

Journal Pre-proofs

Research on Data Transmission of Wireless Sensor Networks Based on Symmetric Key Algorithm

Wei Zhou, Ping Li, QinJu Wang, Narjes Nabipour

PII: S0263-2241(19)31321-1

DOI: <https://doi.org/10.1016/j.measurement.2019.107454>

Reference: MEASUR 107454

To appear in: *Measurement*

Received Date: 23 October 2019

Revised Date: 18 December 2019

Accepted Date: 22 December 2019

Please cite this article as: W. Zhou, P. Li, Q. Wang, N. Nabipour, Research on Data Transmission of Wireless Sensor Networks Based on Symmetric Key Algorithm, *Measurement* (2019), doi: <https://doi.org/10.1016/j.measurement.2019.107454>

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2019 Elsevier Ltd. All rights reserved.



Research on Data Transmission of Wireless Sensor Networks Based on Symmetric Key Algorithm

Wei Zhou^{a,*}, Ping Li^a, QinJu Wang^a, Narjes Nabipour^{b,*}

^a School of Internet of Things Technology, Wuxi Institute of Technology, Wuxi, 214121, China

^b Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam

Abstract: In order to improve the security and transmission efficiency of data transmission of wireless sensor networks, data transmission of wireless sensor networks based on symmetric key algorithm has been studied. Through detailed analysis of the communication model, it is found that the decryption mainly distributes the decryption password and obtains the decrypted secret key. The secret key and the ciphertext are grouped by the decryption function to finally obtain the ciphertext. The decryption algorithm is used to decrypt the ciphertext to realize the secure processing of the wireless sensor networks data. Also, experimental analysis shows that the minimum time required for the decryption and encryption of this method is 0.046ms and 2.146ms when the key length is 16. When adopting this method, the wireless sensor networks have high transmission quantity and long survival time, and the reliability of the transmitted data is up to 98.6%.

Keywords: Symmetric Key Algorithm; Wireless Sensor Networks; Data Transmission; transport protocols ; pseudo code

1 Introduction

Wireless sensor networks are composed of a large number of inexpensive micro sensor nodes deployed in the monitoring area, which is a multi-hop self-organizing network system formed by wireless communication [1]. It has attracted much attention in the international community, involving microwave sensors and micro-mechanics, communication, automatic control, artificial intelligence and many other disciplines. It integrates sensor technology, embedded computing technology, modern network and wireless communication technology, distributed information processing technology, etc. Its purpose is to collaboratively sense, collect, and process information about perceived objects in the network coverage area (such as light intensity, temperature, humidity, noise, vibration, and noxious gas concentrations and send them wirelessly to observers) [2]. Sensors, perceived objects, and observers form the three elements of a sensor network. If the Internet constitutes a logical information world and changes the way people communicate with each other, wireless sensor networks combines the logical information world with the objective physical world to change the way humans interact with nature [3].

People can directly perceive the objective world through sensor networks, thereby greatly expanding the capabilities of existing networks and the ability of humans to understand the world [4]. As an emerging technology, wireless sensor networks are receiving more and more attention from academic and engineering circles at home and abroad. It has shown broad application prospects in military reconnaissance, environmental monitoring, medical care, space exploration, smart home, industrial control and other commercial applications, and is considered to be one of the technologies that will have a huge impact on the 21st century. In the data transmission process of wireless sensors, data security is more important, so appropriate methods should be used to improve the security of wireless sensor transmission data [5].

A review of relevant literature found that Eschenauer and Gligor scholars proposed a

* Corresponding Authors:

Emails: zhou_wxit@163.com (W. Zhou) and narjesnabipour@duytan.edu.vn (N. Nabipour)

probability-based secret key allocation algorithm. On this basis, Pietro et al. give a random key pre-allocation algorithm, which is to randomly select a key subspace from a selected key space; a set of keys are randomly selected from the subspace to save it into the sensor nodes. After the network topology is formed, each node communicates with its neighbors, and then the public key is found and used as the encryption key. Based on this method, scholar Chan proposed a q -composite method in which the two communicating parties jointly have q keys to enhance network robustness. After the above analysis, the advantages of the symmetric key algorithm are more than the non-symmetric key algorithm. The symmetric key algorithm is a traditional cryptosystem, also known as a single-key cryptosystem. If the encrypted key of the cryptosystem is the same as the decrypted secret key, or one of them can be easily derived from any one of them, the cryptosystem is called the symmetric key cryptosystem [6]. It is characterized in that the encrypted key and the decrypted secret key are the same or essentially the same, and the key must be kept strictly confidential. This means that the security of the cryptographic communication system is completely dependent on the key. After the information of both parties of the communication is encrypted, it can be transmitted on an unsecured channel, but both parties must provide a safe and reliable channel when transmitting the key. The commonly used symmetric cryptographic algorithms are DES and 3DES developed by IBM in the United States, and IDEA and AES designed by Lai Xuejia. These are group ciphers, which have the ability to guarantee the security of encrypted messages when the details of the decryption are fully disclosed. Its calculation is small, the decryption speed is fast and the efficiency is high. But they are all based on the principle that a set of plaintext encryption can only get a set of ciphertext. In the last use of information, encryption can only contain one type of information, and only the entire content of this information can be obtained when decrypted. Therefore, the amount of information to be transmitted at a time needs to be increased, and for a specific use environment, it is not possible to provide different information without using branch judgment, that is, a judgment statement must be used to provide different information. In these respects, the traditional symmetric cipher is technically to be improved. At the same time, the analysis techniques for these block ciphers have also developed rapidly, such as differential cryptanalysis, linear cryptanalysis, and difference attack [7].

