

Special Topic: Integration of Large AI Model and 6G

On privacy, security, and trustworthiness in distributed wireless large AI models[†]

Zhaohui YANG¹, Wei XU^{2*}, Le LIANG², Yuanhao CUI³,
Zhijin QIN⁴ & Mérouane DEBBAH⁵

¹College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China

²National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

³School of Information and Communication Engineering, Beijing University of Posts and Communications, Beijing 100876, China

⁴Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

⁵Center for 6G Technology, Khalifa University of Science and Technology, Abu Dhabi 127788, United Arab Emirates

Received 15 November 2024/Revised 3 March 2025/Accepted 30 May 2025/Published online 23 June 2025

Abstract Combining wireless communication with large artificial intelligence (AI) models can open up a myriad of novel application scenarios. In sixth generation (6G) networks, ubiquitous communication and computing resources allow large AI models to serve democratic large AI models-related services to enable real-time applications like autonomous vehicles, smart cities, and Internet of Things (IoT) ecosystems. However, the security considerations and sustainable communication resources limit the deployment of large AI models over distributed wireless networks. This paper provides a comprehensive overview of privacy, security, and trustworthiness for distributed wireless large AI model (WLAM). In particular, a detailed privacy and security analysis for distributed WLAM is first revealed. The classifications and theoretical findings about privacy and security in distributed WLAM are discussed. Then the trustworthiness and ethics for implementing distributed WLAM are described. Finally, the comprehensive applications of distributed WLAM are presented in the context of electromagnetic signal processing.

Keywords large AI model, privacy and security, 6G and beyond

Citation Yang Z H, Xu W, Liang L, et al. On privacy, security, and trustworthiness in distributed wireless large AI models. *Sci China Inf Sci*, 2025, 68(7): 170301, <https://doi.org/10.1007/s11432-024-4465-3>

1 Introduction

1.1 Motivation

The integration of wireless communication and artificial intelligence (AI) technologies has revolutionized numerous sectors [1], from healthcare [2] to transportation [3], by facilitating the development of distributed wireless large AI models (WLAM) [4, 5]. WLAM encompasses two aspects: large AI models deployed over wireless networks and large AI models designed to solve wireless communication problems. Large AI models leverage the distributed nature of wireless networks to harness computational resources across diverse devices, enabling advanced data processing and real-time decision-making [6, 7]. However, the proliferation of WLAM introduces unique challenges, particularly in the areas of privacy, security, and trustworthiness.

As data are transmitted across wireless networks, it becomes susceptible to interception and unauthorized access, raising significant privacy concerns [8–11]. To realize distributed WLAM, both federated learning and split learning are two potential driving technologies. In federated learning, for instance, while raw data remain on local devices, model parameters communicated to central servers can still be exploited by adversaries to infer sensitive information [12]. Similarly, in split learning, the partial transmission of data between client and server networks creates potential vulnerabilities [13]. These challenges necessitate robust encryption and privacy-preserving techniques to safeguard user data.

* Corresponding author (email: wxu@seu.edu.cn)

[†] Special Topic: The 27th Annual Meeting of the China Association for Science and Technology

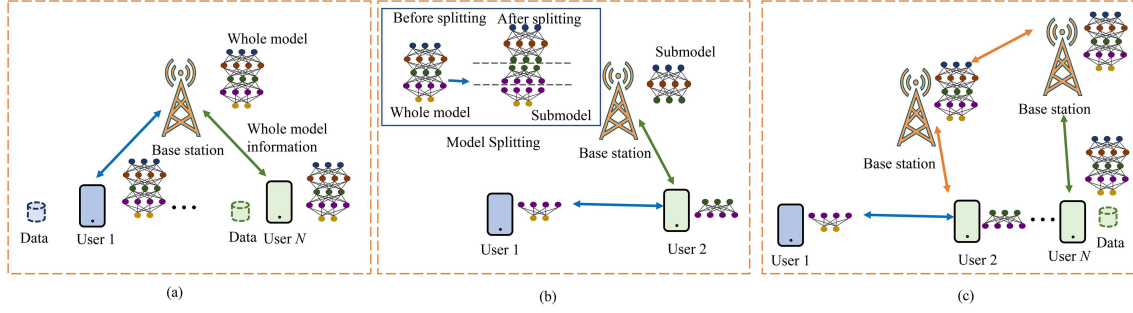


Figure 1 (Color online) Potential classifications of distributed WLAM. (a) Data distribution; (b) model distribution; (c) hybrid architecture.

Moreover, the security of WLAM systems is paramount. Distributed models must be resilient against adversarial attacks that could compromise model integrity or manipulate outcomes. In WLAM, the model is powerful, and a large amount of data is obtained, which can introduce security concerns. Thus, it is required that models are not only secure but also transparent and accountable, which is essential for fostering user trust. In addition, the ethical deployment of WLAM involves addressing biases and ensuring fairness in AI-driven decisions [14], making trustworthiness a multifaceted challenge.

1.2 Classifications of WLAM

WLAM can be broadly categorized into data distribution and model distribution approaches, as shown in Figure 1, each offering distinct advantages and challenges.

- **Data distribution.** This approach involves distributing datasets across multiple devices, as shown in Figure 1(a). Federated learning is a prime example, enabling devices to independently train local models and share updates with a central server [15]. By transmitting only model updates rather than raw data, this method enhances privacy [16]. However, it relies on sophisticated aggregation algorithms to ensure accurate global model convergence without leaking sensitive information. This balance between privacy and performance is a critical focus of ongoing research [17].

- **Model distribution.** In contrast, model distribution involves dividing the large AI model itself across different devices, as shown in Figure 1(b). Split learning exemplifies this approach, where segments of the model are trained on separate devices [18]. This method divides the original model into smaller sub-models, reducing the computational load on individual devices. However, the model distribution method requires secure protocols for transmitting intermediate data and integrating model components, as partial data exchanges can expose vulnerabilities [19]. Ensuring the seamless integration of distributed model components remains a significant technical challenge.

- **Hybrid architecture.** The hybrid architecture combines both data distribution and model distribution. In hybrid architecture, the devices with low computation capacity collaboratively train the model using split learning, while the devices with high computation capacity can cooperatively train the whole model using federated learning. This kind of architecture usually leads to the heterogeneous networks as shown in Figure 1(c).

Both data distribution and model distribution methods aim to maximize the efficiency of distributed resources while mitigating the inherent risks associated with wireless data transmission and model deployment.

Compared to traditional edge AI, there are three kinds of main difference of privacy, security, and trustworthiness for WLAM.

(1) Data-layer risk. The characteristics of being data-driven, highly complex in model structure, and having strong uncertainty lead to endogenous technical defects in WLAMs, such as the issue of model hallucinations.

