文章编号:1671-4598(2022)02-0038-06 DOI:10.16526/j.cnki.11—4762/tp.2022.02.006 中图分类号:TP309.1 文献标识码:A

基于混合随机边缘计算的工控入侵检测系统设计

魏巍巍

(北京信息职业技术学院 数字商务学院,北京 100015)

摘要: 针对传统工控入侵检测系统缺少对边缘入侵信号段的研究,无法及时检测到边缘入侵行为,导致系统入侵潜伏期过长、威胁工控系统网络安全的问题,提出了基于混合随机边缘计算的工控入侵检测系统设计;使用中央服务器处理并发送告警信息,形成统一的告警日志;选择JY211—QTQ—04型号光缆探测器,实时显示信号强度;通过高速网络I/O架构Netmap网络流量采集器采集流量信息,再由TCP/IP协议下的数据预处理器处理数据,利用入侵检测引擎检测入侵行为;构建入侵检测动态模型,结合混合随机边缘算法,确定待检测段的最高能量和信噪比,通过检测到的入侵信号段,判断入侵行为;由实验结果可知,该系统在异常入侵情况下,能够及时发现入侵行为,在入侵时间为7 s时,潜伏期达到最长为2.4 s,与实际入侵后潜伏期变化一致,能够精准检测工控入侵行为。

关键词: 混合随机边缘计算;工控入侵检测;光缆检测器;边缘入侵

Design of Industrial Intrusion Detection System Based on Hybrid Random Edge Computing

WEI Weiwei

(Digital Business College, Beijing Polytechnic College, Beijing 100015, China)

Abstract: Aiming at the problem that the traditional industrial control intrusion detection system lacks the research on the edge intrusion signal segment, and cannot detect the edge intrusion in time, which leads to the long incubation period of system intrusion and influences the network security of the industrial control system, an industrial control intrusion detection system based on hybrid random edge computing is proposed. design. The central server is used to process and alarm information is sent to a unified alarm log. The JY211—QTQ—04 optical cable detector is selected to display the signal strength in real time. The flow information is collected by the high—speed network I/O architecture Netmap network flow collector, and then the data is processed by the data preprocessor under the TCP/IP protocol, and the intrusion detection engine is used to detect intrusion behavior. Constructs a dynamic model of intrusion detection, combined with a hybrid random edge algorithm, determines the highest energy and signal—to—noise ratio of the segment to be detected, and judges the intrusion behavior through the detected intrusion signal segment. It can be seen from the experimental results that the system can detect intrusion behaviors in time under abnormal intrusion conditions. When the intrusion time is 7 s, the incubation longest period reaches 2.4 s, which is consistent with the actual incubation period after the intrusion, and can accurately detect industrial control intrusion behaviors.

Keywords: hybrid random edge computing; industrial control intrusion detection; optical cable detector; edge intrusion

收稿日期:2021-07-29; **修回日期:**2021-08-26。

作者简介:魏巍巍(1980-),女,北京人,硕士,讲师,主要从事计算机大数据,边缘计算方向的研究。

引用格式:魏巍巍.基于混合随机边缘计算的工控入侵检测系统设计[J].计算机测量与控制,2022,30(2):38-43.

0　引言

近年来，工业控制网络的入侵和攻击事件日益增多，信息安全受到破坏，为此研究工业控制网络入侵检测系统具有重要意义[1]。具体地说，入侵检测系统在保障工控网络安全方面起着重要作用。例如，防火墙只能允许或阻止特定的端口访问，但却无法阻止开发端口的攻击入侵[2]。工控网络内部攻击往往比外部攻击更加强大和具有破坏性，而入侵检测系统能够阻止网络内部的攻击，因此入侵检测系统能够对工业控制网络的安全保护起到很大的作用[3]。

