文章编号:1001-5132（2009）02-0170-05

基于嵌入式平台 802.16 AES-CCM 算法的优化及实现

项士标，何加铭*

（宁波大学 通信技术研究所，浙江 宁波 315211）

摘要：通过深入分析 AES-CCM 算法原理，对 AES 算法中运算量最大的轮变化过程进行优化，将轮变化中的 4 个步骤转变为查表和异或运算，进一步简化了算法的执行过程；并对 802.16 协议中 CCM 模式应用规则存在的安全隐患提出了改进措施，增强了算法在抗重放攻击方面的能力. 通过在富士通 3400 WiMAX 开发板“ARM+VxWorks”平台下设计和实现了采用 AES-CCM 算法的数据传输加密方案，最后采用应用模块对算法进行测试，结果表明了改进后算法模块的正确性和有效性.

关键词：AES-CCM; WiMAX；加密；嵌入式系统
中图分类号：TP393.03　　文献标识码：A

在各种通信设备和终端电子产品设计方法中，为使产品具有更强大的功能，越来越多地采用了嵌入式系统，WiMAX 无线通信设备亦是如此. 因此，在设计和开发现代网络和通信技术中的安全技术时，必须同嵌入式技术结合在一起. 因此，笔者提出并实现了一种基于 AES-CCM 加密算法和“ARM+VxWorks”嵌入式系统的 WiMAX 无线接入设备加密技术解决方案，并给出了算法模块在设备中的应用方法.

1 算法介绍

AES 对称密码已经广泛应用于数据的保密和数据完整性认证. 在具体运用时，都会选择相应的具体工作模式. 其中 CCM 模式(Counter with Cipher Block Chaining-message Authentication Code)是可同时提供加密和鉴别服务的全新操作模式.

2004 年 5 月公布的+SP800-38C 文件中，NIST 将 CCM 列为 AES 的认证保密模式的建议标准，同时 CCM 也被 IEEE 指定为用于无线局域网的标准(IEEE 802.11)，并被包含在 RFC3610 中. 在 802.16 协议中，参照 802.11 协议，也采用 AES-CCM 算法做为新的数据加密算法来取代 DES-CBC 算法[1].

2 算法改进

2.1 AES 算法优化

AES 算法加密过程由 4 个不同的处理阶段组成，称为字节代换、行移位、列混淆、轮密钥加. 在输入数据数组 State 进行 10 轮上述处理后，得到加

收稿日期：2008-10-13.　　宁波大学学报（理工版）网址: http://3xb.nbu.edu.cn
基金项目：国家自然科学基金（60671037）；宁波市工业攻关项目（2007B10051）.
第一作者：项士标（1982－），男，浙江宁波人，在读硕士研究生，主要研究方向：无线通信. E-mail: xsbceq@163.com
*通讯作者：何加铭（1949－），男，浙江杭州人，博士/教授，主要研究方向：无线通信. E-mail: jmhe@mail.nbptt.zj.cn

密密文[2].

由于 AES 算法需要执行 10 轮轮处理过程, 因此算法的主要运算都是在轮处理过程中. 笔者提出了一个改进轮处理过程的方法, 以简化算法执行过程.

目前常用的方法是在轮变换前, 计算出 S 盒[3], 并将其存于 16×16 数组中, 在字节代换时才直接查询数组. 虽然该方法能在字节代换阶段简化算法执行过程, 但未能简化后 3 个阶段的执行步骤. 本文在此基础上提出的方法是进一步计算 1 个 4×4 的数组, 使得最终矩阵可直接由查询所得值异或运算后得出.

假设初始 State 矩阵中数据为 a_{ij}, 经字节变换即 S 盒变换后, 该数据标记为 $S[a_{ij}]$, $S[\ ]$则表示 S 盒的变换. 由于行移位只是将 State 矩阵中数据变换了位置, 实际并没有改变数据的值, 因此将行移位后 State 中的数据标记为 $S'[a_{ij}]$. 假设密钥字节数据为 k_{ij}, 轮密钥加后数据为 t_{ij}, 则列混淆和轮密钥加可由下式表示:

$$\begin{bmatrix} t_{0j} \\ t_{1j} \\ t_{2j} \\ t_{3j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} S'[a_{0j}] \\ S'[a_{1j}] \\ S'[a_{2j}] \\ S'[a_{3j}] \end{bmatrix} \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix}.$$