(2) Architecture-layer risk. Due to the deployment in distributed networks, WLAMs face security risks from malicious adversarial attacks, such as model theft attacks, backdoor attacks, and adversarial sample attacks. Besides, training WLAMs typically requires substantial computational power, especially for current large-scale models. These models often involve hundreds of millions to billions of parameters and complex neural network architectures. Coupled with the need for extensive training data and multiple

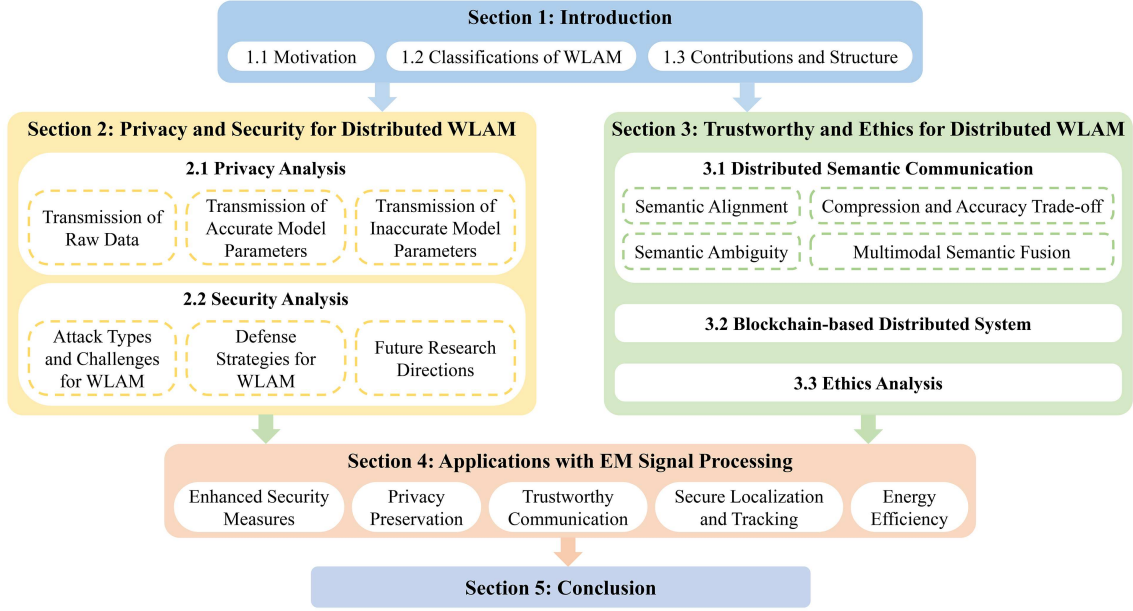


Figure 2 (Color online) Structure of this paper.

rounds of iterative training, executing tasks related to such models becomes a highly time-consuming process.

(3) Application-layer risk. The inherent biases in training data, model design, and the intentions of designers may result in ethical and compliance issues when WLAMs are applied, such as discrimination or value alignment problems.

1.3 Contributions and structure

This paper provides an in-depth exploration of the privacy, security, and trustworthiness aspects of WLAM, offering insights into their implementation and challenges. Our contributions are as follows.

- We have provided unique properties of WLAM compared to traditional edge AI in terms of privacy, security, and trustworthiness.
- We have provided the mathematical models for privacy enhanced WLAM for transmitting inaccurate model parameters.
- We have summarized the attack types, challenges, and defense strategies for WLAM.
- We have discussed the trustworthy strategies for distributed WLAM through introducing distributed semantic communication and blockchain-based distributed systems.

The structure of this paper, as shown in Figure 2, is organized to facilitate a comprehensive understanding of these topics. Section 2 delves into privacy and security strategies for distributed WLAM, providing detailed analyses and case studies. Section 3 addresses the challenges of building trustworthy systems, exploring ethical considerations and proposing solutions. Section 4 concludes with a discussion on potential applications and future research directions, highlighting the importance of continued innovation in secure and ethical WLAM development.

2 Privacy and security for distributed WLAM

This section explores a range of privacy-preserving techniques, including differential privacy, homomorphic encryption, and secure federated learning. These methods are critically evaluated for their effectiveness in protecting data while maintaining model accuracy. We propose algorithms that incorporate noise addition and data obfuscation to enhance privacy without compromising performance. Our analysis highlights the trade-off between privacy protection and computational efficiency, providing guidelines for selecting appropriate strategies based on specific application needs. Besides, this paper examines advanced security strategies, and the methods to defend against adversarial attacks and ensure model robustness.

2.1 Privacy analysis

In WLAM, model pre-training and fine-tuning require extensive data collection and processing. Although original data can be stored locally, the training data transmitted over wireless communication in WLAM systems remains vulnerable to interception, potentially allowing attackers to recover the original data and compromise privacy. The distributed WLAM system involves significant data interactions between devices and servers, increasing the risk of privacy breaches. For example, in federated learning, local model parameters are uploaded from the client to the server [20], and in split learning, partially processed data are transmitted from the client network to the main server-side network, both of which are vulnerable to privacy risks.

To protect the data privacy of the users during model training, encryption of transmitted information can prevent attackers from accessing the original data. This encryption can be categorized into three levels, raw data, accurate model parameters, and inaccurate model parameters.

Transmission of raw data. The most basic privacy protection measure is to use privacy protection techniques such as physical layer security algorithms including artificial noise based secure beamforming to safeguard raw data transmitted between distributed users and servers. While this approach relies on the accurate channel gains, it offers limited privacy protection, making it possible for attackers to access raw data directly.

Transmission of accurate model parameters. Beyond direct data transmission, model parameters can be transmitted to enhance privacy. Through aggregation algorithms, global model parameters can be generated from sample data distributed across distributed users, thereby preventing direct access to the original data. Some existing model aggregation algorithms achieve performance similar to those of centralized machine learning [21]. Additionally, transmitting model parameter data require less bandwidth than raw data, conserving communication resources and building an energy-efficient WLAM system. However, attackers may exploit model parameters by constructing neural networks to reconstruct the original data, thereby posing a risk of privacy leakage. To handle this issue, this paper proposes a personalized federated learning and privacy protection algorithm based on information fusion. Privacy protection is achieved by adding noise according to user preferences and retaining the final layer locally to enhance data confidentiality. The proposed algorithm maintains a level of accuracy comparable to that of unencrypted cases while enhancing privacy.

Transmission of inaccurate model parameters. To prevent privacy breaches, original model parameters can be obfuscated by transmitting inaccurate model parameters. Due to transmitting inaccurate model parameters, the mapping of raw data and transmitted model parameters is converted from one-to-one to one-to-many or many-to-one. Thus, it becomes more difficult for the attackers to recover raw data. Typical inaccurate model parameters transformation methods include linear and nonlinear transformations.

For linear transformations, an example is adding artificial noise to model parameters:

$$g_i(\nabla f_i(x)) = \nabla f_i(x) + n_i, \quad (1)$$

where x is the original data, $\nabla f_i(x)$ is the gradient of the local model parameters to be transmitted, $g_i(\nabla f_i(x))$ is the transformed inaccurate gradient information, and n_i is the artificially added noise. The noise power increases linearly, whereas the gradient amplitude power grows quadratically. Therefore, when there are many users, an accurate global model can be obtained, allowing the federated learning process to converge effectively.

For nonlinear transformations, typical methods include quantized gradient, gradient encoding, and encryption algorithm.

• **Quantized gradient.** This method involves quantizing gradient information. One way of constructing the binary quantized gradient can be given by

$$g_i(\nabla f_i(x)) = \begin{cases} 1, & \nabla f_i(x) \geq 0, \\ -1, & \text{else.} \end{cases} \quad (2)$$

Convergence in model training is achieved by transferring only the gradient descent direction. The work in [22] used random lattice-based vector quantization to add noise to transmitted parameters, avoiding common privacy leakage attacks without significantly affecting performance.

- **Gradient encoding.** Some users upload only certain gradients, while others upload all gradients collectively. Differential privacy or gradient compression can mitigate gradient-based data reconstruction attacks to some extent but may impact accuracy. In [23], a privacy-preserving federated learning method called privacy-encoded FL is proposed, introducing an entangled nonlinear mapping between model gradients and original data by decomposing weight matrices into sub-matrices. This approach significantly reduces the risk of data reconstruction attacks without degrading performance.

- **Encryption algorithm.** To address privacy issues in WLAM, encryption techniques like differential privacy, multi-party computation, homomorphic encryption, and functional encryption are used. Differential privacy methods can be employed to ensure that individual data cannot be inferred from the aggregate outputs of the model. Homomorphic encryption, on the other hand, enables computation on encrypted data, eliminating the need to share raw data with servers. In [24], a secure federated learning approach is implemented by combining fully homomorphic encryption with FL in Internet of Things (IoT)-enabled smart cities, achieving strong security along with high accuracy, low communication overhead, and reduced latency.

Inaccurate data transmission may hinder learning convergence, while accurate transmission poses privacy risks. Optimizing privacy protection measures by combining communication and computation processes to balance privacy enhancement and convergence speed is a valuable research direction.

2.2 Security analysis

The security of distributed WLAM is crucial. Due to the distributed and dynamic nature of wireless communication networks, WLAM systems are vulnerable to various attacks, which can compromise model integrity, manipulate outputs, or disrupt operations. In this subsection, we discuss the primary security threats faced by WLAM, including model injection attacks, Byzantine attacks, and other adversarial interventions. We also propose innovative countermeasures and highlight future research directions.

2.2.1 Attack types and challenges for WLAM

Data poisoning attacks. For example, data poisoning attacks, in which malicious actors inject false data to mislead the AI model, pose a significant threat to system reliability. A key countermeasure against such attacks involves implementing robust data validation mechanisms to identify and isolate malicious contributions in WLAM.

Model injection attacks and environmental complexity. In wireless distributed scenarios, the complexity of model injection attacks increases significantly due to the dynamic environment. Attackers can exploit the instability of wireless networks or communication delays between nodes to inject malicious data or models, affecting the performance of the global model. Unlike traditional centralized systems, WLAM faces more complex channel conditions, making it challenging to detect malicious injections. For instance, attackers may hijack edge devices and leverage the interference characteristics of multipath channels to inject small perturbations at different intervals, leading to a gradual degradation of model performance, which is difficult to detect. Such progressive injection attacks are particularly covert in real-time applications.

Dynamic Byzantine attacks and adaptive strategies. Traditional Byzantine attacks assume that malicious nodes behave consistently throughout the training process. However, in WLAM, attackers can adopt dynamic Byzantine strategies, where malicious nodes randomly switch between normal and malicious behavior during different training rounds, making attack detection more difficult. To counter such dynamic attacks, a dynamic trust evaluation mechanism can be used, which models the historical behavior of each node probabilistically and employs time series analysis to evaluate node trustworthiness in real-time, thereby better identifying Byzantine nodes with dynamic behavior.

Channel manipulation adversarial attacks. The nature of wireless channels makes adversarial attacks more complex. Attackers can manipulate channel conditions (e.g., gain or fading) to interfere with the training and inference processes of the model. Compared to fixed adversarial perturbations, the uncertainty of wireless channels makes models more vulnerable to channel-level interference. Introducing channel-aware adversarial training, where channel state information is included during training, can enhance robustness against channel interference. Additionally, leveraging multipath transmission and channel randomization techniques can effectively reduce the attacker's control over the channel, thus improving defense against adversarial attacks.

2.2.2 Defense strategies for WLAM

Cross-layer aggregation optimization. To counter Byzantine attacks, a cross-layer collaborative aggregation mechanism is proposed, which combines physical layer channel information and application layer model parameters for dual verification. During model parameter aggregation, anomalies in parameter values are considered alongside channel quality indicators to determine node trustworthiness, thereby improving the security of the aggregation process.

Intelligent aggregator. An intelligent aggregator based on large models is introduced, which uses deep learning techniques to automatically detect abnormal parameter updates. By learning the update patterns of normal nodes, it can identify potential malicious updates. The intelligent aggregator continuously optimizes throughout the training process, enhancing adaptability to attacks.

Adversarial game modeling. The interaction between attackers and defenders can be modeled as a game using the Stackelberg game model from game theory. The defender acts as the leader, predicting the attacker's optimal strategy and making corresponding defense adjustments. In this way, defense strategies can be dynamically adjusted to minimize the impact of potential attacks.

Incentive mechanism design. An incentive mechanism based on game theory is designed to reward honest behavior and penalize malicious behavior, encouraging nodes to follow the protocol and reducing the likelihood of attacks. Considering the resource-constrained nature of wireless networks, a lightweight incentive mechanism can be implemented to ensure practicality.

Collaborative security protection using edge computing. In the context of WLAM, collaboration among edge devices is crucial for enhancing system security. A collaborative edge protection mechanism is proposed, where edge nodes work together to detect and share attack information, enabling distributed detection and response. Leveraging the heterogeneity of edge nodes can improve detection accuracy for different types of attacks.

Channel encryption and privacy protection. By integrating channel encryption and differential privacy in edge computing, data confidentiality during transmission and node privacy can be ensured. This approach effectively prevents man-in-the-middle attacks and reduces privacy-related security risks.

2.2.3 Future research directions

Intelligent adaptive security framework. Develop an intelligent adaptive security framework based on deep reinforcement learning, enabling the system to automatically learn the optimal defense strategy against different types of attacks. By continuously interacting with the environment, the framework can adjust defense measures in real-time to adapt to changing wireless environments and attack patterns.

Enhanced federated adversarial training. An enhanced federated adversarial training method is proposed, which combines channel characteristics and adversarial sample generation. By dynamically generating adversarial samples that consider channel conditions during training, the model's robustness in wireless environments can be improved. This method can enhance defenses against adversarial attacks without significantly increasing computational overhead.

Large model-driven explainable security analysis. Utilizing the powerful reasoning capabilities of large models, develop explainable security analysis tools to monitor and interpret the decision-making process of models in real-time, helping to identify potential attack behaviors. By visualizing the internal state of the model, understanding of attack paths can be improved, thereby enhancing the model's response to security threats.

Blockchain-based trust management system. Introduce lightweight blockchain technology combined with edge computing nodes to build an efficient trust management system. The immutability and transparency of blockchain ensure that the behavior of each node is reliably recorded, thereby enhancing the overall trustworthiness of the system. Additionally, smart contracts can be used to automate node behavior auditing and incentive distribution.

2.2.4 Summary

In WLAM systems, security is a key factor for successful deployment. Compared to traditional methods, innovative countermeasures such as cross-layer collaborative protection, game theory-based adaptive defense, and collaborative security mechanisms using edge computing can more effectively address the unique challenges in wireless environments. In the future, intelligent adaptive security frameworks, enhanced adversarial training, and blockchain-based trust management are expected to improve WLAM

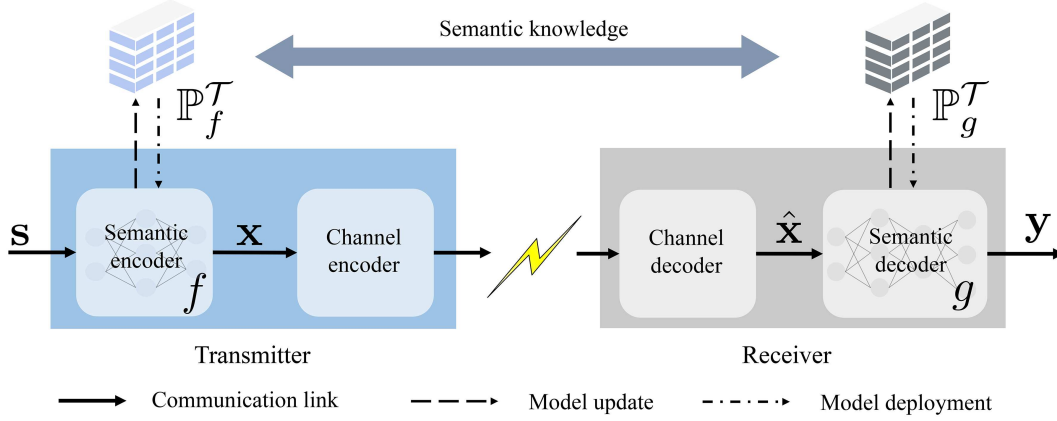


Figure 3 (Color online) Illustration of model distributed semantic communication system.

security and robustness, providing a solid foundation for their practical deployment.