当前相关领域学者已对工控入侵检测系统做出了研究。文献［4］提出了基于深度 Q 网络的工控网络异常检测系统，融合深度学习算法及 Q－learning 方法对工控网络进行训练，及时发现入侵攻击行为并作出预警。然而由于工业控制网络对于网络操作具有特殊要求，如果只对正常运行状态下的工控网络进行训练，会导致入侵行为漏报现象，一旦入侵行为稍作调整，就可以躲避系统检测；文献［5］提出基于优化极限学习机的工业控制系统入侵检测模型，利用混合自适应量子粒子群算法，对入侵行为输入权值和隐含层结点阈值进行优化，增强了算法的全局优化能力，建立了基于 HAQPSO 优化的工业控制入侵检测模型。虽然使用该系统的全局寻优能力较强，但一旦出现边缘入侵问题，那么使用该系统就无法有效检测，导致检测效果较差。

基于上述检测系统存在的无法及时准确检测到边缘入侵行为，威胁工控系统网络安全的问题，提出了基于混合随机边缘计算的工控入侵检测系统设计，分别对系统硬件模块及软件流程做出设计。利用边缘计算将云计算的计算能力渗透到数据端，将边缘云协作融入混合随机边缘计算中，通过混合随机边缘计算得到入侵检测信号的能量，构建动态模型实现工控入侵检测。

1　工控入侵检测系统硬件结构设计

鉴于工业控制系统的特殊性，系统中的每一种设备都需要根据业务逻辑在固定的时间内完成其具体的操作，对实时性要求很高，不能有任何差错，否则将威胁工控系统的正常运行，甚至破坏系统的功能[6]。为了避免工业控制环境下的入侵检测系统受到外界干扰影响，提出了一种基于混合随机边缘计算的工业入侵检测系统，并对其进行了详细的设计。系统硬件结构如图 1 所示。

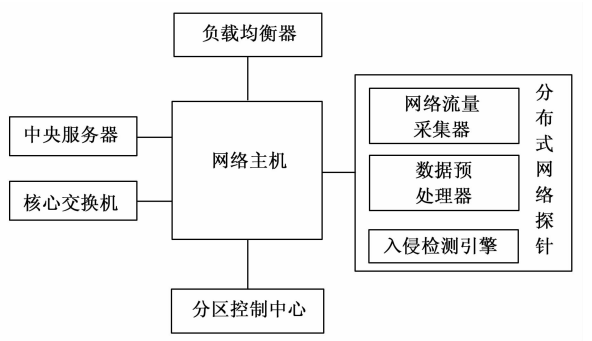

图 1　系统硬件结构

由图 1 可知，本系统采用一台中央服务器和分布在各个工控子网上的多路网探头分布式结构，通过独立交换机构成网络入侵检测系统，利用分布式网络探针，将网络流量接入系统，实现系统的零干扰。中央服务器能够实现工控网络数据大容量存储并提供性能良好的处理器，实现数据的高速处理；分布式网络探针包括网络流量采集器、数据预处理器及入侵检测引擎，能够实现工控网络入侵的实时、可靠检测；核心交换机可实现的网络流量数据的可靠、高速传输。

1.1　中央服务器

系统采用一台中央服务器作为管理和控制中心，通过任务分配机制实现对网络探测器的管理，探测器通过网络发送和接收报警信息，形成一个统一的报警日志，并在一个友好的可视世界中为管理人员显示各种报警统计数据[7]。

