A Symmetric Cryptography Algorithm in Wireless Sensor Network Security

https://doi.org/10.3991/ijoe.v13i11.7752

Juan Li
Inner Mongolia Vocational College of Chemical Engineering, Inner Mongolia, China
lijuan@hgzyxy.com.cn

Abstract—In order to study the symmetric cryptography algorithm, which plays an essential role in ensuring the information security, AES (Advanced Encryption Standard) basic theory is discussed, and AES protocol processor for a small area based on wireless sensor network is designed. In addition, an iterative encryption and decryption AES structure is designed to achieve the nonlinear transformation. And then, the wireless sensor network security is analyzed, and the results showed that in the process of encryption and decryption, making use of multiplexing and sharing technologies can help to obtain a low cost compact structure. And more importantly, it has great advantages in the resources compared with the same kind of designed structures. Based on the above findings, it is concluded that AES algorithm has good performances in wireless sensor networks and it can be widely applied.

Keywords—Wireless sensor, power management, circuit design

1 Introduction

With the continuous establishment and improvement of network infrastructure, the network makes information sharing, online communication and online trading possible. But on the other hand, the information of the state or individual is also threatened by illegal acquisition, destruction, tampering and so on. There is an urgent need to take measures to protect the data stored or transmitted electronically. The core technology of information security is cryptography. Wireless sensor networks (WSN) have broad application prospects in the fields of military, environmental science, medical health, space exploration and disaster rescue. But sensor nodes are often configured in harsh environments, unmanned areas or enemy positions, and need to continue to work, which are easily destroyed and disturbed. Compared with traditional wireless communication networks and mobile networks, wireless sensor networks are characterized by self-organization, low cost, resource constrained and data centric [1]. These characteristics make it possible for wireless sensor networks to carry out a large scale deployment information in forest, desert, battlefield and other harsh places to access to the network. Because the sensor node itself calculation speed, power supply, communication ability and storage space is very limited, the solution ideas and methods of traditional network security are not feasible in the sensor networks.

This puts forward many challenges for the design of sensor network security scheme, and also makes the security problem in sensor networks become a new research hotspot.

The focus is the symmetric cryptography in security mechanisms of wireless sensor network, specifically including encryption algorithm realization; analysis of block cipher, especially the analysis of the block cipher bypass, the working mode of block cipher, and the hash function wireless sensor network security mechanism research. The main work of this paper is as follows: firstly, the AES encryption algorithm is analyzed and implemented. The process of AES encryption algorithm is analyzed, and a small area AES co-processor based on wireless sensor network is designed. In order to adapt to the requirements of micro sensor node in wireless sensor networks for small area, the optimization design of the whole circuit area accounted for most of the S box unit module is focused on. And it uses the composite field arithmetic for its implementation, which greatly reduces the chip area occupied by the encryption circuit. And in the process of encryption and decryption, reuse and sharing technology is adopted to obtain a low-cost and compact AES structure. Secondly, the security mechanism of wireless sensor networks is discussed, and IEEE802.15.4 wireless sensor network security mechanism and sensor network security protocol SPINS are analyzed. According to the basic requirements of wireless sensor network security, it is put forward that a private key is shared between each sensor node and the base station. With the use of the encryption method used counting mode, and through the use of message authentication methods, the security of two nodes' communication can be achieved. And a method of using delayed released one-way key chain is proposed to ensure the security of broadcast communication.

2 Literature review

Because of the limitations of node function, wireless sensor networks can only use symmetric key technology, but seldom use public key technology. Wireless sensor network security protocol IEEE802.15.4, based on advanced encryption standard (AES) algorithm, generates a series of security mechanisms. The SPINS (Security Protocols for Sensor Network) is established based on the symmetric key system, and a more practical security scheme for sensor networks in the security system is put forward.

