عنوان مقاله:

A Scalable And Robust Communication Paradigm For Data In Wireless Sensor Networks

محل انتشار:

دومین همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1394)

تعداد صفحات اصل مقاله: 15

نویسندگان:

Shahram Khazaei Far - Department of Computer, Science and Research Branch, Islamic Azad University, Tehran, Iran

Saeid Moradi - Department of Electrical, Science and Research Branch, Islamic Azad University, Hamedan, Iran

Sajad Rezaei - Department of Computer, Malayer Branch, Islamic Azad University, Malayer, Iran

خلاصه مقاله:

Recently, secure in-network aggregation in wireless sensor networks becomes a challenge issue, there is an extensive research on this area due to the large number of applications where the sensors are deployed and the security needs. In the last few years, aggregation of encrypted data has been proposed inorder to maintain secrecy between the sensors and the sink, so the end-to-end data confidentiality is provided. However, the data integrity was not addressed. In this paper, we propose RSAED that allows integrity verification at intermediate nodes, ensures the base station to receive ciphertexts which come only from legitimate nodes and also improves the efficiency. Through implementation results, we evaluate our scheme using computation and .communication overhead

کلمات کلیدی:

Data Aggregation, Wireless Sensor Networks, Homomorphic encryption, Elliptic Curve Cryptography

لینک ثابت مقاله در پایگاه سیویلیکا: