DOI:10.19304/j.cnki.issn1000-7180.2015.12.018

面向终端的网络安全处理器体系结构设计

朱宁龙，曲思源，戴紫彬
（解放军信息工程大学 密码工程学院，河南 郑州 450000）

摘 要：提出了一种面向终端的网络安全处理器体系结构设计. 该设计采用基于宏流水的总线结构，提高了数据平面的数据传输速率，缓解了总线仲裁压力. 将流存储机制应用到处理器的层次化存储结构中，结合经过指令集优化的网络安全处理引擎，提高了多任务并行计算能力. 同时设计了安全防护电路，用于保证处理器自身的安全性. 实验和分析证明了提出的网络安全处理器具有较高的性能，能够满足终端设备的通信需求.

关键词：网络安全处理器；体系结构；宏流水；总线；流存储
中图分类号：TP393 **文献标识码**：A **文章编号**：1000－7180(2015)12－0080－05

Design of a Network Security Processor for Terminal Devices

ZHU Ning-long, QU Si-yuan, DAI Zi-bin
(Institute of Cryptography Engineering, PLA Information Engineering University, Zhengzhou 450000, China)

Abstract: The paper proposes an architectural design of Network Security Processor for terminal devices. This design uses macro-pipelining bus architecture, which improves the data transmitting rate of data plane and decreases the workload of bus arbitration. By introducing stream memory into the hierarchy memory architecture and using network security processor engine with optimized instruction set architecture, this design improves the ability of multi-task parallel processing. Furthermore, this design uses safe circuit to protect the processor. The results show that this design has high performance, which can meet the demand of terminal devices.

Key words: network security processor; architecture; macro-pipelining; bus; stream memory

1 引言

网络处理器(Network Processor，NP)是一种专门针对网络应用设计的可编程器件，兼具了通用处理器的灵活性以及ASIC的高性能等特点，目前已广泛应用于互联网中. 根据网络设备的需求不同，网络处理器可以应用于核心层、边缘层和接入层[1]. 其中应用于接入层的网络处理器主要面向终端设备，随着终端设备种类和通信量的急剧增长，对网络处理器的安全处理性能提出了更高的要求.

根据国际工程任务组(IETF)制定的标准，目前主要通过IPSec、SSL等协议保证网络数据的安全. 这两种协议都包括大量计算密集型的密码算法，而传统的网络处理器大多通过软件的方式实现安全协议，给终端设备带来了较大的计算负担和网络延时. 针对这一问题，近年来提出了一些网络安全处理器的设计方案[2-4]，但是大多都采用同一设计思路，在很多方面还有较大的开发空间. 本文从总线结构、存储结构等多个方面对网络安全处理器进行研究，提出了一种新的体系结构.

2 网络处理器体系结构设计

2.1 总线结构

片上通讯架构是处理器体系结构设计的关键，决定了网络安全处理器各功能模块之间的通信方式. 根据处理任务类型的不同，网络处理器可以划分为控制平面(Control-plane)和数据平面(Data-plane)[1]，不同平面上的功能模块对通信的需求不同，总线设计既要能满足所有模块的要求，又要节省片上资源. 数据平面为控制平面通信特点如表1

收稿日期：2015－03－17；修回日期：2015－04－20

所示.

表1　数据平面与控制平面通信特点对比

	控制平面	数据平面
通信速度	低	高
数据路径	简单	复杂
实时性	低	高
系统层次	顶层	底层

从表1可以看出，控制平面位于网络处理器的顶层，需要对所有功能模块进行控制，但是对通信速度要求较低，而且数据路径简单，本文使用AHB总线实现控制平面传输.

相比于控制平面，数据平面位于系统的底层，实时性高，对通信速度的要求高，而且数据路径复杂，容易成为总线通信瓶颈. 多数网络处理器采用多个处理单元(Processing Elements，PE)并行处理[5]或串行流水[6]的方式解决这一瓶颈，但仍存在编程模型复杂、资源利用率低等问题. 针对这一问题，本文将宏流水的思想引入到总线设计中，将网络处理器的数据流传输路径分为接收级、处理级、发送级，使用高速AXI总线实现网络数据流水化处理.