So far, a lot of literature have discussed the security of all kinds of block ciphers, and introduced several analysis methods, such as truncated differential cryptanalysis, nonlinear cryptanalysis, interpolation attacks and so on. Since the algorithm was published, many experts and scholars at home and abroad have been devoted to the security analysis of the algorithm, and some new attacks are expected to be introduced. The DES (Date Encipher Standard) algorithm is the first generation cipher standard in America; in February 2003, Camellia was chosen as the standard European block cipher standard [2]. In May 2005, Camellia was accepted as an encryption standard algorithm by the international organization for Standardization. The second generation standard in the United States is the Rijndael algorithm designed by Belgians, Joan Daemen and Vincent Rijmen based on AES, which has many excellent performances. In the fourth AES conference in 2004, Trl VanLe discovered the invariant algebraic properties of constant AES round function. The invariant algebraic properties did not consider the influences of the key, but only considered the iterative character of round function. After several rounds of iterations, the same input will produce the same output.

With the promulgation of the data encryption standard DES, 1980NBS (National Bureau of Standards), now NIST (National Institute of Standards and Technology), released 4 kinds of encryption modes of DES. They are the electronic code book mode (ECB), cipher block chaining (CBC) mode, cipher feedback mode (CFB) and output feedback mode (OFB). After the birth of the advanced encryption standard AES, the above 4 working modes, together with the counter CTR model proposed by Diffie and Hallmna in 1979, have been designated as the basic encryption mode of AES. There are many variations of the CBC mode, and for the HCBC, XCBC, and HPCBC put forward based on the CBC mode, it is essentially adding a few processes. In order to be free from patent restrictions, N.Fergusno, R.Houslyc and D.Whiting put forward the CCM encryption authentication mode on the basis of CTR mode and CBC-MAC [3]. This mode has many advantages. For instance, the block cipher does not require the inverse exists, and it can quickly process the message. As a result, other pseudo-random functions can also be used, not subject to patent restrictions, and provable security and so on. To sum up, there are still a lot of problems to be discussed in block cipher mode, especially in the field of authentication mode design. To this end, this paper takes block cipher model as a research focus.

3 Methods

3.1 AES basic theory

In the password system studies, the most are the algebra systems with limited number of elements. If the number of elements in the collection of F is limited, the algebra system is the finite domain or Galois domain, which is always expressed by G (P), wherein P represents the number of elements in the domain.

Definition 1: The domain is an algebraic system, which consists of a (containing at least two elements) non empty set F. In the set F, two binary operations are defined in the set F: addition (represented by the symbol +) and multiplication (represented by the symbol *, and sometimes a*b can be abbreviated as ab). And it meets the following conditions:

The elements of F, about the addition operation "+", forms an Abelian group, and its unit element is recorded as "0" (called the zero element of domain); the multiplication meets the distribution law in the addition operation. That is to say, for an arbitrary $a,b,c \in F$, it meets:

$$\begin{aligned} &a*(b+c)=a*b+a*c \\ &(a+b)*c=a*c+b*c \end{aligned} \tag{1}$$

Definition 2: if the set F only contains finite elements, the domain F at that time is called finite domain, also referred to Galois field.

Definition 3: the order of the domain F is the number of elements in the domain F.

3.2 Design of a small area AES co-processor based on wireless sensor networks

Researches on the security of wireless sensor network node can be considered from two aspects. The first is the analysis of the security mechanism of IEEE802.15.4 and its deficiencies, and the second is to improve the security of AES algorithm for encryption and authentication. Because of the large amount of wireless sensor network and simple application function, the hardware implementation cost of wireless sensor network is strictly limited, while the transmission bandwidth and time delay are relatively loose. Under such constraint conditions, reliable data communications and computation of intensive security tasks require reasonable allocation of system hardware and software resources, and performance requirements are necessary to be carefully weighed.

In terms of the design, AES is an iterative block cipher that consists of byte substitution (SubByte), row shift (ShiftRow), column mix (MixColumn), and round key addition (AddRoundKey) [4]. In terms of the requirements of wireless sensor networks, in order to implement a low-cost AES architecture, some considerations are taken into account in this design: the key length is fixed to 128bits. In the encryption and decryption and key arrangement, a balanced data path is obtained, and the key length of 128bits is designed and adopted. The number of AES round is fixed to 10. The entire AES structure uses only 4 S boxes. In order to reduce the hardware overhead cost of AES implementation, only 4 S boxes are used in byte replacement instead of 20 S boxes in the traditional design. By multiplexing 4 times, a 128bits (16 byte) nonlinear transformation can be achieved.

