一种轻量级嵌入式防火墙软件架构设计

王玉东[1] 刘 坤[1] 赵 斌[1]
WANG Yudong LIU Kun ZHAO Bin

摘 要 随着嵌入式设备在物联网中的广泛应用，网络安全问题日益突出。文章结合 LwIP 协议栈的轻量特点，针对资源受限的嵌入式设备，设计了一种基于 LwIP（lightweight IP）的嵌入式防火墙软件架构。该架构可以实现低内存资源占用与轻量级数据包过滤功能。实验结果表明，在 STM32 硬件平台上，该防火墙在吞吐量损失低于 15% 的条件下，动态内存占用仅增加 5.2 kB，优于传统嵌入式防火墙方案，为资源受限的嵌入式设备提供了可行的轻量级安全解决方案。

关键词 嵌入式防火墙；LwIP；TCP/IP 协议栈；软件架构；STM32

doi：10.3969/j.issn.1672-9528.2025.11.003

0 引言

随着嵌入式设备在物联网中的部署规模不断扩大，其面临的安全威胁也日益严峻[1]。传统的防火墙解决方案通常基于高性能通用计算平台，难以适应资源受限的嵌入式场景[2]，尤其是在处理能力、内存占用和实时性等方面存在显著局限性[3]。为此，设计一种轻量级、低资源开销且适用于嵌入式系统的防火墙软件架构具有重要意义。

轻型 TCP/IP 协议栈（lightweight IP, LwIP）作为一种广泛应用于嵌入式领域的开源 TCP/IP 协议栈[4]，以其模块化设计和低资源消耗特性成为嵌入式网络通信的优选协议栈[5]。然而，LwIP 本身缺乏完善的安全机制[6]，无法有效应对网络攻击（如泛洪攻击、ARP 欺骗或非法数据包注入）[7]。针对这一问题，本文设计了一种基于 LwIP 的轻量级嵌入式防火墙软件架构。该架构通过深度整合 LwIP 协议栈的层次化数据处理机制[8]，在链路层、网络层和传输层采用多级包过滤与状态检测功能[9]，确保在有限硬件资源下提供高效的安全防护。

本文首先分析 LwIP 嵌入式防火墙的关键技术，其次详细阐述软件架构的分层防护策略、规则管理机制，最后通过实验验证在典型的嵌入式平台 STM32 上的可行性。本研究提供了资源受限场景下高扩展、低开销的网络安全防护方案，对提升物联网设备的安全性具有参考价值。

1 关键技术分析

包过滤器是防火墙的核心[10]，需要在 LwIP 的钩子挂载点上，注册并实现钩子函数来实现数据包过滤功能。

1.1 包过滤器

LwIP 协议栈中，目前仅预留了极少的钩子挂载点（如 INPUT），需要额外扩展部分钩子点：OUTPUT、PRE_ROUTING、POST_ROUTING。较为完整的包过滤器钩子挂载点和数据流如图 1 所示。

