2009 International Conference on Computational Intelligence and Security

Study on Security of Wireless Sensor Network Based on ZigBee Standard

Bin Yang
Department of Computer Technology
Shunde Polytechnic
Foshan,China
e-mail: yangbby@126.com

***Abstract*—The security of wireless sensor networks is very important. In order to research the security of wireless sensor networks based on the ZigBee standard, this paper firstly introduces the stack architecture of the ZigBee protocol, security suites,stating the codes of encryption and data integrity authentication algorithm. Then, it analyzes the security defects on wireless sensor networks-- e.g., channel interference, address assignment conflict and route found flooding in the networking; and key-tapping, defects in the encryption without integrity protection and no identity certification in the security services. Finally, it offers some coping methods: setting standby channel setting, improving routing algorithm, using asymmetric authentication and key exchange based on elliptic curve cryptography, etc.**

Keywords- zigbee;security;AES; channel defect; eavesdropping

I. INTRODUCTION

With the rapid development of wireless communication, people's requirements for wireless sensors networks are higher and higher. While pursuing the low price, they still require low consumption, low complexity, and high dependability. ZigBee is such a standard, through which micro-sensors of ZigBee configuration can interconnect with each other to form an Adhoc. It is widely applied to fields such as industrial control, environment controlling, medical treatment and intelligent building to improve industrialization and informationization.

II. STACK ARCHITECTURE OF THE ZIGBEE PROTOCOL

ZigBee standard set up on the IEEE802.15.4, includes physical (PHY) layer, medium access control (MAC) layer, network (NWK) layer and application layer. And it also defines the mechanism of security services. The PHY layer and MAC layer are defined by IEEE802.15.4. The ZigBee stack architecture is shown in Fig. 1[1][2].

The PHY layer mainly accomplishes such functions as On/Off of the Radio transmitter, energy detection (ED), the link quality instruction (LQI), idle channel assessment (ICA), channel selection, and data sending/receiving. It employs 27 channels. The center frequencies and the corresponding channel numbers are stated below [3]:

Fc=868.3 MHz k=0
Fc=[906+2(k-1)] MHz k=1, 2,…,10
Fc=[2405+5(k-1)] MHz k=11, 12,…, 26

MAC layer is responsible for the generating network beacons (by coordinators), synchronizing the beacons, connecting and disconnecting PAN, providing CSMA-CA access mechanism, and establishing reliable communications links between MAC peer entities.

The NWK layer assigns addresses to the devices, which can join and leave the network. It establishes and maintains the routing lists, and does routing for data frames.

The application (APL) layer is divided into the application support sub-layer (APS), the APL layer framework and the ZigBee device objects (ZDO). A ZigBee network is comprised of the coordinator, the full function device (FFD) and the reduced function device (RFD).

III. SECURITY SYSTEM OF ZIGBEE

ZigBee security mechanism has such functions as encryption, integrity checking and authentication, applying to MAC layer, NWK layer or APS layer. It adopts AES-128 encryption for the confidentiality and a series of security mechanism derived from AES algorithm for the integrality and authenticity. Such security mechanism provides security services for network joining device authentication, data transmission, key establishment, key transport, device management, and so on. ZigBee security mechanism is not a single independent protocol, but a set of security elements based on 802.15.4. It is for the easier realization on the platform with weak computing power that AES is selected. Most ZigBee chips at present have built-in AES hardware acceleration circuit to quicken this mechanism processing.

A. ZigBee security suite

According to ZigBee document, CCM* security mechanism of AES-128 shall be used in every layer protocol. CCM* includes all of the features of CCM and additionally offers encryption-only and integrity-only capabilities. It can employ CTR for confidentiality, CBC-MAC for integrity, and the combination of CTR and CBC-MAC for both confidentiality and integrity[4]. The security levels in ZigBee and the AES application scheme are shown in TABEL I.

