Education Reform and Development, 2024, Volume 6, Issue 11
https://ojs.bbwpublisher.com/index.php/ERD
Online ISSN: 2652-5372
Print ISSN: 2652-5364

Research on Security Strategies for Wireless Sensor Networks in Internet of Things Applications

Fei Lu[1,2]*, **Haojing Huang**[1], **Zhenjiang Shi**[1], **Zihan Lin**[1]

[1]College of Engineering Technology, Open University of Guangdong (Guangdong Polytechnic Institute), Guangzhou 510091, China
[2]Faculty of Data Science, City University of Macau, Macau 999078, China

***Corresponding author:** Fei Lu, flu@gdrtvu.edu.cn

Abstract: With the development of modern science and technology, the Internet of Things has been widely used in many fields, and it involves a wide range of technologies, among which the most important technology is the sensor, the most basic technology. The sensor network node working environment has been very complex and demanding; if slightly relaxed, it will lead to the sensor facing many security risks. Therefore, strengthening the security of wireless sensor networks has become an essential part of the Internet of Things project. This paper mainly starts with an overview of the Internet of Things and wireless sensor networks, analyzes the security challenges and impacts of wireless sensor networks, and discusses the main security threats and countermeasures. The purpose is to implement wireless sensor network security strategies for Internet of Things applications and build a comprehensive and multi-level security protection system through various means. To ensure that the sensor network can operate stably and safely in a complex environment, Internet of Things technology‘s healthy and sustainable development can be promoted.

Keywords: Internet of Things; Wireless sensor network; Security issues

Online publication: November 22, 2024

1. Introduction

With the rapid development and broad application of the Internet of Things technology, Wireless Sensor Network (WSN), as the core component of the perception layer of the Internet of Things, have gradually entered all aspects of People‘s Daily life [1]. According to the DBMR Cloud platform statistics, the global wireless sensor network market has reached 79.17 billion US dollars (2023) and is developing at a compound annual growth rate of 17.23%. By 2030, the market is expected to reach 213.92 billion US dollars. However, with the continuous expansion of wireless sensor network applications, security problems have gradually emerged. For example, due to location limitations, sensor nodes are usually deployed in open and unattended environments, making them vulnerable to various attacks. These security problems will threaten the security of personal privacy and corporate secrets, as well as the security of wireless sensor networks. It may also affect public security, social stability, and development. Therefore, research and analysis on the security problems of wireless sensor networks under the Internet of Things environment and implementing effective security countermeasures can promote the improvement and sustainable development of Internet of Things technology. According to Bitdefender‘s 2023 security report, about 3.6 billion security incidents are generated by IoT devices worldwide, of which wireless sensor networks are one of the main targets. Malware, denial of service (DoS) attacks, and data theft emerged as the primary attack modes in WSN. Through an in-depth analysis of the leading security problems wireless sensor networks face in the current Internet of Things environment, this paper puts forward practical solutions to provide a security guarantee for the sustainable development of future Internet of Things technology.

2. Overview of the Internet of Things and wireless sensor networks

When discussing the security issues of wireless sensor networks in the Internet of Things environment, it is important to first clarify the connotation of the Internet of Things and wireless sensor networks [2,3]. First, the Internet of Things is a network system connecting various physical devices, sensors, software, and other technologies to communicate and exchange data. The core idea is to connect and communicate with objects in daily life through the Internet to realize intelligent and automated control and management. With its unique technology and service functions, the Internet of Things has covered many fields such as home, city, industry, agriculture, and medical care, thus becoming a significant force in promoting social development. Second, the wireless sensor network is integral to the Internet of Things technology. It is a wireless network comprising many static or mobile sensor nodes through self-organization and multi-hop. These sensor nodes can communicate wirelessly, cooperatively collect, process, and transmit the information of the perceived objects in the geographic area covered by the network, perceive and inspect the external world, and report to the user. In addition, the wireless sensor network has large-scale, dynamic, and self-organization characteristics. It is widely used in the military field, medical care environmental monitoring, and other fields through the data acquisition unit, data transmission unit, data processing unit, energy supply unit, and other components to achieve data collection, processing, and transmission functions, providing critical data support for the Internet of things.

