高速网络流量下实时入侵检测系统研究与应用*

宗学军[1,2]，刘欢欢[1,2]，何　戡[1,2]，连　莲[1,2]
（1. 沈阳化工大学　信息工程学院，辽宁　沈阳　110142；
2. 辽宁省石油化工行业信息安全重点实验室，辽宁　沈阳　110142）

摘　要：针对现有实时入侵检测系统（Intrusion Detection System，IDS）面对超千兆每秒高速工业网络流量时实时检测性能与准确率不足，在传统 Suricata IDS 的基础上，引入数据平面开发套件（Data Plane Development Kit，DPDK）技术提升系统数据包捕获处理能力，降低系统消耗。同时在规则匹配时采用高效规则匹配算法 NEW_ WM（NEW－Wu－Manber）提升系统实时检测的效率与检测准确率。系统测试与油气集输攻防演练平台上的应用结果证明，系统面对高速网络流量时在降低系统消耗的同时，提升了系统的实时检测效率与检测准确率。

关键词：DPDK；Suricata；NEW_ WM；实时入侵检测系统；油气集输攻防演练平台
中图分类号：TP309　　**文献标识码**：A　　**DOI**：10. 19358/j. issn. 2097－1788. 2023. 04. 010
引用格式：宗学军，刘欢欢，何戡，等. 高速网络流量下实时入侵检测系统研究与应用［J］. 网络安全与数据治理，2023，42(4)：56－61，84.

Research and application of real-time intrusion detection system under high-speed network traffic

Zong Xuejun[1,2], Liu Huanhuan[1,2], He Kan[1,2], Lian Lian[1,2]
(1. School of Information Engineering, Shenyang University of Chemical Technology, Shenyang 110142, China;
2. Liaoning Provincial Key Laboratory of Information Security in Petrochemical Industry, Shenyang 110142, China)

Abstract: To tackle the shortages of real-time detection performance and accuracy of existing intrusion detection systems when confronted with high-speed industrial network traffic exceeding one gigabit per second, this study proposed the integration of DPDK technology into the conventional Suricata IDS. This integration aims to enhance the system's packet capture processing capabilities and reduce its resource consumption. Furthermore, to improve the efficiency and accuracy of real-time detection it incorporated the NEW_ WM algorithm, an efficient rule matching algorithm, for rule matching. The effectiveness of the proposed system was evaluated using the oil and gas gathering and transportation attack and defense drill platform. The system test and application results revealed that the proposed system reduces resource consumption and improves real-time detection efficiency and accuracy when dealing with high-speed network traffic.

Key words: DPDK; Suricata; NEW_ WM; real time intrusion detection system; oil and gas gathering and transportation attack and defense drill platform

0　引言

受日益增长的数据传输需求的驱动，企业和研究机构正在部署 100 Gb/s 的工业网络，这种高速网络的普及，为工业安全防护带来了重大的技术挑战。如何在高速网络流量下保证工业互联网安全是亟须解决的问题[1]。传统 Suricata IDS 在面对高速网络流量时，无法高效及时地处理网络活动，由于数据处理不及时，造成数据包丢失，降低系统检测的准确率，威胁工业系统安全[2]。

文献［3］研究了两种流行的开源 IDS：Snort 和 Suricata，在相同条件下平衡二者间的比较性能基准，证实了限制 IDS 在高速网络适用性的关键因素为系统资源使用、包处理速度、包丢弃率和检测精度。文献［4］利用单个

*基金项目：辽宁省兴辽英才计划（XLYC2002085）；中央引导地方科技发展基金项目（辽科发规［20. 23］7 号－36）

DPDK 工作线程，通过使用 CPU 亲和力，分配专用 lcore，从而加速 Suricata 工作线程的 IDS 处理。使用了两个专用于 Suricata DPDK 的 0 和 1 端口对系统进行测试，证实了 DPDK 能够提高 Suricata IDS 的工作性能。文献［5］在传统 Snort IDS 的基础上，引入 DPDK 对系统进行优化，验证了基于 DPDK 的入侵检测系统在面对传输速率为 10 Gb/s的网络流量时，系统对报文的检测性能远远优于传统 Snort 入侵检测系统。文献［6］分析了 Snort 的架构，提出在高速网络流量下降低系统误报率的关键是提高 Snort 的数据包捕获能力和检测引擎模块的性能。设计并实现了基于 DPDK 的 Snort DAQ 模块，并搭载高性能正则引擎 Hyperscan，提高 Snort 的抓包模块的性能，优化检测引擎模块。优化后的 Snort 在高速网络流量下的抓包能力和恶意流量检测率都有了很大的提升。

