计算机工程 2011, 37(24) 132-135 DOI: 10.3969/j.issn.1000-3428.2011.24.044 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于双线性对的卫星网络密钥协商协议

矫文成，吴 杨，潘艳辉，李 华，郑天明

(军械工程学院计算机工程系，石家庄 050003)

摘要： 提出一种基于双线性对的卫星网络密钥协商协议，分析卫星网络的特点，给出协议实现过程。对协议的安全性分析表明，该协议不存在密钥托管问题，能抵御主动攻击，会话密钥协商满足不可控性。对协议的性能分析表明，该协议能提高会话密钥协商效率，满足实际的卫星网络密钥协商需求。

关键词： 卫星网络 双线性对 离散对数问题 密钥协商 主动攻击

Key Agreement Protocol in Satellite Network Based on Bilinear Pairings

JIAO Wen-cheng, WU Yang, PAN Yan-hui, LI Hua, ZHENG Tian-ming

(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: This paper proposes a key agreement protocol in satellite network based on bilinear pairings. It analyzes the characteristics of the satellite network and gives the implementation procedure of the protocol. Security analysis demonstrates that the key agreement protocol can resist active and passive attacks without key trusteeship problem and the key generating process is uncontrolled. Performance analysis demonstrates that the protocol can increase the efficiency of the session key agreement, it is more satisfied with needs of key generation in real satellite network.

Keywords: satellite network bilinear pairings discrete logarithm problem key agreement active attack

收稿日期 2011-07-04 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.044

基金项目:

通讯作者:

作者简介: 矫文成(1970－)，男，副教授，主研方向：信息安全，软件工程；吴 杨，硕士研究生；潘艳辉、李华，博士；郑天明，硕士研究生

通讯作者E-mail: baiyanwy@163.com

参考文献：

扩展功能

本文信息

Supporting info

PDF(288KB)

[HTML] 下载

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

本文关键词相关文章

卫星网络

双线性对

离散对数问题

密钥协商

主动攻击

本文作者相关文章

矫文成

吴杨

潘艳辉

李华

郑天明

PubMed

Article by Jiao, W. C.

Article by Tun, Y.

Article by Bo, Y. H.

Article by Li, H.

Article by Zheng, T. M.

[2] 吴 平, 王保云, 徐开勇. 基于身份的Ad Hoc网络密钥管理方案[J].计算机工程.2008, 34(24):143-145 浏览

[3] 杨德明, 慕德俊, 许 钟. Ad Hoc 空间网络密钥管理与认证方案[J].通信学报.2006, 27(8):104-107

本刊中的类似文章

1. 蒋华, 贾永兴, 汪良辰, 杨庆锐.基于身份的P2PSIP可认证密钥协商方案[J]. 计算机工程, 2012,38(3): 134-136
2. 曹素珍, 王彩芬, 陈小云, 吕浩音.一种不含双线性对的可截取签名方案[J]. 计算机工程, 2012,38(3): 110-112
3. 丁清, 朱敏, 闫二辉.一种安全高效的WAPI改进策略[J]. 计算机工程, 2012,38(3): 153-155
4. 牛淑芬, 王彩芬.多源线性网络编码的同态签名算法[J]. 计算机工程, 2012,38(2): 126-128
5. 杨路.无对运算的无证书隐式认证及密钥协商协议[J]. 计算机工程, 2012,38(2): 138-140
6. 张建中, 马冬兰.一种高效的门限部分盲签名方案[J]. 计算机工程, 2012,38(01): 130-131,134
7. 高欢欢, 张建中.一种基于身份的门限代理签名方案[J]. 计算机工程, 2012,38(01): 132-134
8. 戚世杰, 卢建朱, 胡吉旦.增强型相互认证密钥协商方案[J]. 计算机工程, 2012,38(01): 108-110
9. 宋明明, 张彰, 谢文坚.一种无证书签密方案的安全性分析[J]. 计算机工程, 2011,37(9): 163-164
10. 魏靓, 张串绒, 郑连清.一种基于身份的广义签密方案[J]. 计算机工程, 2011,37(8): 4-6

文章评论

反馈人		邮箱地址	
反馈标题		验证码	2507

Copyright by 计算机工程