

# 电子与信息学报

DIANZI YU XINXI XUEBAO

第 42 卷 第 8 期

2020 年 8 月

## 目 次

安全测评与风险评估专题 .....	专题主编:冯登国 院士
一种基于程序执行时间量化分析的软件水印方法 .....	张颖君, 陈 恺, 鲍旭华 (1811)
椭圆曲线 Diffie-Hellman 密钥交换协议的比特安全性研究 .....	魏 伟, 陈佳哲, 李 丹, 张宝峰 (1820)
一种轻量级数据加密标准循环掩码实现方案 .....	王立辉, 闫守礼, 李 清 (1828)
密码产品的侧信道分析与评估 .....	陈 华, 习 伟, 范丽敏, 焦志鹏, 冯婧怡 (1836)
基于国产密码算法的数控网络的认证与验证模型研究及安全评估 .....	.....夏晓峰, 向 宏, 肖震宇, 蔡 挺 (1846)
基于流形学习能量数据预处理的模板攻击优化方法 .....	袁庆军, 王 安, 王永娟, 王 涛 (1853)
CSNN: 基于汉语拼音与神经网络的口令集安全评估方法 .....	.....咸鹤群, 张 艺, 汪 定, 李增鹏, 贺云龙 (1862)
论 文	
基于流量时空特征的 fast-flux 僵尸网络检测方法 .....	.....牛伟纳, 蒋天宇, 张小松, 谢 娇, 张俊哲, 赵振靡 (1872)
空间耦合 LDPC 码的分层译码算法 .....	吴皓威, 武小飞, 邹润秋, 欧静兰 (1881)
椭圆球面函数频域调制解调方法 .....	陆发平, 王红星, 刘传辉, 康家方, 杨大伟 (1888)
基于高斯核显性映射的核归一化解相关仿射投影 P 范数算法 .....	赵知劲, 陈思佳 (1896)
短参考多用户差分混沌移位键控通信系统性能分析 .....	贺利芳, 陈 俊, 张天骐 (1902)
面向服务的车辆网络切片协调智能体设计 .....	吴大鹏, 郑 豪, 崔亚平 (1910)
一种人与人和物到物业务共存下的异构蜂窝网络柔性接入策略 .....	.....田 辉, 何 雷, 马文峰, 王 聪 (1918)
基于云雾混合计算的车联网联合资源分配算法 .....	.....唐 伦, 肖 娇, 魏延南, 赵国繁, 陈前斌 (1926)
认知无人机网络中次级链路吞吐量优化研究 .....	达新宇, 张宏伟, 胡 航, 潘 钰, 井锦玲 (1934)
基于多流融合生成对抗网络的遥感图像融合方法 .....	雷大江, 张 策, 李智星, 吴 渝 (1942)
一种目标响应自适应的通道可靠性跟踪算法 .....	王 鹏, 孙梦宇, 王海燕, 李晓艳, 吕志刚 (1950)
融合时空上下文信息的胸环靶着弹检测算法 .....	王洪玉, 程 杨 (1959)
一种改进的区间型不确定数据模糊聚类方法 .....	肖满生, 张龙信, 张晓丽, 胡永祥 (1968)
基于分解和支配关系的超多目标进化算法 .....	赵 辉, 王天龙, 刘衍舟, 黄 橙, 张天骐 (1975)
基于非线性降维的自然计算方法 .....	季伟东, 孙小晴, 林 平, 罗 强, 徐浩天 (1982)
基于卷积长短时记忆网络的心律失常分类方法 .....	柯 丽, 王丹妮, 杜 强, 姜楚迪 (1990)
经典轨迹的鲁棒相似度量算法 .....	王前东 (1999)
基于电离层色散的短波信道多径特性分析 .....	吴永宏, 王程林, 任渊博, 周福厚 (2006)
一种基于水下无人航行器的多目标被动跟踪算法 .....	王宇杰, 李 宇, 鞠东豪, 黄海宁 (2013)

