文章编号:1001 - 9081(2011)08 - 02159 - 03 doi:10.3724/SP.J.1087.2011.02159

集中式无线局域网分离介质访问控制的 CCMP 设计

刘立群
(甘肃农业大学 信息科学技术学院,兰州 730070)
(llqhjy@126.com)

摘 要:针对临时密钥完整性协议(TKIP)潜在的安全缺陷,提出了一种新的可有效提高无线网络安全性的现场可编程门阵列(FPGA)的计数器模式和密码分组链接消息认证模式协议(CCMP)的设计方案。研究了 CCMP 的机密性原理,分析表明 CCMP 比 TKIP 提供了更为安全的保障。在已有的集中式无线局域网(WLAN)分离介质访问控制(MAC)架构下,给出了 CCMP 模块的实现方法和电路结构。分析比较了现有的 4 种高级加密标准(AES)实现方案的运行性能,测试结果表明该实现方案能提供更高的加密性能,提高了无线网络的机密性。

关键词:分离介质访问控制;计数器模式和密码分组链接消息认证模式协议;高级加密标准;计数器模式数据加密;密码分组链接消息认证码完整性检查

中图分类号: TP309.2; TP393.17 **文献标志码**:A

Design of CCMP based on split medium access control of centralized wireless local area network

LIU Li-qun
(*College of Information Science and Technology, Gansu Agricultural University, Lanzhou Gansu* 730070, *China*)

Abstract: Concerning the potential security flaws of Temporal Key Integrity Protocol (TKIP), a new scheme for implementing counter mode with cipher-block chaining with message authentication code protocol (CCMP) based on Field Programmable Gate Array (FPGA) was proposed. The circuit architecture of CCMP process was implemented based on the existing centralized Wireless Local Area Network (WLAN) split Medium Access Control (MAC) architecture. By comparing the performances of four different Advanced Encryption Standard (AES) implementations, the test results indicate that the proposed scheme can provide higher encryption performance and enhance wireless confidentiality.

Key words: split Medium Access Control (MAC); counter mode with cipher-block chaining with message authentication code protocol (CCMP); Advanced Encryption Standard (AES); Counter Mode (CTR) for data confidentiality; Cipher-block Chaining with Message Authentication Code (CBC-MAC) for authentication and integrity

0 引言

随着无线用户的增多,集中式无线局域网(Wireless Local Area Network, WLAN)分离介质访问控制(Medium Access Control, MAC)架构[1]22-27已经成为当前大规模部署无线网络的主要趋势。在不改变已有接入点(Access Point, AP)的条件下,为了解决有线等效保密(Wired Equivalent Privacy, WEP)[2]规范带来的安全隐患,保证无线用户的安全使用,IEEE 802.11i 标准提出了强健安全网络(Robust Security Network, RSN)[3]22-31,[4]163-278及临时密钥完整性协议(Temporal Key Integrity Protocol, TKIP)[3]43-57,[4]289-316保证数据的机密性和完整性。TKIP 使用的核心加密算法 Rivest 密码 4(Rivest Cipher 4,RC4)存在安全漏洞,这使得 TKIP 只能成为一种过渡机制,并不能从根本上解决无线用户的安全隐患。RSN 提出的另一机密性协议计数器模式和密码分组链接消息认证模式协议(counter mode with cipher-block chaining with message authentication code protocol, CCMP)[3]57-62,[4]323-341,核心加密算法是高级加密标准(Advanced Encryption Standard, AES),从根本上解决了加密算法的漏洞,已经被 RSN 强制实行并广泛接受。本文在文献[5]的基础上,采用集中式 WLAN 分离 MAC 架构,结合集中式设备已有的功能[5]182,[6]5-10,提出了一种新的在现场可编程门阵列(Field Programmable Gate Array, FPGA)上实现 CCMP 的设计方案,并采用 Virtex-4 XC4VLX 1000-12 的 FPGA 芯片实现了 CCMP 模块,通过比较,该方案能提供较高的加密性能,提高了无线网络的机密性。

