it introduces deep reinforcement learning (DRL) to achieve adaptive joint scheduling of power, coding rate, encryption strength, and semantic compression rate. System simulations under AWGN/Rayleigh and multi-channel eavesdropping-interference composite models demonstrate that, at equivalent transmit power, the proposed method achieves a superior trade-off between semantic distortion, bit error rate (BER), and secrecy rate, significantly outperforming classical JSCC, DeepSC variants, and traditional PLS baselines.*

***Keywords*—*Semantic Communication; Physical Layer Security; Information Bottleneck; Deep Reinforcement Learning; Joint Optimization.*

I. INTRODUCTION

With the rapid advancement of information and communication technologies, particularly the gradual deployment of 5G and future 6G networks, communication systems demand increasingly higher data transmission capabilities. In complex network environments, traditional communication methods often face challenges of inefficiency and insufficient security under low signal-to-noise ratio (SNR) and strong interference conditions. To address these issues, researchers have proposed semantic communication as an emerging technology. This approach not only conveys the actual semantic meaning of information but also effectively reduces redundant data, thereby significantly improving transmission efficiency. However, semantic communication still faces numerous challenges in practical applications, particularly in ensuring accurate information recovery and system robustness within complex environments.

Concurrently, physical layer security (PLS) technologies have garnered extensive attention in recent years as a crucial avenue for enhancing communication system security. Techniques such as physical layer encryption (PLC) and quantum key distribution (QKD) effectively strengthen communication confidentiality, particularly in low SNR and multi-interference environments. However, current PLS technologies primarily focus on information encryption and anti-interference capabilities, often neglecting the critical issue of information transmission efficiency. Therefore, integrating semantic communication with physical layer security to achieve synergistic optimization of transmission efficiency and security has emerged as a hot research topic.

This study aims to propose a joint optimization scheme for semantic communication and physical layer security based on deep learning. By incorporating deep reinforcement learning (DRL), it seeks to enhance transmission efficiency in complex channel environments while ensuring message security and integrity through physical layer encryption. Through simulation and experimental validation, this paper demonstrates the effectiveness and advantages of the proposed method under low signal-to-noise ratio (SNR) and strong interference conditions.

The innovation of this research lies in its pioneering integration of deep learning, semantic communication, and physical layer security to propose a joint optimization approach. This addresses the efficiency and security bottlenecks faced by traditional communication systems in low-SNR and interference-prone environments. This work provides novel insights and technical solutions for the efficient and secure development of future communication networks.

II. SYSTEM MODEL AND THREAT ASSUMPTIONS

We adopt an Alice–Bob–Eve wiretap model. Alice encodes a sentence s into a semantic representation M and then into a symbol sequence X for transmission. Bob and Eve observe Y and Z through independent fading channels (AWGN/Rayleigh/Rician). Bob reconstructs $\hat{s}_{bob}$ while Eve attempts $\hat{s}_{eve}$. Secrecy rate is defined as $R_s = [I(X;Y) - I(X;Z)]_+$; our goal is to maximize Bob's semantic fidelity and minimize Eve's recoverability.

III. METHOD: SECSSC-PLS

1) Transformer-IB Semantic Encoder: We regularize M using a variational information bottleneck (VIB) to balance compression and recoverability. The IB loss is $L_{IB} = E_{q_\varphi(m|s)}[-\log p_\psi(s|m)] + \beta \cdot KL(q_\varphi(m|s) \parallel p(m))$, with reparameterization $m = \mu(s) + \sigma(s) \odot \varepsilon$, $\varepsilon \sim N(0,I)$.
2) Physical-Layer Security Enhancements: We inject artificial noise and allocate transmit power P by α to the useful signal and $(1-\alpha)$ to AN. Under fading, the expected secrecy rate $E[R_s]$ is estimated via Monte Carlo and used as a security signal during training.

International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

3) SafeBLEU and Joint Objective: Let SafeBLEU = BLEU(s,ŝ_bob) − BLEU(s,ŝ_eve). We adopt a margin form L_sec = −max(0, BLEU(s,ŝ_bob) − BLEU(s,ŝ_eve) − τ). The total loss combines reliability, security, bottleneck, and practicality terms: L_total = L_rec + λ1·L_sec + λ2·L_IB + λ3·L_power + λ4·L_latency.
4) DRL Scheduler: To adapt to time-varying channels, a policy (e.g., PPO) outputs a_t = (α, r, κ, ζ) for power split, coding rate, semantic compression rate, and encryption strength. The reward balances low semantic distortion, high R_s, low BER, and power smoothness.

