计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(4):120−128 [doi: 10.15888/j.cnki.csa.009049]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于网络安全芯片的 DDoS 攻击识别 IP 核设计①

纪俊彤[1], 韩　林[1], 于　哲[2], 陈　方[2]

[1](中原工学院 前沿信息技术研究院, 郑州 450007)
[2](郑州大学 国家超级计算郑州中心, 郑州 450001)
通信作者: 韩　林, E-mail: strollerlin@163.com

摘　要: 分布式拒绝攻击 (distributed denial of service, DDoS) 作为一种传统的网络攻击方式, 依旧对网络安全存在着较大的威胁. 本文研究基于高性能网络安全芯片 SoC+IP 的构建模式, 针对网络层 DDoS 攻击, 提出了一种从硬件层面实现的 DDoS 攻击识别方法. 根据硬件协议栈设计原理, 利用逻辑电路门处理网络数据包进行拆解分析, 随后对拆解后的信息进行攻击判定, 将认定为攻击的数据包信息记录在攻击池中, 等待主机随时读取. 并通过硬件逻辑电路实现了基于该方法的 DDoS 攻击识别 IP 核 (intellectual property core), IP 核采用 AHB 总线配置寄存器的方式进行控制. 在基于 SV/UVM 的仿真验证平台进行综合和功能性测试. 实验表明, IP 核满足设计要求, 可实时进行 DDoS 攻击识别检测, 有效提高高性能网络安全芯片的安全防护功能.

关键词: 分布式拒绝攻击; 攻击识别; IP 核; 网络安全

引用格式: 纪俊彤,韩林,于哲,陈方.基于网络安全芯片的 DDoS 攻击识别 IP 核设计.计算机系统应用,2023,32(4):120–128. http://www.c-s-a.org.cn/1003-3254/9049.html

IP Core Design for DDoS Attack Identification Based on Network Security Chip

JI Jun-Tong[1], HAN Lin[1], YU Zhe[2], CHEN Fang[2]

[1](The Frontier Information Technology Research Institute, Zhongyuan University of Technology, Zhengzhou 450007, China)
[2](National Supercomputing Center in Zhengzhou, Zhengzhou University, Zhengzhou 450001, China)

Abstract: Distributed denial of service (DDoS) attack, as a traditional network attack method, still poses a great threat to network security. This study proposes a DDoS attack identification method implemented at the hardware level on the basis of the construction mode of a high-performance network security chip system on chip (SoC)+IP to handle network-layer DDoS attacks. According to the design principle for hardware protocol stacks, the logic circuit gate is used to process network packets in a manner of disassembly and analysis. Then, attack determination in the disassembled information is conducted, and the information of the packets identified as attacks is recorded into the attack pool, waiting to be read by the host at any time. Furthermore, an intellectual property (IP) core for DDoS attack identification based on the proposed method is implemented by a hardware logic circuit, and the IP core is controlled by means of advanced high-performance bus (AHB) configuration registers. Comprehensive and functional tests are performed on the system verilog/universal verification methodology (SV/UVM)-based simulation and verification platform. The experiments show that the IP core meets the design requirements and can perform DDoS attack identification and detection in real time to effectively improve the security protection function of the high-performance network security chip.

Key words: distributed denial of service (DDoS) attack; attack identification; intellectual property (IP) core; network security

① 基金项目: 国产先进计算平台创新生态及应用研究 (221100210600)
收稿时间: 2022-09-16; 修改时间: 2022-10-19, 2022-11-04; 采用时间: 2022-11-08; csa 在线出版时间: 2023-02-17
CNKI 网络首发时间: 2023-02-17

随着信息技术的不断发展与深度应用, 数字化程度的不断提升, 数字化转型已经深度渗入各行各业. 随处可见的信息基础设施和各种政务、娱乐、金融、商业等服务平台丰富了人们的生活内容. 但信息化的普及和数字化转型的深入一定程度上增加了网络安全的暴露面, 尤其是分布式拒绝服务 (distributed denial of service, DDoS) 攻击[1] 的暴露.

DDoS 攻击是攻击者控制多台计算机形成僵尸网络且统一发送远程指令来发动的恶意行为, 为的是使目标系统或服务器资源耗尽, 从而造成对正常流量的拒绝服务.

2022 年中国信息通信研究院、中国电信天翼安全科技有限公司、华为技术有限公司联合发布了《全球 DDoS 攻击现状与趋势分析报告》[2], 报告中指出 DDoS 攻击频率和强度明显提升, 以关键信息基础设施为目标的高强度 DDoS 攻击已跃升成为国家级网络安全威胁之首. 随着 5G、云计算、物联网等新兴产业的蓬勃兴起, 信息基础设施建设也随之增加, 使网络资产越来越暴露. 这些资产一旦被 DDoS 攻击者所利用, 将会对网络安全带来严重威胁. 攻击维持了向两端延展的态势, 流量带宽小于 10 Gb/s 的攻击全年占比 38.73%, 流量带宽大于 100 Gb/s 的攻击全年占比 28.37%.

