Hindawi
Journal of Sensors
Volume 2021, Article ID 5800620, 11 pages
https://doi.org/10.1155/2021/5800620

Research Article

Software Implementation and Design of Information Encryption Algorithm Based on DNA Nano Self-Assembled Sensor Array

Caixia Li

Henan Industry and Trade Vocational College, Zhengzhou Henan 450000, China

Correspondence should be addressed to Caixia Li; licaixia@hngm.edu.cn

Received 30 August 2021; Accepted 11 September 2021; Published 30 September 2021

Academic Editor: Guolong Shi

In the field of information security, DNA cryptography based on DNA molecular configuration and special recognition mechanism between molecules has developed rapidly. DNA molecules have great development potential in the field of information security technology such as information encryption, hiding and authentication, which provides a new way for the development of modern cryptography. The nodes of traditional sensor networks are mostly distributed in the form of a net with strong openness. In the process of node data transmission, the information is likely to be stolen, tampered with, and destroyed at any time. In this paper, an information encryption method based on DNA nano self-assembled sensor technology is proposed, and the encryption software based on DNA nano self-assembled sensor array is designed. The information encryption algorithm is designed, tested, simulated and analysed, and compared with other designs. The simulation results show that the encryption algorithm system based on DNA nano self-assembled sensor array has good function and excellent performance, can fully meet the requirements of network real-time encryption, has good feasibility and security, and reveals the great application potential of DNA molecules in the field of information security.

1. Introduction

DNA molecule is a three-dimensional nanowire with exquisite structure and super assembly ability. Its good operability and strong recognition and signal conversion ability have natural advantages for the structure and composition. Therefore, since the concept of DNA nanotechnology was put forward, the research on constructing DNA nanostructures has developed rapidly and attempts to apply and control DNA nanostructures. The direct use of molecules and atoms to manufacture nanomaterials with specific functions can also combine DNA nanomaterials with other nanomaterials, so that people can create new materials in a more refined and efficient direction, which has brought unprecedented impetus to the fields of life science, material science, and environmental science and has achieved certain results [1]. In daily life and learning, information, as the main carrier of transmission and storage, plays an important role in the fields of medical treatment, education, economy, and military. How to transmit and store this information on the network has become the focus of attention and research. The encryption technology of DNA nano self-assembled sensor array is one of the effective ways.

Limited by the current technology, traditional wireless sensor networks have some problems, such as limited power, weak computing power, poor communication ability, and vulnerable to attack. However, the existing encryption methods cannot effectively solve the above problems when applied to sensor networks [2]. DNA self-assembly technology, as a method in biological computing, has its own physical and biological properties that cannot be achieved by other materials. DNA computing has the advantages of simple preparation method, high sensitivity, low complexity, low cost, and exploitability. When solving complex problems, it can match and generate spontaneously, which is operable. In this paper, an information encryption method based on DNA nano self-assembled sensor technology is proposed, and the encryption software based on DNA nano self-assembled sensor array is designed. The information encryption algorithm is designed, tested, simulated and analysed, and compared with other designs [3]. The simulation results show that the encryption algorithm system has good

function and excellent performance, can fully meet the real-time encryption requirements of wireless sensor networks, and achieve the expected goal of high speed and low power consumption.

The content of this paper is arranged as follows: Section 1 introduces the background, significance, and organizational structure of this paper. Section 2 describes the related work. Section 3 introduces the relevant knowledge and technology of DNA nano self-assembled sensor array, analyses the sensing of DNA nanostructure regulation, and analyses the design and implementation of encryption software system. In Section 4, the algorithm is simulated and tested. Section 5 summarizes the full text.

2. Related Work

At present, the improvement of sensor array security at home and abroad mainly includes the improvement of anticracking ability of sensor equipment itself, the strengthening of sensor data protection, the effective defines against malicious attacks, and so on. The improvement of hardware security involves the improvement of memory, arithmetic unit, and communication module in the hardware design of sensor nodes; the protection of data and the defenses against malicious attacks mainly rely on the ability of encryption algorithms for data encryption and identity authentication. At present, scholars at home and abroad have done a lot of research in order to make the existing encryption algorithms effectively used in sensors and pointed out many problems.

For some wireless sensor networks with insensitive real-time data, scholars have proposed a method of data storage combined with homomorphic encryption [4]. Considering the limited energy and processing capacity of wireless sensor networks, they proposed to encrypt the data transmission channel instead of encrypting the data. The specific ideas are as follows: firstly, each WSN node has a built-in random number. During data transmission, the WSN node determines which channel to use to transmit data according to the random number and the number of bits of the data. A piece of data may be sent out separately in several channels [5]. The coordinator receives the data of all channels and then restores the data according to the convention. One advantage of this method is that it saves the cost of data encryption and ensures the security. Of course, it has great limitations. Firstly, wireless sensor networks have limited channels, which makes it impossible for all channels to be secure. Malicious attackers can eavesdrop on all channels to crack [6]. At the same time, for nodes, the energy consumption of data transmission is sometimes greater than that of data processing, which also causes that the final energy consumption of this method may even be greater than that of data encryption, so it also has some defects.

Some scholars have compared the current symmetric encryption algorithms. After comparing AES, RC5, and RC6 algorithms, it is concluded that AES encryption is a symmetric encryption algorithm with the lowest power consumption and the best security [7]. RC5 has relatively low power consumption, but low security; RC6 is not suitable for wireless sensor networks because of its complex operation. Therefore, for the current wireless sensor networks, the most suitable symmetric encryption algorithm is the AES encryption. The author further proposes an improvement on the AES encryption algorithm [8]. He pointed out that the authentication capability of the current symmetric encryption algorithm has limitations. However, the authentication ability of symmetric encryption algorithm has limitations. The AES algorithm should be better applied to wireless sensor networks and cooperate with the asymmetric encryption algorithm to better realize the function of node authentication. The author did not give a plan how to further improve. Although it is convenient to authenticate, the actual network is often the topology of coordinator router terminal node. When authenticating with ordinary asymmetric encryption algorithm, the initiator still needs to obtain the public key of the node to be authenticated from the server to initiate the authentication of other nodes [9]. That is, each authentication needs to communicate with the server first. This is not suitable in wireless sensor networks with complex topology and multihop communication, which also determines that the direct use of asymmetric encryption algorithm is still limited, because the author does not consider the problem of key update in wireless sensor networks but adopts the method that the private key is present at the WSNs point, which also leads to the difficulty of key update in this method.

