The Secure Data Transmission Method of a Cellular Communication Network Based on the Asymmetric Encryption Algorithm

Qingjia Luo[1] and Zongfu Zhang[2,*]
[1] Faculty of Data Science, City University of Macau, Xu Risheng Yin Gong Road, Taizi, Macao, China; Email: D22092100153@cityu.mo
[2] School of Information Engineering, Jiangmen Polytechnic, No. 6, ChaoLian Avenue, Jiangmen, Guangdong, China; Email: jmptzhang@126.com
*Correspondence: jmptzhang@126.com

***Abstract*—In order to improve the cellular network communication security and achieve a high quality data transmission, this paper proposes a method of secure data transmission. The proposed method is based on asymmetric encryption algorithm. This paper analyzes the composition structure of cellular network to establish the network architecture model and master the communication characteristics. The public key system is constructed using the certification center, service provider and users, and the asymmetric encryption process. The public key system is analyzed to obtain the encrypted cipher-text by optimizing the integer grouping method. Overall, results show that the proposed research achieves a higher throughput, and reduces bit error rate compared to the state-of-the-art methods. Results and findings suggest that the proposed transmission method can improve reduce the probability of data theft, and reduces transmission energy consumption to ensure data transmission security from multiple aspects.**

***Keywords*—Asymmetric encryption algorithm, Cellular communication network, Secure data transmission, Public key system, Transmission speed**

I. INTRODUCTION

The development of computer technology has led to great changes in the way information is transmitted and processed, and has also promoted the emergence of diversified communication networks. Cellular networks with their super flexibility and coverage are widely used in the field of data transmission. The form of cellular networking, the terminal, and network equipment using wireless channel connection are aimed to achieve mutual communication between users. However, communication networks generally have the characteristics of openness and anonymity, and the security risks are large, which cannot guarantee the confidentiality and success rate of data transmission. Therefore, in the process of data transmission, the following requirements must be met: to ensure that the transmitted data can only be accessed by authorized users, unauthorized users cannot access the network. It also ensures that the transmitted data can be correctly identified. It should also identify whether there are traces of forgery. The most important point is the integrity of the data, which guarantees data loss and other phenomena cannot occur.

To meet the above data transmission needs, many scholars proposed the following solutions. Zhang Xiaoyu *et al*. [1] used time-division data modulation algorithms to achieve safe data transmission. The parity modulation strategy was used to complete the Fourier transform modulation of the transmitted signal, which reduced the influence of channel noise on data transmission, and then encrypted the transmission content by using the dynamic encryption method of rotation factor to achieve the purpose of safe transmission. Sun Jiafeng *et al.* [2] proposed a data transmission method based on energy optimality. By analyzing the principle of frequency domain equalization, and copying the optimal frame of the transmitted data into the frame head, the proposed approach was used as a cyclic prefix, and obtain the minimum mean squared error in the transmission signal. The use of a single-carrier frequency domain equalization system was aimed to sweep away the serial code interference and realize the communication compensation based on energy optimization, which is more conducive to the safe transmission of data.

With the intensification of illegal theft activities in network communications, the above methods have become difficult to meet the needs of secure transmission. To this end, this paper implements the secure transmission of data over cellular communication networks based on asymmetric encryption algorithms. The proposed method consists of two parts, the public key and the private key [3], and is generated in pairs and cannot be used alone. If the information is encrypted with a public key, it must be decrypted by the corresponding private key. In addition, the algorithm key dcistribution method is relatively simple, if two users communicate, the two sides exchange public keys, if one of them encrypts the other's public key, and the other party only needs to use its private key to decrypt [4]. Based on the earlier mentioned background on the

Manuscript received July 20, 2022; revised August 5, 2022; accepted January 10, 2023.

research topic and purpose of this research, the contribution of this paper is as follows:

a) This paper proposes to construct the asymmetric encryption system to avoid data leakage during data transmission.
b) This paper proposes to establish a comprehensive cellular network model to secure data transmission by considering the different factors.
c) This paper proposes to ensure the secure communication under multiple guarantees.

The remainder of this paper is as follows:

Section II is focuses on establishing the cellular communication network model in this paper. Section III presents the asymmetric encryption using the secure communication method; Section IV shows us simulation-based experiments, results, and their discussion; and Section V concludes the research performed in this paper.