DDoS 攻击作为一种传统的网络攻击方式, 经久不衰, 对网络安全依旧存在着较大的威胁. 基于 TCP/IP 网络架构的 DDoS 攻击可分为基于网络层和基于应用层两类. 基于网络层的攻击使用网络层和传输层协议进行洪泛, 即传输控制协议 (transmission control protocol, TCP)、用户数据报协议 (user datagram protocol, UDP)、互联网控制报文协议 (Internet control message protocol, ICMP) 和网际互联协议 (Internet protocol, IP)[3]. 基于应用层的攻击使用变形的可扩展的标记性语言 (extensible markup language, XML) 消息和超文本传输协议 (hyper text transfer protocol, HTTP) 洪水.

基于网络层的 DDoS 攻击会引起流量、数据包和访问源地址的数量及分布、数据包头信息等多方面上的变化, 并可导致链路拥塞和传输时延大幅增加. 现有的网络层 DDoS 攻击识别方法大都基于上述几个方面统计值的变化. 文献 [4] 提出使用 Cross-Correlation 和 Weight Vector 方法分析骨干网节点流量检测 DDoS 攻击的方法, 并将其部署在网络内, 实现基于异常的检测, 如恒速流量攻击、Pulsing 攻击或 TCP-Target 攻击. 文献 [5] 提出一种两级 DDoS 检测技术, 采用 Snmp 测量路由器接口流量, 并与历史流量数据进行对比, 及时发现流量异常变化, 通过 Netflow 信息提出被攻击地址. 文献 [6] 使用 CUSUM 方法检测攻击, 其中基于 SYN Flood 攻击的检测基于 3 次握手的完成情况. 文献 [7] 采用 Chang-Aggregation Tree 方法对流经同一个 ISP 网络中的路由器流量进行协同分析, 根据路由器每个接口的流量分布情况发现流量异常并将异常警报信号发送给 Chang-Aggregation Tree 构建服务器进行协同处理.

按照检测算法的不同, 应用层 DDoS 攻击识别主要分为基于统计学与机器学习的方法. 基于统计学的攻击识别方法, 基于统计学的算法的攻击识别, 包括利用信息熵、卡方、标准差、概率和熵测量等统计学知识, 可以准确地检测 DDoS 攻击[8]. 例如, 文献 [9] 提出了一种控制器调度算法 MutliSlot 来防御 DDoS 攻击. 该方法依赖于基于时间切片的分配策略, 旨在将流请求从各种交换机中分离出来. 文献 [10] 通过自适应相关性分析设计了一种实时强化 Anti-DDoS 行动的 DDoS 攻击防御系统. 这类方法具有较高的分析精度, 但检测成本也较高, 难以适应大规模网络入侵检测. 一些研究者将机器学习和深度学习技术广泛应用到识别 DDoS 攻击中. 文献 [11] 中提出了一个基于 PCA-SVM 的入侵检测系统, 首先, 利用主成分分析的方法对重要特征进行了提取, 然后利用支持向量机进行流量预测. 两者的结合提升了训练效率, 且取得了有效结果. 文献 [12] 采用人工神经网络 (ANN) 与模糊聚类 (FC) 相结合的方法, 实现了基于 FC-ANN 技术的入侵检测系统, 属性子集簇以 FC 为特征提取算法, 通过 ANN 训练产生. 机器学习方法在大流量处理方面相比传统方法具有一定的优势且具备较强的自学习能力, 但模型的训练开销和稳定性等问题一直是固有的制约因素.

随着大数据、物联网等新兴数字产业的发展以及攻击成本的降低, 当前网络环境下的 DDoS 攻击无论是强度还是复杂度都在明显增加. 传统的 CPU 提供的基于软件的 DDoS 攻击识别技术在成本和响应速度等方面都面临严峻考验. 硬件实现的 DDoS 攻击识别技术逐渐发展起来. 文献 [13] 实现了一种基于 FPGA 的网络安全防护平台, 在此平台基础上展开 DDoS 攻击的研究, 基于 CAM 的数据包过滤引擎和半双工调度机制的设计方法, 实现对数据包的处理. 文献 [14] 基于

FPGA 实时检测防御系统的体系结构, 实现基于非参数累计和算法检测新 IP 地址到达速率变化的 DDoS 攻击识别方法, 实现保护本网络不受攻击影响, 且不损失网络信息吞吐量的效果. 文献 [15] 利用 TOE 和 TSO 等技术的思想, 提出了一种创新的 DDoS 防御技术实现方案, 使用多核网络处理器对报文进行处理, 并将此方案部署在网卡的系统架构中不受上层软件的影响.

高性能网络安全芯片是针对信息安全和自主可控最基础、最核心的网络信息安全需求, 设计开发的一款高性能、高集成度、高兼容性、高安全性的新一代国产自主可控网络主动防御 SoC 系列芯片. 本文提出一种硬件实现的网络层 DDoS 攻击识别方法, 首先按照硬件协议栈设计原理利用逻辑门电路对网络数据包进行拆解分析, 随后依据解析后的包头信息对网络流量进行攻击判定, 将认定为攻击的数据包信息记录在攻击池中, 等待主机随时读取. 基于该方法设计了部署在高性能网络芯片的 DDoS 攻击识别 IP 核, 旨在为高性能网络芯片提供 DDoS 攻击识别功能. IP 核考虑到工程项目的应用环境, 使用 AHB 总线配置寄存器的方式进行控制, 作用于数据通路. 在基于 SV/UVM 的仿真平台对 IP 核进行功能验证. 实验结果显示, 对于不同类型的攻击流量, 攻击识别模块在接收到使能信号后, 各子模块根据实时数据的解析进行攻击识别, 并成功将识别结果写入 LUT 以及攻击池 RAM 中. IP 核可达到预期效果.