上式可变化如下:

$$\begin{bmatrix} t_{0j} \\ t_{1j} \\ t_{2j} \\ t_{3j} \end{bmatrix} = \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \cdot S'[a_{0j}] \oplus \begin{bmatrix} 03 \\ 02 \\ 01 \\ 01 \end{bmatrix} \cdot S'[a_{1j}] \oplus \begin{bmatrix} 01 \\ 03 \\ 02 \\ 01 \end{bmatrix} \cdot$$

$$S'[a_{2j}] \oplus \begin{bmatrix} 01 \\ 01 \\ 03 \\ 02 \end{bmatrix} \cdot S'[a_{3j}] \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix},$$

$$\begin{bmatrix} t_{0j} \\ t_{1j} \\ t_{2j} \\ t_{3j} \end{bmatrix} = \begin{bmatrix} 2S'[a_{0j}] \\ S'[a_{0j}] \\ S'[a_{0j}] \\ 3S'[a_{0j}] \end{bmatrix} \oplus \begin{bmatrix} 3S'[a_{1j}] \\ 2S'[a_{1j}] \\ S'[a_{1j}] \\ S'[a_{1j}] \end{bmatrix} \oplus \begin{bmatrix} S'[a_{2j}] \\ 3S'[a_{2j}] \\ 2S'[a_{2j}] \\ S'[a_{2j}] \end{bmatrix} \oplus$$

$$\begin{bmatrix} S'[a_{3j}] \\ S'[a_{3j}] \\ 3S'[a_{3j}] \\ 2S'[a_{3j}] \end{bmatrix} \oplus \begin{bmatrix} k_{0j} \\ k_{1j} \\ k_{2j} \\ k_{3j} \end{bmatrix}.$$

最后可以发现轮变换结果 t_{ij} 为 $S'[a_{ij}]$ 与密钥 k_{ij} 的异或运算. 再设

$$\begin{bmatrix} 2S'[a_{0j}] \\ S'[a_{0j}] \\ S'[a_{0j}] \\ 3S'[a_{0j}] \end{bmatrix}, \begin{bmatrix} 3S'[a_{1j}] \\ 2S'[a_{1j}] \\ S'[a_{1j}] \\ S'[a_{1j}] \end{bmatrix}, \begin{bmatrix} S'[a_{2j}] \\ 3S'[a_{2j}] \\ 2S'[a_{2j}] \\ S'[a_{2j}] \end{bmatrix}, \begin{bmatrix} S'[a_{3j}] \\ S'[a_{3j}] \\ 3S'[a_{3j}] \\ 2S'[a_{3j}] \end{bmatrix},$$

分别为 $Y_1[a_{ij}], Y_2[a_{ij}], Y_3[a_{ij}], Y_4[a_{ij}]$. 轮变换输出共有 4 列, 因此共有 $Y_1[a_{ij}] \sim Y_{16}[a_{ij}]$ 个值.

在轮变换前将 16 个单元值全部计算出, 存储于 4×4 的二维数组中. 则在一轮轮变换时, 只需 16 次的查表操作和 64 次异或运算即可求得当前轮变换的最终矩阵值, 大大简化了运算复杂程度, 减少了轮变化时间.

2.2　WiMAX 中 CCM 应用规则改进

在 802.16 协议中规定 PDU 数据包加密后结构如图 1[4]:

GMH(6 Byte)	PN(4 Byte)	DATA	ICV(8 Byte)	CRC(4 Byte)

图 1　PDU 加密后数据结构

6 Byte 的包头和 4 Byte 的 PN 无需经过加密处理. PN(Packet Number)在协议中被规定用于防止重放攻击, 如当前收到的数据包的 PN 小于前 1 个数据包的 PN 时, 当前收到的数据包将被丢弃. PN 在发第 1 个包时值为 1, 以后每发 1 个包则加 1. 由于 PN 和包头都未经加密处理, 当窃听者得到 1 个 PDU 时, 也将得到当前 PN, 并推导出以后各个数据包的 PN 值. 因此引进 CCM 模式虽然能提高攻击者进行重放攻击的难度和成本, 但并不能在技术上彻底防止重放攻击.

可采用对 PN 进行加密处理来防止由于 PN 值泄露而遭受可能的重放攻击. 加密算法选择 AES 算法, 密钥为 802.16 协议中的 KEK(密钥加密密钥). 鉴于 AES 及 KEK 在系统中是用于对 TEK(传输加

密密钥)进行加密处理的，本身已经存在于系统中，而且被良好的设计，并且在控制信息交互的过程中，KEK 定时更新. 因此采用该方法不会给系统带来额外的开销，不需要引入新的加密算法以及维护密钥. 采用该方法 PDU 加密后的结构如图 2 所示.

图 2 PN 加密处理后数据结构

由于对 PN 进行 AES 加密处理，因此加密后的 PN 长度将为 16 Byte，比原来仅增加了 12 Byte 的额外消耗. 因此为提高安全性和抗攻击性，牺牲如此少的传输效率是值得的.

3 AES-CCM 算法实现及结果分析

算法模块基于富士通的 3400 WiMAX 开发板“ARM+VxWorks”平台开发，采用通用 C 库函数，因此可以方便移植到各种需要安全加密处理的嵌入式产品中.

