A Comparative Study of Encryption Algorithms in Wireless Sensor Network

Zonghu Xi, Li Li, Guozhen Shi and Shuaibing Wang

Abstract With the development of the Internet of Things, the Wireless Senor Network has been paid increasing attention. It can not only perceive the physical world, collect and transmit information, but also brings new problems in the security of information. As the nodes of Wireless Sensor Network are limited by hardware resources and energy, how to select fast and energy-saving encryption algorithms in terms of Wireless Sensor Network is very important. This paper constructs a test framework for comparing the energy consumption, time efficiency, and space efficiency and then tests parameters of multiple algorithms in the same application environment. The results provide a basis for choosing suitable algorithms for the Wireless Sensor Network.

Keywords Wireless sensor network · Encryption algorithm · Time efficiency · Energy consumption · Space efficiency

1 Introduction

Wireless Sensor Network (WSN) is a self-organized network that composed of micro sensor nodes [1, 2]. With the advantages of low cost, low data, and short distance, it is widely used in agricultural, biological, medical, military, and other fields. In recent years, with the rapid development of wireless sensor networks, security issues become increasingly prominent, especially in the military and commercial fields. As the data is transmitted by wireless, information may be

Z. Xi (✉) · S. Wang
School of Computer Science and Technology, Xidian University,
Xian 710071, China
e-mail: xizonghu@163.com

L. Li · G. Shi
Department of Electronic Engineering, Beijing Electronic Science
and Technology Institute, Beijing 100070, China
e-mail: laury_li@163.com

Q.-A. Zeng (ed.), *Wireless Communications, Networking and Applications*,
Lecture Notes in Electrical Engineering 348,
DOI 10.1007/978-81-322-2580-5_99

illegally eavesdropped, tampered, or destroyed at any time in the transmission process. Therefore, it is particularly important to ensure the safety of data in the wireless transmission. Based on the characteristics of wireless sensor networks, a series of cryptographic algorithm are mainly used to guarantee the network security. Although many mature encryption algorithms already exist, it is not enough. As the especial properties of wireless sensor network, a question is whether encryption algorithms can satisfy the hardware's requirements [3]. Thus, the key is how to select a right encryption algorithm. By exploring the application of cryptographic algorithm, analyzing energy consumption, time and space efficiency of these algorithms, comparing the performance parameters in wireless sensor networks, we will conclude from the data. The algorithms should suitable for application scenarios of wireless sensor networks. This paper introduces the basis for selecting cryptographic algorithms in several situations, and describes the framework of the system which is used to analyze the cryptographic algorithms in tests. On this basis it analyzes the performance of parameters in various algorithms, and explains its reasons. Finally, the characteristics of these cryptographic algorithms in wireless sensor networks are summarized.

2 Algorithm Selecting

Usually, a large number of sensor nodes are deployed to collect information in the monitoring region, which strictly limits their cost, size, and power consumption. Therefore, the most obvious characteristics of wireless sensor network are the limited hardware resources and power energy. As wireless sensor nodes are limited by power and volume, the code space, and data space are smaller than ordinary computer. Now the storage space of program code and data on computer has reached TB grade and GB grade, respectively, while the equipment of wireless sensor node remains in the KB grade [4–7] and its ability in data processing is even weaker than the general embedded system. Thus, in the design of the wireless sensor network system, the cryptographic algorithm should be selected with the standard of small space and fast speed, so it can spare enough hardware resources for other more important functions like data acquisition, transmission, and network management. Nodes in wireless sensor network are usually composed of two batteries to supply power. Because of the limited by volume, the capacity of the battery will not be great, and in the working process of the nodes, the battery cannot be replaced or recharged. Once the battery energy runs out, the node will lose its function. In the special environment, power consumption must be strictly controlled in each step of the design. Even in each technology and protocol, it must take energy saving as the premise. So the power consumption should also be considered in the selection of algorithms.

