基于自组网的轻量化 IPsec 加密设计与实现

张卫敏[1]，焦运良[1]，王　硕[2]，郑和芳[2]，张　攀[1]
（1. 中电长城圣非凡信息系统有限公司，北京　102209；2. 中国电子信息产业集团有限公司第六研究所，北京　100083）

摘　要：针对无线自组网的安全传输需求，提出了一种基于轻量化 IPsec 加密的软硬件设计方案。该方案以“CPU + 算法 FPGA + 基带波形 FPGA”为核心构建基础硬件平台，通过设计轻量化“四次交互”密钥协商协议，精简交互流程次数达 33%，有效降低了流量开销；软件方面采用分层架构实现传输业务管理、加解密处理、基带波形处理、无线收发以及应用管理等功能。经测试验证，该设计在提供轻量化 IPsec 加解密情况下无线通信时延约 16.71 ms，TCP 无丢包传输速率可达 23.28 Mbit/s。

关键词：无线自组网；IPsec；轻量化；密钥协商；安全加密
中图分类号：TN918.4；TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.06.002
引用格式：张卫敏，焦运良，王硕，等. 基于自组网的轻量化 IPsec 加密设计与实现［J］. 网络安全与数据治理，2025，44(6)：11-19.

Design and implementation of lightweight IPsec encryption based on wireless Ad hoc network

Zhang Weimin[1], Jiao Yunliang[1], Wang Shuo[2], Zheng Hefang[2], Zhang Pan[1]
(1. CEC Great Wall Shengfeifan Information System Co., Ltd., Beijing 102209, China;
2. The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: In response to the security requirements of wireless Ad hoc networks, this paper proposes a software and hardware co-design scheme based on lightweight IPsec encryption. The scheme constructs a core hardware platform centered on a "CPU + Algorithm FPGA + Baseband Waveform FPGA" architecture. By designing a lightweight "four-round interaction" key negotiation protocol, the interaction process is streamlined by 33%, effectively reducing traffic overhead. On the software side, a layered architecture is adopted to implement functions such as transmission service management, encryption/decryption processing, baseband waveform processing, wireless transceiver operations, and application management. Test results verify that the design achieves a wireless communication latency of approximately 16.71 ms while providing lightweight IPsec encryption/decryption, with a TCP lossless transmission rate of up to 23.28 Mbit/s.

Key words: wireless Ad hoc network; IPsec; lightweight; key negotiation; secure encryption

0　引言

随着无线通信技术的快速发展，无线自组网（Wireless Ad Hoc Networks，WANS）作为一种无需固定基础设施、快速部署的无中心自组织网络形态，在城市复杂建筑、应急救援、临时网络连接等领域得到了广泛的应用[1-3]。由于自组网无线信道的开放性，信息在无线信道中进行传输时面临着窃听、篡改、伪造等多种安全威胁，如何保证无线通信的安全已成为无线自组网的研究重点[4-5]。

IPsec（Internet Protocol Security）协议作为一种端到端的加密和认证机制，通过使用认证头（Authentication Header，AH）、封装安全负载（Encapsulating Security Payload，ESP）、安全联盟（Security Association，SA）以及互联网密钥交换（Internet Key Exchange，IKE）协议为 IP 层通信提供了数据完整性和机密性保障[6-7]，该协议在传统有线网络环境中得到了广泛应用，但在无线自组网环境下由于其网络动态特性以及资源限制，直接部署传统 IPsec 协议面临着适应性不足和性能下降等挑战。为了解决上述难题，目前主流的解决方案有 IPsec 协议栈裁剪

技术、IKE 密钥协商及 SA 优化技术[8-10]，但现有方法仍存在协议动态适应性不足、协商交互流程复杂、流量开销较大以及动态拓扑下通信时延高等问题。本文针对无线自组网的安全传输需求，提出了一种轻量化 IPsec 加密的无线自组网通信方案，通过设计轻量化密钥协商协议提供 IPsec 加解密安全保护机制，最小化对无线自组网网络性能的影响。

1 系统硬件设计

1.1 总体架构

本方案采用“CPU + 算法 FPGA + 基带波形 FPGA”技术路径，总体架构设计如图 1 所示，主要由管理单元、加解密处理单元、波形处理单元、捷变频单元、功放单元、接口单元等模块组成。管理单元主要负责整个系统的版本管理、数据接口处理、基带配置、算法配置、密钥协商、用户可维可测等功能。加解密处理单元通过算法处理 FPGA 实现用户数据的 IPsec 解析与封装、加密解密处理。波形处理单元负责基带信号编码、组帧、调制等一系列信号处理，实现基带无线波形的设计和成型。捷变频单元主要负责基带数字信号和射频信号的转换，发射端从基带数字信号转换成射频信号，接收端从射频信号转换成数字基带信号。功放单元实现射频信号的放大、收发以及收发开关切换控制等功能。电源单元为系统其他模块提供稳定可靠的直流供电激励，并具备自动断电保护功能。

1.2 硬件选型

管理单元采用龙芯中科公司的 LS2K1000 芯片，对内支持波形 FPGA 和算法 FPGA 的配置管理、时隙调度、码流选择等处理，对外支持密钥协商、设备管理。LS2K1000 基本性能如下：CPU 内核为 GS264 双核，主频 1 GHz，内存 DDR3，位宽 64 位。

算法处理单元采用 Xilinx 公司 XC7K160T 芯片，周围配套上设有 QDR、DDR 等芯片，辅助 FPGA 完成业务数据流的策略控制、协议封装、队列管控、杂凑认证算法和密码算法等处理。