For example, the header of the MAC layer frame has the 1-bit Flags field indicating whether to be encrypted. The value “1” means to be encrypted, otherwise, not to be

978-0-7695-3931-7/09 $26.00 © 2009 IEEE
DOI 10.1109/CIS.2009.208

IEEE computer society

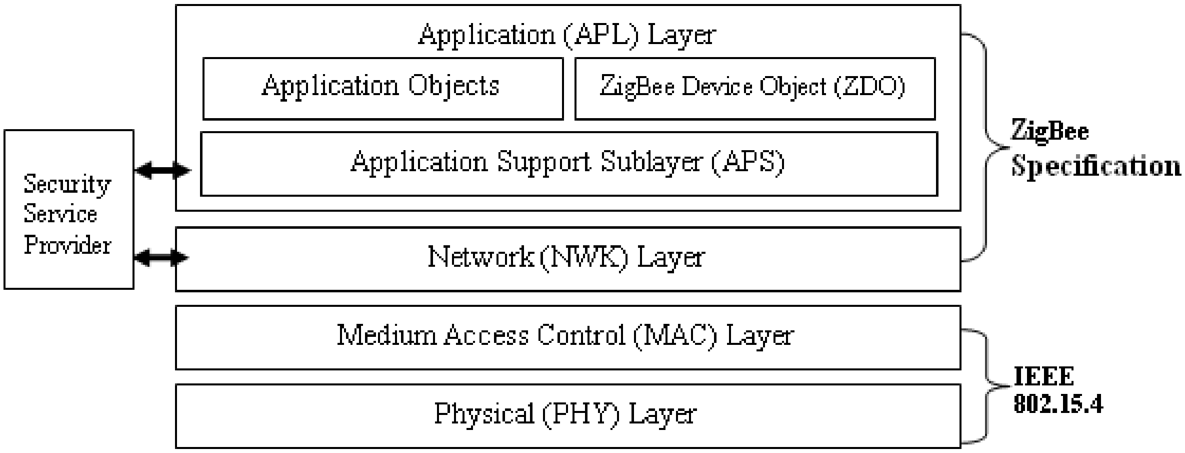
Application (APL) Layer
Application Objects
ZigBee Device Object (ZDO)
Application Support Sublayer (APS)
Security Service Provider
Network (NWK) Layer
Medium Access Control (MAC) Layer
Physical (PHY) Layer
ZigBee Specification
IEEE 802.15.4

Figure 1. Outline of the ZigBee Stack Architecture.

encrypted. If integrity protection is employed, a 4-byte, 8-byte, or 16-byte Message Integrity Code (MIC) can be calculated on the frame header and the payload when transporting a frame, and directly added after MAC Payload. If authenticity protection is employed, a frame and a sequence counter will be added to the left of MAC layer, which can be used to encrypt the payload and ensure its novelty. When receiving a frame with MIC, the device will make the authentication; decryption shall be done if the payload of the received frame is encrypted. The MAC layer maintains a key table, in which the keys are configured when devices join the network. [5].

B. The prerequisites for the operation of AES-128 CCM mode*

The sender and receiver shall have the same definitions of block-cipher encryption function (AES-128 algorithm), cryptographic keys, incoming or outgoing frame counter, key sequence counter or identifier, security level identifier, key length (keylen), and 128-bit block size. Generally, the first order of most-significant-bit is chosen as the bit order of binary strings[5].

The length L of the message length field, in octets, shall have been chosen. Valid values for L are the integers 2 to 8 (the value L=1 is reserved).

The length M of the authentication field, in octets, shall have been chosen. Valid values for M are the integers 0, 4, 6, 8, 10, 12, 14, and 16. (The value M=0 corresponds to disabling authenticity).

The sender's input includes the random value a nonce N of 15-L octets, and the octet strings a and m. The strings a and m through input transformation form the strings AuthData and PlaintextData (both have length divisible by 16), representing authentication data and enciphered data respectively. The string m of length l(m) octets, where $0 \leq l(m) < 2^{8L}$ and the string a of length l(a) octets, where $0 \leq l(a) < 2^{64}$.

