URN etd-0407109-183710-785
Author Tsung-Fu Huang
Author's Email Address No Public.
Statistics This thesis had been viewed 58 times. Download 22 times.
Department
Year 2007
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Threshold Key Management and Signature Scheme Based on the Elliptic Curve Cryptosystem for Ad Hoc Networks
Date of Defense 0000-00-00
Page Count 80
Keyword
Ad Hoc network
Elliptic Curve Cryptosystem
Threshold Signature
Key Management
Security

Abstract
This paper proposed two scheme of digital signature and key management for ad hoc networks.One is threshold signature Scheme based on the elliptic curve cryptosystem(ECCTDS),the other is threshold key management Scheme based on the elliptic curve cryptosystem(ECCTKM).
In ECCTDS,for reduce computing cost,we selecting the certain amount of server node within the network that distribute the certificate center (CA) to the server group,and make use of lagrange interpolation polynomial with elliptic curve signature algorithm to produce and combine a partial signature.In the combine process of signature, the participant doesn't need to disclosure a private key and node after to receive a sub secret namely don't need certificate center.In ECCTKM,we detailed description the process about key generate,new member join,node sub security key refresh and system private key refresh,otherwise,we also solve security channel problem.
Advisory Committee Narn-Yih Lee - advisor

Files etd-0407109-183710-785-001.pdf

indicate access worldwide
Date of Submission 2008-07-29