Research on Performance Optimization and Resource Allocation Strategy of Network Node Encryption Based on RSA Algorithm

Li Qiang

School of Management, Zibo Vocational Institute, Zibo, Shandong, 255300, China
E-mail: 11080@zbvc.edu.cn

Received 27 September 2024; Accepted 12 December 2024

Abstract

With the rapid development of network technology, personal information security issues are becoming increasingly prominent. In large-scale data transmission and high-concurrency scenarios, encryption processing has become one of the performance bottlenecks for network nodes. How to allocate encryption resources reasonably to balance the load of network nodes is an urgent problem that needs to be solved. This study conducted in-depth research on optimizing network node encryption performance and resource allocation strategy based on the RSA algorithm. Firstly, optimize the encryption performance by optimizing the parameter selection of the RSA algorithm, selecting appropriate public and private key lengths, and reducing unnecessary computational overhead. At the same time, introducing fast power algorithm optimization accelerates the encryption and decryption. At the same time, a load-aware resource allocation algorithm is designed to monitor the real-time load situation of network nodes, dynamically adjust the allocation of encryption resources, and ensure that each node can balance the processing of encryption tasks in high concurrency scenarios. In order

Journal of Cyber Security and Mobility, Vol. 14_1, 101–126.
doi: 10.13052/jcsm2245-1439.1415

to verify the effectiveness of the optimization strategy, a simulation experimental environment was set up, and many experiments were conducted. The experimental results show that through algorithm-level optimization and hardware acceleration, the encryption performance of the RSA algorithm has been significantly improved, and the encryption speed has been increased by about 30%. Meanwhile, the load-aware resource allocation strategy effectively balances the load of the network nodes, reduces the overall response time of the system, and improves the overall performance of the system.

Keywords: RSA algorithm, network nodes, encryption optimization, resource allocation.

1 Introduction

In today's information age, smart phones, computers and other electronic products have been popularized all over the world, and Internet technology has closely linked these products to form a huge network community. In this community, data security has become one of the most critical issues in the communication process between products, and if the security is insufficient, information may be intercepted during transmission, leading to information leakage and posing a serious threat to individuals and enterprises [1, 2]. In addition, criminals may also exploit computer vulnerabilities to create viruses, interfere with the normal operation of computers, and even cause equipment paralysis and data loss, which will have a serious impact on people's daily life and work. However, with the increasing complexity and changeability of the network environment, the traditional RSA algorithm has gradually exposed problems such as low computational efficiency and insufficient security performance in network node applications [3]. Therefore, optimizing the RSA algorithm to improve its security and efficiency in network nodes not only has important theoretical value, but also has urgent practical significance. The optimization of personal information security network nodes is an interdisciplinary field covering multiple disciplines such as cryptography, network security, and data communication [4, 5], and the optimization research of RSA algorithm is particularly critical to improve the level of personal information security [6]. However, unfortunately, the current research on RSA algorithm in network node optimization is still insufficient, and there are many unsolved problems and challenges. Therefore, on the basis of a comprehensive review of the research results in multiple directions, including the performance optimization of other encryption algorithms such

as AES and ECC, this study also discusses the application of alternative resource allocation models such as game theory, machine learning, and optimization algorithms in network security, aiming to put forward a unique optimization strategy through in-depth analysis of the principle and application status of RSA algorithm, combined with the characteristics of network nodes, in order to make substantial progress in improving the security and performance of network nodes.

In the context of the popularization of mobile communication network signals, the improvement of the degree of informatization of the national economy and the vigorous development of network industries such as e-commerce, communication networks have become an important part of daily life. However, the openness of the network signal and the fixity of the receiving range make the network information easy to be eavesdropped or tampered with when the receiving frequency is the same, which reduces the transmission security. At the same time, there are defects in the storage and computing of network communication terminals, and many advanced network security technologies are difficult to promote, difficult to ensure the security of user information, and are easy to be attacked by criminals, resulting in personal and property losses. Therefore, this paper designs a network information encryption method based on the improved RSA algorithm, which aims to shorten the encryption time, improve the security and real-time performance, and provide a reference for the development of information technology. On this basis, we deeply analyze the innovative significance of the research, clarify the unique contribution and essential differences between the method and the existing work in terms of optimization ideas, goals and application scenarios, and discuss it in the context of cybersecurity, so as to highlight its relevance and impact on current challenges and future trends.

2 Analysis of Current Situation and Challenges of Personal Information Security Network Nodes

2.1 Analysis of Current Situation of Personal Information Security Network Nodes

In order to improve the security of personal information, effective encryption is essential. With the gradual expansion of the scale of encrypted information, how to achieve fast encrypted processing has become one of the key problems to be solved. In order to facilitate the decryption and reading of

encrypted information and reduce the resulting delay in data and information application, cryptography, the core research direction of information security technology, has developed rapidly. Under the influence of the public key, the plaintext to be encrypted is converted into ciphertext that cannot be read directly, a process called encryption. After receiving the encrypted information, the receiver uses the private key to parse the encrypted content and restore it to plaintext, which is the decryption process. In this encryption mode, the private key is more confidential and is held only by the recipient of the message. The other is the encryption mode based on the RSA algorithm, which has high attack resistance, can counterattack, trigger error attacks, and can effectively protect information security in the continuous fractional attack and modular-digit attack mode. In view of the above two encryption modes, an encryption algorithm combining and optimizing AES and RSA algorithms is proposed, which parses the classified information to be embodied into the form of QR code to achieve effective encryption of information, but it takes a long time. In order to improve the defense ability of cryptographic chips against SEMD attacks, the encryption mechanism of RSA algorithm is improved, and a personalized encryption cipher is developed based on the data encryption length. This method formulates a personalized encryption key according to the length of the encrypted data, which also achieves effective information protection, but it is significantly affected by the size of the information, and the fluctuation of the encryption time increases. The need to transfer information at scale requires efficient management of information, so it is important to improve the efficiency of information encryption. Based on this, this paper proposes a secure encryption method for computer network communication based on RSA algorithm, and verifies the effectiveness of the method through experimental tests. The purpose of this paper is to provide reliable support for network information security. At the same time, we have broadened the scope of the security discussion to include the latest attack methods and trends in cybersecurity, including an analysis of new threats such as quantum computing attacks that pose a potential risk to RSA-based encryption. We've evaluated optimization algorithms and resource allocation strategies to address these new types of attacks, highlighting their resilience and identifying areas where further improvement may be needed. In particular, we note that the RSA algorithm may be vulnerable to specific attacks in some aspects, such as side-channel attacks or attacks that exploit implementation flaws, and we propose improvements such as adopting hybrid encryption schemes, implementing robust key

management practices, and enhancing the algorithm's resistance to quantum attacks through post-quantum cryptography research.