Some scholars put forward improvement ideas according to the use characteristics of some wireless sensor networks. Starting from the insensitivity of some networks to data, they put forward the concept of data prestorage. However, this scheme actually uses a large number of servers and has high limitations [10]. This scheme assumes that the method of data insensitive and distributed storage of a large number of servers can only be applied to a specific network. Therefore, it is not suitable for ordinary wireless sensor networks. Some scholars find another way to improve the physical transmission of wireless sensor networks. However, it is not explained whether frequent channel transformation will increase the communication burden of WSN nodes.

3. Design and Implementation of Information Encryption Based on DNA Nano Self-Assembly Sensor

3.1. DNA Self-Assembly Technology. DNA self-assembly technology is a spontaneous formation and assembly process using DNA peptide chain as the basic assembly element. DNA molecular fragments are connected with each other through viscous ends to form a specific complex structure under appropriate temperature and other conditions. The assembly principle between DNA molecules can be described in the following steps: first, DNA molecules should be encoded. The actual problem is mapped to the corresponding DNA element, encoded by four different bases, and different assembly structures can be designed according to different molecules. Because the sticky end of each peptide chain is a designed base sequence, combined

with the complementary pairing principle between bases, they will spontaneously match the corresponding DNA peptide chain, so as to expand into a larger order of magnitude and more complex structure. Finally, when the self-assembly process is completed, we can get an assembly with relatively stable structure [11]. According to the needs of our problem, we can read the solution space combined with the corresponding biochemical technology.

As a biomaterial, DNA molecule is easy to obtain and prepare, and DNA molecule is a nanosized material, which will naturally become the first choice of self-assembly materials. DNA molecules follow the W-C principle, DNA strands can react spontaneously without manual participation, and the parallelism is huge. Therefore, in the development process of self-assembly technology, these natural advantages of DNA molecules provide conditions for the development of DNA self-assembly [12]. DNA self-assembly mainly uses DNA molecules as basic materials, and the interaction forces such as base hydrogen bond and van der Waals force between molecules make molecules spontaneously form a relatively stable and complex molecular structure. Based on the form of DNA self-assembly structure, it can be briefly divided into three categories: one-dimensional structure, two-dimensional structure, and three-dimensional structure.

With the deepening of research, one-dimensional self-assembly structure is far from meeting the needs of calculation. Therefore, scholars put forward a two-dimensional matrix model with a more complex form and structure on the basis of a large number of experiments. The self-assembly model of peptide chain structure is proposed and applied to Turing calculation [13]. The development of two-dimensional self-assembly structure of DNA complements the shortcomings of one-dimensional structure. Compared with one-dimensional structure, the construction of two-dimensional assembly structure is complex for the following three reasons: it contains single-stranded DNA with longer length, each small unit of self-assembly is composed of multiple DNA strands and sticky ends, and shorter stranded DNA is involved. The stable connection structure is generated by base complementary pairing, and complex multidimensional objects can be assembled accurately.

3.2. Biosensor Based on DNA Self-Assembly. The target detection and amplification technology based on DNA self-assembly is a dynamic nanotechnology independent of enzyme. The concept of DNA is based on the complementary base pairing characteristics of DNA as a genetic material. Therefore, under precise design and control, circular nanomachines or geometric shapes of different spatial configurations can be formed. Among them, DNA self-assembly nanomachines include catalytic hairpin assembly (CHA), hybridization chain reaction (HCR), DNA walker, and entropy-driven strand displacement reaction (ESDR). These nanomachines can be driven by base force. Fast dynamic operation can be used for the amplification strategy of output signal. Then, in order to improve the reaction speed and amplification efficiency of linear HCR, the principle is that the target nucleic acid molecule triggers the self-assembly of two DNA double-stranded dimers to form branched nanostructures [14]. Compared with linear HCR, because the nonlinear HCR is dynamically assembled in three-dimensional space, its amplification efficiency is greatly improved, and dendritic nanostructures with larger molecular weight can be obtained [15]. DNA molecules are first spliced to form the basic assembly module nanostructure of small molecules, and then the basic modules are assembled into a more complex one-dimensional to three-dimensional macromolecular nanostructures through coding program hybridization, which can play an important role in the field of biosensor and drug loading.

Because of its unique flexibility, flexibility, and high biocompatibility, it also has the intelligent response to temperature, pH, ionic strength, and charge effect. It makes DNA hydrogel become a nanomaterial with great potential in biological analysis, drug delivery, and tissue engineering.

3.3. DNA Nanostructure Regulatory Sensor. The process of DNA hybridization is related to the spacing of probes. Therefore, we can further study the performance of tetrahedral DNA nanostructures with different sizes in DNA biosensors. We selected a simple sandwich method, as shown in Figure 1, as an example to investigate the regulation of tetrahedral DNA nanostructures of different sizes on DNA biosensor.

Various nanomaterials, including quantum dots, magnetic nanoparticles, and carbon nanotubes, have been used as signal converters in biosensors. The advantages of nanomaterials include many available signal mechanisms, ultrahigh signal strength, fine adjustable surface chemistry, and large specific surface area. A very small number of nanomaterials can give ultrahigh signals, which is conducive to integration into miniaturized equipment [16]. The customizable optical properties of nanoparticles allow multiple targets to be detected at the same time. For example, nanogold, with stable physical properties, easy synthesis, and diverse functions, makes them especially suitable for multifunctional platforms for creating diagnostic biosensors.