Based on the above analysis, in this paper, based on the symmetric key algorithm, two sets of plaintext and two sets of keys are used for encryption, which can increase the information transmission capacity of the same length ciphertext message by twice, and can effectively prevent exhaustive attacks. At the same time, it also provides a tamper-proof and inspection mechanism to achieve secure processing of wireless sensor networks data. On the basis of this, the data will be transmitted by data transmission protocol of wireless sensor networks, which can effectively improve the security of wireless sensor transmission data [8].

2 Materials and methods

2.1 Data encryption

2.1.1 The mathematical principle of symmetric key algorithm

The mathematical principle of the symmetric key algorithm is as follows: In the two-dimensional plane Cartesian coordinate system, the two-point coordinate is known to determine one straight line. This line has the certain slope k and intercept b , as shown in Fig. 1.

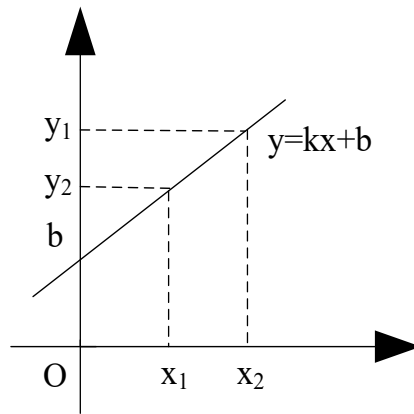


Fig. 1 Linear equation in two-dimensional plane Cartesian coordinate system

For this straight line with the known slope k and intercept b , the abscissa is given arbitrarily, and the corresponding ordinate can be obtained.

(1) Encryption

The given two sets of keys and plaintext (k_1, m_1, k_2, m_2) correspond to two point coordinates, and the simultaneous equations are as shown in equation (1).

$$\begin{cases} m_1 = k_1 A + B \\ m_2 = k_2 A + B \end{cases} \quad (1)$$

The slope A and intercept B are obtained. According to some reversible rule, A and B can be combined to form the ciphertext c .

(2) Decryption

From the received ciphertext c the slope A and intercept B are extracted to form the equation $m = Ak + B$ for determining one line; the key k_1 or k_2 is substituted into k to obtain the corresponding plaintext m_1 or m_2 . In the mathematical principle of the symmetric key algorithm, the slope and intercept of the line equation must be obtained from the two-point coordinates; on the contrary, in the case of the known line equation and the abscissa, the ordinate must be obtained. Then only meaningful horizontal coordinates can be used to get a meaningful ordinate; otherwise, no useful information can be obtained. In other words, the symmetric key algorithm can only provide security services for legitimate users who have keys [9].

2.1.2 Communication model of symmetric key algorithm

Based on the analysis of the principle of the symmetric key algorithm, the communication model of the symmetric key algorithm is studied. The communication model of the symmetric key algorithm is shown in Fig. 2.

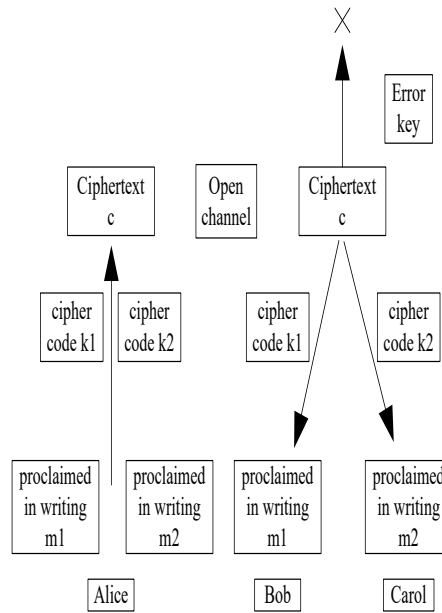


Fig. 2 Communication model

(1) The message sender Alice uses two different keys (k_1, k_2) at the terminal A to encrypt two different plaintexts (m_1, m_2) of arbitrary length, and finally obtains a ciphertext c .

(2) Ciphertext c is received from terminal A to terminal B through a public channel;
 (3) When the message receiver decrypts the ciphertext c at the terminal B , a different correct key is input to obtain one different correct plaintext, and only one set of plaintext can be obtained in a single decryption. If Bob enters the key k_1 , plaintext m_1 will be obtained. Carol enters the key k_2 , which can be obtained in plaintext m_2 . In other words, a decryption process can only get one set of plaintext.

(4) If the wrong key is entered at the terminal B , the decryption will fail [10].

2.1.3 The process of the encryption and decryption

Through the above analysis, it is found that the symbolic key algorithm is used for decryption and encryption in the most important communication model. The complete structure of the symmetric key algorithm is shown in Fig. 3. The left side of the dotted line is the encryption process and the right side is the decryption process.

