The 14th IEEE International Conference on Industrial Informatics (INDIN), 19-21 July 2016, Futuroscope-Poitiers, France

A key distribution scheme using elliptic curve cryptography in wireless sensor networks

J. Louw ; G. Niezen ; T. D. Ramotsoela ; A. M. Abu-Mahfouz

Abstract:

Wireless sensor networks (WSNs) have become increasingly popular in many applications across a broad range of fields. Securing WSNs poses unique challenges mainly due to their resource constraints. Traditional public key cryptography (PKC) for instance is considered to be too computationally expensive for direct implementation in WSNs. Elliptic curve cryptography (ECC) allows one to reach the same level of security as traditional PKC using smaller key sizes. In this paper, a key distribution protocol was designed to securely provide authenticated motes with secret system keys using ECC based cryptographic functions. The designed scheme met the minimum requirements for a key distribution scheme to be considered secure and efficient in WSNs.