3 Trustworthy and ethics for distributed WLAM

In the landscape of distributed WLAM, it is essential to achieve trustworthiness and ethical standards for secure, reliable, and fair deployment. This section explores trustworthiness and ethical considerations in distributed semantic communication systems, blockchain-based distributed systems, and concludes with an ethical analysis addressing key challenges unique to WLAM. To enhance the trustworthiness for distributed WLAM, distributed semantic communication and blockchain-based distributed systems are two representative approaches.

3.1 Distributed semantic communication

By transmitting the context and intent behind the source data, referred to as semantic information, semantic communication enhances the data transmission efficiency [25]. Given the intractable challenges associated with identifying semantic information for various communication tasks, advanced learning algorithms and model designs—especially large AI models—have been applied to semantic communication, facilitating semantic extraction, transmission, and interpretation [26–28]. Thanks to the escalating computational capabilities of edge devices, they can now easily support and execute learning-based models. By processing semantic extraction locally, the amount of data to be transmitted is reduced, promoting energy-efficient and low-latency communication [29–31].

The general framework of a distributed semantic communication system is presented in Figure 3. The deep learning models, empowered by semantic knowledge, are distributed across the transmitter and receiver, denoted by f and g with parameter sets $\mathbb{P}_f^{\mathcal{T}}$ and $\mathbb{P}_g^{\mathcal{T}}$, respectively. Semantic knowledge can be accumulated during model training for communication task \mathcal{T} , where the optimized model parameter sets, denoted by $\mathbb{P}^{\mathcal{T}}$, encapsulate task-specific knowledge and are distributed to the transmitter and receiver. Using these deep learning models, the transmitter encodes the extracted semantic information \mathbf{x} from the sensed data \mathbf{s} , and the receiver interprets the recovered semantic information $\hat{\mathbf{x}}$ for task inference \mathbf{y} .

In distributed WLAM for semantic communication, trustworthiness is pivotal for accurate and secure transmission of semantic information between transmitter and receiver nodes. To this end, several critical challenges need to be meticulously addressed, arising from the intrinsic characteristics of deep learning and accurate semantic representation of data. Particularly, significant challenges inherent to deep learning models include their tendency to exhibit degraded generalization performance when there is a misalignment of semantic knowledge, as well as the trade-off between computational overhead and communication performance during training and inference. Additionally, challenges related to the accurate semantic representation, including semantic ambiguity and semantic integration of multimodal data, further complicate the deep learning-based semantic communication systems. Large AI models can significantly mitigate these issues by providing robust semantic understanding, efficient compression techniques, and advanced disambiguation and multimodal fusion capabilities, thus improving overall communication performance. These challenges and utilization of large AI models are detailed as follows.

3.1.1 Semantic alignment

Existing deep learning-based semantic communication designs typically build the semantic knowledge for distributed models by training on large-scale datasets containing rich and diverse information. These learning strategies, including end-to-end learning [32] and multi-stage learning [33], ensure effective semantic alignment for specific communication tasks. The distributed models learn together, share knowledge, and improve collectively.

However, deep learning models tailored for specific tasks often face challenges in generalization performance due to misalignment of semantic knowledge between the training and inference phases. This issue arises because models are typically optimized for the specific characteristics of the training data and may not adapt well to novel, unseen inference data with different attributes or distributions. We formalize this discrepancy as a change within the underlying task, expressed by

$$d = \mathbb{E}_{\mathbf{s} \sim p(\mathbf{s})} \mathcal{D} \left(g(f(\mathbf{s}; \mathbb{P}_f^{\mathcal{T}_{\text{pre}}}); \mathbb{P}_g^{\mathcal{T}_{\text{pre}}}), g(f(\mathbf{s}; \mathbb{P}_f^{\mathcal{T}_{\text{new}}}); \mathbb{P}_g^{\mathcal{T}_{\text{new}}}) \right), \quad (3)$$

where d quantifies the discrepancy, $\mathcal{D}(\cdot)$ is a discrepancy measure function that evaluates the difference in semantic knowledge represented by the parameters, $\mathbb{P}^{\mathcal{T}_{\text{pre}}}$ represents the parameter set optimized for the previous task \mathcal{T}_{pre} , and $\mathbb{P}^{\mathcal{T}_{\text{new}}}$ signifies the parameter set optimized for the new task \mathcal{T}_{new} . A large d suggests a larger discrepancy and potential degradation in performance, while a small d indicates greater alignment and potentially better generalization.

In order to achieve semantic alignment, one direct solution is model retraining for each new task; however, this approach is time-consuming, resource-intensive, and impractical in dynamic environments where tasks frequently change. Techniques such as domain adaptation and transfer learning, as applied in [34,35], mitigate these issues by adjusting the model to handle variations in data distribution. However, domain adaptation often requires access to both labeled source data and unlabeled or partially labeled target data, which may be difficult to obtain. Additionally, accurately estimating the shift between the source and target domains can be challenging, especially when the shift is subtle or complex. On the other hand, transfer learning can suffer from overfitting if the model is fine-tuned on a small target dataset, and the pre-trained model's representations may be ineffective if the source task differs too much from the target task. Furthermore, the choice of layers to fine-tune and the learning rate used for fine-tuning can significantly impact the performance of the transferred model.

As efficient solutions, large AI models trained on diverse datasets have the potential to capture a broader range of semantic knowledge, enabling robust understanding and inference of semantic information across various contexts. These models, often referred to as foundation models, are pre-trained on large, varied datasets and can be fine-tuned with fewer resources to adapt to new tasks, thereby mitigating the challenges associated with semantic misalignment.

3.1.2 Semantic compression and accuracy trade-off

In semantic communication, semantic compression facilitates the reduction of data size by removing redundant or less important information, while preserving the most meaningful parts. Semantic accuracy refers to the degree to which the compressed data represent the original semantic meaning. High semantic accuracy ensures that the information conveyed after compression closely matches the original meaning, minimizing information loss and maintaining communication quality. The trade-off between semantic compression and semantic accuracy can be characterized by the following aspects.

- **Compression level v.s. information loss.** As the compression level increases, the amount of information lost also increases. This can lead to a decrease in semantic accuracy, as critical details necessary for the correct interpretation of the information are removed. In the process of semantic recovery, receiving more information means less needs to be inferred, resulting in lower computational energy requirements. However, if too much information is lost during compression, task inference becomes more challenging, potentially leading to errors.

- **Selection space and computational complexity.** The process of selecting appropriate semantic information from a large selection space is computationally intensive [36,37]. The higher the compression ratio, the more difficult it becomes to select the right information, thereby increasing the computational complexity.