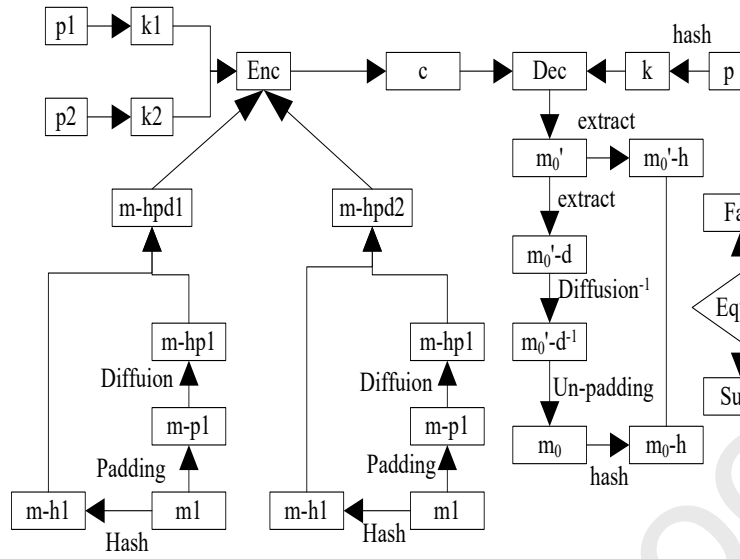


Fig. 3 complete structure of symmetric secret key algorithm

In the process of encryption, raw data is obtained from the sender of the message, such as plaintext m_1 and m_2 , and passwords p_1 and p_2 .

(1) Pre-processing the plaintext [11]. Use the hash function for plaintext 111 and get m_h1 after hashing. The plaintext 111 is filled to obtain m_p1 , and the m_h1 is diffused using m_h1 to obtain m_hp1 . Then put m_h1 in front of m_hp1 and connect to get m_hpd1 . Similarly, from m_h2 , m_p2 , m_hp2 and m_hpd2 are obtained.

(2) Pre-processing the password. The passwords p_1 and p_2 are hashed using the hash function, respectively, to obtain keys k_1 and k_2 .

(3) The pre-processed plaintext m_hpd1 , m_hpd2 and keys k_1 and k_2 are respectively segmented according to a certain packet length [12], and the ciphertext c is obtained by the encryption function.

In the process of decryption, the password p of the decryption is hashed and the decrypted secret key k is obtained. The ciphertext m_0' is obtained by the decryption function from k and ciphertext c . After m_0' -h and m_0' -d are extracted, m_0' -d is inversely diffused, and m_0' -d⁻¹ is obtained. Fill m_0' -d⁻¹ to get m_0 . m_0 is hashed to obtain m_0 -h. m_0 -h is compared with m_0' -h, and if they are equal, the decryption is successful. m_0 is the correct plaintext obtained by decryption. Otherwise, the decryption is a failure. Note that the above description is a packet plus decryption process, and then the ECB mode is used to expand the decryption of a packet to the encryption of arbitrary length data [13].

2.2 Data transmission of wireless sensor networks

2.2.1 Wireless sensor networks model

According to the above analysis, the security of data transmission of wireless sensor networks

can be significantly improved by using the symmetric key algorithm. Based on this, the transmission performance of the wireless sensor networks is further analyzed to improve the transmission performance of the wireless sensor networks. The transmission structure of wireless sensor networks should be analyzed first, and the transmission protocols of wireless sensor networks should be designed according to the transmission structure. The transport protocols of the wireless sensor-based are used to optimize the data transmission of the wireless sensor [14]. The transmission structure of wireless sensor networks is shown in Fig. 4.

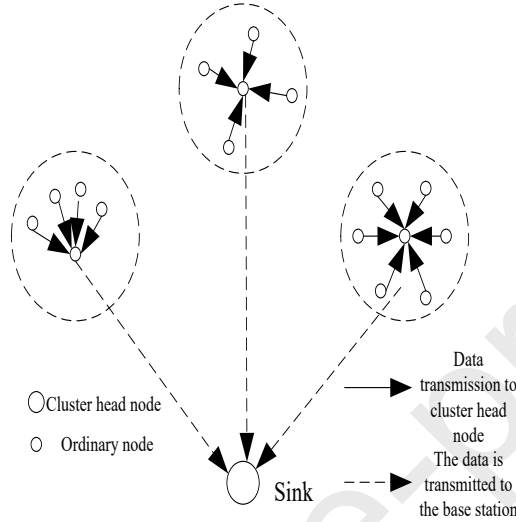


Fig. 4 Network structure of wireless sensors

In wireless sensor networks, there are three main parts of node energy consumption, namely sensor module, processor module and wireless communication module. The energy consumed to transfer 1 bit of data to 100 m is equivalent to the energy consumed to execute 3000 calculation instructions. The energy consumption of the processor module and the sensor module is a constant consumption, and the energy consumption model sets the energy consumption to a constant value P_{c+s} . When the distance that the wireless module transmits n -bit data is d , the power consumption of the transmitting and receiving of the RF module is:

$$\begin{cases} E_{Tx}(n, d) = E_{elec} \times n + \alpha_{amp} \times n \times d^k + P_{c+s} \\ E_{Rx}(n, d) = E_{elec} \times n + P_{c+s} \end{cases} \quad (2)$$

Where, E_{elec} indicates the energy consumed by the transmitting device and the receiving circuit for transmitting and receiving 1 bit of data, α_{amp} indicates the energy consumed by the transmitting amplifier to transmit 1 bit of data for 1 m², and k indicates the propagation attenuation coefficient, which is determined by the complexity of the surrounding environment.

