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

Application Exploration of Virtual Network Technology in Computer Network Security

Weiwei Zhou

Xi 'an Vocational College of Urban Construction, Xi 'an 710114, China

Abstract: ***To safeguard the security of computer network information systems and effectively address network information risks, such as Trojan viruses and hacker intrusions, it is crucial to actively employ advanced technologies. This article takes virtual network technology as its subject of study and provides a brief overview of virtual network technology and the significance of computer network security. It delves into its applications in computer network security from four aspects: technology types, application scope, real-world impact, and effective measures. The aim is to reinforce the stability of computer networks and protect user information security, providing valuable insights for relevant individuals.***

Keywords: Computer; Network Security; Virtual Network Technology; Application Exploration.

1. INTRODUCTION

In the era of big data, computer network security issues are worrying, and how to improve the level of network information security is an important direction for the development of this industry. By introducing virtual network technology, leveraging its security, reliability, flexibility, and other technological advantages, it is possible to establish a virtual private network to achieve end-to-end data information transmission, improve network information security quality, and significantly enhance computer network security protection capabilities. Xu and Lin (2024) [1] developed an empirical computer model to analyze user-perceived value's impact on NEV enterprises, while Xu et al. (2024) [2] designed innovative experience management tools for the electric vehicle market. Expanding to cross-cultural applications, Shan et al. (2024) [3] conducted a comparative analysis of large language models' implications across different cultural contexts. Healthcare AI applications have seen notable progress, with Shen et al. (2025) [4] developing an LSTM-based system for anesthetic dose management in cancer surgery. The same research team (Shen et al., 2025) [5] later applied AI to enhance robo-advisors in wealth management, while Chew et al. (2025) [6] optimized e-commerce financial risk assessment models using AI-driven data integration. Autonomous driving technology was advanced by Wang et al. (2025) [7] through their end-to-end AI system. In cybersecurity and data science, Liu et al. (2025) [8] proposed a privacy-preserving hybrid ensemble model for network anomaly detection, complemented by Guo et al. (2025) [9]'s work on handling imbalanced datasets with focal loss. Earlier foundational work by Dai et al. (2020) [10] applied text sentiment analysis to evaluate enterprise after-sales service images. Educational technology innovations were demonstrated by Huang et al. (2024) [11] through their NLP-enhanced academic assessment system. Network analysis saw advancements with Xing et al. (2024) [12]'s fuzzy spatiotemporal graph neural networks for traffic forecasting, while Wu et al. (2024) [13] explored LLM capabilities in understanding monetary policy. Public safety applications were improved by Yu et al. (2024) [14] through their crime prediction model using graph convolutional networks. LLM enhancements were further developed by Gao et al. (2024) [15] and Xi et al. (2024) [16], focusing on retrieval-augmented generation and problem-solving capabilities respectively. Financial technologies benefited from Wang (2024) [17]'s ensemble learning approach to fraud detection. Computer vision applications progressed with Peng et al. (2024) [18]'s work on 3D human pose estimation, while natural language processing was advanced by Liu et al. (2024) [19] through coreference resolution for contextual understanding.

2. BASIC SITUATION OF VIRTUAL NETWORK TECHNOLOGY

Virtual network technology mainly relies on public network resources to build dedicated information transmission channels. Through network protocols and service providers, network users from various regions are remotely connected to form virtual subnets, which can enable end-to-end information transmission between users and effectively improve the level of network information security. At the same time, the virtuality of this technology is reflected in its virtual subnet attached to the public network, where all users can use public network resources and share information with other users. Its professionalism is reflected in its ability to only access VPN users, and non VPN users cannot connect and use it, fully leveraging its application advantages such as low construction cost, easy technical management, high security performance, high data transmission efficiency, high scalability and flexibility.

If classified according to the direction of technological application, there are three main forms of virtual network technology, which are manifested as: remote access to VPN is remote access to virtual networks, which can connect the user's client to the server gateway network; Intranet VPN is an internal virtual private network that connects the VPN's internal gateway through tunneling technology; External VPN is an extended virtual network that mainly connects the VPN networks of two users to achieve network resource connection and communication, achieving collaborative promotion effect under data sharing.

