Woody International Publish Limited
An Multidisciplinary Academic Journal Publisher
Journal of Artificial Intelligence and Information, Volume 2, 2025
https://www.woodyinternational.com/

The Application and Discussion of Virtual Network Technology in Computer Network Security

Mingxing Tang

Wuchang Vocational College, Wuhan City, Hubei Province, 430200

Abstract: ***The development of information technology has led to an improvement in people's living standards and quality of life. With the widespread adoption of current computer technology, concerns about computer network security are increasingly shared among users. The application of virtual network technology in computer networks can significantly enhance network security and reduce the losses caused by computer vulnerabilities. This paper primarily investigates the utilization of virtual network technology in computer networks and presents the application scenarios of virtual network technology in computer network security. It aims to provide effective references for the application of relevant technologies.***

Keywords: Computer; Network security; Virtual network; Application technology.

1. INTRODUCTION

In the current context of informatization, the widespread use of computer network technology has brought great changes to various aspects of social production and life, effectively improving the quality of people's lives and work. With the continuous advancement and development of computer network technology, in order to further improve the application performance of computer networks and ensure their stability, it is necessary to attach importance to the improvement and management of computer network security. The application of virtual network technology in computer network security can effectively solve the problems of capacity, operational risks, and operational security in current computer networks, providing a good guarantee for the safe and stable operation of computer networks, and has extremely important significance for further deepening the application of computer network technology.

2. OVERVIEW OF VIRTUAL NETWORK TECHNOLOGY

The application of virtual network technology in computer network security can establish a virtual private network in the computer public network to detect and manage remotely accessed information data. In the operation of virtual networks, tunneling technology is involved. Identity authentication technology, key technology, and other technical means can greatly improve the privacy of communication between different regional networks in computer networks. By utilizing relevant information technology processing and encryption, the risk of tampering and theft of most information transmission processes is effectively avoided. Currently, public networks such as enterprises and governments often use virtual network technology to establish virtual servers dedicated to protecting network security. When there are situations such as remote access in the network, a valid security key needs to be entered to access the internal network, effectively improving the security and stability of data in computer networks. Wang et al. [1] explored the cell atlas of the immune microenvironment in gastrointestinal cancers, focusing on dendritic cells and other components, providing valuable insights into tumor immunology. Meanwhile, Li [2] proposed a deep learning-enhanced adaptive interface to improve accessibility in e-government platforms, highlighting the intersection of technology and public service. Yuan [3] investigated efficient techniques for processing medical texts in legal documents using transformer architecture, demonstrating the potential of AI in legal informatics. On the logistics front, Wang [4] developed predictive modeling for sortation and delivery optimization in e-commerce logistics, aiming to enhance operational efficiency. Song [5] leveraged AIGC and human-computer interaction design to boost efficiency and quality in e-commerce content generation, reflecting the evolving landscape of digital marketing. In the realm of data processing, Chen [6] emphasized the importance of efficient and scalable data pipelines as the core of data processing in gig economy platforms, addressing the challenges of big data management. In legal studies, Wang [7] discussed the restriction and balance of prior rights on the right of enterprise name, contributing to the understanding of intellectual property law. Gong et al. [8] optimized enterprise risk decision support systems based on ensemble machine learning, enhancing risk management capabilities. Bohang et al. [9] applied active learning and hyperparameter optimization in image

steganalysis, advancing the field of digital forensics. In the manufacturing sector, Zhao et al. [10] focused on steel production scheduling optimization using deep learning, aiming to improve production efficiency. Yao et al. [11] proposed a drone-3D printing linkage for rapid construction of sustainable post-disaster temporary shelters, offering innovative solutions for disaster relief. In finance, Yang et al. [12] conducted research on stock market sentiment analysis and prediction methods based on convolutional neural networks, providing tools for market analysis. Ji et al. [13] studied the application of artificial intelligence in personalized go-to-market strategies in the retail industry, facilitating targeted marketing. Yang et al. [14] explored cross-asset risk management by integrating large language models for real-time monitoring of equity, fixed income, and currency markets, enhancing risk assessment. Finally, Li [15] optimized clinical trial strategies for anti-HER2 drugs based on Bayesian optimization and deep learning, aiming to improve drug development processes.

