Secure Semantic Communication System Design and Optimisation

Xuesong Liu

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

James Watt School of Engineering
College of Science and Engineering
University of Glasgow

17/06/2026

Abstract

Semantic communication (SemCom) has emerged as a promising communication paradigm that shifts the communication objective from accurate bit transmission to effective semantic delivery. By transmitting semantic information instead of raw data, SemCom significantly improves communication efficiency and enables intelligent communication services for future networks. With the rapid development of artificial intelligence and foundation models, knowledge has become a fundamental element for semantic understanding, semantic reasoning, and intelligent decision-making, driving the evolution of SemCom toward knowledge-centric SemCom. However, the increasing dependence on knowledge also introduces new challenges, such as trustworthy knowledge utilisation, and efficient knowledge management. Existing studies mainly focus on improving SemCom performance, while knowledge security and lifecycle management are not sufficiently explored. Therefore, the development of secure knowledge-enabled SemCom has become an important research topic for future intelligent communication systems.

This thesis investigates secure knowledge-enabled SemCom from four complementary perspectives, namely knowledge-assisted SemCom architecture, privacy preserving transceiver design, knowledge utilisation, and knowledge management. First, this thesis investigates knowledge-assisted privacy preservation in SemCom from a knowledge-centric perspective. Then, potential privacy threats introduced by knowledge utilisation are analyzed. Based on these observations, a knowledge-assisted privacy-preserving SemCom architecture is proposed, consisting of a semantic transmission layer and a knowledge management layer that jointly support secure semantic communications. The corresponding transceiver architecture is then presented to illustrate the integration of knowledge into semantic encoding and decoding. Second, we proposed a knowledge-based differential privacy method, which combines differential privacy with shared knowledge to improve the trade-off between privacy and utility. At the same time, we analyzed the privacy boundaries in SemCom to characterize the impact of differential privacy and knowledge mismatch on semantic reconstruction and sensitive informa-

tion inference, providing a strict privacy proof for the proposed method. Furthermore, we proposed an adversarial optimisation strategy, which alternately minimizes and maximizes joint optimisation of semantic reconstruction and privacy protection, enabling the semantic encoder to learn a potential representation that is invariant to privacy. Third, this thesis focuses on jointly addressing three core issues of power allocation, knowledge caching, and device-to-device user pairing in secure SemCom. a novel performance metric is developed, namely semantic secrecy throughput, to quantify the information security level that can be achieved at each pair of SemCom users. Next, a semantic secrecy throughput maximisation problem is formulated subject to secure SemCom-related delay and reliability constraints. Afterward, a security-aware knowledge management solution is proposed using the Lagrange primal-dual method and a two-stage method.

The studies presented in this thesis establish a unified research framework for knowledge-assisted secure SemCom by integrating knowledge-assisted architecture, knowledge utilisation, and knowledge management into a coherent perspective. The proposed methods not only improve the security, reliability, and intelligence of SemCom but also demonstrate the importance of treating knowledge as a core element rather than an auxiliary component.

University of Glasgow

College of Science & Engineering

Statement of Originality

Name: Xuesong Liu
Registration Number: xxxxxxx

I certify that the thesis presented here for examination for a PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

The copyright of this thesis rests with the author. No quotation from it is permitted without full acknowledgement.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree.

I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issues are raised regarding good research practice based on review of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

Signature: .....
Date: .....

List of Publications

- **Liu, Xuesong**, Yao Sun, Runze Cheng, Le Xia, Hanaa Abumarshoud, Lei Zhang, and Muhammad Ali Imran. "Knowledge-Assisted Privacy Preserving in Semantic Communication." IEEE Wireless Communications 32, no. 2 (2025): 76–83.
- **Liu, Xuesong**, Yansong Liu, Haoyu Tang, Fangzhou Zhao, Le Xia, and Yao Sun. "Joint Knowledge and Power Management for Secure Semantic Communication Networks." IEEE Transactions on Vehicular Technology (2025).
- **Liu, Xuesong**, Yansong Liu, He Sui, Chuan Qin, Yuanxi Che, and Zhaobo Guo. "Anomaly Detection in Cropland Monitoring Using Multiple View Vision Transformer." Scientific Reports 15, no. 1 (2025): 14147.
- **Liu, Xuesong**, Lei Feng, Yao Sun, Yang Yang, Ning Ruan, Yansong Liu, Jiale Quan, Qiyang Zhang, and Zhixiang Qiao. "Over-The-Air Computation-Powered Multi-Layer Federated Learning for Privacy-Preserving Healthcare Devices." IEEE Transactions on Consumer Electronics (2025).
- **Liu, Xuesong**, Junkang Ge, Xiaoqian Li, Yansong Liu, Haoyu Tang, and Gang Feng. "Joint Optimization of Sensing, Communication, and Computation for Cooperative Spectrum Sensing." IEEE Transactions on Network Science and Engineering 13 (2025): 5453–5470.
- Zhao, Fangzhou, Yao Sun, Jianglin Lan, Lan Zhang, **Xuesong Liu**, and Muhammad Ali Imran. "Adaptive Semantic Communication for UAV/UGV Cooperative Path Planning." IEEE Transactions on Vehicular Technology (2026).
- Tatipamula, Mallik, **Xuesong Liu**, Yao Sun, and Muhammad Ali Imran. "The Syntactic-Semantic Internet: Engineering Infrastructures for Autonomous Systems." arXiv preprint arXiv:2602.00818 (2026).

- Cheng, Runze, Yao Sun, Ahmad Taha, **Xuesong Liu**, David Flynn, and Muhammad Ali Imran. "A Survey on Semantic Communication for Vision: Categories, Frameworks, Enabling Techniques, and Applications." arXiv preprint arXiv:2601.22202 (2026).

- Tang, Haoyu, Tianyuan Liang, Han Jiang, **Xuesong Liu**, Qinghai Zheng, and Yupeng Hu. "Decompose and Conquer: Compositional Reasoning for Zero-Shot Temporal Action Localization." In Proceedings of the AAAI Conference on Artificial Intelligence 40, no. 11 (2026): 9404–9412.

- Zhao, Fangzhou, Yao Sun, Jianglin Lan, Lan Zhang, **Xuesong Liu**, and Muhammad Ali Imran. "Semantic Communication Empowered Transmission Policy for UAV/UGV Cooperative Path Planning." In GLOBECOM 2025–2025 IEEE Global Communications Conference, 4421–4426. Piscataway, NJ: IEEE, 2025.

Contents

List of Figures

Acknowledgements

Time flies, and the journey of studying has come to an end. When I finished the last word of the thesis, I deeply realized that this paper not only reflected my own efforts, but also couldn't have been possible without the care, assistance and support from many teachers, classmates, family members and friends. Here, I would like to express my most sincere gratitude to all those who have helped me.

I would like to express my heartfelt gratitude to my supervisors, Professor Yao Sun and Professor Dezong Zhao. During my studies, my supervisors have always guided my learning and research work with a rigorous academic attitude, a sharp academic vision, and a pragmatic research spirit. From topic selection, paper writing to the refinement of research ideas, my supervisors have provided me with patient and meticulous guidance and encouragement. My supervisors not only taught me how to conduct scientific research, but also made me understand the significance of rigor, concentration, and persistence. These valuable academic qualities will benefit me for life. Here, I would like to express my highest respect and sincere gratitude to my supervisors.

I would like to express my gratitude to all the teachers in the research group for their guidance and assistance during my research and study. The rigorous and conscientious work attitude as well as the profound professional knowledge of all the teachers have greatly benefited me.

Finally, I would like to express my special gratitude to my family. I am grateful to my parents for their selfless love, understanding and support over the years. Whether in study or daily life, you have always offered me the greatest tolerance and encouragement, enabling me to face difficulties with determination and keep moving forward. Your trust and companionship have always been the driving force behind my efforts and the most solid support for me to complete my studies.

Chapter 1

Introduction

SemCom has emerged as a promising communication paradigm for next-generation wireless networks, shifting the communication objective from reliable bit transmission to efficient semantic information exchange. Unlike conventional communication systems, which primarily focus on accurately transmitting and recovering bit streams, SemCom aims to deliver the intended semantic meaning required by specific communication tasks. By transmitting semantic information instead of complete bit sequences, SemCom has the potential to significantly improve communication efficiency while satisfying the growing demands of intelligent applications. Consequently, SemCom has attracted increasing research interest and is widely regarded as a key communication paradigm for supporting semantic information exchange in next-generation wireless networks.

A typical SemCom system generally consists of three essential functional components: a semantic encoder, a semantic decoder, and a shared knowledge. At the transmitter, the semantic encoder extracts semantic information from the source message and converts it into compact semantic representations for transmission. Upon reception, the semantic decoder reconstructs the intended semantic meaning from the received semantic representations. Throughout the communication process, the shared knowledge provides contextual information and prior knowledge that enables communication entities to correctly interpret the transmitted semantics. Unlike conventional communication systems, the performance of SemCom strongly depends on effective semantic representation and shared knowledge, making semantic understanding, rather than accurate bit recovery, the primary objective of the communication process.

Among the key components of a SemCom system, shared knowledge plays a fundamental role in semantic information exchange. It provides contextual information that helps communication entities understand the intended

meaning of transmitted messages. Shared knowledge also supports semantic reasoning and reduces semantic ambiguity during the communication process. As communication tasks become increasingly complex, SemCom relies more heavily on shared knowledge to achieve accurate semantic understanding. However, the extensive use of shared knowledge also introduces new challenges in protecting semantic information and maintaining the trustworthiness of shared knowledge. Therefore, designing the secure SemCom system has also become particularly urgent.

1.1 Knowledge as Key Element in SemCom

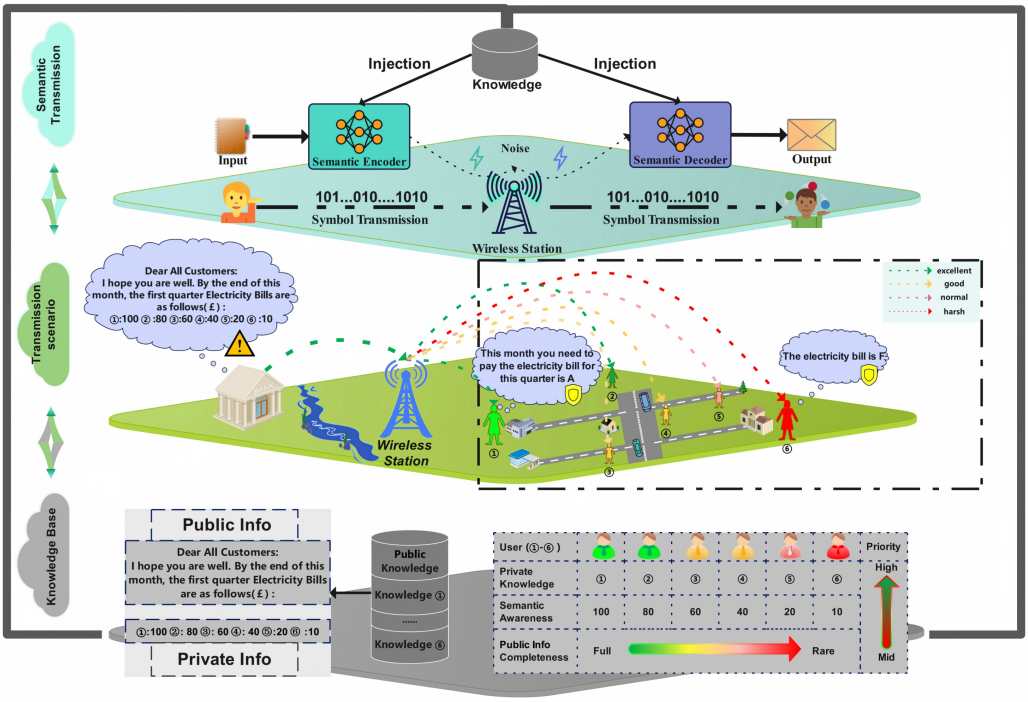

Figure 1.1: Knowledge in SemCom

Knowledge has gradually evolved from an auxiliary component to the pillar of SemCom system, this part consists of three closely related topics, namely knowledge-assisted privacy-preserving architecture, transceiver design of privacy-preserving SemCom, and knowledge management for secure SemCom. Together, these topics provide the technical foundation for developing secure, reliable, and intelligent SemCom systems. The following subsections introduce these three parts in detail.

1.1.1 Knowledge-Assisted Privacy Preserving Architecture

As shown in Figure 1.1, the knowledge-assisted privacy preserving architecture consists of three parts: a knowledge base, a semantic transmission layer, and a wireless transmission scenario. The system achieves semantic compression, transmission, and recovery by injecting public knowledge and private knowledge into the semantic encoder and decoder respectively, enabling the communicating parties to complete these processes based on shared knowledge [1].

The core idea of this architecture is to exploit knowledge disparity to preserve user privacy during SemCom. At the transmitter, knowledge is first separated into public and private, after which knowledge is incorporated to construct personalised semantic representations. At the receiver, the private knowledge enables accurate recovery of sensitive information, whereas an eavesdropper, lacking the complete private knowledge, can recover only partial public information even if the transmitted symbols are intercepted. Consequently, the absence of private knowledge, together with adverse channel conditions, significantly reduces the attacker's ability to infer sensitive information, thereby enhancing the overall privacy protection capability of the proposed architecture [2].

This architecture strikes a balance between semantic transmission accuracy and privacy security, providing a new security architecture for the next-generation SemCom network. This architecture can dynamically adjust the knowledge injection strategy based on different users' knowledge backgrounds, enabling personalized and secure information transmission, and is particularly suitable for scenarios involving a large amount of sensitive information exchange, such as smart cities, vehicle networking, and medical health.

1.1.2 Transceiver Design of Privacy-Preserving SemCom

The core of privacy-preserving SemComs is the joint design of semantic encoding models at the transmitter and receiver. SemCom requires end-to-end optimisation based on semantic representations. The transmitter extracts task-related semantic information and suppresses the leakage of sensitive information. The receiver uses the received semantic features to reconstruct the original message [3]. Therefore, privacy preservation is no longer only a channel security problem. It has become a transceiver co-design problem.

The transceiver design directly determines the trade-off among semantic fidelity, communication efficiency, and privacy protection.

In the knowledge-assisted privacy-preserving transceiver design, the transmitter and receiver introduce privacy protection and knowledge enhancement mechanisms, respectively. These mechanisms enable end-to-end joint optimisation. The transmitter employs a dedicated semantic encoding model. It divides the latent semantic representation into a utility latent space and a sensitive latent space, differential privacy with the Gaussian mechanism is applied only to the sensitive latent space, utility latent space is transmitted without perturbation [4]. This design reduces the semantic information loss caused by privacy protection. Unlike basic semantic decoders in SemCom, the receiver incorporates a shared knowledge to provide semantic priors, which compensates for the distortion introduced by differential privacy. In addition, the system adopts privacy-aware adversarial learning. During training, the semantic encoder, semantic decoder, and adversarial classifier are jointly optimised. As a result, the transmitter learns privacy-invariant semantic representations, while the receiver accurately reconstructs semantic information with the aid of shared knowledge. This forms an end-to-end collaborative transceiver design for privacy-preserving SemCom.

1.1.3 Knowledge Management for Secure SemCom

Knowledge management is an essential component of secure SemCom. As SemCom systems continue to evolve, knowledge can be represented in various formats, making knowledge organisation and utilisation increasingly important [5]. Knowledge management provides systematic support for knowledge storage, sharing, updating, retrieval, and maintenance, ensuring that communication entities can access appropriate knowledge throughout the transmission process.

In SemCom, base stations distribute various domain-specific knowledge to all users uniformly. If an eavesdropping node caches identical knowledge bases as legitimate users, it can fully reconstruct transmitted semantic information merely by intercepting wireless bitstreams [6]. Traditional bit-based physical-layer security metrics such as secrecy throughput and secrecy outage probability fail to quantify this risk of semantic leakage. Meanwhile, knowledge base caching, user pairing and transmit power are tightly interrelated [7]. The type, storage overhead, and preference distribution of cached knowledge bases directly shape the disparity in semantic decoding capability between legitimate and eavesdropper links. Optimising caching strategies or power allocation alone cannot balance semantic security, storage limits and transmission latency. Existing literature lacks a joint resource manage-

ment framework targeting eavesdropping risks caused by knowledge matching. This gives rise to three key challenges: a performance metric tailored for semantic security, differentiated knowledge caching policies for multiple users, and pairing optimisation that accounts for knowledge matching levels.

Knowledge matching acts as the core prerequisite for accurate semantic recovery. However, this mechanism creates unique security risks from semantic eavesdropping, which stands as the top challenge in knowledge management [8].

1.2 Motivation

Knowledge significantly enhances the true meaning of source messages. As communication entities exchange semantic representations instead of raw bit streams, knowledge is able to improve communication efficiency while supporting intelligent communication tasks. However, the semantic representations generated by semantic coding models usually contain much richer information. In addition to the intended semantic content, they can also reveal sensitive user information, contextual knowledge, and task-related characteristics. Consequently, semantic representations become valuable communication assets that require effective protection throughout the transmission process.

Unlike conventional communication systems, protecting transmitted signals alone is insufficient for SemCom. Although semantic representations are typically compressed into low-dimensional features, they still preserve the essential semantic information required for downstream tasks. An adversary may therefore infer private information from intercepted semantic representations or reconstruct sensitive semantic content through semantic reasoning. Furthermore, because semantic information is highly correlated with contextual knowledge, information leakage may occur even without recovering the original source data. These characteristics introduce new security challenges that cannot be fully addressed by existing communication security mechanisms.

Another challenge arises from the diversity of SemCom applications. Different communication scenarios often involve different semantic objectives, communication tasks, and user requirements. The same semantic information may have different sensitivity levels depending on the application context and user privileges. For example, public semantic information can be shared among multiple communication entities, whereas private information should only be accessible to authorized users. Therefore, secure information transmission in SemCom should not only guarantee reliable semantic deliv-

ery but also provide flexible protection according to semantic sensitivity and communication requirements.

Meanwhile, the introduction of artificial intelligence further increases the complexity of semantic security. Modern SemCom systems rely on deep neural networks to extract semantic representations, making the communication process closely coupled with semantic learning and inference. As a result, protecting semantic information is no longer limited to transmission security but also involves knowledge management, Collaboration of knowledge in distributed scenarios. These issues have become increasingly important as SemCom evolves toward intelligent and knowledge-centric communication systems.

Therefore, developing secure information transmission mechanisms has become the first research motivation of this thesis. Such mechanisms should effectively protect sensitive information while preserving semantic fidelity, communication efficiency, and task performance. Achieving a proper balance between semantic utility and information protection is a fundamental challenge for future knowledge-centric secure SemCom.

1.3 Objectives

The overall objective of this thesis is to establish a knowledge-centric secure SemCom framework that supports secure information transmission, secure knowledge utilisation, and knowledge management. By integrating semantic intelligence, communication security, and knowledge management into a unified framework, this thesis aims to improve the security of future SemCom systems. To achieve this objective, the research presented in this thesis focuses on the following aspects.

The first objective is to investigate secure information transmission in SemCom. As semantic representations contain rich semantic information, protecting sensitive information while preserving semantic fidelity has become a fundamental requirement. This thesis aims to develop secure transmission mechanisms that prevent information leakage without compromising semantic understanding and communication performance.

The second research objective is to investigate secure knowledge utilisation for SemCom. As knowledge becomes an indispensable component of semantic understanding and reasoning, its secure utilisation directly affects the reliability and trustworthiness of SemCom systems. This thesis aims to develop secure mechanisms that support knowledge sharing, knowledge interaction, and trustworthy semantic reasoning while protecting knowledge from unauthorized access and malicious manipulation. These studies further

improve the capability of SemCom to support intelligent and secure SemCom in diverse communication scenarios.

The third research objective is to investigate efficient knowledge management for secure SemCom. The continuous growth of knowledge resources and the increasing complexity of SemCom networks require systematic mechanisms for knowledge organisation, sharing, updating, and utilisation. This thesis aims to establish an efficient knowledge management framework that enables scalable knowledge collaboration while maintaining communication security and system reliability. The proposed research provides essential support for the practical deployment of future knowledge-centric secure SemCom systems.

Collectively, these research objectives provide a systematic framework for advancing knowledge-centric secure SemCom from secure semantic transmission to intelligent knowledge utilisation and scalable knowledge management. The major research contributions achieved toward these objectives are presented in the next section.

1.4 Research Contributions

Guided by the research objectives presented in the previous section, this thesis investigates several fundamental issues in knowledge-centric secure SemCom, ranging from secure information transmission to secure knowledge utilisation, secure knowledge collaboration, and efficient knowledge management. Through these studies, a unified framework is established to support secure, reliable, and intelligent SemCom. The main contributions of this thesis are summarized as follows.

- We explore utilizing knowledge to enhance data privacy in SemCom networks. Specifically, we first identify the potential attacks in SemCom based on the analysis of knowledge. Then, we propose a knowledge-assisted privacy preserving SemCom framework, which consists of a data transmission layer for precisely encoding and decoding source messages, and a knowledge management layer responsible for injecting appropriate knowledge into the transmission pair. Moreover, we elaborate on the transceiver design in the proposed SemCom framework to explain how knowledge should be utilized properly. Finally, some challenges of the proposed SemCom framework are discussed to expedite the practical implementation.

- We propose a knowledge-assisted differentially private (DP) SemCom framework that jointly exploits structured knowledge and latent-space

privacy protection. Specifically, a variational autoencoder is employed to decompose semantic representations into sensitive and non-sensitive latent subspaces, where only the sensitive component is perturbed by a DP mechanism. Meanwhile, structured knowledge derived from a knowledge is incorporated as semantic prompts to assist legitimate decoding while creating knowledge asymmetry against eavesdroppers. We further establish theoretical privacy guarantees by proving end-to-end DP preservation under arbitrary post-processing and deriving explicit upper bounds on the eavesdropper's optimal inference accuracy. To further enhance privacy robustness, an adversarial training strategy is introduced to optimize the semantic encoder against attribute inference attacks while maintaining reconstruction quality. Experimental results demonstrate that the proposed framework effectively achieves a favorable privacy–utility tradeoff, significantly improving semantic reconstruction at the legitimate receiver while substantially reducing the inference capability of eavesdroppers compared with existing privacy-preserving SemCom schemes.

- Since the potential eavesdroppers may have the same background knowledge to accurately decrypt the private semantic information transmitted between legal SemCom users, this makes the knowledge management in SemCom networks rather challenging in joint consideration with the power control. To this end, We focus on jointly addressing three core issues of power allocation, knowledge base caching (KBC), and device-to-device (D2D) user pairing (DUP) in secure SemCom networks. We first develop a novel performance metric, namely semantic secrecy throughput (SST), to quantify the information security level that can be achieved at each pair of D2D SemCom users. Next, an SST maximisation problem is formulated subject to secure SemCom-related delay and reliability constraints. Afterward, we propose a security-aware resource management solution using the Lagrange primal-dual method and a two-stage method. Simulation results demonstrate our proposed solution nearly doubles the SST performance and realizes less than half of the queuing delay performance compared to different benchmarks.

- We present a system-level analysis of security risks in knowledge-centric SemCom. We develop an architectural decomposition of the knowledge plane and identify four primary attack surfaces spanning knowledge content integrity, activation and conditioning pathways, evolution and synchronisation mechanisms, and cross-layer availability. We character-

ize their corresponding semantic failure modes, demonstrating that bit-level correctness does not imply semantic correctness. A case study on knowledge version divergence shows that asynchronous updates alone can induce encoder–decoder misalignment under error-free transmission. Finally, we outline defensive design principles and highlight open challenges for building secure, scalable, and knowledge-aware SemCom systems, establishing the knowledge plane as a first-class security domain in next-generation SemCom.

1.5 Dissertation Organisation

The rest of this thesis is organized as follows:

Chapter 2 reviews the related work on SemCom, knowledge-assisted SemCom, secure and privacy-preserving issues in SemCom, and knowledge management for secure SemCom. It also summarizes the existing research challenges and identifies the research gaps addressed in this thesis.

Chapter 3 investigates secure information transmission in knowledge-centric SemCom. A secure transmission architecture is developed to protect sensitive information while preserving semantic fidelity and communication performance.

Chapter 4 investigates secure transceiver design in SemCom. We have proposed the boundaries of differential privacy and the opponent optimisation strategy. Moreover, the proposed framework enables secure knowledge interaction and improves the reliability and trustworthiness of knowledge-assisted SemCom.

Chapter 5 investigates knowledge management for secure SemCom. A unified knowledge management framework is developed to support knowledge organisation, sharing, updating, and utilisation for scalable and intelligent SemCom networks.

Chapter 6 further investigates secure knowledge collaboration in distributed SemCom systems. It develops a secure mechanism for knowledge sharing and collaboration to support trustworthy semantic understanding across multiple communication entities.

Chapter 7 concludes this dissertation by summarizing the main research findings and discussing several promising directions for future research in knowledge-centric secure SemCom.

Chapter 2

Related Works

2.1 Knowledge-Assisted SemCom

SemCom reorients wireless transmission from bit-level reliability to task-aware semantic delivery. The seminal end-to-end deep learning framework DeepSC [9] relies purely on neural networks to extract implicit semantics, which suffers from limited interpretability and fragile performance under noisy channels. To alleviate such drawbacks, scholars introduce shared background knowledge between transceivers, forming the research field of knowledge-assisted SemCom. Existing studies can be naturally divided into two coherent research threads: knowledge representation designs customized for SemCom, and the paradigm evolution from knowledge-enabled toward knowledge-centric SemCom.

2.1.1 Knowledge Representation in SemCom

This research line centers on answering how knowledge can be formally modelled, encoded and synchronized to support semantic encoding and decoding. Research progresses gradually from unstructured knowledge storage toward structured graph representation, and further toward embedding-based compact knowledge expression. As an early attempt, Yi *et al.* [10] developed a SemCom framework built upon shared unstructured knowledge bases. The transmitter only sends semantic content inconsistent with shared priors, whereas predictable information is reconstructed locally at the receiver; nevertheless, the lack of relational modelling restricts its semantic reasoning capability. Moving beyond unstructured text corpora, Jiang *et al.* [11] pioneered knowledge graph (KG) utilisation for textual SemCom, translating original sentences into entity–relation triples as basic semantic units. Although shared KGs assist the receiver in recovering complete information

from partial transmitted triples, the adopted graph remains static without online update functions.

Following this KG-oriented route, Wang *et al.* [12] shifted knowledge utilisation from the transmitter side to receiver-side compensation. The receiver retrieves relevant graph triples to offset semantic corruption caused by channel noise, yet the work fails to establish joint transceiver optimisation for knowledge representation consistency. To reduce the heavy overhead of transmitting raw graph structures, Wu *et al.* Moreover, [13] integrated knowledge graph embedding into zero-shot SemCom, mapping discrete graph elements into low-dimensional continuous vector space. This design improves transmission efficiency and generalisation to unseen concepts, but overlooks knowledge mismatches between communication endpoints.

Apart from graph-based schemes, Wheeler and Natarajan [14] explored an alternative paradigm using geometric conceptual spaces for semantic knowledge representation. They derived theoretical semantic error bounds under geometric semantic metrics, though their analysis is only validated in simplified synthetic settings. From a systematic generative perspective, Ren *et al.* [15] proposed a hierarchical knowledge base architecture, which classifies knowledge into source knowledge, task knowledge and channel knowledge. A critical limitation lies in the strong assumption of perfectly synchronized knowledge, which rarely holds in dynamic wireless networks.

Recently, combining knowledge graphs with large language models, Liu *et al.* [16] put forward KGRAG-SC by introducing GraphRAG into SemCom. Instead of transferring full subgraphs, only pointers of core semantic subgraphs are delivered to cut signalling cost; however, the framework is tightly coupled with LLMs and cannot be easily extended to general multi-modal scenarios.

2.1.2 From Knowledge-Enable to Knowledge-Assisted SemCom

Early knowledge-assisted designs treat knowledge as auxiliary side information appended to conventional SemCom pipelines, which we term knowledge-enabled SemCom. Recent studies gradually rethink the system architecture and push toward knowledge-centric SemCom, where knowledge governs the whole communication workflow. We elaborate this evolutionary trend through representative works.

The DeepSC framework [9] serves as the baseline purely data-driven SemCom architecture without explicit knowledge modules. Nearly all early knowledge-enabled schemes inherit its encoder–decoder backbone and embed

knowledge modules as add-ons, where knowledge merely helps enhance semantic reconstruction quality rather than dominating communication logic. Recognizing the vulnerability of static knowledge, Fang *et al.* [17] pointed out that transceiver knowledge inconsistency severely degrades semantic transmission performance. To tackle this issue, they adopted generative AI to support incremental dynamic knowledge updating via semantic interactions, even though the optimisation objective is still confined to single-link communication performance.

Extending dynamic knowledge to networked systems, Zhang *et al.* [18] constructed a context-aware knowledge-enhanced SemCom framework for digital twin networks. The system continuously accumulates contextual knowledge to optimize transceiver processing, yet the solution is task-specific and lacks native support for network-scale multi-user knowledge coordination.

On the architectural level, Strinati *et al.* [19] proposed the Kraken cognitive 6G vision featuring an independent network knowledge plane. Under this architecture, SemCom becomes an application running on top of distributed shared knowledge infrastructure, clearly drawing the dividing line between knowledge-enabled and knowledge-centric communication paradigms. Built on such architectural insights, Zhang *et al.* [20] formally conceptualized knowledge-centric SemCom. Unlike knowledge-enabled systems that use knowledge to recover transmitted messages, knowledge-centric SemCom prioritizes mutual knowledge alignment among agents; still, fundamental challenges including distributed knowledge synchronisation remain insufficiently addressed.

Despite the above advances, few existing works establish a unified framework that use knowledge to enhance privacy. This gap motivates investigation into knowledge-assisted coding design in secure SemCom.

2.2 Secure and Privacy-Preserving SemCom

There are many threats in SemCom, we organize representative literature into two subsections covering security threats and privacy-preserving threats.

2.2.1 Security Issues in SemCom

Security vulnerabilities of SemCom span the wireless channel, semantic coding models and shared knowledge. Sagduyu *et al.* [21] systematically investigated multi-domain adversarial attacks on deep learning-based SemCom, demonstrating that subtle perturbations imposed on latent semantic repre-

sentations can mislead semantic understanding without obvious bit errors. Shen *et al.* [22] constructed a multi-layer risk taxonomy for SemCom architectures and summarized defensive strategies covering semantic extraction, over-the-air transmission and semantic reconstruction modules. From the viewpoint of knowledge-assisted SemCom, Guo *et al.* [23] pointed out that poisoning or tampering shared knowledge graphs will trigger persistent semantic misinterpretation, whereas dedicated countermeasures targeting knowledge-layer attacks remain insufficiently explored. Li *et al.* [24] built physical-layer security empowered SemCom frameworks to enhance transmission confidentiality against passive wiretapping over fading wiretap channels. Jiang *et al.* [25] proposed model-hopping SemCom inspired by frequency hopping, dynamically switching encoder-decoder parameters to raise the barrier for adversaries launching adversarial eavesdropping. Despite these efforts, most existing security designs separate knowledge synchronization security and semantic transmission security, lacking joint optimisation frameworks tailored for knowledge-assisted SemCom systems.

2.2.2 Privacy-Preserving Issues in SemCom

There are numerous analyses on the issue of privacy leakage in semCom, such as Won *et al.* [7] delivered a comprehensive survey on privacy threats in SemCom, including model inversion, contextual inference and data leakage during knowledge exchange between transceivers. Wang *et al.* [26] adopted adversarial training to defend against model inversion attacks in task-oriented semantic transmission. Zhao *et al.* [27] constructed federated SemCom frameworks with model division multiple access to resist gradient inversion attacks in distributed edge networks. Nevertheless, most existing privacy-preserving strategies seldom balance knowledge synchronization overhead, semantic reconstruction accuracy and strict privacy constraints simultaneously. This research gap motivates our investigation into knowledge-assisted secure and privacy-aware SemCom.

2.3 Knowledge Management in SemCom

Shared knowledge serves as fundamental enablers to improve semantic reconstruction and transmission efficiency. Nevertheless, dynamic knowledge synchronization, update, storage and access bring new security challenges distinct from conventional SemCom. Existing literature splits into two research branches: security risks during knowledge utilisation, and knowledge management frameworks to fortify secure semantic transmission, reviewed as

follows.