波形处理单元采用 Xilinx 公司 ZYNQ7035，该系列 FPGA 集成了 PS 和 PL 两大功能模块，PL 为 FPGA 部分，PS 为嵌入式处理器系统，可进行嵌入式计算任务应用，其内部还继承了 SPI、IIC、UART、Ethernet 等接口[11]，依托异构架构和丰富的硬核资源，ZYNQ7035 可以实现各种灵活的时序和逻辑设计。

捷变频单元采用 ADI 公司高性能、高集成射频捷变收发器 AD9363，AD9363 拥有两个独立的接收器和两个独立的发射器，支持 TDD 和 FDD 模式[12]。该器件集 RF 前端、频率合成器以及灵活的混合信号基带部分为一体，为处理器提供了可配置数字接口，从而大大简化了系统设计。

1.3 射频设计

本方案射频设计采用 2T2R 技术实现，射频系统主要包含射频发射链路、射频接收链路，功能设计如图 2 所示。发射链路和接收链路通过捷变频单元 AD9363、放大器开关进行切换分时工作。

（1）射频接收链路：主要由天线、滤波器、收发开关、低噪放、数控 ATT、巴伦以及 AD Transceiver 器件 AD9363 组成。接收信号通过低噪声放大器进行放大，然后经过混频成为中频信号后经过 AD9363 变换为数字基带信号，送入基带波形 FPGA 进行解调处理。

（2）射频发射链路：主要包括 2 级放大器和 3 级功放管。基带波形 FPGA 基带调制信号经过 AD9363 调制成中频信号，经过混频成为射频信号，再通过发射放大链路发射出去。

