ZigBee 的 MAC 层安全研究

徐 健，李小珉
（海军工程大学 电子工程学院，湖北 武汉 430033）

摘 要：对ZigBee协议MAC层的安全性进行了研究，分析了MAC层使用的安全模式，提供的安全服务以及实现相应安全服务的安全方案。对其中一种具有代表性的安全方案CCM算法进行解析并给出应用实例。

关键词：ZigBee；安全；CCM算法

中图分类号：TN914 文献标识码：A

Security study of MAC layer in ZigBee

XU Jian, LI Xiao Min
(College of Electronic Engineering, Naval Univ.of Engineering, Wuhan 430033,China)

Abstract: This paper studies on the security of MAC layer of ZigBee, analyzes the security patterns, the security services and corresponding security suites. Analyzes the CCM algorithm, a representative algorithm of the security suites, and gives the application example. This contributes to understand the security protocol of the MAC layer better.

Key words: ZigBee; security; CCM algorithm

ZigBee具备省电、可靠、成本低、容量大、安全等诸多优势[1-2]，随着ZigBee协议的不断完善和发展，ZigBee技术越来越为人们所认识和接受，逐渐被应用到无线局域网、家庭自动化、智能建筑、工业自动化、水电气的综合抄表系统、智能交通系统、环境和健康监测以及电子玩具等领域。

信息安全是现代通信中一个至关重要的问题，是信息网络正常运行的基础，ZigBee技术提供可选的安全架构，保证了无线传感网络的可靠性[3]。

本文主要针对ZigBee的MAC层安全进行研究，在对MAC层安全方面进行剖析的基础上对CCM算法进行介绍。

1 MAC帧安全

ZigBee提供的安全服务是在应用层已经提供密钥的情况下的对称密钥服务。在ZigBee MAC层中，以帧为单位提供了4种帧安全服务，为了适用各种不同的应用，设备可以在3种安全模式中进行选择[4-5]，由用户在上层决定。

1.1 安全模式

ZigBee的MAC层在数据传输中提供了如下三级安全模式，由用户在上层协议中决定使用哪一种。

(1)无安全模式，MAC层默认的安全模式。处在这种模式下的设备不对接收到的帧进行任何安全检查。当某个设备接收到一个帧时，只检查帧的目的地址。如果对某种应用的安全要求不高时，可以采用该模式。

(2)访问控制列表ACL (Access Control List)模式，为通信提供了访问控制服务。高层可以通过设置MAC子层的ACL条目指示MAC子层根据源地址过滤接收到的帧。因此这种方式下的MAC子层没有提供加密保护，高层有必要采取其他机制来保证通信安全。

(3)安全模式，同时使用访问控制和帧载荷密码保护，提供了较完善的安全服务。

1.2 MAC层安全服务

根据上层选择的安全模式，MAC层可以为发送和接收帧提供相应的安全服务。ZigBee支持以下4种服务：

(1)访问控制：不对发送和接收的帧进行任何修改和检查，只是让接收帧的设备根据接收帧中的源地址对帧进行过滤。

(2)数据加密：使用指定的密钥对帧中的载荷进行加密处理，并将加密后的数据重新放在帧的载荷部分，但对帧的其他部分不进行加密处理。加密处理完成后，MAC层将重新计算帧的FCS。

(3)帧完整性：帧完整性提供的安全服务使用信息完整码MIC (Message Integrity Code)，可以防止对信息进行非法修改。数据、信标和命令帧均可用这种服务进行处理。

(4)序列号更新：MAC层帧头有一个序列号域，其值为该帧的唯一序列号。设备接收到一个帧后，MAC层管理实体将接收的帧的序列号与保存的序列号做比较。如果接收的序列号比保存的序列号新，则保留、上传接收的帧，同时更新保存的序列号；否则，丢弃该帧。这种方法保证了接收的帧是最新的，能够避免帧重发攻击。

1.3 MAC层安全方案

当MAC层按上层要求对传输的帧进行安全处理时，MAC层按指定的安全方案实现相应的安全服务。安全方案由对帧载荷进行安全处理的操作组成，安全方案的名称指明了对称加密算法、模式、完整性码位长度等。ZigBee协议中，所有的安全方案使用的加密算法都是高级加密标准AES。

