电子与信息学报 2009 31 (10): 2316-2320 ISSN: 1009-5896 CN: 11-4494/TN

论文

分布式CA下空间网络认证密钥安全度量方法

罗长远①, 李 伟①②, 李海林①, 蹇 波①

①解放军信息工程大学电子技术学院 郑州 450004;②解放军63895部队 孟州 454750

收稿日期 2008-10-14 修回日期 2009-3-17 网络版发布日期 2009-9-28 接受日期

摘要
基于分布式CA的密钥管理策略解决了空间网络中不易实施集中式密钥管理的难题，但也给认证密钥的安全带来了新的威胁。该文在描述和分析空间网络中认证密钥的安全威胁的基础上，提出了一种度量认证密钥安全强度的方法。该方法可根据系统门限值、密钥更新周期等参数的设置情况，定量度量认证密钥的安全强度。通过分析系统门限值和密钥分量更新周期对安全强度的影响，给出了合理设置这两个网络安全参数的方法。

关键词 空间网络 分布式CA 门限机制

分类号 TP393.08

Measurement Method for Space Networks Authenticated Key Security under Distributed CA

Luo Chang-yuan①, Li Wei①②, Li Hai-lin①, Jian Bo①

①PLA Information Engineering University, Electronic Technology Institute, Zhengzhou 450004, China; ②The 63895 Unit of the Chinese People's Liberation Army, Mengzhou 454750, China

Abstract
The key management schemes bsaed on Distributed Certificate Authority resolve the difficulty to adopting concentrating key management in space networks, but result in some new threats of authenticated key. Based on discribing and analyzing the threats suffered by authenticated key of space networks, a measurement method for security intensity of authenticated key is proposed. The method can quantitatively measure the security intensity of authenticated key according to the setting of parameters, such as threshold value, key-update period etc. By analyzing the impact of threshold value and key-update period on authenticated key security, a method of setting the two networks security parameters reasonably is given.

Key words Space networks Distributed Certificate Authority (CA) Threshold mechanism

DOI:

通讯作者

作者个人主页 罗长远①; 李 伟①②; 李海林①; 蹇 波①