计算机科学
COMPUTER SCIENCE

基于人工智能的分布式入侵检测研究

王璐，文武松

引用本文

王璐，文武松. 基于人工智能的分布式入侵检测研究[J]. 计算机科学, 2022, 49(10): 353-357.

WANG Lu, WEN Wu-song. Study on Distributed Intrusion Detection System Based on Artificial Intelligence[J]. Computer Science, 2022, 49(10): 353-357.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220700095

基于人工智能的分布式入侵检测研究

王 璐[1] 文武松[2]
1 重庆第二师范学院人工智能学院 重庆 400065
2 清华大学电机系 北京 100084

摘 要 为了解决目前动态加载系统存在的数据处理缺陷以及系统入侵精确度低等问题,以“人工智能技术”应用为例,设计一款功能完善、实用性强的分布式入侵检测系统。首先,在完成系统架构设计和系统数据库设计的基础上,对控制中心、分区控制中心延长网络主机进行全面分析;其次,严格按照响应库相关的响应规则,制定相应的响应对策;然后,借助通信模块判断其入侵行为是否出现异常问题;再次,利用 S5720S-28P-SI-AC24 口核心交换机对相关数据进行交换处理;接着,选用型号为 AD2032 的报警响应器对外来入侵行为进行全面监视;另外,在全面分析主体通信实现方式的基础上,利用 Libpcap 库函数完成对入侵检测流程的科学设计;最后,从环境与参数设置、系统测试结果与分析两个方面入手,对系统性能进行全面测试。结果表明,在人工智能技术的应用背景下,所设计的分布式入侵检测系统可以获得较高的检测精确度,达到了 99%,为后期安全、稳定地使用网络提供重要的平台支持。

关键词:人工智能;分布式;入侵检测系统;设计;实现
中图法分类号 TP393

Study on Distributed Intrusion Detection System Based on Artificial Intelligence

WANG Lu[1] and WEN Wu-song[2]
1 School of Artificial Intelligence, Chongqing University of Education, Chongqing 400065, China
2 Department of Electrical Engineering, Tsinghua University, Beijing 100084, China

Abstract In order to solve the problems of data processing defects and low system intrusion accuracy existing in the current dynamic loading system, a distributed intrusion detection system with complete functions and strong practicability is designed by taking the application of “artificial intelligence technology” as an example. Firstly, on the basis of completing the system architecture and database design, comprehensively analyze the control center and the extended network host of the subregional control center, and then formulate corresponding response countermeasures in strict accordance with the relevant response rules of the response library. Secondly, through the use of the communication module, the intrusion behavior is judged to determine whether the intrusion behavior is abnormal. Again, use the S5720S-28P-SI-AC24-port core switch to exchange related data. Then, through the selection of AD2032 alarm responder, a comprehensive monitoring of external intrusion behavior is carried out. In addition, based on the comprehensive analysis of the main body communication implementation, the Libpcap library function is used to complete the scientific design of the intrusion detection process test. The results show that, under the application background of artificial intelligence technology, the distributed intrusion detection system designed in this paper can obtain high detection accuracy, and its accuracy reaches 99%, which provides an important platform for the later security and stable use of the network support.

Keywords Artificial intelligence, Distributed, Intrusion detection system, Design, Implementation

1 引言

人工智能技术的出现和应用,将人工智能与网络技术进行了有效结合。该技术作为一种新型、先进的软件设计技术,具有交互性高、移动性强、自主性明显等特点,被广泛地应用于图像识别、机器翻译等领域[1-2]。在网络安全检测领域,将该技术科学地应用到分布式入侵检测系统设计中,不仅可以制定出系统、完善的设计方案,还能实现对入侵信息的追踪和采集。因此,在人工智能技术的应用背景下,如何科学地设计分布式入侵检测系统是技术人员必须思考和解决的问题[3-5]。

到稿日期:2022-06-11 返修日期:2022-07-25
基金项目:重庆市教委科学技术研究项目(KJQN201901607)
This work was supported by the Project of Science and Technology Research Program of Chongqing Municipal Education Commission of China (KJQN201901607).
通信作者:王璐(wanglu514@163.com)

2 系统总体架构设计

2.1 系统架构设计

对于整个分布式入侵检测系统而言，其物理拓扑网络主要包含防火墙、交换机、服务器和主机等构件，这些构件与分区控制中心、智能主体库相结合，可以形成如图1所示的系统总体架构设计示意图。该系统各个模块如下：