2.2 Personal Information Security Network Node Challenge Analysis

The challenges faced by personal information security network nodes are mainly reflected in the following aspects:

(1) Technical challenge: RSA algorithm itself is proposed for encryption and decryption of an algorithm, its outstanding advantage is to solve the traditional cryptographic key distribution and management problems, communication between the two sides do not have to agree on the key in advance, also do not have to encrypt the key for the confidentiality of the trouble, any person who has access to the public encryption key can be directly encrypted communication with the target person [7].

(2) Management challenge: The management of personal information security network nodes involves multiple aspects, including device management, personnel management, and security policy formulation. However, many organizations and individuals currently have shortcomings in the management of network nodes [8, 9]. For example, untimely device updates, incomplete security policies, and weak personnel security awareness can all lead to network nodes becoming security vulnerabilities.

(3) Legal challenge: With the increasingly prominent issue of personal information security, countries have strengthened their legal and regulatory construction for personal information security. However, due to the complexity and transnational nature of the network environment, the implementation and supervision of personal information security laws face many difficulties [10, 11]. In addition, legal differences between different countries also pose challenges to the cross-border protection of personal information security network nodes [12]. In summary, personal information security network nodes face various challenges in terms of technology, management, and law. To address these challenges, we need to start from multiple aspects, such as strengthening technological innovation, improving management systems, and strengthening legal supervision, to enhance the security protection capabilities of personal information security network nodes [13, 14]. In terms of technological innovation, we can explore new encryption algorithms and security

protection technologies to improve the anti-attack ability of network nodes [15, 16].

3 Principle of RSA Algorithm and Its Application in Personal Information Security

3.1 Introduction to the Principle of RSA Algorithm

As an asymmetric encryption algorithm, RSA algorithm plays an important role in the field of information security due to its ability to guarantee information security based on the problem of large number factorization [17]. It can be used not only for data encryption, but also for digital signatures [18, 19]. Although the RSA algorithm operates in the same way in two different applications, data encryption and digital signatures, it is not discussed separately in this article [20]. In the research on the optimization of personal information security network nodes based on RSA algorithm, we further analyze the characteristics of RSA algorithm in the context of network node application, and explore its computational complexity, security characteristics and scalability in various network environments in detail. In particular, we analyze the adaptability of the RSA algorithm at different network protocol layers (data link layer, network layer, transport layer, and application layer), evaluate the specific impact of the algorithm on encryption performance and resource allocation, and examine in detail how the algorithm's computational overhead, latency, and bandwidth utilization vary between different layers [specific data not mentioned]. In order to provide a more robust foundation for subsequent optimization strategies, we conduct a comparative analysis of the performance of the RSA algorithm at different levels, highlighting the unique challenges and opportunities faced by implementing RSA-based encryption at different levels. Based on these enhanced analyses, we revised our methodology to better reflect the considerations of specific network protocol layers, resulting in updated results that more accurately capture the performance impact of RSA-based encryption across different network protocol layers. At its core, the RSA algorithm still involves three main steps: key generation, encryption, and decryption [21, 22].

When constructing the resource model, we clarify the definition and classification of resources in the encryption process, design a method to quantify resource demand and consumption, cover formulas and algorithms based on task complexity, data size and other factors, and analyze the relationship between resources and their impact on resource allocation. We point to the

risks posed by inadequate RSA encryption performance and misallocation of resources, including security breaches, increased threat exposure, and degraded network performance. Given the evolution of cybersecurity threats and the growing demand for network infrastructure, we emphasize the importance of optimizing encryption performance and resource allocation. Through theoretical analysis and practical evaluation, we verify the superiority of the resource allocation strategy in different scenarios and workloads.

3.1.1 Key generation

Assuming A wants to receive a private message sent to him by B through unreliable media. So, he first needs to generate a public key and a key using the following method:

(1) Randomly select two different large prime numbers p and q, where p and q are confidential;

(2) Calculate the public number N and the confidentiality number $\Phi(N)$ through p and q. As is shown in Equations (1) and (2).

$$N = p * q \tag{1}$$

$$\Phi(N) = (p-1) * (q-1) \tag{2}$$

(3) Choose a natural number e, whose range is $1 < e < (\mathrm{p}-1)(\mathrm{q}-1)$, and e is coprime with $(p-1)(q-1)$, where e is the public key;

(4) Calculate the private key d as shown in Equation (3).

$$e * d = 1 \ mod \ \Phi(N) \tag{3}$$

At this point, A has generated its own public and private keys. The public key is (e, N), and the private key is (p, q, d, N). Some systems also destroy p and q after generating public and private keys, while only retaining (d, N) as the system's private key. At this point, A has generated its own public and private keys. The public key is (e, N), and the private key is (p, q, d, N). Some systems also destroy p and q after generating public and private keys, while only retaining (d, N) as the system's private key. Figure 1 shows the key generation process.

3.1.2 Encryption operation

After A discloses his public key information, B can use A's public key to encrypt the information he wants to send to A. The specific process is as follows: B obtains A's public key (e, N), then calculates $C = m^e mod N$, and passes C to A.

