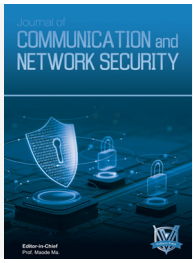
Journal of Communication and Network Security (JCNS)

DOI:http://doi.org/10.65098/jcns.01.2026.12.14



RESEARCH ARTICLE

RESEARCH ON INFORMATION SECURITY ASSURANCE MEASURES IN NETWORK COMMUNICATION

Zhichao Wei

China Mobile Group Shanxi Co., Ltd.
**Corresponding Author E-mail: Esther_Editor@volksonpress.com*

ARTICLE DETAILS

Article History:

Received 18 Oct 2025
Accepted 15 Dec 2025
Available online 9 Feb 2026

Online Article Code

ABSTRAST

Background and Purpose: With the rapid development and widespread application of network technology, network communication security is facing increasingly severe challenges. This study aims to systematically analyze current information security threats in network communication and explore effective approaches to improving its security and reliability.
Methods: The research conducts an in-depth analysis from three dimensions: risk analysis, technical assurance, and management measures. It examines major security threats, vulnerabilities, and typical attack methods in network communication, and discusses optimization strategies for encryption technologies, identity authentication, access control, security monitoring, and early warning systems, as well as relevant security management practices.
Results: The analysis reveals the severity and complexity of current network communication security threats. The proposed technical and management measures contribute to enhancing the effectiveness of security protection and improving overall network communication reliability.
Conclusion: The study indicates that addressing network communication security challenges requires a comprehensive protection system integrating both technical solutions and management measures, providing reliable security assurance for network communication in the digital age.

KEYWORDS

Network Communication Security, Information Encryption Technology, Identity Authentication, Security Monitoring and Early Warning, Emergency Response Mechanism

1. INTRODUCTION

With the rapid development of information technology and the deepening of network applications, network communication has become an important foundation for the operation of modern society. The information security threats faced in network communication are becoming more and more severe, affecting all aspects of people's lives. Especially against the background of accelerated digital transformation, governments, enterprises, and individuals are increasingly dependent on network communication, and network communication security issues have become prominent.

In recent years, global cybersecurity incidents have occurred frequently. Especially during the COVID-19 pandemic, various information and communication technology accidents emerged one after another, seriously affecting the national economic and social order. According to statistics, the number of global cybersecurity incidents in 2023 increased by more than 35% compared with the previous year, causing economic losses of hundreds of billions of US dollars. Due to inherent vulnerabilities in the network itself, a large amount of information is leaked, tampered with, or stolen, which seriously affects people's normal work and living order, and even threatens national economic security. Under such circumstances, the research on information security assurance mechanisms in network communication has important practical significance. Network communication security involves multiple dimensions such as technology, management, and law, and requires the construction of an all-around protection system. As network attack methods are constantly innovated, traditional security protection measures have been difficult to cope with new types of network threats. Therefore, in-depth research on network communication security risks, exploration of advanced technical assurance methods, and improvement of the security management system are of great value for improving the level of network communication security and ensuring the stable operation of information systems. China's network communication is facing many severe challenges, and how to ensure information security in the complex and diverse cyberspace has become an urgent problem to be solved.

This study will start with risk analysis, systematically discuss the technical measures and management countermeasures for network communication security assurance, and provide a reference for building a more secure and reliable network communication environment.

2. ANALYSIS OF NETWORK COMMUNICATION SECURITY RISKS

2.1 Main Threats Faced by Network Communication

Network communication systems are confronted with diverse security threats that directly affect the confidentiality, integrity, and availability of information transmission. The primary threat comes from the deliberate sabotage of malicious attackers, who steal sensitive data and disrupt system operations through various technical means. Secondly, there are internal threats, including the risks of operational errors, irregular operations by staff, and internal data leakage. The third type of threat stems from the security flaws of hardware equipment and software systems themselves, such as equipment failures and system vulnerabilities. In addition, network communication systems may also be threatened by natural disasters and other irresistible external factors.

2.2 Analysis of Security Vulnerabilities and Attack Methods

Security vulnerabilities in network communication are mainly manifested in protocol design, system configuration, application programs, and user behaviors (Zhu, 2023). Among them, the protocol layer is one of the weakest links in network information security. The TCP/IP protocol suite has inherent security weaknesses and is vulnerable to man-in-the-middle attacks, session hijacking, and other threats. Vulnerabilities in system configuration include unchanged default passwords, improper access permission settings, and delayed updates of security patches. Application program vulnerabilities involve common issues such as SQL injection, cross-site scripting attacks, and buffer overflows. A large number of potential vulnerabilities also arise during network connections and transmission. In response to these vulnerabilities, attackers usually adopt methods such as Distributed Denial of Service (DDoS) attacks, phishing, ransomware, and Advanced Persistent Threats (APT), which exert a significant impact on network communication security.