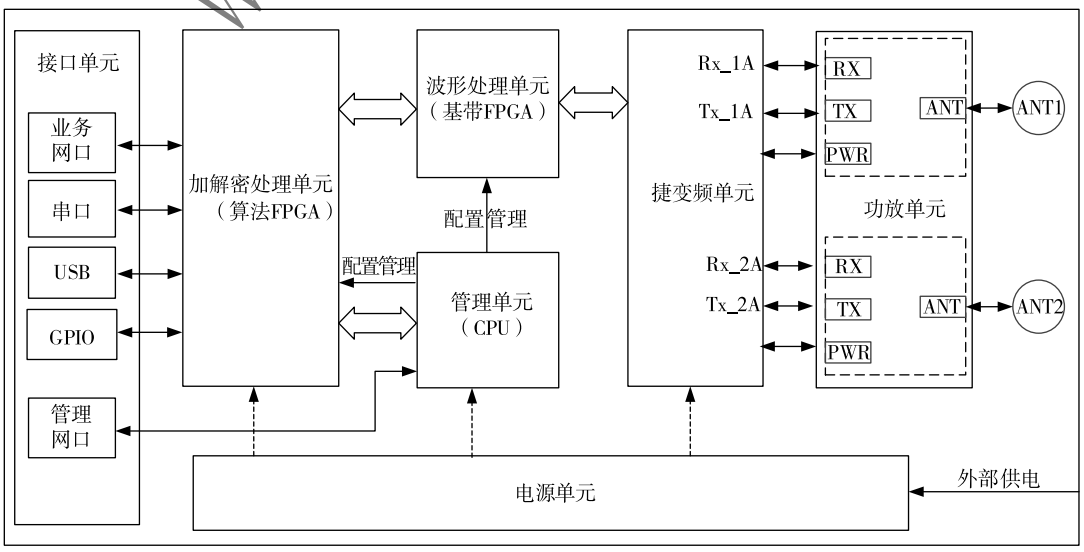


图 1 总体架构设计图

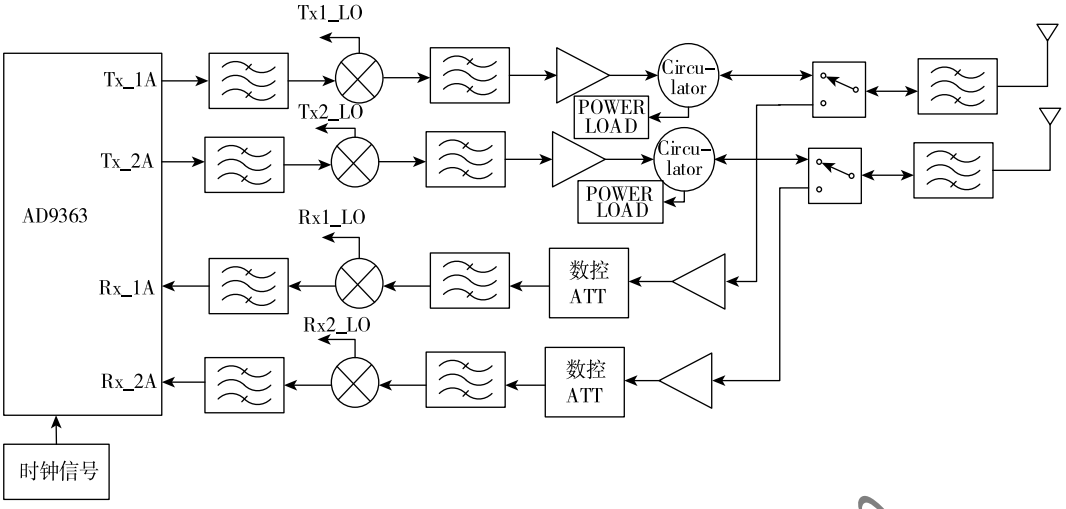


图 2　射频 2T2R 设计图

射频系统采用 TDD 模式，发射链路和接收链路共用一个频点交替工作，因此收发切换要保证严格的时序关系。本方案收发切换设计如图 3 所示，主要涉及发射链路 PA 打开/关闭、接收链路 LNA 打开/关闭、射频电子开关切换以及 AD9363 内部的收发时隙切换，通过 FPGA 的 GPIO 控制 PA、LNA、射频电子开关实现准确的时序控制：在发射时隙到来之前，提前一段时间（至少 30 μs）打开 PA、关闭 LNA，并且将电子开关打到发射链路；在发射结束后，滞后延迟 30 μs 关闭 PA、打开 LNA，同时将电子开关打到接收链路。在单板设计时，通过上下拉电阻使得 PA_EN 默认处于关闭状态，LNA_EN 默认处于打开状态，以保证 FPGA 未开始正常工作时单板处于射频接收状态。

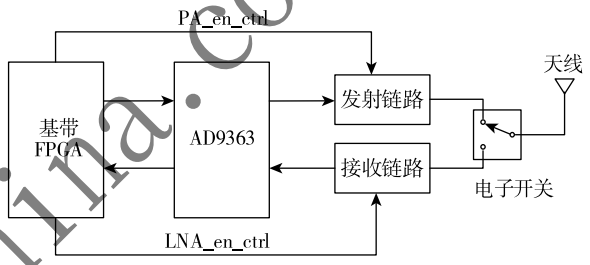


图 3　收发链路开关切换控制设计图

1.4　电源设计

系统电源设计如 4 所示，外部直流电源输入 DC18 ~ 28.6 V，通过专用设计的防反接保护电路分为两路：一路经升压芯片 LM5155 升压为 28 V，为功放单元供电；另外一路经降压芯片 TPS54360 降为 5 V，为数字电路及部

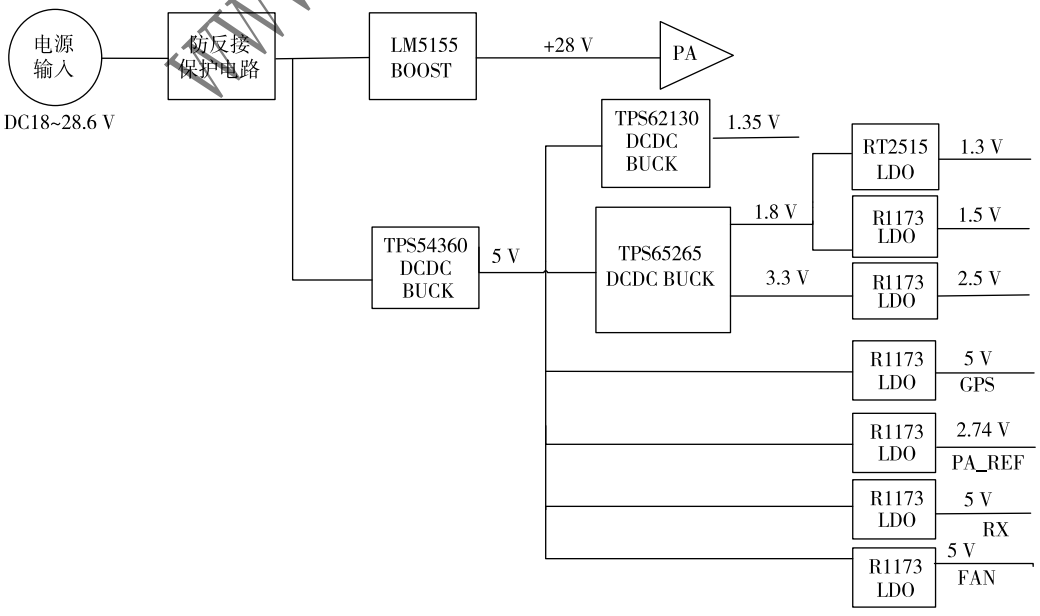


图 4　系统电源树设计图

分功放电路供电，5 V 再经 DCDC 和 LDO 转换为各路低压电源。电源中低压电源的 DC-DC 选择 TPS65265，可同时输出 3 路电源，电流为 5 A/3 A/2 A，效率可达到 90%以上。由于板上的电压种类较多，采用此芯片可节省单板面积，同时也方便电源上电、下电时序的控制。

2　系统软件设计

2.1　软件架构设计

系统软件采用分层设计思想，自下而上依次为基础资源层、业务服务层、应用交互层，如图 5 所示。基础资源层作为系统运行的支撑平台，主要提供嵌入式 CPU、FPGA、操作系统、通信接口等软硬件资源支撑。业务服务层为自组网通信设备提供业务管理、加解密处理、波形处理等功能服务，支撑实现业务加解密及无线射频通信；应用交互层提供可视化人机界面、配置管理查询、声光告警等应用功能。