1 CCMP 的安全性

1.1 CCMP 机密性原理

CCMP 提供了计数器模式(Counter Mode, CTR)和密码分组链接消息认证码(Cipher-Block Chaining with Message Authentication Code, CBC-MAC)模式两种安全机制[3]57。其中 CTR 模式核心是 AES 分组加密算法。AES 是一个对称的迭代型分组加密算法,其分组长度和密钥长度均可变。AES 的分组长度一般指定为 128 位,密钥长度可以为 128 位。

CBC-MAC 模式提供认证和完整性检查机制。CCMP 在原 MAC 协议数据单元(MAC Protocol Data Unit, MPDU)上扩充了 8 个字节的消息完整码(Message Integrity Code, MIC)作完整性检查[3]58-59。CBC-MAC 模式主要是对 MIC 进行完整性检验。

CTR 模式提供数据加密机制,使用 AES 算法作为核心加密算法。CTR 模式要加密的数据包括明文数据和 MIC 两部

收稿日期:2011-01-21;**修回日期**:2011-03-09。 **基金项目**:国家自然科学基金资助项目(61063028)。
作者简介:刘立群(1982-),女,甘肃天水人,讲师,硕士,主要研究方向:信息安全、无线局域网安全、网络计算。

分[3]58-59。

1.2 CCMP与TKIP安全性比较

表1给出了CCMP和TKIP的安全性比较。首先,CCMP是以AES为核心加密算法的,AES比TKIP中的RC4算法具有更高的安全性,目前AES算法仅对差分功耗分析[7]攻击方法有弱的抵抗能力,尚未存在对AES完整的成功攻击。其次,CCMP采用CTR和CBC-MAC两种安全模式,进一步提高了加密算法的安全性。再次,TKIP是包裹在WEP外面的一套算法,仍然存在RC4的安全漏洞。最后,在现有集中式设备[5]182-183,[6]3-5的基础上,可以增加新的硬件支持CCMP以保证现有设备的继续使用。比较表明,在现有设备上实现CCMP可以为无线用户提供更为安全的保障。

表1 CCMP与TKIP安全性比较

安全性能比较项	CCMP	TKIP
机密性机制	数据加密CTR	有线等效保密
完整性机制	完整性检查CBC-MAC	消息完整码
密钥机制	初始密钥和密钥流	密钥混合函数和组密钥
加密算法	AES算法	RC4算法
加密安全性	安全	存在漏洞
WEP设备兼容	不兼容	兼容
WEP设备升级	不能,必须硬件支持	可以软件升级
现有集中式设备	需要新的硬件支持	已实现

2 CCMP的设计

2.1 分离MAC架构中CCMP的设计

集中式WLAN分离MAC方式是依据实时性的敏感度把MAC功能分别实现在AP和接入控制器(Access Controller,AC)上[1]5-31,[5]181,[6]3。本文在现有集中式WLAN分离MAC架构[5]182,[6]3-8下,使用CCMP保证数据的机密性。由于AES算法对硬件要求比较高,CCMP无法在现有AP上升级实现,需要新的硬件支持。因此,结合集中式设备已有的功能[5]182-183,[6]5-10,本文提出了一种新的在FPGA上实现CCMP的设计方案:支持无线网络的物理层和MAC层的实时性功能仍然放在AP上,MAC层的非实时功能和高层服务放在集中式设备AC上[5]181-182,[6]5-7,保证数据机密性的CCMP放在FPGA芯片上实现。

2.2 系统结构设计

本系统结构包括AC的软件结构和FPGA的硬件结构。其中,软件部分完成了无线网络的数据转发以及和硬件的通信功能[5]182-183,[6]8-10,硬件FPGA完成了数据机密性和完整性检查CCMP模块和密钥扩展功能。硬件FPGA和AC之间采用串口连接通信。系统结构如图1所示。

