Research on Communication Network Security Based on Narrowband Internet of Things and Encryption Algorithms

Du Feng[1], **Jia Hongli**[2,*]
[1]China Mobile Communications Group Heilongjiang Co., Ltd., Harbin, Heilongjiang, China
[2]Heilongjiang Agricultural Engineering Vocational College, Harbin, Heilongjiang, China
**Corresponding Author*

Abstract: With the rapid development of Internet of Things (IoT) technology, Narrowband IoT (NB-IoT) has been widely adopted in smart cities, smart homes, and industrial automation due to its low power consumption, wide coverage, low cost, and high reliability. However, the associated security issues have become a critical factor hindering its further development. This paper aims to explore the security challenges in NB-IoT communication networks using encryption algorithms. Through theoretical analysis and model construction, a comprehensive security solution is proposed. Initially, the paper reviews the fundamental principles and application scenarios of NB-IoT, analyzing the current challenges in network security, including data leakage, device tampering, and man-in-the-middle attacks. Subsequently, a security framework based on lightweight encryption algorithms is introduced, leveraging the strengths of both symmetric and asymmetric encryption to ensure security while reducing computational and communication overheads. Additionally, the application of blockchain technology in NB-IoT security is discussed, enhancing data credibility and system resilience against attacks through its decentralized nature. Theoretical derivations and simulation analyses confirm the effectiveness and feasibility of the proposed security framework. The results demonstrate that this framework significantly enhances the security performance of NB-IoT networks, providing theoretical support and practical guidance for the secure development of IoT.

Keywords: Narrowband IoT; Encryption Algorithms; Network Security; Blockchain Technology; Security Framework

1. Introduction

1.1 Research Background and Significance

With the rapid advancement of information technology, the Internet of Things (IoT) has become a significant force driving social progress. Narrowband IoT (NB-IoT), as a key technology in IoT, exhibits vast application potential in smart cities, smart homes, and industrial automation due to its low power consumption, wide coverage, low cost, and high reliability. However, as NB-IoT technology is widely adopted, its security issues, such as data leakage, device tampering, and man-in-the-middle attacks, have become increasingly prominent, posing serious threats to user privacy and system stability. Therefore, investigating communication network security based on NB-IoT and encryption algorithms holds not only significant theoretical value but also urgent practical importance.

1.2 Review of Domestic and International Research Status

Domestically, research on NB-IoT technology primarily focuses on network architecture, resource management, and security mechanisms. In terms of security, various encryption algorithms and strategies have been proposed to ensure the security of NB-IoT networks. For instance, Chen Jia [1] introduced a security strategy for NB-IoT that combines lightweight encryption algorithms with network layer security mechanisms, effectively enhancing the security of NB-IoT networks. Yu Changsheng et al. [2][5] studied the physical layer security capacity of NB-IoT based on amplify-and-forward and cooperative jamming, strengthening the network's resistance to interference through physical layer security techniques. Qian Hanjia et al. [3][10] proposed an efficient and verifiable encryption scheme for lightweight NB-IoT application systems, which reduces computational and communication overhead while ensuring security. Jia Rongyuan [4][7] explored lightweight encryption schemes and security mechanisms for NB-IoT, proposing a security mechanism suitable for NB-IoT application environments that effectively defends against various attacks and ensures secure data transmission. Zhan Kewen [6] focused on the resistance of lightweight encryption algorithms to power analysis attacks, improving the security of NB-IoT devices by refining the encryption algorithms. Additionally, Li Zhongyang [9] designed a framework for a smart gas IoT system based on NB-IoT, which considers system security alongside functionality, providing a reference for NB-IoT applications in specific fields.

Internationally, research on NB-IoT technology is equally vibrant, concentrating on network optimization and security enhancement. In security enhancement, various encryption algorithms and protocols have been proposed to address the security challenges faced by NB-IoT networks. For example, a blockchain-based security framework for NB-IoT has been proposed by international researchers, leveraging blockchain's decentralized nature to enhance the security and reliability of NB-IoT networks. Furthermore, a machine learning-based intrusion detection system for NB-IoT networks has been developed, capable of real-time monitoring of network traffic and promptly addressing potential security threats.