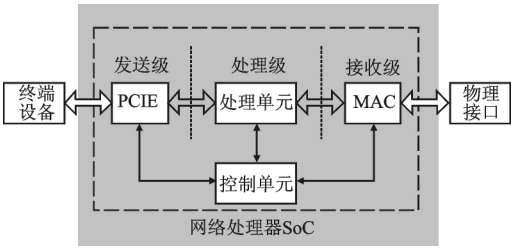

图1　网络处理器数据流传输模型

本文使用处理单元的平均工作频率大约为200 MHz，假设处理1个数据包需要500个时钟周期，则要完成全双工数据包处理，处理器每秒钟可以处理的数据包个数为

200 MIPS÷500 Inst/Packet÷2=0.2 MPPS.

式中，MPPS指Million Packets Per Second，数据包长度按平均长度150字节计算，则处理器的吞吐率为

0.2 MPPS × 150 byte × 8 bit/byte = 240 Mb/s.

以太网MAC的通信速度可达1 000 Mb/s，PCIE的通信速度最高为5 Gb/s，因此处理级流水段是整个流水线的瓶颈，本文通过设置多个处理单元，采用多核并行处理的方法消除宏流水线通信瓶颈，使总线通信速率达到最大.

2.2　存储结构

目前网络处理器存储结构大多采用基于本地存储器或基于Cache的存储结构[7]，能够较好地适应网络协议解析的处理特点. 然而，网络安全处理器除了进行网络协议解析外，还需要对数据包进行加解密处理，属于深度处理应用，具有重复性差、无回溯等典型的流处理特点，使用上述存储机制会带来Cache miss等问题，导致存储系统性能下降[8].

本文借鉴通用处理器存储体系结构，将面向流处理领域的流存储机制应用到网络安全处理器中，提出了基于流存储机制的层次化存储模型，如图2所示.

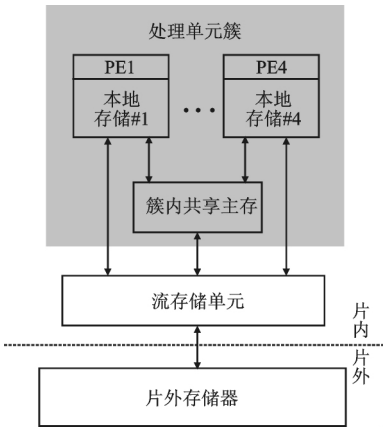

图2　基于流存储机制的层次化存储模型

根据上一节的分析，处理级采用多核并行处理技术，其中每个处理单元都有各自的私有存储，各处理单元间通过共享存储互连成“簇”(Cluster)，构成二级存储单元结构. 处理单元可以通过硬连线的方式直接访问簇内共享数据存储器，增强了各处理单元之间的耦合程度，同时减少数据写回主存再读取的重用开销. 簇内共享存储增强了存储体系的层次性，避免了频繁的片外存储访问，缓解了本地存储与片外存储之间的速度差距，提高了通信速度.

流存储单元用于管理数据在处理单元与片外存储之间的传输. 网络安全处理器的处理单元与片外存储之间的数据传输比较频繁，当数据段存放在片外存储器的不同区域时，通过流存储单元、软件调度等技术可以对传输数据流进行重新组织，实现批量数据传输. 同时，当处理单元对数据包的某一段进行处理时，通过流存储单元可以实现对待处理数据的预取，避免了处理单元访问本地存储失效而需要再次访问片外存储的延时. 流存储机制适应了深度处

理应用特点，能够实现数据传输与运算执行、输入与输出等多种并行，提高了网络处理器处理单元的并行性开发.

基于流存储的层次化存储模型对应的硬件结构如图 3 所示，主要由总线接口、流存储单元(Stream，SM)、中央调度器(Central Scheduler，CS)、共享存储(Shared Memory，SM)、网络安全处理单元(Network Secure Processing Element，NSPE)等部分组成.