2.3.1 Secure Knowledge Utilisation

Transceivers rely on shared knowledge to complete semantic reasoning, while improper access, tampering and leakage of knowledge become critical vulnerabilities. Guo *et al.* [23] summarized security threats in knowledge-augmented SemCom, highlighting that adversaries can launch knowledge graph poisoning to mislead semantic decoding without attacking wireless channels. Sagduyu and Ulukus [21] indicated that exchanged knowledge metadata between communication pairs may leak task semantics, forming an additional leakage channel apart from semantic feature transmission. Zhang *et al.* [20] further pointed out that asymmetric knowledge status between transmitter and receiver inherently causes semantic mismatch, which can be maliciously exploited by active attackers. Li *et al.* [24] demonstrated that static shared knowledge lacks access control mechanisms, allowing unauthorized parties to retrieve background knowledge and infer private communication contexts. Although these works identify diverse risks in knowledge usage, they lack lightweight protection mechanisms suitable for resource-limited wireless SemCom terminals.

2.3.2 Knowledge Management for Secure SemCom

To mitigate the above vulnerabilities, recent research begins to adopt standardized knowledge management strategies to support trustworthy SemCom systems. Won *et al.* [7] outlined basic requirements for knowledge lifecycle management, including knowledge creation, synchronization, version control and revocation in distributed SemCom networks. Shen *et al.* [22] argued that dynamic knowledge updating protocols must be embedded into SemCom pipelines to resist the degradation caused by poisoned static knowledge. Wang *et al.* [26] designed knowledge filtering strategies, removing sensitive entities before knowledge sharing to balance privacy and semantic recovery performance. Jiang *et al.* [25] combined knowledge version negotiation with semantic encoder adaptation, reducing semantic distortion induced by inconsistent knowledge snapshots. Even so, most existing management schemes separate knowledge maintenance and semantic transmission optimization. A unified framework that jointly optimizes knowledge synchronization overhead, knowledge access security and SemCom reliability remains under-explored.

Chapter 3

Knowledge-Assisted Privacy Preserving Architecture

3.1 Introduction

Knowledge, the pillar of SemCom, is capable of underpinning semantics representation, extraction, and recovery [28]. Basically, knowledge is a data repository containing structured information and semantic relations, providing strong context information and reasoning ability for transmitters and receivers [29]. More specifically, knowledge could assist transmitters in compressing source messages into semantics for encoding with low redundancy. At the receiver side, reasoning ability empowered by knowledge is needed to recover the true semantics from the distorted bits. Knowledge usually contains specific domain information and semantic rules. For instance, in the field of medical science, the knowledge may contain information related to diseases, symptoms, treatments, etc. Technically, the indirect relationship between diseases and treatments can be inferred via the contextual information in the knowledge, and their semantic rules are analyzed. Moreover, knowledge should be periodically updated in SemCom systems to keep its timeliness.

Although the prospects of SemCom have been widely recognized, privacy issues exist as a vital barrier to unlocking its full potential. Eavesdropping attacks, referring to the unauthorized interception and monitoring on data transmission, bring significant challenges for privacy leakage [30], especially in SemCom systems. Unlike conventional eavesdropping attacks, eavesdroppers equipped with a capable semantic coding model may be able to reconstruct semantics from only a few stolen bits [31]. Furthermore, if attackers hold partial or even full knowledge of the transceiver, the threat becomes

more severe. In such cases, eavesdroppers can leverage their knowledge in conjunction with capable semantic coding models to infer additional semantics from the stolen bits, such as hidden information and future messages between the transmission pair. To resit to serious privacy leakage issues, privacy-preserving SemCom designs are urgently needed.

To avoid privacy leakage under the aforementioned attacks, the major challenge is to prevent attackers from restructuring source information with eavesdropped semantics. Therefore, privacy-preserving design should be placed on the two core components of SemCom, i.e., coding model and knowledge. Although some researchers have delved into the privacy-preserving SemCom design by securing encoding-decoding models, only a few contributions highlighted the potential of preventing privacy leakage by means of tailored knowledge design and utilisation. Knowledge is not only a simple database that enables the encoder-decoder to compress and restructure source messages, it also has great potential to assist in a dynamic codebook construction for a specific SemCom transceiver. Since the context-specific semantic relationship and semantic entity of the knowledge can be periodically updated, it is difficult for attackers to accurately synchronize the whole knowledge for restructuring the source message. In addition, knowledge could be utilized in a dedicated and pre-agreed manner for the transceiver, misleading eavesdroppers into exploiting the knowledge incorrectly and reconstructing inaccurate semantics.

In this chapter, we design a knowledge-assisted privacy preserving SemCom framework to resist eavesdropping attacks. The main contributions are summarized as follows:

- The categories of knowledge in SemCom are analyzed, followed by a discussion of three typical eavesdropping attacks in SemCom that can lead to privacy leakage.
- We propose a knowledge-assisted privacy preserving SemCom framework by proposing novel designs for a reliable data transmission layer and a knowledge management layer.
- We illustrate the workflow of encoders and decoders in the proposed privacy preserving SemCom framework, and demonstrate the ability of resisting different eavesdropping attacks.
- Finally, to expedite the implementation of the proposed framework, we discuss some potential challenges that may arise in practice.

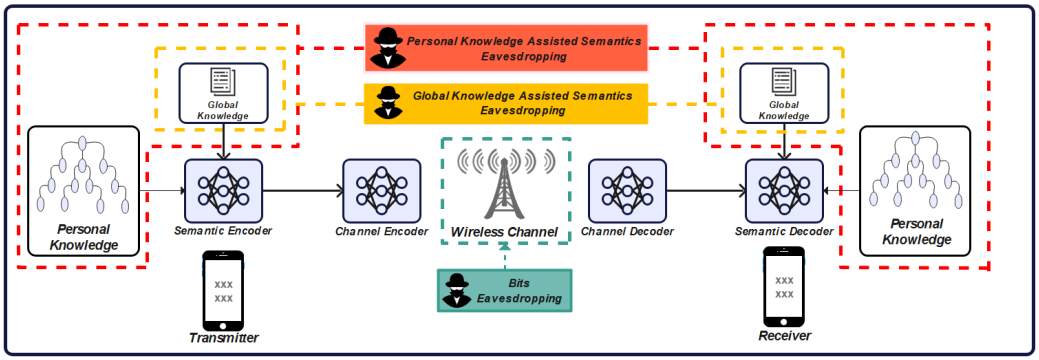

Figure 3.1: Three potential attacks against knowledge in the semantic communication system.

3.2 Potential Privacy Threats in SemCom

Before addressing privacy issues in SemCom, let us first overview the knowledge categories in SemCom. Following that, we define three typical eavesdropping attacks, as shown in Fig.3.1.

3.2.1 Categories of Knowledge in SemCom

As discussed before, knowledge plays a key role in SemCom for semantics extraction and recovery. Generally, there are two categories of knowledge in SemCom.

Global knowledge refers to public information that can be accessed by everyone, such as publicly-available knowledge from the Internet. Therefore, in SemCom networks, it is commonly assumed that transmitters and receivers hold the same global knowledge. By injecting global knowledge into the semantic encoders and decoders, enables two communication ends to hold the same understanding of public information.

Personal knowledge consists of some private and sensitive content of each individual user, such as user behavior, preferences, and the knowledge gained from individual practice. Transmitters and receivers hold their own personal knowledge. At the transmitter end, the semantic encoder exploits personal knowledge to filter out irrelevant information, reducing redundancy during encoding and further compressing the source messages. At the receiver end, the semantic decoder recovers the meaning of source messages from the received bits with the assistance of the receiver's personal knowledge. Moreover, if the recovered messages are ambiguous, personal knowledge can be supplemented to help receivers understand the semantics precisely.

3.2.2 Three Eavesdropping Attacks in SemCom

Based on the discussions on knowledge, we identify the following three types of eavesdropping attacks in SemCom.

Bits Eavesdropping

This kind of attack refers to stealing source messages by purely eavesdropping on wireless signals over a wireless channel. In this way, attackers can only intercept bits but may not decode accurate semantics from these bits due to the lack of a matched semantic coding model. Therefore, attackers can detect that there are some information exchanges between the two ends, but they cannot understand the information itself. Note that the knowledge attackers hold does not matter in this case due to the lack of a qualified semantic coding model.

Global Knowledge Assisted Semantics Eavesdropping

Attackers in this case are equipped with a matched semantic model along with global knowledge, enabling them to eavesdrop on some public semantics. Attackers first intercept bits over a wireless channel, and then decode semantics by using their own semantic coding model, injected with global knowledge. In this way, attackers can recover the public semantics of source messages to some extent, leading to privacy leakage issues at the semantic level. Moreover, by analyzing all eavesdropped bits, attackers diSemComover that limited bits can be decoded into public information, thus determining that the undecoded bits may contain other semantic information.

Personal Knowledge Assisted Semantics Eavesdropping

In this case, attackers acquire both personal and global knowledge as well as a matched semantic coding model. It is evident that attackers in this case are highly capable of eavesdropping on both public and private semantics, thereby posing significant challenges on user privacy in SemCom. Since attackers may hold personal knowledge of transmitters and receivers, the privacy of both sides might be leaked. For transmitters, attackers exploit personal knowledge to infer sensitive information and global knowledge to infer public information. Moreover, the attacker may fully decode the meaning of source messages from the perspective of receivers, particularly for sensitive information of receivers. In addition, attackers can exploit these personal knowledge discrepancies between receivers and transmitters to potentially predict future messages exchanged between the pair.

By analyzing the above three different kinds of eavesdropping attacks, it is clear that the attacker's understanding of personal knowledge directly determines how much privacy can be stolen. Furthermore, general semantic coding models are usually loosely coupled with knowledge and may not protect privacy well. Therefore, it is necessary to design a new SemCom framework that includes knowledge management and data encoding/decoding to wisely exploit knowledge to accurately exchange semantics while protecting data privacy.

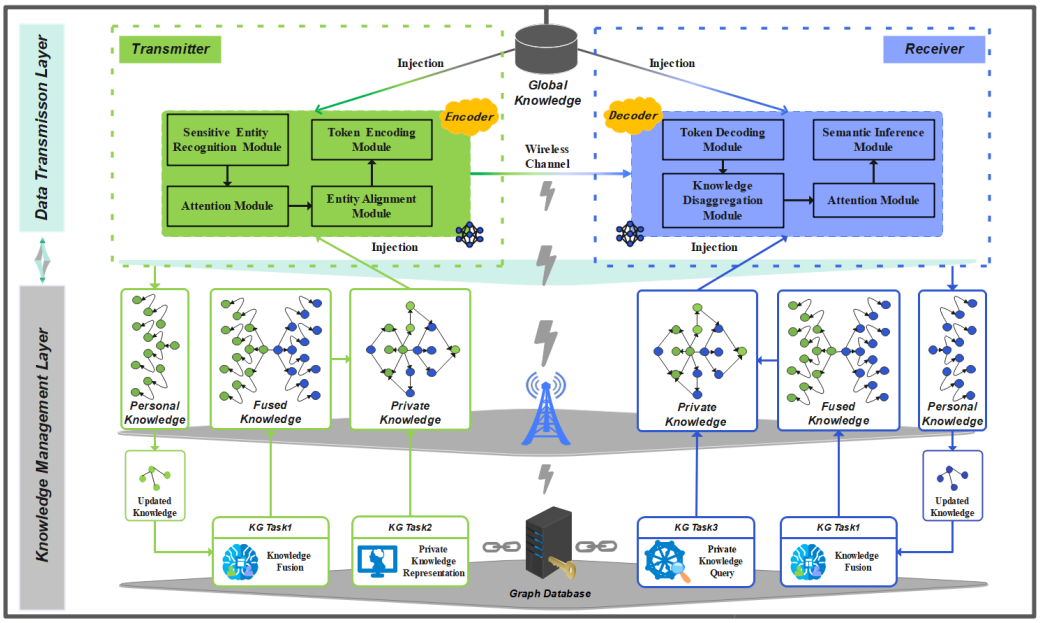

Figure 3.2: Our proposed knowledge-assisted privacy preserving SemCom framework.

3.3 Knowledge-assisted Privacy Preserving SemCom

As shown in Figure 3.2, the proposed SemCom framework consists of two layers: a knowledge management layer and a data transmission layer. The knowledge management layer undertakes knowledge coordination between transmitters and receivers, while the data transmission layer utilizes novel SemCom transceivers with the assistance of injected knowledge. To illustrate the framework clearly, we will focus on the scenario with one transmission pair in the following.

3.3.1 Data Transmission Layer

In this framework, global knowledge is injected into the coding model through word embedding methods, while private knowledge is injected into the coding model through graph embedding methods. Generally, the transmitter extracts the semantic features from source messages by injecting knowledge to minimize the amount of data to be transmitted, and the source message in this way is encoded as a sequence of symbols for transmission via wireless channel. Correspondingly, the receiver decodes the received distorted symbols and recovers the semantics of the original messages with the assistance of its knowledge. Specifically, an encoder located in the transmitter comprises four modules, including sensitive entity recognition, attention, entity alignment, and token encoding module. At the receiver end, a decoder having the same knowledge as that of the encoder is deployed to recover the semantics of source messages from the received channel-distorted bits. This requires another four modules at the receiver side, namely the token decoding module, knowledge disaggregation, attention, and semantic inference. The detailed illustration of the encoder and decoder design will be provided in the next section.

3.3.2 Knowledge Management Layer

As discussed, knowledge plays a unique role in extracting and recovering semantics at both sides. To fully unleash the potential of knowledge, global knowledge is openly accessible as shared datasets, while graph database is utilized as a specialized library for processing personal knowledge and storing private knowledge in the knowledge management layer. Before discussing the process of knowledge management, let us define the concepts of fused knowledge, private knowledge, and updated knowledge, which are specially introduced in our framework. **Fused knowledge** merges the personal knowledge of a transmitter and a receiver through the form of knowledge graph (KG). Here we specify that each entity in this KG represents a basic semantic element, such as place, event, people, etc. An edge connecting two entities in this KG represents the relationships. **Private knowledge** is a subgraph of the fused knowledge, including all entities and their relationships with respect to the coming source messages. Moreover, private knowledge may include extra entities related to the source messages due to the structured KG. Additionally, **updated knowledge** is the newly added information in personal knowledge, which ensures the timeliness of personal knowledge. In this way, both fused knowledge and private knowledge can be dynamically updated.

Knowledge Fusion

This task illustrates the process of merging personal knowledge between the transmitter and the receiver in trusted graph databases, ensuring the same understanding of both sides in SemCom. To construct this fused knowledge in KG format, knowledge alignment, and knowledge disambiguation are required.

Knowledge alignment is the process of matching entities with the same name between the transmitter's and receiver's personal knowledge. For example, an entity "apple" may exist in the personal knowledge of both sides, and we need to replace the two dispersed entities with an entity in the fused KG, thus eliminating redundant knowledge and ensuring its consistency. Private set intersection (PSI) [32] accomplishes this through hash-encrypted knowledge exchanges, without revealing non-intersecting parts of personal knowledge.

Knowledge disambiguation is the process of distinguishing knowledge with the same names but different semantics, thus reducing semantic ambiguity in SemCom. Contextual analysis methods, such as word sense disambiguation [33] are typically exploited. By matching target entities and their relationships in the context of the source message, the semantics of the target entity can be determined. For instance, in the sentence "Apple is a company", analyzing the relationship between the entities "apple" and "company", "apple" refers to a brand rather than a fruit. Consequently, fused knowledge is established in a KG format, and the issues of knowledge redundancy and disambiguation can be resolved. Considering the eavesdropping risk of updated knowledge, it is difficult for the attacker to generate the same fused knowledge as the transmitter and receiver due to the lack of personal knowledge.

Private Knowledge Construction

With the fused knowledge, it ensures the same understanding capability of the transmitter and receiver. However, if we directly inject the fused knowledge into the encoder and decoder, this might be a large-scale and extremely complicated semantic coding model. Moreover, considering that the distribution of a given source message in the fused knowledge may be a subgraph with a very small scope, it is necessary to further clarify the scope of private knowledge in the fused knowledge. This process of private knowledge construction is divided into three steps, namely source message analyzing, source message querying, and minimal KG construction. Source message analyzing is to convert source messages into the format for entity querying, which can

be directly realized by natural language processing techniques. Source message querying is to find all entities and relationships related to the source messages in fused knowledge, with the aim of specifying the scope of the private knowledge, graph traversal languages adapted to fused knowledge can effortlessly implement it. Based on this, The entities of source messages in fused knowledge are collected by random walk [34], and the minimal spanning tree is utilized to extract the minimal connected subgraph in fused knowledge, removing irrelevant nodes and relationships, thereby optimizing the structure of private knowledge.

Private Knowledge Distribution

Private knowledge distribution entails that the transmitter and the receiver can obtain the same private knowledge in the graph database. General queries can be carried out directly via graph query language for information retrieval, whereas private knowledge query requires identity authentication before querying. The receiver will be empowered with different permissions through various traditional encryption methods, such as digital signatures and shared keys. Overall, graph databases are effective in ensuring the consistency and integrity of private knowledge in an eavesdropping environment.

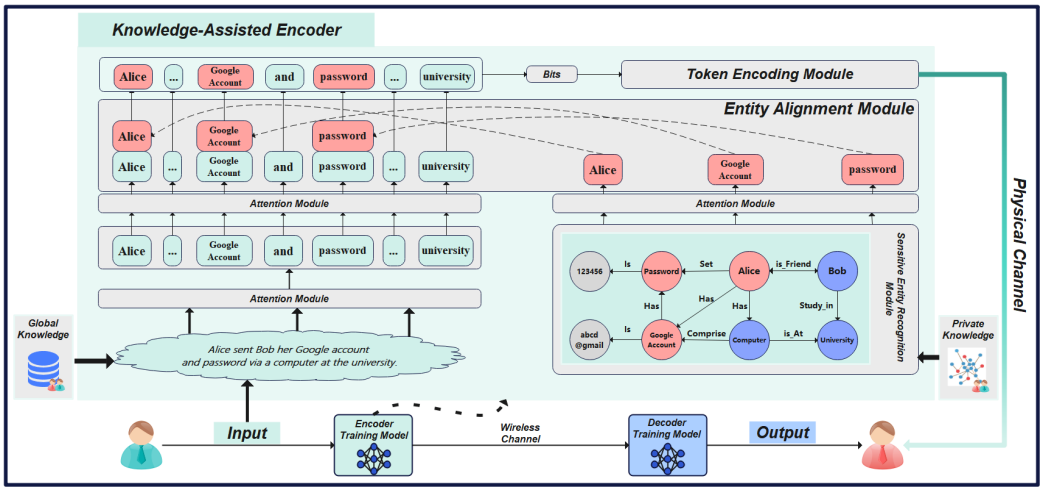

Figure 3.3: The intrinsic structure of knowledge-assisted encoder networks.

3.4 Transceiver Design

In this section, we discuss how to design an SemCom transceiver with the assistance of knowledge to protect sensitive information.

3.4.1 Knowledge-Assisted Encoder Network

The basic idea in this encoder network design is to leverage global knowledge to compress source messages, while utilizing private knowledge of both sides to protect sensitive information. To this end, the knowledge-assisted encoder shown in Fig. 3.3 proposed, which is comprised of four modules, namely sensitive entity recognition module, attention module, entity alignment module, and channel coding module.

The sensitive entities recognition module consists of two functions. The first function is to SemComreen the potentially sensitive information in private knowledge, Named Entity Recognition (NER) method [35] is a core task in natural language processing with the goal of recognizing specific entities in private knowledge. NER determines sensitive content in a source message by matching sensitive keywords, such as personal name, Email, ID, etc. This has the advantage of being able to differentiate the intrinsic sensitivity for entities of the same category. For example, "Bob" and "Alice" are both names and should be identified as sensitive information. However, "Alice" has a direct relationship with "Google account" and "password" in private knowledge, thus only "Alice" is identified as sensitive information. The second function is to analyze the relationships among these sensitive entities in private knowledge. Graph neural network (GNN), specialized for processing graph-structured data, could be exploited for identifying internal relationships of sensitive entities in private knowledge by edge classification [36]. Generally, the complexity of GNN is higher than that of traditional deep neural networks. The computation of GNN involves the sparsity of graph structure data and the aggregation and propagation of neighbor nodes.

The attention module consisting of two layers transforms global knowledge and private knowledge into sequence tokenisation. The lower layer attention module captures the basic word-level and syntactic information of the source message, which can be accomplished by natural language processing models, such as BERT. The upper attention module is responsible for integrating tokens between private knowledge and global knowledge, thus enabling to representation of the heterogeneous information of global knowledge and private knowledge in a unified feature space.

The entity alignment module contains original tokens represented by global knowledge, and sensitive tokens represented by private knowledge. The core idea of this module is to find the sensitive tokens, overlaying sensitive tokens over original tokens with the same semantics. Intuitively, the semantic similarity between original tokens and sensitive tokens can be computed directly using traditional methods, such as structural similarity [5]. Since original tokens are non-structured data, the structural similar-

ity method may cause them to lose their structural properties. Additionally, its low computational complexity makes it applicable in SemCome scenarios with limited wireless resources. Another reliable method is to train a joint embedding model [37] that puts original tokens and sensitive tokens in the same vector space and evaluates their similarity by calculating the cosine angle of the two vectors, overlaying sensitive tokens into original tokens with similar semantics. However, this method has a high complexity in the training phase and consumes a lot of computing resources and time in SemCom that require large data processing. Finally, a set of tokens jointly represented by private and global knowledge is converted into binary bits and entered into the token encoding module for transmission, ensuring the transmission of sensitive information via different channels precisely.

The top part of Fig.3.5 visualizes the data flow as it passes through the proposed SemCom encoder. The source message is unstructured data. Text preprocessing decomposes the source message into words or phrases, and transforms the source message into a vector representation through word embedding, extracting the features in the source message. The word or phrase becomes the candidate entity in turn, and the entity that is most relevant to the knowledge is matched according to its feature ranking. Moreover, entity naming identifies sensitive and non-sensitive information in a source message by labeling it with an entity type. A vocabulary is constructed through the relationships between entities, and a set of relationships will be mapped to a unique ID which can be represented by a token. Additionally, which token represents sensitive information can be accomplished by entity replacement. Finally, these tokens are converted into binary bits via token encoding module, and these bits are then transmitted over a noisy wireless channel.

3.4.2 Knowledge-Assisted Decoder Network

As illustrated in Figure 3.4, the token decoding module within the knowledge assisted-decoder is responsible for recovering the original tokens. Subsequently, these tokens are entered within the knowledge disaggregation module. Original tokens and sensitive tokens are recovered via a neural network, which specially obtains the relationships between sensitive and public information. The cooperative interaction between the attention module and the knowledge representation module enables the parsing of sequences containing sensitive information into sensitive tokens, these tokens are then converted back to corresponding entities to be located in private knowledge. These located entities further enable sensitive information to be better inferred at the receiver side. Next, the tokens represented by global knowledge will be

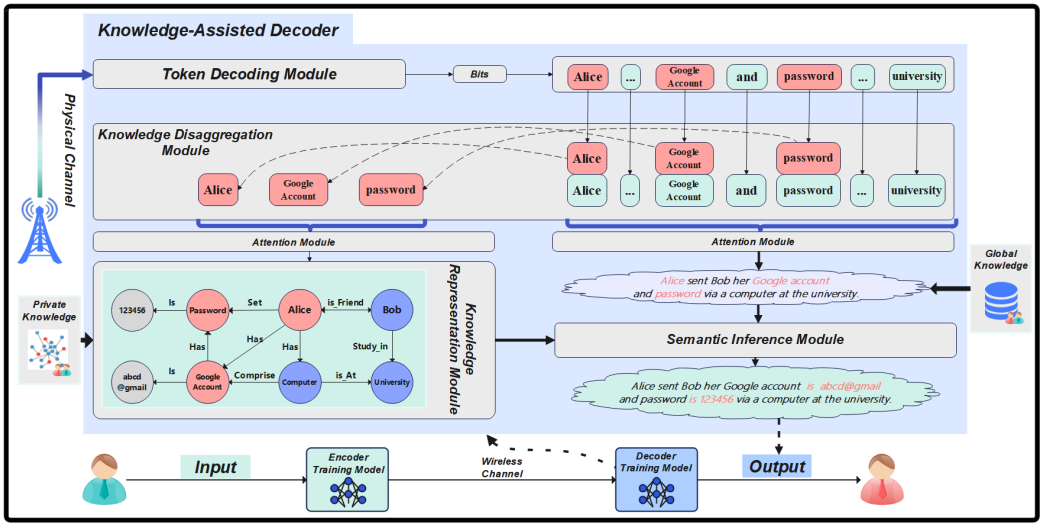

Figure 3.4: The intrinsic structure of knowledge-assisted decoder networks.

recovered directly to source semantics.

The semantic inference module as the main component of the Knowledge-Assisted decoder refers to the retrieval of sensitive information for source messages in private knowledge, thereby understanding the deep sensitive information. Fine-grained sensitive information helps to locate the initial entity in private knowledge, improving the accuracy of inference. Thus, Rule-based local inference methods [38] can analyze the edges of sensitive entities to explore new entities and obtain new relationships, inferring new semantics, such as "Password is 123456" and "Google Account is abcd@gmail". However, this method may have a relatively long reasoning time and limited accuracy. To deal with these issues, neural networks can be used to model triples and multipaths thus establishing the relationship between sensitive entities and other related entities. By converting the rules into vector operations and applying the neural network method with strong learning ability, the end-to-end differentiable model is realized to ensure inference and generalisation. Besides, since harsh channel conditions may cause some core semantics to be lost during the decoding process, the semantic inference module can use private knowledge to infer the missing semantic information, thereby compensating for the information loss caused by channel impairments and noise, and assisting the system to infer reasonable semantics in SemCom scenarios with low signal-to-noise ratio.

As shown in the bottom part of Fig. 3.5, the data flow at the decoder part is illustrated. The distorted binary bits are first decoded by the receiver from the received wireless signals, these bit is converted to a token by the token

decoding module. A vocabulary has been constructed in the encoder during the conversion of entities to tokens. Therefore, the same applies to decoders, and the token will be converted to the corresponding entity. Finally, semantic information can be obtained by inferring various relationships of entities.

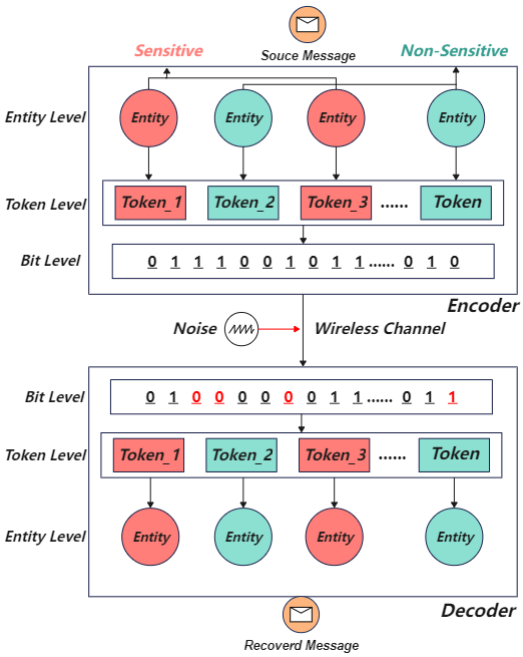

Figure 3.5: Data flows in the proposed transceiver.

3.4.3 Analysis on Eavesdropping Attacks

Despite we assume a trusted graph database in knowledge management of our framework, both global and personal knowledge may still be stolen and exploited by eavesdroppers. As a result, all three kinds of attacks discussed in previous section could occur. Let us demonstrate how our proposed SemCom framework can protect from the three eavesdropping attacks.

In the case of bit eavesdropping, attackers with no matched semantic coding model can only intercept bits via the wireless channel, and decode these bits at a syntactic level. Despite the attackers can detect the information exchanged between the two ends, they cannot obtain semantic information. Therefore, limited privacy could be leaked.

As discussed, the second type of global knowledge assisted semantics eavesdropping attack assumes that the attackers are equipped with a capable decoder along with the global knowledge. This attack may manifest

in the bit and token levels. Second, we match global knowledge with private knowledge in the entity alignment module for heterogeneous information, tokens cannot be turned into source messages without private knowledge. The decoding model from attackers may not have this function, much less private knowledge, resulting in a large number of errors in the decoding process. Thus, it is almost impossible for the attacker to obtain valuable public information from global knowledge. Our designed knowledge management layer and knowledge-assisted encoder provide dual protection against global knowledge assisted semantics eavesdropping.

Personal knowledge assisted semantics eavesdropping attacks empower attackers to decode public and private information. This attack has a great impact on the bit level and token level, and poses a challenge to the entity level. Similar to global knowledge assisted eavesdropping attacks, the graph database stores personal knowledge of the transmitter and receiver, radically reducing the risk of eavesdropping at the bit level. The difference is that we fuse the personal knowledge into private knowledge at the knowledge management layer, and attackers cannot get the private semantics even if it decodes through the personal knowledge, avoiding token level threats. However, smart attackers are likely to fuse personal knowledge to obtain private knowledge, launching a challenge to the entity level. To this end, we design a sensitive entity recognition module to further SemComreen sensitive entities in private knowledge, distinguishing the definition of sensitive information in the same private knowledge between eavesdroppers and receivers effectively, which ensures the transmission of private semantics precisely.

3.5 Open Issues and Outlook

We illustrate the workflow of the knowledge-assisted encoder and decoder and qualitatively analyse how the proposed architectural mechanisms mitigate the three representative eavesdropping attacks identified in Section 3.2. This analysis is intended to establish the security design rationale rather than provide a formal or quantitative security guarantee. Despite the expected prospects of the proposed knowledge-assisted privacy preserving SemCom framework, there are still some challenges that need to be addressed before relishing its full potential.

Dynamic Channel Condition: The transceivers in our proposed SemCom framework are assumed to be trained under a given channel condition. However, wireless channel conditions in practical scenarios are typically dynamic, and this may significantly degrade both data transmission accuracy and privacy levels. For example, severe bit error rate may lead to incorrect

tokens decoded at receivers, while excellent channel conditions might enable eavesdroppers to decode excessive public information, potentially compromising privacy levels. Therefore, enhancing the generalisation capability of transceivers in the proposed SemCom framework should be another non-trivial challenge. Some prompt-based learning algorithms can be exploited to timely adjust or fine-tune parameters in the coding model to adapt channel dynamics.

Scalability of the knowledge management layer: With the increase of network nodes and devices, the graph database needs to process more data, especially in the process of frequent knowledge updates. In the case of unstable networks or frequent node changes, it is particularly important to synchronize knowledge updates between different nodes and maintain the consistency of knowledge in the transceivers [39]. In addition, KG tasks are compute-intensive, and these tasks have different bandwidth requirements. In low-latency scenarios, how to precisely distribute these tasks to different nodes and ensure balanced computing load is an issue.

Overwhelmed Private Knowledge: Compared to global knowledge, the information volumes and training parameters in private knowledge are relatively insignificant, thus private knowledge may be overwhelmed by global knowledge. In this case, the information represented by sensitive entities in private knowledge will be replaced by global knowledge, when performing entity alignment module. A possible approach is to introduce complex attention mechanisms into the model to better utilize the knowledge. Additionally, considering varying knowledge preferences and limited knowledge storage capacities among different SemCom users, how to realize efficient knowledge construction to maximize the overall semantic performance in SemCom-based networks becomes rather challenging.

High Computational Burden on Mobile Devices: Private knowledge may contain numerous entities and edges, and embedding these into a coding model requires dealing with complex graph structures. This significantly increases the computational complexity of the model. Therefore, the training time could be prolonged, affecting the iteration and convergence speed of the model. To alleviate the computing burden on mobile devices, incremental learning and distributed computing can be utilized [40].