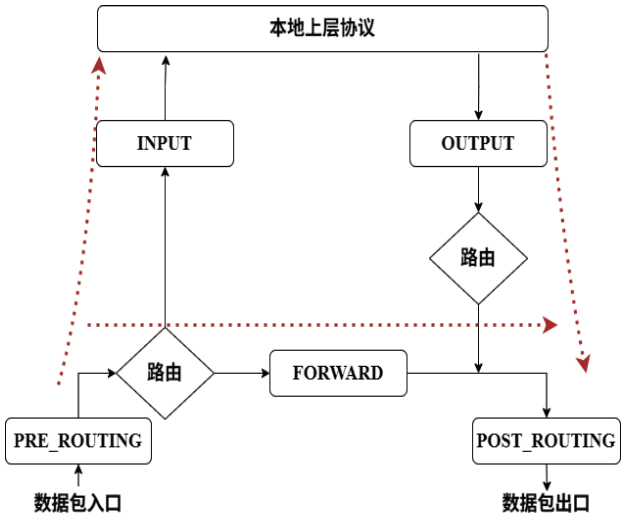

图 1 过滤器钩子位置和数据流

为了适应嵌入式场景，确保在 Cortex-M 等芯片上实现较低的报文处理延迟，数据包过滤器坚持最小化钩子点原则，其过滤流程如图 2 所示。

1.2 关键钩子

在表 1 所述的钩子挂载点上挂载钩子函数，在钩子函数逻辑里查询并匹配规则引擎中预置的访问控制列表（access control list, ACL）规则，过滤满足规则的报文，钩子函数是包过滤器的技术基础。

1. 中国航空工业集团公司西安航空计算技术研究所
陕西西安 710000

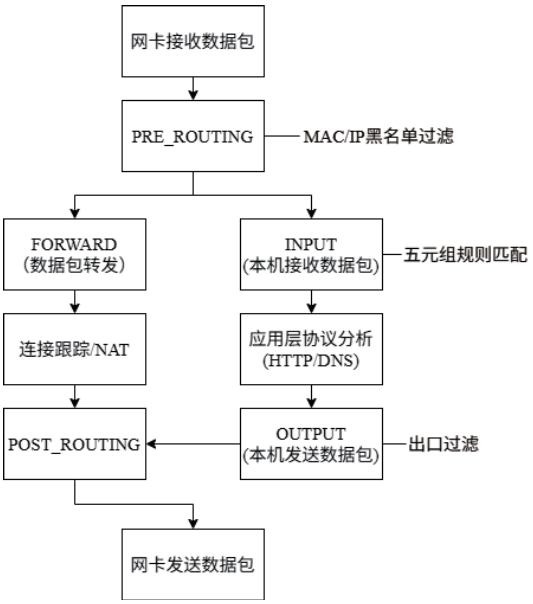

图 2 数据包过滤流程

表 1 关键钩子

钩子挂载点	触发时机	典型操作	LwIP 中位置
LWIP_HOOK_PRE_ROUTING	输入路由前，数据包刚进入网卡未经路由。	过滤 IP/ARP 和 MAC 黑名单。	ethernet_input 函数中插入钩子。
LWIP_HOOK_INPUT	本地输入，数据包目标为本机。	TCP/UDP 和 ICMP/IGMP 报文过滤；SYN Flood 检测。	在 ip_input 函数后调用过滤模块。
LWIP_HOOK_FORWARD	转发决策，数据包需转发到其他接口。需要启用 IP_FORWARD 功能。	五元组规则匹配和连接跟踪。	ip_forward 函数中挂载钩子过滤拦截。
LWIP_HOOK_OUTPUT	本地输出，本机进程发送数据包。	应用层协议限制。	ip_output 函数中注入钩子，过滤拦截。
LWIP_HOOK_POST_ROUTING	输出路由后，数据包即将发送到网卡。	NAT 转换或数据包完整性校验。	netif->output 前处理。

2 软件架构设计

LwIP 嵌入式防火墙软件架构设计原则要满足轻量化、实时性、安全性等需求，软件总体架构如图 3 所示。

软件防火墙需要强化入站防御，能对外部网络入侵进行准确有效的过滤拦截。当然对于出站防御也不容忽视。这里仅以入站防御为例（出站防御原理类似）描述端到端的关键数据流如图 4 所示。