During the communication of wireless sensor networks, the port of the sensor node includes two queues (data transmission queue and data storage queue). In the actual communication process, the energy consumption of data storage is much smaller than the energy consumption of data transmission [15]. Therefore, in this paper, the node consumption model of wireless sensor networks only considers the energy consumption during data transmission. Assume that in wireless sensor networks, X represents the transmitted signal, and the node receives the signal is:

$$Y = X + Z \quad (3)$$

where Z indicates Gaussian interference. Since the wireless sensor networks node is in communication, the data transmission and the transmission power of the signal are directly related. The data transmission of the wireless sensor networks can be optimized by adjusting the transmit power of the nodes [16]. Assuming that $p(t)$ represents the signal transmission power, then the channel instantaneous bit rate of the wireless sensor networks is:

$$r(t) = \frac{1}{2} \lg(1 + p(t)) \quad (4)$$

Time T is divided equally into $n + 1$ shares, denoted as S_i , and $i = 0, 1, 2, \dots, N$. The energy collected at S_i is recorded as E_i , and the corresponding transmission bit rate is recorded as r_i . The optimal formula for the maximum amount of data transmitted at the T is:

$$\begin{aligned} & \max_{p(t) \geq 0} \sum_{i=1}^{n+1} \int_{S_{i-1}}^{S_i} \frac{1}{2} \lg(1 + p(t)) dt, \\ & s.t. \quad (5) \\ & \sum_{i=1}^l \int_{S_{i-1}}^{S_i} p(t) dt \leq \sum_{i=0}^{l-1} E_i, l = 1, 2, 3, \dots, n + 1 \end{aligned}$$

2.2.2 Design procedure for the transport protocol

The wireless sensor networks data transmission is a bottom-up data upload and top-down command release process. The design method of the transport protocols is bottom-up. Starting from the data source, the complete data frame structure is set to realize the ZIGBEE network node communication mechanism and the remote network communication mechanism. The bottom-up data mainly includes command requests, data collection, routing tables, and neighbor tables. The primary problem in designing a data transfer protocol is to design the data frame structure and then design the processing module of the information protocol [17].

The data transfer protocol is developed by directly connecting the Uart interface with the computer serial port. This facilitates the computer to directly communicate with the ZIGBEE network and develop the data format of the serial communication. It also allows all actions of the ZIGBEE network to be controlled by command sending on the computer side. The ZIGBEE network information collected by the computer, combined with relevant theoretical knowledge, the inside story of the ZIGBEE protocol is recognized. Through the investigation of the routing table, combined with the routing algorithm in the relevant ZIGBEE protocol, the real routing situation of the ZIGBEE network is verified, and the routing table neighbor table and the collected data uploading function are implemented. The real ID in the ZIGBEE network is completely blocked in the computer serial port program because the network ID changes after each reset. In the upper computer application, the fixed physical address of each node is used as the label of the node to realize the mapping relationship between the network address and the physical address of the aggregation node. The manual control is removed from the serial port program of the computer, and the serial port event and the internal clock of the program are used to control the running of the program. The relay architecture of the data transmission system is designed. Local communication

includes: node wakeup notification, data collection request, neighbor table request, routing table request, acquisition data upload, neighbor table upload, routing table upload, resume request, and sleep request. The design process of the data transmission protocol of wireless sensor networks is as shown above. According to the above steps, the normality and stability of communication from the node to the host computer are guaranteed, and the scalability of the software program is realized.

2.2.3 Optimization strategy for data transmission

On the basis of satisfying the data transmission protocol of wireless sensor networks, it is assumed that the transmission power of the sensor node remains unchanged during the transmission process, and the constraint problem of equation (5) is transformed into the unconstrained optimization problem by the penalty function [19]. Then

$$F = \sum_{o=1}^{n+1} -\frac{L_i}{2} \lg(1 + p_i) - \sum_{i=1}^{N+1} m_j D_j \quad (6)$$

Where, m_j means the penalty factor, and D_j means the penalty. For any moment, all the energy of the sensor node is exhausted, then:

$$D_j = 0 \quad (7)$$

$m_j = 0$. For any moment, all the energy of the sensor node is not exhausted, then:

$$D_j = \lg\left(\sum_{i=1}^{j-1} E_i - \sum_{i=1}^j L_i p_i\right) \quad (8)$$

When $m_j < 0$, if $f(p_i) = -\frac{L_i}{2} \lg(1 + p_i)$, then:

$$F = f(p_{n+1}) + \dots + f(p_1) - m_1 \lg(E_0 - L_1 p_1) - \dots - m_{n+1} \lg(E_n + \dots + E_0 - L_1 p_1 - \dots - L_{n+1} p_{n+1}) \quad (9)$$

In the time T , all the energy of the sensor node is exhausted, then:

$$E_0 + \dots + E_n - L_1 p_1 - \dots - L_{n+1} p_{n+1} = 0 \quad (10)$$

According to the above two formulas, the formula shown below can be obtained:

$$F = f(p_{n+1}) + \dots + f(p_1) - m_1 \lg(E_0 - L_1 p_1) - \dots - m_n \lg(E_{n-1} + \dots + E_0 - L_1 p_1 - \dots - L_n p_n) \quad (11)$$

