第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0197—03 文献标识码：A 中图分类号：TP316

基于 ARM 处理器的嵌入式防火墙设计与实现

陈 兵，张 峰，丁秋林
(南京航空航天大学信息科学与技术学院，南京 210016)

摘 要：基于软件实现的分布式防火墙存在“功能悖论”，基于专用网络处理器的硬件防火墙成本较高、难以普及到网络末端。该文针对以上问题，提出一种基于 ARM 处理器的嵌入式防火墙设计方案，采用核心板+扩展板的分板设计，进行 U-Boot 的定制、嵌入式操作系统的移植、网卡驱动及包过滤引擎的实现。实验结果表明，该防火墙实现成本小、处理速度快，在其硬件平台上可进行后续安全软件的开发。
关键词：网络安全；防火墙；嵌入式；分布式

Design and Realization of Embedded Firewall Based on ARM Processor

CHEN Bing, ZHANG Feng, DING Qiu-lin
(Institute of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016)

【Abstract】 It is too expensive for distributed firewall built by NP to dispose them to hosts, so this paper gives a solution of an embedded firewall based on ARM processor to solve the problems. The hardware of embedded firewall is designed into core board and expanded board. It designs U-Boot, migrates the embedded OS, and implements NIC driver and packet filter. Test results show that this firewall is powerful and its security is enhanced with a low cost.
【Key words】 network security; firewall; embedded; distributed

随着 Internet 的飞速发展和普及，人们通过 Internet 可以很方便地享受网络上丰富的信息和资源，网络的重要性和对社会的影响越来越大，而且这种趋势还在不断加快。但网络安全问题也越来越突出。防火墙就是一种防范非法访问和攻击的重要手段，它通常设置在网络边界，对进出网络的分组进行检查，可以把网络攻击阻挡在内部网络之外。但是，传统的边界防火墙过份依赖于网络拓扑结构，不能防范内部攻击，同时存在流量集中问题。分布式防火墙的出现有效地克服了传统防火墙的缺陷，但是基于软件实现的分布式防火墙存在“功能悖论”，基于专用网络处理器的硬件防火墙成本较高，难以普及到网络末端。而 ARM 处理器成本低廉、功能强大，基于此，本文提出并设计了基于 ARM 处理器的嵌入式防火墙总体框架，并对防火墙的软硬件进行模块化设计与实现。

1 嵌入式防火墙的提出

目前国内外主要提出了 2 种分布式防火墙的实现方法。

(1)基于软件的实现

文献[1]提出了一种基于 OpenBSD 操作系统内核的分布式防火墙的实现方法。通过修改操作系统的 connect(),accept()函数调用对进出的连接应用安全策略，由于操作系统具有丰富的系统调用和库函数，因此安全策略可以针对某个用户或某个应用程序来具体定义。文献[2]提出了一种基于 Agent 的分布式防火墙的实现方法。文献[3]介绍了分布式防火墙 3 种不同的实现，包括在 OpenBSD 上的实现、在 Windows NT/2000 平台上的实现以及嵌入方式的实现。随后在对分布式防火墙研究的基础上，研究者提出了基于分布的嵌入式防火墙模型。文献[4]介绍了基于分布的嵌入式防火墙的设计与实现。文献[5]阐述了基于 Linux 嵌入式系统的防火墙开发的实现方法和过程。

这些软件防火墙依赖于主机操作系统，而操作系统本身存在许多安全漏洞，所以，很难说是防火墙保护主机操作系统，还是主机操作系统保护防火墙，即这种基于软件实现的嵌入式防火墙存在“功能悖论”。一旦不怀好意的用户利用操作系统漏洞控制了主机，安装在主机操作系统上的软件防火墙就形同虚设，因此，这种软件实现的嵌入式防火墙不具备实用价值。

(2)基于硬件的实现

文献[6]实现了一种基于硬件的分布式防火墙。核心为 3Com 公司生产的 3CR990 系列网卡，该系列网卡嵌入了 3XP 处理芯片。该系统的运行与主机操作系统的关联最小，具有较高的安全性。文献[7]给出了一种基于 U 盘的嵌入式防火墙的设计方法及其实现技术。该防火墙基于 x86 硬件平台，将嵌入式系统软件全部集成在一个 U 盘中，并可以使防火墙从 U 盘中启动，具有一定的实用价值。文献[8-9]讨论了并行高速防火墙的设计。文献[10]则在网卡上综合了多种安全防范技术。

还有一些嵌入式防火墙采用传统集中式防火墙专用的网络处理器(如 IXP 系列)来实现，单件成本较高，不适合推广应用到网络末端防护。鉴于 ARM 处理器强大的功能和低廉的成本，本文提出一种基于 ARM 处理器的嵌入式防火墙硬件实现方案。这种架构对于研究新的嵌入式防火墙实现方式