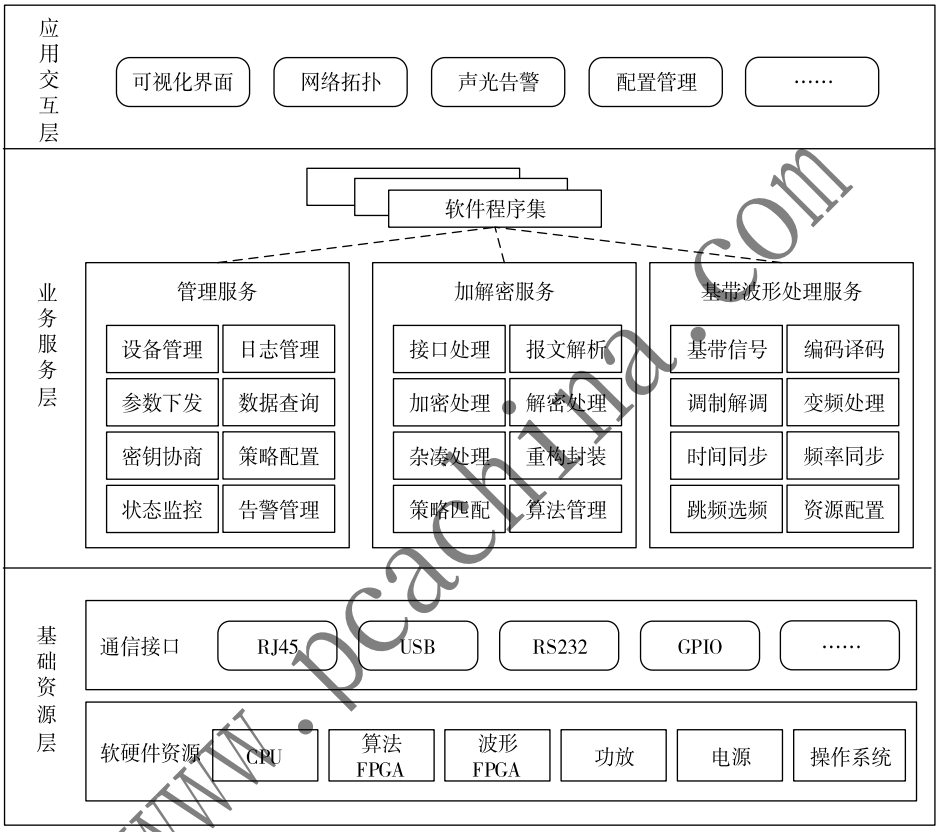


图 5　系统软件分层架构设计图

系统软件整体上分为业务处理软件和应用管理软件两大类，其中应用管理软件运行在用户终端上，业务处理软件运行于自组网通信设备的芯片处理器中，根据不同位置又细分为 CPU 主控软件、加解密处理软件以及波形处理软件，其具体逻辑关系如图 6 所示。

2.2　基带波形 FPGA 逻辑设计

基带波形软件是自组网通信设备实现无线射频收发通信的关键软件，主要通过基带 FPGA 逻辑实现射频发送和接收链路，其逻辑架构设计如图 7 所示。

射频发送链路处理流程依次经过 CRC 校验、编码、打孔、QAM 星座映射、预编码、IFFT 变换、CP 处理、变频等信号处理，最后经过多路射频发射出去。射频接收主要实现 OFDM 信号的解调，主要包括变频、时间/频

