Journal of Artificial Intelligence Practice (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2025.080305
ISSN 2371-8412 Vol. 8 Num. 3

Research on Information Transmission Method Selection and Security Protection Based on Artificial Intelligence

Nailin Bai*

School of Mechanical and Electrical Engineering, Hainan Vocational University of Science and Technology, Haikou, Hainan, 571126, China
**Corresponding author: 38783108@qq.com*

Keywords: Artificial Intelligence, Information Transmission Optimization, Security Protection, Deep Learning, Reinforcement Learning

Abstract: With the rapid development of artificial intelligence technology, its application in information transmission optimization and security protection has shown great potential. This paper systematically analyzes the characteristics of different transmission methods and the critical role of AI in environmental perception and resource scheduling. It proposes an intelligent decision model based on deep learning and reinforcement learning, which significantly improves the adaptability and efficiency of the transmission system. In terms of security, by introducing anomaly detection, dynamic key management, and multi-party collaboration mechanisms, the system's ability to resist diverse threats, including eavesdropping, tampering, and denial of service, is effectively enhanced. Combined with adaptive strategy adjustment, a stable and robust security system is realized, providing theoretical support and technical guarantees for future intelligent communication networks. Research indicates that AI-driven transmission optimization and security systems have broad application prospects in improving communication performance and ensuring information security, injecting new impetus into the intelligent development of future networks.

1. Introduction

With the rapid development of information and communication technology, modern society's demand for high-speed, efficient, and secure information transmission is constantly growing, driving the emergence and innovation of diverse transmission technologies. While traditional communication methods meet the needs of large-scale data flow, they also face many bottlenecks, including the difficulty of configuring network resources, insufficient adaptability in dynamic environments, and the continuous emergence of diversified security threats. In this context, Artificial Intelligence (AI) is gradually becoming an important technical means to optimize information transmission strategies and enhance security protection capabilities[1]. By intelligently sensing environmental states, making autonomous decisions, and dynamically adjusting transmission paths and methods, AI significantly improves the flexibility and intelligence level of communication systems, while promoting the development of next-generation communication technologies[2].

In practical applications, the main role of artificial intelligence in information transmission is reflected in two aspects: first, to achieve intelligent selection and optimization of transmission methods, thereby adapting to changing network environments and improving transmission efficiency and resource utilization; second, to build an autonomous and secure protection system to cope with constantly evolving network threats and attacks[3,4]. Traditional statically configured transmission strategies struggle to meet the demands of complex and variable scenarios, while AI-based dynamic scheduling and optimization mechanisms can autonomously adjust transmission parameters based on real-time environmental information, avoiding potential performance bottlenecks and risk points. At the same time, AI-driven security technologies such as anomaly detection, intrusion detection, and adaptive encryption algorithms enhance the system's resistance to attacks and effectively reduce security risks such as data leakage, eavesdropping, and tampering[5].

However, there are still many challenges in applying artificial intelligence technology to the field of information transmission, including the model's sensitivity to environmental changes, the computational pressure caused by high real-time requirements, and the lack of generalization ability in complex scenarios. How to use advanced algorithms such as deep learning and reinforcement learning to establish intelligent decision-making models that are both highly accurate and robust has become the core of current research[6]. At the same time, balancing the system's scalability and security, and designing intelligent solutions that meet future communication needs, is the key to promoting technological innovation in the industry.

This paper aims to deeply analyze the application potential of artificial intelligence in information transmission and propose a complete solution that integrates multi-source environment perception, intelligent decision-making, and security protection, thereby achieving a dual improvement in transmission efficiency and security assurance, and providing a theoretical basis and technical support for the intelligent development of future communication systems.