综上所述，解决传统 Suricata IDS 在高速工业网络流量下实时检测性能与检测准确率不足，降低系统消耗的关键在于提升系统的数据包捕获与规则匹配的性能。针对这一问题，本文应用 DPDK[7] 的大页内存、CPU 亲和性、无锁环形队列与 UIO 轮询模式等技术，将传统 Suricata IDS 的数据包采集处理流程进行分解并与 DPDK 进行重组，对传统 Suricata IDS 的数据包捕获模块进行优化，提升系统的数据包实时捕获能力。同时为解决传统 Suricata IDS 在面对高速网络流量时规则匹配效率与准确率低、误报率高的问题，应用现有的高速规则匹配算法 NEW_ WM 算法[8]，优化其数据包检测与日志模块，在不提升系统消耗的同时增加系统实时规则匹配效率与准确率，降低系统的误报率。

1　系统构造及优化方案

入侵检测系统是一种积极主动的用于网络设备安全防护的系统。系统能够实时监视网络数据的传输，在发现网络安全威胁后发出告警并采取积极的应对措施以保护系统的安全[9]。图 1 所示为入侵检测系统网络拓扑图。

Suricata 是一个基于 C 语言开发的，免费、开源、成熟、快速、健壮的网络威胁检测引擎。Sunicata 能够完成入侵检测、入侵防御以及离线数据包处理，它利用远程开发的运行集来进行嗅探，监控网络中的异常行为，并做出相应的反应。Suricata IDS 整体分为四大模块：数据包捕获模块、数据包解码模块（数据包处理模块）、数据包检测与日志模块和数据包输出模块，Suricata 提供友好的插件式的开发接口，通过这些开发接口，能够将 DPDK 以及 NEW_ WM 算法完美地融入到 Suricata IDS 中。同时 Suricata 拥有强大且广泛的规则库和签名语言用来对网络流量进行检测，兼容 Snort 的规则库并提供强大的 Lua 脚本支持来检测复杂的威胁[10]。Suricata 架构[11] 如图 2 所示。

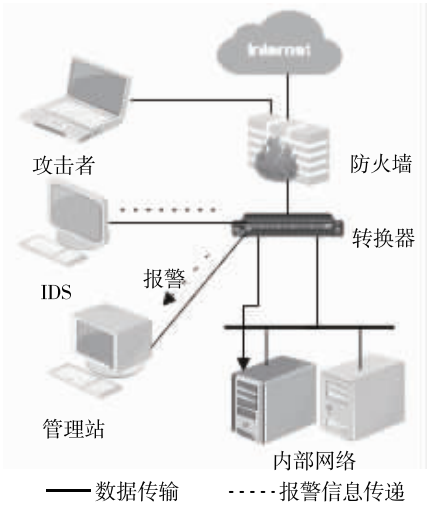

图 1　IDS 网络拓扑图

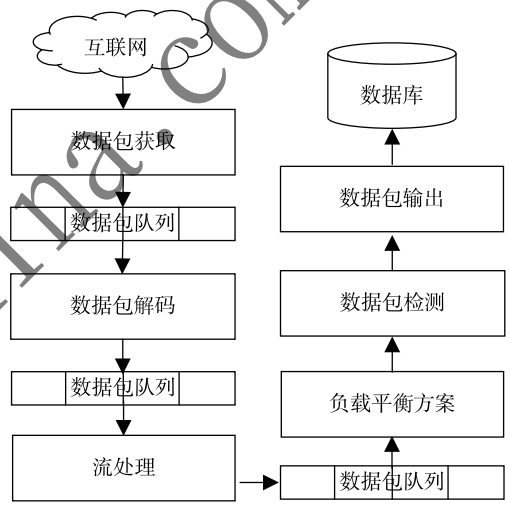

图 2　Suricata 架构

Suricata IDS 的数据包捕获模块有三种不同的工作模式：single 模式、worker 模式和 autofp 模式。系统运行在 Suricata 的 worker 模式下。worker 模式通过将数据包进行一连串的连续操作后，完成数据包的处理并做出相应的反馈，大致流程如图 3 所示。

