文章编号:1671-4598(2023)02-0237-06 DOI:10.16526/j.cnki.11—4762/tp.2023.02.037 中图分类号:TP391 文献标识码:A

基于物联网的异构传感数据入侵风险识别方法

戴建东[1]，戴昊洋[2]
(1.南京理工大学 科学与工程学院，南京 210094；
2.新加坡南洋理工大学 数理科学学院，新加坡 639798)

摘要：异构传感数据入侵风险识别过程中未对采集的异构传感数据进行融合处理，导致数据入侵风险识别完整性较差，为此，引入物联网技术，提出一种新的异构传感数据入侵风险识别方法；根据物联网的组成层次，构建物联网结构模型；依据不同网络入侵攻击类型，设置风险类型识别标准；在物联网结构模型下，采集异构传感数据，得出初始数据的融合处理结果；从传感数据结构以及数据时域变化两个方面，提取异构传感数据特征，计算入侵风险值；最终输出可视化的异构传感数据入侵风险等级以及类型的识别结果；实验结果表明，设计识别方法的风险值识别误差降低了0.015，风险类型识别正确率提高了1.6%，且风险识别方法的响应时间更短，即优化设计的入侵风险识别方法在精度和时效性两个方面更加具有优势。

关键词：物联网；异构数据；传感数据；入侵风险识别

Intrusion Risk Identification Method of Heterogeneous Sensor Data Based on Internet of Things

DAI Jiandong[1], DAI Kimi[2]
(1. School of Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China;
2. School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 639798, China)

Abstract: Aimed at the process of heterogeneous sensor data intrusion risk identification, the collected heterogeneous sensor data is not fused, which leads to the poor integrity of data intrusion risk identification. Therefore, By introducing Internet of things technology, a new method of heterogeneous sensor data intrusion risk identification is proposed in this paper. According to the composition level of Internet of things, the structure model of Internet of things is built. According to the different types of network intrusion attacks, the risk type identification standards is set up. Under the structure model of Internet of things, the heterogeneous sensor data is collected and the fusion processing results of the initial data is acquired. From the two aspects of sensor data structure and data time-domain change, the characteristics of heterogeneous sensor data are extracted, and the intrusion risk value is calculated. Finally, the visual recognition results of heterogeneous sensor data intrusion risk level and type are output. The experimental results show that the risk value identification error of the design identification method is reduced by 0.015, the accuracy of risk type identification is increased by 1.6%, and the response time of the risk identification method is shorter, that is, the optimized intrusion risk identification method has more advantages in the accuracy and timeliness.

Keywords: internet of things; heterogeneous data; sensing data; intrusion risk identification

0 引言

网络入侵指的是黑客或非法用户通过网络对用户机进行远程操控或破坏的访问行为，在动态网络技术不断发展的大背景下，大量的网络入侵攻击事件频繁发生，不仅干扰了网络的安全性与稳定性，同时也降低了网络数据的完整性与正确性[1]。据不完全统计，物联网环境入侵事件占全部网络入侵事件的74%左右，直接给物联网异构传感数据的传输与存储产生负面影响。物联网是以传输协议作为约束条件，利用信息传感器设备将任意物体连接到互联网中，实现设备的智能化识别、定位、监控和管理的一种网络。在物联网环境下，异构传感数据的质量直接决定了物联网控制任务的执行效率，为了降低网络入侵事件对物联网中异构传感数据造成的破坏，提出入侵风险识别方法。

入侵风险识别是一种主动的网络防御机制，它通过对数据、信息、网络行为的监测，识别破坏网络的机密性和完整性的入侵行为，并对可能发生的入侵事件进行报警，从而达到对网络的安全防护。入侵风险识别是网络安全的第二道防线，它是一种有效的防范措施，进一步提升了网络的安全防护水平。目前发展较为成熟的网络数据入侵风险识别方法大多使用了深度学习网络、贝叶斯攻击图以及

收稿日期:2022-07-13； **修回日期**:2022-08-04。
作者简介:戴建东(1972-),男,江苏泰州人,硕士研究生,经济师,主要从事物联网、区块链、大数据和人工智能方向的研究。
引用格式:戴建东,戴昊洋.基于物联网的异构传感数据入侵风险识别方法[J].计算机测量与控制,2023,31(2):237-242.