Lack of Standardized Metrics of Privacy in SemCom: Measuring the level of privacy in SemCom is another challenge. Traditional metrics from information theory, such as entropy and mutual information, may not be directly applied to measure privacy in SemCom. Entropy cannot distinguish between sensitive and non-sensitive information, and if a high entropy of a dataset, this does not mean a high privacy risk. Similarly, mutual information can measure the amount of information between two variables/messages, but

it cannot specifically measure which information poses a threat to privacy. To define a suitable metric, exploiting differential privacy could be a potential way.

3.6 Conclusion

In this thesis, we explored the utilisation of knowledge to enhance data privacy in SemCom networks. We began by analyzing the potential three kinds of eavesdropping attacks in SemCom, then proposed our privacy-preserving SemCom framework, consisting of data transmission layer and knowledge management layer. Especially, we elaborated the transceiver design in this framework to ensure an accurate data transmission at a semantic level while protecting sensitive information from eavesdroppers by exploiting private knowledge at the transmitter and receiver sides. This work can be seen as a pioneer in exploiting knowledge to enhance data privacy in SemCom.

Chapter 4

Knowledge-Assisted Transceiver Design for Privacy Preservation

4.1 Introduction

SemCom has emerged as a promising communication paradigm that shifts the communication objective from accurately transmitting symbols to reliably conveying semantic information [41].

Despite its impressive communication efficiency, the deployment of SemCom introduces new privacy challenges [42] [43] [44]. Existing semantic encoders extract compact latent representations that preserve task-relevant information while simultaneously embedding abundant sensitive semantic attributes. Once the transmitted semantic representation is intercepted by an unauthorized receiver, an eavesdropper may infer sensitive user information through semantic reconstruction or attribute inference attacks [45]. Compared with conventional bit-level communications, semantic representations usually contain much richer contextual information, making privacy leakage considerably more severe. Consequently, privacy preservation has become one of the fundamental challenges for practical SemCom systems [46].

Differential privacy (DP) has been widely recognized as an effective mathematical framework for protecting sensitive information by injecting calibrated random perturbations into the transmitted data [47]. Owing to its rigorous privacy guarantees and robustness against arbitrary post-processing, DP has recently been introduced into SemCom systems. However, directly perturbing latent semantic representations inevitably degrades semantic reconstruction quality because useful semantic information and privacy-sensitive

information are usually highly coupled in the latent space. Although increasing the privacy budget improves reconstruction performance, it simultaneously weakens privacy protection, leading to the well-known privacy–utility tradeoff [48]. Existing DP-based SemCom frameworks therefore suffer from considerable performance degradation under strong privacy constraints [49] [50].

Meanwhile, recent studies have shown that external knowledge can significantly improve semantic representation learning by providing high-level semantic priors during information reconstruction [51]. Shared knowledge enables the receiver to infer missing semantic information from contextual relationships instead of relying solely on the received latent representation. This observation motivates a new opportunity for privacy-preserving SemCom. Specifically, if DP is applied only to the sensitive latent representation while semantic reconstruction is assisted by shared knowledge, the semantic distortion introduced by DP may be effectively compensated without sacrificing rigorous privacy guarantees [52]. Nevertheless, existing studies seldom investigate how knowledge assistance and DP can be jointly optimized, and the privacy advantage brought by knowledge asymmetry between legitimate users and eavesdroppers remains insufficiently understood [53].

Furthermore, simply introducing DP cannot completely eliminate sensitive information contained in the latent representation. Since deep neural networks naturally learn correlated semantic features, privacy-related information may still remain embedded in the transmitted latent space even after perturbation [54]. Therefore, additional representation learning mechanisms are required to explicitly suppress privacy-related semantic features during training. Adversarial learning has recently demonstrated remarkable capability in learning invariant feature representations by introducing competing optimisation objectives. Integrating adversarial optimisation into SemCom therefore provides an effective way to further remove sensitive semantic information while preserving semantic utility.

Motivated by these observations, this chapter proposes a knowledge-assisted privacy-preserving SemCom framework based on DP and adversarial representation learning [55]. Specifically, the latent semantic representation is decomposed into utility and sensitive subspaces, where DP is selectively applied to the sensitive latent variables through the Gaussian mechanism. To compensate for the reconstruction degradation caused by DP perturbation, shared semantic knowledge is incorporated into the semantic decoder to provide high-level semantic priors during reconstruction. Furthermore, a privacy-aware adversarial optimisation strategy is introduced to suppress sensitive semantic information during latent representation learning. To theoretically characterize the privacy protection capability, the relationship among

DP, semantic reconstruction, and knowledge mismatch is analyzed, demonstrating that knowledge asymmetry further amplifies privacy protection beyond conventional DP mechanisms [54].

The main contributions of this chapter are summarized as follows.

- We propose a knowledge-assisted privacy-preserving SemCom framework that jointly optimizes the transceiver under DP-constrained learning and knowledge-conditioned reconstruction to improve the privacy–utility tradeoff.
- A theoretical privacy analysis is developed to characterize the influence of DP and knowledge mismatch on semantic reconstruction and sensitive information inference, providing rigorous privacy guarantees for the proposed framework.
- A privacy-aware adversarial optimisation strategy is proposed to jointly optimize semantic reconstruction and privacy preservation through alternating minimax learning, enabling the semantic encoder to learn privacy-invariant latent representations.
- Extensive simulation results demonstrate that the proposed framework achieves superior semantic reconstruction quality while significantly reducing sensitive semantic inference compared with existing DP SemCom schemes.

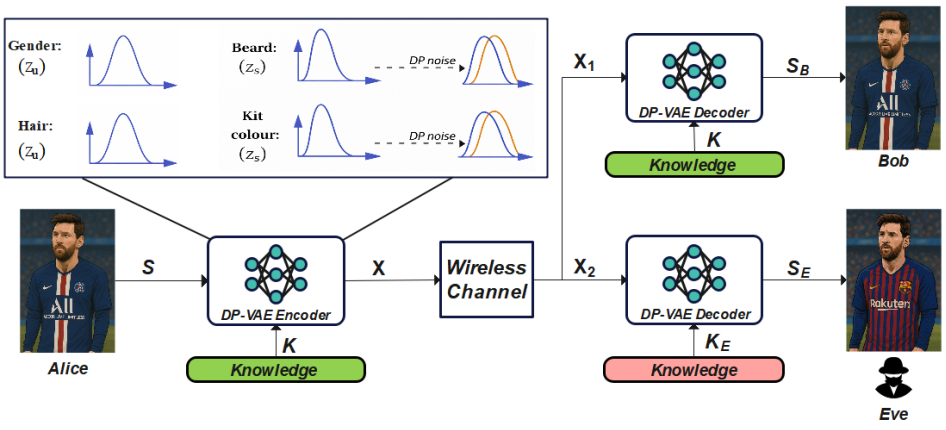

Figure 4.1: Knowledge Assisted DP SemCom System.

4.2 System Model

4.2.1 Semantic Source Model

We consider an end-to-end SemCom system in which a legitimate transmitter, Alice, aims to convey semantic information to a legitimate receiver, Bob, over a wireless channel, while preventing a passive eavesdropper, Eve, from inferring sensitive semantic attributes. Let $S \in \mathcal{S}$ denote the semantic source, which may represent an image, a video frame, or other high-level semantic content. The semantic source is modeled as a random variable drawn from an unknown but fixed distribution

$$S \sim p_S(s). \tag{4.1}$$

Upon observing the semantic source S, Alice employs a variational autoencoder (VAE)-based semantic encoder to map S into a continuous latent representation $Z \in \mathbb{R}^d$, which serves as a compact semantic description for wireless channel transmission. The encoding process is characterized by a conditional variational posterior distribution:

$$Z \sim q_\phi(z \mid s, K), \tag{4.2}$$

where K denotes the shared prior knowledge between Alice and Bob. Such knowledge may include shared model parameters, semantic priors, contextual information, or other side information acquired during training.

The latent representation Z is subsequently processed and transmitted over a wireless channel. At the receiver side, Bob utilizes both the received channel observations and the shared knowledge K to reconstruct the semantic information. In contrast, the eavesdropper Eve is assumed to observe the wireless channel output but possesses different or incomplete knowledge, denoted by $K_E \neq K$. This asymmetry in prior knowledge fundamentally differentiates the semantic inference capabilities of the legitimate receiver and the eavesdropper.

The objective of the system is therefore to enable reliable semantic reconstruction at Bob while ensuring that sensitive semantic attributes remain protected against inference attacks by Eve, even when Eve has access to the transmitted signals.

4.2.2 Latent Space Decomposition Model

To explicitly balance semantic utility and privacy protection, we adopt a structured latent representation in the VAE-based semantic encoder [56].

Specifically, the latent variable Z is decomposed into two semantically distinct components,

$$Z = (Z_u, Z_s), \tag{4.3}$$

where Z_u represents task-relevant but non-sensitive semantic information, while Z_s captures sensitive semantic attributes that require privacy protection, such as identity-related or appearance-related features.

Correspondingly, the variational posterior distribution produced by the encoder is factorized as

$$q_\phi(z \mid s, K) = q_{\phi_u}(z_u \mid s, K)\, q_{\phi_s}(z_s \mid s, K), \tag{4.4}$$

where ϕ_u and ϕ_s denote the parameters associated with the non-sensitive and sensitive latent subspaces, respectively. This decomposition enables privacy-preserving operations to be selectively applied to the sensitive semantic components without unnecessarily degrading the representation of non-sensitive semantics.

To prevent leakage of sensitive semantic information, a DP mechanism is introduced at the latent semantic level. Specifically, the sensitive latent variable Z_s is processed by a randomized mechanism $\mathcal{M}(\cdot)$ before transmission, yielding a perturbed version

$$\tilde{Z}_s = \mathcal{M}(Z_s). \tag{4.5}$$

The resulting latent representation used for semantic transmission is then given by

$$\tilde{Z} = (Z_u, \tilde{Z}_s). \tag{4.6}$$

The DP mechanism $\mathcal{M}(\cdot)$ is designed to satisfy (ε, δ)-DP with respect to a predefined adjacency relation on the semantic source space. In particular, two semantic inputs s and s' are considered adjacent if they differ only in sensitive semantic attributes while sharing identical non-sensitive semantic content. Under this definition, the DP constraint ensures that the distribution of the perturbed latent variable $\tilde{Z}_s$ is statistically indistinguishable for adjacent semantic inputs [57].

Formally, if the mechanism $\mathcal{M}(\cdot)$ satisfies (ε, δ)-DP, for any pair of adjacent semantic inputs $s \sim s'$ and any measurable set $\mathcal{O}$, the following condition holds:

$$\Pr\{\mathcal{M}(Z_s) \in \mathcal{O}\} \leq e^{\varepsilon} \Pr\{\mathcal{M}(Z'_s) \in \mathcal{O}\} + \delta, \tag{4.7}$$

where Z_s and Z'_s denote the sensitive latent variables inferred from s and s', respectively. A smaller ε implies the DP possesses stronger privacy-preserving capabilities.

By enforcing DP directly in the latent semantic space, the proposed system provides a principled and tractable approach to protecting sensitive semantic information.

4.2.3 Knowledge-Assisted Decoding Model

In addition to differentially private latent representations, the proposed SemCom system incorporates structured external knowledge to assist semantic decoding at the legitimate receiver. The primary role of knowledge is not to replace the latent representations but to provide auxiliary semantic priors that facilitate robust image reconstruction under DP perturbations and to induce decoding asymmetry between the legitimate receiver and the eavesdropper.

When the semantic signal passes through the physical channel, the received signal X_1 at the receiver Bob and signal X_2 at the eavesdropper Eve with different properties can be modeled: $X_1 = h_B X + n_B$ and $X_2 = h_E X + n_E$, where h denotes the coefficient of the linear channel, $n \sim \mathcal{CN}(0, \delta_n^2)$ is independent and uniform distributed additive Gaussian noise.

Knowledge as Textual Prompt Conditioning

The external knowledge is modeled in the form of a KG, represented as a set of semantic triples $\mathcal{G} = \{(h, r, t)\}$, where h and t denote entities corresponding to sensitive semantic concepts, and r denotes the semantic relation between them. The KG captures structured relationships among sensitive attributes but does not contain user-specific private information [58]. Therefore, the KG itself is assumed to be private and is not subject to DP constraints. Each entity in the KG is associated with a learnable embedding vector, and the collection of all entity embeddings forms a semantic embedding table that provides structured semantic priors for the decoding process [59].

To integrate knowledge into the semantic decoder, the KG is transformed into a textual semantic prompt using predefined template-based rules. The generated text prompt describes the relevant semantic attributes and relations in natural language form and serves as a compact representation of the available knowledge.

From a modeling perspective, the textual prompt is treated as conditional knowledge information and is denoted by K. Accordingly, the knowledge variable K encapsulates the semantic priors derived from the KG and is provided to the decoder as auxiliary conditioning information.

Bob Decoding

At the receiver side, the semantic decoder directly exploits both the non-sensitive latent variable Z_u and the differentially private sensitive latent variable Z_s for image reconstruction. The presence of DP noise introduces uncertainty into Z_s, which may degrade reconstruction quality if decoded without additional prior information.

To mitigate this effect, the decoder leverages the knowledge variable K to guide the interpretation of the latent representations. Specifically, the semantic decoding process at the legitimate receiver Bob is modeled as

$$p_\theta(s \mid Z_u, \tilde{Z}_s, K), \tag{4.8}$$

where the knowledge-conditioned decoder utilizes structured semantic priors to compensate for the distortion induced by DP perturbations and channel noise.

Eve Decoding

The proposed framework assumes asymmetric knowledge availability between the legitimate receiver and the eavesdropper. While Bob has access to the intended KG and the corresponding semantic prompts, the eavesdropper Eve is assumed to possess a different or mismatched knowledge representation, denoted by K_E.

Although Eve observes the same differentially private latent representations transmitted over the wireless channel, her semantic reconstruction relies on a mismatched conditional distribution

$$p_{\theta_E}(s \mid Z_u, \tilde{Z}_s, K_E), \tag{4.9}$$

which leads to semantic inconsistency and degraded reconstruction quality. This knowledge-induced mismatch significantly impairs Eve's ability to recover the original semantic content, even in the absence of additional channel impairments.

Consequently, the combination of DP perturbation and knowledge asymmetry enables reliable semantic reconstruction at the legitimate receiver while substantially limiting the semantic inference capability of the eavesdropper.

4.2.4 Preliminary of Total Variation

The total variation (TV) distance is adopted as a theoretical privacy performance metric, as it directly characterizes the optimal distinguishability

between different sensitive semantic attributes from the eavesdropper's observation [60] [61]. In particular, TV provides a worst-case, model-agnostic upper bound on Eve's inference capability. However, since TV does not capture semantic reconstruction quality, it is complemented by semantic distortion metrics in the experimental results [62] [63].

We explicitly characterize privacy performance from the eavesdropper's perspective. Let $A = a(S)$ denote a sensitive semantic attribute extracted from the semantic source, and let Y_E denote the observation available to the eavesdropper after wireless transmission and decoding.

For each attribute value $a \in \mathcal{A}$, the induced distribution of the eavesdropper's observation is given by

$$P_{Y_E|A=a}(\cdot) \triangleq \Pr\{Y_E \in \cdot \mid A = a\}. \tag{4.10}$$

We adopt the total variation (TV) distance between these conditional distributions as a privacy performance metric [64]. In particular, for binary sensitive attributes, the privacy leakage is quantified as

$$\mathrm{TV} \triangleq \left\| P_{Y_E|A=0} - P_{Y_E|A=1} \right\|_{\mathrm{TV}}, \tag{4.11}$$

where the total variation distance between two probability measures P and Q is defined as

$$\|P - Q\|_{\mathrm{TV}} = \sup_{\mathcal{O}} \left| P(\mathcal{O}) - Q(\mathcal{O}) \right|. \tag{4.12}$$

The TV metric provides a worst-case, model-agnostic measure of the distinguishability between different sensitive semantic attributes from the eavesdropper's observation [65]. Moreover, for binary attributes with equal prior probabilities, the TV distance is directly related to the Bayes-optimal inference success probability of the eavesdropper as

$$P_{\mathrm{succ}}^{\mathrm{Eve}} = \frac{1}{2}\big(1 + \mathrm{TV}\big). \tag{4.13}$$

Therefore, minimizing the TV distance corresponds to limiting the maximum achievable inference capability of the eavesdropper, and serves as a fundamental privacy performance metric in the considered SemCom system.

4.3 Privacy Analysis

In this section, we present step-by-step derivations for the privacy guarantees of the proposed DP-VAE SemCom system. Our analysis consists of (i) end-to-end DP preservation, (ii) explicit bounds on Eve's optimal sensitive-attribute inference accuracy under (ε, δ)-DP, and (iii) a rigorous characterisation of how knowledge mismatch degrades Eve's semantic inference via mismatched log-loss [66] [67].

4.3.1 End-to-End DP Preservation

Eve is a passive eavesdropper observing the channel output Y_E and knowing the system architecture. Bob and Eve possess different knowledge representations, denoted by K and K_E with $K_E \neq K$. DP is enforced on the sensitive latent variable Z_s at the transmitter, producing $\tilde{Z}_s$.

Throughout, we use the attribute-level adjacency relation: two semantic sources $s \sim s'$ differ only in sensitive attributes while sharing the same non-sensitive semantics. Let the DP mechanism be $\mathcal{M} : s \mapsto \tilde{Z}_s$ and assume $\mathcal{M}$ satisfies (ε, δ)-DP:

$$\Pr\{\mathcal{M}(s) \in \mathcal{A}\} \leq e^{\varepsilon} \Pr\{\mathcal{M}(s') \in \mathcal{A}\} + \delta, \quad \forall \mathcal{A} \subseteq \mathcal{Z}_s, \ \forall s \sim s'. \tag{4.14}$$

The eavesdropper's observation is generated by a (possibly randomized) channel and a subsequent decoding pipeline that depends only on $\tilde{Z}_s$ (and other variables such as Z_u) and Eve's knowledge K_E. Abstract this pipeline as a Markov kernel, which is a stochastic mapping [68] [69].

$$\kappa_E(\mathcal{O} \mid \tilde{z}_s) \triangleq \Pr\{Y_E \in \mathcal{O} \mid \tilde{Z}_s = \tilde{z}_s, K_E\}, \tag{4.15}$$

where $\mathcal{O}$ is any measurable subset of the observation space.

Define the end-to-end mechanism (from s to Y_E) as $\mathcal{T}_E(s) \triangleq Y_E$. For any measurable $\mathcal{O}$, by the law of total probability,

$$\begin{aligned} \Pr\{\mathcal{T}_E(s) \in \mathcal{O}\} &= \Pr\{Y_E \in \mathcal{O} \mid s\} \\ &= \int \Pr\{Y_E \in \mathcal{O} \mid \tilde{Z}_s = \tilde{z}_s, K_E\} \, dP_{\tilde{Z}_s|s}(\tilde{z}_s) \\ &= \int \kappa_E(\mathcal{O} \mid \tilde{z}_s) \, dP_{\tilde{Z}_s|s}(\tilde{z}_s). \end{aligned} \tag{4.16}$$

Now define a measurable set in $\tilde{Z}_s$-space:

$$\mathcal{A}_\tau \triangleq \{\tilde{z}_s : \ \kappa_E(\mathcal{O} \mid \tilde{z}_s) > \tau\}, \quad \tau \in [0, 1]. \tag{4.17}$$

Using the threshold representation for $[0, 1]$-valued functions,

$$\begin{aligned} \Pr\{\mathcal{T}_E(s) \in \mathcal{O}\} &= \int \kappa_E(\mathcal{O} \mid \tilde{z}_s) \, dP_{\tilde{Z}_s|s}(\tilde{z}_s) \\ &= \int_0^1 P_{\tilde{Z}_s|s}(\mathcal{A}_\tau) \, d\tau. \end{aligned} \tag{4.18}$$

Apply (ε, δ)-DP in (4.14) to each $\mathcal{A}_\tau$ (note $\mathcal{A}_\tau$ is measurable):

$$P_{\tilde{Z}_s|s}(\mathcal{A}_\tau) \leq e^{\varepsilon} P_{\tilde{Z}_s|s'}(\mathcal{A}_\tau) + \delta, \quad \forall \tau \in [0, 1]. \tag{4.19}$$

Integrating both sides over $\tau \in [0,1]$ and using (4.18), we obtain

$$\begin{aligned}\Pr\{\mathcal{T}_E(s) \in \mathcal{O}\} &= \int_0^1 P_{\tilde{Z}_s|s}(\mathcal{A}_\tau)\, d\tau \\ &\le \int_0^1 \left(e^{\varepsilon} P_{\tilde{Z}_s|s'}(\mathcal{A}_\tau) + \delta\right) d\tau \\ &= e^{\varepsilon} \int_0^1 P_{\tilde{Z}_s|s'}(\mathcal{A}_\tau)\, d\tau + \delta \\ &= e^{\varepsilon} \Pr\{\mathcal{T}_E(s') \in \mathcal{O}\} + \delta. \end{aligned} \tag{4.20}$$

Equation (4.20) is exactly (ε, δ)-DP for the end-to-end mechanism $\mathcal{T}_E$. This completes the explicit derivation of DP preservation under arbitrary stochastic post-processing.

4.3.2 Eve's Optimal Binary Attribute Inference Bounds

Let $A \in \{0,1\}$ be a binary sensitive attribute (e.g., beard/no-beard) with equal prior $\Pr(A=0) = \Pr(A=1) = 1/2$. Let P_0 and P_1 denote the distributions of Y_E under $A=0$ and $A=1$:

$$P_a(\mathcal{O}) \triangleq \Pr\{Y_E \in \mathcal{O} \mid A = a, K_E\}, \quad a \in \{0,1\}. \tag{4.21}$$

From DP to a two-sided event inequality

From end-to-end DP (4.20), for any measurable $\mathcal{O}$,

$$P_0(\mathcal{O}) \le e^{\varepsilon} P_1(\mathcal{O}) + \delta, \qquad P_1(\mathcal{O}) \le e^{\varepsilon} P_0(\mathcal{O}) + \delta. \tag{4.22}$$

Bounding total variation via a maximizer event

Recall the definition of total variation distance:

$$\|P_0 - P_1\|_{\mathrm{TV}} = \sup_{\mathcal{O}} |P_0(\mathcal{O}) - P_1(\mathcal{O})|. \tag{4.23}$$

Let $\mathcal{O}^\star$ be a (measurable) set achieving the supremum for the difference $P_0(\mathcal{O}) - P_1(\mathcal{O})$ (or arbitrarily close to it), so that

$$\|P_0 - P_1\|_{\mathrm{TV}} \approx P_0(\mathcal{O}^\star) - P_1(\mathcal{O}^\star). \tag{4.24}$$

Applying (4.22) to $\mathcal{O}^\star$ yields

$$\begin{aligned} P_0(\mathcal{O}^\star) - P_1(\mathcal{O}^\star) &\le (e^{\varepsilon} - 1) P_1(\mathcal{O}^\star) + \delta \\ &\le (e^{\varepsilon} - 1) \cdot 1 + \delta \\ &= e^{\varepsilon} - 1 + \delta. \end{aligned} \tag{4.25}$$

This is a valid (but loose) bound.

A tighter bound is obtained by also applying (4.22) to the complement $(\mathcal{O}^\star)^c$:

$$\begin{aligned} P_1((\mathcal{O}^\star)^c) &\le e^\varepsilon P_0((\mathcal{O}^\star)^c) + \delta \\ 1 - P_1(\mathcal{O}^\star) &\le e^\varepsilon (1 - P_0(\mathcal{O}^\star)) + \delta \\ P_0(\mathcal{O}^\star) &\le \frac{e^\varepsilon - 1 + \delta + P_1(\mathcal{O}^\star)}{e^\varepsilon}. \end{aligned} \tag{4.26}$$

Subtracting $P_1(\mathcal{O}^\star)$ from both sides of (4.26), we obtain

$$\begin{aligned} P_0(\mathcal{O}^\star) - P_1(\mathcal{O}^\star) &\le \frac{e^\varepsilon - 1 + \delta}{e^\varepsilon} + \left(\frac{1}{e^\varepsilon} - 1\right) P_1(\mathcal{O}^\star) \\ &\le \frac{e^\varepsilon - 1 + \delta}{e^\varepsilon}, \end{aligned} \tag{4.27}$$

since $(\frac{1}{e^\varepsilon} - 1) \le 0$ and $P_1(\mathcal{O}^\star) \ge 0$.

Similarly, if the supremum is achieved by $P_1(\mathcal{O}) - P_0(\mathcal{O})$, symmetry yields the same bound. Therefore,

$$\|P_0 - P_1\|_{\mathrm{TV}} \le 1 - e^{-\varepsilon} + \delta e^{-\varepsilon}. \tag{4.28}$$

In the common regime where ε is moderate and δ is small, (4.28) is already informative and explicitly computable.

From TV to Bayes-optimal success probability

For binary hypothesis testing with equal priors, the Bayes-optimal success probability satisfies

$$\Pr(\hat{A}_E = A) = \frac{1}{2}\left(1 + \|P_0 - P_1\|_{\mathrm{TV}}\right). \tag{4.29}$$

Combining (4.28) and (4.29) yields the explicit bound

$$\begin{aligned} \Pr(\hat{A}_E = A) &\le \frac{1}{2}\left(1 + 1 - e^{-\varepsilon} + \delta e^{-\varepsilon}\right) \\ &= 1 - \frac{e^{-\varepsilon}}{2} + \frac{\delta e^{-\varepsilon}}{2}. \end{aligned} \tag{4.30}$$

This provides a concrete, end-to-end DP-driven bound on Eve's optimal sensitive-attribute inference accuracy.

4.3.3 Knowledge Asymmetry: Mismatched Log-Loss Derivation and Consequences

We now derive a rigorous, calculation-based statement showing how knowledge mismatch ($K \neq K_E$) degrades Eve's ability to interpret (Z_u, Z_s), while Z_s still directly participates in reconstruction.

Let $Z \triangleq (Z_u, Z_s)$ denote the full latent variable used by both Bob and Eve in decoding. Consider the conditional semantic reconstruction distributions

$$p_B(s \mid z) \triangleq p(s \mid z, K), \qquad p_E(s \mid z) \triangleq p(s \mid z, K_E). \tag{4.31}$$

Assume $p_B(s \mid z)$ represents the (matched) target conditional distribution induced by the legitimate knowledge K (i.e., the "correct" semantic prior for the intended task).

A key identity: mismatch increases conditional log-loss by an expected KL term

Consider the conditional negative log-likelihood (log-loss) of using Eve's mismatched model p_E under the true conditional p_B. Conditioned on $Z = z$,

$$\begin{aligned}
&\mathbb{E}_{S\sim p_B(\cdot|z)}[-\log p_E(S \mid z)] = && (4.32)\\
&\quad \mathbb{E}_{S\sim p_B(\cdot|z)}[-\log p_B(S \mid z)] && (4.33)\\
&\quad + \mathbb{E}_{S\sim p_B(\cdot|z)}\left[\log \frac{p_B(S \mid z)}{p_E(S \mid z)}\right] \\
&\quad = H(p_B(\cdot \mid z)) && (4.34)\\
&\quad + D_{\mathrm{KL}}(p_B(\cdot \mid z) \,\|\, p_E(\cdot \mid z))\,, && (4.35)
\end{aligned}$$

where $H(p_B(\cdot \mid z))$ denotes the conditional entropy (in nats if log is natural).

Now take expectation over the latent variable distribution of Z:

$$\begin{aligned}
\mathbb{E}[-\log p_E(S \mid Z)] &= \mathbb{E}[-\log p_B(S \mid Z)] + && (4.36)\\
&\quad \mathbb{E}_Z[D_{\mathrm{KL}}(p_B(\cdot \mid Z) \,\|\, p_E(\cdot \mid Z))]\,. && (4.37)
\end{aligned}$$

Equation (4.37) is an exact identity (not an inequality): it shows that knowledge mismatch necessarily increases the achievable conditional log-loss by an expected KL divergence term. Importantly, this degradation holds even if Eve observes the same latent variables $Z = (Z_u, Z_s)$ as Bob; the difference is purely due to semantic-prior mismatch ($K_E \neq K$) [68] [70].

From increased log-loss to degraded inference (a computable bridge)

For discrete sensitive attribute inference $A = a(S)$, one can connect log-loss to classification error. Let Eve produce a posterior $\pi_E(a \mid y) \triangleq \Pr(A = a \mid Y_E = y, K_E)$ and use MAP $\hat{A}_E(y) = \arg\max_a \pi_E(a \mid y)$. Then, for any y,

$$\Pr(\hat{A}_E \neq A \mid Y_E = y) \leq \frac{-\log \max_a \pi_E(a \mid y)}{\log 2}, \tag{4.38}$$

which follows since $\max_a \pi_E(a \mid y) \leq 2^{-\ell(y)}$ where $\ell(y) \triangleq -\log_2 \max_a \pi_E(a \mid y)$ and $\Pr(\hat{A}_E = A \mid y) = \max_a \pi_E(a \mid y)$.

Taking expectations and using Jensen-type arguments yields an upper bound of Eve's success probability in terms of her achievable posterior concentration, which is degraded when the mismatch KL term in (4.37) increases. Thus, the mismatch term provides a quantitative lever to argue that knowledge asymmetry amplifies the privacy protection beyond DP perturbation alone.

Interpretation in the proposed DP-VAE system

In our system, Z_s remains a direct input to both Bob's and Eve's decoders for image reconstruction. DP introduces uncertainty in Z_s through $\tilde{Z}_s$, while the knowledge variable provides an auxiliary semantic prior to interpret the (noisy) latent. The derivations above show: (i) DP guarantees remain valid end-to-end regardless of Eve's post-processing; and (ii) knowledge mismatch introduces an unavoidable increase in the conditional log-loss quantified by the expected KL divergence in (4.37), thereby making semantic reconstruction and sensitive inference strictly harder for Eve.

4.4 Privacy-Aware Adversarial Optimisation

To further suppress semantic leakage during representation learning, we introduce a privacy-aware adversarial optimisation [71] [72]. Specifically, an adversarial classifier is incorporated during training to infer sensitive semantic attributes from the transmitted latent representation, while the semantic encoder is optimized to confuse the adversary. Such adversarial optimisation encourages the encoder to remove privacy-related information from the sensitive latent subspace while preserving semantic information required for legitimate reconstruction [73] [74].

4.4.1 Adversarial Learning

The proposed adversarial learning consists of three trainable modules, namely the semantic encoder E_ϕ, the semantic decoder D_θ, and an adversarial classifier C_ψ.

Given a semantic source S, the encoder first generates the structured latent representation

$$Z = (Z_u, Z_s) = E_\phi(S). \tag{4.39}$$

Following the DP mechanism introduced in Section II, the sensitive latent representation is perturbed as

$$\tilde{Z}_s = M(Z_s), \tag{4.40}$$

leading to the transmitted latent representation

$$\tilde{Z} = (Z_u, \tilde{Z}_s). \tag{4.41}$$

The legitimate receiver reconstructs the semantic source according to

$$\hat{S} = D_\theta(\tilde{Z}, K), \tag{4.42}$$

where the shared knowledge K provides semantic priors to compensate for the perturbation introduced by DP.

During training, an adversarial classifier attempts to infer the sensitive semantic attribute from the perturbed sensitive latent variable,

$$\hat{A} = C_\psi(\tilde{Z}_s), \tag{4.43}$$

where A denotes the sensitive semantic attribute defined in Section III. The adversarial classifier is only employed during training and is discarded during inference.

4.4.2 Optimisation Objective

To jointly achieve reliable semantic reconstruction and privacy preservation, the proposed framework optimizes the semantic reconstruction loss, the latent regularisation loss, and the adversarial privacy loss.

Semantic Reconstruction Loss

The semantic reconstruction loss is defined as

$$\mathcal{L}_{\text{rec}} = \mathbb{E}\left[d(S, \hat{S})\right], \tag{4.44}$$

where $d(\cdot, \cdot)$ denotes the reconstruction distortion metric. In this work, the mean squared error (MSE) is adopted,

$$d(S, \hat{S}) = \|S - \hat{S}\|_2^2. \tag{4.45}$$

Latent Regularisation

Following the VAE formulation, the latent variables are regularized toward the standard Gaussian prior,

$$\mathcal{L}_{\text{KL}} = D_{\text{KL}}\left(q_\phi(Z|S, K) \| \mathcal{N}(0, I)\right). \tag{4.46}$$

Adversarial Privacy Loss

The adversarial classifier is optimized using the binary cross-entropy loss

$$\mathcal{L}_{\text{adv}} = -\mathbb{E}\left[A \log \hat{A} + (1 - A) \log(1 - \hat{A})\right], \tag{4.47}$$

where

$$\hat{A} = C_\psi(\tilde{Z}_s). \tag{4.48}$$

The adversarial classifier minimizes $\mathcal{L}_{\text{adv}}$ to improve sensitive attribute prediction, whereas the semantic encoder attempts to maximize the same objective, thereby suppressing privacy-related information contained in the transmitted latent representation.

