DOI:10.20033/j.1003-7241.(2025)07-0129-05

基于局部最优解分析的软件多重攻击安全检测研究

王国梁[1]，许 冬[1]，池少宁[2]，宋若鹏[3]，张 迪[1]

（1.国网安徽省电力有限公司信息通信分公司，安徽 合肥 230061；
2.福建亿榕信息技术有限公司，福建 福州 350003；
3.国网安徽省电力有限公司，安徽 合肥 230022）

摘 要：为了提高恶意软件检测精度，加强办公软件安全性，提出一种基于局部最优解分析的办公软件多重攻击安全检测算法。按照最小-最大标准化方法对数据进行标准化处理，将数据依据特征以及安全性的相关性进行排序，通过计算特征权值和两个变量之间的相关程度提取数据特征。基于特征提取结果采用智能蝙蝠算法对软件多重攻击进行分类，通过发散式的搜索得到局部最优解，同时在保持最大速度探索安全分类界限的基础上计算适应度值，由此实现办公软件多重攻击安全检测。由实验结果可知，所述方法具有较高的检测精度，能有效应用于办公软件的多重攻击检测，具有较高的应用价值。

关键词：智能蝙蝠算法；多重攻击；安全检测；局部最优解分析

中图分类号：TP309.2 **文献标识码：**A **文章编号：**1003-7241（2025）07-0129-05

Research on Multiple-attack Security Detection for Software Based on Local Optimal Solution Analysis

WANG Guoliang[1], XU Dong[1], CHI Shaoning[2], SONG Ruopeng[3], ZHANG Di[1]

(1. State Grid Anhui Electric Power Co., Ltd., Information & Communication Branch, Hefei 230061, China;
2. FuJian YiRong Information Technology Co., Ltd., Fuzhou 350003, China;
3. State Grid Anhui Electric Power Co., Ltd., Hefei 230022, China)

Abstract: In order to improve the accuracy of malware detection and enhance the security of office software, a multi attack security detection algorithm for office software based on local optimal solution analysis is proposed. It standardizes the data according to the minimum maximum standardization method, sorts the data based on the correlation between features and security, and extract data features by calculating feature weights and the degree of correlation between two variables. Based on the feature extraction results, the intelligent bat algorithm is used to classify software multiple attacks, and the local optimal solution is obtained through divergent search. At the same time, the fitness value is calculated while maintaining the maximum speed to explore the security classification boundary, thus achieving secure detection of office software multiple attacks. From the experimental results, it can be seen that the proposed method has high detection accuracy and can be effectively used for multiple attack detection in office software, with high application value.

Keywords: intelligent bat algorithm; multiple attack; safety inspection; local optimal solution analysis

0 引言

在互联网信息中心的相关报告中，我国网民数量已经超过了8亿，互联网普及率超过国际平均标准4.3个百分点，使用手机和计算机上网的人群占比逐年增高。在日常生活中，网络已经成为了人们不可缺少的重要组成部分，其中办公软件更是成为了很多人工作的重要工具。为了提高办公人员的工作效率，很多软件开发商通常会根据用户的需求定制系统，使得人们在使用软件时具有各种各样的选择，然而，功能和种类的繁多及差异使得各类办公软件在使用过程中的安全性很难得到有效保障，经常会出现恶意应用软件干扰办公设备，造成用户经济损失的情况[1]，常见的恶意应用软件不但会导致短信、通话记录、交易记录等敏感信息泄露，严重情况下甚至还会造成电子设备终端的损坏，如果涉及到军事、政治等保密性要求较高的相关使用领域，还会造成巨大的风险，因此，针对上述问题对办公软件进行有效的安全检测具有重要的意义。文献[1]通过反编译的安卓软件，对权限、意图以及组件等进行信息构成特征的提取，同时，考虑到恶意软件运行的时效性，采用并联模式得到最终的检测结果；文献[2]采用一种信息量差加权集成方法，基于样

*基金项目：国网安徽省电力有限公司（B3120522001K）

收稿日期：2023-09-21

本权限的静态特征构造基本策略，对样本的正确与错误时间进行分类处理，进而获取最佳的分类和检测结果；文献[3]使用源代码漏洞作为保证办公软件安全的重要策略，结合CNN-GAP可解释性模型，对漏洞相关代码进行标识处理，同时提出了基于卷积神经网络与全局平均池化的归一化处理方法，以获取更加全面和深入的检测结果。为了进一步提高针对办公软件多重攻击的安全检测效率，综合上述文献，本文研究并设计了一种基于智能蝙蝠算法的办公软件安全检测方法。实验结果表明，所述方法具有较高的检测精度，能够有效的用于办公软件多重攻击的安全检测[3-4]。