(1)服务器控制中心模块。该模块在实际应用中需要根据控制中心相关协助问题对相关规则进行全面更新[6-8]。

(2)分区控制中心模块。该模块主要负责对某个区段网络的处理，确保各个网络主机能够稳定、安全地接收控制中心任务，并借助命令管辖主机，执行网络主机上报的相关任务[9-11]，以实现相关数据的全面化、完整化接收，并诊断信息监测数据是否出现异常情况。然后，选用合适的入侵特征模式，将异常数据安全、可靠地传输和存储到数据库中，便于工作人员及时向控制中心上报异常数据。

(3)网络主机模块。该模块作为一种重要的移动代理平台，为移动系统运行提供了良好的运行环境。当网络主机在处理疑似问题但自己却无法准确判断时，需要向分区控制中心反馈和传输相关数据，便于后期对相关数据的深层次分析和处理，从而确定系统主机是否遭受入侵行为。

(4)智能主体库模块。该模块在提高分布式入侵检测系统运行性能方面发挥了重要作用，在进行执行操作期间，该模块利用控制中心，对相关操作进行直接操控，从而形成新配置[12]，这有助于工作人员结合实际工作需求，有针对性地开展相关工作，以保证执行配置的科学性和合理性，同时，还能删除不必要的操作步骤。

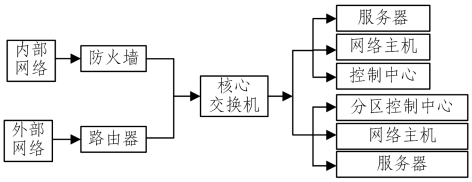

图1 系统总体架构

Fig. 1 Overall system architecture

2.2 系统数据库设计

系统数据库在增删改查数据、保证数据存储的安全性和可靠性方面发挥了重要作用。因此，在设计基于网络中心机房智能化管理系统期间，技术人员要重视对系统数据库的设计。另外，为了确保所设计的数据库能更好地满足数据的增删改查操作，现将数据库操作的封装类主要代码编写如下：

```
namespace NS_MYSQL
{
class CMySQL_Connector
{ public:
CMySQL_Connector(void);
~CMySQL_Connector(void);
public:
//打开连接
bool Open(const char * host,unsigned int port,const char * useL
const char * passwd,const char * db);
//断开连接
void Close(void);
//更新(增、删、改)
bool Update(const char * sql);
//查询
bool Query(CMySQL_RESULTSET * pResultSet. const char * sql);
//是否连接
bool IsConnected(void)const{return m_bConnected;)
private:
bool m bConnected;
MYSQL mysql;
}
}
```

3 系统硬件结构设计

在实际通信期间，多个智能主体之间主要运用了消息传递的方式。利用传递消息功能，可以实现互相通信。系统硬件结构设计示意图如图2所示。从图2可以看出，中心智能主体控制中心用到了大量的服务器，通过对受检测主机进行移动化管理和控制，可以及时、有效地接收和处理移动代理所提交的情况报告[13-15]，从而实现对报警信息的全面化获取。此外，还要处理下级无法判别处理的事务，确保入侵事件响应的及时性和有效性。此外，通过利用控制中心，可以实现对人机交互界面的完整化显示，并向指定的管理人员反馈和传输报告运行状态信息，并对相关警报行为进行及时响应和处理，便于系统及时接收和处理上级指令，使得报告运行状态信息得以有效改变。同时，将改变后的报告运行状态信息安全、可靠地传输到系统智能主题库中[16]，然后，工作人员对各个节点智能主体进行派遣和收回处理。特征库主要是指下层所传输的数据分析操作；响应库主要是指对入侵行为所产生的一系列反应，用以实现对下层智能主体的自动化管控。在实际运行监控期间，主机智能主体主要利用采集系统初步分析和过滤网络相关数据，从而筛选掉冗余数据，减轻系统运行负荷。不同系统间的层次主要起到了保护通信功能的作用，通过利用系统的各个层次，可以实现对重要信息数据的高效化、安全化传输和处理[17]。

