文章编号:1671-4598(2021)08-0062-05 DOI:10.16526/j.cnki.11—4762/tp.2021.08.013 中图分类号:TP393.08 文献标识码:A

基于负载预测的通信网络入侵检测系统设计

谢 凯,代 康
(新疆工程学院 信息工程学院,乌鲁木齐 830023)

摘要:针对传统通信网络入侵检测系统负载不均而导致检测精准度低的问题,提出了基于负载预测的通信网络入侵检测系统设计;设计系统硬件结构,使用T—KOKO型监听器及带有监听面板AP—9812M的语音信息监听工具,使用HDMI分配器传输监听信号,选择JY211—QTQ—04型号光缆探测器,其内部含有发射机和接收机,用于发射和接收数据,采用TCP继电器控制器用于改变指令正常执行的顺序;确定负载指标,动态调整负载预测策略,保证负载均衡,并通过hash函数获取网络攻击行初始判别概率向量,实现通信网络入侵检测;由实验结果可知,该系统的运行时间平均值为86.3 s,吞吐率平均为74 Mbps,网络入侵检测准确率平均值为95%,证明所设计通信网络入侵检测系统运行时间较短,吞吐量较高,证明了该系统的检测速度较快,且检测准确率较好,能够为通信网络的安全运行提供系统支持。

关键词:负载预测;通信网络;入侵检测;负载均衡

Design of Communication Network Intrusion Detection System Based on Load Prediction

XIE Kai, DAI Kang
(Department of Information Engineering, Xinjiang Institute of Engineering, Urumqi 830023, China)

Abstract: Aiming at the problem of low detection accuracy caused by the uneven load of the traditional communication network intrusion detection system, a communication network intrusion detection system design based on load prediction is proposed. Design the system hardware structure, use T—KOKO type monitor and AP—9812M voice information monitoring tool with monitor panel, use HDMI splitter to transmit monitor signal, choose JY211—QTQ—04 type optical cable detector, which contains transmitter inside And receiver, used to transmit and receive data, use TCP relay controller to change the order of normal execution of instructions. Determine the load index, dynamically adjust the load prediction strategy to ensure load balance, and obtain the initial discrimination probability vector of network attacks through the hash function to realize communication network intrusion detection. It can be seen from the experimental results that the average running time of the system is 86.3 s, the average throughput rate is 74 Mbps, and the average network intrusion detection accuracy rate is 95%, which proves that the designed communication network intrusion detection system has a shorter running time and higher throughput, which proves that the detection speed of the system is faster and the detection accuracy is better, which can provide system support for the safe operation of the communication network.

Keywords: load prediction; communication network; intrusion detection; load balancing

0 引言

伴随着网络带宽的不断增加,网络入侵检测系统性能难以满足当下网络速度[1]。采用单机集中检测的方法,很难对当前高速网络流量进行实时分析[2]。为此,有必要对多机并行运行的网络入侵检测系统的相关技术进行研究。同时,网络安全问题也日益成为社会关注的焦点。由于在设计和实施时操作系统、网络协议、应用软件和硬件设备等方面存在缺陷和漏洞,或者系统配置的不当或使用不当,也会造成安全隐患。这些漏洞和隐患为恶意攻击者通过非常规手段入侵系统提供了机会。

以往设计以互联网高性能为主干网的检测系统,具有高带宽的网络服务,主干网传输速度达到10 G,在高速链路下,虽然使用该系统具有快速处理报文性能,但只能被动防御,没有实时报警能力;使用基于防火墙技术设计的检测系统,运行在显示打开端口上,对流经系统所有数据进行实时维护,但无法阻止内部攻击,不能满足通信网络安全通信需求。

针对上述问题,提出了基于负载预测的通信网络入侵检测系统设计。应用动态均衡算法,通过多个分配器和探测器协同工作,系统采用两级并联结构,实现了流量分配,避免了负载集中导致的单一分流装置的使用,具有良好的均衡性能和高冗余、可扩展性。

1 通信网络入侵检测系统拓扑结构设计

基于负载预测的通信网络入侵检测系统群集拓扑以n层解决方案为基础,包括一个Web层群集,为客户机提供内容服务。该网络层集群使用IIS和网络负载平衡来满足IP

收稿日期:2021-04-28; **修回日期**:2021-05-20。

作者简介:谢 凯(1978-),男,山东巨野人,大学本科,讲师,主要从事电子与通信工程方向的研究。

引用格式:谢 凯,代 康.基于负载预测的通信网络入侵检测系统设计[J].计算机测量与控制,2021,29(8):62-66.

