

无线通信系统 MAC 层通用安全协处理器的实现

封 斌, 齐德昱, 韩海雯

(华南理工大学 计算机系统研究所, 广东 广州 510641)

摘 要: IEEE802. 11i 和 802. 16e 无线通信标准的媒体访问控制层(MAC)都使用了基于高级加密算法(AES)的计数器模式(CTR)和密码分组链接消息验证码(CBC-MAC)作为安全机制, 其以 AES 算法为核心, 采用 CTR 模式保证数据机密性, 采用 CBC-MAC 模式对 MAC 帧头的公开信息进行认证. 设计了通用 AES-CCM 安全协议协处理器, 给出高吞吐量的并行 AES 模块和低成本的复用 AES 模块两种实现方案, 并遵循 Avalon 片内总线接口, 在 Altera 公司 EP1C4F324C6 的 FPGA 上进行了验证. 该安全协议协处理器的设计与实现, 符合软件无线电技术采用通用模块化硬件平台满足多种无线空中接口标准的思想, 对无线通信终端底层硬件平台的通用化具有一定的价值.

关键词: 无线通信标准; AES-CCM; MAC; 协处理器; Avalon 总线

中图分类号: TP301

文献标识码: A

文章编号: 1000-7180(2013)10-0033-05

General Security Co-processor Implementation for MAC layer of Wireless Communication Systems

FENG Bin, QI De-yu, HAN Hai-wen

(Research Institute of Computer Systems, South China University of Technology, Guangzhou 510641, China)

Abstract: The MAC layer of IEEE802. 11i and 802. 16e wireless communication standards uses the AES-CCM protocol as security mechanism, it uses the AES algorithm as the core, uses CTR mode to ensure confidentiality of data, uses CBC-MAC mode to authenticate the public information of the header in MAC frame. This paper presents an AES hardware accelerator module and two implementations: one for high throughput with parallel AES module and one for low cost with multiplex AES module. For easy of integration and portability, the standard Avalon bus interface is provided, and verified on Altera EP1CF324C6 FPGA platform. This design and implementation of the common security coprocessor is according with method of software radio which uses common modular hardware platform to meet a variety of wireless air interface standard, and has a certain value for the generalization the wireless communication terminal hardware platform.

Key words: wireless communication standards; AES-CCM; MAC; co-processor; Avalon bus

1 引言

由于无线通信系统采用大气层作为传输介质, 在数据传输时极易受到恶意攻击, 其安全性受到额外的重视. 基于密码学的安全机制在各类系统中已得到了普遍应用, 无线城域网(WMAN) IEEE802. 16e^[1] 标准和无线局域网(WLAN) IEEE802. 11^[2] 标准, 在数据链路层都采用了基于高级加密标准(Ad-

vanced Encryption Standard, AES) 算法^[3] CCM (Counter with CBC-MAC, 计数器模式和密码块链信息认证码)操作模式的安全机制, 但使用的细节略有不同. 由于密码算法的计算复杂性, 在传输大量数据时, 通信终端必须具备较强的计算能力来实现安全机制, 而无线通信终端计算资源的有限性, 决定了用软件实现密码算法会导致系统处理速度的瓶颈, 并增大设备的功耗, 采用硬件加速机制可更好解决

收稿日期: 2012-11-20; **修回日期:** 2013-01-26

基金项目: 国家自然科学基金项目(61070015); 广东省自然科学基金团队项目(10351806001000000)

上述问题.

文献[4-6]也分别从吞吐量和面积功耗等的角度出发,分别实现了 AES-CCM 硬件 IP 核,但都仅从单一标准的实现角度去考虑硬件加速结构,没有考虑到通用性问题.

本文基于软件无线电技术的思想,通过深入分析上述标准 MAC 层中 AES-CCM 协议的具体实现流程,设计了一个通用安全协处理器平台.

2 无线通信标准中的 AES-CCM 协议

2.1 AES-CCM 协议简介

分组加密算法仅定义了一组明文与密文之间的运算关系,而工作模式给出了加密算法的使用方法,其通过将算法与一些反馈及简单的运算进行组合,以防止数据在传输过程中被篡改. CCM 协议是分组加密算法 CTR 模式和 CBC-MAC 模式的结合,CTR 模式保证数据的机密性, CBC-MAC 模式保证数据的完整性鉴权,从而同时实现了数据传输的机密性、完整性和可认证性. AES 算法安全性好,计算速度快,吞吐量高,属于对称密钥算法中的分组迭代密码算法. AES-CCM 协议是采用了 AES 算法的 CCM 协议,其加密过程如下:

(1)将消息 P 按 128 比特分组为 $B(1), B(2), \dots, B(n)$;

(2)构建 CBC 模式初始化向量 IV , 即 B_0 , 并进行加密: $Y_0 = E(K, B_0)$, 其中 K 为密钥, E 为 AES 加密算法;

(3)按 CBC 模式对消息进行加密: for $i=1$ to n , do $Y_i = E(K, B(i) \oplus Y_{i-1})$, 最后一组如不足 128 bit 则需填零补齐;

(4)提取 Y_n 的高有效位 8 个字节作为产生认证码的数据 T : $T = \text{MSB}_8(Y_n)$;

(5)构建 CTR 模式计数器, 利用计数器生成函数产生 CTR 模式所需的计数器 A_i ;

(6)为 CTR 模式产生密钥流 S_i : for $i=1$ to n , do $S_i = E(K, A_i)$;

(7)CTR 模式产生密文 E_p : $E_p = P \oplus (S_1, S_2, \dots, S_n)$;

(8)产生认证码 U : $U = T \oplus E(K, A_0)$;

(9)串接 CTR 密文 E_p 与认证码 U , 输出密文 C : $C = E_p || U$

解密时,接收方收到密文 C 后,将其拆分为 E_p 和 U , 首先利用共享密钥对密文 C 解密,得到有效负荷 P_{rec} , 再通过 $T_{\text{rec}} = U \oplus \text{MSB}_8(S_0)$, 计算出

T_{rec} ; 利用 CBC-MAC 模式对有效负荷 P_{rec} 进行重新计算产生 T_{calc} , 当 $T_{\text{calc}} = T_{\text{rec}}$ 时, 表明该消息正确接收, 否则丢弃该报文.

CCM 协议自身的流程设计, 保证了在模式内部, 两个相同的分组不会产生相同的输出. 同时, 在模式之间对同一分组进行处理时, 两个模式的输出也不相同, 从而保证了 CCM 协议共用加密算法及密钥的安全性, 简化了协议结构, 并降低了密钥管理难度.

2.2 无线通信标准 MAC 层安全机制分析

无线通信标准 MAC 帧的帧头结构有所不同, 但都包含了报文长度、管理信息等需要公开的内容, 并以明文的方式传送, 以保证接收设备正确的识别和处理, 而为了抵御重放攻击等问题, 必须对这些信息进行完整性验证. AES-CCM 协议的输入包括 MPDU 负荷, 密钥, CBC-MAC 模式的初始化向量 IV 和 CTR 模式的计数器 A_0 (A_i 与 A_0 之间存在递增的关系). 在协议中引入瞬时值 Nonce, 其是密码学中的一个时间变量参数, 如计数器或者当前时间, 被广泛使用在密钥管理协议中, 用以避免消息的重发和其他类型的攻击.

802. 11i 的 MPDU 帧头包含了源地址和目的地址等信息. 图 1 中描述了 802. 11i 的 CCMP 封装流程框图: (1) 构建 8 byte 的 CCMP header; (2) 在 CBC-MAC 模式下, 通过 MAC 帧头、CCMP header 和明文计算得到 8 byte 的认证码 U , 作为 MAC 帧头、CCMP header 和明文的完整性认证; (3) 在 CTR 模式下, 对明文和认证码 U 分别进行加密, 产生密文和认证码密文 MIC; (4) 将由原 MAC 的帧头、新构建的 CCMP header、密文及认证码组成的密文 MPDU, 放入队列中准备传送.

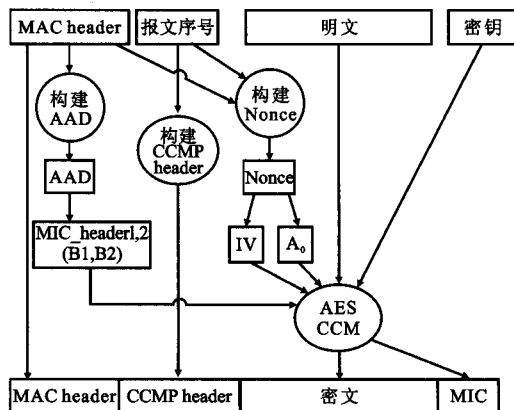


图 1 802. 11i 标准 MPDU 封装过程

其中, CCMP header 中包含了 6 字节的报文序

号 PN,通过 PN 提供了重播保护机制,可防止重放攻击。在 CBC-MAC 模式中计算认证码时,引入了附加认证数据 (Additional Authentication Data, AAD),AAD 中主要包含 MAC 帧头中的地址和相关信息,从而使得认证码对帧头中的上述信息也可验证。需注意的是,在 CTR 模式下,仅加密 MPDU 负荷和 CBC-MAC 计算出的认证码 U,而不对 CC-MP header 进行加密。