本文主要贡献如下.

1) 分析当前的网络安全形势与安全防护手段, 对现有 DDoS 攻击的发展现状与趋势进行研究 , 提出一种部署在高性能网络安全 system-on-chip (SoC) 芯片上检测网络层 DDoS 攻击的方法. 该方法根据硬件协议栈设计原理, 利用逻辑电路门处理网络数据包, 可在芯片内部检测网络层 DDoS 攻击, 更好地提升防御系统的“硬防”.

2) 本文提出一种应用于高性能网络安全芯片实现 DDoS 攻击识别的 IP 核设计, 基于高级处理器总线架构 (advanced microcontroller bus architecture, AMBA) 的研究基础, 采用 AHB 总线配置寄存器的方式进行控制, 通过硬件逻辑电路为网络主动防御 SoC 芯片提供 DDoS 攻击识别的 IP 核. 该 IP 核考虑到工程项目的应用环境, 并基于 SV/UVM 的仿真平台验证 IP 核的性能与实际应用的可行性.

1 准备工作

1.1 网络层 DDoS 攻击

DDoS 攻击可操作性强、攻击门槛低、给网络服务商带来客户流失、商业损失等重大风险[16]. 基于网络层的攻击是针对协议发送大量恶意的数据包, 消耗目标服务器的可用带宽和连接, 导致目标网络的不可到达.

网络层基本攻击根据 TCP 协议、UDP 协议或 ICMP 协议包进行洪泛或是放大攻击, 向被攻击设备发送大量的请求使网络过载, 例 SYN flood、UDP flood、UDP DNS query flood、ICMP flood、Smurf 攻击. 表 1 是根据协议划分的网络层 DDoS 攻击.

表 1 协议划分网络层 DDoS 攻击

协议类型	攻击类型
TCP协议	SYN flood
UDP协议	UDP flood UDP DNS query flood
ICMP协议	ICMP flood Ping of death Smurf

1.2 SoC+IP 模式

IP 核是经过设计并通过实际验证的具有特定功能以及性能优化的电路功能模块, 并且是 SoC 的核心技术之一[17]. 针对专用集成电路 (application specific integrated circuit, ASIC) 开发时间慢、上市时间长等问题, SoC+IP 提供了一种灵活而快速的模式以解决不足.

根据 AMBA 片上总线标准, 高性能网络安全芯片 SoC 架构以高级高性能总线 (advanced high-performance bus, AHB) 为主干, 连接 CPU、SPIFlash 控制器、系统内存、系统控制等高效率模块. 高级外围总线 (advanced peripheral bus, APB) 是 AHB 的二级扩展总线, 主要是为 AHB 总线和低带宽的外围设备之间提供通信桥梁. 其高性能网络安全芯片 SoC 架构如图 1 所示.

2 IP 核模块设计

本文设计的 IP 核经 AHB 总线配置, 作用于数据通路, 攻击模块根据解析后的包头信息进行攻击识别过滤, 将认定为攻击的数据包按一定格式输出给 LUT 维护模块和攻击 RAM 写入模块, 同时将每次攻击的信

息记录在攻击池中, 等待主机随时读取. IP 核内部模块架构如图 2 所示.

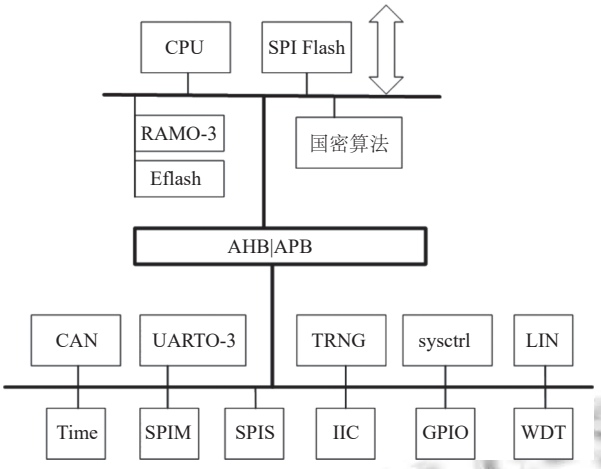

图 1 高性能网络安全芯片 SoC 架构

1) AHB 配置模块, 负责完成对 IP 核中各模块正常工作所需的配置. 实现通过 AHB 总线对 IP 核中各模块使用的寄存器或 RAM 进行配置, 如芯片使能、攻击池相关的寄存器以及攻击模块使能等.

2) 接收模块, 将由 MAC 输入的 8 bit 包数据转换为 128 bit 包数据, 写 RAM 模块根据 LUT 维护模块中对应的固定地址空间将 128 bit 数据写入 RAM 中.

3) 解析模块, 对接收模块传输的数据包进行拆分解析的工作, 根据网络流的特征以及传输位宽提取数据包中相应的关键字段.

4) LUT 维护模块, 从攻击模块、解析模块中获取数据包的攻击使能信号、攻击结果等链表所需的信息写入链表中, 并更新数据 RAM 的包头起始地址.