中央服务器结构如图 2 所示。

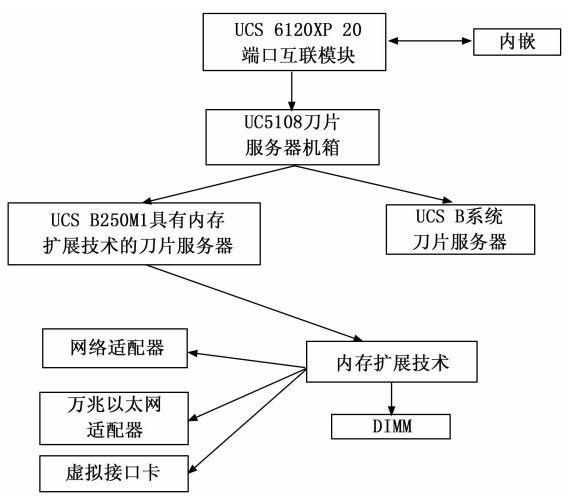

图 2　中央服务器结构

由图 2 可知，中央服务器是通过代理服务器连接到互联网上的局域网，主板使用了 Catalina 型号缓冲器，可扩展 CPU 通道，将 2 个扩展成 8 个，每条通道内包含 DDR3 内存子通道，每条内存通道有两个 CPU，因此总共有 48 个内存插槽[8]。中央服务器需要多个网卡接口，以及大容量存储和一个性能良好的处理器。采用多种网卡接口连接不同的网络探头，采用大容量存储器存储各种报警信息和日志记录[9]。另外，为了保证良好的用户体验，还必须对处理器的性能提出了要求。

1.2 分布式网络探针

分布式网络探头部署在各种工控子网上，具有监听、捕获、解析网络包的功能。选用 JY211－QTQ－04 型光缆检测仪，它由一台变送器和一台接收机组成，能够自动检测并显示电池的电压，在低于 10 V时报警迅速停止。关电后，阻抗匹配自动启动，启动时实时显示信号强度。接收者接收来自光纤的信号，并检测线路和深度。操作人员根据指针显示，蜂鸣器发出声音提示确认电缆线路，埋设部门进行埋深[10]。

经晶形振子处理后，产生 5 M 的正弦波，再将其分解为 7.8 k 左右的正弦波，电流通过晶体管和线圈发出强大的电磁波。每一区域的线圈都可以接收到电磁波，而中心控制器在电磁波发送期间，可以扫描 5 张采集卡，并在界面上显示其结构。每个网络检测器至少有两个端口，一个端口用于工控交换机镜像通信，另一个用于连接中央服务器[11]。

1.2.1 网络流量采集器

为了提高网络流量捕获效率，使用网络 I/O 结构，避免数据丢失，结合开源函数库，在 1 000 MHz 单核 CPU 下处理 10 G 网络流量。基于零复制思想，结合网络地图设计的网络流量采集器，相对于传统的网络流量采集方式，可以显著提高网络数据采集速度，有效地节约了系统设计费用。网络流量采集器中，网卡通过网卡环对入站和出站组进行管理。每个网卡都要维护至少几个小空间，每一个空间都包含大量的缓冲信息，主机网络堆栈通过一个网卡直接访问缓冲区存储区域，使数据按顺序依次进行接收[12]。

1.2.2 数据预处理器

主要包括会话解析数据处理、工业控制协议数据处理、协议解析数据处理等，其中会话解析数据处理主要包括对提取源 IP、源数据、目的 IP、目标日期、传输层协议等信息进行处理；工业控制协议数据处理主要包括对用于识别行业协议的特征域进行处理；协议解析数据处理主要包括对开放源码的处理以及工控协议代码。