To address this trade-off, information-theoretic formulations, optimization methods, and adaptive compression techniques are employed. On one hand, semantic compression and accuracy are characterized

based on information entropy theory, such as the informativeness of the extracted semantic information and the mutual information between the recovered semantic information and task inference [38,39]. Using information-theoretic measures, an information bottleneck (IB)-based optimization problem is formulated to characterize the minimal and sufficient information required for a given task [40]. Specifically, the optimization problems aim to find a compressed representation of the input data that maximally preserves relevant information for predicting the task, while minimizing the amount of irrelevant information. To optimize the IB-based problem, variational inference is typically used to provide a tractable lower bound.

On the other hand, adaptive compression techniques adjust the compression level based on the importance of the information and the context. These techniques apply varying compression levels to different layers of semantic information. Leveraging the powerful ability of large AI models to learn complex representations, these models can efficiently encode and compress semantic information while retaining essential details, as proposed in semantic communication. For instance, context-aware compression dynamically adjusts the compression rate based on the importance of the transmitted information, leveraging the understanding of context by large AI models to optimize performance. In [41], a semantic importance-aware communication scheme is proposed to quantify the importance of each frame and enable priority-based communication based on semantic importance. Generative language models, such as ChatGPT, quantify semantic importance by statistically analyzing the key terms within a frame. In contrast, discriminative language models, such as BERT, define the importance of words/frames based on the semantic loss caused by missing words/frames. By conveying frame importance across various layers, priority-based parameter configurations can be implemented across layers. In [42], during the source compression phase, the initialized weights of the pre-trained language model BART are utilized to integrate the encoder-decoder transformer into the end-to-end SIONNA link-level communication system. Specifically, the AI Source Encoder labels the sentence s as tokens, maps them, and encodes them into a state. The vector quantizer then quantizes the continuous feature vector into discrete indices using the codebook Z . The receiver, using the shared codebook Z , reconstructs the sentence. By utilizing pre-trained weights for initialization, the AI Source Encoder reduces dependence on specific channel conditions and data distributions during training.

3.1.3 Semantic ambiguity

Semantic ambiguity refers to situations where the intended meaning of the transmitted data is unclear or can be interpreted in multiple ways. In wireless communication, it encompasses both linguistic issues, such as polysemy and contextual misinterpretation [43], and technical issues, such as signal degradation and interference [44,45]. Specifically, polysemy occurs when a word or phrase has multiple valid interpretations depending on the context in which it is used. This can be problematic when the context necessary to disambiguate the meaning is not properly conveyed. Even if a word or phrase is unambiguous in itself, the lack of proper context can lead to misinterpretation. Beyond the linguistic aspect, wireless distortion and interference introduce additional challenges related to signal quality. Although these technical issues are not directly related to the linguistic content, they can exacerbate semantic ambiguity by making it more difficult to recover the intended meaning. Robust signal processing algorithms and designs have been widely studied to minimize transmission errors. Therefore, in this section, we will focus on the linguistic issues of semantic ambiguity.

Existing methods for resolving semantic ambiguity include disambiguation protocols or context-specific rules. Specifically, disambiguation protocols offer a structured approach to resolving semantic ambiguity by defining clear and standardized rules for interpreting information. However, overly complex protocols may be challenging to understand and implement, potentially leading to errors or misinterpretations. Context-specific rules offer a more adaptable approach to addressing semantic ambiguity by tailoring interpretations to specific contexts. These rules can be customized to fit the specific needs and conditions of a scenario, thereby improving the accuracy of interpretation. However, the effectiveness of these rules depends heavily on the accuracy and completeness of contextual information. Fixed protocols or rules may lack the flexibility needed to adapt to rapidly changing or unpredictable situations. Furthermore, implementing and maintaining these protocols can require significant resources, including time and effort for training and documentation.

Large AI models can address semantic ambiguity through their context-aware processing capabilities, which allow them to disambiguate information by considering the broader context in which the information is used. Hierarchical representations in deep neural networks capture complex relationships and

contextual dependencies, enabling the model to understand nuanced meanings. Attention mechanisms within these models further enhance their ability to focus on relevant parts of the input, reducing the likelihood of ambiguity. Pretrained models, like transformers such as BERT and GPT, learn generalizable patterns and relationships from large corpora that can aid in disambiguation. By leveraging context-aware processing and attention mechanisms, large AI models can significantly mitigate the challenges posed by semantic ambiguity, enhancing the accuracy and reliability of communication in both static and dynamic environments.

3.1.4 *Multimodal semantic fusion*

Fusing multimodal data in advanced applications, such as metaverse, present a significant challenge due to the heterogeneous nature of these data types [46]. Existing multimodal semantic communication designs not only explore the correlation among modaldata [28, 47], but also consider the influence of the wireless channel for information fusion [48]. Through multimodal data fusion, these designs enhance both data transmission efficiency and task inference performance. However, there are still ongoing challenges related to real-time processing, dependency on accurate contextual information, and the variability of data streams. Especially, the high computational demands of fusing and analyzing multiple data streams can strain the resources of wireless devices, especially those with limited processing power. The performance of multimodal semantic communication systems can degrade significantly if the contextual information is not precise or if data are missing. Furthermore, variations in the quality or availability of different modalities may impact the effectiveness of the system. Addressing these challenges will be crucial for the continued advancement of multimodal semantic communication systems.

Large AI models, particularly those designed for multimodal processing, can effectively handle and fuse different data types, ensuring cohesive and accurate semantic interpretations [49]. These models use shared latent spaces and advanced fusion techniques to seamlessly integrate information from various modalities. Cross-modal embeddings and techniques like cross-modal attention and multimodal fusion layers allow the model to learn joint representations that capture the relationships between different modalities. Adversarial training can ensure that the representations learned by the model are consistent across modalities. Advanced fusion techniques, such as late fusion, early fusion, and hybrid fusion, can integrate information from various modalities at different stages of the processing pipeline, leveraging the strengths of each modality while mitigating their weaknesses. By combining information from multiple modalities, large AI models can achieve a more comprehensive and accurate understanding of the underlying semantics, improving the robustness of the model against noise and missing data. This capability is essential for applications that require a holistic understanding of complex real-world scenarios, such as multimedia analysis, augmented reality, and multimodal dialogue systems.

3.2 **Blockchain-based distributed system**

Blockchain-based distributed systems offer a promising framework for wireless communication networks, particularly for the management and optimization of resources in environments where trust, transparency, and security are essential. In the context of distributed WLAM, blockchain provides a decentralized infrastructure well-suited to handle the complex data and security requirements of these networks. Key elements of blockchain-based systems in wireless settings include nodes functioning as transmitters or receivers, distributed ledgers that record and verify information, consensus mechanisms like proof of stake or practical Byzantine fault tolerance, and smart contracts like automated scripts that enforce rules on the blockchain. Together, these components create a self-sustaining network where nodes collaborate without central authorities, improving resilience, efficiency, and trustworthiness.

In a blockchain-based wireless network, data transmission flows from individual nodes to a shared blockchain ledger, where it is validated through consensus protocols and recorded immutably. This immutability ensures that once data are confirmed, it cannot be tampered with, thereby providing high levels of data authenticity and traceability. Blockchain's decentralized structure not only avoids single points of failure, which are common in centralized systems, but also offers a transparent and verifiable audit trail for every data interaction within the network. Privacy-preserving techniques, such as zero-knowledge proofs, offer solutions for data validation without compromising sensitive information [50]. Smart contracts further automate routine operations based on predefined rules, enabling consistent data handling across nodes without the risk of human error, thus enhancing the network's overall reliability.