5) 攻击识别模块, 是 DDoS 攻击识别 IP 核的主要模块, 对网络数据包进行安全检测, 防止带有恶意攻击的数据包对系统造成进一步危害.

6) 攻击 RAM 写入模块, 将每次攻击的信息按照一定格式写入攻击池 RAM 中对应的固定地址空间.

7) 攻击池, 存放攻击模块认定攻击的 IP 包包头内容, CPU 需要先读取攻击池中的计数器获得攻击者和被攻击者的 IP、MAC 的个数信息, 再从池中读取相应个数的具体信息. CPU 也可对计数器进行清零操作, 使攻击池重新生成.

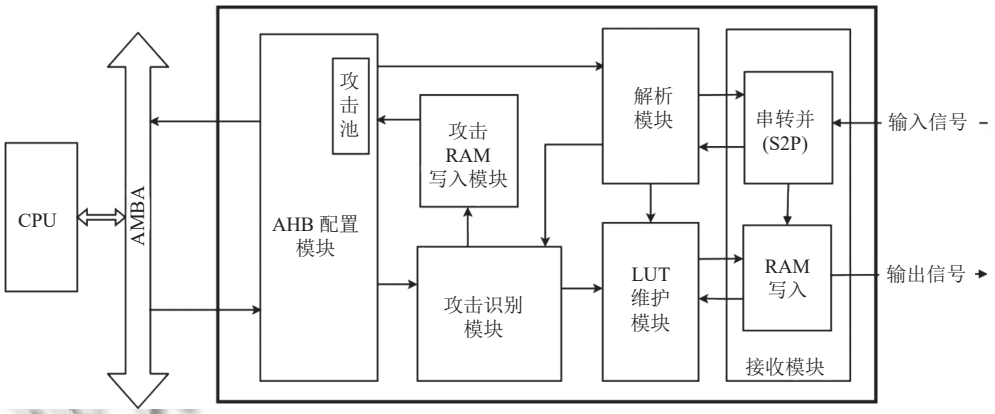

图 2 IP 核模块架构

下文围绕本 IP 设计的核心解析模块和攻击模块展开介绍.

2.1 解析模块

解析模块主要完成对接收模块传输的数据包进行拆分解析工作, 从接收模块中依次提取包头部分的相应信息, 如 MAC 地址、数据包类型、IP 地址、协议类型、端口等信息.

解析数据流采用“状态机+计数器”方式对接收模块传送的数据进行拆分解析, 状态转换图如图 3 所示.

解析模块接收到 AHB 配置模块的使能信号后, 对接收模块信号进行解析工作, 根据总线时钟频率、数据传输位宽计算得出关键字段信息在数据流中的位置, 即状态跳转时触发相应的计数器累加, 结合计数器数值和关键信息字节长度记录到对应的寄存器中. 其中传送给解析模块的数据位宽为 8 bit, 解析模块处理逻辑如图 4 所示.

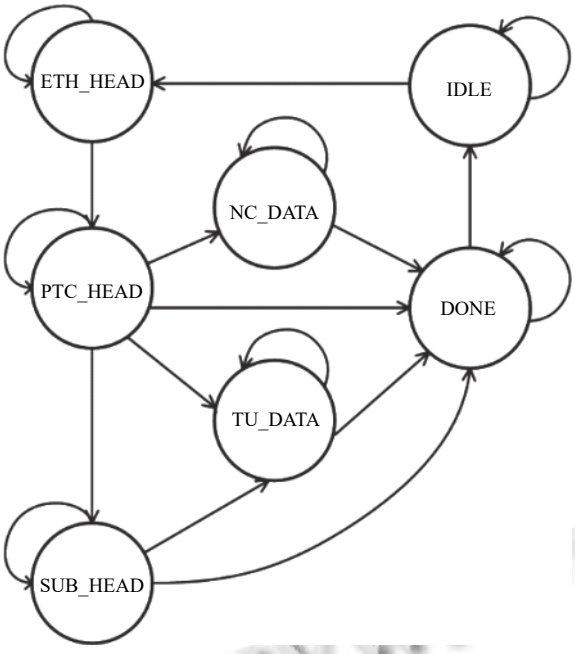

图 3 解析模块状态转换图

2.2 攻击识别模块

DDoS 攻击识别 IP 核的主要模块为攻击识别模块, 网络数据流写入系统内存前进行接收控制, 对网络数据包进行安全检测, 防止带有恶意攻击的数据包对系统造成进一步危害.

攻击识别模块从解析模块获得所需要的数据包信息, 由 AHB 配置模块开启攻击识别总使能信号. 实现方式运用模块化设计, 采用自顶向下的设计原则. 顶层模块负责与解析模块中的输出信号连接, 每个攻击子模块例化 、参数例化传递、端口例化对应等都由顶层模块实现. 各子模块根据输入信号以及阈值判定是否符合攻击定义.

判定为攻击的 IP 数据包:

(1) 输出此数据包的攻击识别结束使能信号、攻击结果信号给 LUT 维护模块.

(2) 包头信息、攻击信息存到 RAM 中, 构建为攻击池, 使用标识寄存器记录攻击池中存放的数量. 当其累加到设定的阈值后, 标识寄存器将保持不变, 攻击池继续从头覆盖更新. CPU 根据标识寄存器对攻击池进行相应数量的读取用于生成网管包上报, 然后将标识寄存器清零. 攻击识别流程如图 5 所示.

