计算机工程与应用 2009 45 (25): 105-107 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

改进的错误容忍的会议密钥分配方案

丰继林，高焕芝，高方平

防灾科技学院 信息技术系，北京 101601

收稿日期 2008-5-20 修回日期 2008-8-13 网络版发布日期 2009-9-8 接受日期

摘要 提出了一个改进的基于身份并且错误容忍的会议密钥分配方案，分析结果表明，改进的协议在继承原协议安全特性的基础上，具备了抗被动攻击性、抗篡改攻击性和前向安全性，跟同类协议相比较，其安全性最高，通信量居中，因此，其实用性最强。

关键词 会议密钥分配 基于身份 错误容忍

分类号 TP309

Improved fault-tolerant conference key distribution scheme

FENG Ji-lin，GAO Huan-zhi，GAO Fang-ping

Department of Information Technology，Institute of Disaster Prevention Science and Technology，Beijing 101601，China

Abstract

Fault-tolerance is an important property of conference key distribution protocol.Recently，Yang et al proposes an identity-based fault-tolerant conference key distribution scheme which is much different from the traditional ones.But their scheme can not withstand passive attack and modification attack.Moreover，it also can not provide forward security.An improved identity-based fault-tolerant conference key distribution scheme is proposed.Compared with the Yang et al's scheme，Tzeng's scheme and Xun's scheme，the new scheme has illustrated the highest security and its communication cost is intervenient of Yang et al's scheme and Tzeng's scheme.As security is the first-line property in conference key establishment protocol，this scheme is the most practical one in the mass.

Key words conference key distribution identity-based fault-tolerant

DOI: 10.3778/j.issn.1002-8331.2009.25.032

通讯作者 丰继林 fengjilin@fzxy.edu.cn