Analysis of Feasible Solutions for Railway 5G Network Security Assessment

XU Hang[1], SUN Bin[1], DING Jianwen[1], WANG Wei[2]
(1. Beijing Jiaotong University, Beijing 100044, China;
2. ZTE Corporation, Shenzhen 518057, China)

DOI: 10.12142/ZTECOM.202503007
https://kns.cnki.net/kcms/detail/34.1294.TN.20250805.1051.002.html, published online August 5, 2025
Manuscript received: 2024-01-26

Abstract: The Fifth Generation of Mobile Communications for Railways (5G-R) brings significant opportunities for the rail industry. However, alongside the potential and benefits of the railway 5G network are complex security challenges. Ensuring the security and reliability of railway 5G networks is therefore essential. This paper presents a detailed examination of security assessment techniques for railway 5G networks, focusing on addressing the unique security challenges in this field. In this paper, various security requirements in railway 5G networks are analyzed, and specific processes and methods for conducting comprehensive security risk assessments are presented. This study provides a framework for securing railway 5G network development and ensuring its long-term sustainability.

Keywords: railway 5G network; 5G-R; information security; risk assessment; penetration testing

Citation (Format 1): XU H, SUN B, DING J W, et al. Analysis of feasible solutions for railway 5G network security assessment [J]. ZTE Communications, 2025, 23(3): 59 - 70. DOI: 10.12142/ZTECOM.202503007
Citation (Format 2): H. Xu, B. Sun, J. W. Ding, et al., "Analysis of feasible solutions for railway 5G network security assessment," *ZTE Communications*, vol. 23, no. 3, pp. 59 - 70, Sept. 2025. doi: 10.12142/ZTECOM.202503007.

1 Introduction

The rapid integration of 5G technology has driven the railway industry to explore its potential applications in addressing the evolving demands of railway mobile communication systems. The railway 5G communication system, a specialized iteration of 5G, is designed to provide more efficient and reliable communication services for railway operations and safety management[1].

In railway 5G networks, there are two main types of non-public networks (NPN): the railway 5G standalone NPN, standardized as the Fifth Generation of Mobile Communications for Railway (5G-R), and the railway 5G public network integrated NPN (PNI-NPN). Each configuration presents unique backgrounds and characteristics.

Specifically, 5G-R is a dedicated 5G private network independently constructed by the railway sector to meet its specific operational and management communication requirements, exclusively for internal railway use. In contrast, the railway 5G PNI-NPN leverages the public networks of telecommunications operators (e.g., the Mobile, Telecom, and Unicom) to support various railway services. These two systems are entirely independent and isolated, with no interchangeability of terminals. The characteristics and differences between the 5G-R network and the railway public dedicated network are outlined in Table 1. Both the 5G-R network and the railway 5G PNI-NPN play crucial roles in ensuring the secure

Table 1. Differences between 5G-R network and railway 5G PNI-NPN

Aspect	5G-R Network	Railway 5G PNI-NPN
Construction department	Railway Department	Operators
Carried services	Critical services such as operational safety, running, and service tasks	Non-critical services like passenger communication services and general data transmission
Network frequency band	Independent frequency band for railways	Shared operator frequency bands
Network architecture	Closed, independent network architecture specific to railways	Public 5G network architecture
Performance requirements	High reliability, low latency, high speed, and high security	General performance requirements

5G-R: the Fifth Generation of Mobile Communications for Railway
PNI-NPN: public network integrated non-public network

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant No. 2025JBXT010, in part by NSFC under Grant No. 62171021, in part by the Project of China State Railway Group under Grant No. N2024B004, and in part by ZTE Industry-University-Institute Cooperation Funds under Grant No. I23L00010.

and reliable operation of railway 5G systems. Therefore, an effective network security assessment approach is necessary to evaluate the safety performance of railway 5G networks.

However, current generalized network security assessment techniques fail to meet the specialized demands of railway 5G networks. Moreover, comprehensive approaches for identifying network vulnerabilities specific to railway 5G networks remain insufficient. Both the 5G-R network and the railway 5G PNI-NPN encounter complex network security challenges and require dedicated assessment methods.

In light of these circumstances, this paper aims to ensure the security and reliability of railway 5G communication systems by analyzing the distinct network security requirements of the two modes: the 5G-R network and the railway 5G PNI-NPN. This study presents feasible solutions for railway 5G security assessment, offering actionable guidance for network security assessment and security strategy deployment in future railway communication systems.

2 Railway 5G Network Security Requirements

The new-generation railway communication network, leveraging 5G technology, features a novel architecture and incorporates cutting-edge technologies. While demonstrating significant potential and advantages, this system faces diverse, complex, and unpredictable security threats with substantial latent risks. To mitigate these vulnerabilities, this section comprehensively examines the security requirements for both the 5G-R network and the railway 5G PNI-NPN, alongside the associated information security management framework.

2.1 5G-R Network Security

Ensuring the security and reliability of the 5G-R network necessitates the integration of robust network security measures throughout design and deployment phases. This integration is fundamental to meet essential technical security requirements including confidentiality, integrity, availability, robustness, and scalability. Consequently, a multidimentional assessment of 5G-R security requirements is indispensable, encompassing physical security environments, network architectures, network domains, terminals, and operational support systems.

To address the diverse security demands across different sectors and levels within the 5G-R network, a security architecture is established, as shown in Fig. 1. This architecture divides the security requirements of the 5G-R system into three core layers: the application stratum, home network stratum /serving network stratum, and transport stratum. The requirement comprises network access security, network domain security, subscriber domain security, application domain security, service-based architecture (SBA) security, and security visibility and configurability[2].

1) Network access security: The network access security requirements of 5G-R networks primarily involve authentication and access authorization for network entry. These mechanisms ensure secure access and authentication for user equipment (UE) accessing via both 3GPP access and non-3GPP access protocols[3].

2) Network domain security: The network domain in 5G-R systems constitutes the fundamental platform for 5G-R network service provisioning. Its security plays a crucial role in facilitating the secure transmission of data and control signaling among network nodes. The security scope covers critical components including the core network, transmission network, access network, mobile edge computing (MEC), and mission-critical (MC) service platform[4].

3) Subscriber domain security: Subscriber domain security covers terminal devices, SIM cards, terminal access networks, service providers, and related protocols and technologies for authentication and authorization, access control, data encryption, integrity protection, and trustworthiness verification[5]. These security measures are designed to ensure user privacy, security, and confidentiality when using the 5G-R network[6].