Overall Objective

The overall optimisation problem is formulated as

$$\min_{\phi,\theta} \max_{\psi} \; \mathcal{L}_{\text{rec}} + \beta \mathcal{L}_{\text{KL}} - \lambda \mathcal{L}_{\text{adv}}, \tag{4.49}$$

where β controls the latent regularisation strength and λ balances semantic utility and privacy preservation.

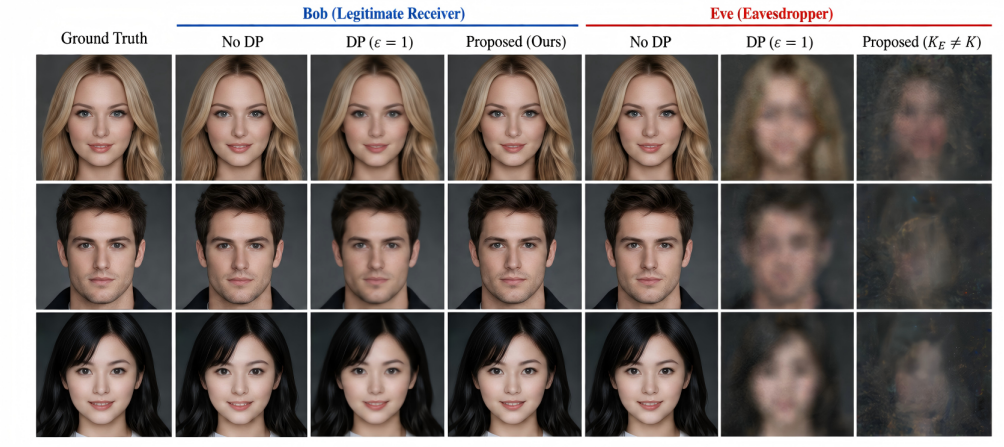

Figure 4.2: Legitimate Receiver Bob and eavesdropper Eve.

4.4.3 Alternating Optimisation Strategy

The proposed optimisation strategy is trained using an alternating minimax optimisation strategy. During each iteration, the adversarial classifier is first optimized while fixing the encoder and decoder. Subsequently, the classifier is frozen, and the semantic encoder together with the decoder are updated to minimize the overall objective while confusing the adversary. The complete training procedure is summarized in Algorithm 1.

Algorithm 1 Privacy-Aware Adversarial Optimisation

Input: Training dataset $\mathcal{D}$, shared knowledge K, privacy budget (ε, δ)
Output: Trained encoder E_ϕ and decoder D_θ

Initialize encoder E_ϕ, decoder D_θ, and adversarial classifier C_ψ.
Sample a mini-batch (S, A) from $\mathcal{D}$.
Encode the semantic source to obtain $(Z_u, Z_s) = E_\phi(S)$.
Generate the DP-protected latent representation $\tilde{Z}_s = M(Z_s)$.
Construct the transmitted latent representation $\tilde{Z} = (Z_u, \tilde{Z}_s)$.
Reconstruct the semantic source $\hat{S} = D_\theta(\tilde{Z}, K)$.
Infer the sensitive attribute $\hat{A} = C_\psi(\tilde{Z}_s)$.
Compute $\mathcal{L}_{\text{rec}}$, $\mathcal{L}_{\text{KL}}$ and $\mathcal{L}_{\text{adv}}$.
Update the adversarial classifier by minimizing $\mathcal{L}_{\text{adv}}$.
Update the encoder and decoder by minimizing $\mathcal{L} = \mathcal{L}_{\text{rec}} + \beta\mathcal{L}_{\text{KL}} - \lambda\mathcal{L}_{\text{adv}}$.
return E_ϕ and D_θ.

4.5 Simulation Results

In this section, comprehensive simulations are conducted to evaluate the performance of the proposed knowledge-assisted privacy-preserving SemCom framework. The proposed scheme is compared with representative SemCom methods under different privacy budgets. The experimental evaluation focuses on semantic reconstruction quality, privacy protection capability, and the effectiveness of the proposed adversarial optimisation. Unless otherwise specified, all experimental results are averaged over five independent runs to ensure statistical reliability.

4.5.1 Simulation Settings

The proposed framework is implemented using PyTorch and trained on a workstation equipped with an NVIDIA RTX 4080 GPU. The CelebA dataset is employed as the benchmark dataset since it contains abundant facial semantic attributes and is widely adopted in SemCom and privacy-preserving learning tasks. All face images are resized to 128×128 before training. The entire dataset is randomly divided into training, validation, and testing subsets with a ratio of 8:1:1. A fixed random seed of 42 is used for dataset partitioning to ensure reproducibility, and the resulting split is kept unchanged across all experiments. No additional identity-disjoint constraint is imposed beyond this random split. For repeated experiments, five independent random seeds $\{0, 1, 2, 3, 4\}$ are used for model initialisation, mini-batch shuffling, and stochastic perturbation.

The SemCom system is implemented based on a variational autoencoder (VAE). Specifically, the semantic encoder extracts latent semantic features from the source image and decomposes them into the utility latent variable Z_u and the sensitive latent variable Z_s. Following the proposed privacy-preserving framework, DP is applied only to Z_s using the Gaussian mechanism, while the utility latent representation is transmitted without perturbation. At the receiver, the shared semantic knowledge is incorporated into the decoder to compensate for the information distortion introduced by DP. Furthermore, an adversarial classifier is employed during training to infer sensitive semantic attributes from the perturbed latent representation, forcing the encoder to learn privacy-invariant semantic features through adversarial optimisation.

The entire network is optimized using the Adam optimizer with an initial learning rate of 1×10^{-4} and a batch size of 64. The latent dimension is fixed at 256 throughout all experiments. Unless otherwise specified, the privacy budget is set to $\varepsilon = 1$ with $\delta = 10^{-5}$. The weighting coefficients of the KL

divergence loss and the adversarial loss are empirically chosen as $\beta = 0.01$ and $\lambda = 0.1$, respectively.

To demonstrate the effectiveness of the proposed framework, four representative schemes are considered for comparison: 1) conventional SemCom without privacy protection, 2) DP SemCom 3) knowledge-assisted DP SemCom without adversarial optimisation (KA-DP), and 4) the proposed knowledge-assisted privacy-aware SemCom framework (Proposed).

The reconstruction performance is evaluated using Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Learned Perceptual Image Patch Similarity (LPIPS). Higher PSNR and SSIM together with lower LPIPS indicate better semantic reconstruction quality. To evaluate privacy preservation capability, the attack accuracy of the adversarial classifier is adopted as the primary metric. A lower attack accuracy indicates stronger protection against semantic inference attacks.

4.5.2 Performance Evaluation

Fig. 4.2 presents the qualitative comparison of reconstructed images under different SemCom schemes. Without privacy protection, the reconstructed images preserve abundant semantic details, but simultaneously expose sensitive information that can be exploited by an eavesdropper. Although DP effectively suppresses sensitive semantic leakage by perturbing the sensitive latent representation, the injected Gaussian noise inevitably causes reconstruction distortion. Benefiting from the proposed knowledge-assisted semantic reconstruction mechanism, the legitimate receiver successfully compensates for the semantic information lost during perturbation, producing visually clearer reconstruction results than conventional DP-based SemCom. Meanwhile, owing to the lack of correct shared semantic knowledge, the eavesdropper fails to recover meaningful semantic structures, demonstrating the effectiveness of the proposed privacy-preserving framework.

The quantitative reconstruction performance under different privacy budgets is illustrated in Fig. 4.3. As the privacy budget ε increases, less perturbation is injected into the sensitive latent representation, resulting in gradually improved reconstruction quality. This observation verifies the inherent tradeoff between semantic utility and privacy preservation. Compared with the conventional DP SemCom framework, the proposed method consistently achieves higher PSNR and SSIM across the entire privacy budget range. This improvement mainly originates from the semantic compensation provided by the shared knowledge, which effectively mitigates the semantic distortion introduced by DP while preserving communication reliability.

The corresponding privacy protection performance is illustrated in Fig. 4.4.

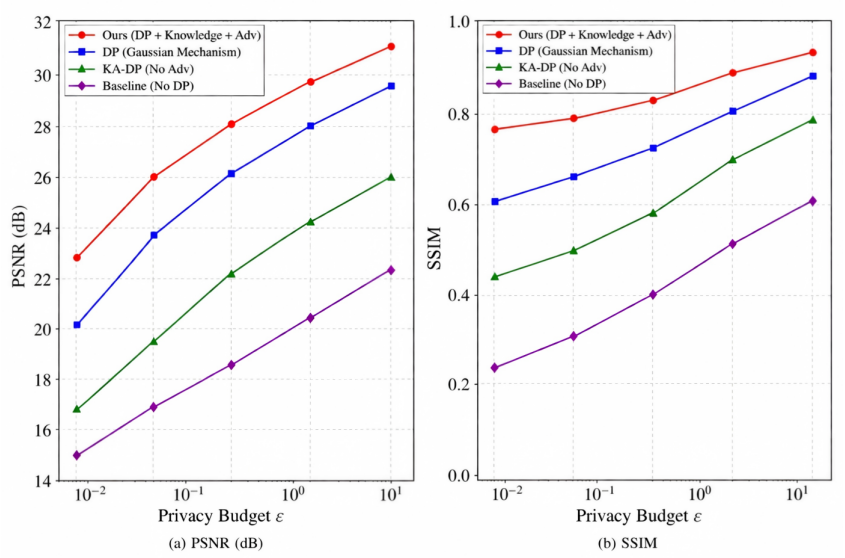

Figure 4.3: Reconstruction performance under different privacy budgets.

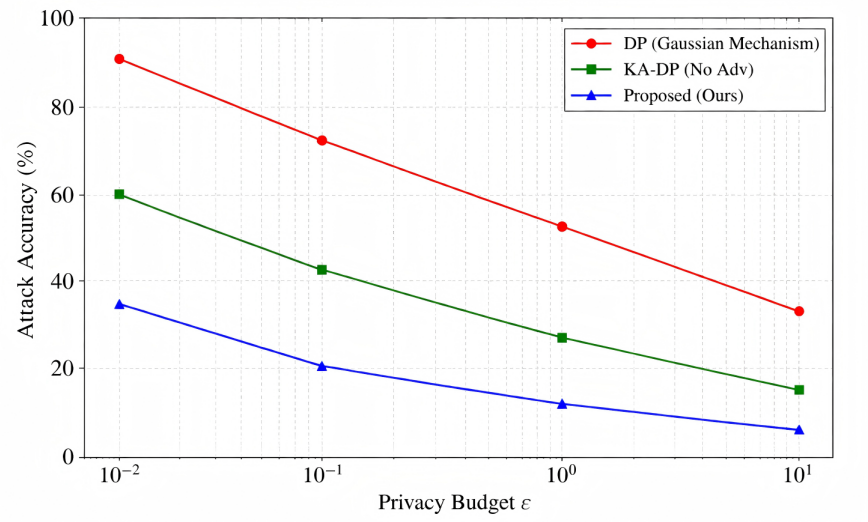

Figure 4.4: Attack accuracy of the adversarial classifier under different privacy budgets.

As expected, decreasing the privacy budget significantly reduces the attack success rate due to stronger perturbation applied to the sensitive latent representation. More importantly, compared with the conventional DP SemCom framework, the proposed adversarial optimisation further suppresses the inference capability of the attacker under all privacy budgets. This result indicates that the encoder gradually learns privacy-invariant semantic representations during adversarial training, making sensitive semantic information increasingly difficult to infer even when part of the latent representation is intercepted.

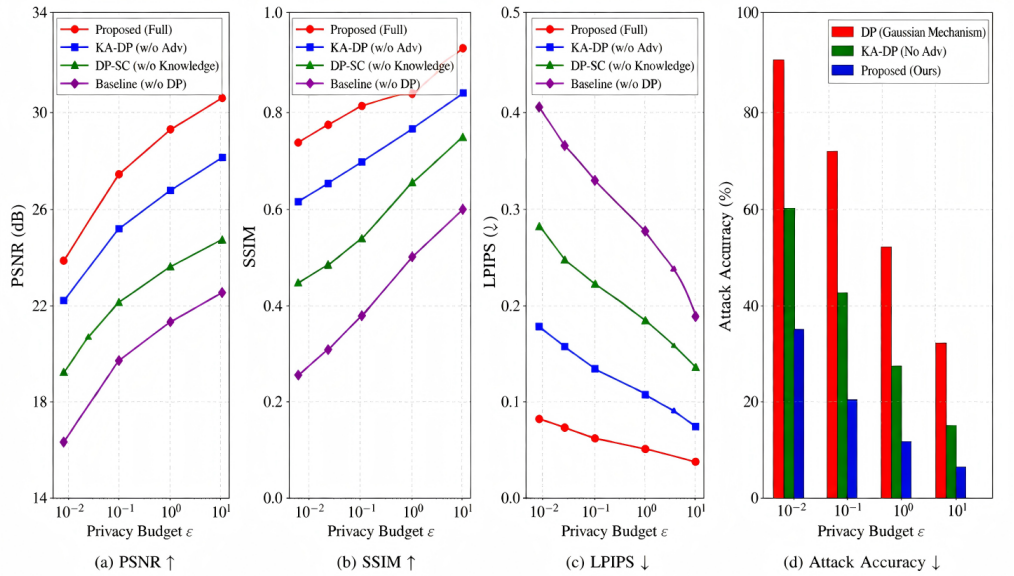

Figure 4.5: Ablation study of the proposed privacy-preserving SemCom framework.

To further verify the contribution of each proposed module, an ablation study is conducted by progressively enabling DP, knowledge-assisted semantic reconstruction, and adversarial optimisation. As shown in Fig. 4.5, introducing DP effectively reduces semantic leakage but inevitably degrades reconstruction performance due to perturbation noise. By incorporating the shared semantic knowledge into the semantic decoder, most reconstruction degradation is successfully compensated without sacrificing privacy protection. Finally, adversarial optimisation further removes privacy-related information from the latent representation while maintaining competitive semantic reconstruction quality. These observations demonstrate that all proposed components contribute positively to the overall framework and jointly improve the privacy–utility tradeoff.

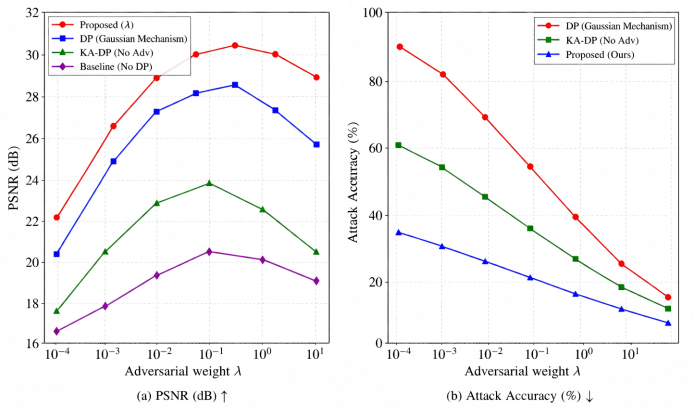

Figure 4.6: Parameter sensitivity analysis with respect to the adversarial loss weight λ.

The influence of the adversarial loss weight λ is further investigated in Fig. 4.6. Increasing λ continuously strengthens the adversarial constraint, leading to lower attack accuracy. However, excessively large values of λ slightly decrease the reconstruction quality because the encoder gradually prioritizes privacy preservation over semantic reconstruction. Consequently, selecting an appropriate adversarial weight is essential for balancing semantic utility and privacy protection.

Table 4.1: Quantitative Performance Comparison of Different SemCom Schemes ($\varepsilon = 1$)

Method	**PSNR (dB)↑**	**SSIM↑**	**LPIPS↓**	**Attack Acc. (%)↓**
Baseline	31.52	0.962	0.045	96.3
DP-SC	27.84	0.913	0.112	35.8
KA-DP	29.67	0.941	0.073	34.1
Proposed	**30.85**	**0.955**	**0.058**	**18.6**

Finally, Table 4.1 summarizes the quantitative performance comparison among different SemCom schemes. The proposed method consistently achieves the highest reconstruction quality under identical privacy constraints while maintaining the lowest attack accuracy. Compared with conventional DP SemCom, the proposed framework significantly improves semantic reconstruction through knowledge-assisted compensation and simultaneously enhances privacy protection via adversarial representation learning.

Overall, the experimental results demonstrate that the proposed knowledge-

assisted privacy-preserving SemCom framework effectively balances semantic utility and privacy preservation. By jointly integrating DP, shared semantic knowledge, and adversarial optimisation, the proposed framework achieves superior reconstruction performance while substantially reducing the risk of sensitive semantic inference, validating both the theoretical analysis and the optimisation strategy developed in the previous sections.

4.6 Conclusion

In this chapter, a knowledge-assisted privacy-preserving SemCom framework has been proposed by jointly integrating differential privacy, shared semantic knowledge, and adversarial representation learning. Differential privacy is selectively applied to the sensitive latent representation to provide rigorous privacy guarantees, while shared semantic knowledge compensates for the semantic distortion introduced by privacy perturbation during semantic reconstruction. Furthermore, a privacy-aware adversarial optimisation strategy is developed to encourage the semantic encoder to learn privacy-invariant latent representations, thereby further suppressing sensitive semantic information leakage.

Future work will investigate adaptive privacy allocation strategies, multimodal SemCom, and large language model empowered semantic knowledge generation to further improve privacy-preserving SemCom in next-generation intelligent wireless networks.

Chapter 5

Joint Knowledge and Power Management for Secure Semantic Communication Networks

5.1 Introduction

The most common manner now to achieve SemCom is device-to-device (D2D) transmission [75], in which the delivery of semantic information is further improved, especially in scenarios with limited bandwidth, network congestion, or device arithmetic constraints [32, 76, 77]. Although D2D SemCom has great potential in improving communication efficiency and task execution, it is also facing new security and privacy challenges in coordination with the requirement of background knowledge matching among multiple SemCom users. In recent studies, a key concept of knowledge base (KB) is introduced in SemCom, which is deemed a small entity containing a specific domain of knowledge that can be cached in advance in local devices or shared during communication [78]. To be more concrete, the base station (BS) is a central knowledge scheduler responsible for distributing KBs to its serving users. However, eavesdroppers equipped with advanced coding models and the same KBs may exist in the cellular area, aiming to eavesdrop private information from D2D SemCom links. Especially if there exist some eavesdroppers adjacent to a D2D SemCom pair, the KBs shared between the two D2D users may be eavesdropped by malicious users and then the transmitted semantics can also be recovered by others, which may cause severe communication security issues. In this case, traditional information security performance

metrics, e.g., secrecy bit throughput or secrecy outage probability [79], are no longer applicable to such a case, since these eavesdroppers concentrate more upon stealing semantic information rather than bit information. Accordingly, there is a pressing demand to explore the protection of semantic information for D2D SemCom underlying cellular networks.

In parallel, it is worth pointing out that different resource management solutions, particularly in knowledge and power allocation, can affect the overall semantic secrecy performance of D2D SemCom networks to a certain degree. For instance, in a scenario with multiple SemCom users (SUs) and eavesdroppers, if each SU is assigned with the suitable KBs matching its paired SU, the semantic information throughput that can be conveyed by the corresponding D2D link is obviously greater than that can be eavesdropped. This is due to the unique knowledge equivalence mechanism in SemCom, where the more the background knowledge of the transceiver matches, the more the semantic recovery rate can be accurate, i.e., more semantic information can be precisely obtained by the receiver. Apart from this, the power control at each SU is paramount of importance, which has been a classical communication security challenge in cellular networks. Generally, given the fixed relative position of two SUs and one eavesdropper, if the distance between two paired SUs is closer than that between the transmitter SU and eavesdropper, the higher the transmit power, the more the bit secrecy throughput, and vice versa. Hence, both the power and KB management can lead to different semantic information secrecy performance of the SemCom network, which becomes rather critical and tricky, especially when jointly considering their optimality.

In fact, there has been some noteworthy related works paving the way for the development of SemCom. Benefit from advanced DL algorithms, the authors in [30] developed efficient deep multiple access in D2D scenarios to improve the performance of image transmission. [80] developed a generative AI-integrated end-to-end SemCom framework in a cloud-edge-mobile design for multimodal AIGC provisioning. In addition, a series of studies related to secure SemCom have also emerged. In [31], the authors proposed a privacy-preserving SemCom framework that leverages knowledge to protect sensitive information. Meanwhile, in [32], the authors pointed out the risk of eavesdropping on knowledge and identify resource allocation schemes in KBs as a viable future research direction. Some other works [79, 81, 82] also surveyed and discussed semantic information security in a comprehensive way, in particular comparing it to classical physical layer security. For the unique requirements of knowledge pairing in D2D SemCom, [83] proposed a reliable and low-latency knowledge matching method to solve the problem of semantic service provisioning among multiple vehicle-to-vehicle SemCom

users. Besides, [84] developed a long-term robust resource allocation strategy to satisfy the trade-off between user satisfaction, queue stability and communication latency for D2D SemCom.

Nevertheless, to the best of our knowledge, none of these papers technically investigate the semantic information security-aware resource management problem for D2D SemCom. In this work, our main task is to seek optimal resource allocation in *secure SemCom network* (SSCN) to reach the best overall semantic network performance. Especially considering the unique knowledge matching demands between multiple SUs and the existence of eavesdroppers, devising the best resource management solution becomes quite indispensable, which can yield many benefits, such as further improving bandwidth utilisation, and ensuring secure, efficient, and high-quality SemCom service provisioning. In view of these unique requirements, there exist three fundamental networking challenges as follows.

- *Challenge 1: How to find an appropriate metric to measure semantic network performance related to secure SemCom?* The longer it takes to allocate knowledge, the more susceptible transmitted information is to eavesdropping. Considering this, scheduling the delay a semantic packet spends in the queue buffer of each D2D SemCom link is of paramount importance. Moreover, traditional system metrics, e.g., bit throughput, is no longer applicable to measure the SSCN. Especially taking into account the presence of eavesdroppers and semantic information importance in SemCom, how to define appropriate secure SemCom-related metrics should be the first challenge.

- *Challenge 2: How to accurately assign KBs to multiple SemCom users with different knowledge preferences?* In SemCom, the KB is the key to perform semantic inference and recovery. Considering that each SemCom user has its own knowledge preference and KB storage capacity, it is quite tricky for each user to realize the best caching policy for size-varying KBs. In particular, potential eavesdroppers pose continuous threats to semantic transmission. If being aware the knowledge distribution at eavesdroppers, how to achieve a secure knowledge base caching (KBC) model should be the second difficulty.

- *Challenge 3: How to determine the best D2D SemCom pairing strategy among all uses to maximize knowledge protection against eavesdropping?* Note that high semantic fidelity can be guaranteed based on equivalent knowledge matching conditions between two SemCom users. In line with different KBC situations, varying channel conditions, and the potential eavesdropping, it poses the third challenge to find the

best D2D user pairing (DUP) for all SemCom users in order to realize the optimal semantic secrecy information delivery.

To address the above gaps that have never been jointly investigated in the current literature, in this chapter, we jointly optimize KBC, DUP, and power allocation in the SSCN with the consideration of unique SemCom characteristics and semantic information security. Both theoretical analysis and numerical results validate the performance superiority of our proposed solution in terms of semantic secrecy throughput, queuing delay, and semantic knowledge satisfaction. In a nutshell, our main contributions are summarized in the following:

- We first identify two core resource management problems of KBC and DUP and construct their mathematical models. Specially, considering the potential eavesdropping center and its knowledge distribution conditions, we develop a novel metric, namely semantic secrecy throughput (SST), to measure the overall semantic information security for all SemCom users.

- By taking into account personal preference for different knowledge bases, we derive the average queuing latency and define the average semantic knowledge satisfaction for each potential D2D SemCom link in a mathematical manner. In this way, a joint SST-maximisation problem is then formulated for power allocation, KBC, and DUP subject to several practical constraints.

- We propose an near-optimal security-aware resource management solution with polynomial-time complexity. Specifically, a Lagrange primal-dual method is first utilized to obtain the dual problem, which is able to be decomposed to multiple subproblems. Without loss of optimality, in each iteration, we leverage a two-stage method to separately solve these subproblems, where the first stage is to determine the KBC and power allocation strategies and the second stage is to finalize the DUP policy.

The remainder of this paper is organized as follows. Section II first introduces the system model of SSCN and formulates a joint security-aware resource optimisation problem. Then, we present our proposed solution and complexity analysis in Section III. Numerical results are demonstrated and discussed in Section IV, followed by the conclusions in Section V.

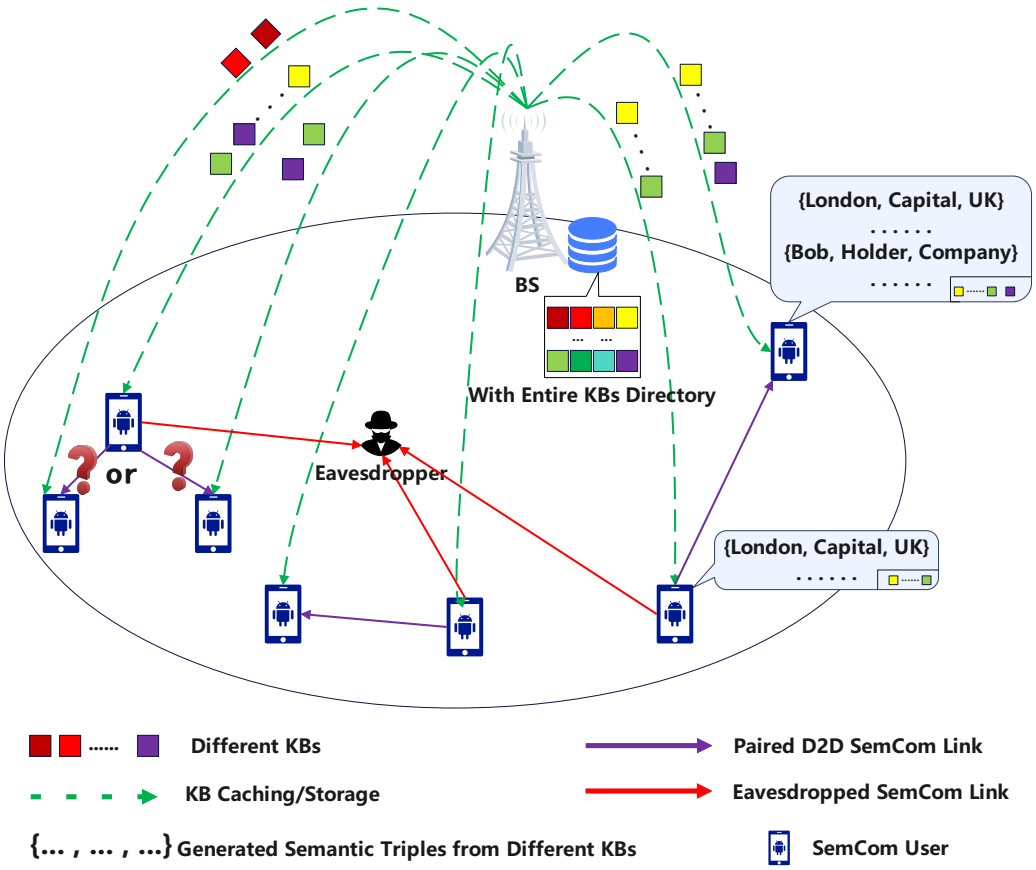

Figure 5.1: The SSCN with KBC, DUP, and PC.

5.2 System Model and Problem Formulation

In this section, the considered SSCN scenario is first elaborated along with the knowledge caching model, secrecy queuing model, and semantic secrecy throughput model. Then, the corresponding optimisation problem is formulated.

5.2.1 SSCN Scenario

Consider a single-cell SSCN scenario as shown in Fig. 5.1, a total of M SUs are distributed within the coverage of one BS, and each SU $i \in \mathcal{M} = \{1, 2, \cdots, M\}$ is capable of providing D2D SemCom services to others. Without loss of generality, each SU is stipulated to be paired with only one (another) SU at a time for D2D SemCom. Herein, let $\beta_{i,j} \in \{0, 1\}$ denote the binary DUP indicator for a potential SU i-SU j ($j \in \mathcal{M}, j \neq i$) pair, where

$\beta_{i,j} = 1$ means SU i is paired with SU j for D2D SemCom, otherwise $\beta_{i,j} = 0$. Besides, each D2D SemCom link has been pre-allocated an orthogonal subchannel with equal channel bandwidth W, and each SU i has a maximum allowable transmit power P_{max} for SemCom. Meanwhile, assume that there exists an eavesdropping center with a fixed spatial location, constantly attempting to eavesdrop on the conveyed semantic information from all D2D SemCom links and using the same subchannel and bandwidth resources as the correspondingly target links. Having these, let $G_{i,j}^{D}$ denote the channel power gain of the D2D link between the transmitter SU i and the receiver SU j, and let G_{i}^{E} denote the channel power gain of the eavesdropping link between the transmitter SU i and the eavesdropping center. Further denoting the transmit power of SU i as P_i, the signal-to-noise ratio (SNR) experienced by the D2D link is $\gamma_{i,j}^{D} = P_i G_{i,j}^{D}/\zeta^2$, where ζ^2 is the noise power. Likewise, the SNR of the eavesdropping link regarding SU i is $\gamma_{i}^{E} = P_i G_{i}^{E}/\zeta^2$. Hence, the bit rates at the D2D link and the eavesdropping link should be $r_{i,j}^{D} = W \log_2\left(1 + \gamma_{i,j}^{D}\right)$ and $r_{i}^{E} = W \log_2\left(1 + \gamma_{i}^{E}\right)$, respectively.

Note that we allow SU i to provide D2D SemCom services to SU j only if the SNR $\gamma_{i,j}$ is above a specified threshold γ_0, hence the set of eligible communication neighbors of SU i is defined as $\mathcal{M}_i = \{j \mid j \in \mathcal{M}, j \neq i, \gamma_{i,j} \geqslant \gamma_0\}$. Moreover, let the BS act as a semantic service controller to efficient schedule and coordinate the whole secure D2D SemCom process based on the request and state information received from all participating SUs within its coverage.

5.2.2 Knowledge Base Caching Model

The acquisition of necessary background knowledge is known to be inevitable for accurate semantic inference and interpretation in SemCom. Note that each KB contains the background knowledge of only one particular application domain (e.g., music or sports), and thus different KBs are associated with different background knowledge, and holding some common KBs becomes the necessary condition to perform SemCom between two D2D SUs in accordance with the knowledge equivalence principle.[1] Especially considering the existence of the eavesdropping center, different knowledge base caching (KBC) schemes can significantly affect the overlapping degree of background knowledge between different nodes, since the transmitted semantic information can only be decoded under the equivalent background knowledge. In

[1]The structure of a KB can roughly cover multiple computational ontologies, facts, rules and constraints associated to a specific domain [85]. In recent deep learning-driven semantic coding models, the KB is also treated as a training database serving a certain class of learning tasks [86].

this work, suppose that there is a KB library $\mathcal{K}$ with a total of K differing KBs in the considered SSCN, and each KB $k \in \mathcal{K} = \{1, 2, \ldots, K\}$ is corresponding to a specific type of SemCom service. On this basis, all SUs should proactively download and cache their respective interested KBs from the BS to achieve D2D SemCom based on the desired semantic services. Note that each requires a unique storage size s_k, and each SU $i \in \mathcal{M}$ has a finite capacity C_i for its local KB storage. In this way, we define a binary KBC indicator as

$$\alpha_i^k = \begin{cases} 1, & \text{if KB } k \text{ is cached on SU } i; \\ 0, & \text{otherwise.} \end{cases} \tag{5.1}$$

It is worth mentioning that the same KB cannot be cached repeatedly at one SU for reducing redundancy and for promoting the storage efficiency.