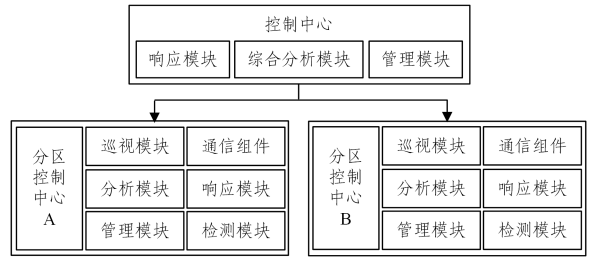

图2 系统硬件结构示意图

Fig. 2 System hardware structure diagram

3.1 系统主机设计

系统主机主要由探测器、控制库、响应库和通信模块等部分组成，系统主机结构设计示意图如图3所示。

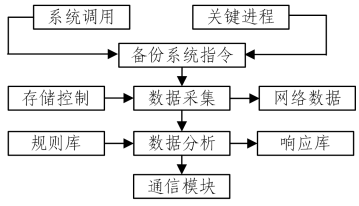

图3 系统主机结构示意图

Fig. 3 System master structure diagram

从图 3 可以看出，系统主机运行原理如下：首先，利用探测器实现对重要数据的全面化、完整化采集[18]，并在严格遵循控制管控原则的基础上，实现对主机数据的有效获取。其次，初步分析相关数据，将分析处理的数据进行匹配处理，一旦数据匹配成功，表明主机遭受了入侵行为，这表现出了较高的危险性。此外，还要严格按照设置好的响应规则，采取网络终端处理、预警处理等措施，向系统主机安全、可靠地传输所获取的最终数据。一旦系统主机无法准确地判断该行为是否存在异常[19]，则需要利用通信模块向智能主体传输相关数据，以便对后期数据进行深层处理，同时便于若干个主机智能主体能够安全、可靠地运行于每个主机上。

3.2　核心交换机设计

本文选用的核心交换机是 5720S-28P-AC-24 的网络核心交换机，该核心交换机主要由以下几个层次组成。

(1)接入层。接入层主要是指网络用户对网络层次进行直接或间接的访问，该层次与核心层之间连接的部分属于汇聚层。接入层的功能是负责将用户安全、可靠地连接到终端网络中。该层交换机接口具有高密度、低成本等特点。

(2)汇聚层。汇聚层作为核心交换机的重要层次，主要负责对重要数据的汇聚处理，利用该汇聚层可以高效化、科学化处理接入层数据，然后将结果安全、可靠地传输到上行链路中。

(3)核心层。核心层属于网络的核心组成部分，该部分除了可以实现对通信数据的传输和共享外，还可以向骨干结构传输相关数据，使交换机的数据吞吐量得以大幅度提高，为确保分布式入侵检测系统能正常、稳定、安全地运行创造了良好的条件。

3.3　报警响应器设计

当系统借助报警功能对图像进行调用时，技术人员要选用型号为 AD2032 的报警响应器，对外来入侵行为进行全面监视。所有报警响应器均用到了 32 个大小相同的继电器，16 个继电器为一组。单组摄像机地址需要操作人员手动设置，报警器型号及设置如表 1 所列。

表 1　报警器型号及设置

Table 1　Alarm model and settings

报警器	A	B	C	D	E
1－15	0	0	0	0	0
16－30	0	0	0	0	0
31－45	0	0	0	0	0
46－60	0	0	0	1	1

注：0 代表 OFF；1 代表 ON

3.4　信息检测器设计

本文所选用的信息检测器是型号为 V1.2 的绿色电脑信息检测器，该检测器具有重量轻、配置科学等特点。电脑信息检测器如图 4 所示。

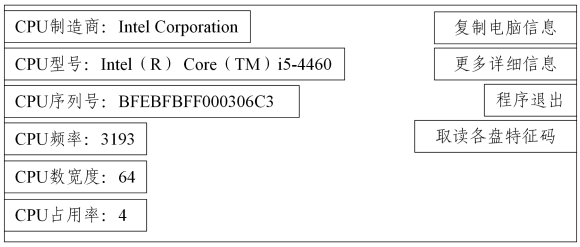

图 4　电脑信息检测器 v1.2

Fig. 4　Computer information detector v1.2

该检测器主要用于显示电能主机多个领域的重要信息数据，表现出协助超频能力强、检测性能高等特点，为实现系统驱动磁盘的全面化、科学化评估打下坚实的基础。

4　系统软件设计

由于智能主体所对应的操作对象与主机之间相互独立，与各个操作系统之间保持完全分离的状态，因此，所分析的重要数据主要来自系统主机的智能主体；同时，分析数据模块主要负责对主机智能主体所发送的数据进行全面化、深入化的分析和处理，而这一功能的实现离不开系统软件的设计，因此，加强对系统软件的科学设计显得尤为重要。