4) Application domain security: Application domain secu-

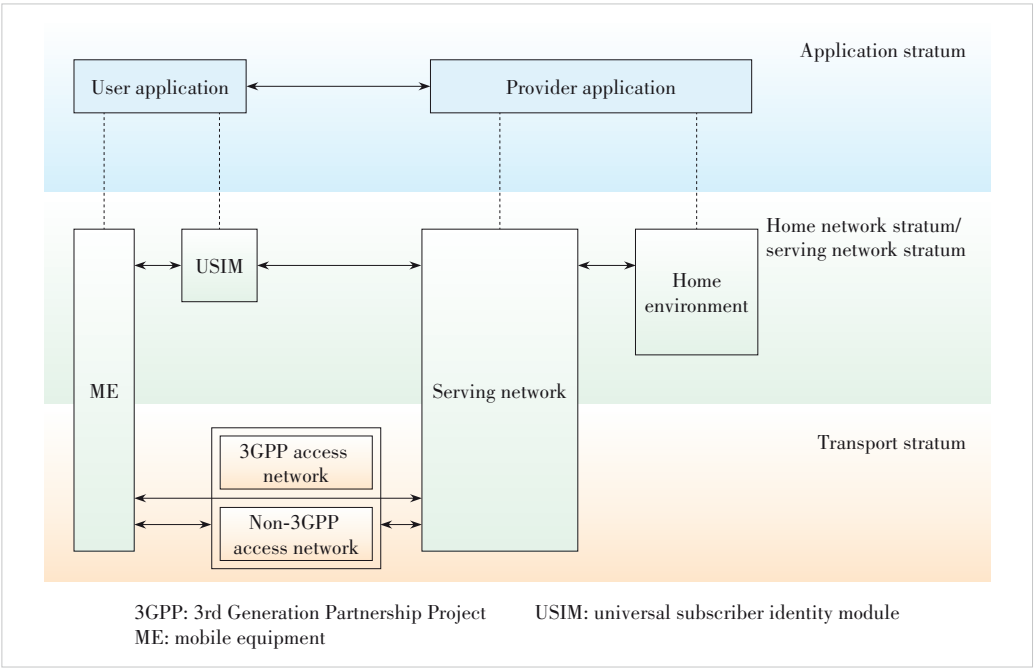

Figure 1. Security architecture for the Fifth Generation of Mobile Communications for Railways (5G-R) network

rity guarantees secure information exchange between user applications and service providers while protecting application-layer privacy from unauthorized access.

5) SBA domain security: SBA in the 5G-R system segments network functions into reusable services, which enables high efficiency, software-driven capabilities, and openness, all being an integral characteristic of the 5G-R network. SBA domain security is pivotal in ensuring secure communication among SBA-based network functions, both within the network and across different network domains. This security framework encompasses functions such as network registration, service discovery, dynamic authorization, and the guarantee of the security of service network interfaces[2].

6) Security visibility and configurability: Security visibility and configurability enable users to conveniently monitor the operational status of security features. In the 5G-R network, although security features are typically concealed from endpoints or applications, there arises the need for specific events to offer the capability to present relevant access stratum (AS) and non-access stratum (NAS) security features in operation. Additionally, authenticated 5G-R users should have the ability to configure specific security feature settings on UE. This allows users to manage additional capabilities or leverage specific advanced security features.

2.2 Railway 5G PNI-NPN Security

The railway 5G PNI-NPN delivers the transportation of services associated with the railway communication system through public 5G networks. Consequently, secure communication and interaction are required between the public network and the railway communication system to exchange data and services. This interaction between the railway 5G PNI-NPN and the 5G-R system creates an interconnection which introduces potential security risks. Therefore, it is imperative to analyze and understand the security requirements of this interaction.

When the railway 5G PNI-NPN and 5G-R network interoperate, establishing boundaries between them is essential. However, these boundaries may become vulnerable targets for attacks. Adversaries could exploit these boundaries to bypass security measures or launch attacks, threatening network security. Moreover, during data transmission between the railway 5G PNI-NPN and the 5G-R network, there are risks of interception, eavesdropping, tampering, or data destruction. Unencrypted data transmission may lead to data leakage and integrity issues.

Addressing the security risks in the railway 5G PNI-NPN and 5G-R network collaboration necessitates additional security measures. These measures are crucial to ensure secure data transmission and interoperability between the two networks.

1) Confidentiality protection: To maintain the security of data transmitted between the railway 5G PNI-NPN and 5G-R network, preventing unauthorized access is crucial. Implementing data encryption (including end-to-end and transmission encryption) protects data confidentiality. Furthermore, deploying corresponding attack protection technologies becomes essential to ensure the security of data shared between the railway 5G PNI-NPN and the 5G-R network.

2) Integrity protection: To prevent data tampering or corruption during transmission, it is essential to implement measures such as data integrity checks and digital signatures at the boundary between the railway 5G PNI-NPN and 5G-R network. These measures verify the integrity of data entering and exiting both the networks.

3) Authentication: To guarantee the legitimacy and authorization of networks, devices, and other components involved in the communication between the railway 5G PNI-NPN and 5G-R network, preventing unauthorized access is crucial. This is achieved through two-factor authentication, certificates, and tokens to validate user and device identities.

4) Network availability: To ensure continuous network and system availability for legitimate users in both the railway 5G PNI-NPN and the 5G-R network, protection against denial-of-service (DoS) attacks and hardware failures is essential. Deploying data and traffic intrusion detection systems, along with load balancing and redundancy mechanisms between the railway 5G PNI-NPN and the 5G-R network, is imperative to safeguard data integrity and maintain network availability across the public-private and private networks.

5) Update and vulnerability management: Regular vulnerability scans should be conducted on the 5G public network to identify potential weaknesses. The operating systems, applications, and network devices must be promptly updated to address security vulnerabilities. This proactive approach helps prevent the lateral movement of security threats and enables timely responses to emerging threats.

6) Data encryption: All data transmitted between the railway 5G PNI-NPN and the 5G-R network must be encrypted. Tailored data encryption strategies are developed based on specific business requirements, which may include encrypting the entire data transmission process or selectively encrypting data entering and exiting the private network. These measures enhance the confidentiality, integrity, and availability of data, ensuring secure and reliable network communications.

The integration between the railway 5G PNI-NPN and 5G-R systems introduces notable security challenges. This interaction demands meticulous attention to security requirements to ensure robust network transmission and interoperability. The imperative exchange of data and services between the railway 5G PNI-NPN and railway communication systems necessitates prioritized protection of data confidentiality, integrity, and availability. Consequently, comprehensive security measures must be implemented to address potential risks such as data leakage, tampering, and DoS attacks, thereby ensuring secure data transmission.

Simultaneously, the 5G-R network itself requires rigorous security considerations, encompassing network access secu-

rity, network domain security, user domain security, SBA domain security, and security visibility and configurability. To address these requirements, implementing data encryption, integrity verification, and identity authentication measures is essential for ensuring data confidentiality and integrity. These security protocols enable secure transmission and interoperability between the railway 5G PNI-NPN and 5G-R systems, while mitigating potential security risks and preserving the credibility of network communication.