1 数据标准化与特征提取

在对数据进行标准化处理的过程中，首先需要采集办公软件安全检测过程中的使用特征数据。在常见的办公应用系统中，系统内核通常没有记录系统资源使用状态的文件，只能通过底层私有函数进行调用，进而区分CPU各种使用状态信息，如用户态、系统态、空闲态等。为了降低离散型数据对特征数据造成的影响，首先需要对数据进行标准化处理[5-6]，文中采用基于最小-最大标准化的方法将其规范到[0,1]的区间，最小-最大标准化的计算如下：

$$V_k = L_m + \sqrt{\frac{(L_u - L_m)\times \min(A_i)}{\max(A_i) - \min(A_i)}} \tag{1}$$

式中，V_k表示经过标准化处理后得到的数据；L_m表示标准化前的数据下界，L_u表示经过标准化处理前的数据上界，L_m和L_u在本文中分别使用0和1表示；$\min(A_i)$表示样本的最小值，$\max(A_i)$则表示样本的最大值。经过上述标准化处理后，需要对所得到的数据可以进行特征提取，所提取到的特征共分为两类，一类是权限特征，另一类则是API调用特征，进行特征提取时需要将数据依据特征以及安全性的相关性进行排序以计算特征权值，特征权值的计算如下：

$$W_d = W_k - \frac{\sqrt{\mathrm{diff}(k_i, R_h, P_h)} + \sqrt{\mathrm{diff}(k_i, R_h, M_h)}}{M_n} \tag{2}$$

式中，W_d表示经过标准化处理后的数据安全相关性特征权值；W_k表示应用权限特征系数；$\mathrm{diff}(k_i, R_h, P_h)$表示应用程序$R_h$和应用程序$P_h$在$k_i$权限处的数据相关性；$\mathrm{diff}(k_i, R_h, M_h)$则表示应用程序$R_h$和应用程序$M_h$在$k_i$权限处的数据相关性；$M_n$表示数据总量[7-8]。重复上述过程，即可得到不同权限特征的平均权值，进而根据特征权限的排序去除冗余特征。最后使用皮尔逊相关系数法计算两个变量之间的相关程度，计算公式为

$$G_{ik} = \frac{\sum_{i=1}^{n}(h_i - h_k)(p_i - p_k)}{\left(\sqrt{\sum_{i=1}^{n}(h_i - h_k)^2}\right)\left(\sqrt{\sum_{i=1}^{n}(p_i - p_k)^2}\right)} \tag{3}$$

式中，G_{ik}表示两个变量i和k之间的相关程度系数，其取值一般在[-1,1]之间；h_i表示变量i的权限特征，h_k表示变量k的权限特征；p_i表示变量i的关联特征；p_k则表示变量k的关联特征[9]。综合上述方法，可以在将数据进行初始化处理的前提下，对办公软件中的数据特征进行提取，得到不同办公软件的特征关联程度，为进一步选择合适的检测方法提供依据。

2 基于智能蝙蝠算法的多重攻击安全分类模型

智能蝙蝠算法是一种启发性的群体智能算法，通过对蝙蝠位置和速度的实时更新，得到发散式的局部搜索结果[10-11]，位置和速度的更新方法如下：

$$\begin{cases} v_i^{t+1} = \dfrac{f_i}{v_i^t + v_i^{t-1}\cdot x_i^t} \\ x_i^{t+1} = \dfrac{f_i}{x_i^t + x_i^{t-1}} \end{cases} \tag{4}$$

式中，f_i表示全局发散因子；v_i^{t+1}表示在t+1时刻，第i代更新后的局部搜索速度，v_i^t表示t时刻的速度，v_i^{t-1}表示t-1时刻的速度；x_i^{t+1}表示在t+1时刻的第i代局部搜索位置，x_i^t表示t时刻的搜索位置，x_i^{t-1}表示t-1时刻的搜索位置[12]。通过上述公式可得到蝙蝠在群体优化中的最优位置与最优速度，其智能蝙蝠寻优算法的示意图如图1所示。