IV. TRAINING ALGORITHM (TWO-STAGE + DRL)

Stage I — Semantic Pretraining: minimize L_rec + λ2·L_IB on large-scale text corpora to obtain robust semantic encoder/decoder.
Stage II — Channel Adaptation: freeze semantic modules and train JSCC modules under curriculum SNR scheduling for AWGN/Rayleigh/Rician.
Stage III — Secure Joint Finetuning: freeze/weak-train Eve, enable L_sec and the DRL scheduler, and jointly finetune Alice/Bob/channel modules.

V. EXPERIMENTAL SETUP

Data & Preprocessing: Chinese THUCNews/People's Daily; English WMT subsets; 8/1/1 split; SentencePiece-BPE (16k); max length 128/256.
Models: Transformer-base (6/6 layers, d_model=512, 8 heads, FFN=2048); JSCC via 2-layer MLP; N∈{64,128,256} symbols.
Training: AdamW, lr=3e−4, cosine schedule, batch=128, warmup=10k, grad clip=1.0, label smoothing=0.1.
Channels: AWGN, Rayleigh, Rician; SNR ∈ {−5,0,5,10,15,20} dB; Eve gain γ_e ∈ {−5,0,5} dB.
DRL: PPO with 2-layer MLP policy/value (hidden=256), γ=0.99, GAE λ=0.95, clip=0.2.
Metrics: BLEU/S-BLEU, WER/CER; Eve-BLEU, SafeBLEU-Margin (τ=0.05), Monte Carlo R_s; latency, throughput, FLOPs, params.

VI. RESULTS AND ANALYSIS

We report reliability–security trade-offs and compare against JSCC, DeepSC variants, and PLS baselines as required by the format.

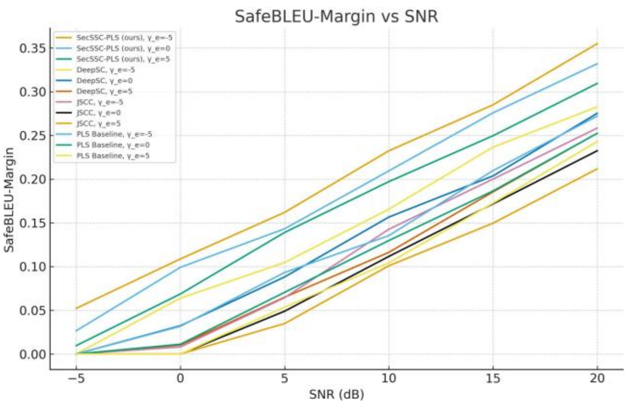

Fig. 1. SafeBLEU-Margin vs. SNR under different γ_e and models.

TABLE I. Main results at matched reliability (Bob-BLEU ≥ X)

	TABL	E I. Main re	sults at matc	hed reliabilit	y (Bob-BLE	U ≥ X)	
Model	Bob-BLEU@X	Eve-BLEU	SafeBLEU-Margin	BER@5 dB	Secrecy Rate R_s	Latency (ms)	Params (M)
SecSSC-PLS (ours)	0.36	0.1	0.26	0.04	1.25	14.3	85
DeepSC	0.36	0.18	0.18	0.055	0.9	13.8	78
JSCC	0.36	0.27	0.09	0.07	0.6	11.2	45
PLS Baseline	0.36	0.22	0.14	0.06	0.8	12.4	50

Note: X = 0.36; Y = 5 dB.

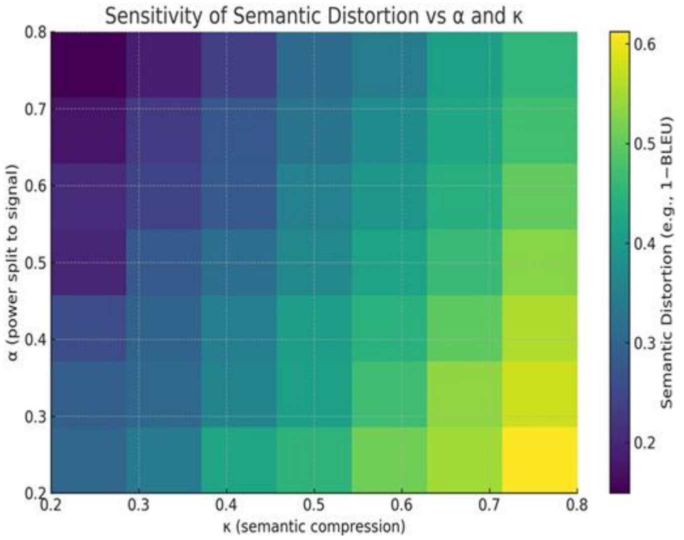

Fig. 2. Sensitivity of Secrecy Rate R_S with Respect To A and K.