Inorganic nanoparticles can be surface modified to improve their colloidal stability and functionalization. Surface modification generally covers nanoparticles with molecules, so as to give nanoparticles good properties. To prevent the aggregation of nanoparticles in solution, they can be charged to produce electrostatic repulsion, or the surface can be covered with polymers that provide steric hindrance for polymerization [17]. These end capping agents are often used in the synthesis of nanoparticles and the colloidal stability of nanoparticles. The surface of nanoparticles can provide an effective biological interface and biological related target interaction by combining various functional groups to become a multivalent surface. The relatively easy functionalization route enables nanomaterials to meet our required functions, so they can be applied to clinical diagnosis. However, some nanomaterials pose great challenges in constructing effective surface modification and stable biological related media. Gold nanorods (GNRs) are an example of this because they have strong dispersion interactions between transverse particles [18]. A series of methods have

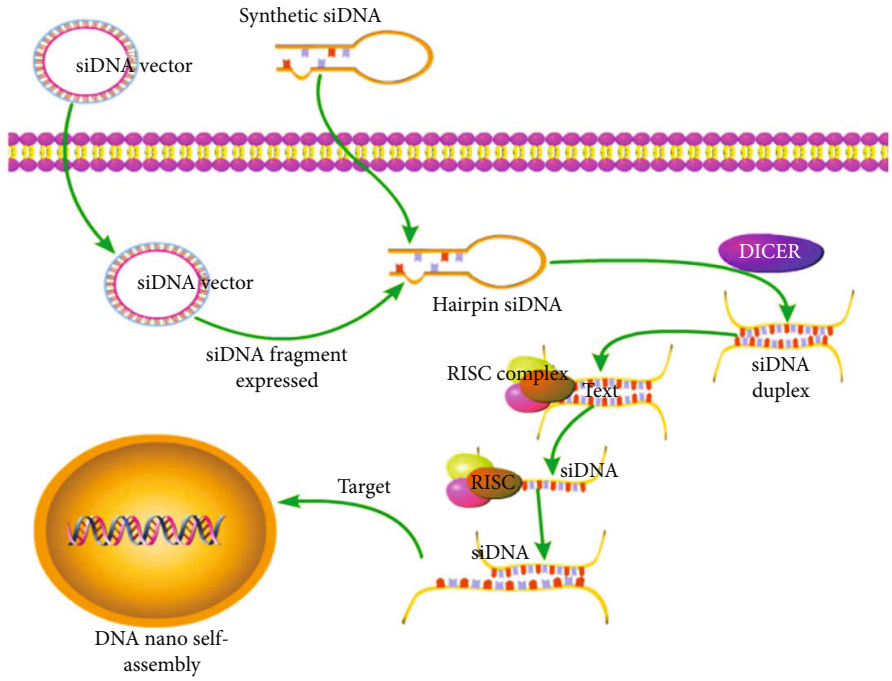

Figure 1: DNA nano self-assembled structure regulatory sensor.

been tried, including covalently modifying quaternary amine bases and physically adsorbing charged polymers, although the typical practice is to use number glycol to form a steric barrier layer around the particles. The key to ensure the formation of this dense steric layer is the use of effective spatial stability, even in electrolyte-rich solutions.

3.4. Design and Implementation of Encryption System. The encryption system is mainly designed for the actual network layout of WSN. For different network environments, use the wife or wick encryption method of your choice. The system needs an x86 host as a server, a WSN coordinator, and several WSN nodes during deployment. The server side runs in Windows\Linux environment. Its main functions are receiving and managing the data collected by WSN, setting the relevant parameters of WSN by users as needed, encrypting and decrypting the data transmitted by WSN nodes, and actively initiating authentication for some WSN nodes [19, 20]. WSN end mainly includes coordinator and WSN node. Its running system environment is stack hardware protocol stack environment. Before WSN device deployment, the user needs to burn in the relevant hardware program in advance. After WSN device deployment, the program written by its hardware cannot be changed [21]. The coordinator is mainly responsible for WSN network initialization and receiving the data collected by WSN nodes. The main functions of WSN node are collecting environmental data, processing the collected data, WSN node authentication and response authentication, etc. The whole system can be divided into several modules according to function: data display module, data statistics module, WSN management module, data acquisition module, encryption/decryption module, initialization module, authentication module, etc. [22–24]. The first two modules are mainly deployed on the server side, while the latter modules are mainly deployed on the WSN node, and some functions are realized by the server. The system module design is shown in Figure 2.

4. Simulation Analysis and Test

4.1. Correlative Analysis. The correlation between the pixels of the original image is very high. In order to resist statistical attacks, the correlation of the encrypted image must be reduced. We randomly select 3000 pairs of adjacent pixels in the horizontal, vertical and diagonal directions from the original image and encrypted image and then calculate the correlation between pixels. Correlation coefficients of adjacent pixels in original information and encrypted information are shown in Figure 3.

The horizontal correlation between the original image and the encrypted image is shown in Figure 3, and the correlation coefficients are 0.9248 and 0.0023, respectively. The correlation coefficients in other directions are shown in Figure 4, and the correlation between the pixels of the encrypted image is very low, almost close to 0. Again, this algorithm has strong antistatistical attack ability.

4.2. Analytical Performance of Sensor. In order to investigate that the sensor can be used for quantitative analysis of S_1 nuclease activity, under the optimal reaction conditions, the sensor system detected the activities of a series of S_1 nucleases with different concentrations. As shown in Figure 5, with the increase of S_1 nuclease concentration, the fluorescence intensity of double-stranded copper nanoparticle complex gradually decreases from 1 U/ml to 50 U/ml; Figure 5 depicts the relationship between fluorescence response and S_1 nuclease concentration. The proposed sensor is highly sensitive according to slope calculation, and