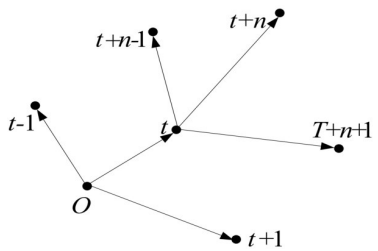


图1 蝙蝠寻优算法示意图

在标准的分类算法中，通过群体最优位置进行全局寻优，可以引入平均速度的概念：

$$V_{i+n}{}^t = \sqrt{\frac{\sum_{i=1}^{n} X_{i+n}{}^{t+1} - \sum_{i=1}^{n} X_{i+n}{}^{t-1}}{t}} \tag{5}$$

式中，$V_{i+n}{}^t$表示在全局寻优过程中t时刻第i+n代算法的平均速度；$X_{i+n}{}^{t+1}$和$X_{i+n}{}^{t-1}$分别表示全局巡游过程中t+1时刻和t-1时刻第i+n代算法的位置。针对此类问题，通过设置适应值得分作为安全分类的解[13-14]。当蝙蝠算法的整体权重位置相对较优时，可以保持最大的速度探索安全分类界限，计算方式如公式(6)：

$$S_{\text{core}}=\begin{cases}\dfrac{f_i}{f_w},if\left(f_i<f_w\right)\\1,if\left(f_i=f_w\right)\\\dfrac{f_w-f_i}{f_w-f_b},if\left(f_i>f_w\right)\end{cases}\tag{6}$$

式中，S_{core}表示软件安全性分类的适应度值，其数值一般在[0,1]之间，通常以0.5为界限，判断软件是否具备安全性，当S_{core}接近1时，表示软件相对安全，当S_{core}接近0时，表示软件相对不安全。f_i表示算法个体在第i代的个体适应值，f_w和f_b分别表示当前迭代次数下算法个体的最优适应度值和最差适应度值。结合上文，可以利用智能蝙蝠算法对软件使用过程中所受到的多重攻击进行分类。

3 多重攻击安全检测

采用上文所述方法可以得到软件在恶意样本与非恶意样本下的分类模型，依据该模型所设计的软件安全检测算法流程如图2所示。根据图2，检测过程中首先需要反编译文件，以提取文件信息并选择特征属性，进而计算不同特征属性之间的相似度，取其中相似度更高的项目进行办公软件安全检测，然后，获取APK文件并以此形成特征向量。在上述分类模型下，使用文中所述方法可以达到局部最优的速度与位置[15-16]；如果没有达到局部最优，则需要重新选择特征属性，达到局部最优后，可以继续训练数据集，进而计算整体的最优解，最终所返回的分类结果，即为本文方法下的办公软件多重攻击安全检测结果。

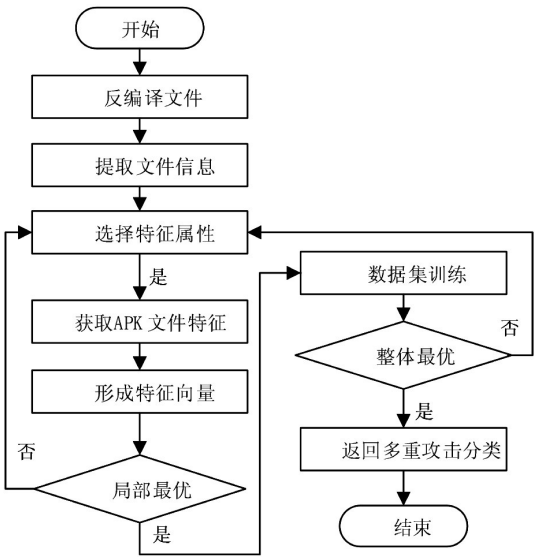


图2 算法流程

4 实验研究

4.1 实验设置

在本实验中，为测试采用上文所述智能蝙蝠算法下办公软件安全检测的有效性，需要首先建立应用软件安全检测的数据集。这些训练数据集中均为来自于安卓基因组计划的恶意应用程序，其中来自于多个恶意应用家族恶意样本共包括1 536例，这些恶意应用家族及其所包含的样本数量如表1所示。

表1 恶意应用家族及包含样本数量

序号	恶意应用家族	样本数量
1	BeanBot	136
2	Dog Wars	445
3	DroiKungFu1	285
4	DroiKungFu2	242
5	DroiKungFu3	136
6	GamblerSMS	106
7	GGTracker	186