C. Data integrity authentication

The symmetric authentication algorithm of AES-CBC-MAC includes encryption, calculation of message and generation of integrity code on cipher block in CBC mode. The authentication operations include calculating integrity code and comparing it with the integrity code received. If the result is consistent the data integrity is proved. The authentication tag T is created as below.

```
Reserved=0
IF l(a)=0 THEN
Adata=0
ELSE
Adata=1
ENDIF
IF M >0  THEN
M1=BIN( (M-2)/2)    // converte (M-2)/2 to binary
```

TABLE I. SECURITY LEVELS AVAILABLE TO THE MAC, NWK, AND APS LAYERS

Security Level Identifier	Security Level Sub-field	Security Suite	Security Attributes	Data Encryption	Frame Integrity (length M of MIC, in Number of Octets)
0x00	000	None	None	OFF	No(M=0)
0x01	001	AES-CBC-MAC-32	MIC-32	OFF	YES(M=4)
0x02	010	AES-CBC-MAC-64	MIC-64	OFF	YES(M=8)
0x03	011	AES-CBC-MAC-128	MIC-128	OFF	YES(M=16)
0x04	100	AES-CTR	ENC	ON	No(M=0)
0x05	101	AES-CCM-32	ENC- MIC-32	ON	YES(M=4)
0x06	110	AES-CCM-64	ENC- MIC-64	ON	YES(M=8)
0x07	111	AES-CCM-128	ENC-MIC-128	ON	YES(M=16)

```
ELSE
M1=0
ENDIF
Flags = Reserved || Adata M1 || L
B0 = Flags || N || l(m)
t= l(AuthData)/16
FOR i=1 to t ,DO
$B_i$ = left((i-1)*16+1, i*16,AuthData)
ENDFOR
$X_0 = 0^{128}$
FOR i=0 to t , DO
$X_{i+1} = E(Key, X_i \oplus B_i)$
ENDFOR
T = left (1,M,$X_{t+1}$ )
```

The authentication tag T is the leftmost M octets of the CBC-MAC value X_{t+1}.

D. Data encryption

ZigBee encryption uses AES-CTR (Counter mode), which encrypts a series of input data blocks, or counting blocks, and creates a series of ciphertext output blocks. The cipher text is the result of XOR-ing ciphertext output blocks and the plaintext data to be protected. The encryption and decryption of CTR do not depend on those of the previous blocks. Therefore, CTR permits the parallel computation on many blocks of plain text and cipher text, utilizing the CPU parallel technology bestly. The process of the data encryption can be described as below.

```
L1= BIN(L - 1)
Flags = Reserved || Reserved || 0 || L1
t= l(PlaintextData)/16
FOR i=0 to t , DO
$A_i$ = Flags || N || Counter i
ENDFOR
FOR i=1 to t , DO
$M_i$ = left((i-1)*16+1, i*16, PlaintextData)
$C_i = E( Key, A_i ) \oplus M_i$
ENDFOR
Ciphertext = left(1,l(m),$C_1$ || $C_2$ ||…|| $C_t$ )
$S_0 = E( Key, A_0 )$
$U = T \oplus$ left(1,M,$S_0$ )
C = Ciphertext || U
```

If all the above operations have succeeded, then output the encrypted message C, which is the right-concatenation of the encrypted message Ciphertext and the encrypted authentication tag U, Otherwise, output 'invalid'.

IV. ZigBee Security Problems

A. Channel Defects

ZigBee uses 868MHz (1 channel, 20kbit/s), 915MHz (10 channels, 40kbit/s), 2.4 GHz ISM bands (16s channel, 250kbit/s, O-QPSK modulation). However, most wireless LANs currently operate at 2.4 GHz (2.4~2.483 GHz) ISM band, such as Bluetooth, wireless USB and Wi-Fi (IEEE 802.11b/g), plus cordless phones and microwave ovens, which makes this frequency band very crowded and noisy.

