HiLL PUBLISHING

Advances in Computer and Communication, 2024, 5(4), 223-227
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Research on Computer Security Protection Mechanism in Marine Communication Network

Hongfeng Chen

Mingpai Technology Group Co., Ltd., Qingdao 266109, Shandong, China.

How to cite this paper: Hongfeng Chen. (2024) Research on Computer Security Protection Mechanism in Marine Communication Network. *Advances in Computer and Communication*, 5(4), 223-227.
DOI: 10.26855/acc.2024.10.004

Received: September 20, 2024
Accepted: October 15, 2024
Published: November 11, 2024

***Corresponding author:** Hongfeng Chen, Mingpai Technology Group Co., Ltd., Qingdao 266109, Shandong, China.

Abstract

With the vigorous development of the marine economy and the rapid progress of marine science and technology, the importance of marine communication networks as information bridges connecting key facilities such as offshore operating platforms, ships, and underwater detectors has become increasingly prominent. However, the complexity and particularity of the marine environment have brought unprecedented challenges to the security of communication networks. This article deeply explores the diverse security threats faced by marine communication networks, including harsh physical environments, network attacks, wireless communication interference, and communication link vulnerabilities. It elaborates on a variety of security protection technologies, such as data encryption, identity authentication, intrusion detection and prevention, and vulnerability scanning and repair, which together constitute a solid line of defense for marine communication network security. At the strategic level, specific measures such as strengthening physical environment protection, strengthening network access control, encrypting wireless communication data, and strengthening communication link protection are proposed to comprehensively improve the security of marine communication networks. It provides important theoretical basis and practical guidance for building a safe and reliable marine communication network.

Keywords

Marine communication network; computer security; protection mechanism

1. Introduction

As an important information channel connecting the ocean and the land, the Marine communication network is of great significance for the effective development and utilization of Marine resources, the safety of maritime operations and the promotion of the development of Marine economy. With the extensive application of computer technology and network technology in the field of Marine communication, the Marine communication network is increasingly powerful, but it also faces the increasingly severe computer security threat. For example, hacker attacks, virus infections, information theft, and other security incidents occur from time to time, which seriously affect the normal operation of the Marine communication network and data security. Therefore, it is of great practical significance and urgency to strengthen the research of the computer security protection mechanism in the Marine communication network.

2. Analysis of computer security threats in the marine communication network

2.1 Physical environment threats

The physical environment of the Marine communication network is extremely harsh, which brings many potential threats to the computer system. First, the high humidity and high salinity of Marine air can easily lead to equipment

corrosion, greatly shortening the service life of computer hardware. For example, metal lines on circuit boards may be broken due by corrosion, causing equipment failure. Secondly, the strong wave impact and high winds may cause direct physical damage to the communication facilities [1]. For example, communications equipment installed on offshore platforms or buoys may be damaged by waves or even blown into the sea. In addition, drastic changes in temperature can also affect the performance and stability of the computer equipment. Under extremely hot or extremely cold conditions, the electronic components may fail, causing the system to collapse.

2.2 Network attack threat

Cyberattacks are a serious threat to marine communication networks. Distributed of Denial-of-service (DDoS) attacks could paralyze the network and prevent legitimate users from accessing critical marine data and services. By controlling a large number of puppet machines, the attacker sends massive requests to the target server, causing the server to run out of resources and be unable to respond normally. In addition, hackers may use vulnerabilities to invade computer systems and steal sensitive Marine information, such as Marine resource exploration data, ship navigation trajectory, etc. For example, gain control of the system by exploiting an unpatched vulnerability in the operating system or application to obtain valuable information [2]. There is also a common cyber attack that is the spread of malware, such as viruses, worms, and Trojan horses. The malware could damage system files, steal data or encrypt the system, causing huge losses to Marine communications networks.

2.3 Wireless communication threats

Wireless communication is widely used in marine communication networks, but it also brings significant security threats. Signal interference is one of the common problems, and interference from other wireless devices or the natural environment may lead to communication interruption or data loss [3]. For example, thunderstorms at sea may produce strong electromagnetic interference, affecting the transmission of wireless signals. In addition, wireless communications are easy to monitor and intercept. Due to the openness of wireless signals, unauthorized attackers can receive and analyze signals through specific devices and obtain the transmitted information. For example, unencrypted wireless communications may be stolen by attackers from ocean surveillance data or ship communications. In addition, identity counterfeiting is also a risk in wireless communications. An attacker can disguise himself as a legitimate communication node and merge into the network to destroy or steal information.

2.4 Communication link threat

The stability and security of the communication links are crucial in the marine communication network. Link interruption is one of the common threats, which may be caused by damage to submarine cable, failure of satellite communication, or interference of wireless links. For example, an undersea earthquake could cause an undersea cable to break and disrupt communications. In addition, the bandwidth limitation of the link may lead to data transmission delay or congestion, affecting Marine services with high real-time requirements [4]. Moreover, the communication link may also be attacked by the middleman. An attacker can insert his own device in the communication link, intercept and tamper with the transmitted data so that the receiver receives the wrong or false information. For example, in the ship's communication with the shore-based control center, an attacker tampering with instructions may cause dangerous ship navigation.