II. Cellular Communication Network Model Establishment

Cellular networks are based on high-capacity voice and high speed data communication networks. Cellular networks aim at enhancing seamless and multimedia roaming capabilities and support several types of cellular devices. They have become the source of communication for life-mission-critical services, life savings, and sensitive business transactions [5].

A recent work [6] highlighted two serious challenges of services providers (SPs) regarding cellular networks. The first challenge is to determine the type of data to be cached on SPs. The second challenge is to ensure the quality of experience to cellular users. The intrinsic user mobility has adverse effects on network topology as changes overtime that brings difficulties in transmitting online information such as videos.

Suppose there is a K layer of a cellular network, each representing a base station class, and different base stations have different transmission power and distribution density [7]. If the i spatial distribution density of the base station in the first layer is, the ρ number of base stations is, n_i for all base stations in i layer, the overall transmission power is described p_i as, the number of antennas is described as, the threshold value for setting the safe transmission speed is, and N_i the number γ_i of eavesdroppers is n_e. The channel environment can be described by Eq. (1):

$$Q = \left(\frac{n_i \times N_i}{K} \times \gamma_i \right) \rho \tag{1}$$

In the communication environment described above, assuming that all users select the strongest base station as the service object, the ideal road status can be obtained after measurement [8]. In the above case, this paper constructs a cellular network model as shown in Fig. 1.

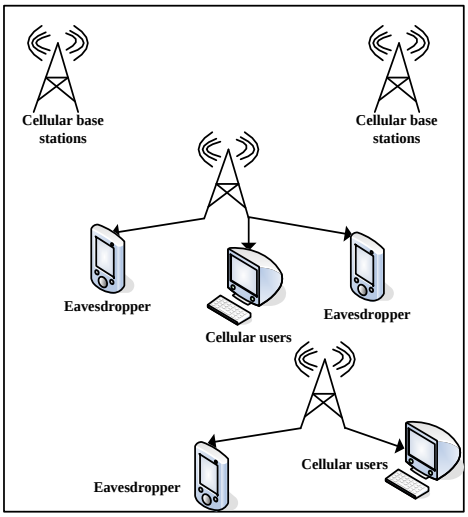

Figure 1. Cellular network structural model diagram

A cellular network model was analyzed to understand how users communicated under the network. When setting the data transmission method, the communication needs should be met to the greatest extent according to the characteristics of the communication mode.

III. Secure Data Transmission Method Based on Asymmetric Encryption

This section presents the construction of a public key that is worldwide available. Secure data transmission is ensured by using the asymmetric encryption that makes less consumption of energy and improves the transmission rate. Overall, the workflow diagram of the proposed research is given in Fig. 2.

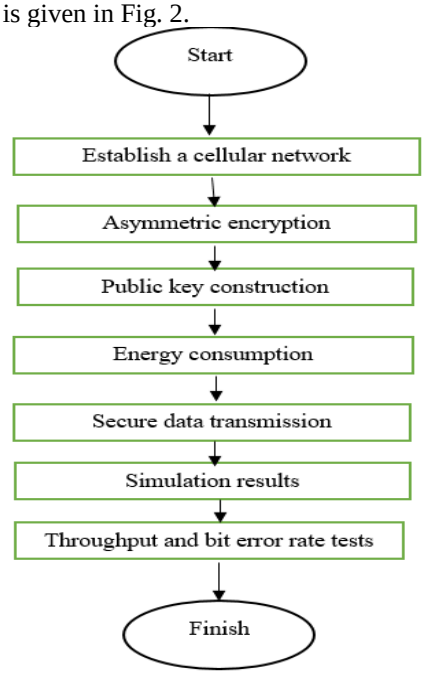

Figure 2. Workflow diagram of the proposed research

The flow chart of the proposed research is shown in Fig. 2. The research proposed in this paper begins by establishing a cellular network, and finishes after covering

several steps such as asymmetric encryption, public key construction, energy consumption, etc. All steps after establishing a cellular network have been explained in the subsequent part of this paper.

A. Construction of a Public Key System

PKI (Public Key Installation) system is a network basic service device that combines cryptographic principles to provide a secure environment for key construction. PKI is typically applied in public key management and signing services, as shown in Fig. 3.