The wireless sensor network (WSN) in the Internet of Things environment faces many security challenges [4–6]. First, the problem of data leakage is serious because WSN transmits data through unencrypted, open wireless communication, which attackers easily monitor and tamper with. Although the traditional encryption and access control mechanism can play a particular protective role, adapting to the ever-evolving network threats is still tricky. Second, physical attacks are frequent, and sensor nodes are often deployed in unattended areas vulnerable to breach or illegal access. With the development of network applications, routing attacks have become one of the main threats to the stability of networks. Attackers can block network communication by tampering with routing information or forging messages, causing the entire network to break down. Due to the limited computing and storage capacity of WSN nodes, traditional security protocols may lead to excessive energy consumption and emerging technologies such as machine learning. However, they perform well in intrusion detection but face problems such as extensive training data and insufficient adaptability.

3. Wireless sensor network security challenges and their impact

With the rapid development of Internet of Things technology, wireless sensor networks (WSN), an essential part of the Internet of Things, have been widely used in smart homes, industrial automation, environmental monitoring, and many other fields. However, the unique characteristics of WSNs cause them to face many security challenges in their application. First of all, most WSN nodes are deployed in open or unattended environments, which makes it easy to become the target of malicious attacks. Data leakage, node destruction, and illegal access are severe threats to network security. Secondly, WSN has the characteristics of limited resources. The nodes are usually very limited in computing power, storage capacity, and battery life, which makes them unable to carry the complex security protection mechanism of the traditional network. Although the self-organization of the network enhances its flexibility, it also increases the complexity of network management and control. When dealing with dynamically changing threats and attacks, it lacks a robust security guarantee mechanism, which is also a severe challenge to WSNs. Finally, WSN faces various potential threats during data transmissions, such as routing attacks, denial of service attacks (DoS attacks), and man-in-the-middle attacks. These attacks can lead to data tampering or loss and cause network paralysis, seriously affecting the overall operation of the Internet of Things system. More importantly, the continuous expansion of Internet of Things applications makes the security threats WSNs face increasingly diversified. Traditional security means such as encryption technology and access control are imperfect under the emerging attack mode. These security problems threaten the protection of personal privacy and may lead to economic losses for enterprises and infrastructure paralysis. Therefore, an in-depth analysis and response to the security challenges faced by WSN are significant in ensuring the security of Internet of Things applications and are the keys to promoting its future healthy development. Data related to wireless sensor security issues in recent years are shown in **Table 1**.

Table 1. Data related to wireless sensor security issues in recent years

A given year	Security challenge overview	Major threat types	Frequency of occurrence(trend)	Range of effects	Progress of response measures
2021	Node safety and environmental exposure	Data breaches, node vandalism, illegal access	High incidence	Privacy disclosure, compromised system	Encryption technology popularization, essential access control
2022	Resource constraints and security mechanisms	Limited resources (computing, storage, batteries), insufficient security mechanisms	Persistent presence	Stability, limited security protection, performance degradation	Implementation of lightweight security protocol development, energy optimization strategy
2023	Threats during data transmission	Routing attacks, DoS attacks, Man-in-the-middle attacks	Diversifying growth	Data tampering, loss, service disruption	encryption, intrusion detection and response system, security certification