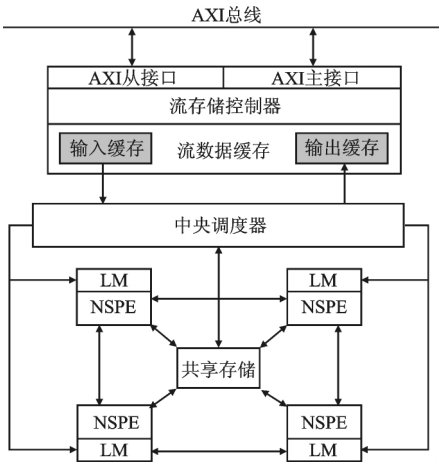

图 3 基于流存储的层次化存储硬件架构

(1)AXI 总线接口

多核网络安全处理单元既可以作为总线从设备又可以作为总线主设备使用. 当作为从设备时，控制平面 CPU 通过 AXI 从接口完成对流存储控制器的寄存器配置、传输描述符输入、数据包输入/输出等工作.

当作为主设备使用时，网络安全处理单元具有总线控制功能，流存储控制器可以通过 AXI 总线主接口向总线发送传输控制信号，在获得总线使用权后可以向目的设备地址写入数据或从源设备地址读取数据，减轻了控制平面 CPU 的负担，提高了总线使用率.

(2)流存储单元

流存储单元包括流存储控制器和流数据缓存. 流存储控制器负责数据在处理单元内部存储和片外存储之间的传输，通过链表 DMA 的方式完成数据传输，实现数据预取与 DMA 传输相结合的优化策略. 链式 DMA 传输指将多组 DMA 传输串连，每一个 DMA 传输的目的地址和数据长度都可以不同，直到本次所有 DMA 传输完成后向总线发出中断完成信号.

流数据缓存是连接片外存储和处理单元本地存储的中间缓存，用来缓存处理单元输入/输出数据，匹配总线数据传输速率和处理单元处理速率，可以分为输入缓存 FIFO 和输出缓存 FIFO，深度均设计为 512×32 bit.

(3)中央调度器

中央调度器是整个流存储机制的控制核心，起着流存储控制、任务调度、协调系统中各单元正常工作的重要作用，完成流数据缓存部件与处理单元本地存储之间的数据调度.

中央调度器由一个通用微码处理器构成，通过执行微代码实现对流存储单元的控制.

(4)本地存储

本地存储用于存储待处理数据和中间结果，供处理单元调用. 和流数据缓存一样，本地存储使用 FIFO 缓存数据，为提高数据传输速率，网络安全处理单元的本地存储采用输入/输出相分离的结构，即本地存储分为输入缓存和输出缓存两部分，各为 256×32 bit.

(5)簇内共享存储

簇内共享存储采用一个大小为 4 KB 的共享数据 RAM. 为提高访存速度，处理单元与共享存储之间采用硬连线的方式连接，处理单元对共享存储的访问需要 2 个时钟周期，仅比本地存储多 1 个时钟周期，与传统多级存储结构中的访存延时相比有了很大改善.

为解决不同处理单元同时访问共享存储带来的访存冲突问题，同时出于硬件精简性和低功耗特性考虑，簇内共享存储采用固定优先级的方式以避免复杂的仲裁逻辑.

(6)片外存储

片外存储器负责接收/发送数据包、系统程序、配置信息等的存储，设备通过总线访问片外存储.

通过在网络处理器中引入流存储机制，一方面通过数据预取减少了处理单元访问片外存储的延迟，另一方面通过链式 DMA 传输，加快了数据传输速率，提高了总线利用率，更加符合网络安全处理器的需求.

2.3 安全防护电路

网络安全处理器芯片属于安全芯片范畴，除了为通信数据进行安全保护外，其本身也要进行安全防护，本文设计以下安全防护电路实现这一目的.

JTAG：通过 JTAG 模块可以实现对 JTAG 接口的管理，使普通用户无法通过该接口访问芯片内部信息，保护芯片安全.

环境检测：用于对芯片电压、温度以及内部频率进行检测，当芯片内部工作环境超出正常范围时，该模块向 CPU 发出中断请求.

噪声源：用于产生对数据包加解密过程中需要的随机数，同时可以产生随机功耗. 包含随机数检测机制，当随机数的品质不符合要求时产生中断请求.

CLKM：时钟管理模块，通过配置寄存器可以关闭当前不需要的时钟，降低系统功耗.