程序提供AES算法接口和AES-CCM算法接口. 前者可用于对传输加密密钥 TEK 的加密处理，后者则可用于对传输数据的加密处理，使用者只需简单的调用函数即可. 程序结构如图 3 所示.

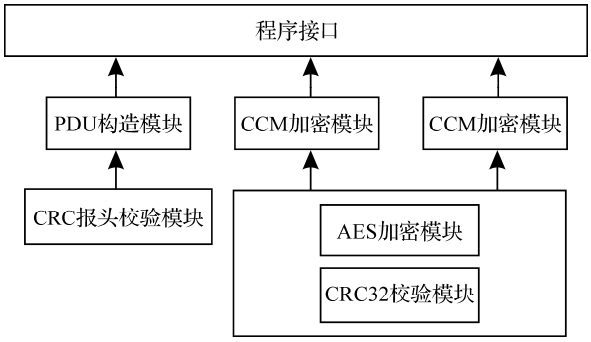

图 3 算法结构

程序中实现了 802.16 MAC PDU 的构建、8 位 CRC 报头校验、32 位 CRC PDU 校验、CCM 加密模块、CCM 解密模块及 AES 加密模块.

3.1 CCM 加密模块

AES-CCM 算法中，加密函数使用 128 位数据分组和128位密钥长度的AES算法. 算法数据完整性的校验部分使用密码分组链接模式的消息认证码CBC-MAC；而在加密部分使用的是CRT计数器模式.

CCM 加密模块流程如图 4 所示. 该模块输入为密钥 K 和明文 P，在计算 MAC 值 T 和计数块 S 时，调用 AES 加密程序.

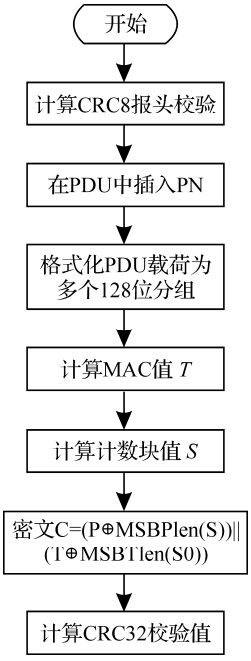

图 4 AES-CCM 加密函数

3.2 算法模块应用方法设计和实现

算法模块的应用方法主要根据 TEK 和 CID(连接标志)的对应关系设计. 在 802.16 协议中，每个 CID 都对应唯一的密钥资源，因此可以根据 CID 找到对应的密钥. 在系统中创建 2 个表，1 个是 TEK 表用于存放加密密钥，另 1 个是 CID 表用于存放 CID 值和对应密钥索引. CID 表的记录结构如图 5 所示. Type 字段表示使用的加密方法，0 表示 DES-CBC，1 表示 AES-CCM；Key index 字段值表示该 CID 标志对应的密钥信息，以及在 TEK 表中的索

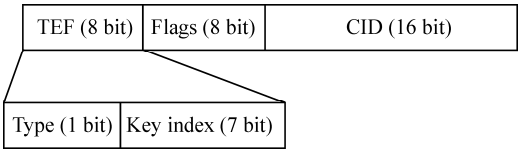

图 5 CID 记录结构图

引位置; CID 字段表示 CID 标志值.

3.2.1 发送端算法模块调用流程

在数据发送前，系统检测报头中加密控制位的值，如为 1 则表示该 PDU 需要加密处理；再根据报头中密钥索引号及加密模式选择位，选择特定的加密算法和密钥对数据进行加密处理；如加密方法为 AES-CCM，则调用 CCM 加密模块对数据进行加密.

3.2.2 接收端算法模块调用流程

当接收到 1 个 PDU 数据时，系统先检测报头中的 CID 标志值是否存在于本地 CID 表中，如不存在则丢弃该 PDU；如存在则找到对应的 CID 记录，则从中读取 Type 和 Key index 的值，并根据 Key index 值，从 TEK 表中读取解密密钥，然后调用 CCM 解密模块对 PDU 进行解密处理.

3.3 算法测试

3.3.1 正确性测试

测试密钥 Key 和数据 PDU 如下:

Key:

f8 6d 6f bc 8c e5 b1 35 a0 6b 16 60 54 f2 d5 65

明文 PDU:

40 40 27 be 8a 9d ce 75 dc 85 1e 0b cd d8 f0 71

41 c4 95 87 2f b5 d8 c0 c6 6a 8b 6d a5 56 66 3e 4e 46 12 05 d8 45 80

密文和接收端解密后 PDU 如下:

密文 C:

40 40 37 be 8a 94 cf 44 00 00 7c 8b 16 c9 cc 66

f5 ef 01 6b d9 6f c5 9d cc 31 99 5e 6f 2c 80 9d

56 ea 42 93 d3 1a 48 9e c7 1f ad 95 8b 6e 1c df 67 d0 b5 3e c6 87 71

解密后 PDU:

40 40 37 be 8a 94 cf 44 00 00 ce 75 dc 85 1e 0b

cd d8 f0 71 41 c4 95 87 2f b5 d8 c0 c6 6a 8b 6d

a5 56 66 3e 4e 46 12 05 d8 45 80 64 78 f3 52 7c f8 f9 07 3e c6 87 71

发送端加密后的密文，一共包含 3 个部分. 起始的 10 Byte 为 6 Byte 的 PDU 报头和 4 Byte 的 PN; 从末尾算起的 4 Byte 为 32 bit 的 CRC 校验码；其余的 41 Byte 为密文，密文又分为 2 部分，分别是 33 Byte 的净荷密文和 8 Byte 的分组链接模式校验码密文.

接收端解密后的 PDU. 起始 10 Byte 为报头和 PN；其后的 33 Byte 和明文 PDU 的 33 Byte 的数据净荷相同，表明本文设计的 AES-CCM 模块和模块应用方法，能正常工作；最后的 4 Byte 3e c6 87 71 为 CRC 校验码用于接收端的 CRC 校验.

3.3.2 优化前后性能比较

为方便测试算法时间，将算法移植到 PC 机上 visual C++ 6.0 中运行. 使用 clock( )函数测试 CCM 加密过程时间，该函数能精确到毫秒级. PC 机处理器为 AMD 2000 1.6 G. 测试数据为原始 PDU，结果见表 1.

表 1　速度比较

	实验数/个			
	1 000	2 000	3 000	4 000
优化前算法/ms	0.182	0.356	0.548	0.713
优化后算法/ms	0.163	0.315	0.492	0.647

从表 1 中可以发现优化后可以得到 11%左右的速度提升.

4　方案比较

当前，WiMAX 设备方案的提供商对数据加密模块主要有 2 种实现方案. (1)采用专门的硬件算法模块; (2)采用高速 DSP 或 FPGA 芯片[5]. 第 1 种方法优点是速度快，价格便宜，但其可扩展性和可升级性不强；第 2 种方法既有速度快的优点，也有很好的可扩展性和可升级性，但成本比较高. 在采用这 2 种方案的设备中，通常需要一个额外的嵌入式系统来控制通信设备的运行. 因此系统会比较复杂，成本较高.

新提出的设计方法是将算法设计成嵌入式系

统的 1 个软件模块，使用时只需直接调用即可，使用方便，而且由于系统没有外接独立的加密模块，可以有效的降低系统的复杂度和成本.

5 结束语

AES-CCM 算法可以有效地防止重放攻击和数据篡改攻击. 因此，目前在 IEEE 802.16 和 802.11i 协议中，都采用 AES-CCM 算法为数据加密算法，并被包含在 RFC 3610 中.

在这种情形下，在对该算法深入分析后，对 AES 算法进行了优化，减少轮变化时间，对 CCM 模式的隐患给出了改进，进一步提高了算法抗重放攻击的能力并给出了嵌入式平台下数据传输加密方案设计及实现.

参考文献:

[1] NIST 800-38C(2004). Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality[S].

[2] Daemen J, Rjjmen V. AES proposal: Rijndael[EB/OL]. [2001-02-28]. http://csrc.nist.gov/cryptotoolkit/aes/rijndael/.

[3] 金晨辉，孙莹. AES 密码算法 S 盒线性冗余研究[J]. 电子学报, 2004(4):639-641.

[4] 张智江，李正茂. 宽带无线接入系统 WiMAX 及工程建设[M]. 北京: 人民邮电出版社, 2007.

[5] 何勃，贠卫国. WiMAX AES-CCM 数据加密协议的 FPGA 实现[J]. 通信技术, 2008, 41(4):47-49.

Embedded System Based Improvement and Implementation of 802.16 AES-CCM Algorithm

XIANG Shi-biao, HE Jia-ming*

(Communication Technology Institute, Ningbo University, Ningbo 315211, China)

Abstract: WiMAX takes AES-CCM as its packet data encryption algorithm. Through thorough analysis of the AES-CCM algorithm, this paper optimizes the round transformation of AES algorithm by changing the four step of round transformation into inquiry of the lookup table and xor operation so as to predigest its operation process. Paper also brings forward improvement measures for CCM pattern applicable rules in 802.16 to strengthen the resistance to replay attacking. On the platform of ARM+VxWorks developed by FUJITSU 3400 WiMAX, the data encryption and transmission scheme is designed and realized by adopting the AES-CCM algorithm. The algorithm is put to test proving that the proposed approach can adequately enhance correctness and validity of the algorithm module.

Key words: AES-CCM; WiMAX; encryption; embedded system

CLC number: TP393.03 **Document code:** A

（责任编辑 章践立）