基金项目：国家部委预研基金资助项目
作者简介：陈 兵(1970－)，男，副教授、博士研究生，主研方向：计算机网络，信息安全；张 峰，硕士研究生；丁秋林，教授、博士生导师
收稿日期：2008-06-01 **E-mail：**cb_china@263.net

具有较大的意义，同时具有抢占科技新制高点的重大意义。

2 嵌入式防火墙的设计

嵌入式防火墙硬件采用模块化设计，分成 5 个模块：核心模块，存储模块，以太网接口模块，JTAG 及串口调试接口模块，外围电路模块，如图 1 所示。

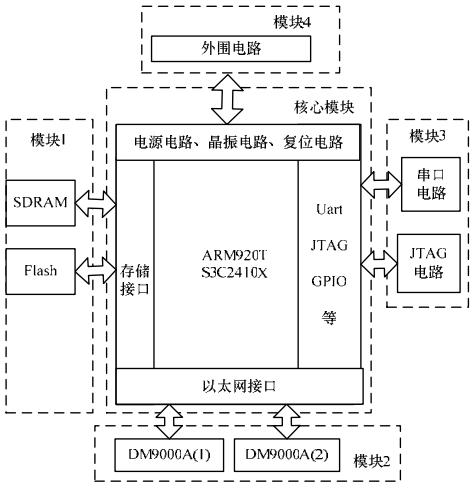

图 1　嵌入式防火墙的硬件模块

核心模块是 ARM 处理器部分。嵌入式防火墙的硬件设计采用三星公司的 32 位处理器 S3C2410X。它是以 ARM920T 为核心的嵌入式处理器，具有较高的处理速度，通过内部的锁相环，最高可在 203 MHz 的系统时钟下运行。S3C2410X 具有极低的功耗，以 1.8 V 核定电压供电，外围 I/O 口使用 3.3 V 电压，具有 3 种低功耗控制方式，甚至可以把 CPU 中除了唤醒逻辑之外的所有功能都关闭，降低了功耗。与其他 ARM 芯片相比，S3C2410X 在片上集成了更多外设接口。例如：外部存储器控制器；LCD、DMA、USB、SD、MMC 卡控制器、UART、SPI 接口；I2C 总线控制器和 IIS 总线控制器、PWM 定时器、看门狗、117 个外部 I/O 口、24 个外部中断源、ADC 和触摸屏接口、实时时钟以及片上 PLL 的时钟产生。使用集成的接口，可方便地进行功能扩展。

模块 1 是存储模块，主要包括 Flash 存储器和 SDRAM，Flash 用来存储程序，SDRAM 提供程序运行的内存空间。Flash 分为 NOR 型和 NAND 型 2 种。NOR 型 Flash 的特点是可靠性高、随机读取速度快，适用于擦除和编程操作较少而直接执行代码的场合，即应用程序可直接在 Flash 内运行，不必把代码读到系统 RAM 中。 而 NAND 型 Flash 能提供极高的单元密度，可以达到高存储密度，并且写入和擦除的速度也很快，适用于纯数据存储和文件存储，如 SM 卡、CF 卡。与 Flash 存储器相比，SDRAM 不具有掉电保持数据的特性，但其存取速度大大高于 Flash 存储器。SDRAM 在系统中主要用作程序的运行空间、数据及堆栈区。当系统启动时，CPU 首先从 Flash 中的复位地址 0x0 处读取启动代码，在完成系统的初始化后，程序代码调入 SDRAM 中运行，以提高系统的运行速度；同时，操作系统、用户堆栈及应用程序也都被加载到 SDRAM 中。NOR Flash 的型号为 E28F128J3A150，容量为 16 MB；NAND Flash 型号是 K9F1208U，容量为 64 MB；SDRAM 采用的是 K4S561632C，使用 2 片并联，容量达到 64 MB。

模块 2 是以太网接口模块，包括 2 块百兆自适应以太网控制器 DM9000A，内置 16 KB 的 SRAM，用于收发缓冲；全双工，收发同时达到 100 Mb/s。其中一块 DM9000A 接收网络上到来的数据包，交给 CPU 处理，再通过另一块发送给主机。从主机发送到外部网络的数据包处理同样如此。以太网接口模块是嵌入式防火墙设计的重点。这种外挂式的设计脱离了传统网卡使用 PCI 接口直接插入主机的模式，使用方便，完全脱离主机本身，使得网络的拓扑结构更加灵活，应用更为广泛。