的输入请求。图 1 中显示了系统拓扑结构。

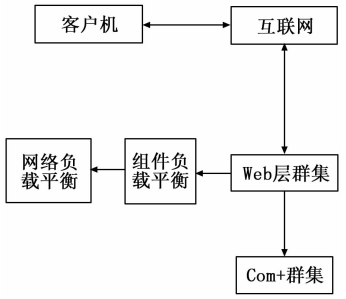

图 1　系统拓扑结构

由图 1 可知，网络层集群中的软件可以在本地计算机上创建并使用 COM＋组件，或者可以使用分布式 COM 在远程计算机上创建并使用 COM＋组件。

网络负载均衡（NLB）是一种基于 IP 的负载均衡技术，基于服务器负载百分比，它提供了一组统计算法的动态缩放功能。也就是，它能自动适应集群中服务器的增加和删除，而不会对客户端造成影响[3]。

COM＋组件负载平衡技术可用于实现组件负载平衡，构件是可用于多种不同语言的编译软件对象。对于 CLB，COM＋组件位于服务器上，位于单独的 COM＋集群中。

2　通信网络入侵检测系统硬件结构设计

通信网络入侵检测系统硬件结构如图 2 所示，它由负载预测器、探测器和控制中心组成。

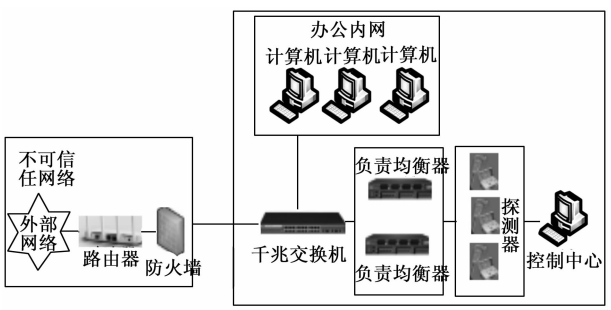

图 2　系统硬件结构

如图 2 所示，并行入侵检测系统的模型主要包括监视器、分配器、探测器和控制器。监听程序是整个结构的中心，它负责捕捉流经该网络段的所有数据包，并将其转发给每个分发器；显示器可以是交换机在特定网络环境中的一个显示器端口或镜像端口，监听程序并不专门向每一个检测器分发数据包，而只是使用简单的循环算法来划分流量，然后再向分发器分发。这能够更好地适应高速网络，避免出现数据传输拥塞问题，实现业务级的第一次业务分流；分配器通过交换机向各个检测器转发数据包，完成二级流分配。探测器在相同配置下运行 Snort；控制器负责获取各个检测器的处理能力和负载信息，并根据当前网络流量的变化动态地进行流量分配算法的调整[4]。

2.1　监听器

监听器，也叫窃听器，是一种 T－KOKO 型监听器，带有监听面板 AP－9812M 的语音信息监听工具。它包括全球移动通信系统，其工作原理是在系统信道中对语音信号进行编码、加密和交织，形成突发信号，经调制后发送。接收话机端对信号进行解调、解交错、信道解码、语音解码，然后还原为用户手机语音信号[5]。在 GSM 系统中，采用了 TDMA（窄带时分多址）技术。载频带宽为 200 kHz 的每帧具有 8 个时隙。在理论上，一个 RF 可以同时进行 8 次呼叫，每个时隙的长度为 0.577 ms，帧的持续时间为 4.615 ms，也就是将时间划分为周期性帧，每帧分为若干时间段。基于特定的时隙分配原理，手机用户通过每帧帧间将信号发送到基站，基站分别位于各自指定的时隙内[6]。