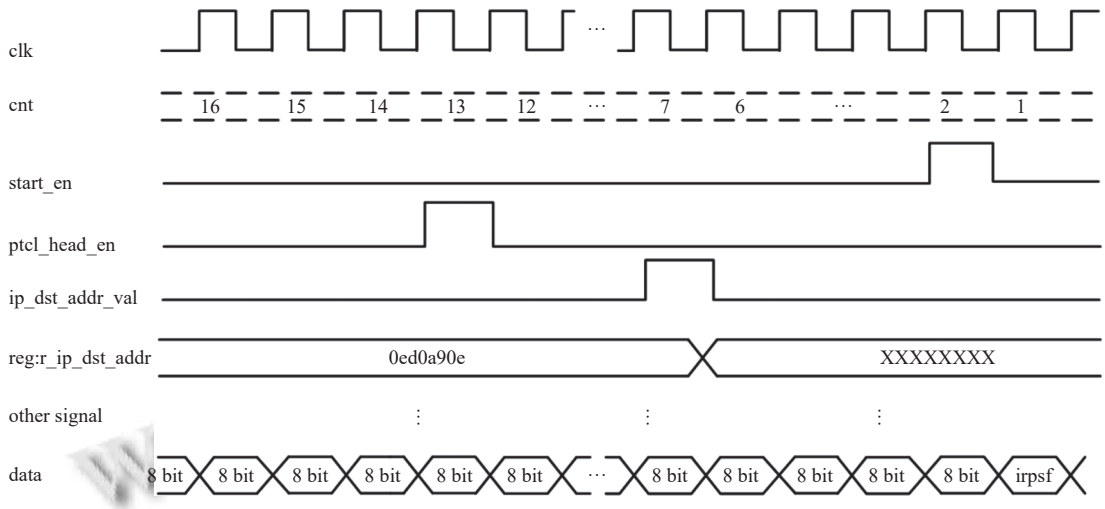

图 4 解析模块处理逻辑图

2.2.1 模块设计结构

整体的攻击识别模块设计后, 在顶层模块中, 根据攻击方式的不同划分为多个子模块, 便于实现. 由 SYN flood 模块、UDP flood 模块、UDP DNS query flood 模块、ICMP flood 模块、Ping of death 模块、Smurf 模块构成.

顶层模块的输入信号需求来自解析模块输入信号、AHB 配置信号. 子模块分使能信号由顶层模块中输出控制, 根据从解析模块中获取协议信号, 通过协议分类模块按照表 1 中协议划分 DDoS 攻击启用对应攻击的子模块使能信号. 攻击识别顶层模块结构图如图 6 所示. 表 2 为解析模块中数据包输入信号描述.

控制寄存器针对不同类型的 DDoS 攻击设置了相应的控制使能信号和攻击内的阈值数值信号, 实现

了对每种攻击的针对性防御. 如表 3 所示, DDoS_en 信号为攻击识别总使能启动信号, 1–6 位分别为 SYN flood、UDP flood、UDP DNS query flood、ICMP flood、Ping of death、Smurf 攻击子模块的使能启动信号. icmp_flood_vld、dns_query_flood_val、udp_flood_vld、syn_flood_val 分别为对应子攻击内阈值.

攻击识别总使能信号优先级最高, 其他子模块分使能信号需要结合攻击识别总使能才会有效. 其中攻击识别总使能、子模块分使能、子模块阈值由 AHB 配置模块启用. 图 7 是攻击识别模块的寄存器描述.

攻击识别的顶层模块根据不同协议的数据包开启不同的攻击识别子模块, 将模块内控制寄存器和数据包的关键字段的相关信号与对应攻击子模块进行连接, 识别结果传输给下一阶段使用.

2.2.2 攻击池

攻击池存放攻击识别模块标记为攻击包的数据包包头信息, 其中每个包头信息中包含源 MAC 地址、目的 IP 地址、源 IP 地址, 以及对应的攻击类型. 不同的包头信息之间的源 MAC 地址或源 IP 地址不同.

经攻击识别模块判定为攻击的数据包, 通过图 2 中的 RAM 写入模块写入到攻击池中, CPU 可读取攻击池中的信息. 标识寄存器记录写入攻击池数据包的个数, CPU 可根据标识寄存器从攻击池中读取相应数量的包头信息并生成网管包上报.