1.2.3 入侵检测引擎

入侵检测引擎为系统的核心引擎，具备实时、可靠检测功能，入侵检测引擎如图 3 所示。

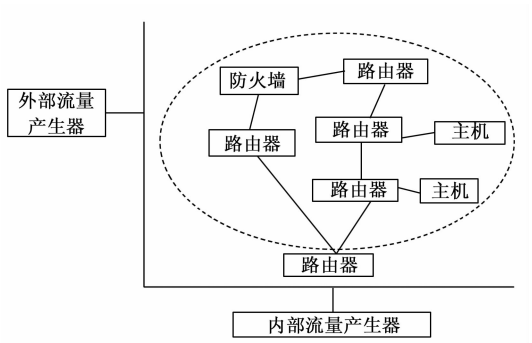

图 3 入侵检测引擎

由图 3 可知，入侵检测引擎通过获取和分析通信数据包，采用规则自学习、特征提取、分类、入侵检测等技术，建立了一个工业控制系统，以实现分布式入侵检测功能。

1.3 核心交换机

采用 S5720S－28P－SI－AC 型号，24 口全千兆网络核心交换机，可直接与网络用户连接。核交换接入层与核心层之间设有汇合层，其中接入层的作用是支持终端用户直接接入网络，其特点是端口高、密度低；汇流层的作用是将多个节点数据汇合到一层，处理所有从接入层传送的流量数据；核心层的作用是提供可靠的网络流量传输结构，实现数据高速传输[13]。

2 基于混合随机边缘计算的工控入侵检测系统软件设计

在硬件结构的基础上，设计工控入侵检测系统软件流程。客户机根据所需完成的服务生成任务来执行请求包，在这个请求包中，使用跟踪身份表示正在执行服务，而边缘计算会将云计算的计算能力渗透到数据端。所以，局部边缘计算具有高实时性，能够存储短期数据，而云计算则能存储大量数据，远距离进行大数据分析，以及本地支持边缘计算的决策能力[14]。

本文通过边缘计算和云计算在入侵检测业务中的应用，分析了边缘云协作在入侵检测业务中的作用。

设计的基于混合随机边缘计算的工控入侵检测系统，主要步骤包括：

步骤 1：由于网络中可以有多个节点处理某项任务中的一个步骤，因此请求包中任务执行的每一个服务也需要指明它将在哪个节点上执行。当发送给网络的任务执行请求包时，如果是按串行顺序执行的，那么服务序列中的每个项都是连续执行的[15]。在边缘节点上，跟踪标志指向子服务序列中的下一个服务。

步骤 2：根据所构建的业务网络拓扑图和当前需要执行的业务，客户选择具有最佳指标的边缘节点，将任务执行请求包发送到相关的边缘节点。

服务网络拓扑图如图 4 所示。

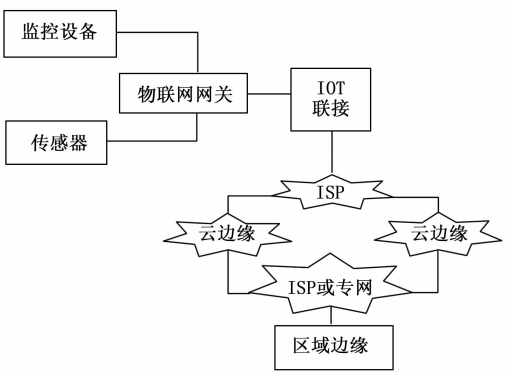

图 4　服务网络拓扑图

步骤 3：关联边缘节点解析任务执行请求包，当相关服务出现局部执行结果时，直接读取相应的执行结果。而且，如果服务队列中的同一个服务等待执行，那么队列就跳到请求包执行相关任务的位置[16-18]。不然，在服务队列之后重复这个过程，直到服务完成。

步骤 4：基于混合随机边缘计算的入侵检测动态建模，分析一段待检测的工控网络入侵信号 W，其计算公式为：

$$W = \sum_{i=1}^{m} |\lambda_i|^2 \tag{1}$$

公式（1）中，λ_i 表示待检测信号中各个检测点的有效幅值；m 表示待检测信号的有效长度。

由于工控系统中存在随机噪声扰动，通过分数阶变换对随机噪声扰动进行自相关特征匹配，抑制噪声输出，得到去噪后的检测信号。

$$\lambda(m) = W\left(\frac{k}{2}t^2\right) + S(t) \tag{2}$$

公式（2）中，$\lambda(m)$ 表示去噪后的检测信号，k 为调频斜率，$S(t)$ 为零均值高斯噪声。

基于混合随机边缘算法计算噪声去除后的功率 p_{sl}，计算公式为：

$$p_{sl} = \frac{1}{m}\sum_{m}\lambda^2(m) \tag{3}$$

设 $maxW_1$ 表示待检测某段 R_1 的最高能量，该段能量所对应的信噪比为 $maxSNR_1$，$maxW_2$ 为表示待检测某段中剩下部分的 R_2 最高能量。