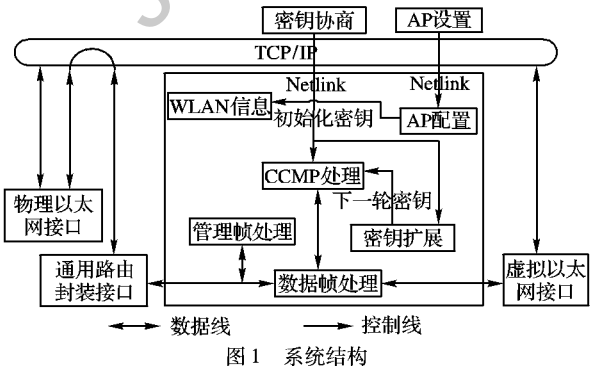

图1 系统结构

相关的模块包括如下。1)数据帧处理。处理数据帧,将数据帧通过串口送至CCMP模块处理。2)CCMP处理。提供CCMP安全机制,用于封装/解封装数据帧,需要从密钥维护模块中获得初始密钥,并将封装后的帧通过串口送至数据处理模块。3)密钥扩展。用于计算产生AES算法的10轮迭代子密钥。4)密钥协商。处于AC的用户空间,用于向AC内核空间发送初始密钥。

3 CCMP的实现

3.1 CCMP模块的实现

CCMP处理模块主要实现了数据帧的封装/解封装操作。主要包括通过CBC-MAC模式计算MIC的操作和通过CTR模式对明文MPDU和MIC进行加密的操作。

为了保证加密速度并适应MAC层数据帧传输的吞吐量,本文采用Xilin公司的Virtex-4 XC4VLX 1000-12的FPGA芯片设计CCMP,以提高加密和解密的速度。芯片电路的结构如图2所示。其中CCMP接口是AC内核和芯片电路的串口接口,用来转发来自AC的802.11帧。CCMP处理模块接收到802.11帧后,将其数据部分分成128位为一组的明文分组。控制单元是芯片中的主控电路单元,用来确定整个芯片的工作状态。明文MPDU用于在加密阶段分别将明文数据送到AES-MIC单元和AES-CTR单元中。它们是实现AES算法的运算单元。AES-MIC单元用来计算MIC值。AES-CTR单元用作CTR加密过程。将计算出的MIC值和明文MPDU一起与AES-CTR单元的结果异或,将得到所要的密文和加密后的MIC值。

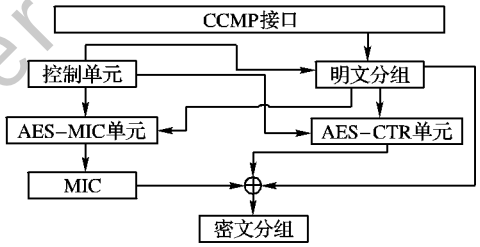

图2 CCMP模块的电路结构

由于AES算法是CCMP模块的核心,因此芯片电路中决定加密速度和吞吐量的主要单元是AES-MIC和AES-CTR。为此,本文比较了现有的四种AES方案的运行性能,如表2所示。比较结果表明,采用Virtex-4 XC4VLX 1000-12的FPGA芯片实现AES算法,可以使AES加密达到相当高的吞吐量,同时还保证了系统有较高的每个基本单元的吞吐量(Throughout Per Slice,TPS)和每个面积的吞吐量(Throughout Per Area,TPA)性能。因此,为了保证本电路中CCMP的加密速度,本文选取了最后一种Virtex-4 XC4VLX 1000-12芯片实现AES算法。测试结果表明,采用该芯片设计实现CCMP,CCMP的加密核心AES达到了相当高的吞吐量,并保证了较高的TPS和TPA系统性能,系统响应时间达到0.88 μs,加密速度满足用户需求。