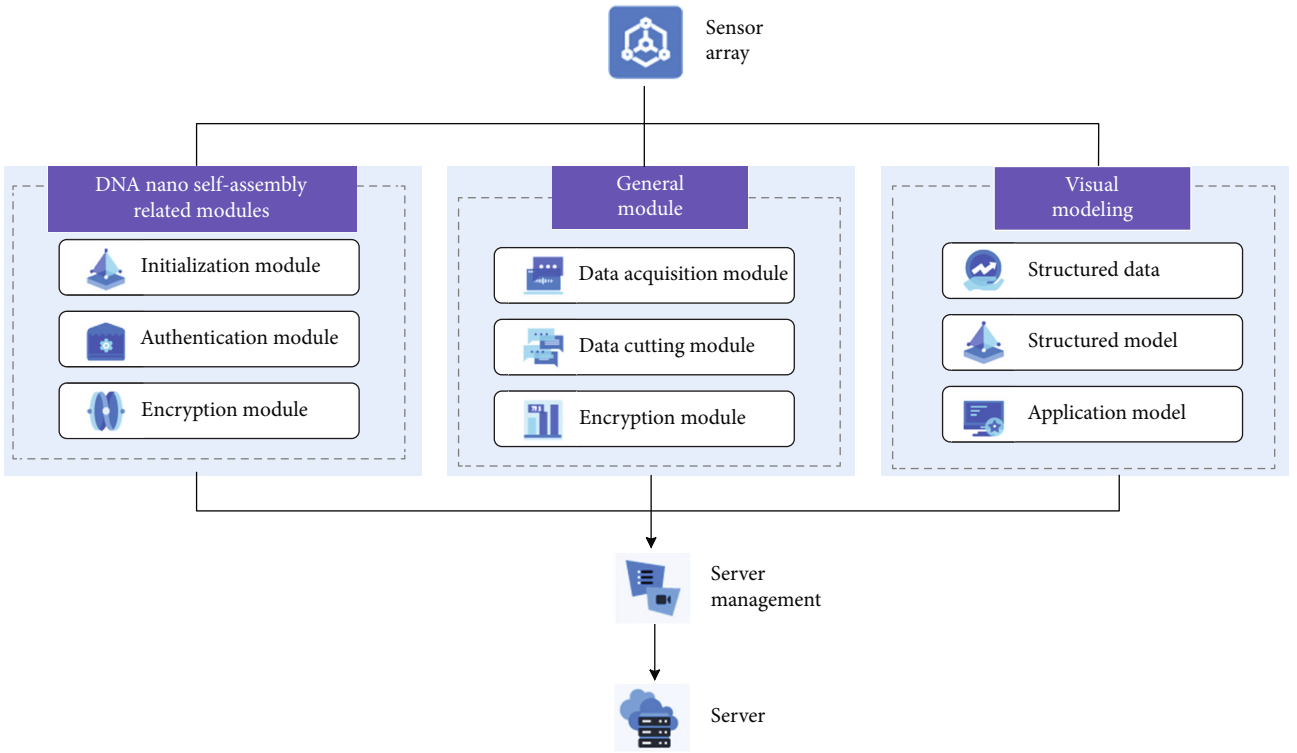

Figure 2: Implementation of encryption system based on DNA nano self-assembled sensor array.

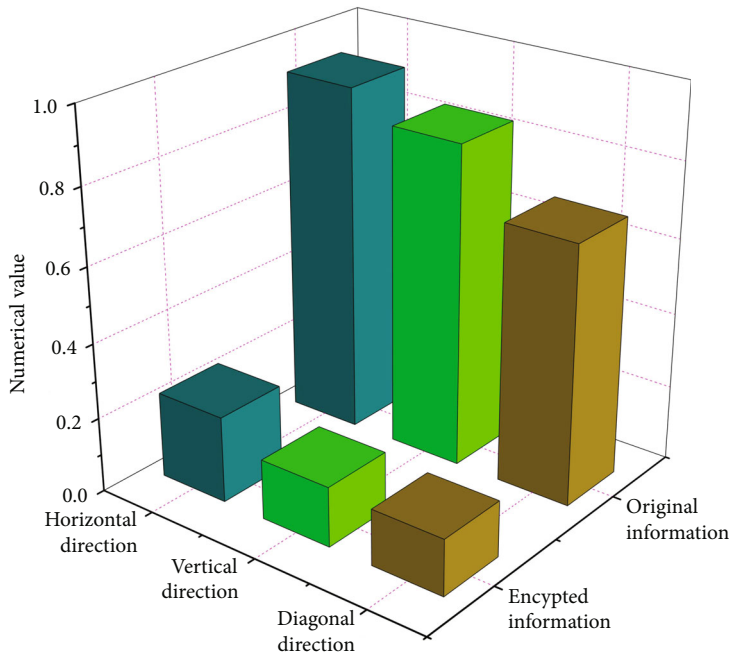

Figure 3: Correlation coefficients of adjacent pixels in original information and encrypted information.

the lower detection limit is 0.3 U/ml. This lower detection limit is an order of magnitude better than the traditional methods for detecting nuclease activity and UV-based methods, although the detection limit of the sensing method is slightly worse than that of the labelled fluorescent sensor based on cationic copolymer.

The selectivity of the sensing system was investigated by detecting the fluorescence response value in the presence of other nucleases. Under the same conditions, only S_1 nuclease can cause a significant decrease in fluorescence, as shown in Figure 6. The results show that the sensing system has good selectivity for S_1 nuclease.

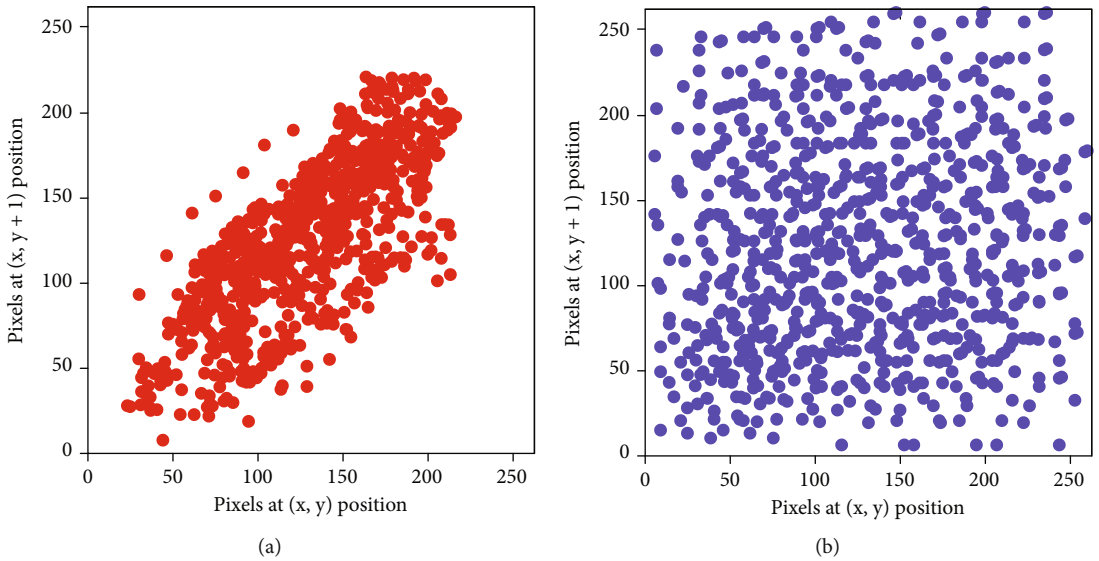

Figure 4: Correlation of adjacent pixels in original information and encrypted information. (a) Original information. (b) Original information.