802.16e MAC 层的 MPDU 经 CCMP 封装后比原文增加了 4 字节的报文序号 PN 和 8 字节的认证码 MAC。其 CCMP 封装流程如图 2 所示。与 802.11i 的 CCMP 封装流程相比,802.16e 的 MAC 帧头中不包含地址信息,因此不需要构建附加认证信息来对其进行验证,只需要以报文序号构成瞬时值 nonce,再以 nonce 为基础构建 CBC-MAC 模式的初始向量 IV 和 CTR 模式的计数器 A_0 。

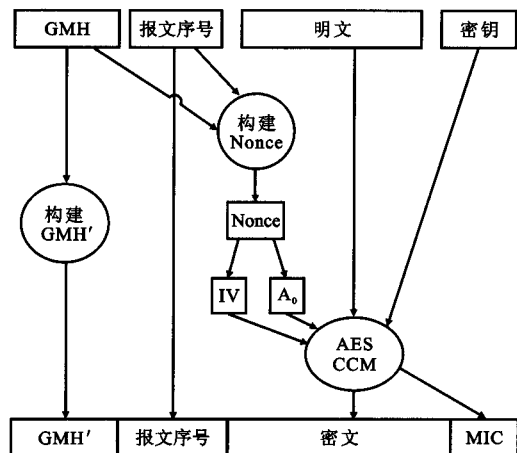


图 2 802.16e 标准 MPDU 封装过程

3 AES-CCMP 协处理器的实现

从上述分析可以看出,这两种无线通信标准的 AES-CCMP 处理流程是相同的,不同的仅是两种模式对应的输入数据。本节给出了通用 AES-CCM 协议 IP 核及其两种实现方案,即 AES 模块并行方案和复用 AES 模块方案。并行 AES 实现方案吞吐量大,但面积大,复用 AES 方案中 CBC-MAC 模式与 CTR 模式时分复用了同一个 AES 模块,节省了面积,但吞吐量比并行方案减少一半。这两种方案核心 AES 模块完全相同,仅协处理器的控制逻辑不同,可以通过配置实现两种方案。不同无线通信标准的 AES-CCMP 核的输入数据,可由 MAC 层控制软件对 MPDU 的分析直接得到,不影响系统处理效率。

3.1 AES 模块的实现

本文 AES 模块的硬件实现分为密钥扩展、轮变

换和状态控制三部分。密钥扩展模块采用了提前生成子密钥的方法,从而在一次性生成子密钥后,可闲置密钥扩展模块来降低系统功耗。密钥扩展模块先计算出 AES 各轮变换所需要的轮子密钥并存储在 RAM 中,然后在轮变换时直接读取。对于 128 bit 的密钥,需要 1 408 bit (128 bit $\times$ 11) 的 RAM 空间存储生成的子密钥流,该方法可共享 S 盒。同时,考虑到 AES-CCM 协议中 CBC-MAC 模式和 CTR 模式采用同一密钥进行子密钥流的扩展,本文中 CCM 的两个模式共用了密钥扩展模块,进一步降低了面积和功耗。

AES 算法字节替换函数 SubBytes 中的 S 盒可通过复合域算法用逻辑电路^[7]或查表法实现,本文采用了存储查找表方法,通过 Altera 公司提供的 altsyncram 器件实现了双口 ram,通过双口 ram 可实现对查找表数据的共享,在存储查表法中只需存储 8 张 256×8 bit 的查找表,有效地节省了存储器空间。

本文采用 Moore 型有限状态机 (FSM) 来控制 AES 算法处理流程。采用三进程描述方式,分别描述了次态逻辑、状态寄存器和输出逻辑。把 FSM 的组合逻辑和时序逻辑分开实现,有利于对 FSM 的组合逻辑和时序逻辑分别进行测试,并在硬件逻辑进行综合时效果较好。AES 模块内部以 128 比特数据块为单位进行并行处理及通信,时序控制简单,逻辑结构清晰。FSM 与多路复用器共同控制着 AES 模块内部数据的迭代流程。本方案的 AES 核的状态机的状态转换关系如图 3 所示。