表2 AES硬件运行性能比较

芯片	吞吐量/Gbps	TPS/Mbps	TPA/Mbps
Virtex-E 2000-5[8]	20.230	3.494	1.091
Virtes-Ⅱ VP20-7[9]	21.640	2.291	2.291
Virtex-Ⅱ4000[10]	23.570	1.392	1.392
Virtex-4 XC4VLX 1000-12[11]	31.640	3.195	3.195

3.2 CCMP模块处理过程

3.2.1 CBC-MAC计算MIC过程

由AC用户空间的密钥协商模块得出一个初始密钥(128位)和一个128位的MIC初始化向量(MIC Initialization

Vector, MIC-IV),通过 Netlink 消息送给 AC 内核,经由串口发送给 CCMP 处理模块中的 CCMP 接口。AC 内核的数据处理模块将 802.11 帧也通过串口发送给 CCMP 接口。CCMP 处理模块接收到 802.11 帧后,将其数据部分分成 128 位为一组的明文分组。首先将 128 位的初始化密钥和 MIC-IV 经过 10 轮的 AES 加密算法得到初始化向量(Initialization Vector, IV)。再对每个明文分组和相应的前一个密文分组进行异或操作后,送入 AES 加密模块得到下一个密文分组。其过程如图 3 所示。直至得到最后一个密文分组时,取该密文分组的前 64 位作为 8 字节的 MIC 校验。

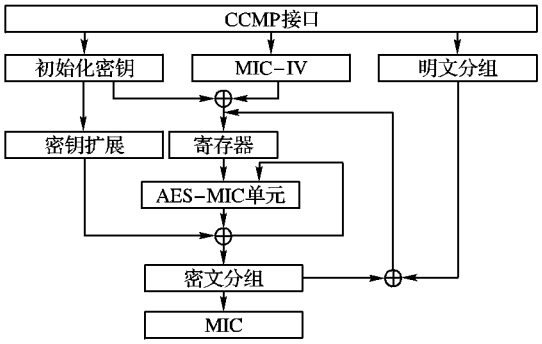

图 3　CBC-MAC 计算 MIC 过程

3.2.2　CTR 加密过程

CTR 模式要加密的数据包括明文数据和 MIC 两部分。通过 CBC-MAC 模式得到的初始密钥、明文 MPDU 及 MIC 将作为 CTR 加密操作的初始输入。CCMP 处理模块将明文 MPDU 和 MIC 一起分成 128 位为一组的明文分组。对每个明文分组利用 CTR 加密算法分别加密。图 4 结构描述了其中一个明文分组加密的过程。首先,设置硬件的计数器为 1,初始化密钥和计数器进行一次轮密钥加(这里为二进制异或运算)变换后进入 10 轮加密迭代。前 9 轮加密使用的密钥为密钥扩展模块生成的轮密钥。每一轮加密依次经过字节代替、行移位、列混合和轮密钥加运算。第 10 轮加密跳过了列混合运算。通过 10 轮的 AES 加密运算后得到一个加密的密钥流,使用该密钥流和第一个明文分组进行二进制异或运算,从而得到这个分组明文对应的密文分组。然后,硬件计数器加 1,按照同样的 CTR 加密算法求出下一个明文分组对应的密文分组。直到最后一个分组为止。最后,将计数器清零,与初始化密钥一起送入 10 轮 AES 加密模块后得到密钥流,将其与 MIC 进行异或运算后得到加密的 MIC。它和已加密的密文分组一起作为密文传送至 CCMP 接口,并发送给 AC 的数据帧处理模块。