3. THE APPLICATION SIGNIFICANCE OF VIRTUAL NETWORK TECHNOLOGY IN COMPUTER NETWORK TECHNOLOGY

3.1 Improve the security of computer network

Virtual network technology can utilize virtualization of servers and networks to improve computer network security. At the same time, other key technologies such as tunneling, identity authentication, and encryption can be used to enhance the security of computer networks, avoiding information and data security issues caused by physical factors during operation. This provides a secure and stable transmission environment for computer information and data, and improves the reliability of computer networks.

3.2 Reduce the operational complexity of computer networks

The application of computer networks in various fields and industries is constantly deepening. With the progress of society, the application of computer networks in industries is becoming increasingly widespread, and the application environment is also becoming more and more complex. In such a situation, the operational security risks and other issues that arise during the operation of computer networks also increase, seriously affecting the security and stability of computer networks during operation. The use of virtual network technology can simplify the system operation process of computer network technology to a certain extent, reduce the complexity of computer networks, and further upgrade the security of computer network systems.

3.3 Improve the reliability of information data transmission in computer networks

The application of virtual network technology in the maintenance of computer network security can directly repackage relevant information data within the local area network where the computer is located, identify and protect important information data in the computer network, avoid illegal tampering or theft of data during transmission and operation, and effectively improve the security of information data transmission in computer networks. In addition, the application of information data transmission in computer network technology can to some extent avoid problems such as frame loss during information transmission and ensure the integrity of data transmission.

4. SECURITY ISSUES IN COMPUTER NETWORKS

4.1 Network viruses

In the process of computer network operation, once a network virus intrusion occurs, it can easily lead to the destruction of data and other information, and even cause system paralysis and other phenomena in the computer network, seriously affecting the normal use of the computer network. Viruses that exist in computer networks have latency and concealment, causing great damage to the security of computer networks. Therefore, the security protection of computer networks is extremely important. Without effective computer network security protection measures, a series of operations by users during use, such as opening mini programs at will, will cause network viruses to stay in the computer, leading to security failures in the computer network.

4.2 Trojan virus

Trojan virus is a common network virus that has a significant impact on computer networks. Trojan viruses have strong concealment in computer networks. With the continuous development and progress of computer network technology in recent years, Trojan viruses pose an increasingly significant threat to the security of computer network operating environments. Generally speaking, Trojan viruses can be divided into two types of programs: control end and controlled end. During the operation of computer networks, some illegal elements invade users' computers through Trojan viruses, and then use Trojan viruses to modify the operation of computer networks, and even damage and steal users' relevant data information. In addition, Trojan viruses in computer networks can also monitor the running process of computers. If users do not pay attention to the protection of Trojan viruses during use, it will seriously affect the security of computer network operation.

4.3 Unauthorized access to computer networks

Illegal access authorization in computer networks mainly refers to the unauthorized use of network resources. Generally speaking, illegal access authorization involves unauthorized users performing illegal operations on systems and networks, as well as legitimate users performing unauthorized operations. Unauthorized access poses a significant threat to computer networks. Using unauthorized access can lead to mandatory attacks on computer networks, intentionally disrupting system security and stability, and causing system paralysis.

5. THE MAIN APPLICATION TECHNOLOGIES OF VIRTUAL TECHNOLOGY IN COMPUTER NETWORK SECURITY

5.1 Encryption Technology

Encryption technology is the most common application of virtual technology in computer network security, which can effectively maintain computer network security in most cases and has extremely important application significance. In practical applications, virtual network technology has a certain degree of independence, which requires users to first use virtual technology to transform the current public network area into their own usage area, and complete the conversion of digital resources in the computer network through the use of relevant computer languages. Subsequently, encryption technology in virtual technology is utilized to resist illegal user intrusion, information theft, and other situations in computer network technology, effectively protecting user privacy and reducing economic losses caused by related privacy breaches in computer networks.

