Study and Application of Security Based on ZigBee Standard

Maoheng SUN, Yicheng QIAN
College of Electronic and Information Engineering
Tongji University
Shanghai, China
158874395@163.com

Abstract—**Despite, in recent year, ZigBee has wide applications in our lives because of many outstanding advantages, defects of its technology lead to poor application of its security. So it's very important for us to have a study on application of ZigBee security. First of all, this paper analyzes the stack structure of ZigBee protocol. And then it has a discussion on the ZigBee date security features, encryption technology, key management and typical attack models of network. Finally, it introduces a security mode based on Advanced Encryption Standard (AES) algorithm to realize the security application in the ZigBee application support sub-layer (APS).**

Keywords-security; ZigBee; AES; date integrity check

I. INTRODUCTION

ZigBee is an open Wireless Local Area Networks (WLAN) communication technology standard for low data rate network, which is built upon the IEEE 802.15.4 protocol. Because of some advantages of ZigBee such as low-complexity, low-cost, high reliability and so on, the application of WLAN based on ZigBee has penetrated to every aspect of our live; for instance, industrial automation, medical health and intelligent control etc.

Despite of numerous merits, ZigBee still exposes many restrictions, for example, the computing speed of nodes, memory space, the communication ability and the limit of energy consumptions, these defaults make the traditional security mechanism unable to transplant to ZigBee network directly. Hence, it's one of the most popular researches in recent years that how to design a practical security scheme for ZigBee network.

Current most of security modes of ZigBee still stay in theory stage. So the rest will mainly focus on the applications of ZigBee and is organized as follow. In second section, it summaries and analyzes the stack structure of ZigBee, the feature of security system and the types of secret keys. In the third section, according to the structure of frame of APS layer and some typical modes of network attacks, it gives an algorithmic based on AES-128 which is used to encrypt and decrypt the MSG packet. And it presents the flow chart and codes. The conclusions are given finally.

II. TYPE STYLE AND FONTS

IEEE802.15.4 defines physics (PHY) layer and medium access control (MAC) layer [1], while the architecture of ZigBee standard includes network (NWK) layer, application layer and defines the security services. The application layer comprises APS layer and ZigBee devices object (ZDO). The stack architecture of ZigBee is showed in Fig1. [2]-[5].

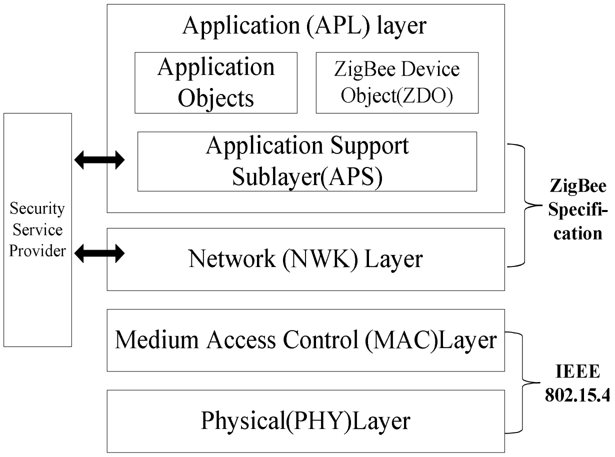
Application (APL) layer
Application Objects
ZigBee Device Object(ZDO)
Application Support Sublayer(APS)
Security Service Provider
Network (NWK) Layer
Medium Access Control (MAC)Layer
Physical(PHY)Layer
ZigBee Specifi-cation
IEEE 802.15.4

Fig1. The stack architecture of ZigBee

ZigBee protocol has inherent security services such as providing encryption, data integrity check and identity authentication. These functions utilize AES-128 encryption technology to ensure the privacy of MAC, NWK and APS layer.

A. Security Suites

There are some features in security of ZigBee technology as following [6]:

1) ZigBee provides data integrality check. It takes advantages of message integrity codes (MIC) to prevent data from being modified by the attackers without secret key. The further function of MIC makes sure that the data were from the side with key. Valid values of MIC are 0, 32, 64 and 128.