Besides the specific security requirements discussed above, both systems share additional common security needs such as privacy protection and network isolation. Table 2 summarizes the security requirements of 5G-R networks and railway 5G PNI-NPN systems.

2.3 Network Information Management

As the next-generation mobile communication infrastructure for railways, the railway 5G communication system plays a pivotal role in ensuring the safety and stability of railway transportation. The seamless operation of both the 5G-R network and the railway 5G PNI-NPN is crucial due to their transmission of highly sensitive data including train locations, passenger information, and transportation plans. Any potential leakage or tampering of this critical data in the railway 5G communication system could result in severe consequences. Given that railway 5G communication systems comprise numerous interconnected end devices, terminals, and sensors interacting with external networks, they face an intricate threat landscape that heightens their vulnerability to various cyber threats such as malware infections, cyberattacks, and ransomware incidents. Therefore, the information management system of railway 5G networks must satisfy the following core requirements:

1) Security and reliability: The railway 5G network must guarantee secure and reliable communications, ensuring both sensitive data protection and communication integrity.

2) Threat identification and mitigation: The system proactively identifies and mitigates potential threats and vulnerabilities in the network, effectively addressing security weaknesses.

3) Performance monitoring: Continuous monitoring of network performance and configuration is required to ensure the ongoing effectiveness of security policies.

4) Resource allocation and planning: Systematic allocation and strategic planning of network resources are required to enhance security and efficiency of the network.

5) Sensitive data management: The railway 5G communication system places a high priority on managing sensitive data, encompassing train operations and passenger information, to protect against unauthorized access and data breaches and ensure that all sensitive information is handled responsibly and securely.

A comprehensive and efficient network security assessment framework is essential to safeguard the railway communication system against potential cyber threats, data breaches, and service disruptions. It ensures uninterrupted training operations and positions the system to meet future communication requirements while adhering to regulatory mandates. Such information management security assessment constitutes a fundamental requirement for ensuring the continuous safe operation of the railway 5G network.

3 Overview of Network Security Assessment Methods

Network security assessment technology, particularly relevant to 5G railway networks, involves various technical methodologies to evaluate and fortify the security of network systems. In the railway 5G context, these assessments are crucial for understanding the unique security challenges and implementing measures to mitigate threats to passenger safety and operational integrity. Cybersecurity assessments in this domain enable the identification of risks that could lead to cyber intrusions, data breaches, or service disruptions.

The main cybersecurity assessment methods suitable for the railway 5G network include:

1) Risk-based security assessment: This method prioritizes threats and vulnerabilities based on their potential impact on critical railway operations. Through collaboration between testers and security experts to identify and categorize threats, it ensures that resources are focused on the most significant vulnerabilities[7].

2) Penetration testing: Especially important for 5G railway networks, penetration testing simulates attacks to identify

Table 2. Security requirements of 5G-R network and railway 5G PNI-NPN

Security Aspects	5G-R Network	Railway 5G PNI-NPN
Privacy protection	Industry-tailored privacy protection	Customer data privacy enforcement
Network isolation	Granular network segmentation	Service-level isolation enforcement
Security auditing	Strict audit and monitoring protocols	Comprehensive periodic audits
Reliability	Railway-operation-specific reliability	High-availability service maintenance
Attack protection	Industry-specific threat mitigation	Specific railway attack prevention
Data encryption	Mandatory strong encryption standards	End-to-end data encryption implementation
Updates & patches	Frequent security patch deployment	Timely critical update application

5G-R: the Fifth Generation of Mobile Communications for Railway PNI-NPN: public network integrated non-public network

weaknesses. It mimics potential attacker behavior to uncover real threats, which is vital in a railway context where the consequences of a breach can be severe. This method provides valuable insights into enhancing security in a railway-specific environment.

3) Vulnerability scanning: While providing a proactive approach to detect and resolve security issues, its role in the railway 5G network is somewhat limited due to its focus on known vulnerabilities. It might not fully address the complex threat landscape of the railway 5G network.

4) Red team/blue team exercises: While useful for testing system resilience and response mechanisms, these exercises require substantial resources and time. They may prove impractical for ongoing security assessments in operational railway 5G networks.

In the railway 5G network context, the intricacy and criticality of the network, combined with sophisticated potential threats, make risk-based security assessment and penetration testing the most effective methods. However, their successful implementation requires tailored adaptations to address specific railway-related security challenges. Risk assessments should concentrate on vulnerabilities in communication systems and network privacy data protection, with an emphasis on information safety impacts. Penetration testing, meanwhile, must be tailored to simulate threats unique to railway 5G, such as attacks on communication systems and signal disruptions. These tests need to consider the distinct structure of railway networks, including control centers and track systems. By customizing these approaches, they can more accurately reflect actual threats to the railway 5G network, facilitating the development of robust security frameworks that simultaneously support secure digital transformation and ensure operational safety across rail infrastructure.

4 Railway 5G network Security Risk Assessment System

The network security assessment of both the 5G-R network and the railway 5G PNI-NPN requires strict compliance with established standards and specifications. Given the established fundamental process in standard specifications and their shared support for railway-related services, they share consistent security assessment techniques. The security risk assessment system for railway 5G networks comprises two crucial components: railway 5G network security risk assessment and vulnerability identification in railway 5G networks. These two elements work collaboratively to evaluate and enhance the railway 5G network security.

1) Railway 5G network security risk assessment: The systematic approach and specific techniques for conducting risk assessments of the railway 5G network are detailed in Section 4.1.

2) Railway 5G network security vulnerability identification: Section 4.2 focuses on penetration testing methods for identifying vulnerabilities within the risk assessment process.

3) Deployment guidelines for railway 5G network security assessment: To implement the railway 5G network security assessment process and collective methods presented in Sections 4.1 and 4.2, this study focuses on developing practical implementation guidelines for both the 5G-R network and the railway public-private network.

4.1 Railway 5G Network Security Risk Assessment Process

The security risk assessment process for railway 5G networks comprises three primary stages: pre-assessment preparation, element identification, and risk analysis[8], as illustrated in Fig. 2.

4.1.1 Preparation for Railway 5G Network Assessment

To ensure the precision and efficacy of the security risk assessment for the railway 5G network, several preliminary preparations are indispensable. Before commencing the network security risk assessment, it is imperative to determine the assessment scope, gather relevant information, establish the assessment methodology, define the assessment criteria, assemble a proficient team for evaluation purposes, and formulate a comprehensive assessment plan. One of the primary tasks involves precisely defining both the object and scope of the security assessment for the railway 5G network. The scope typically encompasses various aspects such as network system topology, network communication protocols, network devices, network services, and network operating systems.