According to the current development trend of password and the characteristics of sensor networks, five kinds of common influential algorithms in two systems of

Table 1 Introduction of algorithms

Name	Source	Type	Key length	Security
DES	1972, U.S.A	Symmetric	192 bit (Triple-DES)	Brute force attack
AES	2001, U.S.A, Rijndael	Symmetric	128/192/256 bit	Anti difference, Linear analysis [8]
SM1	OSCCA (China)	Symmetric	256 bit	Unbreakable
SM2	OSCCA (China)	Asymmetric	512 bit pri.key, 256 bit pub.key	Unbreakable
RSA	1977, U.S.A	Asymmetric	1024/2048 bit	Depending on the decomposition of large numbers

symmetric and asymmetric cryptography are selected as the study object. Five algorithms are given in Table 1.

Asymmetric cryptography has great advantages in key management. With different encryption and decryption keys, the complex process of the wireless sensor network key negotiation can be resolved [9, 12]. Therefore, asymmetric cryptography is suitable in the application of unidirectional data transmission, and it is the development trend of cryptography algorithm in wireless sensor networks in the future. But because of its complexity, the cryptographic algorithm has not been widely used now.

3 Test Framework

To guarantee the integrity and reliability of the test results, the framework for tests is very important in the early stage of requirements analysis. It standardizes the testing work, improves the efficiency and quality of tests, so a good test framework is an important basement for the comparison of algorithms. The test framework in this paper is shown in Fig. 1.

3.1 The Hardware Component

The test framework consists of three parts: input section, hardware section, and monitor section. The hardware section is the core of the whole framework, a complete hardware system composed of an 8051 core, power management, timer, DES, AES, SM1 algorithm module, SM2/RSA unit, and the SM2/RSA library. The functions of these components are shown as follows:

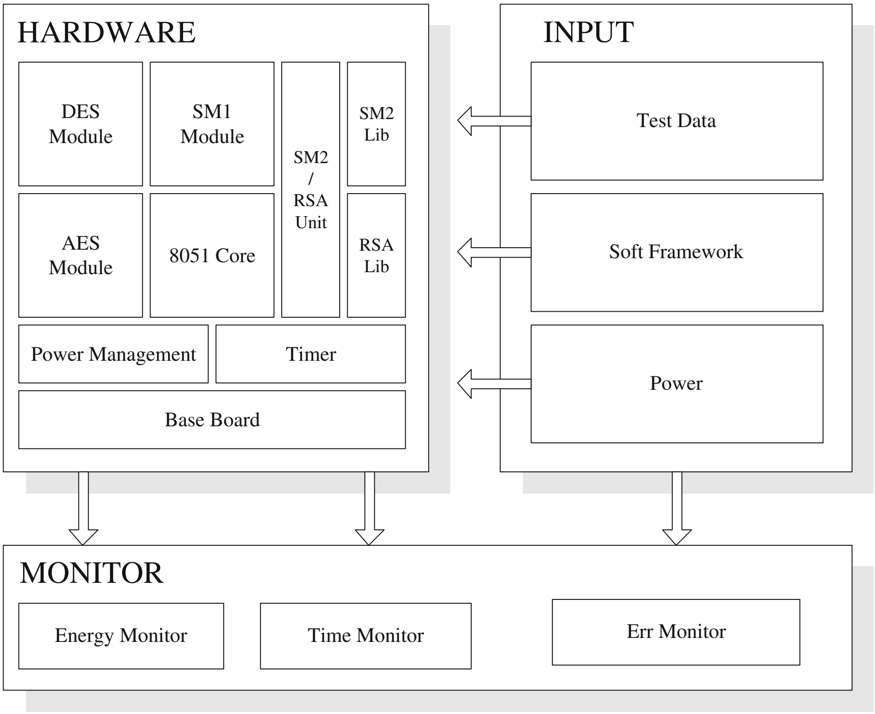


Fig. 1 The test framework of encryption algorithms

(1) The microprocessor executes the test program to control the coordination between the various modules and data processing.
(2) Power management is used to control the energy consumption of each module, and support the following analysis of the algorithm.
(3) Timer is used to record time and measures the speed of implementation of algorithms.
(4) DES, AES, and SM1 algorithm modules implemented by hardware are symmetric encryption, and they are the entity in tests.
(5) SM2/RSA unit and the SM2/RSA library provide hardware implementation of the two algorithms partly, and they are also the entity in tests.