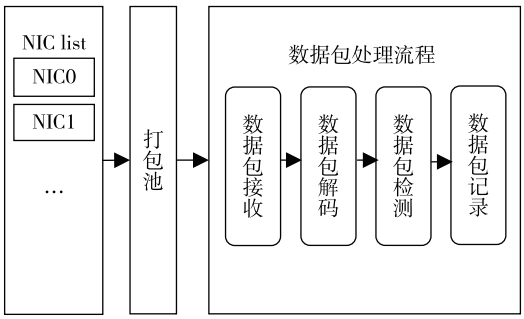

图 3　Suricata worker 模式工作流程

1.1 系统优化方案

随着高速网络的快速发展和网络攻击的日益复杂，需要高性能的 IDS 工具来快速处理报文，重构流，并应用模式匹配进行基于特征的威胁检测。如何快速有效实时地在高速网络流量下进行系统入侵行为检测，是当下工业安全防护研究的重点。影响 Suricata IDS 检测效率的因素有很多，本文针对主要的两点：数据包的接收处理速率、模式匹配引擎的效率。

DPDK 是一套由 Linux 基金会管理的开源软件项目数据平面库，如图 4 所示，DPDK 具有轮询模式驱动程序的网络接口控制器，其函数库与驱动集合能够对数据包快速地进行处理，将数据包处理从操作系统内核卸载到用户空间，这种卸载实现了更高的效率和包吞吐量[12]。DPDK 绕过了 Linux 内核，运行在操作系统的用户态上，节省了 CPU 中断时间，同时利用自身提供的数据平面库对接收到的数据包进行处理，提高了报文处理效率[13]。

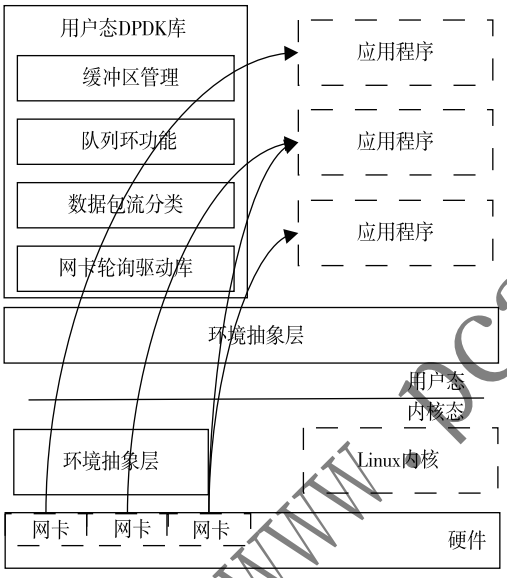

图 4 DPDK 架构

NEW_ WM 是一种基于 WM 改进的算法，解决了传统 WM 多模匹配算法在进行规则匹配时，每次参与匹配的模式串数量大、字符比较次数多、失配时文本串匹配窗口向右移动距离过小的问题。该算法采用后缀表与前缀表相结合的方式对地址进行二次过滤，前缀表采用平衡二叉树[14]存储，减少了每次匹配时的模式串数量。

为了减少每次匹配时的比较次数，NEW_ WM 采用字频匹配的方式快速找到失配的字符，在失配时匹配窗口采用 BMH 和 BMHS 算法的跳跃距离的较大者右移。

NEW_ WM 在 WM 算法原有的 Suffix 后缀表的基础上引入基于平衡二叉树的前缀表。假设字符串为

T = "knowledge is better than money to the human"

模式串为

P = {blank, fund, minded, hand, than, plan, thread, this, that, think, there, these}

基于平衡二叉树构造的前缀表如图 5 所示。

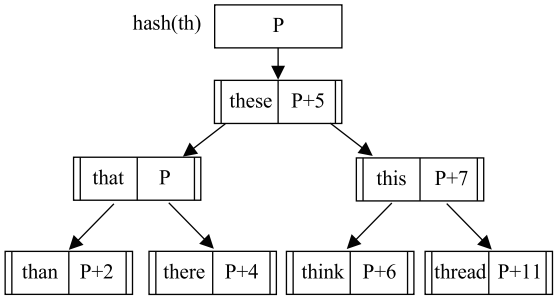

图 5 基于平衡二叉树的前缀表

采用字频匹配的方法，要计算出每个模式串中最低频率字符的位置，用该位置上的字符与文本串匹配窗口中对应的字符进行比较，有效减少了每轮匹配字符需要比较的次数。

由于 WM 算法本身会生成一个存放着基于 BMH 字符块的跳跃数组 Shift，NEW_ WM 算法基于 BMHS 算法建立另外一个跳跃表 Skip，用来存放文本串匹配窗口最后 $B-1$ 个字符（B 为字符块的长度）与匹配窗口下一个字符组成的字符块 B 的右移距离，每次失配时采用上述跳跃数组的较大者，以此来增大文本串匹配窗口向右移动距离。