2. Current Status

2.1 Classification and Characteristics

With the continuous evolution of information technology, traditional communication methods are gradually developing towards diversification and intelligence. In this process, a deep understanding of the classification of different transmission methods and their inherent advantages and limitations lays the theoretical foundation for promoting AI-based transmission optimization solutions. Communication methods mainly include wired transmission, wireless transmission, and fiber optic communication, each with distinct characteristics and applicable scenarios, demonstrating different advantages and disadvantages for different environments and needs.

Wired transmission achieves data transfer through physical lines, with the advantages of low line loss, stable signal, and controllable bandwidth, and is widely used in enterprise LANs, data centers, and core backbone networks. Its disadvantages are high deployment costs and lack of flexibility, making it difficult to meet rapidly changing mobility needs and large-scale coverage scenarios. Wireless transmission achieves information transfer through radio waves in the spectrum, with the advantages of flexible deployment, wide coverage, and adaptation to mobile scenarios, and is suitable for personal communication and mobile internet. However, the channel is subject to severe interference, signal attenuation is fast, bandwidth is limited, and security is low[7]. Fiber optic communication excels in high-speed, large-capacity transmission needs, with extremely low signal loss, extremely high data transmission rates, and instantaneous bandwidth, but its deployment cost is high and it is difficult to achieve wide coverage. The complementarity of different transmission methods makes multi-modal hybrid transmission a future development trend.

2.2 Application of Artificial Intelligence Technology in Transmission Optimization

Traditional transmission optimization focuses on static parameter tuning and matching with hardware characteristics, making it difficult to fully cope with complex and changing network environments. The introduction of artificial intelligence unfolds in this context, with deep learning and reinforcement learning models being applied to transmission method selection and scheduling optimization in dynamic environments. Deep learning models can learn potential transmission characteristics and environmental patterns through massive amounts of historical data, thereby achieving accurate prediction and analysis of transmission states. In complex environments such as network load changes and channel interference, these models can provide decision support for transmission strategies, enabling intelligent path selection and scheduling. Simultaneously, reinforcement learning optimizes the learning process through exploration and utilization strategies, enabling the system to continuously adapt to environmental changes and gradually form an efficient autonomous scheduling mechanism. This AI-based dynamic resource management greatly enhances the adaptability and robustness of communication systems.

In practical applications, automatic scheduling and dynamic resource allocation have gradually become key research directions. By monitoring network status in real-time and using intelligent algorithms to dynamically adjust spectrum resources, regulate routing paths, and control transmission parameters, efficient use of limited bandwidth resources can be achieved. At the same time, by using intelligent prediction models to predict network traffic changes, resources can be reserved and adjusted in advance to avoid bottlenecks or overloads. These techniques play a crucial role in ensuring transmission quality, reducing latency, and increasing network capacity.

2.3 Existing Research and Technical Bottlenecks

However, the current application of artificial intelligence in information transmission optimization still faces many challenges. Intelligent scheduling requires extremely high real-time performance, requiring environmental perception, decision-making, and regulation to be completed in a very short time to ensure timely system response. However, the complexity and computational load of models often contradict real-time performance, affecting actual deployment effectiveness. Enhancing the reliability of models is also a challenge, especially in dynamically changing and diverse environments, where insufficient generalization ability of models leads to prediction errors, affecting system stability[8]. In addition, inconsistent channel conditions and multiple interferences in large-scale environments limit the adaptability and scalability of models. Achieving deep models with high generalization ability, reducing overfitting and bias, and ensuring excellent performance in different environments has become a core problem in current research.

3. AI-Based Intelligent Transmission Mode Selection Model

In complex and dynamic communication environments, intelligent transmission mode selection relies on accurate perception and precise modeling of the environmental state. To achieve autonomous decision-making, it is necessary to construct a highly adaptive model that integrates multi-source data for environmental awareness and designs efficient decision algorithms based on this. Continuous optimization of the model training process enhances the overall decision-making ability and operational efficiency of the system, driving the communication system towards a higher level of intelligence.