2) ZigBee supports the identity authentication service founded on public-key cryptography, which provides a safe means for a device to synchronize messages with another. In addition, it provides authenticity simultaneously for reason of utilizing a common key and has advantages over its counterpart by eliminating the public key directory.

3) ZigBee encryption adopts AES algorithm, which is approved by National Institute for Standards Technology

978-0-7695-4559-2/11 $26.00 © 2011 IEEE
DOI 10.1109/MINES.2011.79

(NIST, [7]), to encrypt input packets and create ciphertext outputs and, in particular, it will be detailed in later chapter.

4) There exists a Trust Center [8] in ZigBee network. Trust Center can decide whether new devices are allowed to join the WLAN or not. In the beginning, it informs all devices with the primal network key encrypted of new one and switching it by broadcasting. Because there is only one Trust Center in secure system, all members will distinguish the new message which Trust Center has issued.

5) ZigBee technology gives three keys: Master, Network and Link.

Master key is the most important and basic key among communicating of nodes. It may be installed during manufacturing devices, or may be set up manually. After being installed, new coming nodes can apply the master key by means of SKKE protocol to set up the link keys together with other nodes in network. Link key spreads unicast messages between two devices in the application layer. Through encrypting link key, we can obtain the network key, which is responsible for the NWK layer. Network encryption uses a network key, shared among all devices in the network, which protects against outsider attack with little resource requirement at devices.

B. Typical types of network attack

ZigBee nodes is always assigned in no man's land, so we often meet with nodes invalidation, destroyed or captured. It’s necessary for us to update and change network nodes. Attackers always tap the communication of nodes by assigning some malice ones or joining a large numbers of false messages to make the network paralysis. There are some typical types of insider network attacks as following: a) Sinkholes; b) Sybil; c) Wormholes.

By researching, we can find out that these network attacks of WLAN have one thing in common: a malice node enters the WLAN and makes other nodes sure that it’s a new legitimate one. Then it can destroy the data packet and even make the network paralysis by altering, discarding or rebroadcasting. So data integrality check and authentication are effective approach against these attacks. In this paper, we will utilize MIC to ensure that the receiver can get data correctly and avoid hostility nodes coming into the WLAN.

C. Security mechanism Based on AES

ZigBee2006 criterion adopts the encryption mode that is the Counter mode with Cipher-block chaining Message authentication code (CCM*) of AES-128 to provide cryptograph and assure integration of data blocks. AES uses Rijndael algorithm. CCM* is obtained from doing some modifications of CCM, which includes all characteristics of CCM. Further, the mode needs only one cryptographic key for all security layers unlike other security modes of MAC layer which require that every security layers has a different key. As a result of its wide applications on all stacks of ZigBee, CCM* may make MAC, NWK and APS use the same key repeatedly.

At present, there are some operation modes of AES as following: CBC, CTR, CFB, CCM and so on. For example, AES-CBC-MAC mode is often used for data integrity check. And AES-CCM mode always supplies combination encryption. Users can choose the corresponding security schemes based on their demands of security.Table1 gives the security levels of ZigBee.

III. Applications of ZigBee Security on APS

It’s complicated to realize the algorithms of ZigBee security. In many ordinary applications, the security modes of ZigBee will cons1ume a lot of resources such as memory, computing time of CPU and management of data frame. First, this paper will simplify the frame of APS layer. Then the packet will be encrypted by using symmetry data integrality check.

A. The frame type of MSG

The MSG frame type of application layer format is showed in Table 2.The field of transmission count and type frame are both 4 bits.

The former specifies number of transmission and the latter indicates that the frame would be MSG type if this value is 0x02. Every packet with MSG type has a transmission sequence (8 bits), length (8 bits) and data.The transmission sequence demonstrates an identification number in order to be responding to the request side. The data compromises original messages and its field is variable in length.