Although the optimized degree of hardware implementation for the same algorithm will affect the execution time and energy consumption, the differences produced by the hardware implementation for the same algorithm is much smaller than implementation for the different algorithm. So the implementation of one algorithm can represent the average level of implementation in the construction of the test framework. Thus we can focus on the comparability of the performance of different algorithms rather than on the effect of the comparative results produced by different optimization of one algorithm. This effect exists, but appears to be negligible by comparing the differences among different algorithms.

3.2 The Input Component

The input component is the front part of the test framework and consists of test data, test program, and test power. It is used to provide the necessary data, energy, and other resources for hardware component to ensure the hardware section under normal operation. The test data in different test program offers different data, which is an important basement for the analysis of time efficiency. The test program for different objects provides different programs. At the same time, in comparing space efficiency of the algorithms, the information about the data of stored space is provided by the test program. The test power supports for hardware component, and provides the basis of calculation in comparing energy consumption of the algorithms.

3.3 The Monitor Component

The monitor component provides the output results of test framework. It monitors and records the results from the input component and hardware component. It is an important source of data for comparative analysis. The monitor component is composed of energy monitor, time monitor, and err monitor. Power monitor mainly detects energy consumption of hardware component, and provides data for energy consumption comparison. Time monitor records execution time of algorithm and program, and provides data for comparative efficiency. Err monitor is responsible for the state of the input component and prevents it from showing abnormal test results or wrong results.

4 Analysis of Algorithm

This paper respectively compares the energy consumption, time efficiency, and space efficiency of AES, DES, SM1, SM2, RSA these five kinds of common cipher algorithm. Among them, AES, DES, SM1 belongs to the symmetric system, and SM2, RSA belongs to the asymmetric system. The process of algorithm analysis is shown in Fig. 2.

In the analysis of time efficiency and energy consumption, the test runs on the same hardware platform, and the algorithms are implemented by the same method. The paper takes the algorithm as primary section, regardless of operating system, network protocol, data transmission, and other indicators. In order to make the comparative analysis more convincing, the test platform is measured under the standard of non-operating system, and except DMA transmission and the timer.

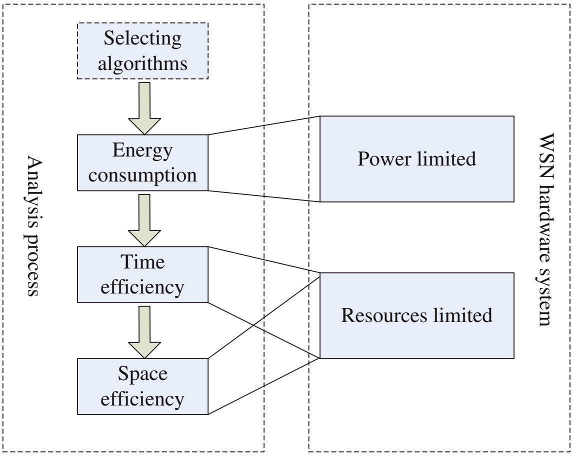


Fig. 2 The process of algorithm analysis

4.1 Energy Consumption

As sensor nodes become micro shapes with limited energy of batteries and physical constraints which make them difficult to be replaced. The limited energy is one of the most important constraints in the design of the whole wireless sensor network system. It directly determines the lifetime of the network. The modules of energy consumption mainly contain sensor module, processor module and wireless communication module [9]. In order to limit the overall energy consumption, the nodes should maintain at a saved power state, and the energy consumption of cryptographic algorithm should be as low as possible at encryption and decryption of data to extend the service lifetime of nodes and the whole network [9, 10].

