

[Improving performance overhead of a trust-clustering key management protocol in ad hoc networks](#)

Authors

Mustapha Sadi, Mourad Amad, Nadjib Badache

Publication date

2020

Journal

International Journal of Electronic Security and Digital Forensics

Volume

12

Issue

2

Pages

214-228

Publisher

Inderscience Publishers (IEL)

Description

Group key management is a challenge for securing group communications in the networks. This area is well studied in the literature. The strict characteristics of mobile ad hoc networks makes the adaptation of classical existing solutions a real challenge. *Elliptic curves cryptography* (ECC) became the choice of encryption for wireless ad hoc and sensor networks. It uses very small keys and is mathematically very effective, which makes them ideal in communication for small devices used today. Scalability is a basic factor that determines the efficiency of any group key management protocol. Recent solutions for *MANETs* are oriented towards hierarchical solutions of group key agreement using clustering. Trust oriented clustering scheme is the most adequate for secure group communication. We focus in this paper on *ECC* technology and its contribution for group key agreement solutions in mobile ad hoc networks ...