To simplify the encryption algorithm, this paper redefines the MSG frame type. The new structure of it is showed in Table 3. The security data material is 32bits in length, which is divided into two groups in average. The Key

Table 1 The security level of NWK layer and APS layer

Security level identifier	Security Level sub-field	Security Suite	Security Attributes	Data Encryption	Frame Integrity （length M of MIC,Octet）
0X00	000	None	None	No	No(M=0)
0X01	001	AES CBC MAC 32	MIC 32	No	Yes(M=4)
0X02	010	AES CBC MAC 64	MIC 64	No	Yes(M=8)
0X03	011	AEC CBC MAC 128	MIC 128	No	Yes(M=16)
0X04	100	AEC CTR	ENC	Yes	No(M=0)
0X05	101	AES CCM 32	ENC MIC 32	Yes	Yes(M=4)
0X06	110	AES CCM 64	ENC MIC 64	Yes	Yes(M=8)
0X07	111	AES CCM 128	ENC MIC 128	Yes	Yes(M=16)

Table 2 Application Framework with MSG Type

Bits:4	4	8	8	V	V	8	8	V
Tranmissmion count	Type Frame	Transmission sequence	Length	Data	…	Transmission sequence	Length	Data
		Packet 1			…	Packet n		
Application Frame								
Application support sub-layer protocol Data Unit (ASDU)								

（V:variable）

bit sequence and MIC are both 8 bits in length. The sequence number of the first group occupies high four bits of key bit sequence and the sequence number of the second group occupies the low four bits of it.

Table 3 Redefinition of MSG frame type

Bits： 8	8	8	8	V
Transmission sequence	Lenght	Key bit sequence	MIC	Data
		Transmission Data		
Transmission packet 1				

B. *Realization of encryption and decryption*

CBC [9] is a general operation mode for symmetry encryption. And its encryption algorithm comes true by XOR-ing between initialized vector and plaintext.

We make use of a simplified integrity algorithm to implement encryption. During the operation, we make the first plaintext XOR initialized vector and get the later plaintext to XOR the former one. Then the data which have been XOR-ed encrypt with a same key. Thus, there is no fixed relation between input of encryption function and every plaintext packet. So we reach the goal of encryption.

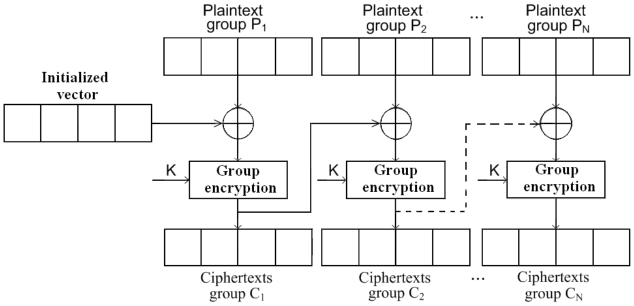

Fig 2 Mode of Encryption Operation

The mode of simplified encryption operation is given in Fig2.If the input secret key is K, plaintext group is $P_1,...,P_N$ and output is $C_1,...,C_N$, the initialization variable defines as C_0 .

The encryption and decryption formulae of this algorithm are given as following:

$$1 \le j \le N, C_j = E_k(C_{j-1} \oplus P_j) \qquad (1)$$

$$1 \le j \le N, P_j = C_{j-1} \oplus D_k(C_j) \qquad (2)$$

C. *Define Variables*

```
unsigned char ency[32]=
{ 0xa6, 0x62, 0xd6, 0x3d, // first group
  0x93, 0x73, 0xad, 0x27,
  0xad, 0xc1, 0x2b, 0x3e,
  0x3b, 0x23, 0x38, 0xa5,
  0xc3, 0x18, 0x45, 0xa4, // second group
  0x8a, 0x32, 0x9d, 0x35,
  0xe9, 0x4e, 0xa2, 0x93,
  0x9e, 0xa3, 0x11, 0x57};
  unsigned char ency_list[8]; // encryption talbe
  unsigned char mic_for, grp_1,grp_2, mic;
```

This security packet ”ency” includes a 32-bits array table which divided into two teams equally.The “ency_list” is a dynamic generation 8-bits data pakcet. The variable “mic_for” is a initialization vector for computing MIC.”mic” is a alterable MSG message integrated code.