Trustworthiness in blockchain-based wireless systems is crucial as it directly impacts the integrity and reliability of data used for decision-making and resource allocation in distributed WLAM. Given the dynamic and heterogeneous nature of wireless networks, data accuracy and consistency are vital, as erroneous or tampered data can disrupt real-time operations and impair model performance. Blockchain's decentralized and immutable framework helps ensure that every transaction and update within the system remains transparent, verifiable, and resistant to unauthorized manipulation, reinforcing user confidence. This trust is essential in privacy-sensitive scenarios, as blockchain's inherent transparency enables data validation without exposing user identities, making it an ideal solution for resource sharing and secure data handling in next-generation wireless networks [51].

However, while blockchain offers significant benefits, maintaining trustworthiness in these systems presents several challenges.

- **Energy consumption.** Traditional blockchain consensus protocols, like proof of work, are resource-intensive and may be impractical for wireless systems with power-constrained nodes, e.g., IoT devices. This limitation necessitates more energy-efficient consensus mechanisms suitable for wireless networks to maintain performance without exhausting device resources, as demonstrated by IoT implementations using the Raft consensus for increased throughput [50].

- **Privacy compliance.** Blockchain's transparency can sometimes conflict with privacy needs, particularly in wireless applications where sensitive or location-specific data is involved. Immutable public ledgers may inadvertently expose user data, making compliance with privacy standards challenging.

- **Security risks.** Although blockchain architecture offers robust security, it is not immune to attacks. For instance, a 51% attack, where a malicious actor gains control of the network's majority computational power, remains a significant threat, especially in wireless networks with heterogeneous nodes of varying security capabilities. The security advantages of blockchain are often tempered by this vulnerability, underscoring the need for complementary security measures within the system [52].

- **Scalability and latency.** Blockchain's consensus mechanisms, while reliable, often lead to slower data processing times. This delay can become a bottleneck as network traffic grows, which is problematic in real-time wireless applications where rapid responses are critical. The issue is especially pertinent in large-scale networks with high device density [53].

To address these challenges, large AI models provide effective solutions that enhance blockchain's functionality and trustworthiness within wireless networks. First, large AI models can optimize consensus protocols by leveraging predictive algorithms to monitor and anticipate network activity, dynamically adjusting protocol parameters to minimize latency and enhance scalability. For instance, AI-enhanced dynamic resource sharing in 6G networks has shown significant improvements in adapting consensus processes to real-time conditions, effectively reducing processing delays without compromising reliability [51]. Second, AI-based security measures can proactively identify and mitigate threats by detecting abnormal network patterns, which is particularly useful for countering attacks. Machine learning models trained on diverse network data can autonomously monitor and flag potential security issues, thus strengthening the overall security of blockchain-based wireless systems [52]. Third, AI models equipped with advanced data compression algorithms can significantly reduce the data loads on wireless networks, promoting scalability while maintaining semantic fidelity. Additionally, privacy-focused AI solutions, like federated learning, allow nodes to process data locally, transmitting only essential insights to the blockchain to maintain user privacy without sacrificing transparency, which is crucial in 5G and 6G wireless IoT networks [53]. By integrating large AI models, blockchain-based distributed wireless systems can overcome critical issues related to scalability, security, and privacy, fostering a trustworthy, resilient, and efficient environment that meets the demands of next-generation wireless AI applications.

3.3 Ethics analysis

In the context of WLAM, ethics center around issues of privacy, fairness, and accountability, given the sensitive nature of data in wireless networks and the extensive interconnectivity among nodes. The high data volume and sensitive information flow in wireless communication amplify these ethical considerations, making it essential to address privacy risks, prevent data misuse, and ensure that model outcomes are unbiased and transparent.

Ethical analysis in distributed WLAM typically involves technical methods, such as differential privacy for protecting user data, fairness checks to avoid biased outcomes, and explainable AI techniques to clarify decision-making processes. In semantic communication systems, ethical analysis prioritizes main-

taining semantic consistency and transparency. For example, fairness checks can ensure that compression algorithms do not introduce bias or information loss that affects certain demographics disproportionately. Ensuring ethical compliance means preserving data accuracy during compression and anonymizing personal data during transmission. In blockchain-based distributed WLAM, ethical analysis emphasizes balancing transparency with privacy requirements. For instance, implementing privacy-preserving cryptographic protocols, such as zero-knowledge proofs, enables nodes to verify transactions without exposing personal information. Additionally, smart contracts must be reviewed and audited to ensure compliance with data protection standards, guaranteeing that automated processes uphold ethical principles. Through these measures, ethical analysis helps WLAM systems align technical performance with broader social values, fostering responsible and fair use across applications.

4 Applications with EM signal processing

The application cases of WLAM include two parts. In the use case about large AI model for wireless network (LAM4Net), large AI model can be used to identify the security of data used for wireless transmission. Besides, WLAM can also be applied to configure the wireless parameters, such as bandwidth, power, and time to protect the security of the wireless network. In the use case of the wireless network for large AI model (Net4LAM), the joint wireless resource and hardware resource allocation can be designed to protect the security of WLAM over wireless networks.

The distributed nature of WLAM offers significant flexibility and robustness for electromagnetic (EM) signal processing. For instance, WLAM can enable real-time beamforming by leveraging the computational power of edge devices to optimize wireless signal transmissions. Moreover, WLAM supports dynamic spectrum management in wireless networks by predicting spectrum availability and efficiently allocating resources.

Besides, EM signal processing [54–56] can significantly enhance the privacy, security, and trustworthiness of distributed WLAM. By leveraging EM properties [57], WLAM systems can achieve secure communication, robust privacy measures, and reliable system integrity, as illustrated in Figure 4. This section delves into these aspects, highlighting their impact and potential advancements.

- **Enhanced security measures.** EM signal processing techniques, such as physical layer security, exploit the inherent characteristics of EM waves to establish secure communication channels. These methods can effectively mitigate risks like eavesdropping and jamming by using techniques such as beamforming [58] and spread spectrum [59]. By dynamically adjusting signal parameters, WLAM systems ensure data integrity and confidentiality, creating robust defenses against potential security threats.

- **Privacy preservation.** Privacy is a critical concern in WLAM systems, especially when dealing with sensitive data. EM signal processing can enhance privacy by implementing techniques like signal obfuscation and masking [60,61]. These methods obscure the data being transmitted, making it difficult for unauthorized entities to intercept and decipher the information. Additionally, the use of differential privacy at the signal level [62] ensures that individual data points remain protected while still allowing for accurate aggregate analysis.

- **Trustworthy communication.** The trustworthiness of WLAM systems relies heavily on the reliability and authenticity of the data being transmitted. EM signal processing contributes to this by enabling secure key distribution and authentication protocols that ensure only authorized devices can communicate within the network. Techniques such as radio frequency (RF) fingerprinting [63] can verify the identity of devices based on their unique signal characteristics, preventing spoofing and unauthorized access.

- **Secure localization and tracking.** EM signal processing facilitates precise and secure localization and tracking, which are vital for applications requiring spatial awareness, such as logistics and augmented reality. By using methods like time-of-flight and RF fingerprinting, WLAM systems can accurately determine the position of devices while maintaining privacy. These techniques ensure that tracking data are securely transmitted and accessed only by authorized entities, safeguarding against potential misuse.

- **Energy efficiency.** While enhancing security, EM signal processing also supports energy efficiency. Techniques such as adaptive modulation and coding adjust signal parameters based on current conditions, reducing power consumption without compromising security. This capability is essential for maintaining the sustainability of large-scale WLAM deployments, ensuring that security measures do not excessively drain device resources.