基于上述内容，构建的入侵检测动态模型为：

$$\left|\frac{maxW_1 - maxW_2}{maxW_1}\right| \geqslant \left|\frac{maxSNR_1 - maxSNR_2}{maxSNR_1}\right| \tag{4}$$

当入侵信号满足公式（4）时，则检测到的 R_1 信号段为入侵信号段，否则 R_2 为入侵信号段。通过该模型实现工控系统入侵检测。

综上所述，基于混合随机边缘计算的工控入侵检测系统软件流程如图 5 所示。

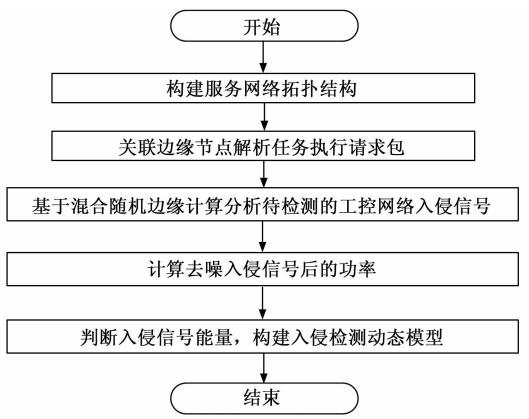

图 5　基于混合随机边缘计算的工控入侵检测系统软件流程

3　实验结果与分析

3.1　实验环境

为了验证基于混合随机边缘计算的工控入侵检测系统设计合理性，利用上位机结合具体工况业务逻辑，分析燃气管网的工作模式，其拓扑结构如图 6 所示。

由图 6 可知，为了方便入侵检测系统移植，在控制层设置了两种 PLC，并部署在控制子网中。

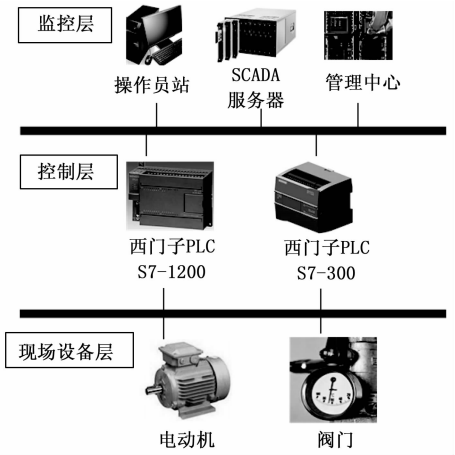

图 6 实验环境拓扑结构

3.2 实验数据集

KDD CUP 99 数据集包含了 TCP dump 网络数据和审计数据，模拟多种用户种类，使其看起来像是在真实环境下构建的网络环境。其中 TCP dump 网络数据主要分为两个部分，分别是包含 5 000 000 个训练数据和 200 万条的测试数据。

联网连接是指在某一时期内，从头到尾的 TCP 数据组成序列协议，将数据从源 IP 地址传输到目标 IP 地址。未知攻击出现在测试集内，主要包括 4 种异常情况，如下所示：

1）拒绝攻击模式，比如受到畸形报文攻击、协议缺陷、IP 欺骗；

2）远程主机未授权访问，比如密码猜测；

3）未授权本地用户访问，比如缓冲溢出攻击；

4）端口监视，比如端口扫描。

3.3 实验结果与分析

在上述 4 种异常情况下，触发基于混合随机边缘计算的工控入侵检测系统的告警日志记录，如图 7 所示。

由图 7 可知，图 7（a）拒绝服务攻击下的入侵检测报告：在局域网中可能存在攻击畸形报文攻击、协议缺陷、IP 欺骗行为的主机，直接通过强制断网操作，就可阻断入侵行为；图 7（b）远程主机未授权访问下的入侵检测报告，通过对局域网中运行的影响网速的软件检测，可及时发现入侵行为；图 7（c）未授权本地用户访问，通过在安全工具窗内，选择自动向局域网发送攻击免疫信息，由此开启入侵检测功能；图 7（d）为端口监视，通过将 IP 地址和 MAC 进行静态绑定来实现端口扫描，阻断入侵行为。