This section will calculate the power of the encryption and decryption operations and the following five algorithms will be tested in the same framework. In this test framework, a 3.0 V (equivalent to the voltage of two 5# batteries) constant-voltage source as power, a wattmeter, and an ammeter will be selected. The formula is P = UI ("P" represents power, "U" represents voltage, "I" represents current). The model of testing energy consumption (closing unrelated modules) is shown in Fig. 3.

In the model, the measurement of energy consumption contains two parts, the consumption of system and consumption of algorithm. The consumption of system is the sum of necessary consumption in keeping the processor, memory, and other electronic component of the whole hardware system running. The consumption of algorithm is generated by the algorithm module itself [11]. Figure 4 shows the comparison of energy consumption in encryption and decryption algorithms.

From the data above, the gap in energy consumption among cryptographic algorithms is not great. In extreme cases, the maximum power consumption of RSA encryption with 24.3 mA can keep working 82 h with two 1.5 V 2000 mAh batteries. But the minimum power consumption of AES with 22.3 mA can keep

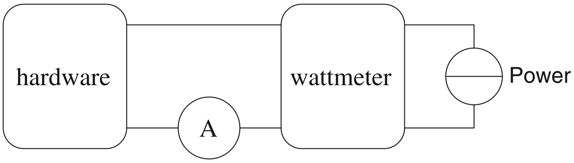
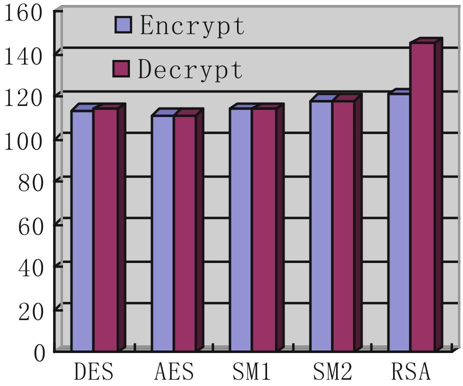


Fig. 3 The model of testing energy consumption

Fig. 4 The energy consumption of algorithms



89 h under the same conditions with the same batteries. So by changing algorithms to reduce the energy consumption is almost undesirable.

4.2 *Time Efficiency*

At present, the wireless sensor network is based on IEEE 802.15.4 standard which provides a transmission rate of 20, 40, and 250 kbit/s, corresponding to the radio frequency 868, 915, and 2450 MHz. Time consumption by the cryptographic algorithms should not be too much in this low rate communication technology [12] which is less considered in conventional wired networks.

This section focuses on testing time consumption by the operations of the encryption and decryption algorithms. Because of the small amount of data in wireless sensor networks, the length of data frame cannot exceed 127 bytes in MAC layer [13]. Large block data is not considered suitable to transmit in wireless sensor networks. 2 K (2048) is defined as the largest length of transmission capacity here. With 16 M system clock frequency, 16 bits timer, 1 μs as the unit of time measurement and 2 K bytes of test data used in the encryption and decryption operation on, the test results are as follows.

Table 2 shows that the symmetric cryptography runs faster than asymmetric as expected. In the symmetric cryptography, DES runs the fastest, followed by AES,

Table 2 The consumption of running time

Name	Operation	Time (μs)	Key length (bit)
DES	Encryption	13,297	64 * 3
	Decryption	13,297	
AES	Encryption	49,781	192
	Decryption	49,877	
SM1	Encryption	57,856	128 * 2
	Encryption	1,640,345	
SM2	Decryption	1,345,076	512 + 256
	Encryption	81,173	
RSA	Decryption	731,905	1024*2
	Encryption	1,640,345	