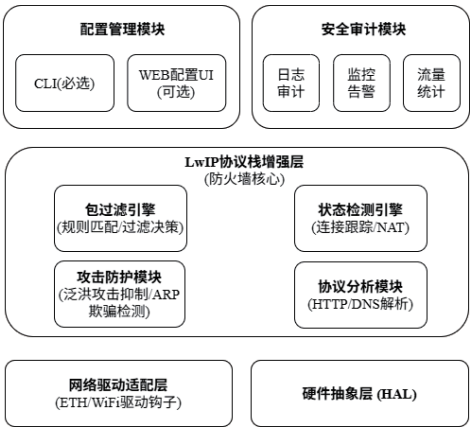

图 3 防火墙软件架构

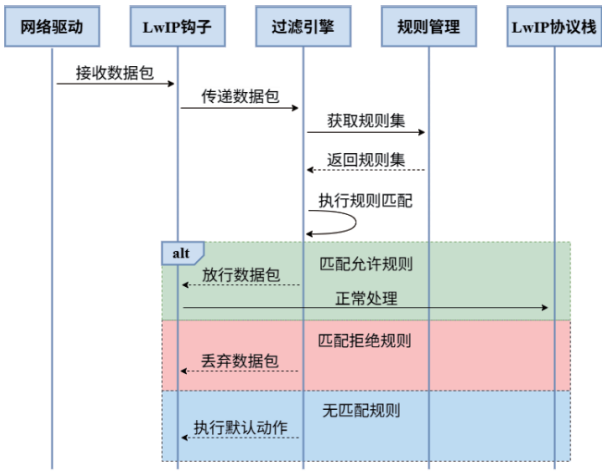

图 4 关键数据流

2.1 配置管理和安全审计

配置管理提供了 ACL 规则配置与管理功能，CLI 功能是一种常用接口。安全审计用于记录安全事件、分析异常行为并提供事后追溯能力。

2.2 包过滤引擎

（1）规则存储结构：

```
typedef struct {
uint32_t rule_id;    // 规则编号：值越小，优先级越高
    ip_addr_t src_ip;    // 源 IP 地址
    ip_addr_t src_mask; // 源 IP 掩码
    ip_addr_t dest_ip;   // 目的 IP 地址
    ip_addr_t dest_mask  // 目的 IP 掩码
    uint16_t src_port;   // 源端口
    uint16_t dest_port;  // 目的端口
    uint8_t proto;  // 协议类型：TCP/UDP/ICMP/IGMP
    uint8_t action;      // 过滤决策：允许 / 拒绝
    uint8_t direction;   // 过滤方向：入站 / 出站
    uint8_t log;         // 记录日志：记录 / 不记录
    uint32_t rate_limit;   // 速率限制
} firewall_rule_t;
```

（2）ACL 规则语法：

{10, DENY, INBOUND, TCP, ANY, 192.168.6.8/24, ANY, 8080, LOG, RATE_MAX}

{11, PERMIT, OUTBOUND, UDP, 172.20.1.9/24, ANY, 3066, ANY, LOG, RATE_MAX}

（3）规则匹配算法：小规模规则，如小于 50 条规则，可以采用线性搜索加位掩码快速比较；大规模规则，可以采用分层 Trie 树，按 IP/ 端口分段索引。

2.3 攻击防护模块

泛洪攻击抑制，如SYN Flood防御，可以采用令牌桶算法，限制每秒 SYN 包数量（如 100 个 /s）。

ARP 欺骗检测，维护合法 IP-MAC 映射表，校验 ARP 响应包。

2.4 状态检测引擎

（1）连接跟踪表设计：

```
typedef struct {
    ip_addr src_ip;    // 源 IP
    ip_addr dst_ip;    // 目的 IP
    uint16_t src_port;  // 源端口
    uint16_t dst_port;  // 目的端口
    uint8_t  state;    // 状态：SYN_SENT, ESTABLISHED
    uint32_t last_pkt_time; // 最后活跃时间戳
} conn_entry_t;
```

（2）超时机制：通过硬件定时器定期清理超时的连接，如 TCP 60 s 无活动则删除。

2.5 协议分析模块

解析协议，对协议进行合规性检查，检测出违规和异常行为对其拦截。

2.6 网络驱动适配层

（1）在该层挂载两个重要的包过滤钩子：

LWIP_HOOK_PRE_ROUTING

LWIP_HOOK_POST_ROUTING

（2）接收路径挂载点：在 ethernet_input 函数中插入 PRE_ROUTING 钩子，实现 MAC/IP 层过滤。发送路径挂载点：劫持 netif->output() 函数，实现 POST_ROUTING 钩子。