2.4　整体结构

网络安全处理器的整体结构如图 4 所示. AXI1、AXI2 和 AXI3 构成了网络安全处理器数据平面宏流水结构，接收级、处理级和发送级分别连接在三条高速 AXI 总线上，AXI4 为存储访问总线，流水线各级设备均可以通过该总线访问 SRAM2. AHB 总线为控制平面总线，该总线上只有一个主设备 CK810 CPU，负责对所有设备进行配置和管理，X2H 为总线桥，实现了 AXI 总线设备与 AHB 总线设备之间的通信. 低速总线 APB 用于连接系统外围低速设备.

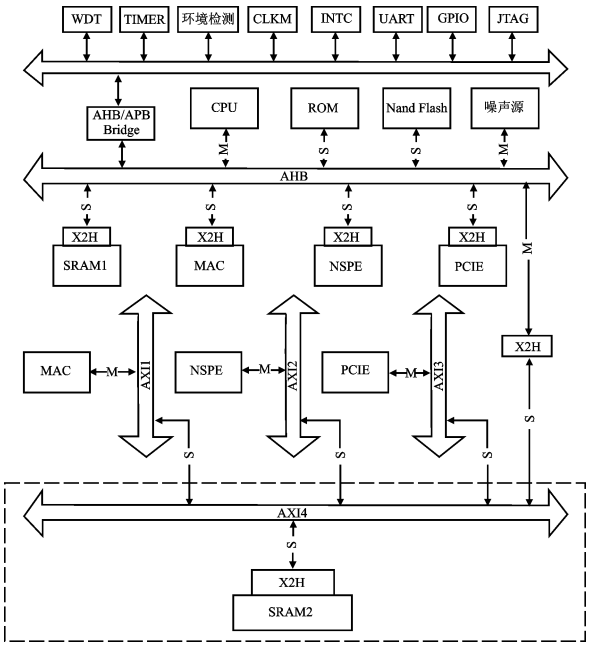

图 4　网络安全处理器整体结构

NSPE 是整个网络安全处理器的处理核心，采用实验室自主开发的处理引擎实现. NSPE 采用 VLIW 指令架构，具有面向密码运算和网络协议解析进行优化的指令集，能够高速实现协议解析和数据包的加解密处理.

MAC 控制器是系统的以太网接口部件，它在 NSPE 的控制下对外围 PHY 接口进行控制，实现以太网数据包的接收/发送.

PCIE 控制器管理系统的 PCIE 总线接口，用于连接外部终端设备，实现了网络安全处理器与终端设备之间的高速通信. 通过 CPU 对 PCIE 控制器的寄存器进行配置可以实现对通信速度、工作模式等的控制.

ROM 为只读存储器，用于存放系统引导程序，Nand Flash 用于存放用户程序，系统上电后，CPU 从 ROM 中读取指令执行，完成系统引导，然后直接跳转到用户程序区，将 Nand Flash 中存放的用户程序搬移到 CPU 指令 Cache 中执行.

看门狗定时器 WDT 可以检测系统程序运行状态，避免程序锁定. TIMER 是一个计时器/定时器，可以为系统提供周期的定时中断. 中断控制器 INTC 用于接收其他模块的中断信号，并将这些中断请求发送给 CPU. 异步收发传输器 UART 可以实现串行通信与并行通信之间的传输转换. GPIO 为通用可编程接口，可以通过软件配置成输入或输出.

3　性能评估

本文使用 Verilog 硬件描述语言对整个处理器系统进行实现，并采用 65 nm CMOS 工艺标准单元库，使用 Design Compiler 逻辑综合工具对系统进行综合，结果如表 2 所示.

表 2　网络安全处理器综合结果

工艺/nm	面积/百万门	最高工作频率/MHz
65	4.31	285

为了评估系统的整体性能，本文在仿真环境下对系统进行了功能验证和性能评估，选择若干初始输入长度从 1 kB 到 32 kB 的数据负载，请求网络安全处理器进行密码算法及 IPSec、SSL 协议处理，测试网络安全处理单元的整体吞吐率，并与文献[2]和文献[4]中的进行对比，结果如表 3 所示.