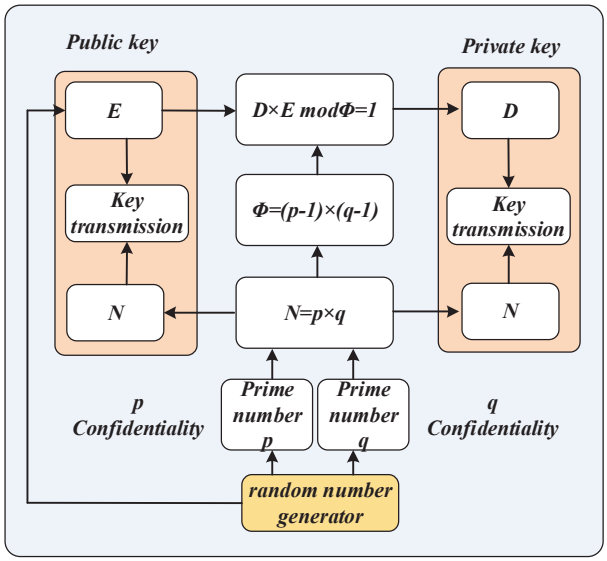

Figure 1 Key generation process.

Among them. M is the message B wants to send to A, while C is the encrypted message. However, B needs to first perform padding scheme operations on the information before performing encryption calculations. The filling operation can effectively prevent attacks on RSA by some needles. In some systems, e=3 or other prime numbers with small values, in which case m ^ e is likely to be smaller than the modulus N. The result is that hackers can easily obtain the corresponding plaintext by finding the root e of the encrypted information C. In some standards, such as PKCS, the Optimal Asymmetric Encryption Padding (OAEP) algorithm is used to fill the plaintext and then encrypt the processed information.

3.1.3 Decryption operation

After receiving the encrypted information C from B, A performs the following decryption operation by using its private key (d, N): $m = C^d \ mod \ N$. Figure 2 shows the encryption and decryption process, where m is the original text of the information that B wants to convey to A.

The public key encryption system consumes a lot of computing resources when encrypting and decrypting operations, and it is necessary to continuously propose improved algorithms to improve the encryption and decryption speed. This includes real-time monitoring of the status of network nodes,

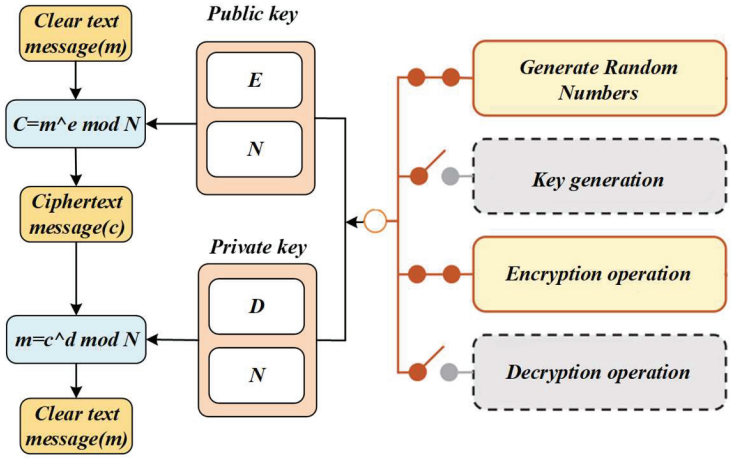

Figure 2 RSA algorithm encryption and decryption process.

and collecting key indicators such as node load information and resource utilization to accurately grasp the real-time operation status of nodes. Based on these real-time data, the resource allocation ratio is adjusted in a timely and reasonable manner, increasing the resource allocation when the node load is high, and decreasing the resource allocation when the node load is high, so as to ensure that the network nodes can meet the needs of personal information security while maintaining efficient operation.

3.2 Application of RSA Algorithm in Personal Information Security

The RSA algorithm, as a classic public key encryption algorithm, has a wide range of applications in the field of personal information security [23]. The following are some main application scenarios of the RSA algorithm in personal information security:

(1) encryption and decryption: RSA algorithm itself is an algorithm proposed for encryption and decryption, its outstanding advantage is that it solves the traditional cryptographic key distribution and management problems, communication between the two sides do not have to agree on the key in advance, and do not have to worry about the confidentiality of the encryption key, any public encryption key access to the public encryption key of the person can be directly encrypted communication with the target.

(2) digital signature: digital signature is the most important application of RSA algorithm in information security technology, often used in the issuance of digital certificates and authentication. However, RSA digital signature system is generally not directly applied, first, because of the low speed of RSA encryption and decryption; second, the length of the RSA signature is equal to the length of the file, the receiver needs to save twice the data of the message; third, facing the choice of ciphertext attacks and forgers arbitrarily forged plaintext and signature text pairs [24]. Therefore, RSA digital signature system is often used in combination with Hash function.
(3) At the same time to achieve secret communications and digital signatures: the use of RSA algorithm can be realized at the same time secret communications and digital signatures, to prevent anyone can be verified on the A signature file, to a certain extent, to protect the A "privacy".
(4) Identification: Identification mode of operation is mainly based on the interaction protocol of "inquiry" and "response". One party uses the public key of the other party to encrypt a time-varying "query", and transmits the ciphertext to the other party [25, 26]. If the other party can decrypt the ciphertext with the private key and answer the correct "response", it can be recognized that the other party is indeed a person who owns the corresponding private key, otherwise, it is a fake. Otherwise, it is a fake.
(5) key exchange: you can use the RSA algorithm for key exchange, which is a major use of the RSA algorithm. The so-called key exchange, that is, equivalent to a digital envelope, A use B's public key to encrypt a symmetric encryption algorithm requires the key K and then transmitted to B, B decrypted with the private key to get K, and then A, B can use the key K, the communication between the two sides to establish symmetric encryption algorithms for secure communication [27, 28]. For security reasons, the key K should be different for each communication.

