计算机应用 2008 28 (05): 1158-1160 ISSN: 1001-9081 CN: 51-1307/TP

信息安全(Information security)

一种基于令牌环的密钥元更新方案

黄河[1];王亚弟[2];韩继红[1];栗帅[1]

解放军信息工程大学电子技术学院[1]

解放军信息工程大学[2]

收稿日期 2007-11-22 修回日期 网络版发布日期 2008-5-7 接受日期

摘要 分析现有密钥元更新方案存在的问题，提出一种基于令牌环的密钥元更新方案，方案基于分簇Ad Hoc网络体系结构，包括门限更新和更新组扩展两个阶段。门限更新阶段由簇首发起，可以有效防止多个数字证书中心(CA)节点在同一更新期发起密钥元更新的冲突；第二阶段通过更新组完成其他CA节点的密钥元更新，减少网络风暴发生的概率。另外方案提出一种不同更新期密钥元冲突解决办法，借助NS2仿真工具证实了方案的有效性。

Abstract This paper analyzed the advantages and disadvantages of existing secret share update schemes in Ad Hoc network, presented a token-ring based secret share update scheme. ,This scheme was established according to Ad Hoc network architecture. It included threshold update phase and update group spread phase. Threshold update phase, initiated by cluster head, can effectively avoid the conflict of more than one node initiating secret share update at the same update period. The second phase finished the secret share update of other Certification Authorities (CA) nodes by the update group, which reduced the probability of network storm. In addition, the scheme also put forward a method to tackle the conflict arising from different period secret shares; finally, simulations confirmed the effectiveness of our design.

关键词 Ad Hoc网络 簇 移动对手 密钥元更新 令牌

Key words Ad Hoc network;cluster;mobile adversary;secret share update;token

分类号

DOI:

通讯作者:
黄河 amos412328@yahoo.com.cn

作者个人主页: 黄河 王亚弟 韩继红 栗帅