表 3　网络安全处理器性能评估对比

协议/算法	本文	文献[2]	文献[4]
DES	2.86 Gb/s	2.133 Gb/s	1.13 Gb/s
AES	2.03 Gb/s	1.841 Gb/s	—
RSA	2 040 次/s	2 000 次/s	520 次/s
ECC	1 080 次/s	1 240 次/s	1 000 次/s
SHA1	3.254 Gb/s	2.622 Gb/s	—
IPSec	1.973 Gb/s	1.651 Gb/s	—
SSL	1.428 Gb/s	1.014 Gb/s	—

从表中可以看出，高性能的体系结构设计、基于宏流水总线的数据传输路径，以及优化的存储结构使本系统在大多实验情况下优于同类网络安全处理器.

4 结束语

本文提出了一种面向终端设备的高性能网络安全处理器体系结构，该处理器采用基于宏流水的数据传输通路，提高了总线通信速率. 基于流存储机制的层次化存储结构更加适合网络安全处理特点，大幅提高了处理单元的并行处理能力. 同时设计了安全防护电路，保证了整个系统的安全性. 通过与同类处理器相比可以看出，本文设计的网络安全处理器具有较高的性能，可以应用于各种终端设备.

参考文献：

[1] 周昔平. 多线程网络处理器分布式内核结构研究[D]. 西安：西北工业大学，2005.

[2] 王海欣，白国强，陈弘毅. 高性能网络安全处理器设计[J]. 清华大学学报：自然科学版，2010，50(1)：13-17.

[3] Wang Chenhsing，Lo Chihyen. A network security processor design based on an integrated SoC design and test platform[C]// IEEE/ACM Design Automation Conf. (DAC 06). USA，San Francisco，IEEE Press. 2006：490-495.

[4] Freescale Company. MPC 190 security processor fact sheet[EB/OL]. [2015-03-11] . http：// www. freescale. com/files/netcomm/doc/fact _sheet/ MPC 190 FACT. pdf.

[5] Allen J R，Bass R M. IBM PowerNP network processor：hardware，software，and applications[J]. IBM J. Res. &Dev.，2003，47(2/3)：177-193.

[6] Intel Company. IXP2800[EB/OL]. [2015-04-14]. http：// www. Intel. com/design/network/products/npfamily/ixp2800. htm.

[7] 袁博. 面向深度处理的网络处理器体系结构[D]. 北京：清华大学. 2013.

[8] 刘祯，刘斌，郑凯，等. 网络处理器中的高速缓冲机制及其有效性分析[J]. 清华大学学报：自然科学版，2008，48(1)：113-116.

作者简介：

朱宁龙 男，(1991-)，硕士. 研究方向为专用集成电路设计. E-mail：860554485@qq. com.

(上接第 79 页)

[3] Kubisch M，Karl H，Wolisz A，et al. Distributed algorithms for transmission power control in wireless sensor networks[C]// Wireless Communications and Networking，WCNC 2003. USA，New Orleans，IEEE，2003(1)：558-563.

[4] 吴雪，马兴凯. 连通性覆盖约束的 WSN 拓扑控制算法[J]. 微计算机信息，2009，25(13)：118-120.

[5] 张建辉，申兴发，陈积明，等. 基于 PID 算法的无线传感器网络传输功率控制研究[J]. 传感技术学报，2007，20(1)：177-182.

[6] Ibriq J，Mahgoub I. Cluster-based routing in wireless sensor networks：issues and challenges[C]// Proceedings of the 2004 symposium on performance evaluation of computer telecommunication systems. Crotia，2004：759-766.

[7] Kleinrock L，Silvester J. Optimum transmission radii for packet radio networks or why six is a magic number [C]// Proceedings of the IEEE National Telecommunications Conference. Alabama，Birmingham，1978(4)：1-4.

作者简介：

何 以 女，(1990-)，硕士研究生. 研究方向为无线传感器网络.

彭月橙 男，(1976-)，硕士，讲师. 研究方向为智能信息处理.

齐建东(通讯作者) 男，(1976-)，博士，副教授. 研究方向为物联网及无线传感器网络、智能信息处理.

E-mail：qijiandong@gmail. com.

张强宇 男，(1991-)，硕士研究生. 研究方向为无线传感器网络.