粒子群算法优化深度极限学习机回归算法（PSO-ELM，particle swarm optimization-extreme learning machine）算法，然而现有的异构传感数据入侵风险识别方法主要针对的是通信网络，将其应用到物联网环境中存在识别效果不佳的问题，主要体现在识别精度低、识别结果时效性低等方面，其主要原因是物联网中传输的数据均为异构数据。为此面向物联网环境对异构传感数据入侵风险识别方法进行优化，以期能够为物联网异构传感数据的安全传输与存储提供有效的辅助工具。

为此，本文提出一种基于物联网的异构传感数据入侵风险识别方法，有效降低识别方法的风险值识别误差，提高风险类型识别正确率，缩短风险识别方法的响应时间。

1 异构传感数据入侵风险识别方法设计

由于各种网络攻击方式具有相似的数据变化特征，因此可以通过分析异构传感数据特征的方式进行入侵风险识别[2]。优化设计的异构传感数据入侵风险识别方法大体包括 3 个阶段，分别为采集、学习和动态优化，并得出包括入侵风险等级、风险类型以及风险位置的识别结果。

1.1 构建物联网结构模型

根据物联网的层次组成可以将其分为感知层、接入网络层、中间件层等部分，组成的物联网结构如图 1 所示。

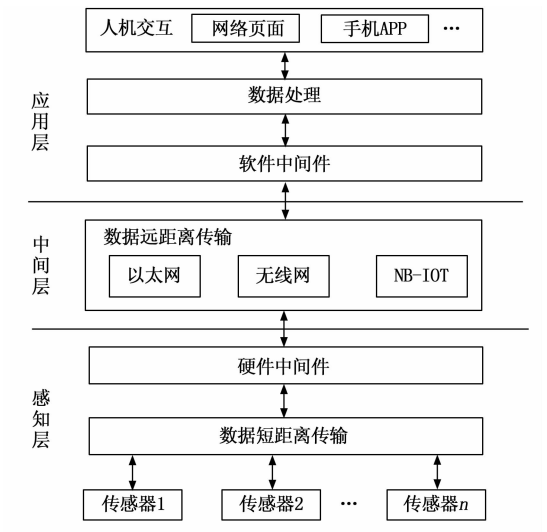

图 1 物联网结构架构图

其中，大部分的物联网感知层都是由普通节点、簇头节点和汇聚节点构成的分簇结构。由基站将物联网的感知层和网络层连接起来，将感知层所收集到的信息传输到传统的网络中，从而完成对数据的远程采集和控制[3]。中间件层的功能主要包括数据存储、异构数据检索、数据挖掘和隐私保护等。而接入网络层的基本理念就是以已有的互联网为主要的传输与分享载体的交换平台。按照上述结构对组成物联网的硬件设备进行连接，完成物联网结构模型的构建。

1.2 物联网异构传感数据入侵类型与标准特征

物联网异构传感数据面临多种类型的入侵攻击，具体的入侵攻击类型及其攻击原理如表 1 所示。

表 1 物联网异构传感数据入侵攻击类型说明表

入侵攻击类型编号	入侵攻击名称	入侵攻击方式
1	欺骗入侵攻击	从可信地址伪造数据包，使计算机认证其他计算机
2	主机模拟入侵攻击	攻击者利用其它结点的标识和许可来攻击，以消耗他们的资源或扰乱正常的网络操作
3	信息泄露入侵攻击	攻击者尝试捕捉和处理某些发送的无线信号数据
4	拒绝服务入侵攻击	通过使用有限的网络、操作系统或应用程序，导致计算机或网络不能正常运行而不能提供正常的服务
5	暴力入侵攻击	使用数字、字母和字符的组合，推测用户名称和密码，重复尝试访问
6	干扰入侵攻击	攻击者通过对程序终端的物联网业务进行干扰，利用损坏的节点来传输无效的数据，导致网络中的数据库冲突
7	槽洞攻击	攻击者通过破坏节点，试图诱使特定区域的网络流量经过受损节点，形成一个以攻击者为核心的“黑洞”