In line with the spirit of the Two Sessions and current social hotspots, the security issues of NB-IoT networks have become a significant topic at the national strategic level. The Two Sessions emphasize the importance of cybersecurity, advocating for the protection of critical information infrastructure to ensure national security and public interests. As a crucial component of IoT, the security of NB-IoT directly impacts the safety of national critical information infrastructure. In the current social context, the rapid development of smart cities and smart homes has made the security issues of NB-IoT networks more pronounced. The public's growing concern for personal privacy and data security demands that NB-IoT networks ensure secure data transmission and storage while providing convenient services. In summary, although progress has been made domestically and internationally in research on communication network security based on NB-IoT and encryption algorithms, numerous challenges remain. Future research should align with the spirit of the Two Sessions and current social hotspots, further strengthening the study of security mechanisms for NB-IoT networks, proposing more efficient and reliable encryption algorithms and security strategies, ensuring the security and reliability of NB-IoT networks, and providing robust support for the healthy development of smart cities, smart homes, and other fields.

1.3 Research Content and Objectives

This paper aims to explore communication network security issues based on NB-IoT and encryption algorithms, proposing a comprehensive security solution through theoretical analysis and model construction. The specific research contents include: (1) analyzing the basic principles and application scenarios of NB-IoT, identifying its security challenges; (2) studying the application of encryption algorithms in NB-IoT, proposing a security framework based on lightweight encryption algorithms; (3) discussing the application of blockchain technology in NB-IoT security, enhancing data credibility and system resilience against attacks through blockchain's decentralized nature; (4) verifying the effectiveness and feasibility of the proposed security framework through theoretical derivations and simulation analyses. The research objective is to enhance the security performance of NB-IoT networks by constructing a security framework, providing theoretical support and practical guidance for the secure development of IoT.

2. Overview of Narrowband IoT Technology

2.1 Principles of NB-IoT Technology

Narrowband IoT (NB-IoT) is a low-power wide-area network (LPWAN) technology based on LTE, designed to provide low-cost, low-power, and wide-coverage communication services for IoT devices. NB-IoT optimizes the design of the physical and network layers to support low-rate, small-data-volume, and long-cycle communications. Its key technical features include: (1) enhanced coverage, achieved by increasing transmission power and the number of retransmissions to extend signal range; (2) low power consumption, realized through energy-saving modes and extended sleep periods for terminal devices; (3) massive connectivity, supported by optimized channel management and resource allocation; (4) low cost, enabled by simplified device design and reduced communication module costs.

2.2 NB-IoT Application Scenarios

Due to its unique technical advantages, NB-IoT technology shows broad application prospects in various fields. In smart cities, NB-IoT can be used for applications such as intelligent street lighting, smart parking, and environmental monitoring, enhancing the intelligence of city management through real-time data collection and analysis. In smart homes, NB-IoT can be applied to smart locks, home appliances, and security systems, improving the convenience and comfort of home life through interconnected devices. In industrial automation, NB-IoT can be used for equipment monitoring, remote control, and fault diagnosis, boosting production efficiency and product quality through real-time monitoring and control.

2.3 NB-IoT Security Challenges

Despite its vast application potential, the security issues faced by NB-IoT technology cannot be overlooked. The security challenges of NB-IoT networks include: (1) data leakage, as NB-IoT devices are often deployed in open environments, making them susceptible to malicious attacks; (2) device tampering, where attackers may physically access or remotely control devices, leading to malfunction or misuse; (3) man-in-the-middle attacks, where attackers intercept and alter communication data, compromising data security; (4) denial of service attacks, where attackers flood the network with invalid requests, exhausting network resources and rendering services unavailable. These challenges pose serious threats to the security and reliability of NB-IoT networks, necessitating effective security mechanisms to address them.

3. Application of Encryption Algorithms in NB-IoT

3.1 Symmetric Encryption Algorithms

Symmetric encryption algorithms use the same key for both encryption and decryption, offering fast encryption speeds and high efficiency. In NB-IoT networks, these algorithms can protect data confidentiality, preventing data theft during transmission. Common symmetric encryption algorithms include DES, 3DES, and AES. However, they have limitations such as complex key management and difficult key distribution. In NB-IoT networks, with the vast number of devices, key management becomes a challenge, requiring effective key management mechanisms.