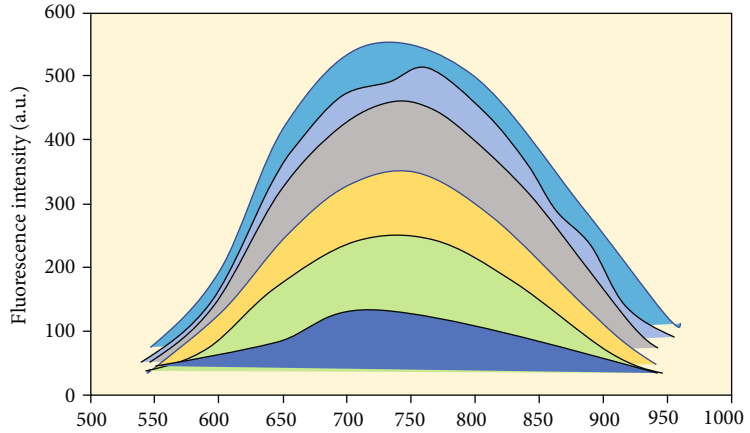

Figure 5: Specificity analysis of sensing system.

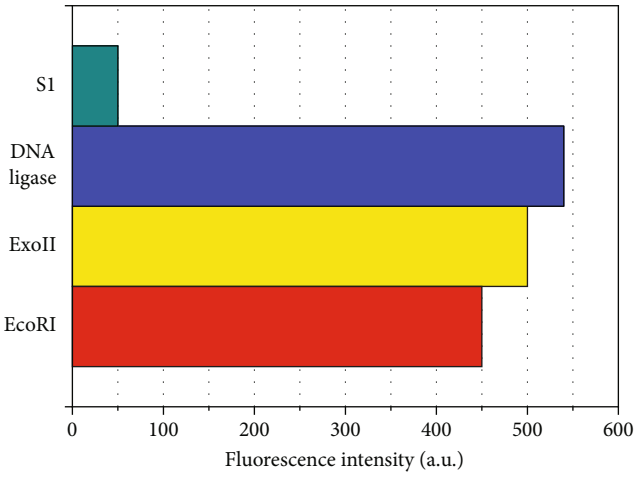

Figure 6: Specificity analysis of sensing system.

4.3. Energy Consumption Test. Firstly, the energy consumption of several encryption algorithms is tested. Because the DNA nano self-assembly sensor encryption algorithm has the ability of key update and node authentication, the DNA nano self-assembly sensor encryption algorithm is set to perform node authentication every 30 minutes and key update every two hours, so as to approach the actual network layout as much as possible, while other methods only perform encryption and decryption. Key update and authentication operations were not joined. A total of about 100000 pieces of actual data are collected in the actual network layout. The ordinate is the average voltage of nodes in the actual network, in volts. Abscissa is the network running time, in hours. It can be seen that when the key length is 40 bit, except for the nonencryption method, the AES encryption supported by CC2530 hardware has the longest duration. The actual encryption duration of DNA nano self-assembled sensing encryption algorithm is about 86 hours, which is reduced by more than 10 hours compared

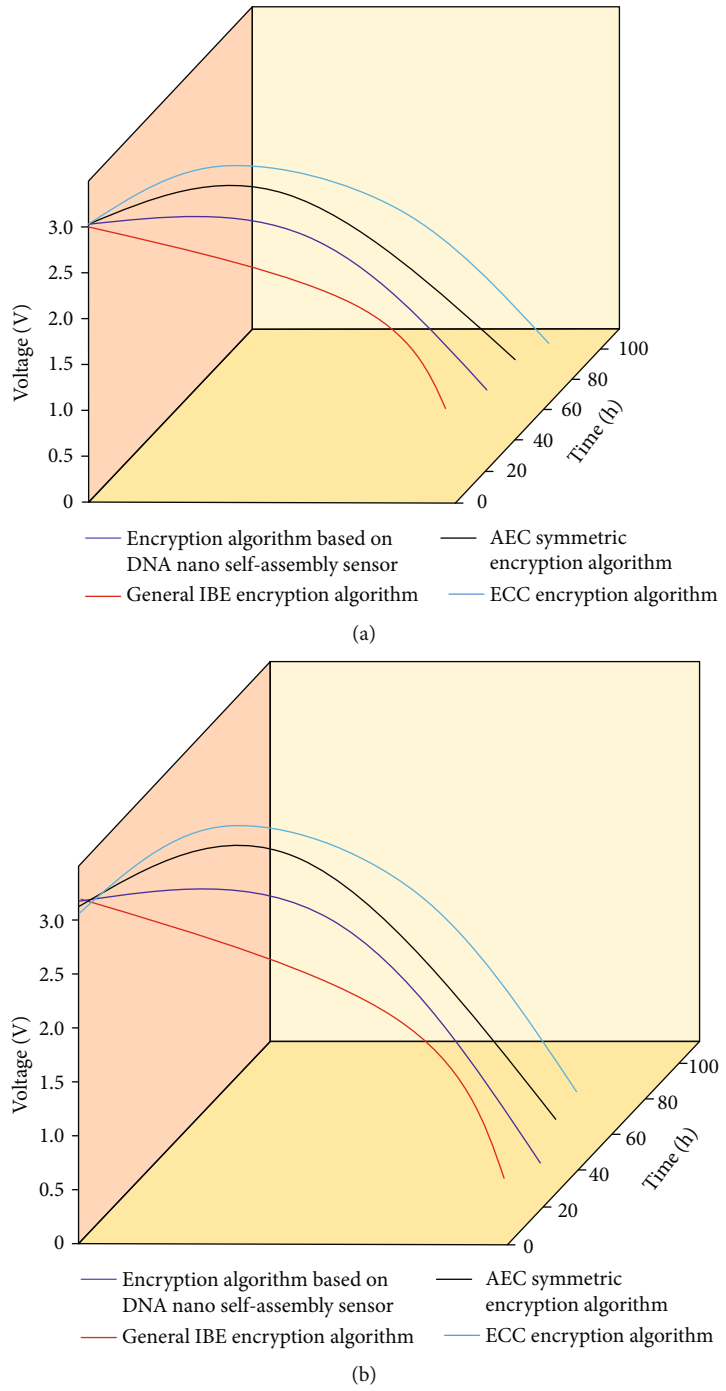

Figure 7: Energy consumption test. (a) Average trend of node voltage in real-time network. (b) Simulation of the average trend of node voltage in the network.