5.2 Key security technology

Applying virtual technology to maintain computer network security can also start from key security technology. Generally speaking, key security technologies in virtual private network technology mainly include ISKAMP technology and SKIP technology. By fully applying these two technologies, the security performance of computer networks can be further improved. In practical applications, ISKAMP technology mainly applies public key security technology, allowing users to obtain keys anytime and anywhere during use, improving the convenience of related operations. However, on the other hand, the use of ISKAMP technology also has certain limitations and cannot effectively protect important information and data in computer networks. In contrast, SKIP technology mainly applies the Diffie rule, which can greatly improve the confidentiality of computer networks in China, comprehensively and efficiently protect computer networks in the process of information or data dissemination, and effectively enhance users' network information security.

5.3 Tunnel safety technology

The application of tunnel security technology in computer network security can improve the security performance of computer networks from the source. Tunnel security technology uses routers and various hardware facilities as technology, and utilizes relevant encryption protocols in virtual technology to upload information and data that virtual network technology needs to protect in public networks. Before uploading, the relevant information is encrypted twice, greatly improving the information security factor in computer network technology. In practical applications, tunnel security technology is mainly achieved through information decryption and encrypted transmission. In order to ensure the effective implementation of tunnel security technology, it is necessary to ensure that the virtual network has router access function and is equipped with devices such as tunnel terminators, switches, and openers. When using a switch, it is necessary to ensure that the switch maintains a good conversion rate during operation, providing scientific application conditions for the application of tunnel security technology.

5.4 Identity verification technology

Identity verification technology is a widely used application function in computer network security technology. By setting the user login name and password, the initial authentication information is uploaded to the computer network. Then, using data conversion and other methods, the internal information in the computer network is compared with the initial information to generate accurate dynamic instructions, improving the security factor of user information and data storage. During the system authentication process, users can apply the corresponding VPC network to build a virtual network in the computer network, and obtain the information and data needed for the operation of the computer network from it. Starting from the internal operating environment of the computer network, they can detect and manage security issues that arise during the operation process. In addition, by utilizing identity verification technology, it is possible to expand associated network resources, further improve the quality of computer network work, and enhance its operational efficiency.

6. APPLICATION SCENARIOS OF VIRTUAL NETWORK TECHNOLOGY IN COMPUTER NETWORK SECURITY

6.1 Addressing Security Issues in Information Channels

With the development of current information technology, traditional computer network security management methods are no longer suitable for modern network office needs, especially in data processing and storage, where information security issues often arise due to unscientific network connections and other reasons. The use of VPN technology in virtual network technology can effectively solve security issues in information connection and transmission pathways, ensuring timely and secure transmission of relevant information. At the same time, using VPN technology can also enhance the security of data transmission in the form of dedicated lines, greatly protecting the information security of computer networks. Finally, using VPN technology can also build a dedicated virtual network, effectively preventing related information from being modified and leaked during transmission due to external factors, greatly improving the convenience of computer network applications.

6.2 Security Protection between Data Transmission

Firstly, fully utilizing virtual technology in computer networks to establish efficient private networks can build a good information technology security management system, thereby providing security protection for data transmission between local area networks and establishing effective security management methods for users. In addition, setting up a virtual private network reasonably in the internal LAN can effectively improve the security of data during high-speed transmission. At the same time, combining keys to protect data can effectively enhance the security protection capability of firewalls and provide a good network environment for information and data transmission. Finally, by establishing a stable network system during data transmission, the efficiency and security of data transmission can be further improved.

6.3 Improve the efficiency of user interaction with enterprises

In the process of connecting users and enterprises, there are also security issues related to computer networks. To achieve effective integration between users and enterprises, it is necessary to optimize the security performance of computer networks. Generally speaking, users achieve efficiency and security in connecting with enterprises through the following scenarios.

(1) The current communication between users and enterprises is based on cooperation in information, data, and resources. In order to ensure that information is not leaked during communication and to prevent criminals from taking advantage of the situation to carry out illegal operations, it is necessary to achieve information security in the process of information transmission and communication.

(2) When storing relevant data, virtual network technology is used to set up firewalls in computers and continuously improve the security factor of firewalls to ensure the security of stored data in computer networks.

(3) Regularly process and update information during verification of relevant information and passwords. Timely detection and effective resolution of security issues in computer network systems, thereby reducing the probability of security problems arising between users and related enterprises during the docking process.