3. Computer security and protection technology in the Marine communication network

3.1 Data encryption technology

Data encryption technology is an important means to ensure data security in the Marine communication network. By encrypting sensitive information, it is difficult for an attacker to understand its content, even if the data is intercepted during transmission. Common data encryption algorithms include symmetric encryption algorithms (such as AES) and asymmetric encryption algorithms (such as RSA).

The symmetric encryption algorithm uses the same key for encryption and decryption, which has the advantages of fast encryption and decryption speed. In Marine communication networks, for a large number of real-time data transmissions, such as the return of Marine monitoring data, the use of symmetric encryption algorithms can ensure rapid data processing [5]. For example, the data such as water temperature, salinity, and other data collected by the

ocean buoy are encrypted with a pre-shared symmetrical key before transmission, and the receiving end is decrypted with the same key, which guarantees the confidentiality of the data.

The asymmetric encryption algorithm uses the public key and the private key pairs, the public key is used for encryption, and the private key is used for decryption. This approach is suitable for key exchange in insecure networks. For example, in the initial establishment stage of the ocean communication network, the communication parties can exchange the symmetric encryption key through the asymmetric encryption algorithm, and then use the symmetric encryption for subsequent data transmission.

3.2 Identity authentication technology

Identity authentication technology is used to confirm the identity of both parties of the communication and prevent illegal users from accessing the Marine communication network. Common identity authentication methods include password-based authentication, certificate-based authentication, and biometric authentication.

Password-based authentication is the easiest way but with relatively low security. The user enters a preset password to verify the identity. However, passwords are easy to be guessed, stolen, or forgotten. In the Marine communication network, the simple password authentication may not be safe enough, usually combined with other authentication methods.

Certificate-based certification is more secure and more reliable. Digital certificates are issued by an authoritative certification authority, including the user's public key and identity information [6]. User identity can be confirmed by verifying the legitimacy of the certificate. For example, when a Marine research ship communicates with the shore-based control center, both the ship end and the shore-based end hold legal digital certificates, and the certificates are verified when the communication connection is established to ensure the authenticity of both parties.

Biometric authentication uses human physiological characteristics or behavioral characteristics for identity identification, such as fingerprint, iris, facial recognition, etc. This authentication method has high accuracy and safety, but it is relatively rarely used in the Marine environment due to equipment and environment limitations.

3.3 Invasion detection and defense technology

Intrusion detection and defense technology can monitor abnormal activities in Marine communication networks in real time to detect and prevent potential intrusion behaviors in time. The intrusion detection system (IDS) identifies the possible attack patterns and abnormal behavior by analyzing the network traffic and system logs.

The intrusion defense system (IPS) can not only detect intrusion, but also take active steps to prevent attacks. For example, when a DDoS attack is detected, the IPS can automatically filter the malicious traffic to ensure the normal operation of the network.

In the Marine communication network, due to the complexity of the network environment and the limited resources, lightweight and efficient intrusion detection and defense technologies need to be adopted. For example, algorithms based on machine learning and artificial intelligence can automatically learn normal network behavior patterns to more accurately detect anomalies. At the same time, combined with the distributed detection architecture, the comprehensive coverage of the large-scale Marine communication network can be realized.

3.4 Vulnerability scanning and repair technology

Vulnerability is a security hazard in computer systems and networks, and attackers often exploit these vulnerabilities to attack. Vulnerability scanning technology can regularly detect the devices and systems in the Marine communication network and discover potential security vulnerabilities.

The vulnerability scanning includes both host vulnerability scanning and network vulnerability scanning. Host vulnerability scanning for a single computer device, check for vulnerabilities in the operating system, application software, etc. Network vulnerability scanning focuses on detecting vulnerabilities in network devices and topology. Once a vulnerability is found, it is crucial to fix it in time. Repair xes include installing patches, updating software versions, adjusting system configuration, etc. For example, after discovering a vulnerability in the operating system, install the patch provided by the vendor in time to fix the vulnerability and prevent the attacker from using it.

At the same time, a vulnerability management mechanism is established to manage the whole process of vulnerability discovery, evaluation, repair and tracking to ensure the security of the Marine communication network. Regular vulnerability scanning and repair can effectively reduce the risk of system attack and improve the overall security level of the Marine communication network.

4. Computer security protection strategy in the Marine communication network

4.1 Strengthen the physical environment protection

In the Marine communication network, strengthening the physical environment protection is the basis of ensuring the computer security. Due to the particularity of the Marine environment, such as high humidity, high salinity, high wind, big waves and extreme temperature changes, the physical protection of communication equipment poses severe challenges. Therefore, corrosion-resistant, waterproof, dustproof, shock-proof and high-temperature resistant materials should be used to ensure normal operation in harsh environments. For example, server cabinets installed on offshore platforms can be made of stainless steel and sealed to prevent the intrusion of seawater and moist air.

