# Research on the Application of an Improved Encryption Algorithm in WSN

Dahui Hu[1, a] and Zhiguo Du[1, b*]

[1]Department of Information Management Rongchang Campus Southwest University, China

[a]hudahui@hotmail.com, [b]du_zhiguo@hotmail.com

*The correspopnding author

**Keywords:** Wireless Sensor Networks (WSN); Encryption algorithm; Montgomery algorithm; Chinese remainder theorem; RSA

**Abstract.** Public key cryptography in wireless sensor networks key management exist problems of slow speed and large energy consumption calculation, will be a kind of improved RSA public key algorithm is applied which, in ensuring the effectiveness of while reducing computational complexity. In the new algorithm, the Montgomery method is used to calculate the modular power of large numbers in order to facilitate the fast encryption. Experimental results show that the proposed method reduces the operation cost, reduces the energy consumption of nodes, reduces the occupation of storage space, and is more suitable for the nodes with low computing power and limited energy of wireless sensor networks.

## Introduction

With the development of sensor technology, communication technology, micro motor technology and computer technology, wireless sensor applications more and more widely, through artificial random arrangement, a huge number of sensor nodes concentrated in need with the development of sensor technology, communication technology, micro motor technology and computer technology, wireless sensor applications more and more widely, through artificial random arrangement, a huge number of sensor nodes concentrated in the need to monitor the area, using the node's own data processing function and data communication function, through the wireless channel connected into a self-organizing network. The wireless sensor network can be connected to the existing local area network or even Internet, and the wireless sensor network can be connected with the existing local area network and even the Internet, so that the remote terminal user can monitor the environment data in real time.

In wireless sensor networks, due to the characteristics of the node's computing power is weak, limited supply capacity, lower ability of small storage space, communication and network topology dynamic change, with the traditional computer networks have larger differences. The traditional computer network has a strong capability of terminal operation and energy is not limited, so we can use more complex encryption algorithm to ensure the security of data and communication. RSA algorithm is one of the representatives. However, a large quantity of RSA algorithm, is not suitable for application in sensor nodes is proposed in this paper an improved method, reduce the number of operations, reduce complexity of processor time and space complexity, which can be used in wireless sensor nodes. The experimental results show that the method is feasible and has good performance characteristics.

## Preliminary Knowledge

**Rsa Algorithm.** RSA public key encryption algorithm was proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It was first published in 1987, when three of them worked at Massachusetts Institute of Technology. RSA is the first letter of the three of them together.

 

RSA is currently the most influential public key encryption algorithm, it can resist so far known for the vast majority of password attacks, ISO has been recommended as the public key data encryption standard.

Today, only a short RSA key can be broken in a powerful way. By 2008, the world has not been any reliable way to attack the RSA algorithm. As long as the length of the key is long enough, the information that is encrypted with RSA can't be broken. But in the growing maturity of distributed computing and quantum computer theory, the security of RSA has been challenged.

RSA algorithm is based on a very simple fact number theory: multiplying two large prime numbers is very easy, but want to factorization of the product is extremely difficult, so you can the product as a public key encryption.

RSA algorithm is an asymmetric cryptographic algorithm, the so-called asymmetric, that is, the algorithm requires a pair of keys, using one of the encryption; you need to use another to decrypt.

RSA algorithm involves three parameters, n, e1, e2.

Among them, n is the two large numbers p, q product, n occupied by the binary digits, is called a key length.

The e1 and e2 is one of the value of e1 can take an arbitrary, but requires e1 and (p-1) * (q-1) coprime; and then select the e2, make (e2*e1) mod (p-1) * (q-1) = 1.

(n, e1), (n, e2) is the key pair. (n, e1) as the public key, (n, e2) as the private key.

RSA encryption and decryption algorithm is exactly the same, set A for the plain text, B for the cipher, then: A=B^e2 mod n; B=A^e1 mod n.

**Montgomerie Algorithm.** Montgomerie power mode operation is a fast calculation of a^b%k algorithm, is one of the core of RSA encryption algorithm.

A modular n (n is odd) length of k bits, namely: $2^{k-1} \le n \le 2^{k}$. To make $r=2^k$, the Montgomery value of the integer a is:

$$\bar{a} = ar \mod n$$

$$\bar{R} = ab \mod n$$

$$\bar{R} = \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot r^{-1} \mod n$$

$$r^{-1} r = 1 \mod r$$

$$\bar{R} = \bar{a} \cdot \bar{b} \cdot r^{-1} \mod n$$

$$= a \cdot r \cdot b \cdot r \cdot r^{-1} \mod n$$

$$= a \cdot b \cdot r \mod n$$

The Montgomery algorithm is applied in the encryption process of RSA, and the following pretreatment process is required.

