

美国 EI 核心数据库检索期刊
中国科协精品科技期刊

ISSN 1000-436X
CN 11-2102/TN

通信学报

Journal on Communications

第 36 卷第 **11** 期
Vol.36 No.11

2015 年 11 月
Nov. 2015



中国通信学会主办

A Publication of China Institute of Communications

中国 · 北京 Beijing, China

目 次

综 述

基于大数据分析的 APT 攻击检测研究综述.....付 钰, 李洪成, 吴晓平, 王甲生 [2015184](1)

移动安全

基于树形模型的轻量级 RFID 组证明协议.....朱大立, 荣文晶, 王思叶, 庞 娜 [2015188](15)
基于代理的移动互联网隐私保护机制.....耿 魁, 李凤华, 李维皓, 李 晖, 牛 犇, 谢绒娜 [2015190](25)
车载网络中安全有效分布式的假名生成.....刘 哲, 刘建伟, 伍前红, 陈 杰, 王蒙蒙 [2015253](33)
多用户 MISO 干扰信道中的安全协同波束成形.....张立健, 金 梁, 罗文宇 [2015198](41)
面向多维数字媒体的访问控制机制.....单芳芳, 李凤华, 谢绒娜, 熊金波, 王彦超 [2015201](52)

云安全

基于身份加密中可验证的私钥生成外包算法.....任艳丽, 蔡建兴, 黄春水, 谷大武 [2015233](61)
基于向量空间不同访问群体的门限方案.....李 滨 [2015212](67)
面向移动云计算的多要素代理重加密方案.....苏 铨, 史国振, 谢绒娜, 付安民 [2015217](73)
基于多分支认证树的多用户多副本数据持有性证明方案.....查雅行, 罗守山, 卞建超, 李 伟 [2015234](80)
云端数据访问控制中基于中间代理的用户撤销新方法.....姚 亮, 杨 超, 马建峰, 张俊伟 [2015235](92)
云计算中虚拟机计算环境安全防护方案.....闫世杰, 陈永刚, 刘 鹏, 闵乐泉[2015236](102)
基于密文采样分片的云端数据确定性删除方法.....张 坤, 杨 超, 马建峰, 张俊伟[2015237](108)

网络安全

自适应 AP 聚类算法及其在入侵检测中的应用.....江 颀, 王卓芳, 陈铁明, 朱陈晨, 陈 波[2015242](118)
基于 Yaksha 密钥托管机制的命名数据网络内容发布/订阅系统.....郭 显, 冯 涛, 曹来成, 王 晶, 鲁 晔[2015251](127)
基于单分类支持向量机和主动学习的网络异常检测研究.....刘 敬, 谷利泽, 钮心忻, 杨义先[2015252](136)
消息和指令分析相结合的网络协议异常行为分析.....胡燕京, 裴庆祺, 庞辽军[2015256](147)
长时间数据流的并行检测算法.....周爱平, 程 光, 郭晓军, 朱琛刚[2015268](156)
面向 MANET 异常检测的分布式遗传 k -means 研究.....李洪成, 吴晓平, 严 博[2015269](167)
对一个基于身份签密方案的分析与改进.....张 宇, 杜瑞颖, 陈 晶, 侯 健, 周 庆, 王文武[2015271](174)
信任感知的安全虚拟网络映射算法.....龚水清, 陈 靖, 黄聪会, 朱清超[2015272](180)
基于主体行为的多方安全协议会话识别方法.....朱玉娜, 韩继红, 袁 霖, 陈韩托, 范钰丹[2015273](190)
RMPCM: 一种基于健壮多元概率校准模型的全网络异常检测方法.....李宇翀, 罗兴国, 钱叶魁, 赵 鑫[2015274](201)

Contents

Comprehensive Review

- Detecting APT attacks: a survey from the perspective of big data analysis.....
.....FU Yu, LI Hong-cheng, WU Xiao-ping, WANG Jia-sheng [2015184](1)

Mobile Security

- Tree-based lightweight RFID grouping proof protocol.....
.....ZHU Da-li, RONG Wen-jing, WANG Si-ye, PANG Na [2015188](15)
Proxy-based privacy-preserving scheme for mobile Internet.....
.....GENG Kui, LI Feng-hua, LI Wei-hao, LI Hui, NIU Ben, XIE Rong-na [2015190](25)
Secure and efficient distributed pseudonym generation in VANET.....
.....LIU Zhe, LIU Jian-wei, WU Qian-hong, CHEN Jie, WANG Meng-meng [2015253](33)
Secure coordinated beamforming for multiuser MISO interference channels.....
.....ZHANG Li-jian, JIN Liang, LUO Wen-yu [2015198](41)
Multidimensional digital media-oriented access control scheme.....
.....SHAN Fang-fang, LI Feng-hua, XIE Rong-na, XIONG Jin-bo, WANG Yan-chao [2015201](52)

Cloud Security

- Verifiable outsourcing private key generation algorithm in an identity-based encryption scheme.....
.....REN Yan-li, CAI Jian-xing, HUANG Chun-shui, GU Da-wu [2015233](61)
Threshold scheme for different access clusters based on vector space.....
.....LI Bin [2015212](67)
Multi-element based on proxy re-encryption scheme for mobile cloud computing.....
.....SU Mang, SHI Guo-zhen, XIE Rong-na, FU An-min [2015217](73)
Multiuser and multiple-replica provable data possession scheme based on multi-branch authentication tree.....
.....ZHA Ya-xing, LUO Shou-shan, BIAN Jian-chao, LI Wei [2015234](80)
New user revocation approach based on intermediate agency for cloud data access control.....
.....YAO Liang, YANG Chao, MA Jian-feng, ZHANG Jun-wei [2015235](92)
Security protection mechanism of virtual machine computing environment under the cloud computing.....
.....YAN Shi-jie, CHEN Yong-gang, LIU-Peng, MIN Le-quan[2015236](102)
Novel cloud data assured deletion approach based on ciphertext sample slice.....
.....ZHANG Kun, YANG Chao, MA Jian-feng, ZHANG Jun-wei[2015237](108)