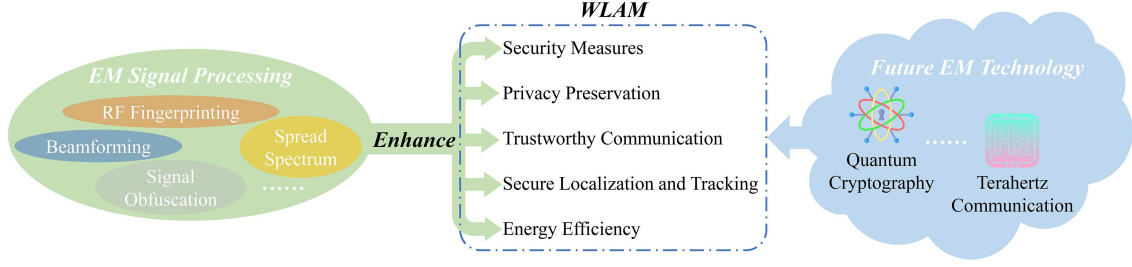


Figure 4 (Color online) Application of EM signal processing in WLAM.

The future of WLAM systems will increasingly depend on advancements in EM signal processing to address evolving privacy and security challenges. Emerging technologies like terahertz communication and quantum cryptography offer promising avenues for further enhancing security protocols. These innovations have the potential to improve the speed, accuracy, and robustness of WLAM applications, ensuring that they remain secure and trustworthy as they adapt to new technological landscapes. Further research is required to develop energy-efficient algorithms capable of operating seamlessly across diverse devices in distributed WLAM systems.

Deploying WLAMs to edge networks involves several steps and considerations to ensure efficient and effective operation. The first step is model optimization. WLAMs are often resource-intensive, which should be optimized for deployment on edge devices with limited computational power and memory. These techniques include model pruning, quantization, and distillation to reduce the model size of WLAMs without significantly compromising performance. The second step is edge device selection. Considering the computation and communication abilities of the edge devices, proper devices are selected to participate in implementing the WLAMs. The third step is model partitioning. Due to limited computation at the edge devices, the model should be properly partitioned and allocated to different edge devices. This can help balance the load and improve performance. The last step is security and privacy. Implement security measures to protect the model and data on edge devices. This includes encrypting data, securing physical layer communication, and cooperative secure transmission.

5 Conclusion and future directions

In this paper, we explored the critical aspects of privacy, security, and trustworthiness in distributed WLAM systems. As the integration of wireless communication and AI continues to advance, addressing these challenges becomes paramount for the successful deployment of WLAM systems. We examined various privacy-preserving techniques, including differential privacy and homomorphic encryption, highlighting their roles in protecting sensitive data. Additionally, we discussed security measures such as physical layer security and blockchain integration, which are essential in safeguarding against potential threats and ensuring data integrity. Furthermore, we emphasized the importance of trustworthiness, focusing on ethical considerations, transparency, and accountability in WLAM systems. By addressing biases and ensuring fairness, we can foster greater user trust and confidence in AI-driven decisions. Looking ahead, ongoing research and innovation in EM signal processing and AI will be crucial in overcoming the challenges associated with WLAM systems. By continuing to develop robust privacy, security, and trustworthiness frameworks, we can unlock the full potential of WLAM, paving the way for more intelligent, secure, and ethical wireless networks.

In conclusion, WLAM offers a promising framework for integrating AI with wireless communication systems, though it necessitates addressing inherent security and privacy challenges. Advancements in cryptographic techniques and distributed algorithms will be pivotal in overcoming these challenges and unlocking the full potential of WLAM. Despite its potential, significant challenges remain for the widespread deployment of distributed WLAM. Scalability remains a challenge, particularly as the number of participating devices increases. Besides, ensuring low-latency communication among distributed components while maintaining data security is a critical challenge.