3. THE IMPORTANCE OF COMPUTER NETWORK SECURITY

Based on the era of big data, the amount of information involved in computer networks has increased, and coupled with the continuous expansion of the network platform atmosphere, computers often face more complex problems, such as various viruses and Trojans infiltrating the network environment in china, it poses risks such as theft and leakage of individual user information. In view of the unique characteristics of computer network security, such as strong concealment, low threshold for users to enter the Internet, and strong concealment of their own identity information, when stealing other people's information, they can break through the barriers of time and space, connect to the network at will to obtain information, and the illegal and criminal process is very hidden, which is not easy to be found by the parties. Therefore, it is necessary to continue to maintain computer network security, do a good job in related protective work, and regularly upgrade the network information system to ensure computer network security.

At present, China attaches great importance to computer network security issues. In addition to vigorously introducing and developing virtual networks, professional technical personnel will also be hired to adjust and optimize virtual network technology, fundamentally reducing negative factors in the virtual network environment. This will help promote the health and stability of the general public when accessing the internet, prevent user information from being stolen and tampered with, and provide protection for the property security, personal privacy security, and other aspects of users.

4. THE PRACTICAL APPLICATION OF VIRTUAL NETWORK TECHNOLOGY IN COMPUTER NETWORK SECURITY

4.1 Technical type

4.1.1 Tunnel technology

Tunnel technology is the core of virtual network technology, which can improve the quality and efficiency of data transmission. It mainly relies on the router network user end to complete communication protocol encryption and address linking, build a dedicated data transmission tunnel, which can allow encapsulated data information to be transmitted through the public network in an unexpressed form. After reaching the target address, the tunnel protocol header is discarded, and the encrypted information is also unsealed, restoring the original expression of the data, fully reflecting the security and stability characteristics of this technology. At present, mainstream tunnel technology can be divided into two categories; One is the second layer tunneling protocol, such as PPTP protocol, which establishes a virtual network for remote access and connects the client and server; The second is the three-layer tunneling protocol, such as IPSec protocol, which builds internal and extended virtual private networks with higher security, mainly used for the transmission of enterprise confidential files.

4.1.2 Encryption and Decryption Techniques

Essentially, encryption and decryption technology is a further upgrade and optimization of tunneling technology, which continues the point-to-point data transmission method in tunneling technology and scientifically processes data encapsulation on this basis to transmit relevant information in the protocol. If this technology is not given enough attention in the application of computer network information, it will not only make network information more complex, but also reduce the security of data information, such as hackers invading computer networks to steal personal information, corporate secrets, etc. To this end, it is necessary to apply encryption and decryption technology reasonably, rely on the computer network system as a carrier, adopt scientific programming settings, and add security locks to data information to provide a secure and stable transmission environment for data information, maintain personal and enterprise information security, protect their legitimate rights and interests from infringement, and fundamentally improve the level of computer network security.

4.1.3 Key Management Technology

As the name suggests, this technology is applied to keys in data encryption and decryption. By following relevant basic requirements and managing the entire lifecycle process of keys, it effectively prevents risks such as key leakage and ensures data security in computer networks. The specific management content is as follows: key generation, generating relevant key data based on a pseudo-random number generator; Key storage, storing keys in dedicated memory devices to achieve secure storage of keys; Key distribution, distributing and sharing public keys for different data; Key backup and recovery are mainly aimed at ensuring the security and availability of keys to prevent them from being compromised and encrypted data information from being decrypted; Key destruction, the destruction of keys that have been used; Key archiving is the process of archiving and storing used key data, which will no longer be used for encryption in the future. Through this process, virtual network data security is ensured.