3.1 Transmission Environment Perception and Feature Extraction

Based on multi-source data fusion technology, achieving multi-angle and multi-dimensional information integration for environmental awareness is key to realizing accurate environmental state modeling. Various data sources from sensor networks, network monitoring systems, and user terminals are used to extract key features through fusion algorithms, such as signal-to-noise ratio, interference level, network load, and mobile state information, to obtain global and fine-grained environmental perception results. The fusion of these multi-source data not only enhances the completeness of the information but also improves the sensitivity to environmental changes, providing a solid data foundation for subsequent decision-making. In dynamic environments, improving the real-time performance and accuracy of feature extraction is particularly important when facing the time-varying nature of channels and complex interference. A feature extraction architecture based on deep learning models can automatically learn deep-level features, reducing the burden of manual feature engineering and significantly improving the robustness of perception.

Modeling dynamic environmental changes requires combining time series analysis and spatial information modeling techniques to achieve multi-scale, multi-temporal-spatial level descriptions of network states. Combining models such as recurrent neural networks (RNNs) and long short-term memory networks (LSTMs) can effectively capture the non-linear changes in the environment and form predictions of future states. Environmental modeling is also the basis for intelligent decision-making, and accurate state prediction can significantly improve the foresight and adaptability of scheduling strategies. Integrating these models into the architecture enables the system to remain sensitive to sudden events and environmental interference, and to adjust transmission strategies in a timely manner to ensure the stability of network performance.

3.2 Intelligent Decision Algorithm Design

In the decision algorithm design phase, reinforcement learning provides a superior solution for intelligent transmission path selection. By defining the state space, action space, and reward function, the agent learns the optimal strategy through continuous interaction, optimizing the allocation of network resources. Combining deep reinforcement learning with a state value function can address the challenges posed by high-dimensional state spaces, effectively balancing short-term and long-term benefits. The agent selects the appropriate transmission method, path, and parameters based on environmental perception inputs, achieving load balancing, energy consumption optimization, and interference avoidance. During the training process, a strategy combining exploration and exploitation is adopted to achieve good convergence and stability.

Deep neural networks also play an important role in classification and prediction tasks. The multi-category division of environmental parameters and the rapid prediction of future states rely on deep learning capabilities. Convolutional neural networks (CNNs) can be used to extract key indicators from spatial features, enhancing feature representation capabilities; and network models combined with gating mechanisms can better capture dynamic changes in time series, providing high-quality prediction data for decision-making. These deep models are not only used for environmental classification, but can also be combined with reinforcement learning for end-to-end policy learning, improving the level of decision-making automation.

3.3 Model Training and Optimization

Model training is a core component of the intelligent decision-making system. A large amount of real and simulated data needs to be collected from multiple sources to construct a representative data set to cover a variety of complex environmental conditions. During the data preprocessing

process, feature screening, dimensionality reduction, and enhancement should be performed to ensure the effectiveness and diversity of model input data. The training strategy combines transfer learning, online learning, and incremental learning to form an adaptive and efficient training mechanism. Through cross-validation and hyperparameter tuning, it is ensured that the model can maintain good generalization ability in different scenarios.

Performance evaluation indicators include decision accuracy, convergence speed, robustness, and resource utilization. Decision accuracy measures the correctness of the model's choices in a real-world environment, providing direction for model tuning. Convergence speed reflects the efficiency of the training process and is an important guarantee of system real-time performance. Robustness reflects the model's stability in the face of environmental disturbances and data noise, ensuring the reliability of decisions. Resource utilization evaluates the model's system resource consumption under normal and extreme conditions, balancing performance and cost. Through a multi-dimensional indicator evaluation system, the model structure and training strategy are continuously optimized to improve the overall level of intelligent decision-making.

