

目次

学 术 论 文

基于传输路径质量的无线 mesh 网络可靠多播	胡致远, 王晓翔, 张 贤 (1)
基于高斯和粒子滤波的联合码和载波相位的伪距估计算法	李理敏, 龚文斌, 刘会杰, 余金培 (9)
可行的基于 CIOQ 的并行分组交换结构	任 涛, 兰巨龙, 扈红超 (14)
P2P 网络中具有激励机制的信任管理研究	胡建理, 周 斌, 吴泉源 (22)
IR-UWB 系统中采用锯齿波匹配的低复杂度 TOA 估计	郑 霖, 符杰林, 刘争红, 仇洪冰, 林基明 (33)
标准模型下身份匿名签名方案分析与设计	张明武, 杨 波, 姚金涛, 张文政 (40)
线性网络编码运算代价的估算与分析	蒲保兴, 王伟平 (47)
基于前置反馈的两级交换结构	申志军, 曾华荣, 夏 羽 (56)
基于警报序列聚类的多步攻击模式发现研究	梅海彬, 龚 俭, 张明华 (63)
面向椭圆曲线密码的处理器并行体系结构研究与设计	杨晓辉, 戴紫彬, 李 森, 张永福 (70)
标准模型下基于因子分解问题的短签名	王志伟, 张 伟 (78)

技 术 报 告

基于 SIP+P2P 系统的多业务流分离传输方案	雷为民, 张秀武, 贾军营, 于 波 (82)
无线网状网中基于 D-S 证据理论的可信路由	杨 凯, 马建峰, 杨 超 (89)
分群协议中冲突与拓扑信息误差研究	韩江洪, 魏 臻, 蔡志文, 韩 东, 魏振春 (97)
面向卫星网络的流量工程路由算法	肖 甫, 孙力娟, 叶晓国, 王汝传 (104)
基于攻击图的风险邻接矩阵研究	叶 云, 徐锡山, 贾 焰, 齐治昌, 程文聪 (112)
多源入侵检测警报的决策级融合模型	李志东, 杨 武, 王 巍, 苟大鹏 (121)
无线传感器网络 SL- n 迭代定位算法	罗 旭, 柴 利, 杨 君 (129)
传感器网络安全协议的分析和改进	闫丽丽, 彭代渊, 高悦翔 (139)

学 术 通 信

基于混沌的带密钥散列函数安全分析	郑世慧, 张国艳, 杨义先, 李忠献 (146)
异构无线网络中基于标识的匿名认证协议	侯惠芳, 季新生, 刘光强 (153)
单圈 T-函数的构造	杨 笑, 武传坤, 王亚翔 (162)
可证明安全的可信网络存储协议	段新东, 马建峰 (169)

Contents

Papers

Reliable multicast in wireless mesh networks based on routing quality.....	HU Zhi-yuan, WANG Xiao-xiang, ZHANG Xian (1)
Pseudorange estimation algorithm combining code and carrier phase based on Gaussian sum particle filtering	 LI Li-min, GONG Wen-bin, LIU Hui-jie, YU Jin-pei (9)
Practical parallel packet switch architecture based on CIOQ	REN Tao, LAN Ju-long, HU Hong-chao (14)
Research on incentive mechanism integrated trust management for P2P networks.....	 HU Jian-li, ZHOU Bin, WU Quan-yuan (22)
Low-complexity TOA estimation using sawtooth-waveform matching in non-coherent impulse radio systems	 ZHENG Lin, FUJie-lin, LIU Zheng-hong, QIU Hong-bing, LIN Ji-ming (33)
Cryptanalysis and design of signature schemes with identity ambiguity in the standard model	 ZHANG Ming-wu, YANG Bo, YAO Jin-tao, ZHANG Wen-zheng (40)
Evaluation and analysis of the computation cost of linear network coding.....	PU Bao-xing, WANG Wei-ping (47)
Front-feedback-based two-stage switch architecture	SHEN Zhi-jun, ZENG Hua-shen, XIA Yu (56)
Research on discovering multi-step attack patterns based on clustering IDS alert sequences	 MEI Hai-bin, GONG Jian, ZHANG Ming-hua (63)
Research and design of parallel architecture processor for elliptic curve cryptography	 YANG Xiao-hui, DAI Zi-bin, LI Miao, ZHANG Yong-fu (70)
Short signature based on factoring problem in the standard model	WANG Zhi-wei, ZHANG Wei (78)

Technical Reports

Separated multi streams transmitting method based on SIP+P2P system	 LEI Wei-min, ZHANG Xiu-wu, JIA Jun-ying, YU Bo (82)
Trusted routing based on D-S evidence theory in wireless mesh network	YANG Kai, MA Jian-feng, YANG Chao (89)
Collision and information error of topologies in clustering protocol	 HAN Jiang-hong, WEI Zhen, CAI Zhi-wen, HAN Dong, WEI Zhen-chun (97)
Routing algorithm for MPLS traffic engineering in satellite network	 XIAO Fu, SUN Li-juan, YE Xiao-guo, WANG Ru-chuan(104)
Research on the risk adjacency matrix based on attack graphs	 YE Yun, XU Xi-shan, JIA Yan, QI Zhi-chang, CHENG Wen-cong(112)
Decision-level fusion model of multi-source intrusion detection alerts	LI Zhi-dong, YANG Wu, WANG Wei, MAN Da-peng(121)
SL- <i>n</i> iterative localization algorithm in wireless sensor networks.....	LUO Xu, CHAI Li, YANG Jun(129)
Analysis and improvement of sensor networks security protocol.....	YAN Li-li, PENG Dai-yuan, GAO Yue-xiang(139)

Correspondences

Cryptanalysis of some chaos-based keyed hash functions.....	 ZHENG Shi-hui, ZHANG Guo-yan, YANGYi-xian, LI Zhong-xian(146)
Identity-based anonymity authentication protocol in the heterogeneous wireless network	 HOU Hui-fang, JI Xin-sheng, LIU Guang-qiang(153)
On the construction of single cycle T-functions	YANG Xiao, WU Chuan-kun, WANG Ya-xiang(162)
Provable secure trusted protocol for network storage	DUAN Xin-dong, MA Jian-feng(169)