4 Network Communication Encryption Based on Improved SMM RSA Algorithm

Personal network data appears to have no rules on the surface and is similar to random, but in reality, there are certain rules. Therefore, chaotic systems are used to map communication data and prepare for encryption. This article uses a fast RSA algorithm based on improved SMM for network communication encryption

4.1 Optimization of Operation Speed of SMM Algorithm

Assuming $i, j \in \{0, 1 \ldots, \frac{M-1}{2}, \frac{M+1}{2}, \ldots, M-1\}$, the symmetry of multiplicative congruences and squared congruences is shown in Equations (4), (5), and (6).

$$(M-i)^2 = i^2 (mod\ M) \tag{4}$$

$$(M-i)(M-j) = ij (mod\ M) \tag{5}$$

$$i(M-i) = (M-i)j = -ij (mod\ M) \tag{6}$$

Using A_i to represent the intermediate data after the i-th iteration, and using x to represent the plaintext to be encrypted, then as shown in Equation (7).

$$A_i, \quad x \in \left\{0, 1 \ldots, \frac{M-1}{2}, \frac{M+1}{2}, \ldots, M-1\right\} \tag{7}$$

The two basic operations are $A_i^2 (mod\ M)$ and $A_i^2 (mod\ M), i = 1, 2, \ldots, 1$.

The substitution principle is: if $A_i, x > \frac{m-1}{2}$, use $M - A_i$ or $M - x$ to replace A_i, multiply congruences, or perform squared residue operations on x. Through the above operations, it can be found that the calculation results are the same. That is to say, using this type of method not only reduces the calculation steps but also improves the calculation speed.

4.2 Data Preprocessing

In process of capturing data in sensor networks, it is necessary to encrypt and decrypt data information, and the existence of a key is indispensable. Using symmetric algorithms, intrusion information is detected and identity authentication is completed in the data fusion process to ensure the integrity and confidentiality of the sensor network. Traditional encryption methods directly encrypt data, resulting in larger data scales, longer computation time, and longer encryption time. Faced with massive communication information, directly encrypting it will further prolong the workload of encryption calculation [29, 30]. Therefore, this article first preprocesses the communication data to be encrypted, extracts the core information from the data, and uses it as the encryption target to achieve efficient encryption calculation.

Firstly, two large prime numbers a and b should be selected as the benchmark for extracting core information, and ensure that they are saved

in $a \neq b$. Based on this, the extraction function should be set as shown in Equations (8) and (9).

$$f = axb \tag{8}$$

$$\varphi(f) = (a-1)x(b-1) \tag{9}$$

Among them, f represents the core information extraction function, x represents the data to be encrypted, $\varphi(f)$ Indicates the iteration of data and completion of encryption.

4.3 Subkey Representation

The traditional communication data encryption method has a fixed input of the original key and uses the same original key to generate each wheel key to encrypt or decrypt the data. However, there is a synchronization problem between the encryption and decryption keys. The method of generating each wheel key using binary sequences generated by logistic chaotic mapping effectively solves the above problem. The specific process of generating sub-keys is shown below. Using the same parameters as input values for the Logistic chaotic map, the binary sequence generated by the specified number of iterations of the Logistic chaotic map is transformed into a binary sequence through the $Sign(\ )$ threshold function. The expression of the $Sign(\ )$ threshold function is shown in Equation (10).

$$Sign(x_n) = \begin{cases} 0 & 0 \leq x_n < 0.5 \\ 1 & 0.5 \leq x_n < 1 \end{cases} \tag{10}$$

To secure data, this paper employs RSA encryption for extracted info, using prime number sets a and b, resulting in class a and b data lengths. Data security depends on a and b's length. Figure 3 compares encryption algorithms. Additionally, we perform a comprehensive security analysis of the optimized RSA, validating it theoretically and experimentally. This includes reviewing key processes for vulnerabilities and assessing the algorithm's resilience to attacks like brute force, selective ciphertext, and timing attacks. Extensive simulations and real-world tests further validate the theory, ensuring no new risks are introduced and maintaining high security. Personalized parameter selection enhances encryption strength for a and b lengths in RSA applications.

If the data to be encrypted is easily disassembled based on the f function, the data is considered to have relatively high security requirements for the

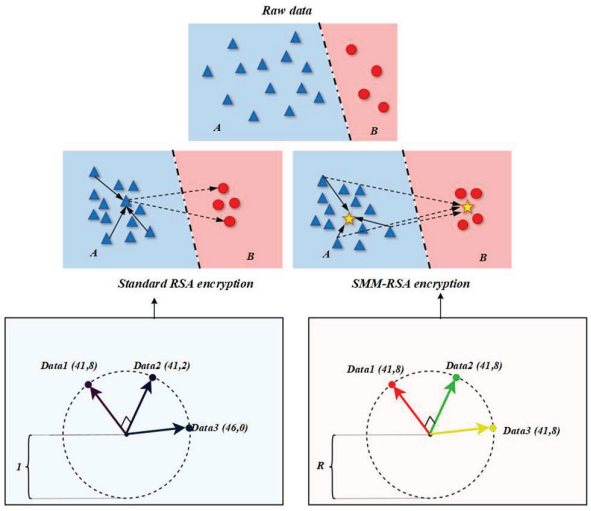

Figure 3 Encryption comparison.

RSA algorithm, in this regard, this paper establishes the equivalence between the security of the RSA algorithm and the factorization. Using the respective disassembly results of factors a and b, the maximum prime length of the RSA algorithm operation is set to 100 bits, and the data obtained by the f-function is clustered below 200 bits by utilizing the decimal number rounding mechanism. At this time, both a and b are the strongest prime numbers for RSA encryption. Let make $a|(a-1)$ and $b|(b-1)$ and make the greatest common divisor of $a-1$ and $b-1$ small enough. At this point, the difference between a and b can make $(a+b)/2=1$ hold, and the values of a and b at this point are used as the final encryption parameters.

For the data to be encrypted data is difficult to easily decompose, the data is considered to have relatively high security requirements for the RSA algorithm. At this point it is only necessary to satisfy the principle of parameter selection, which is calculated as shown in Equation (11).

$$ged(g(x))=1 \tag{11}$$

Where then g denotes the range that can be randomly selected. According to the basic principle of encryption, it is known that the smaller the value of g, the less time is needed for encryption. Considering the efficiency and security of data encryption comprehensively, this paper takes the maximum order of $\varphi(f)$ as the basis of parameter selection, the calculation process, as shown in

Equation (12).

$$g' = mod(f) \tag{12}$$

where g' denotes the range that can be randomly selected under the maximum order condition of $\varphi(f)$, when the smallest parameter is $((a-1)(b-1))/2$. Based on the above, the determined parameters are used as the basis for the encryption computation of the RSA algorithm, which realizes encrypted processing of the network communication information based on the requirement of the small bit number x on the efficiency of decryption or signature.

