Wireless Sensors Lightweight Encryption Project
Implementation and Application

Bei HONG*, Xue-peng JIANG, Kang-kang BAO and Jia CUI
Naval Aeronautical and Astronautical University, Yantai Shandong 264001, China
*Corresponding author

Keywords: Wireless Sensor Networks, Lightweight, Integer grouping encryption algorithm.

Abstract. In order to guarantee Wireless Sensor Networks communications security, a variety of secure protocol had been widely followed. While currently tradition networks established secure protocol, such as IPSec, SSL and traditional ad hoc wireless network project, are under the limit of sensor node computing resource and energy. They are not appropriate to apply to Wireless Sensors. This article used integer grouping encryption algorithm. The encryption algorithm had high safety and low consumption. Experiment indicated this encryption algorithm consume lower, execute faster and have high safety, comparing to AES and so on. And this Encryption Project can meet internetwork communication safety demand under the gradually sever secrecy circumstance.

Introduction

With the rapid development of wireless sensor network technology, wireless sensor network with low cost, low power consumption, multi function (Wireless Sensor, Networks, WSN) has been used in military defense, intelligence Home Furnishing, environmental monitoring, health data collection etc.. However, the classical encryption algorithm used in WSN such as AES, SkipJack etc. a lot of the replacement table, with less energy, low computing ability, limited storage resources WSN is not the ideal solution, identity authentication and WSN authentication algorithm is mostly ignored or high power consumption, easy to crack, the application of these problems the WSN have a greater threat.

To solve these problems, a lightweight communication encryption method suitable for wireless sensor networks is implemented and validated in this paper. Using a wireless sensor node to realize data communication between the encryption block encryption algorithm based on integer chaos, the algorithm saves a lot of replacement table, and has the advantages of high safety and low power consumption, the balance of security and power consumption of wireless sensor this contradiction. Experimental results show that the algorithm has the advantages of less resource consumption, high execution efficiency and high security. The wireless sensor network constructed by the algorithm can be applied to smart home, wireless IP camera, environmental monitoring and other aspects, and push the integration of animal networking technology and real life.

Block Encryption Algorithm based on Integer Chaos

The Principle of Block Encryption Algorithm Based on Integer Chao

The block cipher algorithm based on integer chaos adopts a basic structure of 8 bit Feistel, and its structure is shown in Figure 1. A group of plaintext is divided into high and low 4 bit, respectively. Under the action of round key, a new Feistel operation is completed by generating the row after the function and xor.
The Feistel structure shown in Figure 1 can be represented as

\[
\begin{align*}
L_i &= R_{i-1} \\
R_i &= L_{i-1} \oplus F
\end{align*}
\]  

(1)

The lengths of $R_i$, $R_{i-1}$, $L_i$, $L_{i-1}$, $F$ are 4 bit.

The function $f$ is 8 bit integer chaotic iteration, and its structure is shown in figure 2. $R_{i-1}$ was first expanded from 4 bit to 8 bit, with the same round key XOR 8 bit, input to the function of Chaos for 8 bit integer chaotic iterative, 8 bit iterative output values were again divided into high and low 4 bit are generated the final output $F$ after XOR.

The Chaos function receives the input $Z_i$ and iterates, $Z_{i+1}$ is outputs of the Chaos function. The intermediate output $F$ of each wheel is related to the input $R_{i-1}$ and current wheel keys $k_i$, and the nonlinearity of the 8 bit integer chaos can improve the security of the encryption wheel.

The complete 8 bit block encryption process is shown in Figure 3.

In the plaintext group into the round before encryption, first 8 bit data P replacement, complete preliminary diffusion. The number of wheels in the encryption process is variable, like the general Feistel structure block encryption, the last round does not perform the left and right interaction steps. Once the round encryption is completed, the 8 bit data is replaced again by P. This encryption process has the same structure as the decryption process, and only the encrypted sub key sequence can be used in reverse order to form the corresponding decryption operation. When encryption is used, 4 wheel keys $k_1$, $k_2$, $k_3$, $k_4$ are used sequentially, and then the correct sub keys $k_4$, $k_3$, $k_2$, $k_1$ are used in decryption.
After the text input and the ciphertext output, 8 bit P replacement should be called for the conventional diffusion effect. The replacement structure is shown in Figure 4.

