基于入侵检测的并行网络安全系统的设计与实现

摘　要

本文通过研究入侵检测技术及模式匹配算法，提出一种分级嵌套精确串匹配算法，并结合此算法实现一种树状结构的网络安全体系架构以及单节点网络安全系统。具体研究如下：

(1)入侵检测系统架构研究。对 IDS 的相关技术进行深入研究，提出一种高效的分布式并行 IDS 系统架构及安全策略，并给出了单一结点网络安全系统的设计思路。

(2) 子网结点网络安全系统的研究与实现。研究并实现流过滤系统、并行入侵检测系统以及数据统计系统。其中双链层分级嵌套算法用于流过滤系统中过滤器的设计，并行双链层分级嵌套算法用于 DIDS 中数据分析器的设计。

(3) 分别对由 KMP、BM 以及改进算法实现的数据分析器进行实验验证，证明以改进算法的高效可行性。

关 键 词: 入侵检测；模式匹配；MPI；流过滤；DIDS

论文类型：应用研究

目 录