D. *Encryption and Decrypiton algorithm*

The encryption algorithm of this paper mainly refers to AES CBC MAC mode as introduced above.And the flow chart is showed in Fig3.

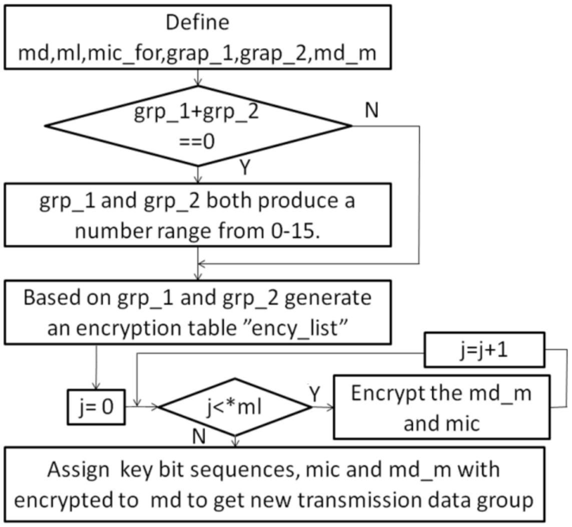
Define md,ml,mic_for,grap_1,grap_2,md_m
grp_1+grp_2 ==0
N
Y
grp_1 and grp_2 both produce a number range from 0-15.
Based on grp_1 and grp_2 generate an encryption table "ency_list"
j=j+1
j= 0
j<*ml
Y
N
Encrypt the md_m and mic
Assign key bit sequences, mic and md_m with encrypted to md to get new transmission data group

Fig 3 Flow Chart of Encryption

The encryption algorithm is described as following:

```
  void Encycrypt(unsigned char*md,int *ml)
{//md:data of MSG;
 //ml:length of MSG;
   grp_1 = 0; grp_2 = 0;
   mic_for = 0x42; //format the MIC
   while ( grp_1+grp_2 == 0)
    {grp_1 = rand()%16;//generate a integer from 0 to 15
     grp_2 = rand()%16;
    }
   grp_2 +=16;
```

```
    for (j=0; j < *ml; j++)
      {mic_for = mic_for ^ md[j];
       md _m[j] = md[j] ^ ency_list[j%8];
       ency_list[j%8]=ency_list[j%8]^ency[(grp_1+8+j)%32]^
       mic_for;
     mic +=md_m[j] ^ ency[(grp_1+j)%32] ;
      } // using CBC mode of AES-128,making data XOR mic and obtaining mic and data with encrypted.
  md[0] = (grp_1<<4) + grp_2 -16; //secret key bit sequence
  md[1] = mic; // MIC
  for (j=0;j < *ml; j++)
      {md[j+2] = md_m[j];
      }
  *ml += 2; // Because of additonal value:secret key bit sequence and mic,the length of former packet should add 2.
}
```

The process of decryption is just opposite. And the flow diagram is in Fig4.