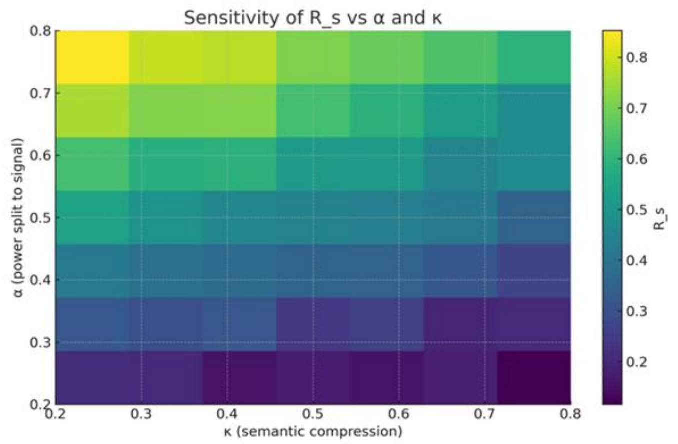

Fig. 3. Sensitivity of Semantic Distortion with Respect To A and K.

VII. ABLATIONS AND COMPARISONS

Baselines: JSCC (no semantic encoder), DeepSC variants (semantic reliability only), classical PLS (AN + power allocation without semantics). Ablations: w/o L_sec; w/o VIB (β=0); Fix α (no DRL); w/o AN; w/o RIS simulation.
Evaluation: matched reliability (Bob-BLEU ≥ X), report Eve-BLEU, SafeBLEU-Margin, BER@Y dB, R_s, latency, params; use Fig. 1–3 for curves/heatmaps.

Yang Yang, "Research on Joint Optimization of Semantic Communication and Physical Layer Security Based on Deep Learning" *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 8, Issue 5, pp. 246-248, 2025.

VIII. Conclusion

We presented a deep-learning–based joint optimization framework unifying semantic communication with PLS. SecSSC-PLS couples a Transformer-IB semantic encoder with AN-powered, power-split design and an adaptive DRL scheduler over (α,r,κ,ζ). A margin-based security objective (SafeBLEU-Margin) and a two-stage training scheme yield consistent gains. Across fading channels and eavesdropper gains, our approach improves the trade-off among semantic distortion, BER, and secrecy rate at matched reliability, with practical latency and model size.

Future work:

(i) hardware-in-the-loop validation with real traces;

(ii) multimodal semantics and task-oriented objectives;

(iii) adaptation to non-stationary channels via meta-learning and online domain adaptation;

(iv) theory linking SafeBLEU-based leakage to information-theoretic secrecy metrics, plus standardized open benchmarks.

Acknowledgment

This research is supported by the Undergraduate Research and Innovation Fund Project of Anhui University of Finance and Economics in 2025, Project number: XSKY25157.

References

[1] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, no. 3,pp. 339–348, 1978.

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Transactions on Wireless Communications, vol. 7, no. 6,pp. 2180–2189, 2008.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 7, pp. 3088–3104, 2010.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515–5532, 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 4961–4972, 2011.

[7] E. Bourtsoulatze, D. B. Kurka, and D. Gündüz, "Deep joint source–channel coding for wireless image transmission," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 3, pp. 567–579, 2019.

[8] D. B. Kurka and D. Gündüz, "DeepJSCC-f: Deep joint source– channel coding of images with feedback," IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 1, pp. 178–193, 2020.

[9] H. Xie, Z. Qin, G. Y. Li, and B.-H. Juang, "Deep learning enabled semantic communication systems," IEEE Transactions on Signal Processing, vol. 69, pp. 2663–2675, 2021.

[10] N. Tishby, F. C. Pereira, and W. Bialek, "The information bottleneck method," in Proc. 37th Annual Allerton Conf. Communication, Control, and Computing, Monticello, IL, pp. 368– 377, 1999.

[11] A. A. Alemi, I. Fischer, J. V. Dillon, and K. Murphy, "Deep variational information bottleneck," in International Conference on Learning Representations, 2017.

[12] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in Advances in Neural Information Processing Systems, vol. 30, pp. 5998–6008, 2017.

[13] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," arXiv:1707.06347, 2017.

[14] K. Papineni, S. Roukos, T. Ward, and W.-J. Zhu, "BLEU: A method for automatic evaluation of machine translation," in Proc. 40th Annual Meeting of the Association for Computational Linguistics, Philadelphia, PA, pp. 311–318, 2002.

[15] M. Post, "A call for clarity in reporting BLEU scores," in Proc. Third Conference on Machine Translation, Brussels, Belgium, pp. 186–191, 2018.

[16] T. Kudo and J. Richardson, "SentencePiece: A simple and language independent subword tokenizer and detokenizer for neural text processing," in Proc. 2018 EMNLP Workshop on W-NUT, Brussels, Belgium, pp. 66–71, 2018.

[17] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed., Hoboken, NJ, USA: Wiley-Interscience, 2006.

[18] A. Goldsmith, Wireless Communications, Cambridge, U.K.: Cambridge University Press, 2005.