由于基站接收到来自不同手机用户的信号，因此也会按照指定的时间间隔发送给不同手机用户。每个移动用户在规定的时间间隔内接收到信号，但不能保证他们都在同一频道，用户之间不能相互干扰[7]。

2.2　分配器

使用 HDMI 分配器输入视频信号：0.5～1.0 V p－p、输入 DDC 信号：5 V p－p（TTL）、最大单链路范围：1 920x1 080，1 080 P，3D 1 080 P / 24 Hz、输出视频：HDMI 1.4V ＋ HDCP1.0 / 1.1 / 1.2。

在 CATV 传输系统中，配分器是最常用的信号传输元件。它的作用是将一个输入信号平均分为几个输出信号，通常是二分布、三分布、四分布、六分布等等。在 C++编程中，分配程序是 C++标准库的重要组成部分。C++库定义了一系列数据结构，并统称为容器。两者的共同点是，它们的大小可以用来对程序进行操作。对于这个问题，动态内存分配尤其重要，它是用来处理内存分配和释放容＋器请求的。

2.3　光缆探测器

选择 JY211－QTQ－04 型号光缆探测器，内部含有发射机和接收机，其中发射机自动测试并显示电池电压，低于 10 V 时，蜂鸣器会发出急促的声音告警并停机。停机后，开始自动阻抗匹配，并在工作中实时显示信号强度；接收机是从光缆上接收信号，探测光缆路由、埋深。操作者根据表头指针的显示、蜂鸣器声音的提示来确认光缆的路由、埋深[8]。

晶型振荡器产生 3.5～4.95 M 的正弦波，然后把它分解成大约 7.8 K 的正弦波。电流通过晶体管和线圈后，把电磁波传送到门板上的一个较大的线圈（7 区），由门 1－6 发出电磁波，各区线圈各自接收。接收时，将接收到的信号与参考信号进行比较[9-11]。捕获卡的输出级别也会随之发生改变，中控机在 300 ms 内扫描 6 张捕捉卡，判断金属的位置并输出显示出来。

2.4　控制器

采用 TCP 继电器控制器，4 路输入，联动控制。控制器是通过改变主电路或控制电路的接线方式，按照预定的顺序改变电阻值，从而对电机的启动、速度、制动和倒转进行控制的主要装置。它包括程序计数器、指令寄存器、

指令译码器、时序发生器和操作控制器。它是发号施令的“决策主体”，也就是协调和指挥整个计算机系统的运行完成。

在控制器结构中，命令寄存器用于存储命令的执行。这条指令包括操作代码和地址代码。操作码用来表示指令操作的性质，如加，减等；地址码用来给出指令的操作数地址，或关于操作数地址的信息[12-14]。其中有一种指令被称为传输指令，用于改变指令正常执行的顺序。这个指令的地址编码部分提供了指令发送和执行的地址。

操作码解码器：对指令进行解码时所使用的操作码，并生成相应的控制级别，从而完成指令分析功能[15-17]。

时序电路：用于产生时间标记信号，微机上的时标信号一般分为 3 个层次：指令周期，总线周期和时钟周期。微指令产生电路产生各种微指令，完成指令所规定的动作。这些命令主要是根据时间戳和命令来执行的。该电路是一种实现单一微操作控制信号（如上面 A→ L 表达式）的电路，是组合逻辑控制器中最复杂的部分[18]。

指令计数器：用来产生要执行的下一个指令的地址，一般来说，指令按顺序执行，指令也按顺序存储在内存中。因此，在正常情况下，可以向当前地址添加 1，以组成下一条指令的地址，微操作命令“1”也可以使用。如果执行是分支指令，那么下一条要执行的指令的地址就是它传递给指令的地址。传输指令在地址码域中，直接发送到指令计数器。

3 基于负载预测的通信网络入侵检测系统软件功能设计

在此基础上，设计通信网络入侵检测系统软件功能。通过确定负载指标，实现对通信网络入侵状况的监测，根据检测结果动态调整负载预测策略，通过反馈控制实现通信网络入侵实时检测，最后通过 hash 函数判断通信网络入侵攻击类型，获取网络行为最终判别概率向量。