4.1.2 Element Identification for Risk Assessment

The identification of elements related to assets, threats, and vulnerabilities plays a fundamental role in executing network security assessments for railway 5G networks. This process forms the basis for developing customized security strategies, which are crucial for protecting sensitive information, enhancing risk management, and ultimately ensuring the reliability and security of railway communication networks.

1) Identification of assets in railway 5G networks

The assets within a railway 5G network can be categorized into various components, including hardware, software, communication elements, communication links, network data, physical infrastructure settings, and personnel involved in network operations. The identification of these assets primarily focuses on evaluating their fundamental attributes such as confidentiality, integrity, and availability. By assessing the value and key characteristics of these assets through weighted calculations, their significance within the railway 5G network can be quantitatively determined.

2) Identification of threats to railway 5G networks

Threats to railway 5G networks are present in diverse forms, including malicious activities, eavesdropping, surveillance, interception, physical attacks, intentional and unintentional damages, network disruptions, equipment failures, and natural catastrophes. These threats are classified by their target domains, covering core networks, access networks, bearer

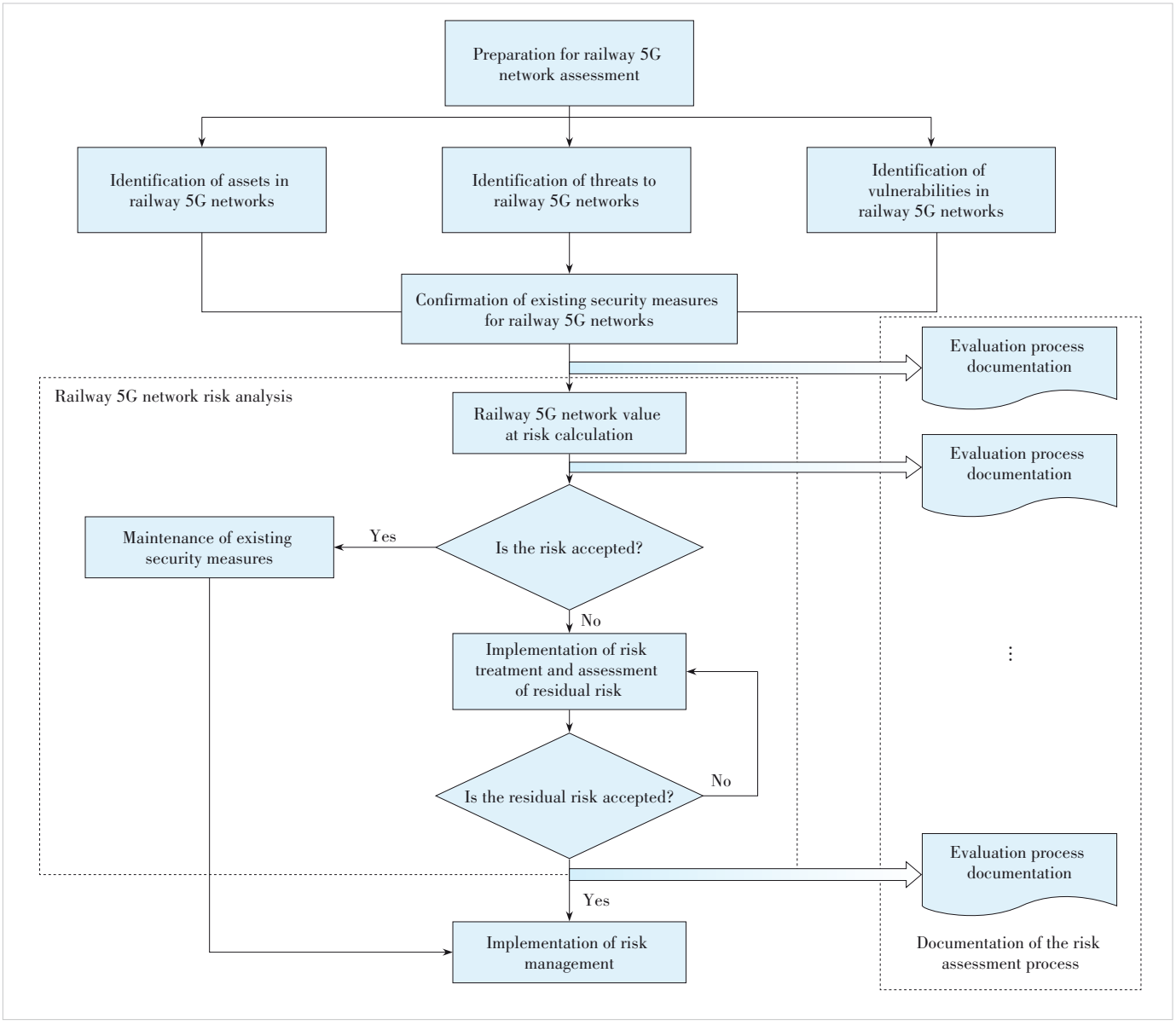

Figure 2. Railway 5G cybersecurity risk assessment flowchart

networks, as well as Software-Defined Networking (SDN), Network Functions Virtualization (NFV), and edge computing architecture[9]. Core network threats involve issues such as memory capture and errors in network configuration, while access network concerns include Address Resolution Protocol (ARP) spoofing, Multiple Access Control (MAC) address spoofing, and signal storms. Bearer network risks include the manipulation of configuration data by malicious actors or man-in-the-middle attacks. SDN vulnerabilities may result from information leakage or flow rule conflicts, while NFV-related risks pertain to virtualization bypassing. Edge computing challenges mainly relate to MEC gateway forgery or Application Programming Interface (API) risks[10]. The severity of these hazards is assessed through quantitative values that consider factors such as location and frequency.

3) Identification of vulnerabilities in railway 5G networks

The process of identifying vulnerabilities in railway 5G networks entails the application of diverse testing methodologies to compile a comprehensive list of flaws inherent in the assets. These flaws may lead to unauthorized access, information leakage, loss of control, damage, service unavailability, or security mechanism circumvention. Cyber vulnerabilities pose significant risks to the security of railway 5G network assets. Once identified, quantitative values can be assigned to these vulnerabilities based on the associated assets and their exploitability.

4) Confirmation of existing security measures for railway 5G networks

The process of validating existing security measures in rail-

way 5G networks involves the systematic collection, categorization, and evaluation of their effectiveness, along with documenting identified issues and vulnerabilities. This procedure facilitates organizations in comprehending their current security measures and system security policies, ensuring efficient security policy formulation and implementation.