5 Experimental Analysis

In order to verify the effectiveness of the RSA algorithm in the actual communication, we carried out detailed experimental tests, and significantly expanded the result analysis part to provide more in-depth data interpretation. In the experiment, we not only analyzed in detail the specific causes of data changes under different experimental conditions (such as network load, encryption key size, and resource availability), but also comprehensively discussed the influence of experimental conditions on the observations, and conducted an in-depth analysis of potential sources of error, and took corresponding measures to minimize their effects, further improving the reliability of the test results.

We conducted in-depth comparisons and evaluations. This includes a detailed analysis of the strengths and weaknesses of each approach, focusing on the strengths and weaknesses of each approach in terms of performance, resource allocation, and cryptographic efficiency. Specifically, the execution time of any cryptographic algorithm is an important indicator to measure the performance of its encryption and decryption technology, which directly defines the speed at which the algorithm runs. In this paper, an improved scheme of RSA cryptographic algorithm based on SMM is proposed, and the execution time analysis of classical RSA and SMM-RSA is shown in Tables 1 and 2, respectively. The analysis results show that although the improved RSA encryption and decryption algorithm surpasses the classical RSA in terms of computational complexity, which means that the algorithm structure is more complex, it also increases the difficulty of attackers to crack it, requiring them to invest more time. This finding provides a strong basis for us to optimize the encryption performance of network nodes.

In order to analyze the encryption accuracy of the proposed algorithm even further, Figure 4 shows the comparison of the memory consumption of

Table 1 RSA execution time analysis

Algorithm	Message Size (MB)	Encryption Time	Decryption Time
RSA	15	3.01	4.51
RSA	25	3.11	8.96
RSA	35	3.32	10.65
RSA	45	3.39	11.99
RSA	55	3.46	12.99
RSA	65	3.47	13.43
RSA	75	3.51	14.98

Table 2 SMM-RSA execution time analysis

Algorithm	Message Size (MB)	Encryption Time	Decryption Time
SMM-RSA	15	4.25	40.60
SMM-RSA	25	3.33	43.00
SMM-RSA	35	2.75	26.58
SMM-RSA	45	3.86	20.05
SMM-RSA	55	3.60	18.00
SMM-RSA	65	3.70	30.03
SMM-RSA	75	3.49	17.01

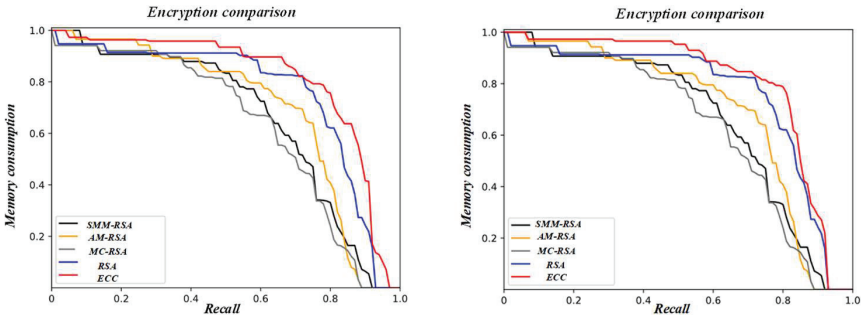

Figure 4 Encrypted memory consumption comparison.

different encryption schemes, which is crucial for encryption schemes. In this paper, the memory consumption of different algorithms is compared. It can be seen that the proposed SMM-RSA encryption algorithm achieves better results using less memory consumption.

In order to further improve the convincing power of the experimental results, we set the personal communication information security protection method based on RSA algorithm as the experimental group, and compared it with the related algorithms. As shown in Figure 5, the graph shows the

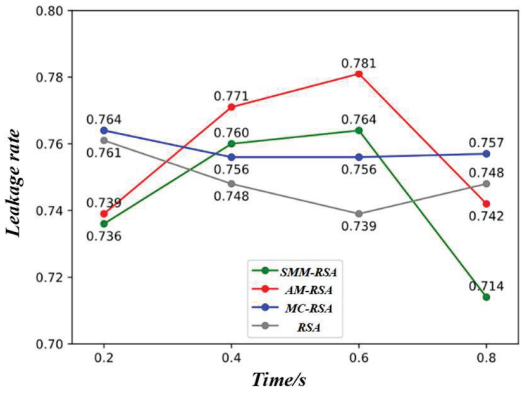

Figure 5 Encryption leakage rate comparison.

comparison of encryption leakage rates, and tests the comparison effect of the three encryption methods with the methods proposed in this paper. In this experiment, the information leakage rate was used as an evaluation indicator. As can be seen from Figure 5, the proposed encryption algorithm achieves the best results in different time periods. With the increase of protection time, the fluctuation of leakage rate index is more obvious, which indicates that the proposed RSA algorithm has a high degree of feasibility and application advantages in security protection. In the case of changing protection time, its information security protection effect is better, and it can accurately respond to the dynamic changes of personal information and effectively avoid potential security risks. In addition, we have significantly enhanced the data interpretation in the results analysis section, which not only presents the indicators of encryption performance and resource allocation efficiency, but also deeply analyzes the reasons for data changes under different experimental conditions, including the impact of factors such as the size of the encrypted data, the computing power of nodes, and the network topology on encryption performance and resource allocation. At the same time, we also performed a detailed analysis of the specific experimental conditions under which the data were collected, discussed how these conditions might affect the experimental results, and reviewed potential biases or limitations in the experimental setup. Finally, we explore the potential impact of the research results on real-world network applications, and analyze the feasibility of the proposed performance optimization and resource allocation strategy in real-world networks, as well as the potential benefits it may bring to improve security, reduce latency, and increase network throughput.