2.3 Analysis of Security Incident Cases

Major cybersecurity incidents that have occurred in recent years have provided us with profound warnings (Pan & Cheng, 2024). In 2021, Colonial Pipeline Company in the United States was attacked by ransomware, resulting in a business interruption of nearly a week and widespread fuel supply shortages. Analysis indicates that the attackers invaded the system using a VPN account not protected by two-factor authentication, highlighting the importance of identity authentication mechanisms. In 2022, a well-known social platform suffered a large-scale data leakage incident, with more than 500 million users' information illegally obtained. The reason was that there were design flaws in the API interface, and the data encryption and storage mechanism were imperfect. In 2023, many financial institutions around the world encountered DDoS attacks, with the peak attack traffic reaching hundreds of Gbps, demonstrating that traditional protection methods are difficult to cope with new types of attack threats. These cases reveal the weak links in the network security protection system and emphasize the urgency of strengthening security protection.

3. NETWORK COMMUNICATION SECURITY TECHNICAL ASSURANCE SYSTEM

3.1 Application and Optimization of Encryption Technology

Encryption technology is the core means to ensure network communication security. By encrypting data, it guarantees the confidentiality and integrity of information during transmission (Zheng, 2024). With the continuous development of computer and network technology, people have paid increasing attention to the research and application of encryption technology. At present, the widely used encryption technologies mainly include symmetric encryption and asymmetric encryption. Symmetric encryption algorithms such as AES and SM4 have the characteristics of fast encryption speed and high efficiency, making them suitable for real-time encrypted transmission of large amounts of data. Asymmetric encryption algorithms such as RSA and ECC, although having high computational overhead, offer higher security and are mainly used for key exchange and digital signatures.

In practical applications, it is necessary to optimize the encryption scheme according to the characteristics of the business scenario. For example, for high-concurrency data transmission, block encryption technology can be adopted, supplemented by an efficient key management mechanism; for resource-constrained scenarios such as the Internet of Things, lightweight encryption algorithms can be selected to reduce computational load while ensuring security. The development of quantum computing technology poses challenges to the existing encryption system. It is imperative to conduct timely research and deploy post-quantum cryptography algorithms to make technical reserves for future network security.

3.2 Identity Authentication and Access Control Mechanisms

Reliable identity authentication and refined access control are important guarantees for ensuring network communication security (Liu et al., 2023). With the rapid development of network technology and the continuous increase in user application demands, traditional identity authentication and access control methods can no longer meet the current complex and diverse network security environment. Modern identity authentication mechanisms have evolved from single username-password authentication to multi-factor authentication systems, combining multiple methods such as biometric identification, hardware tokens, and SMS verification codes, which have significantly enhanced the security of identity verification. The introduction of the zero-trust security architecture has further strengthened the authentication mechanism, requiring strict identity verification and permission validation for each access request. In terms of access control, the Role-Based Access Control (RBAC) model has been widely applied, realizing flexible access control through role assignment and permission management; the Attribute-Based Access Control (ABAC) model can make more accurate access control decisions based on dynamic factors such as user attributes and environmental status. The principle of least privilege requires users to only possess the minimum permissions necessary to complete their work, which can effectively reduce the risk of permission abuse.

To improve the availability of authentication and access control, a unified identity authentication center can be established to achieve single sign-on and centralized permission management. Additionally, behavior analysis technology can be introduced to conduct real-time monitoring and analysis of user access behaviors, promptly detect abnormal requests, and prevent identity theft and unauthorized access.

3.3 Construction of Security Monitoring and Early Warning Systems

Network security monitoring and early warning systems are the key support for realizing network security situation awareness and active defense. In response to the problems existing in current network security detection methods, a network anomaly detection system based on big data mining technology is designed. The system collects multi-dimensional information such as network traffic, system logs, and application data in real time by deploying distributed probes, and uses big data analysis and machine learning algorithms to conduct in-depth analysis of massive data, thereby improving the ability to identify unknown threats.

In terms of system architecture, a three-layer structure of "collection-analysis-response" is generally adopted. The data collection layer is responsible for real-time acquisition of traffic, logs, and asset information; the analysis and processing layer integrates rule engines and AI algorithms to conduct in-depth analysis and threat detection of collected data; the response and processing layer automatically triggers protective measures according to the analysis results, such as blocking suspicious connections or isolating infected devices.

The design of the early warning mechanism needs to balance real-time performance and accuracy. Multi-level early warning thresholds can be set, and the disposal processes for security incidents of different severity levels can be clarified. By integrating with the threat intelligence sharing mechanism, the latest attack methods and vulnerability information

can be promptly obtained. The security monitoring system should also be equipped with visualization technology to help managers quickly grasp the network security situation through intuitive data display and situation analysis. Regular evaluations and optimizations of system performance should be conducted to ensure that it can adapt to emerging network environments and security threats.