4.1.3 Railway 5G Network Risk Analysis

Railway 5G network security risk analysis involves selecting appropriate methods or tools to calculate risk levels. This selection is based on evaluations of railway 5G network assets, threats, vulnerabilities, and the confirmation of existing security measures. This assessment aims to determine potential impacts on network assets within the security management scope, addressing risks such as data leakage, modification, unavailability, and destruction. To facilitate the identification and selection of appropriate security controls, a list of risk measurements is generated. This list assists in the analysis of the assessed data and supports the calculation of a "value-at-risk", which subsequently guides the determination of railway 5G network security risk levels. Fig. 3 illustrates this risk analysis workflow.

The process for calculating risk values in railway 5G network security analysis involves the following steps:

1) Estimating the probability: Calculate the likelihood of a cybersecurity event occurring in the railway 5G network. This estimation is based on the assessment results of the frequency of railway 5G cyber threats and the ease of exploiting vulnerabilities.

2) Assessing the impact: Evaluate the potential damage that could result from the occurrence of a cybersecurity event in the railway 5G network. This assessment is based on the importance of railway 5G cyber assets and the severity of identified vulnerabilities.

3) Quantifying the risk: Compute the overall risk value for the railway 5G network based on the likelihood of a security event and the potential damage it could cause. This calculation integrates the estimated probability of an event with the assessed impact.

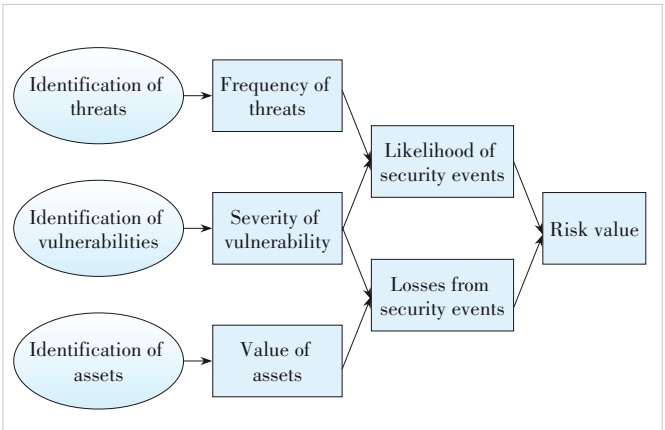

Figure 3. Analysis process of railway 5G network risks

In railway 5G network security analysis, two primary methods are employed for risk calculation: the function method and the matrix method.

The function method is commonly used for calculating network security risk, which can be expressed as:

$$R = f(L(t,v), F(a,v)) \tag{1},$$

where R represents the risk value, a represents the asset value, t represents the frequency of the threat, v represents the severity of the vulnerability, L represents the possibility that the threat utilizes the vulnerability of the asset to lead to a security event, and F represents the loss caused by the occurrence of the security event[11]. This method is a multiplication method, which is calculated as follows:

$$z = f(x,y) = \sqrt{x \cdot y} \tag{2},$$

where x and y denote the value assigned to the element.

The matrix method begins with the creation of appropriate matrices, including the security event likelihood matrix, security event loss matrix, and risk matrix, according to the principles of this approach. The formula applied in the matrix method is as follows:

$$\boldsymbol{Z}(ij) = a \cdot X(i) + b \cdot Y(j) \tag{3},$$

where $\boldsymbol{Z}(ij)$ is the value at the position of the row i and column j of the matrix (e.g., security event likelihood level, security event loss level, or risk level); $X(i)$ is the i-th parameter level and $Y(j)$ is the j-th parameter level involved in the matrix; a and b are two weighted values depending on the situation and the increment of the function. The matrix $\boldsymbol{Z}(ij)$ does not require a uniform formula but must maintain a consistent increasing or decreasing trend. Since the matrix method results in different hierarchies, it is important to hierarchize the assignments in the matrix before constructing the risk matrix.

To ensure effective control and management of security risks in the railway 5G network, the outcome of the network's risk assessment holds pivotal importance. Evaluating the calculated risk value helps determine the acceptability of security risks faced by the railway 5G network.

If the risk is considered acceptable, the existing security measures remain unchanged, and the planned security management for the railway 5G network continues as scheduled. However, if the risk is deemed unacceptable, a corresponding risk treatment plan is devised, and necessary actions are initiated to mitigate the identified risks.

For risks that have undergone treatment, continuous risk assessment is vital to gauge the residual risk. The acceptability of this residual risk is then evaluated. If the residual risk is deemed acceptable, a revised railway 5G network security strategy is formulated, and security management is adjusted based on the established plans, measures, and out-

comes of risk treatment. Conversely, if the residual risk remains unacceptable, further risk treatment measures are pursued until the residual risk reaches an acceptable level. Subsequently, diligent railway 5G network security management is maintained.

4.2 Railway 5G Network Vulnerability Discovery Methods Based on Penetration Testing

The security penetration test for the railway 5G network involves conducting extensive attack simulations that mimic potential intrusion scenarios, covering both the 5G-R network and the public-private railway 5G network. This rigorous examination aims to identify vulnerabilities within the railway 5G network and subsequently assess its overall security posture comprehensively. The primary objective is to guarantee the smooth and secure functioning of the railway 5G network.

4.2.1 Security Penetration Testing Framework

The railway 5G network security penetration testing framework comprises both security penetration routes and attack methods.

The railway 5G terminal establishes connectivity with the railway 5G access networks via the 5G base station, subsequently interfacing with the railway 5G core networks (comprising the 5G-R core network and public 5G core network) through the bearer network. In scenarios demanding high broadband capacity or low-latency applications, railway 5G terminals establish initial connectivity through the access network before transitioning to MEC nodes, and then interconnect with the railway 5G core networks via the bearer network. Consequently, the pathway for conducting security penetration tests in the railway 5G network primarily commences from the attack initiator, progresses to infiltrate the railway 5G terminal, proceeds to penetrate the railway 5G access network, MEC, bearer network, and culminates in the railway 5G core network.

The methods employed in the railway 5G network penetration testing primarily involve steps as follows. Initially, information including attack target IP addresses, device fingerprints, and related data is gathered. Subsequently, communication hijacking is attempted through techniques like man-in-the-middle attacks or brute-force decryption. Another aspect involves attempting "unauthorized" access to the railway 5G network, encompassing both the 5G-R network and the railway 5G PNI-NPN. In the testing process, testers aim to obtain and sustain privileges within the network using methods such as deserialization (Remote Code Execution) RCE, malicious code injection, and (Structured Query Language) SQL injection[12]. Following a series of network penetrations, testers can potentially breach the railway 5G network and further exploit vulnerabilities to explore deeper network weaknesses[13]. Fig. 4 shows the railway 5G network penetration testing process.