NEW_ WM 算法能够很好地应用于 Suricata IDS 上，在匹配速度以及匹配准确性上相较于传统的模式匹配算法有了很大的提升。

Suricata IDS 通过撰写规则的方式对流经的数据包进行检测。选取 DPDK 这一强大的数据包捕获处理套件，可提升系统数据的实时采集处理能力。同时为了在提高系统实时性与检测效率的同时不提升系统的硬件需求，对比现有的模式匹配算法，采用检测精度更高、速度更快的 NEW_ WM 模式匹配算法，增强系统对流经流量的实时采集处理能力。改进后的系统框架如图 6 所示。

1.2 系统测试

在同一硬件环境下，对基于不同包捕获与检测机制的 Suricata IDS 进行对比测试研究，测试不同入侵检测系统的数据包捕获速率、误报率以及搭建系统的服务器系统消耗情况。评判标准为：

（1）丢包率：在相同网络流量下，数据包捕获模块对发送出的数据包的捕获能力，即发送的数据包数量与接收到的数据包数量的差与发送数据包数量的比值。这

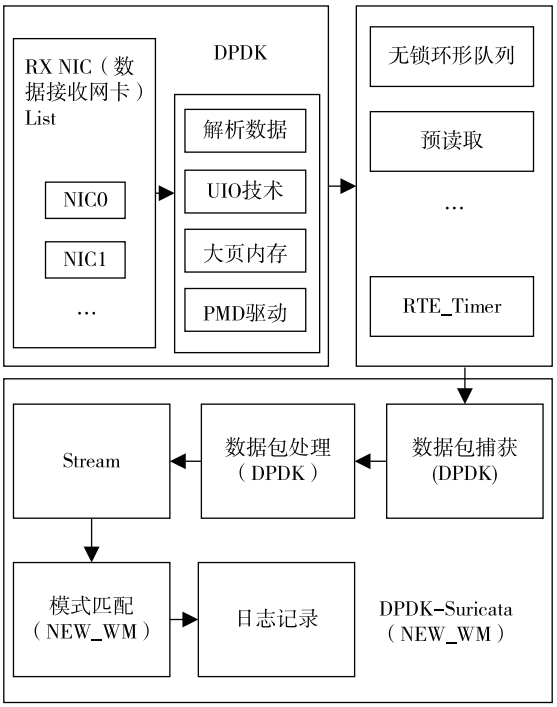

图6　优化后的系统构架

个值越小则表示系统的数据包捕获性能越强，系统面对高速网络流量时的实时性越好。

（2）准确率：在相同网络条件下，采用同样的攻击手段，系统所检测到的攻击数量与系统内攻击总数的比值。这个值越大，表示系统检测准确率越高，系统入侵检测性能越好。

（3）误报率：把正常应用判定为恶意应用的个数占所有正常应用个数的比值。这个值越低，表示系统的检测能力越精确，入侵检测性能越好。

（4）系统消耗：当系统进行数据包捕获时，系统的CPU使用以及内存使用率。该值越低则代表系统消耗越小，对系统的配置要求越低。

系统的测试环境如表1所示。

表1　系统测试环境

role	sender	receiver
model	Dell PowerEdge R750	Dell PowerEdge R750
CPU	Intel（R）Xeon（R）CPU E5－2667 v3 @ 3.20 GHz	Intel（R）Xeon（R）CPU E5－2667 v3 @ 3.20 GHz
NIC	Inter X540T2	Inter X540T2
memory	128 GB	128 GB

测试1：在相同的硬件配置、不同的包捕获机制下，使用iPerf3生成并发送一个180 s的UDP流。使用prometheus中的node_ exports来监视CPU和内存利用率，同时使用tcpdump来监视包丢弃率。报文发送速率从10 Gb/s逐步递增到100 Gb/s，测试系统的报文捕获能力以及系统消耗，结果如图7和表2所示。

