DYCRASEN: A Dynamic Cryptographic Asymmetric Key Management for Sensor Network using Hash Function

Abstract

In sensor networks security is an important issue. Mission critical networks show great potential in emergency response and recovery. It is challenging to design a key management scheme to fulfill the required attributes for secure communication. The Secure Group Communication (SGC) requires common network wide key for confidentiality of control...
messages and data reports. The group key should be updated when a node enters inoperative state. Each member of a group of users can compute a common key for secure communication. We define Asymmetric key pre-distribution scheme in terms of storage. The complex encryption and decryption operations are replaced by hash functions and simple AND operations. This proposed scheme minimize the storage computation and computation cost.

Reference


Index Terms

Computer Science Security
Key words

Key Management

Sensor Network

Hash Function

Asymmetric Key