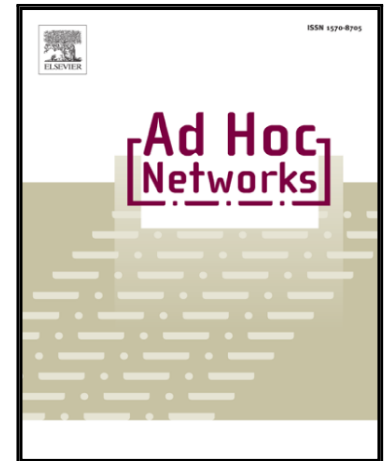


## Accepted Manuscript

Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme

Jianmin Zhang , Hua Li , Jian Li

PII: S1570-8705(17)30225-1  
DOI: [10.1016/j.adhoc.2017.12.006](https://doi.org/10.1016/j.adhoc.2017.12.006)  
Reference: ADHOC 1619



To appear in: *Ad Hoc Networks*

Received date: 5 April 2017  
Revised date: 8 November 2017  
Accepted date: 20 December 2017

Please cite this article as: Jianmin Zhang , Hua Li , Jian Li , Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme, *Ad Hoc Networks* (2017), doi: [10.1016/j.adhoc.2017.12.006](https://doi.org/10.1016/j.adhoc.2017.12.006)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

# Key Establishment Scheme for Wireless Sensor Networks Based on Polynomial and Random Key Predistribution Scheme

Jianmin Zhang , Hua Li, Jian Li

School of Computer, Henan Institute of Engineering, Zhengzhou 451191, China

Corresponding author: Jianmin Zhang

Email :zjm7008@163.com

Tel :86-15515692603

**Abstract:** Establishing communication keys for pairs of neighbouring sensor nodes is the foundation of the security in wireless sensor networks (WSNs). However, due to the resource constraints on nodes, this task is challenging for the constrained memory, energy, and computational capabilities of sensor nodes. This paper proposes a novel key predistribution scheme based on the polynomial pool-based key predistribution scheme and random key predistribution. In the proposed scheme, parts of the preloaded information in each sensor node are the polynomial shares and the rest of the preloaded information are the keys generated by the polynomial shares preloaded in the sensor nodes. Performance analyses and comparisons with other schemes are performed in this paper. The comparison of security results confirm that the proposed scheme has better resilience against node compromising attacks when compared to previous schemes.

**Keywords:** Wireless sensor network, security, key predistribution, polynomial-based key predistribution

## 1. Introduction

Wireless sensor networks (WSNs) usually include battery-powered sensor nodes that are deployed in a designed area to sense and collect information [1]. That information is transmitted by sensor nodes to the sink node where it is aggregated [2]. The applications of WSNs include environmental monitoring, health care, battlefield targeting and surveillance, and disaster relief networks [3,4]. However, WSNs are usually subject to many security threats and attacks such as impersonation, intentionally providing false information, eavesdropping, data modification, and sensor node capture attacks.

Confidentiality, authenticity, availability, and integrity are typical security goals of WSNs [5]. As the basic requirement for providing security functionality, key management is an important fundamental security service that enables sensor nodes to securely communicate with each other using cryptographic techniques [6]. The prime problem in key management is the establishment of a secure key shared between two communicating sensor nodes [7]. Meanwhile, inherent constraints of computational power, memory capability, and bandwidth make the direct use of traditional pairwise key establishment algorithms (such as public key

Download English Version:

<https://daneshyari.com/en/article/6878588>

Download Persian Version:

<https://daneshyari.com/article/6878588>

[Daneshyari.com](https://daneshyari.com)