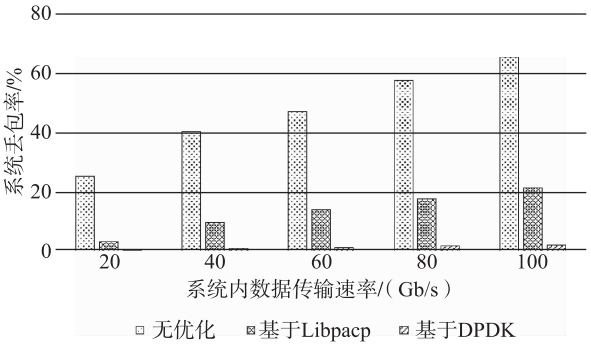

图7　不同数据包捕获机制的系统丢包率

表2　不同数据包捕获机制的系统消耗（%）

	数据传输速率/(Gb/s)	20	40	60	80	100
CPU使用率	传统IDS	45.50	56.80	70.20	83.90	98.50
	Libpacp	30.80	38.60	45.80	58.70	70.40
	DPDK	15.00	19.20	22.60	24.80	26.50
内存消耗	传统IDS	1.80	3.50	6.10	8.10	11.50
	Libpacp	1.30	2.80	4.20	7.40	10.80
	DPDK	0.60	1.30	1.90	3.08	4.50

由测试结果得出，在面对高速流量时，相较于传统的Suricata IDS，基于Libpacp与基于DPDK的Suricata IDS在系统丢包率以及CPU使用率上大幅度降低。在以DPDK作为Suricata IDS的数据包捕获机制时，优势尤为明显，丢包率、CPU以及内存利用率都为三者最优。该结果证实了以DPDK替换传统Suricata IDS的数据包捕获模块在面对高速网络流量时的优越性能。

测试2：在相同的硬件配置以及默认规则下，发送端使用iPerf3发送数据，发送速率从10 Gb/s逐渐提升到100 Gb/s。并行使用Pytbull，启动其7个测试用例生成攻击数据包。测试在相同的基于DPDK的包捕获机制下，传统的检测机制、Hyperscan与NEW_ WM规则匹配算法的入侵检测系统，在面对高速网络流量时系统的检测准确率以及系统的CPU使用率。测试结果如图8、图9所示。

由图8、图9可以得出，更改数据包检测机制后Suricata IDS攻击检测准确率明显优于更改前。采用NEW_ WM算法改进的Suricata IDS在攻击检测准确率方面略优于采用Hyperscan改进的Suricata IDS，但对比二者的CPU使用率，基于NEW_ WM算法改进的Suricata IDS明显更有

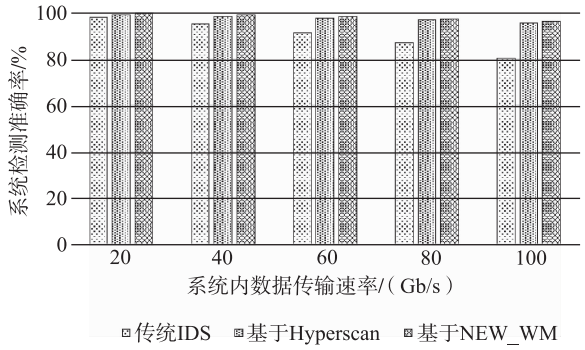

图8　优化前后的系统检测准确率

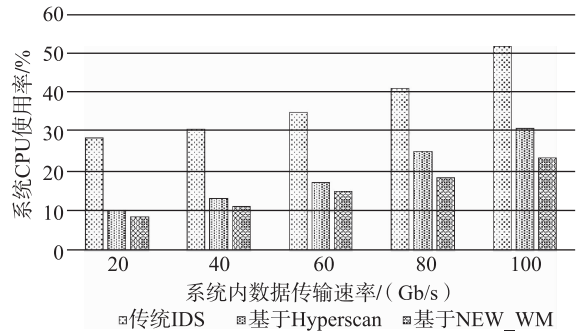

图9　优化前后的系统 CPU 使用率

优势，在提高系统检测准确率的同时，减少了系统开销。

测试3：使用目前在入侵检测系统研究测试领域受到共同认可且最为全面的攻击测试数据集——DARPA 1999 数据集。其中包含了常见的五大类攻击方式，描述如表3所示。DARPA 1999 数据集给出了三周的数据，其中只有第二周的数据中带有攻击实例。选取 DARPA 1999 数据集第二周星期一的 outside 数据集，采用 Trex 并以 100 Gb/s 的传输速率对数据集进行实时回放。测试结果如表4所示。