The formula is partial derivative and the following formula is obtained.

$$\frac{\partial F}{\partial p_n} = \frac{-L_n}{2(1 + p_n)} + \frac{L_n m_n}{E_0 + \dots + E_{n-1} - L_1 p_1 - \dots - L_n p_n} \quad (12)$$

When the amount of data transmitted by the wireless sensor networks is large and the transmission power tends to be constant, the amount of transmitted data is the largest [20], that is

$p_{n+1} = p_n$, and the equation (12) can be changed to:

$$p_{n+1}^* = p_n^* = \frac{2m_n + E_n}{L_{n+1} - 2m_n} (13)$$

From (9) to (13), the optimization formula for the transmit power of the wireless sensor can be obtained:

$$p_i^* = \frac{1}{\sum_{j \in i} \frac{2m_j}{\sum_{k=j+1}^{n+1} L_k P_k - \sum_{k=j}^n E_k}} - 1 (14)$$

3Results

In order to verify the effect of the data transmission method in this paper, actual analysis is needed. The analysis process uses Intel 2.8 GHz 4 core CPU, 4 G memory, 800 G hard disk, Windows XP operating system computer, and uses Matlab 2012R software to realize simulation test. The experimental object is the wireless sensor networks of a certain urban logistics. The simulation experiment parameters are shown in Table 1.

Table 1 Design of Simulation parameters

parameter name	short-cut process
Detection area size	100×100
Number of nodes	100
Sink position	-100,400
Node communication distance (m)	100
Node initial energy (J)	200
Data lange (byte)	521
Transmission energy consumption (J/bit)	50

In order to make the experiment more convincing, the method of this paper is compared with the data transmission method of wireless sensor networks based on non-symmetric key algorithm and data transmission method of the wireless sensor based on compressed sensing algorithm. The effectiveness of the proposed method is verified by comparing the three methods from multiple angles.

3.1Time and space occupancy

In order to analyze the time and data space occupied by the encryption and decryption in the data transmission process of wireless sensor networks, it is necessary to compare the time and data space required for the encryption and decryption of the three methods in different amounts of data. The comparison results are shown in the table.

Table 2 Comparison results

methods type	Secret key length	Encryption time/ms	Decryption time/ms	Occupy space (bit)
This paper methods	16	2.416	0.046	783
	32	2.428	0.048	791
	48	2.431	0.049	795

	64	2.439	0.051	801
	80	2.445	0.053	812
	96	2.457	0.055	819
	112	2.495	0.056	821
	128	2.512	0.059	824
	144	2.529	0.062	828
	160	2.524	0.069	836
	16	2.986	0.098	987
	32	3.012	0.101	995
	48	3.019	0.109	1001
Asymmetric secret key methods	64	3.024	0.112	1009
	80	3.028	0.118	1012
	96	3.037	0.121	1019
	112	3.041	0.128	1021
	128	3.049	0.134	1028
	144	3.052	0.137	1035
	160	3.059	0.142	1043
	16	5.126	0.179	1215
	32	5.139	0.184	1219
	48	5.142	0.198	1221
Compressed sensing methods	64	5.148	0.213	1228
	80	5.156	0.219	1230
	96	5.164	0.245	1237
	112	5.173	0.251	1244
	128	5.179	0.259	1254
	144	5.182	0.263	1263
	160	5.189	0.269	1269

As can be seen from Table 2, as the length of the key increases, the decryption and encryption times increase, and the space occupied by the decryption and encryption is gradually increasing. Under the same key length, the encryption time and decryption time of this method are significantly lower than the two comparison methods, and the space occupied by this method is significantly lower than the two comparison methods under the same key length. In the method of this method, when the key length is 16, the minimum time required for decryption and encryption is 0.046ms and 2.146ms, and the minimum occupied space is 783bit. That is, the decryption and encryption performance of this method is better, and it is suitable for application to actual the transmission of the wireless sensor networks.

3.2 Energy consumption analysis

In order to verify the energy consumption of the wireless sensor during data transmission, it is necessary to compare the energy consumption of the three methods under different data quantities. The comparison results are shown in Table 3.

Table 3 Results of comparative analysis of energy consumption

Transmission data	This paper methods/J	Asymmetric secret key methods/J	Compaction methods/J
16	318.62	399.81	468.76
32	319.46	398.76	469.52
48	325.68	401.52	470.31
64	324.36	406.98	474.68
80	320.57	410.37	472.56
96	321.96	412.49	479.31
112	327.48	416.79	481.24
128	328.92	418.52	483.62
144	329.73	419.63	486.78
160	330.12	420.56	487.69

As can be seen from Table 3, as the amount of data transmitted by wireless sensors continues to increase, the energy consumed by the three methods is also increasing. Comparing the three methods, the energy consumed by the method is lower than the two comparison methods under the same amount of transmitted data. The minimum energy consumed by this method is 318.692J. With the method of the present invention, the energy consumption of the wireless sensor networks can be significantly reduced during the transmission of data.

3.3 Analysis of the total amount of data transmission

In order to study the total amount of data transmitted by the wireless sensor networks under the proposed method, it is necessary to compare the total amount of data transmitted by the wireless sensor networks under the three methods. The comparison results are shown in Fig. 5.