4.1.4 Identity authentication technology

Identity authentication technology is used to verify the user's identity and usage permissions by logging in to their account and entering their password, effectively preventing illegal login or access to resources. As a mature virtual network technology, it is widely used in daily life. For example, when users use online banking, WeChat and Alipay to pay, they mainly confirm their identity by entering passwords, fingerprints, or SMS verification codes to prevent others from stealing property; For example, in recent years, the anti addiction system for minors in gaming has been validated by inputting identity information or facial recognition, effectively controlling the duration of minors' gaming and recharging.

4.2 Application level

4.2.1 Network

When applying virtual network technology to the network level, the first priority should be to focus on network data centers and exchange channels, adopting comprehensive supervision of access and application network lines. This can not only achieve intelligent identification and supervision, but also improve the security of data information storage and management to prevent criminals from releasing viruses or direct attacks, effectively improving computer network security management capabilities. At the same time, it is necessary to regularly update and upgrade computer network security data, continuously promote the modernization and intelligent development of computer network technology, enhance the system's intelligent recognition ability, properly respond to computer network threats in subsequent applications, provide high security information storage conditions for users, and fully utilize the application efficiency of virtual network technology.

4.2.2 Software

Applying virtual network technology at the software level can gradually enhance the security and stability of computer networks by maintaining adaptability and adjusting protocols. From a coordination perspective, virtual network technology can reasonably allocate servers, efficiently manage various computer resources, and comprehensively enhance system data processing capabilities. In response to the open network environment, personalized virtual network design should also be implemented to eliminate unstable factors in virtual networks. By scientifically applying this technology, many personalized networks can be adjusted to further improve the security level of computer networks, and multiple verifications of user identity information can also be performed, such as password, fingerprint verification, and facial recognition, to maximize the security and stability of data transmission.

4.2.3 Equipment

Applying virtual network technology to computer devices can significantly improve the current computer network security environment through devices such as network cards, Ethernet cables, and hard drives.

Firstly, the network card is mainly used to connect the computer to the server, complete packet verification, and build dedicated links while ensuring the security of the computer network.

Secondly, network cables utilize the physical functions of virtual technology to promptly detect abnormal situations in network lines and take targeted measures to solve them, completely eliminating potential faults.

Thirdly, the application of hard disk and virtual network technology can upgrade hard disk devices in a timely manner, and cooperate with daily management and maintenance to effectively improve data storage and transmission efficiency.

4.2.4 User docking

By applying virtual network technology, the security of computer networks can be effectively enhanced, enabling users to connect with each other and achieve the goal of data information sharing, thus better expanding the available information resources. In general, there are four main points:

One is the firewall, which can connect computer hardware and software to provide security protection for data files in the computer system, especially when dealing with common threats in the network, such as hacker attacks and Trojan viruses, which can have a good defense effect.

The second is to choose the sending route. In order to reduce the risk of data leakage during communication and cooperation between users, a specific transmission route of a computer can be selected.

The third is to obtain confirmation information. In real life, identity verification uses software to streamline the process for users to obtain identity authentication. Therefore, a comprehensive verification of information should be adopted to enhance its security.

The fourth is to choose secure clients, by selecting a client with a high security factor and a scientific management system, to ensure the security and stability of all information resource storage and transmission processes, and to improve work efficiency.

4.3 Application effect

4.3.1 Enhance the security level of data information

In the operation of computer networks, security and stability are the primary concerns of technical personnel to avoid risks such as hacker intrusion, Trojan viruses, and malicious programs. Therefore, it is necessary to scientifically and reasonably use virtual network technology to ensure the security of computer network information. During this period, technicians can use virtual network technology to build a secure, reliable, efficient, and stable network operating environment, which can improve the data transmission speed between clients and servers while providing better information security services for users.

4.3.2. Quickly Complete Data Information Sharing

As a raw material, data can be divided into two types: structured and unstructured. For example, office OA systems, financial systems, etc. belong to structured data, while office documents, images, etc. belong to unstructured data. By applying virtual technology to data transmission, secondary packaging can be achieved, effectively protecting data information security, preventing it from being stolen and used by others, and also solving problems such as frame loss, making data transmission more complete. For example, applying virtual network technology to the management of educational and teaching resources in universities can not only prevent problems such as loss and incompleteness of educational resources, but also connect the education systems of different colleges and achieve the sharing of educational resources.