3.1 负载预测算法

首先设计负载预测指标，对检测器的负载状态、可用性和分析能力进行连续监测，基于反馈控制负载情况动态调整负载分布，在获取的默认输出端口过载时，动态调整组件在最小负载输出端口上的流量，以避免丢包，达到负载平衡。

3.1.1 负载指标确定

响应系统负载状态的理想负载指数应该满足：收集量小，可以频繁收集，保证信息更新；能够反映所有竞争资源的负载；收集和控制负载指数相互独立。负载度量包括：节点等待任务队列长度、节点利用率、响应时间等。

选择探测器节点等待任务队列中的任务数 t_i 和连续 10 次采集所获得的等待任务队列中的任务数的平均值 e_i 来量化计算探测器的负载量 L_i，即：

$$L_i = t_i * a + e_i \cdot^* (1-a)(i = 1,2,\cdots,n) \quad (1)$$

则探测器 i 的当前处理能力 P_i 为：

$$P_i = r_i/(1+L_i)(i = 1,2,\cdots,n) \quad (2)$$

式中，L_i 表示探测器负载量；t_i 表示探测器当前等待任务数；a 表示影响因子；e_i 表示等待任务数平均值；P_i 表示探测器当前处理能力；r_i 表示探测器处理能力系数。

根据探测器的当前处理能力 P_i，将探测器的负载状态用一个负载指示器变量 $B_i(i = 1,2,\cdots,n)$ 来量化，B_i 正常取值范围为 1～－100，是该探测器负载状态的一个度量，当 B_i 取值为－1 时代表此探测器不可用。

当某一时刻没有接收到检测器的心跳信号时，就认为检测器已关闭，检测器的负荷指数为－1。该负载指示器对检测器的负载状态、可用性和分析能力进行连续监测，并根据监测结果动态调整当前所使用的负载预测策略。

3.1.2 负载预测动态调整策略

基于反馈控制，根据后端处理器的负载情况动态调整负载分布。图 3 中显示了动态调整模型。

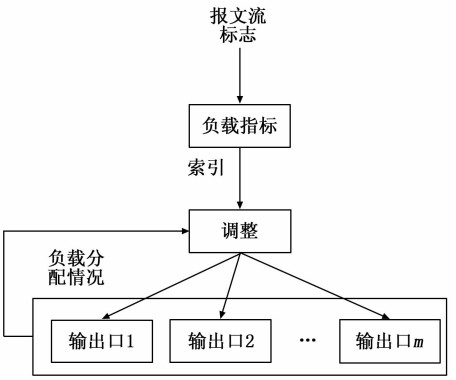

图 3 动态调整模型

由图 3 可知，获取到达消息的流标记，获取确定负载索引下的默认输出端口号，然后根据反馈动态调整组件，在获取的默认输出端口过载时，动态调整组件在最小负载输出端口上的流量，以避免丢包，达到负载平衡。该负载平衡结果将系统的所有信息映射到其他网络入侵检测行为中，实现了并行检测系统的连续不间断检测能力。

3.2 网络入侵检测流程设计

判定所有未知攻击类型后，设计网络攻击行为检测流程。将用户访问请求作为输入数据，通过区块链技术实现网络攻击行为检测，具体过程为：

Step1：预处理输入数据，补充缺失值，删除离散数据。合并存储多个数据，由此构建数据仓库，完成数据集检测；

Step2：计算 hash 值，保证数据集完整且不被篡改。hash 值计算过程为：输入长度不固定数据，给定 hash 函数 $h:X \to Y$，任意选 y 属于 Y，x 属于 X，满足计算公式 $y = h(x)$。hash 函数哈希值范围为 224～512 位，数据输入长度范围为 $[<2^{64} \sim <2^{128}]$ 位，循环次数为 80 次，在该限制范围内的数据，即为不会被篡改数据，具有完整性和使用安全性。