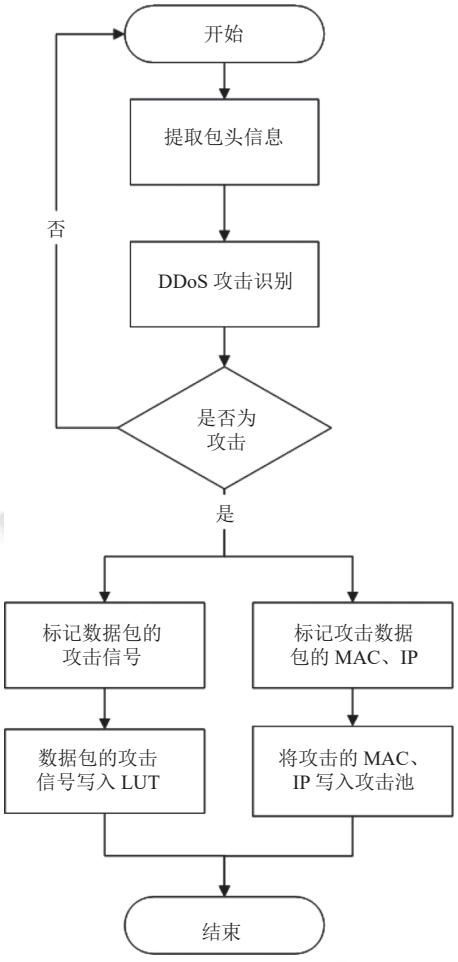

图 5 攻击识别流程图

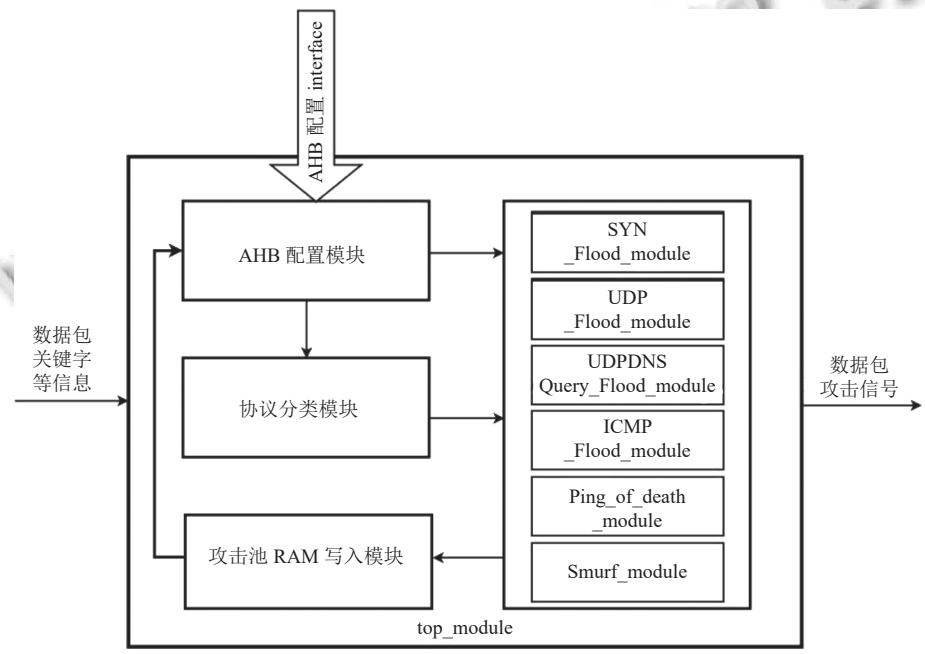

图 6 攻击识别顶层模块结构图

表 2 数据包输入信号

Name	Width	Description
irpsf	1	数据包帧开始信号
i8Protocol	8	数据包协议类型
i32Src_ip	32	数据包源IP地址
i32Dst_ip	32	数据包目的IP地址
i16R_total_length	16	IP数据包长度
i16R_ip_offset	16	IP数据包标识号
i8R_tcp_ctrl	8	TCP数据包控制位
i16Rport_dst	16	报文目的端口号
i16Rudp_length	16	UDP数据包长度
i8R_icmp_type	8	ICMP数据包类型

使用标识寄存器记录攻击池中存放的数量. 攻击识别模块将数据包通过 RAM 写入模块到攻击池的过程中, 标识寄存器开始累加, 当其累加到设定的阈值之后, 标识寄存器将保持不变, 攻击池继续从头覆盖更新. 当 CPU 读取完攻击池中信息后, 将标识寄存器其清零, 此时攻击池中写入地址也相应归零, 重新记录. 攻击池设计如图 8 所示.

攻击池 RAM 由深度为 16 bit, 宽度为 128 bit 单口 Dpram 和 AHB 接口以及 RAM 接口的选通器构成. 标识寄存器 (DDoS_Cnt Register) 的位宽为 4 bit, 初始值为零. 当接收到数据包写入使能时, 自动加一; 当累加到阈值后, 保持直到 CPU 清零.

3 设计验证与分析

本文采用硬件描述语言 Verilog HDL 对所设计的 DDoS 攻击识别 IP 核进行建模, 并基于 SystemVerilog/验证方法学 (universal verification methodology, UVM) 的仿真平台进行综合和功能评估. 通过 SystemVerilog 类库的形式提供实验环境和测试用例的可重用机制[18]. 以 Verdi 为软件仿真环境追踪 RTL 代码、生成并查看 fsdb 波形文件以便完成 IP 核的测试验证.