表3　攻击方式描述

攻击名称	攻击描述
Denial of Service（DoS）	拒绝服务攻击。消耗网络资源，使计算机或网络无法提供正常服务
User to Root（U2R）	提权攻击。低权限用户通过绕过一些验证，通过一些系统网站的漏洞直接获取 root 权限
Data Compromise（Data）	在没有授权的情况下，强行访问或修改本地主机或远程主机上的数据
Surveillance or Probe（Probe）	在没有得到授权的情况下，对网络进行嗅探，查找网络漏洞，研究网络配置及网络拓扑
Remote to Local（R2L）	远程用户攻击。远程主机在没有得到授权的情况下，远程获取本地主机上的用户权限

表4　不同系统的准确率和 CPU 使用率（%）

系统	准确率	CPU 使用率
传统的 Suricata IDS	60. 52	90. 78
引入 DPDK 的 Suricata IDS	83. 56	35. 63
基于 DPDK，Hyperscan 的 Suricata IDS	93. 53	29. 33
基于 DPDK，NEW_ WM 的 Suricata IDS	96. 13	25. 67

由表4可以看出，高性能数据包捕获框架 DPDK 以及 NEW_ WM 模式匹配算法对 Suricata IDS 在性能上都有所提升。系统在面对 100 Gb/s 的高速网络流量时，相较于传统的 Suricata IDS 在检测准确率上提升了 35. 61%，同时在 CPU 使用率上降低了 65. 11%。相较于基于 DPDK 的 Suricata IDS 提高了 12. 48% 的检测准确率，降低了 9. 96% 的 CPU 使用率。相较于基于 DPDK，Hyperscan 的 Suricata IDS 提升了 2. 6% 的检测准确率，降低了 3. 66% 的 CPU 使用率。由此得出，本文搭建的系统在面对 100 Gb/s的高速网络流量时，相较于其他系统拥有较低系统开销的同时拥有很好的入侵检测性能。

综上所述，选取 DPDK、NEW_ WM 对 Suricata IDS 的数据包捕获模块以及数据包检测与日志模块进行改进之后的入侵检测系统，在高速网络流量下节省系统开销的同时，提升了系统的数据包捕获能力与系统检测准确率。系统在高速网络流量下展现出了较为优秀的入侵检测性能。

2　系统实际应用

油气集输攻防演练平台是辽宁省石油化工行业信息安全重点实验室的一套工业网络攻防演练平台。该平台包含西门子、罗克韦尔等主流 PLC 设备，将一整套油气集输的工业环境进行仿真，能够模拟现实工业环境上的数据以及参数变化，平台能够进行工业审计，具备工业威胁探测器以及工业防火墙，能够完成多种针对工业环境的攻防演练操作。

将本文所搭建的基于 Suricata 的实时入侵检测系统部署在实验室油气集输攻防演练平台上，网络拓扑图如图10所示。

由于油气集输攻防演练平台内的正常数据流量较小，无法满足测试需要，选取 NLS－KDD 数据集中的 KDDTest＋子集对系统进行测试，为了使发送端所发送的流量更加接近真实场景，采集平台内的正常流量，同时在数据发送端启用 Pytbull 的所有攻击测试用例增加系统攻击的丰富性。使用 Trex 对数据流量进行实时加速回放，使得系统内的流量由 10 Gb/s 逐步递增到 100 Gb/s，测试所搭建的系统在真实场景下，面对带有攻击的高速网络流量时