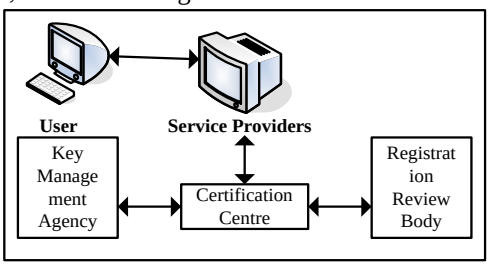

Figure 3. Schematic diagram of the PKI public key system

(1) Certificate authority (CA) [9]: This is the main module of PKI. The basic task of CA is to distribute and manage certificates, which can verify the legitimacy of users. The confidentiality of key management is extremely high. Therefore, certificates assigned by the certificate authority are highly authoritative.

(2) Service provider [10]: A service provider submits an application to the certificate authority with a legitimate business license to obtain a digital signature certificate, which includes the key required in the process of encrypting the information.

(3) User: If the user needs to verify the reliability of the service provider, the certificate can be obtained from the certificate authority. The certificate authority will first verify whether the user is legitimate, and if the audit is passed, the decryption key will be provided to the user.

B. Asymmetric Encryption

RSA (Rivest, Shamir, Adleman) is a commonly used asymmetric encryption algorithm [11] and is currently the most authoritative public key encryption method. In the RSA system, a key pair consisting of a public key and a private key is included, where the public key has an open character and the private key is handed over to the user for safekeeping. However, the RSA algorithm process relies too much on large number of factorization and uses public keys and ciphertexts to obtain plaintext, which is equivalent to decomposing the product of different large prime numbers, and the decomposition is too difficult. The RSA-based key generation process is as follows:

Step 1: p Arbitrarily generates two large prime numbers q with conditions that must be as p meets q and are mutually different [12];

Step 2: $p \times q$ The result of the calculation, which is represented by an integer and has $\varphi(n)$ a $\varphi(n)=(p-1)(q-1)$;

Step 3: Select an integer of some and $\varphi(n)$ intervocalic, assume e, $(e,\varphi(n))=1$ and meet the $1<e<\varphi(n)$ requirements;

Step 4: Operation $e^{-1}\left(\mathrm{mod}\,\varphi(n)\right)=\mathrm{d}$, is given as $d\times e\equiv 1\left(\mathrm{mod}\,\varphi(n)\right)$

Step 5: The generated public and private keys are represented as $PU\{e,n\}$.

$PR=\{d,n\}$ It is worth noting that $\gcd(\ )$ the function is to send back the greatest common divisor of the certificate, the symbol '≡' that describes the congruence [13], and that both ends must be congruent.

Due to the difficulty of decomposition of the above process, this article has made the following improvements: the use of integer grouping to divide the plaintext encoding into m groups, m which should be less than the integer, that n is, m the number of digits is expressed as, $\log_2 nbits$ and then the private key is used to encrypt all $PR=\{d,n\}$ the packets, c and for cipher-text, there is. $m=c^e\left(\mathrm{mod}\,n\right)$

In summary, the asymmetric encryption process is completed, and the cipher-text can only be owned by both parties to the communication, so that the data obtained during transmission is not easily attacked, as it adds a security barrier to the cellular network communication.

C. Safe Transmission of Energy Consumption

In cellular networks, data transmission and energy consumption are also the key to the success or failure of communications. To reduce the energy consumption of the network, the energy consumption level of all nodes is comprehensively analyzed, and the energy loss of the node receiving and transmitting modules are considered. Suppose D, it represents the communication distance of two nodes, if the distance is short, the transmission loss index is, if the distance is D^2 long, the loss index is D^4, is the constant D_{co} that determines the length of the distance. It can be seen that to reduce energy consumption, nodes need to avoid single-path transmission over long distances as much as possible.