- Solve $n'$, make it meet $r^{-1} r - n' n = 1$;
- Calculation $\bar{a} = ar \mod n, \bar{b} = br \mod n$
- Calculation $\bar{R}$, $\bar{R} = (t + m \cdot n)/r$, in which $\bar{t} = \bar{a} \cdot \bar{b}, m = t \cdot n' \mod r$;
- Calculation of R, solving the R function assumption is GetPara, then

$$R = GetPara(\bar{R}, 1)$$

$$= \bar{R} \cdot 1 \cdot r^{-1} \mod n$$

$$= \bar{a} \cdot \bar{b} \cdot r^{-1} \cdot r^{-1} \mod n$$

$$= ab \mod n$$

In the encryption process of RSA algorithm, the above method is applied to solve the modular exponential operation. Assuming that the length of e is k bit, 0<M<n, $x=M^e$ mod n, then the calculation steps of X are as follows.

- Calculation $n'$;

 

- Calculation $\overline{M}, \overline{M} = M \cdot r \bmod n$;
- Calculation $\overline{x}, \overline{x} = 1 \cdot r \bmod n$;
- To make i=k-1, the loop makes i decrease by 1 until i=0. If $e_i$=1, Then $\overline{x} = GetPara(M, \overline{x})$, otherwise $\overline{x} = GetPara(\overline{x}, \overline{x})$; $x = GetPara(\overline{x}, 1)$.

In the above steps, the step i can be calculated by the extended Euclidean algorithm, step ii, iii requires a division operation; step IV can get me Montgomery value, step v to get the x values. The mod index in the operation process, the procedure needs to be performed only once, when e⩾3, the efficiency of the high step. It is obvious that the higher the index, the higher the efficiency of the method.

**Chinese Remainder Theorem.** China remainder theorem is one of the commonly used theorem in number theory, p1, p2…, pk (k>1) is mutually prime of k positive integers. Given ui∈ [0, pi-1] (1⩽ i⩽k), the system of congruence u=ui (mod pi) (1⩽i⩽k) inevitable the existence and uniqueness of the solution:

$$u = \sum_{i=1}^{k} uiciPi (\bmod P)$$

(Where P= $\prod_{i=1}^{k} pi$ , Pi= $\frac{P}{pi}$ , ci= $P_i^{-1}$ mod pi)

RSA algorithm in the public key (e, n), the private key for the d, p, q is to generate a pair of large prime number RSA key pair, C is the cipher text, M is the corresponding text.

Decryption operation of RSA algorithm: $M=C^d \bmod n=C^d \bmod (p\ q)$

Using the Chinese remainder theorem, the formula can be divided into: $M_1=C^d \bmod q$, $M_2=C^d \bmod p$

Using the Fermat Theory can be known, $a^{m-1}=1 \bmod m$ (where m is prime, and a is not a multiple of m), so the formula can be further simplified as: $M_1=C_{d1} \bmod q$, $M_2=C_{d2} \bmod p$. Among them, d1=d mod (q-1), d2=d mod (p-1).

According to the Chinese remainder theorem

$$M = (M_1 c_1 \frac{pq}{q} + M_2 c_2 \frac{pq}{q}) \bmod n$$
$$= (M_1 c_1 p + M_2 c_2 q) \bmod n$$

Because: c1=p-1 mod q，c2=q-1 mod p,

So: M=（M1（p-1 mod q）p）+M2 (q-1 mod p) q） mod n

In this algorithm, the length of n is k, then the length of p and q is k/2. Assuming d1、d2、$p^{-1}$ mod q、$q^{-1}$ mod p are known, then the entire calculation process requires about bit times $3k^3/8$ computing. If you do not use the Chinese remainder theorem, it is about $3k^3/2$ times bit operations, so the new algorithm can reduce the amount of computation by 81%.

## Experiment and Data Analysis

**Experimental Platform and Control Software.** The hardware of the experiment platform is MOTE-KIT 5040 series. It includes 4 Processor/Radio Boards MICA2, 4 Boards MICA2DOT, 3 Sensor Boards MTS310, 2 MICA2DOT MDA500 prototypes and data acquisition board and 1 MIB510 programming interface board.

 

The main components of the MOTE-KIT5040 is MICA2. It is improvement of the early products of mica, the TinyOS operating system is a small, open source, energy-saving software operating system, support for large-scale, self-configuration of the wireless sensor network, the source code and software development tools can be downloaded from the Internet.

Measurement and control software is an important part of the wireless sensor network system. It is an important tool to obtain and analyze the data of the sensor network. The experiment uses SNAMP software platform to obtain and analyze the data. SNAMP (Network Analysis and Management Platform Sensor) is a wireless sensor network analysis and management platform, its remarkable characteristic is the measurement and control process visualization, can provide the relative data directly.

**Data Analysis.** Experiments were conducted in a lab which area is 20m * 20m, using 10 wireless sensor nodes, nodes are randomly placed on the experimental platform, the node uses 800mA lithium battery, the node does not use the external antenna and the expansion port. Node experiment is mainly divided into two times, once running RSA algorithm on each node and the other operation of the improved algorithm proposed in this paper.