6.4 Ensure the security of enterprises when connecting with remote departments

The use of computer network technology can enable remote communication between enterprises and relevant departments. By utilizing virtual network technology in the communication process, it is possible to comprehensively grasp the communication rhythm between enterprises and departments, effectively coordinate the relationship between enterprises and relevant departments, and improve communication efficiency. At the same time, utilizing virtual network technology can also ensure the security of relevant data and information during the docking process between enterprises and remote departments. Timely detect and prevent intrusion during data transmission to avoid security issues during data generation. Finally, most current enterprises have already implemented internal resource sharing functionality. The use of virtual network technology can enhance the efficiency of internal communication within enterprises, improve the management of data and resources within enterprises through the construction of data networks, and greatly improve the efficiency and security of internal work.

7. CONCLUSION

In short, the application of computer networks in various industries is becoming increasingly profound, effectively promoting the development of the social economy. Whether it is social production or learning, it is necessary to pay attention to the security issues of computer networks in the process of using them, improve the security factor of computer networks, and avoid situations such as data loss caused by computer network intrusion, which seriously affects the user experience. The use of virtual network technology can effectively protect computer network security. In computer network security management, it is necessary to fully utilize the application advantages of virtual network technology, apply virtual networks to computer networks, reduce the occurrence of computer network intrusion by viruses, illegal means, etc., and maintain the operational security of the entire network. In the process of social production and development, protecting the security of computer networks plays an extremely important role in the information security and resource management of enterprises and other users. In this regard, relevant units and individuals must fully utilize virtual technology to strengthen computer network security, maintain the stability and security of social and economic development.

REFERENCES

[1] Wang, Y., Yang, T., Liang, H., & Deng, M. (2022). Cell atlas of the immune microenvironment in gastrointestinal cancers: Dendritic cells and beyond. Frontiers in Immunology, 13, 1007823.
[2] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
[3] LI, X., & Wang, Y. (2024). Deep learning-enhanced adaptive interface for improved accessibility in e-government platforms.
[4] Yuan, J. (2024, December). Efficient techniques for processing medical texts in legal documents using transformer architecture. In 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC) (pp. 990-993). IEEE.
[5] Song, X. (2024). Leveraging aigc and human-computer interaction design to enhance efficiency and quality in e-commerce content generation.
[6] Chen, J. (2025). Efficient and Scalable Data Pipelines: The Core of Data Processing in Gig Economy Platforms.
[7] Wang, H. (2024). The Restriction and Balance of Prior Rights on the Right of Enterprise Name.
[8] Gong, C., Lin, Y., Cao, J., & Wang, J. (2024, October). Research on Enterprise Risk Decision Support System Optimization based on Ensemble Machine Learning. In Proceeding of the 2024 5th International Conference on Computer Science and Management Technology (pp. 1003-1007).
[9] Bohang, L., Li, N., Yang, J. et al. Image steganalysis using active learning and hyperparameter optimization. Sci Rep 15, 7340 (2025). https://doi.org/10.1038/s41598-025-92082-w
[10] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.
[11] Yao, T., Jian, X., He, J., & Meng, Q. (2025). Drone-3D Printing Linkage for Rapid Construction of Sustainable Post-Disaster Temporary Shelters.
[12] Yang, W., Lin, Y., Xue, H., & Wang, J. (2025). Research on Stock Market Sentiment Analysis and Prediction Method Based on Convolutional Neural Network.
[13] Ji, F., Zheng, X., Xue, H., & Wang, J. (2025). A Study on the Application of Artificial Intelligence in Personalized Go-to-Market Strategy in Retail Industry.

[14] Yang, J., Tang, Y., Li, Y., Zhang, L., & Zhang, H. (2025). Cross-Asset Risk Management: Integrating LLMs for Real-Time Monitoring of Equity, Fixed Income, and Currency Markets. arXiv preprint arXiv:2504.04292.
[15] Li, T. (2025). Optimization of Clinical Trial Strategies for Anti-HER2 Drugs Based on Bayesian Optimization and Deep Learning.

Author Profile

Mingxing Tang (1984-02-01), gender: male, ethnicity: Han, native place: Xiaochang County, Hubei Province, education: bachelor's degree, title: lecturer, research direction: computer network technology.