4. NETWORK COMMUNICATION SECURITY MANAGEMENT MEASURES

4.1 Construction of Security Management Systems

Establishing a sound network security management system is the institutional foundation for achieving security assurance. Against the backdrop of the increasingly complex and diverse network environment in China, how to establish and improving an effective network security management mechanism has become an urgent problem to be solved.

Firstly, it is necessary to formulate an overall plan for network security management, clarify security goals, organizational structure, and division of responsibilities, and build a hierarchical management system in parallel, including security policies, operating procedures, technical standards, etc., to ensure that various security measures are carried out in accordance with regulations. Secondly, it is essential to improve the data classification and grading management system, adopt differentiated protection strategies based on data sensitivity, and establish a regular system evaluation and update mechanism to promptly adjust and improve in response to changes in the security situation. The implementation of the system can be linked to performance appraisal, and the effective implementation of various requirements can be promoted through reward and punishment mechanisms. Regular audits on the implementation of the system should be conducted to promptly identify and rectify problems, thereby ensuring the effectiveness of the system implementation.

4.2 Training of Personnel's Security Awareness

Personnel's security awareness and skills are an important cornerstone of network security protection. To ensure enterprise information security, it is necessary to attach importance to the cultivation of employees' security awareness and operational skills. A systematic security training plan should be formulated to carry out differentiated training for personnel in different positions: management focuses on security strategy and risk decision-making, technical personnel focus on new technologies and threat response, and ordinary users focus on basic security knowledge and operational specifications. The training method can combine theoretical explanation, case analysis, and practical drills, and the interest and participation in training can be enhanced by organizing activities such as security knowledge competitions and protection skills contests. An evaluation mechanism for training effects should be established to test learning outcomes through examinations, assessments, and other methods, and the coverage of training should be expanded through diversified means such as network platforms and mobile terminals. By regularly conducting security awareness assessments, such as simulated phishing emails and social engineering tests, the weak links of employees in security awareness can be promptly identified and improved. Efforts should be made to create a network security culture atmosphere, so that all employees realize that network security is not only a technical issue but also the responsibility of everyone.

4.3 Improvement of Emergency Response Mechanisms

Faced with increasingly complex network security threats, an efficient emergency response mechanism is crucial. Under the current situation, how to improve the response capacity in network emergencies is an urgent problem to be solved. Firstly, a professional emergency response team should be established to clarify the team's responsibilities and work processes. Detailed emergency plans should be formulated, establishing standardized disposal processes and technical means for different types of security incidents, and reserving necessary technical tools and professional talents. At the same time, it is necessary to improve the linkage mechanism of early warning, reporting, and response, and carry out 24/7 emergency on-duty to ensure that security incidents are detected and disposed of in a timely manner. The emergency response process should be standardized, including incident reporting, level determination, emergency disposal, cause analysis, and follow-up rectification, and cross-departmental linkage should be activated when necessary. Regular emergency drills should be organized to test the feasibility of the plan through tabletop exercises and actual combat drills, identify deficiencies, and make timely improvements. In addition, attention should be paid to post-event summary and continuous improvement, conduct in-depth analysis of the management and technical vulnerabilities exposed by security incidents, and take targeted improvement measures. Only through repeated drills and improvements can the ability to respond to cybersecurity incidents be continuously enhanced.

5. CONCLUSION

Through the systematic research on network communication security risks and assurance measures, it can be concluded that a comprehensive protection system combining technology and management should be built to respond to the evolving network security threats. At the technical level, it is necessary to combine a variety of advanced means to strengthen encryption technology, optimize identity authentication and access control, and improve security monitoring and early warning systems, thereby constructing a in-depth defense network; at the management level, emphasis should be placed on system construction, strengthening personnel training, and improving emergency response mechanisms to provide institutional and human guarantees for security protection. In the future, with the rapid development of new technologies and the continuous emergence of new threats, technological innovation and management innovation should be promoted simultaneously. On the one hand, strengthen forward-looking research and promptly apply new technologies to the protection system; on the other hand, improve existing protection measures and management systems through continuous practice and summary. Only by integrating technology and management can we build a stronger network communication security defense line in the digital age and provide a solid and reliable guarantee for the steady development of the information society.

REFERENCES

Liu, Y., Li, Y., & Chen, S. (2023). A survey of internet of vehicles security based on blockchain. *Science China: Information Sciences*, *53*(5), 841–877. https://doi.org/10.1016/j.dcan.2022.12.019

Pan, W., & Cheng, C. (2024). Uniting as one for development and forging ahead into the future: Deputies and members of the 2024 National Two Sessions put forward suggestions for emergency management and work safety. *China Work Safety*, *19*(3), 8–31.

Zheng, Z., He, J., Tang, L., et al. (2024). Key theories and cutting-edge applications of privacy computing. *China Science Fund*, *38*(4), 603–611.

Zhu, X. (2023). Analysis of data information security assurance technology in network communication. *Electronic Quality*, (12), 65–68.