Besides, it is noticed that different SUs may have different personal preferences for these KBs, thus resulting in the diversity of KB popularity. Naturally, the more popular the KBs, the higher the KBC probabilities. Herein, we assume that the KB popularity at each SU follows the Zipf distribution [87,88].[2] Hence, the probability of SU i requesting its desired KB k-based SemCom services (generating the corresponding semantic data packets) is $p_i^k = \left(r_i^k\right)^{-\xi_i} / \sum_{e \in \mathcal{K}} e^{-\xi_i}, \forall (i,k) \in \mathcal{M} \times \mathcal{K}$, where ξ_i ($\xi_i \geqslant 0$) is the skewness of the Zipf distribution, and r_i^k is the popularity rank of KB k at SU i.[3] Such a modeling is supported by empirical evidence from real-world D2D content request patterns, which often exhibit Zipf-like long-tailed distributions, as observed in measured datasets from video platforms such as BBC iPlayer and YouView [91]. Based on p_i^k, we specially define a KBC-related metric η_i, namely *semantic knowledge satisfaction*, to measure the satisfaction degree of SU i caching its interested KBs, given as $\eta_i = \sum_{k \in \mathcal{K}} \alpha_i^k p_i^k$. It is further noticed that $\eta_i \geqslant \eta_0$, where η_0 is the unified minimum threshold that needs to be achieved at each SU.

As for the eavesdropping center, let us assume it has its own KB preference for illegal eavesdropping and decoding of their interested semantic information from these D2D SemCom links. Without loss of the generality, let r_E^k and ξ_E ($\xi_E \geqslant 0$) denote the popularity rank of KB k at the eavesdropping center and the skewness of its Zipf distribution, respectively. As such, the probability of KB k being held by the eavesdropping center can be expressed by $p_E^k = \left(r_E^k\right)^{-\xi_E} / \sum_{e \in \mathcal{K}} e^{-\xi_E}, \forall k \in \mathcal{K}$. In other words, if denoting α_E^k as the KBC indicator of the eavesdropping center, where $\alpha_E^k = 1$ indicates

[2]Note that other known probability distributions can also be adopted for KB popularity without changing the remaining modeling and solution.

[3]The KB popularity ranking of each SU can be analyzed and estimated based on its historical messaging records [83, 89, 90], which will not be discussed in this chapter.

that KB k is cached and $\alpha_E^k = 0$ otherwise, we have $\Pr\left\{\alpha_E^k = 1\right\} = p_E^k$ and $\Pr\left\{\alpha_E^k = 0\right\} = 1 - p_E^k$.

5.2.3 Secrecy Delay Model

In secure communications, the longer the delay incurred in the communication process, the more likely it is that the transmitted information will be eavesdropped on [92]. Being aware of this, the knowledge matching based semantic packet queuing delay is jointly considered as a long-term metric in this work, which is to characterize the average sojourn time of semantic data packets in the receiver SU's queue buffer (following the first-come first-serve rule). This is mainly considered from the large-timescale perspective, as we only focus on the queuing latency under the steady-state of the semantic packet queuing system. Note that each semantic data packet is associated with a specific service type, i.e., a certain KB, while we assume that semantic data packets generated based on different KBs can co-exist in the queue and have independent average arrival rate and interpretation time. Besides, not all semantic data packets arriving at the receiver SU are always allowed to enter its queue, as some of them may mismatch the KBs currently held, rendering these packets uninterpretable [83]. As for these mismatched packets, we can choose the traditional bit transmission, where the additional delay introduced can be easily covered by applying SemCom due to the considerably saved bits and communication delay.

To preserve generality, we first suppose a Markovian arrival process with average rate $\lambda_{i,j}^k = \lambda_{i,j}^D p_i^k$ for the D2D SemCom link between transmitter SU i and receiver SU j to account for semantic packet generation based on KB k, where $\lambda_{i,j}^D$ is the total arrival rate of all semantic packets from transmitter SU i to receiver SU j. Herein, if assuming that each semantic packet has an average size of L bits, given its achievable bit rate $r_{i,j}^D$ with variable P_i, we can approximately calculate $\lambda_{i,j}^D$ by $\lambda_{i,j}^D = r_{i,j}^D / L$. Combined with the KBC situation at SU i and SU j, the effective arrival rate of semantic packets (i.e., semantic packets based on matched KB between them) in the queue is given as $\lambda_{i,j}^{eff} = \sum_{k \in \mathcal{K}} \alpha_i^k \alpha_j^k \lambda_{i,j}^k$. In parallel, let a random variable I_j^k denote the Markovian interpretation time [93] required by KB k-based packets at SU j with mean $1/\mu_j^k$, which is determined by the computing capability of the SU and the type of the desired KB. However, since multiple packets based on different KBs are allowed to queue at the same time, it is seen that the interpretation time distribution for a receiver SU should be treated as a general distribution [94]. If further taking into account the KB popularity, we can calculate the ratio of the amount of KB k-based packets to the total packets in the SU i-SU j pair's queue by $\epsilon_{i,j}^k = p_i^k / \sum_{f \in \mathcal{K}} \alpha_i^f \alpha_j^f p_i^f$. With the indepen-

dence among packets based on different KBs, the interpretation time required by each packet in the queue is now expressed as $W_{i,j} = \sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \epsilon_{i,j}^k I_j^k$.

Since the Markovian arrival process leads to the correlated packet arrivals while the service pattern of packets obeys a general distribution, the queue of each D2D pair in the SSCN can be modeled as an M/G/1 system, which has been widely used to model data traffic in wireless networks. According to the *Pollaczek-Khintchine formula* [95], the average queuing latency for the SU i-SU j pair, denoted as $\delta_{i,j}$, is determined as follows[4]

$$\delta_{i,j} = \frac{\lambda_{i,j}^{eff} \cdot \left(\mathbb{E}^2\left[W_{i,j}\right] + Var\left(W_{i,j}\right)\right)}{2\left(1 - \lambda_{i,j}^{eff} \cdot \mathbb{E}\left[W_{i,j}\right]\right)}. \tag{5.2}$$

To calculate the close form of $\delta_{i,j}$, again leveraging the independence of I_j^k over k, we can obtain the expectation of the interpretation time for all semantic data packets by

$$\mathbb{E}\left[W_{i,j}\right] = \sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \epsilon_{i,j}^k \mathbb{E}\left[I_j^k\right] = \sum_{k\in\mathcal{K}} \frac{\alpha_i^k \alpha_j^k \epsilon_{i,j}^k}{\mu_j^k}, \tag{5.3}$$

and the variance of $W_{i,j}$ can be calculated by

$$\begin{aligned} Var\left(W_{i,j}\right) &= \sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \left(\epsilon_{i,j}^k\right)^2 Var\left[I_j^k\right] \\ &= \sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \left(\frac{\epsilon_{i,j}^k}{\mu_j^k}\right)^2. \end{aligned} \tag{5.4}$$

By substituting (5.3) and (5.4) into (5.2), $\delta_{i,j}$ can be rewritten in (5.5), as shown at the bottom of the next page. Due to the security consideration, let δ_0 denote a unified secrecy latency threshold that should be satisfied at all associated D2D SemCom links.

5.2.4 Semantic Secrecy Throughput Measurement

Lately, a concept of *semantic triplet* is dedicatedly introduced in the realm of SemCom to represent the interpretable relationship between two specific semantic entities implied in source information [96–98], and its typical expression is *(Entity-A, Relationship, Entity-B)*, as depicted in the exemplification

[4]In order to guarantee the steady-state of the queuing system, a condition of $\lambda_{i,j}^{eff}\mathbb{E}\left[W_{i,j}\right] < 1$ must be satisfied before proceeding [94]. In this work, we assume that the packet interpretation rate is larger than the packet arrival rate to make the queuing latency finite and thus solvable.

of Fig. 5.1. In the context of the above secrecy queuing latency model, we assume that each semantic data packet contains exactly one semantic triple, which is corresponding to a certain KB. To be more specific, all source information of transmitters in SemCom is first encoded in the minimum unit of semantic triplets by semantic encoding models.[5] Afterward, each semantic triplet is encoded by each SU's channel encoder and then encapsulated into an L bits-size semantic data packet for wireless transmission [98]. As such, we clearly have the total number of semantic triplets transmitted from transmitter SU i to receiver SU j per second given by $\lambda_{i,j}^{D}$, as aforementioned, and likewise, obtain that for the eavesdropping link as $\lambda_{i}^{E} = r_{i}^{E}/L$.

Since each KB has its popularity rank at each SU as identified in the KBC model, it means that each semantic triplet also has the same preference level. Naturally, transmitting the higher-ranked semantic triplets contributes more valuable semantic information for each SemCom receiver. Inspired by this, we employ a performance metric called *semantic value* proposed in [98] to measure the semantic information importance of semantic triplets with different rankings at each SU. Proceeding as in [98], the calculation of semantic value for each KB k-based semantic triplet relies on SU i's Zipf distribution, which is exactly the numerator of p_i^k, given by $\left(r_i^k\right)^{-\xi_i}$. Note that the semantic value above is measured according to the transmitter's KB preference only, which is reasonable as the primary purpose of SemCom is generally determined by the sender, rather than the receiver. With these and further combining the effective semantic packet arrival of KB k from SU i to SU j given in $\lambda_{i,j}^{eff}$, i.e., $\alpha_i^k \alpha_j^k \lambda_{i,j}^k$, we can obtain the effective semantic value

[5]This assumption is justified since core semantic information can be extracted by state-of-the-art DL models from multimedia services (e.g., text [9], image [99], and video [100]) to draw the semantic KG, which can be decomposed into multiple semantic triplets [101,102]. In other words, it is reasonable that source information in any format can be conveyed in units of semantic triplets for SemCom service provisioning.

$$\delta_{i,j} = \frac{\left[\left(\sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \frac{p_i^k/\mu_j^k}{\sum_{f\in\mathcal{K}} \alpha_i^f \alpha_j^f p_i^f}\right)^2 + \sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \left(\frac{p_i^k/\mu_j^k}{\sum_{f\in\mathcal{K}} \alpha_i^f \alpha_j^f p_i^f}\right)^2\right] \cdot \left(\sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \lambda_{i,j}^k\right)}{2\left[1 - \left(\sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \lambda_{i,j}^k\right) \cdot \left(\sum_{k\in\mathcal{K}} \alpha_i^k \alpha_j^k \frac{p_i^k/\mu_j^k}{\sum_{f\in\mathcal{K}} \alpha_i^f \alpha_j^f p_i^f}\right)\right]} \tag{5.5}$$

transmitted via the SU i-SU j D2D pair per second as

$$V_{i,j}^{D} = \sum_{k \in \mathcal{K}} \alpha_i^k \alpha_j^k \lambda_{i,j}^k \left(r_i^k\right)^{-\xi_i} = \frac{r_{i,j}^{D}}{L} \sum_{k \in \mathcal{K}} \alpha_i^k \alpha_j^k p_i^k \left(r_i^k\right)^{-\xi_i}. \tag{5.6}$$

Similarly, based on the semantic triplet transmission rate λ_i^E and the KBC situation α_E^k pertinent to the eavesdropping center, the average number of KB k-based semantic triplets that can be eavesdropped per second should be

$$\begin{aligned} V_i^E &= \sum_{k \in \mathcal{K}} \lambda_i^E \alpha_i^k p_i^k \Pr\left\{\alpha_E^k = 1\right\} \left(r_i^k\right)^{-\xi_i} \\ &= \frac{r_i^E}{L} \sum_{k \in \mathcal{K}} \alpha_i^k p_i^k p_E^k \left(r_i^k\right)^{-\xi_i}. \end{aligned} \tag{5.7}$$

Therefore, drawing on the classical metric of secrecy throughput in traditional secure communications [79, 103, 104], we define here a new metric, namely *semantic secrecy throughput* (SST), by subtracting V_i^E in (5.7) from $V_{i,j}^D$ in (5.6) as

$$\begin{aligned} V_{i,j}^{S} &= \left[V_{i,j}^{D} - V_i^E\right]^+ \\ &= \frac{1}{L} \left[\sum_{k \in \mathcal{K}} \alpha_i^k \left(r_i^k\right)^{-\xi_i} \left(r_{i,j}^{D} \alpha_j^k p_i^k - r_i^E p_i^k p_E^k\right)\right]^+, \end{aligned} \tag{5.8}$$

where the operator $[\cdot]^+$ is to output the maximum value between its argument and zero. To provide an intuitive explanation, $V_{i,j}^S$ is the secure semantic value transmission rate at which the legitimate SU i-SU j pair is able to communicate safely without enough valuable semantic information being stolen by the eavesdropping center. If $V_{i,j}^D > V_i^E$, the D2D SemCom users can transmit semantic information to each other with a secure rate of $(V_{i,j}^D - V_i^E)$. Otherwise, any transmitted semantics at the SU i-SU j pair will be stolen by the eavesdroppers. If taking into account all DUP possibilities, the overall SST of SSCN should be the sum of $\beta_{i,j} V_{i,j}^S$ corresponding to all potential SU i-SU j cases, that is,

$$\begin{aligned} SST &= \sum_{i \in \mathcal{M}} \sum_{j \in \mathcal{M}_i} \beta_{i,j} V_{i,j}^S \\ &= \sum_{i \in \mathcal{M}} \sum_{j \in \mathcal{M}_i} \frac{\beta_{i,j}}{L} \left[\sum_{k \in \mathcal{K}} \alpha_i^k \left(r_i^k\right)^{-\xi_i} \left(r_{i,j}^{D} \alpha_j^k p_i^k - r_i^E p_i^k p_E^k\right)\right]^+. \end{aligned} \tag{5.9}$$

5.2.5 Problem Formulation

For ease of illustration, we first define three variable sets $\boldsymbol{\alpha} = \left\{\alpha_i^k \mid i \in \mathcal{M}, k \in \mathcal{K}\right\}$, $\boldsymbol{\beta} = \{\beta_{i,j} \mid i \in \mathcal{M}, j \in \mathcal{M}_i\}$, and $\boldsymbol{P} = \{P_i \mid i \in \mathcal{M}\}$ that consist of all possible indicators pertinent to KBC, DUP, and PC, respectively. Without loss of generality, the objective of our optimisation is to maximize SST in (5.9) by jointly optimizing $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$, while subject to SemCom-relevant latency and performance requirements alongside several practical system constraints. The problem is specifically formulated as follows:

$$\mathbf{P0}: \max_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P}} \quad \sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{M}_i} \beta_{i,j} V_{i,j}^S \tag{5.10}$$

$$\text{s.t.} \quad \sum_{k\in\mathcal{K}} \alpha_i^k \cdot s_k \leqslant C_i,\ \forall i \in \mathcal{M}, \tag{5.10a}$$

$$\eta_i \geqslant \eta_0,\ \forall i \in \mathcal{M}, \tag{5.10b}$$

$$\sum_{j\in\mathcal{M}_i} \beta_{i,j} = 1,\ \forall i \in \mathcal{M}, \tag{5.10c}$$

$$\beta_{i,j} = \beta_{j,i},\ \forall (i,j) \in \mathcal{M} \times \mathcal{M}_i, \tag{5.10d}$$

$$\sum_{j\in\mathcal{M}_i} \beta_{i,j}\delta_{i,j} \leqslant \delta_0,\ \forall i \in \mathcal{M}, \tag{5.10e}$$

$$\sum_{j\in\mathcal{M}_i} \beta_{i,j} V_{i,j}^S \geqslant V_0,\ \forall i \in \mathcal{M}, \tag{5.10f}$$

$$\alpha_i^k \in \{0,1\},\ \forall (i,k) \in \mathcal{M} \times \mathcal{K}, \tag{5.10g}$$

$$\beta_{i,j} \in \{0,1\},\ \forall (i,j) \in \mathcal{M} \times \mathcal{M}_i \tag{5.10h}$$

$$0 \leqslant P_i \leqslant P_{max},\ \forall i \in \mathcal{M}. \tag{5.10i}$$

Constraints (5.10a) guarantees that the total size of KBs cached at each SU cannot exceed its maximum storage capacity, while constraint (5.10b) represents the aforementioned semantic knowledge satisfaction requirement. Then, constraints (5.10c) and (5.10d) jointly model the single-D2D pairing limitation of SUs. Next, constraint (5.10e) indicates the maximum secrecy queuing latency threshold, while constraint (5.10f) is the minimum SST requirement at each D2D SemCom link indicating the reliability level of the system. Moreover, constraints (5.10g) and (5.10h) characterize the binary properties of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Finally, constraint (5.10i) determines the transmit power range for all SUs.

Carefully examining **P0**, it can be observed that the optimisation is quite challenging to be solved straightforwardly due to several intractable mathematical obstacles. First of all, **P0** is an NP-hard optimisation problem

as demonstrated below. Consider a special case of **P0** where all $\boldsymbol{\beta}$- and $\boldsymbol{P}$-related constraints have been satisfied. In this case, constraints (5.10c)-(5.10d) and (5.10h)-(5.10i) can all be removed, and the primal problem degenerates into a variant 0-1 multi-knapsack problem that is known to be NP-hard [105], thereby **P0** is also NP-hard. Besides, **P0** involves both continuous and discrete variables, and its objective function (5.10) is quite complicated alongside constraints (5.10e) and (5.10f), which prevents us from using the conventional two-step solution (i.e., relaxation and recovery) to approach optimality. In more detail, the problem after relaxing $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ should still be a nonconvex optimisation problem owing to the non-convexity preserved in (5.10) and constraints (5.10e) and (5.10f). Therefore, a severe performance penalty and a high computational complexity will be incurred from the procedure of integer recovery due to the huge performance compromise on solving the nonconvex problem for relaxed variables [106–108]. In view of the above mathematical challenges, we propose an efficient resource allocation strategy in the next section to reach the optimality of **P0** and obtain the joint KBC, DUP, and PC solution.

5.3 Security-Aware Resource Allocation for SSCN

In this section, we illustrate how to achieve the optimal security-aware resource management in the SSCN. We first employ the Lagrange dual method to transform the primal problem **P0** to its dual optimisation problem. Then, given dual variables in each iteration, the dual problem is decomposed into multiple subproblems, which are solved by the proposed two-stage method. Finally, the workflow of our solution and its complexity analysis are provided.

5.3.1 Primal-Dual Problem Transformation

To make **P0** tractable, we first incorporate constraints (5.10e) and (5.10f) into the objective function (5.10) by associating two Lagrange multipliers $\boldsymbol{\tau} = \{\tau_i \mid i \in \mathcal{M}\}$ and $\boldsymbol{\rho} = \{\rho_i \mid i \in \mathcal{M}\}$. As such, its Lagrange function is found by (5.11), as shown at the bottom of the next page, in which $\widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$ is defined for expression brevity. Then, the Lagrange dual problem of **P0** becomes

$$\mathbf{D0}: \min_{\boldsymbol{\tau},\boldsymbol{\rho}} \quad D(\boldsymbol{\tau}, \boldsymbol{\rho}) = g_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P}}(\boldsymbol{\tau}, \boldsymbol{\rho}) + \delta_0 \sum_{i \in \mathcal{M}} \tau_i - V_0 \sum_{i \in \mathcal{M}} \rho_i \tag{5.12}$$

$$\text{s.t.} \quad \tau_i \geqslant 0, \ \rho_i \geqslant 0, \ \forall i \in \mathcal{M}, \tag{5.12a}$$

where

$$\begin{aligned} g_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P}}\left(\boldsymbol{\tau},\boldsymbol{\rho}\right) &= \sup_{\boldsymbol{\alpha},\boldsymbol{\beta}} \widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}\left(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P}\right) \\ &\quad \text{s.t.} \quad (5.10\text{a}) - (5.10\text{d}), (5.10\text{g}) - (5.10\text{i}). \end{aligned} \tag{5.13}$$

Notably, the optimality of the convex problem **D0** gives at least the best upper bound of **P0**, even if **P0** is nonconvex, according to the duality property [109]. Hence, our focus now naturally shifts to seeking the optimal solution to **D0**.

Given the initial dual variable $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$, we can solve problem (5.13) in the first place to find the optimal solution of $(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P})$, the details of which will be presented in the subsequent subsections. After that, a subgradient method is employed for updating $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$ to solve **D0** in an iterative fashion. Particularly, the partial derivatives with respect to (w.r.t.) $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$ in $D\left(\boldsymbol{\tau},\boldsymbol{\rho}\right)$ are set as the subgradient directions, respectively. Suppose in a certain iteration, say iteration t, each dual variable $\tau_i(t)$ $(i \in \mathcal{M})$ is updated by

$$\tau_i(t+1) = \left[\tau_i(t) - \nu_1(t) \cdot \left(\delta_0 - \sum_{j\in\mathcal{M}_i} \beta_{i,j}(t)\delta_{i,j}(t)\right)\right]^+, \tag{5.14}$$

and each $\rho_i(t)$ is updated by

$$\rho_i(t+1) = \left[\rho_i(t) + \nu_2(t) \cdot \left(V_0 - \sum_{j\in\mathcal{M}_i} \beta_{i,j}(t)V_{i,j}^S(t)\right)\right]^+. \tag{5.15}$$

$\nu_1(t)$ and $\nu_2(t)$ are the stepsizes w.r.t. the update of $\tau_i(t)$ and $\rho_i(t)$ in iteration t, respectively. Generally, the convergence of the subgradient descent method can be ensured with the proper stepsize preset in practice [110].

$$\begin{aligned} L\left(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P},\boldsymbol{\tau},\boldsymbol{\rho}\right) &= \sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{M}_i} \beta_{i,j}V_{i,j}^S + \sum_{i\in\mathcal{M}} \tau_i \left(\delta_0 - \sum_{j\in\mathcal{M}_i} \beta_{i,j}\delta_{i,j}\right) \\ &\quad + \sum_{i\in\mathcal{M}} \rho_i \left(\sum_{j\in\mathcal{M}_i} \beta_{i,j}V_{i,j}^S - V_0\right) \\ &= \sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{M}_i} \beta_{i,j}\left[\left(1+\rho_i\right)V_{i,j}^S - \tau_i\delta_{i,j}\right] + \delta_0\sum_{i\in\mathcal{M}}\tau_i - V_0\sum_{i\in\mathcal{M}}\rho_i \\ &\triangleq \widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}\left(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P}\right) + \delta_0\sum_{i\in\mathcal{M}}\tau_i - V_0\sum_{i\in\mathcal{M}}\rho_i. \end{aligned} \tag{5.11}$$

5.3.2 Dual Problem Decomposition for Optimality Guarantee

As discussed earlier, given $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$ in each iteration, the optimal $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$ need to be obtained by solving problem (5.13). However, solving such a problem is still challenging due to the inseparability of these variables $\widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$. To this end, we propose a two-stage method to reach its optimality with a low computational complexity.

In the first stage, we focus on multiple independent KB caching subproblems, each corresponding to a potential D2D SU pair in the SSCN. Specifically, the performances of an SU i-SU j single pair (i.e., the sender SU i and the receiver SU j) and an SU j-SU i pair (i.e., the sender SU j and the receiver SU i) should be jointly considered, and for ease of distinction, we refer to the two case as the same *SU* i, j *pair*, $\forall (i,j) \in \mathcal{M} \times \mathcal{M}_i, j > i$. In other words, for each KBC subproblem, we have $\beta_{i,j} = \beta_{j,i} = 1$ in $\widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$ corresponding to a given SU i, j pair, while all other SU pairs are not taken into account. Therefore, different KBC subproblems can be tackled independently, and in this way, let

$$\omega_{i,j} = \left[(1+\rho_i) V_{i,j}^S - \tau_i \delta_{i,j}\right] + \left[(1+\rho_j) V_{j,i}^S - \tau_j \delta_{j,i}\right]. \tag{5.16}$$

Clearly, we have $\omega_{i,j} = \omega_{j,i}$, thus only the case of $j > i$ needs to be considered for each potential SU i, j pair, and constraints (5.10c), (5.10d), and (5.10h) are satisfied at the same time.

Clearly, we have $U = \left(\sum_{i \in \mathcal{M}} |\mathcal{M}_i|\right)/2$ subproblems in total, each of which is denoted as $\mathbf{P1}_{i,j}$, $\forall (i,j) \in \mathcal{M} \times \mathcal{M}_i, j > i$, to seek the optimal KBC sub-policy only for an individual SU i, j pair. Note that the optimal KBC solution to problem (5.13) cannot be achieved by simply combining the obtained sub-policies of these $\mathbf{P1}_{i,j}$, but these sub-policies will be used to construct the subsequent DUP and power allocation subproblems to finalize the joint optimal solution of $(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{P})$ for (5.13). Given the dual variable $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$ in

each iteration, $\mathbf{P1}_{i,j}$ becomes

$$\mathbf{P1}_{i,j}: \max_{\{\alpha_i^k\},\{\alpha_j^k\},P_i,P_j} \quad \omega_{i,j} \tag{5.17}$$

$$\text{s.t.} \quad \sum_{k\in\mathcal{K}} \alpha_i^k \cdot s_k \leqslant C_i, \tag{5.17a}$$

$$\sum_{k\in\mathcal{K}} \alpha_j^k \cdot s_k \leqslant C_j, \tag{5.17b}$$

$$\eta_i \geqslant \eta_0,\ \eta_j \geqslant \eta_0, \tag{5.17c}$$

$$\alpha_i^k \in \{0,1\}, \alpha_j^k \in \{0,1\}, \forall k \in \mathcal{K}, \tag{5.17d}$$

$$0 \leqslant P_i \leqslant P_{max},\ 0 \leqslant P_j \leqslant P_{max}. \tag{5.17e}$$

If we can obtain the optimal KBC and power allocation sub-policies by solving $\mathbf{P1}_{i,j}$ for SU i (denoted as $\boldsymbol{\alpha}^*_{i_{(j)}}$ and $P^*_{i_{(j)}}$) and SU j (denoted as $\boldsymbol{\alpha}^*_{j_{(i)}}$ and $P^*_{j_{(i)}}$),[6] corresponding to the individual SU i,j pair. The following proposition explicitly shows how $\mathbf{P1}_{i,j}$ correlates to the problem (5.13).

Based on Proposition 1, it is seen that the optimal KBC and power allocation policies of each SU can be obtained by solving a certain $\mathbf{P1}_{i,j}$. Moreover, due to the single-association requirement of D2D SemCom pairing, the optimal DUP strategy becomes the only key to finalize the optimal solution to (5.13). Hence, we first construct the optimal coefficient matrix for $\boldsymbol{\beta}$ in (5.13) to account for all DUP possibilities. By calculating the optimal $\omega_{i,j}$ (denoted as $\omega^*_{i,j}, \forall (i,j) \in \mathcal{M} \times \mathcal{M}_i$) in $\mathbf{P1}_{i,j}$, the optimal coefficient matrix is given by

$$\boldsymbol{\Omega} = \begin{bmatrix} +\infty & \omega^*_{1,2} & \omega^*_{1,3} & \cdots & \omega^*_{1,M} \\ \omega^*_{2,1} & +\infty & \omega^*_{2,3} & \cdots & \omega^*_{2,M} \\ \omega^*_{3,1} & \omega^*_{3,2} & +\infty & \cdots & \omega^*_{3,M} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^*_{M,1} & \omega^*_{M,2} & \omega^*_{M,3} & \cdots & +\infty \end{bmatrix}. \tag{5.18}$$

$\boldsymbol{\Omega}$ is an $M \times M$ symmetric matrix in which $\omega^*_{i,j} = \omega^*_{j,i}$, and all elements on its main diagonal are set to $+\infty$ to indicate $i \neq j$. In addition, some $\omega^*_{i,j}$s in $\boldsymbol{\Omega}$ may have a value of $+\infty$ when SU j is not the eligible neighbor of SU i, i.e., $j \notin \mathcal{M}_i$.

On this basis, we will focus on finding the optimal DUP strategy by constructing a related subproblem in the second stage. With the objective $\widetilde{L}_{\boldsymbol{\tau},\boldsymbol{\rho}}(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{P})$ and $\boldsymbol{\beta}$-related constraints in (5.13), the DUP subproblem is

[6]For auxiliary illustration, we use $(\cdot)$ in the subscript to specify the SU pair attribute (relation) for each SU's KBC and power allocation sub-policies obtained from $\mathbf{P1}_{i,j}$.

constructed as

$$\mathbf{P2}: \max_{\boldsymbol{\beta}} \quad \frac{1}{2}\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{M}_i}\beta_{i,j}\omega^*_{i,j} \tag{5.19}$$

$$\text{s.t.} \quad (5.10\text{c}), (5.10\text{d}), (5.10\text{h}). \tag{5.19a}$$

Given any $\boldsymbol{\tau}$ and $\boldsymbol{\rho}$, the optimal DUP strategy $\boldsymbol{\beta}$ (denoted as $\boldsymbol{\beta}^*$ $= \left[\beta_{1,j_1^*}, \beta_{2,j_2^*}, \cdots, \beta_{M,j_M^*}\right]^T$) can be straightforwardly finalized by solving **P2**, where β_{i,j_i^*} $(\forall i \in \mathcal{M})$ means that SU j_i^* is the optimal D2D SemCom node for SU i, i.e., $\beta_{i,j_i^*} = 1$. Then, we feed the obtained $\boldsymbol{\beta}^*$ back to $\boldsymbol{\Omega}$ to further determine the optimal KBC and power allocation policies $\boldsymbol{\alpha}^*$ and $\boldsymbol{P}^*$ for all SUs. In other words, for any $i \in \mathcal{M}$, we have $\boldsymbol{\alpha}_i^* = \boldsymbol{\alpha}^*_{i_{(j_i^*)}}$ and $P_i^* = P^*_{i_{(j_i^*)}}$, which is established by giving the following proposition.

It is worth emphasizing that although the primal problem **P0** is NP-hard, the proposed primal–dual decomposition ensures that the solution obtained in each iteration reaches the optimal point within the convex relaxation domain. Since the dual problem **D0** provides a tight upper bound on **P2** the final solution can be regarded as a near-optimal one approaching the duality bound. Therefore, the optimality gap between the obtained solution and the true global optimum remains theoretically bounded and negligible in practice, as further supported by the fast convergence behavior observed in our numerical evaluations. Based on Proposition 2, we have proved that the proposed two-stage method is guaranteed to reach the optimality of problem (5.13) in each iteration. Most importantly, the optimisation to either $\mathbf{P1}_{i,j}$ or **P2** becomes quite tractable owing to the significantly reduced number of variables. In the next two subsections, we will elucidate our optimal solutions to $\mathbf{P1}_{i,j}$ and **P2**, respectively.