2 CCM算法研究

CCM是MAC层安全方案中的一种，提供了全部4种安全服务，由计数器CTR(Counter)模式和密码分组连接消息认证码CBC-MAC (Cipher Block Chaining-Message Authentication Code)对称认证算法相结合构成。该算法首先利用CBC-MAC计算MIC，然后用CTR对MIC和明文数据进行加密，输出则由加密的数据和加密的完整码组成。在CCM算法中，要确定2个参数。第1个是认证字段的长度M，即选取的MIC长度。它的有效值是4 B、6 B、8 B、10 B、12 B、14 B和16 B。第2个是表示消息字段的长度L，有效值是2 B~8 B。

2.1 输入

要发送一个消息，必须提供如下信息：

(1)分组加密的密钥K；

(2)15-L字节长的现时值N。在使用同一个密钥加密的过程中，不能出现重复的现时值；

(3)要发送的消息m。它的长度范围是$0 \leqslant l(m) \leqslant 2^{8L}$ B，即能够用LB的长度来表示；

(4)附加认证数据a。它的长度范围是$0 \leqslant l(m) \leqslant 2^{64}$ B。附加认证数据只用于计算认证码，不加密，也不包含在输出分组中。

2.2 认证

CCM的第1步是用CBC-MAC计算认证码T，即MIC。首先定义一系列分组B_0，B_1，…，B_n，然后用于CBC-MAC。第1个16字节分组B_0的格式如表1所示。

表1 第一个分组认证B_0

字节序号0	1, …, 15-L	16-L, …, 15
标志$flag$	现时值N	$l(m)$

其中标志字节格式如表2所示，预留位作为将来的扩充，设为0；Adata位用于指示是否有附加认证数据，当$l(a)$=0时，Adata设为0，否则设为1；3位M域表示整数$(M-2)/2$；3位L域表示整数L-1。

表2 认证标志字节

比特位7	6	5~3	2~0
预留	Adata	M	L

如果$l(a)$>0，则通过对$l(a)$和a的编码会增加一些分组。首先对$l(a)$进行编码，得到$l(a)$字段$L(a)$：

(1) 0<$l(a)$<216-28，则$L(a)$以2个字节对$l(a)$值进行编码；

(2) 216-28 ≤ $l(a)$<232，则$L(a)$有6个字节，前2个字节是0xFFFE，后4个字节以最高有效位在前对$l(a)$进行编码；

(3) 232 ≤ $l(a)$<264，则$L(a)$有10个字节，前2个字节是0xFFFF，后8个B以最高有效位在前的方式对$l(a)$进行编码。

把生成的$L(a)$与附加认证数据a级联，生成的数据划分为16 B的分组，最后一个分组不足16 B时用0补足，再把生成的数据分组添加在B_0之后。

附加认证数据之后添加消息分组。把发送的消息划分为16 B的分组，最后一个分组不足16 B时用0补足。这样就得到了数据分组$B_0, B_1, \cdots, B_n$，然后通过CBC-MAC计算消息认证码T。

$$X_1 = E(K, B_0)$$

$$X_{i+1} = E(K, X_i \oplus B_i) \qquad i = 1,2,\cdots,n$$

$$T = MSB_M(X_{n+1})$$

其中：$E(\ )$表示AES加密，K是共享密钥，X_i是加密输出分组，MSBM(X_n+1)表示CBC-MAC链式加密最后一次输出分组的最高M个有效字节。

2.3 加密

计算好消息认证码后，使用CTR对明文数据和消息认证码进行加密。CTR的密钥流分组定义为：

$$S_i = E(K, A_i) \qquad i = 1,2,\cdots$$

其中输入分组A_i的格式如表3所示：

表3 加密分组A_i

字节序号0	1, …, 15-L	16-L, …, 15
标志flag	现时值N	计数器i

标志flag的格式如表4所示，2个保留位用以将来扩展设为0；5~3位设为0，以用来区分B0，B0块在该位区对M的编码是非0的；3位L域代表整数L-1，其编码方式和B0一样。

表4 加密标志字节

比特位 7~6	5~3	2~0
预留	0	L

消息明文 m 与级联密钥流 $S_1,S_2,S_3,\cdots$ 的前 $l(m)$ 个字节进行异或运算得到加密的消息。第一个密钥流 S_0 用来加密消息认证码 T，得到加密的认证码：

$$U = T \oplus MSB_M(S_0)$$

最后得到的 CCM 加密认证后的数据 c 是加密的消息级联加密的认证码。

2.4 解密

解密时，必须获知以下信息：分组加密的密钥 K、现时值 N、附加认证数据 a、加密认证后的数据 c。

首先计算密钥流 S_i，把密文和密钥流“异或”恢复出消息 m 和认证码 T。利用恢复出的消息 m 和附加认证数据再次计算认证码，并与恢复得到的 T 进行比较。如果认证码不正确，接收机将只指示完整性验证失败，而不会有其他任何信息。