模块 3 是调试电路模块，包括串口电路和 JTAG 调试电路 2 个部分。UART 串口是开发平台和用户界面之间的通道；通过 JTAG 接口可以实现系统的调试、Flash 烧写等功能。

模块 4 是外围电路模块，包括电源电路、晶振电路和复位电路 3 个部分。晶振电路提供全部的核心时钟和大多数内部设备时钟。复位电路根据 CPU 的复位信号，提供硬件平台的手动复位控制。

3 嵌入式防火墙的实现

3.1 嵌入式防火墙硬件部分的实现

ARM920T 处理器作为一个功能强大、性能优秀的嵌入式处理器芯片，为硬件布局设计带来了一定的挑战。由于三星公司的 S3C2410X 芯片是 uBGA 封装，至少需要 6 层板来布线，如果将所有芯片都集中布线在一块板上，那么布线的难度会比较大，而且给以后的调试带来不便。嵌入式处理器工作在几百兆的频率下，在高频电路板设计时，要注意电路的布局和信号线的走向，高频信号要尽量远离其他信号，尽量减小地弹、串扰等干扰以及电路中的电磁干扰和热设计等。采用核心板+扩展板的硬件布局设计策略，在核心板上实现最小系统，集成核心芯片，通过接插件将功能引入扩展板，在扩展板上实现一些基本外围设备功能，如网络通信、JTAG 调试。

整个硬件布局如图 2 所示。

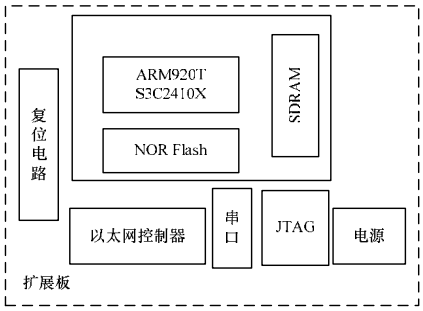

图 2　嵌入式防火墙的硬件布局

核心板上的最小系统包含了 ARM9 处理器、存储模块中的 SDRAM 和 NOR Flash、外围电路模块中的晶振电路。这里的最小系统就是在理想情况下，只要几个芯片能正常工作，就可以满足最基本的系统应用需要。在此基础上，配合相应的扩展板，进行具有针对性的某个特殊应用或一系列功能的开发。这样核心板的布线设计会相对容易，并且扩展板采用 2 层板布线设计，便于后续的升级和调试。

3.2 嵌入式防火墙软件部分的实现

嵌入式防火墙的软件总体框架如图 3 所示。其中，以嵌入式操作系统为核心，Bootloader 由 Flash 启动，负责硬件设备的初始化；网卡驱动程序实现与物理传输介质的交互，而应用程序实现嵌入式防火墙的各种功能。Bootloader、操作系统和网卡驱动是嵌入式防火墙的基础软件，在此基础上编写或移植应用程序，实现防火墙的功能。

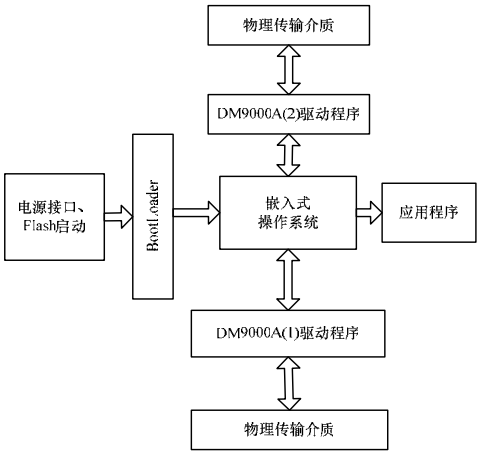

图 3　嵌入式防火墙的软件模块

根据嵌入式防火墙软件总体框架的设计，可以把软件层分为 4 个模块：Bootloader，嵌入式操作系统，网卡驱动和应用程序，它们之间是相关联的。图 4 是这 4 个模块的工作时序图：(1)Bootloader 初始化硬件设备、建立内存空间的映射图，为最终调用嵌入式操作系统内核准备正确启动的环境。(2)操作系统加载驱动程序，使防火墙能够接收和发送数据包。(3)由操作系统调用应用程序，处理接收的数据包，并返回处理结果。(4)根据应用程序的处理结果，操作系统调用驱动程序发送允许通过的数据包。因此，相应的软件开发工作包括 U-Boot 的移植、嵌入式操作系统的移植、网卡驱动以及包过滤引擎的实现。