From the relationship between communication energy consumption and distance, it can be concluded that when a node transmits k a bit packet, the energy consumed is calculated using Eq. (2):

$$E_{Tx}(d)=E_{elec}(k)+E_{amp}(D) \tag{2}$$

$$E_{Tx}(d)=\begin{cases}kE_{elec}+k\varepsilon_{fs}D^2 & D<D_{co}\\ kE_{elec}+k\varepsilon_{mp}D^4 & D\geq D_{co}\end{cases} \tag{3}$$

The energy required for the node to receive the packet is:

$$E_{RX}(k)=kE_{elec} \tag{4}$$

In Eq. (2), E_{elec} and E_{amp} represent the energy required for a node to send and receive a certain amount of data, respectively, ε_{fs} and ε_{mp} belong to two different constants in Eq. (3).

Before communication, the above methods are used to calculate the energy required for data transmission, and the transmission path [14] is adjusted in time to ensure the lowest transmission energy consumption, improve the success rate of data transmission, and achieve safe transmission.

D. Secure Transmission Rate

Compared with other networks, the life of the cellular network node is short. There are certain unstable factors in the network, and the probability of the packets sent by the node being acquired by the neighbor node is low, and it needs to be forwarded multiple times before it can be stored by the neighbor node. In the topology of a cellular network, assuming that the data originating node is, the packet A sent to the node at the transmission rate of, the probability R of the neighbor M node successfully saving the data that is and the number of times the node $P_{A,M}^{R}$ needs to send repeatedly is expressed as follows Eq. (5):

$$N_{A,M}^{R}=\frac{P_{A,M}^{R}}{P_{M,A}^{R}}\times R \tag{5}$$

To ensure the security of data transmission by neighbor nodes, the same node will continue to send the same packets for a certain period, so the A probability that the node will h be successfully saved by the neighbor node at the time of C_i the first forward is expressed as Eq. (6):

$$P=\int_{j}^{h}\left(\frac{1}{P_{A,C}^{R}}\right)^{j-1}\times P_{A,C}^{R} \tag{6}$$

In the process of storing data from neighbor nodes, to ensure the security of the data and verify whether the neighbor nodes are legitimate, network coding technology is introduced [15].

Encoding process: Suppose the initial node needs to transmit data l grouped to neighbor nodes, then generate a random number, constitute l a dimension vector, l according to the vector and $\left(\xi_1,\xi_2,...,\xi_h\right)$ the packet to be transmitted $\left(\xi_1,\xi_2,...,\xi_h\right)$ to form a data block, $B_1,B_2,...,B_l$ combined with the number F vector $\left(\vec{r}_1,\vec{r}_2,...,\vec{r}_l\right)$ constitutes a new coefficient vector $\vec{a}$:

$$F=\frac{\xi_1}{B_1}+\frac{\xi_2}{B_2}+...+\frac{\xi_l}{B_l} \tag{7}$$

$$\vec{a}=\frac{\xi_1}{\vec{e}_1}+\frac{\xi_2}{\vec{e}_2}+...+\frac{\xi_l}{\vec{e}_l} \tag{8}$$

The decoding process [16] is:

$$\begin{bmatrix}F_1\\F_2\\\vdots\\F_l\end{bmatrix}=\begin{pmatrix}\xi_1^1 & \cdots & \xi_l^1\\\vdots & \ddots & \vdots\\\xi_1^l & \cdots & \xi_l^l\end{pmatrix}\begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix}\Rightarrow \begin{bmatrix}B_1\\B_2\\\vdots\\B_l\end{bmatrix}=\begin{pmatrix}\xi_1^1 & \cdots & \xi_l^1\\\vdots & \ddots & \vdots\\\xi_1^l & \cdots & \xi_l^l\end{pmatrix}\begin{bmatrix}F_1\\F_2\\\vdots\\F_l\end{bmatrix} \tag{9}$$

To obtain A as the transmission information of the node, the node with the help of the intermediate M node's forwarding, in this process the node S successfully obtains the packet of the node S the probability is: A

$$P_{[A,M],S}^{R_A}=\frac{\sum_{l=1}^{\infty}\left(1-P_{A,M}^{R_A}\right)^{l-1}}{P_{A,M}^{R_A}\times P} \tag{10}$$

At the same time, we can get the node A and the total length of the M L_A successfully transmitted data under Broadcast length and, L_M are, respectively:

$$L_t=P_{(A,M)}^{R_M}\times L_A+P_{(A,M)}^{R_M}\times L_M \tag{11}$$

If the time required for data transfer is expressed as, in a cellular network, the data transfer throughput is calculated as follows [16]:

$$\theta_{nc}=\frac{L_t}{T'} \tag{12}$$

According to the network throughput, to reasonably select the node transmission rate, set the decoding probability ψ threshold, and the transmission rate calculation formula is as follows Eq. (13):

$$R=\frac{P_{A,M}^{R_A}}{\psi} \tag{13}$$

Through the above process, a reasonable node transmission rate is determined, the communication capacity of the cellular network is improved, and the efficient and secure transmission of data is ensured.