Step3：获取的网络攻击行为初始判别概率向量为：

$$P_{\mathrm{DNN}} = (P_{\mathrm{n}}, P_{\mathrm{im}}, P_{\mathrm{f}}, P_{\mathrm{in}}) \quad (3)$$

式（3）中，P_n 表示正常网络行为发生概率；P_{im} 表示伪装攻击网络行为发生概率；P_f 表示洪泛攻击网络行为发生概率；P_{in} 表示注入攻击网络行为发生概率。

Step4：结合纠正未知攻击类型判别结果，获取网络行为最终判别概率向量：

$$\boldsymbol{P}=\left(\frac{K_{\mathrm{DNN}}}{K_{\mathrm{DNN}}+K_{\mathrm{kmens}}}\times P_{\mathrm{DNN}}\frac{K_{\mathrm{kmens}}}{K_{\mathrm{DNN}}+K_{\mathrm{kmens}}}\times\beta\right) \tag{4}$$

式（4）中，K_{DNN} 表示网络攻击行为初始账本记录阶段。

使用区块链技术对记录账本数据判别结果是未知攻击类别时，未知攻击类型判别纠正项为 1，K_{kmens} 值越大，则未知攻击类别出现可能性就越大；反之，未知攻击类型判别纠正项为 0。当 $P_{\mathrm{DNN}}=1$ 时，4 个元素最大值的攻击行为是最终判别结果。

综上，通信网络入侵检测系统软件编程流程如图 4 所示。

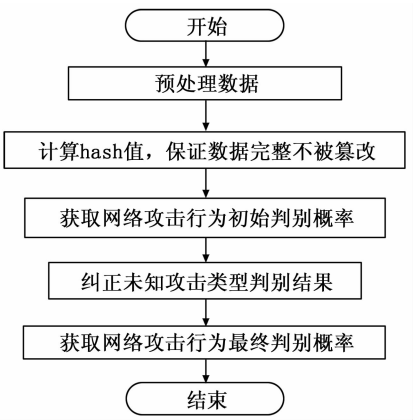

图 4　通信网络入侵检测系统软件编程流程图

如图 4 所示，首先对网络攻击行为数据进行预处理，计算 hash 值，保证数据集完整且不被篡改。计算网络攻击行为初始判别概率向量，结合纠正未知攻击类型判别结果，获取网络行为最终判别概率向量，实现通信网络入侵检测系统软件编程流程设计。

4　实验结果与讨论

为了验证检测方法在提高系统抗入侵性能方面的意义，在双核 CPU 机器上对设计的基于负载预测的通信网络入侵检测系统进行测试。

4.1　测试环境与数据

硬件平台为：Intel Core 2 Duo P8400CPU/2 GB 内存和 160 GB 硬盘；

软件平台为：Window Vista Home Premium 操作系统、编译和执行环境 Visual C++6.0。

实验待测数据来源分别是 IDS 评测数据集和 DEFCON9 的 Capture the Flag 黑客大赛数据集。其中，IDS 评测数据集包括了 U2R、R2L、Data 共计 60 种网络攻击方式，被公认为基准评测数据集；DEFCON9 的 Capture the Flag 黑客大赛数据集，是不同黑客队伍在有安全缺陷计算机上运行的程序，能够实现不同队伍间相互攻击和自身防守。

部分数据集如表 1 所示。

表 1　部分数据集

名称	来源	时间	规模/MB	数据包数量/个
LC1	数据集 1	2019－03－25	200	1 663 550
LC2	数据集 1	2019－04－08	990	3 352 518
LC3	数据集 1	2019－04－15	1 065	3 510 024
DEF1	数据集 2	2019－05－02	680	3 948 054
DEF2	数据集 2	2019－05－25	845	1 052 354