4.2.2 Typical Methods for Terminal Penetration Testing

1) Firmware penetration test

This method involves extracting firmware from railway 5G terminal equipment by establishing a connection to the flash memory chip via interfaces such as Universal Asynchronous Receiver/Transmitter (UART), Serial Peripheral Interface (SPI), or Joint Test Action Group (JTAG) interface. Tools like Flashrom are typically used for firmware extraction. Once the firmware is obtained, tools like Binwalk are utilized to perform reverse analysis of the firmware's executable programs or codes within the railway 5G terminal. The objective is to explore and potentially decipher critical function calls or relevant logic embedded in the terminal device's programs. These functions may relate to authentication, authorization, or access to the railway 5G network. Additionally, attempts are made to retrieve hard-coded data, such as device passwords or identity information, involving privacy concerns within the terminal device[14].

The firmware penetration test in the railway 5G network, while effective in uncovering deep-seated vulnerabilities and hard-coded data in terminal firmware, poses challenges such as ensuring precise firmware extraction without damaging the terminal device. The test's complexity necessitates skilled interpretation of extracted data, balancing the discovery of security flaws against the risk of disrupting critical embedded functions and maintaining terminal functionality. This approach is essential for revealing hidden security weaknesses but requires careful execution to preserve the overall integrity and performance of the railway's 5G network.

2) Serial port privilege test

This process involves disassembling railway 5G terminal devices and establishing a connection to the terminal either via the serial port or the terminal development board interface. This connection aims to exploit default or weak passwords that might be in use. Using tools like PuTTY or XSHELL, attempts are made to gain access to the terminal device's shell through its serial port. Alternatively, privileges might be acquired by implanting a program into the terminal device that elevates

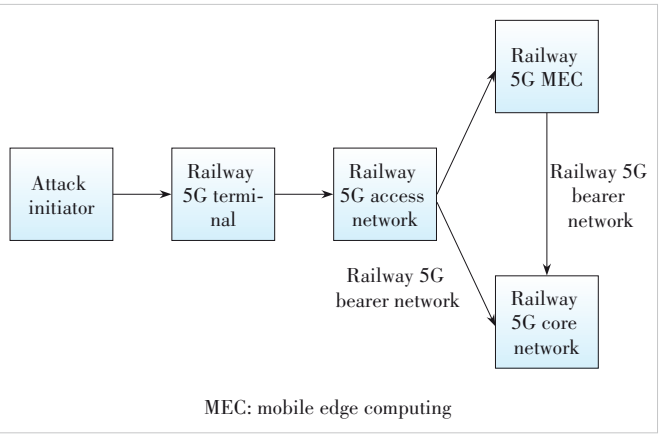

Figure 4. Penetration testing flowchart for railway 5G networks

power access or by analyzing vulnerabilities within the terminal system, including examining Set User ID (SUID) files and sudo privileges, to obtain control privileges over the terminal.

Therefore, both the firmware penetration test and serial port privilege test are crucial for assessing terminal security but require careful handling to avoid compromising the device.

4.2.3 Typical Methods for Access Network Penetration Testing

1) ARP attack test

This test entails the use of tools such as Arpspoof, Ettercap, and Netfuke to send maliciously crafted Address Resolution Protocol (ARP) requests or replies to specific terminals or gateways within the railway 5G network. Its primary aim is to associate the IP address of the gateway with an incorrect MAC address, thereby manipulating the ARP cache table within the targeted gateway[15]. ARP spoofing poses the risk of disrupting normal access to the railway 5G network, enabling interception of network traffic and potentially intercepting traffic to and from targeted terminals or gateways within the network.

ARP attack testing in the railway 5G network can effectively identify vulnerabilities and assess network resilience, but carries risks like potential service disruptions and limited scope. The complexity of railway 5G infrastructure, the need for high operational availability, and stringent regulatory compliance pose significant challenges in implementing these tests without impacting critical services.

2) MAC spoofing test

This test aims to infiltrate railway 5G terminal devices to acquire control privileges through methods including serial port exploitation, analysis of terminal devices, and implantation of a backdoor program. The process involves gathering device driver information to identify potential vulnerabilities, followed by adding the MAC address of the target terminal to the list of legitimate MAC addresses. This evaluates whether the railway 5G network improperly grants access to spoofed terminals[16].

The test assesses network security against MAC address manipulation. Its advantage lies in pinpointing network vulnerabilities to spoofing attacks, which is crucial for security enhancement. However, this test poses challenges like replicating realistic attack scenarios without disturbing the network and avoiding false security triggers. Executing this test demands precision to ensure it thoroughly assesses vulnerabilities without compromising network stability or affecting other terminals.

4.2.4 Typical Methods for Edge Computing Penetration Testing

1) MEC application attack

This test involves the use of an attack machine to access devices within the railway 5G network's edge computing network. Vulnerability scanning tools such as OpenVAS, Nessus, and Sqlmap are employed to scan for potential vulnerabilities in protocols, software components, and transmission channels within this network. Furthermore, the assessment includes executing malicious code and making configuration modifications to determine the existence of exploitable vulnerabilities in MEC applications and to evaluate the effectiveness of security reinforcements.

In the railway 5G network, the MEC application attack test identifies vulnerabilities in edge computing by scanning and executing malicious code. Its strength lies in uncovering deep security flaws, particularly in mobile edge computing applications. However, the test's complexity and potential to disrupt network operations or introduce new vulnerabilities present significant challenges. Conducting this test requires a careful balance between detailed security assessment and preserving the stability and integrity of the railway's 5G network.

2) API vulnerability exploitation test

This test comprises accessing the pertinent railway 5G network edge computing platform equipment using an attack machine. Information like IP addresses, version numbers, and operating systems is gathered. Various tools such as Nmap, Postman, Katalon Studio, and Scanless are employed to conduct API port scanning. Its primary goal is to pinpoint open APIs within the mobile edge platform (MEP) and evaluate the security aspects, including two-way authentication support and other pertinent security measures.

The API vulnerability exploitation test in the railway 5G network, focusing on edge computing platforms, uses tools to uncover open API vulnerabilities and assess security features. This method effectively reveals API weaknesses, crucial for network protection. However, it faces specific challenges, such as ensuring minimal impact on network traffic during scanning and the need for targeted testing to avoid affecting non-relevant system components. Additionally, the test must be precisely managed to avoid false positives and ensure that the identified vulnerabilities are actionable and relevant to the network's security posture.

4.2.5 Typical Methods for Bearer Network Penetration Testing

1) Man-in-the-middle attack test

In a man-in-the-middle attack test, the attacker strategically places test equipment or attacker machines, including fake base stations and Software Defined Radio (SDR), within the communication link between railway 5G network equipment and the 5G base station or other critical network components. The attacker impersonates a legitimate device using techniques like MAC address spoofing and ARP protocol spoofing. This allows for the tampering and redirection of railway 5G network communication packets through traffic sniffing and packet capture.