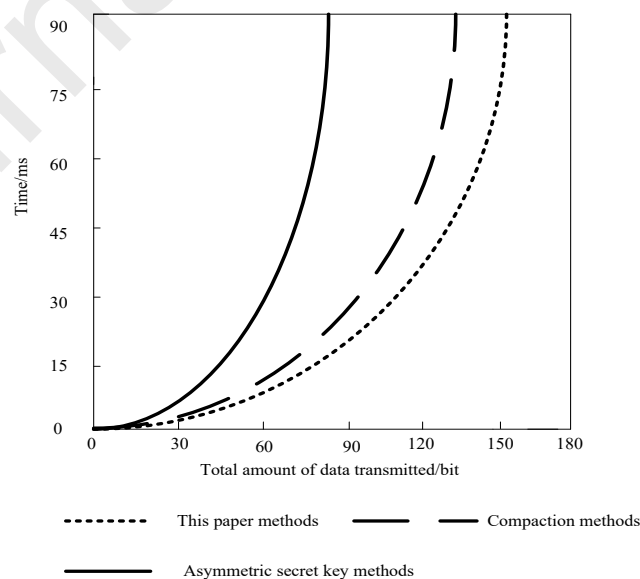


Fig. 5 comparison of the total amount of transmitted data

As can be seen from the figure, the total output data of wireless sensor networks is increasing

with time. Compared with the two comparison methods, the total amount of data transmission of the wireless sensor networks under this method is faster, and the total amount of data transmitted is larger. After theoretical analysis, this paper has optimized the logistics data transmission strategy of wireless sensor networks. Wireless sensors continuously acquire energy in the environment and maximize the wireless sensor transmission by introducing a penalty function. The two comparison methods consume all of the acquired environmental energy in the middle stage of data transmission of the wireless sensor networks, which results in lower transmission power and less data transmission of the wireless sensor nodes. After the above analysis, the method mainly introduces a penalty function to dynamically optimize the energy utilization of wireless sensor nodes, ensure the amount of data transmitted by the sensor nodes, and finally increase the total amount of data transmitted by the nodes.

3.4 Comparison of the survival time of wireless sensor networks

After analysis, it is found that there is a certain relationship between the lifetime of wireless sensor networks and the amount of data transmitted. Therefore, the lifetime of wireless sensor networks under this method needs to be analyzed. The lifetime of wireless sensor networks was analyzed by node mortality. The curves of node mortality for the three methods were compared and the results are shown in Fig. 6.

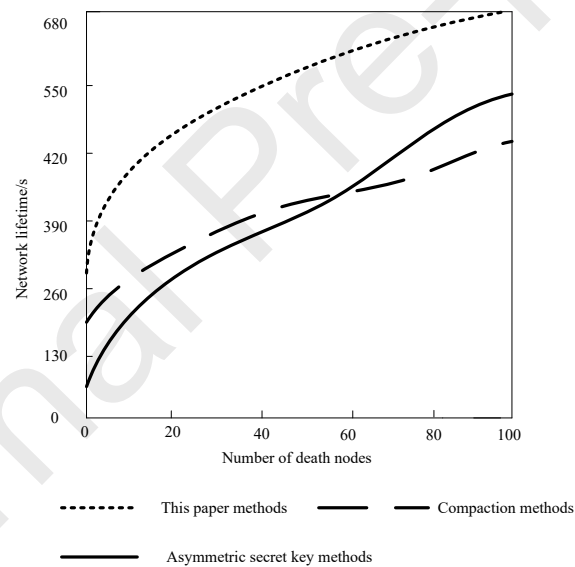


Fig. 6 comparison of lifetime of wireless sensor networks

It can be seen from the figure that compared with the two comparison methods, the network lifetime of this method is relatively long, which is mainly due to the introduction of the penalty function. It adjusts the energy consumption of each node to extend the living space of a single node, thereby prolonging the lifetime of the entire wireless sensor networks and transmitting more data.

3.5 Reliability Analysis

In order to study the security of wireless sensor data transmission under this method, it is necessary to compare the transmission reliability of the three methods in the non-transmission path. Turn off the password visibility function on the login system of a company and set it to be invisible. Then introduce the method designed in this paper and other methods, and test repeatedly and compare the actual effect of these methods. The analysis results are shown in Fig. 7.

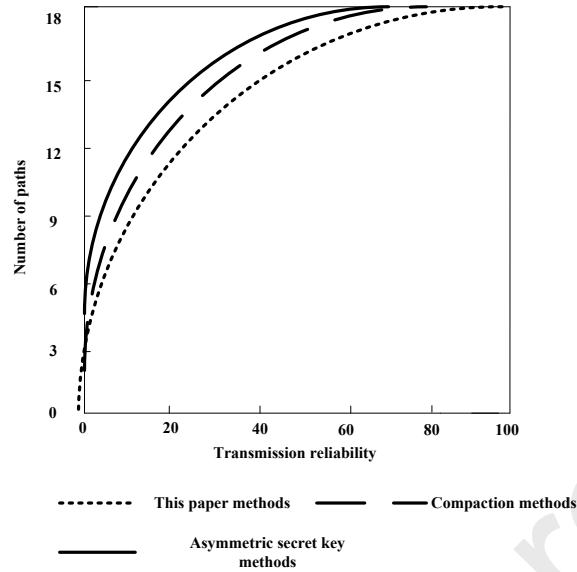


Fig. 7 results of reliability analysis

As can be seen from Fig. 7, as the number of paths continues to increase, the reliability of data transmission of wireless sensor networks is also increasing. Compared with the two comparison methods, the data transmission reliability of this method is higher than the two methods. The reliability of data transmission in this method is up to 98.6%, while the highest reliability of data transmission in the two comparison methods is 80.1% and 76.4%, respectively. That is, the wireless sensor networks data transmission of the method has the highest reliability.

