计算机工程　2010 36 (1): 170-173,180　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

基于分簇的Ad Hoc网络密钥协商协议

张小彬，韩继红，王亚弟，刘 敏

(解放军信息工程大学电子技术学院，郑州 450004)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　以节点的公钥证书为基础，基于椭圆曲线密码体制提出一种分簇结构的Ad Hoc网络会话密钥协商协议，对协议的安全性和效率进行分析。该协议满足普遍认可的密钥协商安全要求，可抵抗中间人攻击、重放攻击、消息伪造攻击等多种攻击，有效地降低终端的计算、存储能力需求，减少了协商过程的通信开销。

关键词　Ad Hoc网络；椭圆曲线密码体制；分簇；密钥协商

分类号　TP393

DOI:

通讯作者:

作者个人主页: 张小彬;韩继红;王亚弟;刘 敏