2) Management and network orchestration (MANO) malicious tampering test

Through methods such as malicious code injection and configuration file modification, or by directly manipulating the MANO, the attacker manipulates configurations related to network functions[16]. Modifying the behavior of network functions by changing settings in the coordinator can disrupt the separation between network functions.

The man-in-the-middle and MANO malicious tampering tests in the railway 5G network have the advantage of effectively simulating sophisticated cyber-attacks, providing valuable insights into network vulnerabilities and the effectiveness of security protocols. However, they carry the disadvantage of potential network disruption during testing. In practice, these tests face the unique challenge of accurately replicating complex attack scenarios while ensuring they do not interfere with critical network operations or compromise sensitive data. Additionally, there is a need to manage the risk of inadvertently introducing new vulnerabilities into the system, requiring a nuanced approach to maintain network security and integrity.

4.2.6 Typical Methods for Core Network Penetration Testing

1) User Plane Function (UPF) unauthorized access test

In this test, Session Management Function (SMF) emulation software like MAPS 5G N4 Interface Emulator is installed on the attacker's machine. The emulated SMF initiates coupling requests to UPFs within the railway 5G core networks, establishing N4 associations and using the Packet Forwarding Control Protocol (PFCP) to exchange control plane information. By simulating the generation and sending of various PFCP messages using emulated SMF software, the objective is to detect whether the UPF in the railway 5G core networks accepts coupling requests initiated by the malicious emulated SMF and assess the presence of a robust security authentication mechanism.

In the railway 5G network's UPF unauthorized access test, using tools like MAPS 5G N4 Interface Emulator assesses UPF's response to simulated attacks, highlighting security vulnerabilities. While effective in security validation, this test is complex and risks disrupting network operations, with challenges in creating accurate attack simulations and integrating the test without impacting ongoing network services.

2) Pseudo-signaling attack test

The pseudo-signaling attack test stimulates signaling forgery on both N2 and N4 interfaces in railway 5G core networks[16].

N2 signaling forgery attack testing involves capturing Next Generation Application Protocol (NGAP) messages from legitimate railway 5G network users through man-in-the-middle attacks using tools like Wireshark. Appropriate NGAP message types are analyzed and obtained, and then corresponding NGAP messages are forged. The NGAP-ID in the AMF-UE-NGAP-ID and RAN-UE-NGAP-ID are modified to match the target device's ID. This test determines whether the railway 5G core networks change the current operational state of the target device based on the forged NGAP message, and assesses the presence of a security isolation mechanism for N2 sessions.

In the N4 signaling forgery attack test, Packet Forwarding Control Protocol (PFCP) messages are intercepted, analyzed, and processed to identify suitable types. Corresponding PFCP messages are forged by modifying the Session Endpoint Identifier (SEID) to match the target device's identifier. This test assesses whether the UPF of the railway 5G core networks rejects the forged PFCP request and examines the presence of an N4 session security isolation mechanism.

The pseudo-signaling attack test evaluates railway 5G network resilience against session hijacking through coordinated N2 and N4 signaling forgery. The N2 test involves forging NGAP messages to test operational state alterations, while the N4 test uses forged PFCP messages to examine UPF response. While providing a thorough evaluation of session security mechanisms, this method faces challenges in attack simulation accuracy and network disruption risks.

4.3 Recommendations for Railway 5G Network Security Assessment

The methodology for railway 5G security evaluation requires the following recommendations to ensure effective deployment of security measures.

1) Scope definition

Before evaluation, the assessment scope must be precisely defined with clear objectives. A critical first step is to identify whether the target network is a dedicated 5G-R network or a railway 5G PNI-NPN, as this distinction fundamentally influences the assessment methodology. Assessments for the 5G-R network likely concentrate on custom-tailored security measures for rail communications, emphasizing the security of internal network structures and core functionalities to mitigate insider threats. Contrastingly, assessments for the railway 5G PNI-NPN prioritize defenses against external network boundaries, particularly against threats from the public Internet. Private-public network interconnectivity demands special attention.

2) Purpose determination

The security assessment for the railway 5G network must clearly define its purpose, whether to identify potential threats, discover vulnerabilities, or enhance the security strategy. This purpose will determine the assessment's focal points. For instance, if compliance with industry standards, regulations, or security requirements is the primary aim, the assessment should evaluate regulatory compliance. Alternatively, if the objective is to identify potential threats and vulnerabilities within the system, the assessment will focus on risk analysis and vulnerability detection, pinpointing system weaknesses that could pose threats and proposing measures to mitigate risks.

3) Differences in asset identification

Assessing the 5G-R network entails identifying and evaluating all critical assets pertinent to railway communications to gauge their significance and sensitivity, and compiling a comprehensive list of assets. Conversely, for the railway 5G PNI-NPN, attention should extend beyond railway-specific equipment to critical equipment deployed on the public network, such as edge computing nodes and gateways. Evaluating the significance of these devices in the context of railway communications and documenting their relevant information is crucial.

4) Differences in vulnerability identification

In conducting in-depth penetration testing and vulnerability scanning for the 5G-R network, the focus should be on potential vulnerabilities of terminal equipment, access networks, and core networks. Conversely, for the railway 5G PNI-NPN, assessing the effectiveness of firewalls and intrusion detection systems becomes imperative. This evaluation emphasizes data transmission security and the system's capability to thwart external attacks.

Similarly, there are numerous differences between the specific implementations of network security assessments in the 5G-R network and the railway 5G PNI-NPN, including the focus on evaluation and security measures, among others. These specific disparities are outlined in Table 1. Based on the assessment implementation distinctions highlighted in Table 3, a more detailed network security assessment of the railway 5G network can be conducted.

In conclusion, meticulous consideration of the distinct characteristics of the 5G-R network and the railway 5G PNI-NPN is vital during security assessments. Tailoring security assessment methodologies to these unique networks and specific situations ensures the efficacy and reliability of security evaluations for the railway 5G network.

5 Conclusions

This paper provides a comprehensive analysis of security requirements within the railway 5G network context, encompassing both the 5G-R network and the railway 5G PNI-NPN. Specifically, it delves into the security prerequisites across the network, users, and SBA domains within the 5G-R network security framework. Furthermore, it addresses the security requirements interlinking the railway 5G PNI-NPN and the 5G-R network. This study lays the groundwork for evaluating the security facets of the railway 5G network.

To facilitate risk assessment within the railway 5G network, we introduce a robust security risk assessment process. This process delineates procedures for asset identification, threat assessment, vulnerability analysis, and the validation of existing security measures. The framework outlined here is crafted to furnish organizations with a comprehensive toolkit for effectively managing network security risks and enhancing the reliability and security of their networks.