with AES encryption. However, considering that the DNA nano self-assembled sensing encryption algorithm is set to authenticate between nodes every half an hour, which is different from AES only performing encryption and decryption operations, it can be considered that the DNA nano self-assembled sensing encryption algorithm can meet the energy consumption requirements when the key length is 40 bit. In contrast, ECC encryption requires complex elliptic curve operation for encryption and decryption. Not only the encryption strength is weaker than hardware AES encryption, but also the power consumption is much larger. The network has been paralyzed in less than 70 hours of actual test. Due to the high complexity of bilinear pair operation, the IBE encryption method has the shortest network deployment duration, which can only last for more than 50 hours. From the energy consumption of the actual network, although the duration of DNA nano self-assembly sensor encryption algorithm is weaker than AES encryption, it still

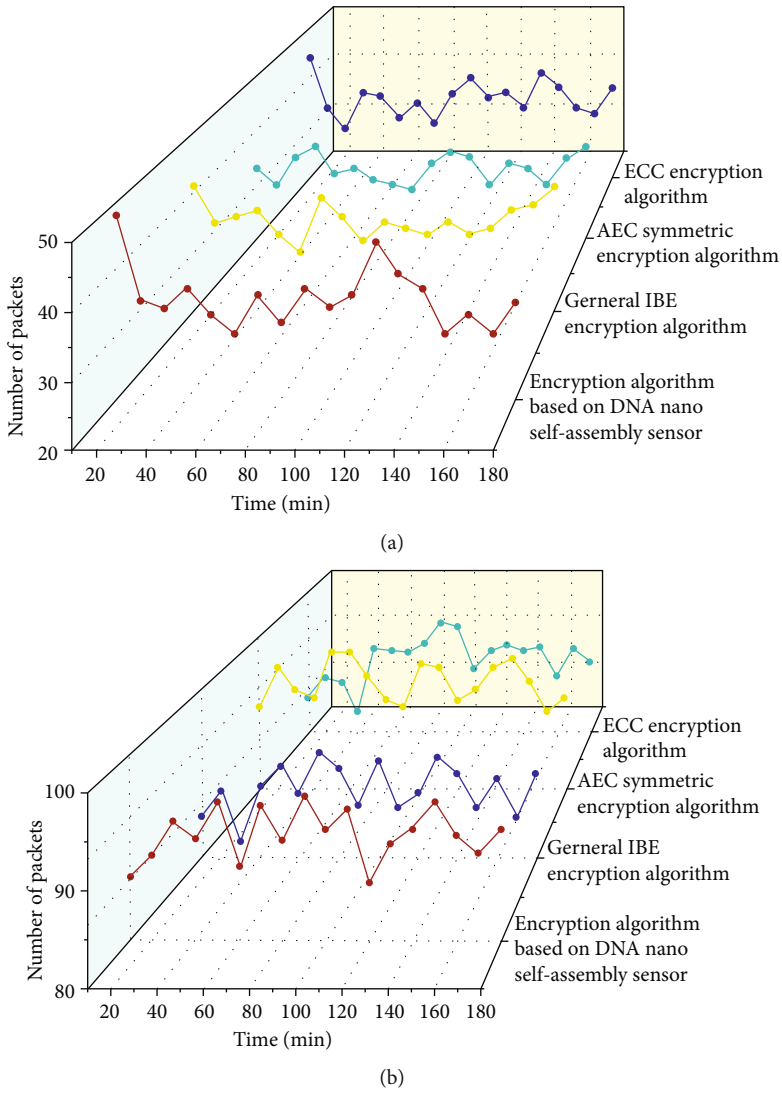

Figure 8: Test of actual network traffic with different encryption algorithms. (a) Statistical comparison of real power saving. (b) Reception rate of actual network data.

lasts for a long time, which basically meets the design goal. The energy consumption test is shown in Figure 7.

It can be seen that the simulation test of 100 nodes is slightly different from the actual network test of 12 nodes. With the increase of network scale, the duration of the whole network tends to decrease. After analysing the data, it can be considered that this is related to the way of network distribution. In the test, in order to approach the actual network layout, the simulation adopts uniform distribution, that is, the probability of nodes falling in the area close to the coordinator is the same as that far away from the coordinator. As the nodes closer to the coordinator bear more and more heavy data forwarding tasks, the life of nodes undertaking forwarding tasks will be shorter and shorter with the increase of network scale. Therefore, the network lifetime is affected. However, several algorithms in the test adopt the same square method, so it does not affect the comparison of encryption algorithms. Based on the results of actual network layout experiment and simulation experiment, it can be seen that the duration of DNA nano self-assembly sensor encryption basically meets the actual network layout requirements and achieves the expected goal.

