Journal of Electronics and Information Science (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2024.090216
ISSN 2371-9524 Vol. 9 Num. 2

# *Exploration of the Encrypted Transmission Technology of Network Communication Information Based on AES Algorithm*

**Ying Ding***

*IT Solution Consulting, MOYI Inc, New York, USA*
**Corresponding author*

***Keywords:*** AES Algorithm, Network Security, Data Transmission, Secure Communication, Encryption Technology, Information Privacy

***Abstract:*** With the rapid progress and wide application of Internet technology, the security problem of network communication has become increasingly prominent; this has become a major bottleneck restricting the development of information society. Therefore, this research aims to develop an innovative encryption transmission technology based on AES algorithm to meet the security requirements of network communication. By using AES algorithm as the core encryption mechanism, we build a new network communication information encryption transmission model, and adopt the strategy of information isolation to enhance the security of data. At the same time, we design an efficient encryption transmission platform to improve the encryption efficiency and effectively resist potential information theft. The experimental results show that our technology significantly reduces the risk of information theft and provides a reliable and innovative solution for network communication security problems. This research has important theoretical and practical significance in the field of network communication security, and provides a strong support for the future development of network security technology.

## 1. Introduction

Nowadays, with the popularity and convenience of network communication, ensuring the security of communication has become a vital task, especially to avoid the disclosure of user information. However, there are many challenges in the traditional network communication information encryption transmission technology, such as imperfect encryption transmission model, poor encryption effect, high total amount of information stolen and so on. It is particularly important to design a new network information encryption transmission technology to improve the security of network communication and protect user privacy. In the complex communication network transmission environment, because of the large number of information sources, accurate encryption becomes very difficult. The traditional network communication information encryption technology often uses CAN for encryption, but there is encryption delay when dealing with a large number of communication information, which increases the risk of information theft. In contrast, the AES algorithm has efficient encryption efficiency, can dynamically adjust the data length, and

make dynamic transmission keys according to the communication status, thus enhancing the encryption strength and efficiency. This paper is devoted to designing an innovative network communication information encryption transmission technology based on AES algorithm, which provides important support and guarantee for the future network communication message security maintenance. The application of this technology will help to improve the security level of network communication, reduce the risk of information theft, and ensure the secure transmission and privacy protection of user data.

## 2. Related Research

In recent years, with the rapid development of network communication and the increasingly prominent problem of information security, many related neighborhoods have done a lot of in-depth research on network communication information encryption transmission technology based on AES algorithm. In terms of information security management, S Nair,A Jerichow,N S Bykampadi studies the communication system (600) including a first network (610) and a second network (630). Messages constructed through the first network (617) contain indicators to perform security operations before being sent to the second network [1]. AES algorithm, D Kashmar proposed an efficient image encryption scheme based on functional AES algorithm [2]. K Kageyama,S Arai,H Hamano,X Kong,T Kumaki,T Koide proposed the CAMX accelerator, which is suitable for mobile CPU. It uses the large-scale parallel single instruction multiple data (SIMD) matrix core of content addressable memory to significantly improve the processing speed of AES encryption operations. CAMX has two CAM modules, high parallel processing ability, and can quickly perform table lookup and coding operations. The research results show that the performance of CAMX is about 2.1 times higher than that of related work and existing mobile processors. [3] in an article in 2015, Zhang,X,Parhi,K.K briefly discussed how to improve speed and reduce complexity by using composite domain algorithms in AES hardware implementation, providing 16 constructs for composite domain GF. It also introduces an algorithm to effectively find the isomorphic mapping between GF (2) and the composite domain, so as to optimize the minimum number of gates and critical paths of AES implementation. [4] Yan J J also proposed a new AES algorithm based on chaos, which uses synchronous dynamic keys generated by sliding mode control. Different from the traditional AES system, this method eliminates the need for static key exchange and enhances encryption security by dynamically generating secret keys. The effectiveness of the algorithm is verified by statistical analysis and simulation experiments. [5] M Mushtaq, An Akram,MK Bhatti,NBR Rao,G Gogniat also introduced a run-time detection mechanism for access-driven cache-based side channel attacks (CSCA) on Intel's ×86 architecture. The experimental results show that under the Prime+Probe attack, the detection accuracy of the mechanism for AES is more than 99%, and the performance overhead is 3-4%. [6] to sum up, in recent years, the research on the encrypted transmission technology of network communication information based on AES algorithm has shown a rich and diverse trend, and the cooperation and communication between academia and industry continue to promote the development of this field. In the future, we can further learn from previous research results, combined with the latest technological progress, and jointly explore a more efficient and secure network communication information encryption transmission technology.