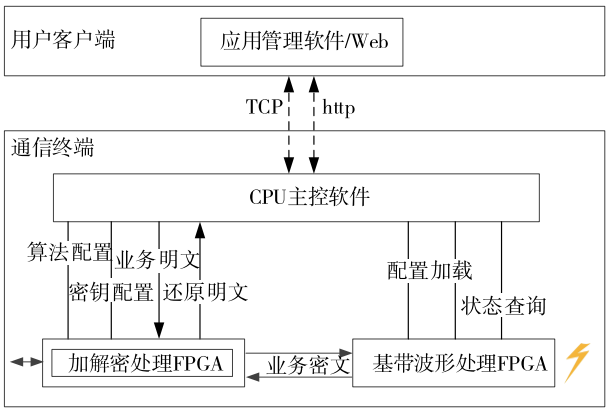


图 6　系统软件逻辑架构图

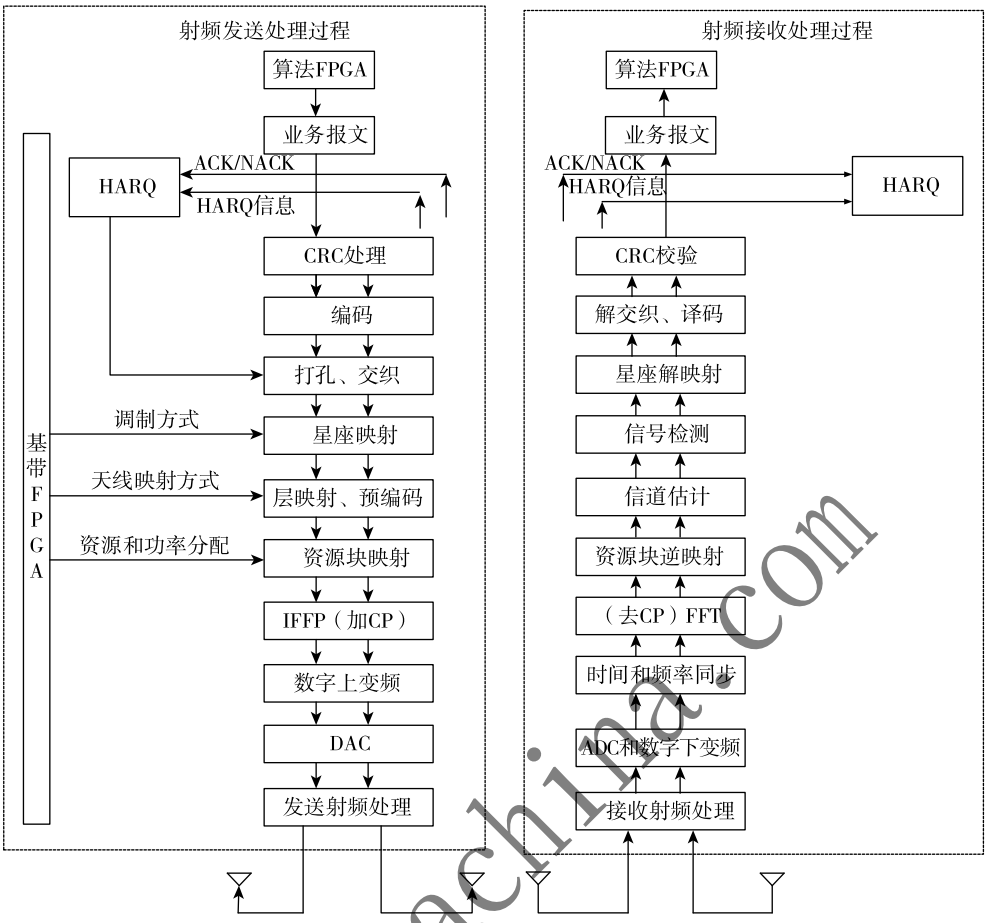


图7　波形 FPGA 逻辑架构设计

率同步、FFT 以及 CP 处理、频偏估计与补偿、信道估计、星座解映射、解交织、译码及校验等处理模块。

2.3　加解密 FPGA 逻辑设计

自组网通信设备的无线通信加密传输功能通过加解密 FPGA 来实现，其逻辑架构设计如图 8 所示。业务网口面向用户终端，对其业务明文进行加密保护，加密方向处理流程依次包括报文解析、二层分类、分片重组、五元组匹配、策略匹配、IPsec 包封装、加密算法处理、IP 包封装、以太网封装等，进一步通过基带波形 FPGA 发射出去；基带 FPGA 对射频信号通过变频、解调、译码得到业务密文，加解密 FPGA 解密方向处理流程依次为报文解析、二层分类、分片重组、三元组匹配、策略匹配、IPsec 解封装、解密算法处理、抗重放、IP 包封装、以太网封装、CRC 校验等。

3　关键算法设计

3.1　算法密钥设计

IPsec 是 IETF 定义的为 IP 网络提供完整安全性解决方案的一系列服务和安全协议簇，它是一种标准化的网络框架，旨在提供一个端到端的安全机制，以透明的方式在 IP 网络中提供安全服务，保障数据的完整性和机密性，从而有效地抵御各种网络攻击。IPsec 核心组件主要包括 AH、ESP、SA 以及 IKE 等协议，这些协议组件各自承担着不同的安全功能[13-15]。

为了保证无线自组网中信息传输的机密性、完整性和可用性，本方案基于 IPsec 协议对系统整体算法进行轻量化设计，算法配用情况如表 1 所示。在密钥方面，设计了设备主密钥、初始共享密钥、业务加密密钥等三大类，其中主密钥用于加密保护“初始共享密钥”、设备身份 ID 信息，初始共享密钥主要用于密钥协商报文的加密保护，业务加密密钥则用于业务数据的加密保护，密钥之间关系及启用流程如图 9 所示。

表 1　算法配用设计列表

算法名称	工作模式	用途
资源加密算法	SM4-ECB	用于保护本地初始共享密钥、设备身份 ID 等资源
密钥协商算法	DH 算法	用于节点之间密钥协商
业务加密算法	SM4-CBC	用于业务数据加密保护
杂凑算法	SM3-HMAC	用于数据完整性保护