5.3.3 Near-Optimal KBC and Power Allocation for A D2D Pair

Carefully examining $\mathbf{P1}_{i,j}$, it is seen that the two binary variables $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ are the main tricky points during the solving process. Suppose that we fix $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ to any feasible solutions in the first place, only constraint (5.17e) remains and then we just need to concentrate upon its objective function $\omega_{i,j}$ w.r.t. variable P_i and P_j. Note that $\delta_{i,j}$ and $\delta_{j,i}$ in $\omega_{i,j}$ are monotonically increasing functions on P_i and P_j, respectively, which fact is quite obvious by observing (5.5). Moreover, when $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ are fixed to be known, $V_{i,j}^S$

can be rephrased to a more precise form, that is

$$V_{i,j}^{S} = \left[\theta_{i,j}^{D}\log_2\left(1+\frac{P_i G_{i,j}^{D}}{\delta^2}\right) - \theta_{i}^{E}\log_2\left(1+\frac{P_i G_{i}^{E}}{\delta^2}\right)\right]^{+}, \tag{5.20}$$

where $\theta_{i,j}^{D}$ and θ_{i}^{E} are constant parameters obtained by substituting the fixed $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ into (5.6) and (5.7), respectively. From (5.20), we can easily calculate $V_{i,j}^{S}$'s first order derivative w.r.t. P_i and obtain its monotonicity between 0 and P_{max}. Likewise, the monotonicity of P_j in $V_{j,i}^{S}$ can be easily determined at the same time. As such, since $V_{i,j}^{S}$ and $V_{j,i}^{S}$ are convex functions while $\delta_{i,j}$ $\delta_{j,i}$ are linear functions, their linear combination $\omega_{i,j}$ must also be convex given any $\boldsymbol{\rho}$ and $\boldsymbol{\tau}$. Therefore, if $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ can be fixed first, we can directly apply efficient linear programming toolboxes like CVXPY [111] to find the optimum P_i and P_j for the best $\omega_{i,j}$. As such, we propose a heuristic KBC search algorithm by drawing on tabu search [112] to efficiently determine the near-optimal solution for each $\mathbf{P1}_{i,j}$. In detail, the search process is illustrated as follows:

- *Initial KBC Solution Generation:* In the beginning, we first determine a feasible solution of $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ (jointly denoted as a $2K$-dimensional vector $\boldsymbol{\alpha}_{i,j}^{I} = \left[\boldsymbol{\alpha}_i^{I}, \boldsymbol{\alpha}_j^{I}\right]$) as the search starting point, where $\boldsymbol{\alpha}_i^{I}$ and $\boldsymbol{\alpha}_j^{I}$ are two K-dimensional vectors with all elements being 0 initialized to represent the KBC sub-policies at SU i and SU j, respectively. Considering constraint (5.17c), let $\hat{\mathcal{K}}$ and $\check{\mathcal{K}}$ denote two variable sets to record η_i-relevant information, where $\hat{\mathcal{K}} = \mathcal{K}$ and $\check{\mathcal{K}} = \emptyset$ are initialized. Having these, we determine a certain KB k_0 that leads to the highest sum of KB preferences of SU i and SU j by

$$k_0 = \arg\max_{k\in\hat{\mathcal{K}}} \left(p_i^n + p_j^n\right), \tag{5.21}$$

such as

$$\alpha_i^{k_0} = 1 \quad \text{and} \quad \alpha_j^{k_0} = 1. \tag{5.22}$$

Then, let $\hat{\mathcal{K}} = \hat{\mathcal{K}} \backslash n_0$ and $\check{\mathcal{K}} = \check{\mathcal{K}} \cup \{n_0\}$, and repeat the two procedures in (5.21) and (5.22) until both SUs meet constraint (5.17c). However, it should note that constraint (5.17a) or (5.17b) may be violated during the above process. Once that happens, the corresponding KBC indicator of the KB with the maximum size in $\check{\mathcal{K}}$, i.e.,

$$k_1 = \arg\max_{k\in\check{\mathcal{K}}} s_k, \tag{5.23}$$

should be reset by

$$\alpha_i^{k_1} = 0 \quad \text{and} \quad \alpha_j^{k_1} = 0. \tag{5.24}$$

As a result, we can finally generate an initial feasible solution of $\boldsymbol{\alpha}_{i,j}^I$ to problem $\mathbf{P1}_{i,j}$. Meanwhile, as mentioned earlier, the optimal P_i^I and P_j^I corresponding to $\boldsymbol{\alpha}_{i,j}^I$ can be obtained.

- *Neighboring Space Exploration:* Our search algorithm is started from all solutions neighboring to the obtained $\boldsymbol{\alpha}_{i,j}^I$, and let $\mathcal{H}(\cdot)$ denote the neighboring solution set of its input solution. Next, we need to find the optimal solution within $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^I\right)$ that can yield the minimum value of $\omega_{i,j}$, and then replacing the previous solution $\boldsymbol{\alpha}_{i,j}^I$ as well as P_i^I and P_j^I with the current solution, denoted by $\left(\boldsymbol{\alpha}_{i,j}^C, P_i^C, P_j^C\right)$. By repeating the above search process in an iteration fashion, we can obtain multiple different current solution in different search iterations. Besides, let $\mathcal{I}$ denote an optimal solution list with a given maximum length, and once we have a new better $\boldsymbol{\alpha}_{i,j}^C$ from searching $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^C\right)$, the solution of $\left(\boldsymbol{\alpha}_{i,j}^C, P_i^C, P_j^C\right)$ should be added into $\mathcal{I}$ if it is not already in $\mathcal{I}$. The existence of $\mathcal{I}$ is to prevent each search from looping back to previously visited solution spaces, i.e., avoiding trapping into the local optimum. Technically, $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^C\right)$ is given as

$$\begin{aligned}\mathcal{H}(\boldsymbol{\alpha}_{i,j}^C) = \big\{\boldsymbol{\alpha}_{i,j} \colon \|\boldsymbol{\alpha}_{i,j} - \boldsymbol{\alpha}_{i,j}^C\| \leqslant \sigma, \\ \boldsymbol{\alpha}_{i,j} \notin \mathcal{I}, \boldsymbol{\alpha}_{i,j} \in \psi\big\},\end{aligned} \tag{5.25}$$

where σ is the maximum neighboring length, and ψ is $\mathbf{P1}_{i,j}$'s entire feasible solution space.

- *Optimal Solution Update and Termination Check:* Let $\left(\boldsymbol{\alpha}_{i,j}^*, P_i^*, P_j^*\right)$ denote a variable vector to record the best solution obtained so far. Specifically, if we find the current $\left(\boldsymbol{\alpha}_{i,j}^C, P_i^C, P_j^C\right)$ that is better than $\left(\boldsymbol{\alpha}_{i,j}^*, P_i^*, P_j^*\right)$ in any iteration, this should not be added into $\mathcal{I}$ but let

$$\boldsymbol{\alpha}_{i,j}^* = \boldsymbol{\alpha}_{i,j}^C, \quad P_i^* = P_i^C, \quad \text{and} \quad P_j^* = P_j^C. \tag{5.26}$$

Moreover, a search termination criterion is checked by either reaching a maximum number of iterations or a performance growth threshold in terms of $\omega_{i,j}$.

5.3.4 Near-Optimal DUP Scheme

After solving each $\mathbf{P1}_{i,j}$, the optimal coefficient matrix $\boldsymbol{\Omega}$ as well as $\mathbf{P2}$ can be determined. Clearly, its objective function and constraints (5.10c) and (5.10d) are all linear, the only challenge to solve $\mathbf{P2}$ is the 0-1 constraint in (5.10h). Herein, we relax $\boldsymbol{\beta}$ into the continuous variable, denoted as $\boldsymbol{\beta}^R$,

between 0 and 1, which makes **P2** a linear programming problem that is able to be efficiently tackled by CVXPY. Afterward, we need to recover $\boldsymbol{\beta}^R$ to its binary property, and for this, we propose a heuristic DUP strategy as follows. First, we determine one single SU i'-SU j' pair by

$$\beta^*_{i',j'} = \beta^*_{j',i'} = 1 \tag{5.27}$$

if

$$\left(i^{'}, j^{'}\right) = \arg \max_{i\in\mathcal{M}, j\in\mathcal{M}_i, j>i} \beta^R_{i,j}. \tag{5.28}$$

For the remaining $\beta^*_{i,j}$ w.r.t. SU $i^{'}$ and SU $j^{'}$, we have

$$\begin{cases} \beta^*_{i',j} = \beta^*_{j,i'} = 0, & \forall j \in \mathcal{M}_{i'}, j \neq j^{'} \\ \beta^*_{j',i} = \beta^*_{i,j'} = 0, & \forall i \in \mathcal{M}_{j'}, i \neq i^{'} \end{cases}. \tag{5.29}$$

Then we let $\mathcal{M} = \mathcal{M}\backslash\{i, j\}$, and repeat the above processes until finalizing the optimal DUP solutions for all SU pairs. It is observed that the number of variables is only $\left(\sum_{i\in\mathcal{M}} |\mathcal{M}_i|\right)/2$ in solving **P2**, which is a fairly acceptable problem scale in practice, and the performance compromise is believed to be small.

5.3.5 Algorithm Analysis

To better demonstrate the full picture of the proposed solution, we summarize the relevant technical points and enclose them in the following Algorithm 2.

Algorithm 2 The Proposed Resource Management for SSCN

Input: *The system parameters* M, K, W, L, ζ, P_{max}, γ_0, η_0, δ_0, V_0, *and the parameters of the eavesdropping center and all SUs* $G^D_{i,j}$, G^E_i, s_k, C_i, r^k_i, r^k_E, ξ_i, ξ_E, μ^k_j

Output: *The optimal KBC strategy* $\boldsymbol{\alpha}^*$, *optimal DUP strategy* $\boldsymbol{\beta}^*$, *and optimal power allocation strategy* $\boldsymbol{P}^*$

Initialize dual problem iteration index $t \leftarrow 1$, $\tau_i(1)$, $\rho_i(1)$, $\nu_1(1)$, *and* $\nu_2(1)$ *to proper positive values for* **D0**
Set the maximum number of iterations Q
while $t \leqslant Q$ **do**
  for $i \leftarrow 1$ *to* M **do**
    for $j \leftarrow 1$ *to* M **do**
      if $j \in \mathcal{M}_i$ *and* $j > i$ **then**
        Find $\left(\boldsymbol{\alpha}^I_{i,j}, P^I_i, P^I_j\right)$ *in the context of (5.21)-(5.24)*

Initialize KBC search iteration index as $t' \leftarrow 1$, $\mathcal{I}(1) \leftarrow \emptyset$, $\boldsymbol{\alpha}_{i,j}^{C}(1) \leftarrow \boldsymbol{\alpha}_{i,j}^{*} \leftarrow \boldsymbol{\alpha}_{i,j}^{I}$, $P_i^C(1) \leftarrow P_i^* \leftarrow P_i^I$, *and* $P_j^C(1) \leftarrow P_j^* \leftarrow P_j^I$

Set a suitable maximum neighboring length σ *and maximum number of iterations* Q' *for* $\mathbf{P1}_{i,j}$

while $t' \leqslant Q'$ **do**

Determine $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^{C}(t')\right)$ *by (5.25)*

Find the best KBC solution in $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^{C}(t')\right)$ *and then obtain the corresponding optimal power allocation solution by CVXPY*

Assign them to $\boldsymbol{\alpha}_{i,j}^{C}(t'+1)$, $P_i^C(t'+1)$, *and* $P_j^C(t'+1)$, *respectively*

if $\left(\boldsymbol{\alpha}_{i,j}^{C}(t'+1), P_i^C(t'+1), P_j^C(t'+1)\right)$ *is better than* $\left(\boldsymbol{\alpha}_{i,j}^{*}, P_i^*, P_j^*\right)$ **then**

Update $\left(\boldsymbol{\alpha}_{i,j}^{*}, P_i^*, P_j^*\right) \leftarrow \left(\boldsymbol{\alpha}_{i,j}^{C}(t'+1), P_i^C(t'+1), P_j^C(t'+1)\right)$

Keep $\mathcal{I}(t'+1) \leftarrow \mathcal{I}(t')$

else

Update $\mathcal{I}(t'+1) \leftarrow \mathcal{I}(t') \cup \left\{\left(\boldsymbol{\alpha}_{i,j}^{C}(t'+1), P_i^C(t'+1), P_j^C(t'+1)\right)\right\}$

end if

Update $t' \leftarrow t'+1$

end while

Calculate $\omega_{i,j}^{*}$ *by substituting* $\left(\boldsymbol{\alpha}_{i,j}^{*}, P_i^*, P_j^*\right)$ *into (5.16)*

$\omega_{j,i}^{*} \leftarrow \omega_{i,j}^{*}$

end if

end for

end for

Generate $\boldsymbol{\Omega}(t)$ *according to (5.18)*

Solve $\mathbf{P2}$ *by CVXPY and obtain* $\boldsymbol{\beta}^{R}(t)$

Finalize $\boldsymbol{\beta}^{*}(t)$ *by (5.27)-(5.29)*

Finalize $\boldsymbol{\alpha}^{*}(t)$ *and* $\boldsymbol{P}^{*}(t)$ *by feeding* $\boldsymbol{\beta}^{*}(t)$ *back to* $\boldsymbol{\Omega}(t)$

Update $\tau_i(t+1)$ *and* $\rho_i(t+1)$ *by (5.14) and* (5.15)*, respectively*

Update $\nu_1(t+1)$ *and* $\nu_2(t+1)$ *under a given rule*

$t \leftarrow t+1$

end while

return $(\boldsymbol{\alpha}^{*}, \boldsymbol{\beta}^{*}, \boldsymbol{P}^{*}) \leftarrow (\boldsymbol{\alpha}^{*}(Q), \boldsymbol{\beta}^{*}(Q), \boldsymbol{P}^{*}(Q))$

Regarding the computational complexity of Algorithm 2, it is first observed that for each $\mathbf{P1}_{i,j}$, we need to obtain all feasible KBC solutions within $\mathcal{H}\left(\boldsymbol{\alpha}_{i,j}^{C}\right)$ in any of its iterations. Note that σ is a very small parameter compared with N in (5.25), the complexity of determining the neighborhood

solution space is approximately $\mathcal{O}\left(\binom{2K}{\sigma}\right) = \mathcal{O}\left(K^{\sigma}\right)$. With the maximum number of search iteration Q', solving each $\mathbf{P1}_{i,j}$ needs complexity $\mathcal{O}\left(Q'K^{\sigma}\right)$. Besides, the CVXPY toolbox employed for the relaxed **P2** requires $\mathcal{O}\left(M^4\right)$ complexity [113] to solve a group of $\left(\sum_{i\in\mathcal{M}}|\mathcal{M}_i|\right)$ DUP variables. Since there is a total of $\left(\left(\sum_{i\in\mathcal{M}}|\mathcal{M}_i|\right)/2\right)$ subproblems $\mathbf{P1}_{i,j}$ and one subproblem **P2** need to be tackled in each iteration of **D0**, its corresponding complexity is $\mathcal{O}\left(M^2Q'K^{\sigma}+M^4\right)$. Further combining the maximum number of dual problem iteration Q, the proposed Algorithm 2 has a polynomial-time overall complexity of $\mathcal{O}\left(QM^2\left(Q'K^{\sigma}+M^2\right)\right)$.

5.4 Numerical Results and Discussions

In this section, numerical evaluations are conducted to demonstrate the performance of our proposed resource allocation solution in the SSCN, where we employ Python 3.7-based PyCharm as the simulator platform and implement it in a workstation PC featuring the AMD Ryzen-9-7900X processor with 12 CPU cores and 128 GB RAM. In the basic system setup, we first model a single-cell circular area with a radius of 300 meters, in which multiple SUs and one eavesdropping center are randomly dropped, while multiple KBs are preset to provide SUs with a variety of distinct SemCom services. Correspondingly, we set a uniform KB storage capacity for all SUs, and each of them has a randomly generated storage size. For brevity, other relevant simulation parameters not mentioned in the context along with their values are summarized in Table 5.1.

Besides, the preference rankings for all KBs (i.e., r_i^n) at the eavesdropping center and each SU are generated independently and randomly, where their Zipf distributions are assumed to have the same skewness 1.2. The average interpretation time for semantic packets based on each KB n is considered to be the same for all SUs. Here, we randomly generate $1/\mu_i^n$ in a range of $5\times10^{-3}\sim1\times10^{-2}$ s/packet w.r.t. each KB n, as the average interpretation time of different KBs-based packets is different from each other. Further, the minimum knowledge preference satisfaction threshold η_0, the maximum queuing delay threshold δ_0, and the maximum SST threshold V_0 are prescribed as 0.5, 5 ms, and 50, respectively. Notably, all the above parameter values are set by default unless otherwise specified, and all subsequent numerical results are obtained by averaging over a sufficiently large number of trials.

For comparison purposes, here we employ two different benchmark schemes of SemCom-empowered service provisioning herein [83,120,121]: 1) Random Power allocation with Distance-first pairing (RPD) strategy, which assumes

Table 5.1: Simulation Parameters

Parameters	**Values**
Subchannel bandwidth (W)	0.1 MHz
Number of SUs (M)	100
Number of KBs (K)	12
Size of KB k (s_k)	$1 \sim 5$ units (randomly) [83]
KB storage capacity of SUs (C_i)	24 units
Skewness of the Zipf distribution w.r.t. each SU's KB preference (ξ_i)	1.2
Average interpretation time of KB n-based semantic packets ($1/\mu_i^n$)	$5\times10^{-3} \sim 1\times10^{-2}$ s/packet (randomly) [83]
Maximum transmit power of each SU (P_{max})	21 dBm [114]
Noise power (ζ^2)	-111.45 dBm [115]
Path loss model	$34 + 40\log(d\ [\text{m}])$ [116]
Average number of bits required for encoding one semantic triplet (L)	800 bits [117]
Minimum semantic knowledge satisfaction threshold (η_0)	0.5 [88]
Maximum queuing delay threshold (δ_0)	5 ms [118]
Minimum SST threshold (V_0)	50 [119]

each SU has a random assigned transmit power while choosing its nearest SU for DUP; 2) Maximum Power allocation with Knowledge-first pairing (MPK), in which each SU is assigned with a transmit power of P_{max} while selecting its neighboring SU with the highest KB matching degree for DUP.

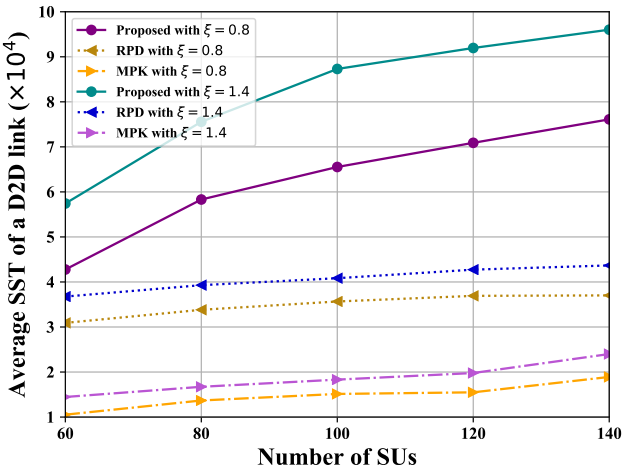

Figure 5.2: Average SST vs. different numbers of SUs.

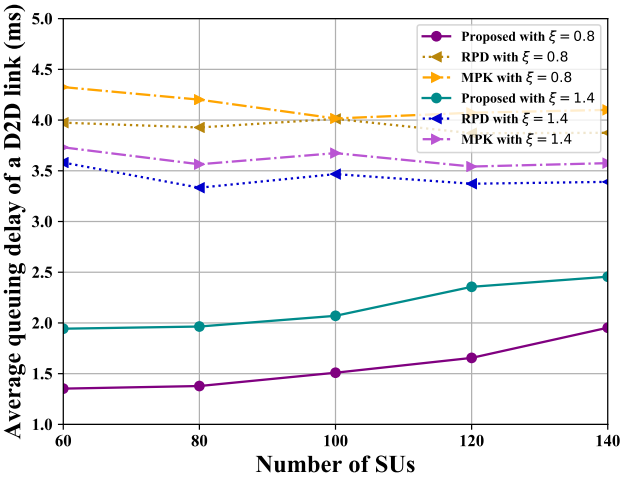

Figure 5.3: Average queuing delay vs. different numbers of SUs.

In addition, a personal preference-first KBC policy is considered for RPD and MPK, which allows each SU to cache KBs with the highest preferences until η_0 is satisfied, and then randomly cache the remaining KBs until reaching maximum capacity.

We first verify the average SST performance and the average queuing latency performance obtained by each D2D SemCom link under varying numbers of SUs in Fig. 5.2 and Fig. 5.3, respectively, in which two different skewness values of the Zipf distribution of $\xi = 0.8$ and $\xi = 1.4$ are taken into account. In comparison with the two benchmark schemes, our solution always renders an obvious SST performance gain at any number of SUs, while reaching a positive SST performance representing that the semantic information security has been adequately guaranteed in the SSCN. For example, in Fig. 5.2, our solution reaches a high SST performance of around 7.7×10^4 at 140 SUs with $\xi = 0.8$, which is much higher than around 3.8×10^4 SST of the RPD and around 1.9×10^4 SST of the MPK.

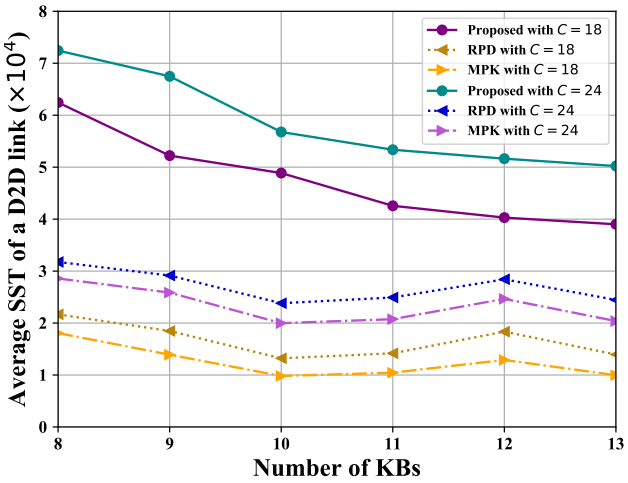

Figure 5.4: Average SST vs. different numbers of KBs.

In addition, in Fig. 5.3, a lower queuing latency is seen by our solution, which is less than half of that obtained by the comparison schemes. Note that as the increase of the number of SUs, both the SST performance and queuing latency show a grow trend. The former is because that the more SUs mean the more neighbors for each SU, and thus each SU should have a higher chance to find a better SemCom counterpart for D2D pairing and to achieve a better SST performance. However, such an increase will be eventually stabilized since the bandwidth budget is already fixed. Likewise, for the latter queuing delay trend, when each SU has a better semantic value rate, the semantic data packet arrival rate becomes correspondingly higher, thereby leading to a higher queuing delay. Furthermore, it is observed that the higher skewness of the Zipf distribution is with the better SST and a worse queuing delay. The rationale behind the former phenomenon is that the higher skewness makes each SU easier meet the semantic satisfaction

as it only needs to cache the KBs with high probabilities, and the semantic triplets generated based on these KBs precisely have the high semantic value. Meanwhile, such a situation happens to cause that each SU is more difficult to find a high knowledge-matching D2D pair due to the higher deviation, hence the queuing delay becomes higher as well compared with the low skewness.

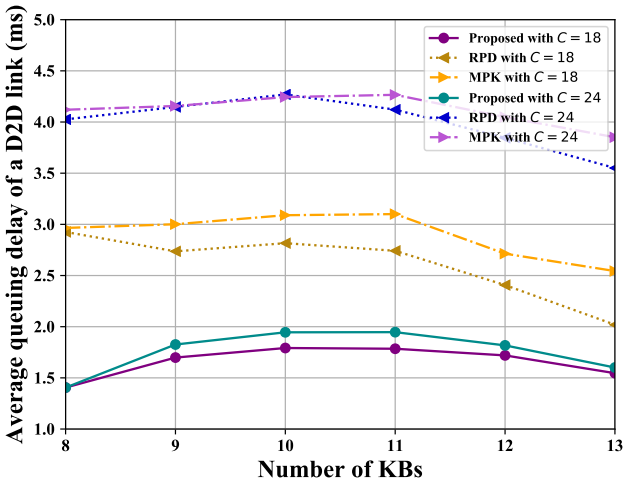

Figure 5.5: Average queuing delay vs. different numbers of KBs.

Fig. 5.4 and 5.5 compare the average SST and queuing delay performance of each D2D SemCom link with the benchmarks under varying numbers of KBs, respectively, with two different KB storage capacities of $C = 18$ and $C = 24$. In both figures, it is seen that our proposed solution far superior to either the RPD or the MPK at each point. For instance, when the number of KBs is set to 10 and $C = 24$, an average SST performance of 5.8×10^4 is observed by the proposed solution in Fig. 5.4, which is around 1.9 times higher than that of the MPK and around 1.4 times higher than that of the RPD. Specially, in Fig. 5.4, our solution shows a downtrend of SST with the increase of the number of KBs. This is because that the more the number of KBs, the less the discrepancy of KB preference between SUs and the eavesdropping center, resulting in the higher probability for the eavesdropping center having the same KBs as SUs, which inevitably causes a lower semantic secrecy information rate. Besides, a larger KB capacity C has a better SST, which can be interpreted as the more KBs are cached at each SU, the more semantic value is transmitted.

In Fig. 5.5, an increase trend of the average queuing delay performance is first seen by the proposed solution with the number of KBs, and then decline slowly after 11 KBs. This is attribute to the fact that at the very beginning, the more KBs indicates a higher effective packet arrival rate, which can lead

to a grow trend of queuing delay. However, such performance saturation will get better as a higher probability for two SUs caching the same KBs with high interpretation rates, which dominates the overall queuing delay performance change. Moreover, there is only a small queuing delay gap between the cases with different KB storage capacities. This is because that our solution always gives high caching priority to the KBs with lower interpretation times, and once the semantic knowledge satisfaction threshold or the queuing delay threshold is met, the remaining capacity will not be in use.

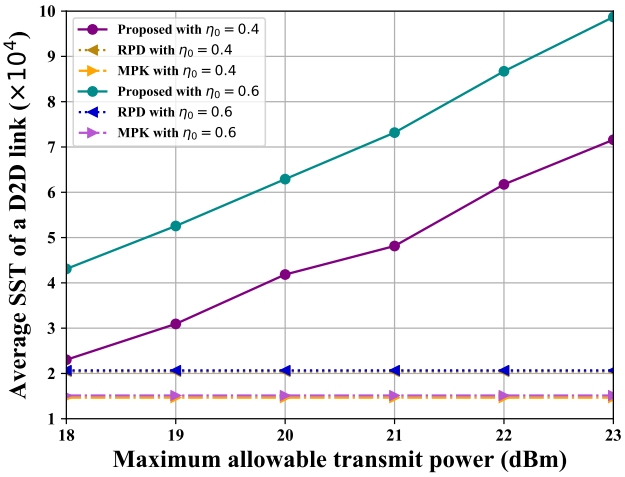

Figure 5.6: Average queuing delay vs. different maximum allowable transmit powers.

In addition, Fig. 5.6 and Fig. 5.7 validate the average queuing delay and SST performance under varying maximum allowable transmit powers, respectively, under two semantic knowledge satisfaction thresholds of $\eta_0 = 0.4$ and $\eta_0 = 0.6$. Consistent with the previous results, our solution still outperforms the two benchmarks with a significant performance gain. Specifically, at the point of $P_{max} = 21$ dBm and $\eta_0 = 0.6$, the proposed solution reaches an average SST performance of around 73000 in Fig. 5.6, which is 53000 higher than that of RPD, and obtains an average queuing delay of around 1.4 ms in Fig. 5.7, which is 2.3 ms lower than that of MPK. Apart from this, note first that in Fig. 5.6, the SST performance increases as P_{max}. This is because that based on our efficient DUP solution, most of the SUs can always find a best SU for D2D SemCom pairing to guarantee a positive SST, in which case each SU is able to be assigned with a highest transmit power to improve the semantic value transmission rate as much as possible. Also, the higher η_0 leads to the better SST, which trend is quite obvious due to the looser KBC constraints.

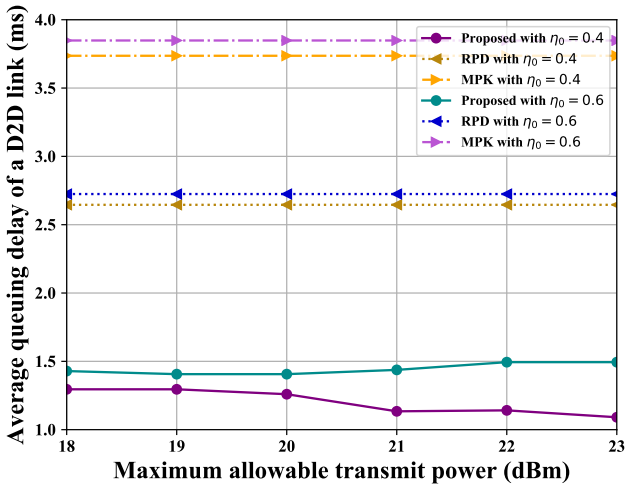

Figure 5.7: Average queuing delay vs. different maximum allowable transmit powers.

Finally, as in Fig. 5.7, it is observed that the average queuing latency performance obtained by all resource allocation schemes shows a similar stable trend as the growth of P_{max}. This phenomenon can be understood by the fact that we just set a queuing latency limitation in the optimisation problem, and our main focus is on the maximisation of SST rather than minimizing the queuing delay. Hence, the corresponding solution here is just to satisfy the delay constraint, resulting in the stable trend. Nevertheless, our proposed solution still has a better delay performance compared with the benchmarks, as aforementioned. In the meantime, it is noticed that the lower the η_0, the lower the average queuing delay. This is because that the lower semantic knowledge satisfaction threshold clearly makes each SU cache less KBs, thus the knowledge overlapping rate between the two paring SUs is more likely to be smaller. Consequently, the effective semantic packet arrival rate at a lower η_0 should be smaller than that at a higher η_0, rendering a better queuing latency performance.

5.5 Conclusions

This chapter has explored the semantic information security-aware resource allocation in the SSCN. We have first identified two key problems of KBC and DUP with the joint consideration of power allocation. Then, the knowledge matching based queuing delay has been derived and a novel performance metric of SST has been developed. On this basis, we have formulated a joint

SST maximisation problem, followed by a corresponding solution proposed. Our solution first leveraged primal-dual transformation and decomposed the dual problem into multiple subproblems, which can be separately solved by our devised two-stage method. Compared with the two benchmarks, simulation results have shown superiorities in SST, average queuing delay, and semantic knowledge satisfaction.

We hope this chapter can provide some valuable insights for follow-up research on secure SemCom. It is worth noting that this work also has several limitations. First, the current model considers a single-cell SemCom network with centralized resource control, which may not scale directly to multi-cell or ultra-dense scenarios. Second, the Zipf-based knowledge base popularity model provides a tractable approximation of user preferences but may deviate from highly dynamic or context-dependent behaviors. Third, although the proposed primal-dual framework achieves near-optimal performance with polynomial complexity, the computational cost could still increase with the number of users and knowledge bases.

Chapter 6

Attack Surface in Knowledge-Assisted SemCom

6.1 Introduction

In a SemCom system, semantic encoders extract information considered meaningful under shared knowledge between transmitter and receiver. As this paradigm matures, knowledge repositories, ontologies, and structured semantic priors are increasingly embedded directly into encoding and decoding processes. Recent knowledge-enabled SemCom frameworks explicitly incorporate source, contextual, and channel knowledge bases, as well as graph- and retrieval-driven pipelines, into semantic encoding and reconstruction [3, 122, 123]. Knowledge mappings are therefore conditioned on shared and evolving knowledge states rather than fixed transformations.

Therefore, SemCom networks introduces a new system dependency, i.e., the knowledge plane emerges as a semantic control layer governing how meaning is extracted, compressed, and interpreted. To ensure high accuracy of meaning delivery, knowledge should be carefully managed (including knowledge replication, versioning, and synchronisation) across transceivers, [124]. Knowledge, the pillar of SemCom, is capable of underpinning semantics representation, extraction, and recovery. Consistency of knowledge becomes a foundational requirement for reliable communication [78].

Accordingly, the concern of security surface expands beyond symbol transmission. In traditional systems, protection primarily focuses on the data plane, whereas in knowledge-centric SemCom the integrity of the knowledge plane becomes equally critical. While prior work has recognized that semantic correctness reshapes classical security objectives in SemCom [23, 79], and emerging frameworks increasingly treat knowledge as a core architectural de-

pendency [81, 122], the knowledge plane itself remains insufficiently analyzed as an independent security domain within communication system design. In knowledge-centric SemCom, however, influencing the knowledge plane, through corruption, biased activation, inconsistent updates, or availability disruption, can alter semantic interpretation without modifying transmitted bits. In such systems, agreement on bits does not guarantee agreement on meaning. Version skew or inconsistent replicas can induce encoder–decoder misalignment under error-free transmission, leaving symbol delivery intact while silently breaking semantic alignment beyond the reach of conventional integrity checks.

In this chapter, we reconceptualize the knowledge plane as a first-class communication layer whose integrity, synchronisation, and availability fundamentally determine semantic reliability in SemCom systems. We develop a systematic architectural perspective on knowledge-centric SemCom, identify four knowledge-plane attack surfaces and their corresponding semantic failure modes, and demonstrate through a controlled version-divergence case study that semantic misalignment can arise even under error-free symbol transmission. We further articulate defensive design principles and outline key research challenges, establishing knowledge-plane security as a foundational requirement for secure, interoperable, and scalable SemCom systems.