2.5 应用实例

已知条件如下：

(1)参数 M 取值为 8，L 取值为 2；

(2)密钥长度为 128bit，设为：K=8E 28 B0 31 6D 2B 85 1D 61 C6 72 F7 00 78 6A 8D

(3)现时值 N 为 15−L，则 N 为 13，设为：N=A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC

(4)要发送的消息数据为：m=01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17

(5)附加认证数据为:a=B0 B1 B2 B3 B4 B5 B6 B7

2.5.1 认证变换

(1)形成认证标志字节：$flag$=59

(2)第一个认证分组 B_0=59|A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC|00 17；

(3)对 $l(a)$进行编码得到 $L(a)$=00 08，并与附加认证数据 a 右连接并分组，不足 16 B 用 0 补足得到：$L(a)|a$=00 08| B0 B1 B2 B3 B4 B5 B6 B7|00 00 00 00 00 00。

(4)添加消息分组，不足 16 B 用 0 补足得到数据分组，再计算求得 X_i 值，如表 5 所示。

(5)求得消息认证码 T=E9 79 A8 2C 70 4F 97 36。

2.5.2 加密变换

(1)形成加密标志字节：$flag$=01。

(2)定义 A_i 的值，并计算 S_i，如表 6 所示。

(3)将 S_i 进行级联并取前 $l(m)$个字节与消息明文 m 进行异或运算，得到加密的消息 C=98 A6 DC 6C B0 4A BD 9D E5 E5 3F 03 9E B8 F7 F0 04 5E FF 5C C6 73 D7。

(4)将第一个密钥流 S_0 的前 M 个字节和消息认证码 T 进行异或运算，得到加密的认证码 U=6D F3 9B 3C 76 80 2B 53。

(5)最后得到输出的密文 c=98 A6 DC 6C B0 4A BD 9D E5 E5 3F 03 9E B8 F7 F0 04 5E FF 5C C6 73 D7 6D F3 9B 3C 76 80 2B 53。

以上即是一个 CCM 认证加密过程，解密的过程较

表5 B_i和X_i的值

i	B_i	X_i
0	59 A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC 00 17	
1	00 08 B0 B1 B2 B3 B4 B5 B6 B7 00 00 00 00 00 00	41 F1 1E 4D 7B 18 9D 78 B7 19 07 38 44 53 2F 88
2	01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10	F1 73 7E 7A 87 92 3E 59 4B 8E 17 CD 84 39 67 35
3	11 12 13 14 15 16 17 00 00 00 00 00 00 00 00 00	1C 36 6A D9 4E 98 81 A3 E1 4F 3C A6 A5 15 E5 98
4		E9 79 A8 2C 70 4F 97 36 96 54 87 5D 82 14 39 D6

表6 A_i和S_i的值

i	A_i	Si
0	01 A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC 00 00	84 8A 33 10 06 CF BC 65 A2 0D 95 AB 9F BB A6 9F
1	01 A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC 00 01	99 A4 DF 68 B5 4C BA 95 EC EF 34 0F 93 B6 F8 E0
2	01 A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC 00 02	15 4C EC 48 D3 65 C0 61 1B C3 60 EB 31 B4 2A 17

（下转第42页）

（上接第38页）

为简单，是一个逆过程，在此不用实例进行表述。

ZigBee技术是最新的短距离无线通信技术之一，其安全方面越来越受到人们的关注。本文主要针对ZigBee的MAC层安全进行分析，介绍了MAC层的安全结构。对其中的一种安全方案CCM算法进行了详细的研究，该算法提供了数据完整性检查、加密等功能，可以提供高质量的安全防护。通过对MAC层的安全研究，了解MAC层所提供的安全功能，便于进一步开展ZigBee技术的安全研究。

参考文献

[1] ZigBee specification. http://www.zigbee.org ,2008.

[2] 胡江.ZigBee无线传感器网络安全性分析[J].科技论坛,2007

[3] 周公博,韩振铎,胡宁宁. ZigBee标准的密钥协商机制分析[J].电子技术应用,2007,33(10):61-69.

[4] 吕治安. ZigBee网络原理与应用开发[M]. 北京:北京航空航天大学出版社,2008:76-79.

[5] 翟雷,刘盛德,胡咸斌. ZigBee技术及应用[M]. 北京:北京航空航天大学出版社,2007.

(收稿日期：2009-06-21)