P substitution can be simplified as

\[
\begin{align*}
    b_0 &\leftrightarrow b_6 \\
    b_1 &\leftrightarrow b_3 \\
    b_2 &\leftrightarrow b_5 \\
    b_4 &\leftrightarrow b_7
\end{align*}
\]

The zero bits and the six bits are interchangeable; 1 bit bit and 3 bit bit swap; Number 2 bit and bit number 5; The number 4 bit is interchangeable with the 7 bit bit.

**Performance Analysis of Packet Encryption Algorithm Based on Integer Chaos**

In the encryption process, the system security can be guaranteed because of the complex chaotic sequence as the sub-key of the wheel encryption. In addition, the number of keys can be increased by increasing the number of Feistel structures to further improve security.

For example, four rounds of encryption are used, and four rounds of subkeys are required. The length of each sub-key is 8 bits. The encryption of a single packet requires 32 bits of key. A single iteration of a composite chaotic system produces a random sequence of 32 bits, which can be used to provide the subkeys needed for four rounds of encryption. This scheme USES a chaotic mapping...
iteration to add and decrypt a clear text grouping, which can effectively improve the efficiency of encryption operation under the premise of guaranteeing the security of the password system.

Because the classical encryption algorithms such as AES, SkipJack heavily used the replacement list, so in the software algorithm, high requirements for hardware stores, seriously affect the operation performance of sensor nodes, and 8 bit data of the displacement of simple structure, without complex replacement list, more suitable for the sensor node storage resources are limited.

The Implementation of Packet Encryption Algorithm Based on Integer Chaos

In this paper, CC2530 communication module is selected as an example to carry out the programming, and the program language is C. With the support of a variety of micro platforms, including 8051, MSP430, AVR and many ARM devices, this design theoretically can be extended to other chips. This paper only takes CC2530 as an example to implement and test.

The program code is divided into the encryption part, the decryption part and the function three parts. Will write good program code loaded in the form of application in Contiki embedded operating system, the input to generate the hex file's instructions, and the generated hex file burn to CC2530 module, implementation CC2530 encrypted communication module, as shown in Figure 5.

In this experiment, in order to facilitate observation CC2530 encrypted communication module, using serial debugging assistant to display of data encryption, specific test equipment as shown in Table 1, Table 2, the test project as shown in Table 3.

![Figure 5. The CC2530 module realizes encrypted communication.](image)

### Table 1. PC test equipment.

| project          | configuration                  |
|------------------|--------------------------------|
| PC               | Intel core i5 2.0GHz           |
|                  | 8GB                            |
|                  | Windows 7                      |
|                  | Standard USB2.0 interface      |

### Table 2. Development board test equipment.

| project                | configuration                                           |
|------------------------|---------------------------------------------------------|
| CC2530 development board| 2.4 GHz IEEE 802.15.4 compatible RF transceiver        |
|                        | 8051 microcontroller kernel 8 KB RAM                    |
|                        | 5 channel DMA function hardware supports CSMA/CA        |

### Table 3. Test items.

| test items                                                                 | expected result                                   |
|---------------------------------------------------------------------------|---------------------------------------------------|
| Start the sending device, send the data encrypted, send the encrypted data from the transmitter. | The serial debugging assistant displays the plaintext before encryption |
| Start the information receiving device to detect the received data (close the ciphertext decryption program) | The serial debugging helper displays encrypted data |
| Open the cipher decryption program to detect the received data              | The serial debugging helper displays the decrypted data |
Analysis of the Results of Communication Encryption Module

This paper measured the DESXL XTEA, HIGHT, DES, the PRESENT, LBlock and chaotic encryption algorithm based on integer cipher algorithm is applied to the same sensor, this paper adopts CC2530 communication module of speed and power consumption performance, specific experimental data as shown in Table 4.