References

- 1 You X, Wang C X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. *Sci China Inf Sci*, 2021, 64: 1–74
- 2 Puri V, Kataria A, Sharma V. Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. *Trans Emerging Tel Tech*, 2024, 35: e4245
- 3 Lv Z, Lou R, Singh A K. AI empowered communication systems for intelligent transportation systems. *IEEE Trans Intell Transp Syst*, 2021, 22: 4579–4587
- 4 Chen Z, Zhang Z, Yang Z. Big AI models for 6G wireless networks: opportunities, challenges, and research directions. *IEEE Wireless Commun*, 2024, 31: 164–172
- 5 Zhang Z, Debbah M, Eldar Y C, et al. Guest editorial: sustainable big AI model for wireless networks. *IEEE Wireless Commun*, 2024, 31: 18–19
- 6 Zeng L, Ye S, Chen X, et al. Implementation of big AI models for wireless networks with collaborative edge computing. *IEEE Wireless Commun*, 2024, 31: 50–58
- 7 Cui Q M, You X H, Wei N, et al. Overview of AI and communication for 6G network: fundamentals, challenges, and future research opportunities. *Sci China Inf Sci*, 2025, 68: 171301
- 8 Lin J, Yu W, Zhang N, et al. A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. *IEEE Int Things J*, 2017, 4: 1125–1142
- 9 You X H, Huang Y M, Zhang C, et al. When AI meets sustainable 6G. *Sci China Inf Sci*, 2025, 68: 110301
- 10 Jiang F, Dong L, Peng Y, et al. Large AI model empowered multimodal semantic communications. *IEEE Commun Mag*, 2025, 63: 76–82
- 11 Yang Z, Li D, Zhao N, et al. Secure precoding optimization for NOMA-aided integrated sensing and communication. *IEEE Trans Commun*, 2022, 70: 8370–8382
- 12 Wei K, Li J, Ding M, et al. Federated learning with differential privacy: algorithms and performance analysis. *IEEE Trans Inform Forensic Secur*, 2020, 15: 3454–3469
- 13 Pham N D, Abuadbbba A, Gao Y, et al. Binarizing split learning for data privacy enhancement and computation reduction. *IEEE Trans Inform Forensic Secur*, 2023, 18: 3088–3100
- 14 Ashok M, Madan R, Joha A, et al. Ethical framework for artificial intelligence and digital technologies. *Int J Inf Manage*, 2022, 62: 102433
- 15 Chen M, Yang Z, Saad W, et al. A joint learning and communications framework for federated learning over wireless networks. *IEEE Trans Wireless Commun*, 2021, 20: 269–283
- 16 Yang Z, Chen M, Wong K K, et al. Federated learning for 6G: applications, challenges, and opportunities. *Engineering*, 2022, 8: 33–41
- 17 Lin L, Zhao Z, Yang Z, et al. Joint communication and learning design of differential privacy for federated learning over multi-cell networks. In: *Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023. 770–775
- 18 Thapa C, Mahawaga Arachchige P C, Camtepe S, et al. SplitFed: when federated learning meets split learning. In: *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022. 8485–8493
- 19 Pasquini D, Ateniese G, Bernaschi M. Unleashing the Tiger: Inference Attacks on Split Learning. New York: Association for Computing Machinery, 2021. 2113–2129
- 20 Yang Z, Chen M, Saad W, et al. Energy efficient federated learning over wireless communication networks. *IEEE Trans Wireless Commun*, 2021, 20: 1935–1949
- 21 Qu Z, Tang Y, Muhammad G, et al. Privacy protection in intelligent vehicle networking: a novel federated learning algorithm based on information fusion. *Inf Fusion*, 2023, 98: 101824
- 22 Lang N, Sofer E, Shaked T, et al. Joint privacy enhancement and quantization in federated learning. *IEEE Trans Signal Process*, 2023, 71: 295–310
- 23 Liu H, Li B, Gao C, et al. Privacy-encoded federated learning against gradient-based data reconstruction attacks. *IEEE Trans Inform Forensic Secur*, 2023, 18: 5860–5875
- 24 Hijazi N M, Aloqaily M, Guizani M, et al. Secure federated learning with fully homomorphic encryption for IoT communications. *IEEE Int Things J*, 2024, 11: 4289–4300
- 25 Guler B, Yener A, Swami A. The semantic communication game. *IEEE Trans Cogn Commun Netw*, 2018, 4: 787–802
- 26 Zhao Z, Yang Z, Gan X, et al. A joint communication and computation design for semantic wireless communication with probability graph. *J Franklin Inst*, 2024, 361: 107055
- 27 Huang D, Gao F, Tao X, et al. Toward semantic communications: deep learning-based image semantic coding. *IEEE J Sel Areas Commun*, 2023, 41: 55–71
- 28 Xing C, Lv J, Luo T, et al. Representation and fusion based on knowledge graph in multi-modal semantic communication. *IEEE Wireless Commun Lett*, 2024, 13: 1344–1348
- 29 Dong C, Liang H, Xu X, et al. Semantic communication system based on semantic slice models propagation. *IEEE J Sel Areas Commun*, 2023, 41: 202–213
- 30 Ding G, Liu S, Yuan J, et al. Joint URLLC traffic scheduling and resource allocation for semantic communication systems. *IEEE Trans Wireless Commun*, 2024, 23: 7278–7290
- 31 Zhao Z, Yang Z, Huang C, et al. A joint communication and computation design for distributed RIS-assisted probabilistic semantic communication in IIoT. *IEEE Int Things J*, 2024, 11: 26568–26579
- 32 Xie H, Qin Z, Li G Y, et al. Deep learning enabled semantic communication systems. *IEEE Trans Signal Process*, 2021, 69: 2663–2675
- 33 Jankowski M, Gunduz D, Mikolajczyk K. Wireless image retrieval at the edge. *IEEE J Sel Areas Commun*, 2021, 39: 89–100
- 34 Zhang H, Shao S, Tao M, et al. Deep learning-enabled semantic communication systems with task-unaware transmitter and dynamic data. *IEEE J Sel Areas Commun*, 2023, 41: 170–185
- 35 Yang W, Liew Z Q, Lim W Y B, et al. Semantic communication meets edge intelligence. *IEEE Wireless Commun*, 2022, 29: 28–35
- 36 Yang Z, Chen M, Zhang Z, et al. Energy efficient semantic communication over wireless networks with rate splitting. *IEEE J Sel Areas Commun*, 2023, 41: 1484–1495
- 37 Zhao Z, Yang Z, Chen M, et al. A joint communication and computation design for probabilistic semantic communications. *Entropy*, 2024, 26: 394
- 38 Shao J, Mao Y, Zhang J. Learning task-oriented communication for edge inference: an information bottleneck approach. *IEEE J Sel Areas Commun*, 2022, 40: 197–211
- 39 Xu W, Yang Z, Ng D W K, et al. Edge learning for B5G networks with distributed signal processing: semantic communication, edge computing, and wireless sensing. *IEEE J Sel Top Signal Process*, 2023, 17: 9–39
- 40 Tishby N, Pereira F C, Bialek W. The information bottleneck method. In: *Proceedings of the 37th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, 1999. 368–377
- 41 Guo S, Wang Y, Li S, et al. Semantic importance-aware communications using pre-trained language models. *IEEE Commun Lett*, 2023, 27: 2328–2332

- 42 Lee J H, Lee D H, Lee J, et al. Integrating pre-trained language model with physical layer communications. 2024. ArXiv:2402.11656
- 43 Shi G, Xiao Y, Li Y, et al. From semantic communication to semantic-aware networking: model, architecture, and open problems. *IEEE Commun Mag*, 2021, 59: 44–50
- 44 Luo X, Chen H H, Guo Q. Semantic communications: overview, open issues, and future research directions. *IEEE Wireless Commun*, 2022, 29: 210–219
- 45 Yang Z, Chen M, Li G, et al. Secure semantic communications: fundamentals and challenges. *IEEE Netw*, 2024, 38: 513–520
- 46 Zhang G, Hu Q, Qin Z, et al. A unified multi-task semantic communication system for multimodal data. *IEEE Trans Commun*, 2024, 72: 4101–4116
- 47 Zhu Z, Zhang R, Cheng X, et al. Multi-modal fusion-based multi-task semantic communication system. 2024. ArXiv:2407.00964
- 48 Luo X, Gao R, Chen H H, et al. Multimodal and multiuser semantic communications for channel-level information fusion. *IEEE Wireless Commun*, 2024, 31: 117–125
- 49 Jiang F, Peng Y, Dong L, et al. Large AI model empowered multimodal semantic communications. 2023. ArXiv:2309.01249
- 50 Dhar Dwivedi A, Singh R, Kaushik K, et al. Blockchain and artificial intelligence for 5G-enabled Internet of Things: challenges, opportunities, and solutions. *Trans Emerging Tel Tech*, 2024, 35: e4329
- 51 Hu S, Liang Y C, Xiong Z, et al. Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond. *IEEE Wireless Commun*, 2021, 28: 145–151
- 52 Zhou Z, Onireti O, Xu H, et al. AI and blockchain enabled future wireless networks: a survey and outlook. *Distrib Ledger Technol*, 2024, 3: 1–30
- 53 Zuo Y, Guo J, Gao N, et al. A survey of blockchain and artificial intelligence for 6G wireless communications. *IEEE Commun Surv Tut*, 2023, 25: 2494–2528
- 54 Stratton J A. *Electromagnetic Theory*. Hoboken: John Wiley & Sons, 2007
- 55 Paul C R, Scully R C, Steffka M A. *Introduction to Electromagnetic Compatibility*. Hoboken: John Wiley & Sons, 2022
- 56 van Bladel J G. *Electromagnetic Fields*. Hoboken: John Wiley & Sons, 2007
- 57 Xu J D, Yuen C, Huang C W, et al. Reconfiguring wireless environments via intelligent surfaces for 6G: reflection, modulation, and security. *Sci China Inf Sci*, 2023, 66: 130304
- 58 Xu Q, Jiang C, Han Y, et al. Waveforming: an overview with beamforming. *IEEE Commun Surv Tut*, 2018, 20: 132–149
- 59 Imai H. Information security aspects of spread spectrum systems. In: *Proceedings of International Conference on the Theory and Application of Cryptology*, 2005. 193–208
- 60 Pham D P, Marion D, Mastio M, et al. Obfuscation revealed: leveraging electromagnetic signals for obfuscated malware classification. In: *Proceedings of the 37th Annual Computer Security Applications Conference*, 2021. 706–719
- 61 Wang Y, Sun L, Du Q. Multi-antenna signal masking and round-trip transmission for privacy-preserving wireless sensing. *IEEE Trans Inform Forensic Secur*, 2024, 19: 6305–6320
- 62 Abadi M, Chu A, Goodfellow I, et al. Deep learning with differential privacy. In: *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016. 308–318
- 63 Ureten O, Serinken N. Wireless security through RF fingerprinting. *Can J Electr Comput Eng*, 2007, 32: 27–33