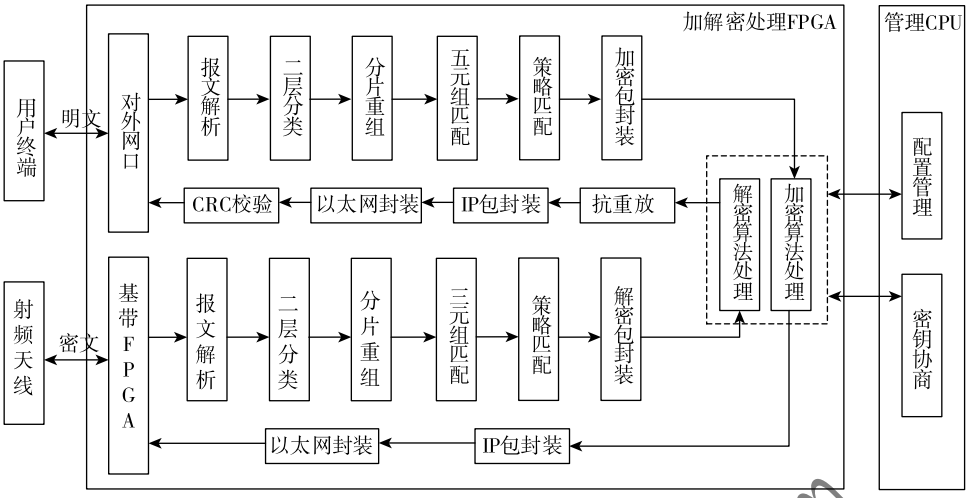


图 8　加解密 FPGA 逻辑架构设计

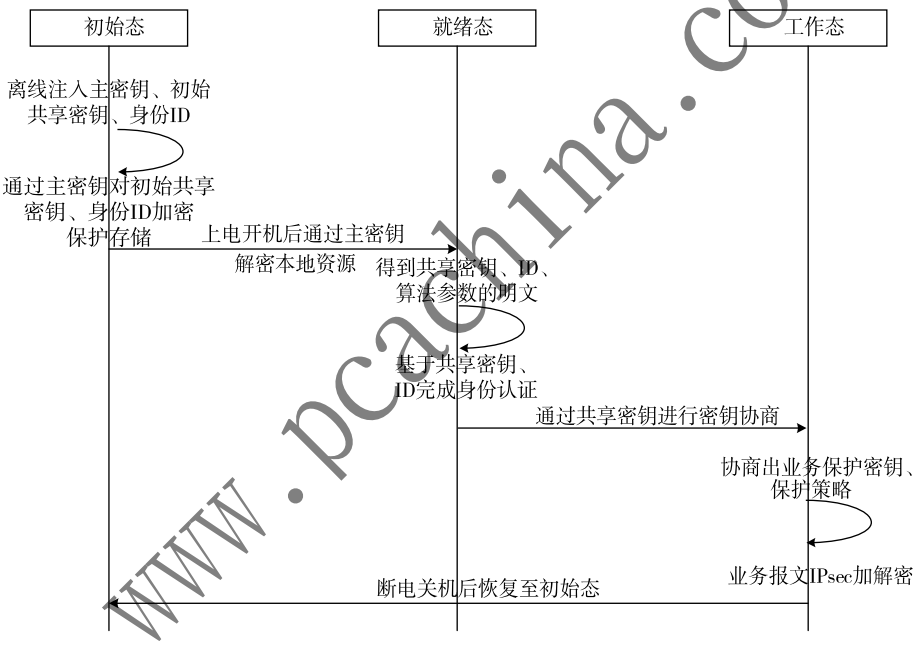


图 9　密钥启用关系流程设计图

3.2　密钥协商设计

无线自组网中业务数据传输保护密钥通过“协商”的方式产生，本方案采用轻量化协商机制，提出并设计了一种“四次交互”密钥协商协议，主要包括协商请求（ClientHello）、协商响应（ServerHello）、协商响应（ClientFinish）、协商确认（ServerFinish）四个阶段，协议交互流程如图 10 所示。

在密钥协商协议的实现中，采用基于共享密钥的消息验证方式来确认双方的身份合法性，并通过保护算法对协商报文的部分字段进行机密性、完整性保护。具体协商方案步骤如下：

（1）发起方 A 按照协商协议，基于共享密钥对自身 ID 信息进行加密、杂凑算法保护，向 B 发送协商请求报文 ClientHello。

图 10　轻量化密钥协商处理流程设计

（2）响应方 B 收到协商请求报文后，先检查报文类型是否为 ClientHello，如果不符合则退出本次协商过程，并给 A 发送错误通告；如果报文类型检查通过，则基于共享密钥按照算法协议进行密码解密运算、CRC 校验和身份验证，若验证失败则退出本次协商过程并给 A 发送错误通告，若身份验证通过则向 A 发送协商响应报文 ServerHello。

（3）发起方 A 收到协商响应报文后，检查报文类型是否为 ServerHello，如果不是则继续检查是否为通告包，若是通告包则解析通告后退出本次协商过程；如果 ServerHello 报文类型检查通过，则按密码算法协议进行解密运算、CRC 校验和身份验证，若验证失败则退出本次协商过程并给 B 发送错误通告，若验证通过则向 B 发送协商响应报文 ClientFinish。

（4）B 收到协商报文，先检查报文类型是否为 ClientFinish，如果不符合则退出本次协商过程，并给 A 发送错误通告；如果报文类型检查通过，则基于共享密钥按照算法协议进行密码解密运算、CRC 校验，若验证失败则退出本次协商过程并给 A 发送错误通告，若验证通过则向 A 发送协商确认报文 ServerFinish，告知对方本次协商成功。

经过上述一次性协商过程，节点双方共享新的协商密钥、安全参数索引（Security Parameter Index，SPI）、协议标识（AH、ESP 或者二者结合）、工作模式（传输模式、隧道模式）、密钥生存周期、加密算法等 IPsec 安全策略，主要协商参数如表 2 所示。

表 2　密钥协商主要参数列表

名称	位宽/bit	用途
安全策略	2	00：禁通；01：密通；10：明通；11：保留
工作模式	2	00：当前 SA 无效；01：传输模式；10：隧道模式；11：保留
SPI	32	安全索引参数
序列号	64	抗重放序列号
算法标识	8	算法选择类别
加解密密钥	256	协商加密密钥
加密密钥使能	1	0：加解密密钥无效；1：加解密密钥有效
认证密钥	256	协商认证密钥
认证密钥使能	1	0：认证密钥无效；1：认证密钥有效
源 IP	32	隧道模式下重构源 IP
目的 IP	32	隧道模式下重构目的 IP

本方案提出的轻量化协商协议相较于传统的互联网密钥交换协议 IKE，通过精简协议流程将密钥交换的交互流程从 IKE 标准的两阶段六消息模式压缩为单阶段四消息模式，减少握手次数达 33%，同时通过动态参数预置降低协商数据流量开销，使其在无线自组网、物联网等无线信道资源受限的网络环境下展现出更强的适应性。