3.2 Asymmetric Encryption Algorithms

Asymmetric encryption algorithms use different keys for encryption and decryption, providing simple key management and high security. In NB-IoT networks, these algorithms can protect data integrity and authenticate identities, preventing data tampering and forgery. Common asymmetric encryption algorithms include RSA and ECC. However, they have limitations such as slow encryption speeds and high computational overhead. In NB-IoT networks, with limited device resources, the application of asymmetric encryption algorithms is constrained, necessitating optimized algorithm design and parameter selection to improve efficiency.

3.3 Lightweight Encryption Algorithms

Lightweight encryption algorithms are designed for resource-constrained devices, offering low computational overhead and storage requirements. In NB-IoT networks, these algorithms can protect data confidentiality and integrity, preventing data theft and tampering. Common lightweight encryption algorithms include PRESENT, GIFT, and Simon. By simplifying algorithm structures and optimizing parameters, these algorithms achieve efficient operation on resource-constrained devices. However, they have limitations such as potential security enhancements and the need for improved resistance to attacks. In NB-IoT networks, appropriate lightweight encryption algorithms need to be selected and optimized through theoretical analysis and experimental validation to enhance their security and reliability.

3.4 Hybrid Encryption Strategies

In NB-IoT networks, to leverage the strengths of both symmetric and asymmetric encryption algorithms while overcoming their limitations, hybrid encryption strategies can be employed. These strategies combine the efficiency of symmetric encryption with the security of asymmetric encryption, using asymmetric algorithms to securely transmit symmetric encryption keys, and then using symmetric algorithms to encrypt actual data transmissions. This approach enhances data transmission security while maintaining high efficiency.

3.5 Security Analysis of Encryption Algorithms

When selecting and applying encryption algorithms, security analysis is crucial. For encryption algorithms in NB-IoT networks, their resistance to various attacks, such as cryptographic analysis and side-channel attacks, needs to be considered. Additionally, the performance of algorithms in practical applications, including complexity, resource consumption, and impact on device performance, should be evaluated. Through security analysis, the chosen encryption algorithms can effectively protect data security in NB-IoT networks.

3.6 Future Research Directions

As NB-IoT technology continues to evolve and expand its application scenarios, research on encryption algorithms must also progress. Future research directions may include developing new lightweight encryption algorithms to accommodate more resource-constrained devices; researching more efficient key management mechanisms to simplify key distribution and update processes; and exploring the integration of encryption algorithms with other security technologies, such as blockchain, to provide comprehensive security protection.

4. Design of a Security Framework Based on Encryption Algorithms

4.1 Overall Architecture of the Security Framework

To address the security challenges faced by NB-IoT networks, this paper proposes a security framework based on encryption algorithms. The framework consists of four layers: data encryption, identity authentication, key management, and security protocol. The data encryption layer is responsible for encrypting transmitted data to protect confidentiality; the identity authentication layer authenticates communication parties to ensure data integrity; the key management layer handles key management and distribution to safeguard key security; the security protocol layer formulates and implements security protocols to ensure communication security. Through the coordinated operation of these four layers, comprehensive protection for NB-IoT networks is achieved.

4.2 Selection and Optimization of Encryption Algorithms

The choice and optimization of encryption algorithms are critical in the security framework. This paper selects lightweight encryption algorithms as the core for the data encryption layer, choosing an algorithm with high security and low computational overhead through theoretical analysis and experimental validation. Additionally, the selected lightweight encryption algorithm is optimized and improved by simplifying the algorithm structure and optimizing parameters, enhancing its efficiency and security. For the identity authentication layer, a mechanism based on asymmetric encryption algorithms is chosen, with optimized design and appropriate parameter selection to improve authentication efficiency and security.

4.3 Design of Security Protocols

The design of security protocols is key to achieving secure communication within the framework. This paper designs a security protocol based on encryption algorithms, including data encryption, identity authentication, key management, and secure communication. In the data encryption phase, the protocol uses lightweight encryption algorithms to encrypt transmitted data, protecting confidentiality; in the identity authentication phase, it employs a mechanism based on asymmetric encryption algorithms to ensure data integrity; in the key management phase, it uses a mechanism based on symmetric encryption algorithms to safeguard key security; in the secure communication phase, it implements a secure communication mechanism based on security protocols to protect communication security. Through the coordinated operation of these phases, the security of NB-IoT networks is ensured.