The comparison between channel frequencies for IEEE 802.11 b and IEEE 802.15.4 shows that only four IEEE 802.15.4 channels (n = 15, 16, 21, 22) fall in two IEEE 802.11b frequency intervals. So when ZigBee and Wi-Fi coexist, the channel number available for ZigBee will greatly reduce (See Fig. 2). Since most 2.4 GHz cordless phones work at 5 ~ 10MHz channel width, interference from cordless phones employing FHSS can absolutely interrupt an operation on the ZigBee network [6].

The channel for Zigbee network is defined when the network is established and all nodes are sharing this channel without dynamic handover. This version and formers of Zigbee-2006 do not support the dynamic channel switch. If an interference source joins after the Zigbee channel has been determined, the channel cannot change on its own, resulting in the retransfer of a large amount of data frames by interference, or even network interruption.

For example, when ZigBee works in 18th channel(2440MHz) of IEEE 802.15.4 and newly-joined Wi-Fi in 7th channel(2442MHz) of IEEE 802.11 b, both channels overlap. In such case, the BER of data frame is 89.2% for 16-byte frames and 91.7% for 32-byte when the distance between a ZigBee node and a Wi-Fi node is 10 cm; while the result becomes 14.8% and 16.7% respectively when the distance is 50 cm. Experiments show that communication will be seriously interfered if the ZigBee channel overlaps a frequently used Wi-Fi channel.

Although ZigBee 2007 specification has an additional function Frequency Agility, a large number of devices and terminals which can only support ZigBee 2006 have not. And there exists a compatibility problem between the devices and terminals.

In addition, ZigBee star- or cluster-network is rather sensitive to the fault of a single node , then being unreliable, especially the damaged of a network coordinator, which makes communication unworkable. Data can only be transmitted slowly in spite of ZigBee mesh network technology, because excessive nodes will increase the delays in message delivery and the costs of communication.

B. Network address assignment and routing defects

In ZigBee network the addresses distributed to the nodes can be changed or even repeated in some cases, e.g. a node or a coordinator is removed or damaged, or rejoined in, or a network is reconstructed. So it is difficult to send the data to the correct destination.

ZigBee employs on-demand routing algorithm AODVjr, which is based on flooding diffusion method when the routing is unknown. In a large-scale network with many nodes, RREQ messages controlled by routing increase sharply, creating network overload and congestion and greatly reducing the network performance. Therefore, in order to reduce the routing message number of the network is the key to improve the performance. By the way, the implementation of such functions remain to be solved as routing repair and best routing.