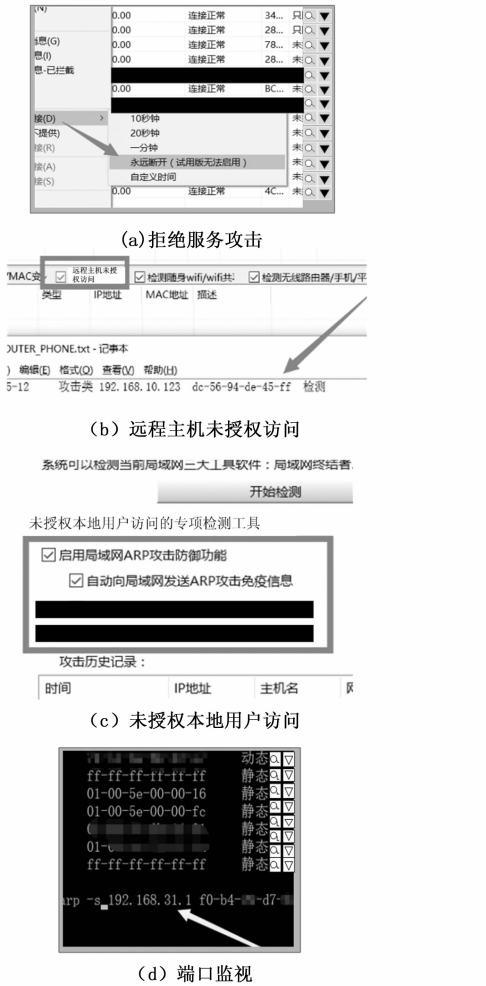

图 7 4 种异常数据下入侵检测系统的告警日志记录

分别采用文献［4］方法、文献［5］方法作为实验对比方法，对比分析不同入侵时间段下系统的潜伏期，对比结果如图 8 所示。

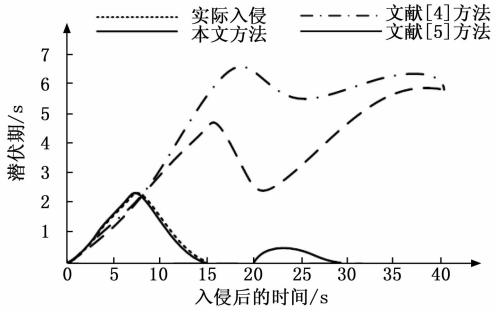

图 8 3 种系统不同入侵时间段下系统潜伏期对比分析

由图 8 可知，使用文献［4］方法在入侵时间为 13 s 时，潜伏期达到最长为 6.4 s，并且随着入侵时

间增加，潜伏期也在 5～6.4 s 间波动；使用文献[5]方法的入侵检测系统在入侵时间为 40 s 时，潜伏期达到最长为 5.8 s，潜伏期时间较长；使用基于混合随机边缘计算的入侵检测系统在入侵时间为 7 s 时，潜伏期达到最长为 2.4 s，随着入侵时间增加，该系统有效抵抗了黑客入侵，虽然在 20～30 s 范围内出现小幅度的变化，但最终成功抵抗了外界入侵。分析可知，文献[4]方法采用深度强化学习算法训练工控网络入侵数据，输出入侵攻击行为数据，该方法未对不同运行状态下的工控网络进行训练，因此存在入侵行为漏报现象；文献[5]方法采用混合自适应量子粒子群算法，在 HAQPSO 的基础上优化入侵行为的输入权值和隐含层节点阈值，增强了算法的全局优化能力。但该方法无法有效地检测出边缘入侵行为。而本文方法采用混合随机边缘计算方法，将边缘云协作融入混合随机边缘计算中，获取入侵检测信号的能量并判断入侵信号段，因此能够得到准确的入侵检测值。