4.1　智能主体移动分析

本节主要介绍该系统中的各个智能主体主要用到的通信机制。

4.1.1　各个智能主体间的通信功能

主要利用 Message 对象进行实现，该对象主要包含消息发送功能和消息处理功能；此外，该对象还含有消息队列，该队列主要用于存储所接收的消息。

4.1.2　通信消息格式和通信协议

在整个分布式入侵检测系统中，要在参照入侵检测交换协议的基础上，利用设计好的 IDMEF 入侵检测消息交换格式和 IDXP 入侵检测交换协议，制定和完善相关通信机制。其中，在利用 IDMEF 入侵检测消息交换格式期间，通过选用合适的对象，科学地定义和设计入侵检测数据模型，同时，结合不同检测组件之间的相互作用，完成对不同警报消息的统计。此外，还要精确化、详细化描述控制命令和配置信息等通信数据。另外，还要在结合 XML 相关文件的基础上，利用 ID-MEF 消息格式对数据模型进行精确化描述和实现。在使用 IDXP 入侵检测交换协议期间，要利用分布式入侵检测系统内部的智能主体，不断提高该交换协议的通信能力。IDXP 入侵检测交换协议的应用目的是全面化入侵检测各个实体间的应用层协议，确保非结构文本信息和二进制数据之间能够有效地交互和利用。为了确保各安全特征信息能够有效地融合，技术人员要确保 IDXP 入侵检测交换协议完整性高、保密性强、认证方便。

以智能主体为基础的移动过程如图 5 所示。

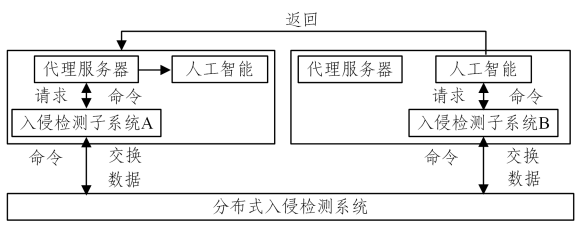

图 5　以人工智能为基础的移动过程图

Fig. 5　Diagram of AI-based mobile process

从图 5 可以看出，在进行检测期间，利用入侵检测子系统 A 可以获得异常信息，其由于自身机体存在一定的局限性，造成该子系统无法对异常信息进行正确、精确地判断。此时，代理服务器会在第一时间发出大量的服务信号，通知和调用多个代理模块，及时处理和分析信号。然后，将最终处理结果安全、可靠地传输到入侵检测子系统 B 中，并指派专门的代理负责执行相关操作，只有这样，才能实现对异常信息的高效化、及时化处理。最后，代理服务器将最终处理结果反馈和传输到

主机 A 中，从而实现对子系统 A 处理能力的有效检测。

4.2 入侵检测流程设计

当分布式入侵检测系统正式运行后，需要将初始化工作全部执行完毕，并对口令进行解释，以实现对系统规则数据库的全面化、精确化读取，从而形成相应的二维规则链表，确保最终检测入侵操作的规范性和合理性。接着，循环执行抓包、规则匹配等相关操作。入侵检测流程如图 6 所示。

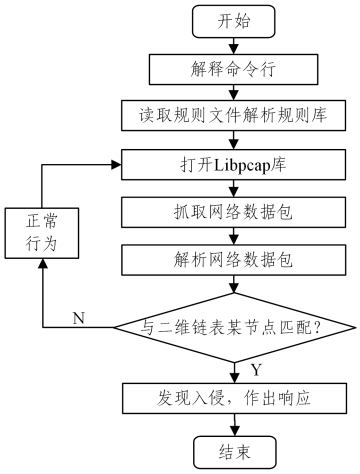

图 6 入侵检测流程

Fig. 6 Intrusion detection flow

5 系统测试

为了更好地验证分布式入侵检测系统的稳定性和有效性，现利用 NS2 网络仿真软件，对该系统的运行性能进行全面的仿真测试，同时，还要严格按照所设置的攻击次数，科学地测试系统的检测准确率。另外，为了实现对入侵攻击方式的科学化、真实化模拟，测试人员要优先选用 flooding 攻击方式，该攻击方式属于典型的 DoS(拒绝服务)攻击方式，利用该方式，可以向目标节点安全、可靠地发送非正常数据包。此外，还要结合 IDS 数据包的尺寸，对正常和非正常的数据包进行科学改变，从而实现对不同类型数据包的有效区分，这样才能对分布式入侵检测系统运行性能是否良好、稳定进行有效测试。

