系统工程与电子技术 2010, 32(12) 2707-2710 DOI: 10.3969/j.issn.1001-506X.2010.12.43 ISSN: 1001-506X CN: 11-2422/TN

软件、算法与仿真

基于IBC策略驱动的组播内容分发方案

苏锐丹，丁振国，周利华

西安电子科技大学教育部计算机网络与信息安全重点实验室， 陕西 西安 710071

摘要：

针对内容分发应用中的组播加密方案和多接收者加密方案所存在的动态组密钥管理复杂、计算和通信代价高等问题，分析了内容分发系统的典型安全需求，采用基于身份密码学提出了一种新的面向群组的安全内容分发系统模型与方案，经安全性与性能分析表明，方案满足接收方访问控制、发送方鉴别与防抵赖、策略加密等安全要求。将发送方的计算和通信代价降为O(1)，同时具有密钥管理简单、组密钥更新开销小和易于实现等特点，能方便地应用于商业的组播内容分发系统。

关键词： 内容分发 组播 基于身份密码学 组密钥管理 策略驱动

IBC-based policy-driven multicast content distribution scheme

SU Rui-dan，DING Zhen-guo，ZHOU Li-hua

Key Lab. of Computer Network and Information Security of the Ministry of Education, Xidian Univ., Xi'an 710071, China

Abstract:

The multicast encryption and multi-recipient encryption schemes used in content distribution applications encounter some common problems, such as heavy key management for dynamic groups, high computation and communication costs, etc. Exploits identity-based cryptography is exploited to propose a new group-oriented secure content distribution model and scheme based on security requirements for practical application. The analyses on security and performance show that the scheme meets many essential requirements which include receiver access control, source authentication and non-repudiation, policy driven encryption, has a O(1) computation and communication cost for sender, and owns properties such as simple group key management, low cost of group key update, ease for implementation. It can be used to deploy a commercial multicast content distribution system.

Keywords: content distribution multicast identity based cryptography group key management policy-driven

收稿日期 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-506X.2010.12.43

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1．蒲保兴1，2,杨路明1，王伟平1.最优线性网络编码的分布式构造方法[J]. 系统工程与电子技术，2009,31(11): 2761-2766

2．蒲保兴 1,2 ，王伟平 1， 杨路明 1.多源多宿组播网络线性网络编码的优化构造[J]. 系统工程与电子技术，2010,32(2): 380-385