基于频域稀疏压缩感知的星载 SAR 稀疏重航过 3 维成像 .....	
..... 田 鹤, 于海锋, 朱 宇, 刘 磊, 张润宁, 袁 莉, 李道京, 周 凯 (2021)	
基于时频集中度指标的多旋翼无人机微动特征参数估计方法 .....	
..... 宋 晨, 周良将, 吴一戎, 丁赤飏 (2029)	
一种提升汽车雷达方位角分辨率的成像处理方法 .....	王同军, 吴 锋, 徐 伟 (2037)
基于同步压缩小波变换的主信号抑制技术 .....	吴龙文, 牛金鹏, 王 昭, 何胜阳, 赵雅琴 (2045)
基于随机平均梯度下降和对比源反演的非线性逆散射算法研究 .....	周辉林, 欧阳韬, 刘 健 (2053)
通信电台电磁辐射 2 阶互调低频阻塞效应与作用机理 .....	魏光辉, 赵 凯, 任仕召 (2059)

# JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

Vol.42 No.8 August 2020

## CONTENTS

<b>Special Topic on Safety Evaluation and Risk Assessment</b> .....	<b>Leading Editor: FENG Dengguo</b>
A Software Watermarking Method Based on Program Execution Time .....	
..... ZHANG Yingjun, CHEN Kai, BAO Xuhua	(1811)
Research on the Bit Security of Elliptic Curve Diffie-Hellman .....	
..... WEI Wei, CHEN Jiazhe, LI Dan, ZHANG Baofeng	(1820)
A Lightweight Implementation Scheme of Data Encryption Standard with Cyclic Mask .....	
..... WANG Lihui, YAN Shouli, LI Qing	(1828)
Side Channel Analysis and Evaluation on Cryptographic Products .....	
..... CHEN Hua, XI Wei, FAN Limin, JIAO Zhipeng, FENG Jingyi	(1836)
Research and Security Evaluation of AUTH-VRF Model for NCS Network Based on Domestic Cryptographic Algorithms .....	
..... XIA Xiaofeng, XIANG Hong, XIAO Zhenyu, CAI Ting	(1846)
An Improved Template Analysis Method Based on Power Traces Preprocessing with Manifold Learning .....	
..... YUAN Qingjun, WANG An, WANG Yongjuan, WANG Tao	(1853)
CSNN: Password Set Security Evaluation Method Based on Chinese Syllables and Neural Network .....	
..... XIAN Hequn, ZHANG Yi, WANG Ding, LI Zengpeng, HE Yunlong	(1862)
<b>Papers</b>	
Fast-flux Botnet Detection Method Based on Spatiotemporal Feature of Network Traffic .....	
..... NIU Weina, JIANG Tianyu, ZHANG Xiaosong, XIE Jiao, ZHANG Junzhe, ZHAO Zhenfei	(1872)
A Layered Decoding Algorithm for Spatially-coupled LDPC Codes .....	
..... WU Haowei, WU Xiaofei, ZOU Runqiu, OU Jinlan	(1881)
PSWFs Frequency Domain Modulation and Demodulation Method .....	
..... LU Faping, WANG Hongxing, LIU Chuanhui, KANG Jiafang, YANG Dawei	(1888)
A Kernel Normalization Decorrelated Affine Projection P-norm Algorithm Based on Gaussian Kernel Explicit Mapping .....	
..... ZHAO Zhijin, CHEN Sijia	(1896)
Performance Analysis of Short Reference Multi-User Differential Chaos Shift Keying Communication System .....	
..... HE Lifang, CHEN Jun, ZHANG Tianqi	(1902)
Service-oriented Coordination agent Design for Network Slicing in Vehicular Networks .....	
..... WU Dapeng, ZHENG Hao, CUI Yaping	(1910)
A Flexible Network Access Scheme in Heterogeneous Cell Networks with H2H and M2M Coexistence .....	
..... TIAN Hui, HE Lei, MA Wenfeng, WANG Cong	(1918)
Joint Resource Allocation Algorithms Based on Mixed Cloud/Fog Computing in Vehicular Network .....	
..... TANG Lun, XIAO Jiao, WEI Yannan, ZHAO Guofan, CHEN Qianbin	(1926)
Throughput Optimization of Secondary Link in Cognitive UAV Network .....	
..... DA Xinyu, ZHANG Hongwei, HU Hang, PAN Yu, JING Jinling	(1934)
Remote Sensing Image Fusion Based on Generative Adversarial Network with Multi-stream Fusion Architecture ..	
..... LEI Dajiang, ZHANG Ce, LI Zhixing, WU Yu	(1942)
An Object Tracking Algorithm with Channel Reliability and Target Response Adaptation .....	
..... WANG Peng, SUN Mengyu, WANG Haiyan, LI Xiaoyan, LÜ Zhigang	(1950)
Detection Algorithm of Chest Bitmap Based on Spatio-temporal Context Information .....	
..... WANG Hongyu, CHENG Yang	(1959)
An Improved Fuzzy Clustering Method for Interval Uncertain Data .....	
..... XIAO Mansheng, ZHANG Longxin, ZHANG Xiaoli, HU Yongxiang	(1968)

