عنوان مقاله:

An Efficient End to End Key Establishment Protocol for Wireless Sensor Networks

محل انتشار:

مجله محاسبات و امنیت, دوره 1, شماره 1 (سال: 1393)

تعداد صفحات اصل مقاله: 16

نویسندگان:

Ali Fanian - Professor Assistance in isfahan university of thecnology

Mehdi Berenjkoub - Assistance Professor in Isfahan University of Technology

خلاصه مقاله:

Sensor networks are eligible candidates for military and scientific applications such as border security and environmental monitoring. They are usually deployed in unattended or hostile environments; therefore, security is a major concern with these networks. A fundamental requirement is the capability to establish pairwise keys between sensors. Many key establishment protocols have been proposed to address the security issues in wireless sensor networks. However, most of these protocols have security and/or performance restriction. In this article, we propose a new key establishment protocol based on symmetric polynomials and random key pre-distribution. In our protocol, contrary to others, we use several symmetric polynomials to generate polynomial shares for a group of sensors, and the distribution of polynomial shares to each sensor is done using a combinatorial design. Since a limited number of shares are generated from a symmetric polynomial, the polynomial degree is very low. As a result, the common key between sensors can be generated without imposing significant overhead to them. Further, in the proposed protocol, key establishment between near sensors is provided via symmetric polynomials, while key establishment between far sensors is accomplished via random key pre-distribution. Using these two techniques simultaneously allows end to end key establishment between every pair of sensors with reasonable overhead.

کلمات کلیدی:

Wireless Sensor Networks, Key Management, Network Security, Random Key Pre-distribution, Symmetric Polynomial, Deployment Knowledge, Combinatorial Design