以欺骗入侵攻击类型为例，攻击者必须先确认目标的位置，然后关掉伪装的宿主，或者让宿主沉睡，然后伪造宿主的位置，再用假宿主的身份与宿主进行联系，最终确定宿主的编号[4]。在完成这个步骤时，攻击者必须将一个连接请求发送给一个目标主机，这个主机用一个序列号来回应，攻击者记录序列号后关闭链接，并利用该序列号用来进行身份验证。同理可以得出其他网络入侵攻击类型的作用过程，得出不同类型入侵攻击作用下，网络流量与异构传感数据的变化特征，以此作为识别当前异构传感数据入侵风险的比对标准[5]。

1.3 物联网异构传感数据采集与融合处理

采用周期性数据采集模式，利用物联网中的传感器设备进行实时异构传感数据的采集，数据采集模式如图 2 所示。

根据配置进行周期性的数据采集，再经过初步融合、清洗等处理，最终将处理后的数据作为报文的形式传送给报文队列[6]。为保证不同传感器产生异构数据之间的计算，需要对初始异构数据进行归一化处理，处理结果可以表示为：

$$x_{\text{Unify}} = \frac{x-\mu}{\sigma} \tag{1}$$

式（1）中，x 和 x_{Unify} 分别为归一化处理前后的传感数据，μ 和 σ 对应的是初始采集数据的平均值和标准差[7]。在此基础上对统一结构的传感数据进行融合处理，采用动态

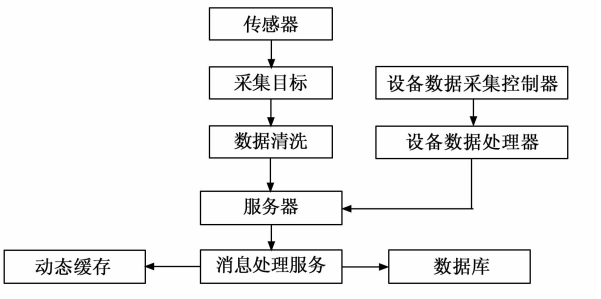

图 2　异构传感数据采集模式图

的融合方式利用式（2）计算任意两个传感数据之间的相似度。

$$Sim(x_i,x_j)=\sqrt{|x_i-x_j|^2} \tag{2}$$

若式（2）的计算结果低于设置阈值，则直接对传感数据 x_i 和 x_j 进行融合处理，否则需要重新对该数据进行规范化处理，最终得出的数据融合结果满足如下关系式：

$$\frac{\sum_{i=1}^{N}X_i}{N}\in[x_{\min},x_{\max}] \tag{3}$$

其中：X_i 为物联网异构传感数据的融合处理结果，N 表示融合传感数据的数量，$x_{\min}$ 和 $x_{\max}$ 分别为初始采集数据中的最小值和最大值。重复上述步骤，直到采集的所有物联网异构传感数据均融合完成为止。

2　异构传感数据入侵风险识别

2.1　提取物联网异构传感数据特征

为实现对物联网异构传感数据入侵风险的识别，首先需要以采集并处理的物联网异构传感数据为基础，分别从实时数据以及数据变化两个方面，提取数据特征[8]。设置的实时异构传感数据特征参数包括传感数据流量、互联网协议（TCP，transmission control protocol）连接数、上下行流量差异等，以传感数据流量为例，该特征参数的提取结果可以表示为：

$$\tau_{\text{flow}}=\sum_{i=1}^{n_{\text{channel}}}\lambda_{\text{send}-i}\times d\times l_{\text{occupy}} \tag{4}$$

式（4）中，变量 $\lambda_{\text{send}-i}$ 为 i 信道中的发送数据量，该变量的具体取值由传感器设备决定，d 为物联网的信道带宽，l_{occupy} 表示当前物联网异构传感数据传输占用的信道数量[9]。由于多个不同的传感器设备都在同时进行不同的 TCP 连接，因此，流量特征参数可采用建立和拆除 TCP 连接时通信的特定报文的数量来进行标识，即 TCP 连接数特征参数的提取结果可以表示为：

$$\tau_{\text{TCP}}=\frac{1}{3}\times\frac{\chi_{\text{FIN}}+\chi_{\text{RST}}+\chi_{\text{SYN}}}{2} \tag{5}$$