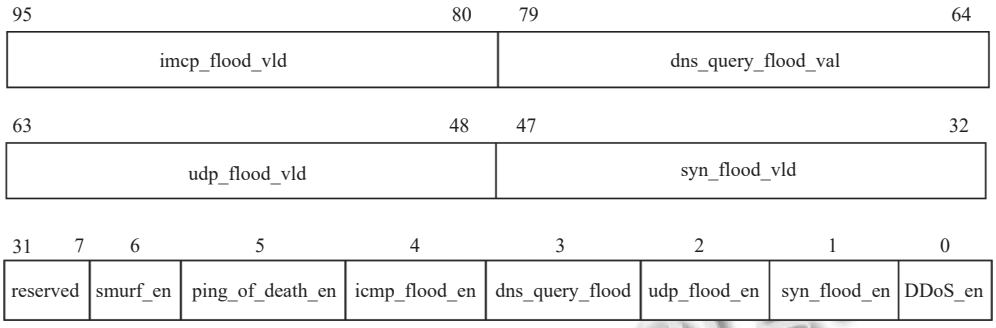

图 7 攻击识别模块的寄存器描述

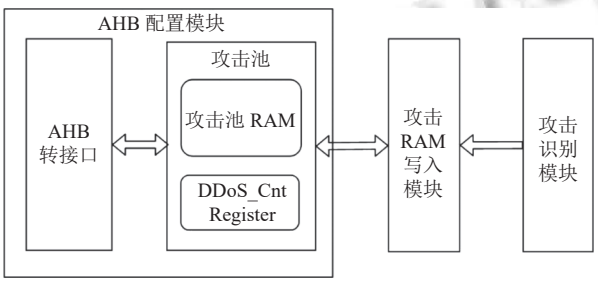

图 8 攻击池

3.1 数据通路测试

数据通路测试包括复位、时序、接收数据包字段的完整性等测试. 通过 SystemVerilog 定义编写激励源文件, 定义 TCPFrmItem 类、UDPFrmItem 类 、ICMPFrmItem 类分别为 TCP 数据包、UDP 数据包、ICMP 数据包的激励源.

通过带有数据的激励文件向被测模块发送正常流量大小的 IP 数据包, 其中包括 TCP、UDP、ICMP 协议数据包.

攻击识别顶层模块的仿真波形如图 9 所示, 解析模块成功接收到数据信息进行拆分解析工作并发送给攻击识别模块, 输入信号包括各关键字段, 以及字段的有效使能信号. 数据通路测试通过.

3.2 功能测试

本文对表 3 中测试用例进行了开发. 在数据通路测试的基础上, 表 3 中的测试用例针对每种不同特征的 DDoS 攻击设置了不同的攻击流量.

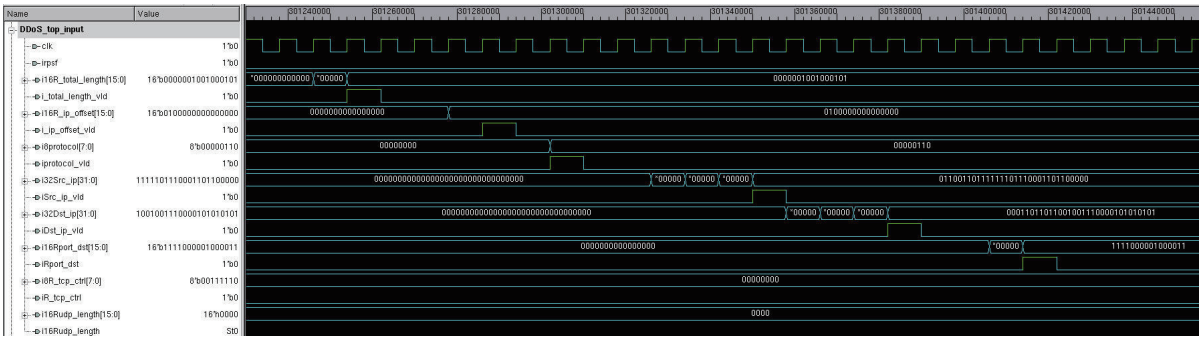

图 9 攻击识别顶层模块输入信号仿真波形图 (部分)

表 3 功能测试用例

测试用例名称	测试用例描述
DDoS_tcp_tb	发送带有SYN flood攻击的TCP数据包测试
DDoS_udp_1_tb	发送带有UDP flood攻击的UDP数据包测试
DDoS_udp_2_tb	发送带有UDP DNS query flood攻击的UDP数据包测试
DDoS_icmp_1_tb	发送带有ICMP flood攻击的ICMP数据包测试
DDoS_icmp_2_tb	发送带有Ping of death攻击的ICMP数据包测试
DDoS_icmp_3_tb	发送带有Smurf攻击的ICMP数据包测试

在对表 3 中测试用例完成开发后, 进行功能仿真, 攻击识别模块的输出仿真波形如图 10 所示. 针对验证平台发送不同的攻击流量, 攻击识别模块在接收到使能信号后, 开启攻击识别工作. 各攻击子模块根据实时数据的解析进行攻击检测, 识别结果由 ddos_result 信号输入, 并按图 4 流程写入 LUT 以及攻击池 RAM 中.

图 11 为识别到 SYN Flood 攻击的仿真结果. 由 ddos_result 信号可知, AHB 配置模块成功开启攻击识别模块, 对实时数据的解析结果判定该数据包存在 SYN Flood 攻击.

综合数据通路测试和功能测试的测试结果分析, 得出 DDoS 攻击识别 IP 核可达到预期效果, 有效防范网络攻击.