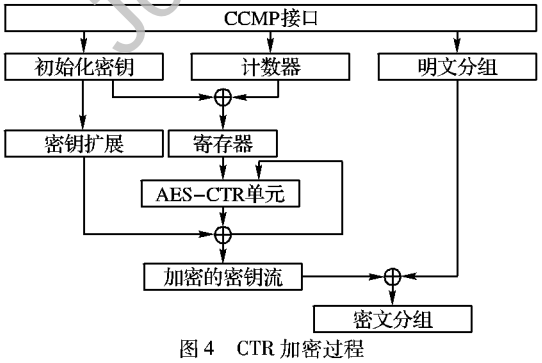

图 4　CTR 加密过程

3.2.3　密钥扩展模块计算过程

密钥扩展模块是将初始化密钥作为种子密钥,经过字节移位、字节代换和轮常数异或运算,计算产生 10 轮迭代子密钥(每一轮子密钥叫做轮密钥)。轮密钥对应于 CCMP 处理模块中 AES 加密的每一轮。图 5 给出了密钥扩展模块计算轮密钥的过程。

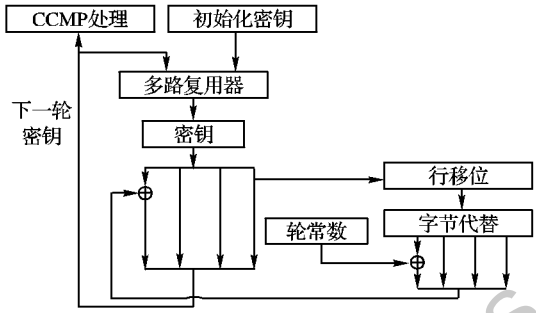

图 5　密钥扩展模块计算过程

4　结语

在集中式 WLAN 结构中实现 RSN,是目前大规模部署安全的无线网络的一个趋势。本文在分离 MAC 架构的基础上,结合集中式设备已有的功能,给出了在硬件 FPGA 上实现 CCMP 的设计方案,并采用 Virtex-4 XC4VLX 1000-12 的 FPGA 芯片实现了 CCMP 模块,使 CCMP 的加密核心 AES 达到了较高的性能。进一步解决了 TKIP 潜在的安全隐患,给无线用户提供了更为安全可靠的网络机制。

参考文献:

[1] IETFRFC 4118: Architecture taxonomy for control and provisioning of wireless access points (CAPWAP) [EB/OL]. [2011-01-02]. http://www.apps.ietf.org/rfc/rfc4118.html.

[2] IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications [S], 1999.

[3] IEEE Standard 802.11i: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) security enhancements [S], 2004.

[4] EDNEY J, ARBAUGH W A. Real 802.11 security: Wi-Fi protected access and 802.11i [M]. Boston: Addison-Wesley, 2003.

[5] 刘立群, 火久元, 唐鼎, 等. 基于集中式 WLAN 分离 MAC 架构的 TKIP 协议研究[J]. 计算机工程, 2008, 34(1): 181-183.

[6] 唐鼎, 唐晖, 林涛, 等. 一种无线局域网接入方法: 中国, 101335663[P]. 2008-12-31.

[7] 邹程, 张鹏, 邓高明, 等. AES 密码电路抗差分功耗分析设计[J]. 计算机工程与应用, 2009, 45(36): 63-65.

[8] McLOONE M, McCANNY J V. High performance single-chip FPGA Rijndael algorithm implementation [C]// CHES'01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2001: 65-76.

[9] CHODOWIEC P, KHUON P, GAJ K. Fast implementation of secret-key block ciphers using mixed inner- and outer-round pipelining [C]// Proceedings of the 2001ACM/ SIGDA Ninth International Symposium on Field Programmable Gate Arrays. New York: ACM Press, 2001: 94-102.

[10] STANDAERT F X, ROUVROY G, QUISQUATER J J, *et al*. A methodology to implement block ciphers in reconfigurable hardware and it s application to fast and compact AES Rijndael [C]// Proceeding ACM/ SIGDA 11th ACM International Symposium on Field-Programmable Gate Arrays. New York: ACM Press, 2003: 216-224.

[11] ZHANG XINMIAO, PARHI K K. High-speed VLSI architectures for the AES algorithm [J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2007, 12(9): 957-967.