IV. Simulation Based experiments, Results, Analysis and Discussion

This research builds a network that simulates cellular communication, assuming that the communication range

is 600m×600m, and determines several user simulation points and cellular base station locations in the network range by random means. The equipment required for emulation consists of one primary and one secondary switch with an Ethernet interface. The packet forwarding rate is 3.66Mpps, and the overall bandwidth of the communication system is 10MHz. To ensure the consistency of the parameters of the cellular base station, the mutual interference generated during signal transmission is not considered during the experiment. First, the implementation of throughput test is explained as follows:

(1) Throughput test

Throughput testing is performed by using the following methods.

- The direct measurement method is proposed in this paper. It aims to measure the performance metric (throughput) of the cellular network.
- Time-division data modulation is based on multiplexing technology that shows a best performance regarding communication. Time-division multiple access (TDMA) is of greater importance in the modern research on secure data communication when a fixed number of time slots are allocated to all nodes, and each node learns where to transmit, listen or state idle [17]. This algorithm allows to handle most recent instances of a cellular network.
- Energy optimal data transmission: Existing techniques ignore the impacts of energy optimization on the data transmission performance [18]. To bridge this gap, this paper considers the energy optimal algorithm that aims to reduce energy loss while making secure data transmission in cellular networks.

The cellular network throughput under the direct measurement method, time-division data modulation, and energy optimal data transmission method is tested as follows:

Step 1: First, the publish-subscribe relationship between the sending and receiving nodes is established to perform throughput test;

Step 2: In the second step, the sending node uses the maximum transmission speed to send packets;

Step 3: The receiving node obtains the packet, and records the packet time and quantity. Next, it adjusts the transmission rate of the sending node in combination with whether there is packet loss, and if there is packet loss, it reduces the transmission rate, and vice versa;

Step 4: At the fourth step, we repeatedly adjust the transfer rate to determine the final throughput.

The simulation experiment is carried out in the cases of single path as well as multipath, assuming that the packet type and size transmitted by the above three algorithms are the same. The test results of the network throughput are shown in Figs. 4-5, respectively.

By comparing the throughput of the three algorithms in different transmission cases, the throughput is low due to factors such as routing transmission in the initial transmission stage, and the throughput shows an upward trend with the passage of transmission time. Under the single-path transmission, the throughput curve of the three methods did not have obvious differences, and when the transmission paths increased, the proposed method gradually showed the advantages of large throughput. This paper shows that under the proposed transmission method, the maximum transmission rate accepted by the network is high and the transmission rate is fast, which reduces the data transmission time and reduces the probability of packet loss.

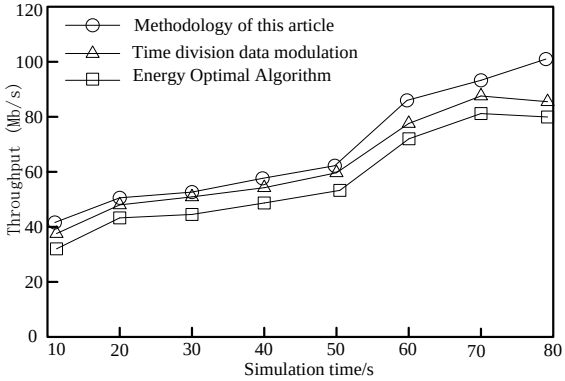

Figure 4. Network throughput test results for different methods under single-path transmission