Network Security

- Adaptive AP clustering algorithm and its application on intrusion detection.....
.....JIANG Jie, WANG Zhuo-fang, CHEN Tie-ming, ZHU Chen-chen, CHEN Bo[2015242](118)
Yaksha scheme based content publish/subscribe system for NDN.....
.....GUO Xian, FENG Tao, CAO Lai-cheng, WANG Jing, LU Ye[2015251](127)
Research on network anomaly detection based on one-class SVM and active learning.....
.....LIU Jing, GU Li-ze, NIU Xin-xin, YANG Yi-xian[2015252](136)
Message combined with instruction analysis for network protocol's abnormal behavior.....
.....HU Yan-jing, PEI Qing-qi, PANG Liao-jun[2015256](147)
Parallel detection algorithm on long duration data streaming.....
.....ZHOU Ai-ping, CHENG Guang, GUO Xiao-jun, ZHU Chen-gang [2015268](156)
Research on distributed genetic k -means for anomaly detection in MANET.....
.....LI Hong-cheng, WU Xiao-ping, YAN Bo[2015269](167)
Analysis and improvement of an identity-based signcryption.....
.....ZHANG Yu, DU Rui-ying, CHEN Jing, HOU Jian, ZHOU Qing, WANG Wen-wu[2015271](174)
Trust-aware secure virtual network embedding algorithm.....
.....GONG Shui-qing, CHEN Jing, HUANG Cong-hui, ZHU Qing-chao[2015272](180)
Towards session identification using principal behavior for multi-party secure protocol.....
.....ZHU Yu-na, HAN Ji-hong, YUAN Lin, CHEN Han-tuo, FAN Yu-dan[2015273](190)
RMPCM: network-wide anomaly detection method based on robust multivariate probabilistic calibration model.....
.....LI Yu-chong, LUO Xing-guo, QIAN Ye-kui, ZHAO Xin[2015274](201)

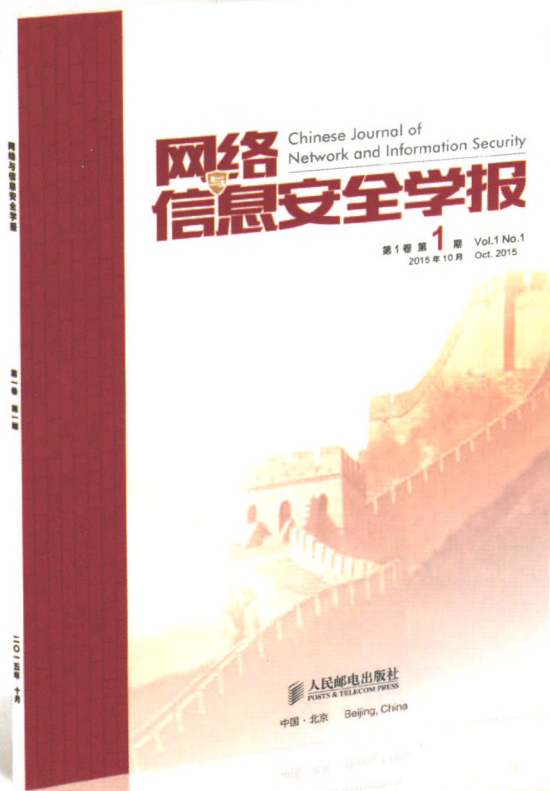
● 工业和信息化部 主管

● 人民邮电出版社 主办

网络 信息安全学报

Chinese Journal of
Network and Information Security

官方网址: www.cjnis.com



**汇聚安全创新思想
传播学术研究成果
提升科学研究实力
服务国家信息安全**

通过刊载信息安全领域有突破的基础理论研究、创新性的关键技术、热点安全问题研究, 以及与信息安全技术相关的交叉领域的科研学术论文, 充分展示我国的研究成果, 向科研人员提供全面的前沿信息, 开展多边的网络国际交流合作, 促进我国信息安全技术的发展与学术水平的提高, 为建设网络强国服务。

本刊与《通信学报》联袂选稿, 敬请登录官网投稿, 如有任何问题或建议, 欢迎您与编辑部沟通, 联系电话: 010-81055607, 邮箱: cjnis@bjxintong.com.cn。

发行部订阅

将订阅信息以传真或邮件方式发送至发行部, 也可致电发行部提交订阅信息

电话: 010-81055598

传真: 010-81055464

E-mail: yrq@bjxintong.com.cn

银行汇款

户名: 北京信通传媒有限责任公司

开户行: 中国工商银行北京体育馆路支行

账号: 0200008109200044661

邮局汇款

北京信通传媒有限责任公司发行部

地址: 北京市丰台区成寿寺路 11 号
邮电出版大厦 8 层

邮编: 100078

发行代号: 国内2-676
国外M395

2015年11月25日出版 定价: 78.00元

万方数据

ISSN 1000-436X