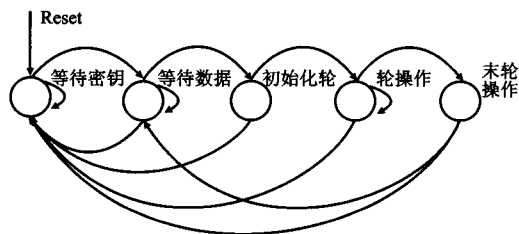


图 3 AES 核有限状态机状态转换图

3.2 协处理器片内总线接口的实现

本文使用 Avalon 总线作为协处理器的接口标准。AES-CCMP 核向 Avalon 总线开放了 32 个 32 bit 长的映射空间,用于协处理器与外部处理器进行数据通信。address 信号指明 AES-CCMP 核开放空间的地址偏移量,外部处理器可通过 address 信号所描述的偏移量对 IP 核开放空间进行访问。read、write 信号指明数据的访问方向,32 bit 宽的 readdata、writedata 数据线从 IP 核中读取或准备写入的

数据, Ctrl 控制寄存器定义了各种状态转换标识. AES 核在片内总线上映射的地址空间说明见表 1.

表 1 AES IP 核在 Avalon 总线上映射的地址空间

Offset	Name	功能
0—7	key	初始密钥. 在 Avalon 总线上只可写.
8—11	data	输入数据. 在 Avalon 总线上只可写.
12—15	Result	运算的结果. 在 Avalon 总线上只可读
16—30	—	保留
31	ctrl	控制和状态字, 在 Avalon 总线上可读写

3.3 两种协处理器结构

AES-CCM 协议中的 CBC 和 CTR 模式都采用了 AES 作为加密算法, AES 算法集中了整个协议主要的计算量. 本文基于对 AES 模块使用方法的不同, 设计了两种 AES-CCMP 协处理器的架构, 并行 AES 架构和复用 AES 架构, 分别用于对高吞吐量和低成本有明确要求的场合. 这两种架构所使用的 AES 模块代码是完全相同的, 不同之处仅在于时序的控制上. 这两种架构可通过配置文件根据需要自动生成.

图 4 中描述了 CCMP 协处理器两个模式各使用一个 AES 模块的并行架构, 这两个模式中的加密工作可以并行执行. 需要说明, 802. 11i 的 IV 是三组 128 比特的数据, 即 MIC_IV, MIC_header1,

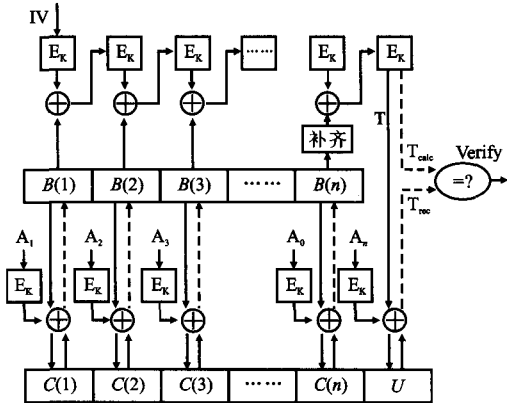


图 4 AES 模块并行架构示意图

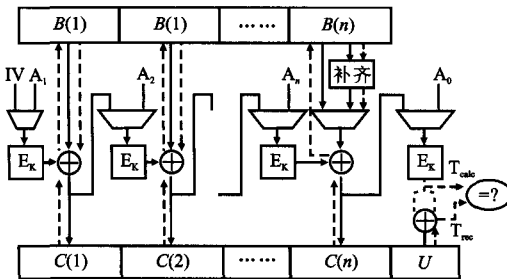


图 5 AES 模块复用架构示意图

MIC_header2, CTR 模式要等到 MIC_header 处理完后才启动. 图 5 中描述了复用 AES 模块的 CCMP 实现方案, 通过对 AES 模块输入数据时序的控制, AES 模块轮流地在 CBC-MAC 和 CTR 模式下进行数据加密运算. 图中的虚线代表了 MAC 层 CCMP 的解封装过程. 可以看到, 协处理器实现的关键部分是 AES 加密模块, 而 Avalon 总线接口及相关的逻辑控制, 可以通过简单的逻辑电路实现.

4 实验结果分析

本文以 VHDL 硬件描述语言实现了上述两种结构的 AES-CCM 协议协处理器, 开发环境为 QuartusII9. 1, 并在 Altera Cyclone EP1C4F324C6 芯片上进行了验证. 在所有的测试方案中都统一采用 NiosII/s 标准型内核, 测试向量采用 NIST^[8] 提供的 CCM 模式基准测试向量. 测试用例运行在 NiosII 处理器上, 通过 Avalon 总线将测试向量传递给 AES-CCMP 协处理器, 接受协处理器返回的数据并进行对比分析.