4.2　性能测试指标

测试时使用加速比指标，计算公式为：

$$Speedup_k=\frac{t_k}{t_1} \tag{5}$$

式（5）中，t_k 表示线程数量为 k 的系统运行时间。吞吐率与系统运行时间是具有一定联系的，吞吐率能反映系统对不同数据集检测速率。

4.3　测试结果与分析

在测试过程中，分别对线程数量为 1～3 个的情况进行测试，由于硬件底层物理核数量是 2 个，理论上测试线程数量应为 3 个，然而由于系统设计时，线程主要分为生产和消费两种，生产线程要比消费线程负载低，因此，需考虑测试消费者的最大线程数量情况。

针对两种不同数据集，对应着线程数量为 1～3 条情况，将每个数据项按照系统运行时间和吞吐率的格式填写，如表 2 所示。

表 2　两种数据集系统运行时间和吞吐率对比分析

名称	线程 1	线程 2	线程 3
LC1	55.16 s 30.75 Mbps	50.28 s 35.73 Mbps	38.12 s 45.35 Mbps
LC2	165.12 s 49.50 Mbps	139.15 s 55.95 Mbps	117.04 s 67.75 Mbps
LC3	165.5 s 50.96 Mbps	147.25 s 58.05 Mbps	127.25 s 65.15 Mbps
DEF1	128.65 s 42.15 Mbps	115.3 s 45.54 Mbps	115.95 s 45.66 Mbps
DEF2	60.15 s 111.95 Mbps	55.35 s 125.75 Mbps	53.28 s 125.40 Mbps

由表 2 可知，对于 DEF2 对于线程不同的各种情况，吞吐率比其它数据集明显要高，主要是因为 DEF2 中攻击数据包占总数据集比例最低，因此，检测速度较快。

基于此，分别使用以互联网高性能为主干网的检测系统 W1、基于防火墙技术设计的检测系统 W2 和基于负载预测的通信网络入侵检测系统 W3 对线程 2 下数据集的运行时间和吞吐率进行对比分析，结果如表 3 所示。

表 3 3 种系统 DEF1、DEF2 数据集运行时间和吞吐率对比分析

名称	W1	W2	W3
LC1	55.15 s 34.65 Mbps	45.28 s 35.73 Mbps	40.28 s 40.73 Mbps
LC2	140.20 s 61.34 Mbps	138.20 s 55.95 Mbps	111.15 s 65.95 Mbps
LC3	138.25 s 60.14Mbps	145.20 s 55.12 Mbps	124.25 s 62.05 Mbps
DEF1	155.1 s 53.26 Mbps	155.0 s 46.55 Mbps	115.3 s 55.54 Mbps
DEF2	55.14 s 143.27 Mbps	54.26 s 135.61 Mbps	40.35 s 145.75 Mbps

由表 3 可知，基于负载预测的通信网络入侵检测系统的数据集运行时间平均值为 86.3 s，吞吐率平均为 74 Mbps，均好于对比方法。由此可见，所设计系统的运行时间较短，吞吐率较高，证明了该系统的检测速度较快。

在此基础上测试不同方法的网络入侵检测准确率，得到对比结果如图 5 所示。

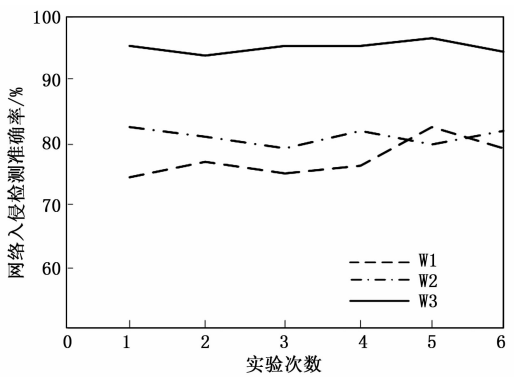

图 5 网络入侵检测准确率对比结果

由图 5 可知，使用以互联网高性能为主干网的检测系统的网络入侵检测准确率平均值为 77%，基于防火墙技术设计的检测系统的网络入侵检测准确率平均值为 81%，基于负载预测的通信网络入侵检测系统检测结果的网络入侵检测准确率平均值为 95%。实验结果表明所设计系统能够准确检测通信网络入侵，对通信网络的安全运行提供系统支持。