式中，χ_{FIN}、χ_{RST} 和 χ_{SYN} 分别表示的是 FIN（FINish）报文、RST（ReSeT）报文以及 SYN（synchronize sequence numbers）报文的数量。物联网环境中安装了多个主机和传感器设备，各个设备的网络行为均不一致，上传和下载方式也会有不同，多个传感数据流量合并后，总的上、下的差别会有不同程度的减小，所以一般情况下，不同类型的物联网异构传感数据之间的数据流会有很小的差别[10]。因此可以利用网络的上下行流量之间的差值和总的网络流量的比例来表示上下行流量差异特征参数。从物联网异构传感数据变化情况来看，可设置异构传感数据信息熵和信息增益特征参数来反映数据的时域变化特征，提取结果如下：

$$\begin{cases}\tau_{\text{entropy}}=-\sum_{i=1}^{n}I^2(x_i)\\ \tau_{\text{gain}}=-\sum_{i=1}^{i}\frac{|D_i|}{|D|}\log_2\frac{|D_i|}{|D|}\end{cases} \tag{6}$$

其中：$I(x_i)$ 代表任意时刻采集的异构传感数据总量，$|D_i|$ 和 $|D|$ 分别对应的是传感器 i 采集的样本数以及样本所含的总数[11]。整合提取的所有物联网异构传感数据的特征提取结果，得出数据综合特征记为 τ_z。

2.2　计算物联网异构传感数据入侵风险值

根据物联网异构传感数据的特征提取结果，从入侵攻击强度和入侵攻击概率两个方面进行入侵风险值的计算。根据非法用户的入侵攻击目标，可以将入侵攻击强度分为节点入侵、主机入侵和网络入侵 3 个部分，其中节点入侵攻击强度是物联网中的某个节点遭受入侵攻击及其所造成的影响，物联网中任意一个节点 v 的入侵攻击强度计算公式如下：

$$\beta_{\text{node}}(v)=CF(v)\cdot cost(v) \tag{7}$$

式中，变量 $CF(v)$ 和 $cost(v)$ 分别表示的是物联网节点 v 的入侵攻击信度以及攻击损失，其中变量 $cost(v)$ 的具体取值与物联网异构传感数据的信息增益特征有关[12]。同理可以得出物联网中主机入侵攻击和网络入侵攻击的攻击强度计算结果：

$$\begin{cases}\beta_{\text{host}}(w)=\sum_{c\in cNode(w)}\beta(c)\\ \beta_{\text{net}}(H_{\text{target}})=\sum_{h\in H_{\text{target}}}\beta_{\text{host}}(h)\end{cases} \tag{8}$$

其中：$\beta(c)$ 表示的是物联网中主机节点 c 的攻击强度值，$cNode(w)$ 表示物联网主机设备上节点组成的集合，另外 $\beta_{\text{host}}(h)$ 为物联网中主机设备 h 的攻击强度，H_{target} 为物联网中主机集合[13]。入侵攻击概率是一个定量的衡量物联网异构传感数据受到攻击可能性的量化指标，根据层次的不同可以将入侵攻击概率分为节点、主机和网络入侵攻击概率 3 个部分，具体的计算结果可以表示为：

$$\begin{cases}P_{\text{node}}(v)=\Pr(v=True\mid G,T)\\ P_{\text{host}}(w)=1-\prod_{c\in cNode(w)}(1-P_{\text{node}}(c))\\ P_{\text{net}}(H_{\text{target}})=1-\prod_{h\in H_{\text{target}}}(1-P_{\text{host}}(h))\end{cases} \tag{9}$$

式（9）中，$\Pr(v)$ 表示的是物联网攻击的所有节点集合，G 和 T 分别为攻击收益和入侵威胁状态变量，$P_{\text{host}}(w)$ 和 $P_{\text{net}}(H_{\text{target}})$ 分别为主机入侵概率和网络入侵概率的计算结果，参数 $cNode(w)$ 和 H_{target} 与式（8）相同[14]。最终