3 实验验证

通过实验对设计实现的防火墙软件进行功能、性能以及安全性测试。首先验证包过滤、状态检测、访问控制等核心功能。其次评估防火墙对嵌入式系统资源（CPU、内存）的占用及网络吞吐量的性能影响。最后模拟攻击（如 SYN Flood 泛洪攻击、ARP 欺骗）检测其防御能力。

3.1 实验环境

实验选用 STM32F407 开发板，硬件环境详情如表 2 所示。软件平台使用 FreeRTOS+LwIP 2.1.2，软件环境详情如表 3 所示。

表 2 硬件环境

硬件类型	名称 / 型号	硬件说明
主控芯片	STM32F407ZGT6	ARM Cortex-M4 内核，168 MHz 主频，192 kB SRAM，1 MB Flash；集成 10/100 MB 以太网 MAC 控制器
以太网 PHY 芯片	DP83848CVV	支持 MII/RMII 接口，自适应 10/100 Mbit/s 速率；通过 RMII 接口与 STM32F407 连接（PA1-PA7 引脚）
调试接口	ST-Link/V2	通过 SWD 协议烧录和调试；UART1（PA9/PA10，用于打印调试日志，波特率 115 200 bit/s）

表 3 软件环境

软件类型	名称 / 版本	软件说明
RTOS	FreeRTOS 10.4.3	任务调度，防火墙任务优先级设为 3
网络协议栈	LwIP 2.1.2	轻型 TCP/IP 协议栈，定制配置
驱动库	STM32 HAL 库 1.27.1	硬件抽象层驱动
构建工具	STM32CubeIDE1.11.2	集成开发环境
测试工具	IPerf、Scapy、Arpspoof	IPerf 用于吞吐量测试；Scapy 攻击模拟；Arpspoof 用于 ARP 欺骗测试
防火墙架构	基于 ACL 的包过滤器和状态检测模块	验证防火墙的包过滤、状态检测、访问控制等核心功能

3.2 实验方案

3.2.1 功能测试

（1）静态规则过滤

测试步骤：配置 ACL 拒绝所有 ICMP 包，从外部主机 ping 目标设备；配置 ACL 拒绝指定五元组的 TCP/UDP 包，从外部主机访问目标 TCP/UDP 服务端。

预期结果：ICMP 请求被丢弃，无响应；指定五元组的 TCP/UDP 数据包被丢弃，无响应。

（2）状态检测

测试步骤：内网主机发起 TCP 连接至外网，外网尝试主动反向连接。

预期结果：防火墙允许已建立的连接通信，拒绝外网主动发起的连接请求。

3.2.2 性能测试

（1）吞吐量对比

步骤：使用 IPerf 测试启用防火墙前后的 TCP/UDP 吞吐量。

指标：带宽下降比例（目标 <15%）、延迟增加量。

（2）内存占用

步骤：通过 FreeRTOS 内存管理接口统计防火墙内存占用。

指标：动态内存消耗增量（如规则表占用大小）。

3.2.3 安全性测试

（1）SYN Flood 攻击

测试步骤：通过 Scapy 模拟每秒 1 000 次 SYN 攻击。

预期结果：触发防火墙阈值后丢弃后续的 SYN 包，系统未崩溃。

（2）ARP 欺骗

测试步骤：通过 Arpspoof 伪造 MAC 地址发送 ARP 响应。

预期结果：防火墙查询合法 IP-MAC 映射表，校验 ARP 响应包，丢弃伪造的数据包。

3.3 实验结果

按照此前实验方案进行测试，实验结果如表 4 所示。

表 4 实验结果

测试维度	评估指标	关闭防火墙	开启防火墙	结论
功能性	ICMP 阻断成功率	100% 响应	0% 响应	规则生效
	TCP 五元组过滤成功率	100% 响应	0% 响应	规则生效
	UDP 五元组过滤成功率	100% 响应	0% 响应	规则生效
性能	TCP 吞吐量 /(Mbit·s^{-1})	12.4	10.8（↓13%）	满足轻型化要求
安全性	检测到 SYN Flood 时间 / ms	N/A	≤ 50	实时性达标
	检测到 ARP 欺骗时间 /ms	N/A	≤ 45	实时性达标
内存占用	动态内存增加量 /kB	0	5.2	占用量可控