(To be continued on inside back cover)

(Continued)

Decomposition and Dominance Relation Based Many-objective Evolutionary Algorithm .....	
.....	<i>ZHAO Hui, WANG Tianlong, LIU Yanzhou, HUANG Cheng, ZHANG Tianqi</i> (1975)
Natural Computing Method Based on Nonlinear Dimension Reduction .....	
.....	<i>JI Weidong, SUN Xiaoqing, LIN Ping, LUO Qiang, XU Haotian</i> (1982)
Arrhythmia Classification Based on Convolutional Long Short Term Memory Network .....	
.....	<i>KE Li, WANG Danni, DU Qiang, JIANG Chudi</i> (1990)
A Robust Trajectory Similarity Measure Method for Classical Trajectory .....	<i>WANG Qiandong</i> (1999)
High Frequency Channel Multipath Analysis Based on Ionosphere Dispersion .....	
.....	<i>WU Yonghong, WANG Chenglin, REN Yuanbo, ZHOU Fuhou</i> (2006)
A Multi-target Passive Tracking Algorithm Based on Unmanned Underwater Vehicle .....	
.....	<i>WANG Yujie, LI Yu, JU Donghao, HUANG Haining</i> (2013)
Sparse Flight 3-D Imaging of Spaceborne SAR Based on Frequency Domain Sparse Compressed Sensing .....	
.....	<i>TIAN He, YU Haifeng, ZHU Yu, LIU Lei, ZHANG Running, YUAN Li, LI Daojing, ZHOU Kai</i> (2021)
An Estimation Method of Micro-movement Parameters of UAV Based on The Concentration of Time-Frequency ..	
.....	<i>SONG Chen, ZHOU Liangjiang, WU Yirong, DING Chibiao</i> (2029)
A Novel Imaging Approach for Improving Azimuth Angular Resolution of Automotive Radars .....	
.....	<i>WANG Tongjun, WU Feng, XU Wei</i> (2037)
Primary Signal Suppression Based on Synchrosqueezed Wavelet Transform .....	
.....	<i>WU Longwen, NIU Jinpeng, WANG Zhao, HE Shengyang, ZHAO Yaqin</i> (2045)
Stochastic Average Gradient Descent Contrast Source Inversion Based Nonlinear Inverse Scattering Method for	
Complex Objects Reconstruction .....	<i>ZHOU Huilin, OUYANG Tao, LIU Jian</i> (2053)
Second-order Intermodulation Low Frequency Blocking Effect and Mechanism for Communication Radio under	
Electromagnetic Radiation .....	<i>WEI Guanghui, ZHAO Kai, REN Shizhao</i> (2059)