上述7个家族的样本共同组成训练数据集，而测试样本则包括恶意样本和非恶意样本两类，其中恶意样本共有700例，其中每个恶意应用家族的样本分别为100例，非恶意样本同样为700例。测试样本中的非恶意样本包括Microsoft Office、WPS、钉钉、腾讯会议、企业微信、金山文档等多种办公软件。在实验过程中，需要设置相应的实验环境，本次实验中办公软件运行过程中CPU的使用率在一段时间内均保持在1%左右，满足实验环境要求。

4.2 测试方法

将表1中的所有恶意应用样本作为反编译的数据，使用Android SDK自带的调试工具aapt作为反编译工具，使用aapt dump permissions<fle_path.apk>作为命令获取这些样本的信息权限，通过编写脚本语言以进行自动化处理并构成权限特征集，进而通过挖掘样本数据特征构造相关恶意应用家族的权限关系库，并将其作为最大权限繁项集。在监测过程中，使用如下四个指标衡量安全检测方法的好坏。

$$W_{\text{TPR}}=\frac{W_{\text{TP}}}{W_{\text{TP}}+W_{\text{FN}}}\tag{7}$$

$$W_{\text{FPR}}=\frac{W_{\text{FP}}}{W_{\text{FP}}+W_{\text{TN}}}\tag{8}$$

$$W_{\text{FNR}}=\frac{W_{\text{FN}}}{W_{\text{FP}}+W_{\text{TN}}}\tag{9}$$

$$W_{\text{ACC}}=\frac{W_{\text{TP}}+W_{\text{TN}}}{W_{\text{TP}}+W_{\text{TN}}+W_{\text{FN}}+W_{\text{FP}}}\tag{10}$$

式中，W_{TPR}表示所有非恶意办公软件中被正确分类为办公程序的比例，即检测率；W_{FPR}表示所有恶意数据中被错误分类为非恶意办公软件的比例，即漏报率；W_{FNR}表示所

有办公软件中被错误分类为恶意数据的比例，即漏报率；W_{ACC}为综合上述几个检测指标的分类精度；W_{TP}为真阳性；W_{FN}表示假阴性；W_{FP}为假阳性；W_{TN}表示真阴性。文中主要使用上述指标对数据集进行测试。