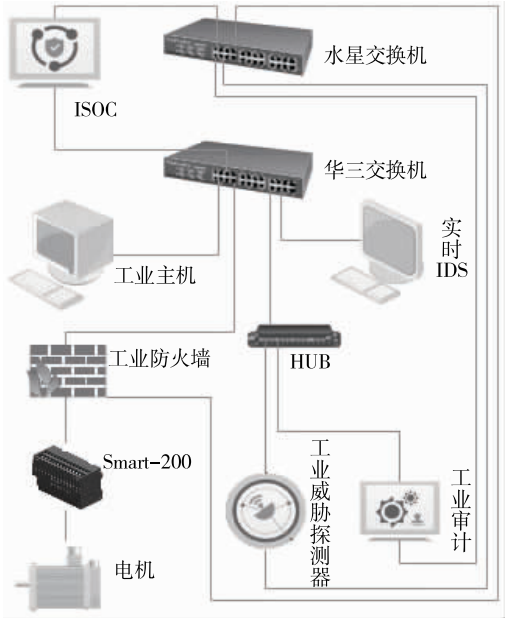

图 10　优化后的系统网络拓扑图

系统检测准确率与系统 CPU 消耗，结果如表 5 所示。

在真实高速网络流量的环境下，系统检测准确率始终保持在 96% 以上，系统漏报率保持在 1.3% 以下，CPU 使用占比在 27% 以下，证实了基于 DKDK 与 NEW_ WM 改进后的 Suricata IDS 在真实工业现场的网络场景中能够很好地对系统入侵行为进行实时检测，在不增加系统消耗的同时，实时地保护高速网络流量下系统的安全。

表 5　系统的检测准确率、漏报率与 CPU 使用率（%）

流量流速/（Gb/s）	系统准确率	系统漏报率	CPU 使用率
10	99.85	0.13	5.61
20	99.54	0.15	8.82
30	99.13	0.28	10.24
40	98.52	0.42	13.57
50	98.21	0.59	16.65
60	97.98	0.71	17.98
70	97.42	0.86	20.14
80	96.85	0.98	23.67
90	96.55	1.13	24.88
100	96.14	1.25	26.96

3　结论

本文通过对当下工业控制网络的安全防护策略进行分析，针对传统防护手段在面对高速网络流量时丢包率高、检测准确率低等问题，通过对传统 Suricata IDS 进行改进，搭建出一个面对高速工业网络流量下基于 Suricata 的实时入侵检测系统。主要工作如下：

（1）本文提出使用 DPDK 高性能数据包捕获套件替换传统 Suricata IDS 数据包捕获模块，解决了传统 Suricata IDS 在面对高速网络流量时性能的不足与丢包问题。利用 DPDK 提供的无锁环形队列、CPU 亲和性等技术，提升系统在面对高速网络流量时的数据采集与处理能力，降低对系统的消耗。

（2）本文提出采用一种基于 WM 算法改进的 NEW_ WM 算法替换传统 Suricata IDS 的数据包检测模块。对比 Suricata IDS 的 AC、BM 算法与高速正则匹配算法 Hyperscan、NEW_ WM 四种模式匹配算法，选择更高效、匹配速度更快、系统消耗较低的 NEW_ WM 算法，可降低系统的漏报率，提升系统检测准确率与模式匹配效率。

整个系统充分考虑了当下国内工业控制系统计算机配置与工业互联网发展情况，提出 DPDK 与 NEW_ WM 算法结合的方式，在降低系统消耗与漏报率的同时，提升了系统在高速网络流量下的数据包实时捕获、处理与检测速率，增强了系统对流经数据检测的准确率以及系统实时入侵检测性能，同时系统具有很好的实际应用性能。

参考文献

[1] 杨鸿深. 工业互联网安全建设的探讨 [J]. 网络安全技术与应用，2021(11)：114－115.

[2] 严益鑫，邹春明. 工业控制系统 IDS 技术研究综述 [J]. 网络空间安全，2019，10(2)：62－69.

[3] HU Q，YU S Y，ASGHAR M R. Analysing performance issues of open-source intrusion detection systems in high-speed networks [J]. Journal of Information Security and Applications，2020 (51)：102426.

[4] PAVITHRA V. Accretion of suricta with DPDK for traffic monitoring using optimized detection system IDS/IPS [J]. International Journal of Engineering Research & Technology (IJERT)，2021，10(7)：52－56.

[5] ZHANG D，WANG S. Optimization of traditional Snort intrusion detection system [C] //IOP Conference Series：Materials Science and Engineering，2019，569(4)：042041.

[6] SHUAI L，LI S. Performance optimization of Snort based on DPDK and Hyperscan [J]. Procedia Computer Science，2021 (183)：837－843.

[7] 郭世现. 基于 DPDK 的实时流量分析系统 [D]. 大连：大连理工大学，2021.

[8] 周延森，张维刚. 一种 WM 多模匹配算法的研究与改进 [J]. 计算机应用与软件，2021，38(7)：251－257，309.