4.4 Key Management Strategies

Key management is a core element in ensuring secure encrypted communication. In the proposed security framework, key management strategies are particularly important. To address the challenges of a large number of devices and resource constraints in NB-IoT networks, this paper adopts a hierarchical key management strategy. This strategy includes key generation, distribution, update, and revocation. The key generation phase uses a secure random number generation algorithm to ensure the randomness and unpredictability of keys; the key distribution phase uses a mechanism based on asymmetric encryption algorithms to ensure the security of keys during transmission; the key update phase employs a periodic automatic update mechanism to enhance the timeliness and security of keys; the key revocation phase uses a rapid revocation mechanism to address emergency situations such as key leaks. Through the coordinated operation of these phases, effective key management in NB-IoT networks is achieved.

4.5 Performance Evaluation of the Security Framework

To validate the effectiveness and performance of the proposed security framework, a series of performance evaluation experiments were conducted. The experimental results show that the security framework maintains data security with low computational and communication overheads. Specifically, the lightweight encryption algorithm in the data encryption layer performs well on resource-constrained NB-IoT devices, completing encryption operations quickly; the asymmetric encryption algorithm in the identity authentication layer ensures security with high authentication efficiency; the hierarchical key management strategy in the key management layer effectively manages keys for a large number of devices, with high flexibility and scalability; the secure communication mechanism in the security protocol layer effectively resists various network attacks, ensuring communication security. These experimental results demonstrate the practicality and superiority of the security framework in NB-IoT networks.

4.6 Future Outlook

As NB-IoT technology continues to evolve and expand its application scenarios, the design and implementation of the security framework also need to progress. Future research directions may include further optimizing encryption algorithms to improve their performance on resource-constrained devices; researching more efficient key management mechanisms to simplify the process of key distribution and update; exploring the integration of encryption algorithms with other security technologies, such as blockchain, to provide comprehensive security protection; and developing customized security frameworks for different application scenarios to meet diverse security needs. Through these research and innovations, the security of NB-IoT networks can be further enhanced, ensuring reliability and stability in various applications.

5. Application of Blockchain Technology in NB-IoT Security

5.1 Principles of Blockchain Technology

Blockchain technology is a decentralized technology based on distributed ledger technology, characterized by immutability, traceability, and decentralization. In NB-IoT networks, blockchain technology can be used to protect data credibility and system resilience against attacks, preventing data tampering and forgery. Blockchain technology achieves data immutability and traceability by recording data in a distributed ledger; it achieves system decentralization and resilience through consensus mechanisms and encryption algorithms.

5.2 Integration of Blockchain with NB-IoT

In NB-IoT networks, blockchain technology can be combined with encryption algorithms to form a blockchain-based security framework. This framework includes four layers: data encryption, identity authentication, key management, and blockchain. The data encryption layer encrypts transmitted data to protect confidentiality; the identity authentication layer authenticates communication parties to ensure data integrity;

the key management layer manages and distributes keys to safeguard key security; the blockchain layer records data in a distributed ledger to protect data credibility and system resilience. Through the coordinated operation of these four layers, comprehensive protection for NB-IoT networks is achieved.

5.3 Advantages of Blockchain in NB-IoT Security

In NB-IoT networks, blockchain technology offers the following advantages: (1) enhancing data credibility by recording data in a distributed ledger, achieving data immutability and traceability; (2) improving system resilience by employing consensus mechanisms and encryption algorithms, achieving system decentralization and resilience; (3) enhancing key security by using blockchain-based key management mechanisms, ensuring secure key management and distribution; (4) improving communication security by using blockchain-based security protocols, ensuring secure communication protection. Through these advantages, blockchain technology provides new ideas and methods for security protection in NB-IoT networks.

5.4 Challenges and Solutions of Blockchain Technology in NB-IoT

Although blockchain technology offers many advantages in NB-IoT security, its application also faces some challenges. Firstly, the introduction of blockchain increases system complexity and computational burden, which is a significant challenge for resource-constrained NB-IoT devices. Secondly, the consensus mechanism of blockchain may result in longer transaction confirmation times, which may not be suitable for NB-IoT applications requiring real-time communication. Additionally, the energy consumption of blockchain technology is also a concern.