4Discussion

Through theoretical analysis, the symmetric key algorithm used in this method is different from the asymmetric encryption algorithm. The comparison found that the key algorithm of this paper has different variables input during the encryption process. The symmetric key algorithm uses two plaintext and two passwords to generate a ciphertext during the encryption process. That is, there are 4 inputs in total. In the decryption process, one key is used at a time, and the corresponding plaintext (one of the two plaintexts) is solved. All the partitions of the symmetric key algorithm in the decryption process are the same, and are all divided into groups in Lbit units. The definition of a group's decryption is expanded into the decryption of arbitrary length data, and the pattern is the same. The key distribution in the decryption process is the same. The padding and spreading in the encryption process are the inverse of the de-filling and de-spreading of the decryption process, respectively. Comparing the decryption process of the symmetric key algorithm with the decryption process of the non-symmetric key algorithm, the order of the two algorithms is reversed in terms of the use of key algorithms. The decryption process is one step more than the authentication process. Whether the decryption succeeds needs to be verified, this is achieved by comparing the hash values of the plaintext before and after the decryption.

The symmetric key algorithm used in this method has many advantages. With the symmetric key algorithm, the amount of information transmitted increases exponentially. In the case of the same length ciphertext, the ciphertext obtained by encrypting using the symmetric key algorithm can contain double-information plaintext. At the same time, the symmetric key algorithm provides a mechanism for selectively unlocking plaintext, and this selectivity does not need to be

implemented by any branch judgment statement. It is difficult for an attacker to find that the decryption process is controlled by a dual key, which greatly increases the difficulty of the attack. It provides the tamper-proof mechanism that increases the guarantee of integrity.

Since there is double plaintexts in the symmetric key algorithm, the decryption is controlled by the dual key. Therefore, if the attacker wants to get all the content, the two correct keys must be input in order to obtain the plaintext. The difficulty of the attack can be at least squared. Excluding the preprocessing of plaintext, ciphertext, and keys, the encryption sub-algorithm and the decryption sub-algorithm have small time complexity. Using the key algorithm of this paper can significantly improve the security of data transmission of wireless sensor networks. Therefore, in the wireless sensor networks, the transmission key can be encrypted and decrypted using a symmetric key algorithm. On this basis, in order to extend the service life of wireless sensor networks and improve the effect of data transmission, the wireless sensor networks model needs to be analyzed. According to the wireless sensor networks model, a data transmission protocol of wireless sensor networks is proposed. On the basis of fully considering the data transmission protocols, the data transmission optimization model of the sensor nodes is used to optimize the data transmission, which reduces the energy consumption in the transmission process of the sensor network data.

5 Conclusions

When using symmetric key algorithm for encryption, it is fast, efficient, and has low requirements on key length. It is widely used in data encryption. Therefore, the proposed method uses the symmetric key algorithm to encrypt the data in the wireless sensor networks, which improves the integrity of the data encryption, the tamper-proof modification, and the expansion of information transmission. The symmetric key algorithm is proposed in this paper. On the one hand, it does not use judgment statements, it uses double keys to achieve feedback of different information; on the other hand, it increases the amount of information in plaintext while improving the difficulty of violent exhaustion. The symmetric key algorithm is used to encrypt the data in the wireless sensor networks to improve the security of the data. At the same time, the wireless sensor networks model is launched, and according to this model, the transport protocols of wireless sensor networks are proposed. The data in the wireless sensor network is transmitted according to the protocol to improve the security of data transmission of the wireless sensor networks. The experimental analysis shows that the proposed method requires less time for encryption and decryption, and the total amount of data transmitted is larger. Therefore, the data in wireless sensor networks can be transmitted by this method.

6. Acknowledgement

Natural Science Research Project of Jiangsu University (No. 18KJB520048).

Reference

- [1] Shu, J., Liu, S., Liu, L. 2017. Research on Link Quality Estimation Mechanism for Wireless Sensor Networks Based on Support Vector Machine. *Chinese Journal of Electronics* 26,377-384.
- [2] Sun, Y., Dong, W., Chen, Y. 2017. An Improved Routing Algorithm Based on Ant Colony Optimization in Wireless Sensor Networks. *IEEE Communications Letters* 21, 1-1.
- [3] Wang, H., Yang, G., Xu, J. 2016. A Reliable Data Transmission Protocol Based on Multipath Routing for Wireless Sensor Networks. *Sensor Letters* 14, 923-927.
- [4] Tan, Q., An, W., Han, Y. 2016. Achieving Energy - Neutral Data Transmission by Adjusting Transmission Power for Energy - Harvesting Wireless Sensor Networks. *Wireless*

Communications & Mobile Computing16, 2083-2097.