将物联网异构传感数据入侵攻击强度和概率的计算结果代入到式（10）中，得出入侵风险值的计算结果。

$$\text{Risk} = \sum P_i(v)\beta_i(v) \tag{10}$$

式中，i 取值为 node、host 和 net。由于物联网异构传感数据处于动态变化的状态，因此在入侵风险值计算过程中需要风险值计算结果的时效性。

2.3 实现异构传感数据入侵风险识别

依据物联网异构传感数据的特征提取结果以及风险值计算结果，从风险等级、风险类型以及入侵位置 3 个方面得出风险识别结果。

2.3.1 入侵风险等级识别

将物联网异构传感数据的入侵风险划分成 4 个等级，风险等级的划分标准如表 2 所示。

表 2 入侵风险等级划分标准

入侵风险等级	入侵风险值	入侵攻击强度	入侵攻击概率
I	[0.35,0.45]	[0.4,0.5]	[20%,100%]
II	[0.25,0.35]	[0.3,0.4]	[10%,20%]
III	[0.15,0.25]	[0.2,0.3]	[5%,10%]
IV	[0.05,0.15]	[0.1,0.2]	[1%,5%]

将物联网异构传感数据入侵风险的计算结果与表 2 中的数据进行对比，若无法通过风险值直接识别风险等级，可以结合入侵攻击强度和概率确定当前物联网的入侵风险等级[15]。

2.3.2 入侵风险类型识别

通过计算不同入侵攻击类型设置特征与实时异构传感数据提取特征之间的匹配度，确定当前物联网的入侵风险类型，具体的识别过程如图 3 所示。

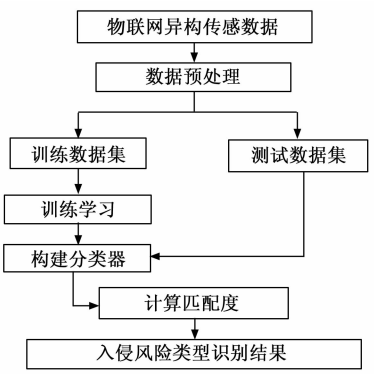

图 3 物联网异构传感数据入侵类型识别流程图

从图 3 中可以看出，异构传感器数据入侵类型识别包括训练和测试两个阶段，训练阶段主要通过设置的入侵类型特征标准构建分类器，依据建立的分类器运用提取的异构传感数据特征划分实时异构传感数据的入侵类型[16]。构建分类器的分类函数如下：

$$G(x) = \text{sign}\left(\sum_{i=1}^{M}\alpha_i L_i(X)\right) \tag{11}$$

其中：$L_i(X)$ 为弱学习器函数，α_i 表示的是 $L_i(X)$ 的组合权重，M 表示设置分类器的数量[17]。将提取的物联网异构传感数据特征与设置的入侵标准特征导入到分类器中，得出匹配度输出结果：

$$Sim(x) = \sqrt{\left|\tau_{\text{set}} - \tau_z\right|^2} \tag{12}$$

将式（12）的计算结果按照降序顺序排列，匹配度最高的入侵攻击类型即为当前物联网异构传感数据入侵风险类型的识别结果。

2.3.3 异构传感数据入侵风险识别结果可视化输出

经过入侵风险识别若确定物联网存在入侵风险，且风险等级达到 I 级和 II 级，则需启动告警程序，将相关的入侵信息上传给物联网服务器以及各个终端[18]。比较物联网上各个节点传感数据的相似度，判定数据异常节点为物联网的入侵节点，确定该节点的作为入侵 IP 地址。最终将包含入侵风险等级、入侵类型以及入侵位置的识别内容以可视化的形式输出。

3 实验分析

为了验证优化设计的基于物联网的异构传感数据入侵风险识别方法的有效性与可行性，通过模拟网络入侵的方式，测试设计入侵风险识别方法的运行性能，并通过与传统识别方法的对比，体现出设计方法的识别性能优势。

3.1 配置物联网实验环境

选择某个自动化生产工厂作为实验环境，在该环境下构建并配置物联网环境。分别安装服务器、路由器以及网关设备，部署一个消息队列遥测传输协议（MQTT，message queuing telemetry transport）代理，代理基于 Eclipse Mosquitto v1.6.2 实现。与路由器直接相连的有 13 个不同类型的传感器，分别为温度传感器、湿度传感器、光照强度传感器、烟雾传感器、机床启动状态传感器、声音强度传感器、加工刀具运动信息传感器等，由于传感器采集的数据内容不同，因此不要求传感器生产厂家与型号的统一性[19]。将实验环境中安装的传感器设备设置成不同的 IP 地址作为唯一表示，并将所有的传感设备调整至启动状态。构建物联网实验环境的覆盖面积为 500 m * 500 m，图 4 表示的是实验配置物联网环境的拓扑结构。