（下转第 84 页）

的自然资源要素综合观测平台构建［J］. 资源科学，2020，42（10）：1965－1974.
［14］夏红军，安燕娜. 数据中台视角下供电企业数据资产管理模型构建［J］. 情报科学，2021，39（10）：70－75.
［15］施俊君. 基于智能运维的城市轨道交通轨道专业数据中台［J］. 城市轨道交通研究，2021，24（S1）：105－107，112.
［16］杨进. 基于数据中台和 GIS 的可视化固定资产管理模式探析［J］. 财务与会计，2021（3）：70－72.
［17］张雯，周子航，周明升. 基于物联网和人工智能的园区安全运营管理平台［J］. 计算机时代，2023（2）：132－136.
［18］雷鸣，姜罕盛，武国良，等. 基于 HBase 的大数据架构下负载平衡技术［J］. 计算机与现代化，2021（6）：91－95.
［19］周明升，韩冬梅. 上海自贸区金融开放创新对上海的经济效应评价——基于“反事实”方法的研究［J］. 华东经济管理，2018，32（8）：13－18.
［20］韩冬梅，周明升. 上海自贸区金融开放创新的宏观效应模拟［J］. 统计与决策，2019，35（9）：155－159.
［21］周明升，韩冬梅. 基于 Rossle 混沌平均互信息特征挖掘的网络攻击检测算法［J］. 微型机与应用，2016，35（14）：1－4.

（收稿日期：2023－01－05）

作者简介：

张雯（1983－），女，硕士，经济师，主要研究方向：大数据分析和预测。

周明升（1981－），男，博士，高级工程师，主要研究方向：智慧城市、决策支持。

（上接第 61 页）

［9］陈晓安. 计算机网络入侵检测系统的研究［J］. 电子测试，2021(18)：76－77，73.
［10］NAM K，KIM K. A study on SDN security enhancement using open source IDS/IPS Suricata［C］//2018 International Conference on Information and Communication Technology Convergence（ICTC）；2018：1124－1126.
［11］WONG K，DILLBAUGH C，SEDDIGH N，et al. Enhancing Suricata in－trusion detection system for cyber security in SCADA networks［C］//2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering（CCECE）. IEEE，2017：1－5.
［12］REN H，NIAN M. Dpdk-based high-speed packet acquisition method［J］. Computer System Applications，2018，27(6)：242－245.
［13］凌质亿. 面向高速网络环境的实时入侵检测系统的研究与实现［D］. 南京：东南大学，2016.
［14］李毅飞，杨进. 一种基于平衡二叉树的 CDP 数据备份及重构方法［J］. 数据通信，2019(2)：13－17.

（收稿日期：2023－03－07）

作者简介：

宗学军（1970－），男，硕士，教授，主要研究方向：工业过程控制、工业信息安全等。

刘欢欢（1997－），通信作者，男，硕士研究生，主要研究方向：工业信息安全。E-mail：1965991358@ qq. com。

何戡（1978－），男，硕士，副教授，主要研究方向：工业过程控制、机器学习等。

（上接第 77 页）

［11］张晓凤，侯艳，李康. 基于 AUC 统计量的随机森林变量重要性评分的研究［J］. 中国卫生统计，2016，33(3)：537－540，542.
［12］Xiang Xinrong，Jin Baisuo，Wu Yuehua. Change-point detection in a high-dimensional multinomial sequence based on mutual information［J］. Entropy，2023，25(2).
［13］李悦，唐振浩，曹生现，等. 基于动态时延分析和典型样本筛选的 NO*x* 排放浓度预测［J/OL］. 中国电机工程学报：1－10［2023－02－06］. https：//doi. org/10. 13334/j. 0258－8013. pcsee. 213189.
［14］HOCHREITER S，SCHMIDHUBER J. Long short-term memory[J]. Neural Computation，1997（9）：1735－1780.
［15］吕鑫，慕晓冬，张钧，等. 混沌麻雀搜索优化算法［J］. 北京航空航天大学学报，2021，47(8)：1712－1720.
［16］毛清华，张强，毛承成，等. 混合正弦余弦算法和 Lévy 飞行的麻雀算法［J］. 山西大学学报（自然科学版），2021，44(6)：1086－1091.

（收稿日期：2023－02－23）

作者简介：

王渊博（1993－），男，硕士研究生，主要研究方向：先进控制策略在大型火电机组的应用。

金秀章（1969－），男，副教授，主要研究方向：先进控制策略在大型火电机组的应用和信息融合技术等。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部