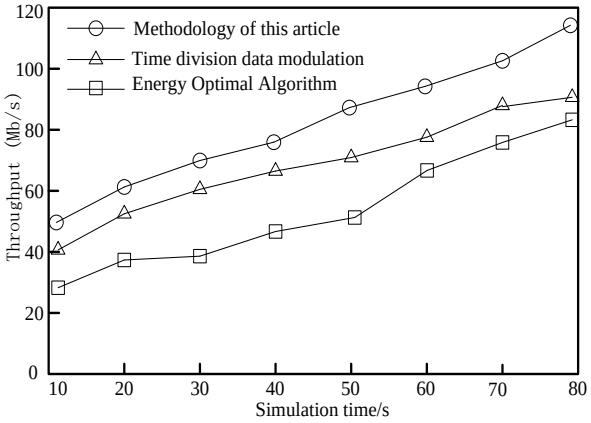

Figure 5. Network throughput test results for different methods under multipath transmission

(2) Average number of retransmissions

The number of retransmissions reflects the anti-attack performance of the transmission algorithm, and if the data is attacked or intercepted during transmission, the packet is resent to the receiving end. Therefore, the average number of retransmissions is used as a measure of the anti-attack performance of the algorithm, and the test results of different algorithms are shown in Fig. 6.

As can be seen from Fig.i 6, in the first 100 simulation experiments, the proposed data transmission method was not affected by any attack, the average number of retransmissions was zero. With the increase of the number of experiments, the number of attack methods was continuously added to the network, and the number of retransmissions of the other two methods increased, and the retransmissions of the method in this article were always the least. This is because the asymmetric encryption algorithm is more confidential, reducing the

possibility of theft, further ensuring the security of data transmission.

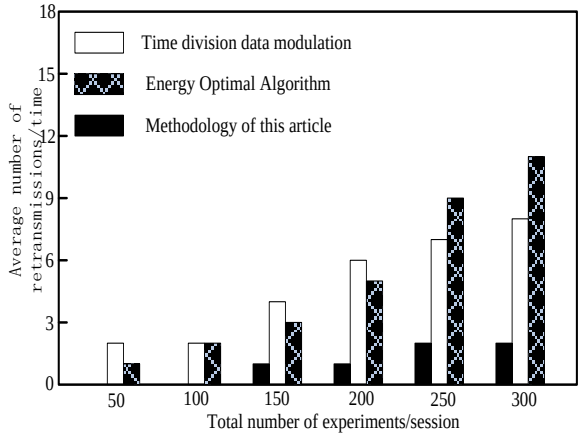

Figure 6. Evaluation diagram of anti-attack performance of different algorithms

(3) Bit error rate test

The bit error rate is to reflect the transmission accuracy of the data in the allowable time, the relationship between the bit error rates. The main variables of the target to be measured are analyzed, and the transmission bit error rate is calculated by using Eq. (14):

$$P^{'} = f\left(\chi, \alpha_1, \alpha_2, ..., \alpha_{n^{'}}\right) \tag{14}$$

The $P^{'}$ formula represents the bit error rate, f is as a function, which can integrate all the factors that affect the signal-to-noise ratio and obtain the bit error rate of the target to be measured. Where χ belongs to the host variable and is another factor that affects the signal-to-noise ratio of communication. f It is mainly related to factors such as coding mode and channel condition. The bit error rate test results for the three algorithms are shown in Fig. 7.

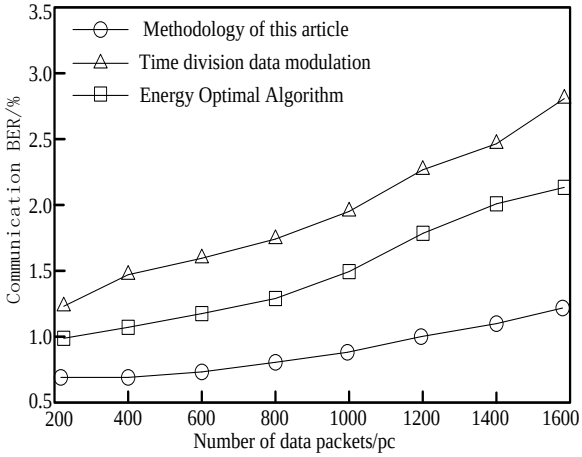

Figure 7. Transmission bit error rate test result graph for different algorithms

As can be seen from Fig. 7, the communication bit error rate of the proposed method is not obvious with the increased number of packets. It makes authors of this paper to be motivated and propose the data transmission rate analysis model in this paper. As a result, it improves the decoding ability of the node and reduces the bit error rate of data transmission through the control of the transmission rate.