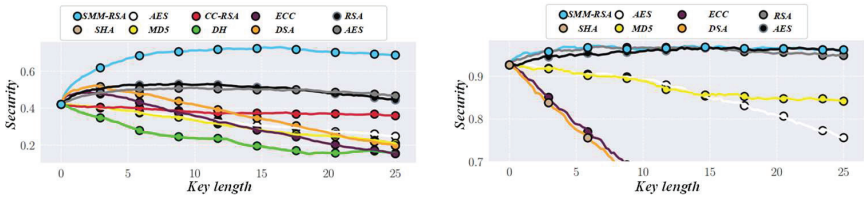

Figure 6 Comparison of encryption security.

In addition to general data messages, other messages contain encrypted digital signatures, only the presumed receiver can decrypt, effectively preventing others from illegal eavesdropping; Figure 6 for the encryption security comparison chart. The receiver to determine the source of the message by verifying the signature, which can prevent others from illegal tampering, or forging the message. For general data messages, encryption, signature, or both, with a certain degree of flexibility. In this way, effectively ensures the security of the communication process, of course, communication security is based on the user keeping their private key, as well as SMM-RSA has the basis of reliability (not controlled by the illegal).

In the process of network security node optimization, we implement basic encryption functions including shell binding, batch encryption, extended encryption, and basic encryption, and also significantly increase the type and scale of comparison experiments. In addition to comparing our optimization strategy with the original RSA algorithm, we now make in-depth comparisons with other classical optimization schemes, based on advanced mathematical techniques, machine learning methods, and heuristic methods. To ensure the comprehensiveness of the experiment, we tested the optimization strategy in a variety of network environments, including wired and wireless networks, and across different data scales, to evaluate its performance under various conditions and scenarios. At the same time, we analyze the performance indicators such as encryption speed, decryption speed, resource utilization and fault tolerance in detail, and provide a comprehensive evaluation of the effectiveness of the optimization strategy in improving the encryption performance of network nodes. In addition, we pay special attention to the adaptability of encryption operations, timely feedback of encryption errors, the influency of encryption systems on incorrectly encrypted content, and the security of network file encryption to ensure that encryption and transmission processes are not intercepted or read, and the integrity of encrypted information can be guaranteed. Figure 7 shows a comparison of encryption accuracy to further ensure the reliability of encryption.

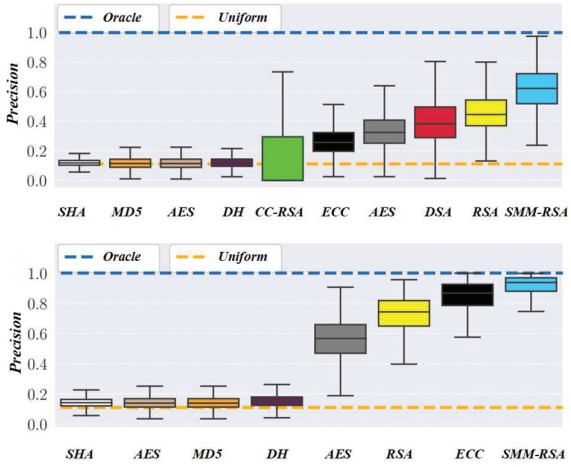

Figure 7 Encryption accuracy comparison.

In the field of personal network information security, in the face of network congestion and data transmission problems caused by excessive network traffic, we propose an improved RSA algorithm. In order to verify the effectiveness of the proposed algorithm, we show the comparative experimental results of network traffic, security and decryption speed in Figure 8, analyze the specific reasons for the data changes under the changes of network load and resource availability, and comprehensively discuss the potential influence of experimental conditions on the results. In this process, we carefully identified potential sources of error, such as equipment performance fluctuations, environmental interference, etc., and took targeted measures such as enhancing the stability of experimental equipment and optimizing the control of the experimental environment to minimize the interference of errors on experimental results and enhance the reliability and practicability of the conclusions.

Key length is a key factor when discussing the security of network information encryption. In this paper, the improved SMM-RSA algorithm is adopted, and the encryption and decryption operations are carried out respectively, and the encryption and decryption times of the designed method are tested. As shown in Figure 9, the graph shows a comparison of encryption performance, from which it can be seen that the proposed algorithm shows excellent security performance as the network size continues to expand. This not only directly verifies the effectiveness of the algorithm, but also indirectly proves its security and stability. In addition, we have significantly enhanced

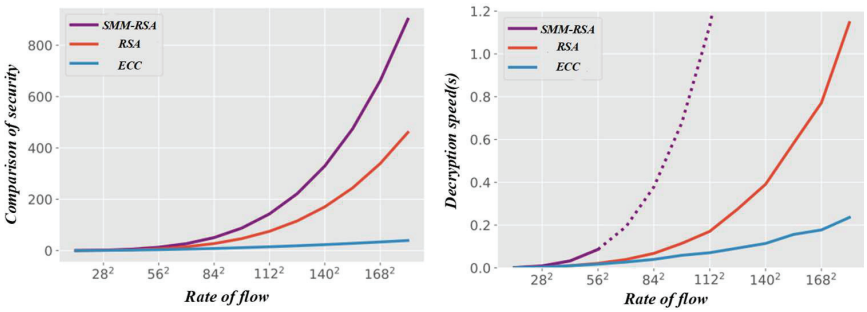

Figure 8 Comparison chart of security and decryption speed.

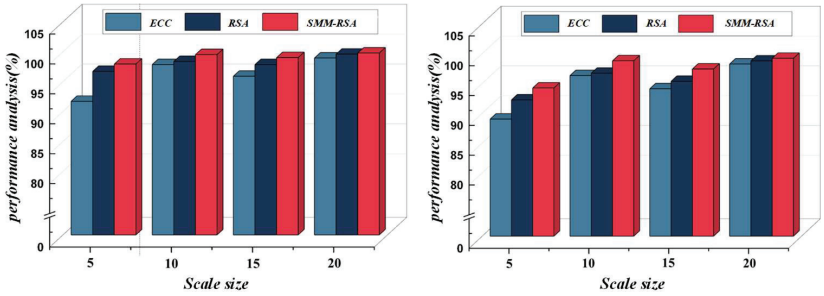

Figure 9 Comparison of encryption performance.

the data interpretation in the analysis section of the results, not only presenting the indicators of encryption performance, but also deeply analyzing the reasons for data changes under different experimental conditions, such as the size of the encrypted data, the computing power of nodes, and the network topology of other factors on encryption performance. At the same time, we also performed a detailed analysis of the specific experimental conditions under which the data were collected, discussed how these conditions might affect the experimental results, and reviewed potential biases or limitations in the experimental setup. Finally, we discuss the potential impact of the research results on real-world network applications, and analyze the feasibility of the proposed performance optimization strategy in real-world networks, as well as the potential benefits it may bring, such as improved security, reduced latency, and increased network throughput.