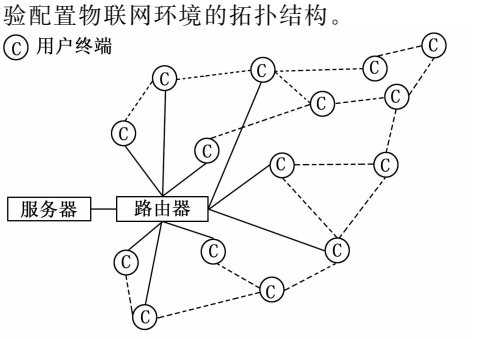

图 4 实验研究物联网拓扑结构图

为方便物联网异构传感数据的采集，需要在实验环境中安装一个采集器设备，要求该设备支持物联网的受限制的应用协议（CoAP，the constrained application protocol）通信传输协议，数据采集器通过节点和通信参数来配置网络方案，具体设置参数包括节点 IP 地址、监听端口等[20]。此外，实验环境中还配置了两个计算机设备，一个作为异构传感数据入侵风险识别方法运行的硬件支持，另一个设置为恶意节点，用来发动入侵攻击。

3.2　编写物联网入侵攻击程序

安装的恶意计算机具有强大的储存与备份能力，所以可以设置并支持多个数据的入侵攻击程序，当攻击者取得网络管理权限后，便可以将其重定向到此 web 服务器以下载相关的恶意软件二进制文件。为了更好地反映实际的攻击场景，将物联网异构传感数据与恶意计算机分在不同的子网中，为了保证网络覆盖足够多的恶意行为。实验分别设置高级长期威胁（APT，advanced persistent threat）入侵攻击、欺骗入侵攻击、主机模拟入侵攻击、暴力入侵攻击等多种不同类型的入侵攻击，并利用编码工具将入侵攻击模式转换成计算机可以直接运行的程序代码。为了保证攻击程序的可控性，在编写程序时加入两个强制控制指令，实现对攻击程序的控制，并保证同一时间物联网不会受到两种入侵程序的攻击。在实验过程中，分别记录入侵攻击程序的运行状态，以此作为判定设计方法入侵类型识别结果的比对标准。

3.3　准备物联网异构传感数据样本

利用物联网环境中的传感器设备获取实验使用的数据样本，数据样本大体可以分为两种类型，一种为无入侵攻击下的异构传感数据，另一种为存在入侵攻击的异构传感数据，其中正常数据样本 19 454 条，数据大小约为 30.5 GB，入侵数据样本共 43 346 条，数据大小约为 52.3 GB，每条异构传感数据样本均包含 41 位属性和一位标签。受到实验平台存储空间的限制，从数据集选择 6 000 个样本作为初始训练集，并从每个标签中选择一定数量的数据，以确保训练集合的代表性。将其余数据平均分成 8 组，采用多次实验求平均值的方式，得到可信度较高的实验结果。

3.4　描述性能测试实验过程

在实验环境中硬件设备调试成功的前提下，将优化设计的异构传感数据入侵风险识别方法转换成程序代码，导入到主测计算机中。启动入侵风险识别程序，并逐一代入准备的异构传感数据样本，得出入侵风险识别结果，如图 5 所示。

按照上述方式可以得出物联网任意时间段的入侵风险识别结果。为了体现出优化设计方法的性能优势，实验设置传统的基于深度学习网络的物联网入侵识别方法作为实验的对比方法，两种识别方法采用相同的开发程序进行代码转换，且运行环境与处理数据样本均相同，以此来保证实验变量的唯一性。