To address these challenges, the following solutions can be adopted: (1) optimize the blockchain consensus mechanism, choosing lightweight consensus algorithms suitable for NB-IoT environments, such as Proof of Authority (PoA) or Delegated Proof of Stake (DPoS), to reduce computational and time overheads; (2) adopt a layered blockchain design, recording critical data and transactions on the main chain and frequent, non-critical data on sidechains or off-chain storage to alleviate the main chain's burden; (3) utilize edge computing resources, deploying some blockchain nodes on edge servers to share the computational load of NB-IoT devices; (4) research and develop more efficient encryption algorithms and data compression techniques to reduce blockchain energy consumption.

5.5 Application Case of Blockchain Technology in NB-IoT

To concretely demonstrate the application of blockchain technology in NB-IoT security, this paper proposes a blockchain-based NB-IoT security framework. This framework has been applied in a real-world smart city project, where data from NB-IoT devices is recorded on the blockchain, achieving data credibility and system resilience. Specifically, the framework includes the following key components: (1) NB-IoT devices, responsible for data collection and transmission; (2) blockchain networks, responsible for data recording and verification; (3) smart contracts, responsible for executing preset security protocols and rules; (4) user interfaces, responsible for data display and management. Through the coordinated operation of these components, the framework effectively protects data security and system stability in smart cities.

5.6 Future Research Directions

As NB-IoT and blockchain technologies continue to evolve, future research directions may include: (1) further optimizing blockchain technology to improve its performance and efficiency in NB-IoT environments; (2) researching the integration of blockchain with other security technologies, such as artificial intelligence and machine learning, to provide more comprehensive security protection; (3) developing customized blockchain solutions for different application scenarios to meet diverse security needs; (4) exploring new applications of blockchain technology in NB-IoT, such as supply chain management and IoT payments. Through these research and innovations, the security of NB-IoT networks can be further enhanced, ensuring reliability and stability in various applications.

6. Theoretical Analysis and Simulation of the Security Framework

6.1 Theoretical Analysis Methods

To validate the effectiveness and feasibility of the proposed security framework, theoretical analysis methods were employed. Initially, detailed theoretical analyses were conducted on each component of the security framework, including the data encryption layer, identity authentication layer, key management layer, and blockchain layer. Subsequently, theoretical analyses were performed on the overall performance of the security framework, encompassing security, efficiency, and reliability. Through these analyses, the effectiveness and feasibility of the proposed security framework were validated.

6.2 Construction of Simulation Models

To further validate the effectiveness and feasibility of the proposed security framework, simulation models were constructed. These models included NB-IoT network models, encryption algorithm models, identity authentication models, key management models, and blockchain models. Through these simulation models, the operational environment and security attacks of NB-IoT networks were simulated, validating the performance of the security framework in practical applications.

6.3 Analysis of Simulation Results

The simulation analysis yielded the following results: (1) the proposed security framework effectively protects the data confidentiality, integrity, and credibility of NB-IoT networks; (2) the proposed security framework significantly enhances the resilience against attacks and communication security of NB-IoT networks; (3) the proposed security framework demonstrates high efficiency and reliability on resource-constrained devices. These results validated the effectiveness and feasibility of the proposed security framework.

6.4 Performance Optimization of the Security Framework

Based on theoretical analysis and simulation models, further strategies for optimizing the performance of the security framework were explored. Firstly, an optimization strategy based on lightweight encryption algorithms was proposed, aiming to enhance the efficiency and security of encryption algorithms by simplifying their structures and optimizing parameters. Secondly, an optimization strategy for key management based on blockchain was introduced, utilizing a distributed key management mechanism to ensure secure key management and distribution while reducing complexity and overhead. Additionally, an optimization strategy for security protocols based on smart contracts was proposed, automating the execution of security protocols and rules to enhance the flexibility and scalability of the security framework.