4　实验验证与分析

根据上述软硬件设计方案，研制了一款基于轻量化 IPsec 安全加密的无线自组网通信设备，为了验证样机加密通信的可行性，搭建如图 11 所示测试环境，对系统的核心功能及性能进行测试验证。

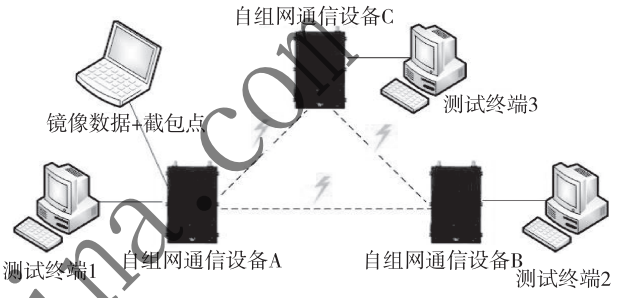


图 11　测试环境示意图

4.1　功能测试

测试中验证了自组网通信设备的密钥协商、ESP 加解密等功能，具体测试方法如下：

（1）CPU 嵌入式程序开启打印，跟踪系统开机解密、初始配置以及密钥协商等过程信息记录；

（2）加解密 FPGA 对加密处理后的报文同步镜像转发至网络接口，通过布设截包点进行 Wireshark 抓包分析；

（3）自组网通信设备配置安全策略为密通，工作模式设置为传输模式，采用 ESP 协议进行 IPsec 加密；

（4）测试终端 1 通过网络工具发送报文，在截包点抓取密文并核对 ESP 格式；

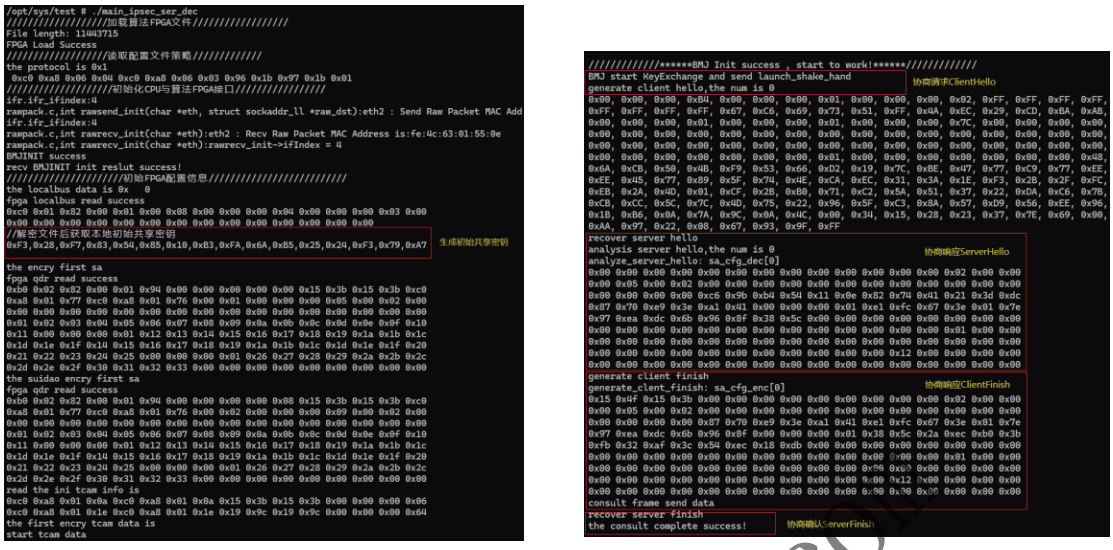
（5）自组网通信设备配置安全策略为密通，工作模式设置为隧道模式，采用 ESP 协议进行 IPsec 加密；