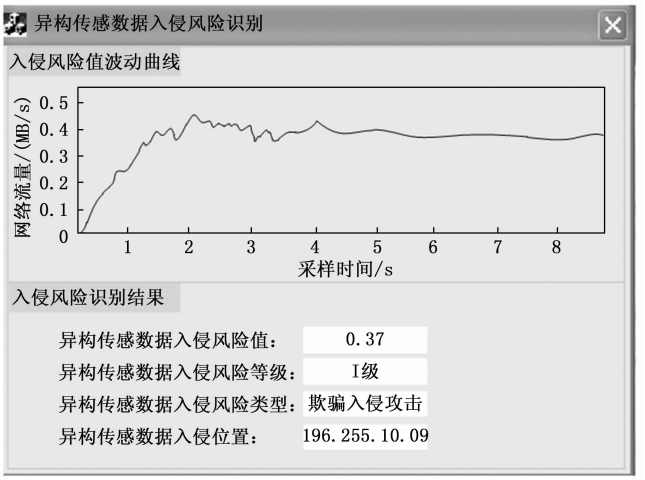

图 5　物联网异构传感数据入侵风险识别结果

3.5　设置识别性能量化测试指标

此次实验分别从异构传感数据入侵风险识别的识别精度性能和识别结果的时效性能两个方面进行测试，入侵风险识别精度性能越优，为物联网入侵防御工作提供数据的价值越高，越有利于提高物联网的安全性。从识别结果的时效性方面来看，异构传感数据入侵风险的快速识别，能够为入侵防御工作的建设提供充足的空间，因此识别结果时效性越高对于物联网的运维越有利。此次实验分别设置风险值识别误差和风险类型识别正确率两个指标来反映识别方法的精度性能，其中入侵风险值识别误差的数值结果为：

$$\varepsilon_{\text{risk}} = \left| Risk - Risk_{\text{act}} \right| \tag{13}$$

其中：$Risk$ 和 $Risk_{\text{act}}$ 分别为物联网异构传感数据入侵风险的计算值和实际值，$Risk$ 可通过式（10）直接计算得出，$Risk_{\text{act}}$ 的具体取值由编写的攻击程序决定。风险类型识别正确率指标的测试结果可以表示为：

$$\eta_{\text{correct}} = \frac{Num_{\text{correct}}}{Num_{\text{all}}} \times 100\% \tag{14}$$

式中，Num_{correct} 和 Num_{all} 分别对应的是入侵风险类型识别正确异构传感数据的数量以及设置的数据样本总量，根据实验样本的准备情况，每组实验中 Num_{all} 的取值均为 7 100 条。另外，入侵风险识别结果时效性的量化测试指标设置为入侵风险识别响应时间，其数值结果如下：

$$\Delta T = t_{\text{out}} - t_{\text{in}} \tag{15}$$

式中，t_{in} 和 t_{out} 表示的是异构传感数据样本的输入时间和入侵风险识别结果的输出时间，上述两个参数的具体取值可通过调取上位机的后台运行数据直接得出。最终计算得出风险值识别误差的值越小、风险类型识别正确率，证明对应识别方法的精度性能越优，识别响应时间越短说明对应识别方法的时效性越高。

3.6　性能测试实验结果分析

通过相关数据的调取与统计，得出异构传感数据入侵风险识别精度性能的测试结果，如表 3 所示。

表 3 异构传感数据入侵风险识别精度性能测试数据表

实验组别	基于深度学习网络的物联网入侵识别方法			基于物联网的异构传感数据入侵风险识别方法		
	实际风险值	计算风险值	类型识别正确数据量/条	实际风险值	计算风险值	类型识别正确数据量/条
1	0.37	0.34	6 933	0.37	0.36	7 100
2	0.24	0.22	7 024	0.24	0.24	7 098
3	0.22	0.21	7 001	0.22	0.22	7 094
4	0.15	0.12	7 014	0.15	0.15	7 086
5	0.06	0.05	6 984	0.06	0.06	7 100
6	0.11	0.10	7 009	0.11	0.10	7 100
7	0.17	0.15	6 852	0.17	0.17	7 097
8	0.14	0.13	7 017	0.14	0.14	7 089

将表 3 中的数据分别代入到式（13）和式（14）中，计算得出对比识别方法的平均风险值识别误差为 0.017 5，类型识别正确率的平均值为 98.3%，优化设计方法的平均风险识别误差和风险类型平均识别正确率分别为 0.002 5 和 99.9%，即优化方法的入侵风险识别精度性能更优。此外，通过式（15）的计算，得出识别方法失效性能的测试对比结果，如图 6 所示。