Comparing the SMM-RSA algorithm proposed in this paper with the ordinary RSA algorithm, we can see that, no matter when the higher encryption accuracy rate means that the utilization value of the algorithm is also higher. Figure 10 shows the relationship between the encryption period and

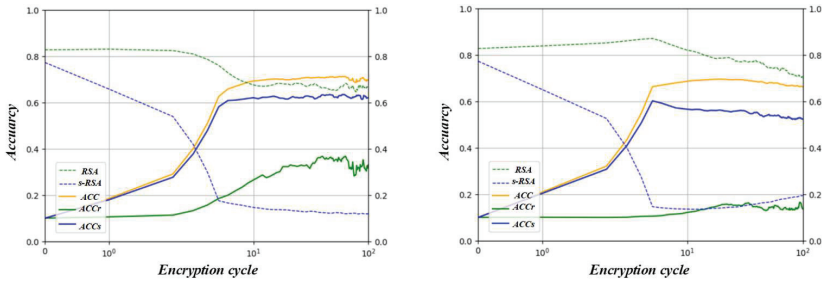

Figure 10 Plot of encryption period versus accuracy rate.

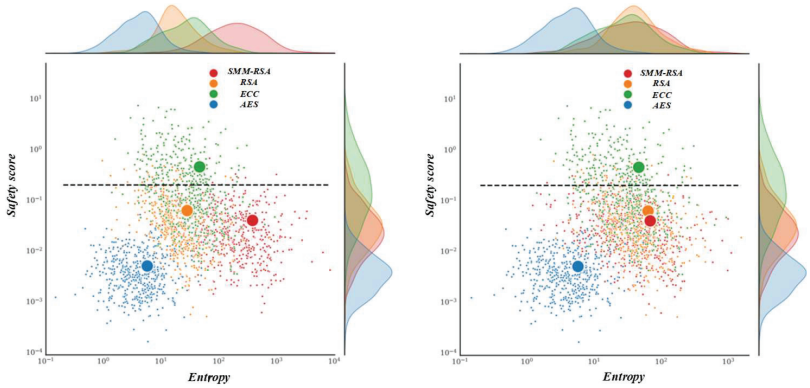

Figure 11 Efficiency scatter plot.

the accuracy rate, in the early stage of the system operation, both algorithms are in a slow state, but with time, the operation period of the cycle of the increase, SMM-RSA is the existence of the undoubted advantage, while the RSA technology, although in the early stage of the time for some time appeared in the acceleration of the speed of the tendency, but later became very slow.

Randomly select a communication node, and record the form of packets at the sending end and the form of packets at the transmission node during the communication process, which will be used as one of the key indexes to test the effect of data encryption of this paper's method. Figure 11 shows the efficiency scatter plot, after using the method designed in this paper for data encryption processing, it can make the data transmission in the wireless heterogeneous communication network present a disordered state, to avoid the risk of ordering data transmission in the network tampered with, stolen and so on.

6 Conclusion

In this study, we deeply explore the optimization of network node encryption performance and resource allocation strategy based on RSA algorithm, aiming to improve data security and transmission efficiency in network communication. After theoretical analysis, algorithm improvement and experimental verification, the optimization strategy shows significant core advantages in encryption performance and resource allocation:

(1) The algorithm proposed in this study dynamically adjusts the length of RSA keys based on the sensitivity level of transmitted data and real-time network conditions. The optimization measures have significantly improved encryption's security, accuracy, and efficiency, increasing by 4.2%, 3.8%, and 5.1%, respectively. In terms of encryption security, the optimized RSA algorithm effectively resists various network attacks by enhancing the security of key management and encryption processes.

(2) By analyzing the computing power, bandwidth resources, urgency of encryption tasks, and security requirements of network nodes, intelligent algorithms are used to schedule and optimize resource configuration dynamically. The algorithm achieves precise data encryption while maintaining high security, reducing data loss during the encryption process and ensuring the integrity and accuracy of information. Analyzing the relationship between network traffic and security, it was found that by optimizing algorithms, the network's security was successfully improved while reducing network traffic, achieving a dual improvement in network security and efficiency.

(3) On the basis of the RSA algorithm, we optimize the personal information security network nodes, significantly shorten the decryption time, and improve the efficiency by about 30%, which is verified by the efficiency scatter plot. We provide an in-depth analysis of innovations, point out the practical impact of unique optimization techniques and resource allocation strategies, and extend our research to the context of cybersecurity, highlighting their unique contributions in this area.

In order to further promote the development of this field, we believe that the integration with emerging technologies such as quantum computing and blockchain will become an important research direction. These cutting-edge technologies are expected to provide new ideas and methods for the optimization of RSA algorithms, so as to play a more critical role in future network security protection and point out a more forward-looking path for follow-up research.

References

[1] Adeniyi, A. E., R. G. Jimoh and J. B. Awotunde, "A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security," Computers and Electrical Engineering, vol. 118, pp. 109330, 2024.

[2] Mojisola, F. O., S. Misra, C. Falayi Febisola, O. Abayomi-Alli and G. Sengul, "An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA)," Egyptian Informatics Journal, vol. 23, no. 2, pp. 291–301, 2022.

[3] Susilo, W., J. Tonien and G. Yang, "Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA," Computer Standards & Interfaces, vol. 74, pp. 103470, 2021.

[4] Alhassan, A. M., "Secure multi-cloud resource allocation with SDN and self-adaptive authentication," Ain Shams Engineering Journal, vol. 15, no. 6, pp. 102742, 2024.

[5] Bai, W., H. Yang, A. Yu, H. Xiao, L. He, L. Feng and J. Zhang, "Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks," Optical Fiber Technology, vol. 40, pp. 18–27, 2018.

