通 信 学 报

第 38 卷第 11 期 2017 年 11 月

目 次

学术论文

基于优化比特分配的有限反馈干扰对齐方案……谢显中，李 丹，雷维嘉，张森林 [2017215](1)

对轻量级分组密码 I-PRESENT-80 和 I-PRESENT-128 的 biclique 攻击……崔 杰，左海风，仲 红 [2017214](13)

ad hoc 云环境中分布式博弈卸载策略……曹 傧，梁裕丞，罗 雷，唐 述 [2017216](24)

基于非线性对的车联网无证书批量匿名认证方案研究……

……宋 成，张明月，彭维平，贾宗璞，刘志中，闫玺玺 [2017227](35)

基于 QoS 的多小区下行 TDD 大规模 MIMO 系统顽健波束成形……曹 杰，廖 勇，沈轩帆 [2017218](44)

新的格上基于身份的分级加密方案……叶 青，胡明星，汤永利，刘 琨，闫玺玺 [2017219](54)

基于相对梯度正则化的 Retinex 变分模型及其应用……智 宁，毛善君，李 梅 [2017212](65)

新的无证书广义指定验证者聚合签名方案……许芷岩，吴黎兵，李 莉，何德彪 [2017220](76)

与 3 类向量值密码函数仿射等价的函数数量研究……袁 峰，江继军，杨 旸，许盛伟 [2017206](84)

基于不等簇半径和动态簇头的 WSN 能量空洞攻击抑制模型研究……周伟伟，郁 滨 [2017209](93)

基于多实例运动学特征学习的动态手势识别研究……周彩秋，杨余旺，庞海波[2017211](103)

移动社交网络中基于拍卖模型的数据转发激励机制……刘 浩，陈志刚，张连明[2017210](111)

综 述

攻击图技术应用研究综述……叶子维，郭渊博，王宸东，琚安康[2017213](121)

软件定义网络及安全防御技术研究……王 涛，陈鸿昶，程国振[2017221](133)

学术通信

多数据拥有者认证的密文检索方案……伍祈应，马建峰，苗银宾，张俊伟，沈丽敏[2017225](161)

连续变量量子密钥分发数据协调加速运算的 GPU 实现……刘绍婷，王晓凯，郭大波[2017222](171)

OpenFlow 中基于精确时间戳的延迟测量方法……邱欣逸，李 俊，周建二，李菁菁[2017223](178)

SDN 中基于可靠性评估的多控制器均衡部署策略……胡 涛，张建辉，马 腾，赵 伟[2017224](188)

期刊基本参数：CN11-2102/TN*1980*m*A4*200*zh*P*¥78.00*2000*18*2017-11

万方数据

Journal on Communications

Vol.38 No.11 November 2017

Contents

Papers

Interference alignment based on optimizing bit allocation with limited feedback in interfering MIMO-MAC networks
XIE Xian-zhong, *LI Dan*, *LEI Wei-jia*, *ZHANG Sen-lin* [2017215](1)

Biclique cryptanalysis on lightweight block ciphers I-PRESENT-80 and I- PRESENT-128
CUI Jie, *ZUO Hai-feng*, *ZHONG Hong* [2017214](13)

Distributed game theoretic approach for offloading in ad hoc cloud
CAO Bin, *LIANG Yu-cheng*, *LUO Lei*, *TANG Shu* [2017216](24)

Research on pairing-free certificateless batch anonymous authentication scheme for VANET
SONG Cheng, *ZHANG Ming-yue*, *PENG Wei-ping*, *JIA Zong-pu*, *LIU Zhi-zhong*, *YAN Xi-xi* [2017227](35)

Robust beamforming for multicell downlink TDD massive MIMO system based on QoS
CAO Jie, *LIAO Yong*, *SHEN Xuan-fan* [2017218](44)

Novel hierarchical identity-based encryption scheme from lattice
YE Qing, *HU Ming-xing*, *TANG Yong-li*, *LIU Kun*, *YAN Xi-xi* [2017219](54)

Variational Retinex model based on an extension of TV regularization with relative gradient and its application
ZHI Ning, *MAO Shan-jun*, *LI Mei* [2017212](65)

New certificateless aggregate signature scheme with universal designated verifier
XU Zhi-yan, *WU Li-bing*, *LI Li*, *HE De-biao* [2017220](76)

Research on affine equivalence enumeration of the three families vectorial function
YUAN Feng, *JIANG Ji-jun*, *YANG Yang*, *XU Sheng-wei* [2017206](84)

Suppression model of energy sink-hole attack in WSN based on the unequal cluster radius and mobile cluster head
ZHOU Wei-wei, *YU Bin* [2017209](93)

Research of dynamic gesture recognition based on multi-instance learning of kinematics features
ZHOU Cai-qiu, *YANG Yu-wang*, *PANG Hai-bo*[2017211](103)

Data forwarding incentive mechanism based on auction model in mobile social network
LIU Hao, *CHEN Zhi-gang*, *ZHANG Lian-ming*[2017210](111)

Comprehensive Reviews

Survey on application of attack graph technology *YE Zi-wei*, *GUO Yuan-bo*, *WANG Chen-dong*, *JU An-kang*[2017213](121)

Research on software-defined network and the security defense technology
WANG Tao, *CHEN Hong-chang*, *CHENG Guo-zhen*[2017221](133)

Correspondences

Multi-owner accredited keyword search over encrypted data
WU Qi-ying, *MA Jian-feng*, *MIAO Yin-bin*, *ZHANG Jun-wei*, *SHEN Li-min*[2017225](161)

Accelerated computational implementation of reconciliation for continuous variable quantum key distribution on GPU
LIU Shao-ting, *WANG Xiao-kai*, *GUO Da-bo*[2017222](171)

New delay measurement method based on accurate timestamp in OpenFlow
QIU Xin-yi, *LI Jun*, *ZHOU Jian-er*, *LI Jing-jing*[2017223](178)

Multi-controller balancing deployment strategy based on reliability evaluation in SDN
HU Tao, *ZHANG Jian-hui*, *MA Teng*, *ZHAO Wei*[2017224](188)

万方数据