Table 4. Running speed and power consumption table.

| Cryptographic Algorithm | Key Length/Bit | Space Usage /Bit | Running Speed /kbps@100Khz | Power Dissipation /mW |
|-------------------------|---------------|------------------|--------------------------|----------------------|
| XTEA                    | 128           | 872.5            | 57.1                     | 45.43                |
| HIGHT                   | 128           | 762.0            | 188.2                    | 48.32                |
| DES                     | 56            | 575.5            | 44.4                     | 33.44                |
| DESXL                   | 184           | 542.0            | 44.4                     | 32.39                |
| PRESENT                 | 80            | 392.5            | 200.0                    | 22.57                |
| LBlock                  | 80            | 330.0            | 200.0                    | 21.36                |
| Chaotic Encryption      | 32            | 300.0            | 210.0                    | 17.09                |

The algorithm encryption system of this work is compared with XTEA, HIGHT, DES, DESXL, PRESENT and LBlock and other lightweight algorithms. The following conclusions are drawn:

1. The key length of DESXL is the longest, which is 184 bits, although the security is sufficient but the encryption time is too long; DES key length is the shortest, only 56 bits, which leads to the low security of DES algorithm. The key length of the LBlock algorithm is 80 bits, and the encryption and decryption is faster. And the packet encryption algorithm based on integer chaos is small, no replacement box, and faster.

2. Compared with six other lightweight encryption algorithms, the integer chaotic packet encryption algorithm takes up the smallest space and the smallest space complexity.

3. Because of all the advantages above, the packet encryption algorithm based on integer chaos consumes the lowest power consumption in the same encrypted condition, only 17.09 mW.

In grouping encryption algorithm based on integer chaos are analyzed in detail and the other its lightweight algorithm parameters is conducted it's discovered that DESXL algorithm in order to ensure adequate safety such as the key length is longer, and this paper USES the chaos algorithm generate the key, the key length is small, but the security high, difficult to break, and running speed, low consumption. Therefore, it is a better one of all the current lightweight cryptographic algorithms.

Conclusion

This article mainly aims at the shortcomings of classical encryption algorithm, in order to meet the WSN nodes with less energy, low computing power and storage resources limited features, such as using the grouping encryption algorithm based on integer chaos to encrypt information, and improves the security and computing speed, reduce the power consumption, effectively improve the performance of the security of wireless sensor network, to meet the current increasingly serious confidential form under the condition of the requirement of wireless sensor network communication, can be applied to safety degree requirements higher intelligent household, industrial and agricultural control, biological, medical, environmental monitoring, hazardous area wireless sensor communication fields such as remote control, has a broad application prospect.

References

[1] Leeea. Cyber Physical Systems: Design Challenges[R].University of California, Berkeley Technical Report.

[2] Chen ti-ming. Lightweight cryptographic algorithms and protocols for wireless sensor networks [M]. Beijing: people's post and telecommunications press, 2013.
[3] Stajanof, Anderson. The resurrecting duckling: security issues for ad-hoc wireless networks[A]. Proceedings of the 7th International Workshop on Security Protocols[C]. Springer-Verlag London, 2000.172-182.

[4] Karlh, Williga. Protocols and Architectures for Wireless Sensor Networks[M]. Chichester. John Wiley & Sons, 2005.

[5] Chens, Zhongxx, Wuzz. Chaos block cipher for wireless sensor network[J]. SciChina Ser F-Inf Sci, 2008,51(8):1055-1063

[6] Niels Provos and David Mazieres. A Future-Adaptable Password Scheme[J].

[7] Zhang xin. Research progress of wireless sensor networks [J]. Information systems engineering, 2016(4):16-16.

[8] Cheng yinbo, si jing, et al. Application of hierarchical distributed compression sensing for wireless sensor networks [J]. Journal of electronic and information technology, 2017, 39(3):539-545

[9] "To feng hong, kong qing equality. Based on ZigBee's low-power wireless sensor network improvement protocol [J]. Sensor and microsystem, 2017(3):33-35

[10] "The research progress of wireless sensor network user authentication protocol [J]. Journal of network and information security, 2017 (1).