4. Research on Transmission Security Protection Technology

In modern communication systems, the security of information transmission is increasingly becoming a critical factor restricting its widespread application. With the rapid integration of network technology and artificial intelligence, various attack methods are constantly evolving, threatening the integrity, confidentiality, and availability of data. Understanding typical threat patterns and their potential risk points provides a theoretical basis for designing effective security protection systems. At the same time, with the help of artificial intelligence technology, security mechanisms with autonomous learning and active response capabilities can be built, significantly improving the overall attack resistance and resilience of the system.

4.1 Transmission Security Threat Analysis

Transmission security threats are diverse and complex, including eavesdropping, tampering, denial of service (DoS) and its variants, and other forms of attack. Eavesdropping attacks aim to listen to the data transmission process without authorization and steal sensitive information. These types of attacks often exploit the vulnerability of channels or unencrypted transmission protocols. Tampering attacks corrupt data integrity by modifying data packets, which in severe cases can lead to system misjudgment or misoperation. Denial-of-service attacks deplete network resources with a large number of bogus requests, preventing legitimate users from accessing services and affecting the normal operation of the system. In addition, as attack techniques continue to improve, threat patterns are becoming more diverse, and deception methods and concealment methods are constantly evolving, posing great challenges to security protection.

Typical security vulnerabilities and risk points are mostly concentrated in protocol design, key management, and system monitoring and response mechanisms. Some communication protocols lack complete authentication and encryption measures in their design, making them vulnerable to man-in-the-middle attacks or replay attacks. Poor key management brings the risk of key leakage or attacks using weak passwords, creating hidden dangers for data security. Insufficient system monitoring capabilities make it difficult to identify abnormal behavior or attack events in a timely manner, delaying response opportunities and aggravating attack losses. With the rise of the Internet of Things and large-scale networks, the system's attack and defense environment has become more complex, and traditional methods are difficult to cope with ever-changing threats, requiring the introduction of intelligent security technologies for improvement.

4.2 AI-Enhanced Security Strategies

The introduction of artificial intelligence offers a new path for upgrading security strategies. Anomaly detection, through deep learning models, can analyze large amounts of real-time monitoring data to identify potential attack behaviors. AI algorithms based on statistical patterns and features can effectively distinguish between normal and abnormal states, reducing false positive rates. Intrusion detection systems continuously learn diverse attack characteristics, improving the ability to identify unknown attack patterns and enhancing the system's proactive defense level. Leveraging AI's self-learning capabilities, security systems continuously improve detection models, enhance the accuracy of detecting new threats, and ensure the system's security posture remains continuously controllable.

Key management, as a core component of information security, expands its application space when combined with intelligent algorithms. Dynamic key exchange protocols, integrated with AI algorithms, automatically generate and update keys based on environmental changes, reducing the risk of key leakage. Real-time analysis of potential threats in the environment allows for the automatic adjustment of key lengths and encryption algorithms, achieving "elastic encryption." Simultaneously, machine learning is used to predict potential key attack paths, enabling proactive risk assessment and defense deployment, thereby enhancing the resilience and security of the key system.

4.3 Implementation of AI-Integrated Security Mechanisms

In multi-party collaboration scenarios, federated learning technology demonstrates significant potential. Data silos across multiple parties limit the monitoring capabilities of a single institution, but through federated learning, all parties can jointly train models without sharing sensitive data, achieving improved global attack detection capabilities. Multi-party security collaboration systems can implement distributed threat monitoring, collaboratively responding to complex attack behaviors, greatly enhancing overall security protection capabilities.

The implementation of intelligent strategies also involves the design of adaptive security mechanisms. Security strategies are continuously adjusted based on environmental awareness to adapt to constantly changing attack postures. The system can automatically enable different levels of security measures based on the detected threat level, transitioning from a static mode to dynamic and elastic defense. For example, when a potential attack is detected, the system can automatically restrict certain ports or invoke additional encryption layers, and even activate rapid response mechanisms to block attack paths, effectively mitigating or even preventing attack spread. These autonomous adjustment strategies significantly enhance the system's resilience and flexibility.