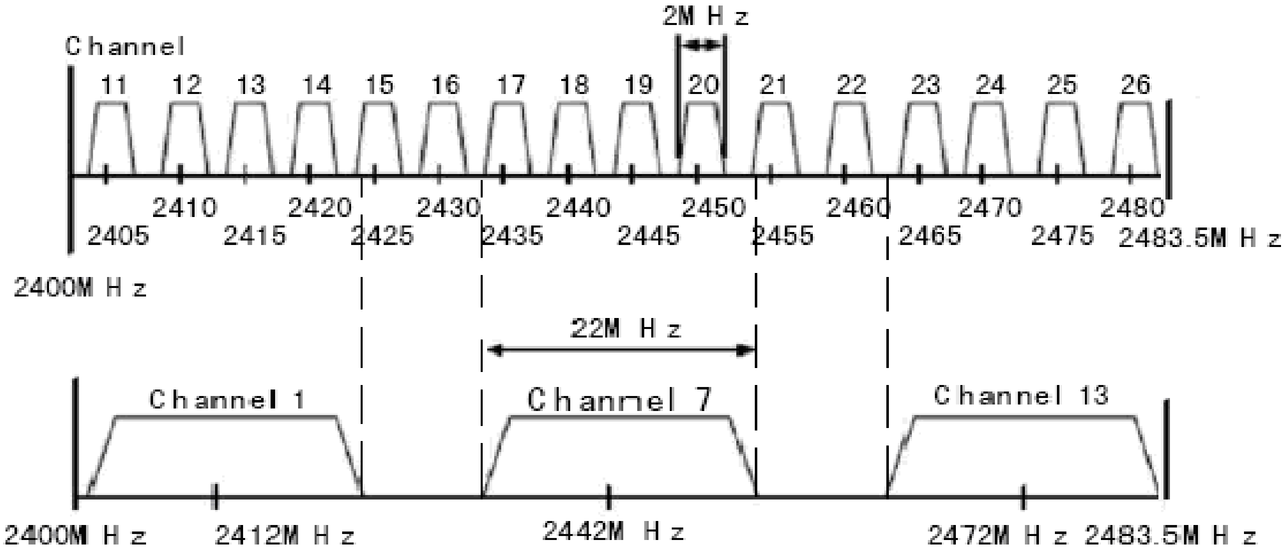

Figure 2. Comparison between Channel Frequencies for IEEE 802.11b and IEEE 802.15.4.

C. *Communication key eavesdropping*

The ZigBee security bases on AES, which is a symmetrical encryption algorithm. Both parties shall negotiate the keys for encryption before communication. But during the negotiation illegal eavesdropping cannot be prevented, especially in the course of the networking or a new node joining. In this case, attackers can easily tap the keys during the key distribution. And wireless sensor network nodes in the open country often become the targets. On the other hand, methods of energy attack, cache attack and bypass attack on AES are increasingly emerging. The National Institute of Standard and Technology estimated that AES-128 encryption will have been safe by 2036. Yet this deadline is likely to come earlier due to the technological progress. A method has been brought forward which uses cache hit as side channel attack on AES encryption in OpenSSL v.0.9.8(a). Under the condition of Intel Celeron 1.99 GHz and Pentium4 3.6 GHz CPU, this technique regains within 5 minutes the AES 128-bit keys in OpenSSL v.0.9.8(a) by employing RedHat v2.4.20-8 and gcc v3.2.3 on 2^{21} and 2^{25} samples of random plaintext samples [7].

In addition, with the growth of number of terminals, the number of cipher keys will increase rapidly. Since a N-node network has(N×(N-1))/2 keys, the number of keys on a 100-node network will reach (100 ×99) / 2 = 4950. The growth of the keys will lead to the complexity of management and the reuse of Nonce for key generating, then increasing security risks.

D. *Defects in the encryption without integrity protection*

ZigBee provides encryption-only without integrity protection in the security scheme. If AES-CTR adopted, the data-frame protection can only rely on the CRC check and the message can easily suffer tampering or denial-of-service attacks due to the limited CRC protection. Additionally, 802.15.4 protocol has no definite requirement of integrityprotection for confirm packages, on which the attacker can capitalize and forged such packages. On the other hand, integrity-only security scheme without encryption is subject to replay attacks [8].

E. *No anti-denying*

ZigBee has no identity authentication mechanism and no anti-denying capability. In the times when attacks on the wireless sensor network are increasingly diversed and automated, ZigBee is subject to impersonation attack. Because node authentication avoids denying of message sent, public key mechanism or digital signature can be adopted.

V. SUGGESTIONS FOR IMPROVEMENT

A. *To set spare channels*

Due to the increasing popularity of WI-FI network, WI-FI channel will greatly interfere the 2.4G ISM channel ZigBee employs. Therefore, in the ZigBee networking and idle channel assessment, WI-FI space channels, namely the channels 15, 16, 21 and 22, must have priority and backup coordinator and spare channels must be set. When the BER exceeds 20%, the coordinator shall broadcast commands and all the devices enable the spare channels, saving the networking time and the device energy.