6.2 Knowledge Plane in SemCom

SemCom aims to convey task-relevant meaning rather than raw data representations, and such knowledge should be typically embedded into the process of encoding and decoding. In this way, a shared and evolving knowledge plane is formed that governs what is considered meaningful, how it is compressed and interpreted.

6.2.1 Two-plane Semantic Communication System

A typical SemCom process transforms source data into semantically grounded meaning through semantic encoding, physical transmission, and semantic decoding [125]. The key characteristic of this SemCom system is that both encoder and decoder, performing data compression and recovery in a data plane, are conditioned on local knowledge managed by a knowledge plane.

As illustrated in Fig.6.1, the transmitter leverages its current knowledge to extract task-relevant information and construct a compact semantic representation. After channel coding and transmission over a noisy wireless channel, the receiver applies its own knowledge to interpret the recovered

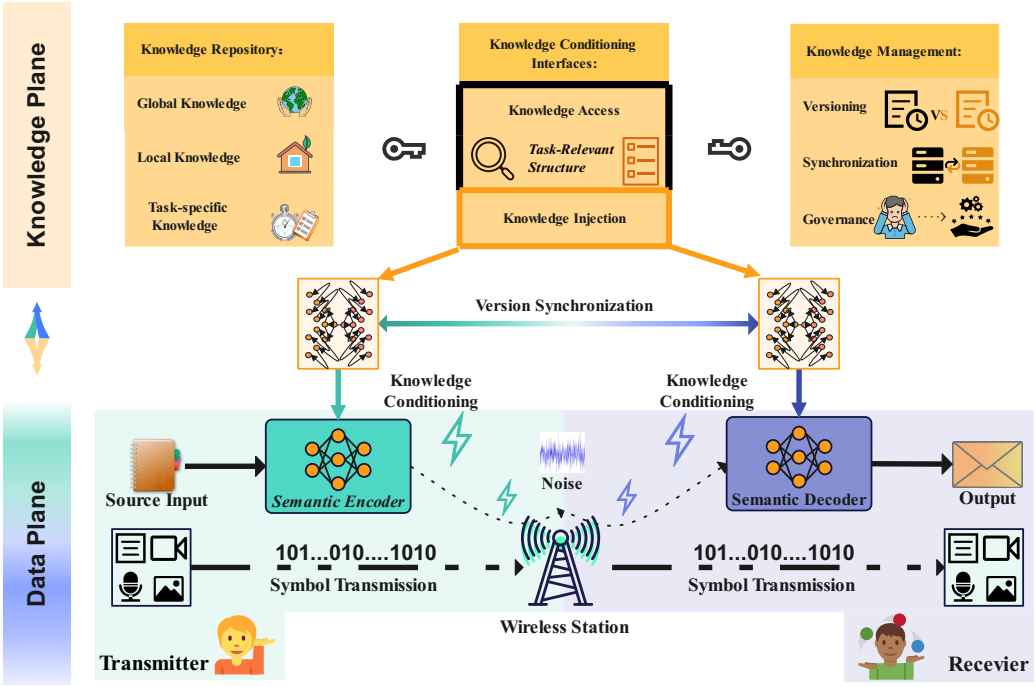

Figure 6.1: A Two-Plane Knowledge- Based Architecture: The data plane transports semantic representations through the channel, while the knowledge plane conditions encoding and decoding through shared and evolving knowledge states. Semantic reliability, therefore, depends on both symbol delivery and knowledge-plane consistency.

representation and generate the final output. Semantic reliability, therefore, depends on two conditions: (i) correct symbol delivery over a noisy channel in the data plane and (ii) compatibility of knowledge across communicating nodes. Even when the physical channel is error-free, discrepancies in knowledge can lead to divergent interpretations of the same transmitted representation.

To formalize this dependence, a two-plane SemCom network architecture is presented. The *data plane* carries semantic representations through the channel, while the *knowledge plane* constructs, validates, versions, and distributes the structured knowledge that conditions encoding and decoding. The knowledge plane interfaces with the data plane through two key mechanisms: a *knowledge access interface* that selects task-relevant structures, and a *knowledge injection interface* that integrates selected knowledge into semantic coding models. Because transceiver behavior is conditioned on this knowledge, inconsistencies or drift in the knowledge plane can alter commu-

nication outcomes without modifying transmitted symbols.

6.2.2 Layered Knowledge Structures

In practice, the knowledge plane is not monolithic but layered [2]. *Global knowledge* provides shared semantic grounding across nodes, including public corpora, ontologies, pretrained models, and widely accepted entity relationships. This layer establishes a common reference frame for interpretation. *Local knowledge* captures context-specific information such as user preferences, mission constraints, operational environments, or domain rules. This layer may differ across nodes and must be coordinated to preserve semantic compatibility.

For each communication instance, only a subset of knowledge is typically activated. Many architectures construct a *content-specific substructure*, such as a retrieved subset of entries or a subgraph tailored to the current message. This content-scoped knowledge focuses on reasoning and reduces model complexity. Because semantic encoding and decoding depend on these layered structures, inconsistencies or corruption at any level, either global, local, or task-specific, can alter interpretation. Crucially, semantic correctness depends not only on what knowledge is stored, but also on how it is activated and incorporated into the transceiver pipeline.

6.2.3 Knowledge-Driven Encoding and Decoding

Knowledge influences communication through coordinated operations at both transmitter and receiver [122]. At the *transmitter*, semantic encoding identifies key entities or semantic elements in the source message, aligns them with entries in the maintained knowledge base, resolves ambiguities using contextual relationships, and constructs a structured representation for transmission. For example, in graph-based knowledge systems, this may involve building a minimal task-specific subgraph, while in embedding-based knowledge systems, it may involve conditioning representations on retrieved knowledge vectors [123]. At the *receiver*, decoded symbols are mapped back into semantic representations, relevant knowledge structures are retrieved or expanded, and contextual reasoning reconstructs the intended meaning. The same transmitted representation can therefore yield different outputs if the receiver's knowledge state differs from that of the transmitter.

This perspective highlights a central architectural insight, i.e., semantic behavior depends not only on the physical signal but also on the correctness and compatibility of the knowledge selection and conditioning processes.

6.2.4 Knowledge Evolution and Synchronisation

Knowledge in practical SemCom systems is typically dynamic [2]. It evolves through data ingestion, model updates, structural refinement, and adaptation to changing tasks. In distributed deployments, knowledge is often replicated across transceivers and propagated asynchronously [78]. While many SemCom frameworks implicitly assume shared knowledge, this assumption becomes fragile in practical SemCom networks. Nodes may maintain different knowledge versions, receive updates at different times, or retain partial replicas. In effect, the knowledge plane is in charge of the coordination of knowledge version control, validation, distribution, and synchronisation.

Without effective synchronisation mechanisms, well-functioning transceivers may apply incompatible semantic mappings to the same transmitted representation. As a result, semantic misalignment can emerge even when the data plane operates flawlessly. This architectural dependence elevates the knowledge plane to a vital component whose consistency is essential for reliable SemCom.

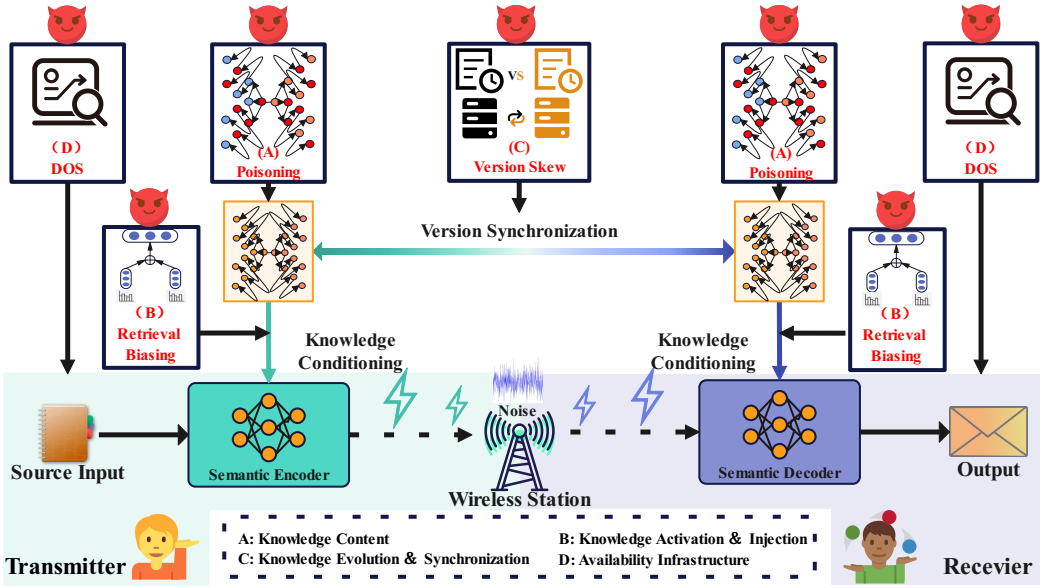

Figure 6.2: The construction of knowledge plane attack surfaces includes two major parts: 1) encoder-decoder knowledge-based SemCom, 2) different attacks on knowledge plane.

6.3 Knowledge Compromise in SemCom

Section II established that SemCom systems rely on a layered knowledge architecture that shapes how meaning is extracted, compressed, and reconstructed. Since both encoding and decoding are conditioned on their knowledge, semantic correctness depends not only on reliable symbol transmission but also on the integrity and consistency of the knowledge plane. This architectural dependency reshapes the security landscape. In conventional communication systems, the primary attack surface lies in the transmission channel. In knowledge-driven SemCom, however, the attack surface extends beyond symbol delivery to the structures and processes that govern knowledge content, activation, and evolution. Rather than modifying transmitted bits, an adversary can induce semantic failure solely through influencing the knowledge plane, thereby reshaping the semantic interpretation while leaving the physical signal unchanged.

In the following, we discuss threats across the knowledge content, activation and injection mechanisms, evolution and synchronisation processes, and cross-layer availability surfaces of the knowledge plane.

6.3.1 Knowledge Content Compromise

As shown in Fig.6.2, knowledge content constitutes the semantic reference shared by encoder and decoder. It defines the entities, relationships, priors, and embedding structures upon which semantic interpretation relies [125]. When this layer is compromised, the reference frame for meaning itself is altered.

The attack surface lies in the *stored semantic structures*. Adversaries may insert malicious entries, modify relationships between entities, delete critical structures, or perturb embedding representations in ways that distort semantic proximity. For instance, if the knowledge of a SemCom system is in a graph-based format, even small structural modifications can cascade into incorrect inference. If the knowledge is exploited as embeddings in a SemCom system, subtle shifts in representation space may bias alignment or disambiguation.

Because knowledge content may be shared across nodes or replicated across links, corruption at this layer can persist across sessions and propagate system-wide [78]. Unlike signal-level adversarial perturbations, which affect individual transmissions, content compromise systematically reshapes how meaning is interpreted over time. Crucially, such attacks do not require altering transmitted symbols. Bit-level correctness may be preserved while semantic interpretation has been silently redefined.

6.3.2 Knowledge Activation and Injection Compromise

While knowledge content determines what semantic structures exist, activation and injection mechanisms determine which portions of that knowledge influence a particular communication instance. This operational pathway forms a distinct attack surface.

The vulnerability arises not from modifying stored knowledge, but from *biasing how it is selected or integrated*. Many SemCom encoding/decoding schemes rely on retrieval, similarity search, graph traversal, or rule-based selection to activate task-relevant knowledge [123, 126]. Adversaries may manipulate these pathways through index poisoning, similarity skewing, decoy insertion, or structural graph manipulation [127, 128]. Even when the underlying knowledge remains correct, biased retrieval can redirect semantic compression at the transmitter or alter interpretation at the receiver.

The knowledge injection interface can likewise be targeted. If retrieved knowledge is incorporated through embeddings or graph-conditioned encoders, adversarial perturbations at this interface can influence downstream inference without altering stored structures. In this category, knowledge remains intact but is operationally misused. As with content compromise, physical-layer signals may remain unmodified, making these attacks difficult to detect using conventional channel integrity mechanisms.

6.3.3 Knowledge Evolution and Synchronisation Compromise

Knowledge evolve over time and are often replicated across distributed nodes [78]. Evolution and synchronisation processes ensure that communicating parties maintain compatible semantic understanding and inference abilities. When these temporal and distributed mechanisms are compromised, semantic alignment between transmitters and receivers can fail even if local knowledge appears internally consistent.

The attack surface lies in *update pipelines, version control mechanisms, provenance validation, and distribution processes*. Adversaries may delay or suppress updates to induce version skew, inject unauthorized modifications through compromised governance channels, or manipulate validation procedures to legitimize corrupted knowledge.

In distributed or heterogeneous deployments, SemCom nodes may already maintain partial or asynchronous replicas [2]. Induced inconsistencies can therefore cause the encoder and decoder to apply incompatible semantic understanding and inference abilities. Because transmitted symbols may remain valid under local knowledge, traditional physical-layer security checks

cannot detect the resulting divergence. Unlike content compromise, which alters semantic structures directly, synchronisation attacks exploit temporal inconsistency, making the communicating parties hold different knowledge versions, thus unmapped semantic understanding and inference abilities.

6.3.4 Knowledge Plane Availability and Degradation

Beyond integrity and synchronisation, SemCom depends on the continuous availability of the knowledge plane. Retrieval services, indexing systems, update channels, and validation mechanisms should remain correctly operational for encoding and decoding processes. Thus, this infrastructure of knowledge plane forms the fourth attack surface.

Adversaries may target this surface through *denial-of-service attacks* against retrieval systems, index corruption, disruption of update propagation, or resource exhaustion within the knowledge plane [129]. More subtle degradation may selectively restrict access to portions of knowledge, increasing uncertainty or reducing confidence when compressing and recovering data, without triggering explicit failures.

Unlike the previous categories, availability attacks do not necessarily alter knowledge structures or their correctness. Instead, they disrupt the operational continuity of the knowledge plane. Because semantic processing depends on timely and reliable access to knowledge, degradation at any architectural layer can cascade into reduced task accuracy, delayed interpretation, or inconsistent outputs. Similarly, while the bit-level transmissions may remain unaffected, the failure occurs within the knowledge-dependent control plane that shapes meaning.

6.4 Failure Modes Induced in SemCom

According to the four knowledge-plane attack surfaces identified in Section 6.3, here we examine how these compromises manifest at the semantic level. In conventional communication systems, failures appear as bit errors or degraded signal quality. In knowledge-based SemCom, however, failures often arise even when symbol transmission is correct. Because interpretation depends on shared and evolving knowledge, disruptions in the knowledge plane can distort meaning without introducing detectable channel errors.

Each attack surface produces a distinct semantic symptom. Specifically, content compromise leads to gradual drift; activation manipulation induces inference distortion; synchronisation breakdown causes communication parties misalignment even they hold the same syntax data and availability degra-

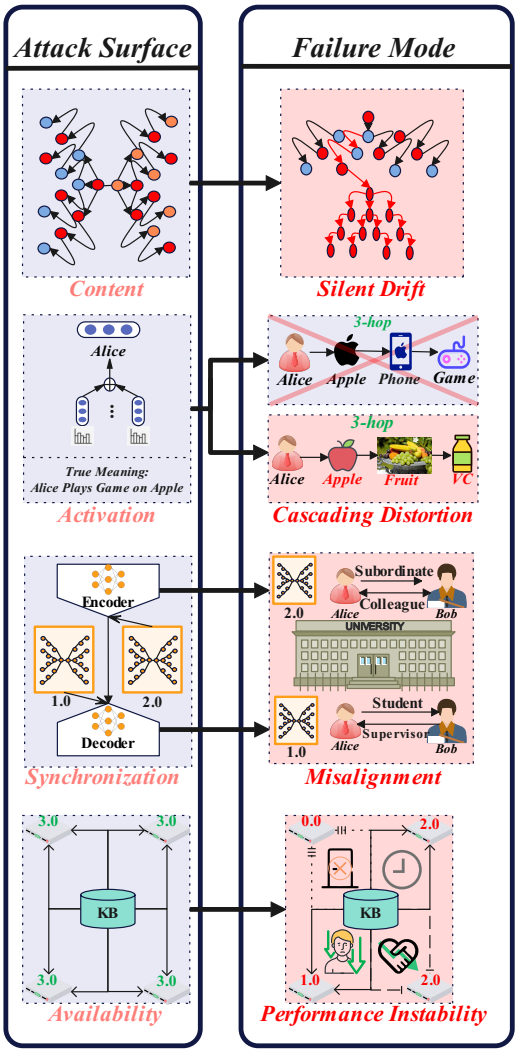

Figure 6.3: The failure mode includes two columns: The left column illustrates the SemCom components that will be attacked, the right column provides the status of the attacked SemCom components.

dation results in unstable semantic performance. Recognizing these patterns is essential for effective detection and mitigation.

Silent Semantic Drift Compromise of knowledge content induces silent semantic drift, i.e., a gradual redefinition of entities, relationships, or contextual priors [23]. When stored knowledge is altered, encoders and decoders continue operating consistently with respect to the modified state. The system appears coherent, yet its semantic grounding has shifted. Drift accumulates over time and propagates across sessions and nodes. Unlike transient transmission errors, it preserves symbol-level correctness while progressively redefining meaning. No abrupt failure occurs; instead, interpretation steadily diverges from its intended reference.

Cascading Inference Distortion When activation and injection mechanisms are manipulated, the failure manifests as cascading inference distortion. Stored knowledge remains intact, but the subset activated for a specific content is biased. Because semantic encoding and decoding depend on retrieved entities and contextual structures, even a minor perturbation in retrieval, such as a decoy entry or skewed similarity ranking, can redirect downstream reasoning. In multi-hop or graph-based systems, this distortion may amplify across inference steps [23]. The output may remain logically consistent under the activated context, yet deviate sharply from the intended meaning. Unlike semantic drift, which evolves gradually, cascading distortion produces abrupt, task-specific deviations driven by biased knowledge selection.

Encoder–Decoder Semantic Misalignment Compromise of knowledge evolution and synchronisation leads to encoder–decoder semantic misalignment [78]. Transmitter and receiver operate with incompatible knowledge states due to version skew or inconsistent replicas. Each node may remain internally coherent, yet semantic mappings differ across transceivers. The channel faithfully delivers encoded representations, but interpretation fails because the underlying semantic references are no longer shared. The same representation can therefore yield different task-level outputs. This failure reflects a breakdown of shared semantic assumptions rather than corruption of transmitted symbols.

Semantic Performance Instability Degradation of knowledge-plane availability manifests as semantic performance instability. Instead of altering knowledge content or selection, availability failures disrupt reliable access to

knowledge resources. When retrieval services degrade or updates are delayed, semantic processing may fluctuate unpredictably [127]. Systems may rely on incomplete or outdated knowledge, resulting in varying accuracy, increased latency, or unreliable confidence estimates. Here, the dominant symptom is variability rather than systematic bias: physical transmission remains intact, yet semantic robustness erodes due to weakened knowledge infrastructure.

6.5 Case Study

In this section, we constructed a controlled simulation environment to evaluate the semantic impact of the four attack surfaces identified earlier: knowledge content compromise, knowledge activation and injection compromise, knowledge evolution and synchronisation compromise, and knowledge-plane availability degradation. The objective is to illustrate how each attack surface can independently induce semantic failures even when the physical transmission channel remains reliable.

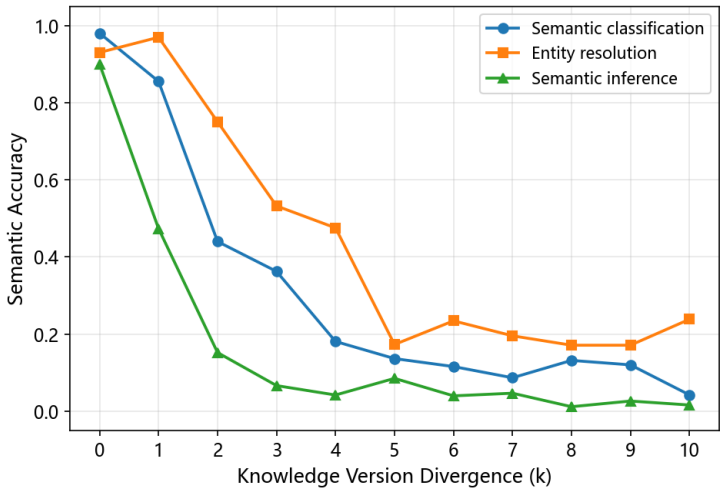

Figure 6.4: Accuracy vs Knowledge Version Divergence

6.5.1 Case I: Semantic accuracy evaluation under diverged Knowledge Versions

Among the attack surfaces identified in Section 6.3, **compromise of knowledge evolution and synchronisation** is particularly subtle. Unlike direct corruption of stored knowledge or biased activation, version divergence can

arise naturally in well-functioning distributed systems through delayed updates, partial replication, or asynchronous propagation across nodes. This scenario is therefore both realistic and structurally revealing. It requires no adversarial modification of transmitted symbols, yet it can induce encoder–decoder semantic misalignment as described in Section IV. In other words, agreement on bits does not guarantee agreement on meaning.

System Setup and Controlled Knowledge Divergence We consider a distributed SemCom setting in which transmitter and receiver maintain replicated knowledge bases that are periodically updated. The semantic encoder extracts structured representations from source inputs based on its local knowledge state, and the decoder reconstructs meaning using its own knowledge state.

To isolate the impact of knowledge divergence, we introduce a controlled version gap between transmitter and receiver. The transmitter operates with the latest knowledge state, while the receiver lags by k updates. These updates modify selected entity relationships or contextual priors that influence semantic interpretation. Importantly, the semantic encoder, channel coding, modulation, and physical transmission pipeline remain identical across all experiments. The transmitted symbol sequence is therefore unchanged; only the receiver's knowledge version differs. This controlled setup ensures that any observed semantic discrepancy arises solely from knowledge version divergence, without conflating it with channel errors, adversarial perturbations, or direct knowledge poisoning.

Semantic Misalignment and Quantitative Impact In version divergence, the transmitter encodes semantic representations based on its updated knowledge state, while the receiver decodes them using an outdated reference. Although the transmitted symbols are delivered correctly and bit integrity is preserved, the reconstructed meaning may differ from the intended interpretation. To quantify this effect, we evaluate task-level performance as a function of knowledge version divergence, where three tasks are semantic classification, entity resolution, and semantic inference. The transmitter maintains the latest knowledge state, while the receiver operates with a lag of k updates. We measure semantic agreement between intended and decoded outputs across increasing version gaps, while keeping the physical channel error-free.

As shown in Fig.6.4, semantic accuracy remains high when knowledge states are synchronized ($k = 0$), but degrades progressively as the version gap increases. This degradation occurs despite identical transmitted symbols

across all settings. The results demonstrate that semantic reliability depends not only on channel integrity but also on knowledge-plane synchronisation. Even in the absence of transmission errors, divergence in knowledge states alone is sufficient to induce measurable semantic failure.

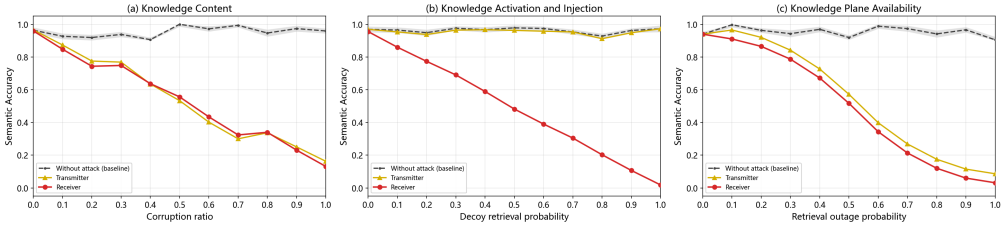

Figure 6.5: Accuracy vs knowledge content, knowledge injection and knowledge-plane availability

6.5.2 Case II: Semantic accuracy evaluation under knowledge content, knowledge injection and knowledge-plane availability

System Setup To compare different knowledge-plane attacks, we adopt the same SemCom coding model across all simulations. The transmitter and receiver share the same knowledge before being attacked, the physical transmission channel is maintained under a good channel condition so that semantic accuracy are induced only by the knowledge plane. Under different attack intensities, semantic performance is evaluated using semantic accuracy.

Compromise of knowledge content In this setting, a subset of entity relationships within the shared knowledge is intentionally modified. The transmitter and receiver continue operating with the same imprecise knowledge, while the semantic encoder, decoder, and physical channel remain unchanged. The attack intensity is controlled by the corruption ratio of knowledge, which represents the percentage of modified semantic information.

As shown in Fig 6.5(a), semantic accuracy decreases gradually as the corruption ratio increases. Because both communication parties remain consistent with respect to the imprecise knowledge, the degradation of the receiver and the transmitter appears to be similar and cumulative, rather than sudden. Although transmitted symbols remain correct, the transmitted messages progressively shifts away from the original meaning.

Compromise of knowledge injection In this scenario, the original knowledge content remains intact, but the process of knowledge injection is manipulated via selected decoy knowledge. During encoding and decoding, these misleading knowledge may be selected instead of the correct knowledge. Moreover, the decoy knowledge can be utilized by attackers to recover meaning only in the decoder without encoding, which results in the receiver cannot understand the meaning of the message precisely, but the transmitter still can encode messages correctly. Conversely, if the decoy knowledge is utilized in encoding process, the decoder with correct knowledge still cannot recover semantic information. Thus, we discussed the injection of decoy knowledge into the decoder, the attack intensity is characterized by the probability of decoy retrieval.

As illustrated in Fig 6.5(b), For receiver, semantic performance remains relatively stable under low attack intensity but drops rapidly once misleading knowledge dominates the retrieval process. Since the decoy knowledge acts on the decoder, the transmitter has almost no influence. Unlike knowledge content compromise, decoy knowledge introduces abrupt semantic distortion rather than slow degradation. Small retrieval errors can propagate through the semantic reasoning process and produce incorrect semantic outputs.

Degradation of knowledge-plane availability In this setting, the semantic retrieval service is intermittently disrupted, forcing the receiver to recover meaning by incomplete or delayed knowledge access. The attack intensity is represented by the retrieval outage probability. During outage periods, the decoder relies on partial knowledge or cached semantic information.

As shown in Fig 6.5(c), the semantic accuracy decreases moderately as the outage probability increases. Unlike the previous two attacks, availability degradation mainly introduces unstable semantic behavior, such as a decrease in the credibility of knowledge, rather than systematic semantic bias. Although physical transmission remains reliable, inconsistent access to knowledge causes fluctuating task performance. This phenomenon demonstrates the semantic performance instability discussed in Section IV.

6.6 Defensive Design Principles for SemCom

Section III identified four distinct attack surfaces within the knowledge plane: knowledge content, activation and injection mechanisms, evolution and synchronisation processes, and cross-layer availability. Because these surfaces arise directly from the architectural decomposition of Section II, defensive

strategies should address each component explicitly rather than relying solely on channel-level protection.

We therefore outline architectural safeguards corresponding to each attack surface. The goal is not to prescribe specific algorithms, but to establish design principles that preserve semantic alignment under adversarial and distributed conditions.

6.6.1 Principle 1: Protecting Knowledge Content Integrity

To mitigate knowledge content compromise (Section III-A), systems need to ensure the integrity and authenticity of stored semantic structures. Because this layer defines the semantic reference shared by encoder and decoder, corruption can induce persistent semantic drift. Content validation pipelines should incorporate provenance tracking, digital signatures, and authenticated updates to prevent unauthorized modification.

For structured knowledge bases, graph consistency checks and anomaly detection can identify suspicious structural perturbations. For embedding-based systems, distributional monitoring can detect abnormal shifts in representation space. Importantly, integrity protection must apply not only to global knowledge repositories but also to local and task-specific knowledge constructions. By establishing verifiable trust in stored semantic structures, systems can reduce the risk of persistent and system-wide semantic drift. In knowledge-based SemCom, content integrity should therefore be treated with the same rigor as model integrity in distributed learning systems.

6.6.2 Principle 2: Securing Knowledge Activation and Injection

To counter manipulation of knowledge activation and injection (Section III-B), defensive design should ensure that retrieval and conditioning pathways cannot be silently biased. Because activation determines which semantic structures influence a specific communication instance, even subtle bias can redirect meaning without altering stored knowledge. Robust retrieval strategies may incorporate redundancy, cross-verification across indices, and adversarially robust similarity measures. Injection interfaces should enforce validation of retrieved knowledge before integration into semantic models, preventing decoy or poisoned structures from disproportionately influencing inference. Separating knowledge storage from activation logic can also improve auditability. By logging retrieval decisions and injection pathways,

systems gain visibility into how semantic interpretations are formed, enabling post hoc detection of anomalous behavior.

6.6.3 Principle 3: Robust Knowledge Evolution and Synchronisation

To prevent semantic misalignment arising from knowledge evolution and synchronisation compromise (Section III-C), version control and compatibility validation must be treated as explicit security objectives. Compatibility negotiation between transceivers should become an explicit protocol layer rather than an implicit assumption. Transceivers may exchange knowledge version identifiers alongside semantic payloads to verify compatibility before interpretation. In heterogeneous or distributed environments, conflict resolution policies and rollback mechanisms are essential to prevent cascading divergence. By formalizing synchronisation assumptions rather than treating shared knowledge as implicit, systems can prevent subtle misalignment caused by version skew.

6.6.4 Principle 4: Ensuring Knowledge Plane Availability and Resilience

To address knowledge plane availability and degradation threats (Section III-D), semantic systems must incorporate resilience mechanisms that maintain operational continuity under partial disruption. Availability of the knowledge plane is not merely a performance concern but a semantic correctness requirement. Redundant knowledge storage, distributed indexing, rate limiting, and graceful degradation strategies can prevent localized failures from cascading into system-wide semantic breakdown. When full knowledge access is unavailable, fallback semantic models with bounded capability may preserve partial functionality [78]. By engineering resilience into the knowledge plane, systems can maintain semantic performance even under resource exhaustion or denial-of-service conditions.

Collectively, these defensive principles highlight that security in SemCom is fundamentally architectural. Protecting symbol transmission alone is insufficient; systems must ensure the integrity, correct activation, consistent evolution, and continuous availability of the knowledge plane that governs meaning. As SemCom systems scale across heterogeneous and distributed environments, knowledge-aware security mechanisms will become as essential as channel coding and encryption in traditional communication architectures.

6.7 Open Challenges and Research Directions

Knowledge-based SemCom introduces a fundamental shift: meaning is no longer determined solely by transmitted symbols, but by the knowledge state that conditions interpretation. While this architecture enables semantic-aware compression and intelligent inference, it also exposes new system-level challenges that remain largely unexplored. We highlight three research directions that are critical for advancing secure and scalable SemCom systems.

6.7.1 Rigorous Models of Semantic Consistency and Divergence

Current communication theory provides rigorous tools for analyzing symbol-level reliability and channel capacity. In contrast, semantic consistency across knowledge-conditioned transceivers lacks a formal foundation. When knowledge states differ, semantic divergence can occur even under error-free symbol transmission, yet there is no widely accepted metric to quantify this divergence.

Future research should develop rigorous mathematical models that characterize semantic compatibility between distributed knowledge states. Such models should define measurable metrics of semantic drift, alignment error, and knowledge-induced distortion. Bridging information-theoretic principles with knowledge-aware semantic representations remains an open challenge. A rigorous framework would enable provable guarantees for semantic alignment under bounded knowledge discrepancies and adversarial conditions.

6.7.2 Knowledge-Aware Security and Trust Architectures

Traditional communication security focuses on protecting transmitted data. In knowledge-based SemCom, however, trust should extend to the knowledge plane itself. This raises foundational questions about governance, provenance, and trust management for evolving knowledge bases.

Open problems include designing secure knowledge update protocols, defining compatibility negotiation mechanisms between heterogeneous transceivers, and establishing distributed trust models for shared semantic resources. Particularly in multi-domain or cross-organisational deployments, ensuring that knowledge evolution remains authenticated, verifiable, and auditable is essential. Developing standardized knowledge-aware security architectures will be crucial as SemCom systems scale across distributed and heterogeneous

environments.

6.7.3 Scalable and Resilient Knowledge Management for Distributed SemCom Systems

As SemCom expands toward edge intelligence, swarm systems, and cross-network collaboration, knowledge management becomes a scalability bottleneck. Synchronizing large and evolving knowledge bases across resource-constrained nodes poses significant efficiency and privacy challenges.