4　结束语

设计工控入侵检测系统，将混合随机边缘计算方式融合到工控入侵检测系统中，可将检测任务划分到检测环节中，在工控环境下对入侵信号段进行精准识别与监测，实现对工控系统的全面检测。实验结果表明，所设计系统能够准确监测到实验设置的 4 种异常情况，其入侵检测潜伏期最长为 2.4 s，能够成功抵御外界入侵，使其更加适用于工控网络。

虽然所设计系统发挥了良好的作用，但还存在许多有待改进的地方，值得进一步研究：在应用场景中，如何设计出适合于工业网络安全的模式匹配算法，对进一步提高检测效率具有重要意义。

参考文献：

[1] 华昊辰，李宇童，王同贺，等. 一种基于混合随机 H_2/H_∞方法的能源互联网边缘计算系统控制策略[J]. 中国电机工程学报，2020，40（21）：115－125.

[2] 张　瑞，陈红卫. 基于特征优化与 SVPSO 的工控入侵检测[J]. 计算机工程，2020，46（4）：25－31.

[3] 谭　彬，赵嵩源，吴　俊，等. 基于移动边缘计算的虚拟现实压缩与传输系统[J]. 通信学报，2020，41（4）：49－57.

[4] 王竹晓，张彭彭，李　为，等. 基于深度 Q 网络的电力工控网络异常检测系统[J]. 计算机与现代化，2019，（12）：114－118.

[5] 赵国新，陈志炼，魏战红，等. 基于优化极限学习机的工业控制系统入侵检测[J]. 计算机工程与设计，2020，41（3）：608－613.

[6] 马　琳，张莎莎，宋姝雨，等. 基于 SDN 的智能入侵检测系统模型与算法[J]. 高技术通讯，2020，30（5）：103－107.

[7] 梁玉珠，梅雅欣，杨　毅，等. 一种基于边缘计算的传感云低耦合方法[J]. 计算机研究与发展，2020，57（3）：639－648.

[8] 曹德胜. 基于密度聚类的数据库入侵检测系统研究[J]. 西南师范大学学报（自然科学版），2019，44（5）：109－114.

[9] 简琤峰，平　靖，张美玉. 面向边缘计算的 Storm 边缘节点调度优化方法[J]. 计算机科学，2020，47（5）：285－291.

[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] 邹　萍，张　华，马凯蒂，等. 面向边缘计算的制造资源感知接入与智能网关技术研究[J]. 计算机集成制造系统，2020，26（1）：40－48.

[12] 池亚平，杨垠坦，李格菲，等. 基于 GR－CNN 算法的网络入侵检测模型设计与实现[J]. 计算机应用与软件，2019，36（12）：297－302.

[13] 路艳巧，孙翠英，曹红卫，等. 基于边缘计算与深度学习的输电设备异物检测方法[J]. 中国电力，2020，53（6）：27－33.

[14] 薛建彬，安亚宁. 基于边缘计算的新型任务卸载与资源分配策略[J]. 计算机工程与科学，2020（6）：959－965.

[15] 王伏亮，李　澄，李春鹏，等. 基于边缘计算的中低压配电网多类型传感器接入技术[J]. 自动化与仪表，2020（7）：11－15.

[16] 殳雪城，范平清. 基于边缘计算的物联网网关监控系统的研究[J]. 电子器件，2019，42（6）：1569－1573.

[17] 殷　佳，管昕洁，白光伟. 基于移动边缘计算的任务迁移和协作式负载均衡机制[J]. 计算机科学，2019，46（12）：126－131.

[18] 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.