通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

李慧贤,庞辽军,王育民.适合ad hoc网络无需安全信道的密钥管理方案[J].通信学报,2010,(1):112~117

适合ad hoc网络无需安全信道的密钥管理方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
李慧贤	
庞辽军	
王育民	

中文摘要：

密钥管理问题是构建ad hoc安全网络系统首要解决的关键问题之一。针对ad hoc网络特点，提出了一个无需安全信道的门限密钥管理方案。该方案中，可信中心的功能由局部注册中心和分布式密钥生成中心共同实现，避免了单点失效问题；通过门限技术，网络内部成员相互协作分布式地生成系统密钥；利用基于双线性对的公钥体制实现了用户和分布式密钥生成中心的双向认证；通过对用户私钥信息进行盲签名防止攻击者获取私钥信息，从而可以在公开信道上安全传输。分析表明该方案达到了第III级信任，具有良好的容错性，并能抵御网络中的主动和被动攻击，在满足ad hoc网络安全需求的情况下，极大地降低了计算和存储开销。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