4. Main security threats and countermeasures of wireless sensor networks

4.1. Main security threats of wireless sensor networks

The wide application of wireless sensor networks (WSN) in the Internet of Things makes its security challenges increasingly prominent [7–9], including data leakage, physical attacks, routing attacks, and resource constraints. First, data leakage is one of the main challenges WSN faces. WSN is usually deployed in an open, unattended environment, and most nodes communicate through wireless channels, making data easily intercepted or tampered with in the transmission process. Attackers can steal sensitive data by monitoring wireless signals, cracking encryption algorithms and other means, and then cause immeasurable losses. Secondly, physical attacks are also a security threat that WSNs can't ignore. WSN has the characteristics of wide distribution, small size, and weak protection ability, making it very vulnerable to physical damage. Attackers can interfere with the regular operation of the network by directly touching the node, destroying its physical structure, replacing the node, etc., to control WSN remotely or launch more sophisticated attacks [10]. Thirdly, routing attacks are one of the security threats unique to WSN. It mainly interferes with network communication by tampering or forging routing information, thus affecting the overall stability of the Internet of Things system, which will not only affect the availability of WSN but also may leak sensitive information or mislead decisions. Finally, the resource-constrained nature further exacerbates these problems, as complex security mechanisms often lead to excessive node energy consumption and shorten the network lifetime. There are also security threats such as denial of service attacks (DoS attacks), man-in-the-middle attacks, and the introduction of malicious nodes. In brief, a DoS attack sends useless data or requests to WSN to occupy most of the network resources so that legitimate users can't get the service and cause the network performance to decline sharply or even crash. Man-in-the-middle attacks mainly occur when the attacker can control or monitor the communication path between WSN nodes. In this case, the attacker destroys the integrity and confidentiality of the data by intercepting, tampering, or forging the transmitted data. The introduction of malicious nodes is a more secret and complex threat. By deploying malicious devices disguised as normal nodes, attackers infiltrate WSNs to steal data, destroy network structures, or launch other types of attacks, posing a severe threat to the security and reliability of WSNs.

4.2. Analysis of countermeasures that wireless sensor networks can adopt in the face of security threats

4.2.1. Pay attention to the problem of data leakage and improve encryption technology

In the Internet of Things environment, the current wireless sensor network still has the problem of data leakage, which has become a significant challenge restricting its wide application and security [11–13]. To deal with this problem effectively, technicians must attach great importance to the risk of data leakage and constantly upgrade the application level of encryption technology. First of all, technical personnel should realize the seriousness of data leakage. Most of the information in wireless sensors is sensitive information involving personal privacy, corporate secrets, and even national security. Once data leakage occurs, it will bring severe losses to residents, individual enterprises, institutions, and the country. Therefore, every link from design and deployment to operation and maintenance should prevent data leakage and prioritize this work. Second, technologists should also improve the use of encryption technology. Encrypting sensitive data can ensure higher security in transmission and storage, and relevant data can't be easily cracked when intercepted to safeguard data security. For example, in the Internet environment, you can use high-strength encryption algorithms, such as AES, RSA, etc., to encrypt the data. At the same time, it is important to pay attention to the latest developments in encryption technology, such as quantum encryption and other cutting-edge technologies, and constantly improve the level of encryption to cope with possible security threats in the future.

4.2.2. Pay attention to physical attacks and improve the level of physical security protection

In the process of putting into operation, because the sensor node is exposed, physical attacks can directly target itself and the surrounding deployment environment, resulting in network interruption, data tampering, and system breakdown, so the vital link to ensure the security of wireless sensor network is to pay attention to the problem of physical attacks [14]. On the one hand, physical attacks can enhance the protection of the physical layer of the sensor node, such as the use of durable shell materials to improve the anti-damage ability of the node, but also can reasonably arrange the location of the node to avoid exposing it to the area that is easy to be attacked. The process of node design can also be integrated into the anti-disassembly mechanism, increasing the difficulty of illegal access to nodes to improve the sensor network‘s essential defense function. On the other hand, it is necessary to strengthen the monitoring of the deployment environment and enhance the protection capability. The most basic way is to install monitoring cameras, intrusion detection systems, and other equipment to achieve a full range of monitoring of the deployment environment and ensure that relevant technical personnel can detect and prevent potential physical attacks in time. At the same time, physical isolation can be directly adopted for important nodes or areas, such as increasing fences and setting up separate access control systems to improve the protection level further. In addition, personnel security awareness should be strengthened. Operations and management personnel should fully understand the harm of physical crisis, recognize the severe consequences of such attacks, and train corresponding protection methods to detect and deal with abnormal situations promptly [15].