4.3.3 Strengthen cooperation and communication among different entities

Firstly, between the remote branch and the corporate headquarters. In the context of economic globalization, the scale of enterprises is gradually expanding, and there are branch offices in different regions. Their communication with headquarters is mainly through dedicated lines, which are expensive and inflexible. By applying virtual network technology, a data information transmission channel can be established between the two, ensuring the security of information transmission between remote branches and enterprise headquarters. It can also facilitate the supervision and management of remote branches by the enterprise headquarters, further enhancing the communication and connection between the two.

Secondly, between remote employees and other employees. In the context of the COVID-19, some employees work at home. In order to ensure the normal operation of the enterprise, these employees can use virtual network technology to connect their own computers with the enterprise network. They can access the enterprise information system remotely, promote the exchange and interaction between remote employees and other employees, and ensure the security and stability of data information transmission.

Thirdly, between enterprises. In general, business partners include suppliers, transporters, distributors, etc., and their information exchange often involves a lot of confidential information. In order to ensure the security of information exchange, virtual network technology can be applied, which not only enables face-to-face communication online, saves meeting time for both parties, but also improves work efficiency.

4.4 Application Strategy

Firstly, enhance awareness of network security. Only by ensuring that computer technicians have a good sense of prevention can we fundamentally prevent the occurrence of computer network security risks. Therefore, it is necessary to strengthen the popularization of network security knowledge education for users, actively learn network security knowledge, so that they can fully understand and recognize the importance of network security, and gradually develop good computer application habits. At the same time, the government and relevant departments should also strengthen education, publicity and guidance, carry out network security education for computer users, and use new media platforms such as Weibo and Tiktok to promote, imperceptibly helping the masses to form a good awareness of network security.

Secondly, increase efforts to protect against hackers. Compared to ordinary computer users, hackers generally have strong computer skills and can use networks to invade user clients, steal valuable and confidential information, and cause huge property losses, personal information leaks, and other problems. In the era of big data, this issue has become increasingly prominent, so it is necessary to take measures to prevent network hackers, enhance users' awareness of preventing hackers, strengthen their understanding of hackers, actively learn some advanced network security technologies, and ensure their own information security. At the same time, enterprises and institutions should actively attract computer professionals, regularly update and upgrade their firewalls, improve their own network security levels, in order to better prevent hacker attacks and ensure the security of the computer network environment.

Thirdly, establish a sound network security mechanism. On the one hand, it is necessary to improve the network usage management mechanism. Relevant departments should vigorously strengthen the supervision of bad websites, crack down on illegal websites, thoroughly clean up risky websites and URLs in the network environment, and formulate detailed legal regulations to make hackers aware of their illegal behavior; On the other hand, it is necessary to implement security protection mechanisms, establish network security officers in enterprises, introduce relevant technical personnel to ensure network security, and effectively improve the effectiveness of network security protection.

5. CONCLUSION

In summary, virtual network technology has played an important role and value in computer network security. It can improve interaction efficiency, enhance work quality, and provide convenient conditions for important data information management while ensuring the security of data information transmission. To this end, it is necessary to continuously and deeply explore virtual network technology, correctly understand the application value of this technology, conduct in-depth analysis from the technical types and application levels, and continuously ensure the security of computer networks, ensure the security of data information resources, and effectively improve work efficiency by enhancing network security awareness, increasing hacker protection, and improving network security mechanisms.

REFERENCES

[1] Xu, Y., & Lin, Y. (2024, November). Exploring the Influence of User-Perceived Value on NEV-Enterprises Using an Empirical Computer Model. In 3rd International Conference on Financial Innovation, FinTech and Information Technology (FFIT 2024) (pp. 4-10). Atlantis Press.

[2] Xu, Y., Shan, X., Guo, M., Gao, W., & Lin, Y. S. (2024). Design and application of experience management tools from the perspective of customer perceived value: A study on the electric vehicle market. World Electric Vehicle Journal, 15(8), 378.

