电子与信息学报 2010 32 (4): 852-856 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于HuffMHT的自组织网络实体认证协议

周贤伟, 郭继文

北京科技大学信息工程学院 北京 100083

收稿日期 2009-2-13 修回日期 2009-11-22 网络版发布日期 2010-4-7 接受日期

摘要
针对自组织网络节点能量消耗和存储有限的特点，该文提出一种适合于自组织网络的基于HuffMHT的实体认证方案。该方案利用HuffMHT的思想可获得有效的安全策略；并使用对称密钥算法和公钥加密算法相结合，有效地降低了认证时延，提高了网络生命期和安全性。此外，在自组织网络设定簇头和建立HuffMHT时，该文给出了功耗最小算法和引入Christofides算法，缩短节点之间发射信号的距离，有效地降低节点能耗，提高了网络生命期。

关键词 自组织网络 网络安全 实体认证 Huffman-Merkle散列树

分类号 TP393.04

HuffMHT-Based Entity Authentication Scheme for Ad hoc Networks

Zhou Xian-wei, Guo Ji-wen

School of Information Engineering, University Science and Technology of Beijing, Beijing 100083, China

Abstract
Ad hoc Networks is characteristic of limited energy and memory. A novel entity authentication scheme based on HuffMHT for Ad hoc Networks is proposed to solve such problems. This method using the concept of HuffMHT can obtain an effective safe strategy. At the same time, symmetrical key algorithm and public key algorithm are just combined to reduce the authentication delay effectively and increase the network lifetime and enhances the security of the networks. Moreover, when clustering head and HuffMHT is built up in the Ad hoc Networks, Power-consumption-least algorithm are designed and Christofides algorithm are used in this paper, respectively, distance which notes effectively transmit signal together are reduced, the power which notes consume is debased, the network lifetime is increased.

Key words Ad hoc network Network security Entity authentication Huffman Merkle Hush Tree (HuffMHT)

DOI: 10.3724/SP.J.1146.2009.00169

通讯作者 郭继文 guojiwen@yeah.net

作者个人主页 周贤伟; 郭继文