An enhanced encryption algorithm with key update scheme for Internet of Things

Hong Chen*
Big Data School, Chongqing Vocational College of Transportation, No.69, Xuefu Road, Chongqing 402247, China

*chen_honghit@163.com

Abstract. The protocols in the Internet of Things are more complex than the Internet. Once the Internet of Things devices have security problems, it will lead to a decline in user experience and huge economic losses. Therefore, this paper proposes a secure communication scheme for the Internet of Things based on a dynamic key update mechanism. This paper uses a variety of chaotic equations with good random characteristics to generate the session key library, and then uses the lightweight symmetric encryption algorithm Present-80 to encrypt the communication data. The simulation test results show that under the condition of ensuring communication efficiency, the security communication protocol of the Internet of Things based on the dynamic key update mechanism proposed in this paper has higher security.

Keywords: Internet of things security, key update, Present encryption algorithm, Internet of things transmission

1. Introduction
Since the development of the Internet of Things, its security incidents have also occurred frequently. For intruders, attacking the IOT system can cause greater attention or gain more benefits [1]. Therefore, IOT communication security technology has become a hot issue to be solved urgently. Lightweight identity authentication is a key technology to improve resource-constrained IOT devices. Its purpose is to establish a shared session key for confidential communication and can selectively provide confidentiality and integrity of communication data.

The hierarchical structure of the Internet of Things can be divided into three layers from bottom to top. Xu et al [2] proposed the PSAP owing to the lack of a secure authentication mechanism for NFC applications. Although PSAP is slightly more expensive, it has better privacy and higher security compared with other protocols. Reference [3] adopted a Neuro-Fuzzy method on the basis of trust management model in order to guarantee safe and credible data transmitted in IoT devices. The simulation results in NS2 also verify the validity and reliability of the TMM model. Reference [4] used Bayesian learning methods to score the trustworthiness of IoT entities considering trusted access mechanism of IoT devices and proposed a trust computing model combining the trustworthiness of entities and data. Experimental data demonstrated that the proposed scheme can evaluate and calculate the credibility of entities and data more accurately and can provide a better access control method for IoT devices.
Lightweight block cipher is a special block cipher system with lower implementation cost and lower energy consumption. It is mainly used in resource-constrained computing environments. The typical structure of block cipher includes Feistel structure and SPN structure. With the rapid development of the Internet of Things, IOT terminal sensor components are widely deployed and the demand for lightweight cryptosystems is increasing.

2. Secure communication scheme Design for IOT based on dynamic key update mechanism

2.1. The overall design of the IOT secure communication scheme

The IOT secure communication scheme proposed in this paper is divided into two stages. The first stage is the interaction between the IOT client and the server to determine the secure communication session key, and the second stage is the confidential communication between client and the server using definite communication session key. The specific protocol process is shown in Fig. 1.

![Fig. 1 Secure communication process](image)

Step 1: The IOT client and the Server generate the same key library from the chaos equation in this article, and each key has a consistent number. The client will send a communication encryption request to the server. The request contains the key number randomly selected by the client and the supported encrypted communication algorithm.

Step 2: After receiving the client request, the server will return a response message in which the server determines the protocol version and adopted encryption algorithm type.

Step 3: After receiving the response message from the server, the client uses the selected key to call the determined communication encryption algorithm, and sends the data to server in cipher text.

Step 4: After receiving the ciphertext message from client, the server determines the decryption key from the key library according to the key number and calls the corresponding decryption algorithm to decrypt the received data and completes the entire secure communication process.

2.2. The Design of key library generation algorithm

The key in the key library is randomly generated by a random number generator, stored in the chip directly and kept by both parties in communication. The use process is illustrated in Fig. 2.

In this paper, the Coupled Map Lattice model (1) and the corresponding local mapping chaos equation (2) are used as pseudo-random number generators where \( \varepsilon \in [0,1] \) is the coupling strength coefficient, \( \gamma \in [10,100] \) is as the adjustment coefficient of the local mapping equation (2). When using equations (1) and (2) to generate the key library, the IOT client and server have the same initial key \((\varepsilon, \mu, \gamma)\).
2.3. Implementation of the Lightweight Encryption Algorithm Present-80

Lightweight cryptographic algorithms are widely present in the entire Internet of Things. The PRESENT [5] algorithm is simpler in implement than other cryptographic algorithms. It adopts SPN structure and the input is 64 bits, the number of iteration rounds is 32, and the key is 80 or 128 bits. The hardware implementation of PRESENT-80 algorithm only needs 1570GE and its proposal is of great significance in the research and development history of lightweight cryptography.