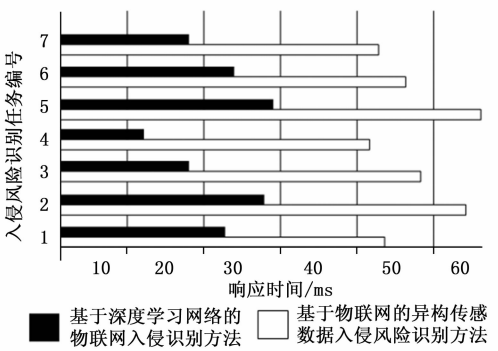

图 6 入侵风险识别方法时效性测试对比结果

从图 6 中可以直观地看出，与传统识别方法相比，优化设计方法的响应时间更短，由此证明优化方法得出识别结果的时效性更高。

4 结束语

物联网是智能时代的产物，实现了物与物、人与物之间的通信，为生产、生活的自动化运行与管理提供了技术支持，可以说，物联网的运行安全性直接影响了生活质量以及生产效率。通过基于物联网的异构传感数据入侵风险识别方法的优化设计，为物联网提供了网络安全保障，有利于物联网及其技术的推广。然而此次优化设计的入侵风险识别方法未考虑非法用户同时使用多种入侵攻击方式的情况，针对这一问题还需要在未来的研究工作中进一步探讨。

参考文献：

[1] 张娅. 基于深度学习网络的物联网非法入侵识别研究 [J]. 微电子学与计算机，2020，37（6）：75－78.

[2] 王 赟，于 尧，赵雨佳，等. 家庭物联网中基于 SDN 的入侵检测防御机制 [J]. 控制工程，2021，28（5）：1027－1032.

[3] 乔 楠，李振兴，赵国生. XGBoost-RF 的物联网入侵检测模型 [J]. 小型微型计算机系统，2022，43（1）：152－158.

[4] 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）：1680－1684.

[5] 王加梁. 基于属性分类建模的入侵检测方法 [J]. 计算机工程与设计，2022，43（4）：907－913.

[6] 田桂丰，单志龙，廖祝华，等. 基于 Faster R-CNN 深度学习的网络入侵检测模型 [J]. 南京理工大学学报，2021，45（1）：56－62.

[7] 罗智勇，杨 旭，刘嘉辉，等. 基于贝叶斯攻击图的网络入侵意图分析模型 [J]. 通信学报，2020，41（9）：160－169.

[8] 王艺霏，莫 爽，吴文睿，等. 基于内外卷积网络的网络入侵检测 [J]. 北京邮电大学学报，2021，44（5）：94－100.

[9] 杨至元，张仕鹏，孙 浩，等. 基于 Cyber-net 与学习算法的变电站网络威胁风险评估 [J]. 电力系统自动化，2020，44（24）：19－27.

[10] 王春东，刘懿铭，叶 欣. 基于入侵检测的网络安全态势评估技术 [J]. 南开大学学报（自然科学版），2021，54（5）：36－41.

[11] 陈爱萍. 基于 PSO-ELM 算法的网络入侵检测研究 [J]. 安阳师范学院学报，2022（2）：35－39.

[12] 孙海丽，龙 翔，韩兰胜，等. 工业物联网异常检测技术综述 [J]. 通信学报，2022，43（3）：196－210.

[13] 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.

[14] 章 缙，李洪赭，李赛飞. 针对基于随机森林的网络入侵检测模型的优化研究 [J]. 计算机与数字工程，2022，50（1）：106－110，179.

[15] 许彩芳. 基于 PSO-FCM 智能算法的计算机网络入侵检测方法 [J]. 佳木斯大学学报（自然科学版），2022，40（1）：60－62，68.

[16] 葛继科，刘浩因，李青霞，等. 基于改进 CNN-LSTM 的网络入侵检测模型研究 [J]. 软件工程，2022，25（1）：56－58，55.

[17] 伍德军，韩宝华. 萤火虫优化的异构集成学习网络入侵检测方法 [J]. 火力与指挥控制，2021，46（12）：26－31.

[18] 刘奇旭，王君楠，尹 捷，等. 对抗机器学习在网络入侵检测领域的应用 [J]. 通信学报，2021，42（11）：1－12.

[19] 李忠成，高惠燕，张文祥. 边缘计算中改进 ELM 的高效入侵检测算法 [J]. 计算机测量与控制，2021，29（7）：223－228，234.

[20] 郭志民，周劼英，王 丹，等. 基于 Transformer 神经网络模型的网络入侵检测方法 [J]. 重庆大学学报，2021，44（11）：81－88.