5.1 攻击环境与参数设置

为了实现对分布式入侵检测系统性能的科学验证，本文利用网络技术对入侵检测实验进行模拟，然后将分布式入侵检测系统安装和部署在某大学校园的两处位置，以开展系统测试工作。首先，机房 1 属于实训楼所在区域的管控中心，在机房 1 中安装和部署 1 台监控服务器和若干台主机。其次，将机房 2 和机房 3 均安装在各个楼层中，将 1 台监控服务器和若干台主机均陈列在各个机房中，借助交换机，确保监控服务器与各个主机之间建立良好的互联关系。此外，还要将各个机房内的路由器进行有效地连接，校园网内部通常会用到 TCP/IP 网段。本次测试实验主要用到了两种布局环境：一种是将该实验选定在五楼的机房 2 与机房 3 之间；另一种布局环境是将该实验选定在六楼机房 1 中，同时，将主控台运行于机房 1 的主服务器上，并利用机房 2 和机房 3 中的两台服务器，确保人工智能运行水平。最后，从以上 3 个机房中，将主机 A、主机 B、主机 C、主机 D 统一设置为攻击主机，主机 E 负责主动发起攻击，通过使用主机 C 与主机电子工程，可以更好地协助该系统进行拓展性实验。参数设置如表 2 所列。

表 2 参数设置

Table 2 Parameter settings

设备	操作系统	IP	CPU 内存	以太网卡
参数	Win8	202.112.14.123	512 MB	100 Mbps

当攻击发起机向主机发送和传输相关数据时，通常会用到表 3 所列的攻击发起机发送的数据包。

表 3 攻击发起机发送的数据包

Table 3 Data packet sent by attack initiator

服务器和客户端连接：Socket[addr=/192.168.1.3]建立连接	
攻击发起机 1	1 个数据包
攻击发起机 2	2 个数据包
攻击发起机 3	3 个数据包
攻击发起机 4	4 个数据包
攻击发起机 5	5 个数据包
攻击发起机 6	6 个数据包
攻击发起机 7	7 个数据包
攻击发起机 8	8 个数据包
攻击发起机 9	8 个数据包
攻击发起机 10	10 个数据包
服务器关闭连接完成	

5.2 系统测试结果与分析

结合上述内容，本文采用伪装入侵检测的方式，全面地检测样本测试数据，数据采样序列的幅频表现如图 7 所示。从图 7 可以看出，数据采样序列通常表现出一定的规律性，当客户端数量为 10 时，数据采样序列所对应的波动范围为 $-1\sim1$，实现了对入侵行为的全面化检测。

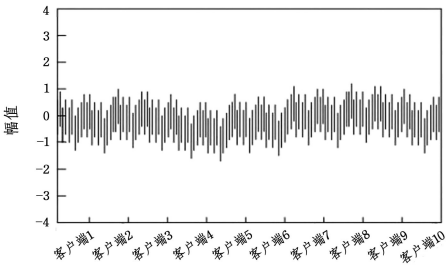

图 7 数据采样序列的幅频特性

Fig. 7 Frequency-domain performance of sampling sequence

客户端所发送的 TCP 数据包主要包含以下两种类型：一种是将前 5 个客户端设置为 S1，另一种是将后 5 个客户端设置为 S2。利用 IDA 系统和基于人工智能(Agent)分布式入侵检测系统全面化地检测分布式入侵行为，其检测结果如图 8 所示。

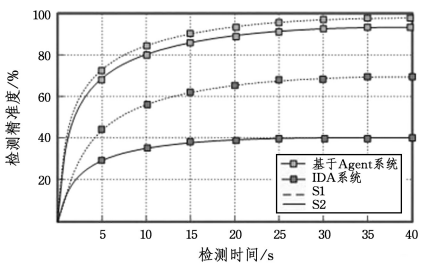

图 8 两种系统检测精确度对比分析

Fig. 8 Comparative analysis of detection accuracy of two systems

从图 8 可以看出，对于以上两种系统而言，随着检测时间的不断延长，其检测精准度也出现了明显的变化。对于 IDA 系统而言，当前 5 个客户端被入侵攻击时，通过利用自身的检测功能，可以实现对异常情况的及时、高效检测；当检测时间达到 40s 时，检测精准度较高，达到了 70%，但是，当后 5 个客户端被入侵攻击时，由于自身的检测功能缺乏一定的完善性，其精确度在 25s 检测时间内并没有出现明显的提升，从 25～40s 这一检测时间段内，IDA 系统的检测精确度相对较低，始终保持在 40%。对于基于人工智能（Agent）的分布式入侵检测系统而言，当前 5 个客户端被入侵攻击时，其检测精确度最高，达到了 99%，当后 5 个客户端被入侵攻击时，其检测精确度仍然保持在较高的状态，高达 95%。这说明利用本文所设计的分布式入侵检测系统可以获得较高的检测精确度，表明本文提出的系统设计方案具有较高的科学性和合理性。