As far as the AES structure is concerned, based on the above considerations, this paper designs an iterative encryption and decryption AES structure, as shown in figure 1.

Most of the hardware implementation schemes of the AES algorithm employ 128 bits parallel computing. Although the data throughput is high, the area is larger. AES algorithm is the block operation so that each round 128 bits encryption and decryption is divided into 4 times 32 bits operation to be completed. In ensuring a certain data throughput rate, only 4 S boxes are needed so that encryption and decryption byte replacement can be completed. In concrete structure, a 128 bits shift register REG1 is inserted before the replacement of the 4 S boxes module, which is used to store the 128 bits data input [5]. After the replacement of the 4 S boxes modules, a 128 bits shift register REG2 is inserted to register the replaced data. The shift function is controlled and completed by the controller module. In the first and last round of iterations, each data transmission path is selected by a multiple selection logic. The key extension module is shown in figure 2.

In the AES algorithm, the key expansion module is also very important. In the design of the key expansion, most of them uses the one-time key expansion, and all round keys that a group of 10 rounds of encryption need are calculated once, and they are stored in the ROM [6]. However, due to limited chip resources, the design is not desirable. This design uses the first round of plain-text and initial key or operation, and carries on the second round key generation. And so on, in the k-th round (k<10) operation of the group, another clock cycle is provided for byte substitution in the key extension, so a round of encryption and decryption process takes 5 clock cycles time.