4.3 软件安全测试

测试过程中分别使用智能蝙蝠算法、LSTM-SVM模型、信息量差加权集成算法、CNN-GAP可解释性模型作为对比算法，测试所得到的检测精度如图3所示。

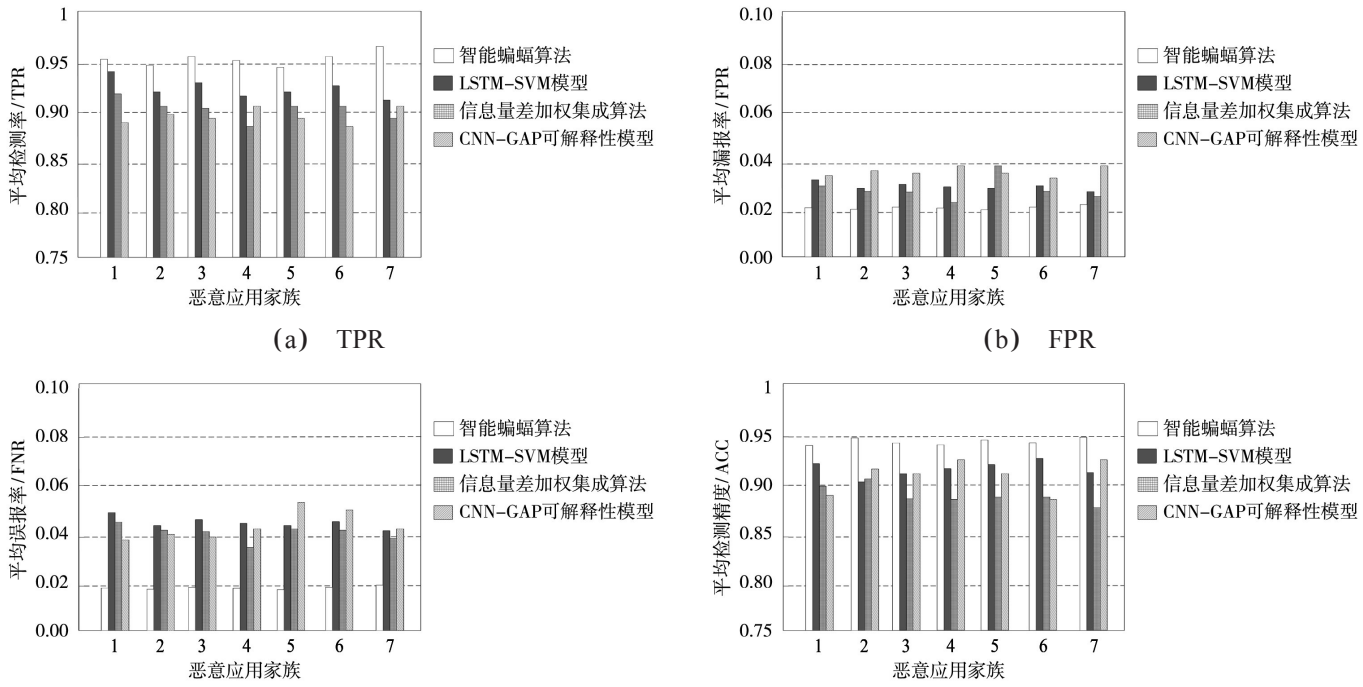


图3 软件安全检测精度

由图3可知，在TPR检测中，本文设计的智能蝙蝠算法在七个恶意应用家族中的平均检测率分别为0.96、0.95、0.96、0.96、0.94、0.96、0.97，LSTM-SVM模型的平均检测率在0.90-0.95之间，信息量差加权集成算法和CNN-GAP可解释性模型的平均检测率则在0.85-0.95之间。综合对比四种检测方法，本文所述方法的检测率在同一恶意应用家族的检测中均高于其他方法。在FPR检测中，四种算法在七个恶意应用家族中的平均漏报率均小于0.04，在FNR检测中，本文方法的平均误报率在0.02以下，其他三种方法则在0.02-0.06之间，在ACC的检测精度测试中，智能蝙蝠算法同样优于其他三种方法。由此可见，本文所设计的方法具有更准确的安全检测结果。

5 结束语

本文设计了一种基于局部最优解分析的办公软件多重攻击安全检测算法，文中在建立检测分类模型的基础上分析并设计了基于智能蝙蝠算法的检测方法。实验结果显示，所述检测方法的检测精度明显优于其他几种检测方法，具有更高的检测效率。在后续研究中，可以对所述方法进行应用扩展，针对移动互联网平台插件以及移动支付等软件，对所述软件多重攻击安全检测算法进行进一步优化。

参考文献：

[1] 刘俊贤，吴新龙. 云计算中心多用户网络隔离性安全检测研究[J]. 微型电脑应用，2020，36(9)：156-159.

[2] 赵敏，张雪芹，朱唯一，等. 基于LSTM-SVM模型的恶意软件检测方法[J]. 华东理工大学学报(自然科学版)，2022，48(5)：677-684.

[3] 张高峰，鲍旭丹，刘敬，等. WEID：一种基于信息量差加权集成的Android恶意软件检测方法[J]. 计算机应用与软件，2022，39(9)：332-338.

[4] 王剑，匡洪宇，李瑞林，等. 基于CNN-GAP可解释性模型的软件源码漏洞检测方法[J]. 电子与信息学报，2022，44(7)：2568-2575.

[5] 黄啸晨，封化民，刘飚，等. 一种基于生物启发特征优化的Android恶意软件检测方法[J]. 计算机应用与软件，2022，39(6)：309-314，341.

[6] 王玉联，鲁鸣鸣. 可解释的基于图嵌入的Android恶意软件自动检测[J]. 计算机工程与应用，2021，57(23)：122-128.

[7] 刘振鹏，王仕磊，郭超，等. 软件定义网络中基于深度神经网络的DDoS攻击检测[J]. 云南大学学报(自然科学版)，2022，44(4)：729-735.

[8] 路登凯，于永斌，余文建，等. 深层内核钩子挖掘算法及其

在软件安全中的应用[J]. 应用科学学报，2022，40(1)：61-68.

[9] 徐国天，刘猛猛. 基于改进哈里斯鹰算法同步优化特征选择的恶意软件检测方法[J]. 信息网络安全，2021，21(12)：9-18.

[10] 张炳，文峥，魏筱瑜，等. InterDroid：面向概念漂移的可解释性 Android 恶意软件检测方法[J]. 计算机研究与发展，2021，58(11)：2456-2474.

[11] 顾绵雪，孙鸿宇，韩丹，等. 基于深度学习的软件安全漏洞挖掘[J]. 计算机研究与发展，2021，58(10)：2140-2162.

[12] 张立群，林海涛，郇文明，等. 基于 OpenFlow 的软件定义网络流规则冲突检测系统[J]. 计算机应用，2022，42(2)：528-533.