## 3. Design of Encryption Method for Transmission Information of Network Communication

### 3.1 Isolate Network Communication Information

With the rapid development of network technology, the problem of network security becomes more and more serious, and all kinds of threats become more and more diversified and complicated,

which puts forward higher requirements for the protection of network communication information. Under this background, this paper proposes an innovative network communication information encryption transmission technology based on AES algorithm, which aims to deal with the increasing network security challenges and ensure the secure transmission of communication information. In order to deal with the increasing network threats, we combine NDIS technology, select appropriate network communication information encryption components, and adopt advanced encryption technology and defense mechanism to ensure the secure transmission of network communication information. This technical scheme can not only effectively filter and isolate potential network threats, but also ensure the confidentiality and integrity of communication information, and improve the security and reliability of network communication. After reviewing several filter drivers, we found that Packet Filtering and Packet Encryption/Decryption may cause security problems in the transmission of network communication information. Under the driving principle of mid-level drivers, the entry points of information encryption components have been selected to meet the requirements of information encryption transmission. Specifically, after the encrypted signal of the transmission component is sent by NDIS, it is transmitted to the driver through the lower layer microport, and then the driver process is completed by the upper layer driver. Then, the encryption transmission center sends the completed data packet to the communication information transmission interface, and uses the NdisMXxxIndicateReceive function to process the data packet to complete the data packet encryption. The whole process is based on the selected transport component driver structure. First of all, the intermediate driver binds with the bottom layer to obtain the Miniport Query Information driver request, and the query processing is carried out by the relevant processing function to complete the connection of the driver component. In this process, the intermediate driver successfully sends the driver data packet and obtains the NdisMInitializeTimer synchronous clock, and successfully obtains the characteristics of the network communication information encryption component. Based on these characteristics, we build a network communication information encryption transmission component architecture, including key manager, packet processor and so on. At the same time, we use packet encryption algorithm to build a key information base for the receiving terminal to check. [7] in view of the challenge of network communication security, we propose an innovative solution: network communication message encryption transmission technology based on AES algorithm. This technology can not only quickly intercept the potentially threatening network communication information, but also effectively resist a variety of network communication attacks.

### 3.2 Design an Encrypted Transmission Platform Based on AES

Under the background of increasingly serious network security problems, in order to deal with the emerging network threats and attacks, we urgently need a more efficient and reliable network communication information encryption transmission technology. Therefore, we build a new encrypted transmission platform to improve the efficiency and security of encrypted transmission of network communication information. The encryption transmission platform adopts a variety of advanced encryption algorithms, such as AES, ECC and RSA[8], and combines them to meet the encryption needs of different types of data and transmission scenarios. Specifically, AES algorithm is used in encrypted transmission of large amounts of data to ensure efficient encryption and transmission speed of data. ECC algorithm is suitable for efficient encryption requirements in resource-constrained environments, especially in mobile devices and other scenarios. The RSA algorithm is used for key exchange and digital signature to ensure the integrity of communication data and the reliability of authentication. This encryption transmission platform realizes the targeted encryption scheme by intelligently classifying and encrypting different types of data, thus

improving the security and transmission efficiency of network communication information to the maximum extent. At the same time, through the ingenious combination of a variety of encryption algorithms, we not only protect the encryption strength, but also reduce the performance overhead as much as possible, and further improve the efficiency and reliability of encrypted transmission. The design of this encrypted transmission platform is not only to protect the security of network communication, but also to deal with the evolving network threats and attacks, and provides omni-directional guarantee and support for the security and reliability of network communication.

## 4. Experimental Comparison

In the experiment, we compare the performance and evaluate the security of the two encryption technologies by simulating the real network environment, as follows:

### 4.1 Experimental Preparation

Our research chose Pentium Dual as the experimental platform, which is a highly sensitive platform with dual-core CPU built in to strengthen the connection between RAM PC computers. In order to truly simulate the network communication environment, we use Visual++ to develop the platform, and connect the server and the test interface through various tools to ensure the smooth progress of the follow-up experiment. Before the start of the experiment, we carefully checked each experimental module to make sure that they were in good condition. Once an abnormal situation occurs, we will take immediate measures to deal with it. After the completion of the inspection, according to the experimental requirements, we connect each empirical link to ensure that it meets the experimental standards, and a specific encryption sequence is designed. In order to improve the efficiency of the experiment and avoid the problem of data homomorphism, we add the hardware of DualCore to the experimental platform and debug it in real time by using UC NS2 software. In the course of the experiment, we find that the influence of communication[9] information transmission signal will lead to the generation of specific parameters, and then affect the transmission of experimental information. Therefore, we classify all the network communication information selected in the experiment, divide the text size into different types, and assign them different bits of keys according to the requirements of the experiment. These preparations have laid a solid foundation for the smooth progress of the experiment, so that we can comprehensively evaluate the encryption effect of the designed network communication information AES encryption transmission technology. We assign different keys to different sizes of information to ensure the accuracy and reliability of the experiment. Based on the above experimental information, we verify the transmission of communication information. The specific method is to send the preset network communication information to the experimental platform through Internet, and then use Socket technology to accurately identify and decrypt the transmission signal. After testing, we confirm that the keys set are in line with the experimental requirements, and can carry out the subsequent network communication information encryption transmission experiment smoothly.

### 4.2 Experimental Results and Discussion

We are preparing to step into the experimental field of network communication information encryption, which is a natural extension of our experimental preparation work. In this experiment, we will deeply explore two different encryption transmission technologies: one is the network communication information encryption transmission technology based on AES algorithm, and the other is the traditional network communication information encryption transmission technology. Our goal is to record the amount of information stolen from the network communication of the two

technologies in different quantities of network communication information. By recording and comparing the data, we will evaluate the performance of the two encryption technologies in different situations and their impact on the security of network communication information. The results show that the network communication information encryption transmission technology based on AES algorithm shows significant advantages in encryption effect and security. Compared with traditional technology, it can protect the privacy and integrity of communication data more effectively and reduce the risk of being stolen and tampered with. This discovery shows that the network communication information encryption transmission technology based on AES algorithm has better encryption effect, higher reliability, and has considerable application potential. These results will provide us with in-depth understanding and provide strong support for improving and strengthening the security of network communications.

## 5. Conclusion

In the process of solving the challenge of data interception in network communication, the adoption of AES algorithm provides a reliable solution. By isolating information, building specialized encryption models, and designing efficient encryption platforms, we not only enhance the security of our data, but also improve our defense against unauthorized access. This method not only improves the effectiveness of encryption, but also accords with the developing security requirements of modern network environment. Our experimental results show that the network communication information encryption transmission technology based on AES shows a better encryption effect, showing reliability and potential application prospects. This technology provides a strong support for ensuring the security of network communication, and provides an important reference for the secure transmission of network communication in the future.

## References


*[1] Nair S, Jerichow A, S Bykampadi N. Security Management In Communication Systems With Network Function Assisted Mechanism To Secure Information Elements: EP20190157496[P]. EP3528456B1[2024-04-13].*

*[2] Kashmar D. Efficient Image Encryption Schemes Based On Developing Aes Algorithm With Fuzzy Function[J]. IEEE, 2021. DOI:10.47832/Minar.*

*[3] Kageyama K, Arai S, Hamano H, et al. Parallel Software Encryption of AES Algorithm by Using CAM-Based Massive-Parallel SIMD Matrix Core for Mobile Accelerator [J]. Journal of Advances in Information Technology, 2023.*

*[4] Zhang X, Parhi K K. High-speed VLSI architectures for the AES algorithm [J]. IEEE Transactions on Very Large Scale Integration Systems, 2004, 12(9): 957-967. DOI:10.1109/TVLSI.2004.832943.*

*[5] Yan J J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm [J]. Applied Sciences, 2021, 11. DOI:10.3390/app11031329.*

*[6] Mushtaq M, Akram A, Bhatti M K, et al. Run-time Detection of Prime + Probe Side-Channel Attack on AES Encryption Algorithm[C]. 2018 Global Information Infrastructure and Networking Symposium, 2018. DOI:10.1109/GIIS. 2018.8635767.*

*[7] Mehta B B. Big Data Privacy[J]. IEEE, 2017. DOI:10.14293/S2199-1006.1.SOR-COMPSCI.CLULSWF.v1.*

*[8] Pfister N A, Vemuri S, Lutz D R. Processing of iterative operation:US201916368930[P]. US10970070B2[2024-04-14].*

*[9] Savari M, Montazerolzohour M, Thiam Y E. Comparison of ECC and RSA algorithm in multipurpose smart card application [J]. IEEE, 2012. DOI:10.1109/CyberSec.2012.6246121.*