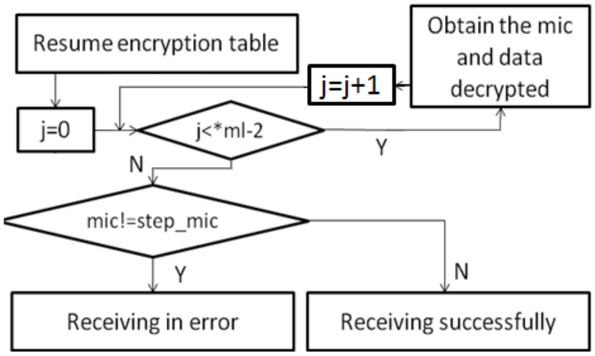

Fig 4 Flow Chart of Decryption

The decryption algorithm is described as following:

```
 bool Decr(unsigned char * md , int *ml)
{ unsigned char step_mic;
   grp_1 = (md[0]>>4) & 0x0f;
   grp_2 = (md[0] & 0x0f)+16;
   for (int j= 0; j< 8; j++)
     {ency_list[i]=ency[(grp_1+j)%32]^ency[(grp_2+ j) %32];
     }//resume encryption table
   step_mic = md[1]; //The recevied MIC is assigned to step_mic.
   mic = 0;
   mic_for =0x42;
   for (j=0; j< *ml -2 ; j++)
     {mic +=md[j+2] ^ ency[(grp_1+j)%32];
      md[j] = md[j+2] ^ ency_list[j%8];
      mic_for = mic_for ^ md[j];
      ency_list[j%8]=ency_list[j%8]^ency[(grp_1+8+j)%32]^
      mic_for;
      }// decryping tha data
    if (mic != step_mic) return false; //compare the computing MIC with receried MIC,if not consistent, it means that
      *ml - = 2;
      md [*ml] = 0;
      return true;
}
```

The“^” and “%”denote XOR and complementation. According to the algorithm, if Decr() return “true”, it gives a signal that the MIC accounting is as same as the received one. So the receiver exactly receives the MSG packet, otherwise, the MSG packet will be discarded.

E. *Critical Analysis*

The proposal not only helps system reduce overhead and complexity, but still keeps the network secured. Every cryptograph group is related with not only the present plaintext, but also the former one by feedback counting. Thereby, even if two identical plaintexts use the same key, they will produce different ciphertext. Thus it is successful to prevent the attackers and tappers from internal attacking or tapping data. So for these typical network attacks as mention, this algorithm has a great defence.Moreover,followed with the flow charts and codes, this method approves to be feasibility and improves the practicability of ZigBee security mechanism.

IV. Conclusion

In this paper, we study security mechanism of ZigBee and some typical network attacks. ZigBee standard adopts the CCM* mode of AES-128 to provide data transmission confidentiality. And it provides many security functions such as: data integrity check, encryption, authentication and so on. Although it has higher security capability, it’s really not perfect. Owing to the confines of communication capability, energy of nodes and computing ability, these aspects restrict applications of ZigBee security in the actual environment. So the paper suggests a simple mode in APS layer based on ZigBee security to protect data from destroying. With the rapid development of WLAN, the problem of security will be more and more serious in future, we should pay more attention to it.

References

[1] Getting Started with ZigBee and IEEE 802.15.4, Daintree Networks, February 2008, http://www.d aintree.net.

[2] ZigBee Alliance. ZigBee Specifications (ZigBee Document 053474r17) [Z]. 20081217.

[3] ZigBee Alliance. ZigBee Specifications (ZigBee Document 053474r13) [Z]. 20061221.

[4] ZigBee Alliance. ZigBee Specifications (ZigBee Document 053474r7) [Z]. 20064228.

[5] ZigBee Alliance. ZigBee Specifications (ZigBee Document 053474r6) [Z]. 200622217.

[6] X. L. Ren, H. B. Yu. Study on Security of ZigBee Wireless Sensor, Network [J] Chinese Journal of Scientific Instrument (in Chinese), Vol28, No 12, December 2007, pp 2132-2137.

[7] National Institute of Standards and Technology. http://www.nist.gov

[8] Y. Xiao, V. K. Rayi and B. Sun, A survey of key management schemes in wireless sensor networks, Computer Communications, vol. 30, no. 11-12, 2007,pp. 2314–2341.

[9] Housley R, Whiting D. Counter with CBC-MAC (CCM) [EB/OL].2002,6,3,http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/ccm.pdf.