5 结束语

针对通信网络，设计了一种高效、可扩展的负载预测入侵检测系统。在高速网络环境中，系统采用负载预测技术，通过多种检测器来适应较大的网络流量。通过理论分析和实验研究得出，所设计基于负载预测的通信网络入侵检测系统的数据集运行时间较短、吞吐率较高，因此该系统对网络入侵的检测速度较快；所设计系统的网络入侵检测准确率平均值为 95%，证明了应用该系统能够准确对网络入侵进行检测。

针对不同类型的攻击，现有的并行入侵检测结构和负载预测技术一般只能通过确保多个流攻击的一致性来保证通常的攻击环境，而对于跨越多个流的攻击，如 DDOS 等，目前没有一个好的解决办法，还需要定义迭代负载系数算法，这些问题有待于在今后的工作中深入研究加以分析。

参考文献：

[1] 王 萌，王亚刚，韩俊刚. 基于 NDNN 的入侵检测系统 [J]. 微电子学与计算机，2018，35 (7)：83 - 86.
[2] 张建珍. 云计算下海上通信网络异类入侵数据实时检测系统设计 [J]. 舰船科学技术，2019，41 (16)：182 - 184.
[3] 戴 敏. 基于并行特征选择和分类的网络入侵检测方法 [J]. 计算机工程与设计，2019，40 (3)：61 - 68.
[4] 王宇耕，肖 鹏，张 力，等. 基于负载预测的自适应权值负载均衡算法 [J]. 计算机工程与设计，2019，40 (4)：140 - 144.
[5] 张 强，梁 杰，许胤龙，等. 基于工作负载感知的固态硬盘阵列系统的架构设计与研究 [J]. 计算机研究与发展，2019，56 (4)：755 - 766.
[6] 赵鱼名，王智慧，苏玉刚，等. 基于 T 型 CLC 谐振网络的恒压型电场耦合电能传输系统负载自适应技术 [J]. 电工技术学报，2020，35 (1)：106 - 114.
[7] 孟小冬，冯 锋. 基于大数据的光纤传感网络入侵检测系统 [J]. 激光杂志，2019，40 (8)：102 - 105.
[8] 朱子龙，李 斌，李 成，等. 浅谈 POL 方案在南水北调中线工程的应用前景 [J]. 水电站机电技术，2019，42 (4)：36 - 37.
[9] 郭 杉，周 佳，贾俊青. 基于负荷预测的地区电动汽车充电设施容量配置 [J]. 内蒙古电力技术，2018，36 (4)：79 - 82.
[10] 张 雷，解 仑，金良辰，等. 基于 COME 模块的单类支持向量机的入侵检测系统 [J]. 北京理工大学学报，2019，39 (9)：102 - 110.
[11] 池亚平，莫崇维，杨垠坦，等. 面向软件定义网络架构的入侵检测模型设计与实现 [J]. 计算机应用，2020，40 (1)：116 - 122.
[12] 翟柱新. 基于双向搜索的电力通信一体化入侵检测方法 [J]. 电子设计工程，2020，28 (3)：75 - 78.
[13] 闫明辉. 计算机网络入侵检测系统匹配算法的研究 [J]. 电子设计工程，2019，27 (8)：40 - 43.
[14] 李 建. 基于 IPSec 安全协议的网络数据传输入侵检测模型 [J]. 电子设计工程，2020，28 (4)：82 - 85.
[15] 王佳骏，林承勋，陈 瑾，等. 基于强化学习的通信网络入侵自适应检测方法 [J]. 信息技术，2019，43 (11)：32 - 35.
[16] 于怡然，常 俊，吴柳繁，等. 基于 Wi－Fi 信道状态信息的免训练入侵检测系统 [J]. 微电子学与计算机，2020 (5)：18 - 22.
[17] 程小辉，牛 童，汪彦君. 基于序列模型的无线传感网入侵检测系统 [J]. 计算机应用，2020，40 (6)：134 - 138.
[18] 郭 华，李 颖，江 浩，等. 基于物联网技术的电力线路信息网入侵检测系统设计 [J]. 电子设计工程，2020，28 (18)：137 - 141.