[13] 董云卫，张涵博，李勇军. 一种嵌入式软件安全漏洞的代码加固方法[J]. 空间控制技术与应用，2021，47(2)：17-24.

[14] 徐国天，沈耀童. 基于 XGBoost 和 LightGBM 双层模型的恶意软件检测方法[J]. 信息网络安全，2020，20(12)：54-63.

[15] 蒋科. 基于数据挖掘算法的医疗网络安全风险评估[J]. 自动化技术与应用，2023，42(5)：99-102，127.

[16] 尤玮婧，刘丽敏，马悦，等. 基于安全硬件的云端数据机密性验证方案[J]. 信息网络安全，2020，20(12)：1-8.

作者简介：王国梁(1980—)，男，硕士，高级工程师，研究方向：电力信息化。

(上接第46页)



图9 电气柜指示灯开机状态

5 结束语

本文通过 VR 虚拟现实技术研究泵站的虚拟巡检。以南京麒麟科创园启迪大街某泵站为例，分析泵站地处偏远，条件恶劣，需要 24 小时专人值守。进行自动化改造后实现了无人值班，但是麒麟科创园共有 9 个泵站，站址分散，巡检工作依然需要专人定时进行，需要付出巨大人力和时间成本。虚拟巡检系统投入试运行之后，可以实现在集控中心进行虚拟巡检，不仅提高了泵站管理的现代化水平，而且大大缩减了泵站管理公司运维成本，取得了良好的经济效益。本文将智能技术应用于水利事业，弥补单项巡检的种种缺陷。泵站虚拟巡检技术的使用保证了对水泵站的正常运行情况的监测，实现自动化、数字化、智能化管理泵站，为泵站的智能化管理打下了基础。

参考文献：

[1] 曹发彦. 配电站直流电源在线监测和诊断系统的应用与研究[J]. 企业技术开发(下半月)，2015，34(24)：24-25.

[2] 田蕴，李帅，王真. 智能巡检机器人的发展与设计趋势探析[J]. 工业设计，2019(11)：143-144.

[3] 陈师哲，王帅，金琴. 多文化场景下的多模态情感识别[J]. 软件学报，2018，29(4)：1060-10770.

[4] 李琢，周旭，张春辉，等. 多场景下复杂监控视频的前景目标提取[J]. 数学的实践与认识，2018，48(15)：220-227.

[5] 李继刚，徐贵，杨凯峰，等. 基于 VR 全景技术的电力工程现场可视化管控系统[J]. 自动化技术与应用，2023，42(11)：165-168.

[6] 包加桐，朱正伟，钱福军，等. 泵站信息化技术研究与应用[J]. 人民长江，2016，47(15)：108-113.

[7] 袁志波，高兴，于洪亮. 大型水利枢纽泵站智能化技术研究[J]. 水利信息化，2021(2)：63-66，75.

[8] 许晨希. 数字孪生与大型泵站智能化管理[J]. 陕西水利，2023(4)：115-117.

[9] 夏正创. 大中型泵站无人值守运行管理模式研究[J]. 水利建设与管理，2020，40(3)：75-79.

[10] 张成栋. 智能化泵站信息系统技术架构的设计和实现[J]. 科技创新与应用，2020(18)：103-105，108.

[11] 沈宇. 变电站巡检机器人路径规划技术研究[D]. 武汉：华中科技大学，2017.

[12] 王越，麻赛军. 基于 RFID 的变电站巡检系统[J]. 四川电力技术，2010，33(2)：77-79.

[13] 李亚会，何成宝，刘坤鹏. 变电站巡检系统的开发与应用[J]. 电气技术，2018，19(9)：97-100.

[14] 陈荭，符华. 数字孪生在电力系统中的应用[J]. 电子技术与软件工程，2020(21)：235-236.

[15] 潘博，张弛，张华，等. 数字孪生变电站在电网企业数智化转型的探索与应用[J]. 电力与能源，2020，41(5)：558-560，590.

[16] 田广强. 一种新颖高效的红外动态场景多目标检测跟踪算法[J]. 红外技术，2018，40(3)：259-263.

[17] 张俊，李骁，陈凯，等. 利用虚拟现实技术提升规划方案的空间认知效果[J]. 测绘通报，2019(9)：108-111.

作者简介：邵知宇(1992—)，男，讲师，研究方向：力触觉感知与再现，工业互联网等。

通信作者：唐鸿儒(1964—)，男，教授，研究方向：测控技术与智能系统的研究。