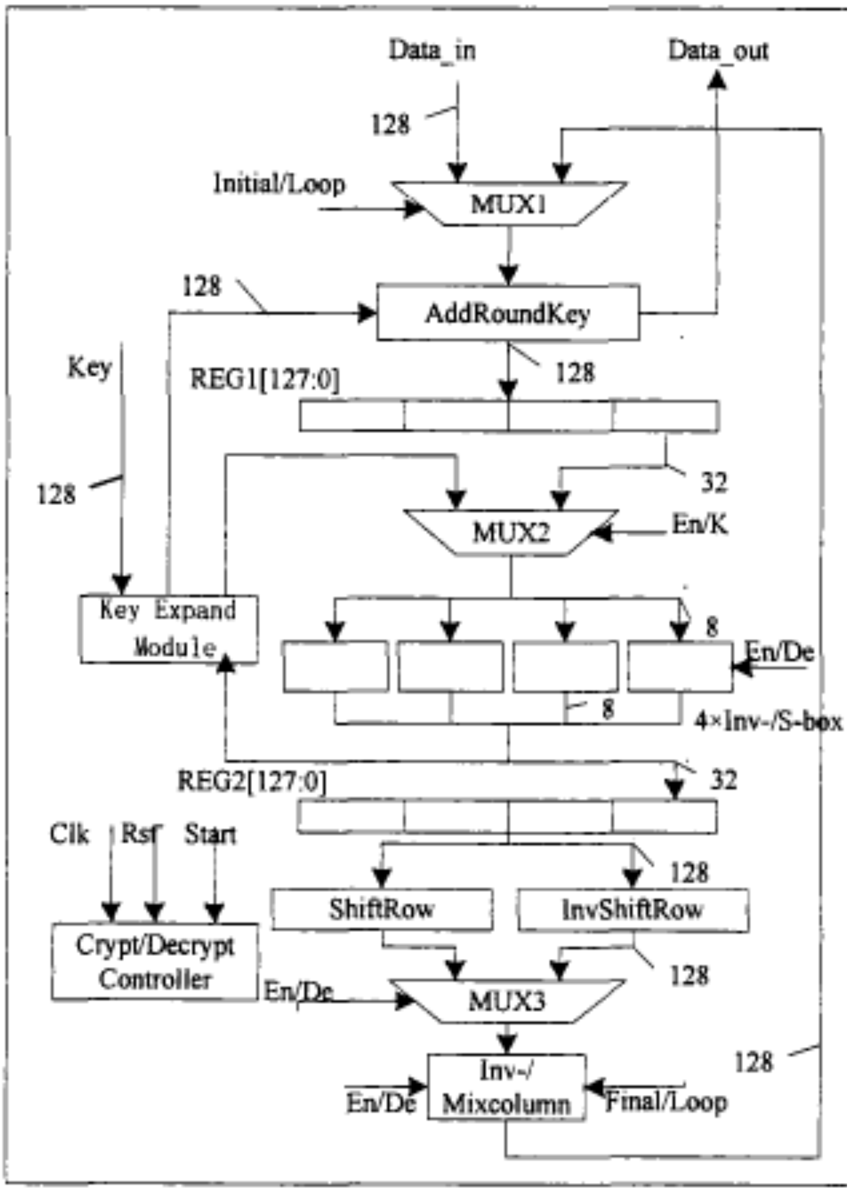

Fig. 1. AES encryption and decryption data path

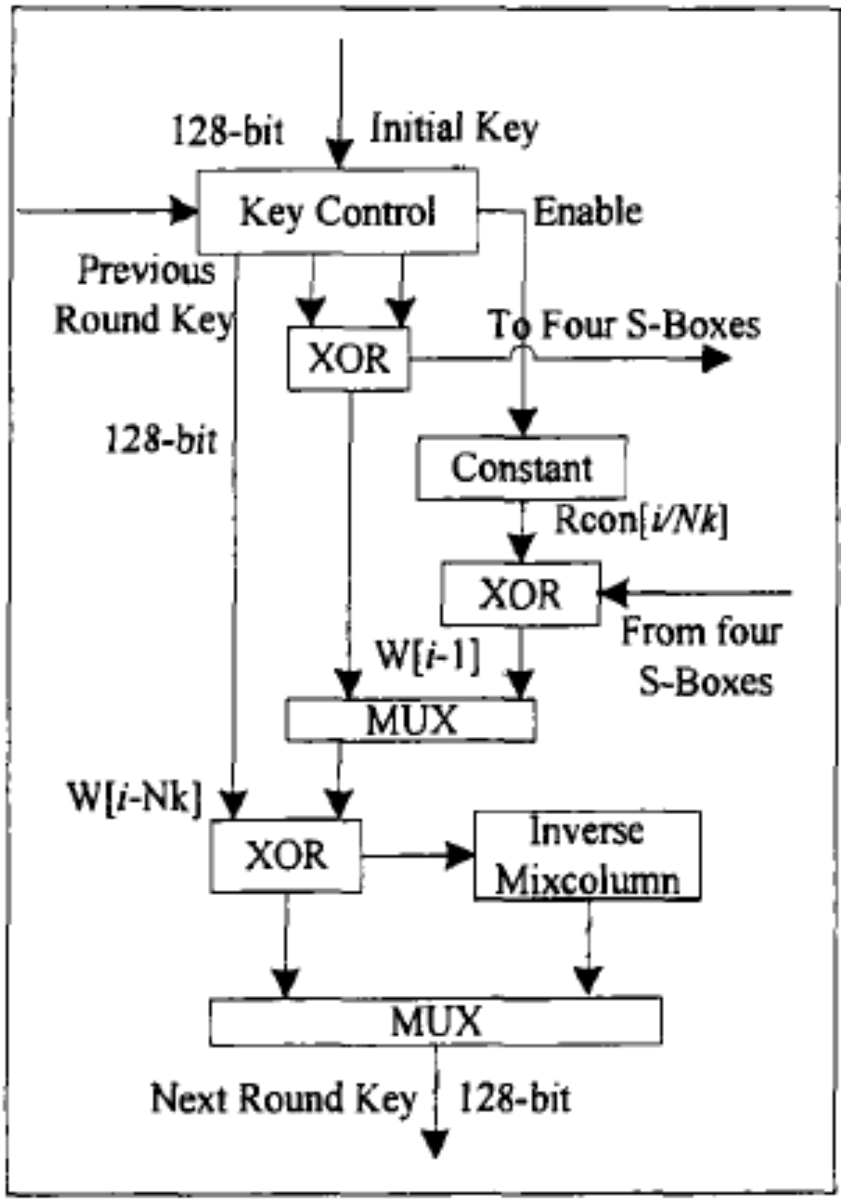

Fig. 2. The key extension module

4 Results and discussion

The security of wireless sensor networks is an open and active research field. In the wireless sensor networks, IEEE802.15.4 standard is adopted, and the standard provides access control, data encryption, frame integrity and freshness security mechanism of MAC sub-layer. The sensor network security protocol security system is a popular and practical sensor network security scheme in the current security systems. It is built on the basis of symmetric key system, and gives full consideration to data confidentiality, integrity, freshness, authentication and so on.

Thoughts and methods to solve the safety problem of the sensor network are different from those of the traditional network, which is mainly decided by the characteristics of the sensor network. They mainly include the limited storage space and computing capability; the lack of post node layout information; physical security layout area unable to be guaranteed; and the limited bandwidth and communication energy. It is not only the point to point security, but also the security of the entire network. In order to achieve the above security requirements in wireless sensor networks, the design method is to ensure the security of data communication between two nodes, and the second is to determine the safety of data communication. To solve the network security, there are usually two ways [7]. Firstly, the focus is put on the security communication protocol, and secondly, a kind of ubiquitous sensor network security solution model is put forward. Starting from the maintenance of line routing security, it requires to find a safe route to ensure the security of wireless sensor networks.