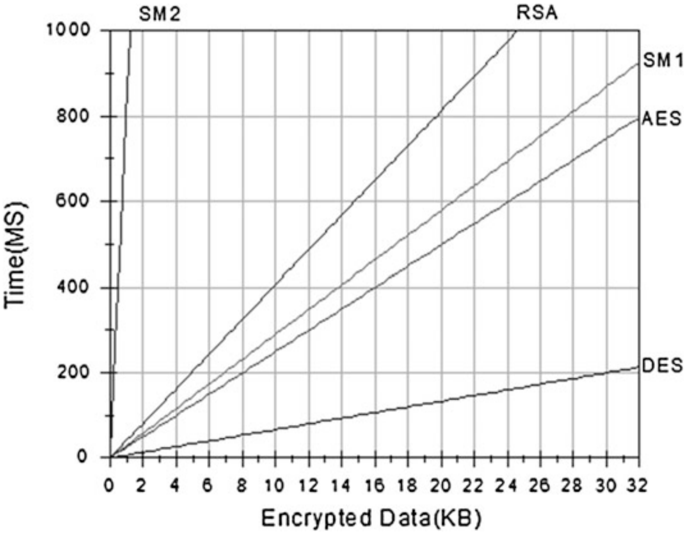


Fig. 5 The costs of running time in classic model

and SM1 is the third. In the asymmetric cryptography, RSA runs much faster than SM2 does. From Fig. 5, all of these kinds of symmetric algorithms could satisfy the standard of the rate that described in IEEE 802.15.4, while two asymmetric algorithms cannot satisfy the rate.

4.3 Space Efficiency

Nodes in wireless sensor networks not only monitor and collect data, but also undertake the function of routers. The data and tables of routers all need the storage

Table 3 The costs of running space

Name	Implementation	RAM (byte)	ROM (byte)
DES	Hardware	50	0
AES	Hardware	64	0
SM1	Hardware	65	0
SM2	Firmware	352 + 2991	About 31,523
RSA	Firmware	1024 + 2328	About 29,755

space which is very sensitive to nodes whose RAM and ROM are relatively limited. Thus the selected cryptographic algorithm should be easy to implement with a small storage space.

In this section, symmetric algorithms implement by hardware and asymmetric algorithms implement by hybrid of hardware and software. As mentioned in the hardware section of the testing framework, SM2 and RSA only have the basic operation and function library which provides sufficient function to implement algorithms. The hardware is equivalent to an accelerator, and the software really makes algorithms implement. In the testing framework, this method is called hybrid implementation. The statistical results of the running space are shown in Table 3.

DES needs three key spaces of 64 bits, two buffer spaces of 64 bits (the input buffer and output buffer), a mode space of 16 bits, and an initial vector space of 64 bits. AES needs a key space of 256 bits and two buffer space of 128 bits. SM1 needs a basic key space of 128 bits, an extern key space of 128 bits, two buffer space of 128 bits, and a mode space of 8 bits.

SM2 needs a public key space of 512 bits, a private key space of 256 bits, two buffer space of 1024 bits, extends a code ROM of 32 kB and a data ROM of 3 kB. SM2 is a kind of algorithm based on elliptic curves. Due to the large amount of computation, it usually runs on computer by pure software. In the environment of embedded devices, mobile terminals with weak processing generally use the hardware to achieve some basic computing and algorithms, such as modular arithmetic and inverse operation [14]. Using software to achieve the logical parts such as data exchange, the hybrid of hardware and software improves algorithm's efficiency on the embedded devices.

RSA needs a public key space of 2048 bits, a private key space of 2048 bits, and two buffer spaces of 2048 bits. To achieve software parts requires additional a code ROM of 30 kB and a data ROM of 2 kB approximately. It belongs to the public key cryptosystem and usually runs in the hybrid of hardware and software the same as SM2.

The RAM space of symmetric algorithms is very small and the maximum length of key is 256 bits. But the asymmetric algorithms not only use large RAM space, but also take up a lot of extra ROM space and its minimum key is 256 bits.