4.2.3. Pay attention to the routing attack problem and improve the secure routing protocol

By tampering with routing information, forging routing messages, and other means, you can destroy the regular communication of the network and even make the whole network stall, affecting its everyday work; this is a routing attack [16]. Therefore, improving the design and application of a secure routing protocol and facing the problem of a routing attack is crucial to ensuring the security of wireless sensor networks. First, the relevant technical personnel should deeply understand the principle and operation methods of routing attacks and, on this basis, formulate effective countermeasures. Routing attacks are usually designed to attack the vulnerabilities or defects of routing protocols to interfere with or destroy the network routing mechanism. Therefore, operations and technical personnel should conduct in-depth research on the standard attack modes, analyze the attack paths and different harm degrees, and provide the basis for formulating effective defense strategies. Secondly, technical personnel should fundamentally improve the design level of secure routing protocol, which is also the most effective way to prevent routing attacks. The secure routing protocol should have security features such as an authentication mechanism, encrypted transmission, integrity check, etc., to ensure the authenticity and reliability of routing information. At the same time, the network‘s dynamic nature and resource limitation should also be considered in the protocol’s design to ensure efficient routing and data transmission can be realized under the premise of providing security.

4.2.4. Pay attention to the problem of resource limitation and improve the level of optimized hardware design

In terms of storage and energy resources, wireless sensor networks still face the challenge of resource limitation. These limitations will not only affect the performance and reliability of the network but also increase the complexity of security issues and improve the difficulty of security protection. Therefore, attaching importance to the problem of resource limitation and enhancing and optimizing the level of hardware design have become the keys to ensuring the security and efficiency of wireless sensor networks. First of all, optimize the hardware design to reduce energy consumption. Batteries usually power sensor nodes, but they are often deployed in environments where it is difficult to replace batteries, so a low-power design is fundamental. Technicians can integrate high-efficiency processors, low-power communication modules, and intelligent power management technology into the hardware equipment, which can significantly reduce the energy consumption of nodes and extend the service life of the network. Secondly, the computing and storage capabilities of the hardware should also be further improved. Although resources are easily limited, nodes' computing and storage capabilities can be enhanced to a certain extent by using high-performance hardware components, optimizing hardware architecture, and rational resource allocation to better support network operation. Finally, the hardware design should pay attention to enhancing security. For example, hardware-level security can be provided by integrating security chips at the hardware level to store keys and sensitive data.

5. Summary

This paper comprehensively analyzes the security challenges wireless sensor networks (WSN) face in the Internet of Things environment. It puts forward corresponding solutions to the main security threats, such as data leakage, physical attacks, routing attacks, and denial of service attacks. The research shows that although traditional encryption technology, authentication mechanisms, and physical protection measures have improved the security of WSNs to a certain extent, with the expansion of network applications and the diversification of attack means. The existing protection mechanism is still insufficient in dealing with the complex network environment. Therefore, the security policy based on lightweight encryption, dynamic routing optimization, and machine learning technology has become an important development direction to ensure the security of WSNs in future Internet of Things applications. In this study, by strengthening data encryption, physical protection, secure routing protocol design, and hardware design optimization, WSN can effectively deal with the security threats faced by wireless sensor networks, such as data leakage, physical attacks, routing attacks, and resource constraints, and comprehensively improve its security, stability, and reliability. In addition, the future development of WSN will focus on the popularization and innovation of lightweight security mechanisms, machine learning, artificial intelligence, and other technologies to achieve intelligent security defense and automated response while promoting cross-domain integration and collaborative security to ensure data privacy protection and compliance. In addition, in the future, WSN will adhere to the concept of sustainability and is committed to developing low-power, long-life, and environmentally adaptable sensor nodes to contribute to the sustainable development of the earth. This series of development trends indicates that WSN will play a more critical role in the Internet of Things era, providing more intelligent, safe, and efficient solutions for various industries.