In order to satisfy the integrity, reliability and freshness of the data, as well as confidentiality, the proposed scheme ensures the security of the communication between the base station nodes and the wireless sensor nodes. As shown in Figure 3, the supervisor key generates the data encryption key K_{encr}, the pseudo-random number generator key K_{rand}, and the message identification code calculation key K_{mac}.

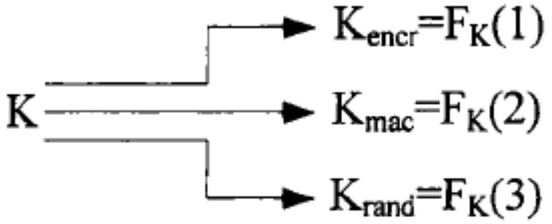

Fig. 3. The supervisor key exporting other keys

In the wireless sensor networks, the pseudo-random function F generates the keys, and repeatedly uses the message identification calculation program code, and the function is $F_k(x) = MAC(K,x)$. In that the one-way function F has strong irreversibility, the keys obtained has quite strong independence in the computer.

Data confidentiality is one of the most basic security features, and the easiest way is to encrypt the data. Another important security feature is the security of primitives. The security of the primitive is that although a decipher can see more than one cipher-text of the same text, he still cannot calculate the plain-text. The simplest approach is before using a key chain to process encrypted information, the sender first of all adds an initial vector randomly to the primitive. In wireless sensor networks, the data sender and the data receiver share a counter as an initialization vector IV of the packet encryption in the counting mode. The counter values are different at each time when the data is transmitted, so the same plain-text is bound to produce different cipher texts. The encrypted data format is $E = \{D\}(Kencr, C)$.

In order to ensure the data reliability and integrity, it is necessary to make use of message authentication code MAC. The message authentication code $MAC : M = MAC(Kmac, C|E)$. $C|E$ refers to the series of counter value C and cipher-text E, which indicates that the message authentication code and the cipher-text are calculated together. From the supervisor key K, K_{mac} and K_{rand} can be obtained. The whole message that A sends to B is: $A \rightarrow B : \{D\}(Kencr, C), MAC(Kmac, C|\{D\}(Kencr, C))$. MAC is used to calculate the message authentication code, as shown in figure 4.