Since all nodes are fully balanced regarding the energy and each node considers the energy optimization when a data transmission path is selected in a cellular network. Based on the distance of a user from the base station determines the energy consumption [19]. A node away from a base station takes several hops to transmit data from the base station. Considering the transmission distance the number of hope is too small that indicates the distance for each hop is relatively long. In such cases, the energy optimal data transmission method shows limitation and fails to use the lowest energy consumption. This problem may be undertaken in future works.

(4) Transmission energy consumption analysis

If the transmission energy consumption is large, the network is prone to crash phenomenon, and data security cannot be guaranteed. To do this, the transmission energy consumption of different methods is tested, and the test results are shown in Fig. 8.

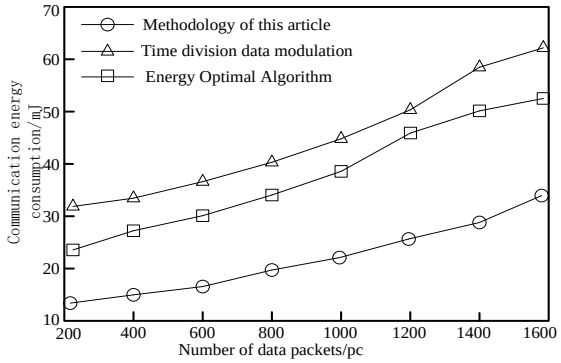

Figure 8. Transmission Energy Consumption Test Diagram

As shown in Fig. 8, in the case of the same transmission of data packets, the proposed method requires the smallest energy consumption during data transmission. Therefore, it indicates that the proposed asymmetric encryption method does not consume additional energy consumption in both the encryption process and the decryption processes, ensuring that the network is always in a low-energy running state.

V. Conclusion

With the advancement of data transmission technology, cellular networks have expanded the scope of application with their various advantages, but transmission security needs to be further improved. To this end, this paper designs a data transmission algorithm based on an asymmetric encryption algorithm. Constructing a sound public key system based on “Rivest–Shamir–Adleman” (SRA) can explore the key generation process to improve the confidentiality of users in the communication process. This paper suggests establishing a transmission rate analysis model, to improve transmission throughput, reduce bit error rate, and ensure transmission security from multiple angles. Simulation experiments show that the proposed method has strong anti-attack performance that improves network throughput, and reduces transmission

bit error rate. In future research, simulation experiments also need to add evaluation indicators such as timeliness to enrich the evaluation system and make the test results more comprehensive.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data used to support the findings of the research are included within this article.

Author Contributions

Qingjia Luo: Conceptualization, writing – original draft, review and editing, Funding; Zhongfu Zhang: formal analysis, Software, review and editing, Funding. All authors approved the final version.

Acknowledgment

This work was supported by the 1. Jiangmen City in 2019 basic and applied basic research key projects, subject name: based on distributed database requirements information real-time query method design and implementation research, number: Jiangke [2019] 256;

2. 2021 Special Fund for Science and Technology Innovation Strategy of Guangdong Province (Special Fund for "Climbing Plan"), project name: Research on the Application of Blockchain Technology in the Source System of Agricultural Products, Number: pdjh2021b0965;

3. 2020 Guangdong Province Science and Technology Innovation Strategy Special Fund ("Climbing Plan" Special Fund), project name: design and development of digital resource copyright protection system based on blockchain technology, number: pdjh2020b1293.

References

[1] X. Y. Zhang and Y. X. Feng. "A weighted fractional order fourier transform communication method based on time division data modulation" *Journal of Ordnance Engineering*, vol. 41, no. 7, pp. 1360-1367, 2020.

[2] J. F. Sun and C. Zhao, "Simulation of frequency domain equalization method for communication security based on energy optimization" *Computer Simulation*, vol. 37, no. 3, pp. 421-424, 457, 2020.

[3] W. Li, K. F. Wei, Y. J. Li, *et al*., "Collaborative design of DUAL security control and communication of CPS under DoS attack," *Journal of the Lanzhou University of Technology*, vol. 46, no. 6, pp. 85-97, 2020.

[4] J. B. Gao, C. H. Yuan, and J. Zhou, "A communication scheme for eavesdropping on multicast system with unknown user location," *Journal of Xidian University*, vol. 47, no. 5, pp. 144-149, 2020.