3.4 实验结论

有效性：防火墙在规则匹配、状态跟踪、泛洪攻击抑制以及 ARP 欺骗防御等场景中功能均符合预期。

轻量化：资源消耗增幅 <15%，适合嵌入式场景。

局限性：复杂攻击（如 IP 分片重组攻击）需扩展规则库。

4 结语

本文针对嵌入式网络设备的安全需求，设计了一种基于 LwIP 协议栈的轻量级防火墙软件架构。通过结合 LwIP 的高效性与模块化特性，该架构在资源受限的嵌入式环境中实现了多层次的安全防护功能，其核心功能包括 ACL 规则配置管理、轻量级包过滤、状态检测、泛洪攻击抑制以及 ARP 欺骗防御等功能。

实验结果表明，该架构的设计在保证系统实时性与低内存占用的同时，能够有效抵御常见网络攻击，如泛洪攻击、ARP 欺骗和非法数据包注入。其吞吐量损失控制在 <15% 以内，满足嵌入式场景性能的基本要求，为资源受限的嵌入式设备提供了可行的轻量级安全解决方案。

参考文献：

[1]Firewalling, NAT, and packet mangling for Linux [EB/OL]. (2025-05-19)[2025-07-20]. https://www.netfilter.org.

[2]STAROLETOV S. Software architecture for an intelligent firewall based on Linux Netfilter [C]//IEEE 25th Conference on Innovation in Clouds, Internet and Networks (ICIN). Piscataway:IEEE,2022: 160-162.

[3] 丁晓东 . 基于 FPGA 和 LwIP 的网络打印安全体系结构研究与系统设计 [D]. 西安 : 西安电子科技大学 , 2013.

[4]lwIP-A lightweight TCP/IP stack [EB/OL]. (2025-02-06) [2025-05-03]. https://github.com/lwip-tcpip/lwip.

[5]DIMOLIANIS M, PAVLIDIS A, MAGLARIS V. SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering [C]// 2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN) .Piscataway:IEEE,2021: 126-133.

[6]MASUD M M, MUSTAFA U,TRABELSI Z. A data driven firewall for faster packet filtering [C/OL]//I Fourth International Conference on Communications and Networking,ComNet-2014. Piscataway:IEEE,2014[2025-10-22].https://ieeexplore.ieee.org/document/6840904. DOI: 10.1109/ComNet.2014.6840904.

[7]Windows Filtering Platform Architecture Overview [EB/OL]. (2021-12-15)[2025-09-06]. https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-filtering-platform-architecture-overview.

[8]Packet MMAP [EB/OL].(2022-04-04)[2025-10-12]. https://www.kernel.org/doc/html/latest/networking/packet_mmap.html.

[9] 江伟勇 . 基于 DPDK 的高速防火墙的设计与实现 [D]. 武汉 : 华中科技大学 ,2022.

[10] 徐明 . Linux 防火墙规则安全分析技术研究 [D]. 武汉 : 华中科技大学 ,2022.

【作者简介】

王玉东（1985—），男，辽宁宽甸人，硕士，软件研发工程师，研究方向：嵌入式软件。

刘坤（1997—），女，山东临邑人，硕士，工程师，研究方向：嵌入式软件。

赵斌（1993—），男，陕西眉县人，硕士，研究方向：嵌入式软件。

（收稿日期：2025-05-31 修回日期：2025-11-14）