The structure of the PRESENT encryption algorithm is shown in Fig. 3. Each round of the input of the PRESENT algorithm must be XORed with the 64-bit subkey $K$. The confusion layer in the PRESENT algorithm consists of 16 identical 4-input and 4-output S-boxes which is revealed in Table 1. For the S box of the PRESENT algorithm, its differential uniformity is 4, and its linear uniformity is 8 which makes the differential and linear characteristics of the algorithm the best. The operation of the diffusion layer of the PRESENT algorithm is shown in formula (3).

$$x_{n+1}(i) = (1 - \varepsilon) \cdot f(x_n(i)) + \frac{\varepsilon}{2} \left[ f(x_n(i-1)) + f(x_n(i+1)) \right]$$  \hspace{1cm} (1)

$$f(x_n) = \left[ \mu \times x_n \times (1 - x_n) + \gamma \times x_n \right] \text{mod} 1$$  \hspace{1cm} (2)

Fig. 2 The principle of using the key store

Fig. 3 The encryption process of the PRESENT algorithm
3. Results

3.1. The establishment of simulation model
The overall network model of proposed IOT security communication scheme constructed in this paper is demonstrated in Fig. 4 in the light of OPNET’s modeling mechanism.

![Overall network model of proposed scheme](image)

**Fig. 4** Overall network model of proposed scheme

3.2. Analysis of experimental results
In order to obtain objective test results and compare the sending and receiving data of the IoT security communication scheme, the experiment introduces four standard test images (camera, lena, house, man) for testing and simulation as shown in Fig. 5.

![Test images](image)

a) camera(plaintext)  c) lena(plaintext)  e) house(plaintext)  g) man(plaintext)
b) camera(ciphertext)  d) lena(ciphertext)  f) house(ciphertext)  h) man(ciphertext)

**Fig. 5** Transmission image of IOT secure communication scheme

A secure key generation algorithm should have a sufficiently large key space to resist brute force attacks. The longer the bits of the initial key are, the larger the key space is. The key space of the algorithm in this paper has more than 2^60 elements which ensure the security of the key library. So as to further test the security of the PRESENT encryption algorithm, this paper compares the information entropy and 0-1 balance of the selected test images and tests the key sensitivity of the algorithm through the NPCR and UACI indicators. The test results are shown in Table 2.

| Image                | Information Entropy | NPCR  | UACI  | 0-1 balance |
|----------------------|---------------------|-------|-------|-------------|
| camera(plaintext)    | 3.2523              | 0.9763| 0.3192| 1.2448      |
| camera(ciphertext)   | 7.5911              | 0.9763| 0.3192| 1.0525      |
| lena(plaintext)      | 7.4900              | 0.9960| 0.2846| 1.0722      |
| lena(ciphertext)     | 7.9837              | 0.9960| 0.2846| 1.0015      |
| house(plaintext)     | 6.5513              | 0.9959| 0.2888| 0.8019      |
| house(ciphertext)    | 7.9791              | 0.9959| 0.2888| 1.0071      |
| man(plaintext)       | 7.0581              | 0.9763| 0.2757| 1.0467      |
| man(ciphertext)      | 7.9913              | 0.9763| 0.2757| 1.0007      |

**Tab. 2** Safety performance analysis results of test images

From the observation of the data in Table 2, it can be seen that the information entropy of the ciphertext image is close to 8 and the value of 0-1 balance is close to 1. At the same time, the NPCR is close to 0.99 and the UACU is around 0.33 which signifies that the PRESENT algorithm is safe and suitable for IOT environment.

4. Conclusion
This article proposes a secure communication scheme suitable for IOT devices, including the design of the key library generation algorithm and the utilization of the PRESENT lightweight encryption algorithm to ensure the confidentiality of the transmitted data. The simulation results and security analysis denote that the proposed scheme has the advantages of low complexity, easy implementation and high security. With the continuous improvement of communication protocols, the development of the Internet of Things will surely promote human society to an automation and intelligent era.

References
[1] Karie N M, Sahni N M, Haskell-Dowland P P 2020 IoT Threat Detection Advances, Challenges and Future Directions *ETSecIoT* (Sydney: IEEE) pp22-29
[2] Jie X, Kaiping X, Qingyou Y and Peilin H J 2018 PSAP Pseudonym-based Secure Authentication Protocol for NFC Applications *IEEE T. Consum. Electr.* 64 (Sydney: IEEE) pp83-91
[3] Mahmud M, Kaiser M S, Rahman M M, Rahman M A, Shabut A, Al-Mamun S and Hussain A J 2018 A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications *Cogn. Comput.* 10 (Berlin: Springer) pp 864-873
[4] Behshid S, Vesal Hakam and Ahmad A J 2020 A trust management scheme for IoT-enabled envi-ronmental health/accessibility monitoring services *Int. J. Inf. Secur* 19(Berlin: Springer) pp 93-110
[5] Bogdanov1 A, Knudsen L R, Leanderl G, Paar1 C, Poschmann1 A, Robshaw M J B, Seurin Y and Vikkelsoe C P 2007 PRESENT An Ultra-Lightweight Block Cipher *Ches* 2007 4727 (Berlin: Springer)