4.4. Test of Communication Performance. The experiment of network communication performance is tested from two aspects: network traffic and data reception rate. The so-called data-receiving rate is the probability that after the WSN node collects data, the data finally successfully reaches the server through the network and is received. In the actual network deployment experiment, the data that can be effectively counted is the number of data sent by the WSN node and received by the server. Therefore, compared with the concept of packet loss rate, the concept of data reception rate can more accurately describe the actual experiment. For wireless sensor networks, the communication bandwidth is limited, and the packet length system of one communication is very strict. When the transmission data is dense, the large traffic will reduce the limited communication capacity of

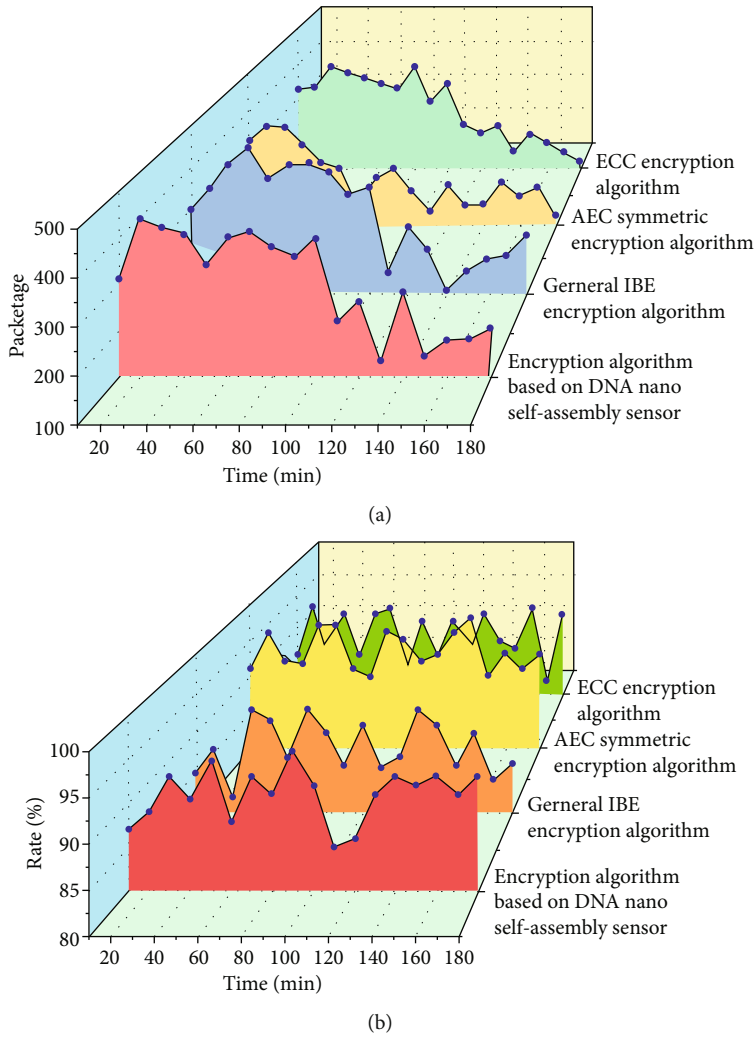

Figure 9: Test of communication in simulation environment. (a) Traffic trend. (b) Trend of data reception rate.

WSN nodes and then reduce the data reception rate of the whole network. The test of the actual network traffic with different encryption algorithms is shown in Figure 8.

In the experiment, the traffic and data-receiving rates of several methods with 40-bit key are tested on the CC2530 WSN node, and about 40000 experimental data are obtained. Because, in the actual test, DNA nano self-assembled sensing encryption is set to perform node authentication every 30 minutes and key update every 2 hours, the communication volume of DNA nano self-assembled sensing encryption will have a peak every 120 minutes. The IBE encryption algorithm and ECC encryption algorithm do not need authentication, but the traffic is large. The AES encryption algorithm with built-in encryption circuit has the shortest encrypted data packet, so the traffic is the smallest. Here, the data reception rates of several algorithms are counted on the real node, and the results. It can be seen that the data reception rate measured by the real node is negatively correlated with the network traffic, and the reception rate is greatly affected by the algorithm traffic. It can be seen from the above figure that the reception rate of ECC, IBE, and other algorithms with large traffic is low, while the reception rate of DNA nano self-assembled sensing encryption algorithm and AES is higher than that of ECC and other algorithms.

In the simulation environment, the statistical results of traffic when several algorithms are deployed on a large scale are shown in Figure 9. It can be seen that when the network scale increases, the trend of traffic not only depends on the algorithm itself but also is greatly affected by the network layout. The random distribution method used in the experiment makes some nodes close to the coordinator consume more energy and die faster. The death of these nodes also affects the communication between other nodes and the coordinator. Therefore, the traffic volume is large at the beginning of network distribution and then gradually attenuates. However, because several algorithms adopt this network arrangement method, it does not affect our comparison of the algorithm itself.

It can be seen that in a large-scale network with 100 nodes, the DNA nano self-assembly sensor encryption algorithm has a key exchange process in the initialization stage, and the traffic in the initial stage is large. With the stability of the network state, the network traffic of DNA nano self-

assembled sensing encryption algorithm is gradually stable, but the traffic will fluctuate every 30 minutes and 120-140 minutes due to the need for authentication and key update. In addition, due to the random network arrangement, the network topology is different each time, resulting in the same traffic and certain error. As can also be seen from Figure 9(b), the traffic of DNA nano self-assembled sensing encryption algorithm is still large, close to ECC traffic. This is also the compromise between security and traffic of DNA nano self-assembled sensing encryption algorithm. It can be seen from the above two statistical figures that although the encryption algorithm of DNA nano self-assembled sensing encryption algorithm has a slightly large traffic due to the addition of node authentication operation, the receiving rate of DNA nano self-assembled sensing encryption algorithm is basically acceptable because the encrypted data packet is shorter than IBE and other algorithms.

5. Conclusion

In this paper, an information encryption method based on DNA nano self-assembled sensor technology is proposed, and the encryption software based on DNA nano self-assembled sensor array is designed. The information encryption algorithm is designed, tested, simulated and analysed, and compared with other designs. Based on the existing algorithms, the encryption system of sensor array is implemented with reference to DNA nano self-assembly technology. It has the characteristics of low energy consumption and high security in application and gives a specific software implementation scheme for the actual deployment of nodes. Finally, the actual network layout test and simulation test are carried out. The test results show that the information encryption algorithm based on DNA nano self-assembled sensor array prolongs the network lifetime by more than 40% compared with the original algorithm, and it can also better deal with malicious attacks. In the face of sudden malicious attacks such as black holes or flooding, the network with 100 nodes can basically return to normal operation after about 10 minutes. Therefore, the information encryption algorithm based on DNA nano self-assembled sensor array can better meet the requirements of network environment with high security requirements and has practical application value. The main application fields of DNA nanosensors include medical care, military, industrial control and robotics, network and communication, environmental monitoring, and so on. With the maturity of related technologies, the powerful advantages of nanosensors in national defense security inspection are gradually emerging. It is believed that in the future, nanosensors will be used in a new generation of military uniforms and equipment and will be used to detect anthrax and other dangerous gases.