RSA algorithm is safe and reliable, but it has a huge amount of computation. The micro controller needs high load operation, and the data processing needs a long time. Improved RSA algorithm greatly reduces the amount of computation, the computation time of the micro controller is significantly reduced, Fig. 1 and Fig. 2 is the 10 nodes in the two cases of computing time comparison.

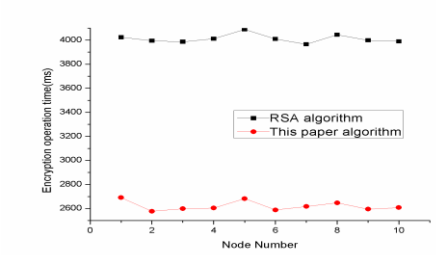


Figure 1. Encryption time of two algorithms

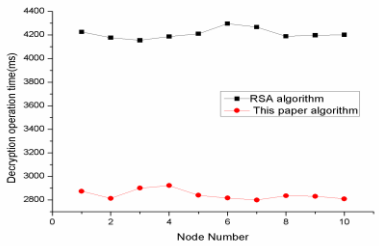


Figure 2. Decryption time of two algorithms

Using SNAMP software, real-time monitoring of the use of storage space in nodes, figure two is the case of 2 different algorithms, nodes consume storage space. As can be seen from Table 1, the improved algorithm is significantly smaller than the original algorithm in the amount of storage space.

Table 1 Memory usage of the two algorithms

| Node Number | RSA(Byte) | Algorithm in this paper(Byte) |
|---|---|---|
| Node 1 | 30654 | 24512 |
| Node 2 | 29874 | 26504 |
| Node 3 | 31427 | 25526 |
| Node 4 | 29766 | 25498 |
| Node 5 | 29897 | 25712 |
| Node 6 | 29868 | 24917 |
| Node 7 | 30879 | 25326 |
| Node 8 | 30902 | 26018 |
| Node 9 | 30329 | 25875 |
| Node 10 | 30468 | 25962 |

## Conclusion

The rapid development of Internet of things, will actively promote the development of wireless sensor network, which has a wide range of applications in military, environmental protection, health care,

 

family life and industrial and agricultural production. Wireless sensor network node is usually an embedded system, because of the manufacturing cost, node size and energy supply and other factors, the computing power, storage capacity and communication distance and so on need to be improved. Solve this problem to be able to begin from two aspects. On the one hand can be by improving node manufacturing technology to improve node performance (for example, increasing the power per unit volume of charge storage capacity); on the other hand, can improving existing algorithms or management mode, to reduce calculation amount of the micro controller, reducing energy consumption, improve the node lifetime.

In this paper, the improved RSA algorithm is applied in the wireless sensor network; improved algorithm of operation significantly reduced the volume of, energy consumption significantly reduced, in ensuring the encryption effects at the same time improve the network data transmission rate and prolong the network lifetime. Experimental results verify the theoretical derivation. Therefore, the application of the improved algorithm in wireless sensor networks has high practicability and good potential.

## Acknowledgement

In this paper, the author was sponsored by "southwest university youth fund project" (project number: 20700909) and "Fundamental Research Funds for the Central Universities"(project number: XDJK2016C048).

## References

[1] Chungen Xu, Sheng Gong, Modeling and Implementing System of Access Control On the Web, Proceeedings of First International Conference on Modeling and Simulation, Nanjin, China,2008, pp.390-394, Auguest.5-7.

[2] Carlos F. Garcia-hermandez, “Wireless sensor networks and applications International Journal of Computer Science and Network Security, Vol.7, No.3, pp. 264-273, March 2007.

[3] Wander, A.S., Gura, N., Ederle, H., Gupta, V, Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, In proceedings of PerCom pp. 324-328, 2005.

[4] David P, Mike D, Reqina E. Pheromone robotics. Autonomous Robots,2001, 11(3):319-324.

[5] Beibei K, Hongyang C, Xiaohu T. Key Pre-Distribution Schemes for Large-Scale Wireless Sensor Networks Using Hexagon Partition[C]. //Wireless Communications and Networking Conference (WCNC), 2010:1-5.

[6] Taekyoung K, Jonghyup L, Jooseok S. Location-Based Pairwise Key Predistribution for Wireless Sensor Networks [J]. Wireless Communications, IEEE Transactions on, 2009, 8(11):5436- 5442.

[7] Oliveira L, Scott M, Lopez J, et al. TinyPBC: Pairings for Authentication Identity-based Non-Interactive Key Distribution in Sensor Networks[C]//Proc. of the 5th International Conference on Networked Sensing Systems. IEEE Press, 2008: 173-180.

[8] Bhise A. Low Complexity Hybrid Turbo Codes[C]//Wireless Communications and Networking Conference, 2008: 1050-1055.

[9] Debessu Y G, Wu H C. Modified turbo decoder for local content in single-frequency networks[C]//IEEE International Symposium on BMSB, 2012:1-5.

[10] Mansour M F, Tewfik A H. A Turbo Coding Scheme for Channels with Synchronization Errors [J]. IEEE Transactions on communications, 2012, 60(8):2091-2100.

 