Future systems should support lightweight knowledge synchronisation, partial replication strategies, and privacy-preserving knowledge sharing. Adaptive mechanisms for graceful degradation under incomplete or delayed knowledge updates are equally important. Research is needed to co-design communication protocols and knowledge management layers so that semantic performance remains stable under dynamic, distributed conditions.

Collectively, these challenges suggest that secure SemCom will require new theoretical foundations, protocol innovations, and system-level co-design between communication engineering and knowledge management. Addressing these open problems will be essential for realizing robust, trustworthy, and scalable knowledge-based SemCom architectures.

6.8 Conclusion

Knowledge-based semantic communication represents a fundamental shift in system design, where meaning rather than symbols becomes the primary object of protection. As knowledge repositories and synchronisation processes are embedded directly into encoding and decoding pipelines, the knowledge plane emerges as a semantic control layer governing cross-transceiver interpretation. This architectural evolution expands the security surface beyond the physical channel: compromise of knowledge content, manipulation of activation mechanisms, synchronisation breakdown, or degradation of knowledge infrastructure can induce semantic failures even when symbol transmission remains correct. Our architectural analysis, threat taxonomy, and version-divergence case study demonstrate that agreement on bits does not guarantee agreement on meaning and that such failures are difficult to detect using conventional integrity mechanisms. Secure semantic communication therefore requires safeguarding the integrity, consistency, and availability of the knowledge plane itself, which will become as fundamental as channel coding and encryption in next-generation distributed communication systems.

Chapter 7

Conclusions and Future Directions

Knowledge has become an indispensable resource for semantic understanding, reasoning, and intelligent decision-making. At the same time, the increasing utilisation of knowledge also introduces new challenges in secure semantic transmission, privacy protection, and knowledge management. Therefore, developing secure and knowledge-centric SemCom has become an important research direction for future intelligent communication networks.

This thesis investigated secure knowledge-assisted SemCom from the perspectives of semantic transmission, knowledge utilisation, and knowledge management. First, a secure semantic transmission framework was studied to improve communication reliability while protecting semantic information from potential attacks and information leakage. By jointly considering semantic fidelity and transmission security, the proposed approach provides a secure foundation for semantic information exchange in intelligent communication systems.

Second, this thesis investigated secure knowledge utilisation in SemCom. As knowledge gradually evolves from an auxiliary resource to a core component of SemComs, ensuring its trustworthy utilisation becomes increasingly important. This work explored secure knowledge interaction mechanisms that enable communication entities to effectively exploit shared knowledge while reducing potential security and privacy risks. The proposed framework enhances semantic understanding and communication intelligence without compromising the security of knowledge resources.

Finally, this thesis focused on knowledge management for secure SemCom. As future SemCom systems become increasingly distributed and collaborative, knowledge must be continuously acquired, shared, updated, and maintained among multiple communication entities. To address this chal-

lenge, this thesis investigated efficient knowledge management mechanisms that improve knowledge availability and semantic consistency while supporting secure semantic collaboration. These studies provide a foundation for scalable knowledge-centric SemCom and demonstrate the importance of integrating knowledge management into future SemCom networks.

Overall, this thesis establishes a systematic research framework for secure knowledge-enabled SemCom by connecting secure semantic transmission, secure knowledge utilisation, and knowledge management into a unified perspective. The proposed studies not only improve the security and intelligence of SemCom but also provide valuable insights for the development of future AI-native communication networks, where knowledge becomes a native communication resource and security is embedded throughout the entire knowledge lifecycle.

7.1 Future Directions

Although significant progress has been achieved in knowledge-enabled SemCom, many open problems remain to be addressed before large-scale practical deployment. Future research is expected to further integrate artificial intelligence, knowledge, and communication technologies to build more intelligent, secure, and autonomous communication systems. Several promising research directions are outlined as follows.

7.1.1 Foundation Models for Knowledge-Assisted SemCom

Recent advances in foundation models have significantly expanded the capability of semantic understanding and reasoning. Future SemCom systems are expected to exploit large language models and multimodal foundation models as universal knowledge repositories to support semantic encoding, semantic decoding, and intelligent semantic reasoning. Integrating foundation models into communication systems can greatly improve semantic generalisation and adaptability across diverse communication scenarios. However, efficiently deploying large models under communication and computation constraints remains a challenging problem that requires joint optimisation of communication and artificial intelligence.

7.1.2 Adaptive and Autonomous Knowledge Management

Knowledge in future SemCom systems will become increasingly dynamic and distributed. Rather than relying on static knowledge repositories, communication entities should continuously acquire, update, and maintain knowledge according to changing communication environments and application requirements. Adaptive knowledge management mechanisms capable of knowledge evolution, synchronisation, and collaborative maintenance will become essential for ensuring semantic consistency and communication reliability in large-scale intelligent communication networks.

7.1.3 Collaborative Multi-Agent SemCom

Future communication networks will consist of multiple intelligent communication entities that cooperate to accomplish complex semantic tasks. Instead of independent point-to-point communications, semantic collaboration among multiple agents will become a fundamental communication paradigm. Efficient coordination of distributed knowledge, semantic reasoning, and collaborative decision-making will therefore become important research topics. Developing scalable multi-agent SemCom frameworks capable of supporting secure and intelligent semantic collaboration will further improve communication efficiency and network intelligence.

7.1.4 AI-Native Knowledge-Centric Communication Networks

Looking beyond current SemCom architectures, future communication networks are expected to evolve toward AI-native systems in which artificial intelligence and knowledge are integrated into every layer of network operation. knowledge will become a native communication resource that supports semantic understanding, network optimisation, resource allocation, and autonomous decision-making. In such networks, communication, computing, artificial intelligence, and knowledge management will be jointly optimized to provide intelligent communication services. Developing unified theoretical frameworks and practical architectures for AI-native knowledge-centric communication networks will therefore remain an important long-term research direction.

In conclusion, future SemCom will continue evolving from semantic-aware communication toward knowledge-centric intelligent communication. By jointly

addressing semantic transmission, secure knowledge utilisation, and adaptive knowledge management, next-generation communication systems will be capable of providing secure, intelligent, and autonomous communication services for a wide range of emerging applications. The research presented in this thesis provides a step toward this vision and offers a foundation for future investigations into secure knowledge-enabled SemCom.

Bibliography

[1] S. Guo, A. Zhang, Y. Wang, C. Feng, and T. Q. Quek, "Semantic-enabled 6g communication: A task-oriented and privacy-preserving perspective," *IEEE Network*, 2025.

[2] X. Liu, Y. Sun, R. Cheng, L. Xia, H. Abumarshoud, L. Zhang, and M. A. Imran, "Knowledge-assisted privacy preserving in semantic communication," *IEEE Wireless Communications*, vol. 32, no. 2, pp. 76–83, 2025.

[3] X. Xu, H. Xiong, Y. Wang, Y. Che, S. Han, B. Wang, and P. Zhang, "Knowledge-enhanced semantic communication system with ofdm transmissions," *Science China Information Sciences*, vol. 66, no. 7, p. 172302, 2023.

[4] W. Chen, S. Tang, Q. Yang, Z. Shi, and D. Niyato, "Enhancing privacy in semantic communication over wiretap channels leveraging differential privacy," *arXiv preprint arXiv:2504.18581*, 2025.

[5] C. Chen, F. Zheng, J. Cui, Y. Cao, G. Liu, J. Wu, and J. Zhou, "Survey and Open Problems in Privacy-Preserving Knowledge Graph: Merging, Query, Representation, Completion, and Applications," *International Journal of Machine Learning and Cybernetics*, pp. 1–20, 2024.

[6] W. Chen, S. Tang, and Q. Yang, "Enhancing image privacy in semantic communication over wiretap channels leveraging differential privacy," in *2024 IEEE 34th International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 2024, pp. 1–6.

[7] D. Won, G. Woraphonbenjakul, A. B. Wondmagegn, A. Tran, D. Lee, D. S. Lakew, and S. Cho, "Resource management, security, and privacy issues in semantic communications: A survey," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 3, pp. 1758–1797, 2024.

[8] X. Liu, Y. Liu, H. Tang, F. Zhao, L. Xia, and Y. Sun, "Joint knowledge and power management for secure semantic communication networks," *IEEE Transactions on Vehicular Technology*, 2025.

[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] P. Yi, Y. Cao, X. Kang, and Y.-C. Liang, "Semantic communication systems with a shared knowledge base," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2023, pp. 1374–1379.

[11] S. Jiang, Y. Liu, Y. Zhang, P. Luo, K. Cao, J. Xiong, H. Zhao, and J. Wei, "Reliable semantic communication system enabled by knowledge graph," *Entropy*, vol. 22, no. 6, p. 846, 2022.

[12] B. Wang, R. Li, J. Zhu, Z. Zhao, and H. Zhang, "Knowledge enhanced semantic communication receiver," *IEEE Communications Letters*, vol. 27, no. 7, pp. 1794–1798, 2023.

[13] W. Wu, F. Zhou, and Q. Wu, "Knowledge graph based explainable and generalized zero-shot semantic communications," 2025.

[14] D. Wheeler and B. Natarajan, "Knowledge-driven semantic communication enabled by the geometry of meaning," 2023.

[15] X. Ren *et al.*, "Knowledge base enabled semantic communication: A generative perspective," 2023.

[16] X. Liu *et al.*, "Kgrag-sc: Knowledge graph rag-assisted semantic communication," 2025.

[17] Z. Fang *et al.*, "Enhancing reasoning ability in semantic communication through generative ai-assisted knowledge construction," *IEEE Wireless Communications Letters*, 2024.

[18] J. A. Zhang *et al.*, "A genai-driven framework for context-aware semantic communication in digital twin networks," *IEEE Internet of Things Journal*, 2026.

[19] E. C. Strinati *et al.*, "The network that thinks: Kraken and the dawn of cognitive 6g," 2026.

[20] P. Zhang, Y. Liu, Y. Song, and J. Zhang, "Advances and challenges in semantic communications: A systematic review," *National Science Open*, vol. 3, no. 4, pp. 172–207, 2024.

[21] Y. E. Sagduyu, S. Ulukus, and A. Yener, "Is semantic communication secure? a tale of multi-domain adversarial attacks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 12, pp. 3672–3686, 2023.

[22] M. Shen, J. Wang, H. Du, D. Niyato, X. Tang, J. Kang, Y. Ding, and L. Zhu, "Secure semantic communications: Challenges, approaches, and opportunities," *IEEE Network*, vol. 38, no. 4, pp. 197–206, 2024.

[23] S. Guo, Y. Wang, N. Zhang, Z. Su, T. H. Luan, Z. Tian, and X. Shen, "A survey on semantic communication networks: Architecture, security, and privacy," *IEEE communications surveys & tutorials*, vol. 27, no. 5, pp. 2860–2894, 2024.

[24] Y. Li, Z. Shi, H. Hu, Y. Fu, H. Wang, and H. Lei, "Secure semantic communications: From perspective of physical layer security," *IEEE Communications Letters*, vol. 28, no. 11, pp. 2607–2611, 2024.

[25] H. Jiang, C. Dong, H. Liang, X. Xu, Y. Liu, Z. Zheng, and P. Zhang, "Model-hopping semantic communication system for a reliable and secure transmission," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 4521–4534, 2025.

[26] Y. Wang, S. Guo, Y. Deng, H. Zhang, and Y. Fang, "Privacy-preserving task-oriented semantic communications against model inversion attacks," *IEEE Transactions on Wireless Communications*, vol. 23, no. 8, pp. 10 150–10 165, 2024.

[27] W. Zhao, Q. Pang, Y. Sun, X. Li, and B. Li, "Secure federated semantic communication with model division multiple access against gradient inversion attacks," *IEEE Wireless Communications Letters*, vol. 15, no. 2, pp. 1310–1314, 2026.

[28] C. Liang, H. Du, Y. Sun, D. Niyato, J. Kang, D. Zhao, and M. A. Imran, "Generative AI-driven Semantic Communication Networks: Architecture, Technologies and Applications," *IEEE Transactions on Cognitive Communications and Networking*, 2024.

[29] F. Zhao, Y. Sun, L. Feng, L. Zhang, and D. Zhao, "Enhancing Reasoning Ability in Semantic Communication through Generative AI-Assisted Knowledge Construction," *IEEE Communications Letters*, 2024.

[30] Z. Yang, M. Chen, G. Li, Y. Yang, and Z. Zhang, "Secure Semantic Communications: Fundamentals and Challenges," *IEEE Network*, 2024.

[31] H. Du, J. Wang, D. Niyato, J. Kang, Z. Xiong, M. Guizani, and D. I. Kim, "Rethinking Wireless Communication Security in Semantic Internet of Things," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 36–43, 2023.

[32] B. Pinkas, T. Schneider, and M. Zohner, "Scalable Private Set Intersection Based on OT Extension," *ACM Transactions on Privacy and Security (TOPS)*, vol. 21, no. 2, pp. 1–35, 2018.

[33] Y. Cao, C. Jin, Y. Tang, and Z. Wei, "Word Sense Disambiguation Combining Knowledge Graph and Text Hierarchical Structure," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 23, no. 12, pp. 1–16, 2024.

[34] Q. Wang, Z. Mao, B. Wang, and L. Guo, "Knowledge Graph Embedding: A Survey of Approaches and Applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 12, pp. 2724–2743, 2017.

[35] J. Li, A. Sun, J. Han, and C. Li, "A Survey on Deep Learning for Named Entity Recognition," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 1, pp. 50–70, 2020.

[36] H. Zhang, B. Wu, X. Yuan, S. Pan, H. Tong, and J. Pei, "Trustworthy Graph Neural Networks: Aspects, Methods, and Trends," *Proceedings of the IEEE*, vol. 112, no. 2, pp. 97–139, 2024.

[37] S. Pan, L. Luo, Y. Wang, C. Chen, J. Wang, and X. Wu, "Unifying Large Language Models and Knowledge Graphs: A Roadmap," *IEEE Transactions on Knowledge and Data Engineering*, 2024.

[38] B. Yang, W.-t. Yih, X. He, J. Gao, and L. Deng, "Embedding Entities and Relations for Learning and Inference in Knowledge Bases," *arXiv preprint arXiv:1412.6575*, 2014.

[39] L. Xia, Y. Sun, D. Niyato, D. Feng, L. Feng, and M. A. Imran, "xURLLC-Aware Service Provisioning in Vehicular Networks: A Semantic Communication Perspective," *IEEE Transactions on Wireless Communications*, vol. 23, no. 5, pp. 4475–4488, 2024.

[40] Y. Wu, Y. Chen, L. Wang, Y. Ye, Z. Liu, Y. Guo, and Y. Fu, "Large Scale Incremental Learning," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 374–382.

[41] X. Luo, Z. Chen, M. Tao, and F. Yang, "Encrypted semantic communication using adversarial training for privacy preserving," *IEEE Communications Letters*, vol. 27, no. 6, pp. 1486–1490, 2023.

[42] H.-L. Qin, J. Dai, G. Lu, S. Shao, S. Wang, T. Xu, W. Zhang, P. Zhang, and K. B. Letaief, "Generative ai meets 6g and beyond: Diffusion models for semantic communications," *IEEE Communications Surveys & Tutorials*, 2026.

[43] W. Chen, Q. Yang, Y. Jia, J. Pan, S. Shao, J. Dai, M. Tao, and P. Zhang, "Secure digital semantic communications: Fundamentals, challenges, and opportunities," *IEEE Network*, 2026.

[44] E. Grassucci, S. Barbarossa, and D. Comminiello, "Generative semantic communication: Diffusion models beyond bit recovery," *IEEE Transactions on Cognitive Communications and Networking*, 2026.

[45] G. Jiang, S. Han, X. Xu, W. Zhang, and P. Zhang, "Task-oriented cloud-edge-device collaborative semantic communication: Trade-off between privacy-preserving and qoais," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 11 134–11 149, 2025.

[46] D. Cao, J. Wu, and A. K. Bashir, "Multimodal large language models driven privacy-preserving wireless semantic communication in 6g," in *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2024, pp. 171–176.

[47] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[48] S. L. Garfinkel, J. M. Abowd, and S. Powazek, "Issues encountered deploying differential privacy," in *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, 2018, pp. 133–137.

[49] S. Guo, A. Zhang, Y. Wang, C. Feng, and T. Q. Quek, "Trustworthy semantic-enabled 6g communication: A task-oriented and privacy-preserving perspective," *Authorea Preprints*, 2024.

[50] Y. E. Sagduyu, T. Erpek, A. Yener, and S. Ulukus, "Privacy-preserving semantic communications via multi-task learning and adversarial perturbations," *IEEE Network*, 2026.

[51] S. Cheng, X. Zhang, Y. Sun, Q. Cui, and X. Tao, "Knowledge discrepancy oriented privacy preserving for semantic communication," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 8, pp. 11 637–11 646, 2024.

[52] F. Qiao, Z. Li, and Y. Kong, "A privacy-aware and incremental defense method against gan-based poisoning attack," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1708–1721, 2023.

[53] L. Zhao, D. Wu, and L. Zhou, "Data utilization versus privacy protection in semantic communications," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 44–50, 2023.

[54] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[55] Y. E. Sagduyu, T. Erpek, A. Yener, and S. Ulukus, "Semantic leakage and privacy preservation in relay-assisted semantic communications," *arXiv preprint arXiv:2606.31973*, 2026.

[56] S. Kumi, M. Ray, C. A. Cann, R. K. Lomotey, and R. Deters, "Privacy-aware health digital twins using centralized differential privacy and tabular vae," in *2026 IEEE World AI IoT Congress (AIIoT)*. IEEE, 2026, pp. 0313–0319.

[57] M. Mohammadi, M. Vejdanihemmat, M. Lotfinia, M. Rusu, D. Truhn, A. Maier, and S. Tayebi Arasteh, "Differential privacy for medical deep learning: methods, tradeoffs, and deployment implications," *npj Digital Medicine*, 2026.

[58] Y. Wei, Q. Huang, J. T. Kwok, and Y. Zhang, "Kicgptv2: Large language model with knowledge in context for knowledge graph completion," *IEEE Transactions on Knowledge and Data Engineering*, 2026.

[59] R. Zhu, C. Shimizu, S. Stephen, C. K. Fisher, T. Thelen, K. Currier, K. Janowicz, P. Hitzler, M. Schildhauer, W. Li *et al.*, "The knowwhere-graph: A large-scale geo-knowledge graph for interdisciplinary knowledge discovery and geo-enrichment," *Transactions in GIS*, vol. 30, no. 1, p. e70184, 2026.

[60] A. Chambolle, "An algorithm for total variation minimization and applications," *Journal of Mathematical imaging and vision*, vol. 20, no. 1, pp. 89–97, 2004.

[61] A. Chambolle, V. Caselles, D. Cremers, M. Novaga, T. Pock *et al.*, "An introduction to total variation for image analysis," *Theoretical foundations and numerical methods for sparse recovery*, vol. 9, no. 263-340, p. 227, 2010.

[62] T. Chan, S. Esedoglu, F. Park, Yip, A *et al.*, "Recent developments in total variation image restoration," *Mathematical Models of Computer Vision*, vol. 17, no. 2, pp. 17–31, 2005.

[63] J. Liang, Z. Huang, and Y. Chen, "Low-dimensional adaptation of diffusion models: Convergence in total variation," *arXiv preprint arXiv:2501.12982*, 2025.

[64] C. R. Vogel and M. E. Oman, "Iterative methods for total variation denoising," *SIAM Journal on Scientific Computing*, vol. 17, no. 1, pp. 227–238, 1996.

[65] J. M. Fadili and G. Peyré, "Total variation projection with first order schemes," *IEEE Transactions on Image Processing*, vol. 20, no. 3, pp. 657–669, 2010.

[66] M. Kroll, "On density estimation at a fixed point under local differential privacy," 2021.

[67] G. Barthe, R. Chadha, V. Jagannath, A. P. Sistla, and M. Viswanathan, "Deciding differential privacy for programs with finite inputs and outputs," in *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, 2020, pp. 141–154.

[68] S. Asoodeh, M. Aliakbarpour, and F. P. Calmon, "Local differential privacy is equivalent to contraction of an f-divergence," in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 545–550.

[69] A. Bertazzi, T. Johnston, G. O. Roberts, and A. Durmus, "Differential privacy guarantees of markov chain monte carlo algorithms," *arXiv preprint arXiv:2502.17150*, 2025.

[70] Y. Jiang, X. Chang, Y. Liu, L. Ding, L. Kong, and B. Jiang, "Gaussian differential privacy on riemannian manifolds," *Advances in Neural Information Processing Systems*, vol. 36, pp. 14 665–14 684, 2023.

[71] G. Beigi, A. Mosallanezhad, R. Guo, H. Alvari, A. Nou, and H. Liu, "Privacy-aware recommendation with private-attribute protection using adversarial learning," in *Proceedings of the 13th International Conference on Web Search and Data Mining*, 2020, pp. 34–42.

[72] X. Xu, X. Liu, X. Yin, S. Wang, Q. Qi, and L. Qi, "Privacy-aware offloading for training tasks of generative adversarial network in edge computing," *Information Sciences*, vol. 532, pp. 1–15, 2020.

[73] K. Li, G. Luo, Y. Ye, W. Li, S. Ji, and Z. Cai, "Adversarial privacy-preserving graph embedding against inference attack," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6904–6915, 2020.

[74] J. J. Hathaliya, S. Tanwar, and P. Sharma, "Adversarial learning techniques for security and privacy preservation: A comprehensive review," *Security and Privacy*, vol. 5, no. 3, p. e209, 2022.

[75] Q. Ye, J. Li, K. Qu, W. Zhuang, X. S. Shen, and X. Li, "End-to-end quality of service in 5G networks: Examining the effectiveness of a network slicing framework," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 65–74, 2018.

[76] V. Niazmand and Q. Ye, "Joint task offloading, DNN pruning, and computing resource allocation for fault detection with dynamic constraints in industrial IoT," *IEEE Transactions on Cognitive Communications and Networking*, 2025.

[77] W. Zhuang, Q. Ye, F. Lyu, N. Cheng, and J. Ren, "SDN/NFV-empowered future IoV with enhanced communication, computing, and caching," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 274–291, 2019.

[78] Y. Sun, L. Zhang, L. Guo, J. Li, D. Niyato, and Y. Fang, "S-RAN: Semantic-aware radio access networks," *arXiv preprint arXiv:2407.11161*, 2024.

[79] H. Du, J. Wang, D. Niyato, J. Kang, Z. Xiong, M. Guizani, and D. I. Kim, "Rethinking wireless communication security in semantic Internet of Things," *IEEE Wireless Communications*, vol. 30, no. 3, pp. 36–43, 2023.

[80] L. Xia, Y. Sun, C. Liang, L. Zhang, M. A. Imran, and D. Niyato, "Generative AI for semantic communication: Architecture, challenges, and outlook," *IEEE Wireless Communications*, 2024.

[81] M. Shen, J. Wang, H. Du, D. Niyato, X. Tang, J. Kang, Y. Ding, and L. Zhu, "Secure semantic communications: Challenges, approaches, and opportunities," *IEEE Network*, vol. 38, no. 4, pp. 197–206, 2023.

[82] Z. Yang, M. Chen, G. Li, Y. Yang, and Z. Zhang, "Secure semantic communications: Fundamentals and challenges," *IEEE network*, 2024.

[83] L. Xia, Y. Sun, D. Niyato, D. Feng, L. Feng, and M. A. Imran, "xURLLC-aware service provisioning in vehicular networks: A semantic communication perspective," *IEEE Transactions on Wireless Communications*, vol. 23, no. 5, pp. 4475–4488, 2024.

[84] H. Zhang, H. Wang, Y. Li, K. Long, and A. Nallanathan, "DRL-driven dynamic resource allocation for task-oriented semantic communication," *IEEE Transactions on Communications*, vol. 71, no. 7, pp. 3992–4004, 2023.

[85] M. Chein and M.-L. Mugnier, *Graph-based Knowledge Representation: Computational Foundations of Conceptual Graphs*. Springer Science & Business Media, 2008.

[86] X. Luo, H.-H. Chen, and Q. Guo, "Semantic communications: Overview, open issues, and future research directions," *IEEE Wireless Communications*, pp. 1–10, 2022.

[87] S. T. Piantadosi, "Zipf's word frequency law in natural language: A critical review and future directions," *Psychonomic Bulletin & Review*, vol. 21, pp. 1112–1130, 2014.

[88] L. Xia, Y. Sun, D. Niyato, K. Ma, J. Kang, and M. A. Imran, "Knowledge base aware semantic communication in vehicular networks," in *ICC 2023-IEEE International Conference on Communications*. IEEE, 2023, pp. 3989–3994.

[89] N. B. Hassine, D. Marinca, P. Minet, and D. Barth, "Popularity prediction in content delivery networks," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2015, pp. 2083–2088.

[90] G. Li, J. Wu, J. Li, K. Wang, and T. Ye, "Service popularity-based smart resources partitioning for fog computing-enabled industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4702–4711, 2018.

[91] M.-C. Lee, M. Ji, A. F. Molisch, and N. Sastry, "Throughput–outage analysis and evaluation of cache-aided D2D networks with measured popularity distributions," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5316–5332, 2019.

[92] C. Li, C. She, N. Yang, and T. Q. Quek, "Secure transmission rate of short packets with queueing delay requirement," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 203–218, 2021.

[93] G. Lavee, E. Rivlin, and M. Rudzsky, "Understanding video events: A survey of methods for automatic interpretation of semantic occurrences in video," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 39, no. 5, pp. 489–504, 2009.

[94] S. M. Ross, *Introduction to Probability Models*. Academic Press, 2014.

[95] F. Pollaczek, "Über eine Aufgabe der Wahrscheinlichkeitstheorie. I," *Mathematische Zeitschrift*, vol. 32, no. 1, pp. 64–100, 1930.

[96] S. Yang, J. Tian, H. Zhang, J. Yan, H. He, Y. Jin *et al.*, "TransMS: Knowledge graph embedding for complex relations by multidirectional semantics," in *IJCAI*, 2019, pp. 1935–1942.

[97] X. Chen, S. Jia, and Y. Xiang, "A review: Knowledge reasoning over knowledge graph," *Expert Systems with Applications*, vol. 141, p. 112948, 2020.

[98] S. Gao, X. Qin, L. Chen, Y. Chen, K. Han, and P. Zhang, "Importance of semantic information based on semantic value," *IEEE Transactions on Communications*, 2024.

[99] G. Shi, Y. Xiao, Y. Li, and X. Xie, "From semantic communication to semantic-aware networking: Model, architecture, and open problems," *IEEE Communications Magazine*, vol. 59, no. 8, pp. 44–50, 2021.

[100] L. Xia, Y. Sun, C. Liang, D. Feng, R. Cheng, Y. Yang, and M. A. Imran, "WiserVR: Semantic communication enabled wireless virtual reality delivery," *IEEE Wireless Communications*, vol. 30, no. 2, pp. 32–39, 2023.

[101] R. Speer, J. Chin, and C. Havasi, "Conceptnet 5.5: An open multilingual graph of general knowledge," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 31, no. 1, 2017.

[102] C. Fellbaum, "WordNet," in *Theory and Applications of Ontology: Computer Applications*. Springer, 2010, pp. 231–243.

[103] D. Qiao, M. C. Gursoy, and S. Velipasalar, "Secure wireless communication and optimal power control under statistical queueing constraints," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 628–639, 2011.

[104] D. W. K. Ng, E. S. Lo, and R. Schober, "Multiobjective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE transactions on vehicular technology*, vol. 65, no. 5, pp. 3166–3184, 2015.

[105] H. Kellerer, U. Pferschy, and D. Pisinger, "Multidimensional knapsack problems," in *Knapsack Problems*. Springer, 2004, pp. 235–283.

[106] H. Tuy, T. Hoang, T. Hoang, V.-n. Mathématicien, T. Hoang, and V. Mathematician, *Convex Analysis and Global Optimization*. Springer, 1998.

[107] C. H. Papadimitriou and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*. Courier Corporation, 1998.

[108] S. Burer and A. N. Letchford, "Non-convex mixed-integer nonlinear programming: A survey," *Surveys in Operations Research and Management Science*, vol. 17, no. 2, pp. 97–106, 2012.

[109] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[110] S. Boyd, L. Xiao, and A. Mutapcic, "Subgradient methods," *Lecture Notes of EE392o, Stanford University, Autumn Quarter*, vol. 2004, pp. 2004–2005, 2003.

[111] S. Diamond and S. Boyd, "CVXPY: A Python-embedded modeling language for convex optimization," *The Journal of Machine Learning Research*, vol. 17, no. 1, pp. 2909–2913, 2016.

[112] F. Glover, "Tabu search-part I," *ORSA Journal on Computing*, vol. 1, no. 3, pp. 190–206, 1989.

[113] Y. T. Lee, Z. Song, and Q. Zhang, "Solving empirical risk minimization in the current matrix multiplication time," in *Conference on Learning Theory*. PMLR, 2019, pp. 2140–2157.

[114] P. Pawar and A. Trivedi, "Joint uplink-downlink resource allocation for D2D underlaying cellular network," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8352–8362, 2021.

[115] H. Boostanimehr and V. K. Bhargava, "Unified and distributed QoS-driven cell association algorithms in heterogeneous networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1650–1662, 2014.

[116] Q. Ye, W. Zhuang, S. Zhang, A.-L. Jin, X. Shen, and X. Li, "Dynamic radio resource slicing for a two-tier heterogeneous wireless network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9896–9910, 2018.

[117] L. Xia, Y. Sun, D. Niyato, L. Zhang, and M. A. Imran, "Wireless resource optimization in hybrid semantic/bit communication networks," *IEEE Transactions on Communications*, 2024.

[118] G. Carlucci, L. De Cicco, and S. Mascolo, "Controlling queuing delays for real-time communication: The interplay of E2E and AQM algorithms," *ACM SIGCOMM Computer Communication Review*, vol. 46, no. 3, pp. 1–7, 2018.

[119] L. Xia, Y. Sun, H. Sun, R. Q. Hu, D. Niyato, and M. A. Imran, "Joint power and spectrum orchestration for D2D semantic communication underlying energy-efficient cellular networks," *arXiv preprint arXiv:2501.18350*, 2025.

[120] T.-S. Kim and S.-L. Kim, "Random power control in wireless ad hoc networks," *IEEE Communications Letters*, vol. 9, no. 12, pp. 1046–1048, 2005.

[121] C. Guo, L. Liang, and G. Y. Li, "Resource allocation for vehicular communications with low latency and high reliability," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 3887–3902, 2019.

[122] J. Ren, Z. Zhang, J. Xu, G. Chen, Y. Sun, P. Zhang, and S. Cui, "Knowledge base enabled semantic communication: A generative perspective," *IEEE Wireless Communications*, vol. 31, no. 4, pp. 14–22, 2024.

[123] F. Zhou, Y. Li, M. Xu, L. Yuan, Q. Wu, R. Q. Hu, and N. Al-Dhahir, "Cognitive semantic communication systems driven by knowledge graph: Principle, implementation, and performance evaluation," *IEEE Transactions on Communications*, vol. 72, no. 1, pp. 193–208, 2023.

[124] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.

[125] C. Chaccour, W. Saad, M. Debbah, Z. Han, and H. V. Poor, "Less data, more knowledge: Building next-generation semantic communication networks," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 37–76, 2024.

[126] D. Fan, R. Meng, S. Gao, and X. Xu, "Kgrag-sc: Knowledge graph rag-assisted semantic communication," in *2025 lEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2025, pp. 1–7.

[127] X. Zhu, Y. Xie, Y. Liu, Y. Li, and W. Hu, "Knowledge graph-guided retrieval augmented generation," in *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2025, pp. 8912–8924.

[128] S. S. Chaturvedi, G. Bagwe, L. E. Zhang, and X. Yuan, "Aip: Subverting retrieval-augmented generation via adversarial instructional prompt," in *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, 2025, pp. 15 872–15 889.

[129] A. Shafran, R. Schuster, and V. Shmatikov, "Machine against the {RAG}: Jamming {Retrieval-Augmented} generation with blocker documents," in *34th USENIX Security Symposium (USENIX Security 25)*, 2025, pp. 3787–3806.