Data Availability

All data, models, and code generated or used during the study appear in the submitted.

Conflicts of Interest

No potential conflict of interest was reported by the author.

Acknowledgments

This work was supported by the Scientific and Technological Achievements of Henan Province, Design and Implementation of Health Monitoring Service Platform (9412014Y1921).

References

[1] S. Sun, H. Yao, F. Zhang, and J. Zhu, "Multiplexed DNA detection based on positional encoding/decoding with self-assembled DNA nanostructures," *Chemical Science*, vol. 6, no. 2, pp. 930–934, 2015.

[2] Y. Wen, L. Li, L. Wang et al., "Biomedical applications of DNA-nanomaterials based on metallic nanoparticles and DNA self-assembled Nanostructures," *Chinese Journal of Chemistry*, vol. 34, no. 3, pp. 283–290, 2016.

[3] Y. L. Jia and H. Z. Gu, "Self-assembly and preparation of long single stranded DNA based on highly integrated sequence information," *Science Bulletin*, vol. 64, no. 10, pp. 28–37, 2019.

[4] Y. Zheng, Y. B. Yang, and Q. Yuan, "Design, assembly and application of nano functional materials based on DNA molecules," *Chemical Bulletin*, vol. 5, no. 80, pp. 6–14, 2017.

[5] Y. N. Zhang, L. H. Wang, H. J. Liu, and C. H. Fan, "Preparation of metal nanostructures based on DNA self-assembly and related nano photonics," *Journal of Physics*, vol. 66, no. 14, pp. 143–159, 2017.

[6] Y. J. Tang, S. Y. Dai, Y. T. Zhou, G. F. Cheng, H. E. Pin-Gang, and Y. Z. Fang, "Detection of miRNA-21 by a novel homogeneous electrochemical biosensor based on DNA template click chemistry and catalytic hairpin DNA self-assembly reaction," *Analytical Chemistry*, vol. 11, no. 7, pp. 1029–1034, 2019.

[7] X. R. Zhao, X. L. Wang, Y. Wang, Y. Qin-Zheng, and T. Xin-Jing, "Research progress of siRNA drug delivery based on nucleic acid self-assembled nanostructures," *Advances in Biochemistry and Biophysics*, vol. 46, no. 6, pp. 533–544, 2019.

[8] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 1, article 1850010, 2018.

[9] X. Zhang, C. Wang, and Z. Zheng, "An efficient chaotic image encryption algorithm based on self-adaptive model and feedback mechanism," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1785–1801, 2017.

[10] C. Xing and K. Wang, "Website information retrieval of web database based on symmetric encryption algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 1–12, 2021.

[11] B. Kılıç and V. Çelik, "Self-assembled growth of tandem nanostructures based on TiO_2 mesoporous/ZnO nanowire arrays and their optoelectronic and photoluminescence properties," *Applied Physics A*, vol. 119, no. 2, pp. 783–790, 2015.

[12] M. C. Brothers, D. Moore, M. St Lawrence et al., "Impact of self-assembled monolayer design and electrochemical factors on impedance-based biosensing," *Sensors*, vol. 20, no. 8, article 2246, 2020.

[13] F. Chen and Z. X. Yin, "DNA computing model based on vertex coloring of self-assembled nanoparticles," *Journal of Changchun University of Technology*, vol. 41, no. 4, pp. 127–130, 2018.

[14] L. Han, Z. Shen, C. Fu, and C. Liu, "Design and implementation of sound searching robots in wireless sensor networks," *Sensors*, vol. 16, no. 9, pp. 1550–1557, 2016.

[15] L. Hou and L. Yang, "Design and implementation of an industrial wireless sensor network for temperature monitoring," *International Journal of Online Engineering*, vol. 12, no. 3, pp. 82–85, 2016.

[16] B. Y. Song, L. Xu, and M. Y. Cao, "Design and implementation of ZigBee based wireless sensor and actuator networks in service robot intelligent space," *Applied Mechanics & Materials*, vol. 740, no. 4, pp. 161–164, 2015.

[17] W. Liu, S. Xu, X. H. Zhang et al., "Design and implementation of wireless sensor network system based on wireless HART," *Electronic Devices*, vol. 40, no. 4, pp. 868–874, 2017.

[18] X. Jiang, C. Xue, M. Ma, and G. Han, "Design and implementation of sensor nodes based on OFDM for underwater sensor networks," *Journal of Computer Science*, vol. 28, no. 5, pp. 293–302, 2017.

[19] W. Shen, Z. Liu, Z. Su, R. Su, and Y. Zhang, "Design and implementation of livestock house environmental perception system based on wireless sensor networks," *International Journal of Smart Home*, vol. 10, no. 5, pp. 69–78, 2016.

[20] M. F. Mosleh, R. A. Fayadh, and S. A. Hamid, "Design and implementation of wireless sensor network based on MATLAB interfaced with Arduino," *International Journal of Engineering and Technology*, vol. 9, no. 4, pp. 2871–2884, 2017.

[21] J. Qi and G. P. Liu, "Design and implementation of an indoor localization system based on wireless sensor networks and ultrasonic," *Kongzhi yu Juece/Control and Decision*, vol. 33, no. 8, pp. 1391–1398, 2018.

[22] J. Charoensuk, J. Thonglao, B. Wichaiyo et al., "A simple and sensitive colorimetric sensor for cadmium (II) detection based on self-assembled trimethyl tetradecyl ammonium bromide and murexide on colloidal silica," *Microchemical Journal*, vol. 160, no. 10, article 105666, 2021.

[23] A. Madani and S. Sedaghat, "Athermalization of a self-assembled rolled-up TiO_2 microtube ring resonator through incorporation of a positive thermo-optic coefficient material in planar bilayers," *Applied Physics B*, vol. 125, no. 12, pp. 123–125, 2019.

[24] P. Jane, R. Ilaria, N. Fabrizia et al., "Nanogravimetric and optical characterizations of thrombin interaction with a self-assembled thiolated aptamer," *Journal of Sensors*, vol. 12, no. 9, 8 pages, 2016.