协处理器吞吐量的计算公式为

Throughput=block_size×F_max / clock_cycles

在 AES-CCMP 核中, 密钥扩展模块提前完成子密钥流生成并进行存储, AES 模块处理 128 bit 负载需要 11 个时钟周期, 即, 10 个轮变换加 1 个初始化轮各需要 1 个 clock. 在对 AES-CCMP 核连续输入输出数据时, 第一个分组的输入和最后一个分组的输出各需要额外 4 个时钟, 其他分组的输入输出与 IP 核中其他分组数据的处理并行执行. 而对 MAC 帧帧头的处理, 802. 11i 需要额外的 2 个分组, 各标准中 MAC 的处理还需要加一个分组的时间. 在吞吐量方面不同标准的区别很小. 如果考虑有效数据, 即把 IV 等激励数据排除在有效吞吐量计算公式外, 那么对两种标准的通用 AES-CCMP 协处理器而言, block_size 和 fmax 是一样的, 而 802. 11i 在每一个报文上需多处理 2 个分组, 多 22 个 cycles. 当采用复用 AES 模块的 AES-CCMP 协处理器结构时, 相当于有效数据的长度翻倍, 吞吐量基本降一半.

表 2 中给出了本文实现的并行 AES 模块架构 (AES_P) 和复用 AES 模块 (AES_M) 两种 AES-CCMP 协处理器, 及相关文献给出同类硬件加速器的性能相关参数. 从表 2 可以得出, 本文为无线通信系统链路层实现的通用 AES-CCMP 协处理器, 具

有面积小、吞吐量高的优点.

表 2 AES-CCMP 协处理器性能相关数据

方案	芯片	面积	存储空间	$F_{\max}/$ MHz	吞吐量/ (Gb/s)
并行 AES ^[4]	xc3s50	487slice	4BRAM	247	0.687
复用 AES ^[10]	EP1C4	1434LE	7 808 bits	78	0.09
并行 AES ^[7]	EP2C35	8438LE	65 536 bits	55.68	0.688
AES_P	EP1C4	2353LE	10 240 bits	134.41	1.5
AES_M	EP1C4	2144LE	6 144 bits	137.46	0.8

5 结语

本文为无线通信标准设计了通用的 AES-CCMP 硬件协处理器,该协处理器具有两种架构,可根据具体情况灵活配置,实现高吞吐量或低成本的特性.将不同无线通信设备的公共部分由硬件实现,而由软件实现功能和接口的多样性,符合软件无线电技术的思想.同时,为该 IP 核设计了基于 Avalon 片内总线的标准接口,使得 IP 核更容易被集成和移植.用硬件协处理器实现 AES-CCM 协议,对无线通信终端底层硬件平台的通用化具有积极的意义,同时,对其他类似的安全模式也具有一定的参考价值.

参考文献:

[1] LAN/MAN Standards Committee, Part 16. Air interface for fixed and mobile broadband wireless access systems[S]. IEEE Std 802.16e—2005, IEEE Standard for Local and Metropolitan Area Networks, 2006.

[2] LAN/MAN Standards Committee, Part 11. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications[S]. IEEE Std 802.11i—2004, IEEE Computer Society, 2004.

[3] Daemen J, Rijmen V. The design of rijndael: AES the advanced encryption standard [M]. Berlin: Springer Verlag, 2002.

[4] Arshad A, Nassar I. An FPGA-based AES-CCM crypto core for IEEE802.11i architecture [J]. International Journal of Network Security, 2007, 5(2): 224-232.

[5] Jae Deokji, Seok Wonjung. Efficient sequential architecture for the AES CCM mode in the 802.16e standard[C]// Second International Conference on Intelligent Networks and Intelligent Systems. China, Tianjin: IEEE Computer Society, 2009: 253-256.

[6] 何勃, 负卫国. WiMAX AES-CCM 数据加密协议的 FPGA 实现[J]. 通信技术, 2008, 41(4): 47-50.

[7] 杨骅, 王东辉, 张铁军, 等. 一种适用于 RFID 标签芯片的 AES 算法结构设计[J]. 微电子学与计算机, 2009, 26(1): 89-92.

[8] Hamalainen P, Hannikainen M, Hamalainen T D. Efficient hardware implementation of security processing for IEEE 802.15.4 wireless networks[C]//48th IEEE Int. Midwest Symposium on Circuits and Systems. Cincinnati: IEEE Computer Society, 2005: 484-487.

作者简介:

封斌 男, (1974-), 博士研究生, 高级工程师. 研究方向为嵌入式系统、高性能计算.