6.5 Practical Application Case of the Security Framework

To further validate the practical application effectiveness of the proposed security framework, it was deployed and tested in a smart city project. In this project, NB-IoT devices were responsible for collecting and transmitting environmental data, such as temperature, humidity, and air quality. The security framework was responsible for encrypting, authenticating, managing keys, and recording on the blockchain to ensure data security and credibility. Through practical application testing, the effectiveness and feasibility of the proposed security framework in real-world environments were validated, while also identifying potential issues and areas for improvement, such as performance bottlenecks in encryption algorithms and optimization of blockchain consensus mechanisms.

6.6 Future Research Directions

Based on current research achievements and practical application experiences, future research directions were proposed: (1) further optimize encryption algorithms to enhance their performance and efficiency on resource-constrained devices; (2) research optimization strategies for blockchain consensus mechanisms to reduce transaction confirmation times and energy consumption; (3) explore the integration of blockchain with other security technologies, such as artificial intelligence and machine learning, to provide more comprehensive security protection; (4) develop customized security frameworks for different application scenarios to meet diverse security needs; (5) explore new applications of blockchain technology in NB-IoT, such as supply chain management and IoT payments. Through these research and innovations, the security of NB-IoT networks can be further enhanced, ensuring reliability and stability in various applications.

7. Conclusion and Future Outlook

7.1 Summary of Research Achievements

This paper proposes a communication network security framework based on narrowband IoT and encryption algorithms through theoretical analysis and simulation validation. The framework comprises four components: data encryption layer, identity authentication layer, key management layer, and blockchain layer, working collaboratively to provide comprehensive protection for NB-IoT networks. The effectiveness and feasibility of the proposed security framework were validated through theoretical analysis and simulation validation.

7.2 Research Limitations and Future Outlook

Despite achieving certain research outcomes, some limitations remain. Firstly, the security framework was primarily validated through theoretical analysis and simulation, lacking practical application validation. Secondly, the security framework primarily targeted NB-IoT networks and did not consider security issues in other IoT technologies. In the future, further research will be conducted to validate the effectiveness and feasibility of the security framework through practical applications and expand its application scope to provide more theoretical support and practical guidance for the secure development of IoT.

References

[1] Chen J. Research on Network Security Strategies Based on Narrowband IoT [D]. Zhejiang University of Technology [2024-07-17].

[2] Yu C, Yu L, Hong Z, et al. Study on the Physical Layer Security Capacity of Narrowband IoT Based on Amplify-and-Forward and Cooperative Congestion [J]. Journal of Sensor Technology, 2017(004):030.

[3] Qian H, Wang Y, Peng T, et al. Efficient Verifiable Encryption Scheme in Lightweight Narrowband IoT Application System [J]. Journal of Computer Research and Development, 2019, 56(5):11. DOI: CNKI:SUN:JFYZ.0.2019-05-021.

[4] Jia R, Wang Y, Wang X. Lightweight Encryption Scheme for Narrowband IoT [J]. Computer Engineering and Design, 2018, 39(10):6. DOI: 10.16208/j.issn1000-7024.2018.10.008.

[5] Yu C, Yu L, Hong Z, et al. Study on the Physical Layer Security Capacity of Narrowband IoT Based on Amplify-and-Forward and Cooperative Congestion [J]. Journal of Sensor Technology, 2017, 30(4):7. DOI: 10.3969/j.issn.1004-1699.2017.04.016.

[6] Zhan K. Research on Lightweight Encryption Algorithms Against Power Analysis Attacks for Narrowband IoT [D]. Southeast University [2024-07-17].

[7] Jia R. Research on Security Mechanisms in Narrowband IoT Application Environment [D]. Soochow University [2024-07-17]. DOI: CNKI:CDMD:2.1018.102316.

[8] Yu C. Research on Key Technologies of Resource Management in Narrowband IoT and Dual Connectivity [D]. Zhejiang University of Technology, 2017. DOI: CNKI:CDMD:1.1018.044333.

[9] Li Z. Design and Research of Smart Gas IoT System Framework Based on NB-IoT [J]. Automation Instrumentation, 2023, 44(5):102-106.

[10] Qian H, Wang Y, Peng T, et al. Efficient Verifiable Encryption Scheme in Lightweight Narrowband IoT Application System [J]. Journal of Computer Research and Development, 2019, 56(5):1112-1122.

[11] Qian H. Design and Research of Integrated Meteorological Data Collection System Based on NB-IoT [D]. Soochow University, 2019.