B. *To modify routing*

A modified routing algorithm is recommended, which combines AODVjr with tree routing to reduce RREQ (route request message) transmission. In the routing list the field of status extends 10 bits, two for routing energy level and eight for time stamp. Routing energy status is defined as the value of the minimum-energy node in the path of the routing established, and it is divided into 4 grades: good, normal, poor and dangerous. In the time stamp , the first four is for month and the last four is for serial numbers in 2 days, which aims at calculating the aging time of the routing and the energy consumption of nodes. In routing selection and routing discovery, in accordance with the information about the link cost, energy level, aging time, energy consumption and mobile probability of nodes, it assesses the reliability of the routing and reduces the transmission of link-state data frames to save the battery energy. Once the router energy is in the form of danger, it sends routing-maintenance messages without delay to other routers for timely routing updated.

In addition, if the amount of data transmission is less and routing rediscovery is needed, data can be carried by the route discovery frame for high transmission efficiency. In two-way interactive data between nodes, piggybacking can be used in data frame transmission to reduce traffic load, save node energy, and improve ZigBee network performance.

C. To add ECMQV security suite

Based on Elliptic Curve Cryptography (ECC), ECMQV is a scheme of asymmetric authentication and key exchange [9], functioning as identity authentication and session key negotiation between both parties in communication. ECMQV with 160-bit key length can obtain 1,024-bit encryption strength through RSA algorithm and it employs implicit authentication reducing public-key computing costs. Obviously, ECMQV has many advantages of high security, low calculating cost, and the like.

With ECMQV security suite ZigBee can avoid key-tapping and attack from false identity through effectively authenticating the identity of both sides in communication.

VI. Conclusion

ZigBee standard has higher security because it adopts CCM* mode of operation with AES-128 encryption algorithm, which offers functions such as encryption, integrity checking and authority identification. And yet, ZigBee has security problems in the circles such as channel interference, address conflict, encryption strength and non-repudiation. Therefore, ZigBee is still a technical standard to be improved though it has been developing from the version 1.0 to version 2007.

Acknowledgment

First I would like to thank Dr. Hu Xuan-zi who gave me the opportunity to attend the 2009 International Conference on Computational Intelligencer Seanity. I also thank the support by Guangdong Foundation of Science and Technology Project (2006A10203004), The Guangdong-Hong Kong Technology Cooperation Funding Scheme (Foshan Section,2006Z1), The Shunde Polytechnic Foundation of Science and Technology Project (2008-KJ01).

References

[1] ZigBee Alliance, ZigBee Specifications (ZigBee Document 053474r17). ZigBee Alliance, January 2008.

[2] ZigBee Alliance, ZigBee Specifications(ZigBee Document 053474r13), ZigBee Alliance, October 2006.

[3] IEEE Std, 802.15.4-2003, Wireless Medium Access Control and Physical Layer Specifications for Low Rate Wireless Personal Area Networks, IEEE, 2003.

[4] NIST, Advanced Encryption Standard (AES) ,FIPS PUB 197, November . 2001.

[5] D. Whiting , R. Housley , N. Ferguson , “Counter with CBC-MAC(CCM)”, http://tools.ietf.org/html/rfc3610, September 2003.

[6] Li Jiao, Yang Renkun,Xiao Jun, “Anti-interference Performance of ZigBee and Analysis of the Mechanism of Coexistence in 2.4GHz ISM Band”,Telecom Engineering Technics and Standardization, March 2006,PP.31-35.

[7] DENG Gao-ming, ZHAO Qiang, ZHANG Peng, CHEN Kai-yan, “Cache Hit Side Channel Attack Based on AES”, Computer Engineering, Vol.34 No.13, July 2008.PP.113-114.

[8] Qiu hui-min, Yang yi-xian , “Research on security mechanism of IEEE 802.15.4”, The Eleventh National Youth Conference on Communications ,china,2006.PP.987-990.

[9] M. Blaser, “Industrial-strength Security for Zigbee: The Case for Public-key Cryptography” , Embedded Computing Design,MAY 2005.