[6] Biswas, K., V. Muthukkumarasamy, M. J. M. Chowdhury, X.-W. Wu and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks," Computer Networks, vol. 232, pp. 109842, 2023.

[7] Che, M., H. Chen, Y. Ueda and K. Kato, "Secured THz communication in photonic microcell networks based on spatial wave mixing of steered beams," Optical Switching and Networking, vol. 54, pp. 100773, 2024.

[8] Chithaluru, P., A. Singh, J. S. Dhatterwal, A. H. Sodhro, M. A. Albahar, A. Jurcut and A. Alkhayyat, "An Optimized Privacy Information Exchange Schema for Explainable AI Empowered WiMAX-based IoT networks," Future Generation Computer Systems, vol. 148, pp. 225–239, 2023.

[9] Gurusamy, S. and R. Selvaraj, "Resource allocation with efficient task scheduling in cloud computing using hierarchical auto-associative polynomial convolutional neural network," Expert Systems with Applications, vol. 249, pp. 123554, 2024.

[10] Mahboubi, A., S. Camtepe, K. Ansari, M. Pawłowski, P. Morawiecki, H. Aboutorab, J. Pieprzyk and J. Duda, "Shared file protection against

unauthorised encryption using a Buffer-Based Signature Verification Method," Journal of Information Security and Applications, vol. 86, pp. 103873, 2024.

[11] Marwan, M., A. Ait Temghart, S. Ouhmi and M. Lazaar, "Security, QoS and energy aware optimization of cloud-edge data centers using game theory and homomorphic encryption: Modeling and formal verification," Results in Engineering, vol., pp. 102902, 2024.

[12] Marwan, M., F. AlShahwan, Y. Afoudi, A. Ait Temghart and M. Lazaar, "Leveraging artificial intelligence and mutual authentication to optimize content caching in edge data centers," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 9, pp. 101742, 2023.

[13] Mershad, K. and O. Cheikhrouhou, "Lightweight blockchain solutions: Taxonomy, research progress, and comprehensive review," Internet of Things, vol. 24, pp. 100984, 2023.

[14] Mohamed, S. A. A. and S. Kurnaz, "Classified VPN Network Traffic Flow Using Time Related to Artificial Neural Network," Computers, Materials and Continua, vol. 80, no. 1, pp. 819–841, 2024.

[15] Nawaz, M. W., W. Zhang, D. Flynn, L. Zhang, R. Swash, Q. H. Abbasi, M. A. Imran and O. Popoola, "6G edge-networks and multi-UAV knowledge fusion for urban autonomous vehicles," Physical Communication, vol. 67, pp. 102479, 2024.

[16] Rehman, A., T. Saba, K. Haseeb, T. Alam and G. Jeon, "IoT-Edge technology based cloud optimization using artificial neural networks," Microprocessors and Microsystems, vol. 106, pp. 105049, 2024.

[17] Sham, E. E. and D. P. Vidyarthi, "CoFA for QoS based secure communication using adaptive chaos dynamical system in fog-integrated cloud," Digital Signal Processing, vol. 126, pp. 103523, 2022.

[18] Shivaramakrishna, D. and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," Alexandria Engineering Journal, vol. 84, pp. 275–284, 2023.

[19] Si, H., W. Li, N. Su, T. Li, Y. Li, C. Zhang, B. Fernando and C. Sun, "A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem," Computer Communications, vol. 223, pp. 68–80, 2024.

[20] Srinidhi, N. N., S. M. Dilip Kumar and K. R. Venugopal, "Network optimizations in the Internet of Things: A review," Engineering Science and Technology, an International Journal, vol. 22, no. 1, pp. 1–21, 2019.

[21] Liu, Y., X. Shen, J. Liu and K. Peng, "Optical asymmetric JTC cryptosystem based on multiplication-division operation and RSA algorithm," Optics & Laser Technology, vol. 160, pp. 109042, 2023.
[22] Talha, A., A. Bouayad and M. O. C. Malki, "An improved pathfinder algorithm using opposition-based learning for tasks scheduling in cloud environment," Journal of Computational Science, vol. 64, pp. 101873, 2022.
[23] Josien, M. and R. Prat, "Parallel and bias-free RSA algorithm for maximal Poisson-sphere sampling," Computer Physics Communications, vol. 305, pp. 109354, 2024.
[24] Thabit, F., O. Can, S. Alhomdy, G. H. Al-Gaphari and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing," International Journal of Intelligent Networks, vol. 3, pp. 16–30, 2022.
[25] Wang, Y., Z. Wang and X. Liu, "Key security measurement method of authentication based on mobile edge computing in urban rail transit communication network," Computer Communications, vol. 215, pp. 140–149, 2024.
[26] Zhang, L., Y. Zou, W. Wang, Z. Jin, Y. Su and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," Computers & Security, vol. 105, pp. 102249, 2021.
[27] Zhang, X., Y. Wang, T. Ma, L. Guo and Z. Hu, "A Lightweight_PAEKS-based energy scheduling model considering priority in MicroGrid," Ad Hoc Networks, vol. 162, pp. 103531, 2024.
[28] Zhou, C. and Z. Jiang, "Computer Network Communication Security Encryption System Based on Ant Colony Optimization Algorithm," Procedia Computer Science, vol. 228, pp. 38–46, 2023.
[29] Anitha, S., S. Saravanan and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission," Measurement: Sensors, vol. 29, pp. 100889, 2023.
[30] Gong, L., K. Qiu, C. Deng and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," Optics and Lasers in Engineering, vol. 121, pp. 169–180, 2019.

Biography

Li Qiang graduated from Harbin University of Science and Technology in 2003 with a Bachelor of Science degree. In 2008, he obtained a Master's degree in Software Engineering from the University of Electronic Science and Technology of China. He used to work for an Associate Professor at Zibo Vocational Institute School of Artificial Intelligence and Big Data Institute in 2015, and he is currently employed at School of Management, Zibo Vocational Institute. His research areas and directions include computer networks, artificial intelligence, big data, and network security.