结束语　在人工智能技术的应用背景下，本文设计的分布式入侵检测系统具有运行稳定、功能完善、实用性强等特点，有效地提高了检测精确度，使得检测精确度最高达到 99%。因此，该系统设计和实现工作取得了圆满成功，其系统应用价值和应用前景得以显著提升，值得被进一步推广和应用。但是，由于受到实际条件的限制，该系统的诸多问题还有待进一步处理。在后期的工作实践和研究中，我们将继续探讨人工智能的智能性和协作性，将人工智能技术更好地应用到分布式入侵检测系统中，大幅度提高升系统的灵活性、动态迁移性。

参 考 文 献

[1] ALLADI T, KOHLI V, CHAMOLA V, et al. Artificial Intelligence(AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles[J]. IEEE Wireless Communications, 2021, 28(3): 144-149.

[2] ZEBIN T, REZVY S, LUO Y. An Explainable AI-Based Intrusion Detection System for DNS Over HTTPS(DoH) Attacks [J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2339-2349.

[3] CHEN X A. Research on the intrusion detection system of computer network[J]. Electronic Test, 2021(18): 76-77, 73.

[4] ZHONG W, YU N C. Applying big data based deep learning system to intrusion detection[J]. Big Data Mining and Analytics, 2020, 3(3): 181-195.

[5] LU L, SUN Y E, HUANG H, et al. Detection of persistent elements in distributed monitoring system[J]. Journal of Computer Research and Development, 2020, 57(5): 1046-1056.

[6] TANJ A, GUAN J F. Distributed intrusion detection system of networks based on artificial bee colony algorithm[J]. Computer Applications and Software, 2019, 36(3): 326-333.

[7] CHENG W Z, ZHANG L. Talking about distributed intrusion detection system[J]. Sci-Tech & Development of Enterprise, 2018(7): 93-94.

[8] HONG B, CAO Z J. Design and implement of distributed intrusion detection system based on Hadoop[J]. Journal of Xi'an Technological University, 2018, 38(4): 390-395, 407.

[9] WANG X Y. Design of temporal sequence association rule based intrusion detection behavior detection system for distributed network[J]. Modern Electronics Technique, 2018, 41(3): 107-110.

[10] LI H. Research on hybrid architecture for distributed intrusion detection system in wireless network[J]. Techniques of Automation and Applications, 2018, 37(5): 52-55, 60.

[11] CHOI I, LEE J, KWON T, et al. An Easy-to-use Framework to Build and Operate AI-based Intrusion Detection for In-situ Monitoring[C]// 2021 16th Asia Joint Conference on Information Security(AsiaJCIS). 2021: 1-8.

[12] ALI M, HU Y F, LUONG D K, et al. Adversarial Attacks on AI based Intrusion Detection System for Heterogeneous Wireless Communications Networks[C]// 2020 AIAA/IEEE 39th Digital Avionics Systems Conference(DASC). 2020: 1-6.

[13] LI X. Research and implementation of intrusion detection system based on spark [D]. Taiyuan: Shanxi University, 2021.

[14] ZHANG S S. Design and implementation of security intrusion detection system based on software definition [D]. Hangzhou: Zhejiang University, 2020.

[15] HU B. Distributed vulnerability emergency detection system [D]. Chengdu: University of Electronic Science and Technology, 2020.

[16] GAO Y, LIU Y, JIN Y, et al. A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System[J]. IEEE Access, 2018, 6: 50927-50938.

[17] ZHANG W X. Design and implementation of intrusion detection system based on improved cann algorithm [D]. Xi'an: Xi'an University of Electronic Science and Technology, 2019.

[18] LI J, ZHAO Z, LI R, et al. AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 2093-2102.

[19] HE J P, LUO L, XIAO K, et al. Framework intrusion detection system based on feature distribution and AI[J]. Application Research of Computers, 2021, 38(9): 2746-2751.

WANG Lu, born in 1980, master, associate professor. Her main research interests include artificial intelligence, power electronics and control engineering.

（责任编辑：何杨）