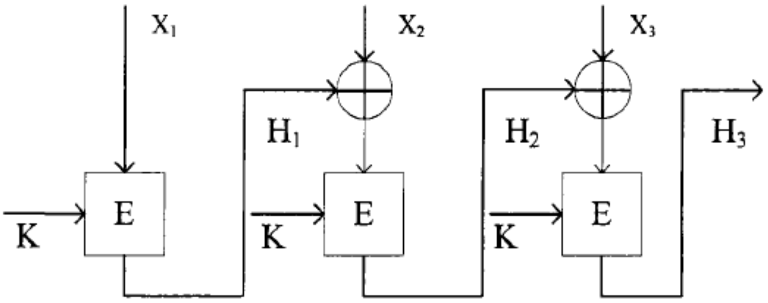

Fig. 4. Message authentication code calculation

This section analyzes the IEEE802.15.4 security mechanisms of wireless sensor network and security protocol of network sensor SPINS. According to the basic requirements of wireless sensor network security, this paper puts forward using the delay of release of symmetric key technology to obtain the non symmetry of data transmission, to achieve the requirement of data transmission.

5 Conclusion

From the security problems of wireless sensor networks, it can be seen that the essence of network security mechanism is the design and analysis of cryptographic algorithms and protocols. In this paper, with the problem of information security in wireless sensor networks as the background, a further study is made on the implementation of the main encryption algorithm in the symmetric cryptography. The main contributions of this dissertation are as follows: a low cost coprocessor based on folding structure in wireless sensor networks is designed. In the process of encryption and decryption, reuse and sharing technology have been adopted to obtain a low-cost and compact structure. Compared with the similar design structure, it has a greater advantage in resources.

The above research is only part of the security research of wireless sensor networks, and there is still a lot of research space for the study of wireless sensor network security. In this paper, we have made some progress in the research of symmetric cryptography in the security mechanism of wireless sensor networks, but there still exist some areas that need to be improved. Future research can be carried out from the following aspects: the circuit implementation of cryptographic algorithms can be optimized in many ways to meet different requirements. This paper is mainly based on low cost architecture, and with area priority taking into account both power consumption and performance, further studies are made. In addition, with power consumption and energy consumption priority, further research different implementation structures of cryptographic circuits can be carried out. With the increasing capability of sensor nodes, it is possible for us to study the application of lightweight public key cryptography in wireless sensor networks, such as applications of elliptic curve cryptosystem.

6 References

[1] Budiman, R. (2013). Utilizing Skype for providing learning support for Indonesian distance learning students: A lesson learnt. Procedia - Social and Behavioral Sciences, 83: 5-10. https://doi.org/10.1016/j.sbspro.2013.06.002.

[2] Jain, A., & Rajpal, N. (2016). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications, 75(10), 5455. https://doi.org/10.1007/s11042-015-2515-7.

[3] Xiao, H. X., Ji, X., & Dong, J. F. (2016). Advanced Encryption Standard algorithm applied research in medical reagent sales management. In International Journal of Engineering Research in Africa (Vol. 21, pp. 209-214). Trans Tech Publications. https://doi.org/10.4028/www.scientific.net/jera.21.209.

[4] Lalitha, R. V. S. S., & Srinivasu, P. N. (2017). An Efficient Data Encryption Through Image via Prime Order Symmetric Key and Bit Shuffle Technique. In Computer Communication, Networking and Internet Security (pp. 261-270). Springer, Singapore. https://doi.org/10.1007/978-981-10-3226-4-26.

[5] Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering, 78, 17-25. https://doi.org/10.1016/j.optlaseng.2015.09.007.

[6] Li, Y., & Cao, Y. (2016). Performance evaluation and analysis of lightweight symmetric encryption algorithms for internet of things. International Journal of Reasoning-based Intelligent Systems, 8(1-2), 84-90. https://doi.org/10.1504/ijris.2016.080072.

[7] Smart, N. P. (2016). Public Key Encryption and Signature Algorithms. In Cryptography Made Simple (pp. 313-347). Springer International Publishing. https://doi.org/10.1007/978-3-319-21936-3-16.

7 Author

Juan Li is with Inner Mongolia Vocational College of Chemical Engineering, Inner Mongolia, China.

Article submitted 24 September 2017. Published as resubmitted by the author 30 October 2017.