[3] Shan, X., Xu, Y., Wang, Y., Lin, Y. S., & Bao, Y. (2024, June). Cross-Cultural Implications of Large Language Models: An Extended Comparative Analysis. In International Conference on Human-Computer Interaction (pp. 106-118). Cham: Springer Nature Switzerland.

[4] Shen, Z., Wang, Y., Hu, K., Wang, Z., & Lin, S. (2025). Exploration of Clinical Application of AI System Incorporating LSTM Algorithm for Management of Anesthetic Dose in Cancer Surgery. Journal of Theory and Practice in Clinical Sciences, 2, 17-28.

[5] Shen, Z., Wang, Z., Chew, J., Hu, K., & Wang, Y. (2025). Artificial Intelligence Empowering Robo-Advisors: A Data-Driven Wealth Management Model Analysis. International Journal of Management Science Research, 8(3), 1-12.

[6] Chew, J., Shen, Z., Hu, K., Wang, Y., & Wang, Z. (2025). Artificial Intelligence Optimizes the Accounting Data Integration and Financial Risk Assessment Model of the E-commerce Platform. International Journal of Management Science Research, 8(2), 7-17.

[7] Wang, Y., Shen, Z., Hu, K., Yang, J., & Li, C. (2025). AI End-to-End Autonomous Driving.

[8] Liu, S., Zhao, Z., He, W., Wang, J., Peng, J., & Ma, H. (2025). Privacy-Preserving Hybrid Ensemble Model for Network Anomaly Detection: Balancing Security and Data Protection. arXiv preprint arXiv:2502.09001.

[9] Guo, X., Cai, W., Cheng, Y., Chen, J., & Wang, L. (2025). A Hybrid Ensemble Method with Focal Loss for Improved Forecasting Accuracy on Imbalanced Datasets.

[10] Dai, Yonghui, et al. "Research on image of enterprise after-sales service based on text sentiment analysis." International Journal of Computational Science and Engineering 22.2-3 (2020): 346-354.

[11] Huang, Xinyi, et al. "Improving Academic Skills Assessment with NLP and Ensemble Learning." 2024 IEEE 7th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE, 2024.

[12] Xing, Jinming, et al. "Network Traffic Forecasting via Fuzzy Spatial-Temporal Fusion Graph Neural Networks." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.

[13] Wu, Yingyi, et al. "Can LLaMA 3 Understand Monetary Policy?." 2024 17th International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE, 2024.

[14] Yu, Chenyang, et al. "Crime Prediction Using Spatial-Temporal Synchronous Graph Convolutional Networks." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.

[15] Gao, Min, et al. "Leveraging Large Language Models: Enhancing Retrieval-Augmented Generation with ScaNN and Gemma for Superior AI Response." 2024 5th International Conference on Machine Learning and Computer Application (ICMLCA). IEEE, 2024.

[16] Xi, Kai, et al. "Enhancing Problem-Solving Abilities with Reinforcement Learning-Augmented Large Language Models." 2024 4th International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI). IEEE, 2024.

[17] K. Wang, "Efficient Financial Fraud Detection: An Empirical Study using Ensemble Learning and Logistic Regression," 2024 IEEE 6th International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 2024, pp. 859-864, doi: 10.1109/ICPICS62053.2024.10796380.

[18] Peng, Qucheng, Ce Zheng, and Chen Chen. "A Dual-Augmentor Framework for Domain Generalization in 3D Human Pose Estimation." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 2240-2249. 2024.

[19] Y Liu, X Peng, J Cao, S Bo, Y Shen, X Zhang, et al., "Bridging Context Gaps: Leveraging Coreference Resolution for Long Contextual Understanding", arxiv e-prints, Oct. 2024.

[20] Liu, Yanming, et al. "Tool-Planner: Task Planning with Clusters across Multiple Tools." arXiv preprint arXiv:2406.03807 (2024).

Author Profile

Weiwei Zhou (1983.7), female, Han, Shaanxi, lecturer, undergraduate, research direction: network technology.