（6）测试终端 1 通过网络工具发送报文，在截包点抓取密文并核对 ESP 格式。

测试结果如图 12、13 所示，结果表明本文提出的轻量化 IPsec 设计方法能够正确实现无线自组网通信的 IPsec 加解密处理功能。

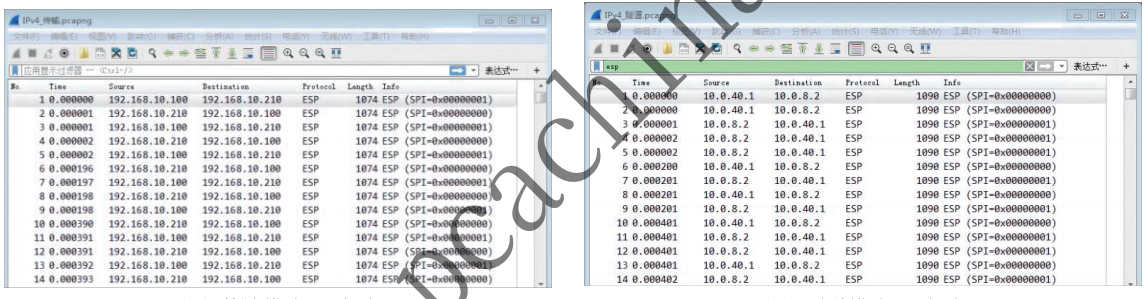
4.2　性能测试

为了测试轻量化加密对自组网通信时延、带宽的影响，分别对不含加密、含加密两种方式进行对比实验，具体测试方法及步骤如下：



（a）产生初始共享密钥　　（b）四次交互密钥协商

图 12　密钥协商过程测试结果



（a）传输模式ESP加密　　（b）隧道模式ESP加密

图 13　IPsec 加解密处理功能测试结果

（1）自组网通信设备配置安全策略为明通模式，对业务报文不进行加密；

（2）通过网络丢包时延工具 ATKKPING，选择“以太网最大 MTU”，Ping 次数为 100 次，统计通信时延以及丢包率；

（3）通过网络灌包工具 iperf3. exe 进行 TCP 网络性能测试，灌包时间持续 120 s，统计灌包速率；

（4）重复 10 轮步骤（2）、（3），测试结果取平均值；

（5）自组网通信设备配置安全策略为密通模式，对业务报文进行 ESP 加密，执行步骤（2）～（4），统计记录结果。

测试结果统计如表 3 所示。经测试，自组网在不加密通信模式下平均时延为 13. 93 ms、TCP 灌包速率为 25. 42 Mbit/s，加密通信模式下平均时延为 16. 71 ms、TCP 灌包速率为 23. 28 Mbit/s。由测试结果可以看出，相比于明文传输，本方案采用轻量化 IPsec 加密后数据加密传输速率仅损失约 8. 4%（约为 2. 14 Mbit/s），单向端到端传输时延仅延长 1. 39 ms（ping 包时延为双向时延），能够满足自组网典型业务场景苛刻要求，符合研发预期。

表 3　测试结果统计表

序号	不加密通信		轻量化 IPsec 加密通信	
	时延/ms	灌包/（Mbit/s）	时延/ms	灌包/（Mbit/s）
1	13. 95	25. 4	16. 64	23. 3
2	13. 98	25. 3	16. 89	23. 5
3	13. 82	25. 2	16. 60	23. 3
4	13. 92	25. 5	16. 56	23. 6
5	13. 75	25. 4	16. 96	22. 9
6	14. 03	25. 7	16. 87	23. 1
7	13. 91	25. 3	16. 52	23. 3
8	13. 96	25. 5	16. 74	23. 2
9	14. 05	25. 6	16. 64	23. 2
10	13. 94	25. 3	16. 69	23. 4
平均	13. 93	25. 42	16. 71	23. 28

5 结论

针对无线自组网的安全加密通信需求，本文以“CPU + 算法 FPGA + 基带波形 FPGA”技术架构为核心设计了一种基于轻量化 IPsec 安全加密的自组网通信设备，通过精简协议设计将 IKE 标准的两阶段六消息模式压缩为单阶段四消息模式，握手次数减少达 33%，有效降低了协商数据流量开销。搭建测试环境进行了技术验证测试，结果表明该设备支持 IPsec 加解密，实现了无线传输过程的机密性、完整性保护，TCP 灌包传输速率达 23.28 Mbit/s，无线通信时延约 16.71 ms。该方案为自组网、物联网等无线安全传输提供了有效可行的技术支撑，具有较高的参考价值。

参考文献

[1] 黄巍，陈俊良，李犹海. 无人机自组网技术综述与发展展望 [J]. 电讯技术，2022，62（1）：138 - 146.

[2] 卓琨，张衡阳，郑博，等. 无人机自组网研究进展综述 [J]. 电信科学，2015，31（4）：134 - 144.

[3] YOUNIS Z A，ABDULAZEEZ A M，ZEEBAREE S R M，et al. Mobile Ad hoc network in disaster area network scenario [J]. International Journal of Online and Biomedical Engineering，2021，17（3）：49 - 75.

[4] 李乃振，刘继光，李朝东. 无线自组网技术安全威胁分析 [J]. 计算机与网络，2015，41（7）：62 - 64.

[5] 王海涛，陈晖，朱世才，等. 无线自组网的安全保障问题和相关机制探讨 [J]. 保密科学技术，2014（2）：40 - 45.

[6] 姬胜凯，王硕，黄毅龙，等. 基于高性能 FPGA 的超高速 IPSec 安全设备设计与实现 [J]. 网络安全与数据治理，2024，43（11）：13 - 18.

[7] HONG S. Issues and security on IPSec：survey [J]. Journal of Digital Convergence，2014，12（8）：243 - 248.

[8] 曾喜娟. IoT 云连接中轻量级 IPSec VPN 的部署 [J]. 绵阳师范学院学报，2020，39（8）：94 - 97.

[9] 薛富实. 轻量级 IPsec 在嵌入式系统中的设计与实现 [D]. 成都：电子科技大学，2011.

[10] 王必韧. 轻量级 IPSec 协议一致性测试集及测试用例开发——基于 IPv6 的无线传感网 [D]. 南京：南京邮电大学，2014.

[11] 高梓超. ZYNQ7035 核心板及高速 ADC 设计 [J]. 无线电，2024（4）：52 - 58.

[12] 白永康. 基于 AD936X 的便携式矢量网络分析仪设计 [D]. 桂林：桂林电子科技大学，2023.

[13] 王硕，胡现刚，杨欢，等. 多通道 10G 网络安全设备的设计与实现 [J]. 网络安全与数据治理，2024，43（10）：7 - 13.

[14] 密码行业标准化技术委员会. IPSec VPN 技术规范：GM/T 0022 - 2023 [S]. 北京：中国标准出版社，2023.

[15] 廖悦欣. IPSec 协议实现技术研究 [D]. 广州：华南理工大学，2013.

（收稿日期：2025 - 04 - 17）

作者简介：

张卫敏（1990 - ），通信作者，男，硕士，高级工程师，主要研究方向：自组网通信及信息安全。E-mail：15210617312@163.com。

焦运良（1985 - ），男，硕士，正高级工程师，主要研究方向：宽带通信及信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部