Moreover, this paper explores methodologies for identifying vulnerabilities specific to the railway 5G network, offering a comprehensive approach and procedure for conducting tailored penetration testing. Our insights aim to assist organizations in informed decision-making when selecting appropriate vulnerability assessment methods. However, this study acknowledges existing research gaps, such as the absence of specific assessment methods and standards for railway communication-related business research, and the omission of mainstream network security assessment models, such as the network attack model. Future research endeavours will address these shortcomings by evaluating security standards across different railway communication services and integrating network security assessment models into railway 5G network security assessment technology. This integration aims to enhance the accuracy and efficiency of network security assessments.

In summary, this paper provides valuable guidance for evaluating security risks within the railway 5G network. It empowers organizations to protect their network assets, fortify network security, and mitigate potential threats. Our research serves as a foundational reference and roadmap for future investigations in the domain of railway 5G network security.

References

[1] ZHONG Z D, GUAN K, CHEN W, et al. Challenges and perspective of new generation of railway mobile communications [J]. ZTE technology jour-

Table 3. Railway 5G network security assessment method differences

Aspect	5G-R network	Railway 5G PNI-NPN
Focus of evaluation	Internal network structure, terminal equipment vulnerabilities, and internal threat prevention	External boundary defence, external connection protection, and boundary security
Assets and devices	Critical railway communication equipment and internal network critical components	Railway-specific equipment and public network critical components
Security measures	Internal network isolation, access control, and internal encryption	Firewall, intrusion detection, and external encryption
Vulnerability identification	Internal vulnerability scanning, risk assessment, and internal penetration testing	External defence strategy assessment and simulated attack testing
Network interconnectivity	Internal communication security, private network isolation, and internal data transmission protection	External connection security, data transmission encryption, and external communication reinforcement
Threat focus	Internal threats and leakage risks, internal access control, and internal permissions management	External attacks and threat prevention; integrity protection of external communication data
Testing focus	Terminal equipment vulnerabilities, core network vulnerabilities, and access network weaknesses	Effectiveness of external defence strategy, network boundary stability, and external security vulnerabilities

5G-R: the Fifth Generation of Mobile Communications for Railway PNI-NPN: public network integrated non-public network

nal, 2021, 27(4): 44 – 50. DOI: 10.12142/ZTETJ.202104009
[2] China National Railway Group. General technical requirements for railway 5G private mobile communication (5G-R) system (preliminary): TJ/DW 246-2022 [S]. China National Railway Group, 2022
[3] 3GPP. Security architecture and procedures for 5G system release 15 (V15.3.1): 3GPP TS 33.501 [S]. 3rd Generation Partnership Project, 2018
[4] GUO Y M, ZHANG Y. Study on core network security enhancement strategies in 5G private networks [C]//Proc. IEEE 21st International Conference on Communication Technology (ICCT). IEEE, 2021: 887 – 891. DOI: 10.1109/icct52962.2021.9657934
[5] LI P Y, LIU J W. Security architecture and key technologies for super SIM-based 5G End-Cloud System [J]. ZTE technology journal, 2023, 27 (1): 13 – 19. DOI:10.12142/ZTETJ.202301004
[6] SURESHSAH R T, BALASUBRAMANIAM M, DAS D. Novel 5G and B5G network architecture and protocol for multi SIM devices [C]//Proc. IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT). IEEE, 2021: 1 – 6. DOI: 10.1109/conecct52877.2021.9622360
[7] ZHANG X Q, HE Y M. Information security management based on risk assessment and analysis [C]//Proc. 7th International Conference on Information Science and Control Engineering (ICISCE). IEEE, 2020: 749 – 752. DOI: 10.1109/ICISCE50968.2020.00159
[8] ALIMZHANOVA Z, TLEUBERGEN A, ZHUNUSBAYEVA S, et al. Comparative analysis of risk assessment during an enterprise information security audit [C]//Proc. International Conference on Smart Information Systems and Technologies (SIST). IEEE, 2022: 1 – 6. DOI: 10.1109/SIST54437.2022.9945804
[9] WEI L, ZHA X, DAI F F. Network security interoperability towards cloud-network convergence [J]. ZTE technology journal, 2023, 27(1):7 – 12. DOI: 10.12142/ZTETJ.202301003
[10] SZARVÁK A, PÓSER V. Review the progress of threat and risk assessment on 5G network [C]//Proc. IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, 2022: 353 – 358. DOI: 10.1109/SAMI54271.2022.9780829
[11] KANG H Y, XIAO Y H, YIN J. An intelligent detection method of personal privacy disclosure for social networks [J]. Security and communication networks, 2021: 5518220. DOI: 10.1155/2021/5518220
[12] PATEL K. A survey on vulnerability assessment & penetration testing for secure communication [C]//Proc. 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019: 320 – 325. DOI: 10.1109/icoei.2019.8862767
[13] XIE X Q, YU X G, YU Y X, et al. Penetration test framework and method of 5G cyber security [J]. Journal of information security research, 2021, 7 (9): 795 – 801
[14] SARIKONDA M, SHANMUGASUNDARAM R. Validation of firmware security using fuzzing and penetration methodologies [C]//Proc. IEEE North Karnataka Subsection Flagship International Conference (NKCon). IEEE, 2022: 1 – 5. DOI: 10.1109/NKCon56289.2022.10126524
[15] SHARMA D, KHAN O, MANCHANDA N. Detection of ARP spoofing: a command line execution method [C]//Proc. International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2014: 861 – 864. DOI: 10.1109/IndiaCom.2014.6828085
[16] YU X G, LI Y H, QIU Q. 5G security: a cybersecurity treasure trove for the age of digital intelligence (in Chinese) [M]. Beijing: Publishing House of Electronics Industry, 2023

Biographies

XU Hang (22125067@bjtu.edu.cn) received his BE degree in communication engineering from China University of Petroleum in 2022. He is currently working toward a master's degree at the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, China. His research interests include network security and 5G-R.

SUN Bin received his BS and MS degrees in electronic engineering from Beijing Jiaotong University, China in 2004 and 2007, respectively. From 2007 to 2015, he served as an R&D manager with Beijing Liujie Technology Co., Ltd. He is currently an assistant researcher with the School of Electronic and Information Engineering, Beijing Jiaotong University. His main research interest is the interconnection and interworking of the core network for dedicated railway mobile communication systems.

DING Jianwen received his BS and MS degrees from Beijing Jiaotong University, China in 2002 and 2005, respectively. He is currently a professor of engineering with the School of Electronic and Information Engineering, Beijing Jiaotong University. He received the second prize for progress in science and technology from the Chinese Railway Society. His research interests include broadband mobile communications and personal communications, dedicated mobile communication systems for railway, and safety communication technology for train control systems.

WANG Wei is the LTE-R technical director and a railway wireless communication system expert at ZTE Corporation, with rich experience in the GSM-R system design. He has a deep understanding of GSM-R and LTE-R and has undertaken several major railway-related projects on wireless communication systems.