4.4 Security Performance and System Assurance

Evaluation metrics regarding security performance and system assurance serve as critical parameters for measuring the overall security protection system. Detection accuracy reflects the ability to identify abnormal behavior and attacks; a high detection rate coupled with a low false positive rate ensures the accuracy of identification. Rapid response capability is related to the timeliness of defense, enabling interception in the early stages of an attack to reduce losses. The robustness of the system is demonstrated by its ability to defend against diverse attacks; the stronger the ability to resist interference and mutation attacks, the higher the overall security. Concurrently, resource utilization rate is an important indicator for measuring the efficient operation of the security system, and security assurance and network performance should be balanced to avoid additional burdens caused by security measures.

By integrating advanced technologies such as deep learning and reinforcement learning to construct a multi-layered, multi-dimensional security system, the resilience of communication systems in the face of increasingly complex threats has been significantly improved. Continuous introduction of novel detection algorithms and dynamic strategies promotes the improvement of the proactive defense system, providing a solid technical foundation for future secure communication. At the same time, the integration of security emergency response and event tracking, automated auditing and other mechanisms has greatly enhanced the overall security assurance capabilities of the system, laying a solid foundation for building a secure and reliable intelligent communication network.

5. Conclusion

This article focuses on the optimization and security assurance of artificial intelligence in information transmission, emphasizing the importance of multi-source environment perception, intelligent decision-making, and dynamic scheduling. By introducing deep learning and reinforcement learning technologies, the autonomous perception of the transmission environment and efficient decision-making are realized, improving the adaptability and resource utilization efficiency of the system. In terms of security, the combination of AI-based anomaly detection, intrusion identification, and dynamic key management significantly enhances the system's ability to resist various threats. Multi-party security collaboration and adaptive strategy adjustment mechanisms improve the resilience and rapid response capabilities of the security system, providing a solid foundation for communication security in future complex environments. Overall, AI-enabled transmission optimization and security protection technologies provide an innovative path for realizing intelligent and automated communication systems, which helps to continuously improve the security, reliability, and efficiency of next-generation networks. In the future, it is necessary to further break through the generalization ability of models and optimize system architectures with high real-time performance and high robustness to enable AI security technologies to demonstrate stronger application value in actual deployment.

References

[1] Wang Haoquan. Research on the Protection Path of Personal Information Security from the Perspective of Generative Artificial Intelligence [J]. Market Weekly, 2025,38(09):153-156.

[2] Guo Kunkun. A Brief Analysis of the Application of Communication Technology and Electronic Information Technology in the Field of Artificial Intelligence [C]// Vocational Education Professional Committee of China Enterprise Culture Promotion Association. Proceedings of the Symposium on the Integration Model and Innovative Practice of Cultural Enterprises Empowering the New Education Ecosystem Hangzhou Gaoxun Internet of Things Technology Co., LTD., 2025:122-124.

[3] Bai Yankun. Theoretical Research on the Application of Artificial Intelligence in Information Transmission Mode Selection and Security Intervention [J] Digital Communication World, 2024,(12):31-33.

[4] Yan Ping. Research on the Application of Artificial Intelligence Technology in Information Security Management [J]. High Technology & Industrialization, 2025,31(03):64-66.

[5] Zhang Xiaoyi. Research on the Application of Artificial Intelligence in the Detection of Cybersecurity Vulnerabilities in Network Information [J] China Broadband, 2025,21(03):46-48.

[6] Chen Min, Wu Gaofeng. Discussion on the Security Monitoring Method of Computer Network Information Transmission under Information Fusion [J]. China Broadband, 2025,21(05):85-87.

[7] He Wangjun. Network Information Security Transmission Protection Method Based on Double-Layer Encryption [J] Network Security Technology and Application, 2025,(05):22-24.

[8] Zhang Kai. Research on Mobile Network Information Security Transmission Method Based on Internet of Things 5G Communication Technology [J] China Broadband, 2025,21(03):88-90.