[5] Peng, L., Yu, X., He, X. 2017. Research on Secure Localization Model based on Trust Valuation in Wireless Sensor Networks. *Security & Communication Networks*2017, 1-12.

[6] Yan, S., Zhang, M., Zhao, X. 2017. Refractive Index Sensor Based on a Metal–Insulator–Metal Waveguide Coupled with a Symmetric Structure. *Sensors*17, 28-79.

[7] Xie, P.S., Wang, Q., Fu, T.X. 2017. An Energy Saving Data Compression Algorithm Based on Wireless Sensor Network. *Journal of Computational & Theoretical Nanoscience*14, 3356-3358.

[8] Bouaziz, M., Rachedi, A. 2016. A Survey on Mobility Management Protocols in Wireless Sensor Networks Based on 6lowpan Technology. *Computer Communications*74, 3-15.

[9] Ghadi, M., Laouamer, L., Moulahi, T. 2016. Securing Data Exchange in Wireless Multimedia Sensor Networks: Perspectives and Challenges. *Multimedia Tools & Applications*75, 3425-3451.

[10] Wu, J., Chen, Z. 2016. Data Decision and Transmission Based on Mobile Data Health Records on Sensor Devices in Wireless Networks. *Wireless Personal Communications*90, 2073-2087.

[11] Lalos, A.S., Antonopoulos, A., Kartsakli, E. 2016. RLNC-Aided Cooperative Compressed Sensing for Energy Efficient Vital Signal Telemonitoring. *IEEE Transactions on Wireless Communications*14, 3685-3699.

[12] Militano, L., Erdelj, M., Molinaro, A. 2016. Recharging Versus Replacing Sensor Nodes Using Mobile Robots for Network Maintenance. *Telecommunication Systems*63, 1-18.

[13] Xu, G.X., Wu, Q., Daneshmand, M. 2016. A Data Privacy Protective Mechanism for Wireless Body Area Networks. *Wireless Communications & Mobile Computing*16, 1746-1758.

[14] Zhou, X., Rezki, Z., Alomair, B. 2016. Achievable Rates of Secure Transmission in Gaussian MISO Channel with Imperfect Main Channel Estimation. *IEEE Transactions on Wireless Communications*15, 4470-4485.

[15] Qiao, J.F., Niu, J., Ma, G. 2018. Research on Wireless Sensor Network Coverage Detection Simulation in Resource Optimization. *Computer Simulation*35, 429-433.

[16] Sun, G.X., Zheng, X.Y., Gao, J.H. 2018. Study on the Method of Measuring the Temperature of the Li-ion Battery of the Electric Vehicle. *Chinese Journal of Power Sources*42,43-45.

[17] Wang, T., Liu, Q.F. 2018. Application of High-Frequency Injection Response in IPMSM System with No-Position Sensor by Pure Time-Delay Filter. *Journal of Power Supply*16, 125-134.

[18] Gao, G.F., Yang, S.C., Yang, K.K. 2019. Study on Chain Reaction of Thermal Runaway Explosion of Lithium Ion Battery. *Automation & Instrumentation*231,8-9.

[19] Luo, H., Zhong, J.J., Li, X. 2019. Single Color Image Enhancement Algorithm Based on Improved Multi-scale Retinex. *Journal of Jilin University (Science Edition)*57,185-190.

[20] Xu, H., Wang, H., Yang, Y.X. 2019. The Exploration of Social Security Prevention and Control System Based on Military - Civilian Integration Collaborative Innovation. *Journal of China Academy of Electronics and Information Technology*14,79-83+96.

Cover Letter

Dear Editor

Please find the enclosed our revised paper entitled “ **Research on Data Transmission of Wireless Sensor Networks Based on Symmetric Key Algorithm**” for possible publication in your journal:

To qualify for authorship of the submitted manuscript, every of the listed authors have made substantial intellectual contributions both to the research and to its preparation. Especially regarding the latter, the authors be involved in activities related to the following categories:

1. Substantial contribution to the conception, research, data acquisition and analysis/interpretation;
2. Collaboration in the preparation/revision of the submitted manuscript
3. Participation in reaching the approval for the publishable manuscript version;
4. Ensuring a proper explanation to possible questions that could be raised regarding accuracy and scientific integrity of the submitted manuscript.





The corresponding author confirm that all the authors of the manuscript fulfill the criteria of authorship as given above, as well as that there is no one else who could claim to be the (co-) author of the submitted manuscript.

By submitting this form, the corresponding author accepts responsibility for having properly included all co-authors of the submitted article. No one else should have contributed in a meaningful and substantial way to its intellectual content.

The list all authors of the manuscript in the table given below and designate their respective contribution(s).

AUTHORS:

Wei Zhou, Ping Li, QinJu Wang, Narjes Nabipour

Author Name	Research Conception/ Design	Data Acquisition	Data Analysis/ Interpretation	Manuscript Preparation	Final Approval	Signature
Wei Zhou	■			■	■	
Ping Li		■	■		■	
QinJu Wang			■	■		
Narjes Nabipour				■	■	

Corresponding Authors

[21]

Highlights

- The decryption algorithm is used to decrypt the ciphertext.
- Using penalty function to optimize node energy consumption during data transmission
- Improving the security and data transmission efficiency of wireless sensor

[22]

Conflict of interest

The authors declare that there is no conflict of interest regarding publication of this paper.

[23]

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

[24]