Funding

2024 Guangdong Polytechnic Institute Teaching Achievement Cultivation Project of the Open University of Guangdong (Project No.: 2024CGPY002); Guangdong Provincial Special Innovation Project (Natural Sciences), "Research on Distributed Applications for Industrial Internet Edge Gateway Protocol Adaptation" (Project No.: JXJYGC2021BY0077); Talent Project of the Open University of Guangdong, "Research on Key Technologies for Improving the Performance of Blockchain Application Platforms" (Project No.: 2021F001); Guangdong Philosophy and Social Science Planning Project (GD23SQGL03)

Disclosure statement

The authors declare no conflict of interest.

References

[1] Behiry MH, Aly M, 2019, Cyberattack Detection in Wireless Sensor Networks Using a Hybrid Feature Reduction Technique with AI and Machine Learning Methods. Journal of Big Data, 11(1): 16.

[2] Hao D, 2021, Research on Wireless Sensor Network Security in Internet of Things Environment. Modern Industrial Economy and Information Technology, 11(8): 147–148.

[3] Wang H, 2019, Research on Wireless Sensor Network Security in the Environment of Internet of Things. Computer Knowledge and Technology, 15(6): 31–33.

[4] Zhu M, Ma H, Ma Y, et al., 2020, Wireless Sensor Network Technology and Application. Publishing House of Electronics Industry, Beijing.

[5] Ge C, 2020, Design and Implementation of Intelligent Gateway for Internet of Things, thesis, Jilin University.

[6] Song X, 2021, Research on Optimization Strategy of Wireless Sensor Network Node Deployment, thesis, Beijing University of Posts and Telecommunications.

[7] Wu S, 2019, Signal Processing and Data Fusion in Wireless Sensor Networks. Heilongjiang Science, 15(16): 153–155 + 158.

[8] Deng M, Ma Q, Song Q, et al., 2024, Enhancement of Wireless Sensor Network Authentication Key Agreement Protocol. Computer Engineering, viewed November 7, 2024, https://doi.org/10.19678/j.issn.1000-3428.0069545.

[9] Xie S, Ma L, Su X, et al., 2019, Chaotic Cross Artificial Bee Colony Algorithm for Coverage Optimization of Wireless Sensor Networks. Journal of Nanjing University of Science and Technology, 48(3): 360–366.

[10] Zhang Y, 2024, Research on Interval Dynamic Charging Path Planning for Wireless Sensor Networks, thesis, Taiyuan University of Science and Technology.

[11] Hu Q, 2024, Research on Wireless Sensor Network Engineering of Intelligent Distribution Communication. Modern Transmission, 2024(3): 76–79.

[12] Wei N, Zhao S, Jia N, et al., 2019, Packet Encryption Algorithm for Wireless Sensor Networks Resisting Leakage Attacks. Journal of Sensor Technologies, 37(5): 892–897.

[13] Cheng W, Zhou W, 2019, Design of Multi-Channel Information Fusion Method for Wireless Sensor Networks. Chinese Journal of Sensor Technology, 37(5): 898–903.

[14] Wen J, Tu X, Zhou J, et al., 2024, Data Sharing System of Wireless Sensor Network Based on Data Center. Yangtze River Information and Communication, 37(6): 173–175.

[15] Shen H, 2024, Research on Non-Range-Ranging Node Localization Technology of Wireless Sensor Networks, thesis, Xi'an Technological University.

[16] Ge X, Tan C, Xue Y, et al., 2024, Coverage Deployment and Scheduling Algorithm of Wireless Sensor Networks. Journal of Jilin University (Information Science Edition), 42(3): 400–405.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.