图 10 攻击识别顶层模块输出信号仿真波形图

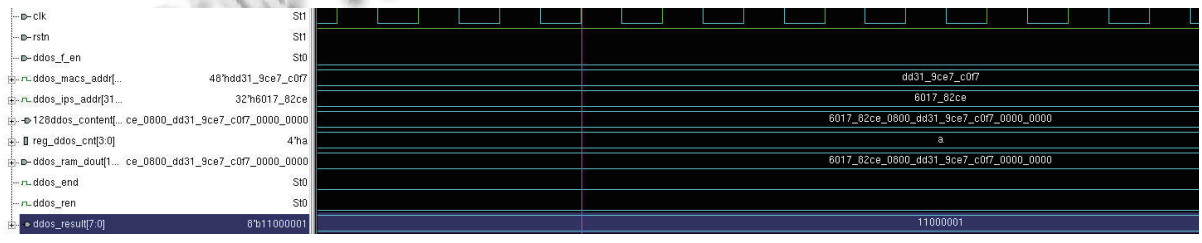

图 11 攻击识别顶层模块输出信号仿真波形图 (部分)

4 结束语

本文通过对 DDoS 攻击的发展现状与趋势进行研究 , 提出一种部署在高性能网络安全 SoC 芯片上检测 DDoS 攻击的方法, 该方法可以在硬件层面检测网络层 DDoS 攻击. 并结合高性能网络安全芯片, 完成了一种 DDoS 攻击识别 IP 核的可编程逻辑电路, 该 IP 核基

于 SV/UVM 的仿真平台进行综合和功能性测试, 为网络主动防御 SoC 芯片提供 DDoS 攻击识别功能. 实验表明, 本文提出的基于硬件层面检测网络层 DDoS 攻击的方法可以有效进行实时的 DDoS 攻击识别检测.

参考文献

1 王磊, 李刚, 王斐玉. 改进属性加密结合代理重加密的云计算安全访问控制策略. 计算机应用与软件, 2019, 36(7): 327–333. [doi: 10.3969/j.issn.1000-386x.2019.07.056]

2 中国信息通信研究院, 中国电信天翼安全科技有限公司, 华为科技有限公司. 2021 年全球 DDoS 攻击现状与趋势分析报告. https://e.huawei.com/cn/material/networking/security/333e0bdd9694437e80aac4b436781fe3. (2022-05-10).

3 王飞雪, 戴蓉. 基于投票 ELM 和黑洞优化的云计算 DDoS 攻击检测. 西南大学学报 (自然科学版), 2022, 44(8): 205–215. [doi: 10.13718/j.cnki.xdzk.2022.08.022]

4 Chen Y, Hwang K. Collaborative change detection of DDoS attacks on community and ISP networks. Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS'06). Las Vegas: IEEE, 2006. 401–410.

5 Yuan J, Mills K. Monitoring the macroscopic effect of DDoS flooding attacks. IEEE Transactions on Dependable and Secure Computing, 2005, 2(4): 324–335. [doi: 10.1109/TDSC.2005.50]

6 Sekar V, Duffield NG, Spatscheck O, *et al*. LADS: Large-scale automated DDoS detection system. Proceedings of the Annual Conference on USENIX'06 Annual Technical Conference. Boston: USENIX Association, 2006. 171–184.

7 Chen W, Yeung DY. Defending against TCP SYN flooding attacks under different types of IP spoofing. International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06). Morne: IEEE, 2006. 38.

8 陈润泽. 软件定义网络环境下 DDoS 攻击研究 [硕士学位论文]. 贵阳: 贵州师范大学, 2022. [doi: 10.27048/d.cnki.ggzsu.2022.000817]

9 Yan Q, Gong Q, Yu FR. Effective software-defined networking controller scheduling method to mitigate DDoS attacks. Electronics Letters, 2017, 53(7): 469–471. [doi: 10.1049/el.2016.2234]

10 Zheng J, Li Q, Gu GF, *et al*. Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1838–1853. [doi: 10.1109/TIFS.2018.2805600]

11 Li YH, Xia JB, Zhang SL, *et al*. An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Systems with Applications, 2012, 39(1): 424–430. [doi: 10.1016/j.eswa.2011.07.032]

12 Wang G, Hao JX, MA J, *et al*. A new approach to intrusion detection using artificial neural networks and fuzzy clustering. Expert Systems with Applications, 2010, 37(9): 6225–6232. [doi: 10.1016/j.eswa.2010.02.102]

13 芦世雄. 基于 FPGA 的抗网络攻击关键技术研究 [硕士学位论文]. 天津: 天津大学, 2014.

14 赵桦, 罗晓富, 程军, 等. DDoS 攻击实时检测防御系统的硬件实现. 微计算机信息, 2005, 21(7–3): 75–76, 98. [doi: 10.3969/j.issn.1008-0570.2005.21.030]

15 汤浩然. 基于网络处理器的嵌入式 DDoS 防御系统设计与实现 [硕士学位论文]. 广州: 暨南大学, 2017.

16 绿盟科技, 中国电信云堤. 2020DDoS 攻击态势报告. https://www.nsfocus.com.cn/html/2021/92_0121/148.html. (2021-01-21).

17 袁文澹. 基于 IP 核的片上结构 MORSE 码处理系统设计与实现研究 [硕士学位论文]. 长沙: 湖南大学, 2005.

18 杜越, 郑杰良, 吴益然. 基于 UVM 的 SoC 系统级外设验证平台设计. 中国集成电路, 2022, 31(6): 37–43. [doi: 10.3969/j.issn.1681-5289.2022.06.006]

(校对责编: 牛欣悦)