

信息与网络安全

基于GDH的协商式虚拟动态子群组密钥管理方案

刘文艳

山东警察学院 网络中心¹

收稿日期 2006-10-13 修回日期 网络版发布日期 2007-4-2 接受日期

摘要 通常的群组密钥协商方案,一般都针对普通的、静态的群组。基于GDH的协商式虚拟动态子群组密钥管理方案实现了利用原来大群的密钥信息,有效地建立和管理虚拟动态安全子群的方法,与GDH方案相比,减少了更多的数据传输和密钥存储空间。

Abstract Key agreement is usually mentioned in general static group. Based on virtual dynamic subgroup, Agreed Virtual Dynamic Subgroup Scheme (AVDSG) was proposed, which can manage the virtual dynamic subgroup by using the key information of the group. Compared with GDH, it can largely reduce the average cost of re-keying and the number of keys held by each user.

关键词 [虚拟群组](#) [密钥协商](#) [动态子群](#)

Key words virtual group; key agreement; dynamic subgroup

分类号

DOI:

通讯作者:

刘文艳 lwy@sdpc.edu.cn

作者个人主页: 刘文艳

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (489KB)
- ▶ [\[HTML全文\]](#) (0KB)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“虚拟群组”的 相关文章](#)
- ▶ 本文作者相关文章
- [刘文艳](#)