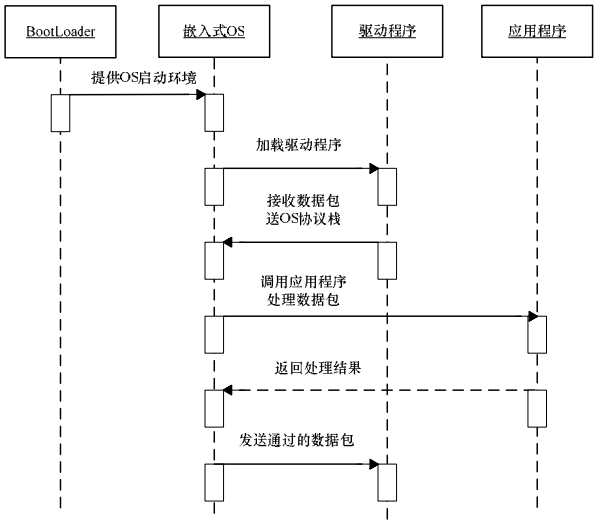

图 4　嵌入式防火墙软件模块的信息交互

4　测试

通过 Ixchariot 软件测试通信期间的速率、吞吐量。最高峰值约达到 22.3 Mb/s，最低在 16.5 Mb/s 左右。吞吐量在 19.5 Mb/s~22.5 Mb/s 之间，表明基于嵌入式防火墙的数据通信可以稳定地进行，50%稳定在 20 Mb/s。图 5 显示了一段时间内的实时吞吐量。从中可以看出，嵌入式防火墙中包过滤模块根据预先设定的访问规则，对进出防火墙的数据包进行了过滤，过滤结果与预先根据策略规则的要求所期望的结果一致。

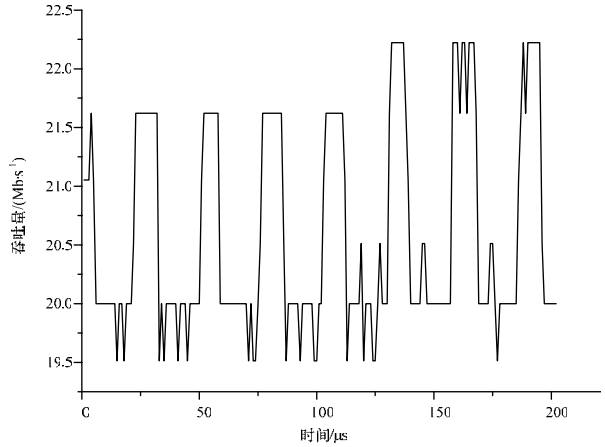

图 5　嵌入式防火墙吞吐量

5　结束语

本文主要介绍了一种基于 ARM 处理器的嵌入式防火墙的设计与实现，这种嵌入式防火墙具有自主版权，实现成本低、功能强大、对主机操作系统的依赖小、部署方便。对于开发具有我国自主版权和知识核心的信息安全产品起着探索作用。后续可在此硬件平台上构造安全应用，更大程度地提升网络末端的安全性能。

参考文献

[1] Bellovin S, Smith J, Keromytis A D, et al. Implementing a Distributed Firewall[C]//Proc. of the 7th ACM Conference on Computer and Communications Security. Athens, Greece: ACM Press, 2000.

[2] 邹学强, 冯登国. 基于 Agent 的分布式防火墙系统的设计与实现[J]. 计算机工程, 2005, 31(13): 129-131.

[3] 陈春玲, 雷世荣, 陈丹伟. 分布式防火墙的原理、实现及应用[J]. 南京邮电学院学报, 2002, 22(4): 5-10.

[4] 蔡淑珍, 陆　阳, 陈　蕾. 基于分布的嵌入式防火墙的设计与实现[J]. 计算机工程与应用, 2003, 39(11): 162-164.

[5] 韩鲁峰, 姚　远, 张其善. 一种基于 Linux 嵌入式系统的防火墙的开发[J]. 微计算机应用, 2005, 26(4): 407-410.

[6] Payne C, Markham T. Architecture and Applications for a Distributed Embedded Firewall[C]//Proceedings of the 17th Annual Conference on Computer Security Applications. [S. l.]: IEEE Press, 2001.

[7] 张锦祥. 基于 U 盘的嵌入式防火墙系统的设计与实现[J]. 武汉大学学报: 理工版, 2005, 51(3): 333-336.

[8] Fulp E W. Parallel Firewall Designs for High-speed Networks[C]// Proc. of the 25th IEEE International Conference on Computer Communications. Barcelona, Spain: [s. n.], 2006.

[9] Farley R J. Parallel Firewall Designs for High-speed Networks[D]. North Carolina, USA: Wake Forest University, 2005.

[10] 陈　昕, 刘　航, 慕德俊. 一种嵌入式安全网卡总体设计[J]. 西北工业大学学报, 2005, 23(2): 261-265.

编辑　张　帆