Secondly, to provide a stable installation and support structure for the equipment. In the case of strong winds and big waves, the equipment may be subjected to violent vibration and shock, so a strong fixture and shock absorption measures are required. For example, the use of special shock absorption bracket to install communication equipment, reduce vibration damage to the equipment. In addition, an environmental monitoring system should be established to monitor the physical environmental parameters, such as temperature, humidity, wind speed, etc. When the environmental parameters exceed the safety range, timely issue the alarm and take the corresponding protection measures, such as starting the ventilation and heat dissipation equipment, closing the susceptible equipment, etc.

4.2 Strengthen network access control

Network access control is an important means to prevent unauthorized users from accessing network resources. In the Marine communication network, a perfect access control mechanism should be established to strictly verify the identity of users and ensure that only legitimate users can access the network resources. On the one hand, the implementation of a strict identity authentication mechanism. Multi-factor identity authentication, combined with passwords, fingerprints, token and other ways to ensure that only legitimate users can access network resources. Set higher levels of certification requirements for important systems and data. On the other hand, develop a fine access policy. According to the roles and responsibilities of the user, assign the corresponding access permissions to him, to minimize the authorization principle, that is, the user only has the minimum permission required to complete his work. For example, for access to Marine research data, researchers can only access data related to their research projects, not access to other irrelevant data. At the same time, review and update the access rights of users regularly, and the permission of former employees or users who no longer need access rights should be revoked in time to prevent the abuse of permission.

4.3 Encrypted wireless communication data

In the Marine communication network, wireless communication occupies an important position, but it also brings great security risks. Due to the openness and broadcasting characteristics of wireless signals, it is easier to intercept, monitor, and tampered with. Therefore, encrypted wireless communication data has become a key and effective means to ensure the security of data transmission. Advanced encryption algorithms, such as AES-256, are used to encrypt the transmitted data. At the data-sending end, the algorithm is used to encrypt the original data and convert the plaintext into ciphertext. At the receiving end, only the legitimate receiver with the correct key can decrypt and restore the original plain data, thus ensuring the confidentiality of the data during wireless transmission.

In addition, by changing the key regularly, the possibility of it being stolen or cracked can be greatly reduced, ensuring the security and effectiveness of the key. For example, the key can be set automatically updated weekly or monthly, and a secure key distribution mechanism is adopted during the update to prevent the key from being intercepted during transmission.

4.4 Strengthen the protection of communication links

A communication link is a data transmission channel in the Marine communication network, and its security is directly related to the integrity and confidentiality of the data. For submarine optical cables, regular inspection and maintenance should be strengthened, and the damage and faults should be found and repaired in time. At the same time, the link redundancy design is adopted to improve the fault tolerance and damage resistance of the communication system. Data is transferred by deploying multiple parallel communication links, and even if one of them fails or is attacked, the other links can continue to work, ensuring the continuity and stability of the communication services.

For satellite communication links, we should prevent interference and malicious attacks. To detect and eliminate interference signals by technical means to ensure the normal operation of satellite communication. During the link transmission process, the data integrity verification technology, such as the hash function, is adopted to ensure that the data is not tampered with during the transmission process.

5. Conclusion

With the continuous advancement of Marine development, the importance of the Marine communication network has become increasingly prominent, and the establishment and improvement of computer security protection mechanisms is particularly important. Through the comprehensive analysis of physical environment threats, Marine communication networks, network attack threats, wireless communication threats, and communication link threats, the computer security protection strategy in Marine communication networks, including strengthening physical environment protection, strengthening network access control, encrypting data of wireless communication and strengthening the protection of communication link. The implementation of these strategies will significantly improve the overall security level of the Marine communication network, and provide a solid guarantee for the smooth development of Marine scientific research, resource development, environmental monitoring, and other activities.

References

[1] Wang Z. Research on computer network security protection technology based on a superiority algorithm. Applied Mathematics and Nonlinear Sciences. 2024;9(1).

[2] Zhu J. Optimization of network security protection posture based on data clustering. Applied Mathematics and Nonlinear Sciences. 2024;9(1).

[3] Natalia M. Network Protection Tools for Network Security Intelligence Centers. Procedia Computer Science. 2021;190597-603.

[4] Sun Long, Wen Jianxin, Ma Kai. Adaptive interface technology based on marine network information system. Journal of China Academy of Electronics Science. 2021;16(09):884-890+905.

[5] Jiang Shengming, Ge Lige, Xu Yanli. Marine data transmission network architecture and challenges. Telecommunication Science. 2021;37(07):16-24.

[6] Wang Yongjiao, Wang Donghai, Zhang Bo, et al. Research on infrastructure of marine network information system. Radio Communication Technology. 2021;47(04):439-443.