Although the asymmetric algorithms use large storage space, it is used to manage the key generation and distribution and verification of signature. In wireless sensor network, information is generally spread from the node to the gateway unidirectional. Nodes only need to encrypt the data without decryption and the gateway only needs to decrypt the data without encryption. Both symmetric encryption and decryption use the same key. Before sending and receiving data, it must finish the key. Asymmetric algorithms use public key for encryption and private key for decryption. Verification of signature can ensure the data security, preventing the data from being illegally tampered. So this extra space is necessary for sensor networks. At the same time, it also effectively solves the problem of key negotiation of asymmetric algorithm in data transmission.

5 Conclusion

According to the features of limited hardware resources and energy in the wireless sensor network, this paper selects several cryptographic algorithms for researching and comparing. The results show that symmetric encryption can achieve high speed, simple implementation, short key, and small space. Therefore, in the application of relatively weak safety requirements, the symmetric encryption is more suitable for wireless sensor networks to encrypt bulk data. With low speed and large space occupied, asymmetric algorithms is difficult to meet real-time requirements in encryption and decryption. But asymmetric algorithms have great advantages in key management and security, indicating that it has a significant development in wireless sensor networks in the future.

Acknowledgments This work was supported by the Grand Science Research Foundation of Central University under Grant (No. 2014CLJH07 and No. 2014XKJS01).

References

1. Yi, F., Li, Z., Wang, H.: Energy-efficient data collection in multiple mobile gateways WSN-MCN convergence system. In: IEEE Consumer Communications and Networking Conference (CCNC), pp. 271–276. IEEE (2013)
2. Healy, M., Newe, T., Lewis, E.: Analysis of hardware encryption versus software encryption on wireless sensor network motes. M. Smart Sensors and Sensing Technology, pp. 3–14. Springer, Berlin, Heidelberg (2008)
3. Biswas, K., Muthukkumarasamy, V., Sithirasenan, E., et al.: A simple lightweight encryption scheme for wireless sensor networks. M. Distributed Computing and Networking, pp. 499–504. Springer, Berlin, Heidelberg (2014)
4. Varalakshmi, L.M., Sudha, G.F., Jaikishan, G.: A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks. J. Telecommun. Syst. 1–9 (2013)
5. Kayalvizhi, R., Vijayalakshmi, M., Vaidehi, V.: Energy analysis of RSA and ELGAMAL algorithms for wireless sensor networks. M. Recent Trends in Network Security and Applications, pp. 172–180. Springer, Berlin, Heidelberg (2010)
6. Baek, J., Tan, H.C., Zhou, J., et al.: Realizing stateful public key encryption in wireless sensor network. In: Proceedings of The Ifip Tc 11 23rd International Information Security Conference, pp. 95–107. Springer, US (2008)

7. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. J. Commun. ACM **47**(6), 53–57 (2004)
8. Suárez, N., Callicó, G.M., Sarmiento, R., et al.: Processor customization for software implementation of the AES algorithm for wireless sensor networks. M. Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, pp. 326–335. Springer, Berlin, Heidelberg (2010)
9. Mancill, T., Pilskalns, O.: Combining encryption and compression in wireless sensor networks. J Int. J. Wirel. Inf. Netw. **18**(1), 39–49 (2011)
10. Mandal, S., Chaki, R.: A novel power balanced encryption scheme for secure information exchange in wireless sensor networks. M. Advances in Computing and Information Technology, pp. 263–271. Springer, Berlin, Heidelberg (2012)
11. Guo, P., Zhang, H., Fu, D.S., et al.: Hybrid and lightweight cryptography for wireless sensor network. J. Comput. Sci. **39**(1), 69–72 (2012)
12. Qiu, W., Zhou, Y., Zhu, B., et al.: Key-insulated encryption based group key management for wireless sensor network. J. Central South Univ. **20**, 1277–1284 (2013)
13. Jin, N., Zhang, D.Y., Gao, J.Q., et al.: A study on the application of symmetric ciphers and asymmetric ciphers in wireless sensor networks. Chinese J. Sens. Actuators **24**(6), 874–878 (2011)
14. Du, X., Chen, H.H.: Security in wireless sensor networks. J. Wirel. Commun. **15**(4), 60–66 (2008)