[5] J. R. Vacca, *Network and System Security*, Elsevier, 2013. Ch. 11, pp. 319-351.

[6] D. Wu, Q. Liu, H. Wang, Q. Yang, and R. Wang, "Cache less for more: Exploiting cooperative video caching and delivery in D2D communications," *IEEE Transactions on Multimedia*, vol. 21, no. 7, pp. 1788-1798, 2018.

[7] L.C. Zhang, Y. B. Xu, F. H. Li, *et al*., "Dynamic empowerment architecture of information network security for space-earth integration" *Journal on Communications*, vol. 42, no. 9, pp. 87-95, 2021.

[8] Z. Y. Wang, J. Y. Wang, J. Xie, *et al*., "Static hierarchical modeling method of power communication system oriented to data availability" *Automation of Electric Power Systems*, vol. 45, no. 20, pp. 9-17, 2021.

[9] T. Cheng, K. Peng, and T. Zhou, "Study on the confidentiality rate of relayed D2D system under cellular network," *Journal of Beijing Jiaotong University*, vol. 44, no. 2, pp. 83-90, 2020.

[10] Z. H. Qian, W. J. Meng, X. Wang, *et al*., "Research on power distribution algorithm for multi-multiplexing D2D communication under full load cellular network," *Journal of Electronics and Information Technology*, vol. 42, no. 12, pp. 2939-2945, 2020.

[11] H. Q. Jiang and J. Zhang, "D2D/Cellular communication mode switching and joint power control scheme" *Signal Processing*, vol. 36, no. 2, pp. 233-239, 2020.

[12] Q. L. Liu, J. H. Yang, Y. J. Xu, *et al*., "Energy efficiency optimization algorithm of intelligent reflective surface network oriented to secure communication" *Telecommunications Technology*, vol. 60, no. 12, pp. 1391-1397, 2020.

[13] Y. Chen, Z. M. Jiang, and Y. Zhang, "Secure transmission of big data based on homomorphic hash authentication in cloud systems," *Computer Engineering and Design*, vol. 42, no. 5, pp. 1250-1256, 2021.

[14] L. X. Wang, K. Dong, X. S. Dong, *et al*., "Lightweight secure transmission method for virtual data space" *Journal of Huazhong University of Science and Technology* (Natural Science Edition), vol. 49, no. 4, pp. 108-113, 2021.

[15] Z. C. Gu, Y. B. Guo, and C. Fang, "Message queuing telemetry transport protocol end-to-end security solution based on broker Re-Encryption," *Computer Applications*, vol. 41, no. 5, pp. 1378-1385, 2021.

[16] M. S. Li, Y. Ma, Z. Y. Yin, *et al*., "Model design of intelligent production line secure communication for industrial Internet of Things with multiple redundancies," *Journal of Microcomputer Systems*, vol. 42, no. 3, pp. 621-626, 2021.

[17] Y. Sun, Z. Zhang, X. Li, S. Xiao, and W. Tang, "An extensible frame structure for time division multiple access medium access control in vehicular ad-hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3912, 2020.

[18] Y. Cui, *et al.*, "Performance-aware energy optimization on mobile devices in cellular network," *IEEE Transactions on Mobile Computing*, vol. 16, no. 4, pp. 1073-1089, 2016.

[19] X. Liu and J. Wu, "A method for energy balance and data transmission optimal routing in wireless sensor networks," *Sensors*, vol. 19, no. 13, p. 3017, 2019.

Qingjia Luo was born in Guangdong Province, China, in 1987. He received his B.S. degree in Computer Science and Technology from Lingnan Normal College in 2010 and M.S. degree in Software Engineering from East China Normal University, in 2015. Currently, he is pursuing his PhD degree at the School of Data Science, City University of Macau. His research interestssss include blockchain technology applications, and distributed data processing.

Zongfu Zhang was born in Guangdong Province, China, in 1981. He received his B.S. degree in Educational Technology, South China Normal University in 2003 and his M.S. degree in Software Engineering from South China University of Technology in 2007. Currently, he is the head of the practical training department of Jiangmen Vocational and Technical College. His research interests include computer application technology and software engineering.